6E-4

ユーザへの予防接種というアプローチによる標的型攻撃対策－２

山口　健太郎†
†情報セキュリティ大学院大学
客員研究員
E-mail: mgs064512@iisec.ac.jp

小宮山功一朗‡
‡有限責任中間法人 JPCERT
コーディネーションセンター
E-mail: office@jpcert.or.jp

内田　勝也††
††情報セキュリティ大学院大学
情報セキュリティ研究科
E-mail: uchida@iisec.ac.jp

1．はじめに

本稿では、標的型メール攻撃に対する情報セキュリティ教育手法のひとつ**「予防接種(Inoculation)」**に注目､その有効性を実験により検証するとともに、その結果から有効な実施手法等について考察、提案するものである。

２．標的型メール攻撃

本稿で対象とする「標的型メール攻撃」は「利用者へのアプローチとして電子メールを利用するタイプ」の誘導（受動）型攻撃であり、主に、特定の受信者に対して、件名や文面をその受信者にカスタマイズしたウィルス付きの電子メールを送ることにより、そのウィルスへの感染などへ誘導するものである。最近その増加が確認されている。

３．標的型メール攻撃への対策

標的型メール攻撃への対策としては様々な方策をあわせて対応する多層防御が有効であるとされ、主に次の３つのアプローチがある。

(1)攻撃自体を防止、発生させない為の技術的対策
(2)トリガーとなる行動をユーザが起こしてしまった場合に、被害拡大を抑制するための対策
(3)受動･誘導型攻撃の対象となる利用者への教育・啓発

「予防接種」は(3)に属し、対象者の具体的な行動の変化を知ることができる点で、カークパトリック(Kirkpatrick,D,L)の教育の４つのレベル評価[1]のうちレベル３(Behavior：行動)の評価が可能であり、大人向けの教育アプローチとして効果的な、コルブ(D,Kolb)の「経験学習論」(Experiential Learning)[1]の具体的経験(Concrete Experience)にあたる重要な経験であるとも考えられる。

４．「予防接種」の方法

「予防接種」は、利用者に対して標的型メール攻撃を摸した「疑似攻撃メール」を送付して行う。疑似攻撃メールは、添付ファイル付きの電子メールで、添付ファイルには、メール自体が疑似攻撃であり無害であることや、連絡先、対策や注意点などが記載される。開封した利用者には、再教育の効果もある。今回の実験では、「予防接種」の効果確認のため異なる発信者､内容で2回メールを送付したが、実際には、１回目の接種メールで効果が発生しているとも考えられる。

５．「予防接種」実験の具体的手順と対象者

実験については次のような流れで行った。

(1)研修（年度当初 5-6 月）
(2)予防接種計画検討、立案、メール作成など準備
(3)テスト（リハーサル）（メール送信直前）
(4)第１回目メール送信（8 月 7 日）
(5)第２回目メール送信（9 月 2 日）
(6)全体の説明とアンケート依頼（9 月 15 日）
(7)結果集約と分析、まとめ

今回対象としたのは、筆者所属する横浜市で各課のパソコン、ネットワークなどの管理を行う管理責任者で、年度当初に管理責任者等としての責務と一般的なセキュリティ知識の研修を実施、標的型攻撃についても知識や対応を学習した。対象人数は **428 名**であり､部署などの偏りができないよう配慮した。

送付文案には A、B2 つの異なる内容を準備、グループは最初に内容 A を送付するグループと、内容 B を送付するグループの２つに分けた。2 回目の疑似攻撃メールは、最初に内容 A を送付したら次は内容 B というように異なる文案で送付した。

送付後約３日程度で開封は落ち着いている。

６．アンケートによる状況確認と結果

アンケートは、対象者の属性(性別、職階、年齢、経験)や各メールの対処、感想等を聞くもので、WEB 上で回答を選択、記入するものとした。

アンケート対象者は**482 名**で､うち**324 名**が回答。回答率は約 **67%**であった。また、分析は **324 名**のうち２通のメールとも受信したと判断できる **185 名**について実施した。主な結果は次の通り。

表１.１回目２回目のメール対応状況

１回目結果（n=185、%は小数点以下第１位四捨五入）

項　目	人数	割合
添付ファイル開封者(開封)数	96 名	52%
添付ファイル未開封者(対処)数	89 名	48%
管理者へ連絡した者(上記内数)	16 名	－

２回目結果（n=185、%は小数点以下第１位四捨五入）

項　目	人数	割合
添付ファイル開封者(開封)数	69 名	37%
添付ファイル未開封者(対処)数	116 名	63%
管理者へ連絡した者(上記内数)	19 名	－

「対処」とは添付ファイルを開かなかった（未開封）
「開封」とは添付ファイルをあけてしまった状態。

表２.１回目２回目の対応推移状況

（n=185、%は小数点以下第１位四捨五入）

項　目	人数	割合	判断
１通目対処２通目対処	68 名	37%	既耐性
１通目開封２通目対処	48 名	26%	接種効果有
１通目対処２通目開封	21 名	11%	接種効果無
１通目開封２通目開封	48 名	26%	接種効果無

「予防接種」の効果があったと明確に判断できるのは１回目開封２回目対処の **48 名(26%)**であろう。

また、元々の攻撃耐性が、既耐性の **68 名(37%)**程度であるところ、予防接種を行うことによって約３割弱が改善し、全体として６割程度の攻撃耐性を有する状況へと向上するという結果となった。

表３.文案による開封、対処の状況の差

（n=185、%は小数点以下第１位四捨五入）

項　目	人数	割合
１通目内部―対処	32 名	17%
１通目内部―開封	57 名	31%
１通目外部―対処	57 名	31%
１通目外部―開封	39 名	21%

「内部」とは、メールが内部の組織(IT 活用推進課)から送信された事を擬装したもの。「外部」とはメールが外部の組織から送信されたものを擬装したもの。

接種メールには２種類の内容を利用したため、異

Countermeasure by "Inoculation" against Targeted attacks-2

† Kentarou YAMAGUCHI
Graduate School of Information Security INSTITUTE of INFORMATION SECURITY　Visiting Researcher
‡ Koichiro KOMIYAMA
Japan Computer Emergency Response Team Coordination Center
††Katsuya UCHIDA
Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

なる傾向の内容によって、その対処に差が出るかどうかの確認を行った。
結果から判断する限り、今回の文案においては、内部からのメールを擬装したものの方がより効果的に対象者を騙す事に成功しているといえる。

表４.感想のポジティブ、ネガティブの割合

(n=185、%は小数点以下第１位四捨五入)

項　目	人数	割合
ポジティブな感想	88 名	48%
ネガティブな感想	4 名	2%
他もしくは記入無し	93 名	50%

アンケートには「今回の予防接種の感想等」の自由記述欄を設けた。「良い訓練方法だと思う」といった積極的に歓迎(ポジティブ)な感想を記入した対象者と、「こういった訓練は行うべきではない」といった否定的(ネガティブ)な感想を記入した者がいたが､今回はポジティブな感想が圧倒的多数を占め、否定したのは全体の **2%**という結果になった。
実施時には、予告をせず抜き打ちで行う「予防接種」についての拒否反応を心配したが、許容又は積極的に賛同されるという結果が出た。

表５.「予防接種」による意識変化の有無

(n=185、%は小数点以下第１位四捨五入)

項　目	人数	割合
意識変化有り	137 名	74%
それ以外、記入無し	48 名	26%

「今回の訓練を経験して自分の中で情報セキュリティへの認識（危機管理意識）の変化などはあったか」という自由記述欄への記入では、**185 名**の対象者中 **137 名(74%)**もが「何らかの意識の変化があった」と記述。一般的には、集合研修等において、受講後に意識変化や行動の変容に至らせるのは困難なことだが「予防接種」は意識変容を発生させる非常に効果的な方法であると判断できる。

７．結果の考察

表２の結果から「予防接種」については、現状改善の効果があると判断できる。全ての対象者にではないが、教育・研修の効果確認と改善に十分に有効といってよいだろう。
メール内容作成等のノウハウ等が必要だが、「メールを出す」という行為のみで実施できるため、コストが低く、組織状況に関係なく実施しやすい、費用対効果が高い方法である事も特筆できる。
また、今回の実験では、メールの内容によって結果に差異が認められた。メール文案作成については、組織の特性などにより、題材や送信者などの想定についての工夫が重要である。実施の際には、経験者のアドバイスを得る事などが必要であろう。

表４、５の結果から、この「予防接種」がほぼ肯定され、好意を持って受け入れられていることがわかる。しかし、これまでの例では、否定的な反応や混乱が発生した報告もある。今回、肯定的な結果が得られた要因を、次のように考察した。

(1)全ての対象者が事前に研修を受け、開封した内容にも「研修効果の確認であること」「研修の内容の復習」といった内容が含まれていたこと。

対応に失敗した者は、研修内容を覚えてなかったと思うであろうし、適切に対処できた者は、後に内容を確認した際に、ある種の達成感等を感じることができたと考えられる。いずれの場合でも、責任の所在を他者ではなく自己にあると考え、そのことが否定的な感想ではなく肯定的な感想を多く述べる結果となったと考えている。
研修という行動が「予防接種」の際にコミットメントと一貫性[2]を発生、それが肯定的な記述をさせたとも考えることができる。これは、感想のいくつかに研修との関連を思わせるものが見られることから推測できる。さらに、教育の一環と意識することで、対象者が「予防接種」を経験学習サイクルの「具体的経験」に位置づけ、自ら学習する機会と捉えたことも影響したと考える。

(2)対象者やその所属組織の持つ特性。

今回の対象者は、管理者ではあるが、IT の専門家ではない一般の地方公務員である。筆者の以前の研究[3]において、本市職員の特性について考察し、非常に高い市民への責任感とともに、個人の価値判断が優先、高い職業的自尊心(ノブレス・オブリジェ)を持つと指摘したが、それが今回の実験の感想として肯定的表現につながり、良い方向の意識の変容を感じる原因となったのではないかと考える。

(3)対象者が IT の専門家ではなかった。

混乱を生じたと聞いた例は、いずれも対象が、IT そのものに関わる業務、専門家を多く含む組織であった。ゆえに、本人を試すような「予防接種」にプライドを傷つけられたり、業務の支障と感じたり、場合によっては解析行為を始めたりと、いわば、過剰反応を起こしたとも考えられる。今回の実験の対象者は、ほとんどが専門家でない(情報部門経験者は **185 名**のうち **28 名**、約 **15%**)ことで、結果を素直に受け止めたとも考えられる。

(4)対象者が 1 課内に少数（1-3 人）であった。

対象者はひとつの課内に多くて 3 名、またはそれ未満であり、対象者以外は「予防接種」メールを受信していないため、対象者は受診したメールの対処を自分自身で考える状況に置かれた。その部署全員を対象者とした場合は、誰もが同時にメールを見ることが多く、対応に集団の影響を受けてしまうこともあるだろう。メールの対処について自分で考え、自己の責任として処理する方が、集団の影響が排除され良い結果を生むと考えた。

８．まとめ

「予防接種」についてのまとめは次のとおり。

- **「予防接種」は状況を改善する効果がある**
- **疑似攻撃メール内容には工夫、注意が必要**
- **単体ではなく研修などの一環として実施すべき**
- **対象に専門家が多い時は実施可否を慎重に判断**
- **可能なら全員ではなく一部を対象に行う**

実施の際には、先例を調査し、できれば経験者とともに計画を立て、実施することが望ましい。
実際、標的型メール攻撃の防御は困難を極める、今後もこの予防接種が多くの組織で実施され、セキュリティ意識向上が図られることを期待したい。
最後に､実験実施の機会を与えてくれた JPCERT/CC、実験とアンケートなど協力いただいた横浜市の職員の方々に感謝したい。

文　献

[1] 日本教育工学会　編「教育工学事典」実況出版(株)
2000 年 6 月　p100-102、p355-356
[2] ロバート・B・チャルディーニ(Robert B.Cialdini)社会行動研究会訳「影響力の武器－なぜ人は動かされるのか」
(株)誠信書房　1991 年 9 月
[3] 山口、内田　人間の行動特性を利用したセキュリティ研修効果向上方策の提案（対象団体の特性を考慮した検討）
情報処理学会　CSS2007　2007/10 論文集 pp211-216
参考 山口、小宮山、内田　ユーザへの予防接種というアプローチによる標的型攻撃対策
情報処理学会　CSS2008　2008/10 論文集 pp385-390