無線LANの解読と「通信の秘密」

立命館大学情報理工学部
上原哲太郎

無線LANとは

- 産業科学医療用（ISM帯）：
  国際電気通信連合において、
  産業用等の非通信応用における利用向けに
  国際的に分配された周波数帯
- このISM帯のうち、主に2.4GHz帯や5GHz帯を使用した無線データ通信規格が無線LAN
  - 小電力通信であれば免許を要しない
    （使用機器の技術基準への適合は必要）

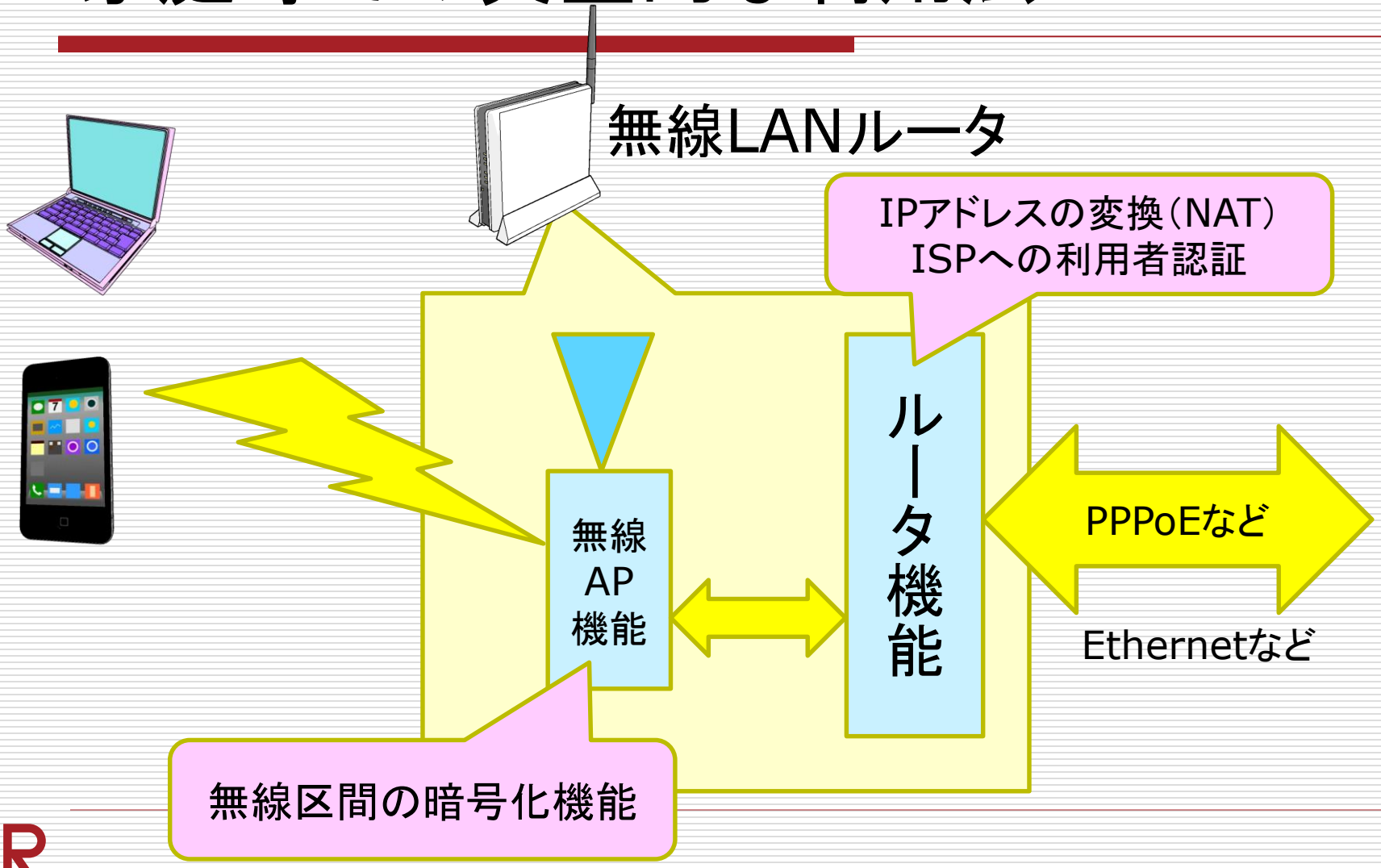
無線LANの規格化

- IEEEの802.11標準化委員会で検討される
- 主な規格
  - IEEE802.11（2.4GHz帯・2Mbps） 1997年
    WEP暗号化はこの規格に含まれている
  - IEEE802.11a（5GHz帯・54Mbps）1999年
  - IEEE802.11b（2.4GHz帯・11Mbps）1999年
  - IEEE802.11g（2.4GHz帯・54Mbps） 2003年
  - IEEE802.11n
    （2.4または5GHz帯・理論最大600Mbps）
  - IEEE802.11ac（5GHz帯・理論最大6.9Gbps）
  - IEEE802.11ax
    （2.4または5GHz帯・理論最大約10Gbps ）

Wi-Fi

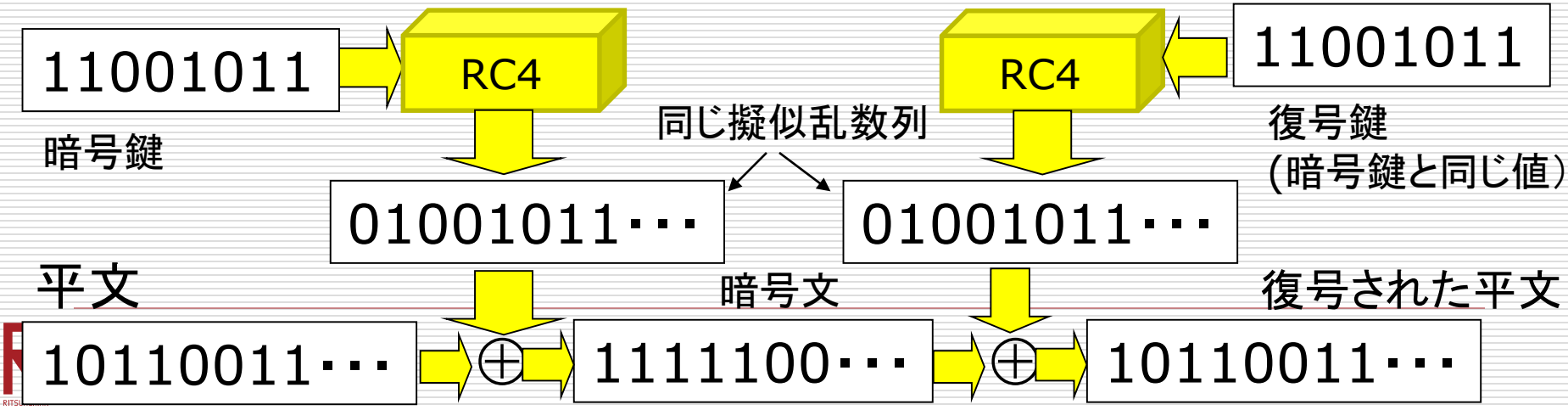
- IEEE802.11等を実装した
  各通信機器が規格に適合しており
  相互に通信可能か技術的に検証するための
  テスト項目の制定を行う業界団体が
  Wi-Fi Alliance（WFA）
- WFAの定めたテストにより
  IEEE802.11規格との互換性が認められた製品には
  Wi-Fi認証が与えられ、適合マークが表示できる
- WEPによる暗号が危殆化した際には
  IEEE802.11委員会による規格化を待たずに
  Wi-Fi Protected Access (WPA)の
  互換性テストを定めて製品への実装を促す
- 現在はIEEE802.11iによる暗号化規格への
  互換性テストWPA2をWi-Fi表記のための
  必須項目にしている

家庭等での典型的な利用法



WEPに用いられるRC4暗号とは

- 固定ビット長の暗号鍵（WEPでは128bit）を入力すると、任意ビット長の擬似乱数列を出力する。
- これを平文と排他的論理和（XOR）演算して暗号文を得る
- 受信者は、同じ暗号鍵を用いると同じ擬似乱数列が得られるので、これと暗号文をXORして復号



WEP暗号化された IEEE802.11フレーム（概略）

無線AP アドレス	送信元 アドレス	送信先 アドレス	IV	暗号化された データ(IPパケット)

アドレスはMACアドレスを指定（無線APではBSSID）

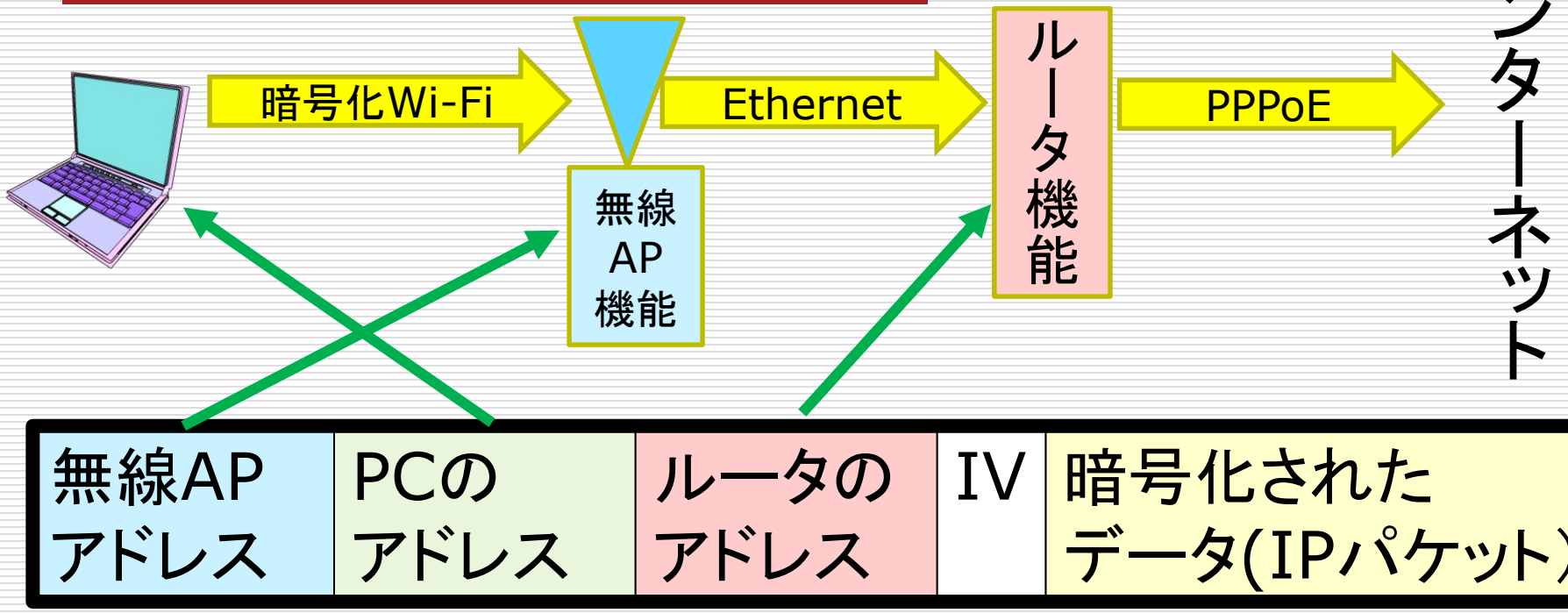
可変のIV（24bit）に104ビットの固定WEP鍵を連結し128ビットの暗号鍵にしてRC4暗号ストリームを生成

データ部分を暗号化する

IPパケットはデータ部分

WEP鍵は秘密の固定値
IVはフレーム毎に適当に変更する
IVとMACアドレスは暗号化されない

例：Wi-Fi対応PCから送信するとき

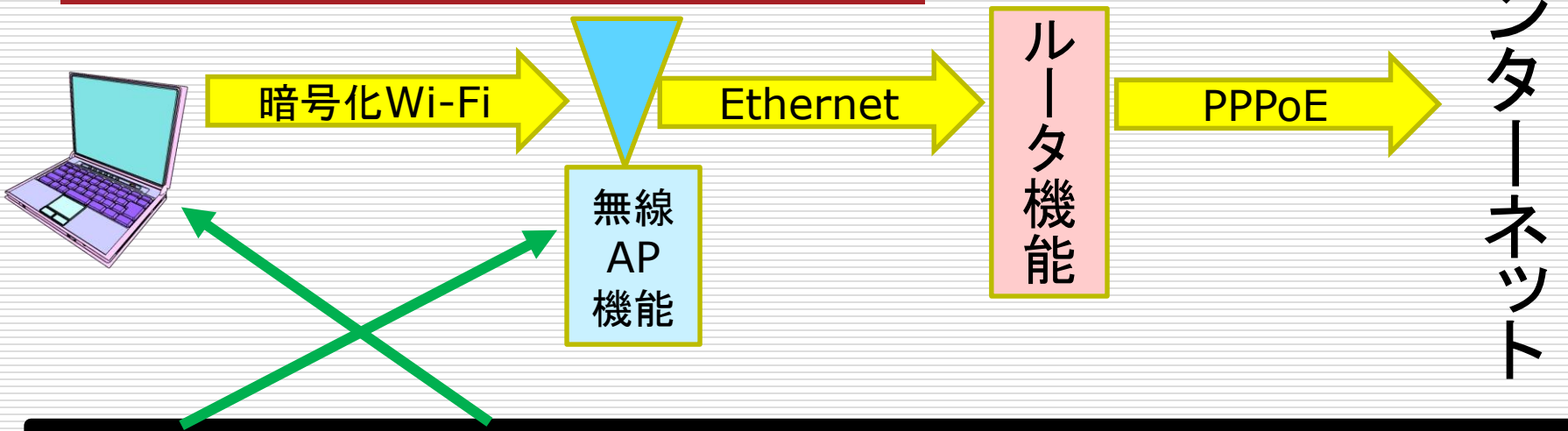


Wi-Fi通信時、IEEE802.11フレームを作るには
「送信元」「送信先」「無線AP」のMACアドレスが必要

ARPとは

- Address Resolution Protocolの略
  IPパケットによる通信の前に必ず発生する
- IPアドレスが分かっているがMACアドレスが
  分からない場合にMACアドレスを問い合わせる
- ARP要求「このIPアドレスを持つ者は返事を！」
  ARP応答「そのIPアドレスの者です！
  MACアドレスはこれです！」
- ARP要求時に送信先MACアドレスは
  「ブロードキャストアドレス」つまり
  「LAN内の全員が受信」するように要求する
- 無線LAN接続直後には
  ルータのMACアドレスが必要になるので
  ARP要求がほぼ発生する
  - その他、「初めて」「久しぶりに」通信するたびに発生

PCがルータを通じて送信する前に発生するARP要求



無線AP アドレス	PCの アドレス	全受信 アドレス	IV	暗号化された データ(ARP要求)

アドレス部分は暗号化されていないので
全受信アドレスを見ればARP要求だという推定は容易
そのARP要求も先頭の32バイトが固定か推定可能
ARP応答についても同様に推定可能

WEPの解読

- WEPにおけるRC4の利用法が不適切で
  暗号的性質の弱いところを突かれやすい
- WEPでは「IVの分だけ異なる暗号鍵」
  →「異なる暗号ストリーム」を多用しているが
  この組合せが十分（数万組）集まれば
  IV以外の部分（つまりWEP鍵）を解読可能
- ARP要求や応答は先頭部分が容易に推定でき
  暗号化されたデータ部分から
  暗号ストリームの先頭部分が復元可能
- よって「暗号化されたARP要求/応答」を
  数万集めればWEP鍵が解読できる

WEPへの攻撃の主な戦略

- 受動的(Passive)な手法
  - ひたすら通信を傍受し続けて、宛先アドレスが「全受信アドレス」のIEEE802.11フレームを収集
    その直後のフレームはARP応答と推定して収集
  - この手法で数万集めれば解読できる
    ただし時間がかかる
- 能動的(Active)な手法
  - 傍受してARP要求(と推定される)フレームを発見したら
    それを記録・複製し、無線APに何度も送信する
  - 無線APはその都度それをルータに送信し、
    ルータはその都度ARP応答を生成して
    無線APを通じて受信者に送信する
  - これも傍受可能なのでARP応答を含むフレームを
    大量に短時間に収集可能である

WEP鍵解読と窃用による「無線LANただ乗り」と電波法

- 電波法が想定しているのは…
  - 通信の秘密を漏らし、または窃用（109条）
  - 「通信の秘密を漏らし、または窃用」する目的で暗号通信の内容を復元（109条の2）
- しかし「無線LANただ乗り」の目的は通信の内容ではなく、インターネット回線そのものの利用
- 電波法で取り締まるなら、どれが「通信の秘密」かどこがその漏示または窃用にあたるかが問題

RITSUMEIKAN

「通信の秘密」にあたる可能性（1）

- WEP鍵は通信の秘密か？
  - あたらないとする立場
    - 通信の暗号化のために使われているが、
      WEP鍵そのものは通信されておらず
      利用者が通信を暗号化するための方法に過ぎない
  - あたるとする立場
    - 通信の際に暗号ストリームが生成されているが
      暗号ストリームを「暗号化されたWEP鍵」と見なせば、
      WEP鍵そのものも通信されていると見なせる
    - WEP鍵をPCや無線AP等に設定し送受信者を
      限定することが「意思の伝達」なので通信を構成する

「通信の秘密」にあたる可能性（2）

- ARP要求は通信の秘密か？
  - あたらないとする立場
    - ARP要求は実際の通信を開始する前の制御信号に過ぎない
    - WEP攻撃ではARP要求自体は暗号化された状態で用いており、内容を知り得ない状態なのでそれを利用することは秘密の漏示や窃用とはいえない
    - ARP要求は受信先を限定しない全受信アドレスで送信されるので、特定の相手方を対象にしておらず、傍受者も含めて「通信の相手方」になっている

「通信の秘密」にあたる可能性（3）

- ARP要求は通信の秘密か？
  - あたるとする立場
    - 暗号化されているとはいえ、通信の内容により受信者がARP応答をすることを期待しているので、それは通信の内容を知り得ているのと同じ
    - ARP要求は受信先を限定しない全受信アドレスだがIPアドレスによって実際の受信者を指定しているので特定の相手方を対象にした通信にあたる当該IPアドレスを持たない端末はたまたま傍受してしまったに過ぎない

「通信の秘密」にあたる可能性（4）

- ARP応答は通信の秘密か？
  - 「全受信アドレス」ではないことを除き
    ARP要求と同様

他の法適用の可能性

- 不正アクセス禁止法は適用可能か
  - 特定電子計算機をどう見るかが難しい
    - 無線LANルータそのものは
      特定電子計算機と見なさない
    - 家庭のLAN内ではなくインターネット側の計算機しか
      アクセスしていないなら、WEP鍵による限定は
      アクセス制御とは言えない
- 私電磁的記録不正作出および供用
  - WEP鍵を私電磁的記録として適用できるか？