情報セキュリティインシデントの二次被害抑止に向けた学生報告の実態調査と報告促進の提言

PBL演習1班　アドバイザー教員: 片岸 一起

202220519 赤﨑 健太郎

202220521 石川 大嵩

202220524 海老原 将

202220553 Li Xintong

背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

情報セキュリティインシデントの変化

新型コロナウイルス感染症の流行以降、企業ではテレワーク、学校ではリモート学習の活用が急速に拡大

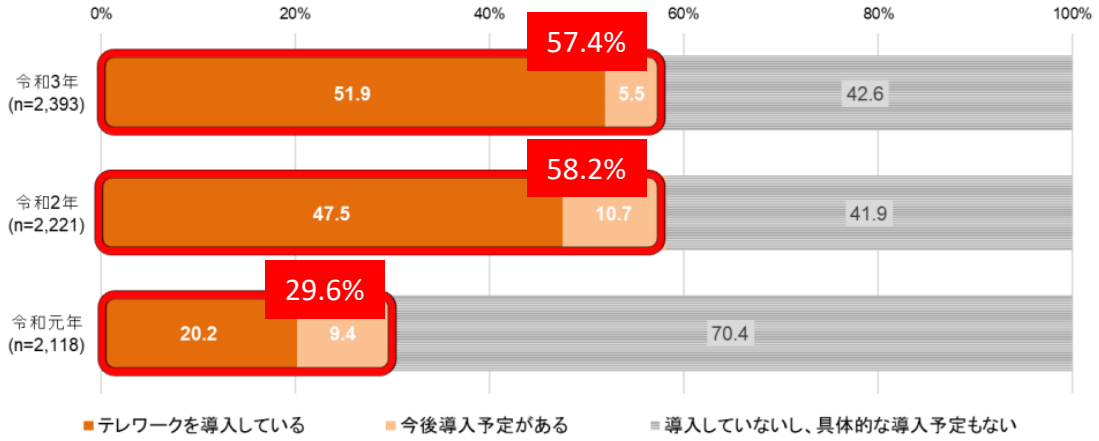


図1　企業でのテレワーク導入状況[1]

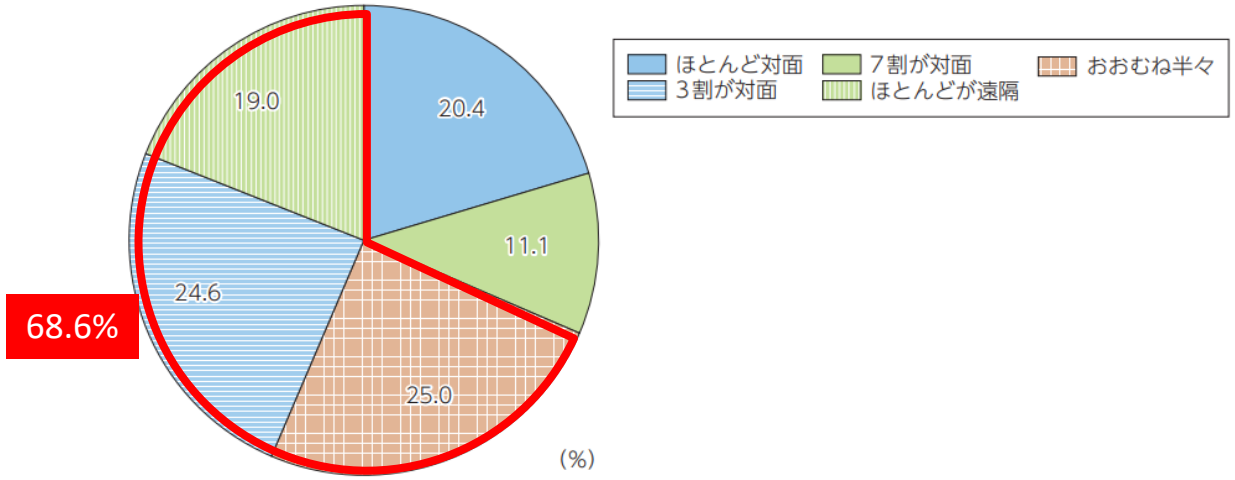


図2　大学等での対面・遠隔授業の併用割合[2]

情報セキュリティの面においては<u>テレワーク環境等を狙った被害が発生</u>[3][4]

[1]:総務省 令和3年 通信利用動向調査　[2]:総務省 令和3年版 情報通信白書
[3]: IPA テレワークを行う際のセキュリティ上の注意事項　[4]: 警察庁 令和2年におけるサイバー犯罪をめぐる脅威の情勢等について

情報セキュリティインシデントへの対策

基本的なセキュリティ対策の重要性

・常に最新のセキュリティアップデートを適用する。
・パスワードとして第三者に推測されにくい複雑なものを設定する。

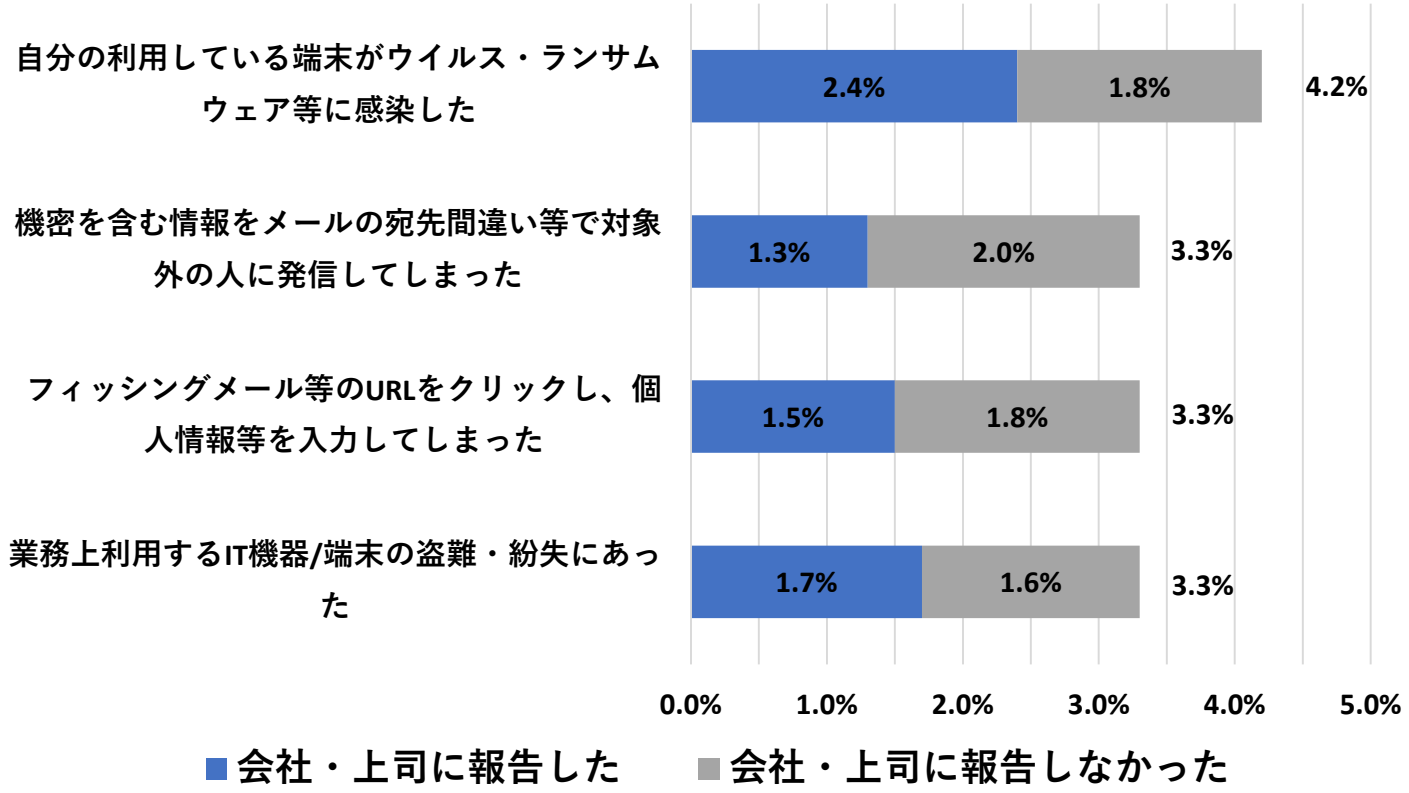
＋

情報セキュリティに関する情報共有体制の強化[5]

適切な仲介者を通じた情報共有：不足情報の補完[6]
→二次被害抑止に効果的

[5]:総務省, 我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]
[6]：JPCERT/CC サイバー攻撃被害情報の共有と公表のあり方について

情報共有の実情[7][8]



中小企業におけるインシデント遭遇後の報告について([7]を基に作成)

情報処理推進機構(IPA)が
中小企業の従業員に実施した調査
回答数:1000人
期間:3年間(2018年10月～2021年9月)

⇒情報セキュリティインシデントに遭遇した際、約半数の人が会社や上司に報告していない。

情報共有がうまく行われていない

[7]:IPA サイバーセキュリティお助け隊【レポート】中小企業従業員アンケート
[8]: 警察庁 不正アクセス行為対策等の実態調査・アクセス制御機能に関する技術の研究開発の状況等に関する調査

大学における情報共有の重要性

大学生のICT端末の利用方法

自身の保有する端末を様々なネットワークに接続し、さらに、学内ネットワークにも接続している。→二次被害拡大の可能性

二次被害抑止には、仲介組織を通じた被害情報の速やかな共有が重要である。

学生の二次被害抑止には、大学を仲介した情報共有が重要である。→学生を対象とした調査されていない

背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

目的

- 大学生(本研究ではR2学位Pの学生)を対象とした
  情報セキュリティインシデントの報告に関する実態調査

- 実態調査を基に学生報告の背景要因を分析し、二次被害の抑止に向け、学生から大学への速やかな報告が促進されるよう提言

背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

大学側がインシデントを認識する必要性

大学を仲介した情報共有
→大学側が学生に発生しているインシデントを認識する必要がある

自組織内で認識する方法[9]

- ファイアウォール等のセキュリティ機器により、脅威のある通信を検知することにより認識する方法。

報告で認識する方法[9]

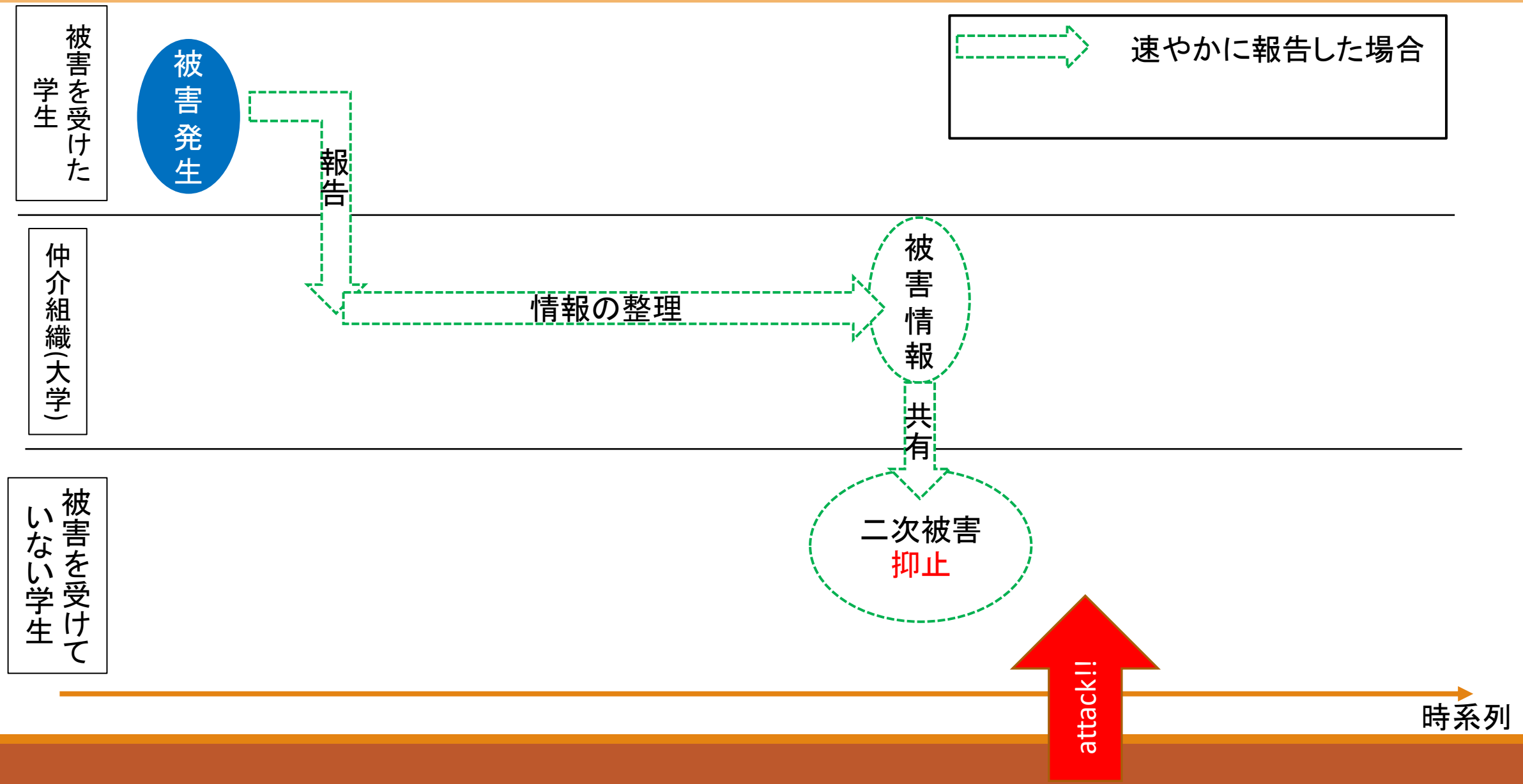
- 被害者本人や外部の第三者からの報告によって認識する方法。

大学の目の届かないところでインシデント遭遇

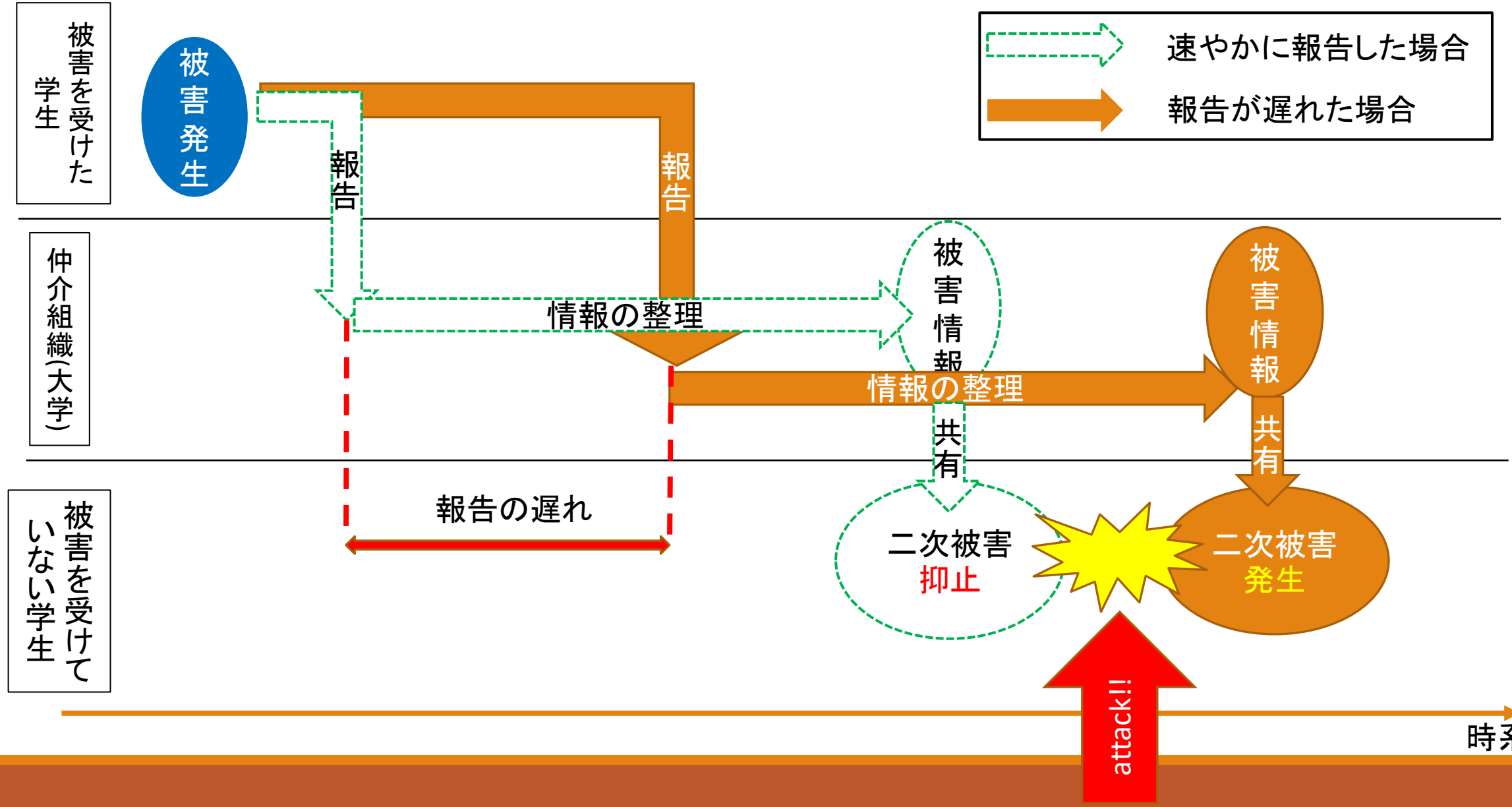
→本人からの報告が重要

[9]: JPCERT インシデントハンドリングマニュアル

大学を仲介した速やかな情報共有の重要性



大学を仲介した速やかな情報共有の重要性



背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

アンケート調査

学生から大学への報告の実態を
把握するため、アンケート調査を実施

・対象：筑波大学リスク・レジリエンス
工学学位プログラムの学生
・調査方法：アンケート調査
(Microsoft Formsを使用)
・回答数：29名

項目	質問内容
インシデントの遭遇状況について	・被害/トラブルに遭遇したことがあるか ・どのような被害/トラブルに遭遇したか
学生から大学への報告の実態について	・報告を行ったか ・どのようなタイミングで報告したか ・どこに報告したか ・報告を行わなかった理由は何か
通報窓口の認知度について	・筑波大学の通報窓口を知っていたか
報告に対する学生の意識について	・今後もし被害やトラブルに遭った場合、通報窓口に報告するか ・報告を行わない理由は何か

アンケートで示した被害・トラブルの選択肢[10]

種類	選択肢
被害	・スマホ決済、クレジットカード決済の不正利用（決済サービスの不正利用） ・偽警告やメール等を使った脅迫・詐欺による金銭要求に応じてしまった（金銭要求に応じてしまった） ・フリーソフト等を実行してしまい、デバイスがマルウェアに感染してしまった（マルウェア感染） ・WEBサーバーの設定ミスなどにより、サイバー攻撃を受けてしまった（サイバー攻撃） ・その他（自由記述）
トラブル	・実在する企業などを騙った偽ウェブサイト等に個人情報を入力してしまった（フィッシング） ・脅迫や架空請求によって金銭を要求する偽警告やメールの内容を鵜呑みにしてしまった（脅迫メールや偽警告の内容を鵜呑みにした） ・メールに不審な添付ファイルがあり、それを開封してしまった（不審なファイルの開封） ・不審なアプリ等を、提供元情報などをよく確認せずにダウンロードしてしまった（不審なアプリダウンロード） ・その他（自由記述）

出典[10]：情報処理推進機構IPA, 情報セキュリティ10大脅威2022

背景

目的

”報告”の重要性

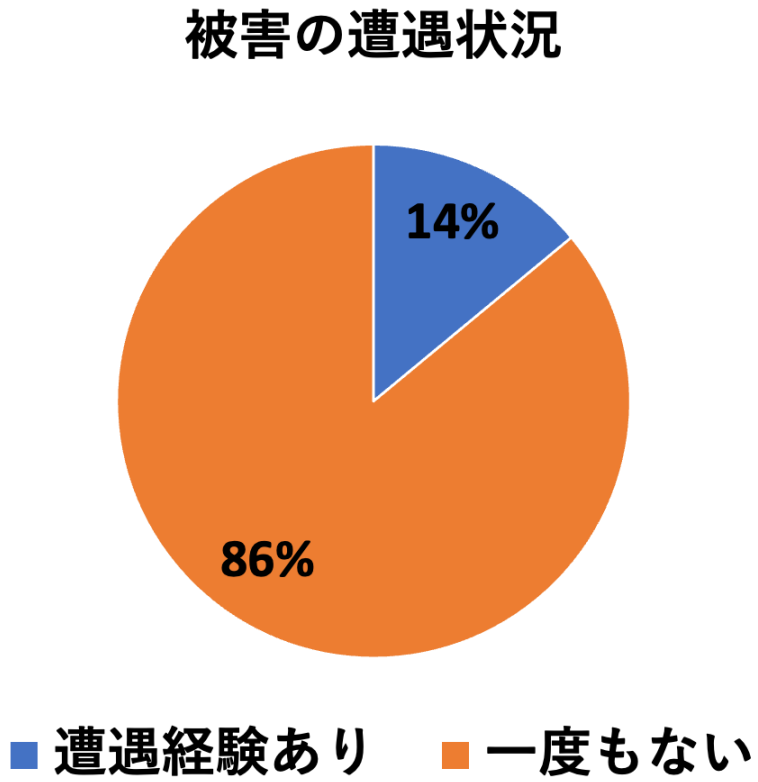
手法

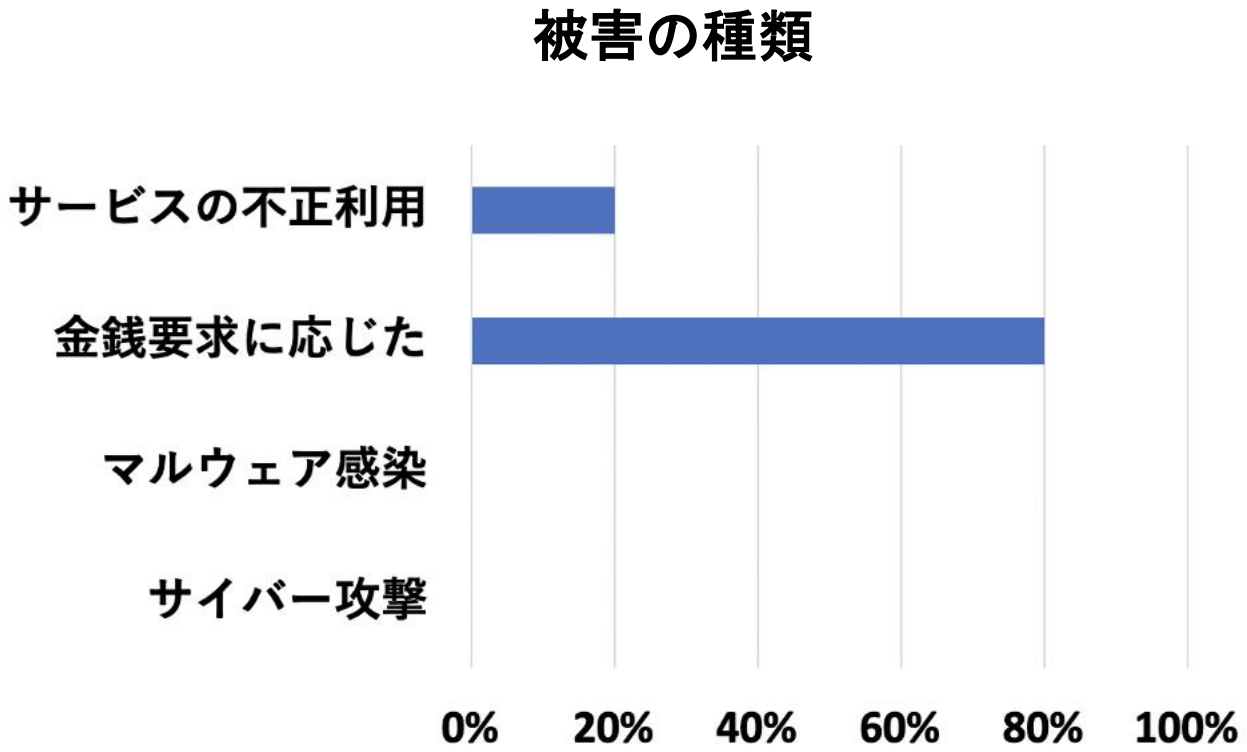
結果・考察

提言

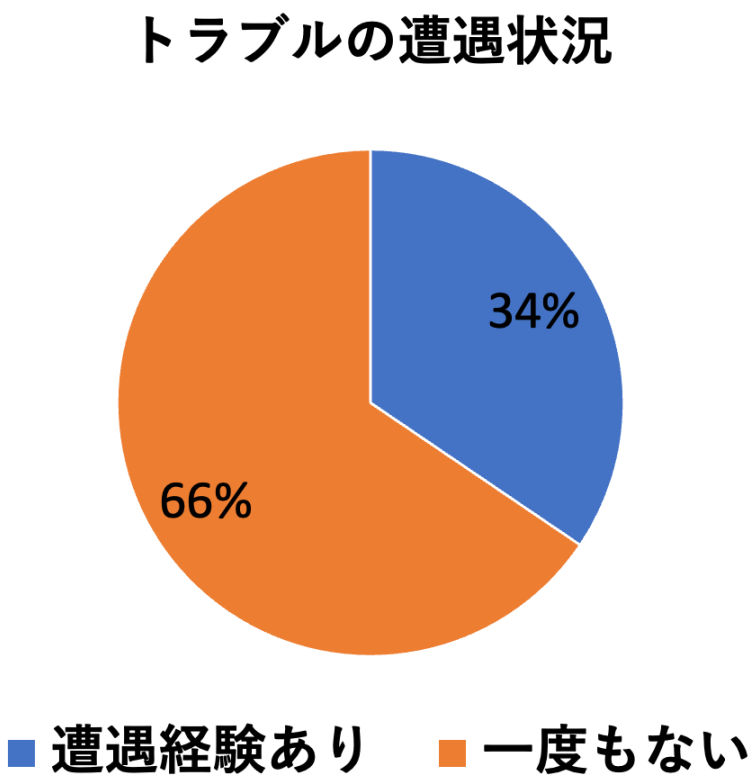
今後の課題

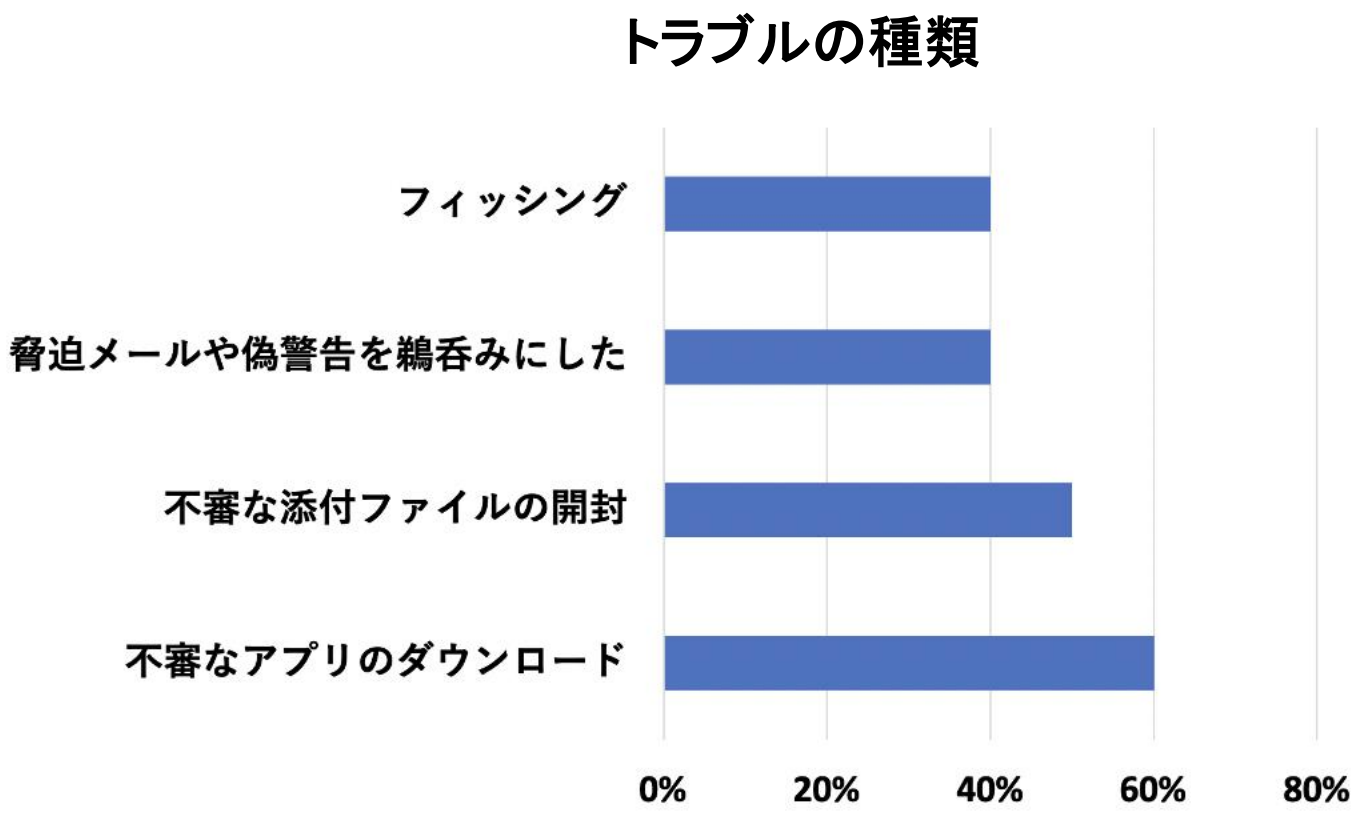
被害の遭遇状況


被害の遭遇状況
14%
86%
遭遇経験あり
一度もない

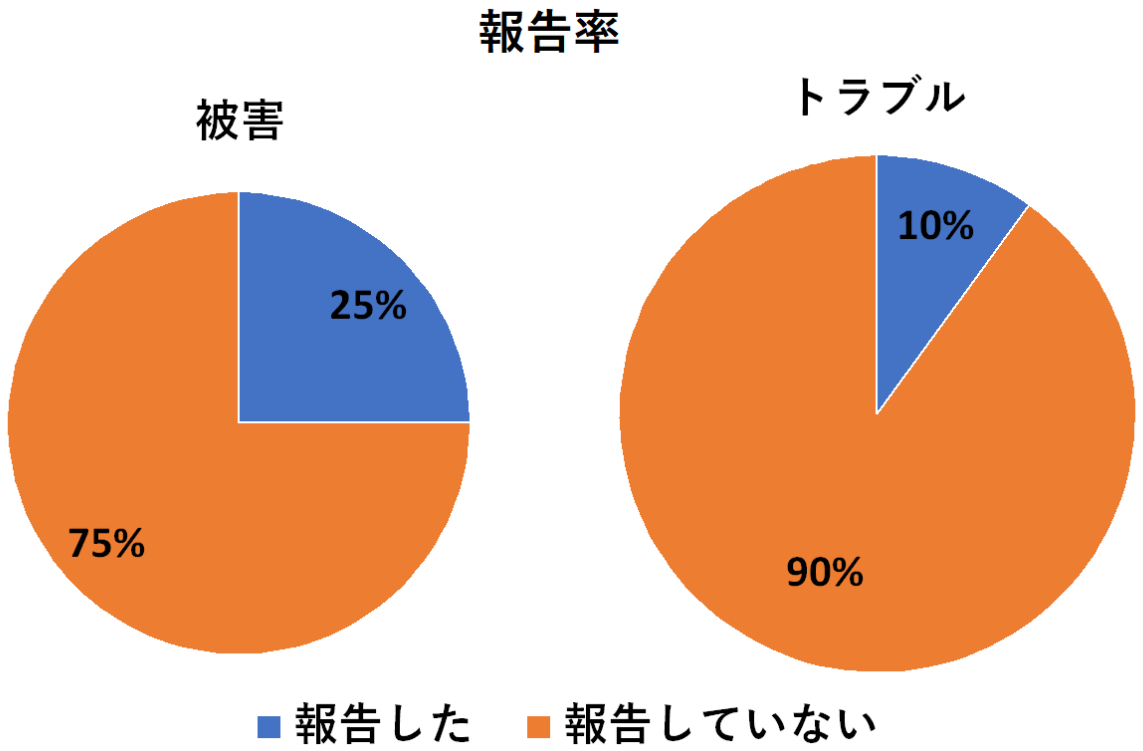

被害の種類
サービスの不正利用
金銭要求に応じた
マルウェア感染
サイバー攻撃
0%
20%
40%
60%
80%
100%

トラブルの遭遇状況


トラブルの遭遇状況
34%
66%
遭遇経験あり
一度もない


トラブルの種類
フィッシング
脅迫メールや偽警告を鵜呑みにした
不審な添付ファイルの開封
不審なアプリのダウンロード
0%
20%
40%
60%
80%

被害やトラブルに遭遇した際の報告の実態



被害やトラブルに遭遇した際の報告率が少ない

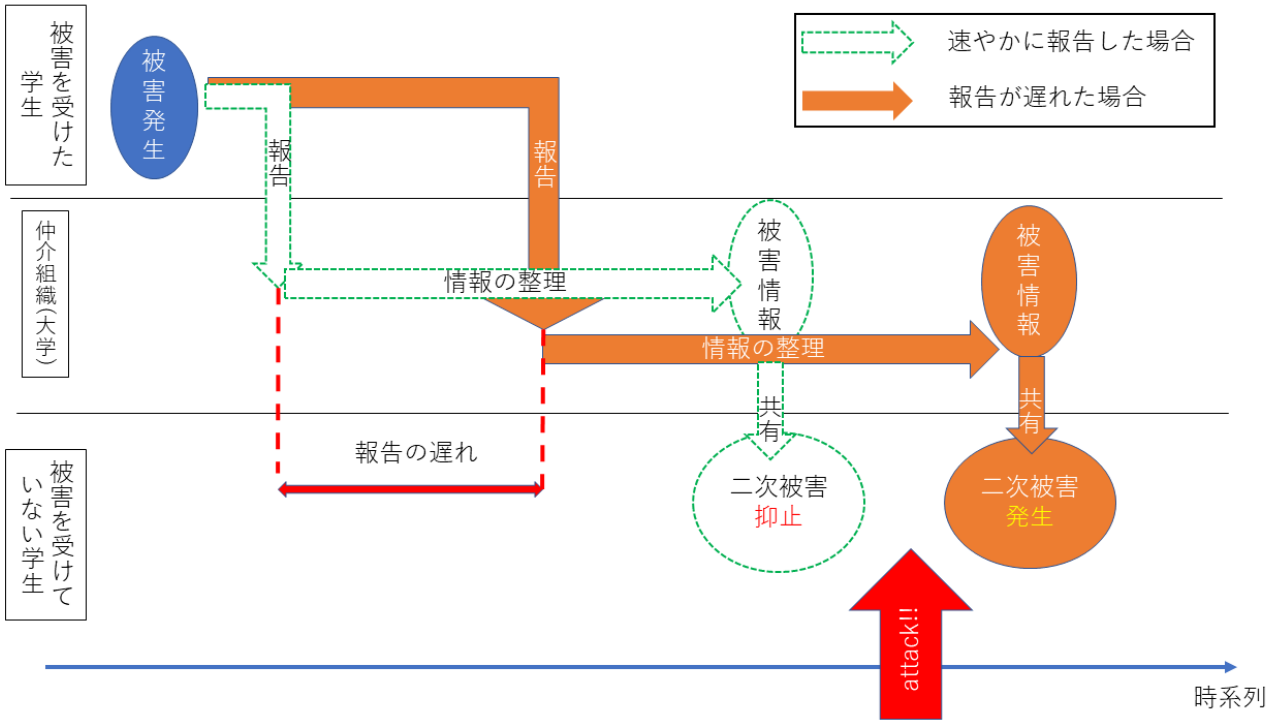
【報告に関する調査】
・報告先
→警察
・報告のタイミング
→自身で対応を試みてから

現状の報告に関する問題点

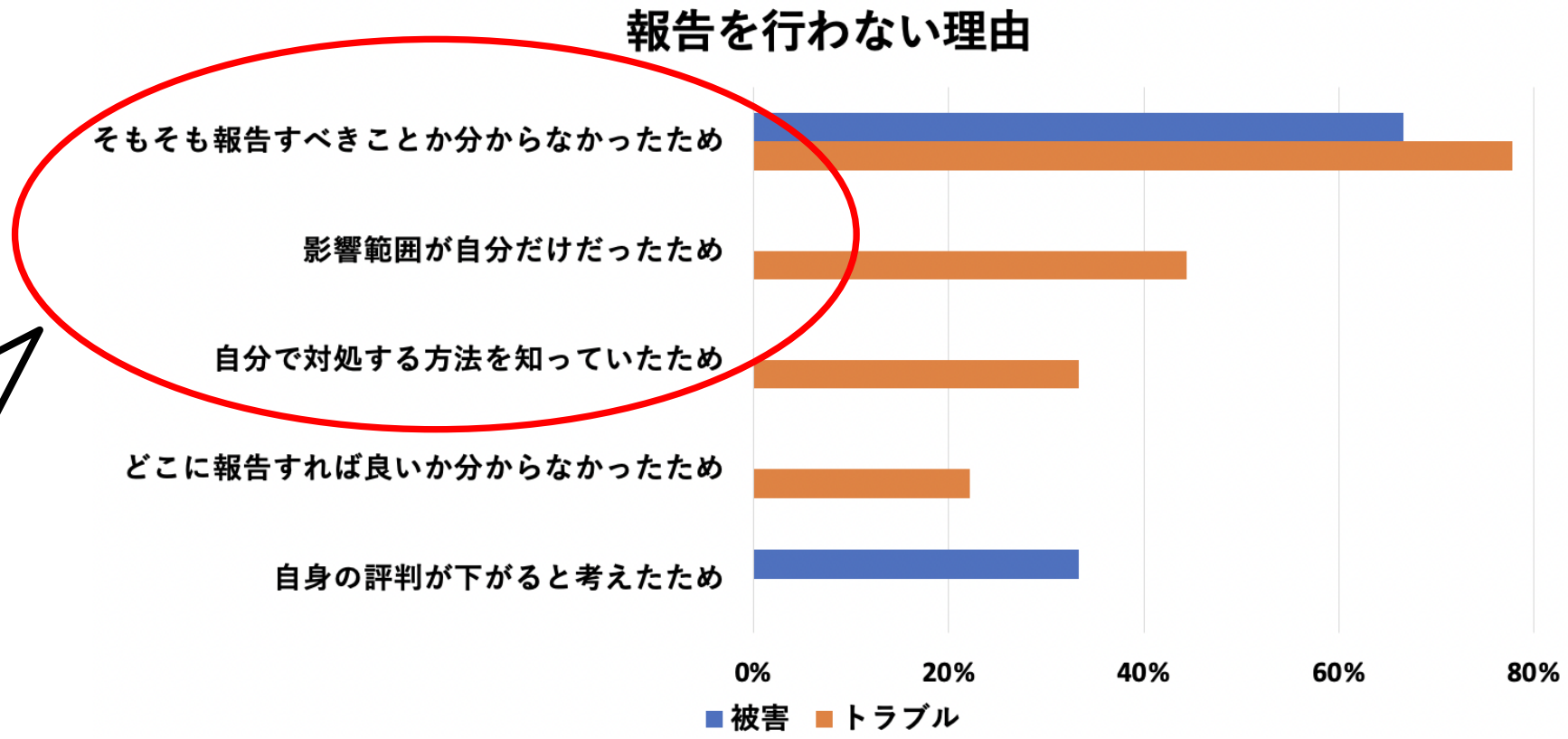
【現状の問題点】
・大学に対して報告が行われていない
・報告のタイミングが遅い

「二次被害抑止に効果的な情報共有のための報告」が行われていない

学生から大学への速やかな報告を促進する必要がある

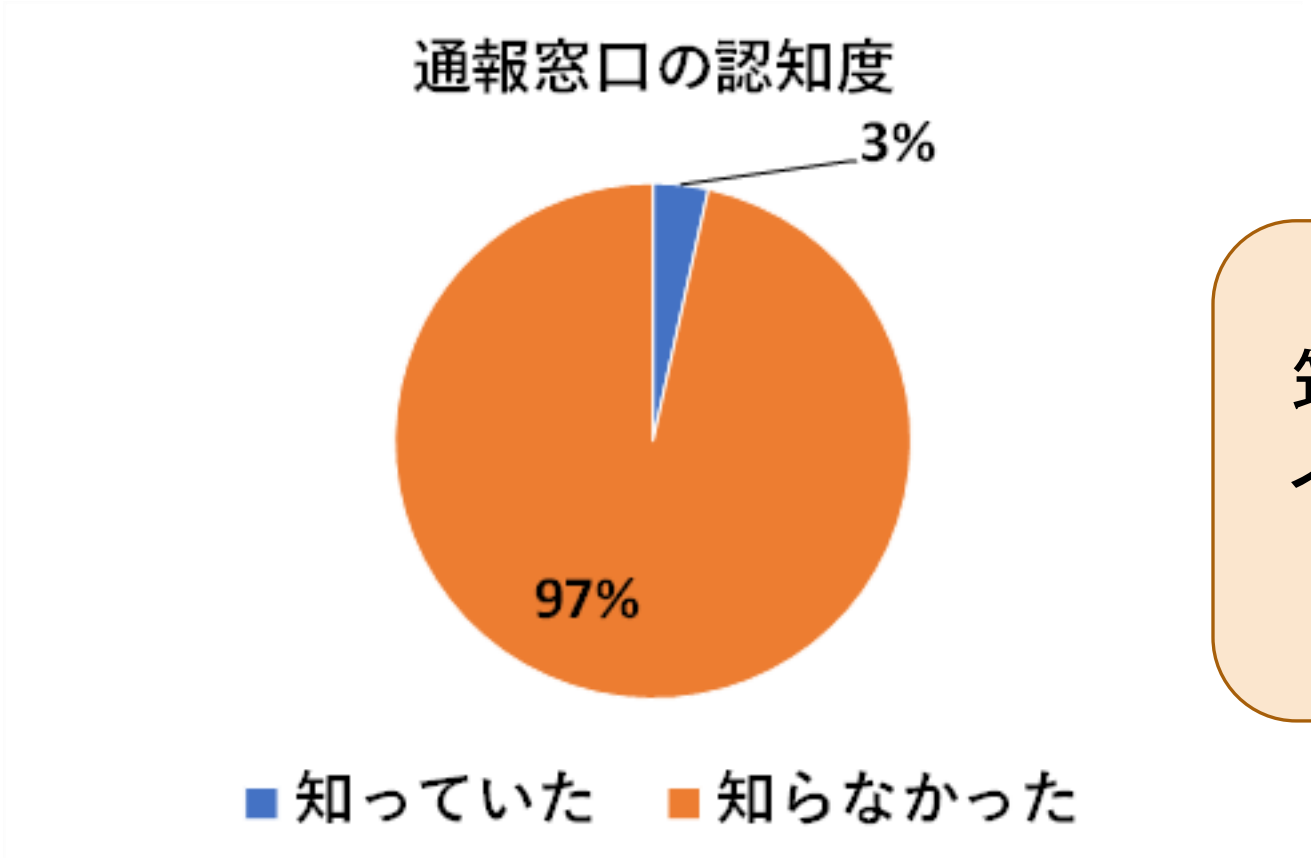


報告を行わない要因



「他の学生への
二次被害抑止の
ために報告を行う」と
いう報告の意義が
伝わっていない

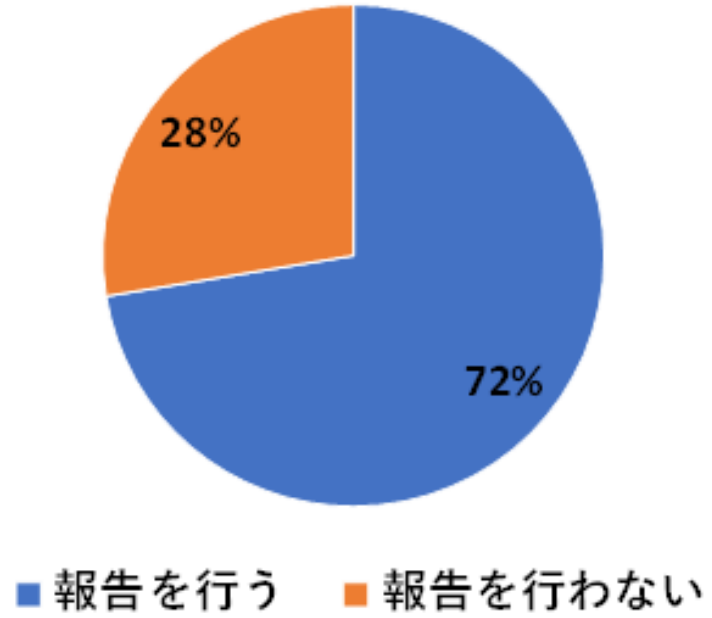
通報窓口の認知度



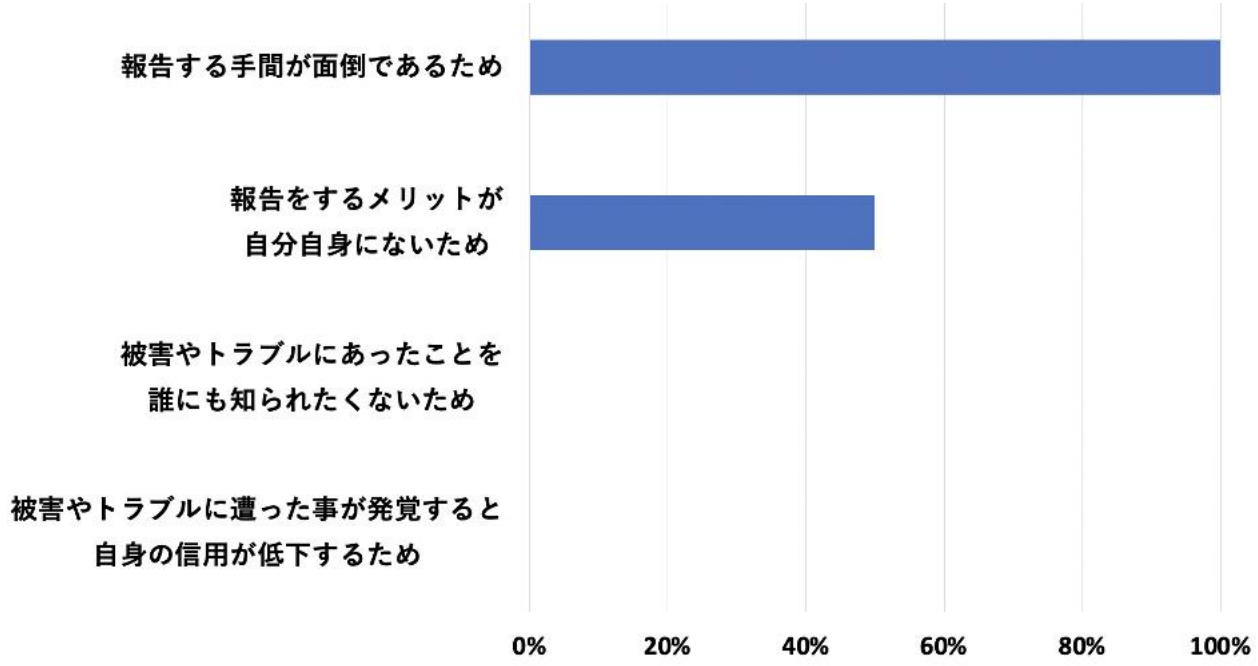
筑波大学の情報セキュリティインシデント通報窓口の存在がほとんど知られていない

通報窓口の周知による意識の変化

通報窓口を知った後での報告に対する意識の変化



通報窓口を知ったうえで報告を行わない理由



通報窓口の存在を周知することで報告率上昇が見込める

報告の意義について周知していく必要がある

背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

学生報告の促進へ向けた提言

① 学生報告の意義について周知する

・被害情報の速やかな共有を通じ、二次被害の抑止が期待できる

→情報共有の起点となる速やかな学生からの報告が重要

② 通報窓口の存在について周知する

・学内に設置された通報窓口はほとんど知られていない

→しかし、通報窓口の存在を知ることがきっかけとなり、今後の報告数の上昇が見込める

背景

目的

”報告”の重要性

手法

結果・考察

提言

今後の課題

今後の課題

・アンケート調査の対象範囲を広げる

→筑波大学全体を対象とする

・報告のタイミングについて定量的に評価

→具体的にどれほど時間がかかっているのか、それにより二次被害にどのような影響を及ぼしているか

・提案した提言について検証

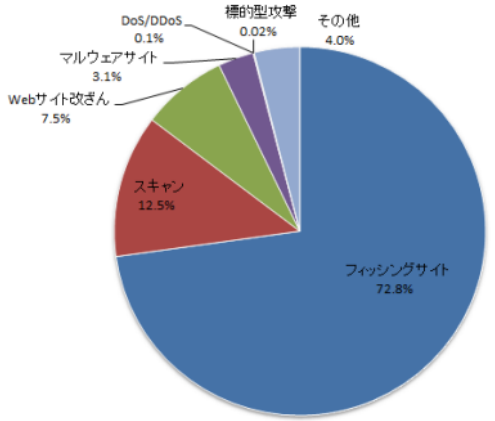
→提言により、実際に学生報告の促進、二次被害の抑止に結びついたのかを検証

今後の課題

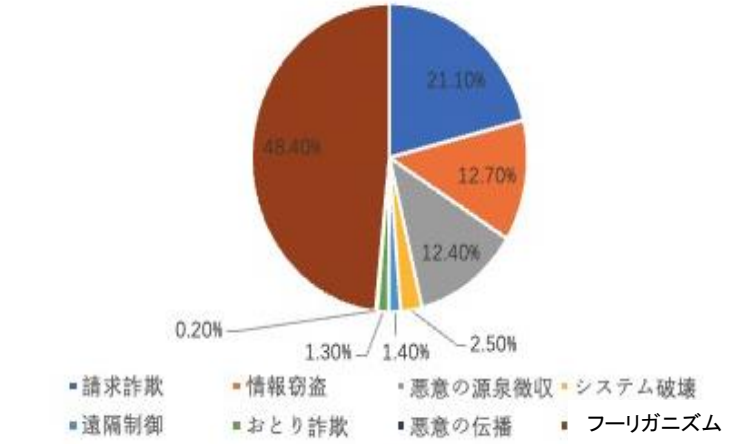
・情報共有による留学生への効果の検討

中国における情報セキュリティインシデントの内訳は日本とは異なる

→留学生が馴染みの無いインシデントによる被害に遭わないためには、被害情報の共有がより重要であると考えられる



2021年度の日本における情報セキュリティインシデントの種類
(JPCERT インシデント報告対応レポートより)



2020年の中国における情報セキュリティインシデントの種類[15]

[15]: 中国インターネット緊急事態センター2021年度安全報告書

参考文献

[1] 総務省 令和3年 通信利用動向調査, 2022/5/27 https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf (閲覧日:2022/11/15)
[2] 総務省 令和3年版 情報通信白書, 2021年7月 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/index.html (閲覧日:2022/11/15)
[3] IPA, テレワークを行う際のセキュリティ上の注意事項, 2021/7/20 https://www.ipa.go.jp/security/announce/telework.html (閲覧日:2022/11/15)
[4]警察庁サイバー犯罪対策プロジェクト, 令和2年におけるサイバー犯罪をめぐる脅威の情勢等について, 2020/3/4 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf (閲覧日:2022/11/15)
[5] 総務省, 我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言], 2020/1/28 https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html (閲覧日:2022/11/15)
[6] JPCERT サイバー攻撃被害情報の共有と公表のあり方について, 2021年3月 https://www.soumu.go.jp/main_content/000762951.pdf (閲覧日:2022/11/15)
[7] IPA, サイバーセキュリティお助け隊【レポート】中小企業従業員レポート, 2021/12/8 https://www.ipa.go.jp/security/otasuketai-pr/assets/pdf/enq20211208.pdf (閲覧日:2022/11/15)
[8] 警察庁, 不正アクセス行為対策等の実態調査・アクセス制御機能に関する技術の研究開発の状況等に関する調査, 2021年12月 https://www.npa.go.jp/cyber/research/r3/R3countermeasures.pdf (閲覧日:2022/11/15)
[9] JPCERT, インシデントハンドリングマニュアル, 2021/11/30 https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf (閲覧日:2022/11/15)
[10] IPA, 情報セキュリティ 10大脅威2022, 2022年3月 https://www.ipa.go.jp/files/000096258.pdf (閲覧日:2022/11/15)
[11] 日本学生支援機構, 2020(令和2)年度 外国人留学生在籍状況調査結果, 2021年3月, https://www.studyinjapan.go.jp/ja/_mt/2021/04/date2020z.pdf (閲覧日:2022/11/15)
[12] CACメールセキュリティデータセンター http://www.cac.gov.cn/index.htm (閲覧日:2022/11/15)
[13] プライバシーの漏洩とサイバー暴力の拡散を取り締まる告知, 2021/10/8 https://zhuanlan.zhihu.com/p/418917677 (閲覧日:2022/11/15)
[14] CON-19感染症が引き起こした10大ネットワークセキュリティ変革(在宅勤務情報の流出), 2020/7/14 https://zhuanlan.zhihu.com/p/159388282 (閲覧日:2022/11/15)
[15] 中国インターネット緊急事態センター 2020年度安全報告書, 2021年6月, https://www.cert.org.cn/publish/main/upload/File/2020%20Annual%20Report.pdf (閲覧日:2022/11/15)