情報セキュリティに関するリスク行動を実施した従業員による報告を促進・阻害する要因の研究

A study of Factors that Promote and Discourage Reporting by Employees of Risk Actions Related to Information security

松本 侑大・法制・倫理分科会・情報セキュリティ大学院大学

The purpose of this study was to determine the psychological factors that influence employees' reporting of their risk behaviors that threaten the information security of their organizations. For this purpose, a hypothetical model was developed by extracting psychological factors of risk behavior reporting based on previous studies in the information security and medical fields. In addition, to verify the hypothetical model, a questionnaire survey was conducted among employees who reported risk behaviors in a targeted attack email training. As a result, the following factors were extracted as influencing employees' intention to report information security risk behaviors: perceived urgency, perceived organizational support, role awareness, trust in the reporting system and perceived vulnerability. Among employees who reported, the higher the perceived urgency, awareness of organizational support and role awareness, the higher the intention to report their risk behavior. On the other hand, these factors were shown to increase this intention less for employees who did not report. For these employees, an increase in perceived vulnerability and trust in the reporting system was shown to encourage them to report their risk behaviors.

1. 研究の背景

- 不審メールの本文URLをクリックしてしまったなどの，従業員による情報セキュリティに関するリスク行動は，情報漏えいやシステム停止などの深刻な事態を引き起こす可能性がある．一方，迅速な報告があれば，被害の極小化が可能となる
- しかしながら，リスク行動を実施した従業員は自ら報告しにくい．また，リスク行動報告を促進・阻害する要因が十分に解明されていない

情報セキュリティに関するリスク行動の一例
- 不審メールの本文URLをクリック，USBメモリの紛失　など

2. 本研究の目的

- 従業員が「情報セキュリティを脅かすリスク行動を実施」した際の，組織や上司への報告行動に影響を与える要因を明らかにする

3. 心理的要因の選定

- リスク行動報告の分野で先行している医療分野の先行研究をもとに，情報セキュリティに関するリスク行動の7つの心理的要因を抽出
- その後，医療分野の報告と情報セキュリティに関するリスク行動報告の違いを確認し，3つの要因を追加

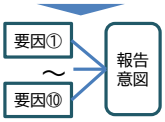
	心理的要因	要因の説明
①	有用性に関する認識	報告が，自分や組織にとってどのような利点があるのか，問題解決にどのように役立つかの認識
②	主観的規範	上司，情報セキュリティ部門などが，自分が報告することを期待している，報告することを当然と考えているとの認識
③	役割意識	報告することが，自分の役割や責任であるとの認識
④	重大性認知	情報セキュリティに関するリスク行動が，組織にとって重大な影響を与える可能性の認知
⑤	脆弱性認知	自分や組織が，情報セキュリティ上のリスクに晒されていることの認知
⑥	緊急性認知	情報セキュリティに関するリスク行動実施時に，迅速に対応する必要があることの認知
⑦	組織支援に関する認識	報告に対し，経営層や上司などが適切な支援をしてくれると認識していること
⑧	心理的安全性	報告することで，罰せられたり，不利益を被ったりしないと感じる安心感や率直に意見や問題点を報告できる雰囲気
⑨	報告手続きのわかりやすさ	報告の手順や方法が明確で，どのように報告すれば良いのかがわかりやすく，容易に報告できること
⑩	報告制度への信頼	情報セキュリティ部門を含め，組織全体の報告制度が適切に機能しており，情報が適切に処理されるという信頼感

：個人的要因　：組織的要因　：報告システムの要因

4.アンケート調査

- アンケートで協力を得られた組織内で標的型攻撃メール訓練を実施
- 訓練メール本文中のURLをクリックした従業員（報告した人／しなかった人）を抽出

- 10の心理的要因毎に，2問ずつ，10段階（1. 全くそう思わない～10. とてもそう思う）で質問．
- 金融グループ7社553名（報告した従業員：414名，報告しなかった従業員：139名）の従業員から回答取得



- 心理的要因を独立変数，報告意図を従属変数として，ロジスティック回帰分析を行い，心理的要因を検証

5. アンケート調査結果と考察

- ロジスティック回帰分析の結果，5つの要因を抽出

＜オッズ比の見方＞

オッズ比が1を宇上回る ➡ 「報告しなかった人」に比べ，「報告した人」が，その要因を高めると報告意図が高まる可能性を示唆

オッズ比が1を下回る ➡ 「報告した人」に比べ，「報告しなかった人」が，その要因を高めると報告意図が高まる可能性を示唆

表　情報セキュリティに関するリスク行動報告の要因分析結果
（報告した従業員の立場からみた結果）

独立変数	オッズ比	有意確率
有用性に関する認識	0.89	0.16
主観的規範	1.16	0.12
役割意識	**1.28**	$P<.005$
重大性認知	1.00	0.99
脆弱性認知	**0.50**	$P<.005$
緊急性認知	**1.91**	$P<.005$
組織支援に関する認識	**1.29**	$P<.005$
心理的安全性	0.98	0.78
報告手続のわかりやすさ	0.84	0.07
報告制度への信頼	**0.78**	$P<.005$

本分析では，報告有に「1」，報告無に「0」を設定
緑字：「報告した人」の促進要因　青字：「報告しなかった人」の促進要因

結果

＜緊急性認知（オッズ比1.91, p<.005）＞

報告した人 ➡ 緊急性認知が高まれば，報告意図は高まる

※組織支援に関する認識，役割意識も同様に高まる

＜脆弱性認知（オッズ比0.50, p<.005）＞

報告しなかった人 ➡ 脆弱性認知が高まれば，報告意図は高まる

＜報告制度への信頼（オッズ比0.78, p<.005）＞

報告しなかった人 ➡ 報告制度への信頼が高まれば，報告意図は高まる

報告した人/しなかった人で報告行動を促すアプローチは異なる．
報告しなかった人への対応が特に重要であり，その観点で考察

考察

- 報告しなかった従業員は，そもそもシステムの脆弱性や，自分の所属する組織に対する脆弱性について，確りと認識できていない
  ⇒「脆弱性認知に重点を置いた教育」をすることが効果的
- 報告しなかった従業員は，報告後に想定される情報セキュリティ部門からの要請や対応などをまだ確りとイメージできていない
  ⇒「報告制度を正しく理解してもらう取組み」が効果的

6. まとめ

- 報告しなかった従業員に対しては，脆弱性認知，報告制度への信頼が報告意図を高める要因として特定された
- 報告しなかった従業員に報告を促すうえで最も効果が高い対策は「脆弱性の認知を高めること」と示唆された