Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

無線 LAN 装置のただ乗りに関する法的考察
--東京地裁平成 29 年 4 月 27 日判決を例に--

須川賢洋[†1]

概要：他人の無線 LAN アクセスポイントを踏み台としてネットワーク犯罪が行われることが大きな問題となっている．東京地判 H29.4.27 では、WEP キーを解読し他人のアクセスポイントに接続しただけでは電波法違反とはならないとの判断がなされた。本稿はこのような場合における不正アクセス禁止法等の諸法の可能性について考察する

キーワード：電波法、通信の秘密、暗号解読、不正アクセス禁止法、無線 LAN ただ乗り

Legal consideration on free-riding of wireless LAN devices
- The Tokyo District Court On April 27, Heisei 29 -

SUGAWA Masahiro [†1]

Abstract: It is a big problem that a network crime is carried out using a wireless LAN access point of another person as a stepping stone. In Tokyo District H.29.4.27, it was judged that it would not be a violation of the Radio Law by merely deciphering the WEP key and connecting to the other access point. This paper considers the possibility of various laws such as the unauthorized access prohibition law in such a case.

Keywords: radio law, secret of communication, decryption, unauthorized access prohibition law, wireless LAN only ride

1. はじめに

他人の無線 LAN アクセスポイントを踏み台としてネットワーク犯罪が行われることが大きな問題となっている。そんな中で、平成 29 年（2017 年）4 月 27 日、東京地方裁判所にて出されたサイバー犯罪の刑事事件において、隣家の WEP 方式によって暗号化されたアクセスポイントにただ乗りして利用し様々な犯罪行為を行った行為に対し、相手先システムに対して行った数々の為は犯罪で有罪であるが、電波法 109 条の「通信の秘密の侵害」部分のみにおいては、犯罪が成立せずに無罪であるとの判断が出された。

本稿では、この判決を一つの例とし、他所の無線 LAN アクセスポイントを不正に利用する行為に関して、各種法律の適用の可否を検討する。なお、あくまで判決を一つの例として捉えており、考察段階には、実際の行為とは異なる形態での不正利用や、裁判所が検討したものとは異なる法適用の可能性についても検討するものであることを断っておく。

2. 判例解説（東京地判 H29.4.27）1

不正アクセス行為の禁止等に関する法律違反、電子計算機使用詐欺、私電磁的記録不正作出・同供用、不正指令電磁的記録供用、電波法違反被告事件

(1) 事実の概要

被告人は、平成 26 年 2 月頃～6 月頃まで、不正アクセスやインターネットバンキングからの他人のお金の不正な引き出し等の数多くの犯罪の嫌疑で起訴された。罪となるべき公訴事実として挙げられたのは次の第 1～第 14 である。（第 4～第 13 については、一般の IT 用語を使い簡単に記すこととする）

第１

１　不正アクセス行為の用に供する目的で、平成２６年２月２０日、インターネットバンキングサービスになりすまし、同サービスに似せたフィッシングサイトの閲覧を促す電子メールを送信し、Ａ銀行に開設されたＢ名義の通常貯金口座のお客様番号、ログインパスワード、インターネット用暗証番号等の識別符号を同サイト上に入力させることにより、同識別符号が記録された電子メールを被告人管理のメールアドレス宛に自動送信させ、もってアクセス制御機能に係る他人の識別符号を取得した。

†1 新潟大学法学部
Faculty of Law, Niigata University
〒950-2181　新潟市西区五十嵐２の町 8050

Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

２　２月２０日午前１１時３７分頃から同月２１日午前９時２０分頃までの間、３回にわたり、被告人方において、パーソナルコンピュータを使用し､電気通信回線を通じて、Ａ銀行が設置したアクセス制御機能を有する特定電子計算機である認証サーバコンピュータに、第１の１記載のとおり取得したＢを利用権者として付された識別符号を入力し、同サーバコンピュータを作動させて前記アクセス制御機能により制限されている特定利用をし得る状態にさせ、もって不正アクセス行為をした。

第２

２月２１日午前９時２２分頃、A 銀行宛に B のメールアドレスが変更された旨の虚偽メールを送信。もって人の事務処理の用に供する事実証明に関する電磁的記録を不正に作出するとともに、Ａ銀行の事務処理の用に供した。

第３

２月２１日午前９時２３分頃、２回にわたり、Ａ銀行のＢ名義の通常貯金口座から、被告人が第三者をして管理させていた同銀行に開設されたＤ名義の通常貯金口座に合計８７万円の振込送金があったという虚偽の情報を与え、財産権の得喪・変更に係る不実の電磁的記録を作り、よって、８７万円相当の財産上不法の利益を得た。

第４

１　２月２６日午前１１時５分頃、E に対して同様のフィッシング

２　２月２６日午前１１時４６分頃から同日午後０時３４分頃までの間、３回にわたり､E の ID/PW で不正アクセス。

第５

２月２６日午後０時１４分頃、あらかじめＦから使用の承諾を得ていた株式会社己銀行庚支店に開設されたＦ名義の普通預金口座に９万６０００円の振込送金があったという虚偽の情報を与え、不法の利益を得た。

第６

３月２７日午後７時７分頃から同月２８日午前１０時１３分頃までの間、２回にわたり、G 銀行のＨの ID/PW で不正アクセス。

第７

３月２８日午前１０時２３分頃、Ｈ名義の普通預金口座から、被告人が第三者をして管理させていた辛信用金庫Ｉ名義の普通預金口座に２００万円の振込送金があったという虚偽の情報を与える。

第８

５月９日午前３時５９分頃から同月１５日午後２時１６分頃までの間、１８２万１２３３回にわたり、Ｊ株式会社のサーバに、脆弱性をついて不正アクセス。

第９

５月１５日午前０時３０分頃から同月１９日午後０時４９分頃までの間、７回にわたり、Ｋ銀行のサーバに株式会社Ｌの ID/PW を使い不正アクセス行為

第１０

第９の状態を利用し、５月１９日午後０時４６分頃から同日午後０時５５分頃までの間、３回にわたり、虚偽のＬが電子メールアドレス等を送信。

第１１

５月１９日午後０時５３分頃から同日午後０時５７分頃までの間、２回にわたり、Ｌ名義の口座から、被告人が第三者をして管理させていた辛信用金庫の M 名義の普通預金口座ほか１口座に合計２２２万７０００円の振込送金があったという虚偽の情報を与える。

第１２

(2) 有限会社Ｎのインターネット口座の暗証番号等を入手しようと考え、６月３日午後１時２６分頃、ウィルス「決済情報 8.exe」を添付した「ご注文決済のお知らせ」と題する電子メールを送信、感染させた。

第１３

６月１０日午後１１時４３分頃、Ｐネット銀行サーバにＯ株式会社の ID/PW で不正アクセス。

第１４

被告人は、総務大臣の免許を受けず、かつ、法定の除外事由がないのに、６月１１日午前１１時２８分頃、被告人方において、無線設備（型番「(△△△△△△△)」。平成２８年押第２５号符号１）を設置して、無線局として運用可能な状態に置き、もって無線局を開設した。

被告人はこれらの犯行を行うにあたって、あらかじめ特殊な無線装置（型番「(△△△△△△△)」を購入し、それと専用のソフトウェアを組み合わせて、空中に飛んでいる電波を解析し、その内の向かいの家にある WEP 方式のアクセスポイントを見つけ、その WEP キーを解読したうえでそのアクセスポイントにただ乗りして犯行をおこなった。

(3) 判旨

・被告人を懲役８年に処する。
・押収してある無線接続機器１式を没収する
・電波法（109 条）違反の点については、被告人は無罪。

(4) 解説

第１～第 14 の公訴事実を見て分かるとおり、本犯行は非常に悪質であり、不正送金による財産的被害は合計５１９万円余りと非常に高額である。また、被告人は同種前科による仮釈放中であった。本事件は無罪となった電波法違反を除いても､不正アクセス禁止法違反(不正アクセス罪、フィッシング罪)、「刑法」の電子計算機使用詐欺罪、私電磁的記録不正作出・同供用罪、不正指令電磁的記録供用罪（いわゆるウィルス使用罪)の事件として立件されている。このうちもっとも量刑の高いのが「電子計算機使用詐欺罪」であり、最高刑は懲役 10 年である、検察はこれを主罪と

Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

し、さらに併合罪として加重し懲役 12 年の求刑をしたものと思われる。裁判所はそれに対して懲役８年を言い渡した。

この事件において、本論文の論点との関連で非常に重要な事項として、被告人はこれらのサイバー犯罪を行う際に自宅の ISP から直接行わず、向かいの家の無線 LAN アックセスポイントに不正にただ乗りしていたことが挙げられる。ちなみに、被告人は向かいの家の無線 LAN にただ乗りしたのは自分ではない旨の反論を行っているが、被告の PC に当該隣家の WEP キーが保存されており、その主張は否定されている。また、その PC からは犯行に使われたコンピュータ・ウィルスも保存されていた。

さて、被告が使用していた無線設備（型番「(△△△△△△△△)」は、PC に外付けする無線 LAN アダプタで、そもそもその出力が日本国内で許可されている出力を超えており、そのまま使うと出力の点でも電波法違反になることが繰り返し警告される（画面に出る）ものであった。当然、被告人はそのことを承知していたはずであり、裁判所はこの点も量刑決定の判断理由に挙げている。

そして何よりも特筆すべきことは、この無線設備（型番「(△△△△△△△△)」はクラッキング用の Linux に組み込まれているソフトウェアと組み合わせると、後述の「ARP リプライ攻撃」によって WEP キーを取得することができる点にある。判決文によれば、被告人はこの無線 LAN アダプタをインターネットオークションにて２回にわたって計３台を購入している。明らかに当初から踏み台用の無線 LAN アクセスポイントを探していたものと推定できる。

かくして被告人は一連の犯罪を行うにあたって身元を隠すためにまず、向かい宅の WEP 方式によって通信保護された無線 LAN アクセスポイントの WEP キーを解読ソフトを使って探りだし、それを使って無線 LAN 装置から各種アクセスを行ったものである。

そこで、検察は刑法や不正アクセス禁止法違反と併せて、この WEP キーを解読して隣家の無線 LAN アクセスポイントに接続した行為が電波法 109 条 1 項『無線局の取扱中に係る無線通信の秘密を漏らし、又は窃用した者は、一年以下の懲役又は五十万円以下の罰金に処する。』に牴触するとしてあわせて訴えた。しかしながら裁判所は、「ＷＥＰ鍵は、無線通信の内容として送受信されるものではなく、無線通信の秘密にあたる余地はない。」との判断を下し、その部分についてのみ無罪と言い渡したものである。

なお、上記電波法 109 条文言より分かる通り、本件で有罪となったとしても、それは最高刑が懲役 1 年であるものであり、不正アクセス禁止法違反の最高刑 3 年と同様、被告人の量刑に直接影響するものではない。この点は注意が必要である。

3. 無線 LAN アクセスポイントただ乗りの違法性の検討--様々な状況を仮定して

前述の東京地裁判決では、WEP キーを解析した上で無線 LAN 装置にただ乗りしたことが即、電波法でいう通信の秘密の漏洩・窃用には当たらないとしたが、このような行為について、様々な確度から法的な検討を行ってみたい。なお、この裁判例の場合とまったく同一の場合だけを想定するのではなく、考えられる様々なパターンを検討するものとする。

3.1 通常の通信傍受により WEP キー解析の違法性の有無

この事件は、たまたま API リプライ攻撃を用いて WEP キーを解読・入手したものであったが、ではそのような積極的な攻撃を行わずに WEP キーを取得した場合はどうなるであろうか。まず、もっとも初歩的な攻撃手法としてこのような純粋なパッシブ方式によるキー取得が何らかの法に触れるかどうかについて考察してみたい。

WEP 方式の暗号化に脆弱性があることは既に知られており、通信を数万パターン収集すれば解読可能であると言われている2。しかしこの手法は長時間にわたって粘り強く大量のパケットを集めなければならない。そこでこれを短時間で行う為に意図的に大量のパケットを相手方に送信させるのが ARP リプライ攻撃である。逆に言うと、十分な時間をかけて収集を行うのであれば、ARP リプライ攻撃を行わずとも WEP キーの解析が可能なことになる。このような完全なパッシブ型（受け身型）の解析の場合、周辺のコンピュータや通信機器に対して何の信号も発したり当てたりしていないので、影響をあたえることはなく、セキュリティの用語で言えば攻撃をしかけたとは解釈することができない。

この場合には、刑法の電磁的記録に関する各種罪はおろか不正アクセス禁止法さえ問うことは困難であると言えよう。電波法 109 条や 109 条の２を前提に考えてみても、この時点ではまだ取得しただけつまり、WEP キーの情報を傍受し鍵を入手しただけの行為であり、暗号通信の内容そのものを復元したわけではないので、即「秘密の漏洩・窃用」ということは無理であろう。当然、どのネットワークに接続してもいないので、不正アクセス罪なども成立しない。

よって犯罪として立件するためには、次の何らかのアクションを待つことになるわけであるが、そもそもこの行為自体を発見することが不可能に近いと言え、この段階での法の適用を考えること自体が現実的ではない。

3.2 アクティブにパケットを出す場合、「電子計算機損壊等業務妨害罪」は問えるか

では、今事件のように、「ARP リプライ攻撃」のような手法を使って自発的に鍵取得のために大量のパケットを発生

Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

させたらどうであろうか。

判決文によれば、被告は PC 購入当日に向かいの家の無線 LAN 装置の WEP キーを取得し、接続している。その際には ARP リプライ攻撃を用いた。ARP リプライ攻撃は「ＷＥＰ鍵を計算で求める前提として、通信している者が出しているパケットが少ない場合に、大量のパケットを発生させることで大量の乱数を収集するというものである」(判決文ママ)。

よって ARP リプライ攻撃の場合、相手方の無線 LAN ルータに対してなんらかの影響を与え作業を発生させていることになる。そうすると、何らかの法律問題が発生しうるのではななかろうか。以下に順に考察してみることとする。

まず、考えられるのは無理にパケットを作り出させることによって相手のコンピュータへの電子計算機損壊等業務妨害罪（刑法 234 条の 2）の可能性が出てくる。

しかしながら、同条は『人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害』とある。まず何よりも主たる判断基準となる電磁的記録の損壊、つまりデータの破壊は起きていない。強制的に新たなパケットを送るようにルータに要求することは、あるいは虚偽の情報若しくは不正な指令を与えたとは言えるかもしれない。しかし、次文の「使用目的に沿うべき動作をさせず、又は使用目的に反する動作」をさせたまでとは言えないであろう。ARP リプライ攻撃の場合、ルータが元々に通信秘密経路確率の為に必要な情報を要求するにすぎない。よって、同条の適用は難しいであろう。

同様に、161 条の 2「私電磁的記録不正作出・供用罪」も文言から適用は難しいであろう。

よって、暗号鍵の解析だけでコンピュータ犯罪に関する何らかの罪に問うことは難しいと言える。

3.3 解読したキーを用いてアクセスポイントを不正利用した場合、不正アクセス禁止法違反は問えるか

では、解読して入手したキーを使って他人の無線 LAN アクセスポイントを使ってしまった時点であれば、何らかの罪状に問えるのではないか。

その場合、もっとも可能性が高いのが「不正アクセス禁止法違反（不正アクセス罪）となるのではなかろうか。以下、考察してみたい。

不正アクセスとなるためには、まずその大前提としてその対象が特定電子計算機である必要があるが、特定電子計算機は電気通信回線に接続している電子計算機であれば良いので、無線ルータも該当する3。

次に、「不正アクセス」の定義に該当するかについてであるが、まず、2 条 4 項 2 号,3 号事例、つまり脆弱性をついての侵入について、ARP リプライ攻撃は WEP の脆弱性を探し出す行為ではあっても、それにおって得られた正規のキーを使うことは自体は脆弱性を用いた侵入にはならない。よってこちらは論外となる。

よって、1 号事例にて検証することになるが、不正アクセス罪が成立するためには、「アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせ」なければならない。WEP もアクセス制御だとは言えるであろう。問題は「識別符号」と言えるかどうかになる。

識別符号とは、「アクセス管理者が…その利用権者等を他の利用権者等と区別して識別するために用いるもの」である。つまり想定しているのは、一つ一つのユニーク ID ごとに一つ一つのユニーク Password が設定されている場合と言えよう4。WEP キーの場合は、アクセスする全員が同じキーを使うため、遽には識別符号と言えない可能性がある。MAC アドレス認証などを併用して個体区別ができるようにしておいた場合には当てはまるであろうが、あいにくとすべての一般家庭の無線 LAN 装置がそのような管理になっているわけではない。

しかし筆者は、これがオープンテラスのカフェテリア等であればともかく、家庭用のアクセスポイントであれば、そもそもホンの 2.3 人での利用しか想定していないので、個々の利用権者を厳格に区別できなくても、後段の「アクセス管理者によって、その内容をみだりに第三者に知らせてはならないものとされている符号」のほうを重視して識別符号と言うことができるのではないかとの見解を示す。その理由は、例えば一般家庭で 2.3 人で使われるパソコンにおいて、一個人ごとにログイン ID と PW を設定している場合は希で、通常はどうかすると認証なしにすぐに操作画面まで立ち上がるようになっているものさえ珍しくない。では、この PC にもし外部から不正侵入された場合に不正アクセス罪が成立しないかと言われるとそんなことはない。それと同様のことと考えるべきだと言えよう。

3.4 電波法 109 条違反に関する考察

最後に東京地裁判決で、無罪とされた電波法違反について考察する。本判決での起訴に用いられた 109 条と、それとは別に 109 条の 2 への牴触可能性と別々に検討することとする。

前述の通り裁判所は、109 条に該当しない理由として、「ＷＥＰ方式の無線ＬＡＮ通信において、ＷＥＰ鍵自体は無線通信の内容そのものとして送受信されることはない。」との前提で、「あくまで暗号文を解いて平文を知るための情報であり、その利用は平文を知るための手段・方法に過ぎない」として、通信の外郭にある情報であり知り得るもの

Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

であるから通信の秘密には該当しないとしている。「無線通信の秘密」とは、当該無線通信の存在及び内容が一般に知られていないもので、一般に知られないことについて合理的な理由ないし必要性のあるものをいうと解される。」との解釈である。なるほど確かに、WEP キーは暗号化通信を行うための外箱にかける錠前でしかないということであり、外箱に掛かっている鍵もしくは封印の番号を知ってそれを外したとしても、その箱を開けなければその箱の中身を見ることはできないので、通信の秘密を侵害したことにはならない…と考えれば、この判断はかなり賛同のできるものである。

しかしながら、総務省はこの裁判後の 2017 年 5 月 12 日に、この場合でも通信の秘密を侵害し得るという見解を出しており5、地裁とは異なる意見となっている。筆者としては裁判所側の見解を支持するものである。

3.5 電波法 109 条の 2 への牴触可能性

本判決において疑問視されていることの一つに、「なぜ検察は電波法 109 条 1 項違反として起訴したのか」という点がある。109 条は法制定よりある条文であるが、それとは別に平成 16 年（2004 年）の改正時に、暗号通信解読を禁じるための条文として「109 条の 2」が追加されている。『暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、一年以下の懲役又は五十万円以下の罰金に処する。』との規定となる。

国会での審議録によれば、サイバー犯罪条約批准のための改正であるようだが6、その際の説明では「従来ですと、無線通信の秘密については、漏示、窃用が実際に行われた後にしか処罰できませんでした。今回の罰則の創設によりまして、暗号通信の復元がなされた段階であっても、その復元が漏示、窃用の目的で行われた場合には処罰を可能とするとともに、その未遂についても処罰をすることが十分な抑止効果を図る」とある。制定意図として、通信内容の窃用前に暗号解読した段階で取り締まることを目指したものであると見て取れ、一見すると今回のような事案でも適用できそうに見える。

しかしながら、暗号化の為の鍵が果たして通信の「中身」であるかどうかという観点に立てば、前節 109 条での論点となんら変わらず、結果は同じになったかもしれない。しかし、109 条の 2 の第 3 項にて『３　前二項において「暗号通信」とは、通信の当事者（当該通信を媒介する者であつて、その内容を復元する権限を有するものを含む。）以外の者がその内容を復元できないようにするための措置が行われた無線通信をいう。』との定義がしめされており、ここからは外郭のスクランブル情報全般までも含めて通信と捉えることか可能であるとも考えられる。むろん確率論でしかないが、109 条の 2 にて起訴したほうが、有罪となる可能性は若干高かったのではなかろうか。

4. おわりに

無線 LAN アクセスポイントのただ乗りに関する法律の適合性を考えるに、筆者の私見として不正アクセス禁止法の適用の可能性があることを示した。

しかしながら、法律として不安定であることには変わりがなく、不正アクセス禁止法、もしくは、電波法の改正をもって不正接続を目的とした暗号キーの解読行為自体を禁じるような立法措置が必要であろう。電波法に「109 条の 3」を追記するほうが、改正の難易でもその後の運用も容易であると思われるが、このような暗号キーの解読だけでなくネットワーク攻撃のための様々な予備行為、例えばポートスキャンなども取り締まるのであれば7、不正アクセス禁止法を改正することのほうが良いとの考えを持つ。

WEP に関しては既に古い技術であり、WEP を使用しないように公私にわたる指導が行われてはいるが、WEP 方式を使った無線 LAN 装置が直ぐにゼロになることはとうてい望めず、このようなことを行う不届き者も今後も現れるであろろう。また、本稿の論点はそれ以外の暗号化通信にも十分に適用できるものであると考える。

悪意をもって他人のアクセスポイントを不正に使う者は、その後、他の犯罪を行うのであるから、そこで検挙し取り締まることはできるかもしれない。しかし、屋外で投稿動画を見るためにとりあえず手頃なところにあったからという理由で繋ぐような者もあとを立たないと思われ、情報セキュリティとネットワークの健全性の観点からは、こういった野良状態のアクセスポイント自体をなくす必要がある。

その為の具体的な法改正のあり方を次の研究課題としたい。

Vol.2017-DPS-172 No.20
Vol.2017-SPT-26 No.20
Vol.2017-EIP-78 No.20
2017/11/30

脚注

1 執筆時、判例集未収録。
裁判所 Web サイト（http://www.courts.go.jp/）収録

2 上原哲太郎 講演資料「無線 LAN の解読と「通信の秘密」」より
https://www.jilis.org/doc/conference2017/wifi2.pdf
3 電気通信事業法 2 条 1 項に電気通信とは「有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう。」とある。
4 警察庁「不正アクセス行為の禁止等に関する法律の解説」より
https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf
5 2017 年 5 月 12 日　朝日および日経
6 「第 159 回国会 衆議院 総務委員会 議事録 第 13 号」平成 16 年 4 月 13 日（火曜日）
7 ただし、ポートスキャンは犯罪の準備行為にあたり、刑罰化するには相当の慎重さを必要とするものであることは、断っておく。

その他　参考文献

・高橋郁夫「無線ＬＡＮただ乗り、電波法は「無罪」…懸念も」
・上原哲太郎，小坂谷聡．西口三千 講演資料「無線 LAN の法的論点」
https://www.jilis.org/doc/conference2017/wifi1.pdf