

無線LANにおけるセキュリティ 技術の最新動向

～ 認証・プライバシー保護技術～

株式会社KDDI研究所

情報セキュリティG 渡辺 龍



コンテンツ

- WLAN
 - Wireless LAN
 - Wireless LANの普及状況
 - WLANセキュリティ
- 暗号化
 - 無線区間の暗号化
 - 暗号化における問題
- 認証手法
- WLANにおけるセキュリティ懸念
 - 企業におけるセキュリティ対策
 - セキュリティ上の懸念
 - プライバシー問題
- 新しいサービス
 - FON
 - メッシュネットワークの利用
 - セキュアなエリア拡張



コンテンツ

- WLAN

- Wireless LAN
- Wireless LANの普及状況
- WLANセキュリティ

-

-
-

-

-

-
-
-

-

-
-
-

Wireless LAN

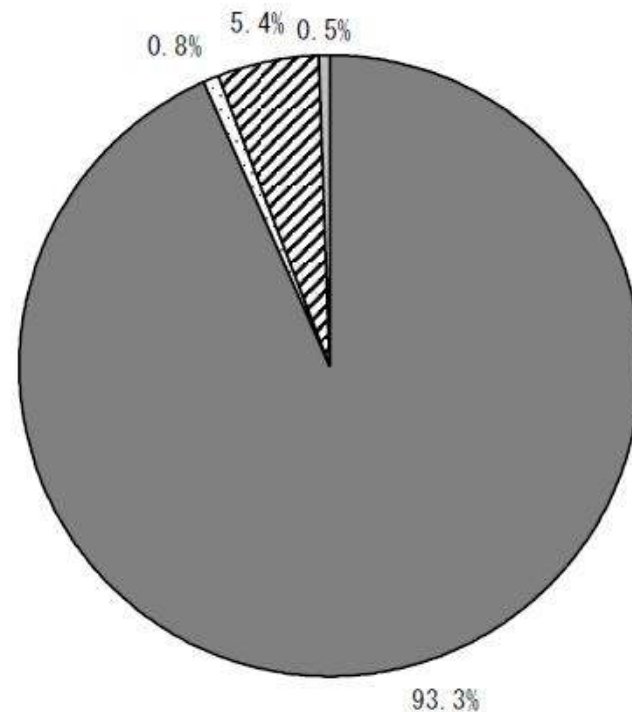
- 無線LANとは、無線通信方式でデータの送受信を行う(コンピュータ)ネットワーク。現状ではIEEE 802.11シリーズが主流。電波を利用する。
- Wi-Fiは、業界団体による名称。Wi-Fiアライアンス認定の機器はロゴマークが利用できる。
- 現在では親機となる基地局、子機用インタフェースも十分安価となり、一般宅にも広く普及している。



無線LANの普及状況

■ 企業におけるインターネット接続の有無

【全体】インターネット接続の有無 (SA, N=613)



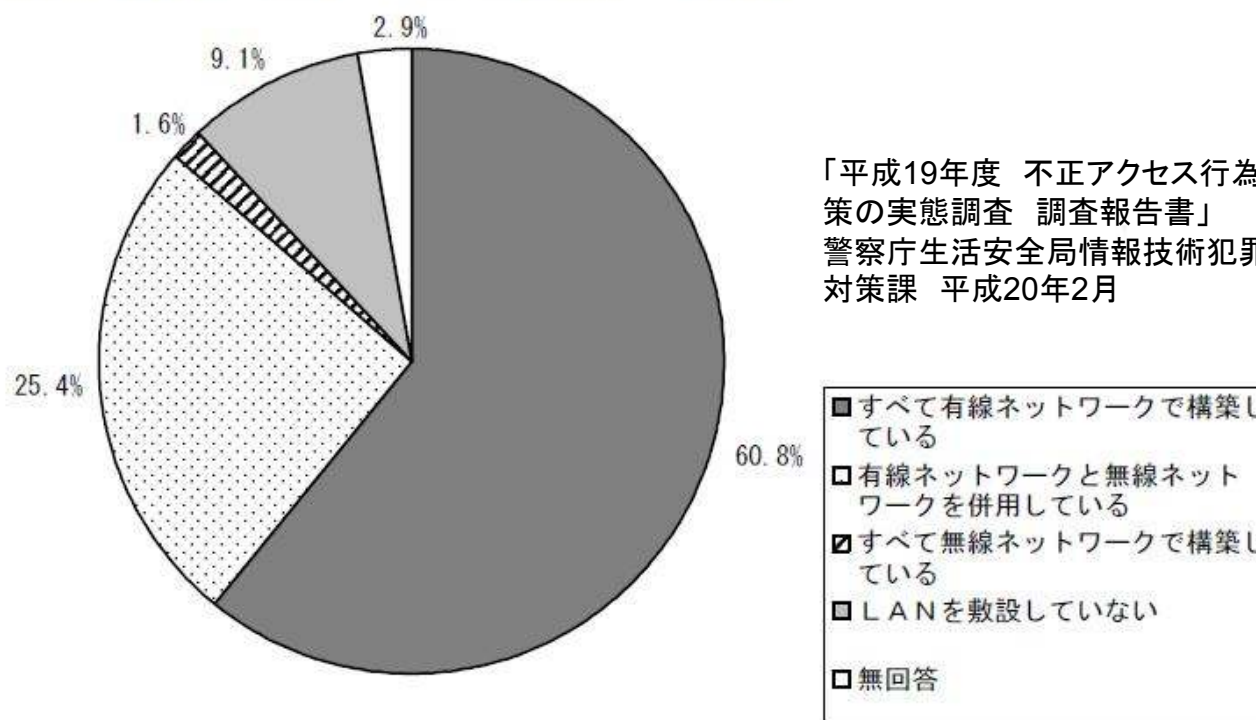
「平成19年度 不正アクセス行為対策の実態調査 調査報告書」
警察庁生活安全局情報技術犯罪対策課 平成20年2月

- 接続している
- 接続していないが、現在接続を計画中である
- ▨ 接続しておらず、接続の計画もない
- 無回答

無線LANの普及状況

■ 企業におけるネットワーク構成

【全体】 事業体内のネットワーク利用状況 (SA, N=613)





WLANセキュリティ

- WLAN利用でのセキュリティの懸念
 - 無線信号は電波が届けば受信できる。
 - 暗号化
 - 不正にAPを利用させない。
 - 認証
 - (アクセス制御)



コンテンツ



■ 暗号化



無線区間の暗号化



暗号化における問題





WLAN通信路の暗号化

- WEP
 - Wired Equivalent Privacy
- WPA
 - Wi-Fi Protected Access
- WPA2
 - WPAの改良版

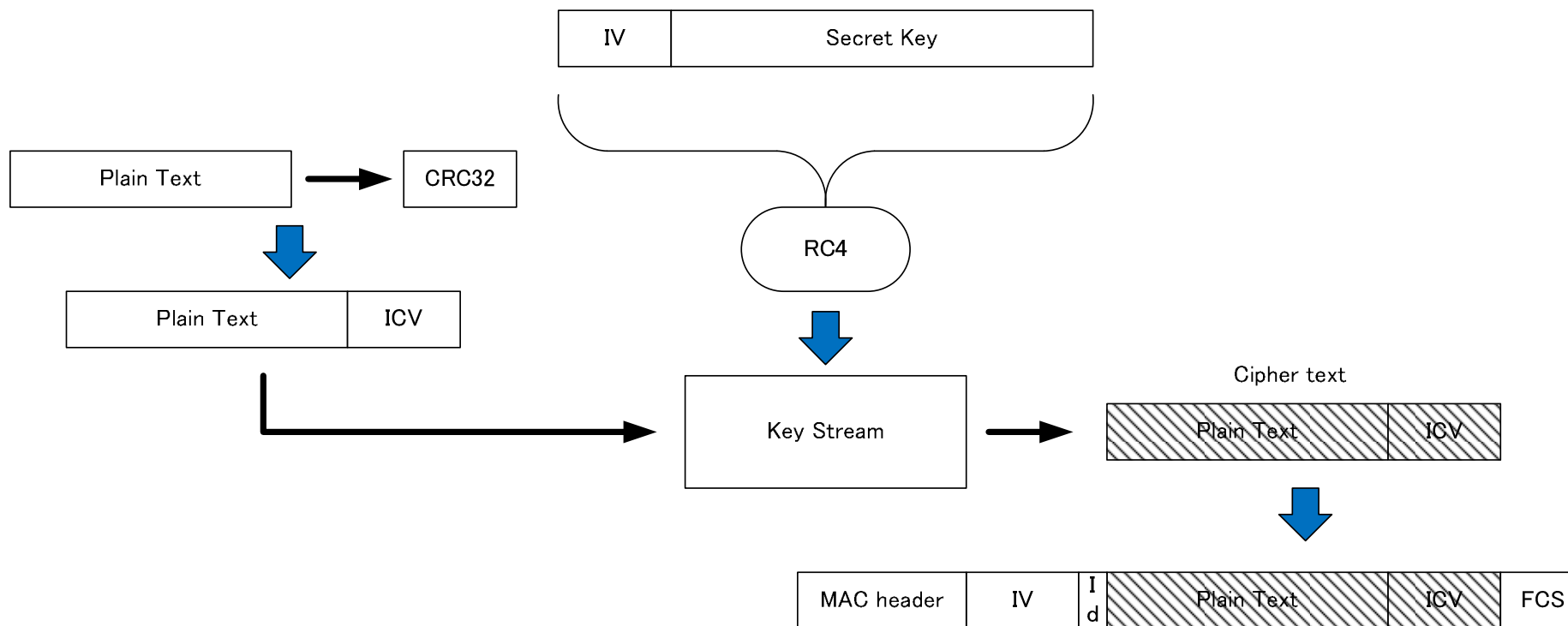


WEP

■ Wired Equivalent Privacy

- 有線接続と同様のプロテクションという意味で名付けられた。
- ユーザが設定する鍵と、製品が決定するパケットごとに変化するIV(初期化ベクタ,24bit)とを元に、RC4により乱数ストリームを生成しデータを暗号化。
- 秘密鍵の長さは、64(40), 128(104)の2パターン。

WEPの仕組み





WEPの脆弱性

■ IVの問題

- IVは平文で送信されており、観測可能。
- IVは非常に空間が小さい(24bit)。
 - やがて同じIVを持つパケットが現れる。
 - これそのものがひどい脆弱性を招いているわけではない。
- 暗号化部でも平文が推測可能な部分(IPのheaderなど)がある。



IVのコリジョン

■ ストリーム暗号

□ RC4はXOR演算で、暗号文を生成する。

■ $C1 = P1 \text{ xor } R1$

■ $C2 = P2 \text{ xor } R2$

□ $R1 = R2$ なるパケットを発見できた場合、

■ $C1 \text{ xor } C2$ から、 $P1 \text{ xor } P2$ がわかる。

□ このことはあまり意味がない。わかったところでそこからの派生は難しい。



FMS攻撃

■ 鍵の回復

- 生成されるRC4鍵ストリームの最初のバイトが判明しており、弱いIVである場合には、Key Byteをある確率で推測できる。
 - 4M～6Mのパケットがあれば、40bit(5文字)のWEPを解読可能。
 - その後さらに改良が加えられ1M程度のパケットで解読可能となった。また、更なる改良(Korek攻撃:FMS攻撃を一般化した攻撃 2004.)では、100～200K個で推測可能となった。

「Using the Fluhrer, Mantin, and Shamir Attack to Break WEP」
S. Fluhrer, I. Mantin, A. Shamir, 2001. AT&T technical report



WPA

■ Wi-Fi Protected Access

- 脆弱性の多いWEPに代わり制定された暗号化規格であり、802.11i (RSN: Robust Security NW)の一部
- SSIDと暗号化のための鍵(WEPキー)の他に、鍵更新プロトコルであるTKIP (Temporary Key Integrity Protocol)を利用している。
- 家庭向けのWPA-PSK方式と、802.1x認証を利用するWPA-EAPがある。



WPAの問題点

■ WPA

- WPAのPSK (Pre Shared Key)モードの場合に、鍵を推測できる攻撃が発覚している。
- 複数のパケットを観測することで、鍵を推測することが可能で、APに辞書攻撃を仕掛けることで、突破できる。
- パスフレーズとして、17文字以上かつ乱数を設定することが望ましい。
 - 個人じゃそんな長い文字を利用しないので、機械に頼る。



WPA2

- Wi-Fi Protected Access 2
 - WPAの改良版
 - WPAとの互換性あり
 - 暗号化手法として、NIST標準のAES (Advanced Encryption Standard)を装備
 - 今のところ大丈夫そう・・・
 - 時間の問題？



コンテンツ



-
-
-



-
-

■ 認証手法



-
-
-



-
-
-



WLANの認証

■ 802.1xの認証

- ユーザ認証後に接続を許可するための認証技術。
- AP側が対応していることが必要。
- クライアント側には専用のソフトが必要 (windows系は装備されている。)

■ 認証手法

- EAP-TLS
- PEAP
- EAP-TTLS



EAP-TLS

■ EAP-TLS

- Extensible Authentication Protocol Transport Layer Security
- サーバとクライアント双方に証明書を利用して認証を実施。TLSのハンドシェイクを利用する。
- 証明書利用のためセキュリティレベルが高いとされる。
- クライアント側での証明書管理を厳密に行う必要がある。



PEAP

■ PEAP

- Protected Extensible Authentication Protocol
- サーバは証明書を利用
- クライアントはID/パスワード利用(このためクライアント側の管理は容易)
- サーバ側証明書を用いて、TLSの通信路を生成しその上でEAPを動作させている。



EAP-TTLS

■ EAP-TTLS

- Extensible Authentication Protocol Tunnel Transport Layer Security
- サーバ側は証明書を利用
- サーバ側証明書により、TLSトンネルを形成する。
- トンネル内での認証方式は設定可能。(ID/パスワードでもいいし、別の手法でもよい。)



コンテンツ



-
-
-



-
-



■ WLANにおけるセキュリティ懸念

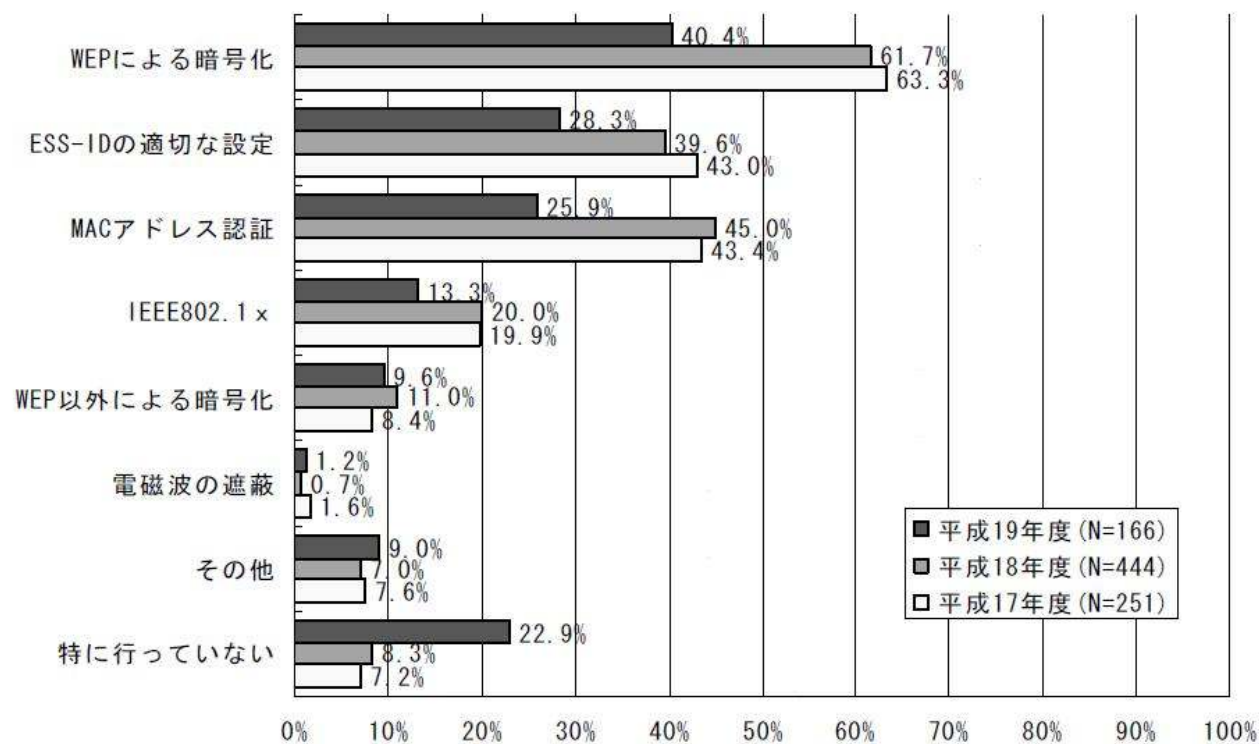
- 企業におけるセキュリティ対策
- セキュリティ上の懸念
- プライバシー問題



-
-
-

企業における無線LAN不正対策1/2

【経年変化】無線ネットワークのセキュリティ対策



「平成19年度 不正アクセス行為対策の実態調査 調査報告書」
警察庁生活安全局情報技術犯罪対策課 平成20年2月

企業に調査票を送付し、回収できたものから統計を取ったもの。

- WEPによる暗号化:
- ESS-IDの適切な設定
 - Any接続拒否:ESS-IDを知らないクライアントからの接続を拒否する。
 - ESS-IDのステルス化:ESS-IDをそもそも通知しない。
- IEEE802.1x
 - IEEE802.1xの認証を利用した上でWLANへの接続を許可する。
- WEP以外による暗号化
 - WPA, WPA2を利用して通信を暗号化する。
- 電磁波の遮蔽
 - 電波を漏えいさせないシートなどを利用する。



遮蔽シートの例



企業における無線LAN不正対策2/2

■ 高いWEP依存

- 危ないといわれているWEPは未だに現役。
- 無対策企業も合わせると、60%以上の企業が危険と考えられている状況にある。

※ 平成19年度におけるポイント低下

□ 対象の変化

- 平成19年度の調査対象は、平成18年度までの対象範囲に、非上場企業および病床数100未満の医療機関を加えた企業・団体から、無作為に抽出を行った。このため、全体的にポイントが低下している傾向にある。



セキュリティ対策を怠ると……

- アクセスポイントが不正に利用される。
 - 他人のダウンロードなどにより遅くなる。
 - 個人的なデータが盗みとられる。
 - 掲示板への不正な書き込みの踏み台にされる。

などの弊害がある。

不正行為

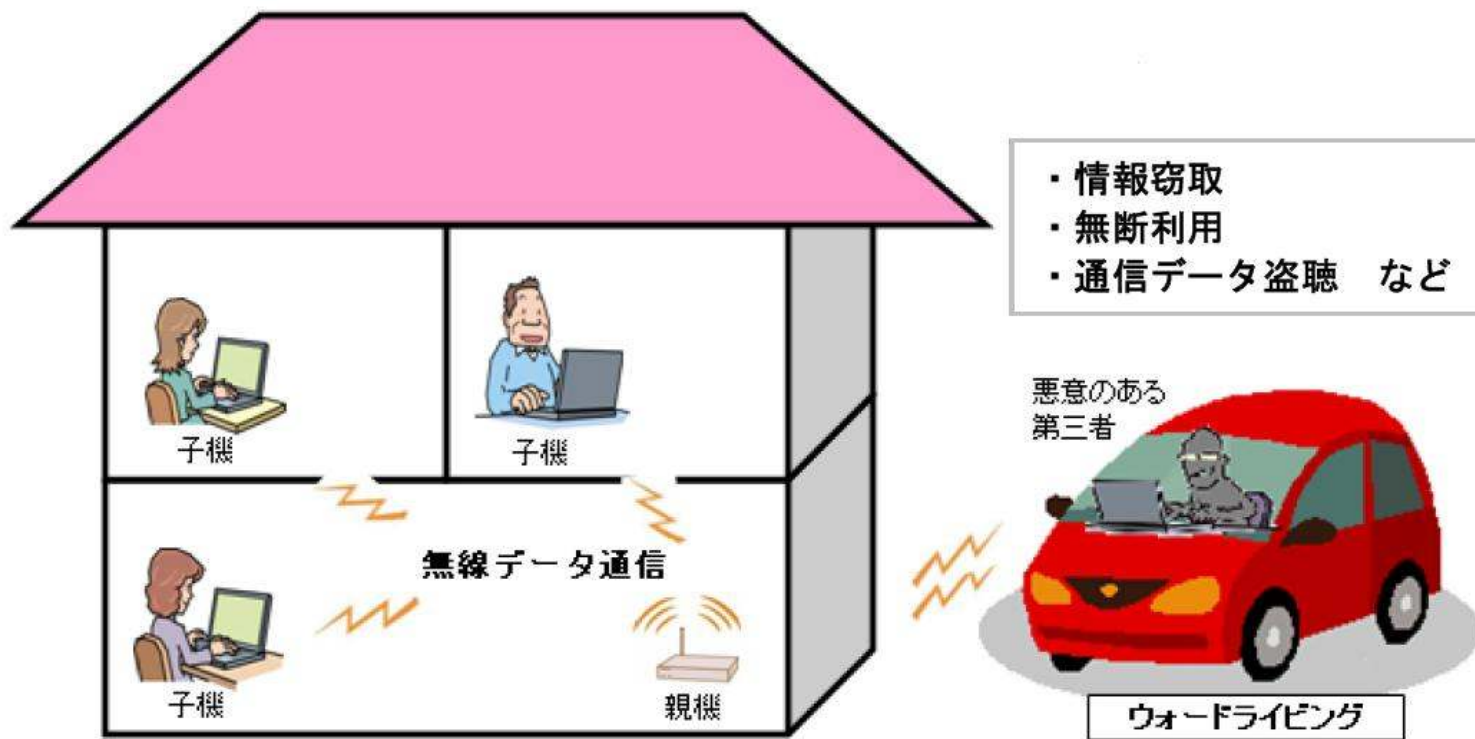


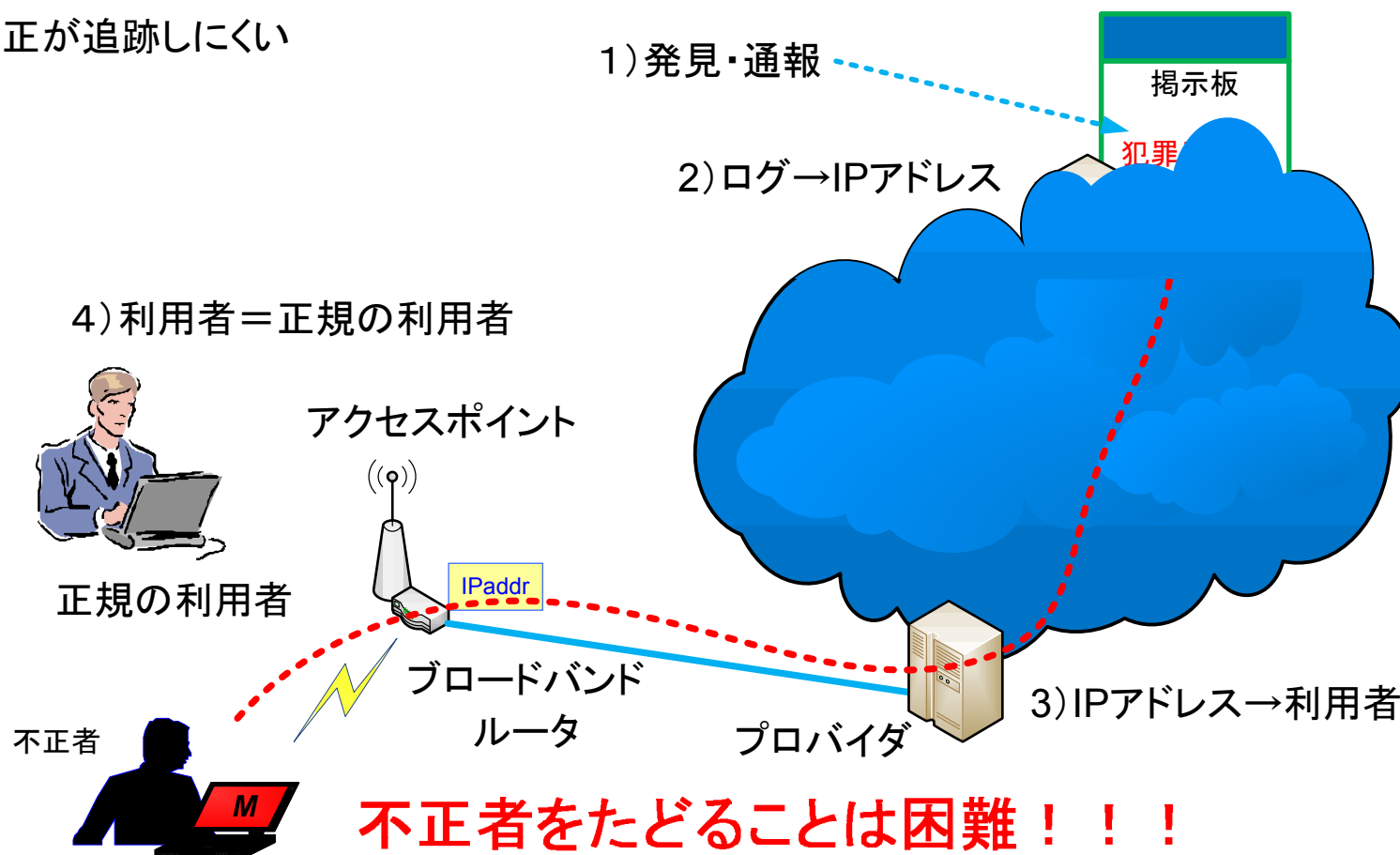
図1-1 無線LANの脅威

コンピュータウイルス・不正アクセスの届け出状況 [2008年6月分]
独立行政法人(IPA) 情報処理推進機構 プレスリリース第08-11-126号

●ウォードライビング:
建物近傍等で、脆弱性の
ある無線LANアクセスポ
イント(親機)を探す行為。

他人のLAN経由での不正な書き込み

- 無断利用してインターネットへアクセス
 - 不正が追跡しにくい





実際の例

■ 2008年6月

- 他人の親機を無断で経由してインターネットの掲示板に脅迫文章を書き込んだとして、高校生が書類送検された事件が発生しています。

「コンピュータウィルス・不正アクセスの届け出状況[2008年6月]」
独立行政法人(IPA) プレスリリース 第08-11-126号



他人のLAN経由での書き込み

- インターネット掲示板に開成中(東京都荒川区)で生徒らを無差別に殺傷すると書き込み、学校業務を妨害したとして、警視庁捜査1課と荒川署は24日、威力業務妨害の疑いで、長野県松本市の高校生(16)を書類送検した。「警察が動くななど、反応があるのが楽しそうに思えた。学校に恨みはなく、有名だったから書き込んだ」と供述している。

少年は**携帯ゲーム機**を使い、他人の無線LAN(構内情報通信網)経由でネットにアクセスしていた。捜査1課によると、**他人のLANを経由して、携帯ゲーム機から出された脅迫文の差出人を特定するのは困難で、摘発は全国初**という。

調べでは、少年は2月18日、松本市の路上からゲーム機を使って近くの民家のLANに無断で接続、掲示板に、「明日、東京の開成中学校に討ち入りに行く。午前9時半に生徒や教師を無差別に刺殺する」と書き込んで、学校側に警戒を強化させるなど、業務を妨害した疑い。

同じ日に、**松本市内**で**携帯ゲーム機**から同様の書き込みが数件あり、**警視庁が周辺を捜査。目撃情報**などから、**少年が浮上した**。

産経新聞 : <http://sankei.jp.msn.com/affairs/crime/080624/crm0806241202015-n1.htm>



一方で.....

■ Schneier on Security (Schneierの日記から)

□ My Open Wireless Network

http://www.schneier.com/blog/archives/2008/01/my_open_wireles.html

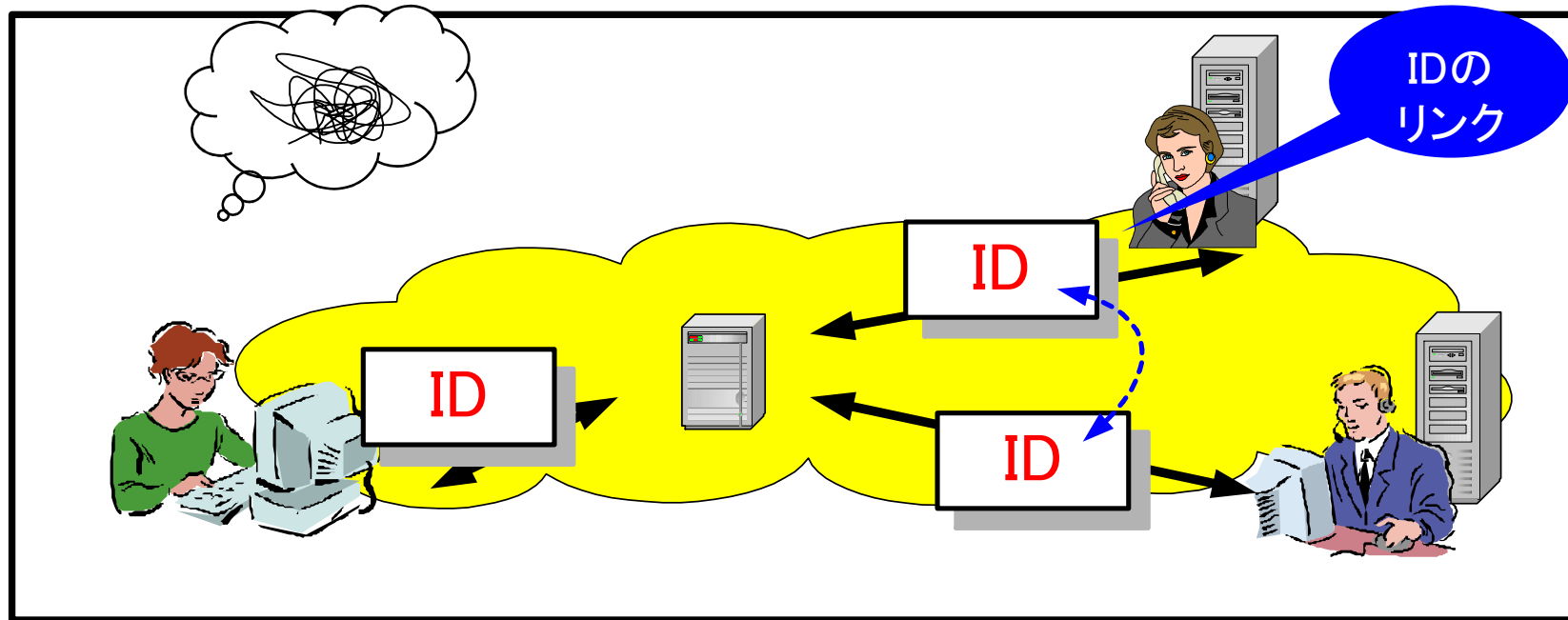
- 自身のWLAN AP にセキュリティは施していない。
 - 近所に、フリー接続の無線LANサービスの喫茶店が5軒はある。(そっちを選ぶはず。)
 - 無線LANのセキュリティはまだまだ不完全。
 - セキュリティをかけておいたにも関わらず、問題が発生した場合、自身の潔白を証明するのが面倒臭い。(誰かが勝手に使ったに違いないという方が楽。)
 - 帯域を占有されたとしても全くかまわない。

※Bruce Schneier (ブルース・シュナイアー)
Applied Cryptography(暗号技術大全)の著者。

プライバシーの漏洩問題

■ リンカビリティ

- 固有IDが異なるサービスで利用されるとサービスが結託することで活動がリンクされる。





固有な情報

■ IPアドレス

- 常時接続環境の増加により、固定IPサービスを利用しなくてもIPアドレスを固定的に利用するケースが増加

■ カード情報、配送先住所

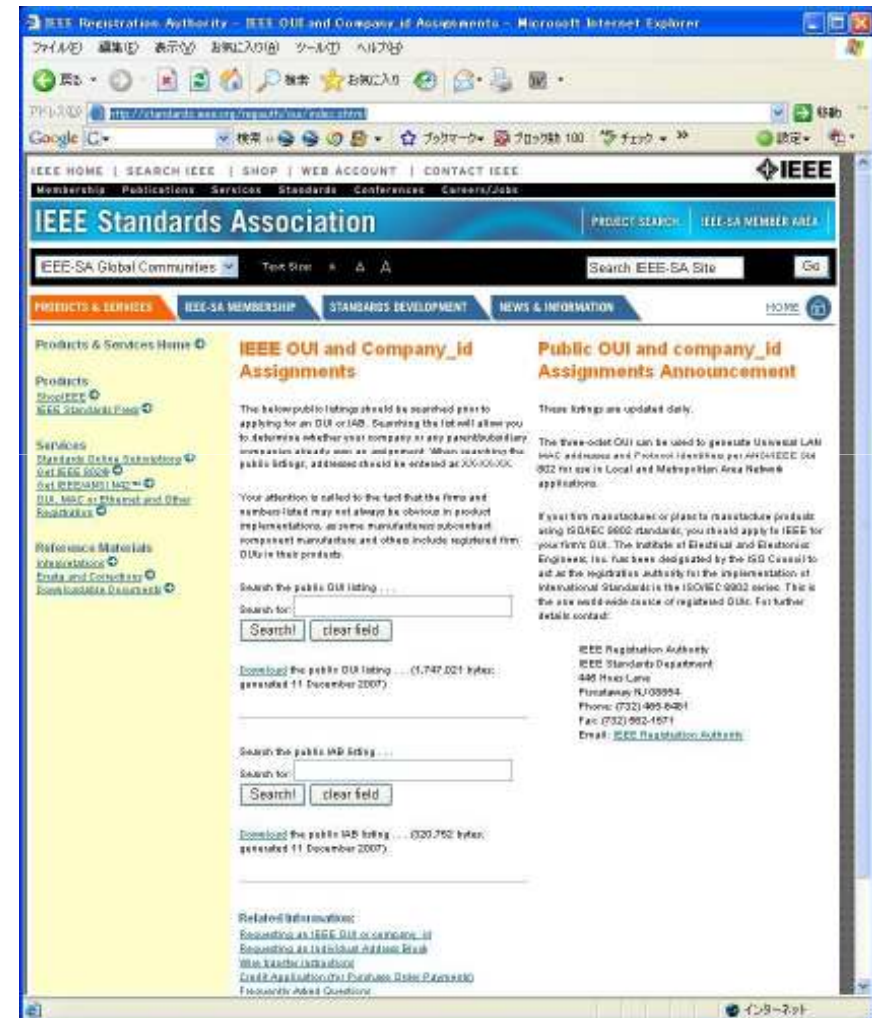
- IPアドレスやIDが異なっても、決裁情報や、配送先住所が同じなら(ほぼ)同じ人

■ MACアドレス

- そもそも固有なIDあることが想定されている。

MACアドレス

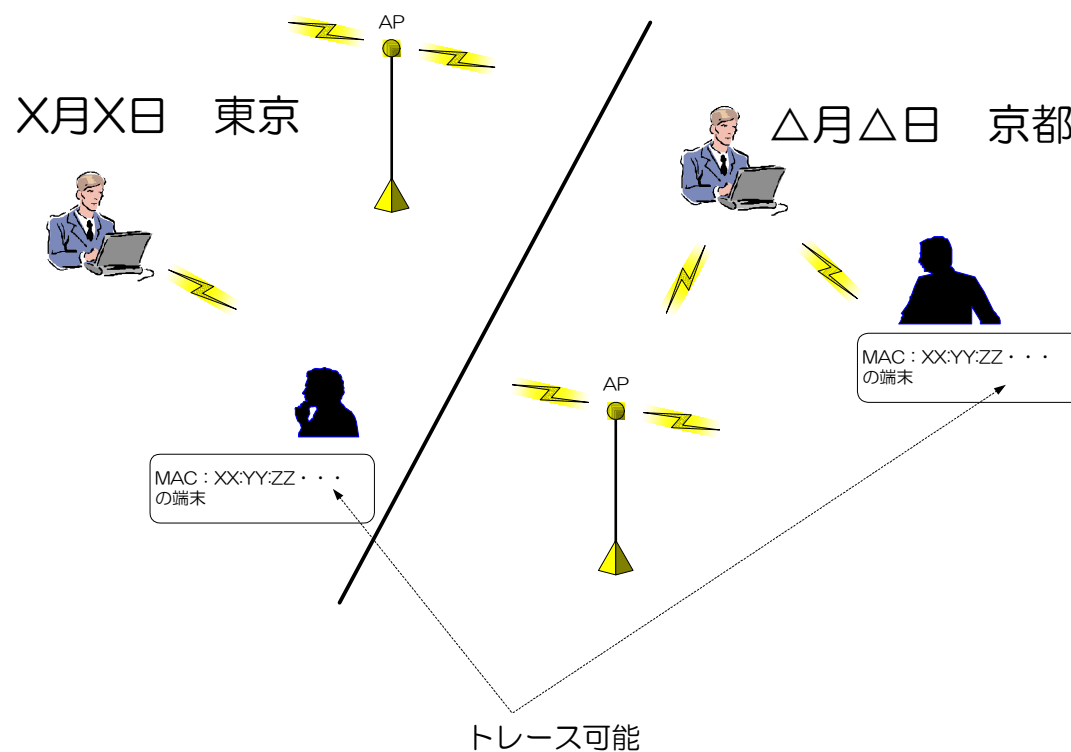
- 48ビットの固有な識別子
 - 前半24ビット
OUI(Organizationally Unique Identifier)
 - いわゆるベンダID
 - IEEEが管理(固有)
<http://standards.ieee.org/regauth/oui/index.shtml>
 - 後半24ビット
ベンダが固有なIDをインタフェースごとに付与



無線ネットワーク上でのMACの問題

■ ユーザプライバシーの漏洩

□ MACを元に追跡される可能性





無線LANアクセスポイントの 位置漏えい問題

- 無線LANの電波を用いた位置検索サービスと無線LAN自動接続とESSIDの運用にまつわるプライバシー漏洩の問題。

高木浩光氏の日記から

<http://takagi-hiromitsu.jp/diary/>

2007年11月5日

Place Engine

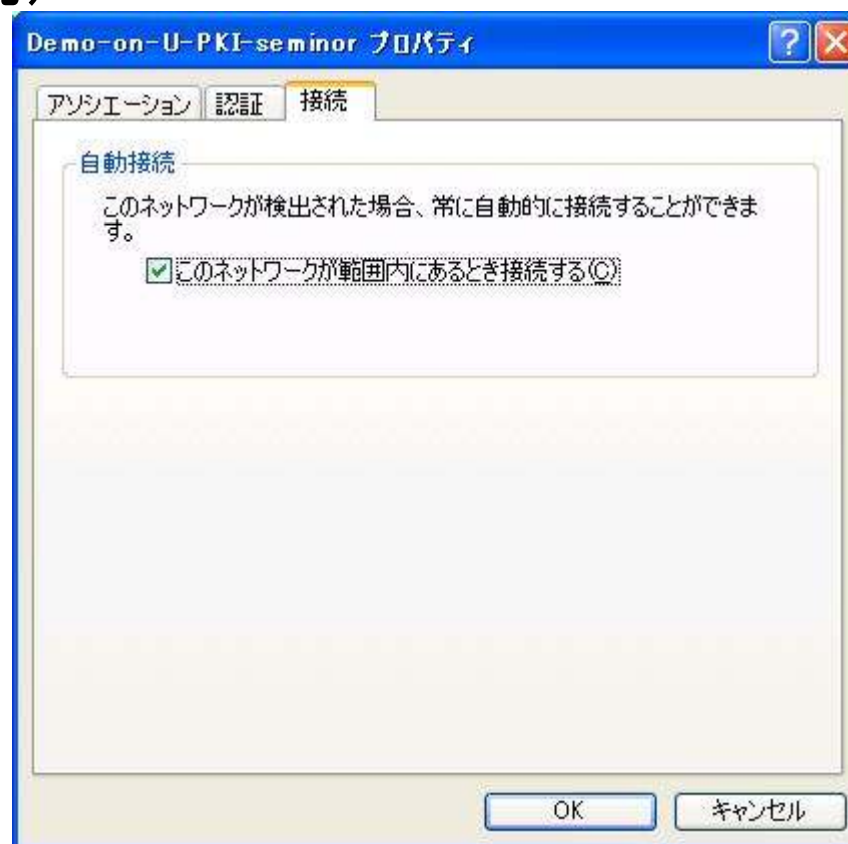
- 無線LANの電波を利用した位置検索サービス
<http://www.placeengine.com/>

- ある地点で観測できた無線LAN電波のMACアドレスと位置情報のデータベース



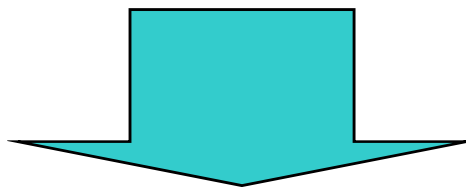
無線LANの自動接続

- 無線LANのプロパティ→有線ネットワークのプロパティ→接続(自動接続)
- 電源が入っている場合、自動的に該当するESSIDの無線LAN基地局と接続するために、常にビーコンを発信している。(すなわちESSIDを広告)



ESSIDの運用

- 市販されている無線基地局は、ESSIDとしてMACアドレス(+ α)を利用していることが多い。



- 先の、自動接続機能と併用すると自宅のMACアドレスが広告されることとなる。
- こうした通信を傍受してMACアドレスを取得し、Place Engineを利用すると住所が特定できる。



コンテンツ

- -
 -
 -
- -
 -
-
- -
 -
 -
- 新しいサービス
 - FON
 - メッシュネットワークの利用
 - セキュアなエリア拡張

FONサービス



■ FON(ユーザ間の相互利用)

<http://www.fon.com/>

- FONのコミュニティに参加して、自身のインターネット接続をFONルータにより公開するユーザ(ライナス)は、他ユーザのインターネット接続を利用できる。
- 日本には97万に程度のアカウトがある。
 - ライナス:相互利用可利用者
 - フォネロ:アカウント取得者

FONマップ(福岡)

Screenshot of the FON Maps website interface in a browser window. The browser title is "Sleipnir - [FON Maps]". The address bar shows "http://maps.fon.com/#". The page features a search bar on the left with the text "住所(例:東京都港区虎ノ門) 福岡県福岡市早良区百道浜" and a "検索" button. Below the search bar is a "絞り検索:" section with various icons for categories like Router On, FONスポット, etc. The main content area displays a map of the "FON maps" area in Fukuoka, Japan, with various locations marked with FON icons. The map includes labels for "百道浜", "シーサイドももち海浜公園", "百道西金所", "シーサイドももち局", "よかとピア橋西", "地行中央公園前", "地行中央公園", "九州医療センター", "樋井川河畔緑道", "中国総領事館", "樋井川", "百道浜", "ハイアットレジデンシャルスイート福岡", "福岡市早良消防署", "西南学院中学校高等学校", "百道通り", "ヴェルデコート7番館", "博物館前", "F・C洲上医療福祉専門学校", "西新通り", "よかとピア", "松", "福岡タワー", "Mタワー", "急患センター", "R&Dセンター", "富士通九州", "マリソン入口", "福岡タワー前", "テレビ西日本本社", "福岡タワー", "福岡市博物館", "第14号百道2号緑道", "シーサイドももちアクアコート", "シーサイドももち海浜公園", "福岡都市高速道路1号線", "百道", "百道西", "金所", "2丁目", "4丁目", "3丁目", "1丁目", "9丁目", "10丁目", "11丁目", "12丁目", "13丁目", "14丁目", "15丁目", "16丁目", "17丁目", "18丁目", "19丁目", "20丁目", "21丁目", "22丁目", "23丁目", "24丁目", "25丁目", "26丁目", "27丁目", "28丁目", "29丁目", "30丁目", "31丁目", "32丁目", "33丁目", "34丁目", "35丁目", "36丁目", "37丁目", "38丁目", "39丁目", "40丁目", "41丁目", "42丁目", "43丁目", "44丁目", "45丁目", "46丁目", "47丁目", "48丁目", "49丁目", "50丁目", "51丁目", "52丁目", "53丁目", "54丁目", "55丁目", "56丁目", "57丁目", "58丁目", "59丁目", "60丁目", "61丁目", "62丁目", "63丁目", "64丁目", "65丁目", "66丁目", "67丁目", "68丁目", "69丁目", "70丁目", "71丁目", "72丁目", "73丁目", "74丁目", "75丁目", "76丁目", "77丁目", "78丁目", "79丁目", "80丁目", "81丁目", "82丁目", "83丁目", "84丁目", "85丁目", "86丁目", "87丁目", "88丁目", "89丁目", "90丁目", "91丁目", "92丁目", "93丁目", "94丁目", "95丁目", "96丁目", "97丁目", "98丁目", "99丁目", "100丁目". The map also shows "POWERED BY Google" and "©2008 ZENRIN". The browser's taskbar at the bottom shows the system tray with a clock at 100% zoom.

2008/7/29

FONマップ(上福岡)

The screenshot displays the FON Maps web application in a browser window. The browser's address bar shows the URL <http://maps.fon.com/#>. The page features a search bar on the left with the text "住所(例: 東京都港区虎ノ門)" and "埼玉県ふじみ野市大原". Below the search bar are several "調整中" (adjusting) buttons and a "見つける" (find) button. A "絞り検索:" (refined search) section contains icons for various categories like Router, Cafe, and Hotel. The main map area shows a street map of Utsunomiya City with several orange circular icons representing FON spots. The text "WiFi EVERYWHERE" is prominently displayed at the top right of the map area. The browser's status bar at the bottom indicates "ページが表示されました" (page displayed).

2008/7/29



FONの接続

■ 二つの信号

□ MYPLACE

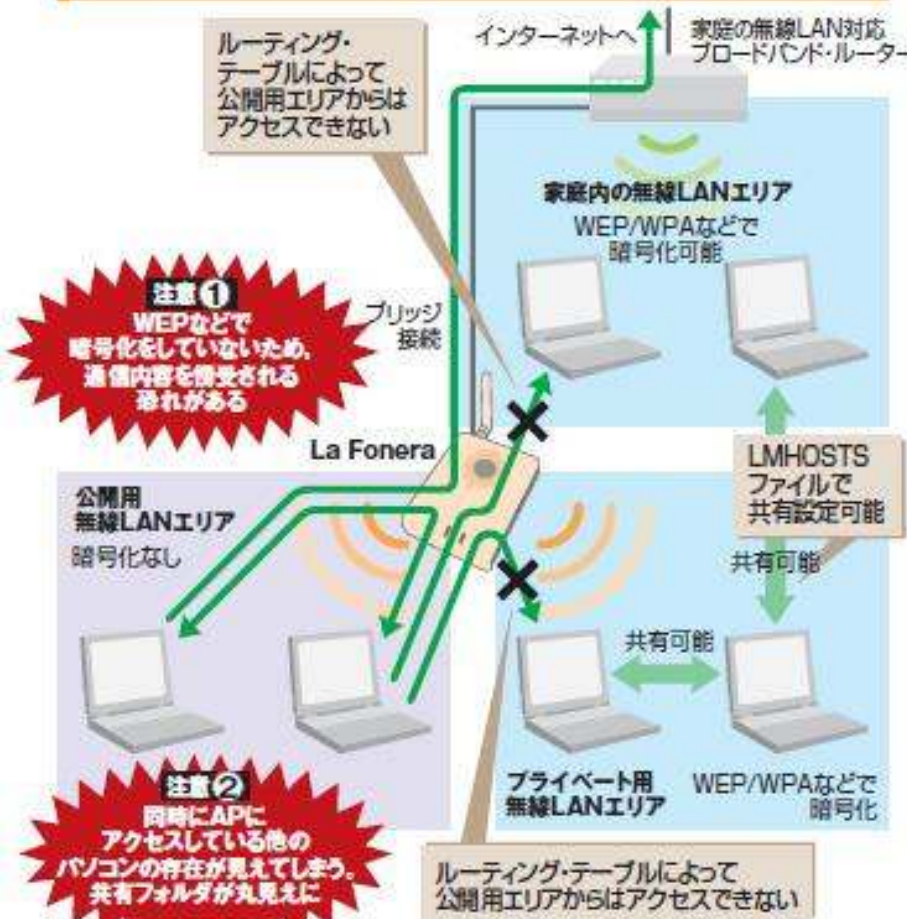
- 暗号化された提供者のプライベートな領域

□ PUBLIC

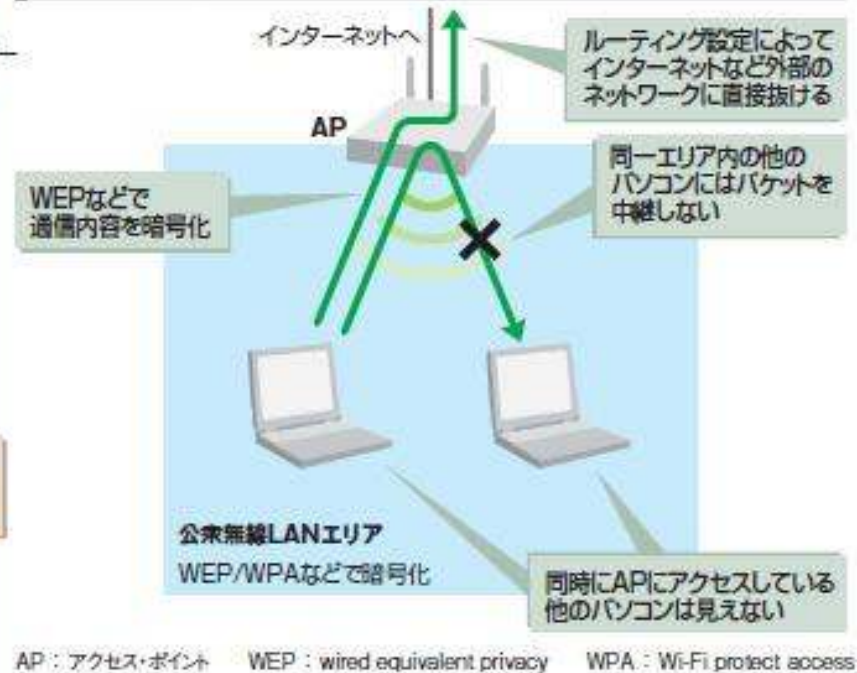
- 他ユーザのために解放される領域。ライセンスならばだれでも利用できる。
- 暗号化されていない。
- ライセンスはネット側での認証後に利用できる。

FONのセキュリティ上の懸念1/2

FON



一般的な公衆無線LANサービス

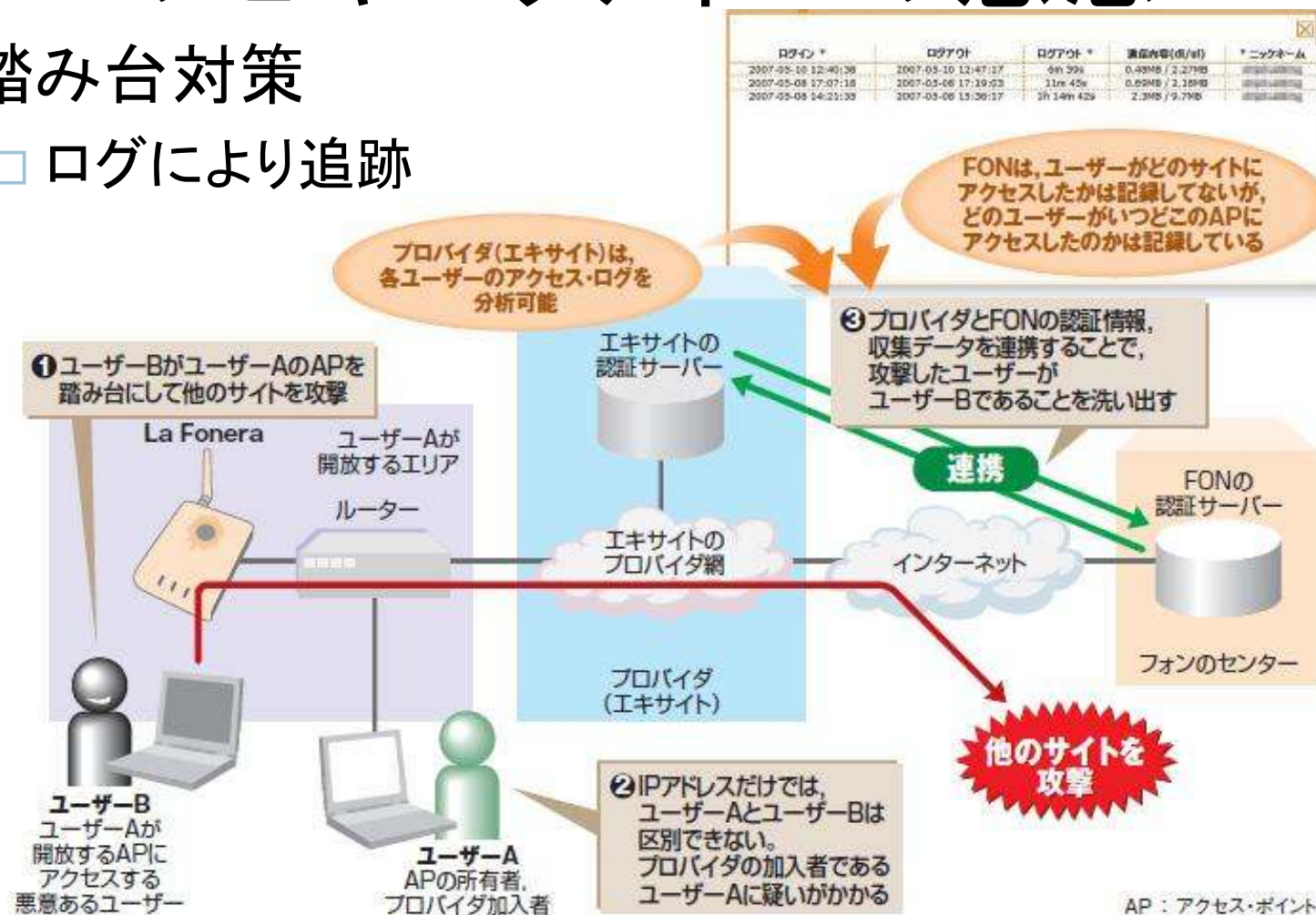


←昔のLAN(リピータハブ)のような接続

FONのセキュリティ上の懸念2/2

■ 踏み台対策

□ ログにより追跡





FONのセキュリティ上の懸念まとめ

- 暗号化がない
 - 自身でみられないように設定。
 - VPNなど別の暗号化を実施。
- 踏み台対策
 - ライナスは利用時に認証が必要
 - 利用ログをNW側で記録
 - 付け合わせることにより追跡
 - 不正行為を逆にビジター(ライナス)になすりつけられる？
 - メールオンリーで取得できるアカウントの追跡はどこまで可能か？(IDの本人性確認の問題。)



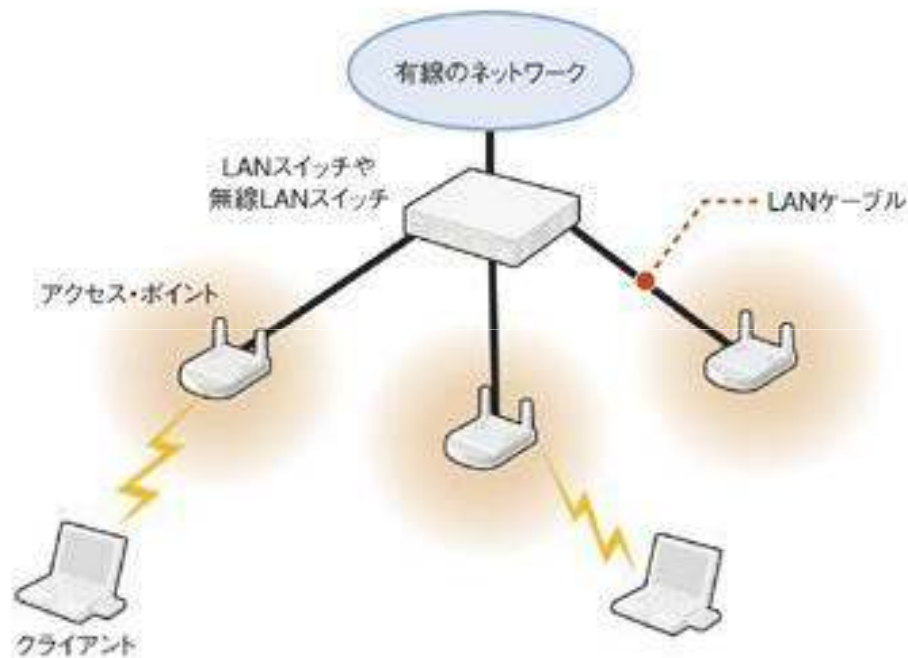
メッシュネットワーク

■ インフラ側での無線利用

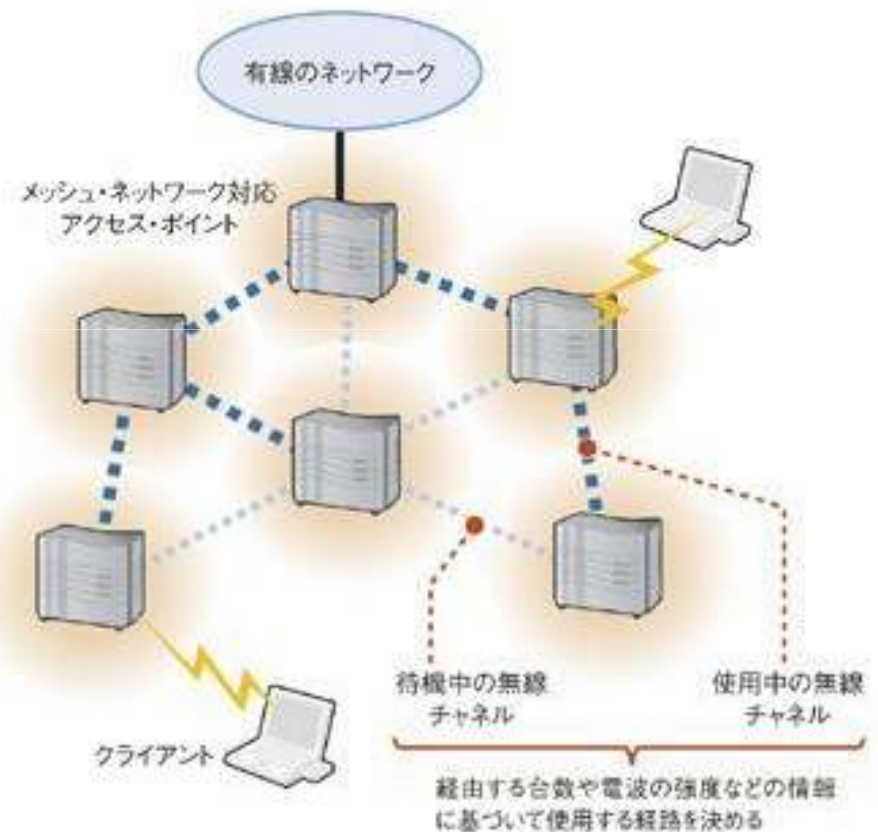
- APと利用者端末ではなく、インフラ構築に無線を利用してネットワークを構築(メッシュネットワーク)。
- 各端末は無線ルータに接続し、そこからインターネットにアクセスする。

メッシュネットワーク概念図

●従来の無線LAN

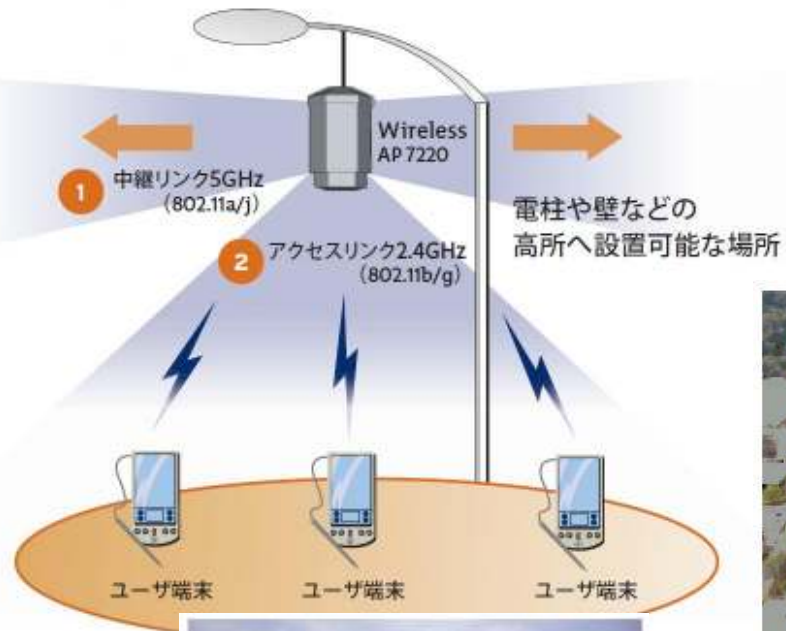


●無線メッシュ・ネットワーク



<http://itpro.nikkeibp.co.jp/article/COLUMN/20060221/230150/?SS=imgview&FD=-948522884&ST=nettech>

製品例(nortel)



端末～AP間のアクセスは、
802.11b/g, エントランスには、
802.11a or WiMAX




Nortel Wireless Mesh Network 製品紹介パンフレットより



その他の事例

- Meraki Network (<http://meraki.com/>)
 - 各家庭・店舗に端末を設置し、メッシュネットワークを構築。
- NextWave wireless
 - Nortel同様メッシュネットワーク用の製品を発表



メッシュネットワークにおけるセキュリティ

■ アクセス部分

- WLANと同様

■ メッシュネットワーク部分

- 802.11s等(802.11のメッシュNWへの拡張)
- メッシュ部分は従来WLANとは構成が異なるため。
- ルーティング部分は、有線用のOSPFやアドホック用のAODVライクのHWMP (Hybrid Wireless Mesh protocol)などを利用。



WiMAX

■ WiMAX

- Worldwide Interoperability for Microwave Access
- IEEE 802.16で規格されている無線通信規格
 - 802.11系とは異なる
 - 802.16-2004
 - 固定通信用の規格(最大50kmの伝送距離)
 - 旧FWAの概念
 - 802.16e
 - モバイル向け通信規格
 - ハンドオーバーを実現



WiMAXのセキュリティ

■ 暗号化

- DES(data encryption standard), 3DES, AES

■ 認証

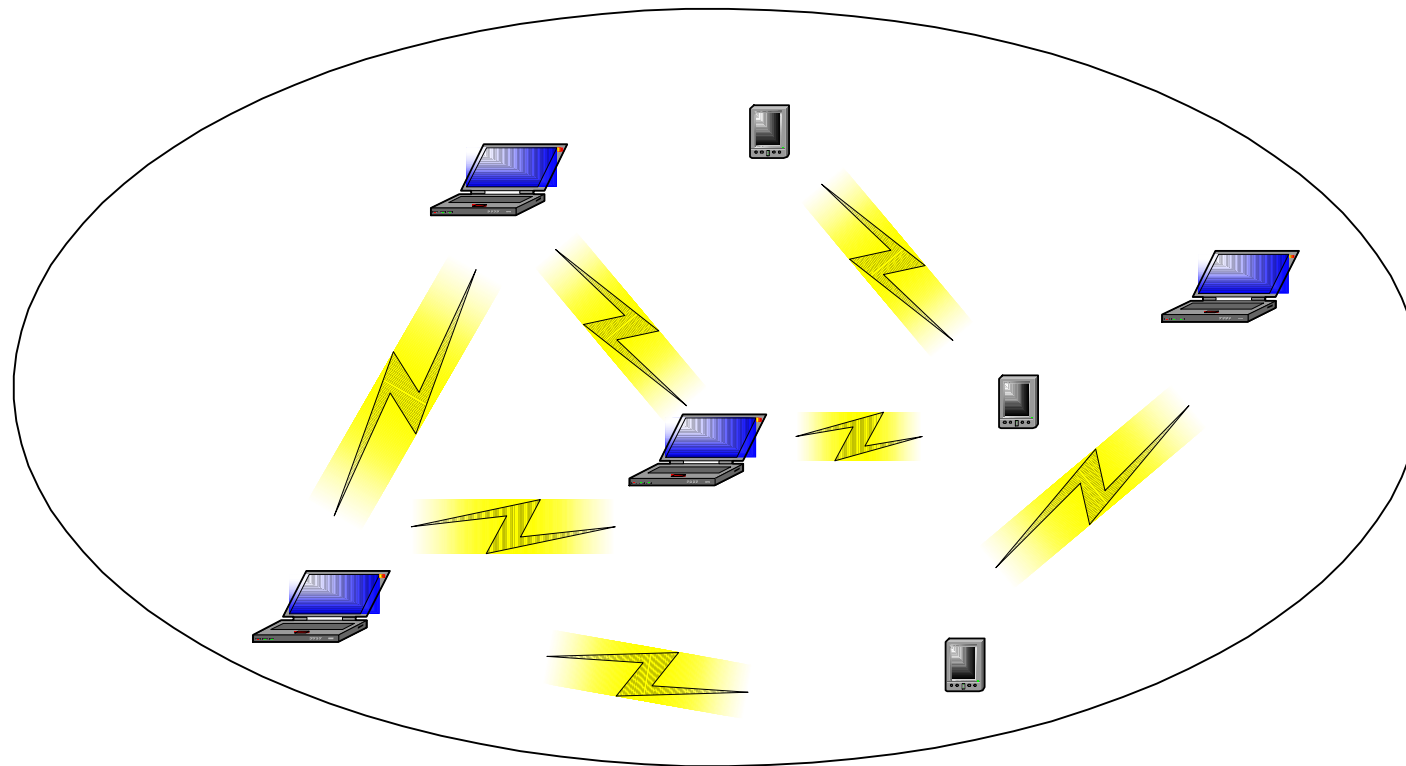
- 証明書利用の機器認証
- EAP利用の利用者認証

KDDIの次世代構想



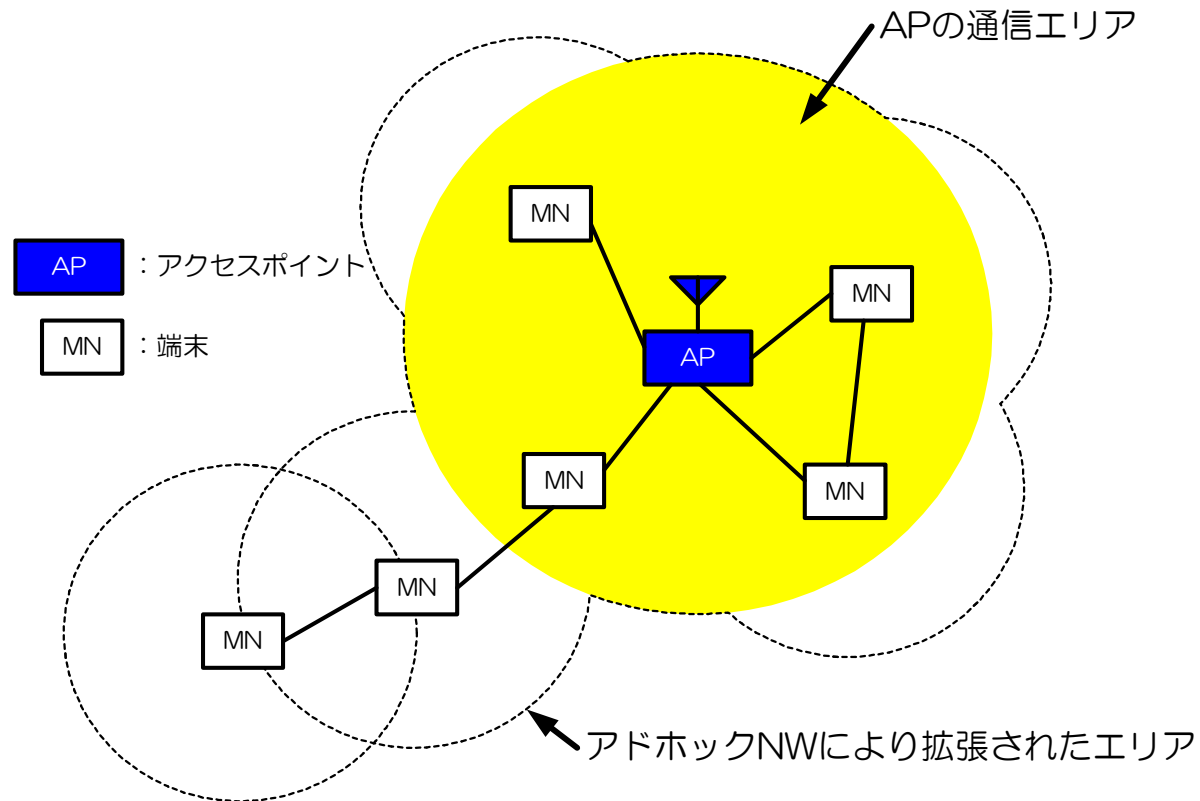
アドホックネットワーク

- 端末同士でネットワークを構築するネットワーク



公衆無線LANエリア拡張

■ 無線アクセスポイントの提供範囲を拡張





メッセージの交換

- 専用のプロトコルが存在

- オンデマンド型

- 通信が必要になった際に経路探査の実施
例) AODV DSR

- プロアクティブ型

- 定期的に経路探査を実施
例) OLSR



ルーティングプロトコル

- セキュリティの観点からは・・・
 - 端末の協調と協力が前提
 - 不誠実な端末を想定していない
 - 全ての情報を正しいと信じて動作
 - 不正な行為が可能
 - 偽の経路情報の流布
 - 故意のパケットドロップ



セキュアな ルーティングプロトコル

■ セキュリティの機能

- 既存のルーティングプロトコルにセキュリティの機能を追加

- 暗号技術の利用

- デジタル署名、MACの利用
- 例) SAODV、ARAN
Secure AODV
公開鍵暗号系を利用
デジタル署名
一方向性ハッシュ関数



セキュアなアドホックルーティング プロトコルを動作させるためには

■ 前提条件

- 必要な情報(鍵やアドレス)をAPから取得するには、セキュアなアドホックルーティングを利用する必要がある。
- セキュアなアドホックルーティングを実施するには、APからそのための情報を取得する必要がある。
⇒矛盾が生じる。

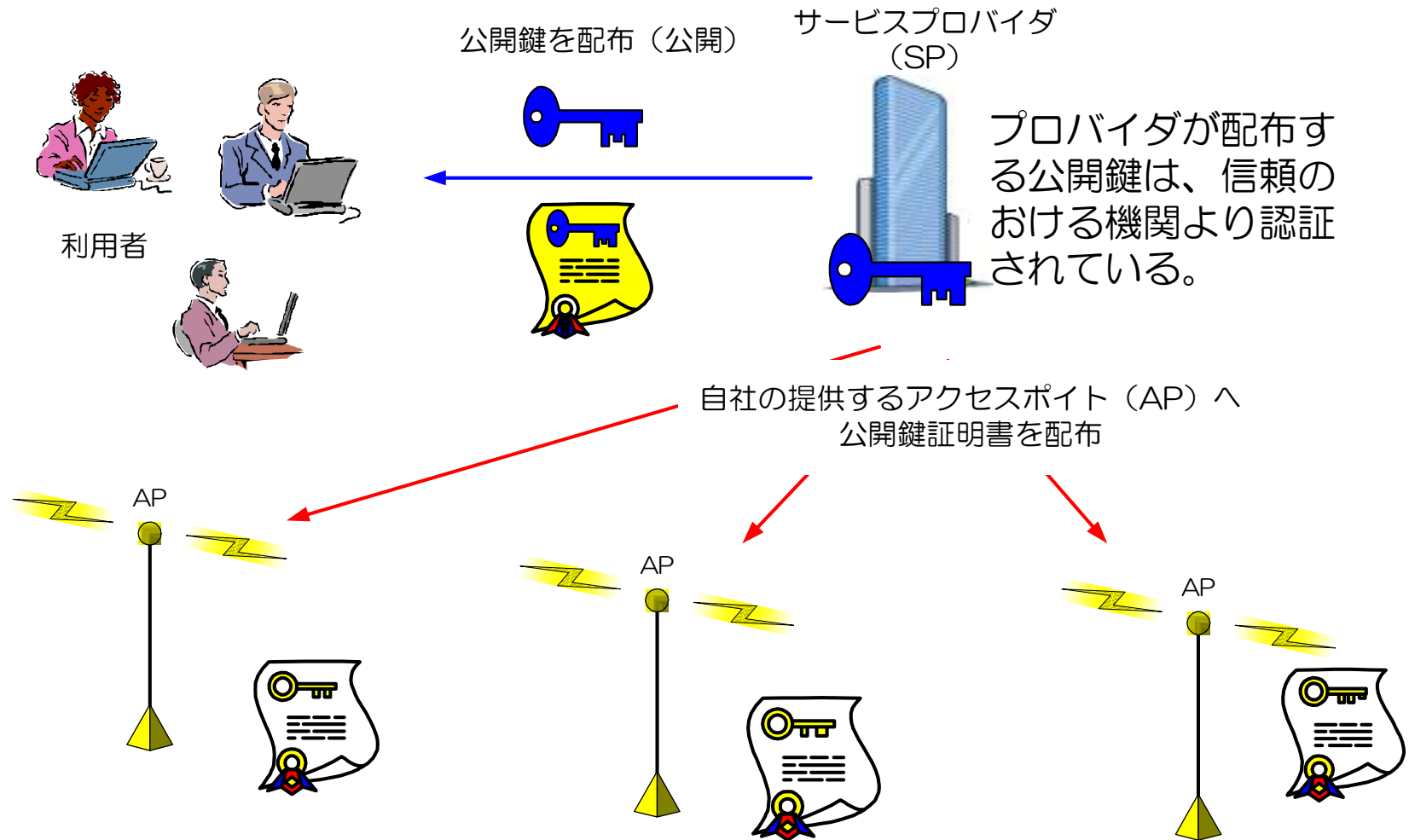


プロキシー端末の導入

■ プロキシー端末

- 提案手法により既にネットワークに参加している端末。
- 新たに参加する端末のために、新規端末とAPとの通信を中継(プロキシー)する。
- 普段は通常のネットワーク端末として動作している。

提案手法の前提条件





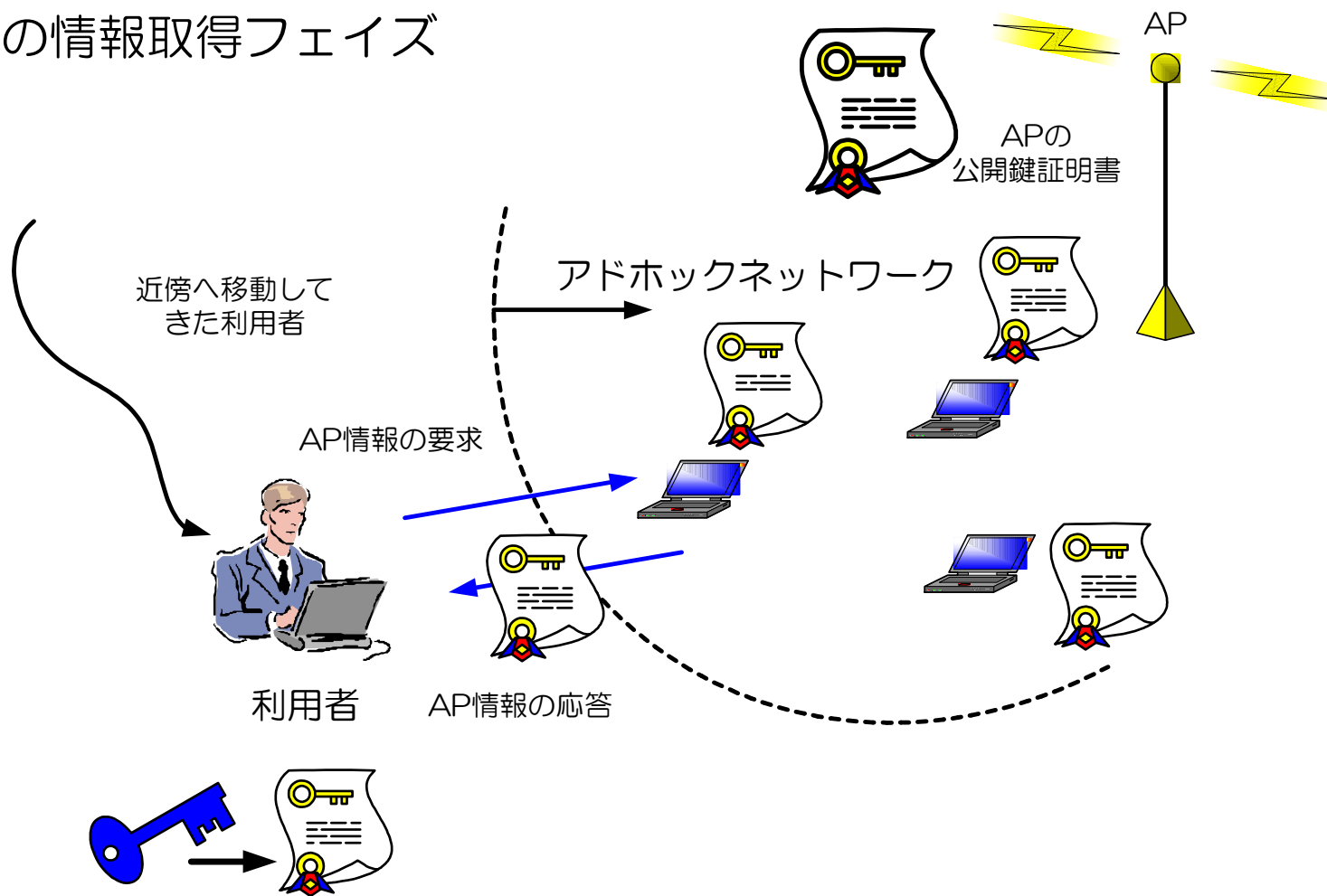
情報取得の手順

提案手法は2つのフェイズから構成される

1. AP情報の取得手順
 - APが提供する公開鍵証明書を取得
2. アドレス及び公開鍵証明書の取得手順
 - APにアドレス及び公開鍵証明書を要求

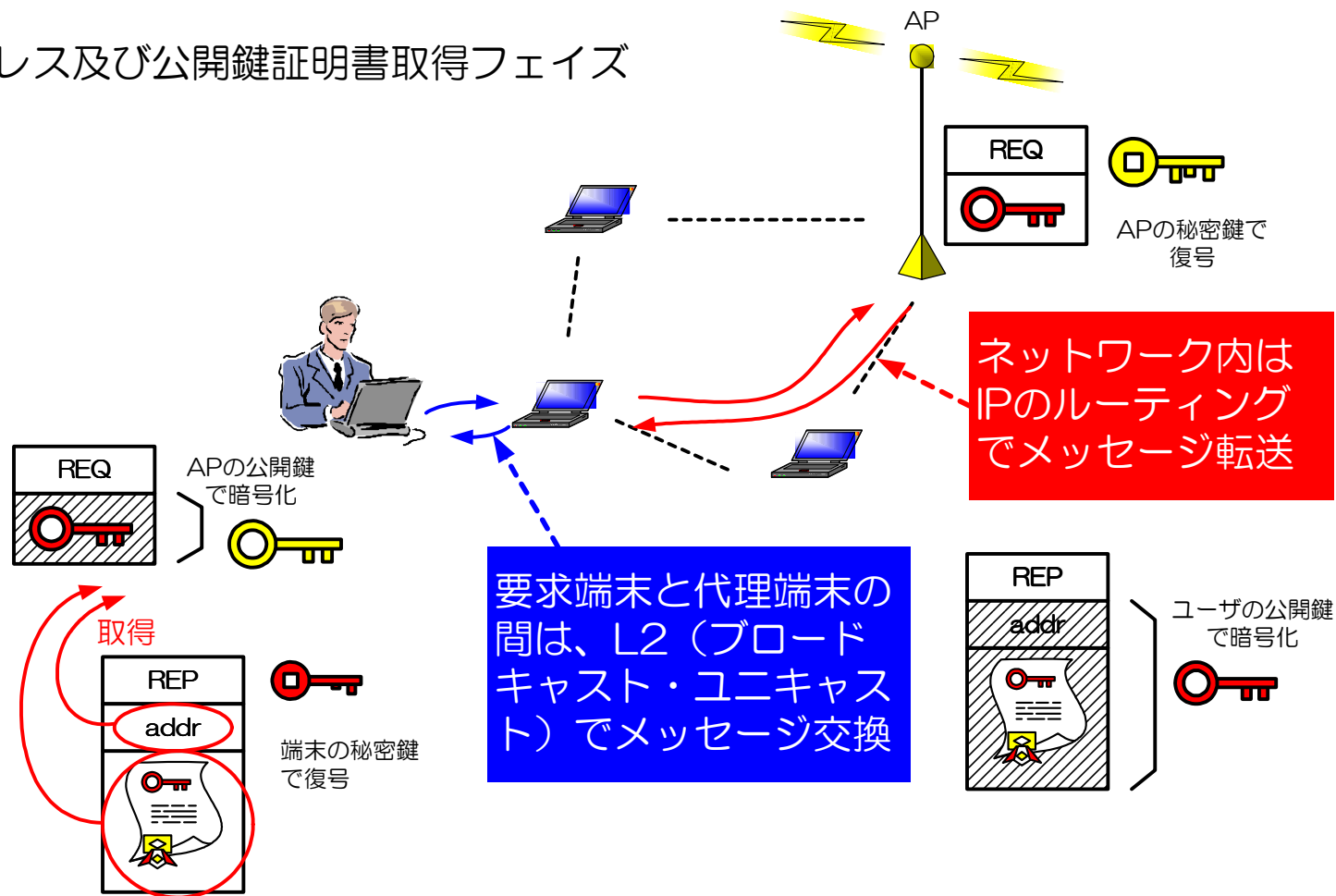
フェイズ(a)

APの情報取得フェイズ



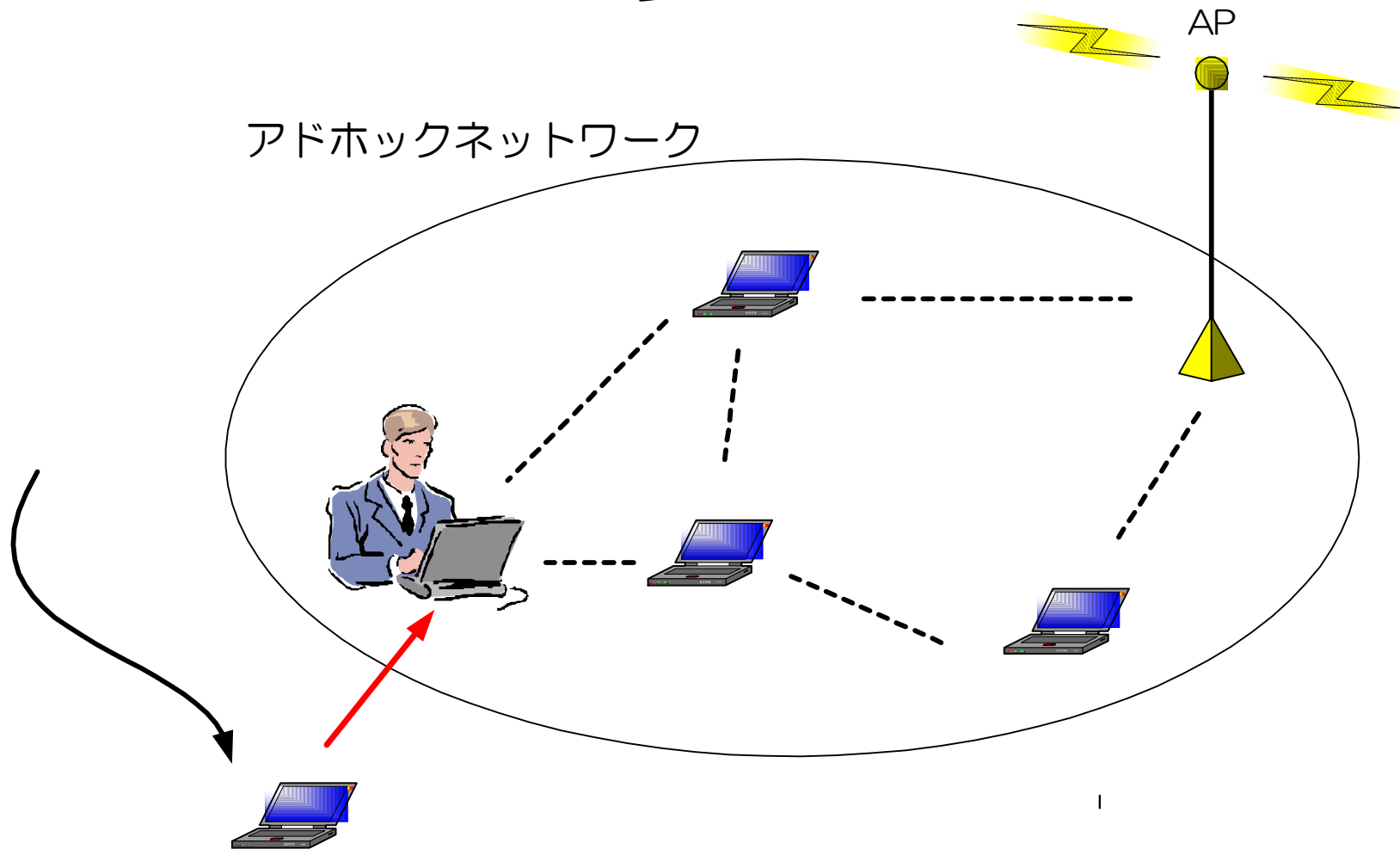
フェイズ(b)

アドレス及び公開鍵証明書取得フェイズ

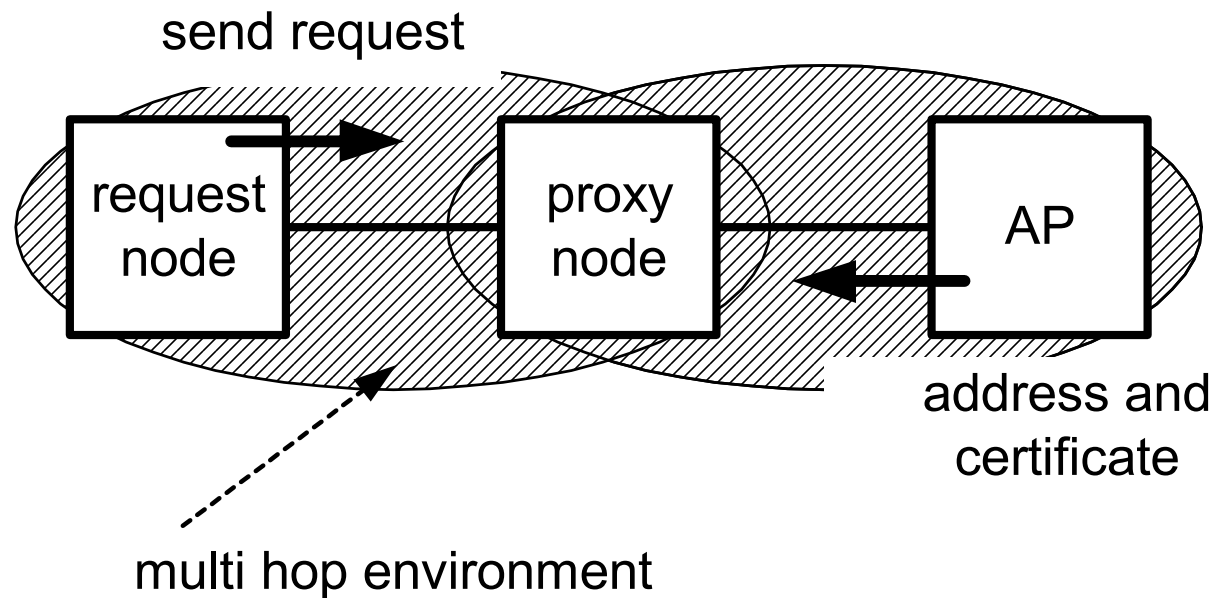


ネットワークに参加

アドホックネットワーク



評価試験(ネットワーク構成)



評価結果 1

アドレスと証明書の取得に要する時間

		Time	
Message Exchange for Addresses and Certificate	Phase 1	22 msec	
	Phase 2	Request Node	214 msec
		Proxy Node	18.3 msec
		Access Point	383 msec
	Others	83.7 msec	
Sub total		721 msec	
LAN device reconfiguration	Request Node	6.88 sec	
Total		7.60 sec	