人はなぜメールのマルウェアを実行するのか？

株式会社ラック
鈴木　悠

1. はじめに

「メールに添付されている不審なファイルやURLはむやみに開かない。」メールからのマルウェア感染等を想定し、その対策として多くの組織でルールの規定、教育・訓練、注意喚起が行われている。しかし、それにも関わらず必ず不審な添付ファイルを開封する人がいる。

メールを用いた攻撃は、システム的対策と人的対策の双方が必要となる。しかし、人的対策に対し、人を起点とした心理的側面から検討する研究は少ない。本稿では、標的型攻撃を想定したメール訓練における現状から、その背景となる人の心理的側面について考察すると共に有効策を述べる。

2. メール訓練における現状

メールを用いた標的型攻撃に対し、教育･訓練という人へのアプローチを試みる施策にメール訓練がある。メール訓練の有効性については、短期的（2週間）および長期的（約1年）な教育効果が確認されている[1]。つまり、メール訓練を定期的に実施することにより、不審な添付ファイルやURLを開く人を減らすことが出来る。

しかし、得られる効果は一定数に留まり、完全に0人にすることは難しい。例えば、メール訓練を毎年実施しているA社では、訓練メールの添付ファイルやURLを開いた人の割合（以下、開封率とする）が15%から下がらない（図1参照）[2]。

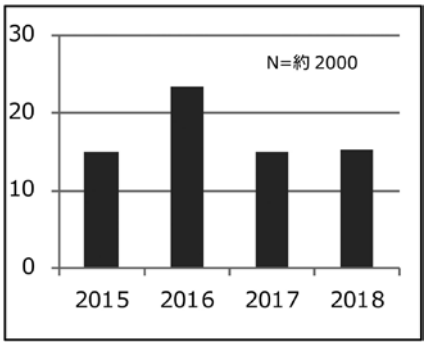

図1.　年度別開封率（%）

A社においては、前年度の開封者に対し、もう一度同じ文面の訓練メールを配信するという試みが行われている。その結果、2017年度では37.2%、2018年度では33.3%が同一文面の訓練メールにて再び添付ファイルを開封していた。このように、メール訓練において学習効果が得られない層が必ず一定数存在する。

3. 態度ー行動の関係

人間が何らかの決定に基づいて行動する背景には、物事に対する考え方や姿勢としての「態度（attitude）」がある。この態度は、先天的なものではなく、様々な経験や学習を通して後天的に形成されている[3]。

この形成された人の態度を外的な力により変化させることを「態度変容」という。人の態度が変容するステップをモデル化したものに「連合命題評価モデル（APEモデル）」がある（図2参照）[4]。

外部の影響からこれまでの経験による推測が活性

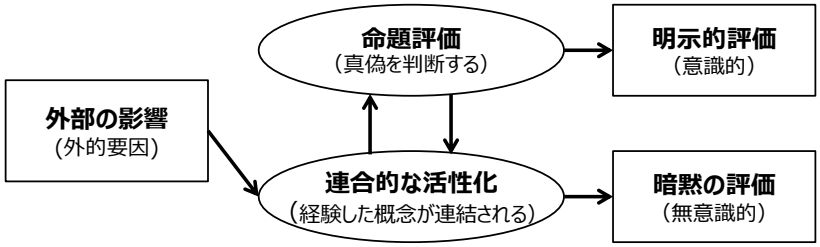

図2.　連合命題評価モデル

化し、その演繹的推論から真偽判断を行い行動するというものである。受信したメールに対し、メールの差出元や本文内容等の情報から推測し、正規か否かを判断し、開封または削除といった行動を行う。

この態度変容を促進するものに「学習[5]」と「説得[6]」がある。メールを利用した攻撃では、攻撃者がメール本文等の「説得」により、受信者の態度を変容させ、添付ファイルや本文内のURLを開かせようとする。これをメール訓練により「学習」することで開封させないという構図である。

学習に関しては既にメール訓練の有効性が示されているため、本稿では説得に焦点をあてる。

4. 攻撃者による説得

説得とは、コミュニケーションにより受け手の理性や感情に働きかけ、相手の自発性を尊重しながら、送り手の意図する方向に受け手の意見、態度、行動を変化させることである。相手の説得に応じれば態度及び行動が変化し、逆に応じなければ元の態度を守る。

説得は、動機付けと認知的能力で決まるとする「精緻化見込みモデル[7]」がある（表1参照）。

表1.　精緻化見込みモデル

		動機付け	
		高	低
認知的能力	高	中心的ルート	
	低		周辺的ルート

「動機付け」とは内容が妥当かどうかを吟味しようとすることであり、吟味する能力が「認知的能力」である。認知的能力は学習により高めることができるが、思考を妨害する要因がある場合には十分に発揮されない。

動機付け及び認知的能力が高い場合、受け手が説得されて開封する確率が高まる（中心的ルート）。逆に、動機付け及び認知的能力が低い場合、受け手は判断に迷い、判断材料を求める（周辺的ルート）。メールを用いた説得では、中心的ルートは本文の説得力、周辺的ルートにおいては差出元への信頼が影響するという結果がある[8]。

5. メール受信者の判断と行動

心理学では性格とリスク行動に関する研究が行われており、性格→認知的要因→リスク行動という因果構造が示唆されている[9]。セキュリティという観点においても、これまでにセキュリティ事故と性格特性を明らかにしようとする研究が行われてきた。

標的型メールの検証実験において、開封群は非開封群よりも自己効力感（課題解決能力の自己評価）が高く、被害を小さく予想するという結果がある[10]。

一方、ヒューマンエラーを起こしやすい性格には情緒不安定性・非調和性・非勤勉性があるとし、スキル向上の意識が低いため事故を起こしやすいと考察されている[11]。

このような性格傾向があることを踏まえたうえで、攻撃者の説得によるメール受信者の態度変容とその有効策を考察する。

6. 態度変容と有効策の考察

6.1. 環境的・身体的要因

図2の連合命題評価モデルでは、外部の影響に対して連合的な活性化が発生しないと無意識的な行動（暗黙の評価）に繋がる。

ヒューマンエラーの発生する環境的な要因として業務集中があり[12][13]、多忙により思考力が低下すると、受信したメールを吟味することなく反射的に開封する可能性がある。このような場合、メール訓練による学習効果は発揮されないため、労務管理も重要である。

6.2. 認知的能力

訓練メールの開封率は、メール習熟度、1日当たりのメール数、処理メール通算、メール訓練経験の有無で差がある[1]。このため、本稿では認知的能力を

メールの利用頻度が高く、メール訓練経験がある人とする。

（1）認知的能力：高

認知的能力が高い人の開封率は、論拠の質、つまりメールの巧妙さに依存する。例えば、同一文面の訓練メールであっても、差出人がフリーメールアドレスの場合は開封率が27.3%だが、自組織のドメインの場合は40.6%と開封率が高くなる [2]。標的型攻撃メールは手口が年々巧妙化しており、「不審メール」ではなくなってきている。このため、認知的能力が高い人であっても開封することも想定し、疑わしいメールを受信した際や開封時の報告は周知徹底しておきたい。また、メール訓練を実施した際には、報告受理後のインシデント対応についても訓練しておくことが有効だろう。

なお、メール訓練において、興味本位で開封する人がいる。これは、ヒューマンエラーとは異なり、意図する違反行動である。心理学では、「リスクテイキング（不安全）行動」に該当し、自己中心性と楽観視により引き起こされるとしている [14]。万が一マルウェア感染被害が発生した場合の組織及び業務への影響とその責任について言及し、違反行動に対するモニタリングを強化することが有効だろう。

（2）認知的能力：低

認知的能力が低い開封者には、これまでの先行研究から、自己に基づき判断する「自己効力感」[10]と他者に基づき判断する「信頼」[8]のいずれかが作用していると考える。

自己効力感が高い人は、自分には「知識」と「これまで感染しなかった経験」があるから大丈夫と思い込む「正常化バイアス」が強く働き、マルウェアに感染する確率とその被害を低く見積もる。

有効策として、訓練により警戒心を高めることが示されており [10]、マルウェア感染を擬似体験することも効果的とされる [15]。

6.3. 動機付け

メール訓練では、複数の文面パターンが用いられる。訓練メールのテンプレート別の開封率では、組織内通達に似た文面において開封率が高い（表2参照）[2]。また、メール訓練後のアンケートにおいても、開封理由を業務への関連性に言及する人が多い（表3参照）[2]。

表3.　訓練メール開封理由の割合（%）

開封理由	回答率
判断できなかった	28.4
業務に関連すると思った	**55.8**
不審だが念のため確認した	7.4
興味本位で開封した	5.3
誤送信と思い確認した	1.1
うっかり開封した	17.9

業務関連度と開封率における統計的な有意差は訓練対象組織によって異なり、業務関連度が高い場合だけでなく無関係である場合も開封率が高く因果関係は不明である [1]。本稿では、動機付けを業務関連度

表2.　訓練メールテンプレート別開封率上位5（%）

件名	平均	添付型	URL型
人事発令	36.7	19.3	42.5
至急：PDFに関する注意喚起	20.4	32.6	14.4
当社代表取締役社長の番組出演に関するお知らせ	18.0	5.4	22.2
【医療費通知】	17.0	17.0	16.9
事業継続計画の定期見直し	16.2	-	16.2

と仮定したうえで、業務への関連有無に関わらず開封率が高くなる理由について考察する。

（1）動機付けに影響を及ぼす要素

他者の行動へ影響を及ぼす潜在能力に「社会的勢力[16]」（表4参照）がある。この社会的勢力の影響が及ぶ背景には、情報源への信頼が関係している[17]。

人は、メールが正規か否かを判断する際、差出元やメール本文に含まれるいくつかの要素による影響を受けている。

表4.　社会的勢力

名称	内容
報酬勢力	報酬、承認、賞賛、見返り
強制勢力	不利益、懲罰、叱責
正当勢力	権威、権力による義務化
準拠勢力	魅力、同一視、追従
専門勢力	集団内の専門的知識
情報勢力	集団外の専門的知識

（2）動機付け：高

メールの受信者が、業務に関連する内容と認識した際、開封という行動に及ぼす影響力として表5のようなものが考えられる。

表5.　業務関連度が高い場合の影響力の例

影響力	内容
強制勢力	・内容を確認しないことの処罰
正当勢力	・上司や親組織からの依頼 ・管理部門からの通達
専門勢力	・システム部門からの注意喚起
情報勢力	・既知の外部組織からの回覧

このような影響力を強く受ける人または組織内環境である程、内容を確認しない事によるデメリットがマルウェア感染リスクを上回り開封する。

業務関連度が高いメールに対しては、判断がつかない場合の開封前の確認手段（電話での本人確認、第三者への確認、イレギュラー対応発生時のマニュアル等）を決め、周囲に相談しやすい環境作りをしておくことが有効だろう。

（3）動機付け：低

メールの内容が業務に関連していなくても開封する場合は、受信者が感じたメリット/デメリット（表6参照）や興味がマルウェア感染リスクを小さく見積もった場合、または思考せず反射的に開封している場合が考えられる。

表6.　業務関連度が低い場合の影響力の例

影響力	内容
報酬勢力	・金銭的報酬（還付金、返金） ・承認的報酬（取材対応依頼）
強制勢力	・支払い請求、訴訟通告 ・情報漏えいへの対処依頼

業務関連度が高い場合は客観的なデメリットによる判断であるのに対し、業務関連度が低い場合は主観的な判断が強く影響する。つまり、好奇心が強い、不安傾向が高い、物事を深く考えないといったような性格との関連があるのではないかと推測している。

心理学の古典的な性格テスト実験に、新聞の占い欄をコピーして配布し自分に当てはまるか5段階で評価をさせるというものがある。その実験結果では、平均4.26とほとんどの被験者が自分の性格に当てはまると回答している[18]。つまり、明らかに不審な点がなければ、人は業務関連度の有無に関わらず、自分宛にメールが来た時点で、どんな内容であっても「自分と結び付ける」可能性がある。このため、業務関連度ではなく、訓練メールテンプレートと開封者の性格特性との関連を検証する必要がある。

ただし、たとえメールを開封しやすい性格特性があったとしても、個人の性格や能力が有効に機能する職

種や業務もある。安易に開封者を叱咤・排除せず、セキュリティ意識を高める人的対策と制限や監視等のシステム的対策を個別に強化することにより、組織も人も守れるようになることが組織にとって有益である。

6.4. 各要因と有効策の実施による効果

メールの不審な添付ファイルやURLを開封する人について、心理的な側面から考察した要因と有効策を図3に示す。

まず、メールを受信した際には、組織が導入しているシステム的対策によってメールが選別される。入口対策としてサンドボックスやフィルタリング等により受信者への不審なメールの到達を防ぐ、出口対策としてネットワーク機器による制限や監視等によりマルウェア感染後の被害を封じ込めることで脅威を低減させる。これらのシステム的対策を標的型メールがすり抜けた場合、または予算の関係上システム的対策が導入できない場合、人的対策に頼るしかない。

攻撃者にとっては、いくつか送信したメールのうち、誰かが開封すればそれで目的は達成する。このため、組織のセキュリティ意識を全体的に高めても、1人の脆弱な人がいれば組織のセキュリティホールとなり得る。1人の脆弱な人が攻撃者が遠隔操作するマルウェアに感染すれば、組織ドメインを管理するActiveDirectory等を経由して組織内の被害は拡大する可能性がある。

本稿の考察では、環境的・身体的、認知的能力、動機付けの3つの要因から開封率が高まる理由とその有効策について述べた。特に注意すべき点は、動機付け（業務関連度）に関係なく反射、興味、恐怖等で開封する人が一定数存在し、セキュリティ教育・訓練を実施してもその効果が得られにくいと考えられることである。図3に示すとおり、各要因に対する有効策は異なる。メール訓練結果から開封者の開封理由についても言及し、効果的な有効策を実施することで、セキュリティの費用対効果を高めることができるだろう。

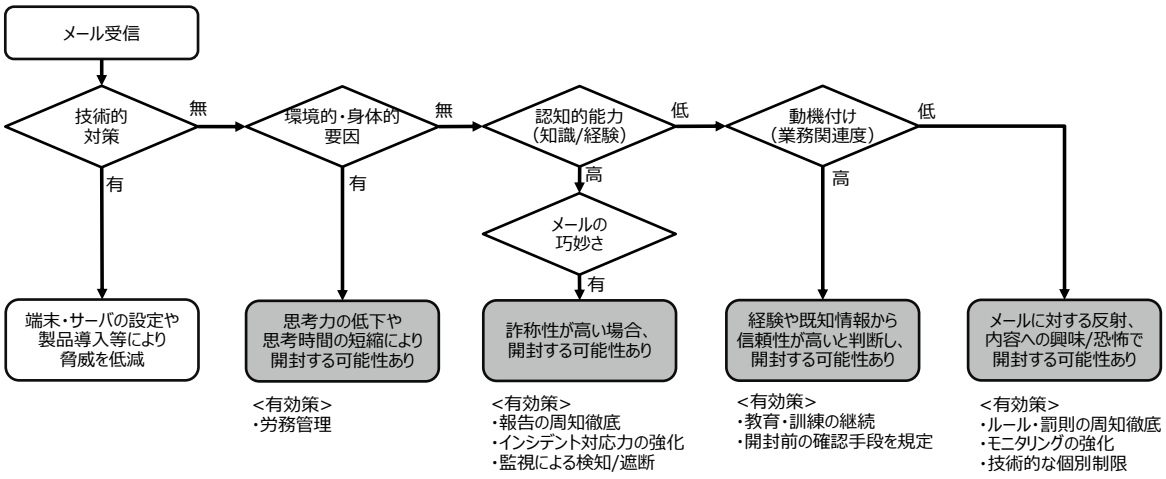

図3.　メールの不審な添付ファイルやURLを開封する過程とその有効策

参考文献

[1] 一般社団法人JPCERT コーディネーションセンター (2011年). 2009年度ITセキュリティ予防接種調査報告書. https://www.jpcert.or.jp/research/2011/inoculation20110309.pdf

[2] 株式会社ラック (2015～2018). ITセキュリティ予防接種サービス結果 (未公刊)

[3] Allport, G. W. (1935). Attitudes. Hand-book of social psychology, 798-844. Clark University Press.

[4] Gawronski, B., & Bodenhausen, G. V. (2011). The associative-propositional evaluation model: Theory, evidence, and open questions. Advances in Experimental Social Psychology, 44, 59-127.

[5] Lott, B. E., & Lott, A. J. (1968). A learning theory approach to interpersonal attitudes. Social Psychology, 67-88. Academic Press.

[6] Hovland, C. J. I., & Kelley, H. (1953). Communication and persuasion. Yale University Press.

[7] Petty, R. E., & Cacioppo, J.T. (1986). The elaboration likelihood model of persuation, Advances in Experimental Social Psychology, 19, 123-162.

[8] 小松文子・高木大資・吉開範章・松本勉 (2011). 情報セキュリティ対策を要請する説得メッセージによる態度変容の調査と実験, 情報処理学会論文誌, 52, 2526-2536.

[9] 上市秀雄・楠見孝 (1989). パーソナリティ・認知・状況要因がリスクテイキング行動に及ぼす効果. 心理学研究, 69, 81-88.

[10] 寺田剛陽・鳥居悟・安野智子・瀧澤弘和・新真知 (2013). リスク認知に基づく標的型メール対策の検討, 情報処理学会研究報告, SPT-5.

[11] 加藤岳久 (2013). 情報事故における性格とセキュリティ意識との相関に関する研究. http://jairo.nii.ac.jp/0063/00006803/en

[12] 島成佳・安 玲未・高木 大資 (2015). ITシステム運用現場のヒューマンエラーに影響を及ぼす要因分析と考察, 情報処理学会論文誌, 56, 2210-2218.

[13] 中村美香・近藤浩子・岩永喜久子・今井裕子・杉田歩美・須川美枝子・永井弥生 (2016). 看護職がインシデント・アクシデントを繰り返す要因に関する研究, 北関東メディカルジャーナル, 66, 279-288.

[14] James, R. (1990). Human Error, Cambridge University Press.

[15] 浜津翔・栗野俊一・吉開範章 (2015). 集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用, 情報処理学会論文誌, 56, 2200-2209.

[16] Raven, B. H. (1965). Social influence and power. Current studies in social psychology, 371–382.

[17] Nesler, M. S.& Aguinis, H. & Quigley, B. M.& Tedeschi, J. T. (1993). The Effect of Credibility on Perceived Power. Journal of Applied Social Psychology, 23, 1407–1425.

[18] Forer, B.R. (1949). The fallacy of personal validation: A classroom demonstration of gullibility. Journal of Abnormal and Social Psychology, 44, 118-123.