



# 本資料について

---

本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください

- 題目: 802.11セキュア無線LANガイドブック
- 監修: 村上満雄
- 著者: 大水祐一
- 発行: 平成16年10月1日
- 発行所: 電気通信協会
- 発行元: オーム社
- ページ数: 235ページ



# 無線LANの技術と発展

---

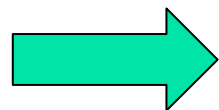
040430703 永井順也



# 1.無線LAN導入の必要性

---

- 配線に関する問題
  - 物理的問題
  - コストの問題
  - 景観・環境の問題
- 端末移動に関する要望
  - いつでもどこでもPCを持ち歩き、システムにアクセスしながら使いたい



無線LANの導入で解決



## 2.1 さまざまな無線技術

---

無線PAN

1. PHS (Personal Handy-phone System)
2. Bluetooth
3. UWB (Ultra Wide Band)
4. IrDA
5. 無線LAN

## 2.1さまざまな無線技術

通信技術	無線LAN技術				PHS	無線PAN技術		
	IEEE802.11a	IEEE802.11b	IEEE802.11g	HiSWAN a		Bluetooth	UWB	IrDA
周波数帯	5.2GHz帯	2.4GHz帯		5.2GHz帯	1.9GHz帯	2.4GHz帯	数GHz以上	赤外線
伝送速度	54Mbps	11Mbps	54Mbps	36Mbps	64/32kbps	1Mbps	100Mbps	16/4/1Mbps 115Kbps
通信距離	数10m	約100m		数10m	100-数100m	10m	約10m	1m
変調方式	OFDM	DS	OFDM,DS	OFDM	QPSK	FH		IrDA
アクセス制御	CSMA/CA			TDD/TDMA	PIAFS	なし		
接続端末	PC	PC,PDA	PC	PC	電話機,PC,PDA	PC,PDA,周辺機器,情報家電		
モビリティ	静止～歩行程度			静止～歩行程度	静止～歩行程度	静止		
ハンドオーバ	あり			あり	あり	なし		



## 2.2無線LANの歴史

---

### 黎明期1

1993年 無線LAN登場

高い(50万)・遅い(1Mbps程度)・かさばる(タバコ箱サイズの外部アンテナ)

1997年 IEEE802.11標準化

標準化しても他社同士つながらず

さらに、電波法の関係で無線LANが使える

周波数帯域が限られていたためいろいろな制限があった



## 2.2無線LANの歴史

---

### 黎明期2

1999年 電波法改正

IEEE802.11b登場

使える周波数帯が増え高速化(11Mbps)

Wi-FiAlliance設立

製品間の接続性アップ

2000年 メルコ(バッファロー) Apple参入

価格破壊 AirMac (アンテナの小型化)



## 2.2無線LANの歴史

---

- 2001年 IEEE802.11a  
5GHz帯使用(54Mbps)
- 2003年 IEEE802.11g  
bと後方互換(54Mbps)  
市場の主流
- 200X年 IEEE802.11n  
実行通信速度100Mbps



## 3.1 無線LANの装置

### 1. アクセスポイント



無線LANの基地局・LANのノードとしてみるとブリッジの役割

家庭・SOHO向け

ブロードバンドルータやスイッチングハブと一体化

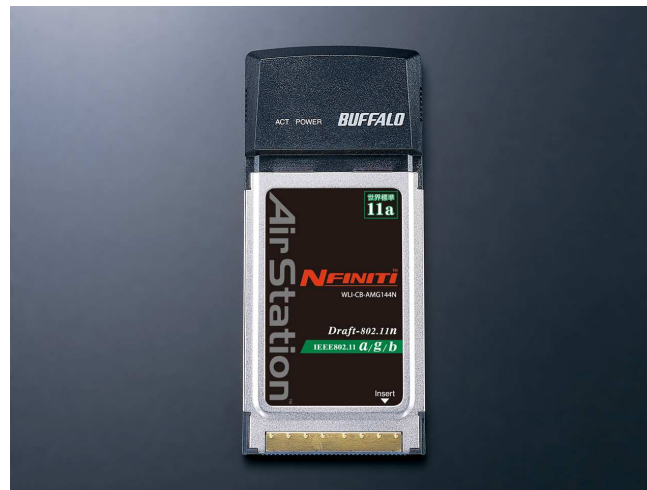
値段：1万円前後と安価

企業向け

ブリッジ＋高度な運用を行うためのさまざまな機能＋セキュリティ

## 3.1 無線LANの装置

2. クライアントアダプタ  
無線LANの機能を端末に持たせるためのアダプタ  
PCカード型やノートPC内蔵型がある

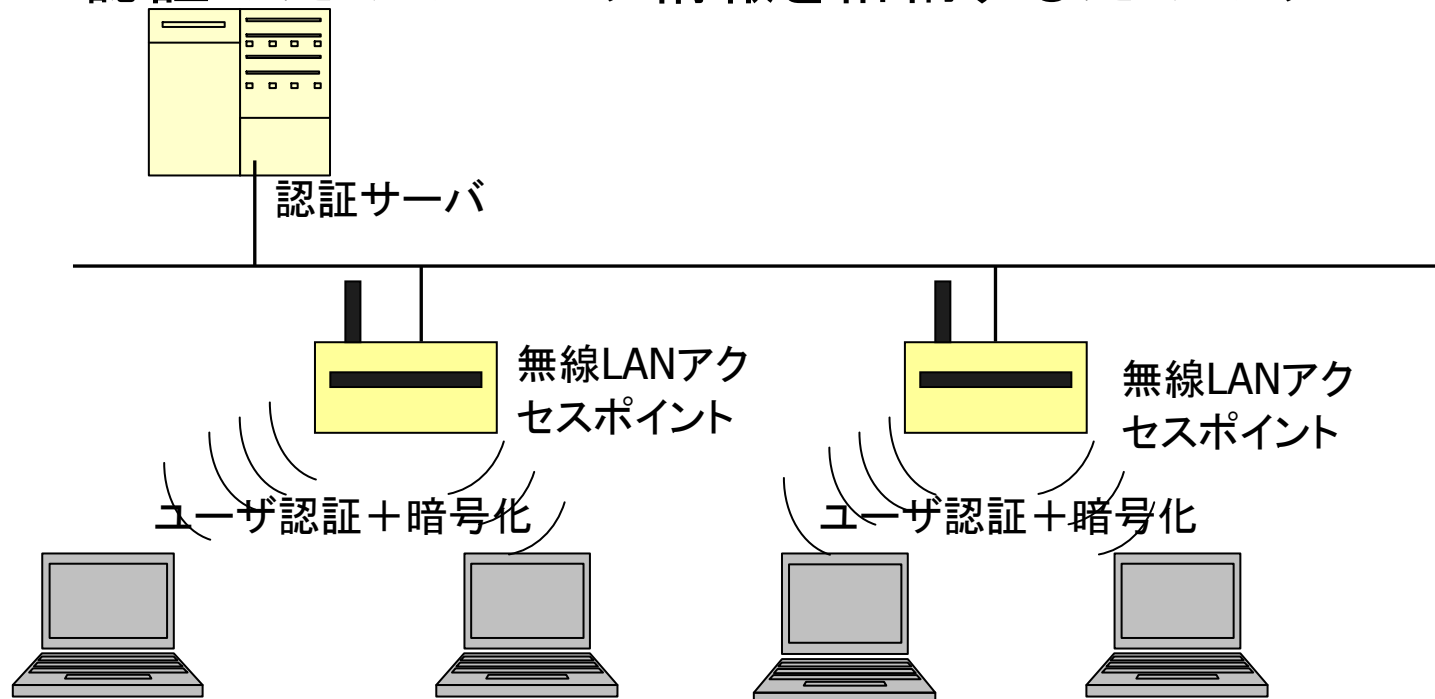


## 3.1 無線LANの装置

### 3. 認証サーバ(RADIUS認証サーバ)

アクセスポイントが複数あるときに必要

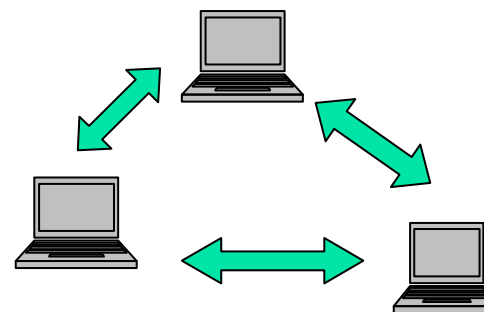
認証のためのユーザ情報を格納するためのサーバ



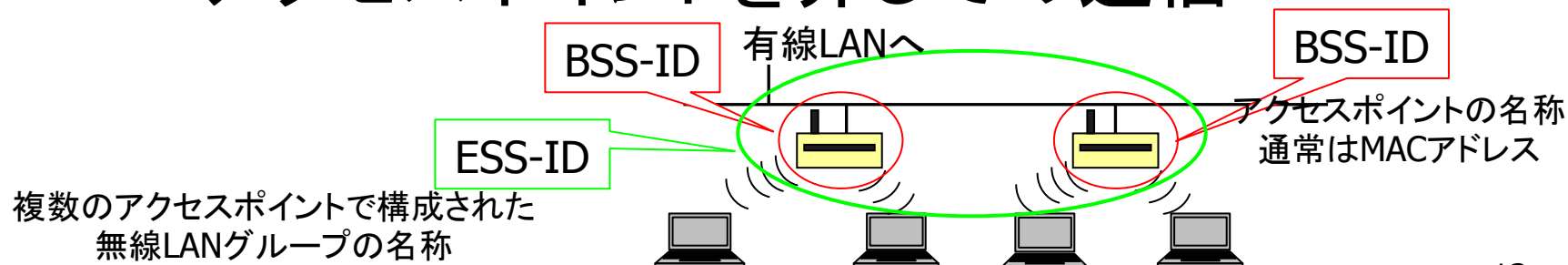
## 3.2 無線LANのネットワーク構成

### 無線LANのネットワークモード

1. アドホックモード  
端末同士での通信

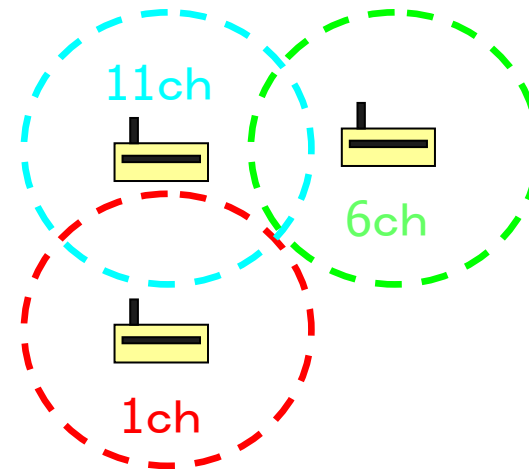


2. インフラストラクチャモード  
アクセスポイントを介しての通信

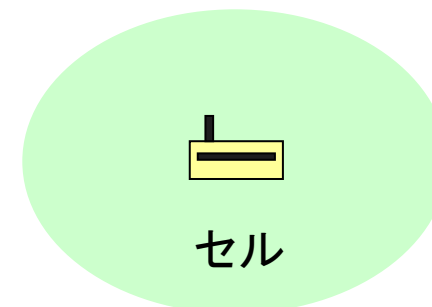


## 3.2 無線LANのネットワーク構成

- チャンネル  
周波数の割り当て  
あらかじめ波の重複を避ける形で割り当てが行われている



- セル  
無線の届く範囲  
図では簡略化のため円にしているが、実際は障害物などの関係で変化し、不定形



## 3.3無線LANを構成する技術

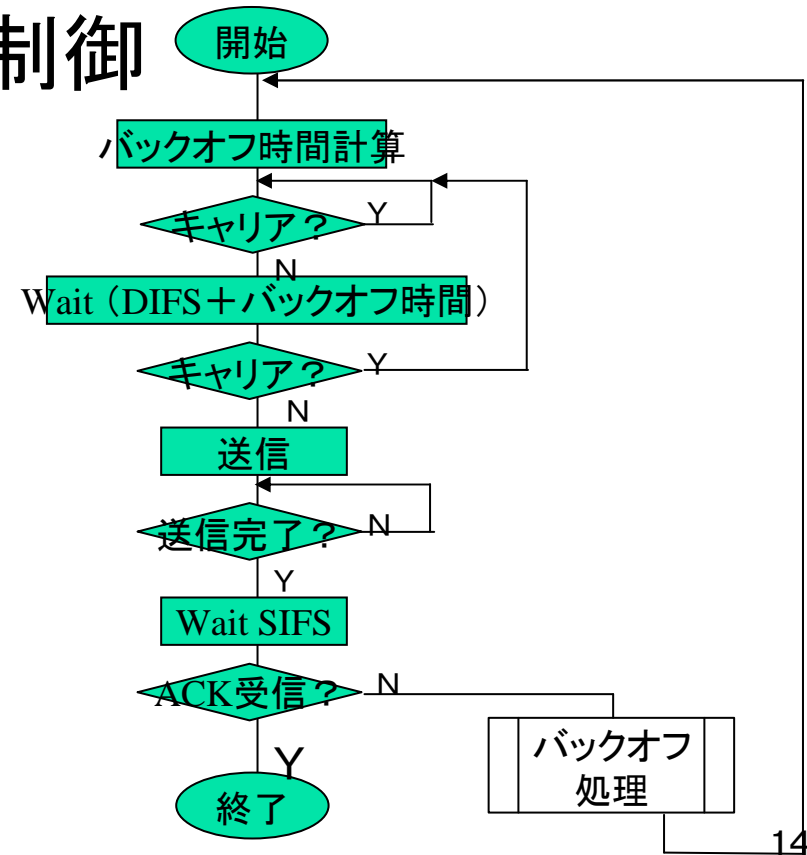
- CSMA/CA方式

IEEE802.11のアクセス制御

無線LANは電波の衝突を検地できない

→衝突を回避する方式

CSMA/CA方式のアルゴリズム  
(情報ネットワーク論より)

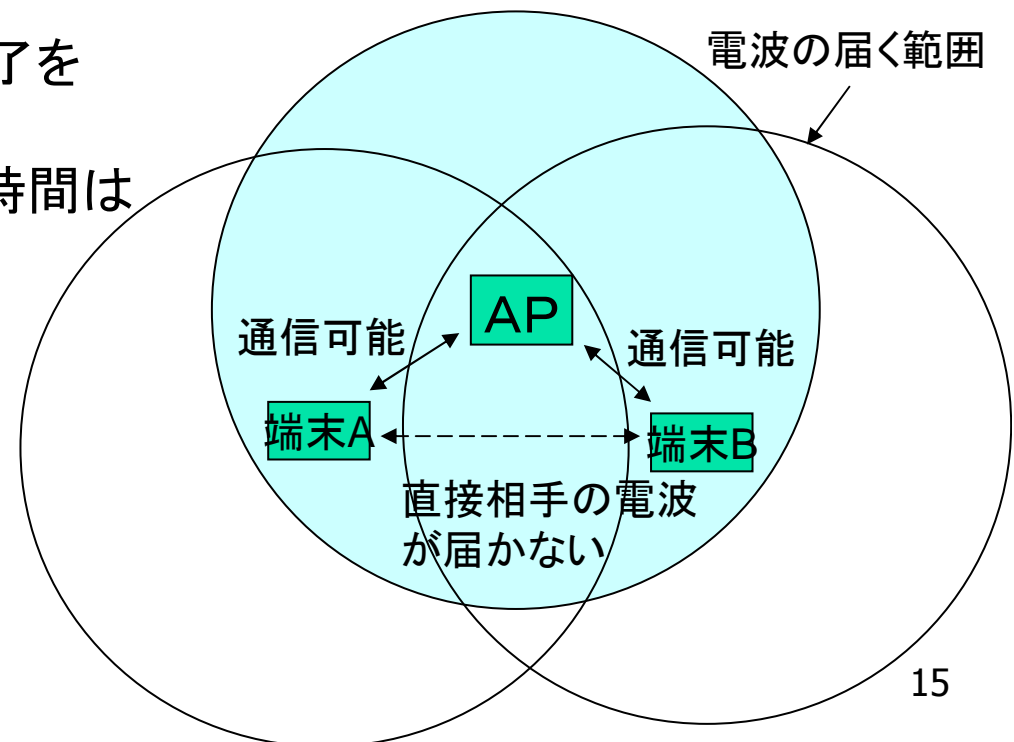


## 3.3無線LANを構成する技術

### ■ RTS/CTS方式

「隠れ端末問題」に対応するため  
端末AはRTSでアクセスポイントに  
送信時間を予約  
アクセスポイントはCTSで予約完了を  
全端末に通知する  
ほかの端末は端末Aが予約した時間は  
情報を送信しない  
よって、衝突を回避できる

### 隠れ端末問題



## 3.3無線LANを構成する技術

### ■ IEEE802.11のフレーム構成



同期信号のビット列  
到来するフレームを検出し、  
同期を取るのに必要な部分

伝送速度やデータ長  
に関する部分



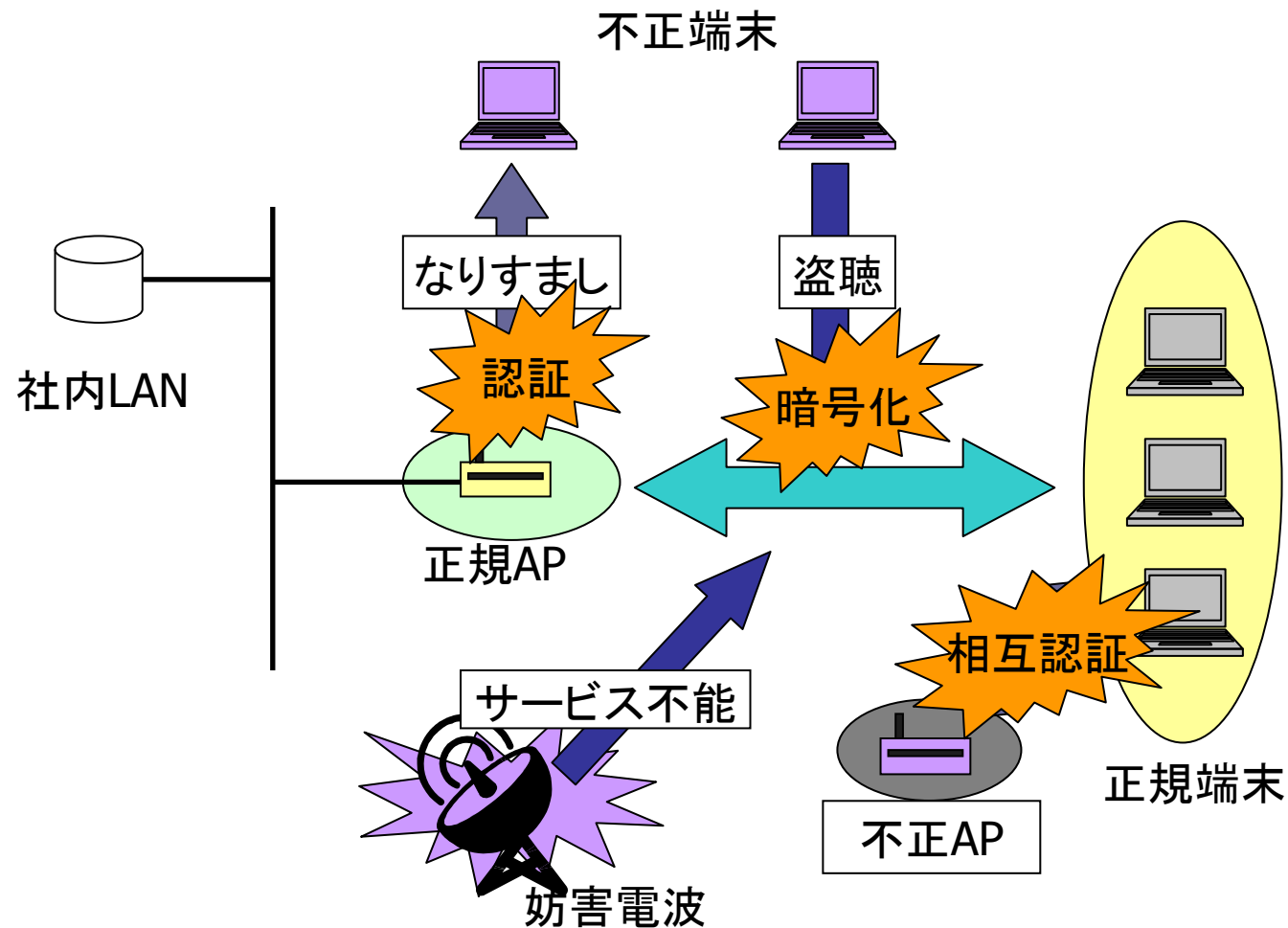


## 3.3無線LANを構成する技術

---

- 無線LANの標準的な設定項目(セキュリティ)
  1. **ESS-ID(Extended Service Set ID)**  
複数のアクセスポイントで構成された無線LANグループの名称
  2. **MACアドレス認証**  
クライアントアダプタのMACアドレスを登録することで、登録外のMACアドレスのクライアントアダプタからの接続を拒否できる。
  3. **WEP(Wired Equivalent Privacy)**  
キー長64bit(5文字or10桁の数字)と128bit(13文字or26桁の数字)がある  
端末に手作業で逐一設定(IEEE802.1xを使えば自動)

# 4.1 無線LANをとりまく脅威





## 4.2標準セキュリティの脆弱性

- **ESS-ID**  
定期的に周囲に送信しているので ×
- **MACアドレス認証**  
無線LANのフレームに平文で乗っている

PLCPプリアンプル	PLCPヘッダ	MACヘッダ	データ部分
------------	---------	--------	-------

さらに、クライアントのMACアドレスは書き換え可能な  
ので ×

- **WEP**  
脆弱性あり。辞書攻撃や総当り攻撃に弱いので ×

# 5.WPA , IEEE802.1xによる セキュア無線LAN

- **WPA** (Wi-Fi Protected Access)  
WEPに変わる新しい無線LANの暗号化方式  
2004年7月 新暗号アルゴリズムAES対応  
強固な暗号化が可能に  
また、RADIUS認証サーバを使った認証方式  
(**IEEE802.1x**)がオプションとして付け加えられた
- IEEE802.1x  
RADIUS認証サーバを用いることで端末とアクセスポイントの相互認証を実現



## 6.1 公衆無線LANの活用

- **公衆無線LANサービス**  
無線LAN技術を用い、公衆空間においてインターネットに接続する通信業者のサービス
- 1. **スポット型**  
人の集まる空間(ファーストフード店や駅)に局所的に配置
- 2. **屋外展開型**  
特定の街区などある一定の範囲で無線LANのアクセスポイントを配置
- 3. **固定型**  
戸建やマンションの近くまで有線でインフラを引きそこから無線LANでサービスを提供



## 6.2 公衆無線LANの実用化例

---

- **FREE SPOT**

無料 アクセス制限・ユーザ認証なし  
セキュリティ対策は任意  
不正アクセスポイントや盗聴・踏み台攻撃  
に利用されることも

- **ホットスポット**

有料 会員制  
IEEE802.1x認証などセキュリティ対策あり



## 7. 無線LANのさらなる発展

---

- 認証VLAN  
有線・無線の認証方式を統合することで  
セキュリティ強化
- 無線LANスイッチ  
コントローラに機能集中、無線環境を統合制御
- ワイヤレスVoIP  
無線LANの上で通話
- 5GHZ帯の周波数解禁  
現行4チャンネルから18チャンネルへ