はじめに

- 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設計ガイドブック

著者：大水祐一

発効日：平成16年10月1日

発売元：オーム社

セキュア無線LAN

渡邊研究室

050428027　後藤秀暢

ユビキタスオフィス

「いつでもどこでも」 「セキュアに」 「快適に」
仕事ができる環境

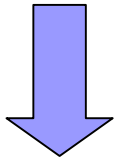
具体的に・・・
オフィスの内外を問わずにどこにいても、あたかも自席にいるときと変わらず仕事が出来る環境を実現したオフィス

■ ユビキタスオフィスで実現されるビジネス環境

・「いつでもどこでも仕事ができる」
・「ブロードバンドで仕事が快適」
・「柔軟にITにアクセス、組織を活性化」
・「高い信頼性とセキュリティ」

ユビキタスオフィスと無線LAN

ユビキタスオフィスを実現するための
本命インフラ技術



無線LAN
(イーサネットをワイヤレスで伝送する技術)

なぜ無線LANが必要なのか

配線に関わる問題

・配管がいっぱい/二重床工事不可で
新規配線ができない
・景観上や環境上の問題で配線工事ができない
・コストがかかりすぎる

端末移動に関する要望

・広い敷地内でPCやPDAを持ち歩き、
システムにアクセスしながら使いたい

学校

・学校インターネット
・情報教室

工場・倉庫

・構内を移動しながら使用

庁舎等

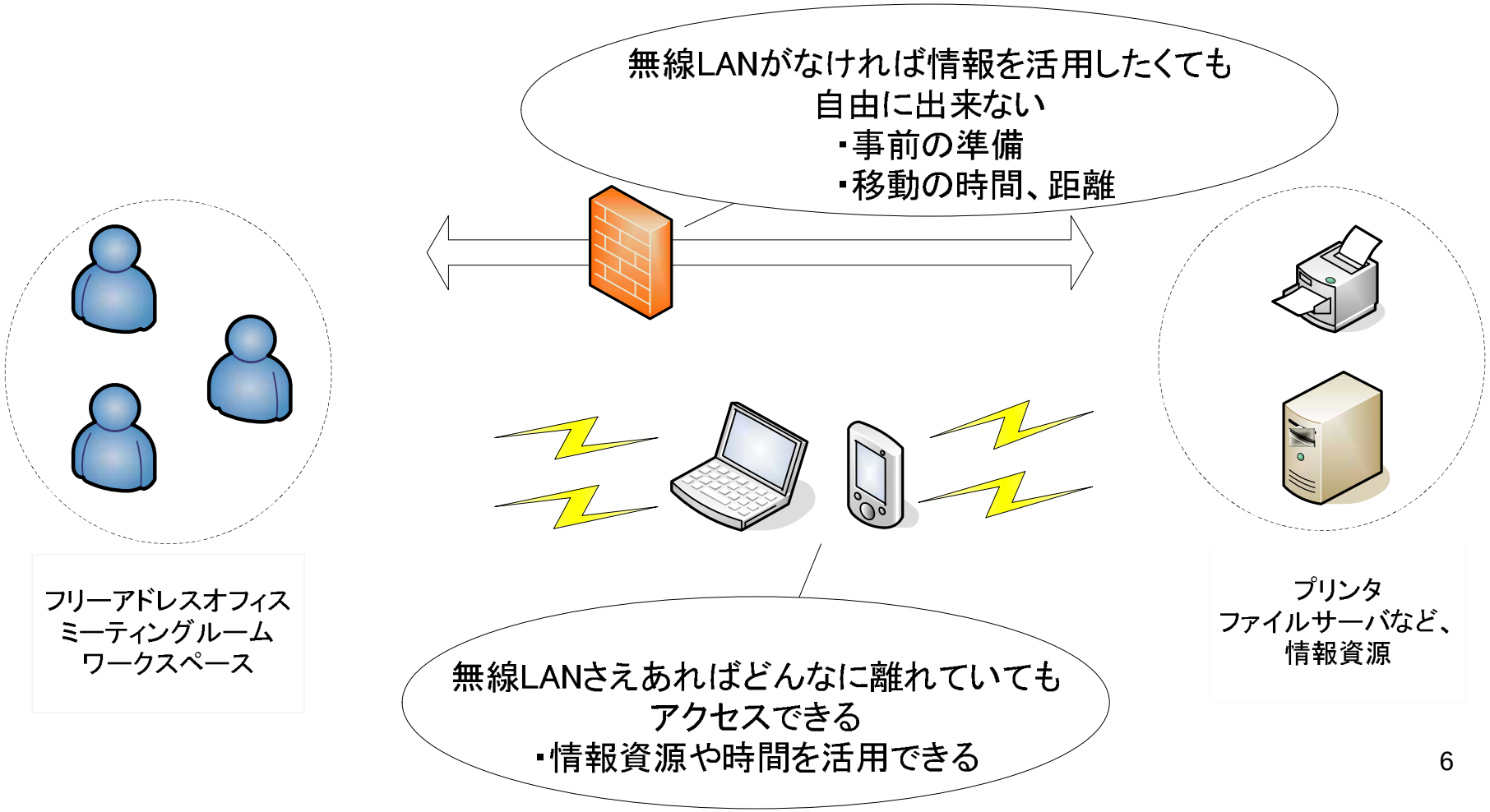
・建物が古い
・配管を行う余地がない

店舗

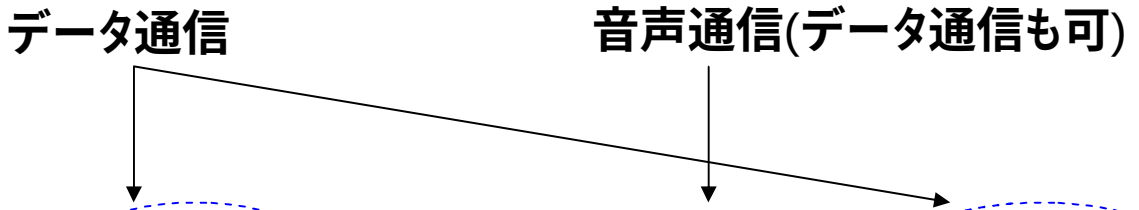
・移動しながらPOS業務に使いたい

無線LANのあるオフィス

無駄なコストを削減し、業務効率アップ！！



さまざまな無線通信技術



通信技術	無線LAN技術				PHS	無線PAN技術	
	IEEE802.11a	IEEE802.11b	IEEE802.11g	HiSWAN a		Bluetooth	IrDA
周波数帯	5.2GHz帯	2.4Ghz帯		5.2GHz帯	1.9Ghz帯	2.4Ghz帯	赤外線
伝送速度	54Mbps	11Mbps	54Mbps	36Mbps	64/32Kbps	1Mbps	16/4/1Mbps 115Kbps
通信距離	数10m	約100m		数10m	100-数100m	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～歩行制度	静止	静止
ハンドオーバー	あり			あり	あり	なし	なし

無線PAN技術

- PAN (Personal Area Network)**とは・・・**

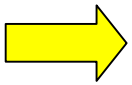
・データ通信に向けた技術

・携帯機器やPCと周辺機器を接続する形態

・LANより小規模、近距離での接続形態

- PAN**向けの無線技術**

・Bluetooth
・UWB



電波による通信

・IrDA

赤外線による通信

さまざまな無線LAN技術

主流の規格

分類	IEEE802.11			HiSWAN a	FH方式無線LAN	19GHz無線LAN	赤外線無線LAN
通信技術	IEEE802.11a	IEEE802.11b	IEEE802.11g				
周波数帯	5.2GHz帯	2.4GHz帯		5.2GHz帯	2.4GHz帯	19GHz帯	赤外線
最大伝送速度	54Mbps	11Mbps	54Mbps	36Mbps	1.6～3Mbps	25Mbps	10/100Mbps
通信距離	数10m	約100m		数10m	数10m	15m	数m
変調方式	OFDM	DS	OFDM,DS	OFDM	FH	ー	輝度変調
アクセス制御	CSMA/CA			TDD/TDMA	CSMA/CA	ー	CSMA/CA

IEEE802.11 a/b/g

- IEEE802.11**とは・・・**

  IEEE802委員会において無線LAN技術の標準規格を検討するためのワーキンググループ

IEEE802.11b

- 周波数：2.4Ghz帯
- 変調方式：スペクトラム拡散
- 11/5.5/2Mbps
- 屋外利用可能
- 標準化：1999年
  製品登録：1999年
- 既に成熟、価格低兼

高速化

IEEE802.11a

- 周波数：5.2Ghz帯
- 変調方式：OFDM
- 54/48/36/24/18/12/9/6Mbps
- 屋外利用不可
- 標準化：1999年
  製品登録：2001年
- 802.11bと非互換

IEEE802.11g

- 周波数：2.4Ghz帯
- 変調方式：OFDM+DS
- 54/48/36/24/18/12/9/6Mbpsほか
- 屋外利用可能
- 標準化：2003年
  製品登録：2003年
- 802.11bと後方互換性
- 市場の主流

IEEE802.11a/b/gは物理層の違い　アクセス制御やセキュリティなどは共通

無線LAN規格活用のポイント１

IEEE802.11a/b/gをどう使い分ければよいか

- **高速性が必要なら** ⇒ IEEE802.11a/g

  :**最大伝送速度**52Mbps**の**a**と**g

- **他システムとの干渉** ⇒ IEEE802.11a

  :2.4GHz**帯は他システムとの電波干渉がある**

- **屋外利用するなら** ⇒ IEEE802.11b/g

  :5.2GHz**帯は使用が屋根のある空間に限定**

- **価格** ⇒ IEEE802.11g

  :**家庭用無線**LAN**向き**

無線LAN規格活用のポイント２

2.4GHz帯無線LANの干渉源となるもの

干渉源	概要
構内無線局 （移動体識別用）	最大300mW 2,440MHz,2450MHz,2455MHzを使用 2.427～2470.5MHzの周波数ホッピング方式もある
特定小電力無線	最大10mW インターホンやトランシーバーなど
アマチュア無線局	最大2W 2,400～2,450MHzを使用
電子レンジ	家庭用は500～600W, 業務用は1,500W 2,450MHzを使用
マイクロ波治療器	家庭用は200～600W 2,450MHzを使用
Bluetooth	最大10mW 2,400～2483.5MHz

無線LANを構成する装置

- **アクセスポイント**

無線LANの基地局、APとも呼ばれる
無線LANのネットワークを構成する軸となる機器

- **家庭・SOHO向け製品**
  - **スイッチングハブ、ルータ、DHCPサーバ、簡易ファイアウォール**
    などの機能が提供
  - **必要な機能が備わっていて価格が安い**
- **企業向け製品**
  - **基本的にはブリッジの機能のみ搭載**
  - **アクセスログをとる機能、送信電力機能などの制御機能…etc**
    などの高度な機能を持つ
  - **セキュリティ機能が充実**

無線LANを構成する装置 2

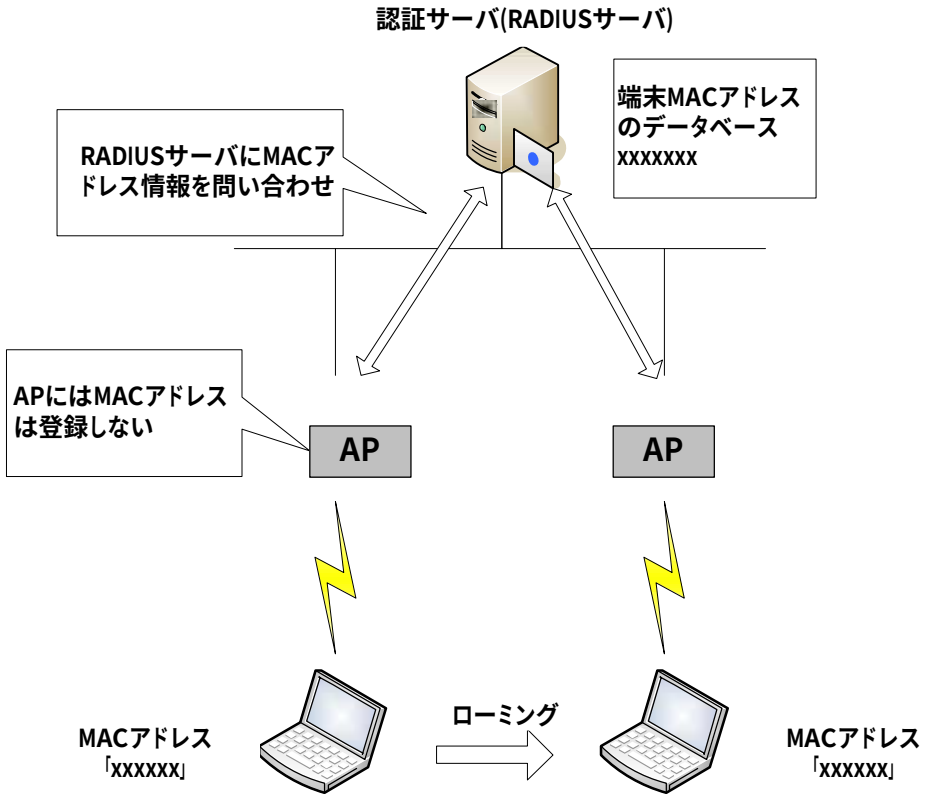
- **クライアントアダプタ**
  - 無線LANの機能を端末にもたせるためのアダプタ
  - ノートPC向けに、PCカード形態で提供されるのが一般
  - クライアントアダプタを内蔵したノートPCもある

無線LANカードとも呼ばれる

- **無線LANドライバ**
  - クライアントアダプタを動作させるドライバ・ソフトウェア

無線LANを構成する装置 3

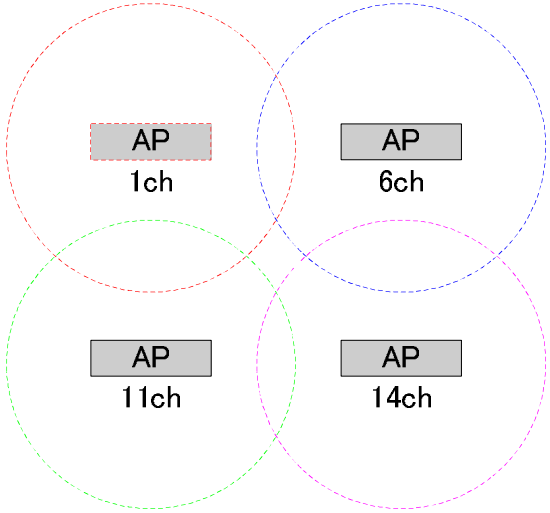
- **認証サーバ**
  - 認証のためのユーザ情報を格納するサーバ
  - 端末のMACアドレスなど保存



セルとチャンネル

・アクセスポイントには、使用する無線LANのチャンネルを設定する
・アクセスポイントから電波の届く範囲をセルと呼ぶ

	設定可能チャンネル	最大チャンネル数
IEEE802.11a	-	34,38,42,46 (4チャンネル)
IEEE802.11b	1～14	1,6,11,14 (4チャンネル)
IEEE802.11g	1～13	1,6,11 (3チャンネル)



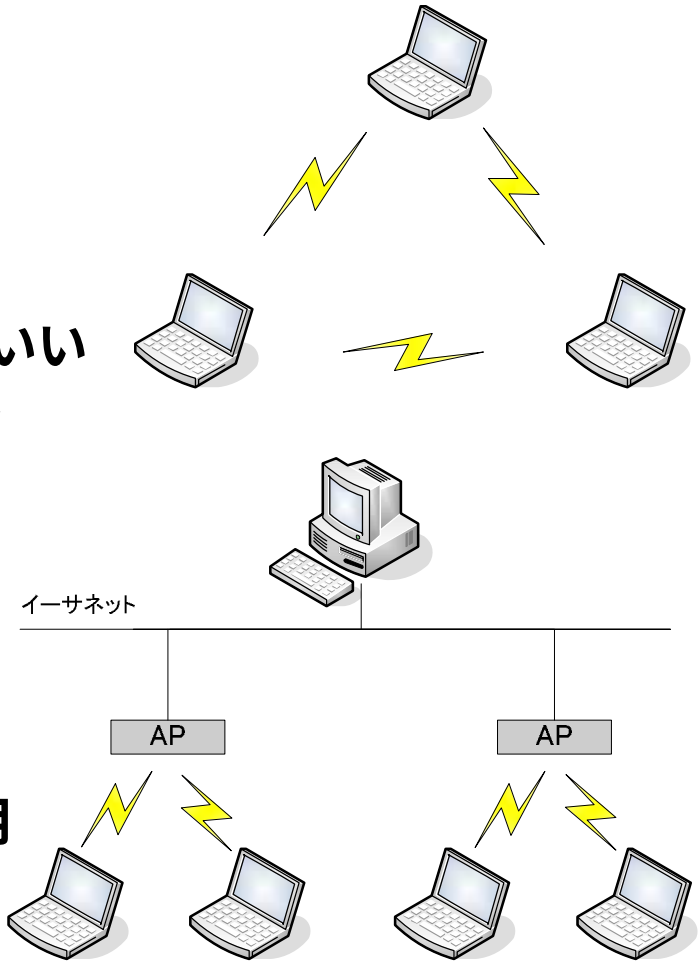
IEEE802.11b

セルについて・・・

・実際のセルは円ではなく、雲のように広がっている
・セルの範囲は、周囲の環境で変化し、不安定

無線LANのネットワークモード

- アドホックモード
  - 無線LAN端末同士が直接通信をする形態
  - 電波の通じる近隣の範囲に設置
  - ESS-IDとチャンネルの設定を一致させるだけでいい
  - インターネットに接続しない小規模なネットワーク
  - ほとんど使わない
- 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通信する形態
  - アクセスポイントがアクセス制御
  - ブロードバンド回線を通してインターネットを利用
  - 一般的な形態

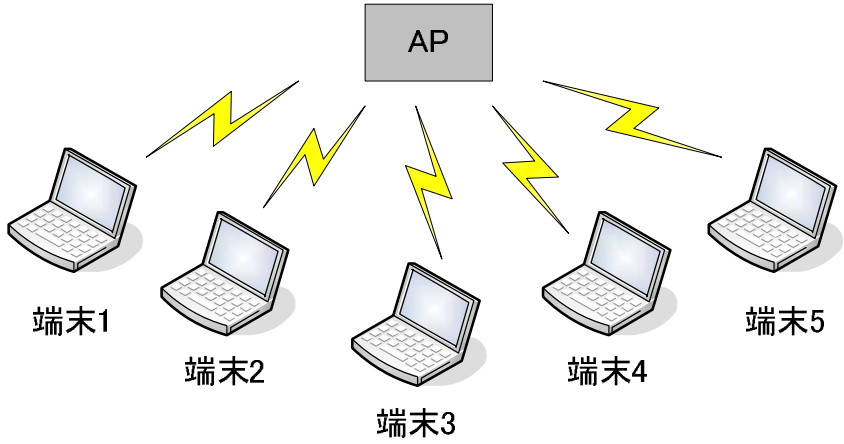


CSMA/CA方式

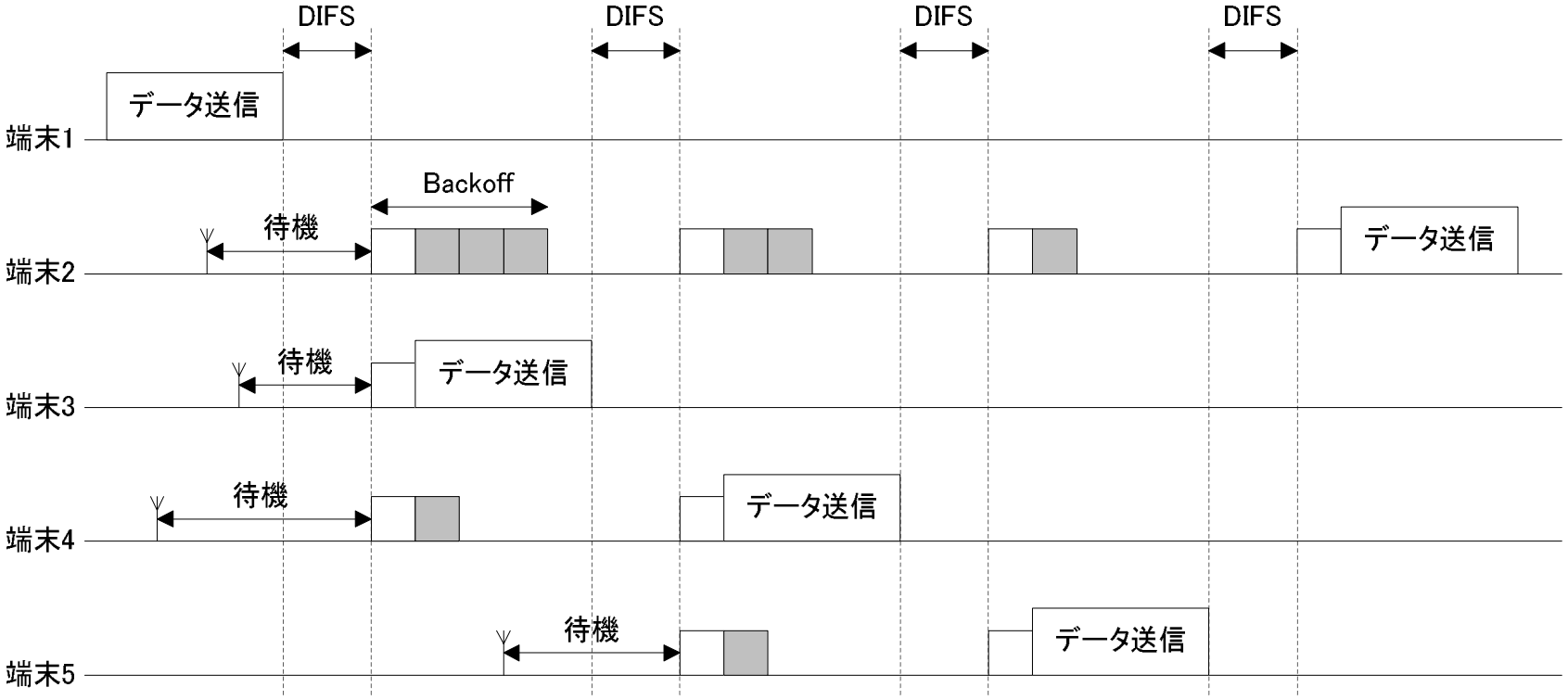
- **搬送波感知多重アクセス･衝突回避方式**

(Carrier Sense Multiple Access with Collision Avoidance)

- **各ノードが随時キャリアセンスを行い、チャンネルがある程度開いていることを確認してから、送信を行なう無線LANのアクセス制御方式**
- **無線上では衝突を“検知”できないので、このようなしくみで衝突を“回避”している**
- **フレーム送信が成功したかは、受信側の端末からACK信号が到達することで判断**



CSMA/CA方式の概要

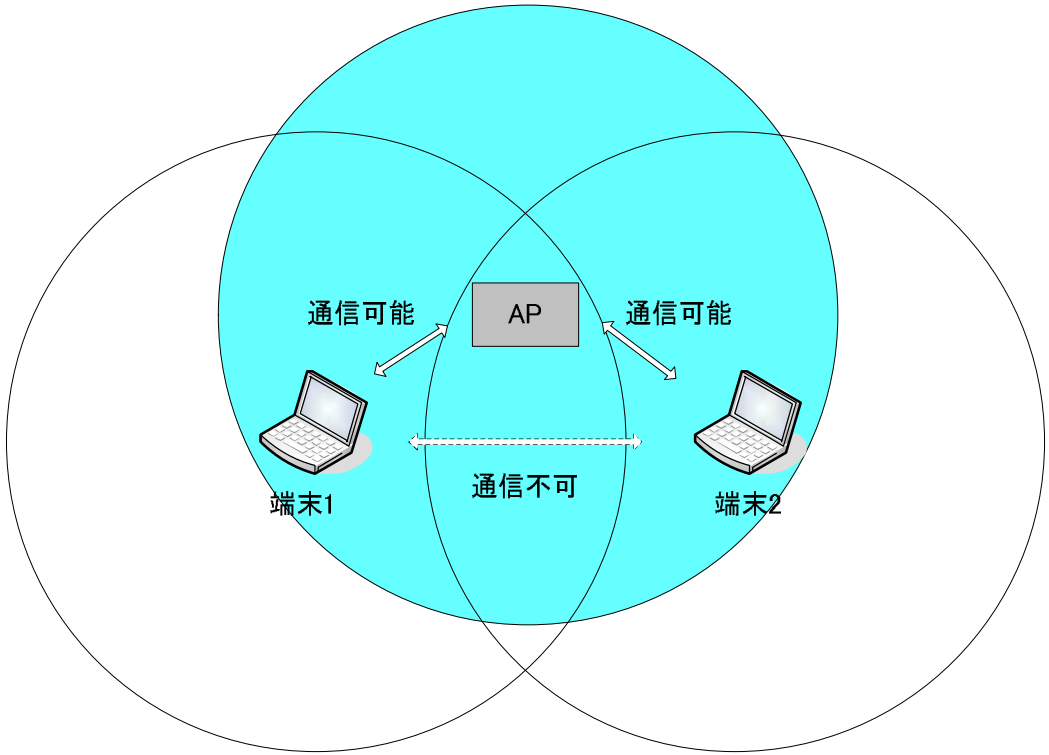


CSMA/CA方式による送信制御の概要
- 待ち時間をランダムな数値として設定、単位時間ごとにキャリアセンスを行い、誰も送信していない状態であれば待ち時間を1減らし、0になったら送信する。
- 上図では、端末2は待ち時間4、端末3は待ち時間1、端末4は待ち時間2を設定し、待ち時間0になったら端末3が送信、次に端末4が送信している。
- 待ち時間中に他の端末が送信したら、待ち時間は次の送信時に持ち越される。

DIFSは無通信状態と判断するまでの時間

隠れ端末問題

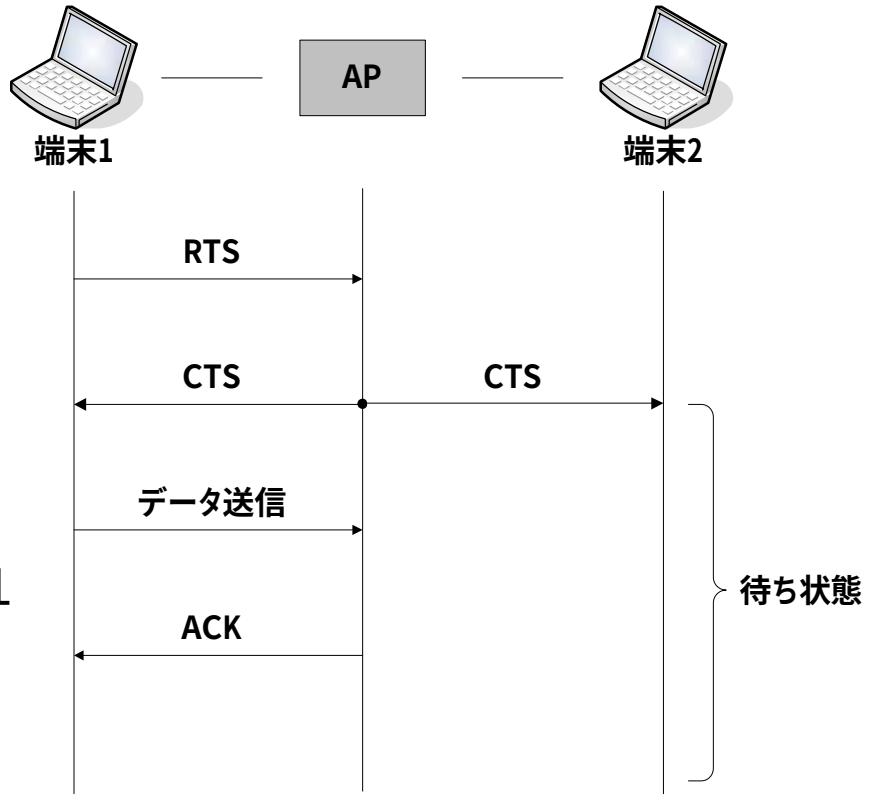
- 端末1と端末2が離れていて、各端末が互いのキャリアを検出できない状態が「隠れ端末問題」
- アクセスポイントから各端末への送信は問題ないが、端末からアクセスポイントへの送信では、端末1が送信中に端末2がそのキャリアを検出できないために送信する可能性がある。その結果衝突が発生しデータが破壊される



RTS/CTS方式

隠れ端末問題への対策が
RTS/CTS**方式**
・RTS (Request To Send) ：**送信要求**
・CTS (Clear To Send) :**受信準備完了**

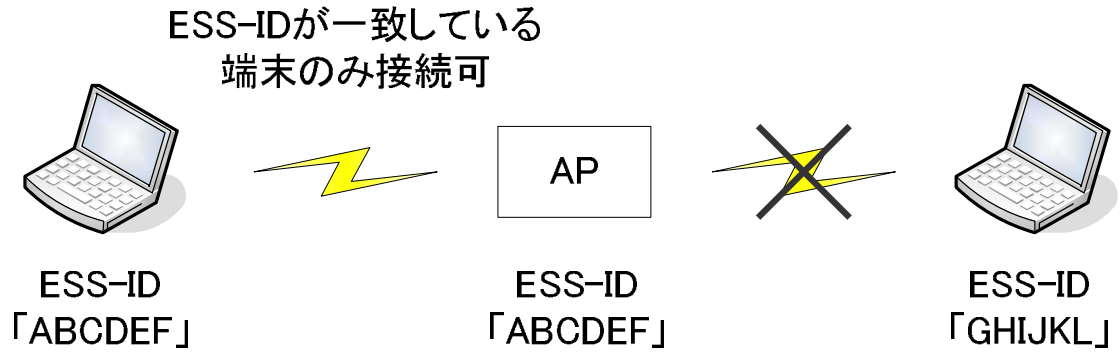
1.**端末1が送信にあたる場合、**RTSを
　APに送信
2.APはCTSとしてすべての端末に送信
3.**端末2はCTSを受け取ることで、端末1
　が送信することを知る**
4.**端末1はデータ送信できる**



無線LANの標準的な設定項目 1

- ESS-ID (Extended Service Set ID)

・所属する無線LANのグループを指定する設定
・アクセスポイントや端末など、無線LANのシステムを構成する
　全てのノードに設定
・IDは任意の文字列
・同じIDを設定したノード同士が、同じ無線LANのグループとして動作
・IDが異なれば通信は成り立たない
・無線LANのグループの識別子の役割



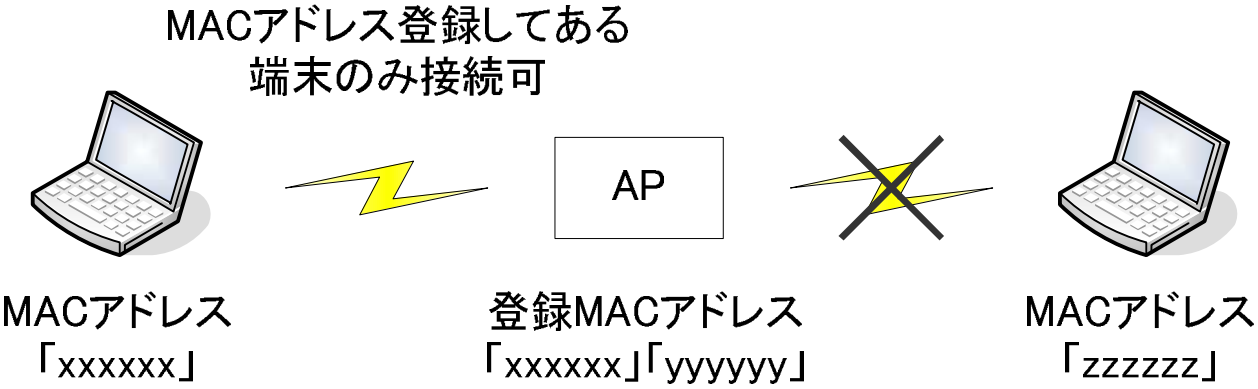
無線LANの標準的な設定項目 2

- **MACアドレス認証**

MACアドレスを端末を識別するための情報として、端末認証を行なうこと

- **MACアドレス認証を行なう場合**

・クライアントアダプタのMACアドレスをアクセスポイントに登録
・登録外のMACアドレスの接続を停止できる
・大規模のネットワークの場合はMACアドレス認証に認証サーバが用いられる

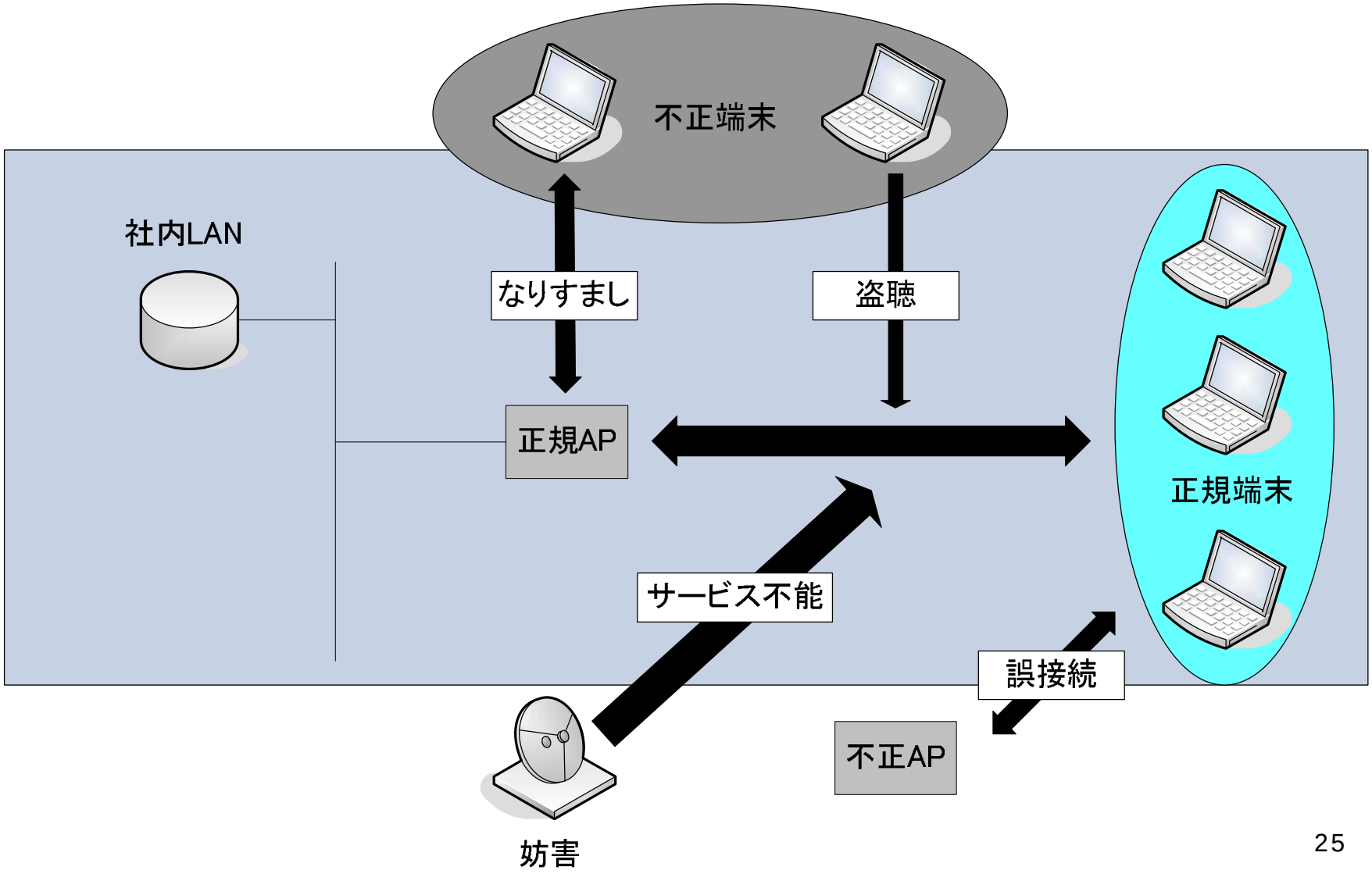


無線LANの標準的な設定項目 3

- WEP (Wired Equivalent Privacy): **有線と同等のプライバシー**
  - **送信されるパケットを暗号化して傍受者に内容を知られないようにすること**
  - 64bitと128bit**の二つのタイプがある**
  - **同じ**WEP**のキーを持つノード同士で暗号化・複合化**
  - **同じ**ESS-ID**を設定するノードなら同じ**WEP**のキーを設定することになる**

- **ＷＥＰの設定**
  - **システム担当者又はユーザが固定のキーを無線**LAN**のノードに設定**
  - 64bit**はキャラクタで設定する場合**5**文字、**16**進数なら**10**桁のキー設定**
  - 128bit**はキャラクタなら**13**文字、**16**進数なら**26**桁のキー設定**
  - **一般的に**WEP**のキーは手作業で設定する**

無線LANをとりまく脅威 1



無線LANをとりまく脅威 2

盗聴

- **盗聴とは・・・**
  - 無線を伝送媒体として使用する以上、セルの範囲を厳密に規定することは困難で、電波が屋外に漏洩する
  - 盗聴可能範囲に潜む第三者に通信内容が傍受され、情報が漏洩

- **対策**
  - 「暗号化」の機能を適切な方式で実装する

具体的に・・・

- 暗号化の強度が一般的に解読できないレベルであること
- 暗号化が施される区間において隙間を生じさせない

無線LANをとりまく脅威 3

なりすまし

- なりすましとは・・・
  - 正規の端末になりすまし、ネットワークに侵入を試みること
  - 進入後に社内サーバのデータ改ざんや、そこから他のインターネット上のサーバに向けたクラッキングが行なわれる (踏み台攻撃)

- 対策
  - 「認証」の機能を適切な方式で実装する

具体的に・・・

  - 認証のために使うユーザの資格情報が、傍受されない形でやりとりする

無線LANをとりまく脅威 4

不正アクセスポイントへの接続

- 不正アクセスポイントへの接続とは・・・
  - 偽の無線LANのネットワークを作り、端末を誤接続させる
  - 誤接続した端末からデータを取り出す
  - 端末に対する破壊工作を行なう

- 対策
  - アクセスポイントが端末を認証するだけでなく、端末もアクセスポイントの正当化を認証する、「相互認証」の機能を実装する

相互認証　：一定の基準を満たした認証機関同士が，お互いの認証機関の公開鍵を証明し合うもの

無線LANをとりまく脅威 5

サービス不能攻撃

- **サービス不能攻撃とは・・・**
  - 無線に対して強力な妨害電波を送信すれば、通信不能の状況を作れる
  - IEEE802.11で規定されている帰属処理のプロセスに割り込み、不正フレームを送信し、認証失敗をみせかけることができれば、無線LANがいつまでも成立しない状況を作れる

- **対策**
  - 技術上の対策は無い
  - 重要性の高い通信を行なうときは有線LANを使う
  - 場合によっては無線LANを導入しないという判断も必要

無線LANをとりまく脅威 6

- なぜ、無線LANのセキュリティが問題になるのか・・・

結論　：　「WEPを設定していないアクセスポイントが多い」

問題を適切に捉えると

“無線LANのセキュリティ”が問題ではなく

“セキュリティの設定をしない無線LAN”が問題!!

WEPを設定しないと・・・

・盗聴

・不正接続

・近隣の住民による誤接続(あるいは故意)

無線LANをとりまく脅威 7

- なぜ、人はWEPを設定しないのか？

  おそらくは、ユーザの知識不足

例　1.家庭で無線LANを使いたいから無線LANを購入する
　　2.マニュアルを読んだり、技術的な理解は後回しして、とりあえずつなぐ
　　3.何の設定がなくてもとりあえずアクセスポイントと端末の間で通信が行なわれている
　　4.その日から快適なコードレスインターネット生活の始まり！！

・・・・ということで
「世の中にまた一つ、WEPが設定されていない無線LANが誕生したのであった・・・」

無線LANをとりまく脅威 8

■ WEPの設定についての対策

1.業界団体や行政による取り組み

・WEP をユーザに認識させ、設定してもらうために
「無線LANのセキュリティに関するガイドライン」を発表

2.メーカーによる取り組み

・WEPが事前設定された無線LANのアクセスポイント製品を出荷

例：NECアクセステクニカの「Aterm WARPSTAR」シリーズでは、
ESS-IDやWEPキーが事前設定された製品がラインナップされている

標準セキュリティの脆弱性 1

- ESS-IDはセキュリティではない
  - ESS-IDはあくまでネットワークを識別するために用いられる情報
  - セキュリティとは無縁の設定

- MACアドレス認証の脆弱性
  - MACアドレス認証は、認証方式としてはきわめて不完全

認証に使われるMACアドレスの情報は暗号化されない

↓

MACアドレスの情報を取得することが可能

  - クライアントアダプタのMACアドレスを書き換えるツールがある

標準セキュリティの脆弱性 2

- WEPの脆弱性

運用の問題点

WEPのキー設定の情報が漏洩すると・・
・そのキーで盗聴され、WEPが設定されていない無線LANと同じ状態になる

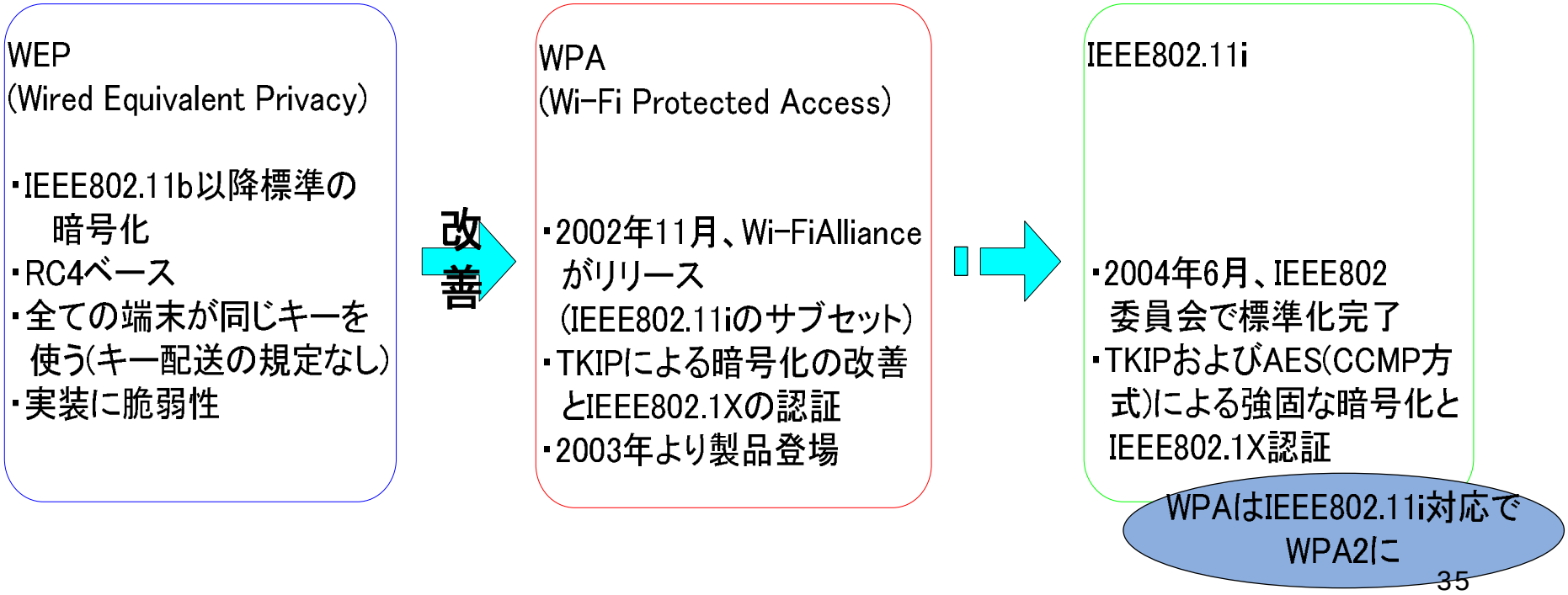
全てのノードが同じキーを設定することの問題
・辞書攻撃、総当たり攻撃などによる割り出しが可能
・同じキーを使い続ければいつかは暗号が解けてしまう

技術上の欠陥

WEPの実装そのものに問題があり、WEPは暗号化の方式としては不完全であることが明らかとされている

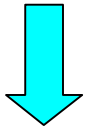
WPAによるセキュア無線LAN

- WPA (Wi-Fi Protected Access)**とは・・・**
  - **脆弱性があることが明らかになった無線LANのセキュリティを改善するため、新たに発表されたセキュリティ規格**
  - **認証と暗号化を強化**



WPAによる暗号化の改善～TKIP

WEPの暗号化プロトコルは周期的に同じキーを使ってデータの暗号化して解読されやすい



欠点の克服

TKIP

キーを自動的に変更して暗号化を行うようにした暗号化プロトコル

■ 暗号化の改善点

強度：TKIPの採用

・TKIPの採用により、既知の手法による解析・盗聴は不可能

区間：適切な区間での採用

・TKIPはクライアントアダプタ、アクセスポイントに標準実装される技術で、無線LAN起動・接続と同時に暗号化

・暗号化されない区間や時間が生じることはない

WPAによる認証の改善 ~IEEE802.1X

WPAの認証方式にはIEEE802.1Xが標準採用

- **認証の改善点**

  資格情報：資格情報は暗号化される

  ・IEEE802.1X認証では、資格情報は暗号化されて送信される

  相互認証：相互認証が行われる

  ・一部の方式をのぞき、IEEE802.1X認証では、相互認証を採用

IEEE802.1Xは必要充分な強固さと可用性を備えた認証方式

WPAによるセキュア無線LAN

WPAによる暗号化・認証の改善により

・盗聴

・なりすまし

・不正アクセスポイントへの接続

を防ぐことができる！！

セキュア無線LANのポリシー

- **無線LANがさらされる脅威を適切に把握する**
  - ネットワーク管理者は無線LANの脅威をあらかじめおさえておく
- **無線LANは定期的に監査する**
  - 社内に無線LANを導入したら、電波が飛んでいく範囲を把握する
  - 管理されていない無線LANの存在をあぶりだす
- **無線LANはセグメントを分離して導入する**
  - 有線と無線は異なるネットワークだから
- **セキュリティレベルは、無線LAN全体で統一する**
  - 同一ネットワーク内では同一のレベルの基準を適用しないと効果なし
- **未知の脆弱性に対処する**
  - 無線LANが使用不可になった場合を考慮し、有線LANのポートも
    あらかじめ確保しておくといった運用をする

完