情報漏洩に対するセキュリティ意識の改善：スマートフォンの盗難と紛失

第５班：高橋 正成　　中川 悠太　　古沢 賢哉　　張 燦倫

アドバイザー教員：古川　宏

1　研究背景

近年、スマートフォンユーザが急激に増加している [1]。スマートフォンは、従来の携帯端末に比べて、多種多様なデータを扱えるようになったことから、ユーザが扱う個人情報量も従来の携帯端末に比べ格段に増加する。

高い利便性の一方で、スマートフォンの利用によるリスクも存在する。PC 同等の機能を持つスマートフォンの利用により、スマートフォンユーザにも、ウィルスやスパム、情報漏洩や架空請求などといったリスクが生じる。また、PC 同等の情報が入っている端末を携帯している場合、盗難・紛失時には、メールアドレス等の個人情報をはじめとする、多種多様な情報についての漏洩リスクが懸念される。

しかし、株式会社ネットマイルがスマートフォンのセキュリティに関する調査を行ったところ、調査対象 959 人の約半数がスマートフォンのセキュリティ対策を行っていないこと（対策の不備）が明らかになった [2]。

また、総務省のスマートフォン・クラウドセキュリティ研究会 最終報告 [3] は、一般利用者はスマートフォンに関する脅威や対策手法を、必ずしも十分に認知していないと指摘した。さらに、Symantec は Honey stick project[4] により、盗難・紛失したスマートフォンを発見した者の 96%が端末に含まれる何らか情報にアクセスすることを明らかにし、スマートフォンの盗難・紛失時における情報漏洩のリスクを示した。

以上を踏まえ、本研究では、スマートフォンの利用により生じるリスクの中でも、盗難・紛失時のリスクに着目した。

2　研究目的

スマートフォンの盗難・紛失による個人情報漏洩のリスクについて、これまでのセキュリティ対策の啓発活動 [3] はハザードの周知や被害の実例を示すことであった。しかし、こうした定性的にハザードを伝えるだけの啓発活動では、ハザードによる影響をユーザが想像しにくいため、ユーザは自身の対策が十分と思っていても、実際のリスクに対するセキュリティ対策が不十分な場合がある。そのため、セキュリティ対策の啓発においては、ハザードに関してスマートフォンユーザ自身に抱えるリスクを認識させる必要があり、リスクに対する定量的な情報を用いることで、定性的な情報を伝えるよりもユーザにリスクをより認識させることが期待できる。また、Symantec[4] の結果から盗難・紛失時の情報漏洩リスクは他のリスクと比較して発生しやすく、優先的に解決する必要がある。

本研究では盗難・紛失時の情報漏洩リスクを対象として、定量的なリスクの提示が、スマートフォンユーザのセキュリティ意識に及ぼす影響を明らかにし、セキュリティ対策の啓発活動としての有効性を検証する。

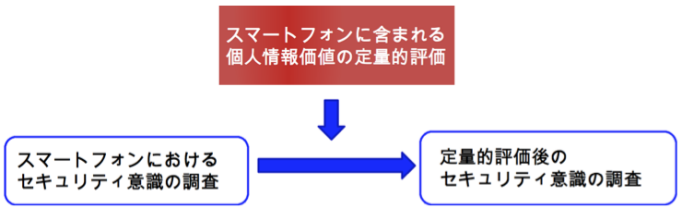

図 1: 定量的評価手法によるセキュリティ意識変化の調査プロセス

3　手法

3.1　定量的評価によるセキュリティ意識検証プロセス

スマートフォンの盗難・紛失により生じる情報漏洩リスクの定量的評価による、スマートフォンユーザにおけるセキュリティ意識変化の調査プロセスを図 1 に示す。

まず、スマートフォンユーザに対し、アンケート調査を行い、現状のセキュリティ意識および対策を調査する。次に、ユーザにスマートフォンの盗難・紛失時に漏洩する個人情報の価値を金額で示し、再度スマートフォンにおけるセキュリティ対策についての考えを調査することで、ユーザのセキュリティ意識の変化を明らかにする。

3.2　個人情報価値の推計

個人情報価値の評価は日本ネットワークセキュリティ協会 [5] および OECD(2013)[6] にて行われていた。本研究が調査対象として価値を推計する情報は、日本国内のユーザが所持するスマートフォンで扱われる個人情報であり、国内事情に特化した推計手法を用いることで精度の高い推計ができると考えられるため、日本ネットワークセキュリティ協会の手法 [5] を用いた。

日本ネットワークセキュリティ協会の手法 [5] では、想定損害賠償額の推計手法が提案されている。想定損害賠償額の推計手法が提案された目的は、セキュリティインシデントにおける「損害賠償の可能性」について、リスクの大きさ（被害規模）や適切な情報セキュリティに対する投資判断の一助となることである。

ここで、日本ネットワークセキュリティ協会により提案された想定損害賠償額の推計式 [5] を以下に示す。なお、想定損害賠償額の単位は円である。

$$\begin{aligned} \text{想定損害賠償額} &= \text{情報漏洩元組織の社会的責任度} \\ &\times \text{漏洩個人情報価値} \\ &\times \text{事後対応評価} \end{aligned} \tag{1}$$

(1) 式では、想定損害賠償額を推計するために、漏洩個人情報価値を推計している。本研究では、この漏洩個人情報価値の推計に着目した。

なお、漏洩個人情報価値の推計では、PC や記録媒体、携帯型情報端末を紛失・置き忘れてしまった場合に発生する情報漏洩価値の推計についても考慮されており、本研究の「スマートフォンの盗難紛失時に発生する情報漏洩価値を推計する」ことに対して適当だと考えたため、この推計手法を選択した。

ここで、漏洩個人情報価値の推計式を以下に示す。なお、漏洩個人情報価値の単位は円である。

$$\begin{aligned} \text{漏洩個人情報価値} &= \text{基礎情報価値} \\ &\times \text{機微情報度} \\ &\times \text{本人特定容易度} \end{aligned} \tag{2}$$

以下に、(2) 式における各項の説明を示す。

- 基礎情報価値：
  情報の種類に関わらず、基礎的な値段として 500 円を設定する。

図 2: EP 図 (日本ネットワークセキュリティ協会 [5]：シンプル EP 図より作成)

なお、ローソンの個人情報流出事故 [7] やヤフー BB の個人情報流出事故 [8] において、情報漏洩の保証として、一人あたり 500 円が流出事故の関係者に対して支払われたことを参考にし、基礎情報価値は 500 円とされている。

- 機微情報度：
  漏洩する個人情報が被害者に与える影響を「経済的損失」と「精神的苦痛」という 2 種類の観点から評価し、影響の大きさを定量化するために縦軸（y 軸）に「経済的損失」の度合いを、横軸（x 軸）に「精神的苦痛」の度合いを持たせた表を使用する（図 2）。　表における「経済的損失」と「精神的苦痛」はそれぞれ 3 段階に分けられ、機微情報度は、漏洩した情報のグラフ上の (x, y) の位置を下記の式に代入して求める。

$$\text{機微情報度} = (10^{x-1} + 5^{y-1})$$

  複数の個人情報が漏洩する場合、漏洩する情報全体で最も大きな x と y の値を使用する。

- 本人特定容易度：
  漏洩した個人情報について、本人の特定しやすさを評価する。評価を以下の基準に沿って判断する。

  本人特定容易度=6
  「氏名」&「住所」が含まれる

  本人特定容易度=3
  「氏名」または「住所」&「電話番号」が含まれる

  本人特定容易度=1
  上記以外

4　調査結果および考察

4.1 節では、スマートフォンユーザにおける現状のセキュリティ意識の調査結果を示し、4.2 節では、スマートフォンに含まれる個人情報価値提示後のユーザのセキュリティ意識の調査結果を示す。

4.1　現状におけるセキュリティ意識

スマートフォンユーザに対するアンケートでは、ユーザのセキュリティ意識について調査するため、スマートフォンで扱う個人情報の種類や、ユーザ自身が行っているセキュリティ対策の満足度、スマートフォン OS の種類やホーム画面ロック機能、スマートフォンの盗難・紛失経験の有無等について質問を行った。

なお、ホーム画面ロック機能とは、スマートフォンの画面が消灯している状態から、電源ボタンを押して解除させたときに、最初に表示される画面で利用される何らかのロック機能のことを指す。本研究では、ホーム画面ロック機能として、パスワード, 軌跡認識（なぞる）, 指紋認証を対象とした。

その調査結果を以下に示す。

スマートフォン内の仕事に関係する情報の有無により、セキュリティ意識に違いがあるのではないかと考え、その条件の下、回答者を分類した。その上でホーム画面ロックにどのような傾向があるのかをまとめた結果を図 3 に示す。

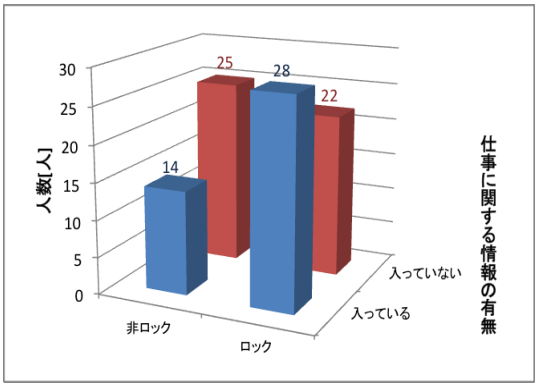

図 3: 仕事情報の有無とホーム画面ロック・非ロックの関係

図 3 によるとスマートフォンで仕事に関する情報を取り扱わないユーザはホーム画面をロックしているユーザとホーム画面をロックしていないユーザがほぼ同数だった。対して、スマートフォンに仕事に関する情報が入っているユーザにおいては、ホーム画面ロックを行なっているユーザはホーム画面ロックを行なっていないユーザの 2 倍の人数となっている。

仕事に関係する情報を扱うと回答したユーザに対し、χ^2 検定を行った結果を以下に示す。

表 1: 仕事に関係する情報を扱うユーザに対する検定結果

仕事情報が含まれるユーザに対する検定	非ロックユーザ [人]	ロックユーザ [人]	合計
実測値	14	28	42
割合	33.3333	66.6667	100
期待値	21	21	42
χ^2 検定	0.0308	$p < 0.05$	有意差あり

表 1 より、仕事に関係する情報を扱うユーザに対して有意差が見られた。

以上の結果から、スマートフォンにおける仕事の情報の取り扱いの有無は、ユーザにセキュリティ対策を意識させたため、ロック使用率に差を与えたと考えられる。

図 2 に示した EP 図の各エリアにおける選択数を図 4 に示す。なお、経済的苦痛レベルおよび精神的苦痛レベルは、図 2 のそれぞれのエリアと対応している。

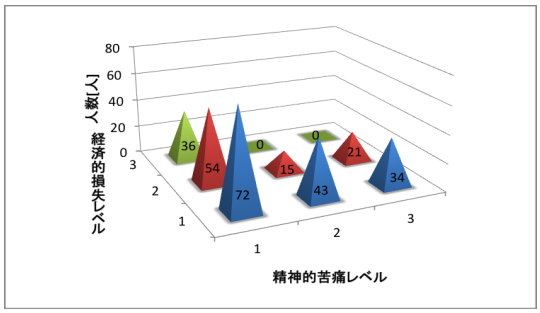

図 4: EP 図の各エリアにおける選択数

図 4 において、スマートフォンに含まれる比率が最も高いデータは $(x, y) = (1, 1)$ のエリアであり、次に $(x, y) = (1, 2), (2, 1)$ という順番であった。これは、生年月日やメールアドレスなどの基本的なデータを扱うユーザが多いことを表している。また、クレジットカード番号情報やアカウント情報などが含まれるエリア $(x, y) = (1, 3)$ が多い理由として、インターネットショッピングを利用しているユーザや SNS の利用者が多いことが考えられる。

図 4 から、ユーザはスマートフォンの利便性の高さを享受し、電話やメールといった従来の携帯電話以外の多様な情報を扱うようになってきている。そのため紛失時に失われる情報の価値は高まってきていると考えられる。

次に、スマートフォンに搭載されている OS（Windows-Phone, iOS, Android）について、OS 別のセキュリティ意識の比較を図 5 に示す。

図 5 における Android 利用者に着目すると、各セキュリ

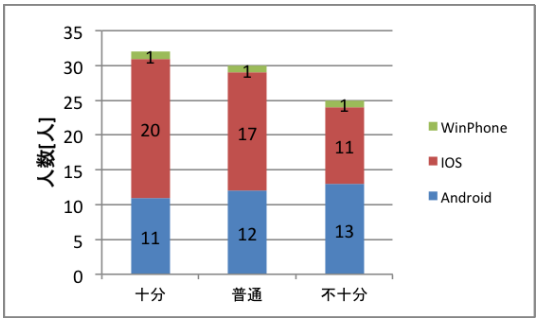

図 5: 金額提示以前のセキュリティ意識と OS の内訳

ティ意識でそれほど人数は変わらないが、iOS に着目した場合、セキュリティが「十分」と回答するユーザの割合が他の OS と比べ高かった。

iOS は 4 ケタのパスワードによるロック解除が初期設定とされており、ロックの手軽さがパスワードロックの利用率を高めていると考えられる。

次に、スマートフォン OS 別のホーム画面ロック機能におけるユーザ数の比較を図 6 に示す。

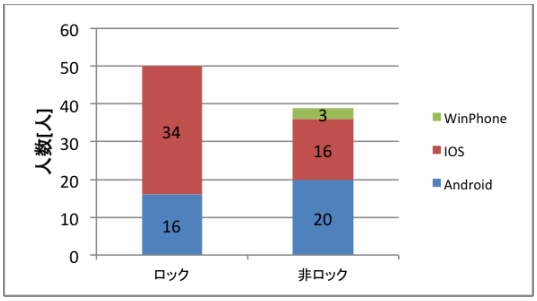

図 6: ホーム画面ロックの有無と OS の内訳

図 6 において Android ユーザに着目すると、ホーム画面ロック機能を利用しているユーザよりも、利用していないユーザの方が多かった。一方で、iOS に着目すると、ホーム画面ロック機能を利用しているユーザの方が、利用していないユーザに比べ多く、Android ユーザと iOS ユーザでホーム画面ロック機能の利用傾向が逆であった。このような利用傾向が現れる理由として、スマートフォンの OS で標準的に利用できるホーム画面ロックの導入のし易さが関係しているのではないかと考えられる。

次に、遠隔操作機能及びセキュリティソフトの利用状況を図 7 及び表 2 に示す。

セキュリティ対策として、ホーム画面ロックの認知度は 100%であったが、遠隔操作機能やセキュリテイソフトといったセキュリティ対策を知らないユーザは多数であった。ホーム画面ロック以外のセキュリティ対策を知らないユー

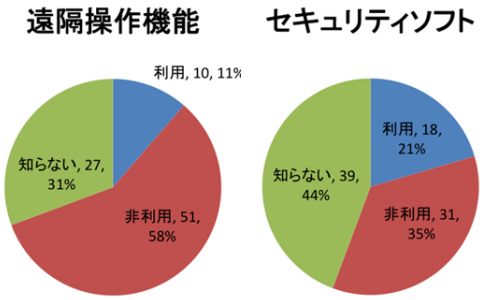

図 7: 遠隔操作機能及びセキュリティソフトにおけるユーザの利用状況

表 2: セキュリティ対策における満足度とホーム画面ロックの認知度

セキュリティ対策における満足度	ホーム画面ロックしか知らないユーザ [人]
十分	9
不十分	10

ザは 19 人で、全体の 2 割を超えており、その中の半数は、現在のセキュリティ対策で十分だと考えていた。これは、総務省の報告 [3] の通り、スマートフォンユーザがセキュリティ対策手法や脅威を十分に認知していないと言える。

次に、スマートフォンユーザに対し、盗難紛失状況の有無に関して質問し、さらにスマートフォンが手元に戻ってきたかどうかを質問した。その結果を図 8 に示す。

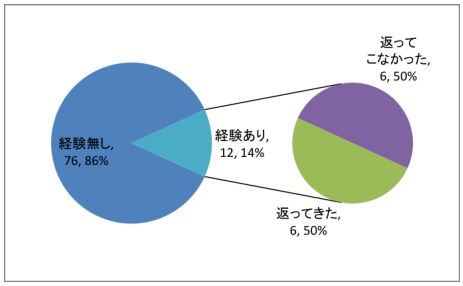

図 8: スマートフォンの盗難・紛失経験とその後の状況

図 8 の結果を見ると、盗難・紛失経験のあるユーザが 14%であり、その中でスマートフォンが手元に返ってきたと 回答したユーザが半数であった。

一方、Symantec Honey stick project[4] で行われた調査によると、スマートフォン 50 台を意図的に放置し、拾った人の行動を観察したところ、約 50%の人が持ち主へ返却しようとしたという結果が得られており、今回の調査結果とおよそ一致していると考えられる。

4.2　金額提示後におけるセキュリティ意識

スマートフォンに含まれる個人情報価値をユーザに示す前後における、ユーザのセキュリティ意識の変化を図 9 に示す。

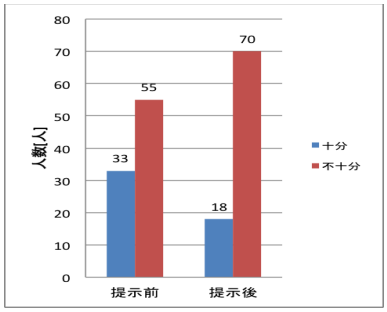

図 9: 金額提示の前後におけるユーザのセキュリティ対策の評価

図 9 において、まず、セキュリティ対策が不十分だと回答しているユーザに着目すると、個人情報価値の金額を見る前後では、回答者全体の 17%の増加が見られた。

一方で、セキュリティ対策が十分だと回答しているユーザに着目すると、金額を見る前よりも見た後の方が回答者全体の 17%の減少が見られた。さらに、図 10 より、金額提示前にセキュリティ対策が十分だと回答していたユーザの 66%が金額提示後で、セキュリティ対策の意識に変化があった。

以上の結果より、個人情報価値の金額をユーザに提示することで、ユーザは金額を踏まえてリスクを考慮することができ、自身が行っているセキュリティ対策を不十分だと認識することができたと考えられる。

なお、金額提示前にセキュリティ対策を「不十分」と回答したユーザのうち、回答者全体の約 1%が金額提示後にセキュリティ対策が「十分」であると回答した。これは、金額を見たユーザが、現在ユーザ自身の行っているセキュリティ対策で、個人情報を保護できると安心したため、これらのユーザに対しては金額提示による啓発活動の効果は低いと考えられ、他の手法を検討する必要があると考えられる。

図 9,10 で、スマートフォンにおけるセキュリティ対策の意識の変化が見られた。さらに詳しい結果について以下に示す。

まず、ホーム画面ロック機能について、金額を見る前後での意識の変化を図 11 に示す。

図 11 では、金額提示前にホーム画面ロック機能は利用しないと回答したユーザが 38 人であったのに対し、金額提示後では 15 人減少した。さらに、金額提示後にホーム

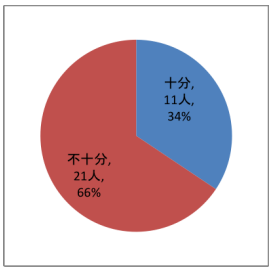

図 10: 自己評価を「十分」としたユーザの金額提示後における自己評価の内訳

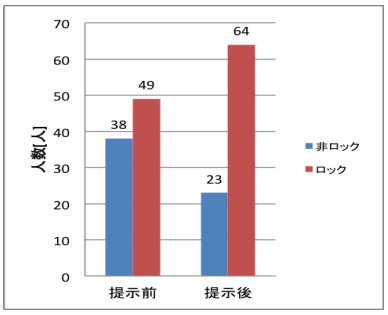

図 11: 金額提示の前後におけるユーザのホーム画面ロック・非ロックの変化

画面ロックを利用すると回答したユーザが、金額提示前よりも 15 人増加した。

また、図 12 より、金額提示前にホーム画面ロックを利用しないと回答したユーザの 61%が、金額提示後でホーム画面ロックに対する意識に変化があり、39%のユーザは金額提示前後で意識に変化が無かった。

これは、ユーザが金額を見た際に、ユーザ自身が受け入れるリスクを考慮したうえで、金額に見合うセキュリティ対策を選択した結果であると考えられ、金額提示後にホーム画面ロックを利用すると回答したユーザが 61%と多いのは、スマートフォンの OS で標準的に利用できるホーム画面ロック機能が、ユーザにとって比較的容易に行えるセキュリティ対策の一つであるためと考えられる。

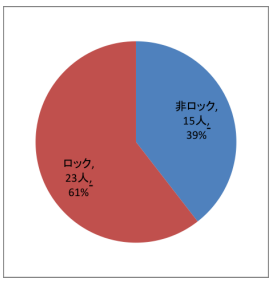

図 12: ホーム画面ロック非利用者における金額提示後のホーム画面ロックの利用・非利用の変化

さらに、スマートフォンユーザにおけるアプリケーショ

ンロックの利用意識や、使用するパスワードの複雑化、セキュリティソフトの利用意識、セキュリティソフトにおける遠隔操作機能の利用意識についても、金額を提示する前後では意識の変化が見られ、ユーザが金額を見た後ではこれまでの結果同様に、ユーザ自身が受け入れるリスクを考慮したうえで、自身に見合うセキュリティ対策を選択する傾向がみられた。

金額を見たユーザの感想とユーザにおけるセキュリティ意識との関係を表した図を以下に示す。

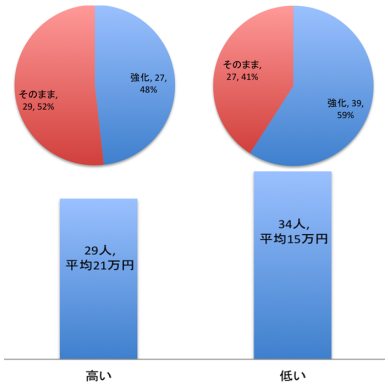

図 13: 金額を見たユーザの感想とセキュリティ意識との関係

図 13 から、個人情報価値の提示によりおよそ半数のユーザがセキュリティ対策を強化する傾向となった。自身の個人情報価値を「低い」と評価したユーザの方がセキュリティを強化する傾向が強くみられたため、金額の大小のみならず他の要因も組み合わせた意識変化の要因を明らかにしていく必要がある。

なお、セキュリティ対策を強化するとは、ユーザがこれまで行っていなかったセキュリティ対策を新たに行うようになることを指す。

5　結論

スマートフォンユーザが行うセキュリティ対策として、ホーム画面ロックの利用、アプリケーションロックの利用や、パスワードの複雑化、セキュリティソフトの利用、およびセキュリティソフトにおける遠隔操作機能の利用の 5 つを挙げた。これらの結果では、個人情報価値の提示後は全ての対策において、スマートフォンユーザが自身で行っているセキュリティ対策を見直し、ユーザ自身が受け入れるリスクを考慮したうえで個人情報価値に見合うセキュリティ対策を選択する傾向が見られた。一方で、遠隔操作機能及びセキュリティソフトに対する認知度はホーム画面ロックよりも低く、総務省の報告 [3] の通り、スマートフォンユーザがセキュリティ対策手法や脅威を十分に認知していないことがわかった。

また、個人情報価値をユーザに提示した場合、金額を見て「高い」と感じたユーザよりも、「低い」と感じたユーザの方が、セキュリティ対策を強化する傾向が見られた。

これまでの研究結果より、個人情報価値を定量的にユーザへ提示することは、ユーザのセキュリティ意識に変化をもたらし、特に、個人情報価値を「高い」と感じたユーザよりも「低い」と感じたユーザの方が、セキュリティ対策を強化する傾向が見られた。この理由として、金額を「低い」と感じたユーザはセキュリティ意識が高く、スマートフォンで扱う情報の価値を過大評価していたため、金額に対し「低い」と感じたと考えられる。

今後の課題は、ユーザが対策に要する費用や手間に対して、対策によるリスク軽減効果といった、セキュリティ対策の費用と便益を示し、ユーザのリスク回避行動を分析することが挙げられる。

参考文献

[1] 総務省, ”平成 24 年通信利用動向調査 別紙 1 ”, 2013 年 6 月

[2] 株式会社ネットマイル, ”スマートフォンのセキュリティに関する調査 ”, 2011 年 12 月

[3] 総務省, ”スマートフォン・クラウドセキュリティ研究会　最終報告 ～スマートフォンを安心して利用するために実施されるべき方策～ ”

[4] Symantec, ”The Symantec Smartphone Honey Stick Project”

[5] NPO 日本ネットワーキングセキュリティ協会 セキュリティ被害調査ワーキンググループ, ”2011 年　情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　第 1.0 版 ”,2012 年 9 月

[6] OECD(2013), ”Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value ”, OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

[7] ”ローソンの個人情報流出事故 ”, http://www. 不祥事.jp/lawson2.html

[8] ”ソフトバンク BB、450 万件超える Yahoo! BB の個人情報漏洩を認め謝罪 ”, http://internet.watch.impress.co.jp/cda/news/2004/02/27/2252.html

付録

スマートフォンユーザに対して行ったアンケートにおける文言を以下に示す。

1. スマートフォンの利用について

1. 1 日に何回スマートフォンを使用しますか。なお、手に取って操作し、置いたときを 1 回と数えることとします。
2. あなたのスマートフォンで、取り扱うデータがあれば、該当のセル（本文中の図 2）にチェックを入れてください。
   また、「氏名」「住所」「電話番号」についても、取り扱いがあるか教えてください。
   ※なお、ここでは『取り扱うデータ』をスマートフォンに保存されているデータや、Web ページなどで入力するデータなども含めることとします。
3. 仕事で使う情報は入っていますか。
4. OS を選択してください。

2. スマートフォンのセキュリティについて

1. あなたの現在のスマートフォンにおける盗難・紛失時のセキュリティ対策は十分だと言えますか。
2. ホーム画面ロックをしていますか。
3. ホーム画面ロックの手段を選択してください。
4. ロックしない理由を選択または記述してください。
5. 本文中の図 2 で選択した情報を扱うアプリケーションにロックをかけていますか。
6. ロックの手段を教えてください。
7. ロックをかける目的を選択してください。
8. パスワードをかけない理由を選択または記述してください。
9. どのようにパスワードを決めていますか。
10. パスワードに含まれる文字の種類を選択してください。
11. 現在、使用しているパスワードはデータを保護するのに十分ですか。

3. スマートフォンのセキュリティソフトについて

1. インストールしておけば、ウィルス対策・フィルタリングや、紛失時の位置の検出、端末を操作できなくする機能、端末内の情報を消去など、さまざまな機能を持つアプリケーションがあります。
   これらの機能を持つセキュリティソフト（アプリ含む）を知っていますか。
2. セキュリティソフト（アプリ含む）を使用していますか。
3. セキュリティソフトを盗難･紛失のために使用しますか。
4. セキュリティソフトを選択してください。
5. セキュリティソフト（アプリを含む）を使用しない理由を教えてください。

4. スマートフォンの遠隔操作機能について

1. スマートフォンの OS やアプリには遠隔操作によって端末を操作できなくする機能や端末内の情報を消去できる機能が搭載されているものがあります。
   このような機能を知っていましたか。
2. このような機能の使い方を知っていますか。
3. このような機能を使用したことがありますか。
4. 紛失時、どの機能を使用しますか。
5. 盗難時、どの機能を使用しますか。

5. リスク認知後のユーザの情報セキュリティに対する意識の変化を明らかにする質問群

1. （アンケート回答者にスマートフォンに含まれる個人情報価値を提示）この金額を見て、あなたはどのように感じましたか。
2. あなたのスマートフォンの盗難・紛失時のセキュリティ対策は妥当だと言えますか。
3. これまでの結果を踏まえ、今後どのような対策をとろうと思いますか。

6. ユーザの基本情報を知る質問群

1. 性別を教えてください。
2. 年齢を教えてください。
3. 職業を教えてください。
4. 携帯事業者を教えてください。
5. 今までに盗難や紛失にあったことがありますか。
6. 失くしたスマートフォンは返ってきましたか。