PBL最終発表

～フィッシングに対する意識調査とその被害低減に向けた分析 ～

5班平野威吹 LIU YUHENG 内堀紘徳 小久保知己

目次

背景

- フィッシング詐欺：
  - ある送信者を偽り，攻撃対象者から個人情報やパスワードを入手する詐欺
  - フィッシング詐欺の被害件数は年々上昇[1]，かつ手口が巧妙になっている

→対策や正しい知識を身に着けることが重要

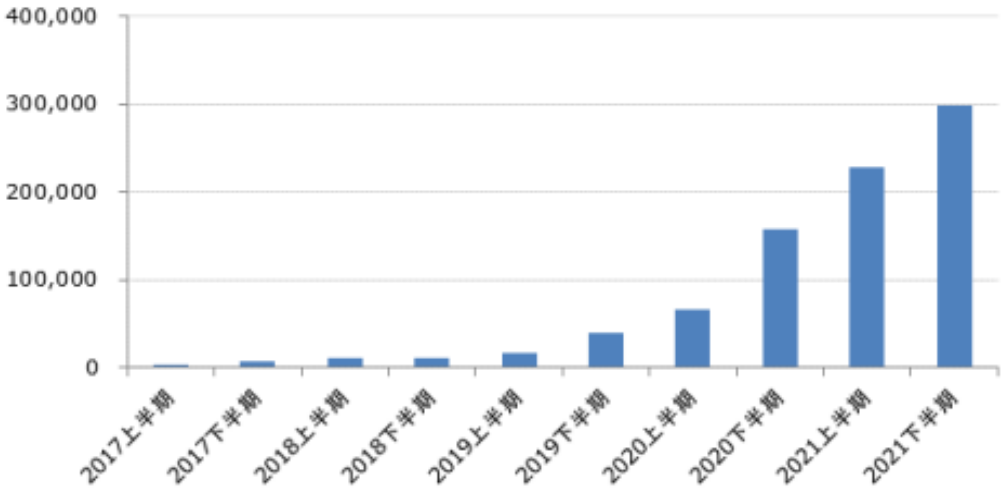


図1 国内のフィッシング情報の届出件数

出典：https://www.antiphishing.jp/report/phishing_report_2022.pdf

目次

関連研究
フィッシング詐欺のビジネスプロセス分類

林ら（2021）によるフィッシングのプロセス図

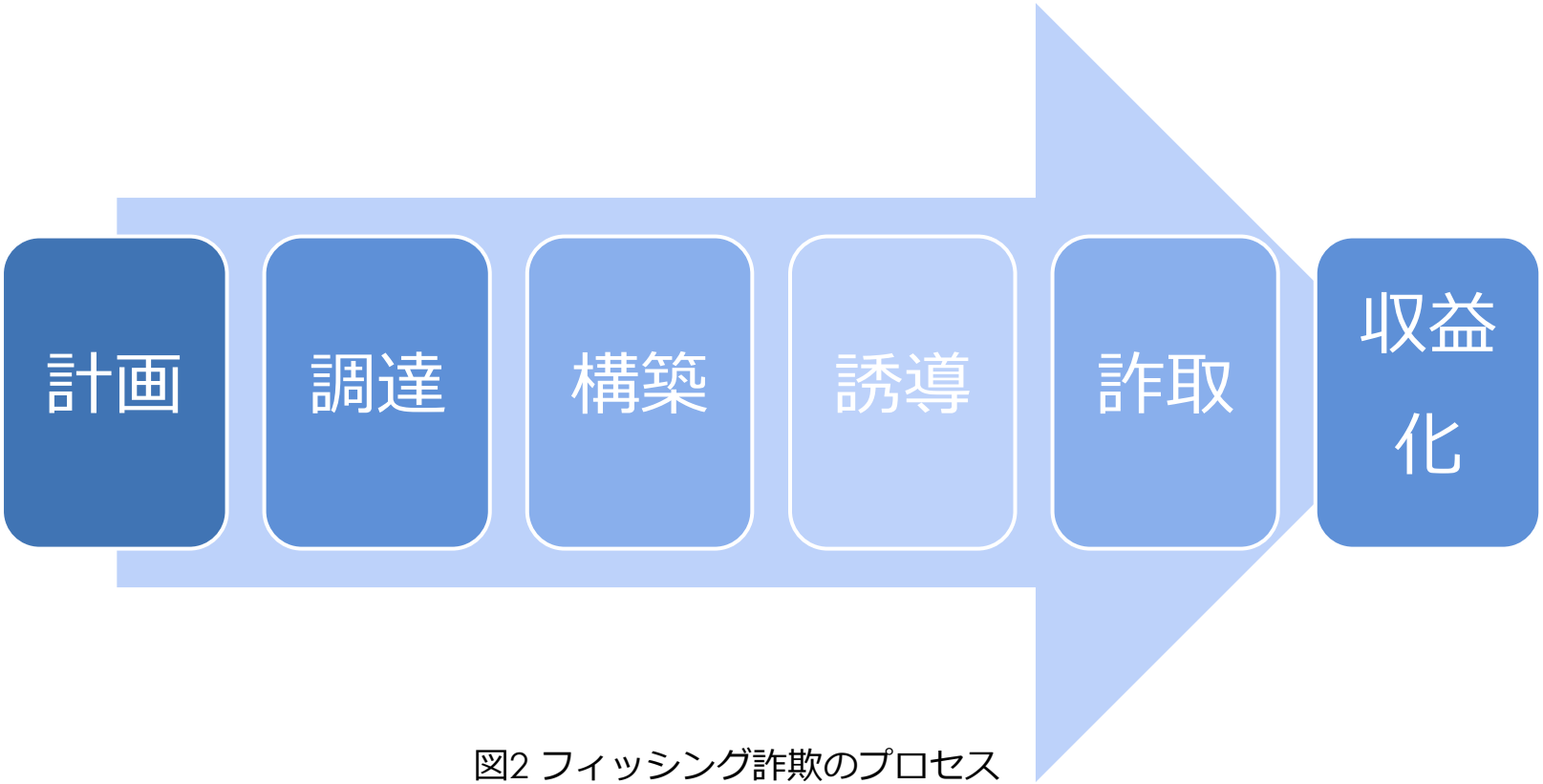


図2 フィッシング詐欺のプロセス

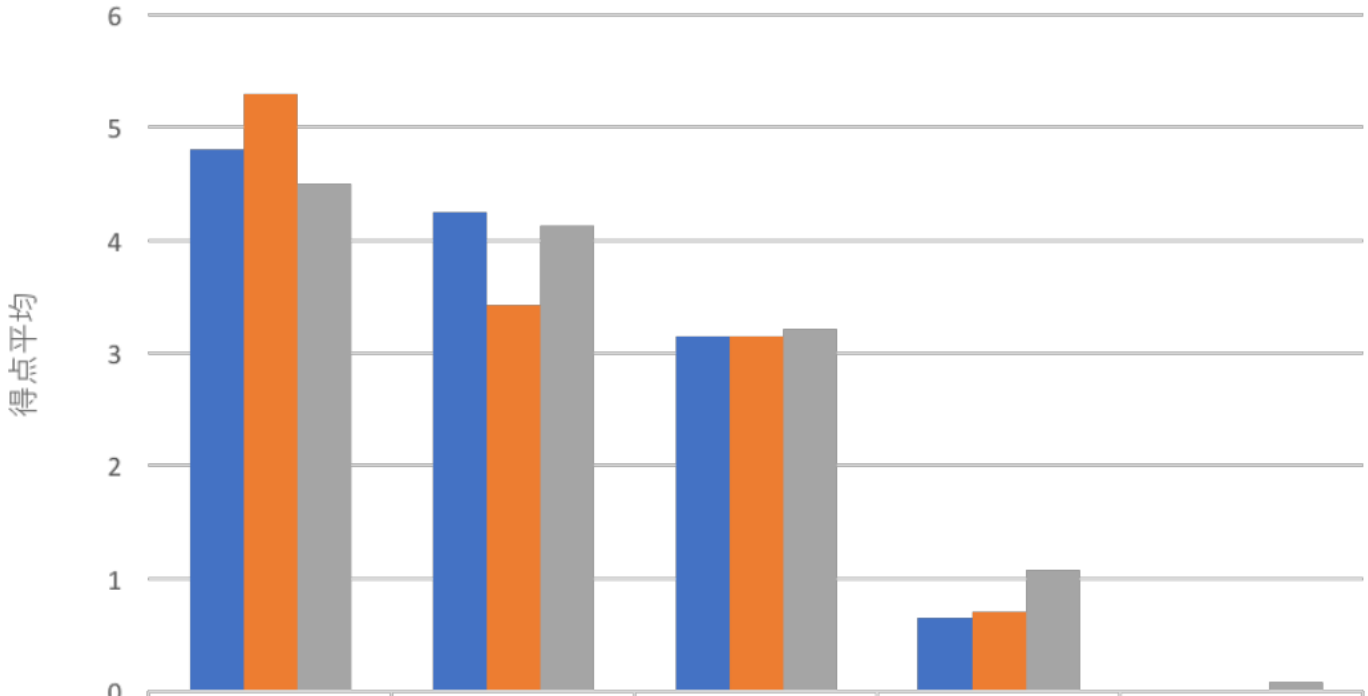
出典：林ら(2021)[3]

関連研究
熟慮性-衝動性の判定方法

小倉ら（2017）によるフィッシング回避に関係する心理特性

- 認知的熟慮性-衝動性尺度10項目
- 「深く物事を考えるほうだ」、「用心深いほうだ」
- 「1:あてはまらない」から「4:あてはまる」の4段階
- 得点が高いほど熟慮性が高いと判断した
- 中央値の28点を基準にし，29点以上を熟慮群，28点を中位群，27点以下を衝動群とした

関連研究
熟慮群,衝動群間の差異の検討



	セキュリティ	フィッシング	メール判定	クリック	危険-クリック
熟慮群	4.8	4.25	3.15	0.65	0
中位群	5.29	3.43	3.14	0.71	0
衝動群	4.5	4.13	3.21	1.08	0.08

図３　各郡の得点

出典：小倉ら[4]

関連研究
熟慮性-衝動性の判定結論

- 批判的思考態度がフィッシング回避の知識と関わる
- フィッシング回避に関係する行動と心理的特性として、熟慮性の高いユーザと比べ、衝動性の高いユーザがメールやサイトの真偽にかかわらず、クリック行動を取りやすい可能性がある。

目次

目的・課題

動機

- 一般向けのフィッシング詐欺への啓蒙が少ない
  例）オレオレ詐欺ポスターのフィッシング詐欺版

目的

- 身近な人がフィッシングメールに騙されないように啓蒙を行う
- フィッシングの被害低減に向けた提言をする

課題

- フィッシングに対するユーザーの認知度について調査する
- 年齢や性別によるフィッシング認知度の相関関係の違いについて分析する

目次

1. 背景
2. 関連研究
3. 目的・課題
4. **進め方**
5. 結果と考察
6. まとめと今後の展望

調査方法・対象

- アンケート方式
  - 期間：2022年9月12日～2022年9月27日
  - Googleフォーム
  - 19歳以下から60代までの計87人から回答を得た

- 依頼方法
  - R2工学学位PのM1～D3のメーリングリスト
  - 班員の家族や知人

⇨可能な限り幅広い年代からの回答を得られるようにした

アンケート概要

計22項目から構成

- 回答者の属性情報
- 普段のインターネットサービス利用状況
- フィッシングや情報セキュリティに関する知識　など

- 相関分析
- 可視化による分析

表1 アンケートの概要

質問番号	項目	質問内容	選択肢
1	基本属性	あなたの年齢をお知らせください	1. ~19歳，2. 20~29歳，3. 30~39歳，4. 40~49歳，5. 50~59歳，6. 60~69歳，7. 70~79歳，8. 80~89歳，9. 90~99歳，10. その他
2		あなたの職業をお知らせください	1. 経営者・役員，2. 会社員，3. 契約社員・派遣社員，4. パート・アルバイト，5. 公務員（教職員除く），6. 教職員，7. 医療従事者，8. 自営業・自由業，9. 専業主婦・主夫，10. 大学生・大学院生，11. 専門学校生・短大生，12. 高校生，13. 士業（公認会計士・弁護士・税理士・司法書士），14. 無職，15. 定年退職，16. その他
3		あなたの性別をお知らせください	1. 男性，2. 女性，3. その他
4	普段のインターネットサービス利用状況	普段のSNSの利用頻度をお知らせください	1. 週0~1日，2. 週2~3日，3. 週4~5日，4. 週6~7日，5. 全く使わない，6. 毎日使う，7. その他
5		オンラインショッピングの利用頻度をお知らせください	1. 週0~1日，2. 週2~3日，3. 週4~5日，4. 週6~7日，5. 全く使わない，6. 毎日使う，7. その他
6		オンラインショッピングでクレジットカードを利用していますか	1. はい，2. いいえ，3. その他
7		インターネットでメールを利用しますか	1. はい，2. いいえ，3. その他
8	基本知識	フィッシングメールと呼ばれる手法/技術をご存知ですか	1. はい，2. いいえ，3. その他
9		フィッシングメールを受け取ったことがありますか	1. はい，2. いいえ，3. その他
10		フィッシングメールと思われるメールを受け取ったときどんな対応をしますか (選択肢にない場合はその他に記述してください)	1. メールを開かず，そのままにする，2. メールを開かず，削除する，3. メールを開いて中身を確認してから，そのままにする，4. メールを開いてから削除する，5. メールは開くが，リンクはクリックしない，6. メールを開き，リンクをクリックしてみる，7. その他
11		フィッシングによる被害を受けたことはありますか	1. はい，2. いいえ，3. その他
12		「はい」と答えた方に伺います どのような被害を受けましたか	自由記述
13		フィッシング詐欺についてあなたはどの程度理解していますか	1. 全く理解していない，2. あまり理解していない，3. どちらともいえない，4. 少しは理解している，5. 大いに理解している
14	普段の対策状況	パスワードの使い分けは行っていますか	1. はい，2. いいえ，3. その他
15		最も利用するメールクライアントは何ですか (選択肢にない場合はその他に記述してください)	1. Gmail，2. outlook，3. Yahoo!，4. thunderbird，5. au，6. softbank，7. docomo，8. その他
16		普段利用しているスマホにウイルス対策ソフトを導入していますか	1. はい，2. いいえ
17		普段利用しているパソコンにウイルス対策ソフトを導入していますか	1. はい，2. いいえ
18	応用知識	ウイルス対策ソフトはどの程度自分をフィッシング詐欺から守っていると考えていますか	1. 全く守っていない，2. あまり守っていない，3. どちらともいえない，4. すこしは守っている，5. 大いに守っている
19		この中であなたが知っていることをすべて選んでください	1. フィッシング詐欺に乗っているurlはのリンク先のurlとは限らない，2. メールだけではなく，SMSやDMを利用したフィッシング詐欺もある，3. フィッシング詐欺の有効な対策方法としてワンタイムパスワードがある，4. 電子メールにおいて差出人アドレスは容易に詐称できる，5.「co.jp」は日本国内に住所が必要なドメイン名であるため、信頼性が比較的高い，6. Webサイトなどで個人情報を入力する場合は，SSL接続であること，及びサーバ証明書が正当であることを確認する，7. 短縮URLは安全性が低い，8. https接続になっていれば通信は暗号化されるが接続先が安全とは限らない
20		次の中から知っているもの，行っているものをすべて選んでください	1. 電子署名，2. SSL証明書，3. 注意喚起をしっかりと読む，4. どれも知らない，行っていない
21	行動	メールに掲載されたurlクリックしてサイトにアクセスするように要求された時どのような対応をとりますか (選択肢にない場合はその他に記述してください)	1. クリックしない，2. メールの信用性を確認してからクリックする，3. とりあえずクリックする，4. その他
22		URLを開き、個人情報を入力する場合，どのような行動をとりますか (選択肢にない場合はその他に記述してください)	1. 入力しない，2. サイトの信用性を確認してから入力する，3. とりあえず入力する，4. その他

目次

1. 背景
2. 関連研究
3. 目的・課題
4. 進め方
5. **結果と考察**
6. まとめと今後の展望

ウイルス対策ソフトの導入割合と意識の関係

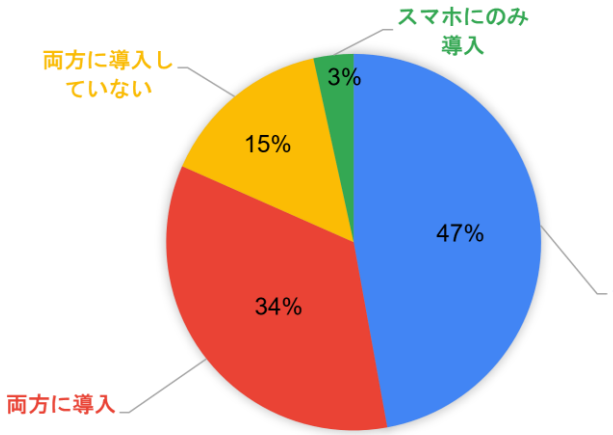


図4　ウイルス対策ソフト導入割合

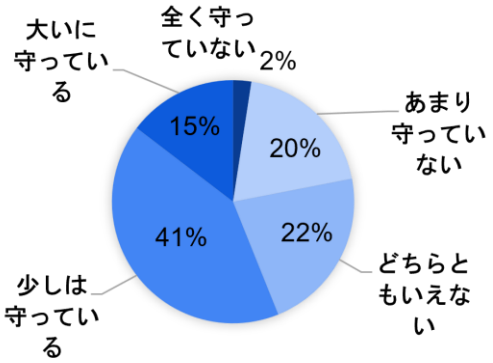


図5-a　パソコンにのみ導入の意識

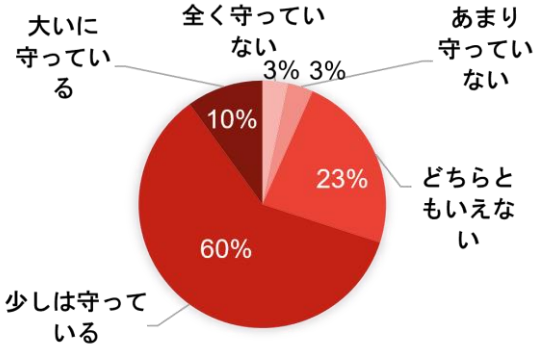


図5-b　両方に導入の意識

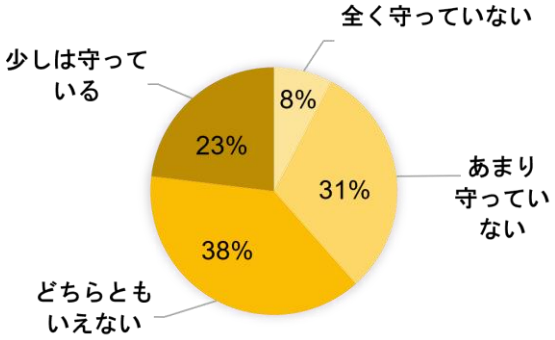


図5-c　両方に導入していないの意識

・ウイルス対策ソフトに対する信頼度が低いことやフィッシング詐欺から守るという目的で導入していないことが考えられる.

・ウイルス対策ソフトがフィッシング詐欺から守ってくれる機能の周知が詐欺被害の低減につながる.

年齢とウイルス対策ソフトの導入率の関係

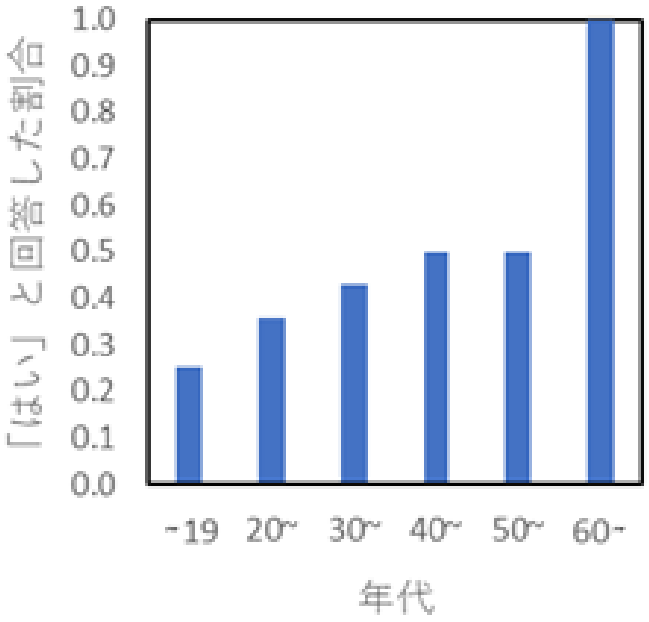


図6-a　スマートフォン

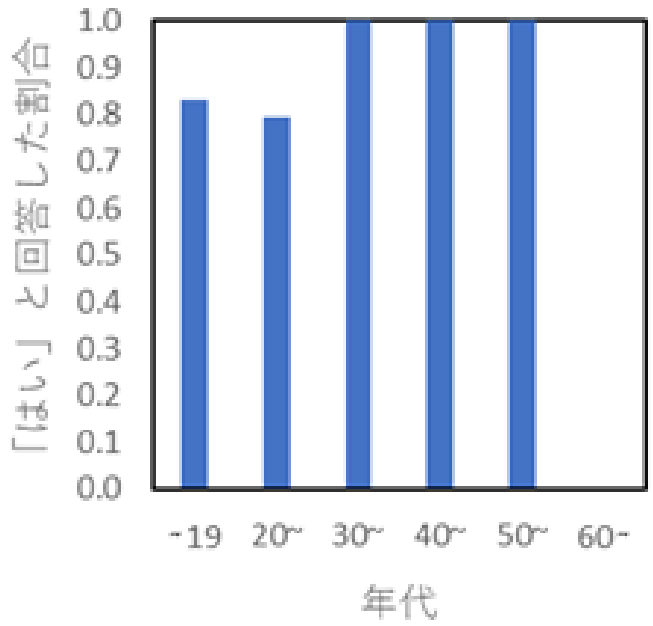


図6-b　パソコン

・若い世代の方がスマホ，パソコンともに導入率が低い
→若い人向けの注意喚起が重要である可能性

オンラインショッピングでのカード利用とウイルス対策ソフトの導入の関係

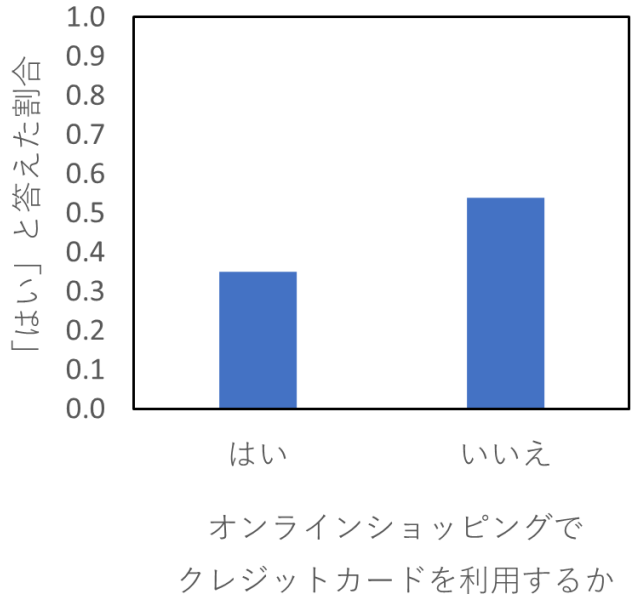


図7-a　スマホ

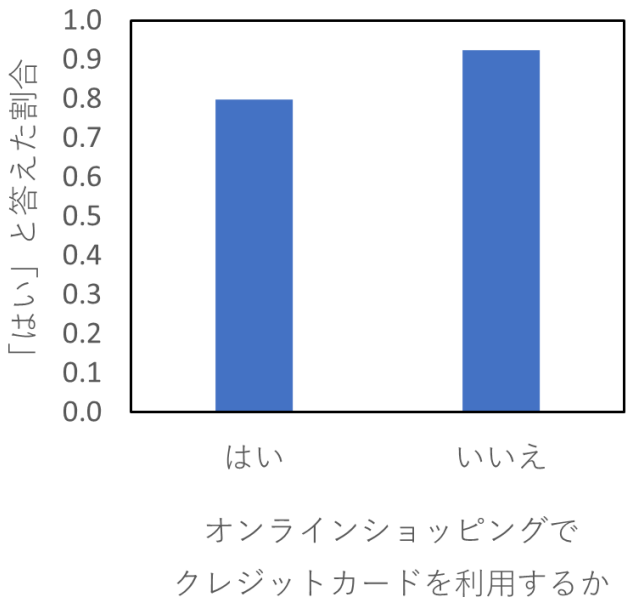


図7-b　パソコン

・カードを使う層の方が対策ソフトを導入しない
→一度自分のデバイスのセキュリティを見直す機会をつくるべきである

人々のフィッシングに対する知識項目

項目番号	項目内容
項目1	フィッシング詐欺に乗っているurlはのリンク先のurlとは限らない
項目2	メールだけではなく，SMSやDMを利用したフィッシング詐欺もある
項目3	フィッシング詐欺の有効な対策方法としてワンタイムパスワードがある
項目4	電子メールにおいて差出人アドレスは容易に詐称できる
項目5	「co.jp」は日本国内に住所が必要なドメイン名であるため、信頼性が比較的高い
項目6	Webサイトなどで個人情報を入力する場合は，SSL接続であること，及びサーバ証明書が正当であることを確認する
項目7	短縮URLは安全性が低い
項目8	https接続になっていれば通信は暗号化されるが接続先が安全とは限らない

各知識項目の認知率

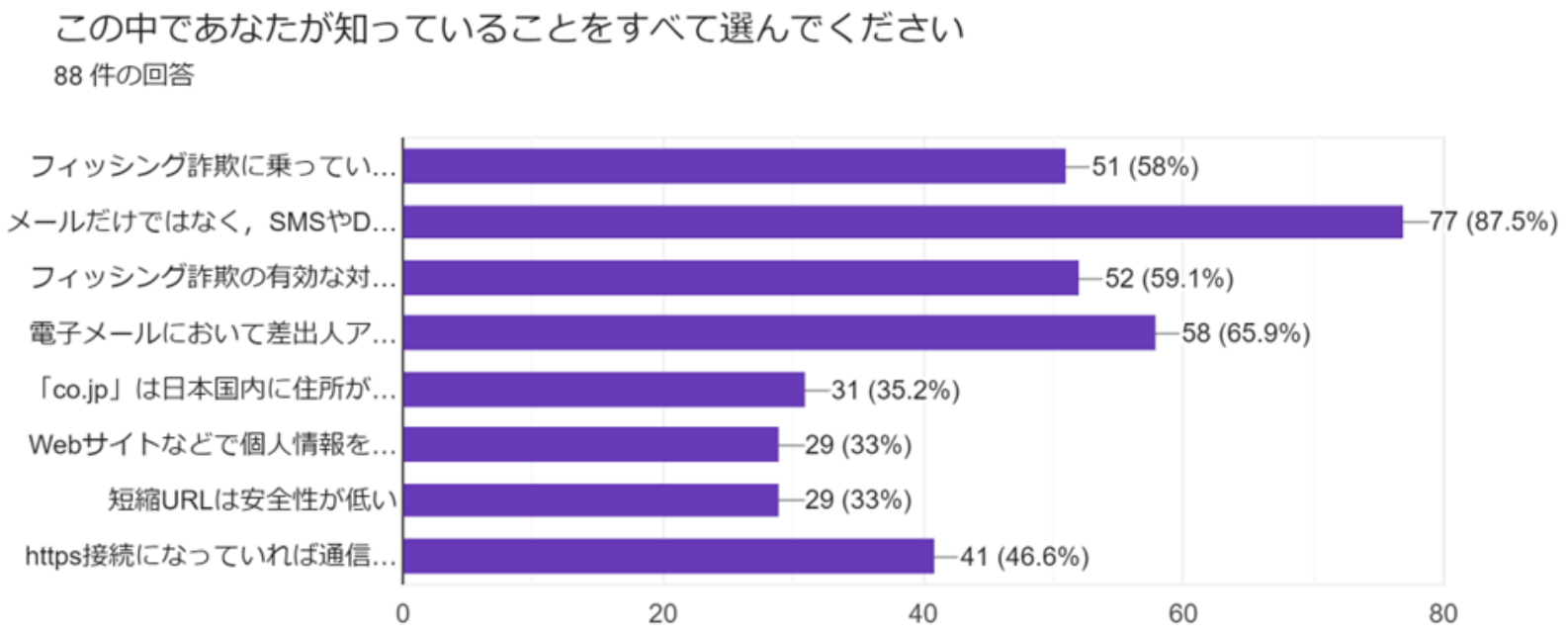


図8　各知識の認知率

・メールだけではなく，SMSやDMを利用したフィッシング詐欺もある：最も高い
・短縮URL,SSL接続について：最も低い

紹介：短縮URLについて

- 短縮URL：長いURLを載せなくていいメリットがある
- 一方で，本来のアクセス先を隠すことができてしまうので
  フィッシング詐欺等によく用いられる.
- 対策
  - リンクをクリックせず，自分でブラウザから検索してそのサイトにアクセスする

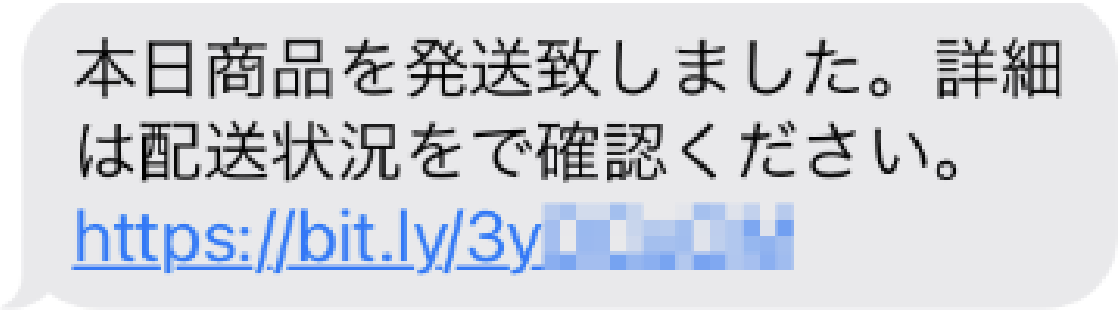


図9　Bitlyが提供する短縮URLサービスを用いた詐欺事例

紹介：SSL接続，サーバ証明書について

SSL接続：通信時に情報を暗号化し，第三者に盗用されることを防ぐ技術

図10　GoogleChromeによるサーバ証明書確認

年齢層と各知識項目の相関関係

- 知識項目の認知度は、「知識項目の選択肢を選んだ数量」とした
- 相関係数の計算結果は-0.250であるので、弱い負の相関が見られた.
  - 相関関係は弱いが、年齢が増えれば、フィッシングに関する知識が弱くなると考える.

- フィッシングの被害を低減する提言：
  - 高齢者が携帯，スマホ，PCを購入する時に、店はフィッシングに関する説明書と説明動画を高齢者に提示する.
  - 若い人は自分の家族の高齢者や職場の高齢者にフィッシングに関する知識を説明する.

行動について

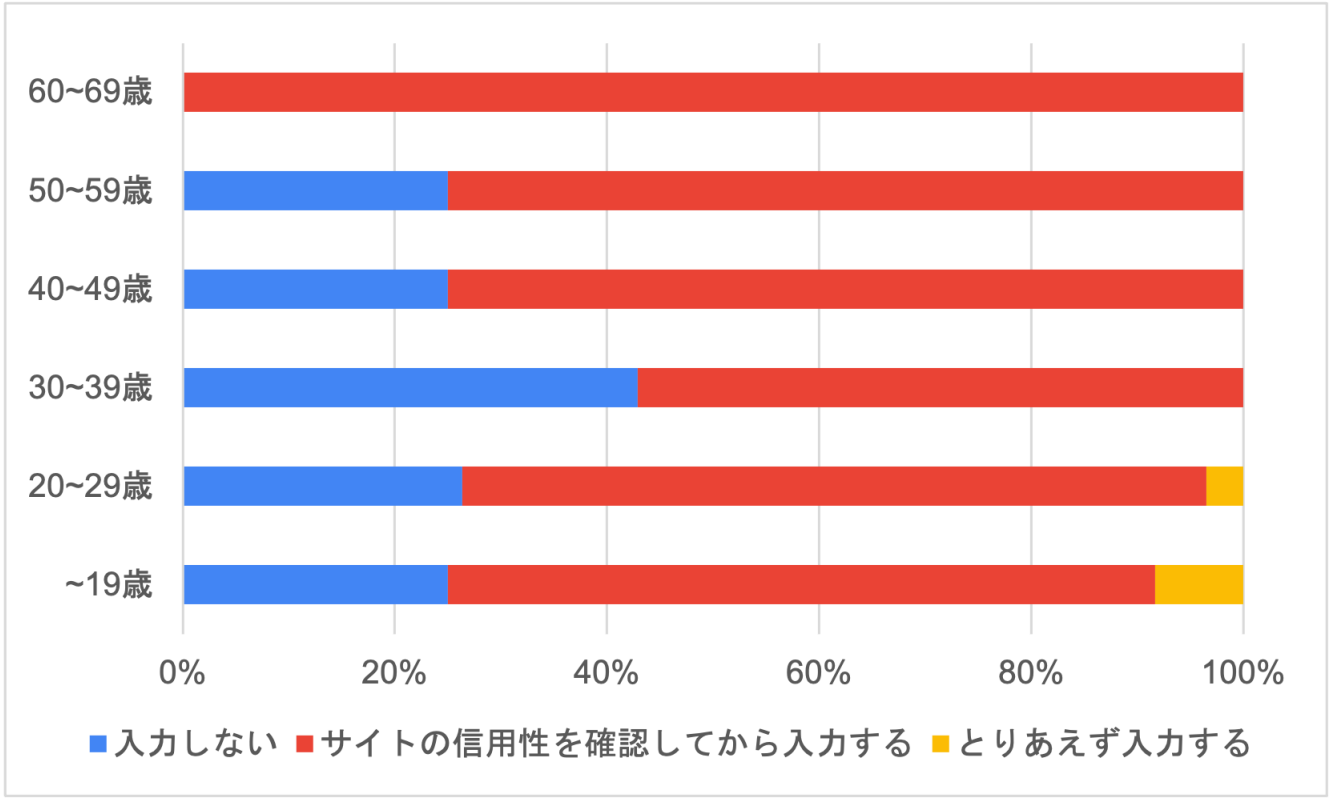


図11　年齢層別個人情報入力時のユーザの行動選択

目次

1. 背景
2. 関連研究
3. 目的・課題
4. 進め方
5. 結果と考察
6. **まとめと今後の展望**

まとめと今後の展望

本研究で得られた主な結果

1. ウイルス対策ソフトにはフィッシング詐欺から守ってくれる機能があるということの周知が必要
2. フィッシングに対する知識量は若い世代の方が多いという結果になった．そのため若い世代による高齢者層への協力が望ましい
3. 個人情報入力に対する警戒心が比較的薄い29歳以下の若年層や40歳以上の年齢層に対する注意喚起が必要
4. SNS 等の運営会社に対してユーザへの注意喚起を義務化するような法整備が有効な対策となるのではないか
5. フィッシング詐欺の対策として，メールに掲載されたURLをクリックした際や個人情報入力時にポップアップで注意喚起をするようなWebブラウザ側の対策が必要

参考文献

- [1]フィッシング対策協議会, https://www.antiphishing.jp/report/other/, 2022-06-23
- [2]Lain, Daniele, Kari Kostiainen, and Srdjan Capkun. "Phishing in Organizations: Findings from a Large-Scale and Long-Term Study." *arXiv preprint arXiv:2112.07498* (2021).
- [3]林憲明, 唐沢勇輔, 中村智史, 等. フィッシング詐欺のビジネスプロセス分類[J]. 研究報告マルチメディア通信と分散処理 (DPS), 2021, 2021(1): 1-8.
- [4]小倉加奈代. ユーザのフィッシングサイト回避能力と心理特性との関係性の検討[J]. 研究報告セキュリティ心理学とトラスト (SPT), 2017, 2017(8): 1-6.