安心安全な公衆無線LAN提供のためのガイドライン

第 1.0 版

2014 年 11 月 5 日

無線 LAN ビジネス推進連絡会
一般利用者向け普及啓発・セキュリティ啓蒙委員会

本ガイドラインは、
公衆無線LANを提供する者が
意識しなければならない事や対策
についてまとめています

情報セキュリティ上の脅威
（第2章）

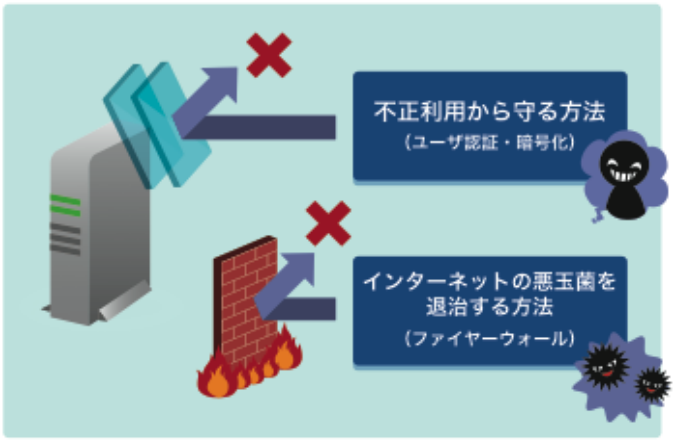
例えば…

盗聴されてクレジット番号、メール本文が盗まれる

なりすまされて、犯人にされてしまう

情報セキュリティ対策
（第4章）

例えば…



セキュリティの脅威に関連する法律や制度
（第3章、第6章）

有害サイトアクセス制限について
（第5章）

利用者の啓発、無線LANの活性化・利便性の向上
（第7章、第8章）

目次

1. はじめに 3
1.1. 本ガイドラインの目的 3
1.2. 本ガイドラインの用語 3
1.3. 本ガイドラインの対象 6

2. 情報セキュリティ上の脅威 7
2.1. 公衆無線 LAN における脅威の特徴 7
2.2. 脅威の発生箇所と種類 7
2.3. 情報セキュリティ上の脅威とその手口 9
2.4. 公衆無線 LAN が抱える課題 18

3. セキュリティの脅威に関連する法律について 21
3.1. 主なセキュリティの脅威についての分類 21
3.2. プロバイダ側にかかってくる責任などについて 22
3.3. 該当する各法律について 24

4. 情報セキュリティ対策 27
4.1. 概要 27
4.2. 通信の暗号化 27
4.3. 接続ユーザの認証 28
4.4. 網羅的な対策 29
4.5. アクセスポイントの適切な管理 31
4.6. 公衆無線 LAN とプライベート LAN の分離 32
4.7. フィルタリングの設定 32
4.8. 利用者への啓蒙 33
4.9. 有事の際のネットワーク開放 33

5. 有害サイトアクセス制限について 35
5.1. 背景 35
5.2. 現状と課題 36
5.3. 対策と今後について 37
5.4. 該当する各法律について 39

6. 通信の秘密と個人情報保護の適切な対応 40
6.1. 定義 40
6.2. ユーザの情報を保持する場合について 40
6.3. パーソナルデータの利活用に関する制度改正大綱と今後のあり方について 42

7. 情報セキュリティの利用者啓発について 45
7.1. ユーザ向けの啓発活動 45
7.2. 青少年に向けた啓発活動 46
7.3. 企業に向けた啓発活動 46
7.4. 利用者への利用規約の周知 47
7.5. 該当する各法律について 48

8. 無線 LAN の活性化・ユーザ利便の向上 50
8.1. ユーザ利便性の向上に向けた取り組み 50
8.2. その他通信との接続品質の維持 53
8.3. 運営課題などの情報共有方法について 54

1. はじめに

1.1. 本ガイドラインの目的

近年において、スマートフォンをはじめとするモバイルインターネット端末の普及が急速に拡大している。街中では多くの人々が当たり前のようにインターネットに接続しており、もはや公衆においても、インターネットに接続する為のインフラは社会的なライフラインといっても過言ではない状況にある。

このような状況下で公衆無線 LAN の利用機会も急激に増加している。スマートフォンやタブレット端末など Wi-Fi 搭載機器が広く利用者に受け入れられただけでなく、インターネット接続において非常に利便性が高い Wi-Fi 利用は、公衆におけるインターネット接続にとって今やなくてはならない存在であり、昨今では多くの事業者が公衆無線 LAN サービスを提供している。その提供主体も多岐にわたり、公衆無線 LAN サービスを主たるサービスとする事業者や携帯電話や固定回線を提供している従来の事業者のみならず、自治体や商店街に加え個別の店舗でもサービスを提供することが少なくない。

こうした無線 LAN 環境拡大の一方で、サービスの提供時における様々な課題も明らかになってきている。情報の窃取やなりすましによる不正アクセスなどのセキュリティ面はもちろんのこと、通信情報や加入者の個人情報の取扱いといった法律で定められている通信の秘密や個人情報保護への対応などである。公衆無線 LAN サービスを提供する事業者はこうした課題に対応しつつ、安心かつ安全なネットワーク環境を提供するということが求められている。

本ガイドラインはこうした社会的なニーズを踏まえ、公衆無線 LAN サービスの更なる発展の為に、国内の公衆無線 LAN すべてが安心して利用できるように、業界で一定水準以上の利用環境を維持することを目的として策定した。

1.2. 本ガイドラインの用語

本ガイドラインにおける用語は、それぞれ以下の意味において使用するものとする。

用語	意味
無線 LAN	広義では「無線を使って構築される LAN」を指すが、本ガイドラインにおいては、IEEE(米国電気電子学会) 802 委員会の IEEE 802.11 グループで標準化された伝送規格等を用いるものであって、特に 2.4GHz 帯又は 5GHz 帯の周波数帯の電波を使用するものを指す。
公衆無線 LAN	公衆無線 LAN アクセスサービス、および公衆無線 LAN サービス全体のことを指す。

公衆無線 LAN アクセスポイント	公衆無線 LAN を提供している事業者が、提供する店舗や事業所等に設置しているアクセスポイントと呼ばれる機器そのものを指す。
規格	IEEE グループで標準化された通信の規格。本ガイドラインでは無線 LAN を対象としているため、IEEE 802.11a/b/g/n/ac などの無線通信規格のことを指す。
事業者	電気通信事業法(昭和 59 年法律第 86 号。以下「事業法」という。)第 9 条による登録又は第 16 条第 1 項の届出により電気通信事業として公衆無線 LAN サービスを提供する者を指す。加えて、無償又は本来の業務に付随する形で公衆無線 LAN サービスを提供する者を含んだ概念を指す。
IP アドレス	インターネットに接続した機器を識別するために割り当てられるネットワーク層（IP 層）における識別子のことを指す。IP アドレスには、インターネット全体で一意に識別可能な「グローバル IP アドレス」と、限定されたネットワーク内でのみ一意に識別可能な「プライベート IP アドレス」がある。本ガイドラインでは、両者の区別が特に必要な場合のみそれぞれを「グローバル IP アドレス」「プライベート IP アドレス」と記して区別する。
MAC アドレス	ネットワーク上の機器を識別するために設定されているデータリンク副層（Media Access Control 層）における識別子のことを指す。
パケット	データをネットワークに伝送する際に分割したデータのかたまりのことを指す。パケットにはヘッダと呼ばれるメタデータが付加されており、ヘッダ内に、送信元や送信先のアドレス、送信するデータのサイズ等が含まれている。
シーケンスナンバー	TCP で送信されるパケットに付与される通し番号のことを指す。この番号を元に、パケットの順序や欠落をチェックし、データを復元する。
ARP	Address Resolution Protocol のことで、IP アドレスからそれに対応する MAC アドレスを動的に得るためのプロトコルのことを指す。
ICMP	Internet Control Message Protocol のことで、通信に関する情報の通知や、TCP/IP で接続された機器間で、互いの状態を確認するために用いられる。

TCP	Transmission Control Protocol のことで、信頼できる順序どおりに配送をおこない、欠損があった場合のエラー訂正を持つ。
http	Hyper Text Transfer Protocol のことで、Web ブラウザと Web サーバ間で HTML などのコンテンツの送受信に用いられるプロトコルのことを指す。通信内容は暗号化せずに転送される。
https	TLS（Transport Layer Security）で暗号化され、セキュリティを確保した HTTP のことを指す。URI（Uniform Resource Identifier）スキームの 1 つで、暗号化されたコンテンツを転送する。
FTP	File Transfer Protocol のことで、ネットワークでファイルの転送をおこなうためのプロトコルのことを指す。すべての通信内容を暗号化せずに転送する。
DHCP	Dynamic Host Configuration Protocol のことで、コンピュータがネットワークに接続する際に必要な情報を自動的に割り当てるプロトコルのことを指す。
DNS	Domain Name System のことで、階層的な分散型データベースシステムである。主に、ホスト名やドメイン名と、IP アドレスとの対応付けの管理に使用されている。
SSID	IEEE 802.11 の無線 LAN におけるアクセスポイントの識別子を指す。
識別符号	ID とパスワード（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）、指紋や虹彩（利用権者等の身体の全部若しくは一部の影像又は音声を用いてアクセス管理者が定める方法により作成される符号）、署名（利用権者等の署名を用いてアクセス管理者が定める方法により作成される符号）など、あるいはそれらの組み合わせを指す。
電気通信役務提供者	固定電話や携帯電話等の電気通信サービスを提供する会社の総称。通信キャリアと呼ばれることもある。
特定電気通信役務提供者	電気通信役務提供者および電子掲示板の管理者など電気通信を用いて他人の通信を媒介している者のこと。
発信者情報	ある情報の発信者を特定できる情報及び特定のために何らかの役に立つ情報のこと。
経由プロバイダ	インターネットサービスプロバイダ（ISP）のこと。いわゆる一般名称としての「プロバイダ」はこれを指すことが多い。電気通信役務のひとつに ISP も含まれる。

電気通信設備	電気通信をおこなうための機械、器具、線路その他の電気的設備のこと。
開示関係役務提供者	開示請求の相手方となる当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者のこと。
青少年	18 歳に満たない者を指す。
インターネット接続役務提供事業者	インターネット接続サービス事業者を指す。
青少年有害情報	青少年の健全な成長を著しく阻害するもの。有害情報を規定する法令は日本には存在せず、総務省は違法・有害情報を「違法な情報」と「違法ではない情報」に分け、「違法な情報」として著作権を侵害する情報、名誉を毀損する情報、児童ポルノ・わいせつ情報およびその他の違法な情報を分類し、「違法ではない情報」の中に人を自殺に誘引するような公序良俗に反する情報と、アダルト情報のような青少年に有害な情報を分類している[1]。
携帯電話インターネット接続役務	携帯電話端末又は PHS 端末からのインターネット接続サービスであって青少年がこれを利用して青少年有害情報の閲覧をする可能性が高いものとして政令で定めるもの。
無線 PAN	無線通信を介し、比較的狭い範囲においてデータの送受信をおこなう Personal Area Network のこと。

1.3. 本ガイドラインの対象

本ガイドラインは日本国内において無線 LAN サービスを提供する、またはこれから提供を考えている事業者を主な対象としている。

[1] 「インターネット上の違法・有害情報への対応に関する検討会 最終取りまとめ」, 総務省, 2009 年 1 月

2. 情報セキュリティ上の脅威

2.1. 公衆無線 LAN における脅威の特徴

公衆無線 LAN を広く設置し、だれでもどこでもインターネットに接続できるようになると、ユーザは便利になる一方で意図しない脅威に巻き込まれることもある。また、ユーザだけでなく事業者側が被害に巻き込まれる場合や、加害者となってしまう場合も存在する。これらネットワーク上での情報セキュリティの脅威には、データの破壊や消去、改ざん（改竄）、機密情報の盗聴や個人情報の漏洩、また、サービスの停止や不正利用、踏み台、ウィルス感染といった種類の脅威がある。さらに、個人利用者へのなりすましにより、クレジットカード情報を盗み出し、個人が金銭的な被害にあうような場合もある。このような脅威からユーザを守るため、セキュリティ対策は欠かすことが出来ない。

これまではインターネットにおける脅威はネットワークの外側、つまり WAN 側からくるものという考えが主流であり、「外部からくる脅威に対して内部のネットワークを守ること」、すなわち「外から来る脅威を如何にして内側に入れないようにするか」がセキュリティ対策の基本であった。しかし公衆無線 LAN においては、同じ LAN に接続されたユーザ（あるいはデバイス）自体が脅威になりうるため、内側からの攻撃も想定しなくてはならない。特に LAN 側ではアドレスの割り当てや経路制御など、インターネットに接続するために必要な極めて重要な手続きがおこなわれており、ここを攻撃されるとインターネットの仕組みそのものを根幹から揺るがす脅威となりうる。このため、ファイアウォールの設置などのような従来型の水際対策のみでは不十分であり、獅子身中の虫が存在することを前提とした内と外それぞれに対する高度なセキュリティ対策が求められる。

本章では、代表的な脅威を紹介しながら、公衆無線 LAN 事業において留意すべきセキュリティ事項を考察する。

2.2. 脅威の発生箇所と種類

公衆無線 LAN サービスの提供に際して想定されるセキュリティ上の脅威は、ネットワーク・システム上のさまざまな場所に潜在する。

図 2-1 は、主たる脅威の発生箇所を示したものである。また、公衆無線 LAN を提供する上で発生しうるセキュリティ上の脅威の分類を表 2-1 に示す。

表 2-1 脅威の分類

通信の傍受	自身が宛先ではない通信を受信する
情報窃取（盗聴）	自身が宛先ではない通信を受信しその内容を盗み見る
不正アクセス	アクセス権を持たない端末やネットワーク、情報に対して不正にアクセスし、情報の漏洩や改ざん、破壊をおこなう
なりすまし	正規のユーザ、アクセスを許可された端末などのふりをする
通信の改ざん	自身が宛先ではない通信の内容を、勝手に変更する
DoS/DDoS 攻撃	不正プログラムなどを使用して、情報の漏洩や改ざん、破壊、またサービスの停止などをもたらす
フィッシング	正規の Web サイトや電子メールを装い、クレジットカードやサービスの ID/パスワードといった個人情報を盗み出す
不正プログラムの実行と配布	不正アクセスやなりすまし、盗聴などをおこなうプログラム（ウィルス、マルウェア、ワームなど）を実行する

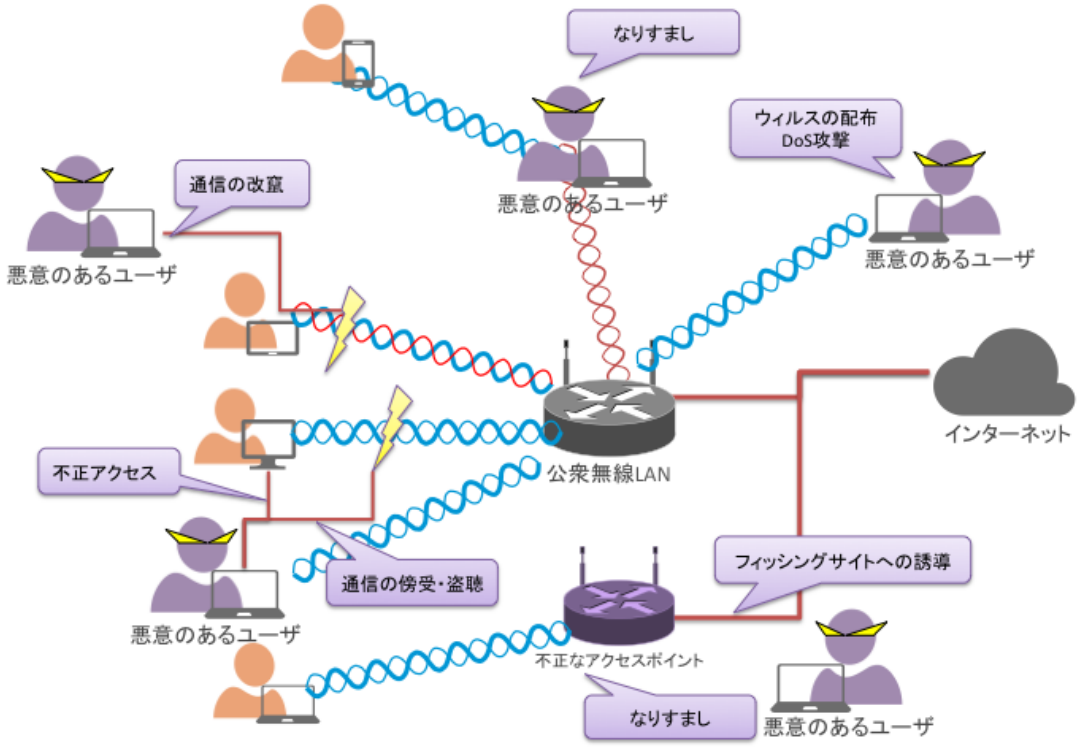


図 2-1 公衆無線 LAN に潜在する脅威

無線 LAN の場合、有線ケーブルでの接続と異なり、通信データは電波を介して空中に出力されるため、利用者が意図するか否かに関わらず、基本的には対応するアンテナさえあれば無線の出力範囲にいるだれもが発信された無線信号を受信することが可能となる。このうち「積極的意思をもって、自己に宛てられていない無線通信を受信すること」を「傍受」と呼ぶ[2]。無線通信の傍受はそれ自体では違法性は問われないが、その存在や内容を第三者に漏洩したり、窃用したりすると、電波法第 59 条に抵触し、罰せられることになる。

一方で、利用者や事業者からみた場合、無線 LAN サービスにおける脅威はこの傍受が容易であることを悪用したものが多く、また悪用される、されないに関わらず、傍受されうる通信の内容については多くの場合プライバシーの問題も関わるため、通信の傍受については法律上の解釈を問わず看過できない問題となっている。そこで、法律上の問題については第 3 章に記すとして、本章では主に技術的な観点から公衆無線 LAN における脅威について考察することを主眼とし、通信の傍受に関しても対象とする脅威の一つとして取り扱うこととする。次節以降で、各脅威について具体例とともに紹介する。

2.3. 情報セキュリティ上の脅威とその手口

2.3.1. 悪意のあるユーザによる通信の傍受

無線通信の場合、通信データは電波を介して空中に出力されるため、基本的には対応するアンテナさえあれば無線の出力範囲にいるだれもが無線信号を受信することが可能となる。

無線 LAN における通信の傍受は、主に利用者の各端末と無線 LAN アクセスポイントの間でおこなわれる。図 2-2 に、公衆無線 LAN において想定される傍受の形態を示す。

[2] 「電波法要説」，情報通信振興会, 2012 年 3 月

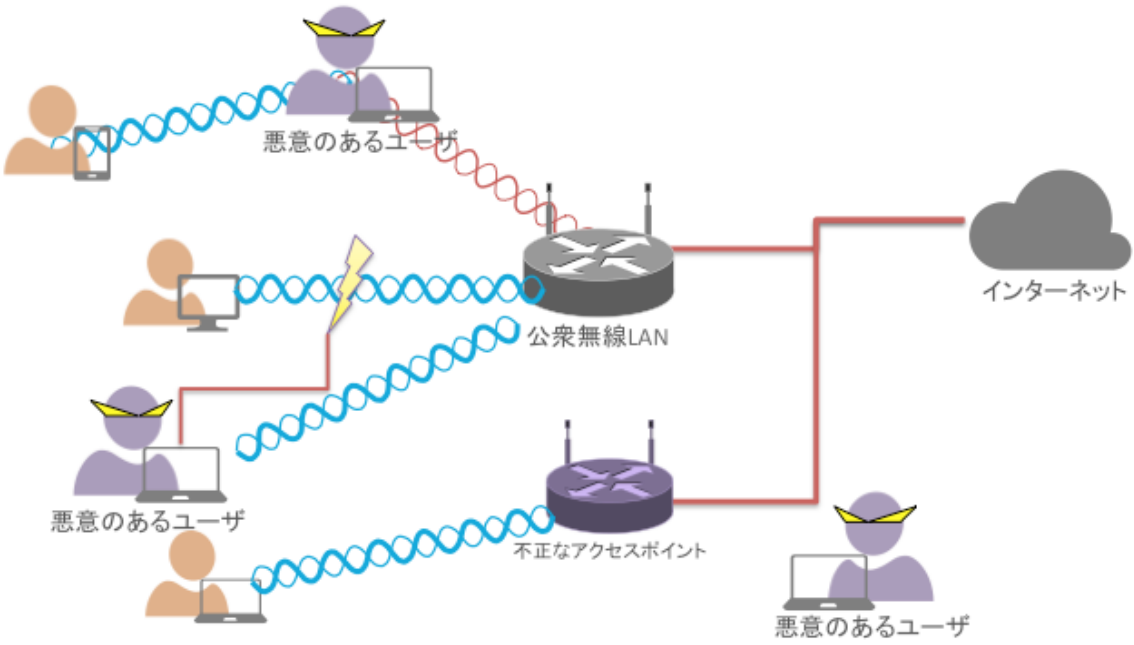


図 2-2 通信の傍受

無線通信の傍受それ自体では違法性は問われず、その存在や内容を第三者に漏洩したり、窃用したりすることによって処罰の対象となる。電波法要説によると、「窃用」とは「無線通信の秘密（存在又は内容）を発信者又は受信者の意思に反してそれを自己又は第三者の利益のために利用すること」と解説されており、悪用を前提とした情報の窃取や、窃取した内容を元におこなうなりすましや改ざん等もこれに該当するといえる。次節以降に通信の傍受を悪用した脅威について記す。

2.3.2. 情報の窃取

公衆無線 LAN における情報の窃取において最も一般的な手口は、正規のユーザが利用する端末と無線 LAN アクセスポイント間でやりとりされる通信データを、第三者がパケットキャプチャソフト等を用いて取得するやり方である。
図 2-3 に示す通り、各ユーザはアクセスポイントを経由して、それぞれの目的とする外部のサーバと通信をおこなう。この場合、アクセスポイントは WAN 側に接続するためのゲートウェイとして動作しており、ユーザからのリクエスト、および外部サイトからのレスポンスを含む全ての通信が経由されている。

多くの場合、端末とアクセスポイント間の通信データは暗号化されているため、無線信号を受信しても中身のデータが解読される可能性は低い。しかし、暗号化が施されていなかったり、暗号化の強度が低かったりする場合などにおいては、傍受者はこの間に流れるデータパケットを取得し、手元で再構築をおこなうことができ、通信データを容易に解読することが可能となる。これによってメールの中身や

WEB サイトへの入力項目、またこれらのアプリケーションサービスに付随する ID やパスワードなど、平文（暗号化されていないデータ）で送られる多くの種類のデータが窃取されることになる。

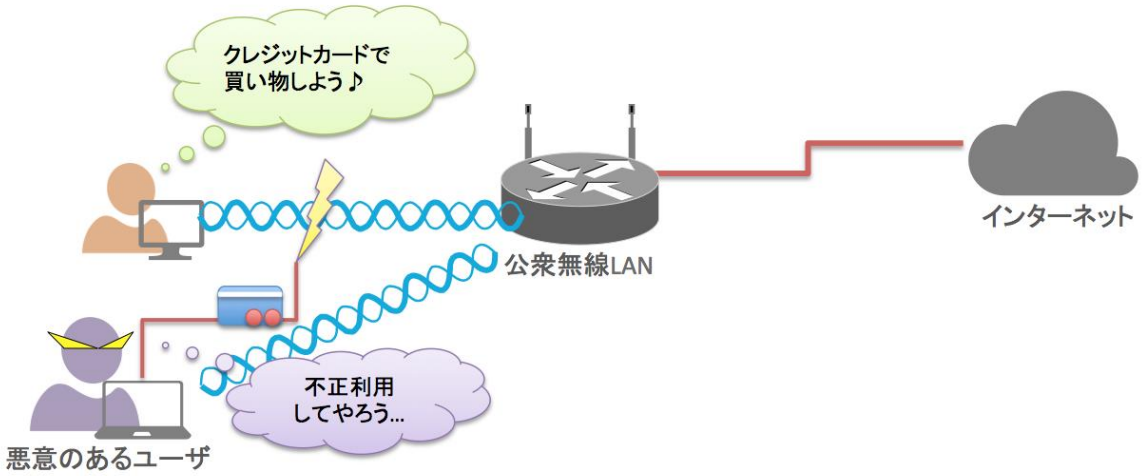


図 2-3 情報の窃取

また、より原始的な手法としては、正規のアクセスポイントの近傍に偽のアクセスポイントを用意し、利用者を偽のアクセスポイントに誘導・接続させることで情報を窃取するやり方もある。無線 LAN アクセスポイントの SSID は容易に取得することが可能なため、公衆無線 LAN が提供されている場所で同一の SSID を付けたアクセスポイントを設定し、利用者が間違えて接続するように仕向けることでそこに流れる情報を窃取する。

2.3.3. なりすまし

端末とアクセスポイント間に流れるデータの中には、制御データや実行命令等も含まれる。ここにはアドレスの割当てや経路制御、セッション管理等、インターネット通信をおこなうために必要となる基礎的な情報が含まれており、これらを窃取・悪用することで悪意の第三者が正規の利用者になりすましたり、通信自体を乗っ取ることもある。以下に代表的な手口を挙げる。

A)　ARP スプーフィング

ARP の応答を偽装することで、間違った IP アドレスと MAC アドレスの対応付けを作成し、悪意のあるユーザが他の端末になりすます。

B)　IP アドレススプーフィング

IP 通信において、悪意のあるユーザが送信するパケットの送信元アドレスを別の

機器の IP アドレスに偽装することでなりすましをおこなう。

C)　DNS スプーフィング
　DNS への問い合わせに対して間違った応答をさせ、悪意のあるユーザが仕掛けた端末にリクエストが送信されるように仕向けることで情報の窃取をおこなう。

D)　TCP セッションハイジャック
　TCP セッションは、シーケンスナンバーでパケットが管理されているため、通信を盗聴しシーケンスナンバーを合わせたパケットを途中で送ることで、クライアント/サーバ間のセッションを奪取（ハイジャック）することができる。

　これらは中間者攻撃（Man-In-The-Middle Attack）と呼ばれる攻撃の手口（またはその準備のための手口）で、第三者が通信の当事者間の通信経路に割り込み、主要な通信を仲介することで、当事者に気付かれずに情報を窃取したり、通信そのものを乗っ取ったりする手法である。
　なりすまし攻撃を受けた利用者は、攻撃者に自身の情報が窃取されたり、サービスを勝手に利用されてしまうばかりでなく、自身の ID（IP アドレスも含む）やアカウントが使われて、気付かぬうちに他の利用者やサービスなどに対して加害者になってしまう可能性もある。図 2-4 にその一例を挙げる。

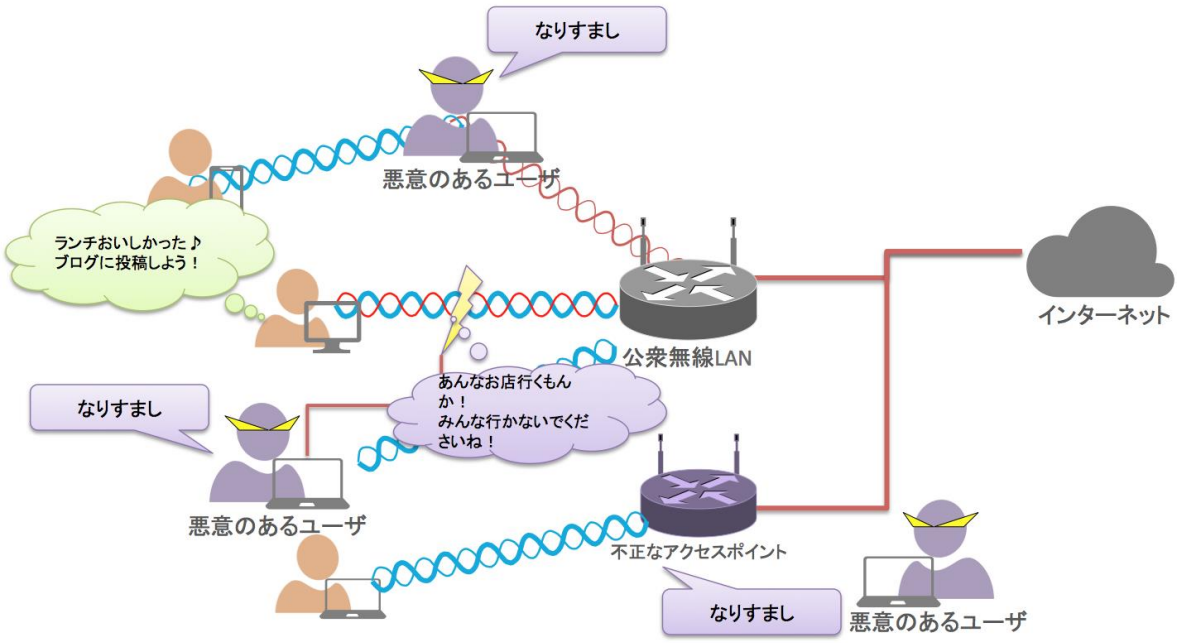


図 2-4 なりすまし

　このように、なりすましでは悪意の第三者が正規の利用者の ID やアカウントを

使って、偽のメールを出したり、ブログや掲示板に書き込みをおこなったり、クレジットカードなどの会員情報を窃取して勝手に EC サイト等で商品を購入したりといった被害を発生させる。

2.3.4. データの改ざん

中間者攻撃では第三者が通信の当事者間の通信経路に割り込み、当事者が気付かぬうちに主要な通信を仲介する。これを利用して、その中継の過程で送信者が送ったメールの内容を書き換えたり、Web サービスへのリクエストをすり替えたりすることもできる。このように、データの中継過程に悪意の第三者が入り込み、送信されるデータを書き換えたり、別のデータにすり替えたりすることを「データの改ざん」と呼ぶ。
データの改ざん例としては、以下のようなものがある。

A)　メールの改ざん

パケットキャプチャや Man-In-The-Middle Attack といった手法を用い、利用者がメールの送受信をおこなう際に、窃取したパケットの内容を書き換えてから中継をおこなう。

B)　Web サイトのデータの改ざん

FTP などのプロトコルを用いて Web サイトの更新をおこなっている場合、パケットキャプチャやセッションハイジャックをおこなうことで、利用者のリクエスト内容を書き換えることが可能である。利用者が更新しようとしたサイト上に、フィッシングサイトへ誘導するリンクの設置や、サイトの内容の書き換えなどがおこなわれる。

図 2-5 にメールを利用したデータの改ざん例のイメージを示す。

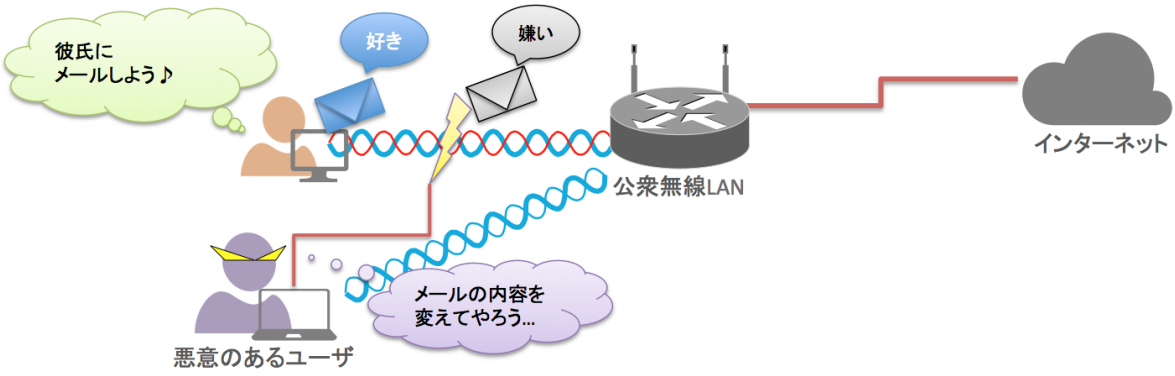


図 2-5 データの改ざん

2.3.5. 不正アクセス

公衆無線 LAN に接続された利用者同士は同一の LAN に属すことになる。そもそも LAN とはローカルエリアネットワーク（Local Area Network）の略であり、一般的には企業 LAN や家庭 LAN など同一組織内の構成員で構成されることを想定したものが多い。このため、同一の LAN に接続された利用者の利便性を高めるべく、プリンタ等のデバイスの共有や、ファイルシステムの共有などの機能が付加されているパソコンやアクセスポイントなども数多く存在する。これらの機能が設定されたまま気付かずに公衆無線 LAN に接続すると、同一のアクセスポイントに接続した見ず知らずの他人にプライベートなファイルを開示してしまったり、重要なアクセス権などを提供してしまったりすることに繋がる。

インターネットは外側（WAN 側）からの攻撃に対しては様々な対策がとられているが、ネットワークの内部からくる攻撃に対しては未だ脆弱である。管理者が不在の（または管理の行き届いていない）ネットワークでは、利用者側の自己管理に依存せざるを得ず、設定によってはコンピュータやネットワーク全体に深刻な影響を与えかねないセキュリティ上の欠陥（以下「セキュリティホール」と記す）が存在しているケースもある。攻撃者はこのようなセキュリティホールを突き、対策の甘いパソコンを攻撃したり、更にそれらを踏み台として内外のネットワークやサーバなどを攻撃する。以下に主な不正アクセスの事例を挙げる。

A)　スパムメール送信

踏み台と同等だが、無差別かつ大量に送信されるスパムメールを、悪意のあるユーザ自身の端末ではなく、利用者など別の端末を経由してメールを送信する。

B)　共有フォルダ/プリンタ等へのアクセス

コンピュータやスマートフォン等、端末同士でファイルなどのデータを交換する際に、共有フォルダという機能がある。共有機能については一般的に同一ネットワーク（セグメント）に接続された機器同士を対象としているものが多い。この場合、同一のアクセスポイントに接続された機器同士であればファイルやデバイスの探索/接続ができるため、共有機能が設定されたまま公衆無線 LAN に接続してしまうことで、悪意のあるユーザからそのファイルやプリンタへアクセスされる恐れがある。

図 2-6 に不正アクセスの一例として、踏み台とされたパソコンからスパムメールが送信されるケースについて図示する。

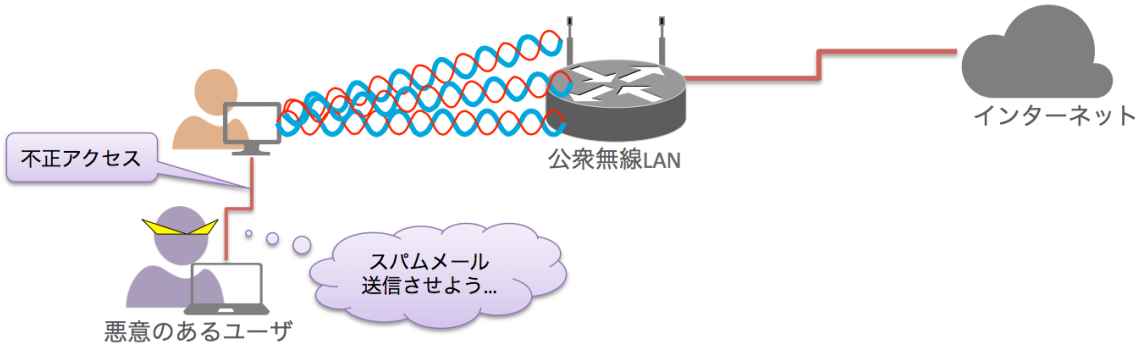


図 2-6 不正アクセス

2.3.6. サービス妨害

サービス妨害攻撃（DoS 攻撃：Denial of Service Attack）とは、攻撃対象となるネットワークやサーバに対し不必要なアクセスを繰り返すことにより、処理負荷やトラヒックを増加させてサービスの低下や機能不全を引き起こす攻撃である。分散した複数のマシンから一斉に攻撃をかける分散 DoS 攻撃（DDoS 攻撃：Distributed Denial of Service）もある。図 2-7 に分散 DoS 攻撃のイメージを図示する。

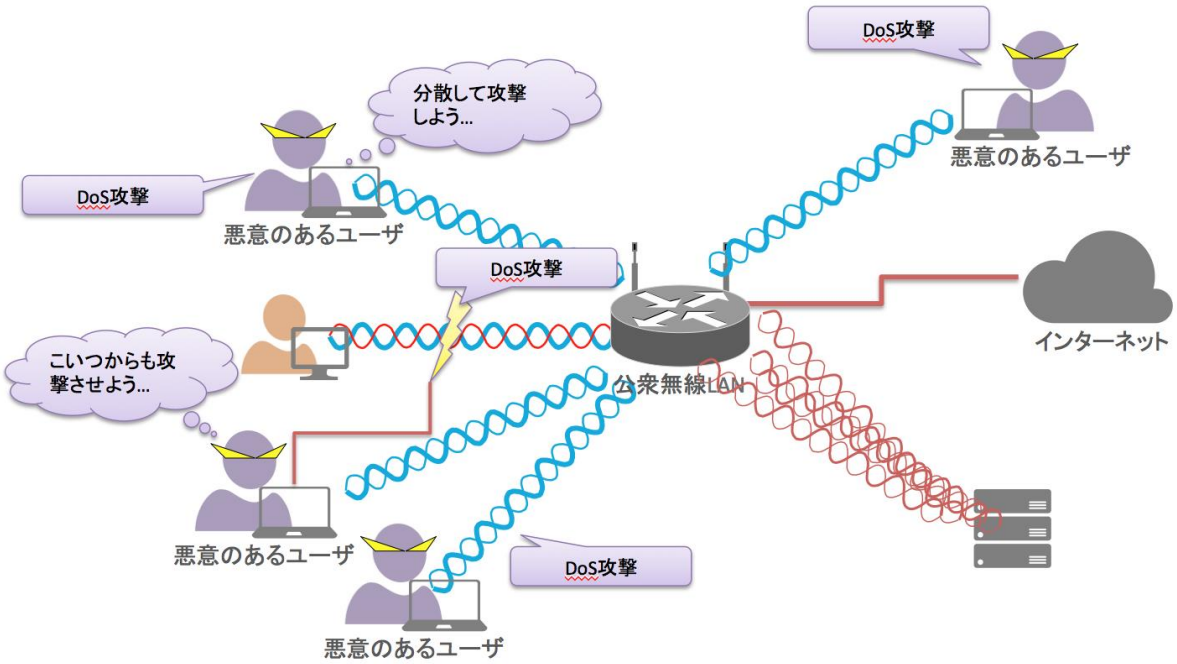


図 2-7 サービス妨害攻撃

サービス妨害攻撃の例としては、以下のようなものがある。

A)　帯域幅攻撃

リフレクター攻撃など、レスポンスのサイズが大きい問い合わせを大量におこない、攻撃対象の端末やネットワーク宛にレスポンスが届けられることで、ネットワーク機器のリソースや帯域を多く使用し、サービスの停止や処理速度の低下を引き起こす。

B)　プロトコル攻撃

スマーフやフラグルといった攻撃に代表されるように、ICMP 等、特定のプロトコルの特性を悪用して DoS/DDoS 攻撃をおこなう。

C)　ソフトウェア弱点攻撃

ランドやティアドロップ攻撃のように、通信の仕組みやソフトウェアの設計上の脆弱性を使用して DoS/DDoS 攻撃をおこなう。SYN パケットのやりとりや、フラグメントした IP パケットの再構成処理など、実装上の問題点を悪用した攻撃である。

2.3.7. フィッシング

フィッシングとは、メールや Web のリンク機能などを利用し、ユーザを偽の Web サイトなどに誘導し、誤って入力したパスワードやクレジットカードなどの情報を引き出す手口である。公衆無線 LAN においては、事業者がアクセスポイントへの接続を提供する際に、ユーザの ID やパスワード等を要求するケースが多い。多くの場合、アクセスポイントに接続したユーザは指定された Web の認証画面に誘導され、そこで ID やパスワード等を入力する仕組みとなっているが、このときに偽の認証画面に誘導し、ID やパスワード等を不正に入手する手口が考えられる。

本来、アクセスポイントは事業者が設置するため、悪意のある事業者でない限りこの事例は発生しないが、アクセスポイントを乗っ取られたり、同じ SSID を持つ偽のアクセスポイントを設置されるなどした場合にこのような被害が発生する可能性がある。図 2-8 にフィッシング攻撃のイメージを図示する。

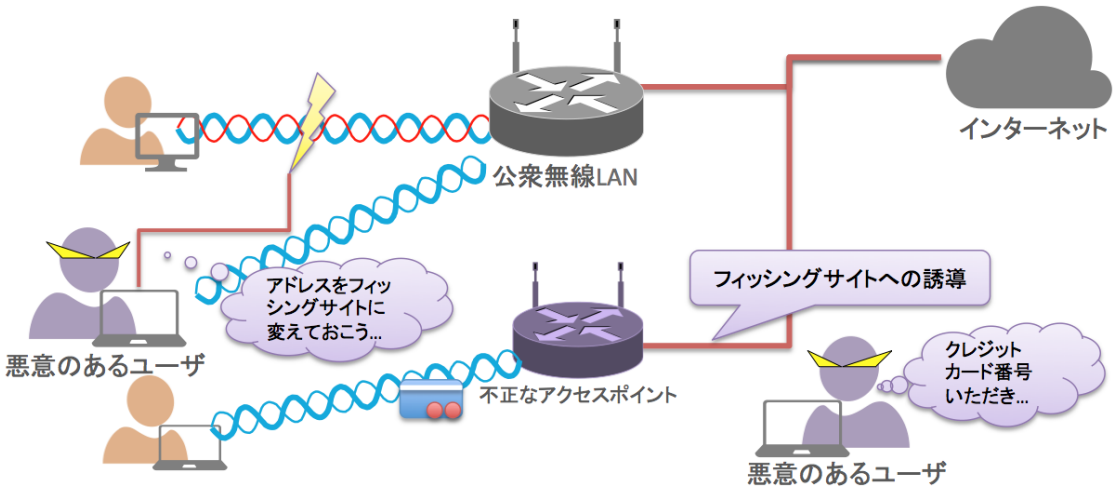


図 2-8 フィッシングサイトへの誘導

以下にフィッシング攻撃の代表的な手口を記す。

A) DNS キャッシュポイゾニング

DNS への問い合わせに対して、間違った対応付けの応答を DNS キャッシュ、または DNS の応答より先におこなうことで、ドメインとアドレスの対応付けを偽装する。これにより、利用者が問い合わせたドメインに対して、悪意のあるユーザが用意したフィッシング用のサイトへ誘導する。

B) アクセスポイントへのなりすまし

SSID の盗聴や、ARP スプーフィングをおこなって、悪意のあるユーザがアクセスポイントになりすまし、利用者からのリクエストに対してフィッシングサイトへ誘導するレスポンスを返却する。

C) 通信データの改ざん

TCP セッションハイジャックなどを用い、利用者へのレスポンスを改ざんすることで、利用者の正常なリクエストに対し、フィッシングサイトのレスポンスをおこなう。

2.3.8. 不正プログラムの実行と配布

不正プログラム（マルウェア）とは、不正かつ有害な動作をおこなう意図で作成された悪意のあるソフトウェアや悪質なコードの総称である。以下に代表的なマルウェアを記す。

A) ウィルス

それ自身は実行可能なファイルではなく、ターゲットとなったコンピュータ上の何らかのファイルに埋め込まれ（感染）、その感染したファイルが実行されることでそのコピーがさらに作成されていく、というものである。

B)　ワーム

ウィルスとは違い、そのプログラム自身が実行可能で、プロセスとしてターゲットとなったコンピュータ上で活動し続け、ネットワークを介して自身のコピーを作成する。また、バックドアといった、外部から侵入可能な経路を設置するようなものもある。

C)　トロイの木馬

有用なアプリケーションに見せかけてユーザに実行させる。内部には、実行したコンピュータ内のデータを破壊したり、個人情報などを漏洩させたり、といったプログラムが仕込まれている。

D)　その他

キーロガーに代表されるスパイウェアや、アプリケーションで実行可能なマクロに仕込まれたマクロウィルス、広告を大量に表示するアドウェアなど様々な種類の不正プログラムが存在する。

認証等をおこなわない公衆無線 LAN では、ネットワークに接続したユーザを特定できないため、上記のようなマルウェアの配布元として利用される可能性が高い。管理の行き届いていない公衆無線 LAN では、アクセスポイントや認証用のサーバなどにマルウェアが埋め込まれるケースもあり、知らずに接続したユーザがコンピュータウィルスに感染したり、更に感染したコンピュータが他のコンピュータに二次感染させるなど、被害がパンデミック化する可能性がある。

2.4. 公衆無線 LAN が抱える課題

2.4.1. 利用者の管理と攻撃者の特定

インターネットではネットワークに接続された端末の識別子として IP アドレスを用いている。何かしらの脅威が発生した場合、ネットワークやサービスの管理者はこの IP アドレスを元に攻撃者を特定し、このアドレスからの接続を遮断したり、サービスを使えなくさせたりといった対応をおこなう場合が多い。

一方、公衆無線 LAN では、多くの場合 NAT (Network Address Translation)機能を用いており、利用者は DHCP サーバ等から割り当てられたプライベート IP アドレスを用いてインターネットに接続する。プライベート IP アドレスは LAN 内でのみ通用する識別子であり、WAN 側から見ると公衆無線 LAN から接続された端末は NAT 機能により全て同一の IP アドレス（グローバル IP アドレス）として認識され

る。またプライベート IP アドレスは時限的であり、特殊な設定をしない限り接続するたびに異なるアドレスが割り振られる。このことから、仮に公衆無線 LAN に接続された端末から攻撃がおこなわれた場合、WAN 側から攻撃者の端末を特定することはほぼ不可能であり、場合によっては該当する公衆無線 LAN をネットワークごと切り離したり、サービスを使えなくさせる処置をとる必要性がある。この場合、同じ無線 LAN を利用する善意のユーザまでサービスを利用できなくなるといった弊害が生じる。

公衆無線 LAN の事業者は、回線を提供する経由プロバイダとしてプロバイダ責任制限法の対象となり、被害者からの申告があった場合には加害者の情報を開示する責任が生じる場合がある。これについての詳細は第 3 章を参照されたい。

2.4.2. 不正なアクセスポイントの排除

第 2.3.2 項で述べたように、正規のアクセスポイントと同じ SSID 等を付けた不正なアクセスポイントを近隣に設置することで、利用者の情報を窃取する手口がある。しかし、技術基準適合を受けた機器を用い、出力制限の要件等も満たしている限りにおいては、免許不要局の無線 LAN アクセスポイントを設置すること自体は法律・制度上問題とはならない。どのアクセスポイントに接続するかは利用者側の裁量に委ねられているため第三者がこれを阻止することは難しく、またそれによって通信が傍受されたとしても窃用などの直接的な被害を受けない限りは利用者側の落ち度ととられる可能性もある。

2.4.3. アクセスポイントの濫立による電波の干渉や使用チャネルの枯渇

日本国内において、IEEE 802.11 規格の無線 LAN に割り当てられた周波数帯は 2.4GHz 帯と 5GHz 帯である。同じ周波数帯の電波は相互に干渉し合うため、無線 LAN では割り当てられた周波数帯を更に複数の周波数帯（チャネル）に分割し、適切な間隔を空けて使用することにより干渉の問題を防いでいる。今日では、個々人でモバイル Wi-Fi ルータなどを持ち歩く人も多く、人の混み合っている場所はほぼ電波も混み合っている場所といえる。無線 LAN で利用できるチャネルは限られているため、このような場所では電波の干渉などから期待する伝送速度を提供できない可能性が高く、提供するサービスの品質（QoS）をどのように保証するかが課題となっている。これはセキュリティ上の脅威からくる問題ではないが、第三者のふるまいによってサービスが影響を受けるという点では共通するため、課題として挙げておく。

2.4.4. 青少年向けフィルタリングの問題

スマートフォンやタブレットは、通常携帯電話事業者の携帯電話網を使用してインターネットに接続しているが、各ユーザの年齢や性別は携帯電話事業者側で登録されており、端末と一意に紐付けられているため、端末情報を基に Web サイトや携帯電話事業者側で設定されたフィルタリングに応じて表示/非表示が切り替わる。

しかし、各ユーザが公衆無線 LAN に接続してそれぞれのサイトを閲覧しようとした場合、通信経路やアドレスが異なることから携帯電話事業者が持っている情報を参照することができず、すべてのユーザに対して情報を表示、または非表示という設定となってしまい、フィルタリング機能などが機能しないことがある。

3. セキュリティの脅威に関連する法律について

本章では、第 2 章で述べたようなモデルケースで発生する事例において、主に公衆無線 LAN 事業者等が関連する法律と、かかる責任の範囲について述べる。

3.1. 主なセキュリティの脅威についての分類

第 2 章で述べたモデルケースを、主なセキュリティの脅威について分類し、関連する法律について列挙する。

3.1.1. 無線通信の傍受

無線通信は通信可能範囲内においてはその通信信号を傍受することが可能である。そのため、通信信号を暗号化することなどによって、電波法でいうところの特定の相手方に対しておこなわれる無線通信とし、不特定多数に対してそれを傍受しその通信の内容を取得できないようにする必要がある。セキュリティの脅威としては、この暗号通信が悪意のある者によって復号され、無線 LAN の通信内容が窃取されることが挙げられる。この場合に関連する法律としては、電波法第 59 条および電気通信事業法第 4 条（通信の秘密）がある。また、無線 LAN の暗号を解読する行為は、電波法第 109 条の 2 で罰則規定が設けられており、これを禁止している。

3.1.2. 個人を詐称する行為

前述の無線通信の傍受などによって、悪意のある者に無線 LAN を利用しているユーザの情報、とりわけユーザ ID とパスワードのような識別符号が窃取された場合、あたかもそのユーザであるかのようにその他の端末と通信をおこなうなりすましがおこなわれる場合がある。また、Man-In-The-Middle Attack のように通信をしているユーザ間に悪意のある者が入り、ユーザ双方に対して通信相手のユーザだと詐称することによって通信内容を傍受あるいは改ざんする行為も存在する。さらに、識別符号を窃取されていない場合でも無線 LAN ネットワーク内の通信内容が傍受されている場合、セッションハイジャックといった行為によって個人を詐称した通信がおこなわれる場合がある。

これら個人を詐称して通信をする行為は、不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）第 2 条に抵触している。

3.1.3. AP やサーバへの攻撃行為

悪意ある者が暗号化された通信を傍受しようとする際、暗号を解読するために AP やサーバへ不正な通信や攻撃行為をおこなうことがある。また、不正な通信や攻撃行為によってサーバ機能を停止させること自体を目的とする DoS/DDoS 攻撃といった脅威も存在する。

これらの行為は、刑法第 234 条の 2（電子計算機損壊等業務妨害）や刑法第 246 条の 2（電子計算機使用詐欺）に抵触している。

3.1.4. 端末やサーバへの不正なアクセスおよびデータの窃用や改ざん

ユーザがあるネットワークに接続している際、共有機能によってファイルのやりとりや、接続されている機器の操作をすることができる。これは公衆無線 LAN についても同様であり、もしユーザが意図しないかたちで共有機能を有効にしている場合、悪意ある者がネットワークに接続しているユーザの共有フォルダへアクセスしたり、ネットワーク上にあるプリンタなどの機器への不正な操作や攻撃をすることが考えられる。また、共有フォルダに不正にアクセスされることで、そこに保存されているファイルを窃取されたり、コンピュータウィルスを送りつけられたりといった脅威も考えられる。

これらの脅威は、不正アクセス禁止法第 2 条や刑法第 234 条の 2（電子計算機損壊等業務妨害）、個人情報の保護に関する法律（個人情報保護法）に抵触している。

また、このような不正なアクセスによって、被害者端末や被害者サーバが DDoS 攻撃の踏み台やスパムメールの送信サーバにされることで加害者側となってしまう危険性もある。

3.1.5. コンピュータウィルスの作成および提供

悪意ある者が、ユーザの端末を不正に乗っ取ったり不正な指令をおこなわせるための不正なプログラムを作成したり送信したりすることが脅威として考えられる。これは、前述の各脅威によってネットワークに不正に侵入されたりユーザの端末やサーバが不正に操作されることによって外部に送信され、またそれによって別の端末に新たな不正なアクセスの経路を作り出したり DDoS 攻撃の踏み台にしたりと複合的な脅威となることが多い。

このようなコンピュータウィルスを作成したり提供したりする行為は、刑法第 168 条の 2 および 3（不正指令電磁的記録作成等）に抵触している。

3.2. プロバイダ側にかかってくる責任などについて

上記の各セキュリティの脅威は、基本的には悪意ある者が不正な通信や操作をすることで発生するのであって、それらのサイバー攻撃に対しての法的な責任や罰則は悪意ある者に課せられる。しかし、法律が定める電気通信役務提供事業者の責任や過去の判例などを参照するに、事業者側が各セキュリティの脅威に関連して責任を負う場合がある。

3.2.1. 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律によって規定されるプロバイダ等の責任の範囲について

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）は、特定電気通信による情報の流通によって、ある個人の権利の侵害があった場合に適用される法律であり、その中でプロバイダ等の責任の制限と被害者による加害者の発信者情報の開示請求権について規定してい

る。プロバイダ責任制限法という通称だが、特定電気通信役務提供者にはプロバイダのような電気通信役務提供者のほかに電子掲示板の管理者など特定電気通信の用に供される電気通信設備を用いて他人の通信を媒介している者が含まれる[3]。

プロバイダ責任制限法によって制限される責任は、情報の送信を防止する措置を誤って講じなかったことにより権利を侵害された者に対する責任と、情報の送信を防止する措置を誤って講じたことによる発信者に対する責任の両方である。

また、被害者によって開示請求される「発信者情報」とは、ある情報の発信者を特定できる情報及び特定のために何らかの役に立つ情報のことである。

3.2.2. 経由プロバイダ問題について

いわゆる経由プロバイダ問題とは、前述のプロバイダ責任制限法の定める対象に、発信者としてインターネットアクセスを提供するプロバイダ（経由プロバイダ）を含むか否かについて、従来よりおこなわれてきた議論と裁判における抗弁のことである。これについて、最高裁判決は、経由プロバイダを特定電気通信役務提供者とする判断をしている[4]。これによって、経由プロバイダも特定電気通信役務提供者としてプロバイダ責任制限法によって定められている責任の制限と発信者情報の開示請求の対象となっている。

3.2.3. その他の法律で規定されるプロバイダの責任について

前述のプロバイダ責任制限法は、特定電気通信による情報の流通によってある個人の権利の侵害があった場合に、プロバイダ等に適用される法律であるが、それ以外にも第 2.2 節で分類したように各セキュリティについての脅威が存在する。これらの各セキュリティの脅威に対する対策の規定としては、事業用電気通信設備規則に、コンピュータウィルスや DDoS 攻撃、不正アクセス等から電気通信設備を防護することを定めた規定がある[5]。また、電気通信事業者は管理規程で、事業用電気通信設備の工事、維持及び運用における情報セキュリティ対策に関する事項を定めなければならないとされている[6]。

これらの規定を遵守するため、DDoS 攻撃等のサイバー攻撃やコンピュータウィルスの感染拡大、不正アクセスなどによる異常なパケットの大量通信を識別し、それを遮断するなどの対処をおこなうに際して、「電気通信事業者による大量通信等への対処と通信の秘密に関するガイドライン（第 3 版）」（2014 年 7 月）が策定されている。この中で、大量通信等が発生した際に電気通信事業者が通信の遮断等の対応を適法におこなうために通信の秘密との抵触関係について整理している。

---

[3] 「プロバイダ責任制限法」第 2 条
[4] 「最判平成 22・48 民集 64 巻 3 号」676 頁
[5] 「事業用電気通信設備規則」第 6 条
[6] 「電気通信事業法施行規則」第 29 条

3.2.4. 発信者情報の開示請求と個人情報保護について

被害者の権利行使の観点から、発信者情報の開示請求時に開示される情報の幅は十分な広さにすることが望ましい。一方、発信者情報は個人のプライバシーに深く関わる情報であって、通信の秘密として保護されるべき事項を含んでいることに鑑みると、被害者の発信者情報の開示請求の権利行使にとって有益ではあるが、必ずしも発信者情報として不可欠とはいえない情報や、高度にプライバシー性があり、開示をすることが相当とはいえない情報まで開示の対象とすることは許されない。

今後予想される急速な技術の進歩やサービスの多様化により、開示関係役務提供者が保有すべきであって開示請求をする者の損害賠償請求等に有用と認められる情報の範囲も時々刻々変動することが予想され、その中には開示の対象とすることが相当であるものとそうでないものが出てくることになると考えられる。これらの関係と実務的運用のあり方については、今後も引き続き議論と検討を重ねていく必要があるだろう。

3.3. 該当する各法律について

以下に、関連する法律と該当する条文を抜粋する。

電波法

第五十九条 何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信(電気通信事業法第四条第一項又は第百六十四条第二項の通信であるものを除く。第百九条並びに第百九条の二第二項及び第三項において同じ。)を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。

第百九条の二 暗号通信を傍受した者又は暗号通信を媒介する者であっ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。

2 無線通信の業務に従事する者が、前項の罪を犯したとき(その業務に関し暗号通信を傍受し、又は受信した場合に限る。)は、二年以下の懲役又は百万円以下の罰金に処する。

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って、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。

4 第一項及び第二項の未遂罪は、罰する。

5 第一項、第二項及び前項の罪は、刑法第四条の二の例に従う。

電気通信事業法

第四条 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

不正アクセス行為の禁止等に関する法律
第二条の四の一
アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該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る行為(当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。)

刑法
第二百三十四条の二 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、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。

第二百四十六条の二 前条に規定するもののほか、人の事務処理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て財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する。

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）
第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
一 特定電気通信 不特定の者によって受信されることを目的とする電気通信(電気通信事業法(昭和五十九年法律第八十六号)第二条第一号に規定する電気通信をいう。以下この号において同じ。)の送信(公衆によって直接受信されることを目的とする電気通信の送信を除く。)をいう。
二 特定電気通信設備 特定電気通信の用に供される電気通信設備(電気通信事業法第二条第二号に規定する電気通信設備をいう。)をいう。
三 特定電気通信役務提供者 特定電気通信設備を用いて他人の通信を媒介し、その他特定電気通信設備を他人の通信の用に供する者をいう。
四 発信者 特定電気通信役務提供者の用いる特定電気通信設備の記録媒体(当該記録媒体に記録された情報が不特定の者に送信されるものに限る。)に情報を記録し、又は当該特定電気通信設備の送信装置(当該送信装置に入力された情報が不特定の者に送信されるものに限る。)に情報を入力した者をいう。

事業用電気通信設備規則
第六条 事業用電気通信回線設備は、利用者又は他の電気通信事業者の電気通信設備から受信したプログラムによって当該事業用電気通信回線設備が当該事業用電気通信回線設備を設置する電気通信事業者の意図に反する動作をおこなうことその他の事由により電気通信役務の提供に重大な支障を及ぼすことがないよう当該プログラムの機能の制限その他の必要な防護措置が講じられなければならない。

電気通信事業法施行規則
第二十九条の六および七
六 事業用電気通信設備の工事、維持及び運用における通信の秘密の確保に関すること。
七 事業用電気通信設備の工事、維持及び運用における情報セキュリティ対策に関すること。

4. 情報セキュリティ対策

4.1. 概要

本章では、第 2 章で述べたセキュリティの脅威に対して、公衆無線 LAN を提供する事業者として対応可能な対策について考察する。

図 4-1 に第 2 章にまとめた主な脅威について図解した。次節以降、それぞれの脅威に対する対応策を記述する。

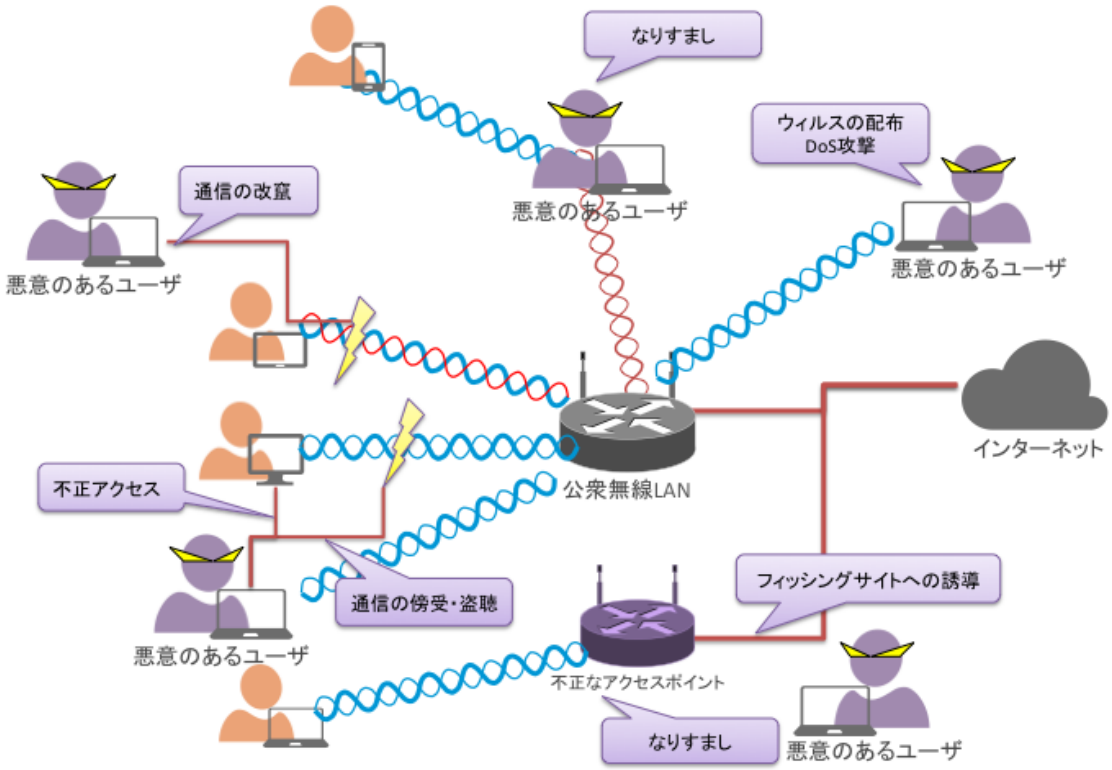


図 4-1 公衆無線 LAN における脅威

4.2. 通信の暗号化

無線 LAN を介した通信では、データは無線信号として空間に出力されるため、対応する受信アンテナがあれば基本的に誰もがこの無線信号を受信（傍受）することができる。また電波法においても通信の傍受自体には違法性はないとしているため、通信の内容を第三者の盗聴などから保護するためには、通信の当事者間で対応する必要がある。本節では、公衆無線 LAN において傍受されたデータを解析、盗聴されないための対策について述べる。

表 4-1 に示す通り、無線 LAN の暗号化方式にはいくつかの種類が存在する。この中で、暗号化していないものは公衆無線 LAN に接続していなくても通信内容を窃取することが可能である。次に、WEP 方式であるが、すでに数秒程度で IP パケットから暗号鍵を解読することが可能である。そのため、WEP 方式では暗号化されていても、解読されてしまうため、暗号化されていない状況と変わらない。現在、日本で多く採用されている WPA 方式での暗号化だが、WPA/WPA2 において、それぞれ複数のアルゴリズムが存在する。どちらもまだ解読はされていないため、少なくとも WPA-TKIP、または WPA-AES 方式を採用することが望ましい。

WPA/WPA2 では、対応している機器に違いがあるため、特に広くユーザを想定する場合に、ユーザが保持している端末の対応状況を視野に入れて、採用方式を検討する必要がある。

表 4-1 暗号化方式比較

	暗号強度	概要
暗号化なし	なし	暗号化せずに、AP-STA 間で通信をおこなうため、盗聴が容易
WEP	比較的容易	WEP 暗号化は解読アルゴリズムが出回っているため、パケットを解析して容易に盗聴可能
WPA（AES）	現状は不可能	CCMP 技術を用いた暗号化のため、現状では解読不可能
WPA（TKIP）	困難	1000 パケットごとに秘密鍵を更新するため、WEP より安全だが、アルゴリズムは WEP と同じため、解読される可能性あり
WPA2（AES）	現状は不可能	CCMP 技術を用いた暗号化のため、現状では解読不可能
WPA2（TKIP）	困難	1000 パケットごとに秘密鍵を更新するため、WEP より安全だが、アルゴリズムは WEP と同じため、解読される可能性あり

4.3. 接続ユーザの認証

公衆無線 LAN サービスの形態として、利用者側からみるとだれもが簡単にアクセスポイントに接続できる環境が望ましいが、提供者側から考えると不特定多数のユーザが接続するという環境を提供することは悪意のあるユーザを招き入れることにも繋がるため、推奨はできない。また、公衆無線 LAN を使用して悪意のある

ユーザが違法行為をおこなった場合、アクセスポイントを提供している事業者等は、違法行為がおこなわれた原因や攻撃者の足跡について調査できる環境を整えておくことが重要である。

インターネットにおいて攻撃者を特定する一般的なやり方としては、IP アドレスを用いるやり方がある。しかし第 2.4.1 項でも述べたように、公衆無線 LAN では利用者に一過性のプライベート IP アドレスを割り当ててインターネットに接続させる形態が多く、IP アドレスを辿って外部から攻撃者を特定することは難しい。このため事業者側では、アクセスポイントへの接続等の初期段階においてしっかりとした認証手続きをおこなうなどして、脅威の発生を未然に防ぐ（または脅威による被害を最小限に抑える）ための対策をおこなっていくことが望まれる。以下に、上記対策の一例を示す。

4.3.1. IEEE 802.1X 認証

IEEE 802.1X とは、無線/有線 LAN で使用可能なクライアント認証の規格である。

サプリカントと呼ばれる LAN 利用者の端末にインストールされたクライントソフトウェア、本規格に対応した LAN スイッチ、および RADIUS 認証に対応した認証サーバで構成される。このモデルを用いることで、認証サーバで認証されるまで、認証用の LAN スイッチ以外と接続することができない。

利用者側の事前登録と提供者側では利用者リストの管理が必要となるが、この方式を用いることで公衆無線 LAN 利用者の情報を管理することができる。認証処理は EAP というプロトコルを用いておこなわれ、ユーザ情報が認証サーバに登録されれば、サプリカントと LAN スイッチ、認証サーバ上でおこなわれるため、利用者が ID やパスワードを不用意に入力する、という事態を避ける事も可能である。

4.3.2. 認証サーバおよび通信ログサーバの設置

IEEE 802.1X 認証を用いることで、認証サーバおよび LAN スイッチ側で認証の仕組みが作成できるが、機能に対応した端末や、専用の認証サーバの作成が必要である。また、認証が完了した後は、通常のアクセスポイントと同様に全ての通信を通すため、サーバ側でログを保持するという機能は持っていない。

そこで、利用者は公衆無線 LAN アクセスポイントと接続した後、アクセスコントロールサーバを経由して認証サーバにて、利用者 ID とパスワードにて認証をおこなう。認証された場合、アクセスコントロールサーバを経由して、インターネット網に接続することこができる。また、アクセスコントロールサーバ側で通信ログの取得、およびフィルタリングをおこなうこともできる。

4.4. 網羅的な対策

4.4.1. 通信ログの保持

前述のような通信の暗号化や適切な認証手続きをおこなうことにより、多くの脅

威を未然に防ぐことが可能である。しかし、今日のサイバー攻撃はますます複雑化・巧妙化してきており、どのような対策をもってしても万全ということにはならない。このため、脅威が発生してしまった場合に備えた対応策も同時に検討しておく必要がある。本項では、何かしらの脅威が起こってしまった場合に必要となる対応として、通信ログの保持について述べる。

不正アクセスやサイバー攻撃といった攻撃がおこなわれた場合に犯人の捜査がおこなわれるが、第 2 章で述べたようにサイバー攻撃などをおこなうユーザは巧妙になりすましや踏み台の使用など、容易に足跡を辿られないような対応をおこなっているケースがほとんどである。このような攻撃者にとって、住所等の物理的な所在が特定されない公衆無線 LAN はそのターゲットにされやすい。

これまでも述べてきたように、公衆無線 LAN では IP アドレスによる攻撃者の特定が困難であるため、それ以外のやり方で攻撃者を特定したり、足跡を追跡したりする方法が求められる。この対応策の一つが通信ログの記録・保持である。

一般的に通信ログの内容は、アクセスポイントへの接続に関わる認証手続きや使用された端末の種類、および MAC アドレス等の固体識別子、また接続後におこなわれた外部サイトへのアクセス等の通信記録などを保持していることが多い。しかしながら通信ログにはユーザの個人情報が含まれる場合もあるため、取得する旨を規約に盛り込むとともに、規約に書かれた用途以外には利用せず、第三者に窃用されないよう安全な場所に保存し、適切に管理しておくことが重要である。

4.4.2. IDS を用いた未然の対策

IDS（Intrusion Detection System）とは、侵入検知システムのことで、ネットワーク上を流れるパケットを監視し、不正なものを検知するシステムである。公衆無線 LAN では､ネットワーク上のパケットをキャプチャして監視するネットワーク型の IDS を用いてパケットを監視することができる。IDS では、シグネチャと呼ばれる攻撃パターンを記録したデータベースを用いて、該当の攻撃につながるようなパケットがないか監視する。

しかし、IDS は侵入検知システムという名前の通り、パケットを監視し不正なパケットを検知するのみであり、検知した後にどのように対応するかが問題となる。

IPS（Intrusion Prevention/Protection System）という侵入防止システムも存在し、この場合は不正なパケット検知後に該当の端末の接続を遮断するということも可能である。しかし第 2 章で述べたとおり、脅威の幾つかは ICMP や ARP など通常の用途に使用されるようなプロトコルを介しておこなわれるため、すぐに遮断をしてしまうと利用者の快適な利用を妨げる場合もある。攻撃の手口も技術の進展とともに日々進化しているため、IDS/IPS ともに絶えず最新のセキュリティ情報に注意しながら、利用者の利便性を損ねないようなチューニングを最適におこなって運用していく必要がある。

4.5. アクセスポイントの適切な管理

近年の無線 LAN アクセスポイントは多機能化しており、さまざまな機能やソフトウェアが搭載されているものも多い。設定項目も多岐に渡っており、設定を誤ると深刻なセキュリティホールに繋がる可能性もある。このため公衆無線 LAN としてアクセスポイントとなる機器を設置する際に、アクセスポイント本体の設定としても対策をおこなう必要がある。なりすましや、アクセスポイントそのものの乗っ取りを防ぐために対策すべき点を以下に挙げる。

4.5.1. アクセスポイントの管理者パスワードの設定

アクセスポイントの管理画面は同一ネットワーク上の端末から、Web ブラウザを経由して表示するものが多い。この場合、同一ネットワーク上に接続されていれば管理画面までは誰でも接続できてしまう。管理者のパスワードは機器によって違いはあるが、初期状態では未設定でありメーカーごとに固有のパスワードであることが多い。そのため初期設定のまま運用している場合、管理者としてログインされてしまうことがある。

管理画面にはアクセスポイントの主要な設定が含まれるため、ここにアクセスされることはアクセスポイントそのものを乗っ取られることに他ならない。このような事態を防ぐために初期設定の ID・パスワードを変更することはもちろんのこと、容易に推定できないような ID・パスワードを設定し、定期的に変更するなどして対応にあたられたい。

4.5.2. SSID の設定

利用者は SSID を指定して公衆無線 LAN との接続をおこなうが、この SSID をステルス化し事前に SSID を知っている利用者でないと見つけられないように設定することができる。しかしながら、SSID は無線で流されるパケットを解析することで容易に取得できるため、根本的な対策とはいえない。よって SSID のステルス化で十分と思われている事業者は留意されたい。

また、1 つのアクセスポイントで SSID を複数設定し、それぞれに認証方式や暗号方式を変更することができる機器も出回っているが、この場合、セキュリティが甘い箇所を狙って攻撃されると他の箇所にも影響を与える可能性があるため、チェック漏れがないように注意する必要がある。

4.5.3. 電波強度の設定

アクセスポイントの機能として、電波の出力値を設定して、通信可能範囲を制御できるものもある。事業者側としては、より出力を大きくしてアクセスポイントあたりのカバーエリアを広げたいという要求もあると思われるが、第 2.4.3 項でも述べたように無線 LAN で利用できるチャネル数には上限があり、不必要に出力を上げると他のアクセスポイントとの干渉を起こし、結果的に伝送速度が落ちるという事態に繋がる。また、出力を上げることでサービスエリアとして想定していない場

所（店舗で設置する場合、その店舗外など）に対してもアクセスを許すことになり、セキュリティ管理上でも問題となるケースもある。このため、アクセスポイントの出力や設置場所については、サービスの提供イメージやアンテナを含む機器の特性を考慮した上で入念に検討することが望ましい。

4.5.4. アクセスポイントの選定

事業者の規模やサービスの提供範囲にもよるが、無線 LAN 環境が一般的になった現在、安価なアクセスポイント機器を利用して公衆無線 LAN サービスを提供することが可能である。しかし、中にはセキュリティ機能が不十分な機器もあるため、サービスの提供にあたっては十分な検討が必要である。

近年では無線 LAN スイッチといった製品を用いてアクセスポイントを一元管理し、不正なアクセスポイントを発見することや、先に述べた IDS のように不正使用に対する予防機能を持ったアクセスポイントも存在している。利用するアクセスポイント等の機器の選定については、提供するサービスの種類や規模、また事業者の管理能力等を考慮した上で最適なものを選定されたい。

4.6. 公衆無線 LAN とプライベート LAN の分離

公衆無線 LAN サービスの提供者としては、それ自体を事業とする方々のみならず、飲食等の本業の付随的なサービスとして実施する方々も多いと思われる。この場合、本業で利用している通信回線を共用するケースも考えられる。提供者によっては、商品管理や売上データといった重要なデータが蓄積されたパソコンなどを同じ LAN に接続させていることもあると思われるが、第 2 章で挙げたような手口を使ってそのような情報を窃取されたり、不正アクセスの踏み台として乗っ取られる可能性もあるため、十分な注意が必要である。基本的には、公衆無線 LAN とプライベートで用いる LAN は別の機器や回線を使って分離しておくことが望ましいが、そのような構成がとれない場合はより注意深いセキュリティ対策が必要である。

4.7. フィルタリングの設定

第 2.4.4 項にて述べたように、スマートフォンなどで公衆無線 LAN に接続した場合、通信経路やアドレスが変わってしまうことから、携帯電話事業者が提供しているフィルタリング機能などが機能しないことがある。これにより青少年などが、携帯電話網では年齢制限のためアクセスが許可されていない Web サイトを閲覧できてしまうという問題がある。

この対応策としては、特定のポートを塞いで提供するサービスを限定したり、アクセスポイントにて表示可能な URL（ホワイトリスト）、または表示不可な URL（ブラックリスト）を設定してそれ以外の Web サイトを表示させない、といったやり方が考えられる。これらの手法はユーザの利便性を損なう可能性もあるため、セキュ

リティや運用に関するポリシーを利用者にしっかりと説明し、合意を得た上で進めることが望まれる。

4.8. 利用者への啓蒙

セキュリティ対策として、これまでサービス提供者側でおこなうものを中心に述べてきたが、セキュリティ上の脅威は端末側の単純な設定ミスや不用意なアクセスなど利用者側のリテラシー不足を狙ったものも多い。これらの脅威に対し、サービス提供者側でできる対策には限界があるため、前述のようなセキュリティ対策と平行し、利用者に安全な利用の仕方を啓蒙していくことも重要である。具体的にどのようなことを利用者側に伝えるべきかについては第7章にいくつかの例を挙げているので参考にされたい。

4.9. 有事の際のネットワーク開放

2011年3月11日に発生した東日本大震災では、災害に対する既存通信網の脆弱性が改めて浮き彫りになった。災害時においては、地震や津波の影響による設備の損壊やケーブルの断絶、また停電等によるサービスダウンのほか、輻輳による大規模通信障害を防ぐためにおこなわれる通信規制も加わり、長期間・広範囲において通信が不通となる可能性が高い。今やネットワークは電気や水道などと並ぶライフラインの一つといっても過言ではない状況の中で、公衆無線LANは有事の際の通信手段として有効であり、サービス提供事業者には有事の際にも安全、かつ安定した通信環境を提供する努力が求められている。

東日本大震災の際には、被災者支援として公衆無線LAN提供事業者が、平時には有料で提供している公衆無線LANを未加入者にも無料で開放するという取り組みがおこなわれた。このような有事の際は、だれでも簡単に使えることが優先されるため、ID認証や暗号化はおこなわず、SSIDが分かれば接続できる状況で提供されていた。

現在、無線LANビジネス推進連絡会では、大規模災害時の通信インフラサポート手段として、キャリアを問わず無料で利用できる災害用統一SSID「00000JAPAN（ファイブゼロジャパン）」の普及を促進している。だれもが自由に使えるネットワークは、裏を反せば攻撃者にとっても攻撃し易いネットワークでもある。特に有事の際には、被災者が特別意識することなく安心安全な無線LANの提供がなされるとともに、適切な情報が渡ること、被災者が適切な情報にたどり着けることが重要であるため、セキュリティの面では、利用者の負担にならないよう、アクセスポイント側でフィルタリングやIPS/IDSといった機能を持ち、一定の安全性を確保していくことが必要といえる。常日頃から公衆無線LANに接続することのメリットとセキュリティ上の脅威について利用者が理解できるような仕組みの提供や、働き

かけをすることも重要である。このことは、今後増加すると推測される外国人旅行者へ公衆無線 LAN を提供する際にも同様である。

5. 有害サイトアクセス制限について

5.1. 背景

公衆無線 LAN を提供するインターネット接続役務提供事業者は、インターネット接続役務の提供を受けるユーザの中に一定数の青少年がいることを前提にしなくてはならない。公衆無線 LAN 事業を営むに際してのガイドラインや青少年の有害情報へのアクセスを制限する規律などは存在するが、近年の情報機器の多様化・多機能化に対応しきれていない部分もある。

本章では、広く公衆無線 LAN 環境が整備されていく上で、青少年が安全に安心してインターネットを利用できる環境づくりのための現状と課題を整理していく。

5.1.1. 対象となる事業者と義務について

インターネット接続役務を提供する契約を締結している者の数が五万を超えるインターネット接続役務提供事業者は、インターネット接続役務の提供を受ける者から求められたときは、青少年有害情報フィルタリングソフトウェア又は青少年有害情報フィルタリングサービス（以下この章において、「フィルタリングサービス等」という）を提供しなければならない[7]、とある。

本規定に基づき公衆無線 LAN 事業者は、ユーザの求めに応じてフィルタリングサービス等を提供する義務を負っており、ユーザから求められた場合は速やかにフィルタリングサービス等を提供できるように、あらかじめ準備しておく必要がある。

5.1.2. 対象となる電気通信機器について

公衆無線 LAN を利用することが想定される電気通信機器について、主なものとしてはモバイルパーソナルコンピュータやタブレット端末、スマートフォンが挙げられる[8]。

これらの当該機器の電気通信機能は、青少年有害情報アクセス制限の観点からインターネット接続を提供する事業者をふたつに分類する。

「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」によると、事業者になるのが、「インターネット接続役務提供事業者」と「携帯電話インターネット接続役務提供事業者」に分かれている。

主な当該機器のうち、モバイルパーソナルコンピュータやタブレット端末などについては、インターネットへ接続する電気通信機能が無線 LAN となるため、関連

---

[7] 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」第 18 条, 同法律施行令第 2 条

[8] 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律施行令第三条の規定に基づき、経済産業大臣が当該機器の種類を定める件」平成 21 年経済産業省告示第 33 号

する義務を負うのがインターネット接続役務提供事業者となる。一方で、スマートフォンについては、インターネットへ接続する際に携帯電話事業者のネットワークを経由することができるため、関連する義務を負うのが携帯電話インターネット接続役務提供事業者となる。

5.1.3. フィルタリングとブロッキングについて

公衆無線 LAN サービスを提供するに際して、違法・有害情報から青少年を保護する観点から特定の通信を遮断する場合、2 つの方法がある。

① フィルタリング

フィルタリングは、保護者・利用者の同意を得たうえで一定のサイトや URL に対するアクセスを遮断等するもので、保護者・利用者側が任意で遮断内容を設定変更できる点に特徴がある。フィルタリングには、大きく分けて、利用者の端末にフィルタリングソフトをインストールする場合と、インターネット接続役務提供事業者のサーバ側でフィルタリングをかける場合がある。後者においては通信の秘密の侵害となり得るため、事前の有効な同意を得ることが必要である[9]。

② ブロッキング

ブロッキングは、ユーザ側の同意を得ずに一定のサイトや URL に対するアクセスを強制的に遮断するもので、利用者が望んだとしても、その設定を変更できない点でフィルタリングと区別される。ブロッキングについてもフィルタリングと同様の理由で、通信の秘密の侵害に該当するものであり、現在、日本でブロッキングが認められているものは、児童ポルノに関して行うものに限定されているので、注意されたい。[9]

5.2. 現状と課題

5.2.1. 現状

事業者が具体的にフィルタリングサービス等を提供する際、フィルタリングの機能をユーザの端末側でおこなう方法と事業者のネットワーク側でおこなう方法がある。これについて、「無線 LAN ビジネスガイドライン」では、以下のように言及している。

上記規定に基づき義務を負う公衆無線 LAN 事業者は、具体的にフィルタリングサービス等を提供する際は、公衆無線 LAN サービスのオプションとして自ら提供したり、青少年有害情報フィルタリングソフトを提供するサイトを紹介するなど、利用者端末側でフィルタリングが行われることを第一に考えることが望まれる。なお、

---

[9] 「無線 LAN ビジネスガイドライン」, 総務省総合通信基盤局, 2013 年 6 月 25 日

こうした対応が困難である場合には、利用者から求められた場合に備えネットワーク側でフィルタリングサービスが提供可能となるようにあらかじめ準備しておくことが必要である。[9]

5.2.2. 現状の課題について

スマートフォンからのインターネット接続については、「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」で以下のように規定されている。

携帯電話インターネット接続役務提供事業者は、携帯電話インターネット接続役務を提供する契約の相手方又は携帯電話端末若しくは PHS 端末の使用者が青少年である場合には、青少年有害情報フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない[10]。

これは、携帯電話事業者のネットワークを経由してインターネットに接続する際の規定であり、スマートフォンで可能となっている無線 LAN を経由してのインターネットへの接続については上記の条件が適用されない。そのため、携帯電話インターネット接続役務提供事業者が条件とする青少年有害情報フィルタリングサービスの利用が携帯電話事業者のネットワーク側におけるフィルタリングだけの場合、インターネットへの接続経路が無線 LAN となった場合に、本来はフィルタリングによって制限されるべき青少年有害情報が閲覧できてしまう。

スマートフォンについては、携帯電話インターネット接続と無線 LAN インターネット接続の切り替えはシームレスであり、ユーザがその切り替えを意識したり設定を変更したりする必要はない。これによって、携帯電話インターネット接続下ではフィルタリングされている青少年有害情報を、青少年本人も気づかないうちにフィルタリングが適用されていない無線 LAN インターネット接続下に入ってしまうことで閲覧してしまう可能性が指摘されている。

この問題については第 2.4.4 項でも情報セキュリティ上の脅威のひとつとして、公衆無線 LAN に接続するユーザ管理の仕組み上の問題として言及している。

5.3. 対策と今後について

ひとつの対策としては、無線 LAN の機能そのものを on/off 設定する機能制限アプリによって公衆無線 LAN への接続を無効にしてしまうというものがあるが、今後公衆無線 LAN 環境が拡充されていく中で、公衆無線 LAN 環境を排除した取り組

---

[10] 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」第 17 条

みを検討するのは現実的ではない。ここでは、公衆無線 LAN 環境を活用していくための対策を検討したい。

第一には、ユーザの端末側でフィルタリングをすることによって、インターネットへの接続経路に関わらずフィルタリングを機能させることができるようにすることが望まれる。ユーザの同意のもとでユーザの端末側にフィルタリング機能を提供できる場合、インターネットへの経路が端末の利用途中で変わったとしても、インターネットへの経路に関わらず横断的にフィルタリング機能を有効にし続けることが期待できる。

ユーザの端末側にフィルタリング機能を導入できないような場合についても、関連事業者が連携してフィルタリングサービス等を提供できる仕組みを作っていくことが求められてくるだろう。「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」第 17 条は、青少年への携帯電話インターネット接続役務の提供についてフィルタリングサービス等の利用を条件としなければならないと言及しており、今後広く公衆無線 LAN 環境が整備されていく中で、スマートフォンが公衆無線 LAN を利用することが前提になっていくと考えられる。その場合、青少年が所有しているスマートフォン端末が、広く普及した公衆無線 LAN に接続した時点でそのフィルタリング機能を無効にしてしまうとなれば、「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」が求める運用ではなくなってしまっているだろう。今後のインターネット利用環境の拡充と多様化に対応できるよう、携帯電話インターネット接続役務提供事業者のみならずインターネット接続役務提供事業者も連携してフィルタリングサービス等が運用されるような環境を整備する必要があるだろう。

インフラやシステム面での機能充実だけでなく、ユーザのリテラシー向上のための啓発活動も重要である。スマートフォンに必要となるフィルタリングが従来の携帯電話と異なる点、および高度に複雑化している各種情報端末の利用者・保護者の理解が十分とは言い難い現状にあるため、関係事業者の連携により、フィルタリングサービス等を利用者・保護者が正しく理解して利用できるよう、啓発活動を進め、利用者・保護者の声を吸い上げることで具体的な改善点を見出すなど更なる改善に取り組むことが望まれる。

フィルタリングと通信の秘密や個人情報の関係とその扱いについては、今後も慎重な議論や検討を重ねる必要がある。既にある判断事例としては、総務省が「電気通信事業分野におけるプライバシー情報に関する懇談会（第 18 回会合）」（2006 年 1 月 23 日）における「電気通信事業者が行う電子メールのフィルタリングと電気通信事業法第 4 条（通信の秘密の保護）の関係について」や、「迷惑メール対策技術導入を検討されている事業者の方へ」で言及しているケースがある。これらについては、個別の事例ではあるが、今度の判断においての参考となるだろう。

5.4. 該当する各法律について

以下に、関連する法律と該当する条文について抜粋する。

青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律
第十七条 携帯電話インターネット接続役務提供事業者は、携帯電話インターネット接続役務を提供する契約の相手方又は携帯電話端末若しくは PHS 端末の使用者が青少年である場合には、青少年有害情報フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない。ただし、その青少年の保護者が、青少年有害情報フィルタリングサービスを利用しない旨の申出をした場合は、この限りでない。
2 携帯電話端末又は PHS 端末をその保護する青少年に使用させるために携帯電話インターネット接続役務の提供を受ける契約を締結しようとする保護者は、当該契約の締結に当たり、携帯電話インターネット接続役務提供事業者に対しその旨を申し出なければならない。

第十八条 インターネット接続役務提供事業者は、インターネット接続役務の提供を受ける者から求められたときは、青少年有害情報フィルタリングソフトウェア又は青少年有害情報フィルタリングサービスを提供しなければならない。ただし、青少年による青少年有害情報の閲覧に及ぼす影響が軽微な場合として政令で定める場合は、この限りでない。

青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律施行令
第三条 法第十九条ただし書の政令で定める場合は、同条に規定する機器にあらかじめブラウザが組み込まれていない場合、青少年による当該機器の使用が十八歳以上の者に目視により監視される蓋然性が高いと認められる場合として経済産業大臣が告示で定める場合、当該機器が専ら事業のために使用されると認められる場合又は経済産業大臣が告示で定める当該機器の種類ごとに、同一の事業者が製造した当該機器の当該年度の前年度における販売数量が一万台を超えない場合において、当該事業者が製造した当該機器を当該年度に販売するときとする。

6. 通信の秘密と個人情報保護の適切な対応

公衆無線 LAN を提供する場合、前章までで述べたとおり、セキュリティ上の脅威が数多く存在する。公衆無線 LAN 提供者として、ユーザが巻き込まれない対策を実施するとともに、何らかの事件が発生した場合、迅速に調査・対応をおこなうことができる体制を整えておくことが重要である。

特に、ユーザの行動ログを記録しておくことで、多くの場合に調査・対応をおこなうことが可能であるが、ユーザの情報を記録することは、通信の秘密や個人情報保護を侵害する可能性があるなど、関連する法律に照らしあわせながらの慎重な取り扱いが必要である。

6.1. 定義

6.1.1. 通信の秘密

通信の秘密は日本国憲法第 21 条でそれを保障されており、さらに電波法第 59 条および電気通信事業法第 4 条でも規定されている極めて重要な項目である。また、保護されるべき通信とは通信内容だけではなく、通信の秘密に属する事項として、通信当事者の住所・氏名、発受信場所、通信日時等通信の構成要素、通信回数等通信の存在の事実の有無を含む[11]。

6.1.2. 個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう[12]。

6.2. ユーザの情報を保持する場合について

6.2.1. 通信の秘密に関する事項

通信の秘密に関する対応については「無線 LAN ビジネスガイドライン」にて詳しく言及されているため、以下にそれを抜粋する。

公衆無線 LAN サービスの提供をおこなう電気通信事業者等は、通信における秘密保護について適切に対応しなければならない。事業法においては、憲法第 21 条第 2 項の規定(通信の秘密の保護)を受け電気通信事業者の取扱いに係る通信の秘密の保護を規定している(「電気通信事業法」第 4 条第 1 項)。通信の秘密を侵害した場合に罰則が適用されるだけでなく、電気通信事業者が秘密を侵した場合にはその

---

[11] 「電気通信事業における個人情報保護に関するガイドラインの解説」第 15 条

[12] 「個人情報の保護に関する法律」第 2 条

刑が加重されている(「電気通信事業法」第 179 条)。また、電気通信事業者の業務方法が「通信の秘密」の確保に支障があると認められるときは、総務大臣が業務改善命令を発動することもある(「電気通信事業法」第 29 条第 1 項第 1 号)[9]。

6.2.2. 個人情報の保護に関する事項

個人情報の保護に関する対応についても同様に「無線 LAN ビジネスガイドライン」にて詳しく言及されているため、以下にそれを抜粋する。

公衆無線 LAN サービスの提供を通じて取得した利用者情報の取扱いについては、個人情報の保護に関する法律(平成 15 年法律第 57 号。「個人情報保護法」という。)及び電気通信事業における個人情報保護に関するガイドライン(平成 16 年総務省告示第 695 号。「個人情報保護ガイドライン」という。)の規定を踏まえ、適切な対応を行う必要がある。具体的には、電気通信サービスを提供するために必要な場合に限り、個人情報を取得するものとし(「個人情報保護ガイドライン」第 4 条)、その利用の目的をできる限り特定するとともに(「個人情報保護ガイドライン」第 5 条)、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱わないこと(「個人情報保護ガイドライン」第 6 条)などが求められる。また、プライバシーポリシーをあらかじめ定めて公表し遵守するとともに(「個人情報保護ガイドライン」第 14 条)、原則としてあらかじめ本人の同意を得ないで個人情報の第三者提供をしないこととされている(「個人情報保護ガイドライン」第 15 条)ことに十分配慮する必要がある。個人情報保護ガイドラインは、電気通信事業を行う者に対し、個人情報保護法を踏まえ、個人情報の適切な取り扱いについてできるだけ具体的な指針を示すものであるので、無線 LAN サービスを提供する事業者等は、事業の推進に当たり個人情報の取扱いに疑義が生じた場合は、適宜当該個人情報保護ガイドラインを参照することが望まれる[9]。

6.2.3. 情報の保持と個人情報保護および通信の秘密について

・ユーザ認証の情報

ユーザ認証型の公衆無線 LAN を提供する場合、ユーザごとに ID とパスワードを発行し、事前に承認されたユーザ以外は接続できないようにする。一般的にはユーザの氏名・生年月日・メールアドレスなどを認証のための情報として登録してもらい、認証サーバ側に収集・記録することで、接続時に登録した本人かを認証できるようにしている。これらの登録者情報は、個人情報保護法で定められた個人情報に該当する情報となる。

・通信のログ

実際に各セキュリティの脅威が発生した場合、違法行為への対応やその発信者および原因や経路を追跡するために、発信者情報に併せて通信のログが残されていることが望ましい。そこで、通信ログサーバの設置などで通信ログを収集・記録して

おくことが必要となってくる。

ここでの通信ログとは、通信内容および通信履歴のことを指す。ここでは通信ログのうち通信履歴について言及する。通信履歴とは、利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信にかかる情報であって通信内容以外のものをいう[13]。通信に利用した端末の ID や移動端末の場合には通信した時点の位置情報などもこれに含まれる。

通信履歴については、プロバイダ責任制限法によって被害者から発信者情報の開示請求がなされることがあり、事業者が通信ログを保持していた場合に開示請求される発信者情報の中にはユーザ認証の情報のほかに電気通信を利用した日時などの通信履歴が含まれてくる。これに関連して「情報処理の高度化等に対処するための刑法等の一部を改正する法律（サイバー刑法）」にて新設された、検察官、検察事務官又は司法警察員による通信履歴の電磁的記録の保全要請の制度によって、その保全を求められる場合がある[14]。この保全要請に強制力はなく、通信履歴の存在の有無の回答や提出が義務となる訳ではない。また、通信履歴の提出についても従来どおり裁判官の令状が必要である。

これらを収集・記録する行為は通信の秘密および個人情報保護法に抵触する懸念があるため、関連するガイドラインに沿った適切なプライバシーポリシーの策定と利用者への周知、その上で利用者への事前の同意を得ることが不可欠である。その取り扱いについても該当する法律とガイドラインに示された指針を参照して適法になされなくてはならない。

6.3. パーソナルデータの利活用に関する制度改正大綱と今後のあり方について

2013 年 12 月 20 日、高度情報通信ネットワーク社会推進戦略本部で「パーソナルデータの利活用に関する制度見直し方針」が決定され、翌 2014 年 6 月 24 日「パーソナルデータの利活用に関する制度改正大綱」にて制度改正の方向性が示された。これにより、個人情報保護法の問題点や課題が整理され、改正に向けての議論・取り組みが具体化されてきている。2014 年 8 月時点では法案化はされていないため、今後の議論で調整や方向修正がおこなわれることも大いにあり得るが、ここではパーソナルデータの利活用に関する制度改正大綱で政府が示した方向性について整理して紹介する。

---

13 「電気通信事業における個人情報保護に関するガイドライン」第 23 条

14 「情報処理の高度化等に対処するための刑法等の一部を改正する法律」第 2 条

6.3.1. 制度改正を検討する背景

パーソナルデータの利活用に取り組む事業者が、個人情報として取り扱うべき範囲の曖昧さ（グレーゾーン）のために社会的批判を懸念して利活用に躊躇しているという「利活用の壁」の存在がある。そのためにパーソナルデータの利活用は十分におこなわれているとは言い難い。

こういった背景のもと、ビッグデータ時代におけるパーソナルデータ利活用に向けた制度見直しをおこなうことによって、政府の成長戦略としては、「利活用の壁」を取り払い、かつ従来通りの個人の権利侵害を防ぎつつ、新産業・サービスの創出と国民の安全・安心の向上等のための利活用を実現する環境整備をおこなうことが求められている。

6.3.2. 制度改正の 3 つのポイント

「パーソナルデータの利活用に関する制度改正の基本的な考え方について」には本制度改正には 3 つの新たな枠組み・ルールのポイントがあると解説している。

1）パーソナルデータの利活用は、目的外利用や第三者提供において大きな効果をもたらすことから、それらを本人の同意がなくてもおこなうことを可能とする枠組みを導入する。

「個人の特定性を低減したデータ」という概念を新設し、個人データ等を「個人の特定性を低減したデータ」へ加工することによって、本人の同意がなくても第三者への提供を可能にする枠組みをつくる。また、医療情報のような適切な取り扱いが求められつつ、本人の利益・公益性に資するために一層の利活用が期待されている情報も多いので、適切な保護と利活用を推進していく。

2）グレーゾーンの内容や、個人の権利利益の侵害の可能性・度合いは、情報通信技術の進展状況や個人の主観など複数の要素により時代とともに変動するものであることから、これに機動的に対応可能とするため、法律では大枠のみ定め、具体的な内容は政省令、規則及びガイドライン並びに民間の自主規制により対応するものとする。

主に以下の事項を制度改正事項とする。

・「個人情報」の範囲を明確化してその取扱を規定することで、事業者がパーソナルデータの利活用に躊躇してしまう「利活用の壁」を取り払う。

・技術の進展に迅速に対応できる制度の枠組みとする。

・消費者等も参画する民間主導による自主規制ルールの枠組みを創設する。業界の特性に応じた具体的な運用ルールや、法定されていない事項に関する業界独自のルールを策定し、その認定等実効性の確保に第三者機関が関与する枠組みを構築する。

3）バランスのよい保護及び利活用の推進に向けて、法令や民間の自主規制を実効

性あるものとして執行するために、独立した第三者機関の体制を整備する。
主に以下の事項を制度改正事項とする。
・法定事項や民間における自主的な取り組みについて実効性ある執行をおこなうための第三者機関の体制を整備する。
・現在個人情報取扱事業者に対して主務大臣が有している機能・権限に加え、立入検査等の機能・権限を有し、また、民間の自主規制ルールの認定等及びパーソナルデータの越境移転に関して相手当事国が認めるプライバシー保護水準との適合性を認証する民間団体の認定・監督等を実施する。
・事業者が法令違反に当たる行為をした場合等の手段として、現行の開示等の求めについて、請求権に関する規律を定める。

このように、通信の秘密と個人情報の保護は極めて重要な事項である。パーソナルデータの利活用のための制度改正が進められており、今後の相互の関係については新たな枠組みでの議論と検討が必要となってくる。民間や業界が主導するルール作りや第三者機関による認定等、新しい取り組みの中で適切に個人情報が取り扱われるよう、どのように法整備がなされていくのかが注目される。

7. 情報セキュリティの利用者啓発について

内閣府が実施した消費動向調査によると、2014 年 3 月時点で 54.7%と一般世帯の半数以上がスマートフォンを所有しており、また高校生の 75%がインターネットに接続する際に最も利用する機器としてスマートフォンを挙げている[15]など、インターネットをいつでも、どこでも、誰でも利用できる環境は拡大してきている。しかし便利になる一方で、インターネットを悪用した事件や事故に巻き込まれる危険性も増えてきている。

第 2 章より述べているとおり、公衆無線 LAN は一般的なインターネットにおける情報セキュリティの脅威に加え、有線に比べて傍受等が容易な無線を不特定多数が利用できることに起因する脅威への対策にも取り組む必要がある。同時に、利用者に対して公衆無線 LAN 利用における情報セキュリティの脅威と、その対策の必要性と実用的な方法について啓発していくことも重要である。

関連する法律やガイドラインにも情報セキュリティについての啓発は必要性および努力義務というかたちで言及されており、[16] [17]ここではその事例を紹介する。

7.1. ユーザ向けの啓発活動

・ 「スマートフォン情報セキュリティ 3 か条」（2011 年 11 月）[18]

総務省が取りまとめたスマートフォン利用に関する情報セキュリティについての 3 つの対策が示されている。従来の携帯電話にはなかった OS（基本ソフト）の更新、ウィルス対策ソフトの導入、アプリケーションのインストールについて紹介し、利用者自身で情報セキュリティ対策を取ることが必要であると啓発している。

・「一般利用者が安心して無線 LAN を利用するために」（2012 年 11 月）[19]

総務省が策定・公開しているユーザが無線 LAN を利用するにあたってのリテラシーや重要度別セキュリティ対策等を示した手引書である。その中でユーザが最低限守るべき情報セキュリティ対策として「無線 LAN 情報セキュリティ対策の 3 つの約束」を取りまとめているなど、分かりやすい表現でユーザに対して啓発している。

---

[15] 「平成 25 年度 青少年のインターネット・リテラシー指標等」, 総合通信基盤局, 2013 年 9 月 3 日

[16] 「不正アクセス行為の禁止等に関する法律」第 10 条

[17] 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」第 13〜16 条

[18] 「スマートフォン情報セキュリティ 3 か条」, 総務省, 2011 年 11 月

[19] 「一般利用者が安心して無線 LAN を利用するために」, 総務省, 2012 年 11 月

・国民のための情報セキュリティサイト[20]
　総務省が公開しているインターネットと情報セキュリティの知識の習得と利用に関する情報をまとめたサイトである。

・情報セキュリティ啓発[21]
　独立行政法人 情報処理推進機構（IPA）が公開している情報セキュリティに関する各種情報や啓発活動をまとめたサイトである。

7.2. 青少年に向けた啓発活動

・青少年のインターネット利用環境づくりフォーラム
　内閣府が関係府省庁や地方自治体と連携して全国 8 箇所で開催したフォーラムで、保護者への啓発活動の事例紹介や、スマートフォンでの情報セキュリティの脅威を疑似体験するツールの説明などがおこなわれた。

・各種コンクール
　総務省が「情報通信の安心安全な利用のための標語」を募集したほか、IPA 主催の「情報セキュリティ標語・ポスター・4 コマ漫画コンクール」などがあり、児童・生徒が情報セキュリティについて自ら考え、表現する機会となっている。

・講演・講座
　e-ネットキャラバン協議会による「e-ネット安心講座」や各携帯電話キャリアが開催する携帯電話の安全利用教室、IPA が実施している「インターネットは善か悪か？」といった各種講演・講座も盛んにおこなわれてきている。

7.3. 企業に向けた啓発活動

・ 「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン~その特性を活かしたワークスタイル変革のために~【第二版】」（2014 年 3 月）[22]
　民間セクターの取組みとしては、一般社団法人日本スマートフォンセキュリティ

---

[20] 国民のための情報セキュリティサイト, 総務省,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
[21] 情報セキュリティ啓発, 独立行政法人 情報処理推進機構,
https://www.ipa.go.jp/security/keihatsu/features.html
[22] 「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン~その特性を活かしたワークスタイル変革のために~【第二版】」, 一般社団法人日本スマートフォンセキュリティ協会, 2014 年 3 月

協会(JSSEC)がスマートフォンおよびタブレット端末を業務利用に導入することを検討する際のガイドラインとして、それらの端末の特性としてメリットだけではなくデメリットも含めて整理をしており、導入目的の明確化と想定される利用シーンの特定が必要であると示している。

・「Android アプリのセキュア設計・セキュアコーディングガイド」（2012 年 6 月、2014 年 7 月改訂第 4 版）[23]

JSSEC が Android 端末用アプリケーションの開発者に向けて公開しており、開発者の知識・認識不足からアプリケーションに脆弱性が生まれてしまうのを避けるためのガイドラインとなっている。年々更新されていくスマートフォン・タブレット端末の機械的およびシステム的な部分に対応して適宜改訂がなされている。

7.4. 利用者への利用規約の周知

公衆無線 LAN 事業だけに限らないが、事業者がユーザにサービスを提供する場合、そのサービスを利用するにあたっての規則である利用規約を事前に提示してユーザに同意を得ておく必要がある。利用規約には一般的には、サービス内容、プライバシーポリシー、セキュリティポリシー、免責事項などが記載される。

・プライバシーポリシーは、個人情報を収集する目的と、どう扱うのかが記される必要がある。

・セキュリティポリシーは、情報セキュリティ対策についての基本的な考え方を記した情報セキュリティ基本方針と、情報セキュリティを確保するための行為や判断の基準を記した情報セキュリティ対策基準が記される必要が有る。

・免責事項には、サービスに不測の事態が発生した場合に責任を免れる項目について記す。

またこれら利用規約はユーザに対して分かりやすい形で提示されることが必要であり、ユーザが意識することが難しいような表示方法は採用されるべきではない。

なお、パーソナルデータの利活用に関する制度改正に際しては、パーソナルデータの第三者提供の例外措置の要件の明確化、利用目的拡大に当たって事業者が取るべき手続きの整備、わかりやすいプライバシーポリシーの明示等、パーソナルデータの取扱いの透明化等を検討することになる[24]ので、今後の動向にも注視されたい。

---

[23] 「Android アプリのセキュア設計・セキュアコーディングガイド（改訂第 4 版）」, 一般社団法人日本スマートフォンセキュリティ協会, 2014 年 7 月

[24] 「パーソナルデータの利活用に関する制度見直し方針」, 高度情報通信ネットワーク社会推進戦略本部, 2013 年 12 月

7.5. 該当する各法律について

以下に、関連する法律と該当する条文を抜粋する。

不正アクセス行為の禁止等に関する法律
第十条 国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。
二 2 国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、アクセス制御機能を特定電子計算機に付加したアクセス管理者が第八条の規定により講ずる措置を支援することを目的としてアクセス制御機能の高度化に係る事業を行う者が組織する団体であって、当該支援を適正かつ効果的に行うことができると認められるものに対し、必要な情報の提供その他の援助を行うよう努めなければならない。
3 前二項に定めるもののほか、国は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律
(インターネットの適切な利用に関する教育の推進等)
第十三条 国及び地方公共団体は、青少年がインターネットを適切に活用する能力を習得することができるよう、学校教育、社会教育及び家庭教育におけるインターネットの適切な利用に関する教育の推進に必要な施策を講ずるものとする。
2 国及び地方公共団体は、青少年のインターネットを適切に活用する能力の習得のための効果的な手法の開発及び普及を促進するため、研究の支援、情報の収集及び提供その他の必要な施策を講ずるものとする。
(家庭における青少年有害情報フィルタリングソフトウェアの利用の普及)
第十四条 国及び地方公共団体は、家庭において青少年によりインターネットが利用される場合における青少年有害情報フィルタリングソフトウェアの利用の普及を図るため、必要な施策を講ずるものとする。
(インターネットの適切な利用に関する広報啓発)
第十五条 前二条に定めるもののほか、国及び地方公共団体は、青少年の健全な成長に資するため、青少年有害情報フィルタリングソフトウェアによる青少年有害情報の閲覧の制限等のインターネットの適切な利用に関する事項について、広報その他の啓発活動を行うものとする。
(関係者の努力義務)
第十六条 青少年のインターネットの利用に関係する事業を行う者その他の関係者は、その事業等の特性に応じ、インターネットを利用する際における青少年のイン

ターネットを適切に活用する能力の習得のための学習の機会の提供、青少年有害情報フィルタリングソフトウェアの利用の普及のための活動その他の啓発活動を行うよう努めるものとする。

8. 無線 LAN の活性化・ユーザ利便の向上

8.1. ユーザ利便性の向上に向けた取り組み

無線 LAN が一般に広く普及して様々な用途に用いられるようになり、利用者のニーズも多様化の一途を辿っている。無線 LAN の標準を策定する IEEE 802.11 ワーキンググループ（以降「IEEE 802.11WG」と記す）では、今日のように多様化したユーザのニーズを充足するために、様々な技術革新の提案がおこなわれ、標準化・規格化に向けた議論がおこなわれている。本章では、IEEE 802.11WG で標準化された（または標準化の準備が進められている）技術のうち、主に公衆無線 LAN に深く関係すると思われるものについて挙げておく。
標準化についての詳細な情報については IEEE 802.11WG の Web サイト[25]に掲載されているので、より詳しく知りたい方はこちらを当たられたい。

8.1.1. 高速化について

インターネットを流れるコンテンツの大容量化・多様化が進んでいる。こうした大容量コンテンツを公衆無線 LAN 経由で利用するユーザにとって、通信速度の高速化がもたらすメリットは非常に大きいといえる。IEEE 802.11n の登場によって無線 LAN の伝送速度は飛躍的に向上したが、更なる伝送速度の高速化を目指して新しい規格が検討・標準化されている。

IEEE 802.11ac

2014 年 1 月 7 日（米国時間）に、IEEE 802.11WG に承認され、IEEE 802.11ac-2013 として正式に規格化された。

6GHz 帯以下の周波数を使用して、最大 6.9Gbps のスループットを実現する規格である。IEEE 802.11n の拡張規格であり、主にチャネル帯域幅の拡大、変調信号の多値化、さらに IEEE 802.11n の MIMO（Multi-Input Multi-Output）技術を拡張したマルチユーザ MIMO を採用することで高速化を実現している。第 5 世代 Wi-Fi と呼ばれ、下位互換性がある。

IEEE 802.11ad

大容量のデータ転送をおこなうことができる 60GHz のミリ波帯を利用して、7Gbps のスループットを実現する規格である。1 チャネル辺り 2.16GHz の広いバンド幅を用いることで高速化通信を実現する。60GHz 帯の電波は周波数が高いため直進性が強く、人体等に遮断されやすい。そのため、ビームフォーミング技術を用い、室内等での近距離機器間通信での活用を想定した規格である。

2013 年 1 月 8 日（米国時間）に、IEEE 802.11WG に承認され、IEEE 802.11ad-2012

[25] IEEE 802.11WG, http://grouper.ieee.org/groups/802/11/

として正式に規格化された。

Wi-Fi Alliance では、IEEE 802.11ad をベースとした WiGig という規格として、IEEE 802.11ac などの Wi-Fi とシームレスに連携するように標準化を進めている。

8.1.2. 認証・ローミングについて

公衆無線 LAN を提供している場所は一般的にスポットと呼ばれることが多い。これは技術特性上広いエリアをカバーするのではなく、スポット単位で通信環境を提供していることが理由である。公衆無線 LAN の利用用途の多様化に伴い、昨今ではこのようなスポットとして点在する公衆無線 LAN 間での接続や、セルラー通信と無線 LAN 間のシームレスな接続といった課題に対応するために、様々な規格が検討・標準化されてきている。

IEEE 802.11r

2008 年 7 月に、IEEE 802.11WG に承認され、IEEE 802.11r-2008 として正式に規格化された。AP 間での高速ハンドオーバー手法である。2012 年 5 月に IEEE 802.11k、r、y、n、w、p、z、v、u、s とともに、IEEE 802.11-2012 として標準化された。

IEEE 802.11ai

公衆無線 LAN が多く設置されさまざまな場所で利用できるようになっているが、アクセスポイントへの接続に時間がかかり移動中の場合には接続と認証が完了する前に、アクセスポイントがカバーする範囲から外れてしまうという課題があった。IEEE 802.11ai は、接続と認証にかかる時間を 0.01 秒程度に高速化する日本初の国際規格である。2014 年 9 月現在、2015 年 11 月の標準化に向けて Draft 2.0 に関する意見交換がおこなわれている状況である。

IEEE 802.11v

2011 年 2 月に、IEEE 802.11WG に承認され、IEEE 802.11v-2011 として正式に規格化された。IEEE 802.11k を拡張し、測定情報を利用して、スループットや信頼性、サービス品質の向上を可能にする規格である。例えば、ステーションが干渉を通知することができるため、これにより AP がチャネルを変更することができる。また、省電力化の拡充機能を提供している。2012 年 5 月に IEEE 802.11k、r、y、n、w、p、z、v、u、s とともに、IEEE 802.11-2012 として標準化されている。

IEEE 802.11k

2008 年 5 月（6 月 12 日（米国時間））に IEEE 802.11k-2008 として規格化した、無線環境の測定に関する規格である。無線ステーションは、他の無線ステーションに対して、AP のビーコン強度や各チャネルにおける無線 LAN の動作レベル、また近隣の AP に関する情報などの測定と報告を要求することができる。2012 年 5 月に IEEE 802.11k、r、y、n、w、p、z、v、u、s とともに、IEEE 802.11-2012 として標準化されている。

IEEE 802.11w

2009 年 9 月に、IEEE 802.11WG に承認され、IEEE 802.11w-2009 として正式に規格化された。マネジメントフレームの一部に対して暗号化や認証をおこなうことで、セキュリティを高める規格である。2012 年 5 月に IEEE 802.11k、r、y、n、w、p、z、v、u、s とともに、IEEE 802.11-2012 として標準化されている。

8.1.3. 利用周波数帯の拡張について

近年のモバイル端末の増加に伴い無線通信トラヒックが急増しており、電波干渉等で接続されない不具合や速度の低下が見受けられる。そこで、利用周波数帯を拡張することで、帯域を有効活用する規格の策定、および標準化が進められている。

IEEE 802.11af

2014 年 2 月 25 日（米国時間）に、IEEE 802.11WG に承認され、IEEE 802.11af-2013 として正式に規格化された。

テレビ用周波数ホワイトスペースを利用した通信規格で、White-Fi、Super Wi-Fi として使用されている。UHF 帯を使用することで、既存の 2.4GHz/5GHz 帯との干渉を回避する。さらに、比較的低い周波数帯を用いることから、長距離伝搬、および遮断されにくいため、通信距離の向上を実現する規格である。

IEEE 802.11ah

1GHz 以下の周波数を利用した低速無線 LAN 規格で、主に 900MHz を活用することで長距離伝送を実現し、大規模なセンサーネットワークへの活用を想定している。また、900MHz 帯での通信は低速であるため、IEEE 802.11ac と同様に MIMO や変調信号の多値化をすることで高速化を検討している。2014 年 9 月現在、2016 年 1 月の標準化に向けて Draft 2.0 に関する意見交換がおこなわれている状況である。

8.1.4. その他

多様化する無線ネットワークを利用者の利便性向上に向けて、ローミングに関して IEEE 802.11WG の枠を超えて検討・標準化が進められている。

IEEE 802.11u

2011 年 2 月に、IEEE 802.11WG に承認され、IEEE 802.11u-2011 として正式に規格化された。802.3 や 802.16 等の 802 系の通信と、3G ネットワークとの連携機能に関する規格であり、Hotspot2.0 にて採用されている。Hotspot2.0 は Wi-Fi Alliance が規定した技術仕様で、最適なネットワークへシームレスに接続する技術である。2012 年 5 月に IEEE 802.11k、r、y、n、w、p、z、v、u、s とともに、IEEE 802.11-2012 として標準化されている。

IEEE 802.21（UMA）

IEEE 802.21 は、IEEE 802.11 の無線 LAN や、IEEE 802.3 の Ethernet、IEEE 802.15 の Bluetooth に代表される無線 PAN、IEEE 802.16 の WiMAX といった IEEE 802 系の通信に加え、3GPP や 3GPP2 といった携帯電話など IEEE 802 系ではない通信との間で、シームレスにハンドオーバーを実現する規格である。802.21-2008 が 2009 年 1 月に標準化され、2014 年 9 月現在、802.21a-2012、802.21b-2012 の拡張が標準化されている。

8.2. その他通信との接続品質の維持

近年モバイル通信のトラヒック量が急増している中で、世界的に無線 LAN を活用したオフロード手法が携帯電話事業者の対策の一つになりつつある。こうしたモバイルトラヒックのオフロードを効果的に実現する為には、携帯電話の通信網と無線 LAN とのシームレスなローミングが実現される必要がある。

このような状況の中で、Wi-Fi 端末のモビリティ特性を考慮した接続品質の維持は、ユーザの利便性を向上させる上で非常に重要であると言える。スマートフォンや携帯電話の通信網である 3G 回線や、無線 PAN である Bluetooth といった既存の通信と、無線 LAN 間をシームレスに移動でき、かつ切り替え先の通信網が快適であることはユーザの利便性を向上させる上で欠く事のできない要素となっている。本節では、先に挙げた IEEE 802.11WG とは別に検討されている、シームレスなローミング技術や、さらなる無線 LAN サービスの付加価値向上に向けて各事業者が独自に進めている取組みについて述べる。

Passpoint

Wi-Fi Alliance により、Hotspot2.0 としてまとめた仕様の技術適合プログラムとして 2012 年に策定された。Hotspot2.0 は IEEE 802.11u をベースとして、自動で認証とハンドオーバーをおこなうことで、シームレスな Wi-Fi ローミングを可能としている。

Hotspot2.0 の具体的な技術として、以下の特徴が挙げられる。

- IEEE 802.11u を用いた最適なネットワークの自動検出・選択機能
  サービスプロバイダの情報や E911 の使用可否、選択可能なローミング先といったどの AP に接続すべきか判断するための情報を、端末側で AP のビーコンから取得し、その情報を使用して最適なネットワークを選択する。
- 信頼できるネットワークへの認証機能
  SIM 認証や、ID/パスワードの組み合わせによる認証、認証 ID などをサポートしている。特に SIM 認証を用いることで、容易に選択したネットワークに接続することができる。
- WPA2 セキュリティ機能
  ネットワークへの接続には、IEEE 802.1X 認証をおこない、AES を用いて通信

の暗号化をおこなう。

Real-Time Traffic Steering

Real-Time Traffic Steering とはエリクソン社が提唱するトラヒックステアリングの手法である。Real-Time Traffic Steering では、携帯電話網と Wi-Fi の両ネットワークにおいて KPI を絶えず評価し、ユーザの端末の接続をネットワーク間でシームレスに切り替えることを可能としている。また、Wi-Fi に接続できる場合には Wi-Fi が選択されるが、端末のリソースから考えた場合に、常に Wi-Fi がベストではない。Real-Time Traffic Steering を用いることで、端末のリソース状況も含めて、ポリシーの判断をおこなうことができ、ユーザの利便性を追求した選択をさせることが可能である。

アクセスポイントによる端末接続制御

無線 LAN アクセスポイントの普及により、屋内のアクセスポイントなどから漏れた弱い Wi-Fi 電波を受信することで、電波状況が悪くなりインターネットアクセスが快適におこなえないという事象が発生しているが、アクセスポイントがリアルタイムに電波環境を把握し、端末との接続を制御するなどの対策により、Wi-Fi ネットワークへのスムーズな切り替えを可能にすることができる。また、3G や 4G といった携帯電話通信網から Wi-Fi ネットワークに切り替える際に発生する無通信時間を解消する機能もある。

8.3. 運営課題などの情報共有方法について

インターネット技術の進展に伴い、サイバー攻撃の手口もますます高度化、かつ巧妙化してきている。また、サイバー攻撃は国境を越えてくるものも多く、攻撃の種類も多様化の一途を辿っている。無線 LAN を提供する事業者にとっても、ますます高度化・多様化するサイバー攻撃に対抗し、被害を未然に防ぐ（または最小限の被害に抑える）ことが求められている。

このためには単独の事業者における対策のみならず、関係者間の情報共有・連携が欠かせない。利用者にとって利便性の高い無線 LAN サービスを提供するための新しい技術、運営方法等については、定期的に複数の事業者で運営課題や情報を共有することが望まれる。

本節では、セキュリティ情報共有における国内外の事例や公衆無線 LAN 提供に関連する情報共有・連携の事例を取り上げる。

8.3.1. 官民連携による国民のマルウェア対策支援プロジェクト（ACTIVE）について

総務省が 2013 年 11 月 1 日から実施している複数のインターネット・サービス・プロバイダ（ISP）事業者やセキュリティベンダー等の事業者と連携し、国内のイ

ンターネット利用者を対象に、マルウェアの感染防止と駆除の取組をおこなう官民連携プロジェクト（ACTIVE:Advanced Cyber Threats response InitiatiVE）。

また、ACTIVE の開始に先立ち、ACTIVE の実施体制の強化を図るため、参加事業者による「ACTIVE 推進フォーラム」の第 1 回会合が 2013 年 10 月 11 日に開催された[26]。

8.3.2. サイバー情報共有イニシアティブ（J-CSIP）について

独立行政法人情報処理推進機構（IPA）が、サイバー攻撃による被害拡大防止のため、経済産業省の協力のもと、重工、重電等、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として、2011 年 10 月 25 日に発足させた。現在は全 5 業界、46 の参加組織による情報共有体制を確立しており、高度化していくサイバー攻撃に関する対策および情報共有の実運用をおこなっている[27]。

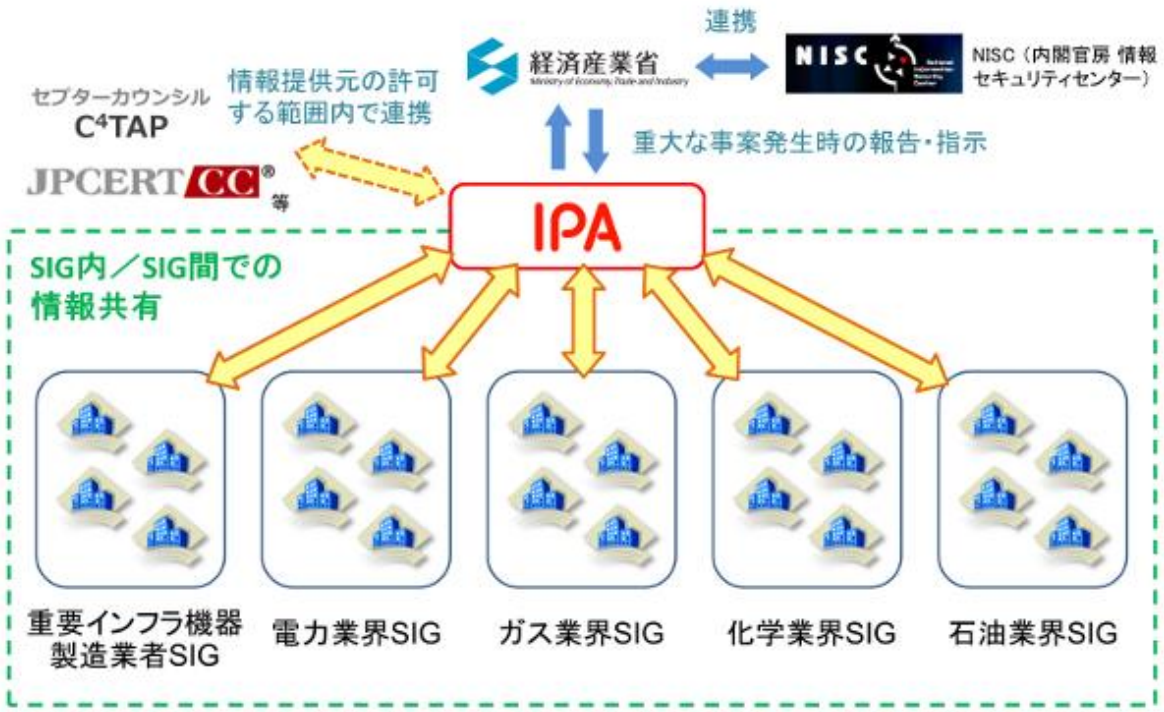


図 8-1 J-CSIP と各業界・関連組織との連携図
（出典：http://www.ipa.go.jp/security/J-CSIP/）

---

[26] 官民連携による国民のマルウェア対策支援プロジェクト（ACTIVE），http://www.active.go.jp/active/index.html

[27] サイバー情報共有イニシアティブ（J-CSIP），http://www.ipa.go.jp/security/J-CSIP/

8.3.3. サイバーセキュリティ情報交換技術（CYBEX）について

ウィルスやワームなどの悪意あるソフトウェアが瞬時に国境を越えて伝染していく現在のサイバー社会において、各国・各機関が独立してサイバーセキュリティ情報を保持していたため、セキュリティレベルの低い地域がサイバー社会全体に対しての脆弱性になっているというセキュリティレベルの格差の問題を解消すべく、2011 年 4 月に勧告された各国・各機関が互いにサイバーセキュリティ情報を交換・共有するためのフレームワークの国際標準である。

「Information Description block」「Information Discovery block」「Information Query block」「Information Validation block」「Information Transport block」の 5 つの機能ブロックから構成されている[28]。

8.3.4. 無線 LAN ビジネス推進連絡会について

「無線 LAN ビジネス推進連絡会」は、総務省が 2012 年 3 月から 7 月にかけて開催した研究会「無線 LAN ビジネス研究会」で取りまとめられた無線 LAN に関する現状の整理と諸問題についての報告書と、事業者間等での意見・情報交換などの連携・協調をする連絡会の設置が有益であるという提言を踏まえて、無線 LAN ビジネス研究会のオブザーバを中心に 2013 年 1 月 31 日に設立した。

通信会社や通信機器メーカーや約 100 社･団体が会員として参加している。また、総務省総合通信基盤局電気通信事業部データ通信課もオブザーバとなっている[29]。

---

[28] サイバーセキュリティ情報交換技術（CYBEX）, http://cybex.nict.go.jp/

[29] 無線 LAN ビジネス推進連絡会, http://www.wlan-business.org/

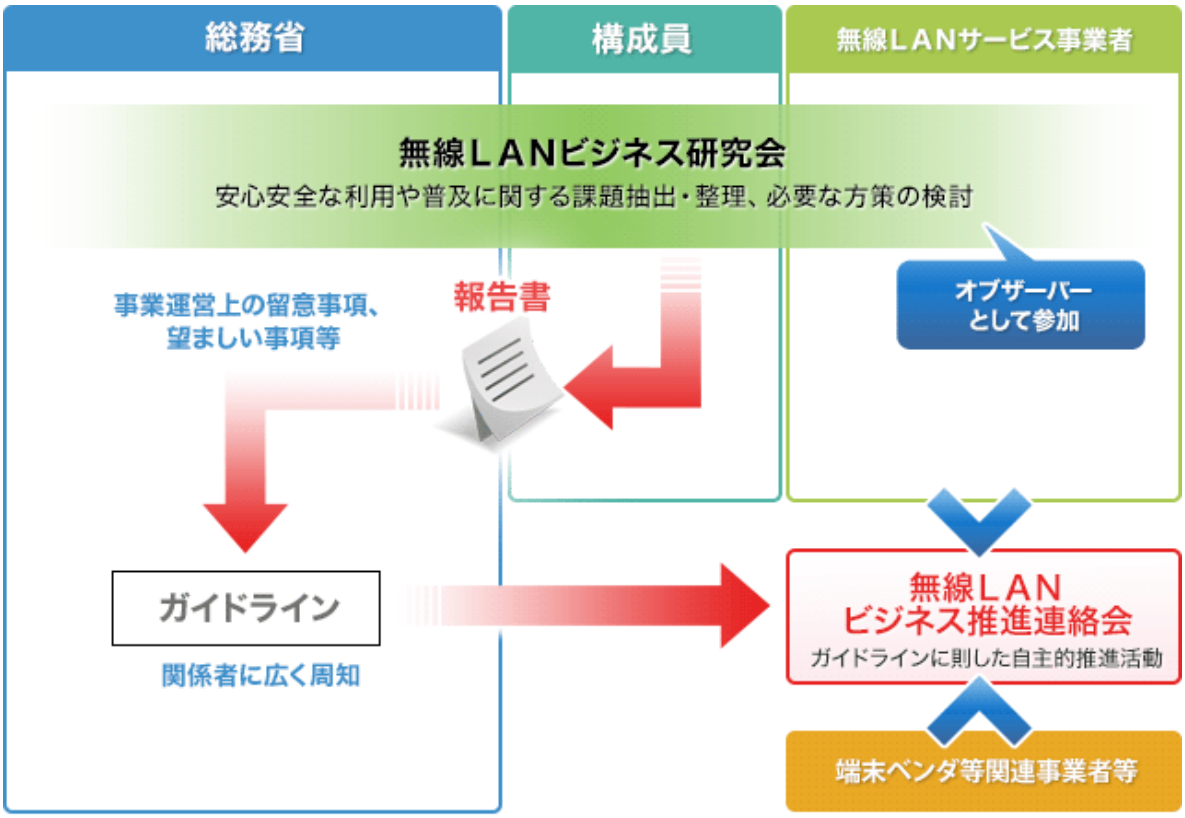


図 8-2 無線 LAN ビジネス研究会と無線 LAN ビジネス推進連絡会の位置づけ
（出典：http://www.wlan-business.org/）

以上

改版履歴

改版日	適用版数	改 版 箇所	改版前	改版後	記事

発行元：無線 LAN ビジネス推進連絡会（Wi-Biz)
〒101-0032　東京都千代田区岩本町 3-2-4　岩本町ビル