標的型攻撃メール訓練の現状と課題に関する調査

A Survey on Current Status and Issues of Targeted Attack Email Training

松本　侑大・ネットワーク分科会・情報セキュリティ大学院大学

1. 研究背景

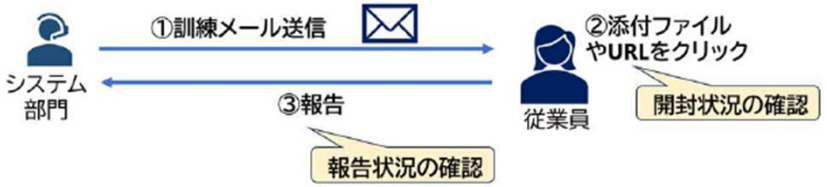
- 組織におけるサイバー攻撃被害が後を絶たない. 特に標的型メール攻撃は，多くの組織でサイバー脅威として認識されている状況（IPA他）.

標的型メール攻撃とは：
標的企業の従業員等にマルウェア付きの電子メール等を送付し社内端末を感染させ，主に重要情報を盗み取ること等を目的とした攻撃

- 標的型メール攻撃を防げない状況を踏まえると，攻撃被害の極小化のためには，被害に遭った際のシステム部門への速やかな報告が重要である.
- 組織内の標的型メール攻撃に対する耐性等を確認する手法として，標的型攻撃メール訓練がある.

2. 目　的

- 本研究では，標的型攻撃メール訓練の「報告」に関する研究を調査し，報告を阻害する要因等を明らかにすることで，報告を促す対策について提案する.



3. 先行研究

- 不審メールと認識する度に報告してくれるユーザが一定数いることや，不審メールを報告するユーザは不審メールを見分けるための一定程度の知識を有していることが明らかとなった. [Daniele等, 2022]
- 自己効力感（適切に対応できるという自信）が標的型攻撃メールの報告可能性に影響を与えることが示唆された. [Kwak等, 2020]

4. 先行研究で解決していない点

- 先行研究での「報告」は，訓練メールや不審メールを「見抜いた」ことに着目した未然防止の観点でのシステム部門への報告要因を研究しており，訓練メールや不審メールのURL をクリックした後（インシデント懸念）の報告要因に特化した研究はない.

5. 今後の研究計画

- 不審メールのURL をクリックした後（インシデント懸念）の報告に焦点を当て，研究を進めていく.
- まずは，従業員が上記報告をする要因／しない要因明らかにする（アンケート調査）.
- アンケート結果から対策を検討し，標的型攻撃メール訓練等の実験を通じて，対策の有効性を評価する.