

# 公衆 Wi-Fi のリスク認知に関する調査分析と安全利用に向けた検討

リスク工学グループ演習 9 班

田中皓介 水無瀬晶 若林建吾 劉舒陽  
アドバイザー教員 古川宏

## 1. 背景

公衆 Wi-Fi とは、外出先や旅行先においてインターネットに接続するために各地で提供される無線 LAN のことである。公衆 Wi-Fi には携帯事業者のような通信事業者が有料で提供しているものや、飲食店や交通機関などの施設運営者や自治体が無料で提供しているものがある。総務省では、2020 年オリンピック・パラリンピックを見据えて公衆 Wi-Fi の整備促進、利用の円滑化等に取り組んでおり、ICT 総研の公衆無線 LAN サービス利用者動向調査によると、公衆 Wi-Fi の利用者数は 2014 年度に 2278 万人に達した<sup>[1][2]</sup>。そして今後も、毎年 400 万人～500 万人程度のペースで増加し続け、2018 年には 4000 万人を超えると予想されている(図 1)。



図 1 公衆 Wi-Fi サービス利用者数<sup>[2]</sup>

一方、無料で提供されている公衆 Wi-Fi の中には、不特定多数の人が利用でき、通信内容が暗号化されていないため、盗聴、無断アクセス、アクセスポイントのなりすましといった危険性が存在する<sup>[3]</sup>。しかし、総務省が実施した公衆無線 LAN 利用に関する情報セキュリティ意識調査結果によると、日本人は公衆 Wi-Fi の危険性の認知度とセキュリティ対策の実施率が訪日外国人に比べて低く、危険性の認知度と実施率の乖離が大きいことが明らかとなった(図 2)<sup>[4]</sup>。

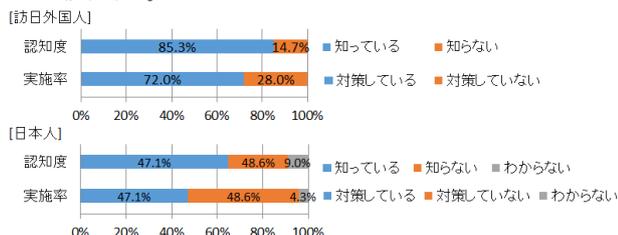


図 2 公衆 Wi-Fi の利用時の脅威の認知度と実施率<sup>[4]</sup>

## 2. 事前調査

以上の背景から、公衆 Wi-Fi に関連した被害は公衆 Wi-Fi の脆弱性だけではなく、利用時の危険性と対策方法の認知不足によるものと考え、まずは身近な筑波大生を対象に公衆 Wi-Fi の利用実態と脅威の認知度に関する調査を行った。

表 1 事前調査の概要

調査方法	アンケート調査
対象者	筑波大学学生 (リスク工学専攻学生)
回答数	40 名
調査期間	6 月 20 日

まず利用実態について、40 人中 29 人が普段公衆 Wi-Fi を利用すると回答した。しかしこの 29 人の中の 3 割以上の人は脅威を全く把握しておらず、半数近い人が対策を取らずに利用していることが明らかとなった。対策しない理由が多かった回答は、「何をすればよいのかわからないため」、「どんな脅威があるのか知らないため」、「危険性を感じない」であった。このことから、脅威と対策を周知させることで、安全な公衆 Wi-Fi の利用につながる可能性があると考え、脅威の存在把握とセキュリティ対策実施状況のクロス集計を行った。図 3 に脅威の存在把握とセキュリティ対策実施状況のクロス集計の結果を示す。カイ二乗検定を行ったところ、 $p=0.064$  となり、10% 水準では有意といえる結果が得られた。このことから、公衆 Wi-Fi 利用時に存在する脅威を知らない人ほど対策を取らない傾向がある可能性が示唆された。

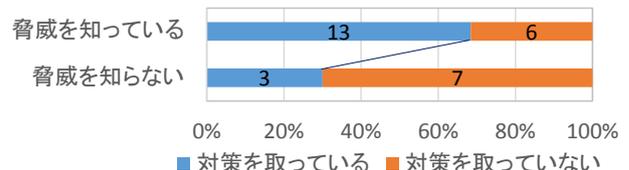


図 3 脅威の存在把握と対策実施状況のクロス集計 (N=29, Fisher の正確確率検定:p=0.064)

## 3. 目的

無料の公衆 Wi-Fi は、利用できる場所が多くその便利さゆえに普及が進んでいる。しかし、無料サービ

スではセキュリティ保護(暗号化)されていないアクセスポイントが多く存在し、盗聴、なりすまし、無断アクセス、ウイルス感染といった危険性も存在している。にもかかわらず、利用者の中には十分な対策を取らずに利用している人もおり、その危険性や対策に関する周知が不足していることが考えられる。

そこで本演習では、公衆 Wi-Fi の安全利用に向けて、危険性や対策に関する効果的な周知方法を検討することを目的とする。そのために、アンケートによる公衆 Wi-Fi 利用時のリスクに対する許容度やその対策についての認知と実施率の調査を行い、さらにその回答理由を事後インタビューにより把握した。

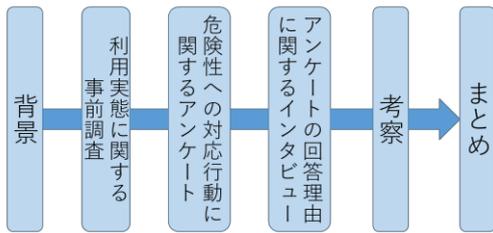


図3 調査の流れ

## 4. アンケート調査

### 4.1 学習方法の違いによる行動変化の調査

公衆 Wi-Fi の安全利用に向けた周知方法の検討および、公衆 Wi-Fi の脅威と学習の違いによる結果の比較を行う。アンケートの質問項目は危険性の認知度、利用頻度、現状行っているセキュリティ対策であり、これらの回答結果を回答者の属性とする。

学習方法の違いによる行動への影響を調査する。図4にアンケート調査に用いた「調べものを行う際の個人情報流出の許容度」の設問を示す。これを用いて学習効果を調査する。以下の手順で実施する。

### 4.2 学習効果の調査手順

- ① アンケート対象者に検索サイトを利用した調べものを行うことを想定させる。
- ② 各状況に応じた許容度を選択する(図4)。
- ③ 各項目の中で最も小さい番号を選択した状況を最も許容できない状況とする。
- ④ 公衆 Wi-Fi に存在する脅威(盗聴・無断アクセス・ウイルス感染)と対策を示す説明文(図5または図6)を示し、学習させる。
- ⑤ 説明文が「対策の手順なし」と「対策の手順あり」の学習方法について、2つのパターンの用紙で別々の回答者に回答させる。

Q7 公衆 Wi-Fi を利用して、検索サイト(Google・Yahoo!など)を利用した調べものを行うと仮定します。この時、あなたは以下の状況をどの程度許容することができますか。あてはまる番号に○をつけてください。(各設問1つに○)

状況	許容できない ←	許容できる →
Q7-1. どこかにアクセスしたという事実のみが他者に流出する	1—2—3—4—5	
Q7-2. 検索したワードが他者に流出する	1—2—3—4—5	
Q7-3. 自分の「ブックマーク」、「お気に入り登録」の情報が他者に流出する	1—2—3—4—5	
Q7-4. アクセスしたページ内容の情報が他者に流出する	1—2—3—4—5	

図4 許容度についての質問

①について以下の設問を用いる。

- Q8 下記の a)~d)にしたがって、設問にご回答ください。
- a) Q7 (図4)に戻り、設定された4つの状況のうち、あなたが選択した番号が最も小さい(最も許容できない)状況をご確認ください。
  - b) いまあなたはその状況が起きないように、公衆 Wi-Fi を利用して、検索サイトを使用した調べものを行いたいと考えているとします。
  - c) 利用する公衆 Wi-Fi は、最初の定義の通り、不特定多数の人が利用するような Wi-Fi であるとしします。
  - d) このとき、あなたは左の【説明文】を読んだ上で、どのような行動をとりますか。あてはまるものすべてを選択し、○をつけてください。(あてはまるものすべてに○)

<選択肢>

1. 何もせずにそのまま利用する
2. アンチウイルスソフトを利用する
3. ネットワークをパブリック設定にする
4. VPNを使用する
5. SSL/TLS 通信のサイトのみを閲覧する
6. 無線 LAN を利用しないときは Wi-Fi 設定を OFF にする
7. 他人に盗まれて困る情報を入力しない
8. その他

②について許容できないものを1、許容できるものを5の5段階とする。③について最も小さい項目が複数ある場合は複数の状況を同時に考慮させる。④について脅威(盗聴・無断アクセス・ウイルス感染)と対策に関する説明文で学習する。⑤について盗聴を例として、手順あり(図6)の赤い部分が手順無しにない追加の説明文であり、手順と対策を導入する欠点がかかれている。学習後、回答者がどのような対策・行動をとるかを選択させる。各回答者の属性と学習による対策の適切さを調査し、どのような属性の人が対策を行うかを分析し、安全に公衆 Wi-Fi を利用できる方法を検討する。

### 4.3 アンケートの概要と対象者

公衆 Wi-Fi の脅威と対策について、アンケート用紙を用いた調査を行った。調査概要は表2に示す通りである。

表2 アンケート調査の概要

調査方法	手順ありと手順なしのアンケートを用いた学習効果の調査
対象者	筑波大学学生(リスク工学専攻学生以外)
回答数	189名(手順あり99名、手順無し90名)
調査期間	7月25日~8月9日

## ○盗聴

盗聴とは通信内容が第三者に見られることをいいます。

### ➤ 対策

#### • SSL/TSL 通信

SSL/TSL 通信を行っているサイトは通信内容が暗号化されているため、通信内容が第三者に読み取られるのを防ぎます。

#### • VPN(Virtual Private Network)

仮想的なネットワークを構築してサイトにアクセスすることで通信内容を暗号化し、通信内容の流出を防ぎます。

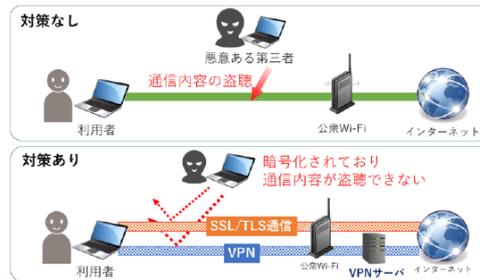


図 5 説明文の一部（手順なし）

## ○盗聴

盗聴とは通信内容が第三者に見られることをいいます。

### ➤ 対策

#### • SSL/TSL 通信

通信内容を暗号化する仕組みです。サイトの URL が「https」で始まっており、こうしたサイトを利用することで、通信内容が第三者に読み取られるのを防ぎます。ただし、全てのサイトが SSL/TSL 通信を行っているわけではないため、得られる情報量が少なくなることがあります。

#### • VPN(Virtual Private Network)

仮想的なネットワークを構築してサイトにアクセスすることで通信内容を暗号化し、通信内容の流出を防ぎます。ただし、通常より通信速度が遅くなる場合があります。VPN の設定は、有料または無料の VPN ソフトをダウンロード・インストールし、VPN サーバへ接続することで行います。

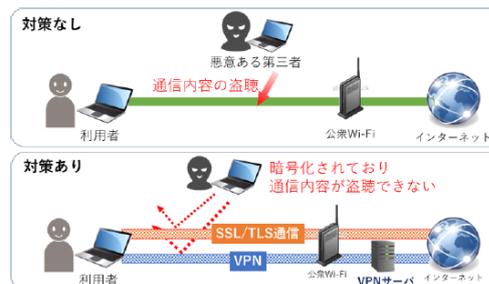


図 6 説明文の一部（手順あり）

## 5. アンケート結果

### 5.1 公衆 Wi-Fi の利用実態

公衆 Wi-Fi の利用実態は、毎日利用する人から半年に 1 回しか利用しない人までいるが、使わないと答えた人が、52 人と最も多くなった。公衆 Wi-Fi を利用しない理由で最も多かったのは、「設定が面倒なため」であり、20 人が回答している。その他には「情報セキュリティに懸念を感じるため」と回答した人が 13 人おり、セキュリティ対策の周知が公衆 Wi-Fi の利用促進につながる可能性が考えられる。

### 5.2 公衆 Wi-Fi の危険性とセキュリティ対策

「公衆 Wi-Fi の利用に際して、どのような危険性の存在を知っていますか」という危険性の把握状況に関する設問に対して、最も把握している人が多かったのは事前調査と同様に、「通信内容を他人に盗まれる」という脅威であるが、これは 189 人中 113 人であり、全体の 6 割にすぎない。そして、189 人中 51 人の人は公衆 Wi-Fi の危険性をまったく把握していないことが明らかとなった。

「公衆 Wi-Fi を利用する際にどのようなセキュリティ対策を行っていますか」というセキュリティ対策の実施状況についての設問では、「アンチウイルスソフトを利用する」、「無線 LAN を利用しないと

きは Wi-Fi 設定を OFF にする」という対策を取っている人は 136 人中それぞれ 3 割程度であり、「取っていない」と答えた人が約半数の 61 人となった。

セキュリティ対策を取らない理由は、セキュリティ対策を取っていない 61 人中の 45 人が「何をすればよいかわからないため」と回答しており、「どんな脅威があるか知らないため」と回答した人が 18 人であった。このことから、脅威や対策に対する知識不足が、対策の実施状況に関連があると考えられるため、脅威の知識と対策の有無のクロス集計を行った。図 7 に脅威の知識と対策の有無のクロス集計の結果を示す。カイ二乗検定を行った結果、 $p < 0.001^{***}$  となったことから、脅威を知っている人ほどセキュリティ対策を取り、脅威を知らない人は対策を取らない傾向があることが統計的に示された。

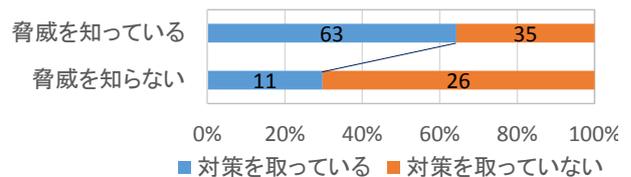


図 7 脅威の知識と対策の有無のクロス集計 (N=135,  $\chi^2=12.949$ ,  $df=1$ ,  $p < 0.001^{***}$ )

### 5.3 被害に対する許容度

個人の被害に対する許容度を把握するため、図3のようにWeb検索を行う際の各状況に応じた許容度について尋ねた。図8に状況別の許容度を示す。ブックマーク、お気に入り情報、アクセスしたページ内容など、個人、プライベート情報が含まれている場合は許容されない傾向にあるが、許容度には個人差があることがわかる。このことから、個人に合ったセキュリティ対策を提示することが望ましいと考えられる。

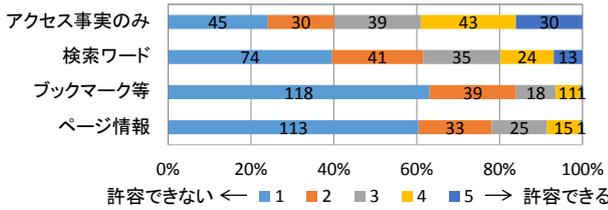


図8 Web検索時における各状況別の許容度(N=187)

### 5.4 セキュリティ対策に関する学習

公衆Wi-Fiに存在する脅威に対する対策を説明した文章を読んでもらい、Web検索を行う際に、自身が許容できないものを防ぐためにどのような対策を取るかについて尋ねた。そして、図5・図6の説明文の手順ありと手順なしの違いによる対策意向と選択した対策の種類の違いについて検討した。

#### 5.4.1 学習前との比較

まず説明文を読む前を学習前とし、学習前にセキュリティ対策を取っていない人について分析を行った。図9に学習前と学習後の対策意向、図10には学習後対策を取る人のうちの手順有無別の対策意向を示す。学習前に対策を取っていない人は63人であったが、そのうち48人の人が学習後に対策を取る意向へと変化した。図10から、Fisherの正確確率検定の結果  $p=0.069$  と10%水準では有意となり、学習前に対策を取っていない人は、その設定方法などが記載されている手順ありの説明文を提示することで、より対策を取るようになる傾向がある。

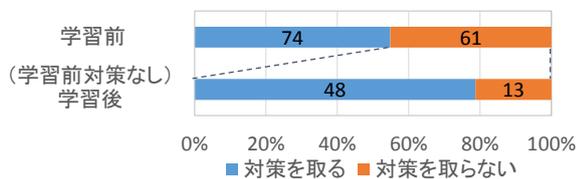


図9 学習前と学習後の対策意向

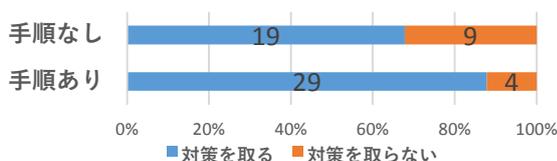


図10 手順有無別の行動意向 (N=61,  $\chi^2=3.621$ , Fisherの正確確率検定  $p=0.069$ )

図11には手順あり・なし別の学習後の行動内訳、図12には学習後にも対策を取らない理由を示す。そして、図11から、手順ありの説明文を読んだが対策を取らないと答えた人は、対策の内容を理解できないのではなく、手順まで表記されていることで対策を面倒と感じるということが分かる。

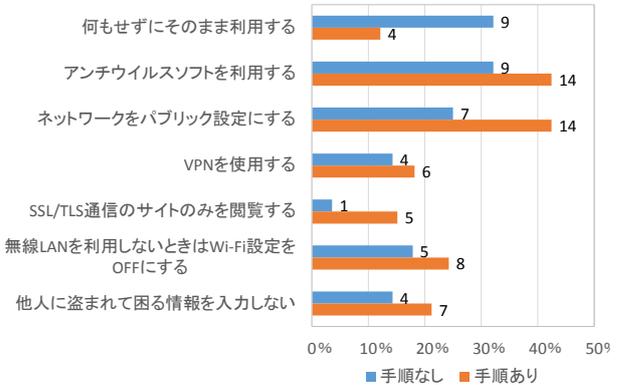


図11 学習後の行動(N=61)

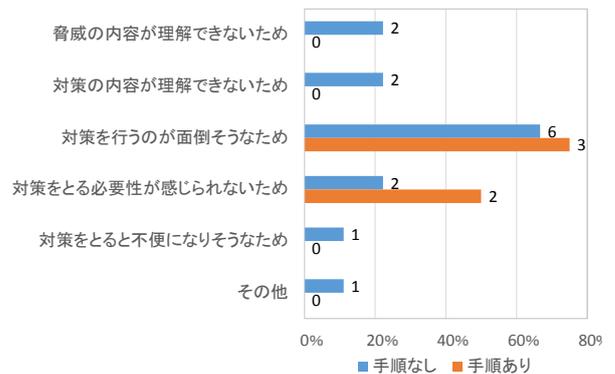


図12 学習後に対策を取らない理由(N=13)

#### 5.4.2 対応行動評価

次に、許容できない脅威に対する対策の十分性を確認した。説明文を読んでもらい、Q7のWeb検索時に許容できないことを守るために取るセキュリティ対策について尋ねた。Web検索において、「ブックマークやお気に入り情報が流出する」ことが許容できない場合は、無断アクセスとウイルス感染を防ぐ必要があり、効果的な対策は、ネットワークをパブリック設定にすることと、アンチウイルスソフトをダウンロードすることである。また、「アクセスしたページ内容の情報が他者に流出する」ことが許容できない場合は、盗聴を防ぐ必要があり、効果的な対策はSSL/TLS通信を利用すること、もしくはVPNを利用することである。

図13に対応行動評価の結果を示す。手順あり・なしに関わらず、ほとんどの人の対策が十分でなかった。手順あり・なしで見ると、カイ二乗検定の結果、 $p=0.080$  と10%水準では有意となり、手順あり

を読んだ人は手順なしを読んだ人よりも対策が十分でない傾向があることが明らかとなった。

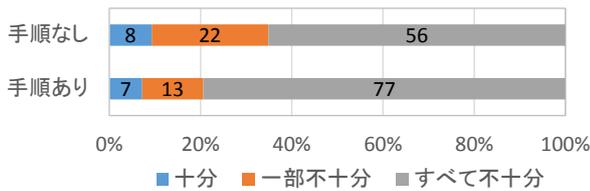


図 13 対応行動評価  
(N=183,  $\chi^2=5.054$ ,  $df=2$ ,  $p=0.080$ )

## 5.5 調査の考察・まとめ

### ① 脅威の認識について

- ・ 公衆 Wi-Fi の利用時に存在する危険性を認識している人は少ない。
- ・ 実際にセキュリティ対策を取っている人はアンケート対象者の約半数であった。
- ・ セキュリティ対策を取っていない理由で最も多かったのは「何をすればよいか分からない」という回答であった。

➤ 脅威と対策に関する認知・知識不足が対策の有無と関連していると考えられる。

### ② セキュリティ対策に関する説明文による学習効果について

- ・ 学習前に対策を取っていないと回答した人のうち約 8 割の人が対策を取る意向へと変化した。
- ・ 個人が許容できないことに対して十分な対策がとれている人は、手順あり・なし共に 1 割未満であった。
- ・ 手順ありを読んだ人が、手順なしを読んだ人より十分な対策が取れていなかった。

➤ 十分な対策を選択しない原因を考察するために、追加インタビュー調査を実施

## 6. インタビュー調査

### 6.1 調査概要

アンケート調査で得られた結果は、回答者がどのような考えをもっていたことによるのか、その理由を把握するために、追加調査を行った。調査概要は、表 3 に示すとおりである。

なお、この調査では回答が少数であり、定量的で詳細な評価を行うことはできていないが、不十分な対策が取られる要因を定性的に把握している。

表 3 インタビュー調査の概要

調査方法	アンケート回答後、回答の理由の詳細をインタビュー
対象者	本アンケートに回答しなかった人 (リスク工学専攻学生)
回答数	16 名(手順あり 8 名、手順なし 8 名)
調査期間	10 月 3 日～5 日

## 6.2 調査結果

調査によって得られた 16 名の回答を整理し、特に代表的な回答をした 3 名について以下で説明する。

### A さん

説明文：手順なし

回答：最も許容できない被害に対して、選択した対策は不十分

<選択した理由>

- ・ 許容できない被害が、説明文の中のどの脅威 (盗聴・無断アクセス・ウィルス感染) に当てはまるのかを判断することができなかった。
- ・ 一つの対策だけでは不十分な場合があることがわからなかった。
- ・ 手順なしの説明文だったので、対策のイメージがわからなかった。
- ・ 説明文を全部読むのが面倒で、あまり理解していなかった。

この回答者は、想定する被害と対応する脅威の情報、一つの対策では不十分な場合があるという情報が説明文になかったこと、また対策の手順が説明されていなかったことから、十分な対策を判断することができなかった。また、説明文の量を見てそもそもきちんと読んでいなかったことにより、理解が不足していたことも明らかになった。

### B さん

説明文：手順あり

回答：最も許容できない被害に対して、選択した対策は不十分

<選択した理由>

- ・ 対策の手順を読んで面倒だと感じたので、簡単で気軽なものを選んだ。
- ・ 被害が目に見えないので対策を取る気が起きない。

### C さん

説明文：手順なし

回答：最も許容できない被害に対して、対策を取らずにそのまま利用

<選択した理由>

- ・ 説明文を読んでどんな対策を取れば何を防げるのかは理解できたが、受ける被害よりも対策を取る手間の方が大きいと思った。
- ・ 自分の情報が流出しても特に困ることは無い。

まず B さんは、手順ありの説明文を読み、対策を取ることが手間だと感じたため、防げる内容ではなく、手軽さを重視して対策を選択している。また C さんは、説明文から対策と防げる内容を理解した上で、流出して困る情報は無いからと、対策を取る手間を考えて実行に及ばないと回答している。このように、説明文の内容理解に関わらず、対策を周知させることでその手間のイメージまでも植えつけ、十分な対応行動に結びつかない可能性があることが明らかになった。

### 6.3 各調査全体のまとめ

本章のインタビュー調査と4章のアンケート調査の結果を合わせて、回答者が不十分な対策を選択するまでの過程を整理したものが、図14である。

今回の調査より、説明文を提示しても理解・判断ができないのは、対策の手順に関する記載の有無の影響、また想定する被害と脅威の対応や、一つの対策では不十分である旨を記載していなかった説明文の不備といった、情報不足が考えられる。加えて、説明文の量だけを見て読むのが面倒だと感じてしまったり、今回の説明文の配置や分量が読みづらいものであったりしたこと、きちんと読んでいなかったことも考えられる。こうした理由から、正しい対策を誤解し、不十分な対策を選択してしまうことが示唆された。また、説明文の理解に関わらず、受ける被害よりも対策を取ることの手間が勝ることで、不十分な対策を選択する、あるいは対策を取らない回答者の存在が確認された。

以上のように、不十分な対策が取られる要因には、説明文の情報不足や回答者の不精読、あるいは対策の面倒さが伝わってしまうことが観測された。ただし、ここには今回作成した説明文の不備に起因する部分も含まれていると考えられ、この部分が回答にどこまで影響を与えているかを適切に判断することはできていない。

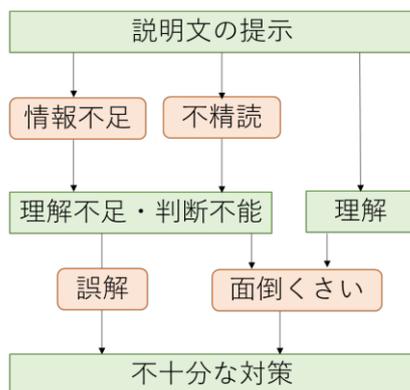


図14 不十分な対策を選択するまでの過程

## 7. まとめ

本演習では、個人に合った公衆Wi-Fi利用時のセキュリティ対策の効果的な周知方法の検討を目的として、利用者の意識・行動意向等に関するアンケート調査とインタビュー調査を行った。

調査を通して、まず説明文上で対策の手順などの詳しい記述を掲載することは、対策実施率を上げる反面、利用者の理解を困難にしてしまうことが明らかとなった。こうした実情を踏まえると、個人の許容範囲に合わせて決まった対策を指定し、「これが許容できないならこの対策を」といったように、利

用者自身に求められる判断の余地をなるべく少なくする周知の仕方が有効であると考えられる。

また、対策を取ることの手間や、普段から被害の実感が無いことから行動を起こさないという実情がインタビュー調査より明らかになった。これに対しては、具体的な被害事例や危険性を示す情報を提示することで、利用者に対策を取ることの重要性を理解させるような工夫が有効であると考えられる。

最後に、今回は公衆Wi-Fiを個人で利用するケースを想定して回答してもらったが、周りに被害が及ばないこうしたケースでは危機意識を持ちづらいという回答もいくつか得られた。他人や組織の情報など流出すると自分以外の人に迷惑がかかるような場合には、より安全な利用を心掛けるようになり、対策意欲や情報の理解度が変化する可能性がある。学校や企業など情報の取り扱いに注意する必要がある組織において、こうした危険性の周知の義務化を推進する必要性が示唆された。

## 8. 今後の課題

今後は、今回作成した説明文について、想定する被害と取るべき対策の対応づけや、防ごうとする被害によって異なる対策が必要となる旨など、不足していた情報を追加し、分量や配置に改善を加えた説明文を作成して調査を行うことが必要である。また、今回は自分の被害を想定する設問であったが、他人や組織など自分以外にも被害が及ぶような場面を想定した調査を行うことで、より対策行動の促進に有効な知見が得られる可能性があると考えられる。このため、今回は調査対象を筑波大学生としていたが、企業で働く社会人など普段利用する公衆Wi-Fi環境が学生とは異なるような対象にも調査を行うことが必要である。

## 参考文献

- [1] 総務省：公衆無線LANの設備の促進  
[http://www.soumu.go.jp/menu\\_seisaku/ictseisaku/public\\_wi-fi/](http://www.soumu.go.jp/menu_seisaku/ictseisaku/public_wi-fi/)（最終閲覧日 2016/10/14）
- [2] ICT総研：2015年公衆無線LANサービス利用者動向調査  
<http://ict.r.co.jp/report/20150416000081.html>（最終閲覧日 2016/10/14）
- [3] IPA：公衆無線LAN利用に係る脅威と対策，2016/3/30  
<https://www.ipa.go.jp/files/000051453.pdf>（最終閲覧日 2016/10/14）
- [4] 総務省：公衆無線LAN利用に係る調査結果，2015/3/16  
[http://www.soumu.go.jp/main\\_content/000347144.pdf](http://www.soumu.go.jp/main_content/000347144.pdf)（最終閲覧日 2016/10/14）