JPCERT CC®

2009/06/19

2008 年度 IT セキュリティ予防接種実施調査報告書

－概要－

JPCERT/CC では、企業における標的型メール攻撃の被害低減を目的とした、「効果的な IT セキュリティ予防接種手法(以後、予防接種)」について、2007 年度から継続的に調査を行ってきている。予防接種とは、被験者に対して擬似標的型メール攻撃[i]を行い、ユーザの意識向上を図る情報セキュリティ教育の一手法である。本調査報告書は、2008 年度に 14 の組織において実施した延べ 2600 人への予防接種事例を紹介した上で、その効果を高める実施手法を考察したものである。

調査報告書について

本報告書は企業/組織のセキュリティ管理者やエンジニアを読者として想定している。自組織で予防接種を実施する際の資料として利用できるよう、ケーススタディを含めて具体的な手順を詳細に記載した。

報告書は下記の構成となっている。

1 章: 調査の背景と目的について

2 章: 具体的な予防接種実施手法について

3 章から 16 章: それぞれの協力企業での実施状況及び個別結果の考察

17 章: 各協力企業での結果を総合した全体の考察

18 章: まとめと今後の課題など

背景

JPCERT/CC では 2006 年度および 2007 年度にも予防接種に関する調査研究活動を行っており、それぞれ「標的型攻撃についての調査」 および「標的型攻撃対策手法に関する調査報告書」 として調査報告書を公開している。 それらの調査から予防接種が標的型メール攻撃に対して有効な教育手法たる可能性が示されていた。2007 年度の調査では比較的小規模な企業・組織を協力企業として実際に予防接種を実施し、効果を確認した。

2008 年度調査の目的

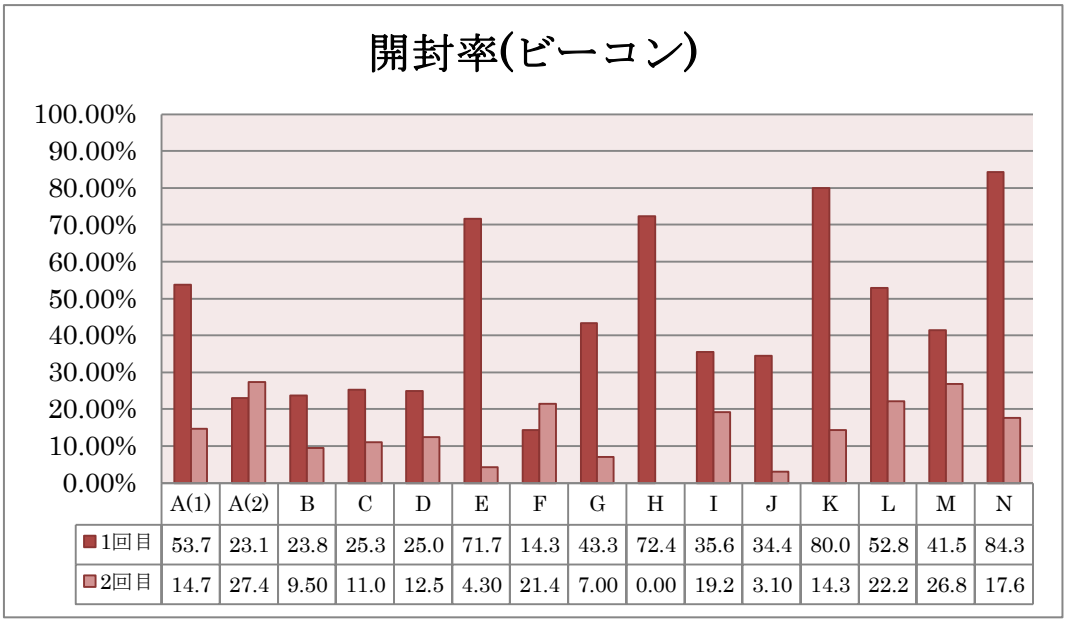
2008 年度の調査では、2007 年度の基本的な予防接種実施手順を踏襲し、より幅広い業種、多くの被験者に対して予防接種を実施し、その効果を定量的に裏付けることを目的とした。また組織形態や従業員の属性に応じた予防接種の最適な手法を探るため、被験者に対してアンケート調査によるフィードバックを求めた。

調査結果サマリー

2008 年度の予防接種調査では、2008 年 6 月 18 日から 2009 年 3 月 31 日までの間に、14 協力企業[ii]、延べおよそ 2,600 人の被験者に対して予防接種を行った。具体的な実施手順については報告書本文の「2 章 実施手法」を参照されたい。一連の調査の結果、以下の事実が明らかにされた。

1. 予防接種により開封率を大幅に減少できる (報告書 17 章 1 節,17 章 2 節)

本調査では、メールに添付するファイルに細工(ビーコン)を施して、開封したことを確認できるようにした。ビーコンの集計を平均すると初回の開封率は 45.4%、2 回目は 14.0%となった。図 1 に示すとおり 2 週間の間隔をおいて実施する予防接種において、ほとんどの場合において 2 回目の開封率が初回と比較して大幅に減少することが確認された。



	A(1)	A(2)	B	C	D	E	F	G	H	I	J	K	L	M	N
1回目	53.7	23.1	23.8	25.3	25.0	71.7	14.3	43.3	72.4	35.6	34.4	80.0	52.8	41.5	84.3
2回目	14.7	27.4	9.50	11.0	12.5	4.30	21.4	7.00	0.00	19.2	3.10	14.3	22.2	26.8	17.6

図 1 企業毎のビーコン集計

2. 年齢や勤続年数にかかわらず予防接種効果を期待できる。(17 章 5 節 2)

本調査では、年齢や勤続年数などの個人属性と予防接種メールの開封率や学習効果になんらかの関係があるという仮説をたてた。そして被験者へのアンケートで下記について尋ね、開封率との関係を分析した。

アンケート項目: 年齢、性別、職種、雇用形態、勤続年数、役職、経験職務、標的型メール攻撃の知識、使用しているメールソフト、情報セキュリティ教育

しかしながら本年度の結果からは、例えば入社 1～3 年の新人だから予防接種メールを開封するなど、属性による開封率に顕著な違いは見られなかった。

このことから標的型メール攻撃が実際に行われた場合、入社 30 年のベテランも経験豊富

なエンジニアも、等しく被害にあう恐れがあると言える。

3.予防接種で明らかになった問題報告体制(17 章 8 節 7)

予防接種実施企業の多くでは、ISMS や社内規程により情報セキュリティ上の問題を報告する窓口が設定されていた。にもかかわらず予防接種メールを受信した時に定められた窓口に報告をおこなったユーザが少ないことが分かった。アンケート結果から、多くの被験者は正規の窓口ではなく近くの IT に詳しい同僚に相談したものと推定される。

これでは予兆をとらえて全社的な対策を打つことも、攻撃の全容を的確に把握することも難しい。効果的にインシデントレスポンスを行う上では、報告手段について組織内に周知徹底をすることの重要性が改めて確認された。なお被験者の 62.6%が今後は管理者への連絡を行うとアンケートに回答しており、本手法を継続することでインシデント発生時により円滑に報告が寄せられることが期待される。

4. 予防接種実施に伴う被験者への負担を軽減する工夫が重要

予防接種は (特にメールの添付ファイルを開封した)被験者に強い印象を与えることが教育効果を高めている。反面、業務のメールと勘違いして開封した被験者などが手法自体に気分を害すことに配慮して、被験者の心証を害さないよう様々な工夫を行った。協力企業には必ず事前教育を依頼し、先だって標的型メール攻撃の特徴や、正しい対応の方法を被験者に伝えるよう心がけた。添付ファイルを開いた際に表示されるコンテンツでは問い合わせ先を明記した。各部署の長には事前に予防接種について説明し、実施時のユーザへの説明に協力いただいた。

このような工夫が功を奏し、被験者アンケートでは予防接種の趣旨を正しく理解したうえで再度の実施を望む声が数多く見受けられた。

その他の発見事項については報告書の 17 章 8 節以降を参照されたい。

まとめ

予防接種を実施することで、標的型メール攻撃に対する警戒心を喚起し、標的型メールを見分けるスキルを獲得させることを通じて、被害を低減することができる。予防接種は、他に類例のない「体験型」の情報セキュリティ教育であり、知識を「体得」させる効果を持つものである。

もちろん、予防接種さえあれば他のセキュリティ対策は要らないなどということはない。事前・事後の、あるいは、継続的な情報セキュリティ教育は当然重要であるし、標的型メール攻撃に限っても、一定の割合で被害を受けるものと想定して多層的な防御態勢を構築することが必要である。

[i] 擬似標的型攻撃メールの基本的なシナリオは、「擬似攻撃メールを受信した被験者がソーシャルエンジニアリングの手法を用いた文面にだまされて添付ファイルを開いてしまう。これによって添付ファイルに仕掛けられたマルウェア(予防接種においては web ビーコン)が動作契機を得る」というものである。

[ii] 横浜市、株式会社ブロードバンドセキュリティ、ラックホールディングス株式会社は協力企業として報告書中に社名を記載することを許可いただいた。