IT セキュリティ予防接種報告書　(2011 年 3 月)

--- 概要 ---

はじめに

JPCERT/CC では、2007 年度から継続的に標的型メール攻撃の被害低減手法の開発と高度化を目的とした「効果的な IT セキュリティ予防接種手法」(以下、単に予防接種と呼ぶ)に関する調査を実施してきた。ここでいう予防接種とは、擬似的な標的型メール攻撃を実際に送付することでエンドユーザのセキュリティ意識の向上を図るという情報セキュリティ教育の手法である。本報告書では、約 3,000 名のエンドユーザ(このうち約半数は過去に[1]予防接種を経験済)に対して予防接種を実施した上で、予防接種手法の効果検証、獲得した耐性の経年変化の検証、標的型メール攻撃に対して脆弱なグループの抽出について議論した。

報告書について

本報告書は、主に一般企業などの組織における情報セキュリティ対策を企画・提案する方々を読者として想定している。時間軸上の動態やリスクグループに関する検討を交えて、標的型メール攻撃が発生した場合に、どの程度のマルウェア感染率を想定するべきかについて分析するとともに、予防接種手法による耐性獲得の状況やその有効期間について得られた知見を記載した。

予防接種 実施の概要

今回は、8 社 2,958 名のご協力を頂いて予防接種を実施した。

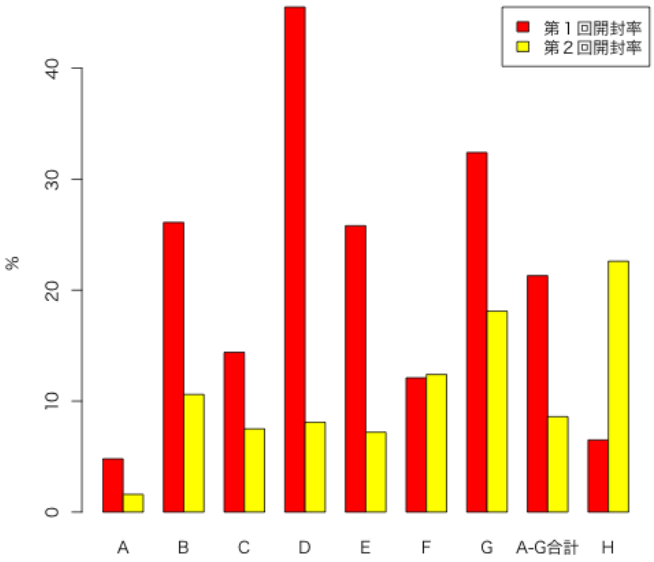
被験者組織	業種など	被験者数
A	セキュリティ対策サービス	63
B	運輸業	161
C	通信サービス業	1,154
D	重要インフラ系システムインテグレータ	198
E	エネルギー関連の研究開発	881
F	Web サービス	282
G	機械工業	188
H	セキュリティ関連の対策検討・助言・調整	31
合計		2,958

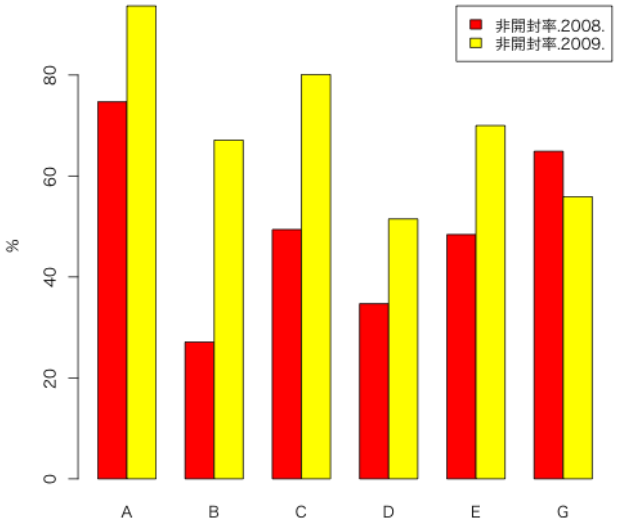
1 標的型攻撃対策手法に関する調査報告書
(http://www.jpcert.or.jp/research/2009/inoculation-summary_20090619.pdf)

調査結果のハイライト

予防接種による短期的効果

予防接種では２週間の間隔をおいて２回の擬似攻撃メール配信を行うが、その２回の配信における添付ファイルの開封率[2]を比較すると、開封率が低下する傾向が見られた（右グラフ）。すなわち、２週間の短期スパンで予防接種手法が有効な教育効果を持つことが確認されたと言える。





予防接種による長期的効果

２年に渡って予防接種に協力していただいた被験者企業について経年変化を調べたところ、非開封率[3]が増加する傾向が見られた（左グラフ）。

また、予防接種の経験者は、未経験者に比べて開封率が低いこともわかった。

したがって、約１年という長期スパンで見ても、予防接種に効果があることが確認されたと言える。

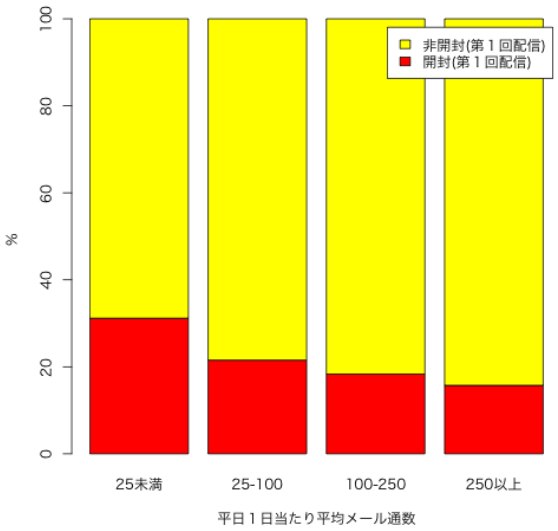
標的型メール攻撃に脆弱なグループ

擬似攻撃メールの添付ファイルを開封した被験者に共通する属性が見つかれば、それは標的型攻撃に脆弱なグループの属性と言えるが、過去の調査結果から性別・年齢層・職務などの属性は開封率に顕著な影響を与えないことがわかっていた。

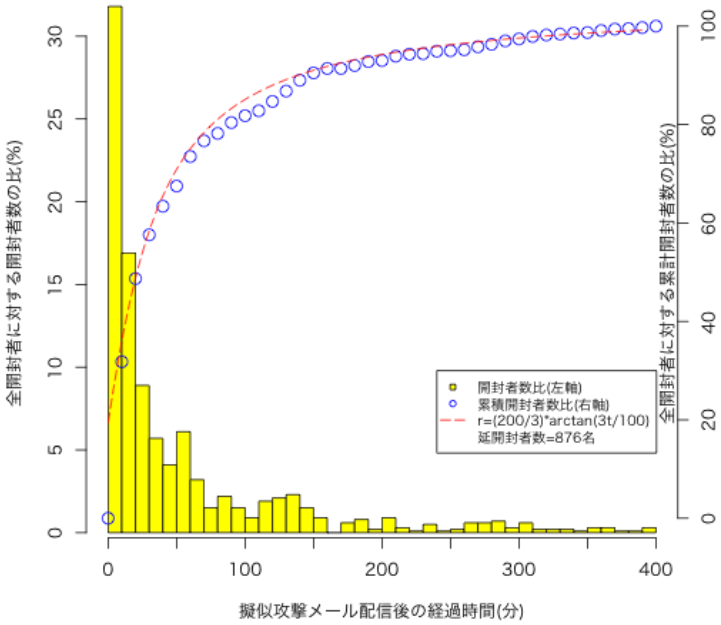
---

[2] 擬似攻撃メールに添付したファイルを開いた人数の比率を開封率と呼ぶ。数字が小さいほど成績が良い指標である。
[3] 擬似攻撃メールの添付ファイルを開かなかった人数の比率を非開封率と呼ぶ。数字が大きいほど良い成績となる指標である。

今回の結果からは、1 日当たりの取り扱いメール数が小さいグループ（右グラフ）やメール処理作業 1 時間当たりの取り扱いメール数が小さいグループで開封率が高くなることがわかった。このふたつのグループは「永遠のメール初心者」層と呼べるかもしれない。



時間軸上の開封状況



時間軸上の開封状況

擬似攻撃メール配信の時点から時間軸上の開封状況を追うと、配信直後の 30 分間に全開封者のうちの約半数が添付ファイルを開いていることがわかった（左グラフ）。これは、組織が違っていてもほぼ共通する性質であった。

標的型メール攻撃対策あるいはウイルス付きメール対策を講じる場合には、この事実を考慮に入れておく必要があるだろう。

おわりに

詳細は報告書に譲るが上記の他にもいくつかの発見事項があった。

標的型メール攻撃はその性質上、攻撃の存在が報道されることが稀ではあるが、今そこにある危機である。予防接種が重要な一部分となって標的型メール攻撃対策が進展すれば、これに優る喜びはない。

これまで予防接種に参加していただいた皆様にはこの場を借りて感謝申し上げる。