2009 年度

IT セキュリティ予防接種調査報告書

一般社団法人 JPCERT コーディネーションセンター

2011 年 3 月 9 日

JPCERT CC®

目次

図表目次

1 はじめに

1.1 標的型メール攻撃とその背景

インターネット上の脅威の質が、好奇心によるものや技術を誇示するものから金銭的利益を追求するものへと変化したといわれて久しい。これは、顕示型・大流行型のものから隠密型・標的型への変化であるといっても良いだろう。

標的型攻撃は、特定少数を狙って換金可能な情報(クレジットカード番号・オンライン銀行アカウントなど、また、防衛・公安・産業上の機密情報など)を窃取しようとするもので、諸外国においては Targeted Attacks と呼ばれることが一般的である。標的型攻撃には幾つかの種類があり、スピアフィッシングと呼ばれる、特定の集団を狙ったフィッシング手法や後述する標的型メール攻撃もその一種である。

標的型メール攻撃の手口は、典型的には次のようなものである。まず、特定少数宛に攻撃メールを送りつける。攻撃メールの表題や本文では、業務連絡や時事問題・アンケートなどの偽の話題で受信者の興味を惹きつけ、添付ファイルの開封や URL のクリックへ誘導する。その結果、トロイの木馬などのマルウェアに起動契機を与えたり、マルウェアを配置した Web サイトへ接続させたりするのである。マルウェアの感染に成功すると、キーロガーを仕込むなど PC 乗っ取りに進むことが多い。

また昨今ではより手口が悪質化し、実際に企業や組織内でやり取りされているメールを入手し、それをもとに作成したとみられる非常に巧妙な攻撃が確認されている。

標的型メール攻撃の被害が公表されることは少ないが、その被害は大きいといわれている。その実態については国内企業へのアンケートを元に調査を行った一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)の報告書「標的型攻撃についての調査[1]」を参照されたい。

1.2 調査の目的

このような状況を踏まえて、JPCERT/CC では、2006 年度の「標的型攻撃についての調査」に引き続いて、2007 年度の「標的型攻撃対策手法に関する調査報告書[2]」および 2008 年度の「IT セキュリティ予防接種調査報告書[3]」において、標的型攻撃の実態調査ならびに予防接種の手法評価を実施してきた。個々の調査活動の結果についてはそれぞれの報告書

1 http://www.jpcert.or.jp/research/#targeted
2 http://www.jpcert.or.jp/research/#targeted2
3 http://www.jpcert.or.jp/research/#inoculation

に詳しいが、これら一連の調査から、標的型メール攻撃と思われる攻撃は実在しており、予防接種手法による教育訓練には一定の効果があることがわかる。

３年目となる今 2009 年度の IT セキュリティ予防接種調査(「予防接種」ないし「予防接種 2009」などと省略して呼ぶ場合がある)では、以下の３点を目的として同様の調査を行うこととした。

1. 予防接種手法による標的型メール攻撃耐性獲得の効果を確かめる。
2. 2008 年度の予防接種の学習効果の継続状況(経年変化)を調査すること。
3. 新リスクグループ仮説(「短時間に大量のメールを捌く者はリスクが高い。」・「擬似攻撃メールの表題や本文が自分の業務に関連がある場合にリスクが高い。」)の検証を試みること。

2　調査実施手法

2.1　調査実施体制と機密保持

2009 年度予防接種調査は、株式会社ブロードバンドセキュリティ(BBSec)に委託して行った。JPCERT/CC と BBSec の間には、業務委託契約の他に機密保持契約(NDA)を締結して被験者組織の秘密の保持を担保した。　また、各被験者組織と BBSec の間でも NDA を締結した。これは予防接種調査のために必要となる被験者リストに含まれているメールアドレスなどを被験者組織から提供いただくための配慮である。

被験者組織の組織名については、JPCERT/CC と BBSec の間ではすべての情報を共有しているが、本報告書など公開に際しては、当該被験者組織のご了承を得たものに限っている。

また、本報告書を公開する前に、機密保持上の問題となるような記述がないことを各被験者組織に確認いただいた。

2.2　調査の流れ

全体としては以下のような流れで調査を実施した。それぞれの詳細は後述するので、ここでは全体の流れに注目して欲しい。

(1)　被験者組織との NDA の締結
　まず協力を申し出ていただいた被験者組織と NDA を締結することで、以後の作業の機密保持の基盤を形成した。

(2)　予防接種実施日程の選択
　2 つの日程を提示し、都合の良い方を選択していただいた。

(3)　擬似攻撃メールの選択と添付ファイルの内容調整
　６種の擬似攻撃メールのメニューを提示し、それから 2 つを選択していただいた。あわせて、擬似攻撃メールの添付ファイルを開いた際に表示されるメッセージの内容を必要に応じて加筆修正いただいた。

(4)　被験者組織における事前教育
　標的型メール攻撃とはどのようなものであるか、またそれが流行していること、したがって注意が必要であることなどを、擬似攻撃メール配信の２から４週間前に被験者組織の中でエンド・ユーザを対象として教育していただいた。

(5) 予行演習とシステム準備

被験者組織側のご担当者(だけ)に宛てて、本番同様の擬似攻撃メールをお送りして予行演習とした。この目的は、ご担当者が具体的な擬似攻撃のイメージを掴んだ上で問題がないかを確認いただくとともに、疑似攻撃メールが届くよう、必要に応じてファイアウォール等のスパム対策の一時的な設定変更をお願いすることにある。

あわせて、被験者アンケート用 Web サイトにアクセスできることもご確認いただいた。

(6) 被験者リストのお預かり

各被験者組織で被験者を選定し、そのメールアドレスのリストを BBSec がお預かりした。

(7) 擬似攻撃メールの配信

擬似攻撃メールを２週間間隔で２回配信した。これらの擬似攻撃メールに添付されたファイルを開封すると、Web ビーコンが作動して BBSec 側の Web サーバにログが残る仕掛けである。

(8) 被験者組織による種明かし

各回の擬似攻撃メール配信後、すべてのユーザがメールを読んだ頃を見計らって担当者から種明かしをしていただいた。

(9) 被験者アンケートの実施

擬似攻撃メール配信が２回とも終わったあとに、被験者アンケートを実施した。被験者アンケートは Web アンケートの形で BBSec もしくは被験者組織が実施した。

(10) Web ビーコンログの計数結果お知らせ

各回の種明かし後に Web ビーコンのログを集計して各被験者組織に BBSec がお知らせした。

(11) 被験者アンケートの集計結果お知らせ

被験者アンケートの回答内容を集計して、各被験者組織に BBSec がお知らせした。

(12) 被験者組織毎に報告書案ご査読

2009 年度予防接種調査の報告書を公開する前に、被験者組織毎に報告書案を査読していただいた。

2.3 日程

今年度の予防接種では、原則として次の 2 つの日程のいずれかを選択して参加していただくようにした。なお、この二つの日程の他に、先行して試験的に予防接種を実施した被験者組織がある。

図表 2-1) グループ別の日程

グループ a	グループ b	項目
2009/09/01		昨 2008 年度の被験者組織へのお声掛け
9/10		応募締め切り
9/01-30	9/01-10/16	NDA 締結作業 システム準備(スパムフィルタなど) 被験者リストお預かり
10/01	10/20	事前教育メール配信
10/14	11/04	第 1 回擬似攻撃メール配信 種明かしメール配信
10/28	11/18	第 2 回擬似攻撃メール配信 種明かしと被験者アンケート依頼のメール配信
10/29-11/06	11/18-25	被験者アンケート実施
11/04	11/24	結果速報(Web ビーコン計数結果)
11/11	11/30	結果速報(被験者アンケート集計結果)

2.4 被験者リスト

各被験者組織から被験者リストとして、被験者のメールアドレス(必須)と氏名(オプション)を表形式でお預かりした。当然であるが、この被験者リストの情報は擬似攻撃メール配信にのみ用いる。

なお、被験者のメールアドレスとしては、被験者個人のものを用いることとし、複数の受信者が受け取るエイリアス(alias)やメーリングリスト(ML)を避けた。これは、alias や ML へ擬似攻撃メールを送った場合、Web ビーコンのログだけでは何人の被験者が開封したのかわからない場合が想定されるからである。

図表 2-2) 被験者リスト表

被験者番号	整理番号	表示名(省略可)	メールアドレス	備考
1000	0	余坊 雪舟	yobou@example.jp	サンプル
	1			二重線枠の内側をご記入下さい。
	2			
	3			
	:			

2.5　システム関連の準備

2009 年度予防接種調査では､擬似攻撃メールの配信と被験者アンケートの実施に際して、被験者側のセキュリティ対策に手を入れていただく必要がある場合がある。

まず、擬似攻撃メール配信に際しては、BBSec は特定のサーバから擬似攻撃メールを送信するので、このサーバを被験者組織側のスパム対策ソフトなどのホワイトリスト設定に入れていただくようにお願いした。

また、同じサーバに Web ビーコンのログ収集用、および、被験者アンケート用の Web サーバを建てるので､このサーバに対する HTTP(80/tcp)および HTTPS(443/tcp)のアクセスを許可するようにお願いした。ログ収集あるいは被験者アンケートにおいて被験者組織の名称などを URL にそのまま用いると被験者組織名が露見する恐れがあるので推測が困難となるような無意味な文字列とした。

2.6　事前教育コンテンツ

本調査では、事前教育用にコンテンツの雛形を作成して被験者組織に提供した。必ずしもこの雛形を用いる必要はないが、これを叩き台にして頂くことで手間が省けることを期待したのである。

また、本報告書では便宜上メールで周知することを前提にしている記述となっている部分があるかもしれないが、事前教育は各被験者組織の通常の方法で周知していただければよいのであって、メールで配らなければならないわけではない。擬似攻撃メール配信の２週間前から４週間前の間に配布するのが望ましい。

最も重要なことは、事前教育を省略して「抜き打ち」で予防接種を実施すると、被験者側に感情的反発が出るなどして効果を期待できなくなることを防ぐことである。抜き打ちの予防接種は過去の予防接種において複数の事例があり、いずれも良い結果につながっていないことをここにあらためて強調しておく。

図表 2-3 に、事前教育コンテンツの雛形を示す。

図表 **2-3)** 事前教育コンテンツの雛形

標的型メール攻撃について

平成 21 年 8 月 5 日
某社 研究開発室
担当：余坊雪舟
(03)CDEF-xxxx

平素より情報セキュリティ対策施策にご協力を頂きまして、誠にありがとうございます。最近、「標的型メール攻撃」の脅威が叫ばれるようになりましたので、以下のとおり注意を喚起します。

覚えて欲しい３項目

A) 標的型メール攻撃は今もひそかに流行しており、あなたも危険です。
B) 標的型メール攻撃では、メールの添付ファイルを開かせること等で、あなたの PC を乗っ取ろうとします。
C) 標的型メール攻撃を防ぐためには、メール受信者が不審なメールをそれと見抜く必要があります。不審なメールを受け取ったら最寄りのセキュリティ担当者に連絡するなどの対応をお願いします。

(1) 標的型メール攻撃の背景

この数年の間に、インターネット上のハッカーの目的は「好奇心・技術誇示」から「金銭的利益」へ、そしてその手口は、派手な大流行型から地味な隠密型・標的型へと変化したと言われています。

なかでも、標的型メール攻撃は「特定少数を狙う」・「換金可能な情報を狙う」もので、新しい脅威の代表例となっています。狙われる換金可能な情報は、一般には、クレジットカード番号・オンライン銀行のパスワードや、防衛・公安・産業上の機密情報などであるようです。

(2) 標的型メール攻撃の手口

標的型メール攻撃では、特定少数のメール受信者に宛てて攻撃メールを送りつけるところから攻撃が始まります。攻撃メールには受信者の興味を惹く話題(時事問題や社内連絡を装うもの等)を巧みに利用して、添付ファイルを開くように誘導します。

受信者が添付ファイルを開くと、その添付ファイルに仕込まれたマルウェア

(悪意のあるプログラム)が起動して、あなたの PC から様々な情報を盗むなどの悪事を働きます。最近のマルウェアは「隠密型」で、悪事を働いていることを気づかれないようにできていますので、キーロガーが知らない間に仕込まれて、キー入力を監視され続けていたなどということになりかねません。

(3) 標的型メール攻撃の事例

残念ながら、標的型メール攻撃の事例が公表されることはほとんどありません。これは、攻撃があったことに気が付いていないか、外聞を気にして公表しないということではないかと思われます。

一般に公開されている事例・調査としては、以下のものがあります。

JPCERT/CC のアンケート調査(2007 年)では、無記名郵送アンケート調査に 282 社が回答しており、その 6.4%が「過去１年間に標的型攻撃を受けた」と回答しています。[i]

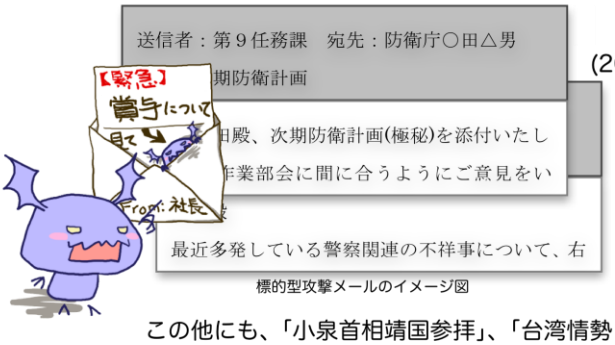
攻撃は増えているのか

アンケート調査では標的型攻撃を受けた経験について、期間を指定しない過去全ての回数と過去１年（2006 年 4 月～2007 年 3 月）の回数を尋ねた。その結果が下図である。

攻撃の例	攻撃を経験したと回答した企業数	回答企業に占める割合
スピアフィッシング	7 (7)	2.6% (2.5%)
関係者を装った社員宛のウィルスメール	18 (15)	6.5% (5.4%)
「DoS をしかける」という脅迫メール	3 (2)	1.2% (0.8%)

( )内は過去１年間

JPCERT/CC アンケート調査(2007)報告書より



標的型攻撃メールのイメージ図

また、白浜シンポジウム(2006 年)での警察庁の講演によれば、警察庁宛に「不祥事への対応について」、防衛庁宛に「次期防衛計画」などという標的型メール攻撃があったとのことです。[ii]

この他にも、「小泉首相靖国参拝」、「台湾情勢について」などという表題でメールを送りつけたり、「平成 19 年度行事計画.lzh」ファイルを添付したりして、攻撃が行われました。[iii]

(4) 標的型メール攻撃への対策

標的型メール攻撃の対策として、スパム対策や情報漏洩対策などの技術的な対策を着実に進めることも大変重要です。しかし、「特定少数を狙う」という標的型メール攻撃の性質上、技術的な対策だけで完全に被害を防ぐことは難しい

と言わざるを得ない状況です。

そこで、「個々のメール受信者が不審なメールを見抜く」ことが重要となっています。攻撃者の技量やその他の状況で変化はありますが、下のリストに掲げる特徴に合致するメールは標的型メール攻撃である可能性があります。(もちろん、標的型メール攻撃ではなく通常のメールである可能性もあります。このあたりが対策を困難にしているところでもあります。)

不審なメールの特徴

- 差出人の名前やアドレスが、見慣れないものである。
- 組織内の話題なのに、外部のメールアドレスから届いている。
- 添付ファイルを開くよう不自然に誘導している。
- 「緊急」などと急がせて、メールの内容を吟味させまいとしている。
- 差出人の署名や名乗りが無いか曖昧である。
- 差出人の名前や組織名として、架空のものを名乗っている。

メールを処理するときには、差出人の情報(名前やメールアドレス)をよく確認するなど、今まで以上に注意をしていただきますようお願いいたします。また、不審に思ったメールについてはそのまま開かずに、メール送信者に確認したり、最寄りのセキュリティ担当者に問い合わせたりする等の対応を行ってください。

---

[i] http://www.jpcert.or.jp/research/2007/targeted_attack.pdf
[ii] http://itpro.nikkeibp.co.jp/article/NEWS/20060529/239209/
[iii] http://www.itmedia.co.jp/enterprise/articles/0510/20/news118.html
http://itpro.nikkeibp.co.jp/article/COLUMN/20070307/264174/
http://biz.plala.or.jp/support/security/backnum/2007/070628.html

2.7　擬似攻撃メール

本調査では、擬似攻撃メール(本文・表題などのテンプレート)を予め準備した上で、各被験者組織が選択することとした。こうすることで、被験者組織間の開封率などの比較や、擬似攻撃メールの種類間の「強さ」の比較などが可能となると考えたためである。

なお、送信元の名称部分については、必要に応じて「ありそうで実在しない」名称に変更できるようにしている。また、差出人として用いたドメイン名は予防接種のために登録したものである。

以下、図表 2-4 から図表 2-9 まで、６種類の擬似攻撃メールを示す。

図表 2-4) 擬似攻撃メール S：インフルエンザ

表題	緊急！新型インフルエンザ強毒化の恐れ
差出人	インフルエンザ対策委員会 <oshirase@SwineFluInfo.jp>
本文	新型インフルエンザの登場以来、感染力は強いものの、毒性が比較的弱いことが指摘されて来ました。 しかし、ついに強毒型の新型インフルエンザが出現し、急速に罹患者を拡大している模様です。 そこで、各位におかれましては、添付の「すぐできるインフルエンザ対策」を参考に、改めてインフルエンザ対策を強化していただきますようにお願いいたします。 新型インフルエンザ対策は初動が大切です。日本発のパンデミック(世界流行)を起こさないために、今こそ行動が求められています。 インフルエンザ対策委員会
添付ファイル名	すぐできるインフルエンザ対策.doc
カスタマイズ	「インフルエンザ対策委員会」を各被験者組織にありそうで実在しない担当組織名に変更する。
気付きポイント	1.差出人の表示名が、実在しない組織である。 2.差出人のアドレスが外部のものである。 3.差出人のアドレスが見慣れないものである。 4.添付ファイルを開かせようとしている。 5.パンデミックを持ち出して急がせている。 6.署名に所在地や連絡先などがない。

図表 2-5) 擬似攻撃メール T：事業継続計画

表題	大地震に対する事業継続計画の見直し
差出人	事業継続計画委員会 <drc@jigyokeizoku.jp>
本文	2009 年 8 月 11 日の駿河湾沖を震源とする地震により、東名高速道路牧ノ原地区の法面が崩落し、５日間にわたって東名高速道路が不通となった災害は記憶に新しいところです。 この事故を教訓として、我々の事業継続計画について特別見直しを行うことと決しましたので、添付ファイルの指示に従って現状の調査にご協力をお願いします。 現状調査の項目には、各自の通勤経路(災害時の帰宅経路含む)の項目もありますので、全員の会頭が必要です。 よろしくお願いします。 事業継続計画委員会
添付ファイル名	事業継続計画現状確認シート 3.doc
カスタマイズ	「事業継続計画対策委員会」を各被験者組織にありそうで実在しない担当組織名に変更する。
気付きポイント	1.差出人の表示名が、実在しない組織である。 2.差出人のアドレスが外部のものである。 3.差出人のアドレスが見慣れないものである。 4.添付ファイルを開かせようとしている。 5.災害と事業継続計画を持ち出して急がせている。 6.署名に所在地や連絡先などがない。 7.誤字がある。(「会頭」→「回答」)

図表 2-6) 擬似攻撃メール U：イントラシステム

表題	緊急アンケートのお願い
差出人	情報システム部 <syuukei@mail1ban.jp>
本文	イントラシステムの使い勝手についてアンケート調査を行いますので、みなさんの忌憚のないご意見をお寄せください。 イントラシステムには Web インタフェースをはじめとして、いくつかのサブシステムがありますが、どれをとっても使いにくいという声が有るようです。 そこで、業務効率改善その他の目的のために、広く意見を収集して改善を図ることになりました。 つきましては、添付のアンケート票に記入の上、至急ご会頭ください。 情報システム部
添付ファイル名	アンケート様式.doc
カスタマイズ	「情報システム部」を各被験者組織にありそうで実在しない担当組織名に変更する。
気付きポイント	1.差出人の表示名が見慣れないものである。 2.差出人のアドレスが外部のものである。 3.アンケートと称して添付ファイルを開かせようとしている。 4.「至急ご返送」せよと急がせている。 5.署名(発信者の記載)がない。

図表 2-7) 擬似攻撃メールⅤ：情報漏洩事故

表題	情報漏洩事故に関するお知らせ
差出人	個人情報保護対策委員会 <kakunin@kojoho.jp>
本文	このたび、あなたのクレジットカード情報が漏洩した可能性があるとの通報を受けましたので、個人情報保護対策委員会として社内の状況確認を行っています。 お心当たりのある方もない方も、万一に備えて確認をされた方がよろしいかと思いますので、添付の用紙に必要事項をご記入の上、至急ご返送いただきますようにお願い致します。 クレジットカード番号を悪用されてしまうと金銭的被害にもつながりかねませんので、お急ぎください。
添付ファイル名	038-クレカ情報照会.doc
カスタマイズ	「個人情報保護対策委員会」を各被験者組織にありそうで実在しない担当組織名に変更する。
気付きポイント	1.差出人の表示名が実在しない組織である。 2.差出人のアドレスが外部のものである。 3.被害の可能性に言及するなど、添付ファイルを開かせようとしている。 4.「至急ご返送」などと急がせている。 5.署名(発信者の記載)がない。

図表 2-8) 擬似攻撃メール W：Windows パッチ

表題	至急：Windows の脆弱性暫定回避策
差出人	情報システム部緊急対策チーム <info@joshisu.jp>
本文	昨日、Windows に極めて深刻な脆弱性が発見されました。 現時点ではパッチが出ておりませんが､暫定回避策がありますので、 添付のマニュアルにしたがって、各自で至急に対策してください。 今回の脆弱性はリモートから PC を乗っ取られる可能性のあるものですので、今すぐに対策していただきますようにお願いします。 情報システム部緊急対策チーム
添付ファイル名	暫定回避策マニュアル.doc
カスタマイズ	「情報システム部緊急対策チーム」の部分を各被験者組織にありそうで実在しない担当組織の名称にする。
気付きポイント	1.差出人の表示名が、実在しない組織である。 2.差出人のアドレスが外部のものである。 3.マニュアルと称して添付ファイルを開かせようとしている。 4.「今すぐに対策」せよと急がせている。 5.署名(発信者の記載)に所在地や連絡先などがない。

図表 2-9) 擬似攻撃メール X：JS 注意喚起

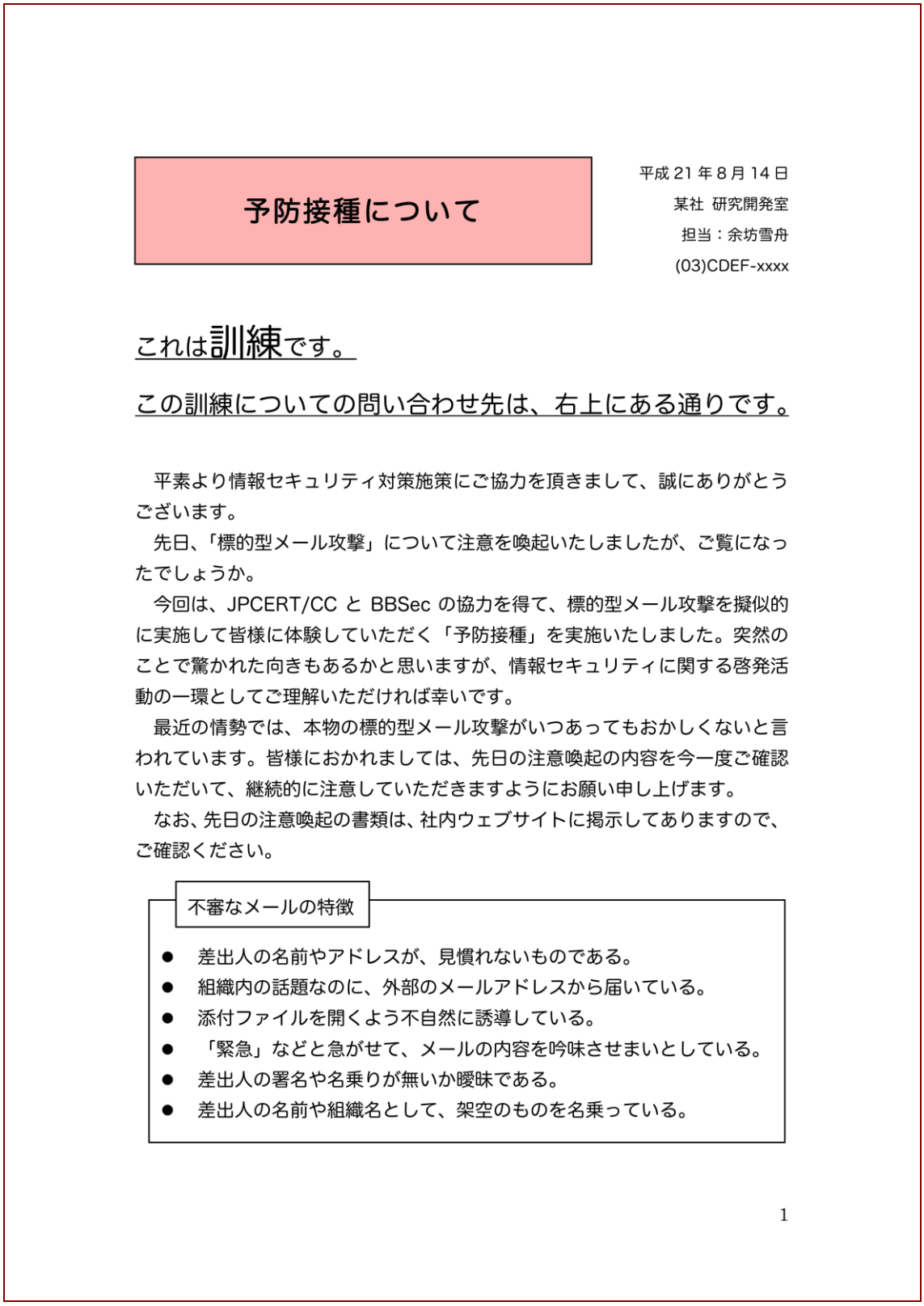
表題	至急：JavaScript などに関する注意喚起
差出人	情報システム部緊急対策チーム <security@joshisu.jp>
本文	各位、 最近、ブラウザ(インターネットエクスプローラなど)における JavaScript のセキュリティホールを使って侵入を試みる事例が激増しています。同様の問題は他のブラウザや JavaScript 類似のスクリプト言語でも見られます。 全部ではありませんが、多くの場合は適切な設定をしておくことで危険を回避できるものですので、 添付の確認手順にしたがってお手元のブラウザの設定を至急点検し、より安全な設定にしていただきますようにお願いします。 情報システム部緊急対策チーム
添付ファイル名	点検手順.doc
カスタマイズ	「情報システム部緊急対策チーム」の部分を各被験者組織にありそうで実在しない担当組織の名称にする。
気付きポイント	1.差出人の表示名が、実在しない組織である。 2.差出人のアドレスが外部のものである。 3.点検手順と称して添付ファイルを開かせようとしている。 4.「至急対策」せよと急がせている。 5.署名に所在地や連絡先などがない。

2.8　擬似攻撃メールの添付ファイル

擬似攻撃メールには、Web ビーコンを埋め込んだ MS-Word 形式のファイルを添付した。擬似攻撃メールの本文・表題などに誘導されてこの添付ファイルを開封すると、Web ビーコンがログ収集サーバへ飛んで開封者として数えられることになる。

この添付ファイルの内容は図表 2-10 に示す通りであるが、少なくとも連絡先の組織名・部署名・担当者名などはそれぞれの被験者組織にあわせて修正する必要がある。他の部分も被験者組織の実情に合わせて必要に応じて適宜修正しても構わない。

図表 **2-10)** 擬似攻撃メールの添付ファイル



予防接種について

平成 21 年 8 月 14 日
某社 研究開発室
担当：余坊雪舟
(03)CDEF-xxxx

これは訓練です。

この訓練についての問い合わせ先は、右上にある通りです。

平素より情報セキュリティ対策施策にご協力を頂きまして、誠にありがとうございます。

先日、「標的型メール攻撃」について注意を喚起いたしましたが、ご覧になったでしょうか。

今回は、JPCERT/CC と BBSec の協力を得て、標的型メール攻撃を擬似的に実施して皆様に体験していただく「予防接種」を実施いたしました。突然のことで驚かれた向きもあるかと思いますが、情報セキュリティに関する啓発活動の一環としてご理解いただければ幸いです。

最近の情勢では、本物の標的型メール攻撃がいつあってもおかしくないと言われています。皆様におかれましては、先日の注意喚起の内容を今一度ご確認いただいて、継続的に注意していただきますようにお願い申し上げます。

なお、先日の注意喚起の書類は、社内ウェブサイトに掲示してありますので、ご確認ください。

不審なメールの特徴

- 差出人の名前やアドレスが、見慣れないものである。
- 組織内の話題なのに、外部のメールアドレスから届いている。
- 添付ファイルを開くよう不自然に誘導している。
- 「緊急」などと急がせて、メールの内容を吟味させまいとしている。
- 差出人の署名や名乗りが無いか曖昧である。
- 差出人の名前や組織名として、架空のものを名乗っている。

1

2.9　種明かし

各回の擬似攻撃メール配信の後、被験者に種明かしをして不安を払拭するように各被験者組織の担当者に依頼した。種明かしの要点は以下の通りである。

(1)　以下の点を強調すべきである。
　　(ア) 擬似攻撃メール配信が訓練であって実害はないこと。
　　(イ) 今回の結果によって各個人を評価するわけではないこと。
(2)　擬似攻撃メール配信の同日夕刻を目処に周知してほしい。
(3)　２回目の種明かしの際には、被験者アンケートへの協力を依頼して欲しい。

種明かしの方法や内容について、適宜修正して使っていただけるように図表 2-11 および図表 2-12 に示す雛形を作成・配布した。

図表 2-11) 種明かし文案(１回目)

社員各位

情報セキュリティ対策委員会

担当：余坊雪舟

予防接種の実施について(報告)

平素より情報セキュリティ対策にご協力を頂きまして、誠にありがとうございます。

本日、標的型メール攻撃に対する教育訓練として、「予防接種」を実施いたしました。
これは、擬似的な標的型メール攻撃を実施して皆さんに体験していただくことで、本当の攻撃に対する訓練とするものです。今回の訓練でうまく対応できなかったとしても、実害もありませんし、マイナスの評価をするわけでもありません。今後の対応の参考にしていただければ十分です。

標的型メール攻撃とはどのようなものか、またどのような対応をする必要があるのか、等については、○月○日に注意喚起した通りです。社内向けウェブサイトに説明文書を掲示してありますので、今一度ご確認ください。ファイル名は、「標的型メール攻撃について.doc」です。
「覚えて欲しい３項目」は、次のとおりです。

A) 標的型メール攻撃は今もひそかに流行しており、あなたも危険です。
B) 標的型メール攻撃では、メールの添付ファイルを開かせること等で、あなたの PC を乗っ取ろうとします。
C) 標的型メール攻撃を防ぐためには、メール受信者が不審なメールをそれと見抜く必要があります。不審なメールを受け取ったら最寄りのセキュリティ担当者に連絡するなどの対応をお願いします。

今後も標的型メール攻撃が行われることが予想されますので、下記の「不審なメールの特徴」に注意して慎重な対応をお願いいたします。

・ 差出人の名前やアドレスが、見慣れないものである。
・ 組織内の話題なのに、外部のメールアドレスから届いている。

・ 添付ファイルを開くよう不自然に誘導している。
・ 「緊急」などと急がせて、メールの内容を吟味させまいとしている。
・ 差出人の署名や名乗りが無いか曖昧である。
・ 差出人の名前や組織名として、架空のものを名乗っている。

図表 2-12) 種明かし文案(２回目)

社員各位

情報セキュリティ対策委員会
担当：余坊雪舟

予防接種の実施について(報告)

平素より情報セキュリティ対策にご協力を頂きまして、誠にありがとうございます。

先日に引き続いて本日、標的型メール攻撃に対する教育訓練として、「予防接種」を実施いたしました。
これは、擬似的な標的型メール攻撃を実施して皆さんに体験していただくことで、本当の攻撃に対する訓練とするものです。今回の訓練でうまく対応できなかったとしても、実害もありませんし、マイナスの評価をするわけでもありません。今後の対応の参考にしていただければ十分です。

標的型メール攻撃とはどのようなものか、またどのような対応をする必要があるのか、等については、〇月〇日に注意喚起した通りです。社内向けウェブサイトに説明文書を掲示してありますので、今一度ご確認ください。ファイル名は、「標的型メールメール攻撃について.doc」です。

なお、予防接種は、JPCERT/CC の調査案件として BBSec が実施しているもので、最終的には報告書として結果を公開する予定で作業を進めているところです。もちろん、最終報告書には許可の無い限り、被験者組織の名称や個々の被験者の方のお名前・メールアドレスなどは掲載しないことになっていますのでご安心ください。

「標的型メール攻撃への対策を考える上で皆さんの予防接種経験から教訓を得たい」と

いう趣旨で、JPCERT/CC 及び BBSec からアンケートの依頼が来ております。匿名アンケートですので、可能な限り協力をお願いします。(二重回答を防ぐためにクッキーを使っていますが、個人を特定する情報にはなりません。)

アンケートは下記の URL で実施しているとの事ですので、よろしくお願いします。
https://inoculation2009.randd.bbsec.co.jp/<被験者組織毎のハッシュ>
(回答期間 ○月○日から○月○日まで)

2.10 被験者アンケート

本調査では、被験者の属性情報や開封状況などをアンケートで収集した。

被験者アンケートは、集計の手間を考えて Web アンケートとしており、また、被験者の安心を得るために匿名形式で実施した。

被験者アンケートの設問は図表 2-13 の通りである。

図表 2-13) 被験者アンケートの設問

IT セキュリティ予防接種 2009 被験者アンケート

この度は IT セキュリティ予防接種 2009 にご協力いただきましてありがとうございます。

IT セキュリティ予防接種は、JPCERT コーディネーションセンター(JPCERT/CC)による調査案件として実施されており、株式会社ブロードバンドセキュリティ(BBSec) が実際の業務を担当しております。
引き続き、以下のアンケートにご協力いただければ幸いです。

本調査では、報告書を作成して公開する予定です。
以下のアンケートの結果も報告書作成に使用します。
貴組織の名称や被験者の方の個人情報などは匿名化しますので、公開されることはありません。(ただし、許可を頂いて組織名を公開する場合があります。)
二重投稿を簡易的に防ぐためにクッキー(１５桁の乱雑な英数字・期間９０日)を利用しています。
昨年度の報告書が JPCERT/CC から公開されています。匿名化の状況の参考になれば幸いです。
ご多忙中に恐縮ですが、どうぞよろしくお願いします。

なお、本件に関するお問い合わせは、貴組織の予防接種ご担当部署か BBSec 予防接種チーム(<メールアドレス>)までお問い合わせください。

IT セキュリティ予防接種 2009 被験者アンケート

Q1) あなたの性別を選択してください。

1. 男性
2. 女性

Q2) あなたの年齢層を教えてください。

1. ２０歳未満
2. ２０歳代

3. ３０歳代
4. ４０歳代
5. ５０歳代
6. ６０歳以上

Q3) あなたの職務は以下のどれに最も近いですか？

1. 役員
2. 管理職
3. 営業・マーケティング
4. サービス・カスタマサポート
5. 事務職
6. コンピュータ関連技術者
7. その他技術者

Q4) 業務上の連絡を電子メールで送受する場合を想定すると、あなたは電子メールの取り扱いにどの程度熟練していますか？

以下の選択肢から最も良く当てはまるものを選んでください。

1. 非常に熟練している
2. 熟練している方だ
3. 平均的だ
4. あまり熟練していない
5. ほとんどできない

Q5) あなたは業務上のメールを送受信合わせて何通程度取り扱いますか？

平日の一日平均で約_____通

Q6) あなたは業務上のメールをどの程度の時間をかけて処理していますか？

断続的にメールを処理している場合は全部の合計で、また、端数は時間単位に切り上げてお答えください。

平日の一日平均で約_____時間

Q7) あなたは過去に IT セキュリティ予防接種を経験しましたか？

昨 2008 年度の予防接種は、2008 年８月から 2009 年３月にかけて今年度と同様の手法で行いました。

1. 経験した(被験者として参加した)
2. 経験していない(今回が初めて)

Q8) あなたは今年度の第１回配信の擬似攻撃メールにどのように対応しましたか？

この擬似攻撃メールは１１月４日に「情報漏洩事故に関するお知らせ」という表題で配信しました。

1. メールを受け取っており、添付されていたファイルの内容も見た。
2. メールを受け取ったが、添付されていたファイルの内容は見なかった。
3. そんなメールは受け取っていない。

Q9) 第１回配信の擬似攻撃メールの本文や表題は、あなたの担当業務とどの程度関連していましたか？

以下のうち最もよく当てはまるものを選択してください。

1. 非常に強い関連を感じた
2. どちらかといえば関連が強い方だと思った。
3. わずかに関連していた
4. まったく無関係であった

Q10) あなたは今年度の第２回配信の擬似攻撃メールにどのように対応しましたか？

この擬似攻撃メールは１１月１８日に「緊急！新型インフルエンザ強毒化の恐れ」という表題で配信しました。

1. メールを受け取っており、添付されていたファイルの内容も見た。
2. メールを受け取ったが、添付されていたファイルの内容は見なかった。
3. そんなメールは受け取っていない。

Q11) 第２回配信の擬似攻撃メールの本文や表題は、あなたの担当業務とどの程度関連していましたか？

以下のうち最もよく当てはまるものを選択してください。

1. 非常に強い関連を感じた
2. どちらかといえば関連が強い方だと思った。

3. わずかに関連していた
4. まったく無関係であった

Q12) 予防接種について、ご感想・ご意見などを自由にご記述ください。(400 字まで。空欄でも構いません。)

内容を確認したので送信する

上記のボタンを押してもこの画面に戻る場合は、赤い字(必須)の設問について回答が不十分です。適切にご回答をお願いします。
適切に回答されると、回答内容を送信して、アンケートは終了となります。ご協力ありがとうございました。

2.11 被験者組織の募集と選定

本調査では、主として昨 2008 年度の予防接種にご協力いただいた被験者組織を中心にして、今年度の予防接種への協力を依頼した。これは、本調査の目的を達成のひとつに経年変化を調べたいという動機があったためである。

最終的に被験者組織としてご協力いただいた組織は、図表 2-14 のとおりである。

図表 2-14) 被験者組織と被験者数

被験者組織	業種など	日程	被験者数
A	セキュリティ対策サービス (株式会社ブロードバンドセキュリティ)	b	63
B	運輸業	b	161
C	通信サービス業	b	1,154
D	重要インフラ系システムインテグレータ	b	198
E	エネルギー関連の研究開発	b	881
F	Web サービス	a	282
G	機械工業	b	188
H	セキュリティ関連の対策検討・助言・調整 (一般社団法人 JPCERT コーディネーションセンター)	先行	31
(合計)			2,958

なお、被験者組織によっては、擬似攻撃メール配信や被験者アンケートの実施に際して若干の条件の違いがあったので、以下にまとめておく。

1. 被験者組織 F では業務上の都合で第２回擬似攻撃メール配信を 2009/Oct/30 に実施した。これはグループ a の予定に比べて２日遅れである。また、対応して被験者アンケートの実施も時期を遅らせた。しかし、これらの日程変更が予防接種の結果に与えた影響はほとんどないと考える。
2. 被験者組織 G では、Web ビーコンのログ収集サーバを被験者組織 G 内に設置していただいた。これが予防接種の結果に与える影響はないものと考えられる。
3. 被験者組織 G では、自組織のアンケートシステムを用いて被験者アンケートを行った。

このため、各設問に対する回答の間の相関関係を知ることができないので、被験者アンケートの一部の集計・解析を行うことができなかった。

4. 被験者組織 H では、被験者リストの一部にメーリングリストのアドレスを用いた。このため、Web ビーコンのログを用いた集計・解析においても、被験者アンケートの集計・解析においても、被験者組織 H のデータを用いることができない。
5. 被験者組織 H では、他の被験者組織よりも先行して予防接種を実施した。被験者組織 H の調査は作業手順を確認するための予備調査と捉えて、被験者アンケートの集計・解析の対象としないことにした。
6. 被験者組織 A・B・C・D・E・G・H は、昨 2008 年度及び今年度の両方にご協力いただいている。被験者組織 F は今年度に初めて予防接種にご協力いただいた。

3　Web ビーコンから見た予防接種の結果

3.1　被験者組織毎の結果

まず、被験者組織毎の被験者数、使用した擬似攻撃メール、各回の擬似攻撃メール配信時の開封者数とその被験者総数に対する比率(開封率)を図表 3-1 に示す。また、あわせて第１回配信での開封率から第２回配信でのそれを差し引いた数値を改善率として示す。

(改善率)　＝　(第１回配信での開封率)　－　(第２回配信での開封率)

改善率が大きいということは、第１回配信に比べて第２回配信で開封率が大きく低下(改善)されたということであり、2008 年度の予防接種調査でも評価指標の一つとして用いたものである。

図表 3-1) Web ビーコンのデータと改善率

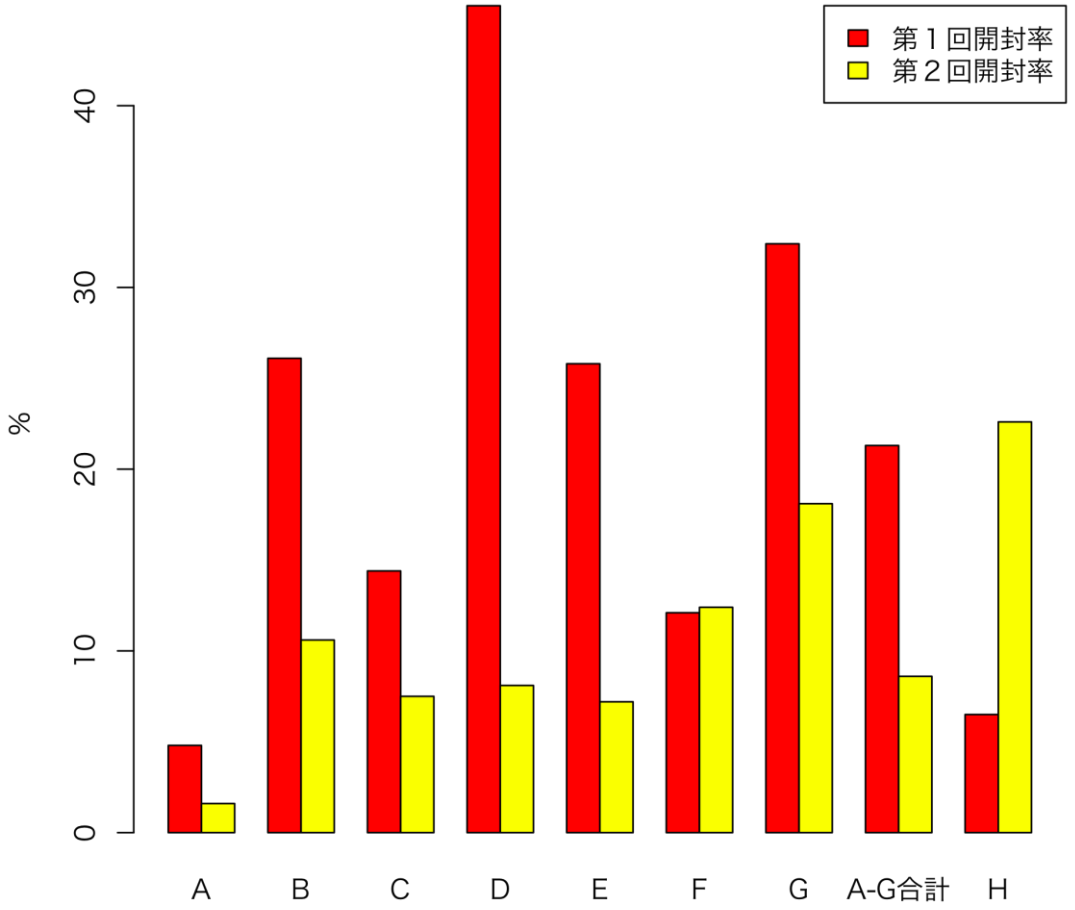
被験者組織	被験者数	擬似攻撃メール		第１回配信		第２回配信		改善率
		第１回	第２回	開封者数	開封率	開封者数	開封率	
A	63	V	S	3	4.8%	1	1.6%	3.2%
B	161	S	T	42	26.1%	17	10.6%	15.5%
C	1,154	S	T	166	14.4%	87	7.5%	6.8%
D	198	V	W	90	45.5%	16	8.1%	37.4%
E	881	S	V	227	25.8%	63	7.2%	18.6%
F	282	S	U	34	12.1%	35	12.4%	-0.4%
G	188	S	T	61	32.4%	34	18.1%	14.4%
A-G 合計	2927			623	21.3%	253	8.6%	12.6%
H	31	V	S	2	6.5%	7	22.6%	-16.1%
合計	2,958			625	21.1%	260	8.8%	12.3%

図表 3-2 には、第１回配信と第２回配信での開封率を被験者組織別にグラフ化したものを示す。

被験者組織 F でほぼ同等の開封率になったのを除けば、各被験者組織で第１回配信よりも第２回配信での開封率が低くなっていることがわかる。(被験者組織 H については、参考

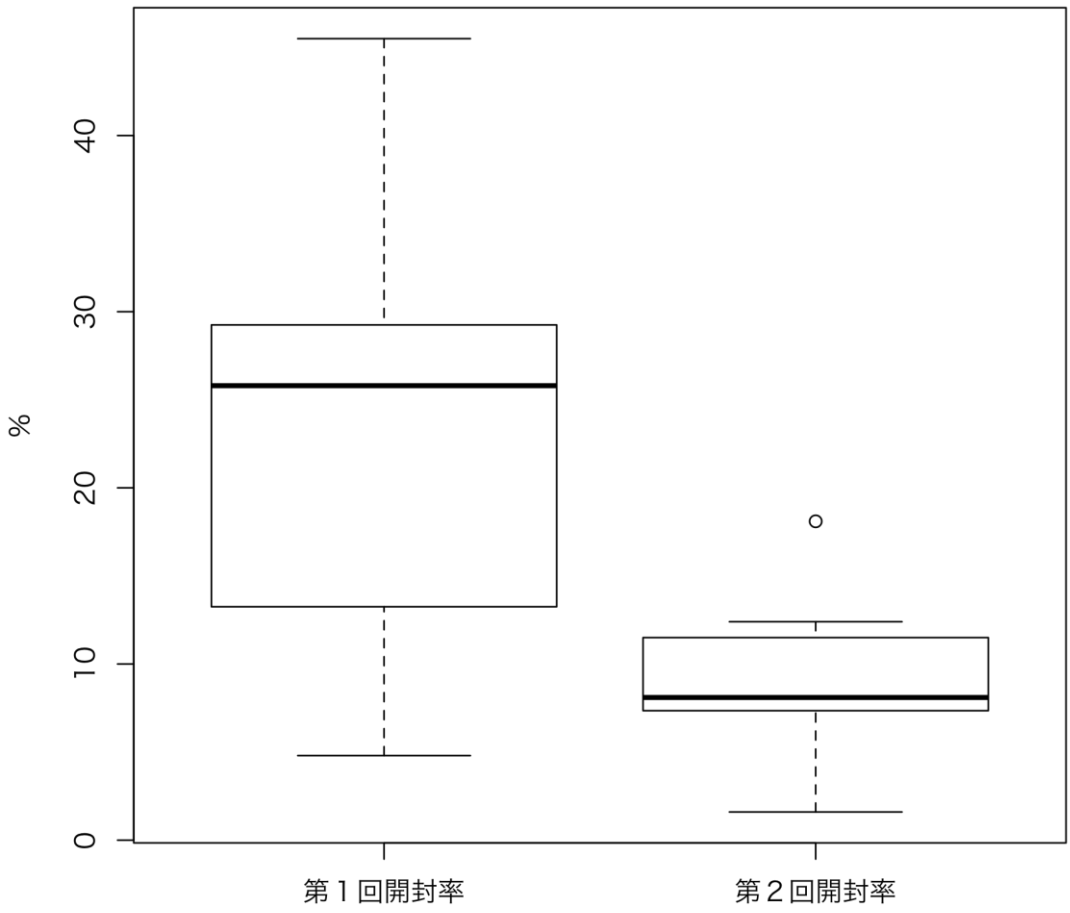
情報として数値やグラフを示してあるが、2.11 節に述べた理由で検討の対象としていない。以下同様である。)

図表 3-2) 被験者組織毎の開封率(第１回・第２回)



さらに、被験者組織 A から G について、箱髭図を作成すると図表 3-3 のようになる。第１回配信での開封率の分布と第２回配信でのそれを t 検定で比較すると、p 値が 0.02791 となって両者には「95%の信頼度で有意な差がある」ことがわかる。即ち、第２回配信の時点では２週間前の第１回配信での教育訓練の効果が現れており、それは統計的に有意な差を生んでいるといえる。

図表 3-3) 被験者組織 A-G の開封率の差



なお、箱髭図では、上下方向中央の太線は中央値であり、箱の上端・下端はそれぞれ上側 25%点・下側 25%点を示している。箱から上下に伸びる髭の端点はそれぞれ上側極値・下側極値であり、外れ値がある場合は、箱髭の上方または下方に◯印をプロットしている。

さらに、被験者の開封状況を４分類に分けて集計することで、Web ビーコンのログを詳細に見ることにしよう。

まず、第１の分類は「開封者⑫」と呼んでいるもので、第１回配信でも第２回配信でも添付ファイルを開封した被験者である。次は「開封者①」で第１回配信では添付ファイルを開封したが第２回配信では開封しなかった被験者であり、「開封者②」の第１回配信では

添付ファイルを開封しなかったが第２回配信では開封した被験者である。最後に、第１回配信でも第２回配信でも添付ファイルを開封しなかった被験者を「非開封者」と呼ぶことにする。これらの分類を表にすれば図表 3-4 のようになる。

図表 3-4) 開封者の４分類

	第１回配信	第２回配信
開封者⑫	開封	開封
開封者①	開封	非開封
開封者②	非開封	開封
非開封者	非開封	非開封

この分類に従って計数すると、図表 3-5 のようになる。ここで、「学習効果率」とは、第１回配信での開封者数に占める開封者①の割合である。

(学習効果率)　＝　(開封者①)　÷　(第１回配信の開封者数)

学習効果率は、第１回配信の開封者のうちどの程度の割合の被験者が「学習して」第２回配信では開封を免れたかを示すので、基本的に大きな学習効果率が好ましいと言える。

図表 3-5) Web ビーコンから見た開封状況と学習効果率

被験者組織	開封者⑫		開封者①		開封者②		非開封者		学習効果率
	被験者数	比率	被験者数	比率	被験者数	比率	被験者数	比率	
A	0	0.0%	3	4.8%	1	1.6%	59	93.7%	100.0%
B	6	3.7%	36	22.4%	11	6.8%	108	67.1%	85.7%
C	23	2.0%	143	12.4%	64	5.5%	924	80.1%	86.1%
D	10	5.1%	80	40.4%	6	3.0%	102	51.5%	88.9%
E	26	3.0%	201	22.8%	37	4.2%	617	70.0%	88.5%
F	3	1.1%	31	11.0%	32	11.3%	216	76.6%	91.2%
G	12	6.4%	49	26.1%	22	11.7%	105	55.9%	80.3%
A-G 合計	80	2.7%	543	18.6%	173	5.9%	2131	72.8%	87.2%
H	0	0.0%	2	6.5%	7	22.6%	22	71.0%	100.0%
合計	80	2.7%	545	18.4%	180	6.1%	2153	72.8%	87.2%

被験者組織毎に開封者の４分類別割合をグラフに描くと図表 3-6 のようになる。

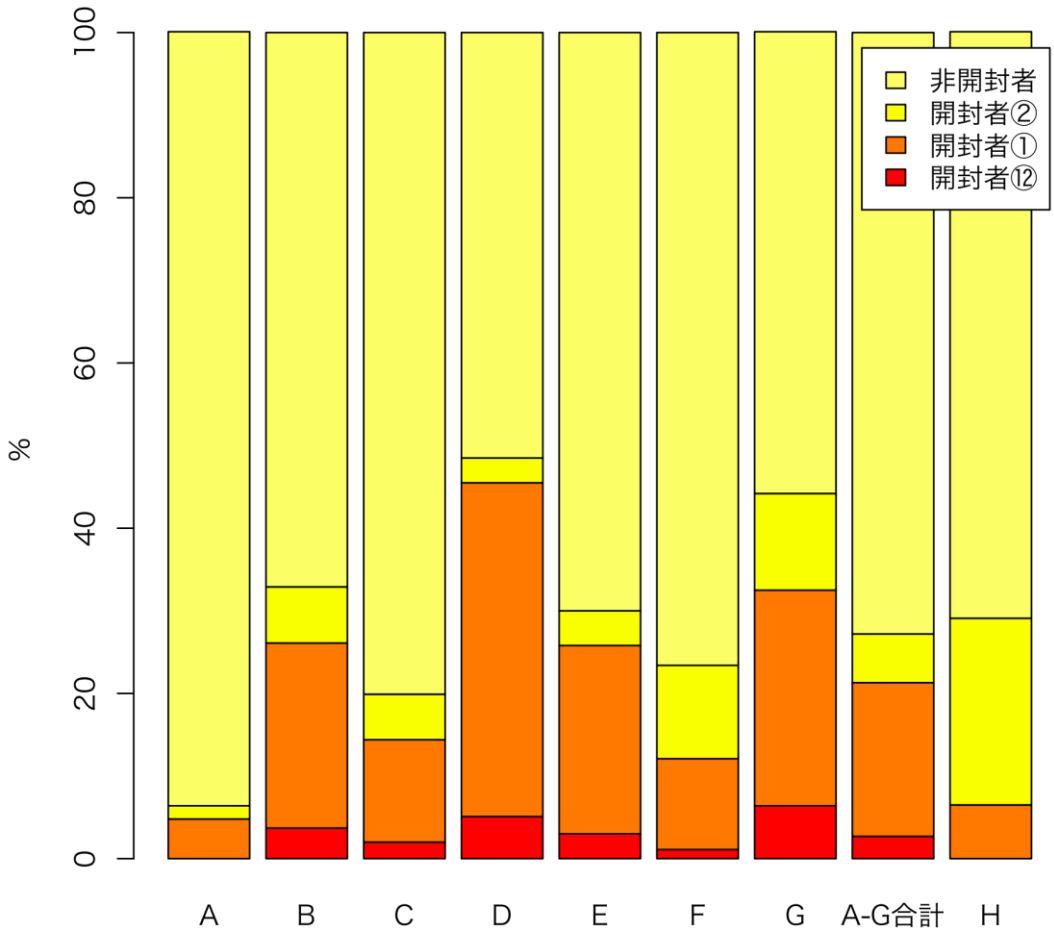
まず、非開封者の割合が大きいほど、全体として標的型メール攻撃に対する耐性が高いと一般的に言えるであろう。

非開封者の比率は被験者組織 A-G の平均で 72.8%であるので、この観点から見ると、被験者組織 A や被験者組織 C の標的型メール攻撃耐性は高いといえる。他方、被験者組織 D や被験者組織 G では非開封者の割合が平均に比べて小さいので、この時点では耐性が低かったと言わざるを得ない。

また、開封者⑫の比率が大きいほど、標的型メール攻撃に気付いていないか、またはそれと察していても敢えて開封する被験者が多いということであり、当該組織にとっては危険であると言えるだろう。

この観点では、被験者組織 G や被験者組織 D は要注意である。

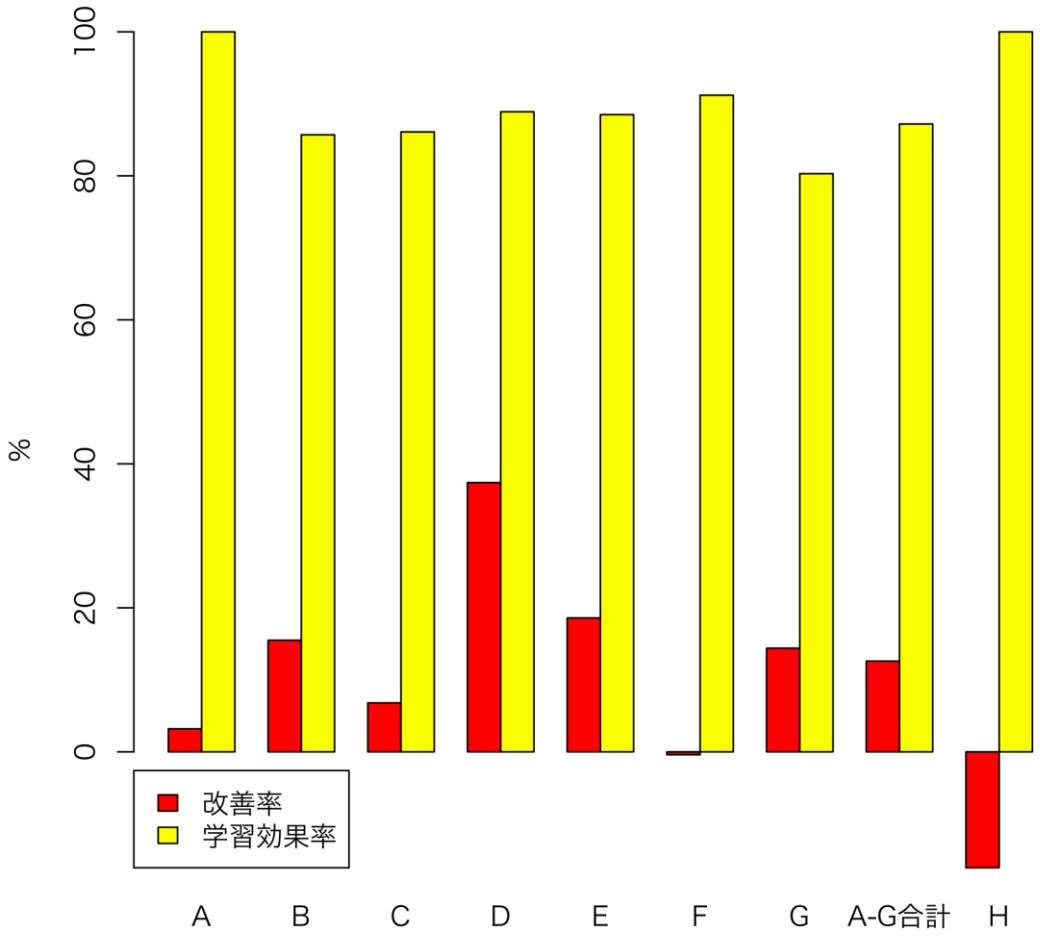
図表 **3-6)** 被験者組織毎の開封者４分類比率



3.2　改善率と学習効果率

被験者組織毎の改善率と学習効果率をグラフに描くと、図表 3-7 の通りである。

図表 3-7) 被験者組織毎の改善率と学習効果率



改善率が大きいということは、第１回配信で学んだ教訓が第２回配信で有効に働いたということである。

今回の結果を見る限り、被験者組織 D・E・G・B の改善率が大きく、被験者組織 F では改善率が小さい。

ただし、第１回配信と第２回配信で用いた擬似攻撃メールの種類が異なるので、第２回配信での擬似攻撃メールが極端に「開封に導きやすい（強い）」場合には改善率は見かけ上小さくなる。個々の状況はそれぞれだと思うが、被験者組織側ご担当者のお話などから推

測して、被験者組織 F では第２回配信で用いた擬似攻撃メールが「強かった」可能性が高いと考えている。

また、非開封者率が高かった被験者組織 A で改善率が小さいのは、開封者率が限界まで抑えられている中で、開封者が偶発的に出ているために第１回配信での開封者数と第２回配信での開封者数に重複がなく、かつ、量的変化も小さかったためであろう。改善率は、予防接種などの教育訓練が行われる前後を通じて、「中→大→小」と推移するのではないかと思われる。

学習効果率については、すべての被験者組織で高い水準にあり、第１回配信で添付ファイルを開封して学んだ教訓が、２週間後の第２回配信で生かされている様子が見て取れる。一部に教育効果率 100%を達成した被験者組織もあるので、教育訓練を実施することで学習効果率は「中または大→100%」のように推移するのではないかと思われる。

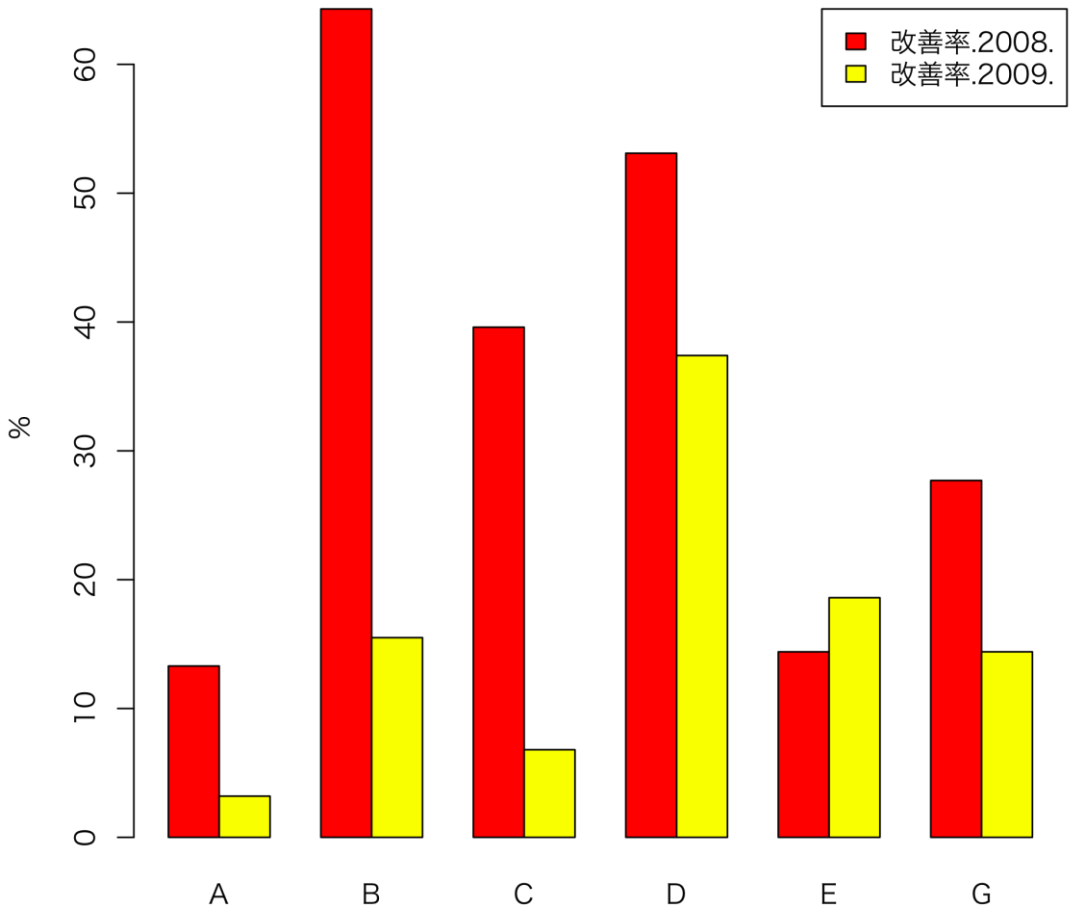
これは、少なくとも２週間程度は予防接種の効果が持続していると言う事であり、先述の第１回配信と第２回配信での開封率に有意差があった点とも符合する。

3.3　改善率・学習効果率・非開封者比率の経年変化

ここでは、比較可能な被験者組織(A-E,G)について、昨 2008 年度と今 2009 年度の改善率・学習効果率・非開封者比率を比較する。

まず改善率については、図表 3-8 のとおりであった。（昨 2008 年度のデータは当該年度の報告書から得た。以下も同様。）

図表 3-8) 改善率の経年変化



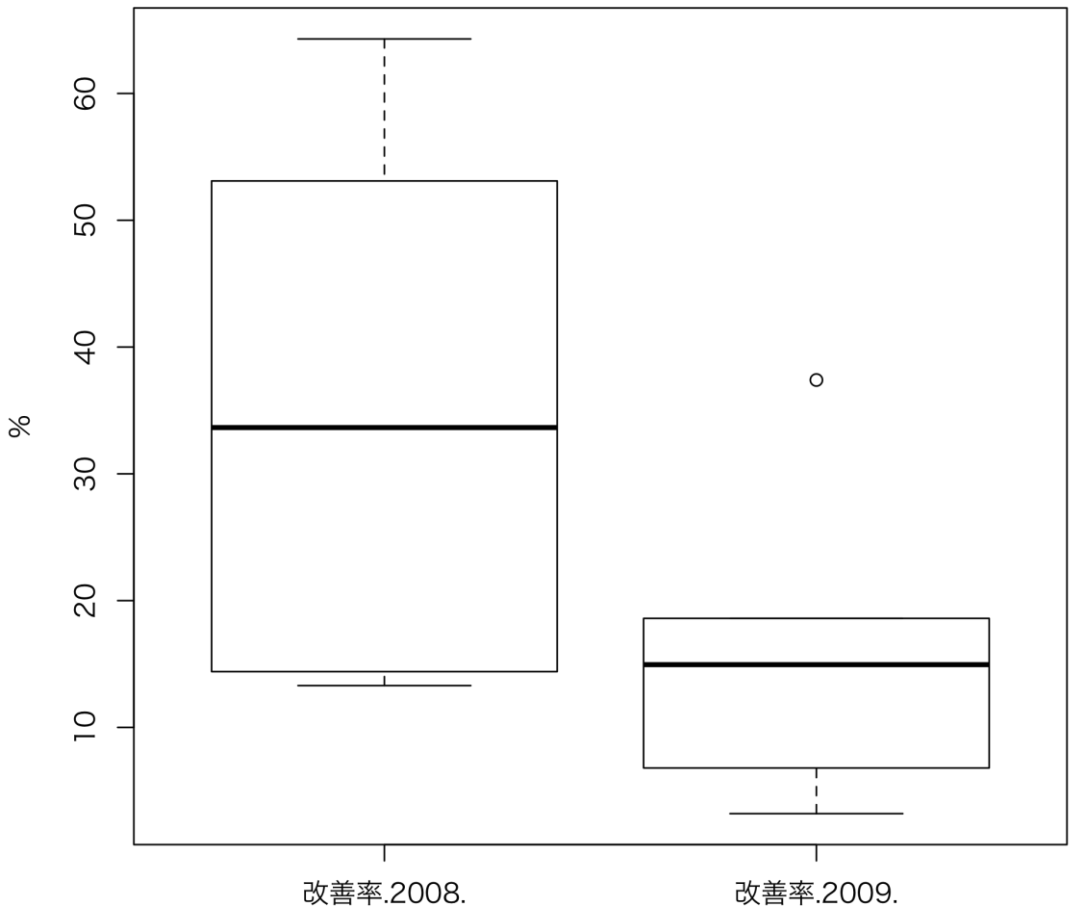
被験者組織 E を除いて、すべての被験者組織で改善率が低下している。予防接種(に限らず情報セキュリティ一般に関する教育訓練やニュースなど)の効果が出ているように思われ

る。

被験者組織 E では昨 2008 年度に比べて被験者数を大幅に増やしたために、訓練初期段階の特徴が強く出たのではないかと思われる。

被験者組織毎のデータを年度別に箱髭図に示すと図表 3-9 のようになる。

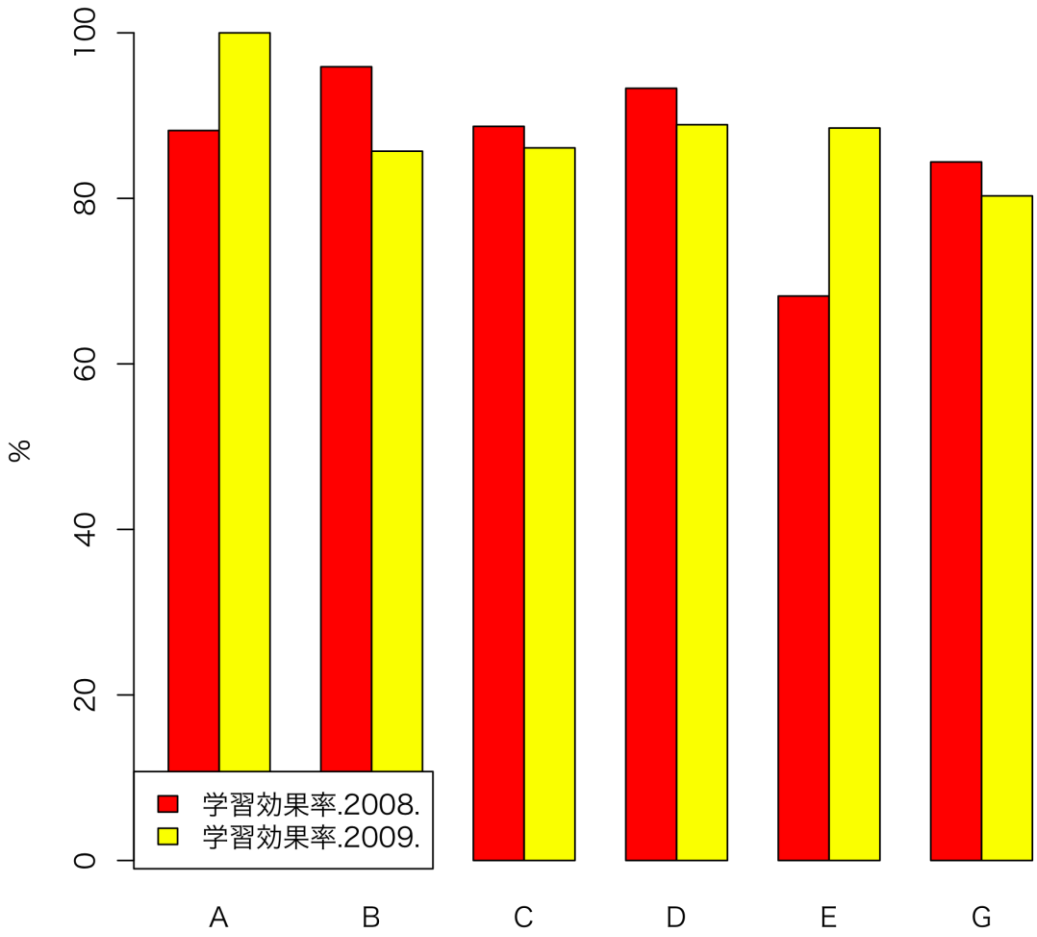
図表 3-9) 改善率の経年変化（箱髭図）



昨 2008 年度と今 2009 年度の改善率の分布について t 検定を行うと、p 値が 0.05122 となって、両者には 90%の信頼度で有意の差が認められる。即ち、改善率は確かに低下しているのである。

次に、両年度の学習効果率の変化を図表 3-10 に示す。

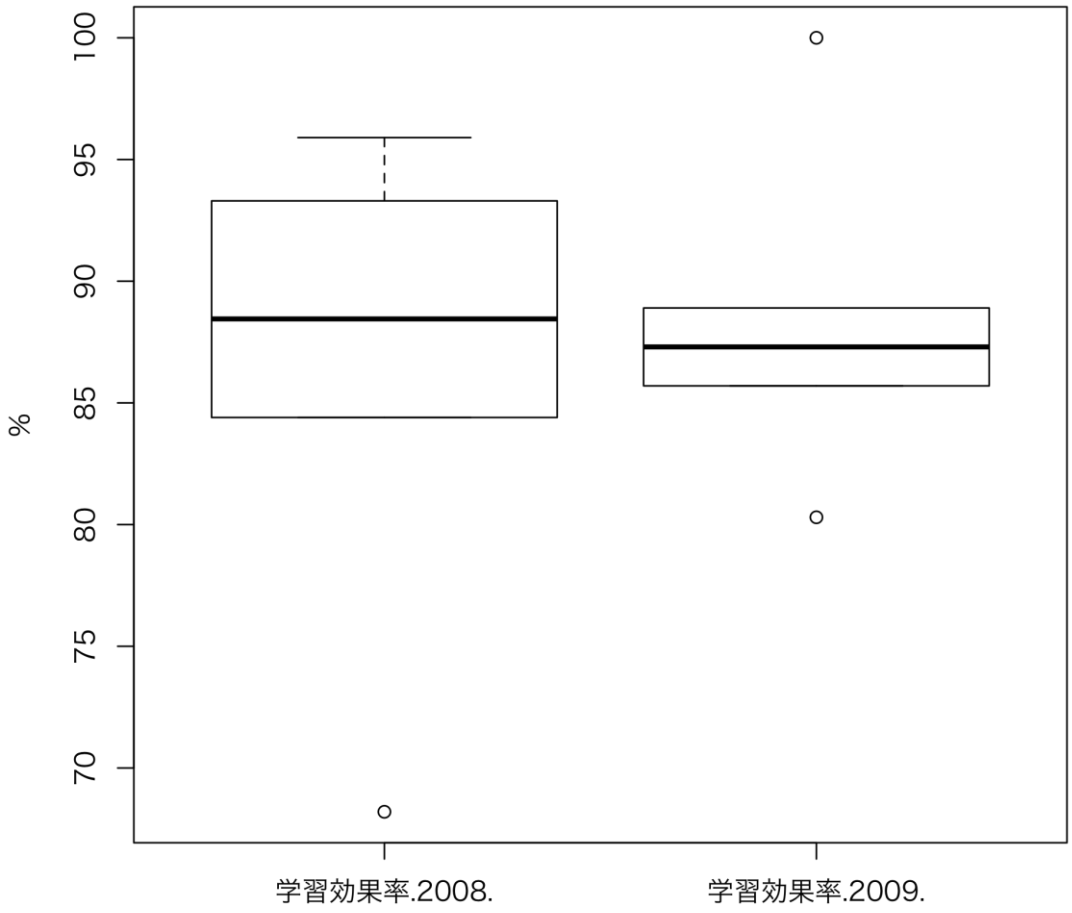
図表 3-10) 学習効果率の経年変化



学習効果率の経年比較では、昨 2008 年度には一部にやや低めの被験者組織が見受けられたが、今 2009 年度では概ね 80%以上と高い水準を達成している。ここでも、少なくとも２週間後までは予防接種の効果が持続するということが言えるであろう。

これを箱髭図にすると図表 3-11 のとおりである。

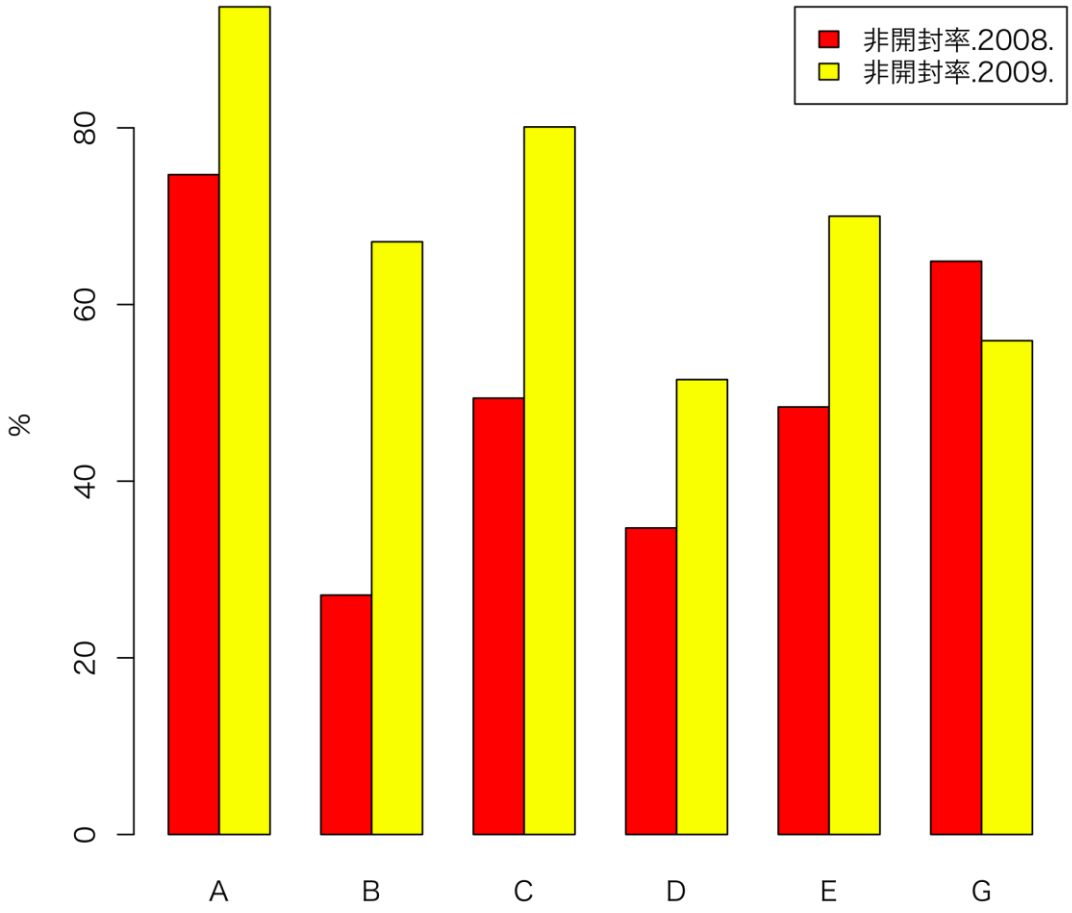
図表 3-11) 学習効果率の経年変化（箱髭図）



箱髭図を見るだけで直感的に学習効果率には明らかな変化はないとわかるが、p 値も 0.7207 となっていて有意の差を認めることができない。

次に、非開封率の経年変化をグラフに描くと図表 3-12 のようになる。

図表 3-12) 非開封率の経年変化

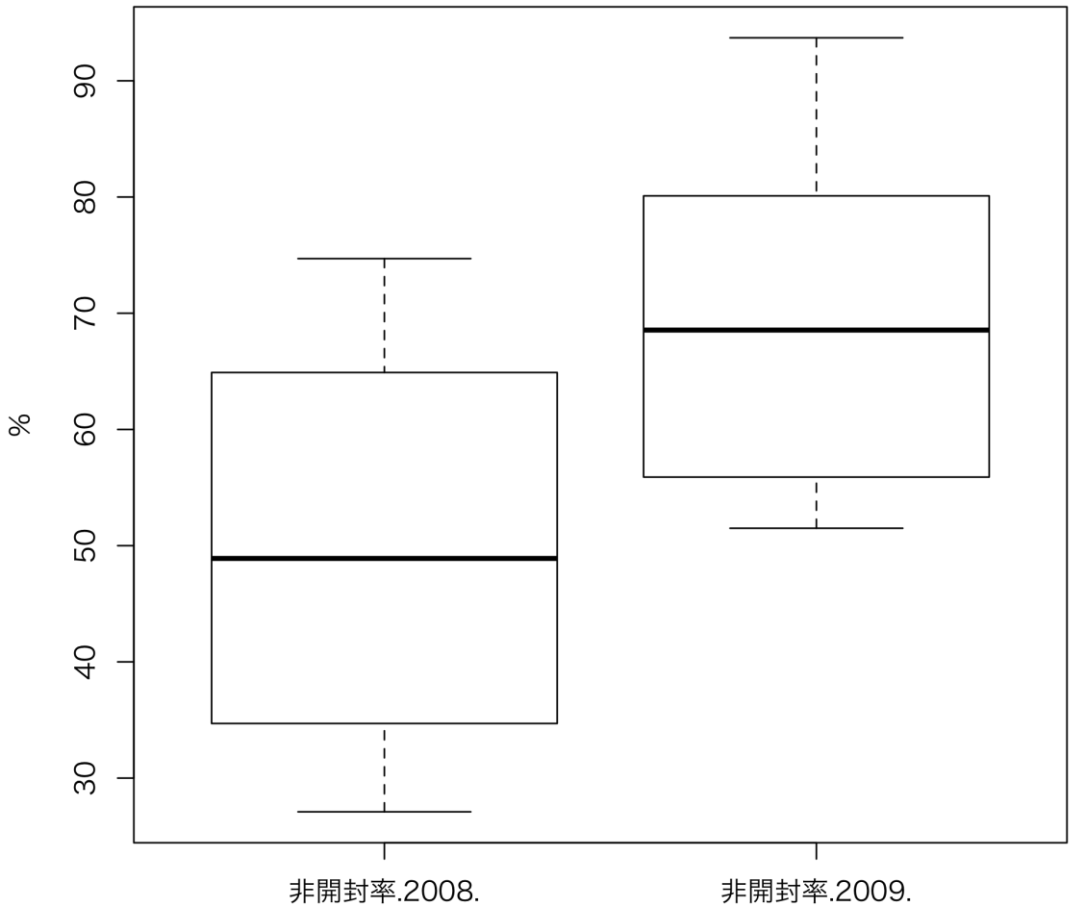


非開封率の経年変化では、被験者組織 G を除いて昨 2008 年度よりも今 2009 年度の方が高い非開封率となっている。組織全体としては順調に標的型メール攻撃耐性を獲得しているものと思われる。

これを検証するために、箱髭図を描くと図表 3-13 の通りである。

p 値は 0.03232 であり、95%の信頼度で非開封率が増大していると言える。

図表 3-13) 非開封率の経年変化（箱髭図）

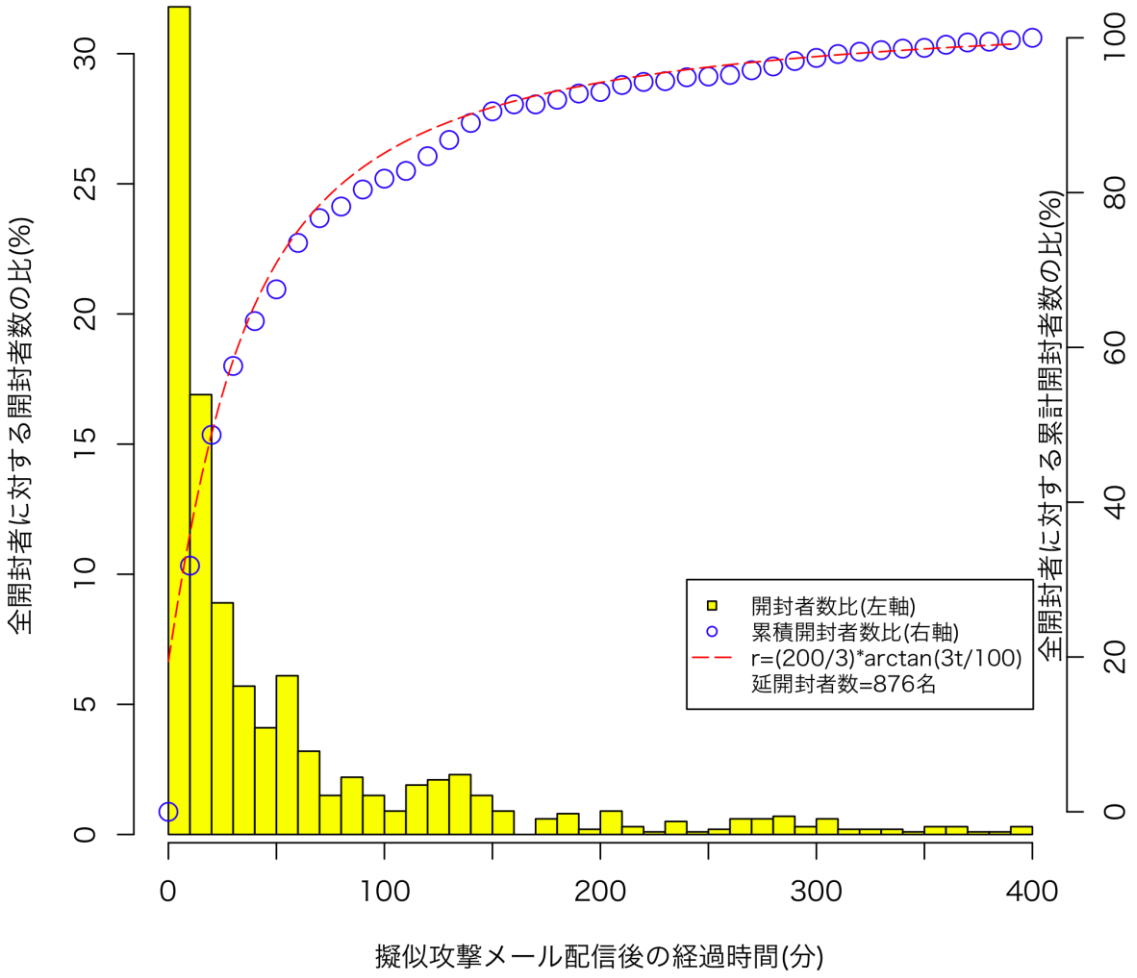


3.4 Web ビーコンから見た時系列開封状況

少し角度を変えて Web ビーコンのログを解析することで、開封者が擬似攻撃メール配信時刻から何分後に開封しているのかについて傾向を見てみよう。

昨 2008 年度に得られた知見では開封者は擬似攻撃メール配信直後に最も多く、時間の経過とともに急速に減少していた。今 2009 年度においても同様の傾向が見られた。今 2009 年度のデータを元に時系列のグラフを図表 3-14 に示す。

図表 3-14) Web ビーコンから見た時系列開封状況



このグラフは、被験者組織 A-G の第 1 回配信・第 2 回配信の Web ビーコンログから各被験者の開封時刻を取り出して 10 分毎のヒストグラム(黄色縦棒・左軸)を作成し、さらにその累計をプロット(青色丸印・右軸)して関数当て嵌めを行った(赤色点線・右軸)ものである。本調査の被験者組織 A-G については、開封のイベントは延べ 876 回発生しており、縦軸にはこの延開封者数 876 名に対する比率を用いた。

開封者数比について関数当て嵌めを行うと、次の式によく合うことがわかった。

$$r = (200 / 3) * \arctan(3 * t / 100)$$

r：全開封者のうち開封済となる割合(%)

t：擬似攻撃メール配信後の経過時間(分)

この関数当て嵌めからは、擬似攻撃メール配信直後の 30 分間で開封者の約半数が開封済となっている様子が読み取れる。すなわち、このような標的型メール攻撃があればその直接的な被害は攻撃直後に多く発生することになるので、この点を考慮に入れて対策を講じる必要があるだろう。

被験者組織 A-G の第１回配信での開封率は平均 21.8%であるが、これを一般的な開封率だと仮定すれば、次のような議論ができるであろう。

即ち、いま 100 名の被験者に対して擬似攻撃メールを配信すれば、約 22 名が添付ファイルを開封するものと思われる。そして、その開封者 22 名の約半数にあたる 11 名は、擬似攻撃メール配信後 30 分以内に開封すると思われる。

3.5　擬似攻撃メール 6 種類の「強さ」

本調査では、図表 2-4 以下にあるように擬似攻撃メール(の本文・表題)を６種類用意しており、各被験者組織が各回の擬似攻撃メールとして二つを選択したことはすでに述べた。その選択結果は図表 3-1 にある通りである。

ここで、ある擬似攻撃メールが別の擬似攻撃メールに比べて、高い開封率を導く傾向があるとすれば、それは「強い」擬似攻撃メールであると言えるだろう。逆に、もし擬似攻撃メールに強弱があるとすれば、これを補正することで、異なる予防接種試行の間で開封率の比較が可能になるかもしれない。

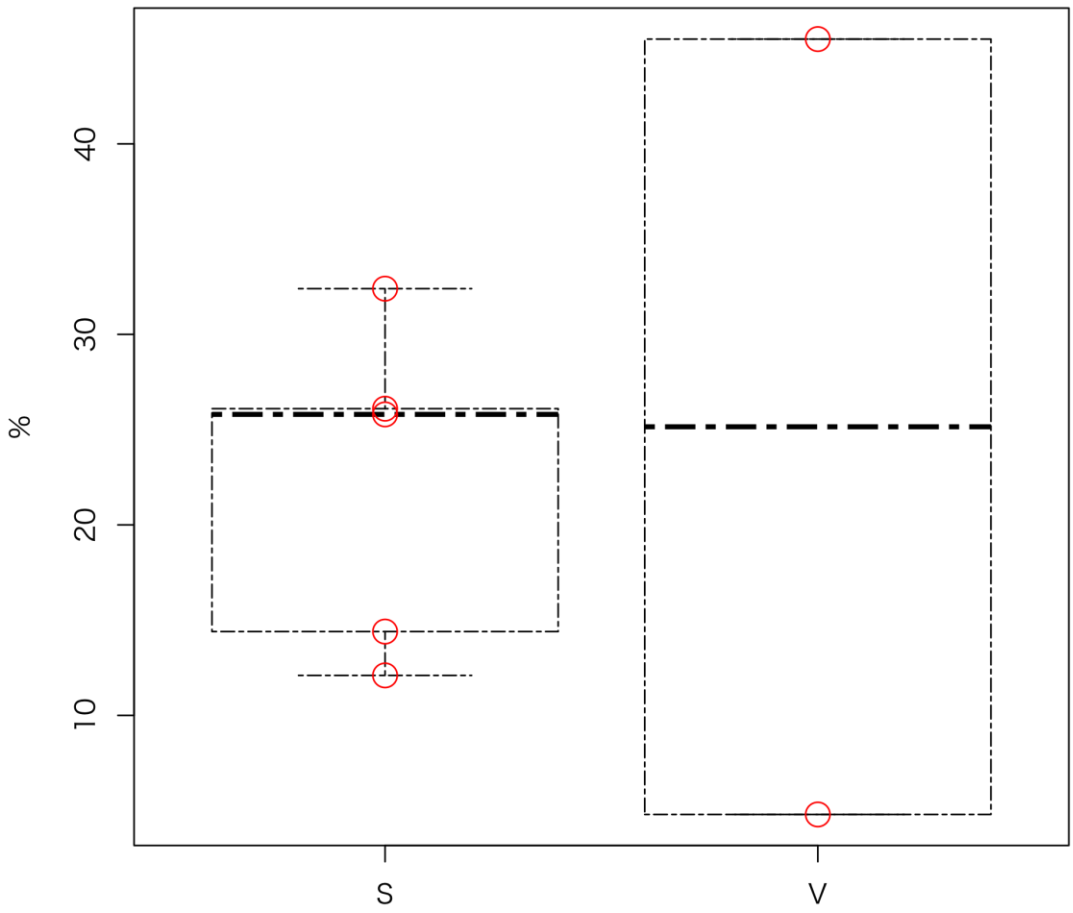
そこで、本調査の結果からそのような傾向を見出すことができるか否かを検討した。

本調査の第１回擬似攻撃メール配信(被験者組織 A-G)では、擬似攻撃メール S および V が選択されている。第１回配信での開封率を擬似攻撃メールの種類毎にプロットすると、図表 3-15 のようになる。

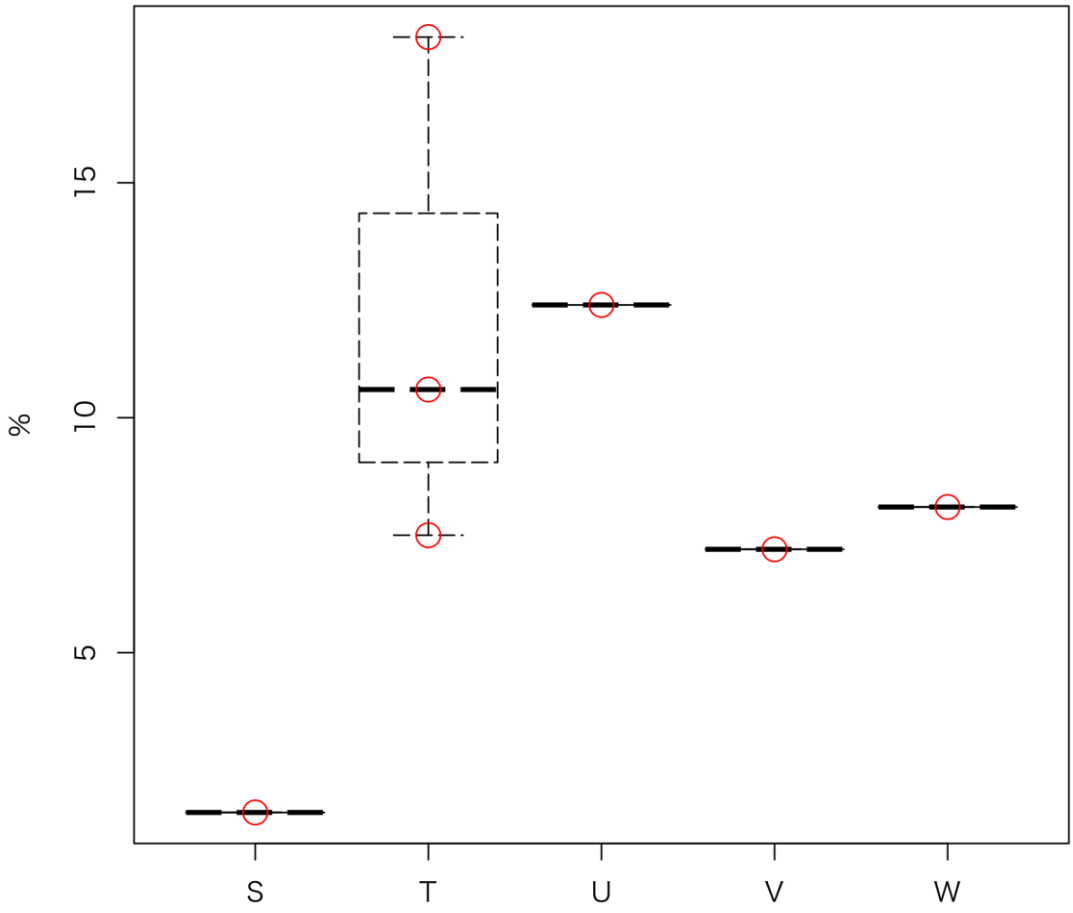
第２回配信についても同様に図表 3-16 のグラフを得ることができる。第２回配信では、第１回配信で用いた擬似攻撃メール種別との関連も問題になるかもしれないが、ここでは単純に第２回配信での擬似攻撃メール種別だけを問題にした。

残念ながら、これらのグラフから何らかの傾向を読み取ることはできないが、これは、試行の数が少ないために傾向を示すに至っていないのかもしれないし、また、本来そのような傾向は副次的であって被験者組織の違いの方が主たる要因となっているのかもしれない。いずれにせよ、現時点で仮説を得ることは困難であり、今後の検討課題としたい。

図表 3-15) 第 1 回配信の擬似攻撃メール種別と開封率



図表 **3-16)**第２回配信の擬似攻撃メール種別と開封率



4　被験者アンケートの結果

4.1　被験者アンケートの回答率

まず、被験者アンケートの回答率を図表 4-1 に示す。各被験者組織で回答率にばらつきはあるが、各被験者組織とも 30%以上の回答率であり、平均すると 38.6%の回答率があるので、回答率には問題はないものと考える。

図表 4-1) 被験者アンケートの回答率

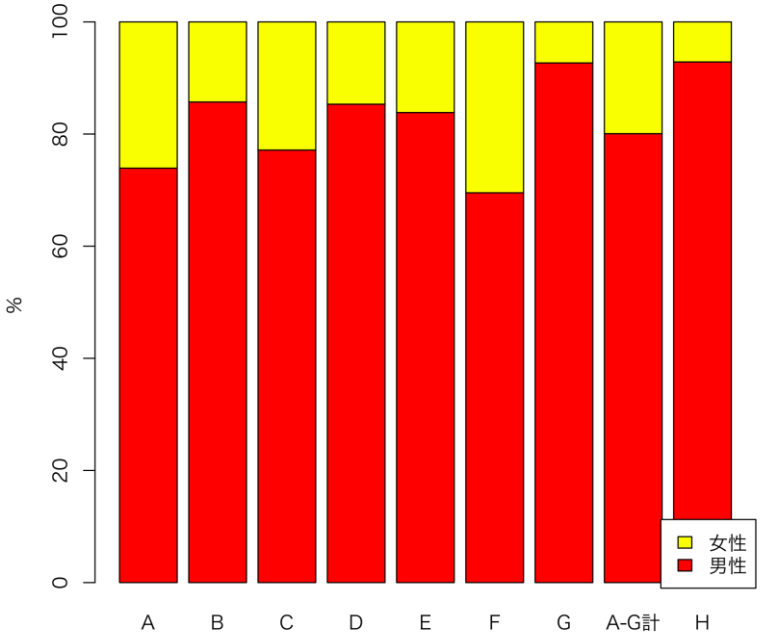
被験者組織	被験者数	被験者アンケート	
		回答数	回答率
A	63	23	36.5%
B	161	63	39.1%
C	1,154	385	33.4%
D	198	109	55.1%
E	881	266	30.2%
F	282	210	74.5%
A-F 計	2,739	1056	38.6%
G	188	123	65.4%
H	31	14	45.2%
計	2,958	1,193	40.3%

4.2　被験者組織のフェイス情報

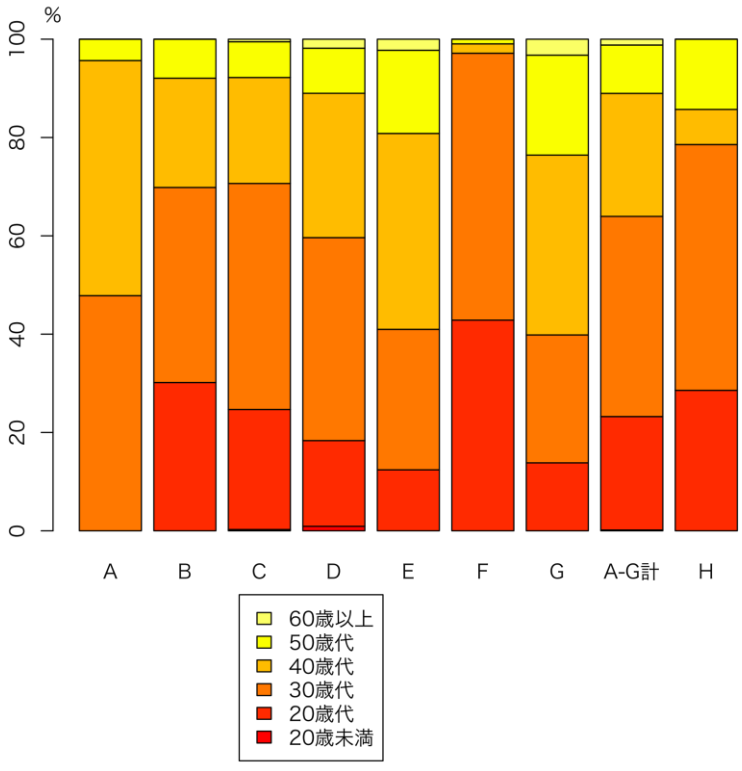
被験者アンケートの結果を集計して、図表 4-2 には性別、図表 4-3 には年齢層、図表 4-4 には職務の種類、図表 4-5 にはメール習熟度といった属性情報を被験者組織毎にグラフ化した。

性別については各被験者組織ともに男性が中心である。年齢層では、20 歳未満は稀で、20 歳代から 40 歳代までの年齢層が中心である。職務では、被験者組織毎にそれぞれ異なるが、管理職系・事務系・技術系に三分されるようである。メール習熟度では、平均的もしくはそれ以上の習熟度を持つと自己評価するものが大半である。

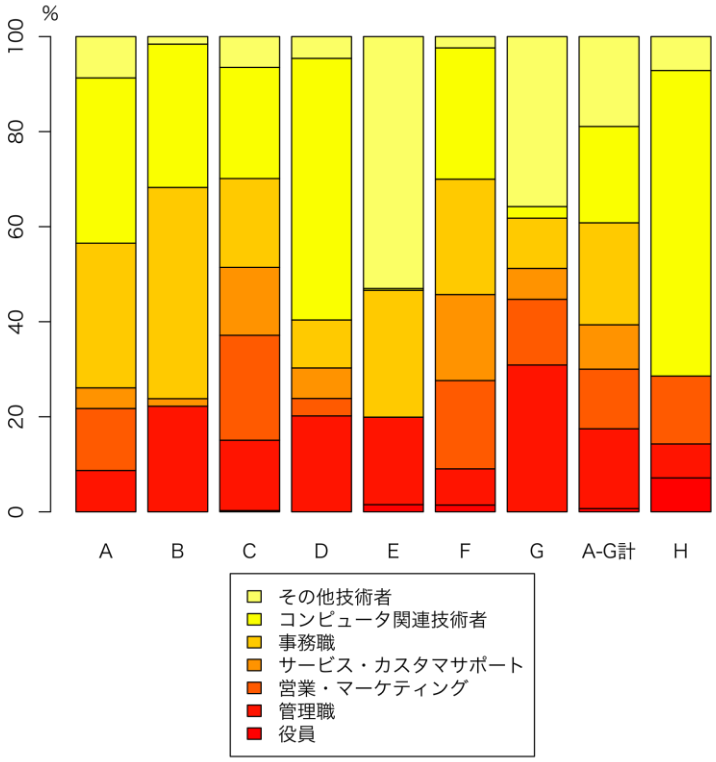
図表 **4-2)** 被験者アンケートから見た被験者組織毎の性別の比率



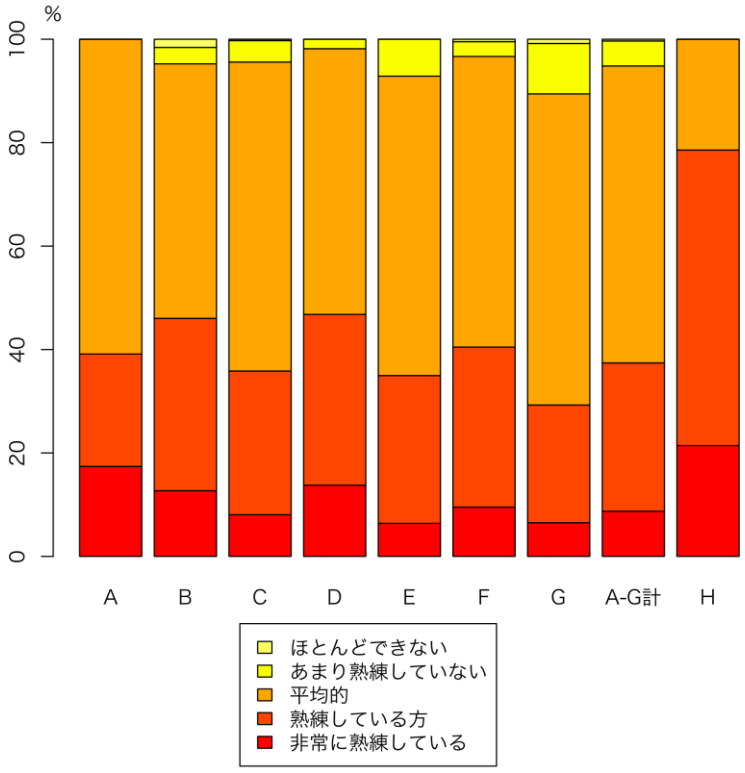
図表 **4-3)** 被験者アンケートから見た被験者組織毎の年齢層の比率



図表 **4-4)** 被験者アンケートから見た被験者組織毎の職務の比率



図表 **4-5)** 被験者アンケートから見た被験者組織毎のメール習熟度の比率



4.3　被験者アンケートから見た開封状況

被験者アンケートの回答を整理して、図表 3-1 および図表 3-5 に相当する表を作成した。被験者アンケートの結果から見た開封状況が、Web ビーコンから見たそれとよく似ていれば、被験者アンケートの分析から得られる解析結果を採用しても良いという根拠の一つになるだろう。

まず、図表 4-6 に各回配信の開封者数・開封率と改善率を示す。

図表 4-6) 被験者アンケートのデータと改善率

被験者組織	回答者数	第１回配信		第２回配信		改善率
		開封者数	開封率	開封者数	開封率	
A	22	3	13.6%	0	0.0%	13.6%
B	63	11	17.5%	4	6.3%	11.1%
C	368	50	13.6%	32	8.7%	4.9%
D	105	53	50.5%	10	9.5%	41.0%
E	252	72	28.6%	10	4.0%	24.6%
F	196	51	26.0%	30	15.3%	10.7%
A-F 合計	1006	240	23.9%	86	8.5%	15.3%
H	13	0	0.0%	3	23.1%	-23.1%

また、図表 4-7 に被験者アンケートから見た開封状況と学習効果率を示す。

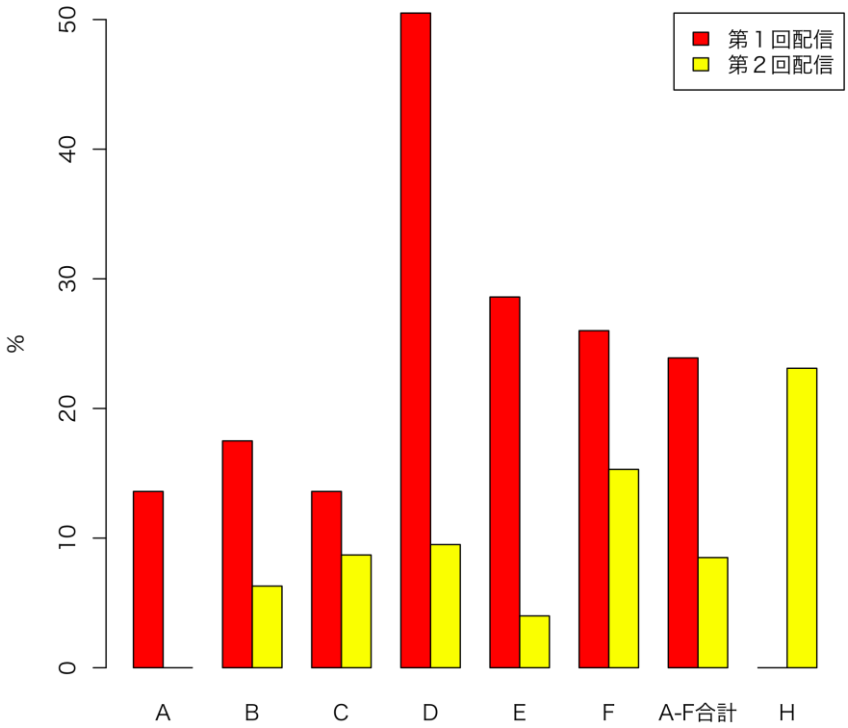
図表 4-7) 被験者アンケートから見た開封状況と学習効果率

被験者組織	開封者⑫		開封者①		開封者②		非開封者		学習効果率
	被験者数	比率	被験者数	比率	被験者数	比率	被験者数	比率	
A	0	0.0%	3	13.6%	0	0.0%	19	86.4%	0.0%
B	3	4.8%	8	12.7%	1	1.6%	51	81.0%	4.8%
C	12	3.3%	38	10.3%	20	5.4%	298	81.0%	3.3%
D	5	4.8%	48	45.7%	5	4.8%	47	44.8%	4.8%
E	8	3.2%	64	25.4%	2	0.8%	178	70.6%	3.2%
F	17	8.7%	34	17.3%	13	6.6%	132	67.3%	8.7%
A-F 合計	45	4.5%	195	19.4%	41	4.1%	725	72.1%	4.5%
H	0	0.0%	0	0.0%	3	23.1%	10	76.9%	0.0%

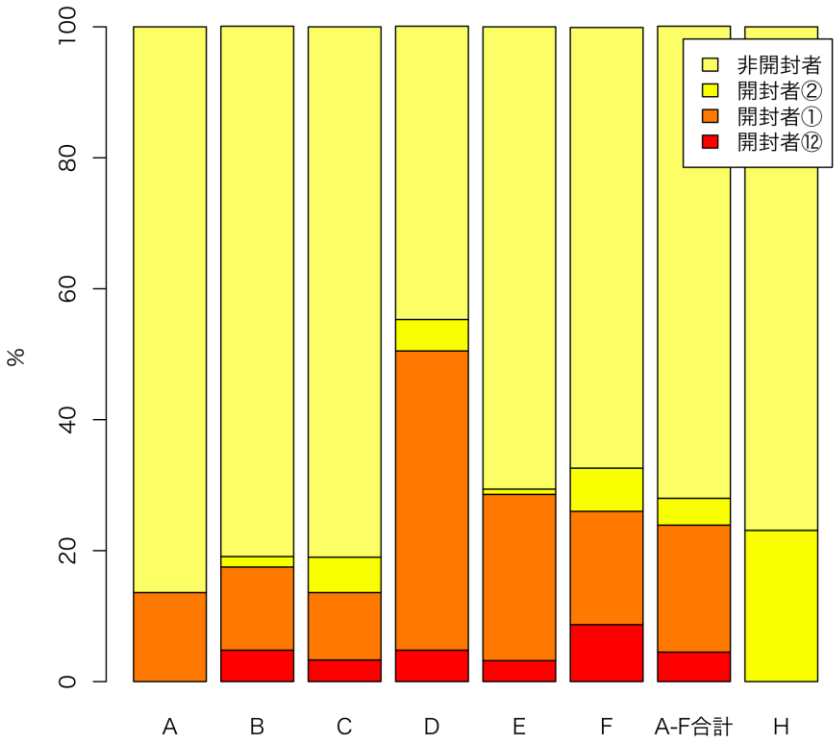
これらの表を元に、図表 3-2 や図表 3-6 に相当するグラフを描くと、図表 4-8 および図表 4-9 の通りである。

これらのグラフがよく似ているので、被験者アンケートの回答のうちの開封状況に係わる部分は、Web ビーコンから見た開封状況とほぼ同様の傾向を示しているのではないかと思われる。したがって、被験者アンケートの回答のうちの被験者の各種の属性について回答した部分を開封状況とともに分析すれば、被験者全体の姿に相当程度一致するものと考えられる。

図表 **4-8)** 被験者組織毎の開封率(第１回・第２回)



図表 4-9) 被験者組織毎の開封者４分類比率



4.4　リスクグループ仮説検証

被験者アンケートの選択肢毎に各回配信の開封者数・非開封者数を集計し、その相関関係を分析して図表 4-10 に示した。

表中に p 値とあるのは、概ね Fisher 検定によるもので、一部 Fisher 検定を適用できない場合についてはカイ自乗検定を援用した。この結果、選択肢間に 95%の信頼度で有意の差があったのは、メール習熟度・(平日１日当たりの)メール数・(メール処理時間１時間当たりの)処理メール通数・予防接種経験の有無・(擬似攻撃メール本文・表題の)業務関連度であった。これらについては、表中に薄緑色の網掛けで示した。

これを見ると、昨 2008 年度の知見と同様に、性別・年齢層・職務などの属性は、開封・非開封の別とはあまり相関関係がないことがわかる。

また、一部の属性は第１回配信での開封率には有意の差を示すが、第２回配信の開封率ではそのような相関関係を認められないものがある。

図表 4-10) 被験者アンケートから見た属性と開封状況の p 値

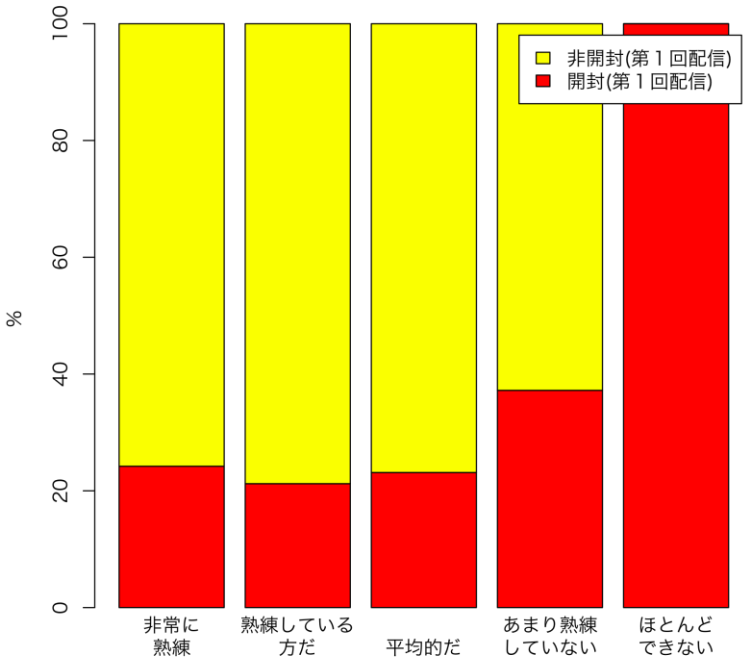
設問	選択肢	第１回配信			第２回配信		
		開封	非開封	p 値	開封	非開封	p 値
性別	男性	198	622	0.3261	69	752	0.2298
	女性	46	174		24	193	
年齢層	20 歳未満	1	0	0.1394	0	2	0.436
	20 歳代	60	194		24	229	
	30 歳代	104	341		35	407	
	40 歳代	52	189		20	221	
	50 歳代	22	68		13	77	
	60 歳以上	5	4		1	9	
職務	役員	2	6	0.2789*	2	6	0.4402*
	管理職	36	120		15	141	
	営業・MKT	25	104		13	115	
	サービス・CS	16	80		6	94	
	事務職	53	183		24	212	
	コンピュータ関連技術者	61	179		22	214	
	その他技術者	51	124		11	163	
メール習熟度	非常に熟練	23	72	0.009841	10	85	0.0006635
	熟練している方	66	245		22	288	
	平均的	136	452		51	537	
	あまり熟練していない	16	27		7	35	
	ほとんどできない	3	0		3	0	
メール数	25 通/日未満	111	245	0.0002386	30	325	0.3122
	25 以上 100 未満	70	255		25	299	
	100 以上 250 未満	46	205		30	221	

	250 以上	17	91		8	100	
延メール処理時間	2 時間/日未満	141	404	0.1619	45	498	0.5005
	2 以上 4 未満	86	323		38	372	
	4 以上	17	69		10	75	
1 時間当たりメール処理数	25 通/時未満	137	352	0.004046	41	444	0.5751
	25 以上 100 未満	71	269		32	310	
	100 以上 250 未満	25	115		16	123	
	250 以上	9	59		4	64	
予防接種経験	経験済	74	405	1.351e-08	29	444	0.004344
	未経験	170	391		64	501	
業務関連度	非常に強い関連	42	67	3.637e-05	24	103	2.027e-05
	どちらかと言えば関連	78	263		35	300	
	わずかに関連	46	242		13	301	
	無関係	78	224		21	241	

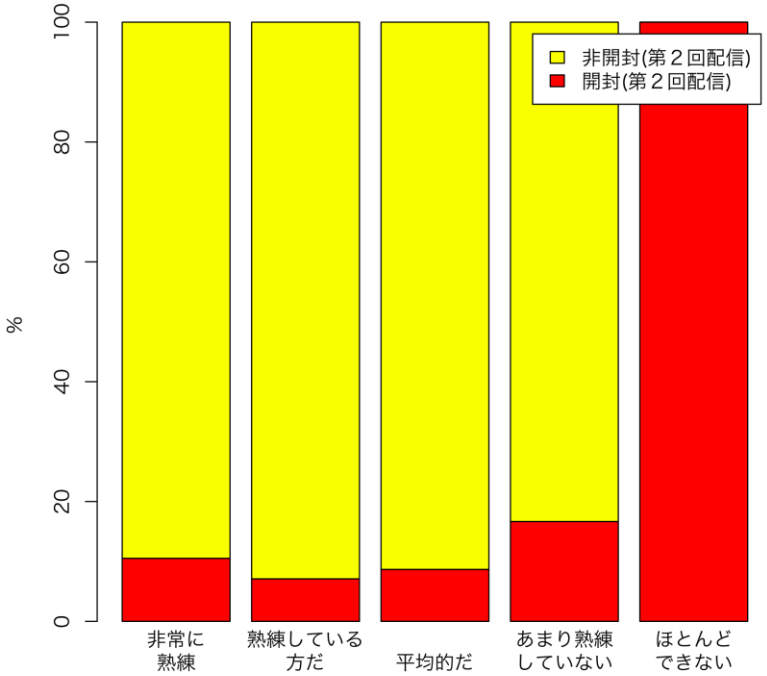
以下では、有意の差があった属性それぞれについて検討を加える。

メール習熟度については、図表 4-11 や図表 4-12 にあるように、「ほとんどできない」と回答している層で開封率が極めて高い。この層がリスクグループである可能性が高いという仮説は自然であるが、他方で開封したことが原因となって「ほとんどできない」という自己評価をしている可能性も否定できない。

図表 **4-11)** メール習熟度と第１回配信の開封状況



図表 **4-12)** メール習熟度と第２回配信の開封状況

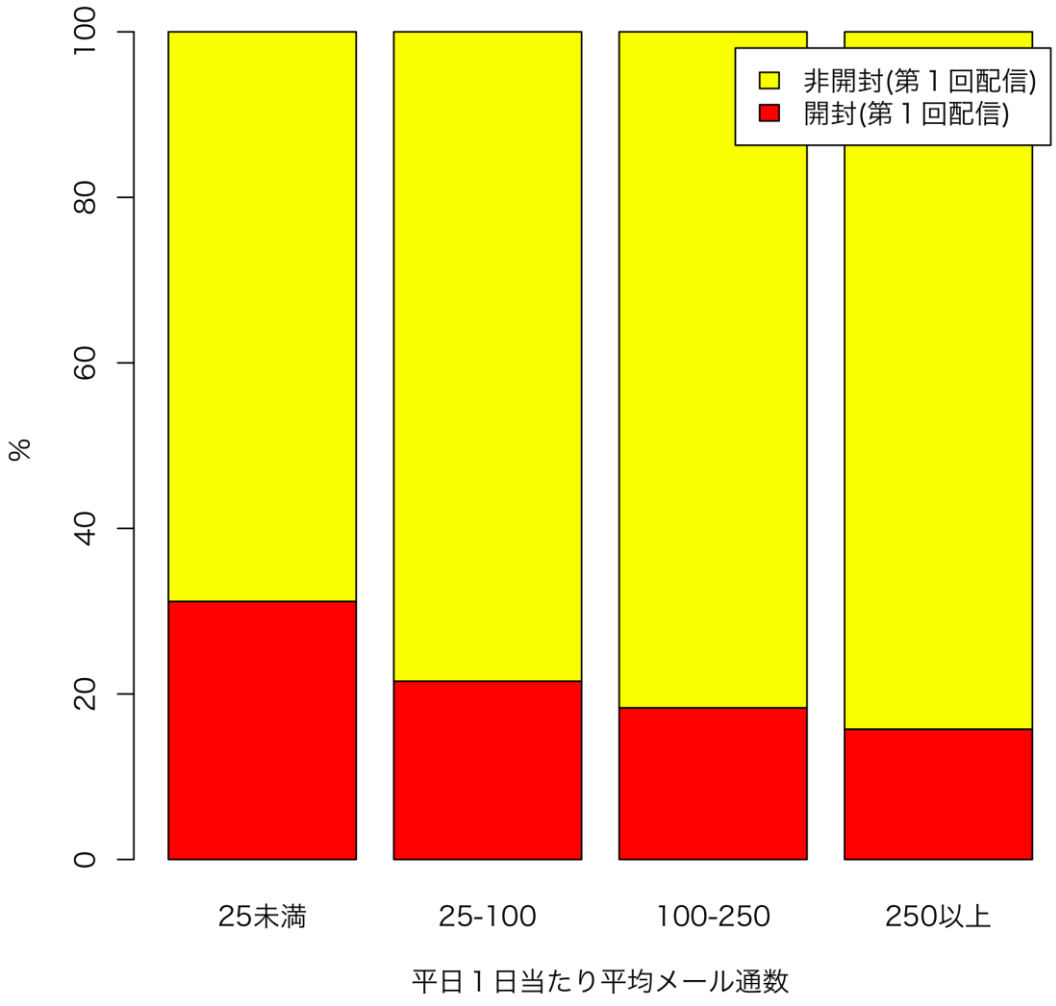


次に、一日当たりのメール通数については、図表 4-13 のグラフを見ると、メール通数が少ないほど開封者が多いようである。

本調査の当初の推測では、多数のメールを捌く者ほどひとつのメールに注ぐ注意力が小さくなって開封しがちであろうと考えていたが、ここでは逆の傾向が見られた。

なお、第２回配信での開封率との相関関係は認められないので、メール通数が少ない層であっても予防接種による訓練・教育から学習することができると言えるであろう。

図表 4-13) 平日１日当たり平均メール通数と第１回配信開封状況

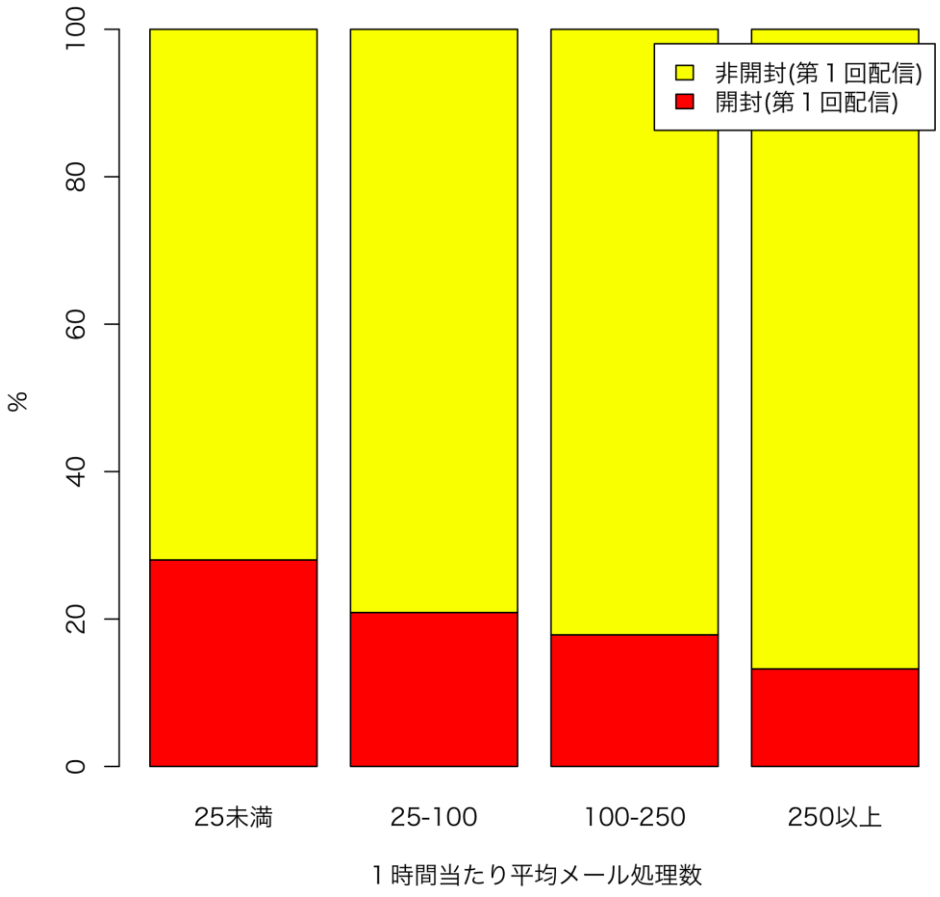


１時間あたりの平均メール処理通数に関しては、この数値が小さい層ほど開封率が高く、大きい層ほど開封率が低いようである。

この属性においても第２回配信での開封率との間には相関関係を認めることができないので、予防接種による学習効果があると言えるであろう。

上述のメール習熟度での「ほとんどできない」層が危険であるという傾向、および、１日当たりの平均メール通数が小さい層が危険であるという傾向と、この１時間あたり平均メール処理通数が小さい層が危険であるという傾向を併せて考えると、メール初心者であまり多くの通数を捌く必要がない層はメールの扱い方を学ぶもしくは慣れることが少ないために危険であると言えるのかもしれない。

図表 4-14) １時間当たり平均メール処理数と第１回配信開封状況

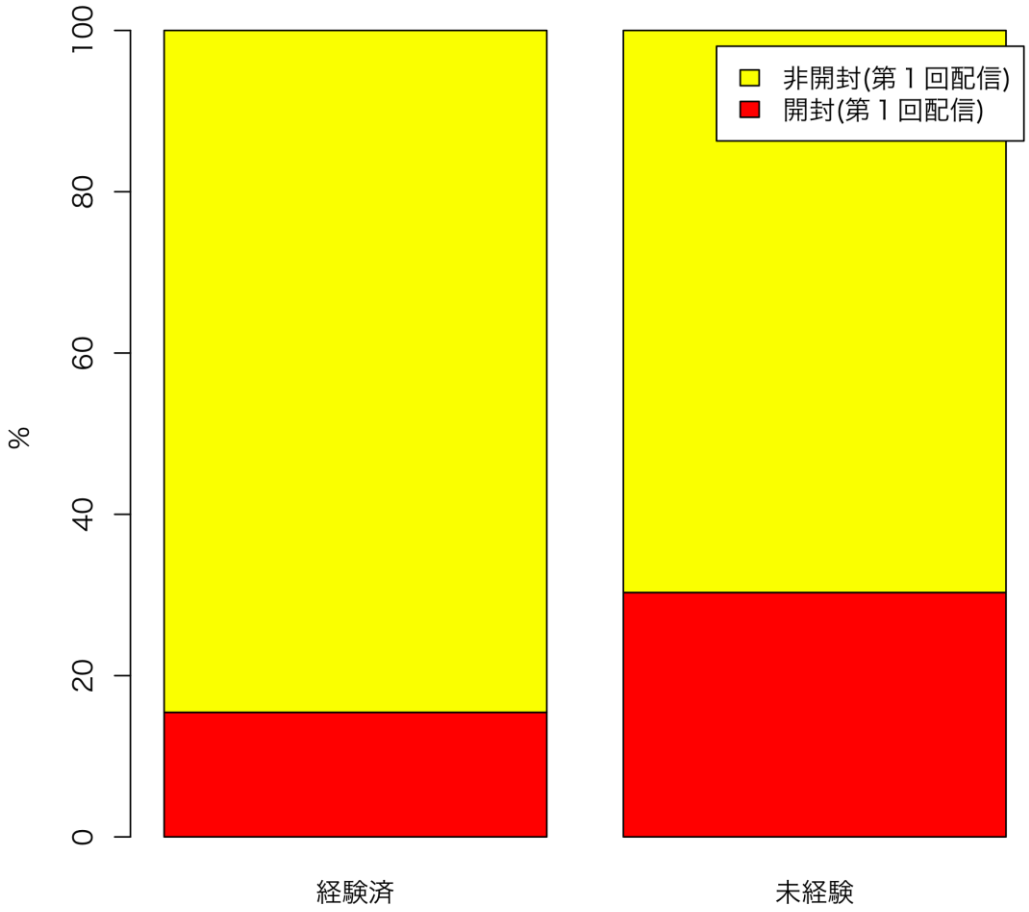


予防接種経験の有無については、経験済のグループで開封率が低く、未経験(今回が初めて)のグループで開封率が高いようである。

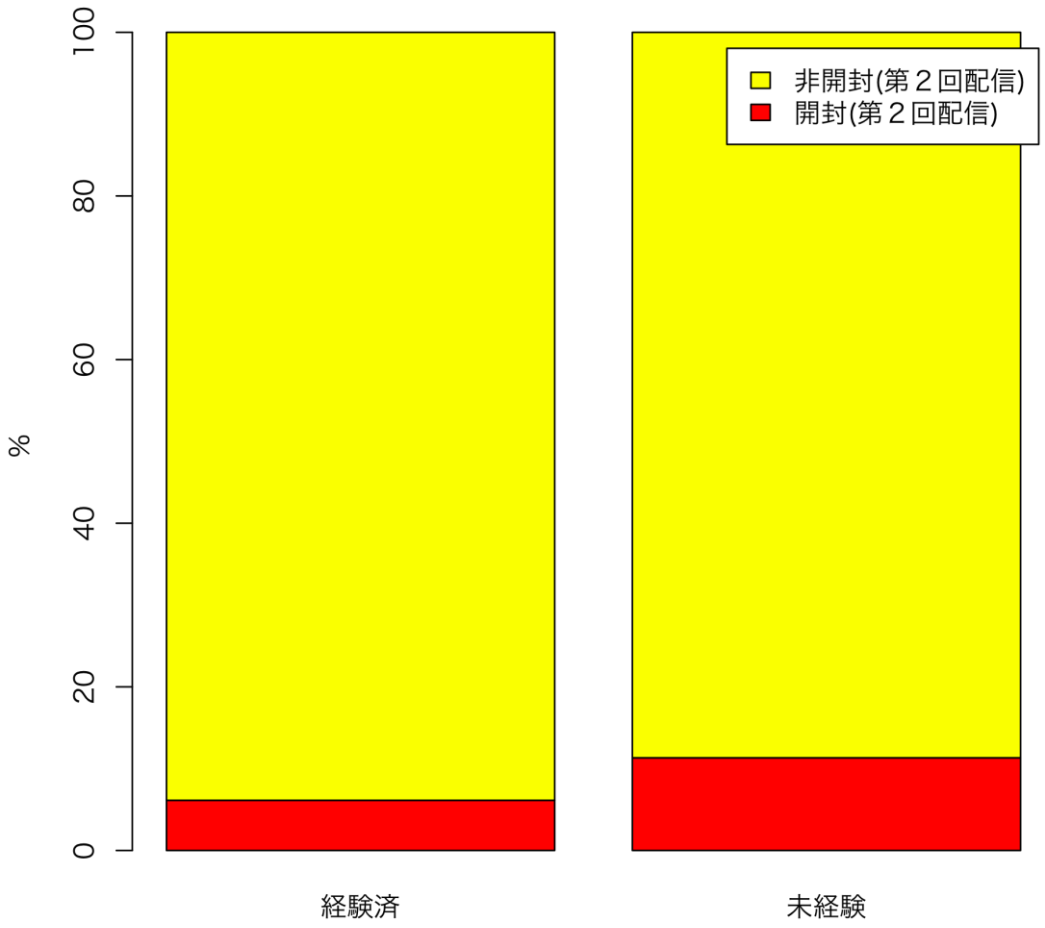
予防接種を経験しているグループはそれだけ教育・訓練を受けているのであるから当然

と言えば当然であるが、予防接種に効果があることの根拠のひとつと言えるであろう。

図表 4-15) 予防接種経験と第 1 回配信開封状況



図表 4-16) 予防接種経験と第２回配信開封状況

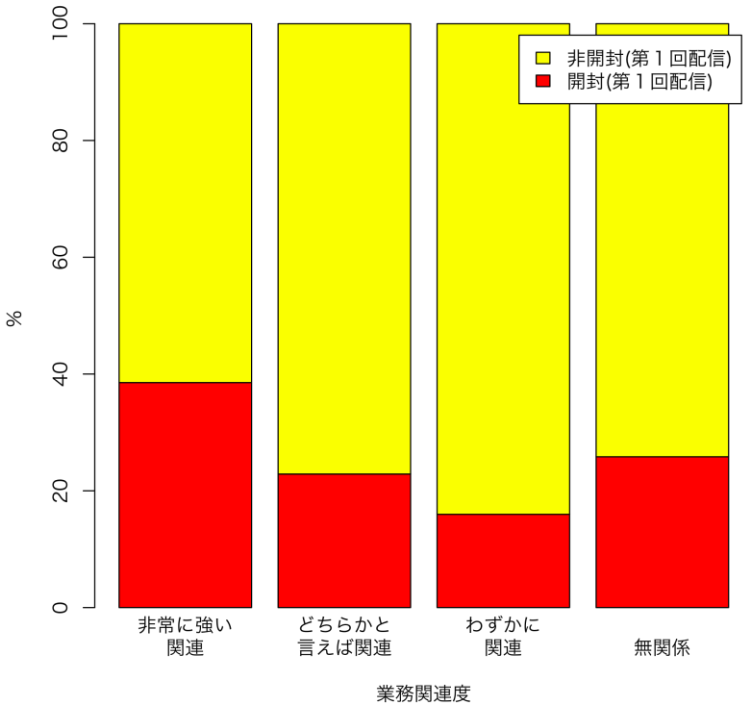


業務関連度に関する相関関係は理解し難い。

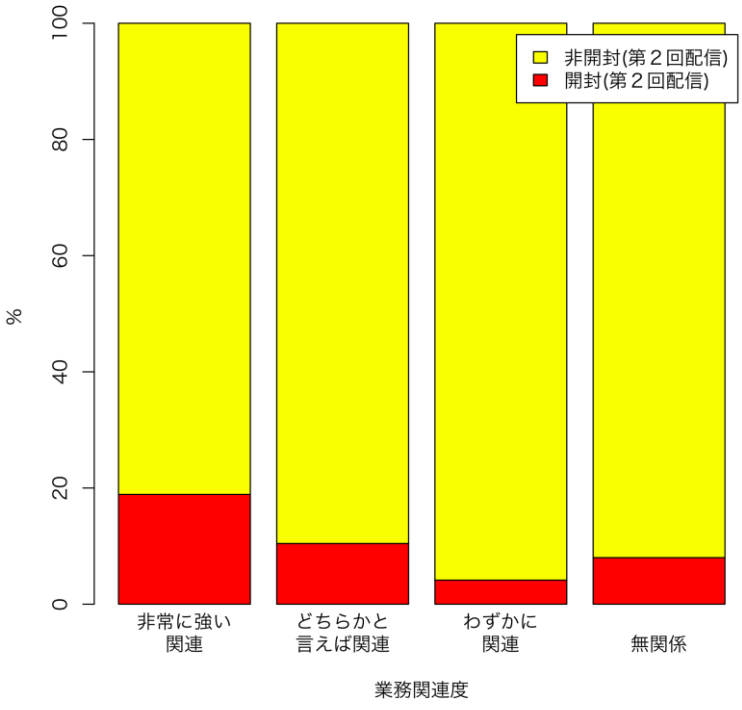
検定の結果から見ると、グループが異なると開封率に統計的に有意な差が出ることは確からしいが、「非常に強い関連がある」と回答したグループと「無関係」と回答したグループで開封率が高く、「どちらかと言えば関連」グループがこれに次ぎ、「わずかに関連」グループが最も低い開封率を示している。

業務関連度と開封率の相関関係については、擬似攻撃メールの種類との相関をも検討するべきかもしれないが、本調査ではややデータ不足のようである。将来の課題としたい。

図表 **4-17) 業務関連度と第１回配信開封状況**



図表 **4-18) 業務関連度と第２回配信開封状況**



4.5　ご感想・ご意見

被験者アンケートのご感想・ご意見の設問には、さまざまなご回答を頂いた。計数したわけではないが、以下のようなものが比較的よく見られた。

1. 予防接種を体験して、標的型メール攻撃の手口への驚きや理解を素直に示すもの
2. ある程度の期間をおいて定期的または反復的に訓練すべきだというもの
3. 予防接種の手法を用いて訓練を行うのであれば、もっと高度な擬似攻撃メールを使うべきだとするもの
4. 業務の妨げとなるので予防接種のようなことはやめてほしいというもの
5. 標的型メール攻撃のメールはスパムなのだから、組織のスパム対策を充実することで被験者の手元まで届かないようにするべきだとするもの

なお、本調査の手法に関係する点だけ指摘しておくならば、本調査ではあまり技術的な知識経験のない層の方々に体験的に学習して頂くことを想定しているので、3.のご意見を頂くようなスキルのある方々には物足りない訓練であったであろうことに異論はない。この程度の擬似攻撃メールでも相当の開封率を示すことを考えれば、現在の予防接種の取り組みが全体的な底上げを意図していることにご了解をいただければ幸いである。

4.のご意見については、誠に申し訳ないことであったと思うが、万一マルウェアに入り込まれた場合の被害の大きさを考えれば、標的型メール攻撃に対する対策は必要である。一方で予防接種実施前の事前研修やフォローアップを丁寧に行うことで業務への影響を減らす工夫も必要である。

5.のご意見については、おそらくは各被験者組織でスパム対策は実施していることと思われるけれども、それをすり抜けてくる標的型攻撃メールを皆無にすることは困難で、したがってこの種の訓練を実施せざるを得ないものとご理解いただければ幸いである。

5 まとめ

本調査による主な発見は次のとおりである。

1. 本調査の第１回配信に比べると、その２週間後の第２回配信の開封率は統計的に有意に低下している。即ち、予防接種手法による学習効果があると言える。
2. 改善率のライフサイクルは、標的型メール攻撃に関する教育・訓練を開始した初期の段階では改善率が中程度となり、教育・訓練が進展するに連れて極大期を迎え、教育・訓練が浸透すると低下していくものと思われる。
   実際に 2008 年度と 2009 年度の改善率を比較すると、統計的に有意な低下を確認することができた。
3. 学習効果率のライフサイクルは、教育・訓練の初期では中程度で、その後増大して 80%以上の状態に高止まりするものと思われる。
   実際に 2008 年度と 2009 年度の学習効果率を比較すると、統計的に有意な変化が存在しないことがわかり、グラフからも上記の傾向を読み取ることができた。
4. 非開封率のライフサイクルは、中程度から徐々に増大して高止まりするものと思われる。
   実際に 2008 年度と 2009 年度の非開封率を比較すると、統計的に有意な増加を確認することができた。
5. 擬似攻撃メール配信時点からの開封状況を時系列で見ると、
   *開封済となる割合(%) = (200/3) * arctan(3 * 配信後経過時間(分)/100)*
   という関係にあることがわかる。
   これは配信後の 30 分間で全開封者のうちの約半数が開封済となるということを示している。
6. 本調査で用いた擬似攻撃メール 6 種類の「強さ」の比較を試みたが、サンプル数の不足から傾向を読み取ることができなかった。今後の課題としたい。
7. 性別・年齢層・職務などの被験者属性は、開封・非開封の別とあまり相関関係がないことがわかった。これは、昨年度の予防接種と同様の傾向を再確認したものと言える。
8. メール習熟度の設問に「ほとんどできない」と回答した被験者は、リスクが高い傾向があった。ただし、自分が擬似攻撃メールの添付ファイルを開封した事実を元にメール習熟度を決定したのかもしれない。
9. 1 日あたりメール通数が少ない被験者ほど、リスクが高い傾向があった。これは本調査の当初の仮説とはちょうど反対の結果であった。

10. 1 時間あたりの平均メール処理通数が小さい被験者ほど、リスクが高い傾向があった。これも当初の仮説とは反対の結果である。
11. 上の 3 点を考慮すると、メール初心者であまり多くのメールを捌く必要のない層は、メールの扱い方を学んだり慣れ親しんだりすることが少ないために標的型メール攻撃に弱いリスクグループとなっている可能性がある。標語的にいえば、「永遠のメール初心者層が危険である」と言えるのではないか。
12. 予防接種経験の有無は、開封率に統計的に有意な違いを示す。すなわち、予防接種の効果はあるということである。
13. 業務関連度が異なると開封率に統計的に有意な差を示し、非常に強い関連を示すかまたは全く無関係である場合にリスクが高い傾向がある。

冒頭に掲げた調査の目的に即して言えば、まず、予防接種手法による標的型メール攻撃耐性獲得の効果は、今年度の 2 回の擬似攻撃メール配信の間においても昨年度と今年度の比較においても、統計的に確認されたと言える。さらに、今年度のリスクグループ仮説については、逆の方向ではあったがリスクグループの抽出ができたと言える。

今後の課題としては、擬似攻撃メール 6 種類の間の「強さ」の違いを検証すること、および、業務関連度と開封率の間の関係を検証することが残された。次の機会があれば、さらなる検証を進めたいものと思う。