

ファイル共有ソフトと SNS における情報漏洩リスクに関する研究

Study on Information Leak Risk of File Sharing Systems and Social Networking Services

筑波大学大学院 システム情報工学研究科 リスク工学専攻 博士前期課程 1 年

6 班 木村雄介 重森敏郎 寺嶋直矢

アドバイザー教員 岡本栄司 満保雅浩

1. 背景

情報化社会である昨今、我々はその恩恵を受けると同時にこれまでは考えられなかったような被害を目にする機会が増大している。ファイル共有ソフトによる情報流出は、その中でも代表的な例の一つであろう。プライベートな情報流出についてはそれほど大きな報道がなされているわけではないが、個人情報 Web 上に晒され、精神的に大きな被害を受けたと推察される。被害者本人が SNS に実名で登録していたことから被害が一層拡大したケースも見られる。

また、SNS からの個人情報流出も近年話題になっている。SNS は実名で登録することで社会的ネットワークが拡大していくというメリットを持ったシステムであるため、実名で登録する人が多い。また会員制であるため、反社会的な内容を安易に書き込み、その内容が匿名掲示板に転載され、不特定多数の人に閲覧され、結果として個人が不利益を被るといった事例も見られる。

どちらの場合も一度 Web 上に情報が流出してしまうと、情報拡散を完全に止めることは不可能である。

以上の観点から、情報漏洩などの問題に普段からどの程度関心を持ち、対策を行っているのかについて把握することは、今後の新たな被害を防止する上で重要である。

2. 研究概要

(1) 研究目的

本研究では、筑波大学の学生を対象として、ファイル共有ソフト、SNS の利用状況から潜在的なリスクを算出する。またリスクに結びつく個人の属性や特徴を明確にし、どういった要因が情報流出被害抑止に影響を及ぼしているのかについて分析し、今後より良い情報教育を行っていくための基礎資料とすることを目的とする。

(2) 研究の進め方

本研究では、まずファイル共有ソフトや SNS における過去の個人情報流出事例及び既往研究を調査した。次に、代表的な流出プロセスの把握を行い、個人情報の流出プロセスの仮説を立てた。そして、筑波大学生を対象としたアンケート調査を実施した。アンケート結果から想定される被害について Event Tree Analysis で算出した。また、Event Tree Analysis と共に、情報流出被害抑止に繋がりそうな結果に着目し、分析を行った。

3. 既往研究・調査及びヒアリング調査

(1) 既往研究・調査

(a) 総務省：「インターネットと匿名性」¹⁾

インターネット利用者の「匿名性」について、利用者の意識を専門家がさまざまな角度から調査・分析を行った。調査結果の一例を以下に示す。

ユーザーが守りたいと意識している個人情報「氏名」、「性別」、「住所」、「生年月日」「家族構成」、「PC メールア

ドレス」、「携帯メールアドレス」、「電話番号」、「クレジットカード情報」の 9 項目について、ウェイトの評価（各項目に対する心理的な重みづけの推定）を調査した。調査の結果、相当程度個人を特定できる「名前」、「住所」と直接的に経済的被害を受ける可能性の高い「クレジットカード情報」のウェイトが高いことが分かった。

(b) 社団法人コンピュータソフトウェア著作権協会他：

「ファイル交換ソフトの利用に関する調査」²⁾

本調査は、ファイル交換の利用実態を把握することで、今後の効果的なファイル交換対策を講じるための基礎的資料を作成することを目的としている。

インターネットを利用している人を対象としたアンケート調査を実施しており、ファイル交換ソフトの利用を過去か現在で分け、使用するに到った経緯や使用目的や使用頻度などについて調査している。

着目すべき結果としては以下のような点が挙げられる。

- ・ファイル交換ソフトを利用したことがある人は全対象者の 9.6% である。
- ・現利用者で「正しい使い方なら問題ない」あるいは「個人が楽しむのは問題ない」と考えている人が全体の 4 分の 3 以上を占めている。
- ・過去利用者の止めた理由として上位 2 つは、「ウイルスや自分のパソコンの情報が流出するのが心配になった」が 32.6% と「著作権侵害などの問題がある」が 31.3% である。
- ・過去利用者において今後のファイル交換ソフトの利用意向として、「また利用したい」 5.4%、「機会があれば利用したい」 30.1% を合わせると、過去利用者の 3 分の 1 以上が利用意向を有している。

(c) まとめ

既往研究についてまとめると、これまで情報漏洩やファイル共有ソフトについての研究は行われているものの、SNS と併せて情報漏洩について研究したものは見られないことが分かった。なお、既往研究(1)でウェイト評価を行った情報については重要な情報と考え、本研究でも採用した。

(2) ヒアリング調査

(a) 筑波大学大学院図書館情報メディア研究科

新保史生准教授

新保准教授は、ネットワーク社会における法制度の研究や個人情報保護を専門としている。以下にヒアリング内容を挙げる。

- ・事例の違いはあるが、情報漏洩者は、プライバシー侵害や名誉棄損を行使すれば訴えることが可能で勝訴する可能性が高い。しかし実際には、訴訟を起こす事例は少ない。これは、訴訟を起こせば、実名を公開しなければならぬためである。

- ・ファイル共有ソフトは今後もなくならない。ただ、ネットワーク社会における法制度を充実させる必要がある。
- ・セキュリティを徹底している大企業でもファイル共有ソフトからの情報が流出するという事件の多くは、自宅における家族共有パソコンが原因である。
- ・被害を防止するための対策として、①普及啓発、注意喚起②刑法を重くする等が挙げられる。

(b)筑波大学環境情報機構

環境情報機構は、筑波大学における教育研究の高度化と効率化を図るための機関である。以下に、ヒアリング内容を挙げる。

- ・最近、学内からファイル共有ソフトを使用したケースが見受けられる。よって、今後、更なる注意喚起を行う。
- ・学内でのファイル共有ソフトの使用に対し、悪質な場合は停学処分も検討している。
- ・大学側が使用禁止の権力を行使できるのは大学内の使用に限る。よって、自宅など個人的に使用する場合は、利用禁止の権利及び処罰の権力をもたない。しかし、自宅で流出した情報が大学に関する機密情報であったら処罰対象になりうる。

(c)まとめ

ヒアリング調査より、現在でも大学内のネットワークを利用したファイル共有ソフトの利用者の存在、また利用者の今後の更なる増加の可能性が示唆された。すなわち、今後の情報流出を防止するための対策が重要になってくると言える。

4. 事例の紹介

本章では、事例の代表的な傾向を把握するために、ファイル共有ソフトを介して個人情報が流出した例、また SNS を介して個人情報が流出した事例をいくつか紹介する。また、事例の内容を纏めたものについて Table 1 に示す。

(1)医学生为患者情報流出事件

ある地方国立大学が医学部付属病院の患者数十人の個人情報情報をネット上に流出してしまったと発表した。医学部の男子学生の自宅パソコンから、ファイル共有ソフトを通じて流出したとみられている。

(2)ゴキブリ騒動

某ファーストフードの店舗でアルバイトをしていた高校生が「店でゴキブリを揚げた」など mixi 日記で告白、大騒ぎになった。この高校生の日記が、mixi 利用者であれば誰でも見られる設定になっていたことから騒ぎは拡大した。高校生は後に冗談のつもりで書いたと述べたが、責任を取って高校を退学した。

(3)女性わいせつ画像流出事件

男性会社員がファイル共有ソフトを使用していたところ、パソコンがウイルスに感染、個人情報が流出した。流出したのは社内情報と共に社員の恋人と思われる女性のわいせつ画像を含む写真の数々である。更に、女性が大手 SNS である mixi に実名で登録していたことから、mixi での登録情報がネット上で晒されてしまう事態となった。その結果、ネット上ではわいせつ画像のほか、女性の個人情報まで

もがばら撒かれることとなってしまった。

Table.1 事例のまとめ

事例	ファイル共有ソフトの関与	SNSの関与	匿名掲示板への書き込み	周囲への影響	本人の処分
(1)	○		○	○	
(2)		○	○	○	○
(3)	○	○	○	○	○

5. 事例に基づいた仮説

本章では、先に調査した代表的な流出事例を基に、被害発生のプロセスを取り纏める。

(1)ファイル共有ソフトのみを使用したケース

ファイル共有ソフトのみを使用したケースから被害が生じた時の仮説を Fig.1 に示す。ファイル共有ソフトを使用していて、個人情報が流出してしまったら拡散を止めることはできない。重要なのは、流出した個人情報の中身である。もし、流出した個人情報が第三者関心を引かなければ、情報は拡散することなく甚大な被害は起こらない。しかし、事例(1)のケースだと流出した情報が患者情報だったため、第三者の関心を強く引き、匿名掲示板に書き込みがされてしまい、甚大な被害が生じてしまった。

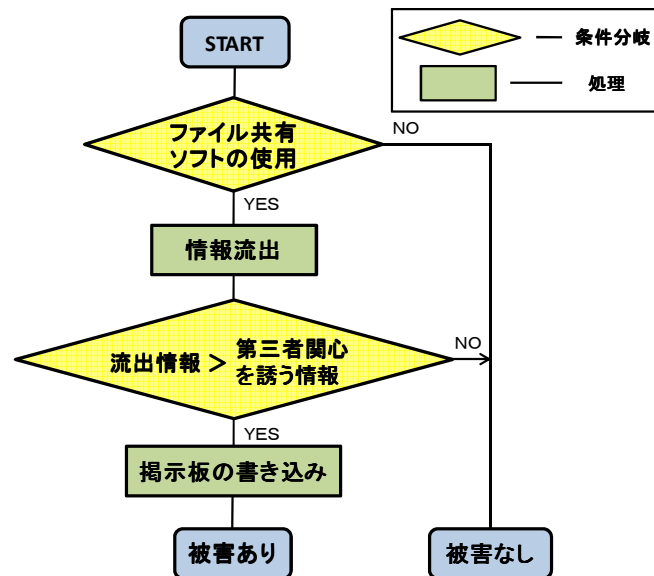


Fig.1 ファイル共有ソフトを使用した時の仮説

(2)SNSのみ使用した時のケース

SNSのみ使用した時の仮説を Fig.2 に示す。SNSを使用していて、ブログに過度な書き込みをしてしまったら、思わぬ形で不利益が生じてしまう。例えば、過度な書き込みをしてしまい、設定の公開レベルにもよるが書き込みが常識を脱している場合なら第三者によって掲示板に書き込みがされてしまうというケースが考えられる。それが広がり SNS 上で過度な書き込みをした本人が所属する団体へ情報が知れ、所属団体および団体に被害が生じてしまう場合である。

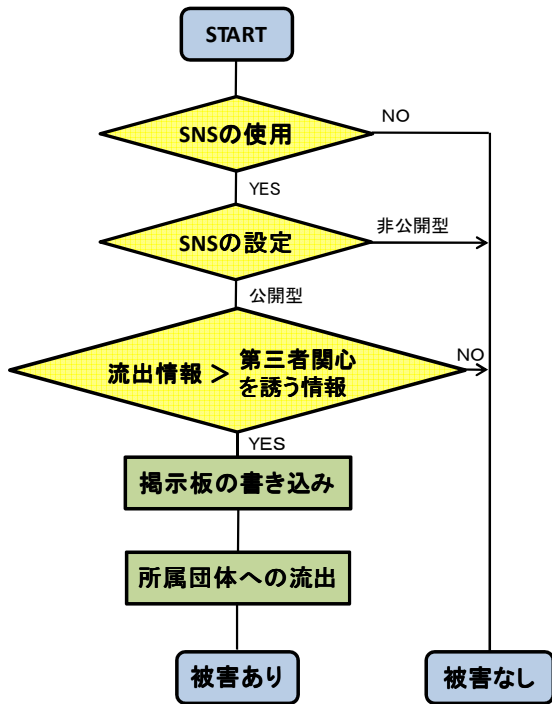


Fig.2 SNSのみを使用した時の仮説

(3)ファイル共有ソフトと SNS を使用した時の仮説

ファイル共有ソフトと SNS を使用した時の仮説を Fig.3 に示す。

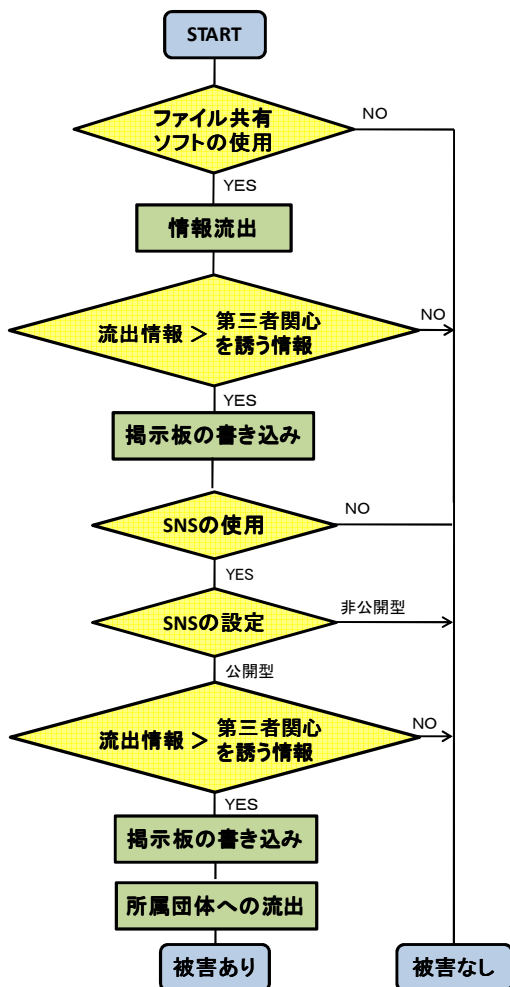


Fig.3 ファイル共有ソフトと SNS を使用した時の仮説

直接的にファイル共有ソフトを使用していない場合でも知人や自宅にあるパソコンがファイル共有ソフトを使用し

ていたなら少なからず個人情報が流出する可能性がある。事例 (3) の女性はその典型である。直接使用している場合なら流出の可能性は更に高くなるであろう。例えば、本人のパソコンにプライベート写真が保存されていてそれが漏れた場合に第三者によって掲示板に書き込みがされるだけで終わるなら気付かない限り不利益が生じる可能性は低いですが、実名や所属先などが含まれていた場合には不利益になるリスクが高くなる。それは、第三者によって SNS で検索されてしまう場合である。SNS を使用し、SNS で個人情報を開示していたなら、さらなる個人情報が漏れ、また第三者によって掲示板に書き込まれるという流れになり、本人はおろか関わりある知人や所属団体にまで被害が及んでしまう場合である。

6. アンケートによる分析

(1)アンケート内容

本研究で行ったアンケート内容について簡単に説明する。内容は大きく分けて以下の 5 つである。アンケート内容を Table 2 に示す。①、②では主にファイル共有ソフト及び SNS の現在の利用状況、情報の所有/公開状況について、③では情報別のリスク認知について、④では現在/今後の情報流出防止対策について、⑤ではアンケート対象者のインターネット利用時間などの個人属性についてそれぞれ質問している。

Table.2 アンケート内容

①ファイル共有ソフトからの情報流出可能性に関する設問
②SNS からの情報流出可能性に関する設問
③情報流出を仮定した場合の被害の大きさに関する設問
④情報流出防止対策に関する設問
⑤個人属性を問う設問

(2)アンケート実施計画

本アンケートは、筑波大学の学類生を対象とし、9月4～11日にかけて行った。異なる学類の3講義にて配布・回収を行った。回収数は合計で189となった。

(3)アンケート集計結果

(a)単純集計結果

まず、アンケートについて単純集計を行った。以下に、代表的な分析結果を示す。Fig.4 は、ファイル共有ソフトの使用経験を示した図である。Fig.4 より、ファイル共有ソフトにおける過去と現在の使用経験を合わせると、27%となり、およそ4人に1人が使用したことがあるという結果であった。

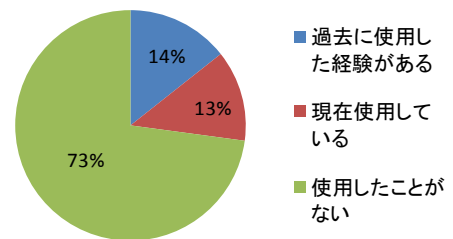


Fig.4 ファイル共有ソフトの使用経験 (N=188)

次に、SNS の利用経験を示した図を Fig.5 に示す。Fig.5 より、SNS を利用したことがある人は約 60%に達する。

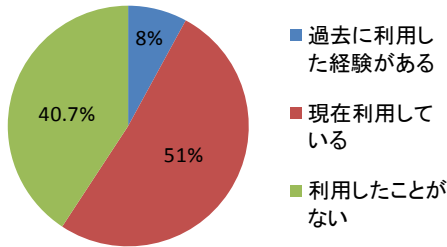


Fig.5 SNSの利用経験 (N=189)

続いて、ファイル共有ソフトの使用経験者及び SNS の利用経験者を母数とし、個人情報流出した人の割合の結果を示す。ファイル共有ソフトを通じて個人情報流出した割合を Fig.6 に SNS を通じて個人情報流出した割合を Fig.7 に示す。Fig.6 と Fig.7 を比べると、ファイル共有ソフト使用時における流出割合の方が SNS 利用時の流出割合よりやや高い。

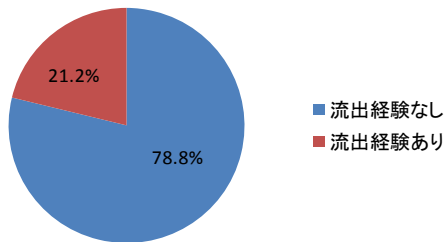


Fig.6 ファイル共有ソフトの使用経験者に対する流出経験者割合 (N=51)

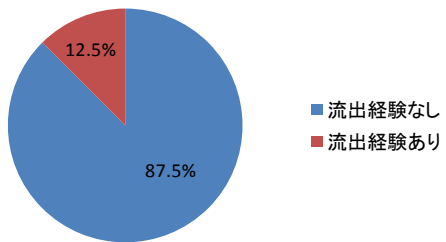


Fig.7 SNSの利用経験者に対する流出経験者割合 (N=112)

(b)情報別流出リスクの算出

リスクとは一般に、「事象の起こりやすさ」×「被害の大きさ」で求められる。今回はファイル共有ソフト及び SNS からの情報流出経験をアンケートから得、そこから「情報流出割合」を算出し、流出確率として用いる。またそれとは別に、ファイル共有ソフト・SNS の利用割合、パソコンにおける情報保有状況や SNS の情報公開状況もアンケートによって求め、情報流出可能性の分析に用いるものとする。また、「被害の大きさ」は、「名前」や「住所」などが不特定多数の人が閲覧できるようところへ晒されてしまった場合の被害を 10 段階評価で回答してもらい、得られた値を平均化して用いた。

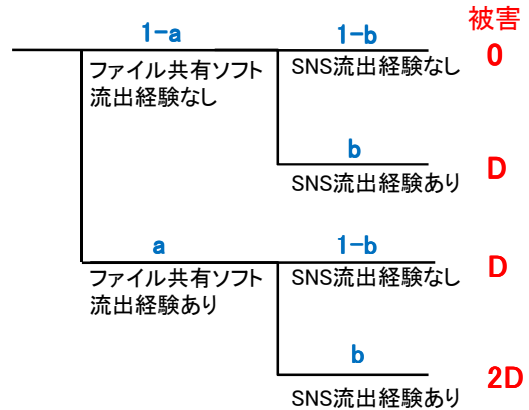
今回は分析のために、第 6 章で定義した被害発生の際の仮説フローから簡易的な情報流出時の Event Tree を作成し、それを元に情報別流出リスクを算出する。Event Tree を用いた分析は、アンケート対象者のファイル共有ソフト及び SNS からの情報流出経験を利用した場合と、ファイル共有ソフト及び SNS の現在の利用状況・情報の保有状況などを考慮した場合の 2 通り行う。区別するため、前者の分析方法によって算出したリスクを「流出リスク」、後者の分析方法によって算出したリスクを「潜在的流出リスク」とする。

①情報流出割合を考慮した場合

Fig.8 に情報流出割合を考慮した場合の Event Tree を示す。

ファイル共有ソフト及び SNS からの情報流出経験の有無によって分岐している。第 5 章より、ファイル共有ソフトを発端とし、更に SNS からも情報が流出した場合の被害は特に大きくなるのが推測されるため、ファイル共有ソフトと SNS 共に流出経験がある場合において最大被害となる。

Fig.8 の Event Tree を用いて算出したファイル共有ソフト使用時の情報別流出リスクを Fig.9 に、SNS 使用時の情報別流出リスクを Fig.10 に、ファイル共有ソフトと SNS 使用時の情報別流出リスクを Fig.11 に示す。ファイル共有ソフト使用時の情報流出リスクは、「ファイル共有ソフトの情報流出割合」×「被害」によって算出した。SNS 使用時の情報流出リスクは、「SNS の情報流出割合」×「被害」によって算出した。



- a: ファイル共有ソフト現在利用者に対するファイル共有ソフトからの情報流出経験者の割合
- b: SNS 現在利用者に対するファイル共有ソフトからの情報流出経験者の割合
- D: 情報流出時の被害の大きさ

Fig.8 流出割合を考慮した Event Tree

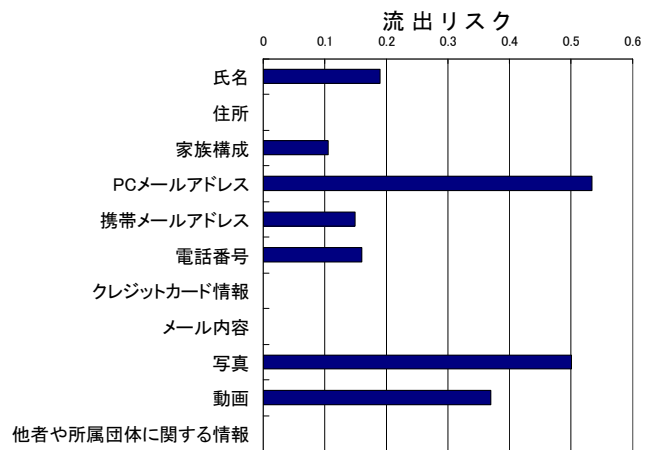


Fig.9 情報別ファイル共有ソフト使用時流出リスク

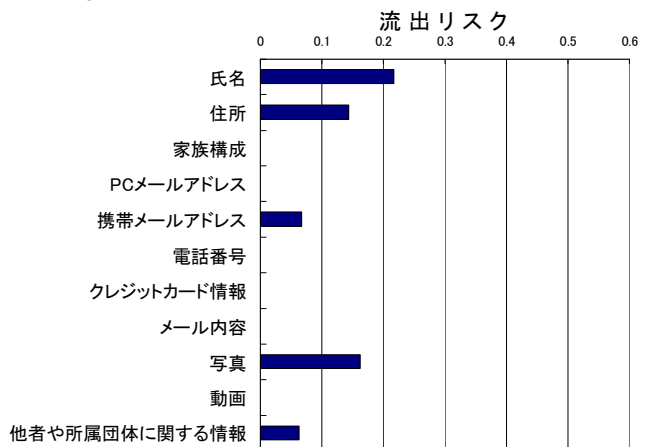


Fig.10 情報別 SNS 使用時流出リスク

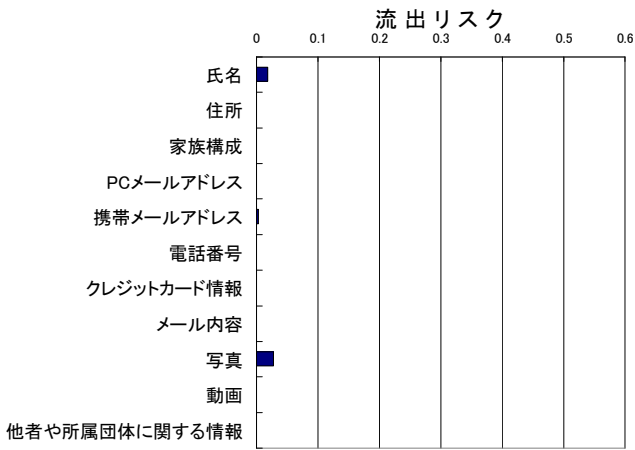


Fig.11 情報別ファイル共有ソフト兼 SNS 使用時流出リスク

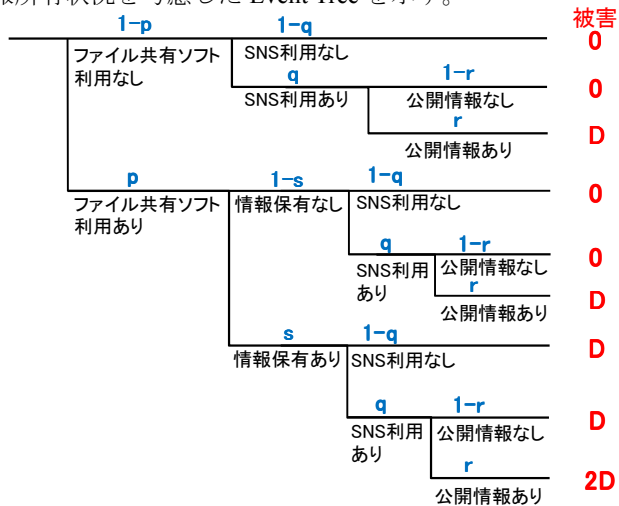
Fig.9 より、ファイル共有ソフト使用時に最も流出する可能性の高い個人情報、PC メールアドレスの 0.53 で、次いで写真の 0.50、動画の 0.37 であることがわかる。また、氏名の流出リスクは 0.19 であるが、ファイル共有ソフトを通じて実際に情報流出した事例(1)でも、氏名を流出している。以上の結果は、ファイル共有ソフトを使用して実際に流出した情報の割合と同じような結果になった。

Fig.10 より、SNS 使用時に最も流出する可能性の高い個人情報、氏名で 0.22、次いで写真の 0.16、住所の 0.14 であることがわかる。以上の結果は、SNS 使用を使用して実際に流出した情報の割合と同じような結果になった。

Fig.11 より、ファイル共有ソフトと SNS を使用した場合に最も流出する可能性の高い個人情報は、写真の 0.03、次いで氏名の 0.02 であることがわかる。ファイル共有ソフトと SNS を使用して実際に情報流出した事例(3)でも、写真、氏名が流出している。

②利用割合を考慮した場合

Fig.12 にファイル共有ソフト及び SNS の利用割合及び情報所有状況を考慮した Event Tree を示す。



- p : ファイル共有ソフトの現在利用者の割合
- q : SNS の現在利用者の割合
- r : SNS における情報公開者の割合
- s : パソコンにおける情報所有者の割合
- D : 情報流出時の被害の大きさ

Fig.12 利用割合を考慮した Event Tree

まず、ファイル共有ソフトについて現在利用者の割合を

算出し、次にパソコンにおける名前などの情報別保有割合を求める。また SNS の現在利用割合を算出し、SNS における情報の公開状況を求め、情報流出可能性の有無を探る。被害の大きさは(a)の場合と同様にファイル共有ソフトと SNS の利用が組み合わさった場合を最大としている。

Fig.12 の Event Tree を用いて算出したファイル共有ソフト使用時の情報別潜在的流出リスクを Fig.13 に、SNS 使用時の情報別潜在的流出リスクを Fig.14 に、ファイル共有ソフトと SNS 使用時の情報別潜在的流出リスクを Fig.15 に示す。ファイル共有ソフト使用時の潜在的流出リスクは、「ファイル共有ソフトの現在使用割合」×「PC における情報保有割合」×「被害」によって算出した。SNS 使用時の潜在的流出リスクは、「SNS の現在使用割合」×「SNS における情報公開割合」×「被害」によって算出した。

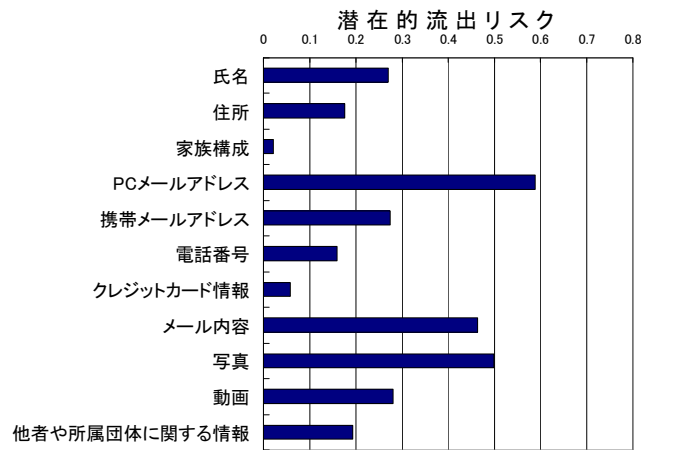


Fig.13 情報別ファイル共有ソフト使用時流出リスク

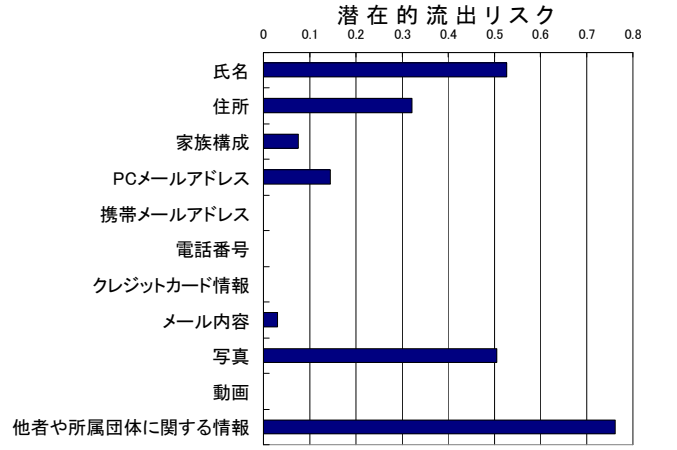


Fig.14 情報別 SNS 使用時流出リスク

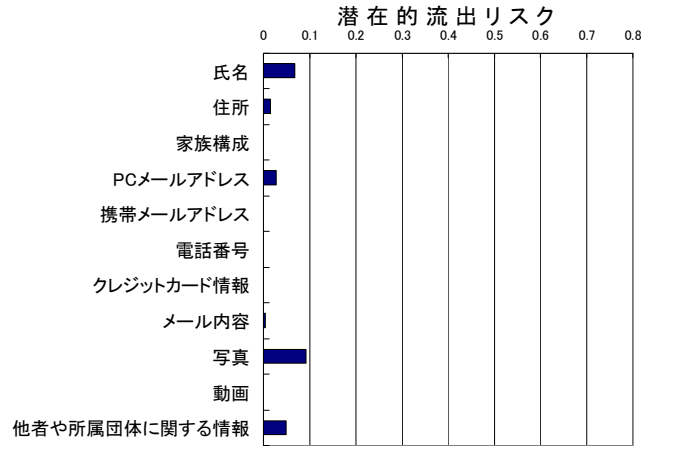


Fig.15 情報別ファイル共有ソフト兼 SNS 使用時流出リスク

Fig.13 より、ファイル共有ソフト使用時に最も流出する可能性の高い個人情報、PC メールアドレスの 0.59 で、次いで写真の 0.50、メール内容の 0.46 であることがわかる。算出した情報流出リスクは、情報保有割合と正の相関があるため、情報保有割合が高い情報は、流出する可能性が高いと結論付けることができる。

Fig.14 より、SNS 使用時に最も流出する可能性の高い個人情報、他者や所属団体に関する情報で 0.76、次いで氏名の 0.52、写真の 0.50 であることがわかる。SNS を使用して実際に情報流出した事例(2)でも、所属団体に関する情報、氏名、写真が流出している。算出した情報流出リスクは、SNS 使用時の情報の公開度合いと正の相関があるため、情報を公開することでその情報が流出するリスクも高まることわかる。

Fig.15 より、ファイル共有ソフトと SNS を使用した場合に最も流出する可能性の高い個人情報は、写真の 0.09 で、次いで氏名の 0.07、他者や所属団体に関する情報の 0.05 であることがわかる。

(c)情報流出を防止していくための対策

今後情報流出を防止していくための対策について検討する。まず、Fig.16 にどの対象から「ファイル共有ソフトをやめる」ように注意された場合、やめようと思うかという設問についての図を示す。

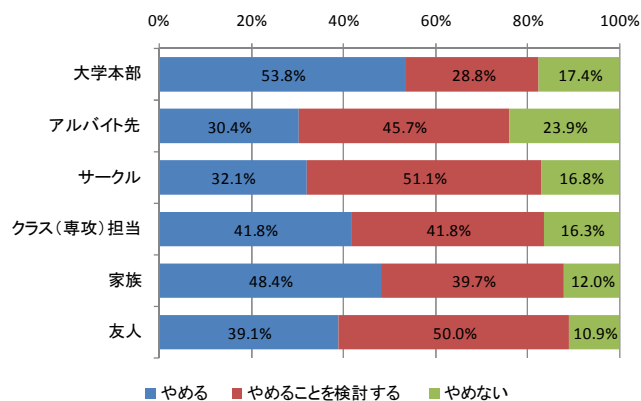


Fig.16 対象別の提言効果 (N=184)

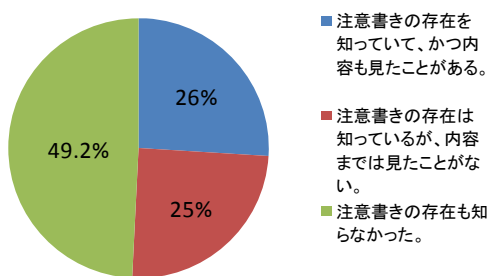


Fig.17 注意書きの認知度 (N=185)

Fig.16 より、「やめる」と「やめることを検討する」の占める割合が高いのは「家族」「友人」と、比較的近い人間関係であるが、「やめる」に絞ってしてみると、割合が高いのは「大学本部」であることが分かる。以上のことから、大学本部の注意喚起はファイル共有ソフトの使用をやめさせるには有効である可能性がある。しかし、その一方で Fig.17 により、大学の出している注意書きのことを知らない学生が約半数にのぼることが分かる。このことから、大学本部は現段階では有効な注意喚起を行っていない可能性があることが指摘できる。大学は注意喚起を行っていることをよ

り広く認知してもらうような広報活動を行っていく必要があるだろう。そのためには Web 上の注意書きだけではなく、普段学生がよく目を向けるような連絡用の掲示板なども積極的に活用していく必要があるのではないだろうか。

また、ファイル共有ソフトの使用をやめさせることができた場合のリスクの減少可能性についても分析を行った。ファイル共有ソフトを現在使用している人の割合は、Fig4 から 13%である。現在使用者が大学本部に注意をされ、やめた場合、現在使用者の割合は 13%から 8%に下がることが期待される。Fig18 に、大学本部から注意されてファイル共有ソフトの使用をやめた場合と、やめる前の潜在的流出リスクを比較したものを示す。

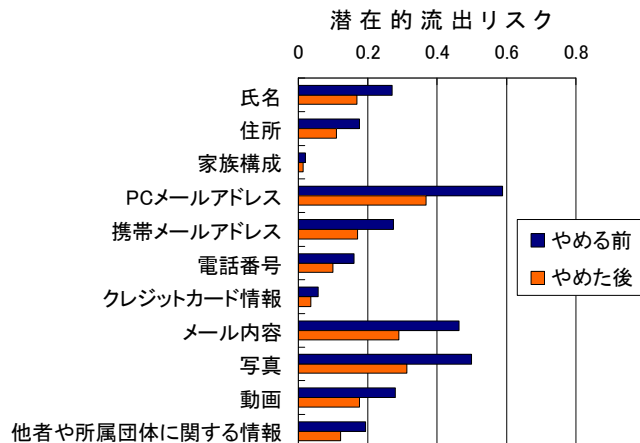


Fig.18 注意喚起によるリスク減少効果

Fig18 から、使用をやめたことにより、潜在的流出リスクが全体的に 70%程度から 60%程度に減少することがわかる。よって、大学本部の効果的な注意喚起により、ファイル共有ソフトのリスクを大幅に減らすことができる可能性があるといえる。そのためには先述したが、大学本部が注意喚起を行っているという現状を学生に知ってもらうことが重要である。

7. まとめ

本研究は、ファイル共有ソフトと SNS のリスクを定量的に解析することによって、相対的に流出リスクの高い情報を抽出、また更なる情報流出を防止するために有効な対策を検討することにより、今後のよりよい情報教育を行っていくための基礎資料とすることを目的とした。アンケート調査を基にした分析の結果、以下のようなことが明らかとなった。

- ・ SNS 利用時に流出リスクの高い情報として、「氏名」「住所」「写真や団体に関する情報」が挙げられた。
- ・ ファイル共有ソフト利用時に流出リスクの高い情報として、「氏名」「PC メールアドレス」「写真」などが挙げられた。
- ・ ファイル共有ソフトの利用者に対して利用をやめさせるための有効な手段として、大学本部からの注意喚起が挙げられた。

参考文献

- 1)総務省：「インターネットと匿名性」2008/3
- 2)社団法人コンピュータソフトウェア著作権協会他：「ファイル交換ソフトの利用に関する調査」2007/12