

従業員の情報セキュリティにおける 問題行動の要因を考慮した対策の研究

A Study of Information Security Measures

Considering Employees' Problem Behaviors

小林泰大・法制倫理分科会・情報セキュリティ大学院大学

背景・調査目的

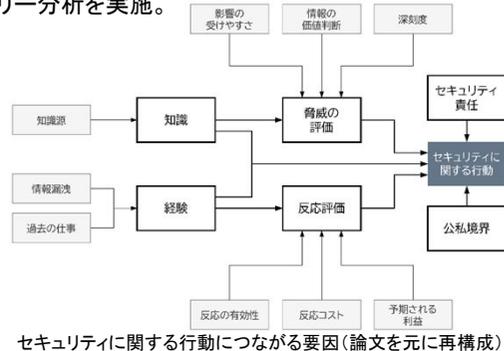
- 組織の情報セキュリティ対策には、従業員が適切に実施することでその効果を発揮するものがある
- しかし、従業員が前述の対策を適切に実施しない事例が見られる
- 対策から十分な効果を得るには、従業員による適切な実施を促す必要がある
- 従業員による適切な実施を促すため、組織が実践できる取り組みとして「従業員が実施しやすい情報セキュリティ対策を設計したり、工夫を施したりする」ことに着目した
- そのためには、従業員の行動の傾向・特徴を理解する必要があるため、まず従業員が対策を実施しない要因を調査した

先行研究1

Blythe, J. M., et. al.: Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors (2015)

目的: 従業員の態度・信念、セキュリティに関する行動への理解を通じて、職場におけるセキュリティに関する行動に影響を及ぼす要因を探る

手法: イギリスの2つの組織で働くのべ20名を対象にインタビュー。発話の一切を文字起こし、ロジックツリー分析を実施。



先行研究2

畑島隆, 坂本泰久: 情報セキュリティ不安全行動に対するテレワーク実施者の性向の分析 (2017)

目的: ルール違反を自覚しながら、業務上の利益を狙う行動のうち悪意(破壊行為)を意図しない情報漏洩行動の要因を探る

手法: 行動理論の先行研究に基づく測定尺度・質問紙を設計。質問紙調査を実施し、被験者を情報漏洩経験の有無で二分して、回答の傾向差を統計的に検定。

結果: 情報漏洩経験のある従業員群は、取っていない群と比べて

- リスクテイキング行動傾向の強さが高値
- 職場の危険度に関する認識(情報の持ち出しやすさ)スコアが高値

先行研究3

岡野裕樹, 奥山浩伸: セキュリティルール違反行動の抑止に関する一考察 (2017)

目的: 従業員が「職場からの許可のない情報持出行動」を取るときの周囲の状況や当事者の心理を明らかにする。

手法: 予備調査から測定尺度と質問紙を設計。質問紙調査を実施し、被験者を持出経験の有無で二分して、回答傾向を統計的に検定。

結果: 持出経験ありの群に見られた要因のうち、状況的要因は「本人が、時間的プレッシャーを抱えている」「本人が、職場に死角が存在することを認識している」。本人の心理的要因は「自らの違反行動が露見する、違反行動のために罰を受けるとの認識に乏しい」。

今後の予定

- 従業員が実施しやすい情報セキュリティ対策を設計したり、工夫を施したりするためには、このほかに現在組織が実施している対策について調査する必要がある
- 事故報告書や報道から、組織が事故に遭遇する前の状況を調査し、組織のセキュリティ対策の実態、立案プロセス、対策自体の問題点を調査・分析予定