ナッジを用いた通知によるセキュリティ対策促進手法に関する研究

1240297　岡崎 香織　【 コミュニケーション&コラボレーション研究室 】

1　はじめに

近年増加し続けるセキュリティインシデントに対処するためには，単なるシステム中心のアプローチだけでなく，人的要因にも焦点を当てる必要がある．本研究では，人間の行動や意識を変えるために，行動経済学の手法であるナッジに焦点を当て，セキュリティ対策への有効性を明らかにすることを目指す．そこで，パスワードの脆弱性がセキュリティインシデントの要因の１つであると考え，ユーザに対して脆弱なパスワードからの変更をより促進する通知手法の調査を行う．

2　ナッジを用いた通知手法

セキュリティ対策を促進するために，行動経済学のナッジを通知手法に導入する．ナッジは行動をそっと促す手法であり，これによりユーザが受ける不快感や強制感の軽減を目指す．本研究では，MINDSPACE フレームワーク [1] から選択した３つのナッジを利用している．Messengers 方式では重要な人物の影響を受け，Incentives 方式では行動に伴う得失を強調し，Norms 方式では他の人の行動に影響される要因を重視している．

3　通知から受ける印象調査

本研究では，ナッジによる通知の有効性を明らかにするために，異なるナッジを用いた３種類の通知方式に従来方式を加えた４つの条件を比較し調査を行う．調査には，大学生 27 名と大学院生７名の計 34 名が参加した．参加者には各通知方式を受けてパスワード変更の必要性を感じたか，また不快感や強制感をどの程度感じたかなどを５段階評価で，全く感じないを１，とても感じたを５として回答してもらう．同時に，評価した理由について自由記述形式の質問も行った．

通知において，ユーザにパスワードの変更を強要することで，脆弱なパスワードの設定を増加させる可能性がある [2]．今回の研究では，強制感の低さが脆弱なパスワードの設定の抑制に役立つと考える．

4　調査結果

４条件を比較した結果,「変更すべきと感じたか」および「実際に変更すると思うか」というアンケート項目において，従来方式と他３条件の比較で有意な差が見られた（$p<0.05$）．特に，表１に示すように，Incentives 方式が最も高い平均値を示し，5 段階評価で 4 や 5 を回答した参加者が最も多かったことが明らかになった．

一方で,「不快感を感じたか」と「強制感を感じたか」の項目では有意な差は見られなかった．表２に示すように，どちらの質問項目でも Norms 方式が最も高い平均値を示し，従来方式が最も低い平均値を示した．この結果から，従来方式においては不快感や強制感を感じる参加者が相対的に少ないことが明らかになった．

表 1　「パスワードを変更すべきと感じたか」の平均値 (標準偏差)

従来	Messengers	Incentives	Norms
2.32(1.4)	3.38(1.3)	3.97(1.1)	3.59(1.3)

表 2　「不快感を感じたか」「強制感を感じたか」の平均値 (標準偏差)

	従来	Messengers	Incentives	Norms
不快感	2.32(1.3)	2.38(1.1)	2.41(1.3)	2.68(1.4)
強制感	2.18(1.4)	2.56(1.4)	2.59(1.3)	2.91(1.4)

5　考察

結果から，今回提案したナッジを用いた３条件は，パスワード変更の促進において従来方式よりも効果があると考えられる．特に Incentives 方式は，表１と表２の結果を合わせて考えると，提案方式の中で不快感と強制感が中程度にとどまりつつも，変更促進の効果が最も高いことが明らかになった．これらの結果から，パスワード変更の促進において最も効果的な方法は Incentives 方式であると考えられる．

6　まとめ

本研究では，ナッジを用いてセキュリティ対策を促進する方式を提案し，パスワードの脆弱性に焦点を当て，変更を促進する通知手法について調査を行った．従来方式と３つのナッジ方式の比較を行った結果から，不快感や強制感を抑えつつ，効果的な手法として，特に Incentives 方式が有力であることが示された．

今後はパスワード変更だけでなく，２段階認証やシステムアップデートなどの促進に有効な方式を明らかにし，セキュリティ意識向上に貢献していくことを目指す．

参考文献

[1] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, and I. Vlaev. Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, Vol. 33, No. 1, pp. 264–277, 2012.

[2] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 173–186, 2013.