JPCERT CC®

2008 年度
IT セキュリティ予防接種実施調査報告書

一般社団法人 JPCERT コーディネーションセンター

2009 年 6 月 19 日

JPCERT CC®

目次

JPCERT CC®

図目次

表目次

リスト目次

1. 調査の背景と目的

1.1. 先行する調査活動

標的型攻撃に関しては、一般社団法人JPCERTコーディネーションセンター(以下JPCERT/CC)が 2006 年度および 2007 年度に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」[1]および「標的型攻撃対策手法に関する調査報告書」[2]として調査報告書を公開している。これらの調査報告書によって、特定少数の被攻撃者に対して、話題を絞り込むなど高度な工夫を施した、標的型メール攻撃が存在し、実際に被害が発生している実態が明らかとなった。他に、IPAが「近年の標的型攻撃に関する調査研究—調査報告書—」[3]で、標的型メール攻撃に利用された脆弱性や手法についてまとめている。

2007 年度の IT セキュリティ予防接種(以下では単に予防接種と呼ぶ)では、比較的小規模な企業・組織を被験者企業として実施し、基本的に教育効果が見られるという結果を得た。他方で、特に抜き打ち実施の場合に被験者側から反発や拒否感が出たこともあった。

今年度の調査研究活動で報告した「2008 年度 標的型メール攻撃に関する事例調査報告書」[4]においても、インタビュー先のセキュリティベンダーから「2008 年 4 月頃からこの攻撃の手口が知れ渡るようになり、模倣犯が登場し攻撃が広がっている印象をうける」との指摘があった。また、同報告書では、このようなソーシャルエンジニアリングの要素を持った攻撃に対しては、ネットワーク境界での既存の技術的対策では不十分であることを指摘した。すなわち、標的型の攻撃は攻撃対象となる個人や組織を少数に限定するだけでなくその内容も個別化されているため、アンチウイルス製品やIPSなどの既存の技術的対策が一般的に必要とする頻度ないし数量の閾値に達しない可能性が高いというものである。

1.2. 目的

2008 年度の予防接種では、前項 1.1 に記載した先行調査を踏まえて、以下のふたつを主要な目的とした。

1. 企業組織を対象にした予防接種を行い、その効果を数値化する。被験者数は延べ 1,000 名以上を目標とする。
2. 対象企業の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考える。

---

1 「標的型攻撃についての調査」(2007 年 3 月公開：2008-09-17 第二版公開)
(http://www.jpcert.or.jp/research/2007/targeted_attack.pdf)

2 「標的型攻撃対策手法に関する調査報告書」(2008 年 8 月公開)
(http://www.jpcert.or.jp/research/#targeted2)

3 「近年の標的型攻撃に関する調査研究—調査報告書—」
(http://www.ipa.go.jp/security/fy19/reports/sequential/index.html)

4 「2008 年度 標的型メール攻撃に関する事例調査報告書」

特に 2.の目的を達するため、個々の被験者や被験者企業に対するアンケート、およびインタビューを実施して、IT セキュリティ予防接種を受けた後の生の感想を調査するように試みた。

2. 実施手法

予防接種の実施手法は、2007 年度のものとほぼ同様である。以下では、まず、今年度の予防接種活動について概要に触れ、さらに今年度の予防接種の実施手法について説明する。

2.1. 調査活動の概要

今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 被験者企業の延べおよそ 2,600 被験者に対して予防接種を行った。被験者企業のリストを表 1 に、また主要なマイルストーンを表 2 に示す。

なお、「被験者企業」については、その多くは一般企業であるが、一部に行政組織・財団法人・有限責任中間法人などを含んでいることに言及しておく。特に許可を頂いた被験者企業については、表中にその組織名を記載した。ここに感謝申し述べる。

また、被験者企業 B および被験者企業 F は昨年度に続いて今年度も被験者企業となっている。前回の予防接種から半年程度の時間が経過しているので、この時間経過の影響がどのように出るかにも注目したい。

表 1 被験者企業リスト

被験者企業呼称	被験者企業の業種など	被験者数
被験者企業 A (横浜市)	地方自治体	428
被験者企業 B (株式会社ブロードバンドセキュリティ)	セキュリティ関連サービスなど	83
被験者企業 C	情報機器販売・システムインテグレーションなど	308
被験者企業 D	セキュリティ関連サービス・コンサルティング	29
被験者企業 E	大手運輸業	70
被験者企業 F (JPCERT/CC)	セキュリティインシデントに関する対策検討・助言・調整など	25
被験者企業 G	大手インターネットサービスプロバイダー	724
被験者企業 H	重要インフラ系システムインテグレータ	49
被験者企業 I (ラックホールディングス株式会社)	情報機器販売・システムインテグレータ・セキュリティサービスなど	280
被験者企業 J	機械製造業	94
被験者企業 K	自動車関連要素技術・システム・部品など	65
被験者企業 L	情報セキュリティサービス・コンサルティング	124

被験者企業 M	エネルギー関連の研究開発	221
被験者企業 N	インターネット証券	103
	合計	2,603

表 2 主要なマイルストーン

年月日	マイルストーン
2008/6/18	予防接種調査開始
2008/8/7	被験者企業 A 第 1 回配信
2008/9/2	被験者企業 A 第 2 回配信
2008/10/2-30	被験者企業の公募(JPCERT/CC web サイト上にて)
2008/10/22	被験者企業 B 第 1 回配信
2008/10/28	被験者企業 C 第 1 回配信
2008/10/28	被験者企業 D 第 1 回配信
2008/11/5	被験者企業 B 第 2 回配信
2008/11/12	被験者企業 C 第 2 回配信
2008/11/12	被験者企業 D 第 2 回配信
2008/11/13	被験者企業 A インタビュー
2008/11/26	被験者企業 E 第 1 回配信
2008/12/5	被験者企業 F 第 1 回配信
2008/12/10	被験者企業 E 第 2 回配信
2008/12/10	被験者企業 G 第 1 回配信
2008/12/10	被験者企業 B インタビュー
2008/12/18	被験者企業 D インタビュー
2008/12/19	被験者企業 F 第 2 回配信
2008/12/24	被験者企業 G 第 2 回配信
2009/1/9	被験者企業 E インタビュー
2009/1/13	被験者企業 H 第 1 回配信
2009/1/13	被験者企業 I 第 1 回配信
2008/1/15	被験者企業 F インタビュー
2009/1/20	被験者企業 J 第 1 回配信
2009/1/20	被験者企業 C インタビュー
2009/1/27	被験者企業 H 第 2 回配信
2009/1/27	被験者企業 I 第 2 回配信
2009/1/28	被験者企業 K 第 1 回配信
2009/1/29	被験者企業 L 第 1 回配信
2009/1/30	被験者企業 M 第 1 階配信
2009/2/2	被験者企業 G インタビュー
2009/2/3	被験者企業 J 第 2 回配信
2009/2/5	被験者企業 N 第 1 回配信

2009/2/12	被験者企業 K 第 2 回配信
2009/2/12	被験者企業 L 第 2 回配信
2009/2/13	被験者企業 M 第 2 回配信
2009/2/13	被験者企業 H インタビュー
2009/2/19	被験者企業 N 第 2 回配信
2009/2/20	被験者企業 J インタビュー
2009/2/25	被験者企業 M インタビュー
2009/3/3	被験者企業 K インタビュー
2009/3/3	被験者企業 N インタビュー
2009/3/6	被験者企業 I インタビュー
2009/3/18	被験者企業 L インタビュー

2.2. 被験者企業の募集と選定

被験者企業の募集に当たっては下記の方法を採った。

1. **昨年度の被験者企業に対する勧誘**
2. **JPCERT/CC の web サイトにおける公募**
3. **知り合い・口コミなどのつながりを使った勧誘**

いずれの場合でも各企業セキュリティ対策全般に取り組む熱意を強く感じたが、重要インフラ関連企業・IT 関連企業に近いほど標的型メール攻撃の脅威について認識した上で予防接種に興味を示し、そうでない被験者企業(候補)ほどどういう脅威であるのかに関心がある傾向があった。

上記 2.の公募では、図 1 に掲げる公募ページを用いた。この公募ページは JPCERT/CC が準備して公開した。

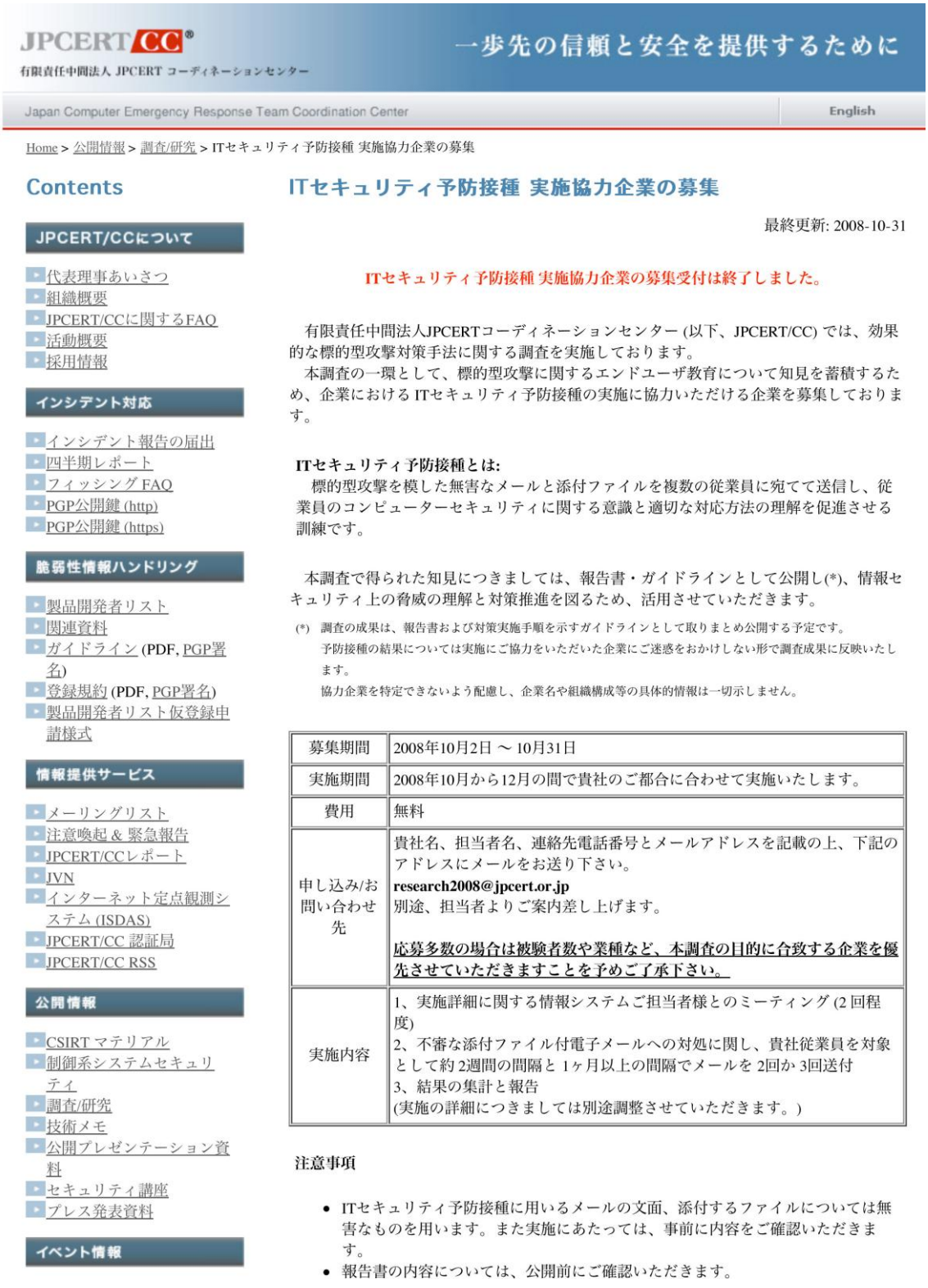
この公募により、表 3 に示す企業から応募があり、応募数・地理的分散・業種や規模のバラエティなどの点で想定していたよりも遙かに多くの応募となった。しかし、作業量と時間の関係で、やむを得ず以下の基準を念頭に置いて取捨選択を行った。

1. **今年度の目標となっている被験者数確保のために、被験者数を多く見込める企業を優先した。**
2. **重要インフラ関連企業が各種の攻撃の対象となっている現実に即して、これらの企業を優先した。**
3. **今年度の運営体制からみて遠隔地の企業に対する十分な調査活動が困難なので、東京近辺の企業を優先した。**

以上の方針によって選定された被験者企業が、先述の表 1 に列挙した 14 被験者企業である。

JPCERT CC®

図 1 JPCERT/CC の web サイトにおける公募ページ



JPCERT CC®
有限責任中間法人 JPCERT コーディネーションセンター
一歩先の信頼と安全を提供するために
Japan Computer Emergency Response Team Coordination Center
English

Home > 公開情報 > 調査/研究 > ITセキュリティ予防接種 実施協力企業の募集

Contents

JPCERT/CCについて
- 代表理事あいさつ
- 組織概要
- JPCERT/CCに関するFAQ
- 活動概要
- 採用情報

インシデント対応
- インシデント報告の届出
- 四半期レポート
- フィッシング FAQ
- PGP公開鍵 (http)
- PGP公開鍵 (https)

脆弱性情報ハンドリング
- 製品開発者リスト
- 関連資料
- ガイドライン (PDF, PGP署名)
- 登録規約 (PDF, PGP署名)
- 製品開発者リスト仮登録申請様式

情報提供サービス
- メーリングリスト
- 注意喚起 & 緊急報告
- JPCERT/CCレポート
- JVN
- インターネット定点観測システム (ISDAS)
- JPCERT/CC 認証局
- JPCERT/CC RSS

公開情報
- CSIRT マテリアル
- 制御系システムセキュリティ
- 調査/研究
- 技術メモ
- 公開プレゼンテーション資料
- セキュリティ講座
- プレス発表資料

イベント情報

ITセキュリティ予防接種 実施協力企業の募集

最終更新: 2008-10-31

ITセキュリティ予防接種 実施協力企業の募集受付は終了しました。

有限責任中間法人JPCERTコーディネーションセンター (以下、JPCERT/CC) では、効果的な標的型攻撃対策手法に関する調査を実施しております。
本調査の一環として、標的型攻撃に関するエンドユーザ教育について知見を蓄積するため、企業における ITセキュリティ予防接種の実施に協力いただける企業を募集しております。

ITセキュリティ予防接種とは:
標的型攻撃を模した無害なメールと添付ファイルを複数の従業員に宛てて送信し、従業員のコンピューターセキュリティに関する意識と適切な対応方法の理解を促進させる訓練です。

本調査で得られた知見につきましては、報告書・ガイドラインとして公開し(*)、情報セキュリティ上の脅威の理解と対策推進を図るため、活用させていただきます。

(*) 調査の成果は、報告書および対策実施手順を示すガイドラインとして取りまとめ公開する予定です。
予防接種の結果については実施にご協力をいただいた企業にご迷惑をおかけしない形で調査成果に反映いたします。
協力企業を特定できないよう配慮し、企業名や組織構成等の具体的情報は一切示しません。

募集期間	2008年10月2日 ～ 10月31日
実施期間	2008年10月から12月の間で貴社のご都合に合わせて実施いたします。
費用	無料
申し込み/お問い合わせ先	貴社名、担当者名、連絡先電話番号とメールアドレスを記載の上、下記のアドレスにメールをお送り下さい。 **research2008@jpcert.or.jp** 別途、担当者よりご案内差し上げます。 **応募多数の場合は被験者数や業種など、本調査の目的に合致する企業を優先させていただきますことを予めご了承下さい。**
実施内容	1、実施詳細に関する情報システムご担当者様とのミーティング (2 回程度) 2、不審な添付ファイル付電子メールへの対処に関し、貴社従業員を対象として約 2週間の間隔と 1ヶ月以上の間隔でメールを 2回か 3回送付 3、結果の集計と報告 (実施の詳細につきましては別途調整させていただきます。)

注意事項

- ITセキュリティ予防接種に用いるメールの文面、添付するファイルについては無害なものを用います。また実施にあたっては、事前に内容をご確認いただきます。
- 報告書の内容については、公開前にご確認いただきます。

表 3 応募企業一覧

No.	被験者数見込み	業種	主要拠点	採用
1	100	運輸	東京都	○
2	100	証券	東京都	○
3	100	製造	東京都	×
4	10	医療サービス	福岡県	×
5	1,600	出版	東京都	×
6	40	SI	東京都	×
7	300	ソフトウェア	東京都	×
8	800	研究開発	東京都	○
9	10	人材派遣	福岡県	×
10	120	IT セキュリティ	東京都	○
11	不明	ソフトウェア	大阪府	×
12	30	ソフトウェア	東京都	×

2.3. 予防接種実施の概要

予防接種は、被験者の集団に対して 2 週間間隔で 2 回の擬似攻撃メール配信を行い、その添付ファイル開封率を測定・比較することで予防接種の効果を見ようというものである。

擬似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。

以上のシナリオをもとに、被験者企業それぞれの事情を勘案しつつ予防接種を実施した。したがって、細部は各被験者企業で異なるが、基本的な実施内容は次の通りである。

1. **窓口となる担当者の決定や機密保持契約(NDA)の締結**
2. **擬似攻撃メールの内容(2 回分)の決定および予行演習の実施**
3. **被験者に対する標的型メール攻撃に関する事前教育**
4. **被験者メールアドレスのリスト授受**
5. **擬似攻撃メールの配信(2 週間間隔で 2 回)**
6. **被験者に対する被験者アンケートの実施**
7. **窓口担当者に対する被験者企業アンケートの実施**
8. **窓口担当者に対する被験者企業インタビューの実施**

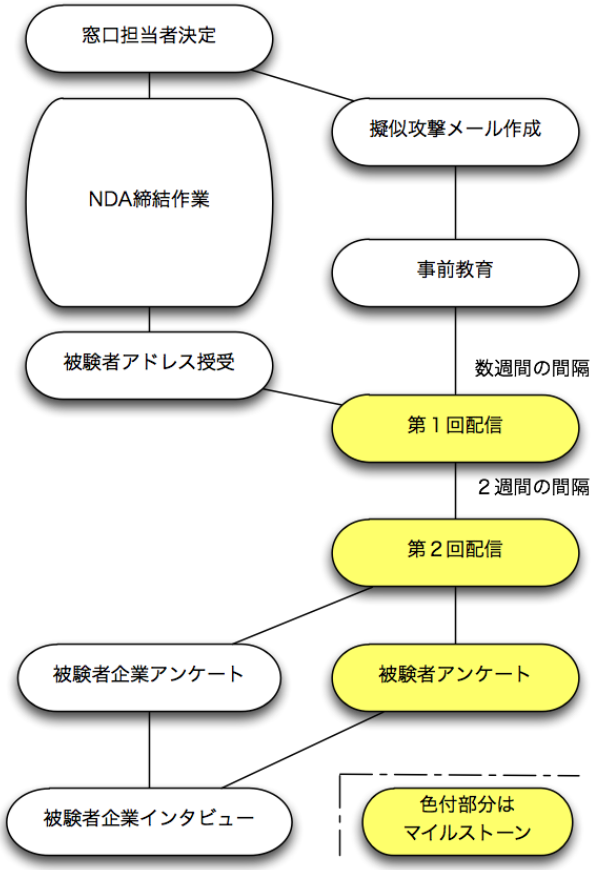
予防接種実施における大まかな流れを図 2 に示した。

被験者のメールアドレスの機密保持のために NDA の締結が必要とされるケースが多く、被験者のメールアドレスの授受は NDA 締結完了を待つ必要がある。

しかし、擬似攻撃メールの作成などは NDA を待つ必要がないので、並行して進めることができた。すなわち、図 2 の左列の NDA 締結作業の完了を待たずに、右列の擬似攻撃メール作成や事前教育の作業を進めることができたので、時間節約にも有効であった。

次項以下に、それぞれの項目について説明する。

図 2 予防接種の大きな流れ



2.4. 立ち上げ事務

予防接種実施の第一歩として、被験者企業側の窓口担当者を決定し、NDA 締結作業を開始した。

窓口担当者には、これ以後の各種事務手続きや被験者企業内の調整の全般をお願いしており、いわば黒子役である。窓口担当者は総務部門・IT 部門・セキュリティ部門など被験者企業毎に所属部門が異なっていた。

ところで、予防接種で配信する擬似攻撃メールは、その名の通り標的型メール攻撃のメールとほとんど同じに見える必要がある。実際の攻撃との唯一の違いは、本物の標的型メール攻撃では添付ファイルを開くとマルウェアが動作を

開始するのに対して、擬似攻撃メールでは web ビーコンが作動するだけで実害はなく、標的型メール攻撃に関する説明と注意喚起などの内容が表示されるだけだという点である。

無用の混乱を避けるとともに法的に自衛するために、被験者企業には、会社として予防接種に参加して擬似攻撃メールの配信を受ける意思決定を、事前にして頂く必要があり、今年度の予防接種でもこの点をまず確認した。

2.5. 擬似攻撃メール作成

擬似攻撃メールの作成に当たっては、昨年度の予防接種報告書にあるサンプルを提示して、被験者企業側とともに本文・差出人(表示名・メールアドレス)・表題・添付ファイルのファイル名・添付ファイルの内容(被験者側の連絡先・特記事項など)を決定した。擬似攻撃メールは 2 回配信するので、各被験者企業に対して 2 回分の異なる擬似攻撃メールを準備した。

擬似攻撃メールの本文は、サンプルのレベルとほぼ同等で、しかも、被験者にとって十分に魅力的であるように努めた。

差出人のメールアドレスは、あらかじめ取得したフリーメールアドレスから適宜選んで用いることとした。したがって、これらのアドレスへのバウンスメールや被験者からの応答が、第三者へ届く可能性は無いと考えられる。この他、特に被験者企業が希望した場合には架空のメールアドレスを使っている。

結局、今年度の予防接種で用いた差出人メールアドレスは、リスト 1 の通りである。

リスト 1 使用した差出人アドレス

```
admin@city.yokobama.jp
censusteam@(フリーメール A)
info-security@mail.jgsecu.jp
moto02501@(フリーメール B)
motok2501@(フリーメール A)
motok2501@(フリーメール C)
office@jpcert.or.jp
qa_staff903@(フリーメール D)
stats_mastor@(フリーメール B)
takasmaster@(フリーメール C)
```

差出人の表示名は、基本的に実在しない個人または組織となるように適宜設定した。これは予防接種実施時に被験者が実在の人物に問い合わせを行うことを防ぐための配慮である。

表題や添付ファイルのファイル名は、本文にあわせて適宜設定した。

添付ファイルの内容としては、原則として昨年度のものを用いたが、被験者企業側の要望に応じて適宜追加修正を加えている。ただし、本物の攻撃だと誤認されないように「訓練であること」を大書し、かつ、被験者企業内の連絡先(多くの場合、窓口担当者とその所属)を明記した。

また、このように準備した擬似攻撃メールを、予行演習として窓口担当者に配信した。これは、次のような意図に基づくものである。

1. **擬似攻撃メール(案)を実際に配信することで、その見え方を被験者と同じ環境で確認する。**
2. **被験者企業側のスパム対策などによって、擬似攻撃メールの配信を拒否される、あるいは、配信が遅れるなどの状況が発生するか否かを確認する。**
3. **配信された擬似攻撃メールの添付ファイルを開封することで、web ビーコンを作動させ、web ビーコンを受信するサーバ側にアクセスログが記録されることを確認する。**

上記の 2.について補足する。予行演習は多数への配信ではないのでスロットリングなどのスパム対策については調べきれない。しかし、文面の特徴などからスパムと判定されて隔離されるか否かなどは確認できる。このような問題が出た場合には、窓口担当者を通じて適切な対策を依頼した。

リスト 2 に、昨年度の予防接種報告書に掲載された擬似攻撃メール本文等のサンプルを再掲する。また、図 3 に添付ファイルの内容を掲げる。

添付ファイルの内容は、以下の点を被験者に伝えることを意図して作成した。

1. **標的型メール攻撃とはどのようなものか**
2. **悪意のある添付ファイルを開くと危険であること**
3. **標的型メール攻撃に対する警戒心を持って欲しいこと**
4. **今回の予防接種の概要と社内の連絡先**

リスト 2 擬似攻撃メールのサンプル集

■サンプル(1)

送信元： ●● <questionable.sender@example.com>
表題： 回覧：マスコミ取材対応方針について

携帯電話コンテンツに関するマスコミ取材への対応方針についてです。添付を参照してください。

添付ファイル名： マスコミ対応方針.doc

■サンプル(2)

送信元： ●● <questionable.sender@example.com>
表題： ご参考：●●セミナー2007 聴講者アンケート回答

各位 ●月●日の●●セミナー2007 での講演聴講者のアンケート回答をまとめたもの

です。

添付ファイル名：　集計結果.doc

■サンプル(3)

送信元：　●●　<questionable.sender@example.com>
表題：　　社内アンケートに関するご協力のお願い

各位

新規事業に関する検討の一環としてウェブメールの活用状況に関して社内アンケート調査を行います。

添付のファイルにご記入の上、●月●日(●)15 時までにご回答ください。お忙しいところ恐縮ですが、ご協力をお願いいたします。

添付ファイル名：　アンケート票.doc

■サンプル(4-1)

送信元：　●●　<questionable.sender@example.com>
表題：　　オンラインセミナー講師協力について

添付資料にあるように「最新ウェブ・テクノロジーに関するオンラインセミナー」に社内からも講師として協力します。講座内容および候補日を示しますので皆さんも検討をお願いいたします。

受講者としての参加も若干名を受け付けますので御相談ください。

以上宜しくお願い致します。

＃既に連絡を受けているようでしたら重複をお許しください。

添付ファイル名：　講師依頼(●●様).doc

■サンプル(4-2)

送信元：　●●　<questionable.sender@example.com>
表題：　　個人情報保護セミナー参加者の募集

各位

添付資料にあるように個人情報保護関連のセミナーを数社から協力をいただいて実施することとなりました。受講希望者は御相談ください。

以上宜しくお願い致します。

＃既に連絡を受けているようでしたら重複をお許しください。

添付ファイル名：　開催概要(●●殿).doc

■サンプル(5)

送信元：　●●　<questionable.sender@example.com>
表題：　　予算計画

皆様、

経営陣からの連絡により、来期の予算計画に関して、添付のようにまとまったとのことですので、添付ファイルを確認頂いて、●●までご連絡頂くようお願いいたします。

--
●●

添付ファイル名：　予算計画.doc

■サンプル(6)

送信元：　●●　<questionable.sender@example.com>
表題：　　セキュリティについて

各位

最近の情報セキュリティに関する脅威について、良くまとまったレポートをみつけたので送ります。参考にしてください。

添付ファイル名：　ウイルス対策.doc

■サンプル(7)

送信元：　●●　<questionable.sender@example.com>
表題：　　先日のテレビ番組出演について

社長の出演した番組をメールに添付しました。
参考までに、閲覧ください。

●●

添付ファイル名：　●●テレビ.doc

■サンプル(8)

送信元：　●●会計事務所　<questionable.sender@example.com>
表題：　　●●事業部の監査結果

●●様、●●様

今期●●事業部の監査結果について
添付ファイルの通りご報告いたします。

添付ファイル名：　●●事業.doc

■サンプル(9)

送信元： ●● <questionable.sender@example.com>
表題： アンケートのご協力

某旅行代理店からの依頼で今年度の消費者の旅行動向についての アンケート調査を実施しています。社員の皆様からも、是非アン ケートにご協力いただきたいので、2，3 日の間でお手すきの際に ご協力ください。旅行の時期、場所、予算、同行人数といった簡 単な内容なので、数分でお答えいただけると思います。よろしく お願いいたします。●●

添付ファイル名： 旅行動向アンケート.doc

■サンプル(10)

送信元： 広報部 <questionable.sender@example.com>
表題： 新サービスについて

事業部長　各位 ●●の新サービスに関するリリースをご確認ください。 --- 広報部 ●●

添付ファイル名： releace.doc

■サンプル(11)

送信元： ●●本部長 <questionable.sender@example.com>
表題： 明日の資料

各事業部門長から提出いただいた内容をベースに、来期事業について まとめた資料です。明日の会議で検討するので、よく目を通しておい てください。 ●●

添付ファイル名： 来期の事業内容(案).doc

■サンプル(12)

送信元： ●●室 <questionable.sender@example.com>
表題： 全社システムのアップデートについて

添付の資料を参照の上、最新のアップデートをお試しください。 新しいプログラムはコンピュータの状態を安定させ、セキュリ ティを向上させます。

添付ファイル名： update.doc

■サンプル(13)

送信元： ●● <questionable.sender@example.com>
表題： 動画コンテンツ視聴アンケート

●●におけるランキングデータです。参考までに、社員に対してもアンケートを実施させていただきたいと思います。お手すきの際に、添付ファイルにリンクがあげられている動画ファイルを閲覧の上、評価してください。

●●

添付ファイル名：動画コンテンツ・ランキング.doc

図 3 添付ファイルの内容

本件に関するお問い合わせ先: ●●部 ●●、●●部 ●●

ご注意！ このような怪しいメールの添付ファイルを不用意に開封すると
あなたを狙うウイルス等に感染する恐れがあります
（このメールは統計調査のためのものです）

本添付ファイルを届けたメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。
調査結果は有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しております。事後のお願いとなりますが、実施にご協力をいただけますよう、何卒よろしくお願い申し上げます。

本添付ファイルに危険性はありません。ウイルス／ワームとしての機能はありません。
添付ファイルを開いた際にインターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示することで、添付ファイルのオープン状況の確認を行なっています。

○不審なメールと添付ファイルがもたらす脅威（標的型攻撃）:
近年、特定の組織・職員を狙う「不審なメールによる攻撃（標的型攻撃）」が増加する傾向にあります。
標的型攻撃の偽メールは、従来のウイルス対策ソフトウェアやスパムフィルタ等を迂回して、あなたのメールボックスまで直接届きます。もっともらしい偽メールの文面・件名に騙されて、添付ファイルを実行してしまうと、ウイルス等への感染や情報漏洩の被害につながります。
被害を避けるためには、各自が不審なメールに対する警戒心を日頃から高めておくことが大切です。

○対処の方法:
怪しげなメールが届いた場合には、標的型攻撃を受けている可能性を疑ってください。騙される前に普段とどこか異なる点や過度に曖昧な点に気づくことができるかもしれません。
怪しげなメールについた添付ファイルの実行や保存は避けてください。

調査実施にご協力いただきありがとうございます

2.6. 擬似攻撃メールにおけるwebビーコン

擬似攻撃メールの内容は上記の通りであるが、本節では、擬似攻撃メールに仕掛けた web ビーコンの仕組みを説明する。

本来の標的型メール攻撃では被攻撃者に添付ファイルを開かせることでマルウェアの作動契機を得ようとするが、擬似攻撃メールではマルウェアではなくweb ビーコンを作動させる。

すなわち、擬似攻撃メールでは、添付ファイルとして用いる Microsoft Word (以下 MS-Word)のファイルに特定の URL へのリンクを入れておくことで、このファイルを開いた時に web サーバ側のアクセスログに記録が残るようにしている。このアクセスログを解析することで、web ビーコンから見た添付ファイルの開封状況がわかる。

なお、対外 HTTP アクセスを禁止している被験者企業では、web ビーコンのアクセスログを収集するための web サーバを被験者企業内に準備する必要があった。また、オフラインの状態で添付ファイルを開いた被験者が居ても、この仕組みでは観測することができないという問題点もある。

web ビーコンの URL は、ディレクトリ部分が各被験者企業と配信回数ごとに異なるように作成し、かつ、被験者ごとに異なるファイル名を用いた。例えば、被験者企業"accompany"に対する第 1 回擬似攻撃メール配信で被験者番号 123 の被験者へ送る添付ファイルには、下に掲げる URL を web ビーコンに用いた。なお、この URL の例のサーバ名と被験者企業名は架空のものである。また、URL 中の下線部分が、被験者企業毎・配信毎・被験者毎に変化する部分である。

http://beaconlogger.example.jp/jpcertcc/inoculation/acompany01/123.bmp

この URL の先には、縦横 1 ピクセルの小さな画像ファイルを置いてあり、この画像が添付ファイルに埋め込まれている。

この web ビーコンの URL を MS-Word のファイルに仕込むために、スクリプト(BeaconSeeder)を用いた。BeaconSeeder は MS-Word 上で動作する Visual Basic for Application (VBA)スクリプトで、MS-Word 2002 で使用した。

BeaconSeeder は、マスターファイルや保存先ディレクトリなどを準備した後、web ビーコンを挿入した添付ファイルを生成する。web ビーコンの挿入は、インライン画像を挿入してその「リンク」を上記の URL とする方法で実現している。

なお、添付ファイルとして用いたMS-Wordのファイルのプロパティを見ることで、ファイル作成者や(ファイルの)表題などを確認することができることがわかっている。これを防ぐために、例えばODPropMan[5]などのツールを用いてプロパティの情報を削除しておく必要がある。

さて、擬似攻撃メールの配信後、web ビーコンのアクセスログを解析することで web ビーコンから見た開封状況を調査し、その結果を表 4 の形式でまとめ

[5] ODPropMan: http://homepage2.nifty.com/f_takasaki/t2_odpropman.html

た。

表 4　web ビーコンの解析結果

	第 1 回	第 2 回
配信日時	yyyy/mm/dd mm.mm	yyyy/mm/dd mm.mm
種明かし	yyyy/mm/dd mm.mm	yyyy/mm/dd mm.mm
被験者数	**名	**名
Web ビーコンへのアクセス総数	**回	*回
開封したと考えられる人数	**名 (**%)	*名 (**%)
2 回とも開封した人	**名 (**%)	

解析の対象とする期間は、擬似攻撃メール配信時点から、種明かしメールの送出または 3 営業日目の終わり [6]のいずれか早い方の時点までとした。

「Web ビーコンへのアクセス総数」は、この期間に被験者企業のものと思われる IP アドレスから送られたアクセスが全部でいくつあったか、である。

「開封したと考えられる人数」は、「Web ビーコンへのアクセス総数」から重複開封や偵察アクセスを除いて「何名の被験者が開封したと思われるか」を数えたものである。

偵察アクセスとは、web ビーコンの存在を看破した被験者が、web ビーコンの URL やリクエストの Method を一部改変して周辺の URL へのアクセスを行うことを指している。上記のような素直な URL を web ビーコンとして用いると偵察アクセスによってアクセスログが汚染されるので、来年度以降の予防接種では、乱数を生成して URL の一部とするなどの推測を難しくする工夫をす必要があると考えられる。

2.7. 事前教育

昨年度の予防接種では、擬似攻撃メールを抜き打ちで配信したために、被験者が感情を害し、第 2 回配信を実施できなくなる例があった。そこで、今年度の予防接種においては、擬似攻撃メール配信より数週間前に以下の内容を被験者に対して周知・注意喚起していただくように窓口担当者にお願いした。

1. **標的型メール攻撃とはどのようなものか**
2. **標的型メール攻撃がここ数年増加傾向にあること**
3. **被験者企業社内においても注意が必要であること**

[6] いくつかの被験者企業で予防接種を実施した結果、早ければ配信後 1 時間程度、遅くとも 1,2 日で開封数が終息することがわかった。そこで、多少の余裕を見て、3 営業日目の終わりまでを区切りとした。

この事前教育によって、次の効果を狙っている。

1. **被験者の反発を避けること**
2. **事前教育の際の説明と 2 回の配信の体験を結びつけることで、被験者に標的型メール攻撃の脅威をより深く体感していただくとともに、ふしんなメールへの対応方法を学んでいただくこと。**

2.8. 被験者のメールアドレスのリスト授受

被験者は、被験者企業の社員(人材派遣や業務委託なども含む)から選定していただいた。これ以外には選定の基準は特に定めなかった。

昨年度はメールアドレスに加えてその被験者の属性(所属部署や年齢層など)を情報収集したが、今年度はメールアドレスだけをお預かりした。

被験者のメールアドレスリストは、擬似攻撃メール配信のために必要であるが、いわゆる個人情報なので取り扱いには注意が必要である。そこで、NDA の締結完了を待って NDA 対象物としてアドレスリストを授受することとした。

また、その送付に際しては、メールで授受する場合には暗号化したり、CD-R などの物理メディアに格納して手渡しで授受するなどの方法で、情報漏洩のないように万全を期した。一部の被験者企業では、個人情報提供と返却の際に確認書類を添付するなど、当該被験者企業の内規に定められた個人情報保護のための手順に従って授受を行った。

さらに、その後の取り扱いにおいても、常時暗号化した状態で保管し、必要な時にのみ復号して利用した。

2.9. 擬似攻撃メールの配信

擬似攻撃メールの準備が整い、被験者のメールアドレスリストを受領すると、擬似攻撃メールの配信の段階となる。

擬似攻撃メール配信は、昨年度に倣って 2 週間間隔で 2 回行うこととし、各回の配信は被験者企業ごとに一斉に行った。その他に以下の諸点に留意した。

1. **事前教育から数週間が経過していること。**
2. **配信はなるべく週の前半に行うこと。これは、被験者が擬似攻撃メールを読むまでの間に休日を挟みたくないからである。**
3. **配信はなるべく 13:00 や 11:00 に行うこと。これは午前中の職務が一段落するタイミングを狙うとともに、その日のうちにある程度の時間を与える意図であった。**

各回の擬似攻撃メール配信の後、タイミングを見計らって窓口担当者から被験者へ種明かしメールを送っていただいた。この内容については次節に記す。

擬似攻撃メールの配信においては、簡単なスクリプト(massmailer.py)を作成して送信サーバ上の MTA(sendmail 8.9.14)へのキューイングツールとして使用した。

massmailer.py は単純な Python スクリプトで、入力となる CSV ファイルから宛先(被験者)の表示名・宛先のメールアドレス・差出人の表示名・差出人のメールアドレス・表題・本文を格納したファイルのファイル名・添付ファイルの実体・添付ファイルのメール添付時の名称を読み取って順次 localhost の SMTP ポートへ送信するものである。

なお、同スクリプトで付与している添付ファイル名はふたつあり、一方は RFC2231 に対応した MUA のためのもの、他方は RFC2231 成立以前に添付ファイル名を扱うために使われていたものである。後者は RFC2046 に違反する。

Outlook 系の MUA が RFC2231 未対応であるため、今年度の予防接種の被験者の一部で、添付ファイルのファイル名を正しく扱えない問題を生じた。当初は RFC2231 形式のもののみを指定していたために Outlook 系 MUA で添付ファイルのファイル名が意図した通りにならず、旧来の形式を追加することで事実上すべての MUA でうまくいくようになった。

リスト 3 に MIME ヘッダの例を示す。6 行目が RFC2231 形式であり、2 行目が旧来の(誤った)方法である。

リスト 3 添付ファイル名の MIME ヘッダ表現

実際の例（ファイル名は「悪い.doc」）

```
1: Content-Type: application/msword;
2:         name="=?iso-2022-jp?b?GyRCMC0kJBsoQi5kb2M=?="
3: MIME-Version: 1.0
4: Content-Transfer-Encoding: base64
5: Content-Disposition: attachment;
6:         filename*=iso-2022-jp'ja'%1B%24B0-%24%24%1B%28B.doc
```

送信側の MTA として、当初は FreeBSD-7.1-Release に同梱された sendmail をそのまま用いていたが、送信時に可能な限り多数の TCP 接続を試みる設定になっていたため、後に SingleThreadDelivery オプションを True に変更した。

2.10. 種明かしメール

種明かしのタイミングについては、被験者の反応によって臨機応変に変更することが求められる。被験者の反応をみるためにはある程度の調査時間が必要であるが、不審に思う被験者があまりにも増えたり、組織において混乱がみられたりした場合などは、想定時刻以前に種明かしを行うことが望ましい。種明かしのメールは、窓口担当者から送付していただいた。この種明かしメールに教育用のコンテンツを追加することも有益であると考えられたので、以下の事項を含めることを推奨した。

1. **今回の擬似攻撃メール配信が、情報セキュリティ対応能力を高めるための訓練を目的として実施した予防接種であること。**
2. **訓練の効果を上げるため、事前説明をしなかったこと。また、予防接種に関する質問に対して即答できない場合があること**
3. **不満や不愉快な感情を与えたとすれば、訓練が目的であるということでご容赦願いたいこと。**
4. **送付した擬似攻撃メールを削除してほしいこと。特に、添付ファイルを開かないで欲しいこと。**

また MS-WORD ファイルを添付する予防接種と混同されぬように、ファイルの添付を控えるか、画像ファイルを添付することとした。

以下のリスト 4およびリスト 5に、種明かしメールのサンプルを示す。また、図 4 に種明かしメールに「標的型攻撃解説.png」として添付した教育用の説明図も併せて示す。

リスト 4 種明かしメールのサンプル(1)

各位

一部の方にはお知らせしたところですが、皆様に宛てて送信されたメール(送信者： questionable.sender@example.com 、表題：社内アンケートに関するご協力のお願い、添付ファイル名：アンケート票.doc、)は情報セキュリティに関する調査のため送信されたものです。有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)からの依頼に基づき、●●の了解のもとで調査を実施いたしました。

調査結果は JPCERT/CC に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しました。メールは JPCERT/CC の方でそれらしいアドレスを作って皆様に送信したものです。今回送付に係る対応状況についての測定を終える旨確認が取れましたので、皆様への説明のため本メールをお送りしています。

事後となりましたが、実施にご協力いただきお礼を申し上げます。ありがとうございました。
不安に思われた方は大変申し訳ありませんでした。

皆様、以下の対応をよろしくお願いします。
・件の表題「社内アンケートに関するご協力のお願い」のメールを削除してく

ださい。
・添付ファイル「アンケート票.doc」は削除してください。

・ご参考のため、標的型攻撃についての解説を添付いたします(PNG 画像形式ファイル)。ご一読ください。

・以下のような点で不審に思った場合には、添付ファイルを開封せずに●●までお問い合わせ下さい。
 - 普段メールをやり取りすることのない人物からのメール
 - 添付ファイルが付いているメール
 (最近の攻撃にはオフィスアプリケーションの未修正の脆弱性を利用するものもあり、word ファイルを開いただけで感染するものもあります。)
 - 中国語フォントが使用されているメール

今後も不定期に同様の調査を行う可能性があります。
また、受信時に気付いた点、今回調査全体についてのコメント等がありましたら、個別にお伺いさせてください。

以上よろしくお願いいたします。

添付ファイル名： 標的型攻撃解説

リスト 5 種明かしメールのサンプル(2)

一部の方にはお知らせしたところですが、実は私の名前で送信された例の「怪しい」メールは情報セキュリティに関する訓練(の試行)として実施されたものです。
●●からの依頼に基づき、◎◎さんの了解のもと実施されていました。

私が問い合わせ先として名前を使われている関係で、私と◎◎さんは承知していましたが、皆さんには事前通知なしで反応を計測するというものでした。先のメールは、●●でそれらしいアドレスを作って送信したものです。

訓練という性質上、ご質問があっても趣旨などをお伝えすることができないことになっていたため、敢えてメールを返信せずにいましたが、先ほど●●の事務局から許可が出たため、本メールをお送りしています。

不安に思っていた方、大変申し訳ありません。

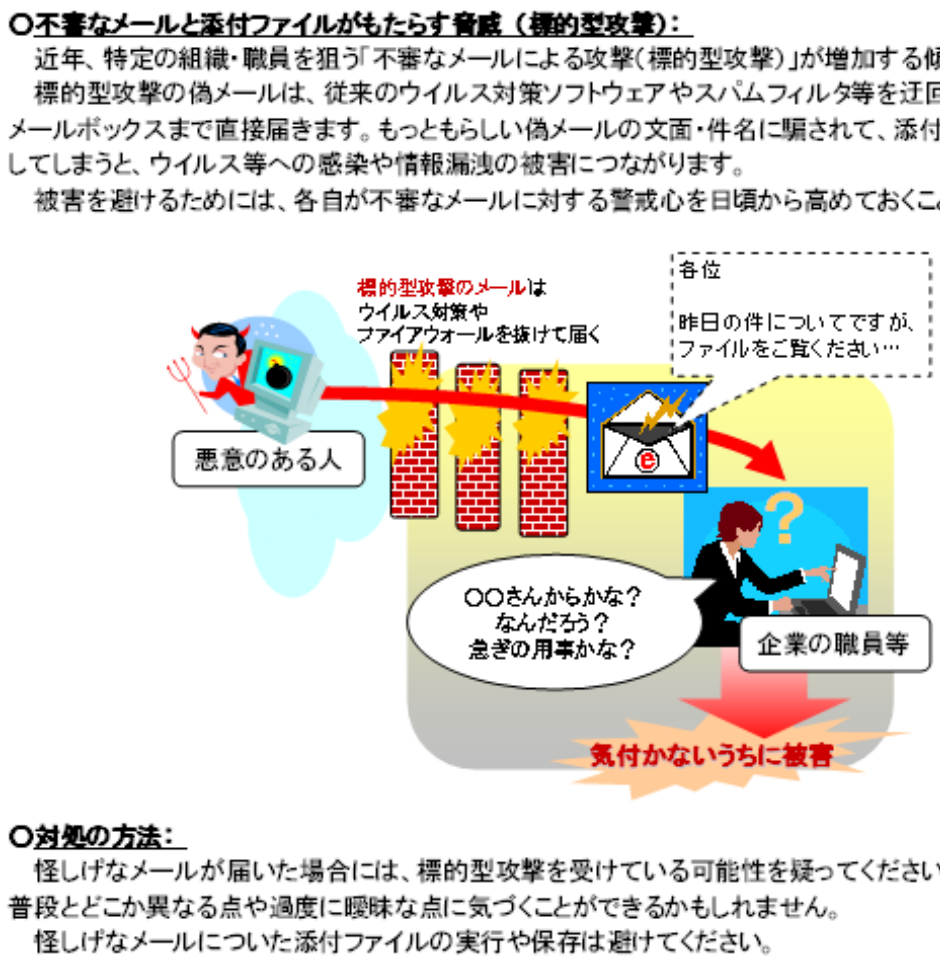
皆様、以下の対応をお願いします。
 ・件の表題「予算計画」のメールを削除してください。

・添付ファイル「予算計画. doc」は開かずに削除してください。

よろしくお願いいたします。

添付ファイル名：　標的型攻撃解説

図 4 種明かしメールに添付した説明図



2. 11. 被験者アンケート

第 2 回擬似攻撃メール配信の後、開封状況が落ち着くのを待って被験者に対するアンケートを実施した。これを被験者アンケートと呼んでいる。

被験者アンケートでは、個々の被験者に対してリスト 6 に掲げる設問内容を問うた。大別すると、被験者個人の属性・社会人としての属性・今回の予防接種での添付ファイル開封状況・PC の取り扱い経験・PC に蓄積されている重要情報の量・今回の予防接種によるセキュリティ意識の変化を尋ねている。

なお、この被験者アンケートに回答することによってどの被験者が添付ファイルを開封したのかがわかると無用の混乱を招きかねないので、匿名での回答

となるように配慮した。
　また、被験者全員からの回答を強制しなかったが、回答率が平均よりも低くなりそうな場合には、適宜、窓口担当者を通じて回答要請を行った。

　被験者にとっては、被験者アンケートに回答することで、標的型メール攻撃について掘り下げて考えることにつながり、ひいてはこの種の攻撃に対する意識付け学習効果も期待される。

　被験者アンケートは、web 上のアンケートシステムか、または、Microsoft Excel(MS-Excel)のファイルを配布することで実施した。

リスト 6 被験者アンケートの設問と選択肢

IT セキュリティ予防接種 被験者アンケート

本調査は企業内電子メール利用者を対象としております。
該当する太枠に X で記入してください。

A) あなた自身についてご回答下さい。
A1) 性別
　a)男性　b)女性
A2) 年齢
　a)20 歳未満　b)20 歳代　c)30 歳代　d)40 歳代
　e)50 歳代　f)60 歳代

B) あなたの所属等についてご回答下さい。
B1) 雇用形態
　a)正社員　b)派遣　c)アルバイト　d)インターン　e)その他
B2) 勤務年数
B2a) 社会人として　　___年___ヶ月
B2b) 現在の勤務先で勤続　___年___ヶ月
B3) あなたの役職をご回答ください。(1 つ選択)
　a)社長・会長・役員クラス　b)執行役員・事業部長クラス
　c)部課長クラス d)係長・主任クラス　e)専門職
　f)一般社員　g)派遣社員　h)業務委託社員
B4) あなたが経験したことのある業務に X をつけ、ご回答ください。
　(該当すべてに X)
　a)総務　b)人事　c)経理　d)企画　e)情報システム管理
　f)情報システム開発　g)営業　h)その他

C) 今回の、予防接種メールについてご回答ください。
C1) 本予防接種実施以前、標的型メール攻撃を知っていましたか

a)もともと知っていた　b)今回知った　c)わからない

C2) 今後あなたやあなたの組織を狙った標的型メール攻撃が行われると思いますか

a)行われると思う　b)行われないと思う　c)わからない

C3) もし、あなたに標的型攻撃と思われるメールがきたとしたら、あなたはどうしますか(該当すべてに X)

a)近くの PC に詳しそうな人に聞く
b)もよりのセキュリティ担当者に連絡する
c)とくに他に連絡せず、メールを削除する
d)何もしない
e)その他

C4) あなたは 1 回目の予防接種メールを

a)メールを見た、添付ファイルを開いた
b)メールを見たが、添付ファイルを開かなかった
c)メールを見ていない

C5) 1 回目の予防接種メールの添付ファイルを開いた場合、開かなかった場合、
それぞれその理由をご回答ください (自由記述)

C6) あなたは 2 回目の予防接種メールを

a)メールを見た、添付ファイルを開いた
b)メールを見たが、添付ファイルを開かなかった
c)メールを見ていない

C7) 2 回目の予防接種メールの添付ファイルを開いた場合、開かなかった場合、
それぞれその理由をご回答ください (自由記述)

D) PC 使用経験についてご回答下さい。

D1) PC使用経験についてご回答ください。　___年

D2) 社内で使用しているメールソフトについてご回答下さい。
(該当すべてに X)

a)Microsoft Outlook　b)Microsoft Outlook Express
c)Thunderbird　d)Eudora　e)LotusNotes　f)サイボウズ
g)WinBiff　h)Shuriken　i)Web メーラー　j)Becky!　k)その他

E) あなたがメールを読み書きするパソコンに、保存されている重要な情報の量について伺います。

E1) メールソフト・アドレス帳ソフト・Excel 表などに蓄積されている連絡先・個人情報など　約___人分

E2) 顧客との契約書など　約___件

E3) 設計情報や社内ノウハウなど、または知財、経営情報　約___件

F) 今回の訓練を経験して
F1) 情報セキュリティ教育を受けたことはありますか?(該当全てに X)
a)現在の会社で受講した
b)(前職などで)受講した経験がある
c)受講経験なし
F2) 今回の実験で、その教育は役に立ったと思いますか？
a)役に立った　b)役に立たなかった　c)わからない
F3) 今後今回の様なメールを受け取った際にはどう行動しますか?
(該当全てに X)
a)管理者に連絡　b)即メールを削除する　c)ウイルスチェックをおこなう
d)近くの同僚に相談する　e)何もしない　f)その他
F4) 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)がどのように変わったでしょうか(自由記述)

G) その他、今回の予防接種訓練の感想を自由にご記述ください(自由記述)

被験者アンケートの回答を集計するにあたって、被験者全体と被験者アンケート回答者の関係や、被験者アンケート回答者の中での分類について、以下の通り整理しておく。(下の図 5 にベン図で示した。)

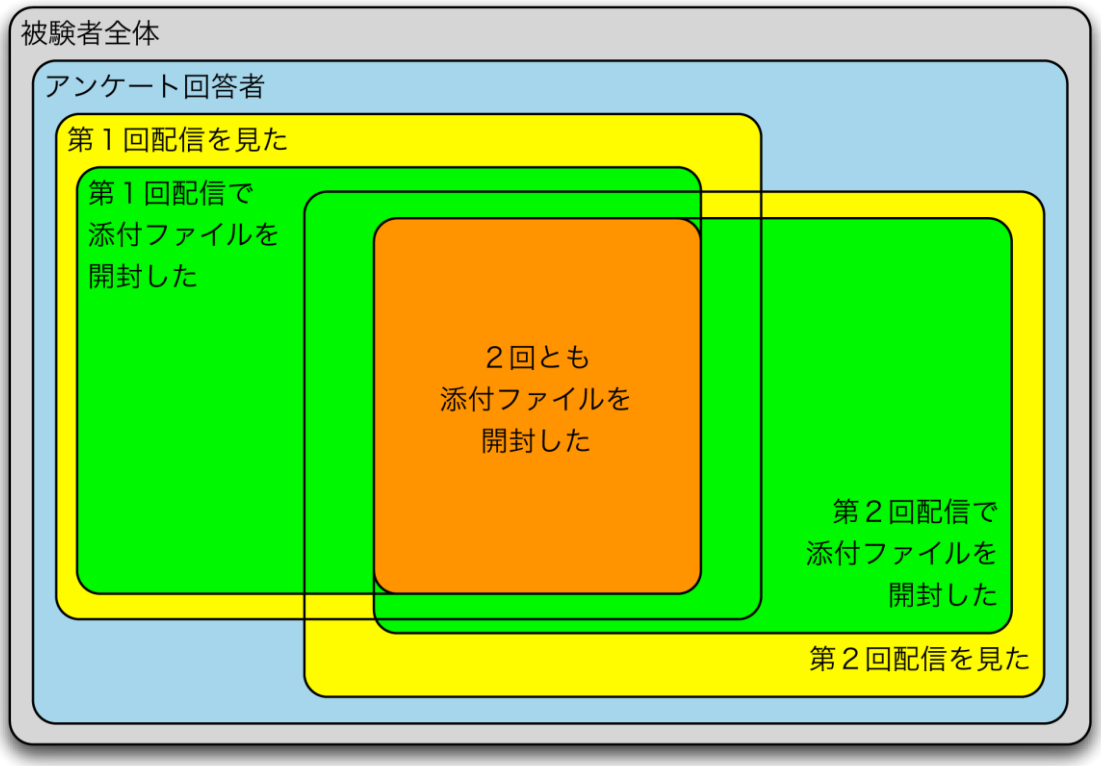
まず、被験者全体のうち、被験者アンケートに回答した者をアンケート回答者としている。

次いで、第 1 回配信と第 2 回配信について擬似攻撃メールが来ていることを認識したか否か(設問 C-4 および C-6)によって、アンケート回答者を分類した。ここでは、「第 1 回配信を見た」グループと「第 2 回配信を見た」グループの論理和に注目して、これを「有効回答者」とする。図中では有効回答者の範囲を黄色に着色した。

さらに、有効回答者の中で、「第 1 回配信で添付ファイルを開封した」グループおよび「第 2 回配信で添付ファイルを開封した」グループの論理和を「開封者」と呼ぶことにする。図中には緑色で上塗りして示した。

この開封者の中には、「2 回とも添付ファイルを開封した」グループが存在する。被験者アンケートの計数では、これに注目して人数を数えた。図中では、オレンジ色を上塗りして示した。

図 5 被験者アンケート回答者の分類



このような分類を踏まえた上で、被験者アンケートから見た添付ファイルの開封状況を調べた。すなわち、「第 1 回配信で添付ファイルを開封した回答者の数」・「第 2 回配信で添付ファイルを開封した回答者の数」・「第 1 回配信および第 2 回配信の両方で添付ファイルを開封した回答者の数」を調査した。

この結果は、表 5 の形式の表にまとめてある。

表 5 被験者アンケートまとめ表

有効回答数	**名	
	第 1 回	第 2 回
開封した人数	**名 (**. *%)	**名 (**. *%)
2 回とも開封した名	**名 (**. *%)	

この他、被験者アンケートの設問のそれぞれについて、グラフを描画して検討を加えた。

さらに、被験者アンケートの設問 C-3 や F-3 を見ると、「被験者企業のセキュリティポリシーでインシデント報告を義務づけている場合に、どの程度の比率の被験者が実際にインシデント報告を行うつもりであるか」がわかる。すなわち、ISO27001 で強調されるようになった「効果の測定」ができるということで

ある。

2.12. 被験者企業アンケート

被験者アンケートでは各被験者にアンケートを取って情報を収集したが、被験者企業の窓口担当者に対してもアンケートを取って被験者企業としての状況を確認した。この被験者企業に関するアンケートを被験者企業アンケートと呼んでいる。

まず、被験者企業アンケートでは、リスト 7 に掲げる内容を問うた。大別すると、被験者企業の属性・セキュリティ管理連絡体制の状況・メール関連の詳細情報・意見感想を訊いている。

被験者企業アンケートは、MS-Excel のファイルを送付することで実施した。

リスト 7 被験者企業アンケートの設問と選択肢

本調査は情報セキュリティの管理者(責任者・担当者)を対象としております。
該当する太枠に X 又は指定の記号でご記入ください。

A) 貴社の基本属性について伺います。
A-1) 貴社の従業員数をご回答下さい。(含む、派遣社員等)
約　　人
A-2) 貴社の拠点数をご回答下さい。(1 つ選択)
a) 1 箇所
b) 2 箇所
c) 3～5 箇所
d) 6～10 箇所
e) 11 箇所以上
A-3) 貴社が属する主要業種をご回答下さい。(1 つ選択)
a) 鉱業
b) 情報通信機械器具製造業
c) その他、製造業
d) 卸売業
e) 小売業
f) 飲食店、宿泊業
g) サービス業
h) 電気・ガス・熱供給・水道業
i) 電気通信業
j) ソフトウェア業
k) 情報処理・提供サービス業
l) インターネット附随サービス業
m) その他、情報通信業
n) 金融・保険業
o) 医療業・福祉業
p) 教育・学習支援業
q) 農林水産業
r) 建設業

s) 運輸業
t) 不動産業
u) 複合サービス事業
v) 政府／官公庁・地方自治体／団体
w) それ以外

A-4) 情報セキュリティ関連予算はありますか。(該当全てにチェック　複数の場合、費用の一番大きいものに○、その他△)
a) ない
b) 情報セキュリティ対策費として計上される
c) 情報システム関連予算の一部として計上される
d) その他予算の一部として計上される
e) 分からない
f) その他

A-5) 情報セキュリティ関連予算の対象をご回答下さい。(該当全てに X)
a) 予算はない
b) セキュリティ対策ハードウェア購入費用
c) セキュリティ対策ソフトウェア購入費用
d) セキュリティ対策ハードウェア保守費用
e) セキュリティ対策ソフトウェア保守費用
f) セキュリティ管理者教育費
g) 従業員教育・啓発活動費
h) セキュリティ関連認証取得費
i) セキュリティ関連認証維持費
k) その他

A-6) 認証取得を計画中の資格に○を、既に取得済の資格に◎をご回答下さい。(該当全てに○又は◎)
a) ISO 27001/ISMS(BS7799)
b) ISO 9000 シリーズ
c) プライバシーマーク
d) BCP(事業継続計画:BS-25999)
e) その他情報セキュリティ関連認証

B) 貴社の情報セキュリティ管理への取組みについて伺います。

B-1) 情報セキュリティに関する規定ついて

B-1-1) 情報セキュリティに関する規定をお持ちですか。(1 つ選択)
a) 持っている
b) 持っていない
c) 作成中
d) わからない

B-1-2) 電子メールに関するセキュリティの規定を
a) 定めている
b) 定めていない

B-1-3) 情報セキュリティに関する規定の運用状況をご回答下さい。(1 つ選択)
a) 改訂のサイクルが定められており、定期的に内容を更新している
b) 改訂に関する取り決めはないが、定期的に内容を更新している
c) 規定が定められてから更新されていない
d) 分からない
e) その他

B-2) 情報セキュリティの責任者、体制、権限について

B-2-1) 情報セキュリティに関わる専門部署がありますか。

a) ある
b) ない

B-2-2) 情報セキュリティ部門の役割はなんですか?(該当全てに X)
a) FW，IDS 等セキュリティ機器の運用
b) セキュリティ教育の企画・実施
c) セキュリティ情報の収集
d) サーバー、ネットワークの運用
e) 全社 PC の導入管理
f) 全社、アプリケーションの導入管理
g) 情報セキュリティ事故関連連絡窓口
h) セキュリティポリシーの策定
i) 社内監査の実施
j) 専門部署はない
k) その他

B-2-3) 貴社全体の情報セキュリティ管理責任者(CSO)は明確になっていますか。
(1 つ選択)
a) 責任者が任命されている
b) 責任者は決まっていない (→3 へお進み下さい)
c) わからない (→3 へお進み下さい)

B-2-4) B-2-3 で、a と回答した方にお聞きします。
貴社全体の情報セキュリティ管理責任者(CSO)の役職をご回答下さい。
(1 つ選択)
a) 取締役クラス
b) 部長クラス
c) 課長クラス
d) その他クラス

B-2-5) B-2-3 で、a と回答した方にお聞きします。
貴社全体の情報セキュリティ管理責任者(CSO)の職務は。(該当全てに X)
a) 専任である
b) CIO と兼任である
c) その他の職務と兼任である

B-3) 情報セキュリティのインシデントの連絡体制について

B-3-1) 組織横断の連絡体制は存在しますか(1 つ選択)
a) 存在しない
b) 各部門に担当者がいる
c) 明確には存在しないが、情報セキュリティ部門が統括している
d) 明確には存在しないが、情報システム部門に連絡する

B-3-2) 脆弱性情報が発表されたり、組織からセキュリティ情報を受け取る際の窓口と社内コーディネーションは
a) 窓口が一元化され、その窓口で問い合わせ対応をする
b) 各部門の裁量で対応する
c) とくに決まっていない

B-3-3) 組織内ないし組織に関係するインシデントが発生した場合の、窓口は
a) 窓口が一元化され、社内に影響する組織に対応を調整する
b) 各部門の裁量で対応する
c) とくに決まっていない

B-3-4) 情報セキュリティ関連事故の連絡体制を全社に周知徹底していますか。
(該当全てに X)

a) 社内向け電子メール・Web システムで告知
b) 情報セキュリティ教育で告知
c) 正社員全員に情報セキュリティのハンドブックを配布
d) 全従業員(派遣、アルバイト、パート含)に情報セキュリティのハンドブックを配布
e) オフィスの壁、掲示板等の目につきやすい場所に管理体制を掲示
f) 分からない
g) その他

B-3-5) 情報セキュリティ関連の事故や事件が発生した場合の連絡体制をご回答下さい。(1 つ選択)
a) 連絡体制が規定されておらず事故・事件の発生を把握する部門がない
b) セキュリティ事故・事件の発生を把握する責任部門はあるが連絡体制が確立していないので機能していない
c) 一部のセキュリティ意識の高い従業員が連絡体制に従った対処をしている
d) 各部門にセキュリティ意識の高い従業員がおり、最終的には責任部門に連絡が来る体制になっている
e) ほぼ全従業員が連絡体制を理解し、セキュリティ関連の事故・事件の情報は責任部門で掌握している
f) 分からない
g) その他

B-4) 情報セキュリティの教育・訓練・注意喚起について

B-4-1) 貴社で実施中の情報セキュリティに関する教育をご回答下さい。(該当全てに X)
a) 未実施
b) 経営者・役員クラスを対象とした情報セキュリティ関連教育
c) 全管理職を対象とした情報セキュリティ関連教育
d) 一部の管理職を対象とした情報セキュリティ関連教育
e) 希望者を対象とした情報セキュリティ関連教育
f) 全社員を対象とした情報セキュリティ関連教育
g) 派遣社員や常駐作業員への情報セキュリティ関連教育
h) 分からない

B-4-2) 情報セキュリティ教育はどのようにおこなっていますか。(該当全てに X)
a) 定期的に全体教育がある(頻度　　月毎)
b) 新入社員や派遣社員などの着任時の研修
c) 所属部署、業務担当異動時の教育
d) E-learning による実施
e) その他

B-4-3) 派遣社員や常駐作業員受入時の配慮点をご回答下さい。(該当全てに X)
a) 特に対策はしていない
b) 情報の取扱いに関する契約(機密保持契約等)締結
c) 情報システム教育の実施
d) 情報セキュリティ教育の実施
e) 分からない
f) その他

B-4-4) 社員の退職時に定めている規定にご回答ください(該当全てに X)
a) 利用アカウントの退職日即時停止と再発行予防
b) 機密情報の確認と廃棄
c) データの保管

d) メールアカウントの引継ぎ期間転送
e) 個人情報の消去
f) その他

B-4-5) 派遣社員、常駐作業員など、勤務者退職時・契約終了時に定めている規定にご回答ください(該当全てに X)
a) 利用アカウントの退職日即時停止と再発行予防
b) 機密情報の確認と廃棄
c) データの保管
d) メールアカウントの引継ぎ期間転送
e) 個人情報の消去
f) その他

B-4-6) 貴社で実施中の情報セキュリティに関する教育の効果確認ついてご回答ください。(該当全てに X)
a) 確認していない
b) 定期的に全社員にチェックテストをおこなっている
c) インシデント演習を行っている
d) その他

C) 貴社のメールシステム構成についてご回答下さい。

C-1) 貴社が保有しているおおよそのメールアカウント数(メーリングリスト、エイリアス等も含む)をご回答ください。
約　　アカウント

C-2) 電子メールサーバーの運用を
a) 自社で実施している
b) アウトソーシングしている
c) ASP メールサービスなどを利用している

C-3) 貴社の電子メールの環境について

C-3-1) 電子メールの読み方で(該当全てに X)
a) メールソフトを指定している
b) Web メーラーを指定している
c) 特に定めていない

C-3-2) クライアント PC でのウイルス対策
a) 実施している
b) 実施していない
c) 分からない

C-3-3) クライアント PC でのスパム対策を
a) 実施している
b) 実施していない
c) 分からない(任意)

C-3-4) メッセージ署名や暗号化(S/MIME・PGP)による、メールの作成者の保障、メールの改ざん防止・秘匿性手法の利用を
a) 規定化している
b) 規定化していない
c) わからない

C-3-5) メッセージ署名や暗号化(S/MIME・PGP)による、メールの作成者の保障、メールの改ざん防止・秘匿性手法を
a) 義務づけている
b) 推奨している
c) 任意

d) 分からない

C-4) 貴社の電子メールのセキュリティ技術対策状況について
C-4-1) 送信ドメイン認証技術(例：SPF/Sender ID/DKIM)を
a) いずれかまたは両方を設定・導入している
b) いずれも設定・導入していない
c) 分からない
C-4-2) メールサーバー及び周辺システム(含む、フィルターASP)側での送受信のウイルス対策を
a) 実施している
b) 実施していない
c) 分からない
C-4-3) メールサーバー及び周辺システム(含む、フィルターASP)側でのでのスパム対策を
a) 実施している
b) 実施していない
c) 分からない(任意)
C-5) 貴社の電子メールの教育について
C-5-1) 電子メールのセキュリティ教育を
a) 実施している
b) 実施していない
c) 分からない
C-5-2) 添付ファイルのパスワード付 ZIP ファイル化を
a) 義務づけている
b) 義務づけていない
c) 分からない
C-5-3) 会社のメールアドレス宛のメールを、社外のメールアカウントへ転送することを
a) 許可している
b) 禁止している
c) 特に定めていない
C-5-4) パスワードの定期的変更を
a) 義務づけている
b) 義務づけていない
c) 分からない
C-6) 電子メールサーバやネットワークシステムの通信監視について
C-6-1) 電子メールサーバのログ (Syslog など)を定期的に解析・監査していますか？(1 つ選択)
a) 解析・監査しており、毎回報告している
b) 解析・監査しているが、変わったことがない限り報告まではしていない
c) ログは蓄積しているが、定期的な解析・監査はしていない
d) ログを蓄積しているか否か不明または蓄積しておらず、解析・監査もしていない
C-6-2) 電子メール利用を監査して、重要情報(顧客情報やクレジットカード番号など)の漏洩を監視していますか？
a) している
b) していない
c) 分からない

万一、マルウェアの侵入を許してしまった場合には、多くのマルウェアが外部ノードと通信して追加的なマルウェアをダウンロードしたり、重要情報を外部へ送ったりします。このような通信には HTTP(S) や IRC などのプロトコルが使われることが多いようです。

C-6-3) 社内から外部への HTTP(S) などの通信のログを取って、定期的に解析・監査していますか？
たとえば HTTP プロクシサーバやネットワークフォレンジック機器などのログがこれに該当します。
a) 解析・監査しており、毎回報告している
b) 解析・監査しているが、変わったことがない限り報告まではしていない
c) ログは蓄積しているが、定期的な解析・監査はしていない
d) ログを蓄積しているか否か不明または蓄積しておらず、解析・監査もしていない

C-6-4) 社内から外部への通信トラフィックを監視して、重要情報(顧客情報やクレジットカード番号など)の漏洩を監視していますか？
a) 監視している
b) 監視していない
c) 分からない

D) 予防接種について感想をご記入ください。あわせて JPCERT/CC への要望等をご記入下さい。(自由記述)

ご協力ありがとうございました。

2.13. 被験者企業インタビュー

被験者企業インタビューでは、以下の項目を実施した。

1. **予防接種の実施結果の報告(web ビーコンから見た開封率など)**
2. **被験者アンケートの集計結果やグラフの報告**
3. **被験者企業アンケートへの回答に関する質疑応答**
4. **予防接種全体に関する質疑応答・意見交換・議論**

被験者企業インタビューは基本的に面会して実施したが、これは被験者企業側の生の声やニュアンスをなるべく汲み取るためである。

3. 被験者企業A

3.1. 被験者企業Aの概要

被験者企業 A は、大規模な地方自治体で、インターネット活用についても比較的早くから取り組み、職員全員が個人単位でインターネットとのやりとりが可能な電子メールアドレスを保有している。

ほとんど全ての拠点がインターネットの利用が可能な庁内ネットワークで接続されており、インターネット利用については、活用を重点として、比較的緩いものとなっている。

表 6 に、被験者企業 A の概要を示す。

表 6 被験者企業 A：概要

業種	地方自治体
設立	N/A
資本金	N/A
所在地	関東地方
拠点数	約 1000
職員数	約 20,000 名
認証	なし

3.2. 被験者企業Aにおける予防接種の概要

下の表 7 に示す日程と規模で、被験者企業 A に対する予防接種を実施した。被験者企業 A での被験者は、管理職および一般職員から構成される 428 名である。

被験者企業 A とその被験者には、以下のような特徴があった。

1. 被験者企業 A では、「横浜市個人情報の保護に関する条例」や一般的なセキュリティポリシーに当たる「横浜市情報セキュリティ管理規程」を制定済みであり、ネットワークの運用管理規程なども既に存在するなど、一通りのルールが整備されている状態である。それゆえ、現状ではプライバシーマークや ISO27001 等の認証を取得していない。
2. 被験者企業 A では、日常的なネットワーク管理を日単位で分担する体制となっており、その管理実務を担当する職員への教育として、運用管理に関わる事やセキュリティの基礎的な事項についての研修を実施している。(後述するが、今回の被験者の全員が、情報セキュリティ教育を受けている。)
3. 前述の情報セキュリティ教育では、標的型メール攻撃についても取り上げており、攻撃者が被攻撃者を研究して被攻撃者に応じた内容

のメールなどで攻撃を仕掛けてくる実態があることを紹介している。

なお、被験者企業 A では、2 種のメールを準備し、被験者をほぼ半数ずつの 2 グループに分けて、擬似攻撃メールの配信の順序を逆にした。擬似攻撃メールの内容については後述するが、擬似攻撃メールを(1)・(2)の順に受け取ったものをグループ A と呼び、(2)・(1)の順に受け取ったものをグループ B と呼んで個別に分析した。

表 7 被験者企業 A：予防接種の実施日時と被験者数

	第 1 回配信	第 2 回配信
配信日時	2008/8/7 16:16	2008/9/2 16:04
種明かし	2008/8/14	2008/9/6
被験者数	428 名	428 名
うち、グループ A の被験者数	215 名	215 名
うち、グループ B の被験者数	213 名	213 名

3.3. 擬似攻撃メールの内容

3.3.1. 擬似攻撃メール(1)

被験者企業 A に配信した擬似攻撃メール(1)をリスト 8 に示した。グループ A には第 1 回配信時に、グループ B には第 2 回配信時に、このメールが配信されたことになる。

擬似攻撃メール(1)では、内部の IT 部門であり、かつ、主に電子メールで利用するネットワークを運用管理している部門から、各職員が利用している PC のセキュリティ対策について注意喚起を行うメールを装った。組織名などについては、容易に調査可能である為、実在の組織名を使用した。

このメールには以下のような気付きのポイントが含まれている。

1. **差出人の表示名を"admin"とした。このような英語表記の表示名は、日本ではあまり利用されず、海外からのスパムの特徴に数えられるほどである。当然、被験者が業務のためにやり取りしているメールと比較すると異質である。**
2. **差出人のメールアドレスを admin@city.yokobama.jp とした。このアドレスのドメインパートは被験者企業 A のドメイン名とよく似ていて誤認混同を誘うものである。また、被験者企業 A では、このアドレスとよく似たアドレスをインターネットのシステム系の問い合わせアドレスとして利用しており、場合によっては送信者などを想起できるものである。**

3. 他に、宛先の個人の名前に対して呼びかけていない点や、差出人の所属・氏名・連絡先を記した署名(シグニチャ)が無い点が、標的型攻撃メールの一般的な特徴に一致する。

リスト 8 被験者企業 A：擬似攻撃メール(1)

From：″admin″ <admin@city.yokobama.jp>
Subject: セキュリティについてのお知らせ

各位
行政運営調整局 IT 活用推進課です。

新たなコンピュータウィルスについての情報とパソコンの設定についての注意をお送りします。最近流行している電子メール感染型のコンピュータウイルス等について注意すべき点を資料としてまとめたものですので、お使いのパソコンについては、設定をご確認いただき、適切な設定としていただきますようお願いいたします。

添付ファイル名： パソコンのセキュリティ設定について.doc

3.3.2. 擬似攻撃メール(2)

被験者企業 A に配信した擬似攻撃メール(2)を下のリスト 9 に示した。グループ A には第 2 回配信時に、グループ B には第 1 回配信時に、このメールが配信されたことになる。

擬似攻撃メール(2)では、架空のセキュリティ団体が、セキュリティについての注意喚起を騙るものとした。多くの被験者にとっては、自らの担当業務に直接には関係のない内容であり、聞きなれないセキュリティ団体(らしきもの)から突然メールが届いたように見えるであろうと思われる。

このメールには以下のような気付きのポイントが含まれている。

1. 差出人の表示名を”Info-Security”とし、メールアドレスを”info-security@mail.jgsecu.jp”とした。このような組織もドメイン名も実在せず、架空の外部組織[7]を騙るものである。
2. 本文中に差出人の氏名・所属・連絡先などを記載していない。(シグニチャがない。)

[7] このドメイン名・組織名について、ドメイン名の登録状況や検索エンジンでの検索結果を調査することで、実在しないであろうことを確認した。これは、被験者がこの擬似攻撃メールを受け取ったときに同様の確認を行って、当該組織へ連絡する可能性を排除するためである。

3. 他に、宛先の個人の名前に対して呼びかけていない点や、差出人の所属・氏名・連絡先を記した署名(シグニチャ)が無い点が、標的型攻撃メールの一般的な特徴に一致する。

リスト 9 被験者企業 A：擬似攻撃メール(2)

From： “Info-Security”<info-security@mail.jgsecu.jp>
Subject:<重要>コンピュータのセキュリティについての注意喚起

自治体ネットワーク関係者様

私ども JGSECu (Japan-Grobal SECurity) は、国内でインターネットなどのセキュリティへ対応することなどをめざして組織された団体です。

主に、ネットワークやコンピュータのセキュリティに関するインシデント(事故)などへの対応を中心に様々な活動を行っております。

インシデントへの対策を行うなかで、セキュリティに関する情報を共有することは、非常に重要です。

私ども JGSECu でも、ネットワーク全体のセキュリティ向上をめざして、積極的な情報提供を行う事としました。

今回は、セキュリティに関係する方々を対象に私たちが発行しているニュースレター等を送らせていただきました。
どうか、セキュリティ向上のため、お役立ていただきたいと思います。

また、あわせて活動内容や各種の取り組み、セキュリティ確保に関連した各種の情報を提供しておりますので、私どもの Web サイトの情報につてもご利用いただければと思います

URL は以下のとおりです。

http://www.jgsecu.or.jp/

それでは、今後ともよろしくお願いいたします。

添付ファイル名： JGSECu ニュース.doc

3.4. Web ビーコンの集計結果

被験者企業 A の添付ファイルの開封状況を、Web ビーコンのアクセスログから見た結果を以下に示す。

前述の通り、被験者企業 A では 2 グループに分けて擬似攻撃メールの配信順序を変えているので、全体の集計に加えてグループ毎の集計を示した。表 8 に被験者企業 A の全体に関する結果を、また、表 9 と表 10 にはそれぞれグループ A とグループ B についての結果を示している。

表 8 被験者企業 A：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2008/8/7 16:16	2008/9/2 16:04
種明かし	2008/8/14	2008/9/6
被験者数	428 名	428 名
Web ビーコンへのアクセス総数	309 回	110 回
開封したと考えられる人数	158 名(36.9%)	109 名(25.5%)
2 回とも開封した人	27 名(6.3%)	

表 9 被験者企業 A(グループ A)：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2008/8/7 16:16	2008/9/2 16:04
種明かし	2008/8/14	2008/9/6
被験者数	215 名	215 名
Web ビーコンへのアクセス総数	246 回	17 回
開封したと考えられる人数	119 名(55.3%)	17 名(7.9%)
2 回とも開封した人	13 名(6.0%)	

表 10 被験者企業 A(グループ B)：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2008/8/7 16:16	2008/9/2 16:04
種明かし	2008/8/14	2008/9/6
被験者数	213 名	213 名
Web ビーコンへのアクセス総数	63 回	92 回
開封したと考えられる人数	39 名(18.3%)	92 名(43.2%)
2 回とも開封した人	14 名(6.6)%	

3.5. Webビーコンログからの時系列開封状況

被験者企業 A での Web ビーコンから見た開封状況を、時系列で見ると以下のようになる。

被験者企業 A では、擬似攻撃メール配信の後の 1 時間ないし 2 時間に開封が集中しており、4 時間ほどでほぼ終息している。また、およそ 16 時間後(翌朝 8 時から 9 時)に開封の第 2 の山があり、その後もおよそ 10 時間にわたって開封が見られる。

他の被験者企業に比べて配信直後の開封の山が比較的なだらかで、また、翌日に第 2 の山が存在する状況からは、次のように推測できる。

1. **被験者企業 A の被験者には即時にメールを見る習慣がなく、各自が自分の勤務の空き時間にメールを読んでいる。**
2. **16:00 に配信された擬似攻撃メールを退庁時間の 17:00 までには確認せず、翌日の出勤時にメールを確認した被験者も多数存在した。**

なお、被験者企業 A における第 1 回配信は盆休みの時期に行われており、配信の後に休日を挟んでいる。

図 6 に、被験者企業 A のグループ A について、擬似攻撃メール配信後 3 日分の開封数を 1 時間刻みのヒストグラムとして示した。図 7 には、グループ B について同様のヒストグラムを示した。

図 8 には、グループ A について、配信後 4 時間分の開封数を 15 分刻みで表示し、図 9 にグループ B について同様のものを示した。

図 6 被験者企業 A(グループ A) : Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

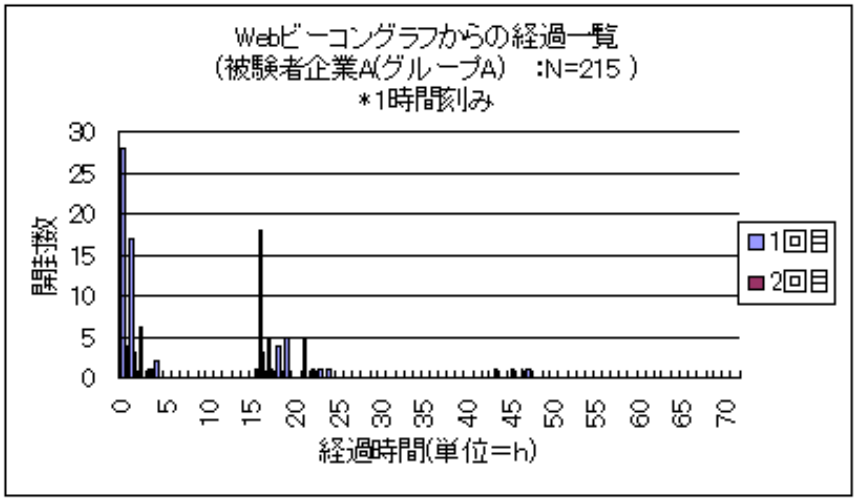


図 7 被験者企業 A(グループ B) : Web ビーコンの時系列開封状況(1 時間刻み 3

日分）

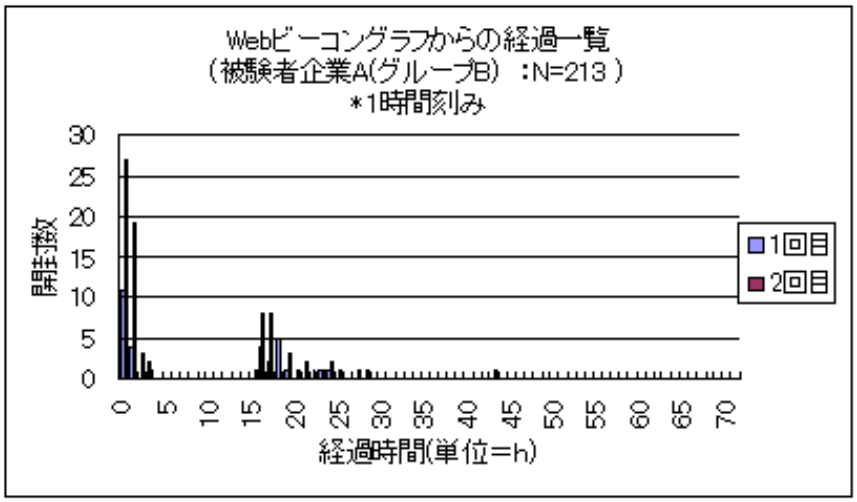


図 8 被験者企業 A(グループ A)：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)

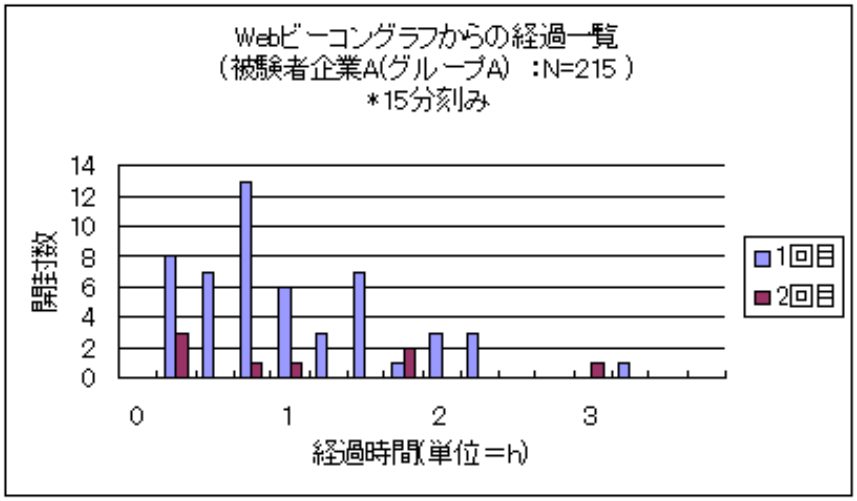
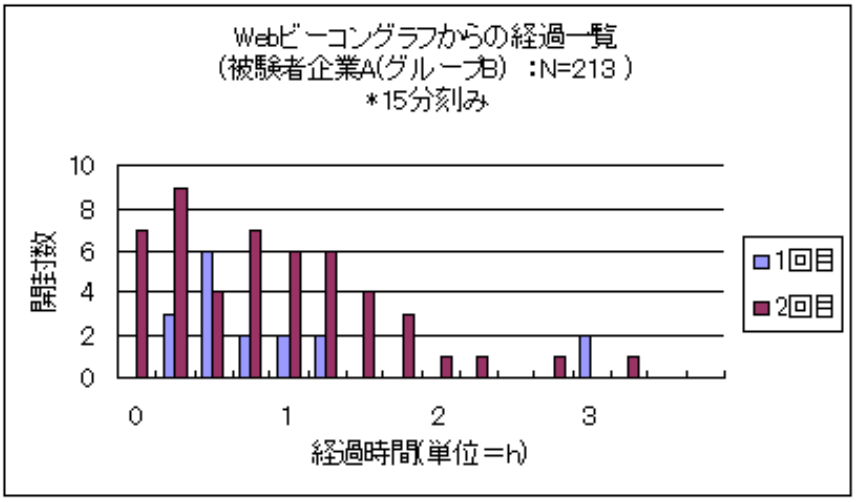


図 9 被験者企業 A(グループ B)：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



3.6. 予防接種実施時の特記事項

3.6.1. 第 1 回配信時の Web ビーコン番号誤記

第 1 回配信に際して、本来であれば Web ビーコン番号を 301 番から 376 番とするべき 76 名の被験者について、103 番から 178 番の Web ビーコンを埋め込んだ擬似攻撃メールを過って送付した。このため、75 名分の Web ビーコンが重複して配信される結果となった。

配信後に窓口担当者と協議した結果、被験者企業 A で用いているソース IP アドレスの割り当てと併せて考えれば、Web ビーコン番号が重複していても区別できるとのことであった。そこで、これら 150 名の被験者についてもデータとして採用している。

3.6.2. 第 2 回配信時の重複配信

第 2 回配信の際に、Web ビーコン番号 1348 番から 1371 番までの 24 名の被験者について、過って同じ擬似攻撃メールを 2 度配信した。これは、送信側のメールサーバでキューに滞留している擬似攻撃メールを見落とした結果、これらのメールが配信されていないものと誤認し、あらためて配信した為である。

同一メールを 2 度受けとったとしても、開封状況にさほどの影響はないものと思われるので、この 24 名の被験者についてもデータを採用した。

3.6.3. 添付ファイルの転送行為

Web ビーコンアクセスログに、同じ Web ビーコン番号を持つ添付ファイルが異なるソース IP アドレスから開封されているものがある。

これは、配信された擬似攻撃メールを見た被験者が、職場の同僚など(被験者

ではない)に擬似攻撃メールを転送して注意喚起や情報共有などを行ったものであることが、被験者に対するヒアリングからわかっている。

被験者が別の端末で二度にわたって擬似攻撃メールの添付ファイルを開封すればこのようなログの状態となるが、被験者企業 A の利用状況からみてその可能性は極めて低い。

3.7. 被験者アンケートの集計

被験者企業 A における被験者アンケートの集計状況について以下に記す。

表 11 被験者企業 A：被験者アンケート回答者の開封状況

有効回答数	302 名	
	第 1 回	第 2 回
開封した人数	114 名 (37.7%)	58 名 (19.2%)
2 回とも開封した人	27 名 (8.9%)	

被験者数 428 名に対し、324 名(75.7%)からアンケート回答があったが、そのうち 22 名が 2 回とも擬似攻撃メールに気づかなかったと回答している。そこで、被験者アンケートの有効回答数を 302 名とする。

表 11 には、被験者アンケート回答者の中で、一度でも添付ファイルを開いたと回答しているものの人数と割合を示した。有効回答中で、添付ファイルを一度でも開封したと答えた被験者は 145 名(48.0%)、このうち第 1 回配信で開封したと答えた被験者は 114 名(37.7%)、第 2 回で開封したと答えた被験者は 58 名(19.4%)、両方を開封したと答えた者は 27 名(8.9%)であった。

次に、グループ A とグループ B のそれぞれの状況を以下に記す。

表 12 被験者企業 A(グループ A)：被験者アンケート回答者の開封状況

有効回答数	136 名	
	第 1 回	第 2 回
開封した人数	73 名 (53.7%)	20 名 (14.7%)
2 回とも開封した人	12 名 (8.8%)	

表 13 被験者企業 A(グループ B)：被験者アンケート回答者の開封状況

有効回答数	117 名	
	第 1 回	第 2 回
開封した人数	27 名 (23.1%)	32 名 (27.4%)
2 回とも開封した人	10 名 (8.5%)	

アンケート有効回答数 302 名の中で、グループ A と判別できる被験者は 136 名(45.0%)であり、グループ B と判別できる被験者は 117 名(38.7%)であった。
なお、49 名(16.2%)についてはグループが不明であったために除いた。このため、グループ A の有効回答数は 136 名、グループ B の有効回答数は 117 名となった。

3.8. 被験者アンケートの分析

本節では、被験者企業 A の被験者アンケートの有効回答の内容から、その特徴となる諸点を示す。

なお、被験者企業 A のアンケート項目については、今回の一連の被験者企業の中で最初に予防接種を実施した組織であるとこから、質問項目が明確に固まっておらず、他の被験者企業での項目と若干異なる部分がある。また、被験者企業 A が地方自治体であることから、企業においては一般的であると考えられる設問についても地方自治体向けに変更したり削除したものがある。
主な相違点は、以下の通りである。

1. 標準被験者アンケートの B-1(雇用形態)にあたる設問は、被験者企業 A 向け被験者アンケートには存在しない。被験者企業 A では、正規職員ではないと業務に利用するメールアドレスは配布されておらず、被験者の全員が正規職員であるからである。
2. 標準被験者アンケートの B-2-a(社会人としての勤続年数)・B-2-b(現在の勤務先での勤続年数)に当たる設問は、被験者企業 A の被験者アンケートでは、Q5(入庁して何年か)・Q6(現在の部署に配属後何年か)となっている。
3. 標準被験者アンケートの B-4(経験職務)に当たる設問は、被験者企業 A の被験者アンケートでは Q7(情報システム部門での勤務経験の有無)となっている。
4. 被験者企業 A の被験者アンケートの Q10 および Q17 は、被験者がグループ A とグループ B のどちらに属するかを知るために追加された設問で、標準被験者アンケートには対応する設問が存在しない。
5. 被験者企業 A の被験者アンケートの Q11 から Q23 までの設問は、標準被験者アンケートの C-4 から C-7 に該当する。ただし、選択肢を選ぶ形式か自由記述形式かが異なっており、所定の問い合わせ先への連絡をしたか否か、また、その理由を記述させるなどの点が相違している。
6. 標準被験者アンケートの設問 E(保有情報数)に該当する設問が、被験者企業 A の被験者アンケートには存在しない。
7. 被験者企業 A の被験者アンケートの Q26(標的型メール攻撃を受けた時に起こりうる被害予想)に該当する設問が、標準被験者アンケー

トには存在しない。

以下では、グループ A とグループ B の対比を中心に、被験者アンケートの回答の特徴を述べることにする。

3.8.1. 添付ファイル開封の有無とその理由

第 1 回配信の際の各グループの添付ファイル開封率を見てみよう。

図 10 にあるように、グループ A では有効回答数 136 名中 73 名(53.7%)が添付ファイルを開封したと回答している。

図 11 にあるように、グループ B では有効回答数 117 名中 27 名(23.1%)が開封したと回答している。

第 1 回配信では、同一被験者企業の中での予防接種であるにも関わらず、擬似攻撃メールの種類によって開封率に 30.6%の差が生じている。

図 10 被験者企業 A(グループ A)：第 1 回配信への対応状況

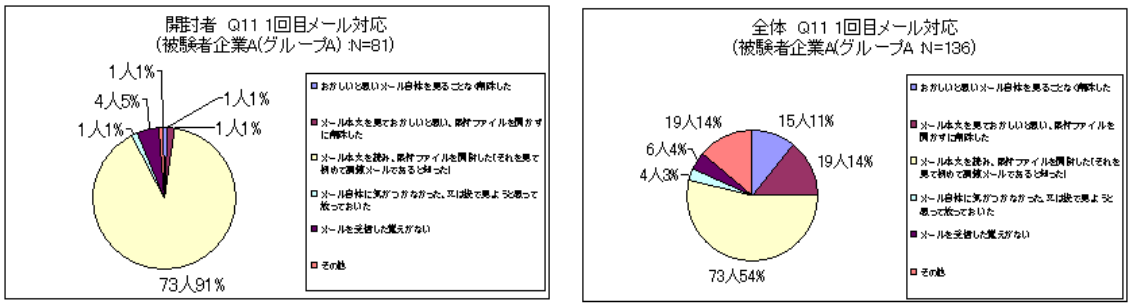
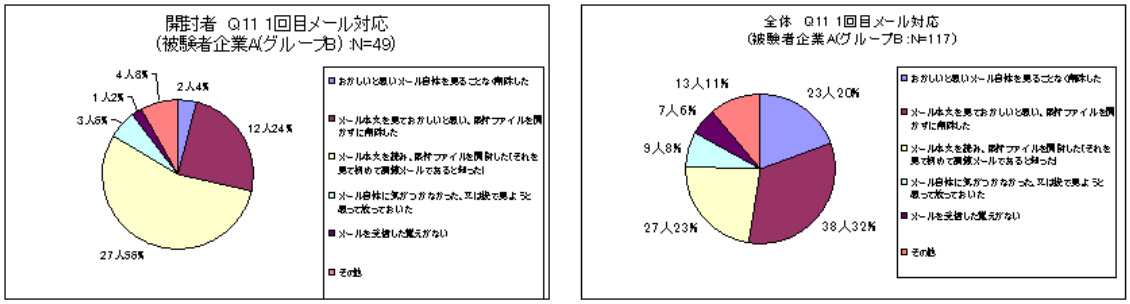
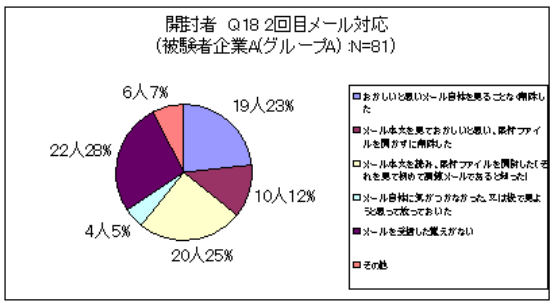


図 11 被験者企業 A(グループ B)：第 1 回配信への対応状況



第 2 回配信では、グループ A は、図 12 にあるように、有効回答数 136 名中 20 名(14.7%)が添付ファイルを開封している。第 1 回配信時と比較すると、開封率で 39.0%減少している。グループ B では、図 13 を見ると、有効回答数 117 名中 32 名(27.4%)が添付ファイルを開封している。第 1 回配信時と比較して、開封率で 4.3%増加している。

図 12 被験者企業 A(グループ A)：第 2 回配信への対応状況



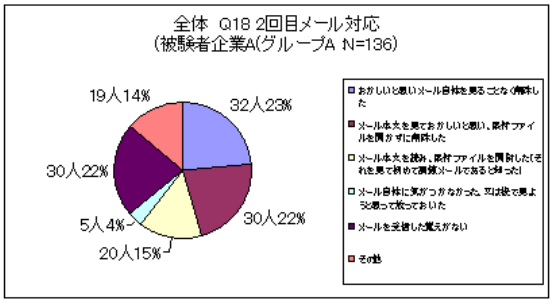
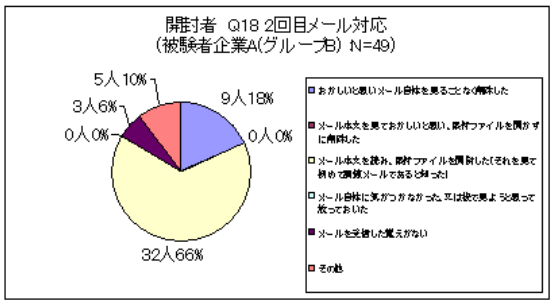
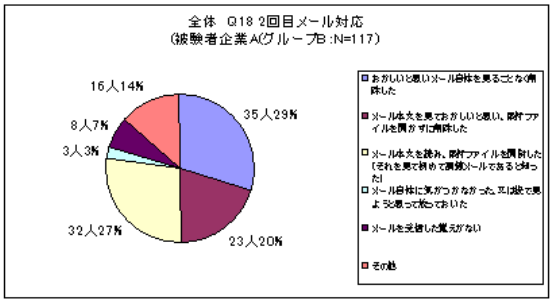


図 13 被験者企業 A(グループ B)：第 2 回配信への対応状況





同一被験者企業でありながら、擬似攻撃メールの開封率に相当の差が出る理由としては、以下のふたつが考えられるので、これらについて結果を分析して原因を調査することとした。

1. 各グループの被験者に、何らかのスキルの差が存在する。
2. 擬似攻撃メールそのものに何らかの差(難易度)が存在する。

。

まず、Web ビーコンから見た開封状況のデータを表 9・表 10 から再掲して、表 14 にまとめた。

表 14 被験者企業 A：Web ビーコンから見た開封率(再掲)

	グループ A	グループ B
擬似攻撃メール(1)を開封	119 名 (55.3%)	93 名 (43.7%)
擬似攻撃メール(2)を開封	17 名 (7.9%)	39 名 (18.3%)
両方を開封	13 名 (6.0%)	14 名 (6.6%)

表 14 によれば、擬似攻撃メール(1)の開封状況は、グループ A では 119 名(55.3%)、グループ B では 93 名(43.7%)となっており、いずれも擬似攻撃メール(2)に対する開封率よりも高い。

しかし、両方を開封した被験者の比率は、グループ A で 13 名(6.0%)、グルー

プ B で 14 名(6.6%)と、大きな違いはないので、グループ A とグループ B の被験者にレベルの差は無いようである。

また、擬似攻撃メール(1)を第 2 回配信で受け取ったグループ B では、第 2 回配信での開封状況は 93 名(43.7%)で、第 2 回だけを開封した被験者が 78 名(36.6%)と、その多くを占める。

これらの傾向から、擬似攻撃メール(1)は、同(2)に比べて見破るのが困難であったと思われる。被験者アンケートの回答(表 12・表 13)から見ても、同様の傾向を読みとることができる。

3.8.2. 添付ファイルを開かなかった理由

被験者アンケートの設問 Q15 と Q22 を使って、添付ファイルを開かなかった理由が、擬似攻撃メール(1)と同(2)でどのように異なるかを検討した。設問 Q15 と Q22 の回答内容について、図 14 と図 15 に示した。

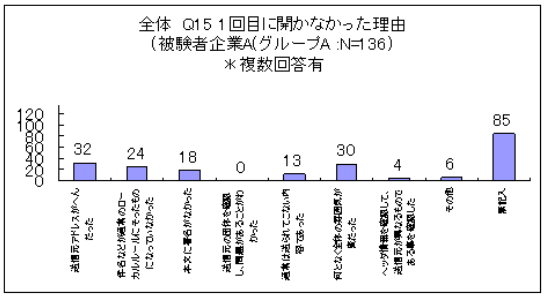
グループ A の Q15 とグループ B の Q22 が、難度の高い擬似攻撃メール(1)に対する判断理由を答えたものであり、グループ A の Q22 とグループ B の Q15 が、難度の低い擬似攻撃メール(2)に対する判断理由を答えたものである。

擬似攻撃メール(2)を受け取った場合には、どちらのグループでも、全体の雰囲気が不審であることと、送信アドレスが不審であることで判断している被験者が多い。

しかし、擬似攻撃メール(1)では、送信アドレスのわずかな違いを指摘している回答が見られるものの数は少ない。

したがって、被験者はまず全体の雰囲気が不審な時には、送信アドレスを確認する傾向にあり、全体として不審だと思わなければ送信アドレスの確認をしない場合が多いと考えられる。

図 14 被験者企業 A(グループ A)：Q15 と Q22 の回答内容



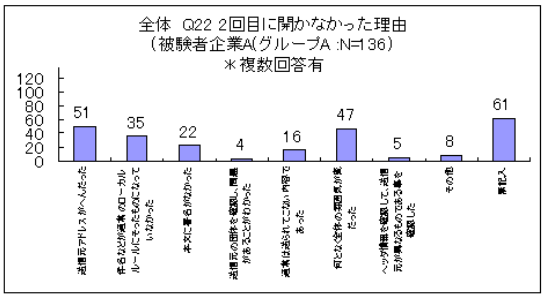
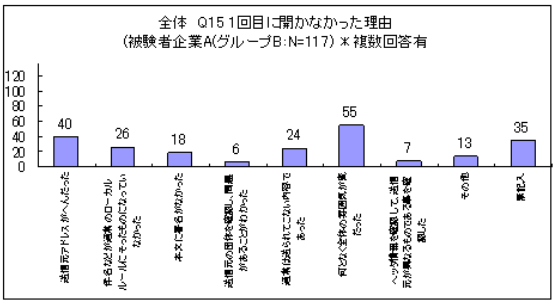
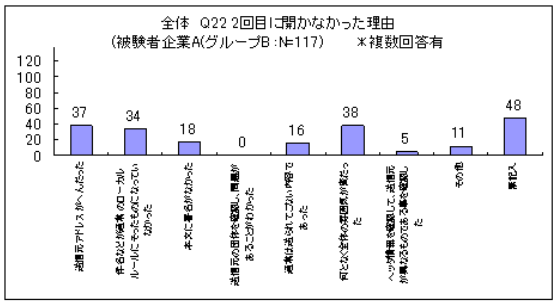


図 15 被験者企業 A(グループ B) : Q15 と Q22 の回答内容





3.8.3. 情報セキュリティ教育の経験

被験者企業 A では、全被験者に対してセキュリティ研修を行っており、その中で標的型メール攻撃についても取り上げている。

しかしながら、被験者アンケートの設問 Q24(標的型攻撃についての研修を受けたことを覚えていたか)に対する回答(図 16)を見ると、「情報セキュリティ教育を受けたが忘れた」と回答した被験者が 115 名(38%)も存在する。

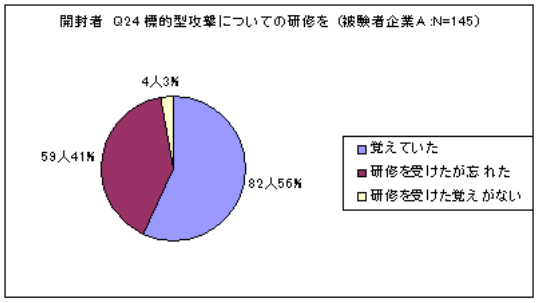
一方、被験者アンケートの設問 Q25(もし標的型攻撃メール攻撃が来たら)に対する回答を見ると、次のようになっている。

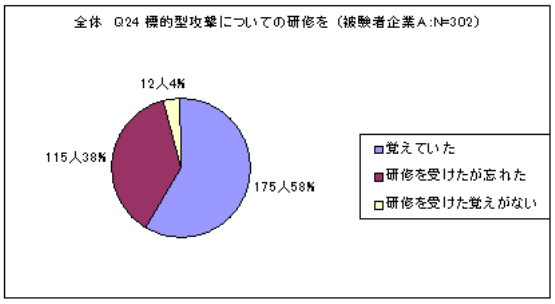
1. およそのものに対処できるという自信がついたと思う(23 名)
2. ある程度見分けがつくものであれば、対処できるようになったと思う(139 名)
3. これまでよりはすこし対処できるようになっていると思う(120 名)
4. 特に変わらないと思う(20 名)
5. これまでより悪くなったと思う(0 名)

何らかの改善があるという意見(a から c まで)の合計が 282 名となっており、全有効回答 302 名中の 93%を占める。

設問 Q25 の結果は、集合研修でその場では習得したと考えられる内容についても、少し時間が経てば忘れてしまうことが十分にあり得ることを示しているといえるだろう。そのような被験者に対して、予防接種を実施することで研修内容を再度認識させ、現実の体験を通してより強く印象づけることができる可能性を示していると考えられる。

図 16 被験者企業 A：Q24 の回答内容





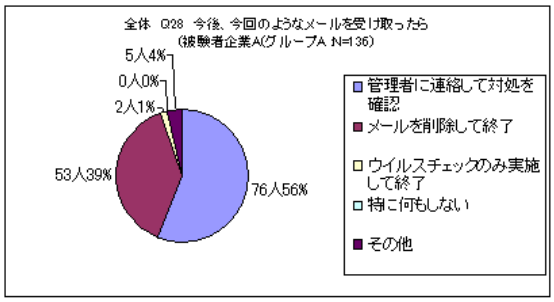
3.8.4. 今後、このようなメールを受け取った場合の対処

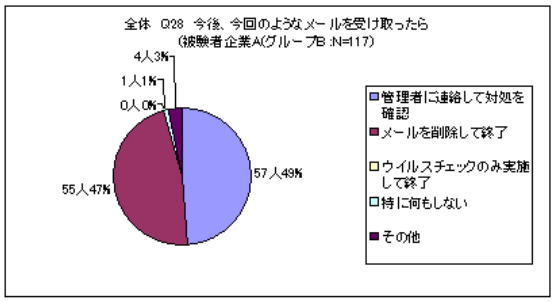
図 17 にあるように、今後に標的型攻撃のメールを受けとった場合の対処方法として、グループ A・グループ B の両方で、約 50%の被験者が、最寄りのセキュリティ担当者に連絡すると答えており、インシデントを報告するという意識があることがわかる。

一方、約 40%の被験者は、連絡せずに(メールを)削除すると回答している。被験者アンケート回答の感想欄には、次のような記述が見られた。

1. **日常的に迷惑メールが多いため、その都度報告していては、受付窓口が忙しくなりすぎるにではないか、と遠慮している。**
2. **迷惑メールだと判断したら、削除するのが習慣化している。**

図 17 被験者企業 A：今後の同種攻撃に対する対応方針





3.8.5. 危機管理意識の変化

被験者アンケートの設問 Q30(危機管理意識の変化)の回答内容を見ると、回答者 221 名中 185 名(83.7%)の被験者が、今回の訓練を通して危機意識を変化させたり、危険を再認識したりしている。

なお、自由記述欄の記述には、メールを開封してしまった(添付ファイルは開封していない)ことについて、自分の不注意を再認識しているものが目立った。

これは、開封してしまった被験者が、研修などを受け一定の責務を与えられているにも関わらずその責を全うできなかったという感覚を持ったり、公務員という責任ある立場に在りながら失敗をしてしまったという感情を持ったりした結果、自分の不注意を再認識するに至ったものと推測している。

また、不審なメールについては、セキュリティインシデント報告窓口への報告が推奨されているが、実務と折り合いがつかない現状について疑問を投げかける記述が見られた。
以下にその内容及び特徴的な記述を抜粋して示す。

1. 現在の職場は、ジャンクメールはほとんどこないが、以前、毎日大量のジャンクメールが来るセクションにいた。メーラーのプレビューは設定しておらず、怪しいメールの添付ファイルは絶対に開けないので、ジャンクメール受信のたびに IT 活用推進に連絡というのも、大げさな感じがする。
2. 普段からメールには気をつけるようにしていましたが、私が配属されている部署は市民からのメールが多く届く部署です。タイトルや様式なども様々で、時には海外からも届きます。その際にどのように注意すれば良いのかが課題だと思っています。(細かく確認後だと、不審メールではなく、本当に市民からの提案等だった場合、迅速性は失われると思う)
3. 危機管理の意識が欠如していることを改めて感じた。1 日のメール受信量が多く、正直読みきれないが、差出人と表題の確認は怠らず、その上で適切な対処を行うよう配慮したいと思う。

3.8.6. 感想

被験者アンケートの設問 Q31 を見ると、回答者 178 名中 129 名(72.5%)の被験者が予防接種を肯定的にとらえ、再実施や方法の工夫を提案している。
また、業務を遂行するにあたって、現在の状況に疑問を感じている記述が見られた。その代表的な意見について以下に抜粋しておく。

1. ヘッダ情報は見るのだが、いまーつ「読み方」が分かっていないので、ヘッダ情報の読み方がわかるようになりたいと思うのですが…。
2. 表題のつけ方などだけでは、見分けがつかない事も多くなりそうなので
3. 自宅において、ウイルス攻撃された経験はあります。この経験より、ウイルスソフトの導入やブラウザを Firefox 等に切り替える等対策をしているつもりですが、職場の管理下にある場合は、自分なりの対策が取れないので、注意力を上げて行くしかないのでしょうか？　OS やオフィスソフト等をマイクロソフトから切り離

すことなどは大きな対策となると思うのですが･･･
4. 個人のスキルでセキュリティレベルを上げることも大切でしょうが･･･
5. 組織のメールルールの徹底をしておかないと、本物も削除され、組織維持そのものに大きな影響を与える。
6. やはりパソコンは、やっかいだと感じ、苦手意識が増大した。
7. 毎日数多くのメールがは送付されてくるが、送る方は関係ない部署まで送っているように見受けられる。送ってしまえば、見ない方が悪いみたいな考えだと思う。この状況では、メールを見る時間だけで一日の相当な時間が割かれてしまうのが現状である。何とかならないのか。改善案は？

3.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 A に対する被験者企業アンケートおよび被験者企業インタビューから、以下の点を読みとることができる。

被験者企業 A では、情報セキュリティポリシーや個人情報保護・ネットワーク運用管理に関わる各種の規程を定めており、一定レベル以上の情報セキュリティ体制を備えているものと判断できる。これらのルールのほとんどは、条例や規程といった職員に対する拘束力の強い形で定められており、遵守していくことが当然に求められている。

また、被験者企業 A は、多数の事務所・事業所や小中学校などが接続された大規模なネットワークを運用している。その運用管理は、いわゆる情報システム担当部署だけでなく、一部は現場の管理職なども含めて実施しているとのことである。

対市民という観点でも、被験者企業 A としては様々な広聴種だｎを備えている中で、電子メールによる問い合わせ受付なども非常に多く、職員はインターネットへいつでもメールを出すことができる環境にある。それゆえ、フリーメールを含む様々なアドレスからの電子メールを受信する機会が多いこともわかった。

3.10. 考察

被験者企業 A では、今回の予防接種の前に管理者向け教育の一環として情報セキュリティ教育を行っていたこともあって、予防接種のような擬似攻撃演習に対して肯定的な受け取り方をしている被験者が多いと考えられる。

被験者アンケートの感想欄には「不審なメールはすぐに削除する習慣にしている」という趣旨の記述が散見されるので、標的型メール攻撃についてセキュリティ研修を行っても、「いつもの迷惑メールの注意」程度に話を聞き流してしまう傾向があるということも考えられる。

また、被験者アンケートでは、標的型メール攻撃についてセキュリティ研修を受けたことを忘れていたと答えた被験者が約 40%いたので、集合研修などについてその効果定着の改善が必要であることがわかると同時に、今回の予防接種がセキュリティ研修のフォローアップになっていたと言える。

さらに、被験者企業 A では、2 種類の擬似攻撃メールの開封率に差が生じた。これは、これらの擬似攻撃メールに何らかの差があったことを示している。この差が何であるのかをはっきりと断定することはできないが、今のところ考えられるのは次のような点である。

1. 差出人が外部の組織を偽装したものであるか、内部の部署を偽装したものであるか。
   今回の擬似攻撃メールでは、内部組織を装ったものの方が開封率が高い。このことから、偽装するのであれば内部組織を装う方が見破りにくいということが考えられる。
2. 差出人のアドレスや気付きのポイントに判別の難易度が合った。
   正確な分析ではないが、差出人のアドレスの見分けが付きにくい(yokohama と yokobama)ことや、本文中に実在の部署が記述されていた事などにより、より見破りにくい擬似攻撃メールとなっていた。

このように何らかの差があるが、よく見ればわかるメールについても、ほんの少しの違いで開封率に大きな差が出ることがわかる。今後の擬似攻撃メール作成においては、このような差が出ることについて十分検討を行う必要がある。

しかし、一度添付ファイルを開封した被験者には、ある程度の「免疫」が生じ、メールアドレスを確認する等の行動の変化が生じた者もいたことから、予防接種自体は効果を生じる取り組みであることも確認できたと言って良いと考えられる。

また、第 1 回目の予防接種に気づいた被験者も、警戒心が必ずしも高まるわけでないないことも発見となった
このような事態に対処するには、例えばメールソフトの側でメールヘッダから逆引きして、不審なドメイン名やメールホストから受け取ったメールに警告表示する機能でもない限り、インターネットのメールの仕組みに詳しくない被験者に気付かせることが難しいことがわかった。しかし、このような機能は、S/MIME や PGP によって技術的に実現されてはいるが、ほとんど普及していないのが実情である。

予防接種には、擬似攻撃メールの詐称をなるべく上手にやって、添付ファイルを極力開かせるようにするアプローチと、気付きのポイントをちりばめてお

いて、ある程度見破ることができるようにするアプローチがある。
被験者企業 A のような行政組織の場合は、公開されている情報が多いので、外部で収集可能な情報で攻撃メールを作ることが容易であろう。であれば、それを前提に、前者のアプローチを採用しても良いかもしれない。
予防接種では、擬似攻撃メールの添付ファイルを開封しないように、メールを細かく注意して見るように習慣づける部分も大切であるが、怪しいメールと気づいた場合にセキュリティ管理者に連絡をする習慣をつけてもらうことも重要である。
標的型メール攻撃を受け取った場合の対処として「すぐにメールを削除する」と回答する被験者が 45%いることは前述のとおりである。
インシデント・ハンドリングの観点からは、「怪しいと思ったらその状態を残しておき、管理者に連絡して指示を仰ぐ」という流れが正しいと考えられる。
しかし、現在の迷惑メールが多い中で管理者に連絡するという行為が、インシデント届出窓口である管理者を忙しくするという現実を前に、それに対する遠慮によって報告を躊躇し、標的型メール攻撃の予兆をつかむ妨げになるとすれば、改善が必要な点であると言える。

被験者企業 A では、各階層にまたがる多くの被験者に配信したことによって、IT リテラシーが高くない被験者からも意見・感想を収集することができた。
その内容を見ると、予防接種は効果的であるものの、予防接種の頻度が増えることに対する被験者の懸念もある。予防接種の実施頻度については慎重に検討しないと、狼少年効果を生んでしまう。また添付ファイルでなく、ただメール本文を開いて読むこと自体を危険なことと意識づけてしまい、少数ではあるが業務上の IT の利用に戸惑いをもつ被験者もいた。

被験者企業 A は地方自治体であり、その特性上市民から送付されてくる様々なアドレスを送信者とする電子メールについて対応しなければならない場合も多い。その中にはフリーメールなどからの送信も含まれるため、そういった場合の対処などについて、より具体的な事前の教育、対応策の徹底などを行う必要があるだろう。
電子メールを特に大量に受信する広聴部門などについては、重点的にその危険を認識する取り組みを進め、必要に応じて、開封専用の環境などを準備することで、防御を固めることも考えられるが、実際にはなかなか困難であることがわかっている。
ネットワークの出入り口で、システム的な対処を進め、一般的な迷惑メールや既知のコンピュータウィルスなどの防御策を確実にするとともに、予防接種のような取り組みを進めていくことは、決定的な効果を生むものではないにせよ、現状を改善することは間違いない。

大規模な組織においては、一律に効果を向上させることはなかなか困難である。また、セキュリティが利便性とのトレードオフという性格を持つものであるとはいえ、電子メールのようなツールの可能性を損なう方向での対策は、や

はり最善の選択肢とは言い難いし、方向としては、制限の最小化を目指すべきであると考えられる。

このような観点から、この予防接種についてさらに効果的・効率的なものとして実現できるよう、検討を進めていくことが求められる結果となったと言って良いだろう。

4. 被験者企業B

4.1. 被験者企業Bの概要

被験者企業 B は、セキュリティ関連サービス・CIX・メール ASP サービス・SI/NI･MSP などを業務とする会社で、3 拠点・社員約 100 名の会社である。被験者企業 B は、プライバシーマークや ISO27001 の認定を受けているので、相応のセキュリティ関連規定を運用しているはずであり、またセキュリティ関連サービスを業務の一環としているので、全般的なセキュリティの意識はある程度高いものと考えられる。

なお、被験者企業 B は、2007 年度 IT セキュリティ予防接種の際にも被験者企業のひとつであった。2007 年度予防接種では社員の一部(総務部門及びセキュリティビジネス部門の 26 名)を対象としたが、2008 年度予防接種ではほぼ全社員を対象とした。

表 15 に、被験者企業 B の概要を記す。

表 15 被験者企業 B：概要

業種	情報通信業
設立	2000 年 11 月 30 日
資本金	3 億 4650 万円
本社所在地	東京
拠点数	3 箇所
社員数	約 100 名
認証	プライバシーマーク(全社)、ISO27001(全社)

4.2. 被験者企業Bにおける予防接種の概要

表 16 に示す日程と規模で被験者企業 B に対する予防接種を実施した。

被験者は、ほぼ全社員の 83 名(派遣社員を含む)で、例外的に経営層および 24 時間監視業務の担当者を除外した。

表 16 被験者企業 B：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2008/10/22 13:00	2008/11/5 13:00
種明かし	2008/10/22 14:00	2008/11/5 17:36
被験者数	83 名	83 名

なお、被験者企業 B では、第 1 回配信の前には特に IT セキュリティ予防接種が行われることを周知していない。

第 1 回配信の後、第 2 回配信までの間に、IT セキュリティ予防接種を実施し

たことの事後通知・標的型メール攻撃の概要説明・標的型メール攻撃についての注意喚起の3点について、窓口担当者から各被験者に電子メールで周知した。

4.3. 擬似攻撃メールの内容

4.3.1. 第1回配信の擬似攻撃メール

第1回配信で用いた擬似攻撃メールをリスト 10 に示した。

このメールはリスト 2 のサンプル(3)を参考にして作成した。本文は、新規事業に関する社内アンケート調査を装うものとし、配信の翌々日を締め切りとして指定することで添付ファイルの開封を急がせるものとなっている。

このメールには以下のような気付きのポイントが含まれている。

1. **差出人の表示名を省略しているので、受信時にメールアドレスが直接表示される。これは、被験者が知っている相手からのメールには見えない。**
2. **差出人のメールアドレスは motok2501@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。**
3. **他は、呼びかけが「各位」となっていて宛先の個人の名前を呼んでいない点や、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。**

リスト 10 被験者企業 B：第1回配信の擬似攻撃メール

From: motok2501@(フリーメール A)
Subject: 社内アンケートに関するご協力のお願い

各位

新規事業に関する検討の一環としてウェブメールの活用状況に関して
社内アンケート調査を行います。

添付のファイルにご記入の上、10 月 24 日(金)15 時までにご回答ください。
お忙しいところ恐縮ですが、ご協力をお願いいたします。

添付ファイル名:アンケート票.doc

4.3.2. 第2回配信の擬似攻撃メール

第2回配信の擬似攻撃メールをリスト 11 に示した。

このメールはリスト 2 のサンプル(2)を参考にして作成した。
実は、予防接種の擬似攻撃メール配信の約 2 ヶ月前に、被験者企業 B は、比較的大規模のセミナーに出展しており、そろそろ聴講者のアンケート集計結果が届いても良い時期であった。恰も、このアンケート集計結果がセミナー主催者から届いたかのように偽装した擬似攻撃メールを用いたのである。ただし、擬似攻撃メールでは、当該セミナーの名称とはよく似ているが異なる名称を用いている。
したがって、この擬似攻撃メールでは、特にセミナーを担当した一部の社員にとって、本物の結果報告と誤認混同することを期待している。また、この種の情報に興味のある被験者の好奇心を刺激し、結果として、添付ファイルを開封することも期待している。

このメールには、以下のような気付きのポイントが含まれている。

1. 1 回目と同様に差出人の表示名を設定せず、メールアドレスが直接表示されるものとした。
2. 差出人のメールアドレスは censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 「Security Solution セミナー2008」というセミナーは架空のものである。
4. 他に、宛先の個人の名前に対して呼びかけていない点や、差出人の所属・氏名・連絡先を記した署名(シグニチャ)が無い点が、標的型攻撃メールの一般的な特徴に一致する。

リスト 11 被験者企業 B：第 2 回配信の擬似攻撃メール

```
From: censusteam@(フリーメール A)
Subject: Security Solution セミナー2008 の聴講者アンケート回答

各位
平成 20 年 10 月 1 日実施の Security Solution セミナー2008 の
講演聴講者のアンケート回答をまとめました。

大変参考になると思いますのでご閲覧下さい。

添付ファイル名:集計結果.doc
```

4.4. Webビーコンの集計結果

被験者企業 B の Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 17 に示す。
Web ビーコンから見た開封率は、第 1 回配信の 20.5%から第 2 回配信の 7.2%

へと改善された。
　また、被験者企業 B では、第 1 回配信時に Web ビーコンのログ収集サーバへの偵察アクセスが多数行われた。これについては後述する。

表 17 被験者企業 B：Web ビーコン集計

	第 1 回	第 2 回
被験者数	83 名	83 名
Web ビーコンへのアクセス総数	121 回	6 回
開封したと考えられる人数	17 名(20.5%)	6 名(7.2%)
2 回とも開封した人	2 名(2.4%)	

4.5. Webビーコンログから見た時系列開封状況

　本節では、被験者企業 B の擬似攻撃メールの添付ファイル開封状況を時系列で概観する。

　図 18 に、第 1 回配信および第 2 回配信について、擬似攻撃メール配信後 3 日分の開封数を 1 時間刻みのヒストグラムとして示した。同様に、図 19 には 15 分刻みの 4 時間分のものを示した。
　被験者企業 B では、ほとんどの開封者が、擬似攻撃メール配信後の約 1 時間に開封していることがわかる。

図 18 被験者企業 B：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

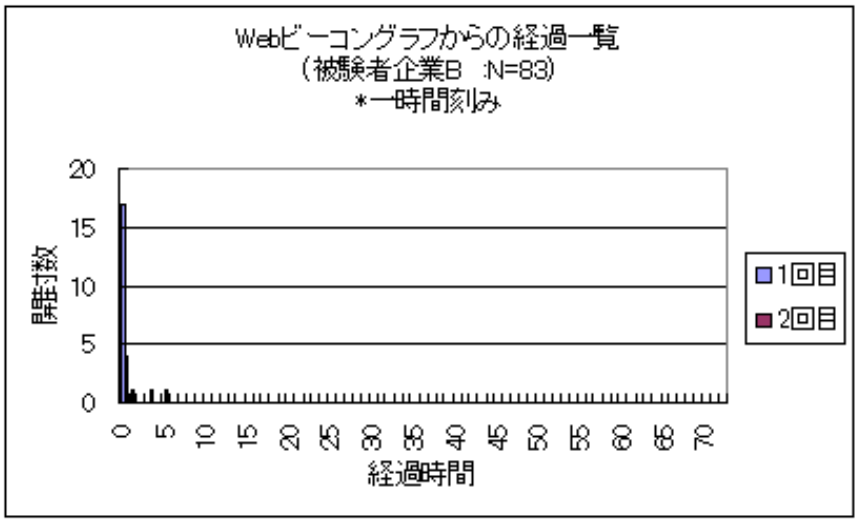
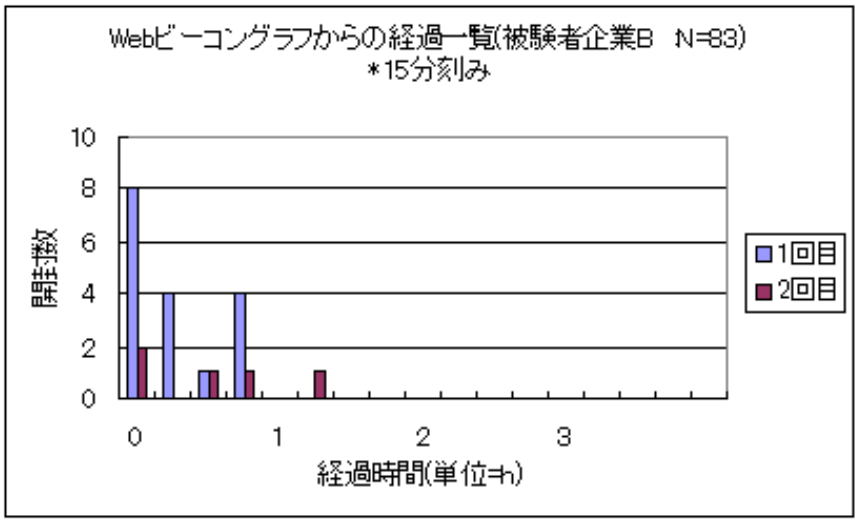


図 19 被験者企業 B：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



4.6. 予防接種実施時の特記事項

4.6.1. 被験者の大声

第 2 回配信の際に、被験者の一人が反射的に「何だこのメール！開けてしまったよ」と大声で叫んだ。

13 時の配信の直後ということもあってオフィスには多数の従業員が居たので、擬似攻撃メールの配信があったことがその場に居た被験者に知れ渡った。

これによって、開封者の数が減ったり、インシデント報告の件数が減ったりといった影響が出たものと思われる。

4.6.2. セキュリティ管理者への報告状況

被験者企業 B では、社内の情報セキュリティ管理責任者が予防接種の窓口担当者を務めたため、擬似攻撃メールを受けとった被験者からのインシデント報告を受ける立場にあり、また、実際に受けている。その記録を窓口担当者から頂くことができたので以下に掲載する。

なお、第 1 回配信では情報セキュリティ管理責任者への報告が行われたが、第 2 回配信では 1 件も報告されなかった。これは、第 2 回配信が第 1 回配信と同工異曲であったために興味の対象にならなかったものと思われる。

リスト 12 被験者企業 B：インシデント報告のリスト

2008/ 10/22 13:00　対象者に対してメール送付開始(訓練開始)
13:00 電子メール技術事業部　不審メール受信の報告あり。開封なし。
13:18 IT サービス事業部　開封の連絡あり。
13:35 電子メール技術事業部　不審メール受信の報告あり。開封なし。

13:40 電子メール技術事業部　不審メール受信の報告あり。開封なし。
13:41 IT サービス事業部　不審メール受信の報告あり。開封なし。
13:47 管理部　不審メール受信の報告あり。開封なし。
13:50 管理部　開封の連絡あり。
13:52 管理部　開封の連絡あり。
13:55 管理部　開封の連絡あり。
14:00 対象者全員に第 1 回配信の種明かしメールを配信。

4.6.3. 偵察アクセス

第 1 回配信時に、総アクセス回数 121 回のうちの 96 回(79.3%)を占めるアクセスが偵察アクセスであった。

第 2 回配信では、複数回開封もなければ、Web サーバへの偵察アクセスも見られなかった。これは、第 1 回配信の際に偵察アクセスを行った被験者であっても、第 2 回配信でも同じパターンなので興味を失ったためであろう。

4.7. 被験者アンケートの集計

被験者企業 B における被験者アンケートの回答から見た添付ファイルの開封状況は以下の通りである。

表 18 被験者企業 B：被験者アンケート回答者の開封状況

有効回答数	42 名	
	第 1 回	第 2 回
開封した人数	10 名 (23.8%)	4 名 (9.5%)
2 回とも開封した人	1 名 (2.4%)	

被験者アンケートでは、被験者数 83 名に対し 44 名(53.0%)から回答があった。そのうち 2 名が 2 回とも擬似攻撃メールに気付かなかったと回答しているので、被験者アンケート有効回答数を 42 名とする。

表 18 に、被験者アンケート回答者の中で一度でも添付ファイルを開いたと回答している者の分布を示した。有効回答の中で一度でも開封した者は 13 名(31.0%)、このうち第 1 回配信で開封した者は 10 名(23.8%)、第 2 回で開封した者は 4 名(9.5%)、両方を開封した者は 1 名(2.4%)であった

前節で Web ビーコンから見た開封率について述べたが、本節のアンケート回答者の開封率と比べてさほどの違いがない。すなわち、第 1 回配信については 20.5%対 23.8%、第 2 回配信では 7.2%対 9.5%である。したがって、開封者の比率という観点から見る限り、被験者アンケートの有効回答の内容は被験者全体の姿をほぼ忠実に反映していると言えよう。Web ビーコンの解析からは開封率

以外の属性を読みとることができないので、以下では被験者アンケートの有効回答の内容が、被験者全体の姿をほぼ忠実に再現しているものと仮定することにする。

4.8. 被験者アンケートの分析

本節では、被験者企業 B の被験者アンケートの有効回答の内容からその特徴となる諸点を示す。

4.8.1. 添付ファイル開封の有無とその理由

ここでは、被験者アンケートから見た開封状況とその理由などを調べる。

図 20 被験者企業 B：被験者アンケートから見た開封状況(第 1 回配信)

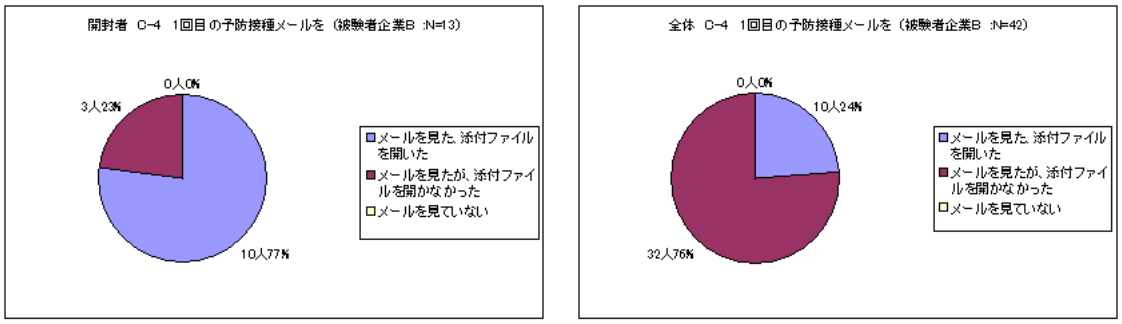


図 20 にあるように、第 1 回配信では有効回答 42 名中の 10 名(23.8%)が添付ファイルを開封したと回答している。被験者アンケートの設問 C-5 に対する回答からその理由を探ると、以下のようなことが読み取れた。

1. **不審なメールだとは思わずに開封した被験者は 4 名である。**
2. **周囲で話題になっていたために好奇心から開封した被験者が 1 名いる。**
3. **2007 年度予防接種の経験者で、同様の演習だと見破った上で開封した被験者が 1 名いる。**
4. **何らかの技術的なチェックをして開封した被験者が 4 名だった。**

なお、技術的なチェックをして開封した 4 名中 3 名が、添付ファイルをある程度は安全だろうと判断した根拠として、差出人のアドレスこそ外部のものだが、送信元は社内の IP アドレスである点を指摘している。

図 21 被験者企業 B：被験者アンケートから見た開封状況(第 2 回配信)

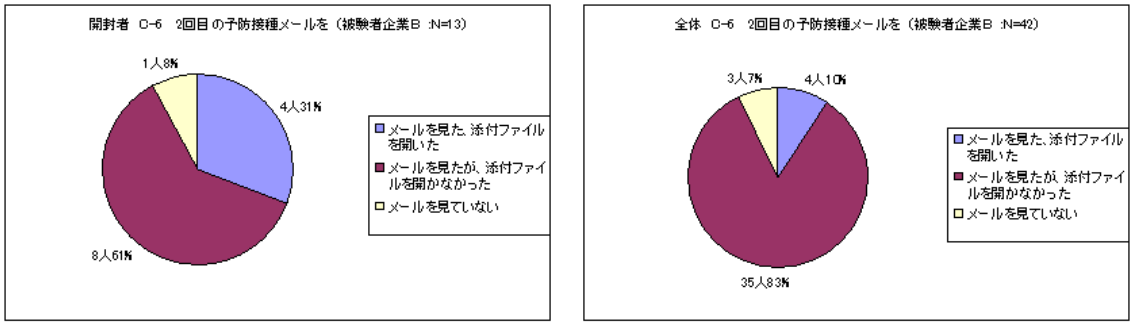


図 21 にあるように、第 2 回配信では有効回答 42 名中の 4 名(9.5%)が添付ファイルを開封したと回答している。被験者アンケートの設問 C-7 に対する回答によれば、その理由は以下の通りであった。

1. **不審なメールだとは思わずに開封した被験者は 2 名である。**
2. **試験だとわかっていて興味本位で開いた被験者が 1 名いる。**
3. **何らかの技術的なチェックをして開封した被験者が 1 名いる。**

次に、被験者アンケートの設問 C-7 に対する回答から、第 1 回配信では添付ファイルを開封した被験者が、どのような理由で第 2 回配信では開封しなかったのかを探った。

このカテゴリに属する被験者のほぼ全員が、差出人の表示名やメールアドレスや、メール本文の内容が本当に自分に関係あるのか否かを注意深く確認した結果、第 2 回配信の際には添付ファイルを開封しなかったということが読み取れた。これは、第 1 回配信とその後の種明かしによる周知・教育の効果ではないかと思われる。

また、第 1 回配信と第 2 回配信の両方で添付ファイルを開封した被験者は 1 名(2%)であったが、この被験者は「メールを見てすぐに訓練のものと気付いたので、Linux 上で Word ファイルを HTML に変換し、マクロウィルス等の感染の危険性がないテキストブラウザ w3m で閲覧した。」(設問 C-5,C-7 に対する回答から)と回答している。

4.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間にどのような関係が読み取れるかについて調べる。

図 22 被験者企業 B：情報セキュリティ教育の経験

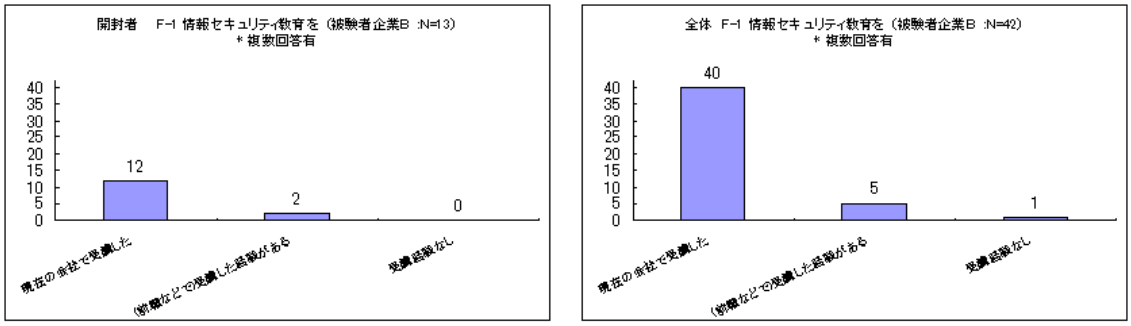
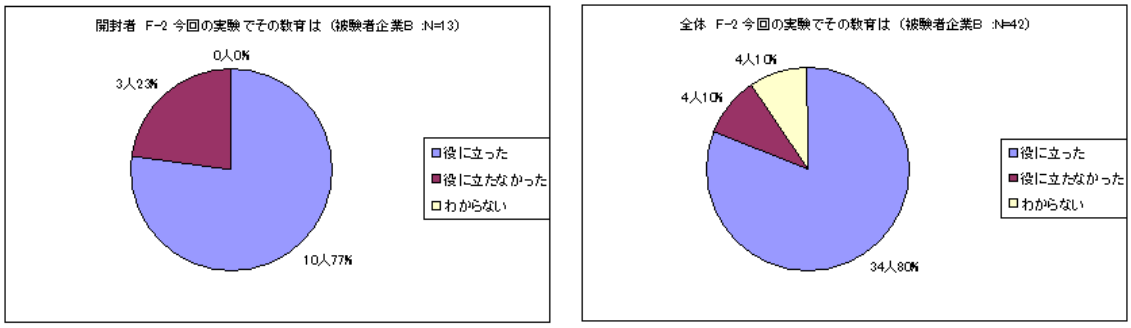


図 22 によれば、被験者全体では、被験者アンケート有効回答者 42 名中の 40 名(95.2%)が現在の勤務先で情報セキュリティ教育を受けていることがわかる。

また、開封者では、現在の勤務先で情報セキュリティ教育を受けた 13 名中の 12 名(92.3%)が第 1 回または第 2 回の擬似攻撃メールの添付ファイルを開封している。

これを見る限りでは、被験者企業 B では、情報セキュリティの教育経験の有無と開封・非開封の別には特筆すべき関係性はみられない。

図 23 被験者企業 B：情報セキュリティ教育の有効性



次に、設問 F-2 に対する回答から、情報セキュリティ教育の有効性を考える。

図 23 にあるように、会社で受けた情報セキュリティ教育が IT セキュリティ予防接種に対して役に立ったと回答している被験者は、有効回答者 42 名中の 34 名(81.0%)であるが、開封者 13 名の中でも 10 名(76.9%)を占めている

両者に大きな差がないことから、個々の被験者の認識の観点でも情報セキュリティ教育が開封率に影響を与えているとはいえない状況である。

なお、開封していながらも、情報セキュリティ教育が役に立ったと回答しているのは矛盾しているようだが、次のような心理ではないかと思われる。

1. 結果的に予防接種の添付ファイルを開封してしまった。
2. しかしながら、開封後の警告メールを読むことによって、過去に受けた教育を思い出し、結果的に標的型メール攻撃の恐ろしさを実感

した。
3. この経験から、過去に受けた教育の内容を振り返った。

4.8.3. もし標的型攻撃がきたら、どう対処するか。

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようなことが起きると思われるかを検討する。

図 24 被験者企業 B：今後組織に攻撃があると思うか

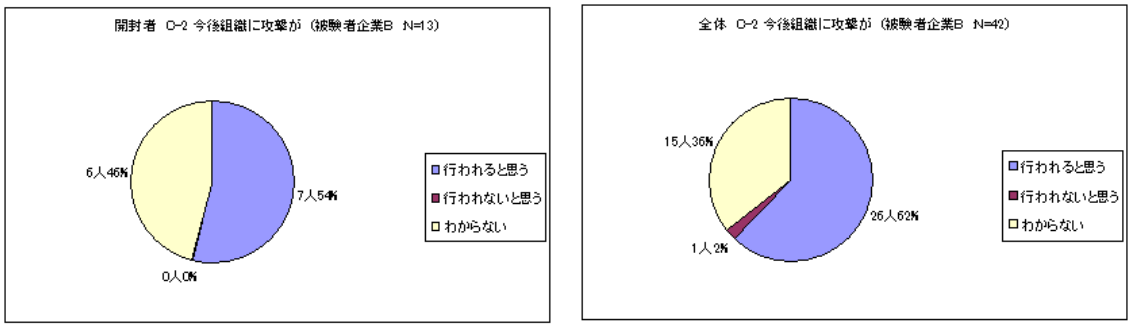


図 24 を見ると、今後組織に標的型メール攻撃が行われるかもしれないと回答している被験者が、有効回答の 62%を占めている。擬似的なものとはいえ、実際の攻撃を受けて、あらためて脅威を認識したということであろう。

図 25 被験者企業 B：もし標的型メール攻撃が来たら

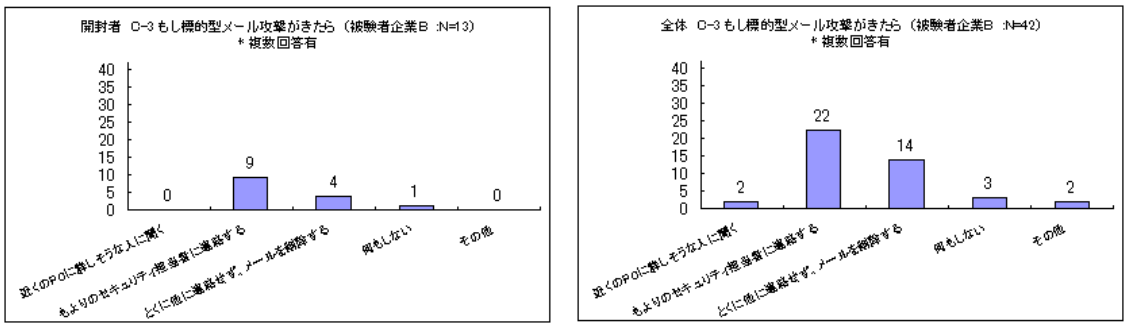


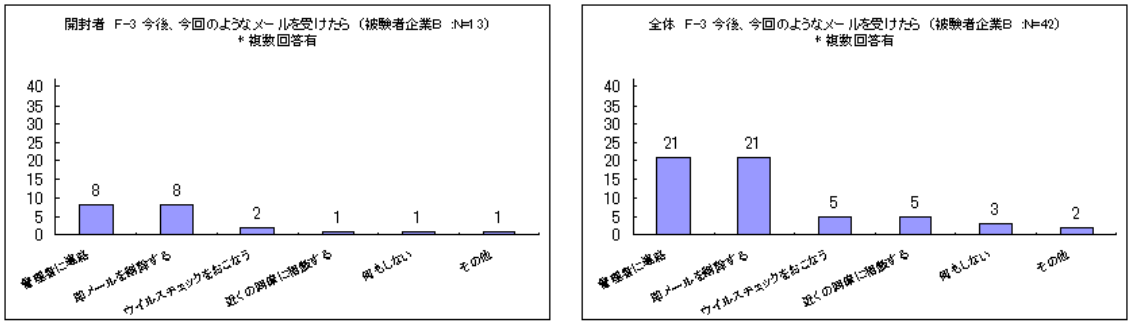
図 25 を見ると、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は有効回答 42 名中の 22 名(52%)であった。他方で、42 名中の 14 名(33%)は、「とくに他に連絡せずに削除する」と回答している。

設問 C-3 の「もし標的型メール攻撃がきたらどう対処するか」を問う設問には、有効回答 42 名中の 69%の被験者が「管理者に連絡する」と回答している。

プライバシーマークや ISO27001 は、インシデントを報告することを要求しているが、これらの回答から見る限り、インシデント報告を行うという意識を

持つのは約半数に過ぎない。約 3 分の 1 は単にメールを削除するだけなので、結果的にインシデントを隠蔽することになる。インシデント報告義務を徹底させることがいかに難しいかのひとつの事例であろう。

図 26 被験者企業 B：今後、今回のようなメールを受けたら



設問 F-3 では、設問 C-3 とほぼ同様の内容について、表現を変えて再度質問している。図 26 にあるように、標的型攻撃のメールがきた場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者が有効回答 42 名中の 21 名(50.0%)となり、先の設問 C-3 での回答と比率はほぼ同じである。逆に、「即メールを削除する」と回答している被験者は 42 名中 21 名(50.0%)と増加している。この誘導では、証拠保全し管理者に連絡することの重要性が認識される方向には向かわず、危険なメールは削除すればよいという考え方に流されているようだ。

4.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4(危機管理意識の変化)に対する回答者 36 名中の 23 名(63.9%)の被験者が、危機管理意識の変化もしくは危険の再認識をしたと回答しており、予防接種を肯定的にとらえている。

また、以下のような回答があり、予防接種による学習が効果的なことがわかる。

1. **メールの取り扱いについて注意が必要だと再認識したものが 9 名いた。**
2. **もともと標的型メール攻撃の手法があることは知っていたが、油断していると自分も開いてしまうだろうと体感したととれる回答をした被験者が 6 名いた。**

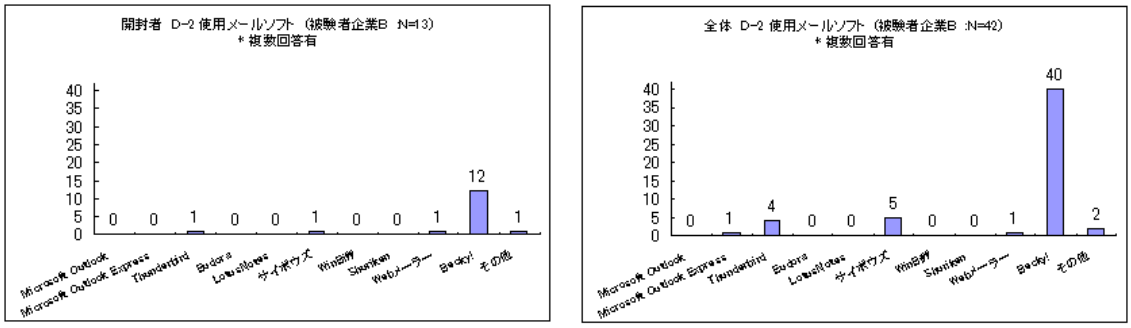
4.8.5. 使用メールソフト

メールソフトの中には、差出人の表示名があればアドレスを表示しないものがあるので、被験者が使用しているメールソフトが異なれば開封率にも差が出るのではないかと予測していた。

しかし、図 27 を見ると、使用しているメールソフトによる開封率の差を読みとることはできない。

なお、被験者企業 B ではメールソフトとして Becky!を推奨しており、被験者アンケートの結果でも全体の 75%を占めている。

図 27 被験者企業 B：使用メールソフト



4.8.6. 感想

被験者アンケートの設問 G(感想意見など。自由記述)の回答者 26 名中の 16 名は、今回の予防接種訓練を肯定的にとらえ、再実施や実施方法の工夫を提案している。

例えば、「怪しいメールは開かないのが原則だが、報告義務や対応に関しての取り決めが明確化されていないと思う」という回答があり、組織としての対応方法を整備するべきだという意見が見受けられた。

また、「メールを閲覧したり、添付ファイルを開くのに、不信感が出来ました。今の時代、一日に来るメールの量が多い中で、メール開封することが不信になり、メールが埋もれる可能性もあるかも知れません。(私だけではなく、もっとメール受信が多い人：管理職の方々など)」という感想もあった。

メールを開くこと自体に不信感を持たないですむように、メール閲覧時の注意や添付ファイルの正しい扱い方などを教育するなどの対策が必要であろう。

4.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 B について、被験者企業アンケートと被験者企業インタビューからの分析を以下に記す。

1. **プライバシーマークと ISO27001 を全社で取得している。**
2. **情報セキュリティの管理体制はほぼ整備されており、インシデントの連絡体制(窓口)も定められている。**
3. **定期的な情報セキュリティ教育を実施している。**
4. **以上により、被験者企業 B では情報セキュリティ体制は概ね整っていると言える。**

今回の擬似攻撃メールのような標的型メール攻撃は、迷惑メール攻撃と同種の攻撃だと思われているため、セキュリティインシデントの報告をしない場合が見られた。

特に、被験者企業 B は 2007 年度にも予防接種を行った企業であるから、「このメールは訓練である」と気付いた被験者も多かった。とりわけ、第 2 回配信では配信直後にすぐ気付いた被験者が非常に多かったようだと、窓口担当者がコメントしている。

4.10. 考察

被験者企業 B は、2007 年度にも予防接種を実施した企業であるためか、普段から送信元のアドレスまでチェックするということを心がけている被験者の割合が多かった。同時に、「これは去年と同じ訓練である」という認識があるために、開封しても安全であると鷹をくくって開封した被験者の数も多かったといえる。

また、擬似攻撃メールが社内の IP アドレスから発信されていることに気付いたので、予防接種であると見抜いたという被験者もいた。この例を見ると、被験者企業の外部から、可能であればセキュリティの専門家と連携しながら擬似攻撃メールを送ることが望ましい。

特筆すべき点としては、第 1 回配信ではメールアドレスを確認して不審なメールだと判断したにも関わらず、第 2 回配信では本物のメールと信じこんで、添付ファイルを開いてしまった被験者がいる点である。この被験者は、その理由として、「サブジェクトが思い当たる案件だったためうっかり開いた」と回答している。

これは、被験者企業 B のように IT の利用に慣れていて、セキュリティ意識が高い企業文化でもあり、なおかつ、予防接種を 2 年連続で行っていても、ソーシャルエンジニアリングを利用した攻撃を完全に防ぐことは非常に困難であるという一例となるだろう。

なお、予防接種 2 年目でも、設問 G(感想)をはじめとする自由記述欄で、予防接種に肯定的な意見が多く見られたのは、予防接種の意義を考える上で大切な点である。

5. 被験者企業C

5.1. 被験者企業Cの概要

被験者企業 C は、情報機器の販売やシステムのインテグレーションなどを手がける商社系大手 IT 企業である。

表 19 に、被験者企業 C の概要について記す。

表 19 被験者企業 C：概要

業種	情報機器販売
設立	1969 年 10 月 25 日
資本金	21,152 百万円
本社所在地	東京
拠点数	12 箇所
社員数	約 3,000 人
認証	プライバシーマーク（全社）、ISO27001（部門取得）、ISO9001、ISO14001

5.2. 被験者企業Cにおける予防接種の概要

被験者企業 C の予防接種を、表 20 に示す日程と規模で行った。

表 20 被験者企業 C：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2008/10/28 14:00	2008/11/12 15:00
種明かし	2008/10/29 10:00	2008/11/13 10:00
被験者数	308 人	308 人

被験者企業 C における被験者は、コーポレート部門(総務・人事・経理などの本社機能)に所属する 308 名である。

被験者企業 C は、会社としてプライバシーマーク認証を取得している。また、コーポレート部門は、部門の単位で ISO27001 認証を取得している。したがって、今回の被験者は、プライバシーマークが要求するヒヤリハット報告の義務を負っているとともに、ISO27001 体制の一環としての情報セキュリティ教育を受けているはずである。

5.3. 擬似攻撃メールの内容

5.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 C における第 1 回配信の擬似攻撃メールは、リスト 2 のサンプル

の(12)を参考にして作成した。その文面をリスト 13 に示す。

この擬似攻撃メールでは、架空の部署「情報システム企画課」から被験者に宛てて、社内システムのセキュリティ機能強化の為に SSL 証明書をインストールするように指示している。「明朝 9 時」までにインストールしないと社内システムが使えないと宣言することで、添付ファイル「証明書インストール手順.doc」の開封を急がせるものとなっている。

このメールには、以下のような気付きのポイントが含まれている。

1. **差出人の表示名を「情報システム企画課」とした。この部署は実在せず、架空の社内部署である。**
2. **本文中に差出人として掲げた「情報システム企画室長」は被験者企業 C には実在しない役職である。**
3. **差出人のメールアドレスは motok2501@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。**
4. **本文中で電子証明書のインストールを指示しており、当日中にインストールをしない者は翌日からシステムへのアクセスができないと明記することで開封を急がせるものとした。**
5. **メール本文の上部に記載された文章番号「ISK-2008-10-28 001」は、実際に被験者企業 C の内部で使用されている書式ではないが、いかにも公式通達であるかのように見せかけることを意図した。**
6. **他には、呼びかけが「各位」となっていて宛先の個人の名前を呼んでいない点や、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点などが、標的型攻撃メールの特徴に一致する。**

リスト 13 被験者企業 C：第 1 回配信の擬似攻撃メール

From: 情報システム企画課 <motok2501@(フリーメール A) >
Subject: 【緊急のお知らせ】システムアクセス認証変更について

ISK-2008-10-28 001

システム利用者各位
各部システム担当者各位

2008 年 10 月 28 日
情報システム企画室長

昨今、ご承知のとおり、様々な情報漏えい事故、不正侵入事故の発生など社会的にセキュリティ事故が増加する中、当社においても、社内情報保護の観点より、Web 系社内システムの SSL 化及びクライアント電子証明書による認証によるアクセス制御を実施することとなりました。

これに伴って利用者各位は、PC への電子証明書インストールが必要になります。本メールにインストール手順書を添付しておりますので、これをダブルクリック(開く)していただき、手順に従ってインストールを実施願います。

誠に急ではありますが、社内システムを標的とした新種ウイルスが拡大中との情報が本日はいっており、感染防止のため明朝 9 時より認証強化を実施いたします。本日中にインストールされない場合は、明朝よりシステムへのアクセスができなくなりますので、ご注意下さい。

各部システム担当者各位におかれましては、部内周知ならびに不在者への周知、サポート等をお願い致します。なお不明の際は社内サポートデスクまでご連絡下さい。

以上

添付ファイル名: 証明書インストール手順.doc

5.3.2. 第 2 回配信の擬似攻撃メール

第 2 回配信の擬似攻撃メールは、擬似攻撃メールのサンプルの(6)を参考にして作成した。その文面をリスト 14 に示した。

この擬似攻撃メールでは、不審なメールに対する対処方法をハンドブックにまとめて添付したので、できるだけ早く読むように、という指示を出している。第 1 回配信のものと同様に架空の社内組織からの通達を装っているが、文面にこなれていない日本語をちりばめていて、非日本語圏からの稚拙な攻撃を真似ているところがユニークである。

このメールには以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「情報システム企画室」とした。この部署は被験者企業 C には存在しない架空の部署である。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールアドレスである。
3. メール本文は、メールによるウイルス感染防止を目的としたハンドブックの送付を騙るものとした。
4. 本文中の日付が「2008 年 3 月 11 日」となっていて、配信日の半年以上前の日付である。これは、同じ文面を何度も使い回して攻撃している状況を暗示している。
5. 本文中で「役員・社員各位」と呼びかけることによって、このメールが、あたかも役員を含む全員に対する重要な通達であるかのように

装っている。

6. 「不安なメール」・「クリックに到る」・「何回発生しています」・「検知できないです」・「早期に読んだの上」などのように日本語として不自然な書き方をしており、日本語を母語としない攻撃者を暗示するものとなっている。
7. 他には、呼びかけが「各位」となっていて宛先の個人の名前を呼んでいない点や、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 14 被験者企業 C：第 2 回配信の擬似攻撃メール

From: 情報システム企画室 ＜censusteam@(フリーメール A)>
Subject: 【社内業務通知】不安なメールのウイルス感染防止について

役員・社員各位

不安なメールのウイルス感染防止について

2008 年 3 月 11 日
情報セキュリティ本部長

最近、我が社において、業務連絡メールを装ったメールにつけられたファイルを開いたり、書きこんだリンクをクリックに到ることによるコンピュータウイルス感染事故が何回発生しています。こんなメールは、社内文書や顧客からの連絡などを装い、受信者に開かせてウイルス感染させる狙いを持ったもので、添付されるウイルスの多くがウイルス対策ソフトで検知できないです。PC のウイルス対策ソフトやメールサーバ上での対策では駆除できないことも大きく、各位の注意が必要であります。

情報セキュリティ本部は、こんなメールの見分け方、対応のしかたをまとめたハンドブックを作成たので、このメールに添付します。できるだけ早期に読んだの上、不安なメールへの備えをおねがいします。

添付ファイル名: 不安メール対策ハンドブック.doc

5.4. Webビーコンの集計結果

被験者企業 C における添付ファイルの開封状況を、Web ビーコンのアクセスログから見ると表 21 の通りとなる。

表 21 被験者企業 C：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2008/10/28 14:00	2008/11/12 15:00
種明かし	2008/10/29 10:00	2008/11/13 10:00
被験者数	308 名	308 名

Web ビーコンへのアクセス総数	105 回	30 回
開封したと考えられる人数	54 名(17.5%)	24 名(7.8%)
2 回とも開封した人	4 名(1.3%)	

被験者企業 C では、第 1 回配信での開封者数が 54 名(17.5%)であり、第 2 回配信では 24 名(7.8%)となって、改善が見られた。

開封者の中には 2 回とも開封した者が 4 名おり、絶対数では少数ではあるが、周知・教育を受けていても開封する者は開封するという傾向が見られる。また、第 1 回配信および第 2 回配信の両方で、Web ビーコンのログ収集サーバへの偵察アクセスが観測されている。

5.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから見ると、時系列の添付ファイル開封状況は以下の通りである。

被験者企業 C では、擬似攻撃メール配信直後の 1 時間に開封が集中しており、4 時間ほどで一旦終息する。

その後、約 18 時間後(翌朝 8 時から 9 時)に若干の開封が見られるのは、翌日の出社時にメールをチェックしたものだと思われる。この時間帯には、第 1 回配信では 4 回、第 2 回配信では 1 回のアクセスを記録している。

図 28 に、被験者企業 C について、擬似攻撃メール配信後 3 日分の開封数を 1 時間刻みのヒストグラムとして示した。

同様に、図 29 には配信後 4 時間分の開封数を 15 分刻みで示した。

図 28 被験者企業 C：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

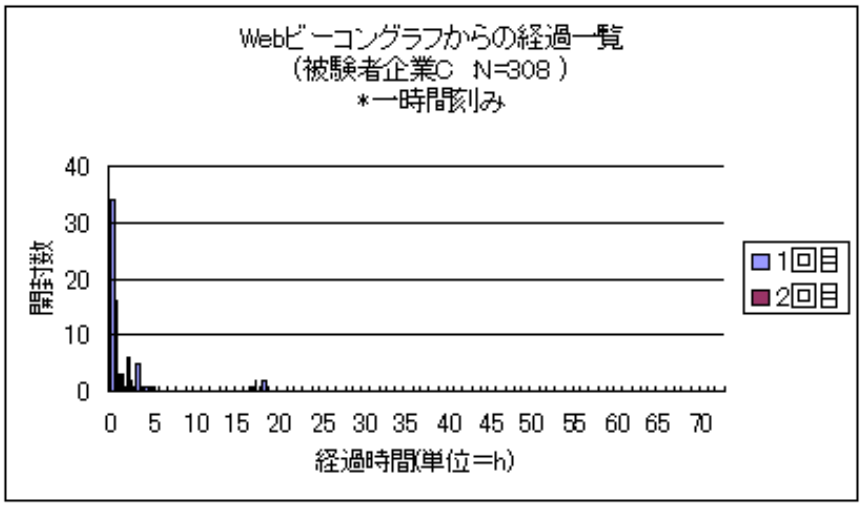
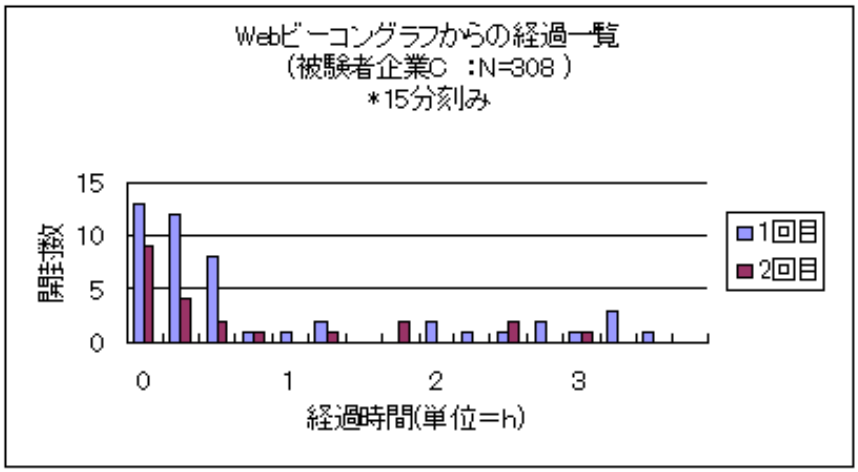


図 29 被験者企業 C：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



5.6. 予防接種実施時の特記事項

5.6.1. 第 1 回配信時の添付ファイル名の文字化け問題

第 1 回配信の際、Outlook 系の MUA では擬似攻撃メールの添付ファイル名が正しく表示されない現象が発生していると、被験者企業 C の窓口担当者から指摘を受けた。

本来であれば、「証明書インストール手順.doc」と表示されるべきところ、実際には、「att?????.dat」(?????の部分は 5 桁の数字)となることを確認した。

調査の結果、Outlook 系 MUA が古くて誤った方法で添付ファイルのファイル名を解釈することしかできないことが原因であることが判明した。

まず、添付ファイルのファイル名をエンコードする方法には、大別して 2 種類が存在する。ひとつは、RFC2231 に記述されたエンコード方法で、RFC に準拠する意味ではこれが正しい方法である。もうひとつは、RFC2231 以前に広く使われていた MIME B-encoding を用いる方法で、メールのヘッダのエンコード方法としては正しいが、添付ファイルのファイル名のエンコードに利用すると RFC2047 に違反することになる。

Outlook 系 MUA は、MIME B encoding による方法にのみ対応しているが、他の MUA では両方に対応していることがほとんどである。

被験者企業 C における第 1 回配信では、RFC2231 方式でエンコードしたものだけを使用したために、Outlook 系 MUA では添付ファイルのファイル名がないものと誤認してデフォルトの名称をつけたのであろう。

そこで、第 2 回配信とそれ以降は、配信スクリプトが両方の方式で添付ファイル名を指定するように対策した。この対策によって、当時の最新版の Outlook および Outlook Express で、添付ファイル名を正しく表示することができることを確認した。その後は、Outlook 系 MUA に限らず、同様の問題は発生していない。

なお、被験者企業 C 向け第 1 回配信の際に、この問題の影響を受けた被験者の数は、被験者数の 60 から 70%ほどではないかとのことであった。

5.6.2. 抜き打ち実施の悪影響

被験者企業 C では、事前教育なしに抜き打ちの予防接種を行ったので、一部の被験者から苦情その他の否定的な反応があった。

その結果、被験者企業アンケートの実施に障害を来した。結果的には被験者企業アンケートを実施することができたが、時期が遅れただけでなく回答回収率も他社にくらべて低めの結果となっている。

今年度の IT セキュリティ予防接種においても、事前の周知(標的型メール攻撃とは何かを解説し、注意を喚起するなど。予防接種を実施することの周知ではない)を依頼していたが、この事前教育の重要性をあらためて認識する結果となった。

参考までに、リスト 15 に苦情メールの例を掲載しておく。非常に短いメッセージであること、配信と同日に送られていること、窓口担当者へも送っていること等から、冷静な中にも強い抗議の意志を感じ取ることができる。

リスト 15 被験者企業 C：苦情メールの例

```
From: (被験者のメールアドレス)
To: '情報システム企画室' <censusteam@(フリーメール A)>
```

Cc: (窓口担当者のメールアドレス)
Date: Wed, 12 Nov 2008 18:33:29 +0900
Subject: お願い

業務上迷惑ですので止めていただけませんか?

5.6.3. 偵察アクセス

第 1 回配信時に見られた偵察アクセスは、総アクセス回数 105 回のうちの 51 回(48.6%)である。

手法としては、何らかの形で Web ビーコンの URL を識別し、その URL を多少改変してアクセスするものである。

このような偵察アクセスを行うためには、相応の知識を持ち合わせている必要がある。被験者企業 C に偵察アクセスが多いのは、IT セキュリティを提供している企業を被験者とした場合の特徴といえよう。

第 2 回配信では、総アクセス回数 30 回のうち 6 回(20.0%)の偵察アクセスが見られた。その手法は第 1 回配信と同様である。この偵察アクセスの数字の低下は、第 1 回配信と同様の状況であったために、興味を失った結果ではないかと思われる。

5.7. 被験者アンケートの集計

被験者企業 C の被験者アンケートの集計状況について表 22 に記す。

表 22 被験者企業 C : 被験者アンケート回答者の開封状況

有効回答数	91 名	
	第 1 回	第 2 回
開封した人数	23 名 (25. 3%)	10 名 (11. 0%)
2 回とも開封した人	4 名 (4. 4%)	

被験者数 308 名のうち、102 名(33.1%)から被験者アンケートの回答があった。そのうち 11 名が 2 回とも擬似攻撃メールに気付かなかったと回答しているので、有効回答数を 91 名とした。

表 22 にあるように、被験者アンケート回答者のうち、一度でも添付ファイルを開いたと答えている者は 29 名(有効回答数の 31.9%)、第 1 回配信で開封した者は 23 名(25.3%)、第 2 回で開封した者は 10 名(11.0%)、両方を開封した者は 4 名(4.4%)であった。

前節の Web ビーコンから見た開封率に比べて、本節のアンケート回答者の開封率が若干多い結果となっている。すなわち、第 1 回配信で Web ビーコンから

見た開封率が 17.5%であるのに対してアンケート回答から見た開封率は 25.3%、第 2 回配信では同 7.8%に対して 11.0%となっている。

前述の抜き打ち実施の悪影響で、被験者アンケートに回答していただけなかった層が、実は標的型メール攻撃に対する耐性が高かったという可能性が高い。

5.8. 被験者アンケートの分析

本節では、被験者企業 C の被験者アンケートの内容から、その特徴となる諸点を示す。

5.8.1. 添付ファイル開封の有無とその理由

被験者アンケートの設問 C-4, C-6 等から、擬似攻撃メールの添付ファイルを開封した状況を調べることにする。

図 30 被験者企業 C：被験者アンケートから見た開封状況(第 1 回配信)

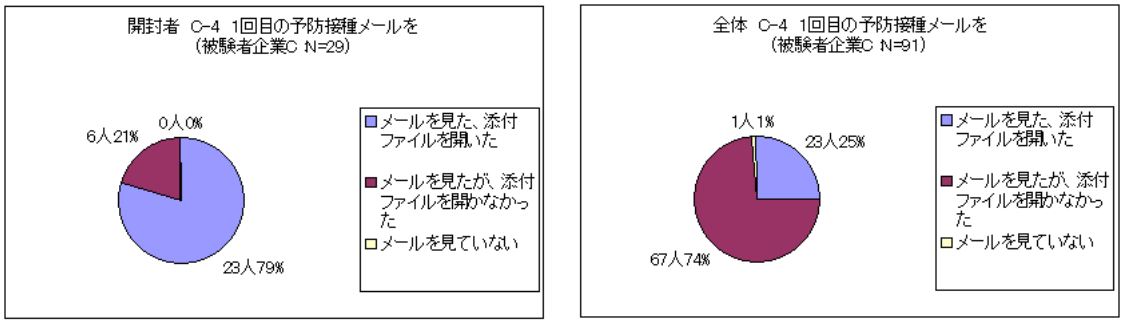


図 30 にあるように、第 1 回配信では、有効回答者 91 名中の 23 名(25%)が添付ファイルを開封したと回答している。被験者アンケートの設問 C-5 に対する回答内容からその理由を探すと、ほとんどの開封者が一瞥して社内の連絡であるものと思いこんで開封している。

図 31 被験者企業 C：被験者アンケートから見た開封状況(第 2 回配信)

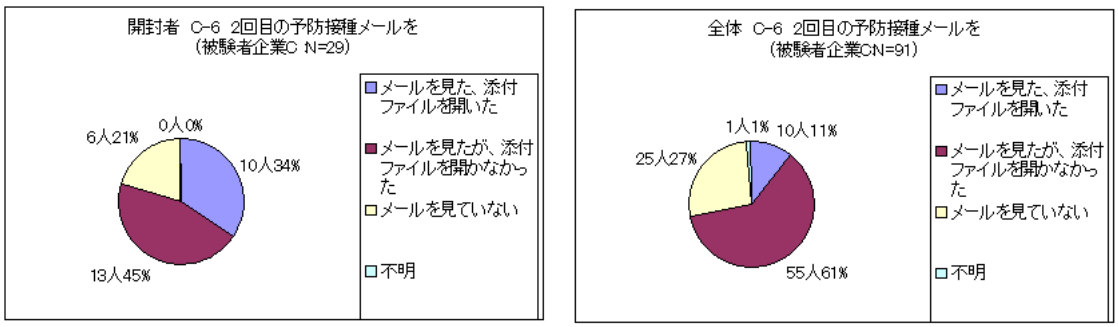


図 31 にあるように、第 2 回配信では、有効回答者 91 名中の 10 名(11%)が添付ファイルを開封したと回答している。第 1 回配信と比較すると、開封者は減

少している。

第 1 回配信での開封者 23 名のうち､19 名は第 2 回配信では開封しなかった。被験者アンケートの設問 C-7 を見ると、この大半の被験者が、第 1 回配信を開封した経験から第 2 回配信では用心した、もしくは、第 1 回配信の体験から学習した等と回答している。

第 1 回配信では開封しなかったが第 2 回配信に開封したという被験者は 6 名いた。設問 C-7 の回答によれば、このうち 4 名が、社内の連絡だと思いこんで開封している。その理由として典型的な 2 名の意見を掲載しておく。

1. **てっきり社内の連絡メールと思い、疑うことなくメールを開き、ファイルも開いた。メール文章が稚拙な印象はあったが、担当者の文章力の問題と判断してしまった。**
2. **作業中で忙しい状態であったので、特に内容を確認せずに添付ファイルまで開いてしまった。**

なお、これらの回答者 2 名は、第 1 回配信の際には差出人のメールアドレスが不審であると判断して､添付ファイルを開かなかった。この 2 名のケースは、常に注意力を働かせてメールを扱い危険なメールを見抜くという作業を継続することが、いかに難しいかを表しているといえるだろう。

5.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間にどのような関係が読み取れるかについて調べる。

図 32 被験者企業 C：情報セキュリティ教育の経験

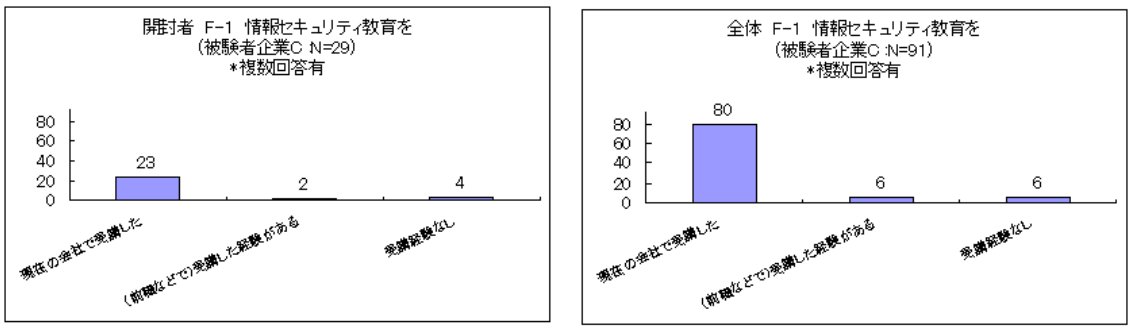
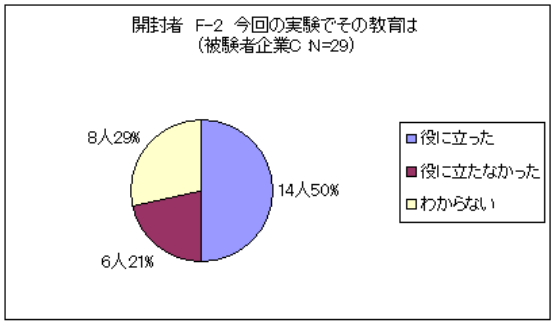


図 32 によれば、被験者アンケート有効回答者 91 名中の 80 名(87.9%)が現在の会社で教育を受けたと回答している。

図 33 被験者企業 C：情報セキュリティ教育の有効性



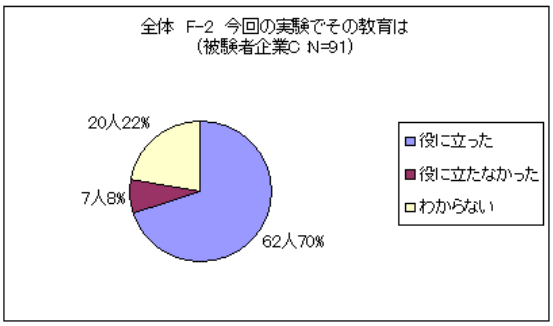


図 33 を見ると、62 名(70%)の被験者が、今回の予防接種でその教育が役立ったと回答している。なお、教育が役にたたなかったと回答した被験者 7 名のうちの 6 名は、添付ファイルを開封した被験者である。

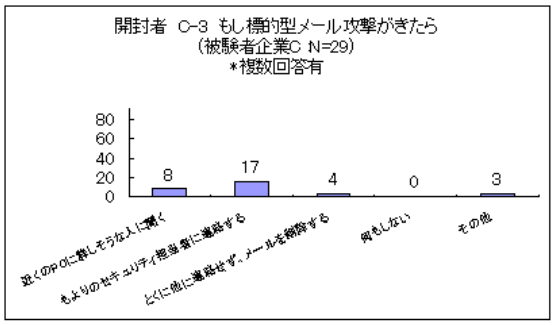
これは、座学の情報セキュリティ教育だけでは実感が伴わず、実際に標的型メール攻撃に狙われた場合に対処できないかもしれないという限界を感じたものではないかと思われる。もしそうなら、ほぼ唯一の体験型教育手段である予防接種は、被験者にとって大変効果が高いものであるといえるだろう。

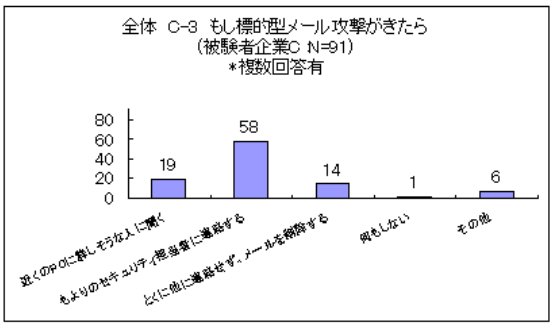
5.8.3. もし標的型攻撃がきたら、どう対処するか。

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようなことが起きると思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答を見ると、今後組織に標的型メール攻撃が行われるかもしれないと考えている被験者は、有効回答者に対して 56%の割合を占めた。今回の予防接種で、実際の攻撃とほぼ同様の擬似的攻撃を受けて、あらためて脅威を認識したということであろう。

図 34 被験者企業 C：もし標的型メール攻撃が来たら





設問 C-3 に対する回答を図 34 に示した。

これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は有効回答者 91 名中の 58 名(63.7%)であった。他方で、14 名(15.4%)は、「とくに他に連絡せずに削除する」と回答している。

図 35 被験者企業 C：今後、今回のようなメールを受けたら

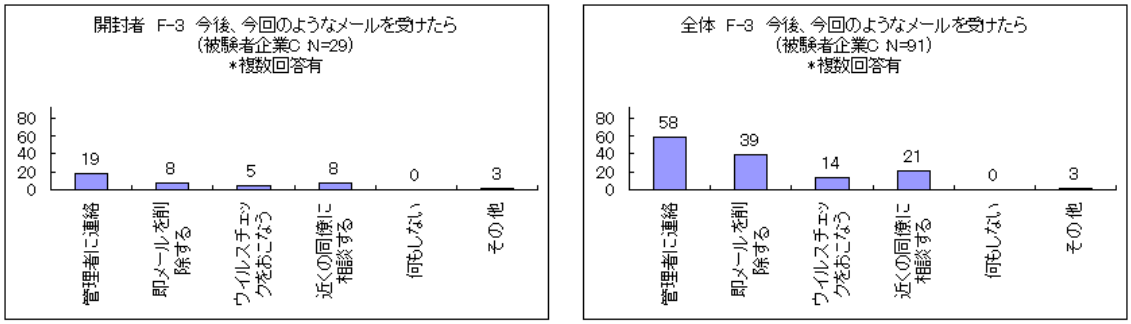


図 35 には、設問 F-3 に対する回答を示した。設問 F-3 は、前述の設問 C-3 とほぼ同様の内容について、表現を若干変えて再質問している。

設問 F-3 への回答から見ると、標的型攻撃のメールがきた場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者が、有効回答者 91 名中の 58 名(63.7%)となり、先の C-3 での回答と同数・同率であった。

今回の被験者は、プライバシーマークや ISO27001 の認証を取得している部署に所属しているので、インシデント報告の義務があるはずである。しかし、上に見たように、正しく報告を行うと回答している被験者は 6 割強に過ぎない。

インシデントの報告義務を徹底させることがいかに難しいかの一例である。

5.8.4. 危機意識の変化

ここでは、被験者アンケートの設問 F-4 に対する回答を用いて、被験者の危機管理意識が変化したか否かについて調べる。

設問 F-4 に対する回答者 55 名中の 42 名(76.4%)が、今回の予防接種を通じて危機意識の変化があった、もしくは、危険を再認識したと回答しており、予防接種を肯定的に捉えている。

また、予防接種による学習は効果的であると評価する趣旨の記述もあったので、一部を抜粋しておく。

1. **被害を受けた時の対処法などについて確認する良い機会だった。**
2. **所属する部署のメンバーに対しても、危機意識を共有し、植え付けることが重要である。**

5.8.5. 感想

ここでは、被験者アンケートの設問 G に対する回答から、メッセージを読みとることを試みる。

設問 G の回答者は 47 名で、このうち 36 名(76.6%)の被験者が、今回の予防接種を肯定的に捉えている。
中には、再実施を求める意見や実施方法の工夫を提案する意見もあった。被験者企業 C は IT セキュリティを手がける会社であるために、実施方法の改善提案が目立つ結果となっている。以下に、一部の意見・感想を抜粋しておく。

1. **人は失敗から「しか」学べないのであれば、いっそのことダミーではなく、スクリーンセーバーの書き換えや、壁紙の書き換え程度の「痛さ」を経験させるのがこういった訓練では重要ではないだろうか。**
   (ついでにしばらく操作不能にすればパーフェクトだ)
   経験として体に刻まれない訓練など無意味。本物のように振舞う擬似ウイルスを使用するのが効果を際立たせるだろう。
   しかし今回のカウント方法についてはとても有用だったので、個人的に大いに活用しようと思う。
2. **このような訓練を全社的に実施して欲しい。その上で危機管理意識向上のため、統計値を公表して欲しい。**
3. **“騙まし討ち”のようであまり気持ちが良いものではないが、教条的な講習を聞くよりも気付きの効果はあるかもしれない。「予防接種訓練」というのは言い得て妙な表現。**
4. **より分かりにくい、凝った擬似メールに適切に対応出来るか不安が残りました。**

5.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 C での被験者企業アンケートと被験者企業インタビューの結果から、以下のことがわかった。

被験者企業 C は、プライバシーマーク・ISO27001・ISO9000 の認証を取得しているだけでなく、事業継続プラン(BCP)の認証も取得している。
BCP 認証は比較的最近になってから必要性が説かれているもので、この認証を取得しているところは被験者企業群の中でも珍しい。

被験者企業 C では、プロクシサーバやフォレンジック機器を用いることで、ネットワークのトラフィックを監視・監査して、情報漏洩防止対策としている。
自社の取り扱い機器を実地に検証しているという側面もあるかと思われるが、さすが大手 IT 機器ベンダであるといえよう。

被験者企業 C は、送信ドメイン認証の設定を行っていないことがわかった。送信ドメイン認証の中でも、SPF による自社側メールサーバの宣言は、DNS にエントリを追加するだけで容易に実現できる。JP ドメインの約 3 分の 1 が設定済みとの報告もあるので、設定することをお勧めしておいた。

なお、被験者企業 C の窓口担当者からは、「今回の予防接種を実施する中で、標的型メール攻撃に関する社内周知を何度も行ったので、啓蒙効果はあったと思う。定期的に予防接種することで、免疫を持続させる必要があるだろう」というコメントを頂いた。

5.10. 考察

今回、被験者企業 C の被験者側から苦情をいただく結果となったことは前述の通りである。年末の繁忙期と重なったことも理由のひとつであろうが、最大の理由は「事前教育なしの抜き打ち実施」にあるだろう。
今回の予防接種では、窓口担当者の強い意向もあって抜き打ちで実施したが、事前教育によってそれとなく被験者に心の準備をさせることが重要であるという教訓を得た。

このような背景があるにもかかわらず、被験者アンケートの回答には、予防接種の必要性を認め、予防接種を冷静に捉える回答が多数を占めた。窓口担当者が事態の収集と沈静化のために時間をかけて調整したことが功を奏したのであろう。
被験者アンケートの回答の自由記述欄を見ると、「もっと巧妙なメールでも良かった」との記述が見られた。今回の予防接種では、窓口担当者の意向で、かなり巧妙な擬似攻撃メールを送付しているにもかかわらず、このような記述が見られるところに、被験者企業 C のセキュリティ意識の高さが伺える。
また、予防接種を肯定的に捉える回答や、手法についての工夫の提案も目立った。
被験者アンケートの結果が総じて肯定的であったのは、予防接種に批判的な被験者層が回答していないだけのことかも知れない。しかし、被験者企業 C が情報セキュリティの体制をしっかり築いており、被験者にも情報セキュリティを守る意識が強いことを強く感じている。

6. 被験者企業D

6.1. 被験者企業Dの概要

被験者企業 D は、中規模の情報セキュリティサービス専門企業である。

表 23 に、被験者企業 D の概要を記す。

表 23 被験者企業 D：概要

業種	情報サービス業
設立	(非公開)
資本金	約 4 億円
本社所在地	東京
拠点数	2 箇所
社員数	約 70 人
認証	「ISO27001」(部門取得)

6.2. 被験者企業Dにおける予防接種の概要

表 24 に、被験者企業 D における予防接種の日程と被験者数を示す。

被験者企業Dの被験者は29名で､ほとんどが情報システム部に所属している。
この被験者の全員が、企業内セキュリティ教育を受けている。これは、情報セキュリティサービスを提供する立場上、当然であろう。
なお、情報システム部は ISO27001 認証を取得していないが、他部門が部門単位で取得している。

今回の予防接種を行うに当たって、訓練についての事前通知や、標的型メール攻撃に関する教育は行わなかった。

表 24 被験者企業 D：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2008/10/28 11:00	2008/11/11 11:00
種明かし	2008/10/28 14:00	2008/11/11 14:00
被験者数	29 名	29 名

6.3. 擬似攻撃メールの内容

6.3.1. 第 1 回配信の擬似攻撃メール

第 1 回配信で用いた擬似攻撃メールをリスト 16 に示す。

この擬似攻撃メールは、リスト 2 のサンプル(12)をほぼそのまま使用した。
内容は、「社内 IT」からの周知連絡でシステムの更新を促す内容となっており、「コンピュータの状態を安定」・「セキュリティを向上」などと利益を強調して添付ファイルの開封を誘うものである。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「社内 IT」とした。この組織は実在せず、架空の社内組織である。
2. 差出人のメールアドレスを motok2501@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 表題「全社システムのアップデート>について」の中の「>」は不自然で、社内周知というにはやや注意散漫である。他にも、本文冒頭に呼びかけがない点や通知責任者の名前を記載していない点など、不審な点がある。
4. 本文でシステムのアップデートを呼びかけているが、その背景や理由などの説明がない。この内容ならば、被験者企業 D に限らず、どの企業にも当てはまるので、汎用の本文を使い回して攻撃している悪意の第三者を示唆していると言える。
5. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点は、標的型攻撃メールの特徴に一致する。

リスト 16 被験者企業 D：第 1 回配信の擬似攻撃メール

```
From: 社内 IT <motok2501@(フリーメール A)>
Subject: 全社システムのアップデート>について

添付の資料を参照の上、最新のアップデートをお試しください。
新しいプログラムはコンピュータの状態を安定させ、セキュリ
ティを向上させます。

添付ファイル名: update.doc
```

6.3.2. 第 2 回配信の擬似攻撃メール

第 2 回配信の擬似攻撃メールをリスト 17 に示す。

この擬似攻撃メールは、リスト 2 のサンプル(13)をほぼそのまま使用した。
内容としては、「社内 IT」から動画コンテンツの視聴状況について行うアンケートを装っている。「定点観測点」・「ランキングデータ」などの文言で、他部門への協力になることを暗示して被験者の参加を誘うものとなっている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 第 1 回配信の際と同様に、差出人の表示名を「社内 IT」とした。架空の社内組織である。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスであり、本文中にも通知責任者の名前を記載していない点も第 1 回配信と同様である。
3. 文面の特徴も第 1 回配信のものと同様に、被験者企業 D への固有性もなく、具体性も薄いものとなっている。
4. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無く、標的型攻撃メールの特徴に一致する点も第 1 回配信と同様である。

このように見てくると、被験者企業 D における擬似攻撃メールの文面は、第 1 回配信で使用したものと第 2 回配信の際のものが、酷似した気付きのポイントを持っていることがわかる。

リスト 17 被験者企業 D：第 2 回配信の擬似攻撃メール

From: 社内 IT <censusteam@(フリーメール A)>
Subject: 動画コンテンツ視聴アンケート

定点観測点におけるランキングデータです。参考までに、社員に対しても
アンケートを実施させていただきたいと思います。
お手すきの際に、添付ファイルにリンクがあげられている動画ファイルを
閲覧の上、評価してください。

添付ファイル名: 動画コンテンツランキング.doc

6.4. Webビーコンの集計結果

被験者企業 D の添付ファイルの開封状況を、Web ビーコンのアクセスログから見た結果を、表 25 に示す。

添付ファイルの開封率は、第 1 回配信での 13.8%から第 2 回配信での 24.1%へと増加した。この被験者企業のように、第 2 回配信の開封率が第 1 回配信のものを上回るというケースは珍しい。

2 回とも開封した被験者はいない。

この開封率の増加だけをみれば、被験者企業 D では、第 1 回配信後に行われた種明かしの際に行われた啓発・教育の効果が薄かったのではないかと思われる。あるいは、被験者の大半が擬似攻撃メールを見破った上で、実害がないことを確信して興味本位に開封しているのかも知れない。

表 25 被験者企業 D：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2008/10/28 11:00	2008/11/11 11:00
種明かし	2008/10/28 14:00	2008/11/11 14:00
被験者数	29 名	29 名
Web ビーコンへのアクセス総数	15 回	10 回
開封したと考えられる人数	4 名(13.8%)	7 名(24.1%)
2 回とも開封した人	0 名(0%)	

6.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 D における添付ファイルの開封状況は、以下の通りである。

被験者企業 D の第 2 回配信では、擬似攻撃メール配信直後の 1 時間に開封が集中しており、これは他の被験者企業での状況と類似している。

しかし、第 1 回配信では、配信直後の 1 時間には開封が見られず、1 時間後から 2 時間後にかけての 1 時間に集中している。被験者企業 D で被験者全員が参加する会議のようなものが開かれていて、この時間帯には誰もメールを確認していなかったのではないかと思われる。

図 36 に擬似攻撃メール配信後の 3 日分の開封数を 1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 37 に示す。

図 36 被験者企業 D：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

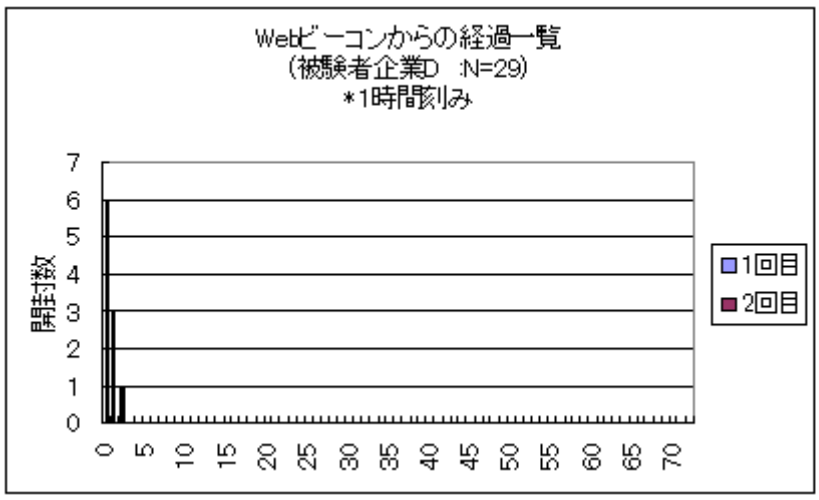
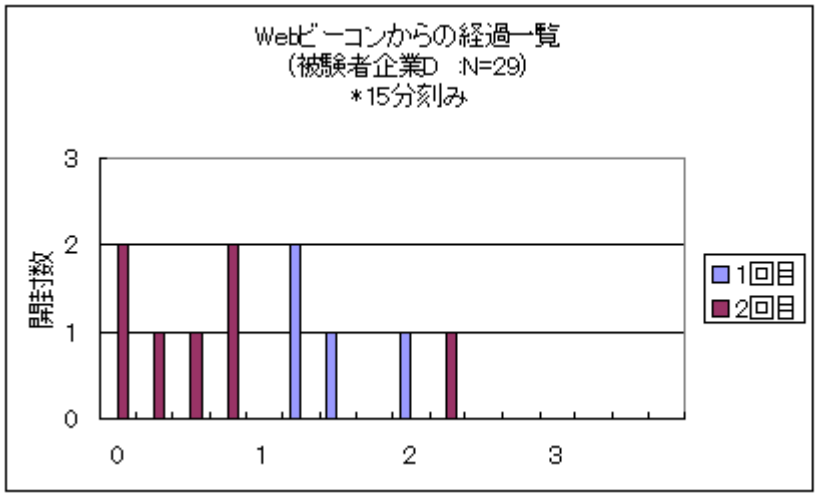


図 37 被験者企業 D：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



6.6. 予防接種実施時の特記事項

6.6.1. 偵察アクセス

第 1 回配信の際に、総アクセス数 15 回のうちの 8 回(53.3%)を占める偵察アクセスが見られた。
偵察アクセスの内容は、Web ビーコンの URL を切り詰めて親ディレクトリの内容を表示させようとするものが主体である。
このような偵察アクセスを行うためには、それ相当の知識を持ち合わせている必要がある。被験者企業 D の技術力を示したものと言えるだろう。

なお、第 2 回配信では、一人の被験者が複数回に渡って添付ファイルを開封することはあったが、偵察アクセスは見られなかった。第 1 回配信の際に偵察アクセスを行った被験者であっても、同じパターンなので興味の対象にならなかったためであろう。

6.7. 被験者アンケートの集計

被験者企業 D の被験者アンケートの集計状況について表 26 に記す。

被験者数 29 名に対して 8 名(27.6%)からアンケートの回答があった。
なお、2 回とも擬似攻撃メールに気付かなかった回答はなかったため、被験者アンケートの有効回答数を 8 名とする。

被験者アンケート有効回答の中で、一度でも添付ファイルを開いたと答えている被験者は 3 名(37.5%)であり、第 1 回配信で開封した者は 2 名(25%)、第 2 回で開封した者は 1 名(12.5%)、両方を開封した者は 0 名(0%)であった。

表 26 被験者企業 D：被験者アンケート回答者の開封状況

有効回答数	8 名	
	第 1 回	第 2 回
開封した人数	2 名(25.0%)	1 名(12.5%)
2 回とも開封した人	0 名(0%)	

前節の Web ビーコンから見た開封率と比較すると、本節の被験者アンケート回答者の開封率は異なる傾向を示している。

すなわち、第 1 回配信では 13.8%対 25.0%、第 2 回配信では 24.1%対 12.5%である。したがって、第 1 回配信よりも第 2 回配信の方が Web ビーコンから見た開封率では高いが、被験者アンケートの有効回答で見た開封率では逆の結果となった。

全被験者数が比較的少ないために 1 回答の百分率への寄与が大きい点や、情報セキュリティに相当詳しい被験者群であったと思われる点などを考慮しても、開封率逆転の理由はよくわからない。

6.8. 被験者アンケートの分析

本節では、被験者企業 D の被験者アンケートの内容から、その特徴となる諸点を示す。

6.8.1. 添付ファイル開封の有無とその理由

以下では、被験者アンケートの設問 C-4 や C-6 などから、擬似攻撃メールの添付ファイルを開封した状況を調べる。

図 38 にあるように、第 1 回配信では、有効回答数 8 名中の 2 名(25.0%)が添付ファイルを開封したと回答している。

しかし、設問 C-5 からその理由を探すと、2 名とも添付ファイルの内容を技術的に確認してから開封しているので、本物の標的型メール攻撃であったとしても実際には被害は出ないであろう。なお、この 2 名は、第 2 回配信では開封していない。

図 39 にあるように、第 2 回配信の開封者は、有効回答数 8 名中の 1 名(12.5%)である。設問 C-7 からその理由を探すと、「差出人で、社内からと判断してしまった為」であった。

なお、この被験者の設問 C-5 に対する回答によれば、第 1 回配信の擬似攻撃メールについては「覚えていない」とのことである。

したがって、この被験者は、第 2 回配信の際に初めて擬似攻撃メールを受け取ったことになり、第 1 回配信の際の周知・教育を確認していないと言える。

このように、第 1 回配信の擬似攻撃メールに気付かなかった被験者が、第 2 回配信擬似攻撃メールを開封してしまう現象は、今年度の予防接種を通してしばしば見られた。

図 38 被験者企業 D：被験者アンケートから見た開封状況(第 1 回配信)

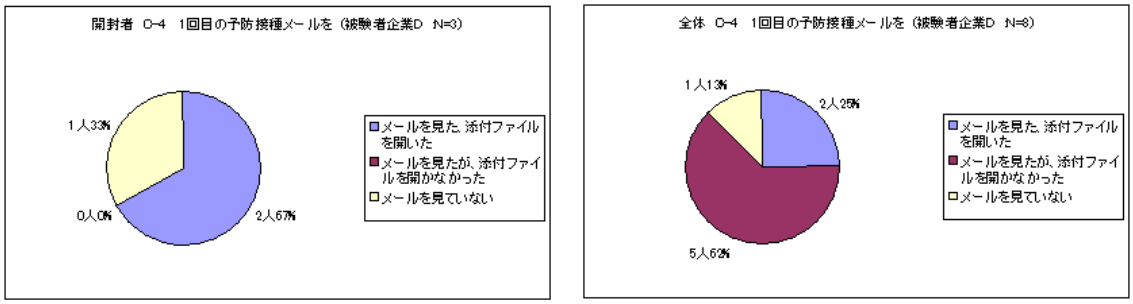
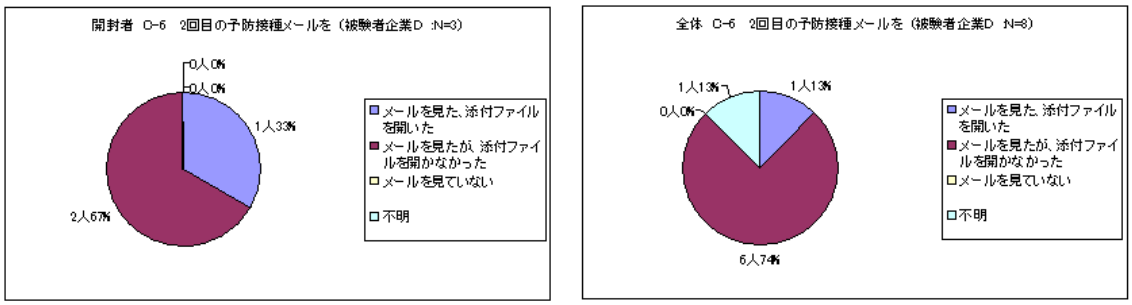


図 39 被験者企業 D：被験者アンケートから見た開封状況(第 2 回配信)



6.8.2. 情報セキュリティ教育の経験

ここでは、被験者アンケートの設問 F-1 や F-2 等から、情報セキュリティ教育の経験の有無と開封率の間にどのような関係が読み取れるかを検討する。

設問 F-1 に対する回答によれば、被験者アンケートの有効回答者 8 名のうち 3 名(37.5%)が現在の勤務先でセキュリティ教育を受けている。また、受講経験がないと答えたのも 3 名(37.5%)である。

前者の 3 名のうちの 1 名が添付ファイルを開封しているのに対し、後者の 3 名では 2 名が開封している。サンプル数が少ない点に注意は必要ではあるが、セキュリティ教育の効果が現れたという結果になっている。

設問 F-1 に対する回答状況を図 40 に掲げておく。

設問 F-2 では、有効回答者数 8 名のうち、セキュリティ教育が役にたったと答えた被験者は 2 名(25.0%)と低い比率に留まり、セキュリティ教育が役に立たなかったと答えた被験者が同じ 2 名(25.0%)、わからないと回答している被験者が最多の 3 名(37.5%)であった。

これは、被験者企業 D が情報セキュリティサービス企業であることもあって、セキュリティ教育の内容について厳しい意見を持っているために現れた結果ではないかと思われる。

設問 F-2 に対する回答状況を図 41 に掲げておく。

図 40 被験者企業 D：情報セキュリティ教育の経験

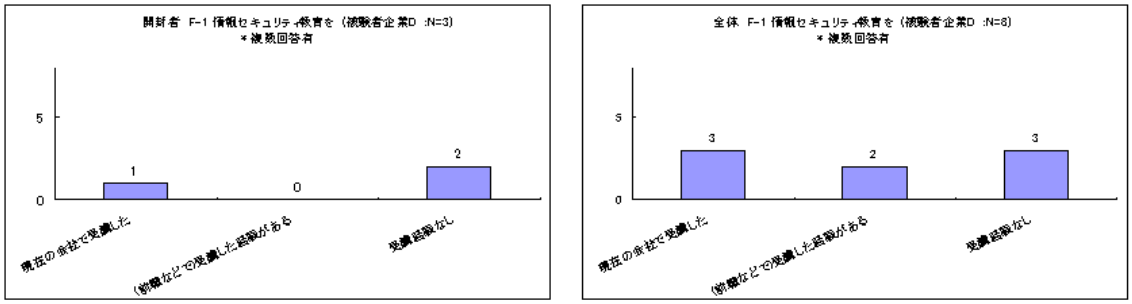
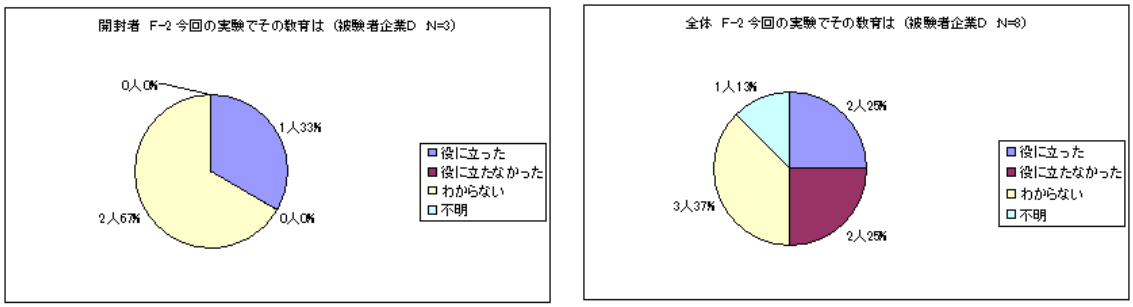


図 41 被験者企業 D：情報セキュリティ教育の有効性



6.8.3. もし標的型メール攻撃がきたらどう対処するか

被験者アンケートの設問 C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようなことが起きると思われるかを検討する。

被験者アンケートの設問 C-3 に対する回答によれば、有効回答 8 名中の 6 名(75.0%)が、最寄りのセキュリティ担当者に連絡すると回答している。これは、インシデント報告の義務意識が高く、連絡体制が被験者に浸透しているからだと考えられる。図 42 に、設問 C-3 に対する回答状況を掲げておく。

しかし、設問 C-3 とほぼ同じ内容について文言を変えて再び訊いた設問 F-3 では、管理者に連絡すると答えた験者が 8 名中の 2 名(25%)となり、設問 C-3 とは異なる傾向となった。図 43 に設問 F-3 に対する回答状況を掲げておく。

これは、「標的型メール攻撃を受け取ったと判断したら連絡する」という被験者であっても、今回の予防接種のような「気付きのポイントがわかりやすく、攻撃としては出来が悪い」レベルの脅威であれば、必ずしもインシデント報告をするとは限らないと解釈できる。

であるならば、インシデント報告をするべきかしなくても良いかを、個々の被験者が下しているという可能性がある。インシデントハンドリングを教条的に解釈すれば、どんなレベルの脅威であっても報告するべきだということになるが、現実的な妥協点を探るべき論点であろう。

図 42 被験者企業 D：もし標的型メール攻撃が来たら

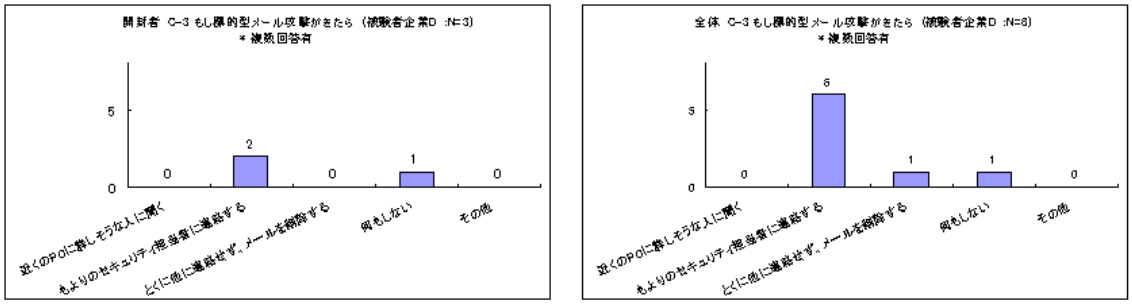
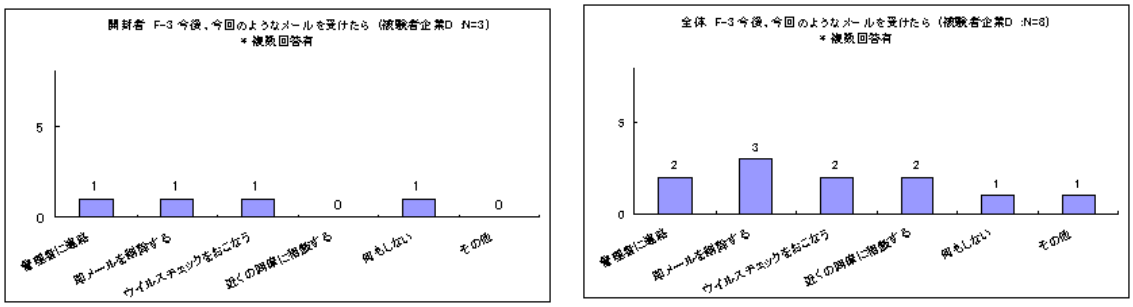


図 43 被験者企業 D：今後、今回のようなメールを受けたら



6.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4 に対する回答から、予防接種を体験することで、被験者の危機管理意識がどのように変化したかを検討する。

設問 F-4 に対する有効回答者 8 名の中で、危機管理意識が高まったと感じている被験者は 3 名(37.5%)である。残りの 5 名(62.5%)は、普段から注意しているため危機意識はかわらない等と回答している。

被験者企業 D は情報セキュリティを専門に提供する会社であるためか、その従業員のセキュリティ意識が高いということがわかる結果となった。

6.8.5. 感想

被験者アンケートの設問 G(自由記述の感想)に対する回答から、被験者が予防接種をどのように受け止めているかを検討する。

設問 G の有効回答者 8 名の全員が、予防接種を肯定的に受け止めていることがわかった。

注目すべき意見としては、将来に本物の標的型メール攻撃が来た場合に、「これも訓練である」と誤解して対応を誤る可能性を懸念するものが見られた。

また、Web ビーコンから見ると第 1 回配信よりも第 2 回配信の方が開封者が多いという逆転現象を説明するためのヒントになるかも知れない意見も頂いた。

以下にその内容を掲載しておく。

1. メールヘッダや添付ファイルデータをよく見ると、ファイルを開かずとも実験であることが明らかだったので、周りを見ていると安全であることをわかったうえで興味本位で添付ファイルを開いているケースがありました。ファイルを開いた人数のカウントに影響があるのかもしれないです。
2. 一方で、今回の予防接種訓練と似た本物の攻撃が来たときが怖いです。「また訓練か」と思われないよう、今回の訓練内容についてや今後はどう対応したらよいかなどについて研修を行うなど、十分なアフターフォローが欲しいです。

6.9. 被験者企業アンケートと被験者企業インタビュー

ここでは、被験者企業 D について、被験者企業アンケートと被験者企業インタビューの結果を分析・検討する。

まず、被験者企業 D が情報セキュリティ関連のサービスを提供する専門会社である事から、自社のセキュリティの体制は相当程度に整っていることがわかる。

また、セキュリティソリューションの動向として、これまでの予防対策重視から今後は事後対策重視へと、軸足が移って行くであろうという見解であった。

6.10. 考察

被験者企業 D では、第 1 回配信の際に、擬似攻撃メールの内容を技術的に解析し、IPA などのインシデント報告窓口に報告すべきか否かという議論にまで到ったとの事である。被験者企業 D におけるインシデント対応の体制が十全に機能している証拠である。

このようにセキュリティ意識の高い被験者企業 D でさえも、最大で約 25%の被験者が擬似攻撃メールの添付ファイルを開封しており、標的型メール攻撃を押さえ込むのがいかに困難かということを示している。

なお、被験者企業 D では、被験者数で 29 名、被験者アンケート回答者で 8 名と被験者の数が少なく、1 被験者が指標に占める割合が大きいので、各種の指

標の値をそのまま信じると危険かもしれない。
　予防接種の被験者数は、100 名程度かそれ以上が望ましいであろう。

7. 被験者企業E

7.1. 被験者企業Eの概要

被験者企業 E は、大口から小口まで、また企業向けから一般家庭向けまで手広く事業を展開している全国規模の大手運輸業を営む企業である。

表 27 に、被験者企業 E の概要について示す。

表 27 被験者企業 E：概要

業種	運輸業
設立	(非公開)
資本金	(非公開)
本社所在地	東京
拠点数	1,000 箇所以上
社員数	(非公開)
認証	ISO27001(部門取得)

7.2. 被験者企業Eにおける予防接種の概要

表 28 に示す日程と規模で、被験者企業 E における予防接種を実施した。

被験者企業 E の被験者は、情報システム部門に所属する 70 名である。

被験者企業 E は、当該情報システム部門において ISO27001 認証を取得しており、被験者は ISO27001 体制の一環としてのセキュリティ教育を受けている。

また、今回の予防接種に際しては、事前教育は特に実施していない。
第 1 回配信と第 2 回配信の間に、窓口担当者から被験者へ周知・教育を行った。その内容は、次の点である。

1. 予防接種を実施したことの事後通知
2. 標的型メール攻撃の概要説明
3. 標的型メール攻撃についての注意喚起

表 28 被験者企業 E：予防接種の実施日時と被験者数

	第 1 回配信	第 2 回配信
配信日時	2008/11/26 13:00	2008/12/10 13:00
種明かし	2008/11/28 16:00	2008/12/10 16:00
被験者数	70 人	70 人

7.3. 擬似攻撃メールの内容

7.3.1. 第 1 回配信の擬似攻撃メール

第 1 回配信で用いた擬似攻撃メールをリスト 1 に示す。

この擬似攻撃メールは、イントラネットの活用状況を問うアンケートを装うものとし、配信の翌々日を締め切りとして指定することで添付ファイルの開封を急がせるものとした。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「社内サービス見直しチーム」とした。この組織は実在せず、架空の社内組織ということになる。
2. 差出人のメールアドレスは censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 呼びかけが「各位」となっていて宛先の個人の名前を呼んでいない点や、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 18 被験者企業 E：第 1 回配信の擬似攻撃メール

```
From: 社内サービス見直しチーム <censusteam@(フリーメール A)>
Subject: 社内アンケートに関するご協力のお願い

各位
社内サービス改善に関する検討の一環として、イントラの活用状況に
関して社内アンケート調査を行います。
添付のファイルにご記入の上、11 月 28 日(金)15 時までにご回答ください。
お忙しいところ恐縮ですが、ご協力をお願いいたします。

添付ファイル名:アンケート票.doc
```

7.3.2. 第 2 回配信の擬似攻撃メール

第 2 回配信の擬似攻撃メールをリスト 19 に示す。
このメールは、リスト 2 のサンプル(8)を参考にして作成した。

擬似攻撃メールの本文では、比較的よくある姓(高橋・渡辺)に対する呼びかけを行い、「秘密監査」の結果報告を装うものとした。宛先となった被験者から見ると、重要なメールが誤った宛先に届いたように見えるはずであり、被験者が所属する部門の秘密情報が添付されているように思うことが期待される。しかも、「問題点もいくつか指摘されている」・「至急ご確認の上」などと添付ファイ

ルの開封を誘導する文言がちりばめられている。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「川崎会計事務所」とした。この組織は実在せず、架空の社外組織ということになる。
2. 差出人のメールアドレスは moto02501@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
3. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 19 被験者企業 E：第 2 回配信の擬似攻撃メール

From: 川崎会計事務所< moto02501@(フリーメール B)> Subject: 上半期の監査結果 高橋様、渡辺様 先の上半期の貴社情報部門の秘密監査の結果について添付ファイルの通りご報告いたします。 問題点もいくつか指摘されておりますので、至急ご確認の上、ご連絡ください。 添付ファイル名:監査結果-200804-200809.doc

7.4. Webビーコンの集計結果

被験者企業 E における添付ファイルの開封状況を、Web ビーコンのアクセスログから見ると、表 29 の通りとなる。

Web ビーコンから見た開封率は、第 1 回配信での 70.0%から第 2 回配信での 5.7%へ、大幅な改善が見られた。

しかし、2 回とも開封した被験者が 2 人おり、絶対数では少数ではあるが、周知・教育を受けているにもかかわらず、開封する者は開封するという側面も見られる。(この 2 人は第 2 回配信での開封者数 4 人の半分を占める。)

また、被験者企業 E では、Web へのアクセス数と開封したと考えられる人数が一致した。これは複数回の開封や偵察アクセスなどの調査とみられる行為は行われなかったということである。

表 29 被験者企業 E：Web ビーコン集計

	第 1 回	第 2 回

被験者数	70 人	70 人
配信日時	2008/11/26 13:00	2008/12/10 13:00
種明かし	2008/11/28 16:00	2008/12/10 16:00
Web ビーコンへのアクセス総数	49 回	4 回
開封したと考えられる人数	49 人(70.0%)	4 人(5.7%)
2 回とも開封した人	2 人(2.9%)	

7.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログ見ると、被験者企業 E における時系列の添付ファイルの開封状況は、以下の通りである。

被験者企業 E では、擬似攻撃メール配信直後の約 1 時間に、ほとんどの開封者が添付ファイルを開封しているといえる。

図 44 に、被験者企業 E の第 1 回配信および第 2 回配信について、その配信日時後 3 日分の開封数を 1 時間刻みのヒストグラムとして示す。同様に、図 45 には、4 時間分の開封数を 15 分刻みで示す。

図 44 被験者企業 E：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

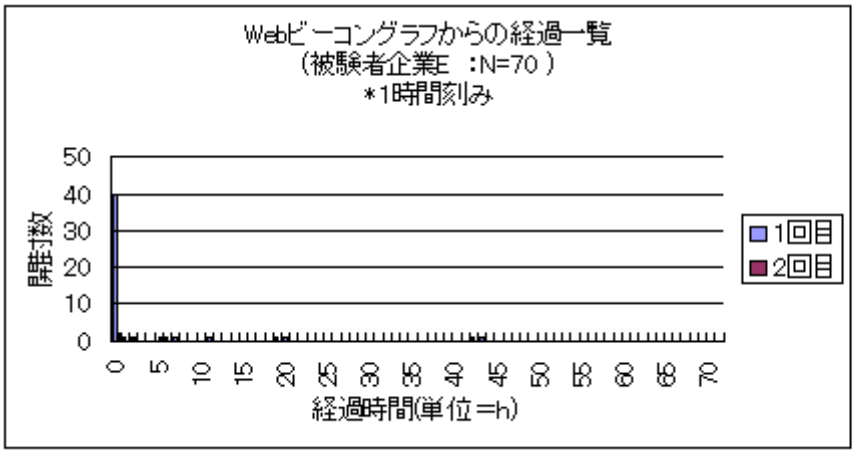
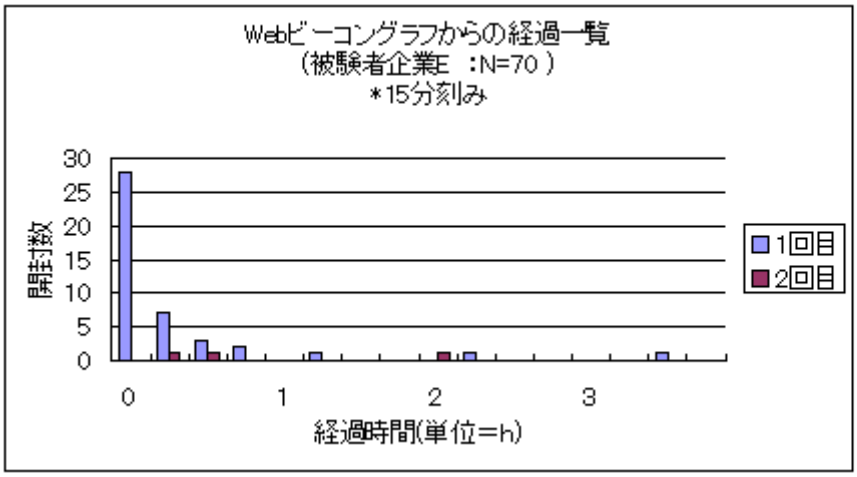


図 45 被験者企業 E：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



7.6. 実施時の特記事項

特になし。

7.7. 被験者アンケートの集計

被験者企業 E の被験者アンケートの集計状況についてに示す。

表 30 被験者企業 E：被験者アンケート回答者の開封状況

有効回答数	46 名	
	第 1 回	第 2 回
開封した人数	33 名(71.7%)	2 名(4.3%)
2 回とも開封した人	1 名(2.2%)	

被験者数 70 名に対し、47 名(67%)からアンケートの回答があった。このうち、1 名が擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答数を 46 名とする。

表 30 にあるように、被験者アンケート回答者の中で、一度でも添付ファイルを開いたと答えている被験者は 34 名(73.9%)である。このうち、第 1 回配信で開封した被験者は 33 名(71.7%)、第 2 回で開封した被験者は 2 名(4.3%)、両方を開封した被験者は 1 名(2.2%)であった。

前節で Web ビーコンから開封率を見たが、本節の被験者アンケートの回答から見た開封率と比べてさほどの違いがない。すなわち、第 1 回配信については 70.0%対 71.7%、第 2 回配信では 5.7%対 4.3%である。したがって、開封者の比率という観点から見る限り、被験者アンケートの有効回答の内容は被験者全体

の姿をほぼ忠実に反映していると言えよう。Web ビーコンの解析からは開封率以外の属性を読みとることができないので、以下では被験者アンケートの有効回答の内容が、被験者全体の姿をほぼ忠実に再現しているものと仮定することにする。

7.8. 被験者アンケートの分析

本節では、被験者企業 E の被験者アンケートの有効回答の内容から、その特徴となる諸点を示す。

7.8.1. 添付ファイル開封の有無とその理由

被験者アンケートの設問 C-4, C-6 等から、擬似攻撃メールの添付ファイルを開封した状況を調べる。

まず、設問 C-4 と設問 C-6 について、被験者アンケートの集計結果を図 46 と図 47 にグラフで示しておく。

図 46 被験者企業 E：被験者アンケートから見た開封状況(第 1 回配信)

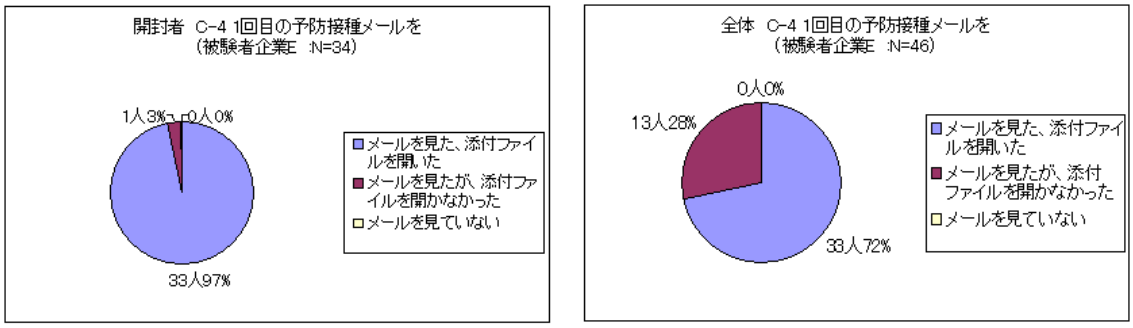
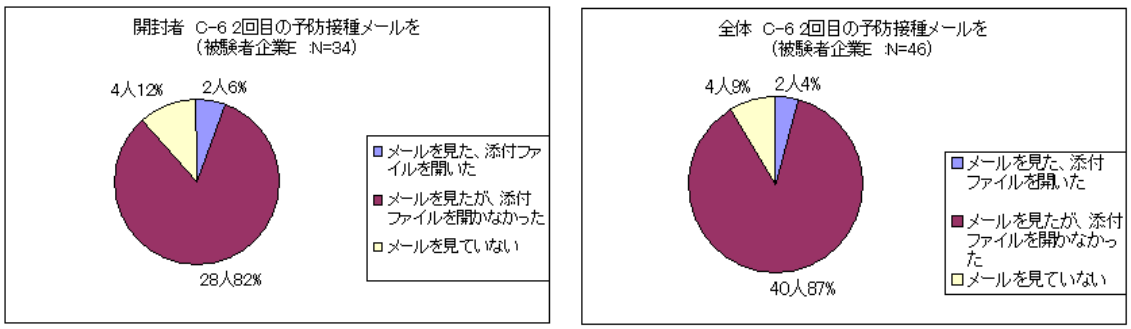


図 47 被験者企業 E：被験者アンケートから見た開封状況(第 2 回配信)



被験者アンケートの設問 C-4 に対する回答から、第 1 回配信では、有効回答 46 名中の 33 名(72%)が添付ファイルを開封したと回答している事がわかる。

開封者が添付ファイルを開封するに至った理由を、設問 C-5 から探ると、以

下の傾向を読み取ることができる。

1. 擬似攻撃メールの本文が一般的な社内連絡と区別がつかなかった。
2. 差出人の表示名だけを見てメールアドレスの確認を怠り、結果として安易に信用してしまう。
3. 宛先の表示名に自分の名前が入っていると、送信者が自分を知っている人であると誤解して、メール内容を疑わない傾向にある。

第 2 回配信では、図 47 にあるように、有効回答 46 名中の 2 名(4.3%)が添付ファイルを開封したと回答している。
第 1 回配信の結果と比較すると開封者が大幅に減少しており、第 1 回配信での体験とその後の周知・教育の効果が認められる結果となった。

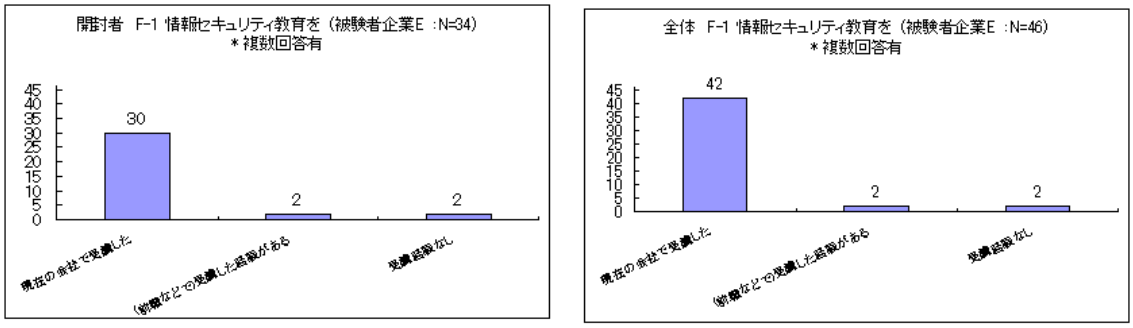
第 1 回配信では添付ファイルを開封したが、第 2 回配信では開封しなかったという被験者が、どういう理由で添付ファイルを開かなかったのかを設問 C-7 に対する回答から検討した。
この結果、多くの当該被験者は、差出人の表示名やメールアドレスを仔細に確認していたり、メール本文の内容が本当に自分に関係あるのか否かを注意深く確認したりしていることがわかった。
これは、第 1 回配信とその後の周知・教育の効果があったという仮説を支持するものである。
ただし、第 2 回配信ではメール本文中の呼びかけ相手が被験者本人ではなかったので、これが原因となって第 2 回配信の差出人を細かく確認した状況も読み取ることができる。

第 2 回配信で添付ファイルを開封した 2 名の被験者について、設問 C-7 に対する回答から開封の理由を検討する。
この 2 名のうちの 1 名は予防接種メールだと判断して、したがって添付ファイルを開いても安全だと思い、興味本位で添付ファイルを開封したと回答している。もう 1 名は社歴 7 ヶ月の派遣社員で、「まだ知らない社内調査だと思い込んだ」結果、添付ファイルを開封している。このような社歴の短い社員は社内の状況をよく把握できておらず、メール本文が業務に関係ありそうだと判断する基準が曖昧で、多少疑わしくてもメールの内容にしたがってしまう心理が読み取れる。

7.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

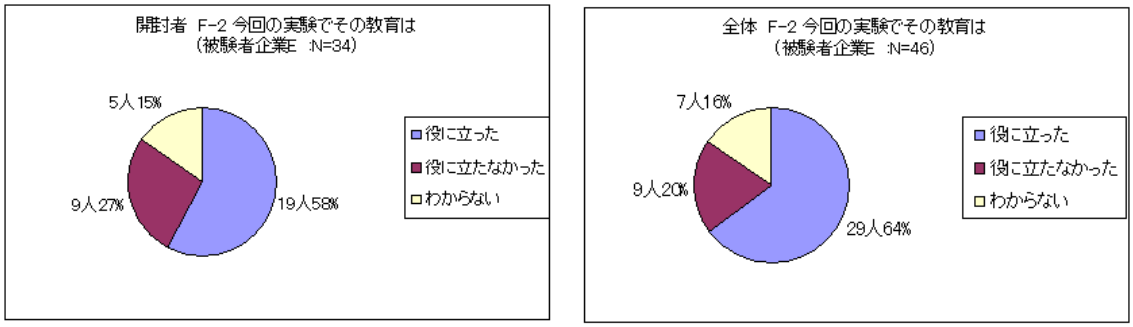
図 48 被験者企業 E：情報セキュリティ教育の経験



被験者アンケートの設問 F-1 の結果を図 48 に示す。

これによれば、被験者アンケート有効回答者 46 名中の 42 名(91.3%)は現在の勤務先で情報セキュリティ教育を受けていることがわかる。
この 42 名の中の 30 名(71.4%)が、第 1 回配信または第 2 回配信の際に、擬似攻撃メールの添付ファイルを開封している。
なお、現在の勤務先で教育を受けたと答えていない 4 名は、その全員が添付ファイルを開封している。

図 49 被験者企業 E：情報セキュリティ教育の有効性



同様に、設問 F-2 の結果を図 49 に示す。

これによれば、会社で受けた情報セキュリティ教育が IT セキュリティ予防接種に対して役に立ったと回答している被験者は、有効回答者 46 名中の 29 名(64%)である。しかし、開封者 34 名の中でも 19 名(58%)と過半を占めている。
教育が役に立ったけれども添付ファイルを開いてしまったというのは、互いに矛盾していて解釈が難しいところである。

ここで、被験者アンケートの設問 F-4(危機管理意識の変化)と設問 G(感想)への回答を見ると、予防接種を体験することによって、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したという記述が多い。
予防接種のような体験型の訓練には、知識としては理解していた(またはその

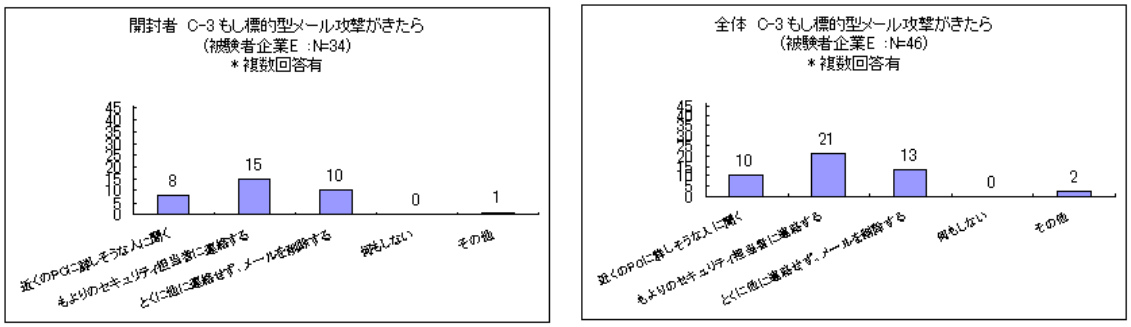
つもりになっていた)セキュリティ教育の内容を体得させる効果があるといえるのではないか。

7.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのような反応を示すと思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答を見ると、今後組織に標的型メール攻撃が行われるかもしれないと回答している被験者は、有効回答者数に対して 61%の割合を占める。
今回の予防接種で、実際の攻撃とほぼ同様の擬似的攻撃を受けて、あらためて脅威を認識したということであろう。

図 50 被験者企業 E：もし標的型メール攻撃が来たら



設問 C-3 に対する回答を図 50 に示す。

これによれば、標的型メール攻撃を受けた場合の対処方法として、「最寄りのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 46 名中の 21 名(45.7%)である。
他方で、46 名中の 13 名(28.3%)の被験者が、「とくに他に連絡せずに削除する」と回答している。

ISO27001 対応の運用規定では、しばしばインシデント報告が義務づけられる。
では、どの程度被験者が実際にこの種の報告を行うのかを考えると、上記を見る限りでは、およそ半分の被験者が届け出るだけであると言える。

図 51 被験者企業 E：今後、今回のようなメールを受けたら

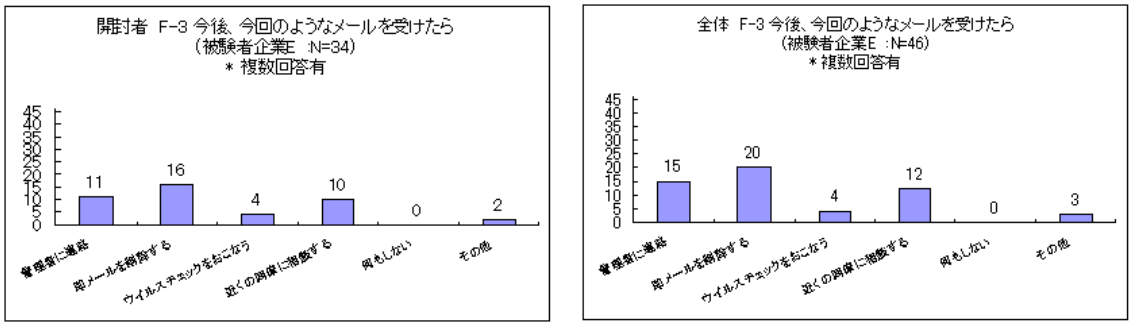


図 51 には、設問 F-3 に対する回答を示した。設問 F-3 は、前述の設問 C-3 とほぼ同じ内容について、表現を変えて再質問するものである。

設問 F-3 への回答から見ると、標的型メール攻撃を受けた場合の対処方法として「セキュリティ管理者に連絡する」と回答した被験者が有効回答 46 名中の 15 名(32.6%)となり、先の C-3 での回答よりも比率が下がっている。

逆に、「即メールを削除する」と回答している被験者は 46 名中 20 名(43.5%)と増加している。

この誘導では、証拠保全し管理者に連絡することの重要性が認識される方向には向かわず、危険なメールは削除すればよいという考え方に流されているようだ。

7.8.4. 危機管理意識の変化

ここでは、被験者アンケートの設問 F-4 に対する回答を用いて、被験者の危機管理意識が変化したか否かについて調べる。

設問 F-4 に対する回答者 37 名中の 35 名(94.5%)の被験者が、今回の予防接種を通して、危機管理意識に変化があった、もしくは、危険の再認識をしたと回答しており、予防接種を肯定的にとらえている。

また、予防接種による学習が効果的であると評価する記述もあったので、一部を抜粋しておく。

1. 標的型メール攻撃および迷惑メール等の危険なメールは、通常は英語(日本語以外)でくるものだという固定観念を持っていたが、それは違うということを学んだ被験者が 2 名いた。
2. メールソフトの送信者の欄には表示名しか表示されないことに気付いた被験者が 1 名いた。

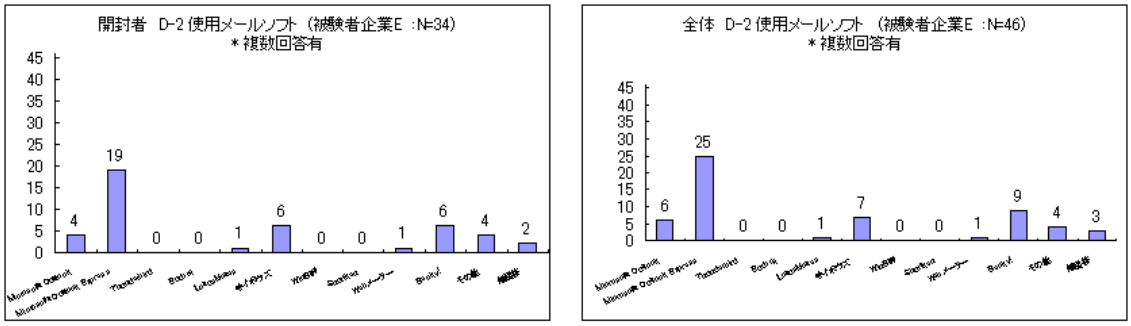
7.8.5. 使用メールソフト

被験者アンケートの設問 D-2 に対する回答を図 52 に示す。

設問 D-2 の回答を見ると、被験者企業 E では、Outlook Express・Becky!・サイボウズの順に使用者が多いことがわかる。

しかし、有効回答者全体とその内の開封者について、メールソフトの構成比率に顕著な差がない。したがって、使用しているメールソフトによって、標的型メール攻撃に対する耐性が異なるとは言えないことがわかる。

図 52 被験者企業 E：メールソフト

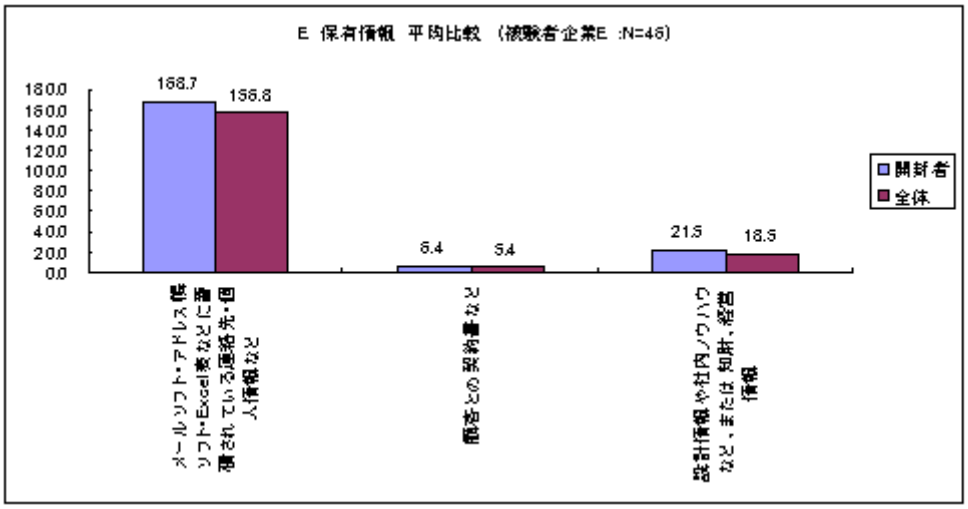


7.8.6. 保有情報数

被験者アンケートの設問 E から各被験者の保有情報数の平均を図 53 に示す。

有効回答者全体の平均よりも開封者の平均の方が、僅かに多いという結果が得られた。

図 53 被験者企業 E：保有情報数の平均



7.8.7. 感想

ここでは、被験者アンケートの設問 G に対する回答から、メッセージを読みとることを試みる。

設問 G の回答者は 24 名で、このうち 18 名(75%)の被験者が、今回の予防接種訓練を肯定的に捉えており、再実施や実施方法の工夫を提案している。

中には以下のように、システム側で対策することを期待する意見や、社内のメール標準ソフトの切り替えを提案する意見が見受けられたので、抜粋しておく。

1. 3～4 年前に迷惑メールが大量に届いていたことがあり、その当時は開くメールや添付ファイルに細心の注意を払っていたが、現在はスパムメール検知の仕組みが導入され、そのようなメールが各個人まで届かなくなっていたため、逆にメール関連のセキュリティには安心しきっていました。
2. スパムメールや DoS 攻撃等のメールは、メールサーバにてチェックすることはできないのでしょうか？
3. 現状のメールソフトでは、表示名だけで判断してしまうのではないかと思う。まずは、社内標準メールソフトの切替が、必要ではないかと思う。

7.9. 管理者アンケートと被験者企業インタビュー

被験者企業 E について、被験者企業アンケートと被験者企業インタビューから以下のことがわかった。

まず、被験者企業アンケートから以下の点がわかるので、被験者企業 E では情報セキュリティ体制は概ね整っていると言える。

1. ISO27001 認証を取得している。
2. 情報セキュリティの管理体制はほぼ整備されており、インシデントの連絡体制(窓口)も定められている。
3. 定期的な情報セキュリティ教育を実施している。

また、被験者企業インタビューの際に、窓口担当者から以下の意見・感想を得た。

1. (情報セキュリティ教育について)現在使用している教育の資料は網羅的に記述されている。このため、受講者の記憶に残りにくいという問題がある。予防接種は体験型なので強く記憶に残る。
2. 予防接種を社内で広く実施する場合には、事前事後の周知・教育

が必要かつ重要である。
3. 情報技術に縁遠い層を対象とする時には、「いったいこれは何をやっているのか」「どういう趣旨で実施するのか」といった内容を噛み砕いて事前に説明しないと、効果が得られないのではないか。
4. 事後にも何が問題でどうすれば良いのかを彼らに理解できる表現で的確に伝える必要がある。

という感想を窓口担当者から得ている。

この他、情報セキュリティのインシデント報告体制について、「一部のセキュリティ意識の高い従業員が連絡体制に従った対処をしている」という回答があった。
これは逆に言えば、特定の人に依存しない体制・業務フローを確立する必要があるという課題を浮き彫りにしている。
実際に今回の IT セキュリティ予防接種では、既定の報告ルートを通した報告は見られず、被験者全員が顔見知りだったためか窓口担当者へ直接問い合わせが来ていたとのことである。

企業の電子メール環境については、被験者企業 E では使用して良い電子メールソフトを指定していると回答している。
しかし、今回の被験者アンケートの結果では、指定外の電子メールソフトが相当数利用されている状況を把握できた。
また、今回の予防接種によって表示名やメールアドレスの表示方法に疑問を感じ、社内指定のメールソフトを再検討すべきという意見もでた。

他にも、メールのパスワードを定期的な変更することを義務付けていない点には、改善の余地がある。

7.10. 考察

今回は、被験者企業 E の中では IT に慣れている層に対して予防接種を実施したが、それでも第 1 回配信では開封率が非常に高かった。第 2 回配信では相当の改善が見られた点や偵察アクセスが皆無であった点を考えると、IT のセキュリティ的側面にこれまでなじみがなかったのかも知れないが、第 1 回配信での経験から学ぶ力は相当のものがあると思われる。
このような被験者であっても、このようなソーシャルエンジニアリングを利用した攻撃が不意に来た場合に、完全に防ぐことは非常に困難であることが再確認された。
特に、自社の内部から送られたと思われるメールを疑う意識が稀薄である点が目立った。

第 2 回配信は開封率が下がり、第 1 回配信での体験や第 1 回配信実施後の周知・教育が教育効果をあげたと思われる。

被験者アンケートの回答からも、今回の IT セキュリティ予防接種により、セキュリティのチェックポイントをあらためて認識したという回答が多く見られた。

このことから、今回の予防接種は、不審なメールの見分け方の意識づけに効果があったと思われる。

8. 被験者企業F

8.1. 被験者企業Fの概要

被験者企業 F は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付・対応の支援・発生状況の把握・手口の分析・再発防止のための対策の検討や助言などを、技術的な立場から行う独立かつ中立の組織である。

表 31 に、被験者企業 F の概要について記す。

表 31 被験者企業 F：概要

業種	情報処理・提供サービス業
設立	1996 年 10 月
資本金	―
本社所在地	東京
拠点数	1 箇所
社員数	約 25 名
認証	なし

8.2. 被験者企業Fにおける予防接種の概要

被験者企業 F に対する予防接種を、表 32 に示す日程と規模で実施した。

被験者企業 F の被験者は 25 名で、ほぼ全職員である。

被験者企業 F は、情報セキュリティの専門機関であるという組織の性格上、ほぼ全員が日々情報セキュリティの最新情報を取り扱い、情報共有している。
そのため、被験者企業 F では、定期的な情報セキュリティ教育は行われていない。
また、同じ理由で今回の予防接種における事前教育を行わなかった。

被験者企業 F は、2007 年度も予防接種を実施している。

なお、予防接種としては例外的に、被験者の個人アドレスに宛ててではなく、組織内メーリングリストのアドレスに対して配信した。

表 32 被験者企業 F：予防接種の実施日時と被験者数

	第 1 回	第 2 回
被験者数	25 名	25 名
配信日時	2008/12/5 13:00	2008/12/19 13:00

種明かし	2008/12/5 17:50	2008/12/22 午前

8.3. 擬似攻撃メールの内容

8.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 F における第 1 回配信の擬似攻撃メールをリスト 20 に示す。

この擬似攻撃メールの文面については、被験者企業 F の窓口担当者と打ち合わせの上で作成した。

この擬似攻撃メールは、架空の 0-day 脆弱性について再現・検証のための環境が不足しており、被験者の手元の環境で再現試験をするように依頼している。被験者企業 F の日頃の業務の中でも緊急性の高い内容であると装って、添付ファイルの開封を促すものである。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「JPCERT/CC 再現検出班」とした。「JPCERT/CC」は被験者企業 F の実名であるが、「再現検出班」は実在せず、架空の社内組織ということになる。
2. 差出人のメールアドレスは office@jpcert.or.jp とした。これは被験者企業 F のドメインのメーリングリストのアドレスであるが、実際にはほとんど使われていない。
3. 本文冒頭の呼びかけが「社員各位」となっているが、被験者企業 F では「職員」と呼ぶことが普通である。
4. 本文中の「MS08-078」は Microsoft 社が用いる脆弱性情報の番号の命名規則に則っているが、配信の時点ではまだ使われていない番号である。同様に、表題にある日付「12 月 16 日」も未来の日付である。
5. 本文中の「patchtesters@jpcert.or.jp」は、被験者企業 F のドメインを用いたメーリングリストのアドレスに見えるが、実在しない。また、このアドレスが「再現検証班」という架空名と対応するように配慮した。
6. 他には、差出人の氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する

リスト 20 被験者企業 F：第 1 回配信の擬似攻撃メール

```
From: JPCERT/CC 再現検出班 < office@jpcert.or.jp >
Subject: 実験台募集（12 月 16 日の Microsoft セキュリティ情報の検証）

社員各位：
```

先日公表された 2008 年 12 月度の Microsoft 社のセキュリティ情報について
検証環境が不足しています。
恐縮ですが、みなさんのお使いになっている PC で再現試験をお願いできれば
助かります。

MS08-78 は「Microsoft Office の脆弱性により、任意のコードが実行される」
というもので、あるシーケンスにしたがって Microsoft Excel を操作するこ
とによって制限ユーザから特権ユーザへの権限昇格が可能となるものです。
具体的な手順を添付ファイルに示しますので、お手元の環境で実際に権限昇格
が可能か否かを実験してください。
手順書の末尾に結果報告用のシートがありますので、これに記入後
patchtesters@jpcert.or.jp まで返送をお願いします。

お忙しいところをすみませんが、よろしくお願いします。

再現検証班

添付ファイル名:MS08-78_検証手順.doc

8.3.2. 第 2 回配信の擬似攻撃メール

リスト 21 に、被験者企業 F における第 2 回配信の擬似攻撃メールを示す。

この擬似攻撃メールは、架空の業界新聞の創刊を装い、その創刊号に論文を寄稿するように依頼するものである。被験者企業 F の中心的業務のひとつである情報セキュリティの分野での新聞創刊ということで、被験者の論文作成意欲を刺激し、論文募集要項を装った添付ファイルを開くように誘導している。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「日本セキュリティ新聞編集部」とした。この組織は実在しない。
2. 差出人のメールアドレスは moto02501@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
3. 本文中の日付「2008 年 12 月 04 日」は、第 2 回配信の 15 日も前のものであり、攻撃者が同じ文面を何回も使い回している状況を暗示している。
4. その他、差出人の氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 21 被験者企業 F：第 2 回配信の擬似攻撃メール

From: 日本セキュリティ新聞 編集部<moto02501@(フリーメール B)>
Subject: 創刊第 1 号寄稿のお願い

拝啓　時下ますますご清栄のこととお喜び申し上げます。

このたび私ども日本セキュリティ新聞社では、来る 2009 年 1 月 1 日に「日本セキュリティ新聞」を創刊し、日本のセキュリティの今を伝える日刊紙としてみなさまのお役に立ちたいものと創業の意気に燃えております。

創刊 1 号では、広くセキュリティの専門家のみなさまの論文を募集して「日本のセキュリティは今！！」という企画にまとめたいものと思っております。つきましては、本メールをごらんのみなさまにおかれましては、日頃の持論を記事にまとめてご応募いただきますようにお願い申し上げます。論文募集の詳細につきましては、添付のファイルをご覧ください。

お忙しい中を大変恐縮ではございますが、なにとぞご協力賜りますようにお願い申し上げます。

略儀ながら、まずは書中をもってご案内申し上げます。

敬具

2008 年 12 月 04 日

日本セキュリティ新聞社 編集部

添付ファイル名:論文募集要項.doc

8.4. Webビーコンの集計結果

被験者企業 F について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 33 に示す。

被験者企業 F で添付ファイルを開封した被験者の数と比率は、第 1 回配信での 2 名(8.0%)から第 2 回配信での 1 名(4.0%)へ改善している。
また、2 回とも開封した被験者はいなかった。

なお、開封者の全員が、技術的に添付ファイルの中身を調べて安全を確認してから開封していることが、被験者アンケートや被験者企業インタビューから判明している。

表 33 被験者企業 F : Web ビーコン集計

	第 1 回	第 2 回
被験者数	25 名	25 名
配信日時	2008/12/5 13:00	2008/12/19 13:00
種明かし	2008/12/5 17:50	2008/12/22 午前
Web ビーコンへのアクセス総数	7 回	1 回
開封したと考えられる人数	2 名(8.0%)	1 名(4.0%)
2 回とも開封した人	0 名(0.0%)	

8.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 F における擬似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業Fは､情報セキュリティに関する専門家集団ということもあって、ほぼ全員が擬似攻撃メールを標的型メール攻撃であると見抜いており、結果として開封が非常に少ない。

数少ない開封者も、添付ファイルにマルウェアが存在しないことを確認して、添付ファイルに何が書かれているかを知りたいという好奇心から開封しているという状況である。

図 54 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 55 に示す。

図 54 被験者企業 F：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

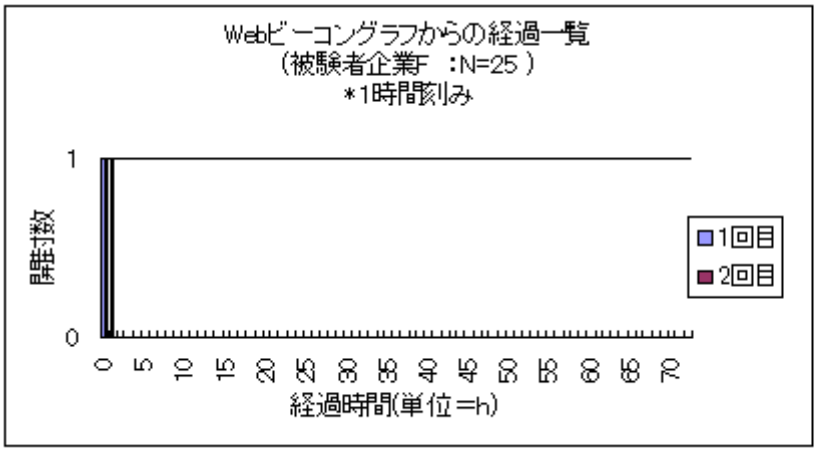
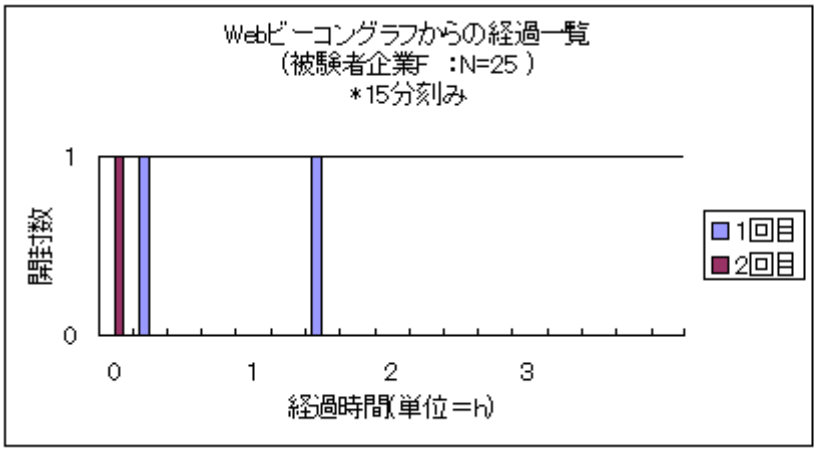


図 55 被験者企業 F：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



8.6. 予防接種実施時の特記事項

8.6.1. メーリングリストへの配信などの例外的方法

被験者企業 F では、被験者個々のメールアドレス宛ではなく、7 個のメーリングリストに対して配信が行われた。

これは、予防接種手法としては例外的である。しかし、対象となる被験者の人数が少ないこと、および、被験者企業 F の社内 LAN における IP アドレス割り当て方法から Web ビーコンのアクセスログに記録されたアクセスを個々の被験者に対応付けることができることから、実験的にメーリングリストへの配信を試みた。

なお、被験者企業 F では、Web ビーコンのログ収集サーバを被験者企業 F 内部に設置して上記の IP アドレスと被験者の対応付けに備えた。

8.6.2. 第 1 回配信に対する被験者の反応

第 1 回配信の直後に窓口担当者が被験者から収集した感想は、次の通りである。

まず、第 1 回配信の擬似攻撃メール本文に、「Microsoft Excel を操作すること」で「権限昇格が可能となる」とあるが、「特権ユーザへの権限昇格は、Office 系アプリケーションの操作だけでは、技術的に不可能である」と回答した被験者がいた。

この種のセキュリティ情報に詳しい被験者企業 F だからこそ、このようなこのような感想が出てきたと言えるだろう。

次に、擬似攻撃メールの Received: ヘッダに BBSec のドメイン名が出現するところから、予防接種であると見抜いた被験者がいた。
これは、この被験者が、種々の組織内資料から予防接種プロジェクトが実施されていることや受注企業が BBSec であることなどを知っていたために起きた現象である。
しかしながら、被験者が Received:ヘッダを確認した例は非常に珍しく、情報セキュリティの専門家集団の面目躍如たるものがある。

また、本文冒頭の「社員各位」という呼びかけに違和感を感じた、とする被験者もいた。
これは、被験者企業 F では、「職員」と呼ぶのが普通であり、「社員」と呼ぶことがほとんど無い為である。

また、第 1 回配信で開封した 2 名が何故添付ファイルを開いたのか、を窓口担当者が聞き取っている。その内容によれば、開封者 2 名は両方とも、技術的な観点から安全だと判断した後に開封したとのことであった。すなわち、以下のコメントを得ている。

1. shell code が見当たらなかったので開いた。
2. 別ツールで(窓口担当者)の名前などを見付けたので開いた。

その他の被験者の感想・意見としては、種明かしメールを出すのが早かったのではないかというものがあった。メールの確認がまだそこまで追いついていない、または、後で読むつもりで取っておいた、といった被験者がいたとのことである。
この指摘は尤もなので、第 1 回配信の際の種明かしまでの時間は約 4 時間半であったが、第 2 回配信では種明かしまでの時間を約 3 日間と十分に取って実施した。

さらに、窓口担当者の感想としては、擬似攻撃メール本文が被験者企業 F の業務に直結しすぎた内容であったために、逆にその文面の些細な破綻から嘘を見抜いた被験者が多かったのではないか、とのことである。

8.6.3. 第 2 回配信に対する被験者の反応

第 2 回配信での開封者は 1 名であったが、窓口担当者によれば、おそらく予防接種と見抜いた上での冷やかしであろうということである。

また、被験者からの感想として、「第 1 回配信の擬似攻撃メールよりも第 2 回配信のものの方が、思わず開封したくなる文面であった」とのことである。
窓口担当者の感想では、第 1 回配信の擬似攻撃メールも完成度は高かったと思うが、あまりにも業務に密着した内容であったために敬遠されたのかもしれ

ない、とのことであった。

8.7. 被験者アンケートの集計

被験者企業 F の被験者アンケートの集計状況について表 34 に示す。

被験者数 25 名に対し、14 名(56.0%)から被験者アンケートに対する回答があった。回答者の中には、擬似攻撃メールに気付かなかった者はいないので、被験者アンケートの有効回答数を 14 名とする。

有効回答中で、一度でも添付ファイルを開封したと回答している被験者は 4 名(28.6%)であり、第 1 回配信で開封した被験者は 2 名(14.3%)、第 2 回で開封した被験者は 3 名(21.4%)、両方を開封した者は 1 名(7.1%)である。

なお、前述の通り、開封者は全て技術的に添付ファイルを検証した後に開封している。そのため真の意味で開封者と呼ぶべきものはいない。

表 34 被験者企業 F：被験者アンケート回答者の開封状況

有効回答数	14 名	
	第 1 回	第 2 回
開封した人数	2 名(14.3%)	3 名(21.4%)
2 回とも開封した人	1 名(7.1%)	

8.8. 被験者アンケートの分析

本節では、被験者企業 F の被験者アンケートの回答内容から、その特徴となる諸点を示す。

8.8.1. 添付ファイル開封の有無とその理由

被験者企業 F では開封者は存在するが、その全員が添付ファイルの中身を技術的に解析し、安全を確認してから開封している。

したがって、開封の理由は好奇心やいたずら心のようである。

図 56 に、被験者アンケートから見た第 1 回配信の際の開封状況を、一応示しておく。同様に、図 57 に第 2 回配信について示す。

図 56 被験者企業 F：被験者アンケートから見た開封状況(第 1 回配信)

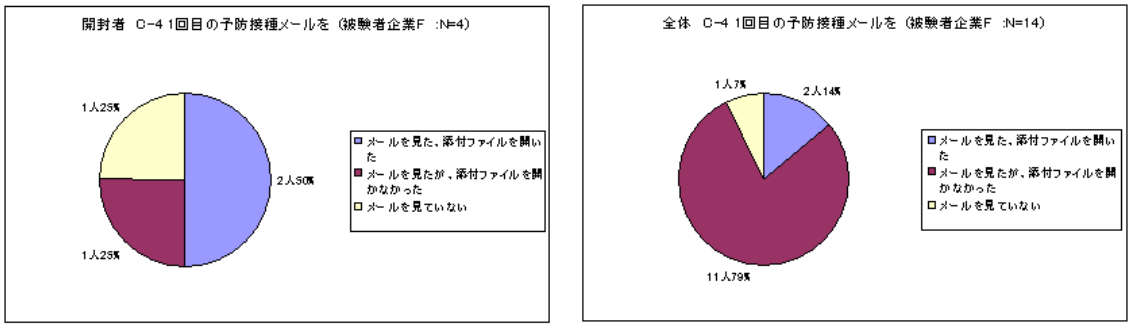
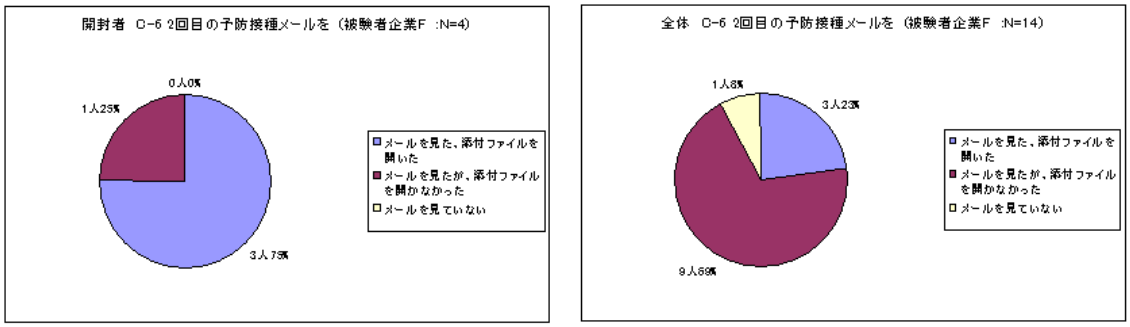


図 57 被験者企業 F：被験者アンケートから見た開封状況(第 2 回配信)



8.8.2. もし標的型攻撃がきたら、どう対処するか

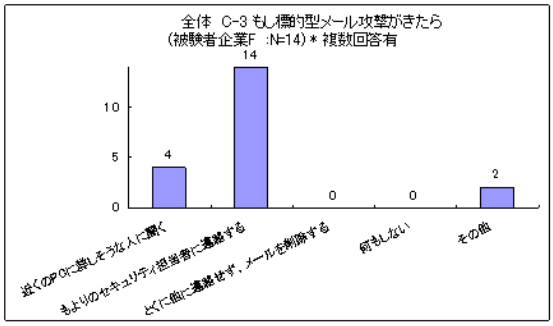
被験者アンケートの設問 C-3・F-3 などに対する回答から、本物の標的型メール攻撃があった場合にどのようなことが起きると思われるかを検討する。

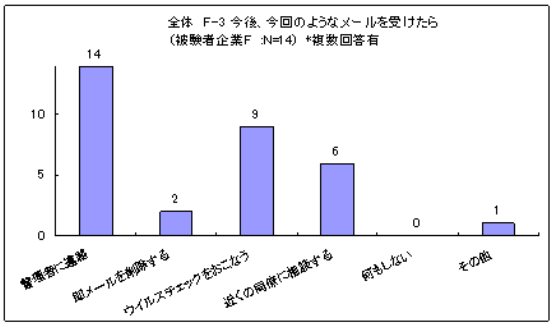
まず、設問 C-3 および F-3 への回答状況を図 58 に示しておく。

被験者企業 F では、有効回答者の全員が「管理者に連絡する」を選択しており、インシデント・ハンドリングの基本が全員に周知徹底されていることがわかる。

これは、他の被験者企業には見られない特徴である。

図 58 被験者企業 F：将来の攻撃への対処行動





8.8.3. 危機管理意識の変化と感想

これまで見てきたように、被験者企業 F の成績は優秀で、予防接種の必要がないかとまで思ったが、被験者アンケートの回答を見るとそうではないとする意見が散見される。

すなわち、このようなセキュリティ対策の専門集団であっても、予防接種を受けることで標的型メール攻撃の脅威を再認識することができたという感想や、時と場合によっては標的型メール攻撃にひっかかる可能性があるのではないかという感想が見られたのである。

8.9. 被験者企業アンケートと被験者企業インタビュー

ここでは、被験者企業 F について、被験者企業アンケートと被験者企業インタビューの結果を分析・検討する。

まず、被験者企業アンケートから、被験者企業 F における情報セキュリティポリシーや内部規則などが整備されていることがわかる。

しかし、被験者企業インタビューでは、「普段からセキュリティ情報を共有することに慣れているため、きちんとした連絡系統が決まっていない」ということが明らかになった。

組織の規模が小さいために隅々まで目が届くことと、情報技術や情報セキュリティに詳しい人員構成であることから、細々とした細則を決めなくても情報セキュリティ対策上の問題にならないことが原因であろう。

これは、専門家集団である被験者企業 F にとっては盲点とも言える問題ではないかと思われる。先に述べた規模の小ささと人員構成上の利点があるために問題として顕在化していないようだが、改善を要する点である。

8.10. 考察

被験者企業 F は昨年度も予防接種に参加しており、また、情報セキュリティ対策の専門家集団でもあるため、今回の予防接種では非常に優秀な成績であった。

しかし、専門家集団であるがゆえの問題も発見されており、また、将来に組織の規模を拡大する時には、別種の問題に直面するであろう。

9. 被験者企業G

9.1. 被験者企業Gの概要

被験者企業 G は、大手インターネットサービスプロバイダーであり、ネットワークやデータセンタなどのインフラ事業・ネットワーク機器・各種サーバ・アプリケーションなどの販売事業・ビリングサービスやセキュリティサービスなどのソリューション事業などを保守・運用も含めて提供している。

表 35 に、被験者企業 G の概要を示す。

表 35 被験者企業 G：概要

業種	電気通信事業者
設立	1985 年 9 月 4 日
資本金	40 億円
本社所在地	東京
拠点数	4 箇所
社員数	約 550 名
認証	「ISO27001」(全社取得)

9.2. 被験者企業Gにおける予防接種の概要

表 36 に示す日程と規模で、被験者企業 G に対する予防接種を実施した。

被験者企業 G は、ISO27001 を全社で取得しており、ISO27001 の体制の一環として社員向けのセキュリティ教育を実施している。今回の予防接種は、このセキュリティ教育の一環として、CSO スタッフを窓口担当者として実施した。

被験者企業 G における被験者は、人材派遣や業務委託を含む 724 名である。

今回の予防接種に際して、第 1 回配信より前に、標的型メール攻撃についての事前教育を実施している。
また、第 1 回配信と第 2 回配信の間には、予防接種を実施したという事後通知・標的型メール攻撃の概要説明・標的型メール攻撃についての注意喚起の 3 点について、窓口担当者から社内へ周知したとのことである。

表 36 被験者企業 G：予防接種の実施日時と被験者数

	第 1 回	第 2 回
被験者数	724 名	724 名
配信日時	2008/12/10 13:00	2008/12/24 13:00
種明かし	2008/12/12	2008/12/26

9.3. 擬似攻撃メールの内容

9.3.1. 第 1 回配信の擬似攻撃メール

第 1 回配信の際に使用した擬似攻撃メールをリスト 22 に示す。

この擬似攻撃メールはリスト 2 のサンプル(10)を参考にして作成した。
その内容は、自社の新サービスについてプレスリリースを行うので、顧客からの問い合わせなどに備えて、添付ファイルのリリース内容説明を読むように、というものである。13:00 に擬似攻撃メールを配信で、2 時間後の同日 15:00 にリリースがあるとしており、対応を急がせている。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「広報 高橋」とした。被験者企業 G の広報担当には高橋氏は存在しないので、架空の担当者を装うものとなっている。
2. 差出人のメールアドレスは motok2501@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 呼びかけが「皆様」となっていて宛先の個人の名前を呼んでいない点や、差出人の所属、氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 22 被験者企業 G：第 1 回配信の擬似攻撃メール

```
From: 広報 高橋<motok2501@(フリーメール A)>
Subject: 報道発表について

皆様

広報の高橋です。お世話になります。

本日午後 3 時、新サービスのプレスリリース(報道発表)を行いますので、
お問い合わせ対応等、宜しくお願い致します。
＊午後 3 時以降に HP で閲覧できます。

プレスリリース内容の詳細については添付ファイル参照

添付ファイル名:新サービスプレス.doc
```

9.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 G における第 2 回配信の擬似攻撃メールをリスト 23 に示す。

このメールは、第 2 章で説明した擬似攻撃メールのサンプル(4-2)を参考にして作成した。
その内容は、無料の「クリティカル・シンキング講座」を開くので希望者は添付ファイルの書式を使って申し込むように、とするものである。「定員が限られている」と称して、添付ファイルの開封を急がせている。また、申し込みの締め切りも擬似攻撃メール配信の翌々日となっており、開封を急がせるものとなっている。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「山本」とした。本文中にも「山本です」とだけ記し、所属部署等は記していない。
2. 差出人のメールアドレスは qa_staff903@(フリーメール D)とした。これは明らかにフリーメールのアドレスである。
3. 差出人の所属、氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 23 被験者企業 G：第 2 回配信の擬似攻撃メール

From: 山本<qa_staff903@(フリーメール D)>
Subject: クリティカル・シンキング基礎講座(無料)のご案内について

皆様

お世話になります。山本です。

社内のビジネススキル向上の一環として、「クリティカル・シンキング　基礎」講座を無料で開催します。曜日別で開催しますが、それぞれ定員が限られていますので、早めの申込みお願いします。

1. 講座内容
「クリティカル・シンキング　基礎」　全 6 回(隔週／約 3 ヶ月：1 日 3 時間)
詳細は、講座内容兼申込書参照。
2. 開催日時
1) 2009 年 1 月～3 月　隔週の水曜日 19 時～
2) 2009 年 1 月～3 月　隔週の金曜日 19 時～
3. 場所
本社ビル　会議室(予定)
4. 講師
有名講師に依頼中
5. 受講定員
1)、2)の開催とも 30～40 名(申込み先着順の予定)
6. 対象者
全社員対象(社員・派遣・委託)
7. 申込み方法
講座内容兼申込書に必要事項を記入し返信ください。
8. 期日

2008 年 12 月 26 日(金)まで

よろしくお願いします。

添付ファイル名:無料研修申込書.doc

9.4. Webビーコンの集計結果

被験者企業 G における添付ファイルの開封状況を、Web ビーコンのアクセスログから見ると、表 37 の通りとなる。

Web ビーコンから見た開封者数と開封率は、被験者数 724 名に対して第 1 回配信では 346 名(47.8%)であり、第 2 回配信では 59 名(8.1%)と、大きな改善が見られた。

しかし、2 回とも開封した被験者が 39 名(5.4%)おり、日頃のセキュリティ教育や事前教育を受けていても、開封する者は開封するという側面が見られる。

なお、この 39 名は第 2 回配信での開封者数 59 名の約 1/3 を占める。

また、被験者企業 G では、Web へのアクセス数が開封したと考えられる人数より 30%以上多い。これは同一被験者が複数回に渡って開封した他、偵察アクセスがが多く行われたためである。

表 37 被験者企業 G：Web ビーコン集計

	第 1 回	第 2 回
被験者数	724 名	724 名
配信日時	2008/12/10 13:00	2008/12/24 13:00
種明かし	2008/12/12	2008/12/26
Web ビーコンへのアクセス総数	511 回	72 回
開封したと考えられる人数	346 名(47.8%)	59 名(8.1%)
2 回とも開封した人	39 名(5.4%)	

9.5. Webビーコンログからの時系列開封状況

被験者企業 G の Web ビーコンのアクセスログから、添付ファイル開封状況を時系列で見ると、以下の通りである。

被験者企業 G では、擬似攻撃メール配信の後、約 1 時間でほとんどの開封者が添付ファイルを開封している。

図 59 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 60 に示す。

図 59 被験者企業 G：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

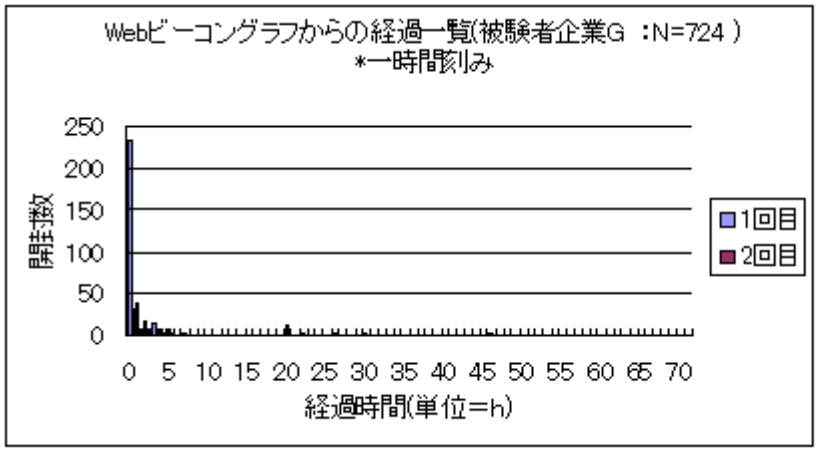
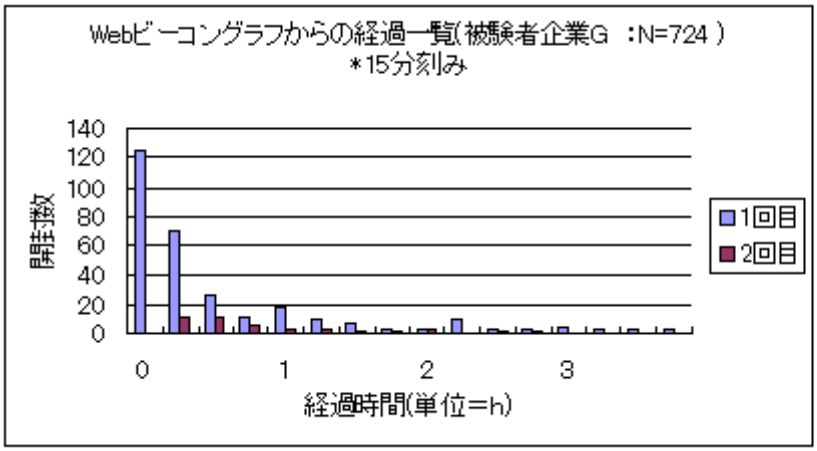


図 60 被験者企業 G：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



9.6. 予防接種実施時の特記事項

9.6.1. 被験者からの返信

第1回配信で用いた擬似攻撃メールの差出人(広報 高橋<motok2501@(フリーメール A)>)に対して、被験者から返信があった。

一通は、宛先を間違っていないかと確認するもので、シグニチャに社名・部署名・氏名・ビル名と階数・電話番号が記載されている。

この被験者は、添付ファイルの内容を見て予防接種だと知る前に、親切心から返信したのかもしれない。あるいは、添付ファイルの内容を見て自分が予防接種にひっかかったために、照れ隠しで返信したのかもしれない。

いずれにしても、攻撃者にとっては、このシグニチャが次の攻撃のための貴

重な情報となる可能性がある。
　また、X-Mailer:ヘッダから被験者が使用しているメールソフトの名称とバージョンがわかるし、Received:ヘッダから被験者企業の内部ネットワークを類推する手懸かりも得られる。一通のメールは攻撃者に多くの手懸かりを与えるのである。
　リスト 24 に、一通目の返信を掲げる。ただし、個人情報などに該当する部分を伏せた。

　なお、第２回配信に対しては、被験者からの返信は無かった。

リスト 24 被験者企業 G：被験者からの返信(1)

```
Subject: Re: 報道発表について
From: "(被験者の表示名)" <(被験者のアドレス)>
To: 広報 高橋 <motok2501@(フリーメール A)>
Date: Wed, 10 Dec 2008 14:08:47 +0900
X-Mailer: Microsoft Outlook Express 6.00.2900.2180

広報　高橋様

(被験者の姓)@(プロジェクト略称)です。
お疲れ様です。

標題の件、メールを頂きましたが、
(被験者の姓)さん違いではありませんか？

ご確認下さいますよう、宜しくお願い致します。

--
(被験者企業名)
(部署名)
(被験者氏名)
(ビル名・階数)
TEL:(電話番号)

(擬似攻撃メールを全文引用)
```

　もう一通の返信は、添付資料が間違っていると指摘するもので、シグニチャは付いていない。これは、おそらく予防接種に対する反感か、または、見抜いたことを誇示したい気持ちから返信しているのではないか。
　リスト 25 に、この返信を掲げる。上と同様に、個人情報などを伏せた。

リスト 25 被験者企業 G：被験者からの返信(2)

```
Subject: Re: 報道発表について
From: (被験者のアドレス)
To: 広報 高橋 <motok2501@(フリーメール A)>
```

Date: Thu, 11 Dec 2008 11:49:20 +0900
X-Mailer: QUALCOMM Windows Eudora Version 6.2J rev4.1

高橋さん

(被験者の姓)です。

添付資料が間違ってます。

At 08/12/10 水 13:00, 広報 高橋 wrote:
(擬似攻撃メールを全文引用)

9.6.2. 受信側メールサーバの機能停止

第２回配信の際に、被験者企業 G 側で擬似攻撃メールを受けとる役割を果たしたメールサーバ(受信側メールサーバと呼ぶ)が、機能停止に陥る事故があった。
予防接種実施中にこのような事態に到ったことは誠に申し訳なく、この場を借りてあらためてお詫び申し上げます。

擬似攻撃メールの送信側メールサーバでは、第１回配信でも第２回配信でも同じ設定で配信作業を実施しており、また、事後の再現試験では現象が発現しなかったので、機能停止の原因はよくわからない。
ただし、この時点の送信側メールサーバの設定では、多数のメールを送る場合になるべく多くの TCP セッションを確立しようとするので、セッション数過多が原因となった可能性はある。
そこで、sendmail の SingleThreadDelivery オプションを On にすることで、あるドメイン名のメールサーバには単独の TCP セッションで配送を試みるように設定変更した。

なお、これ以前にも以後にも、受信側メールサーバが機能を停止するという問題は発生していない。また、SingleThreadDelivery 設定の副作用で、メール配送に余分に時間がかかるようになるが、予防接種に差し障るほどの遅延は出なかった。

9.6.3. 偵察アクセス

被験者企業 G では、第１回配信時に総アクセス回数 511 回のうちの８回(1.6%)の偵察アクセスがあったことがわかる。
これら偵察アクセスは、Web ビーコンの URL を改変して、トップディレクトリや途中のディレクトリの内容を表示させようとするものである。
これは、被験者企業 G の被験者の一部に、相当程度の技術を持つ者がいることを示している。

9.7. 被験者アンケートの集計

被験者企業 G の被験者アンケートの集計状況について表 38 に記す。

表 38 被験者企業 G：被験者アンケート回答者の開封状況

有効回答数	460 名	
	第 1 回	第 2 回
開封した人数	199 名(43.3%)	32 名(7.0%)
2 回とも開封した人	19 名(4.1%)	

被験者企業 G では、被験者数 724 名に対し、504 名(69.6%)から被験者アンケートの回答があった。そのうち 44 名は、2 回とも擬似攻撃メールに気付かなかったと回答しているので、有効回答者数を 460 名とする。

有効回答者の中で、第 1 回配信で開封した者は 199 名(43.3%)、第 2 回で開封した者は 32 名(7.0%)であった。また、一度でも添付ファイルを開封した者は 212 名(46.1%)、両方を開封した者は 19 名(4.1%)であった。

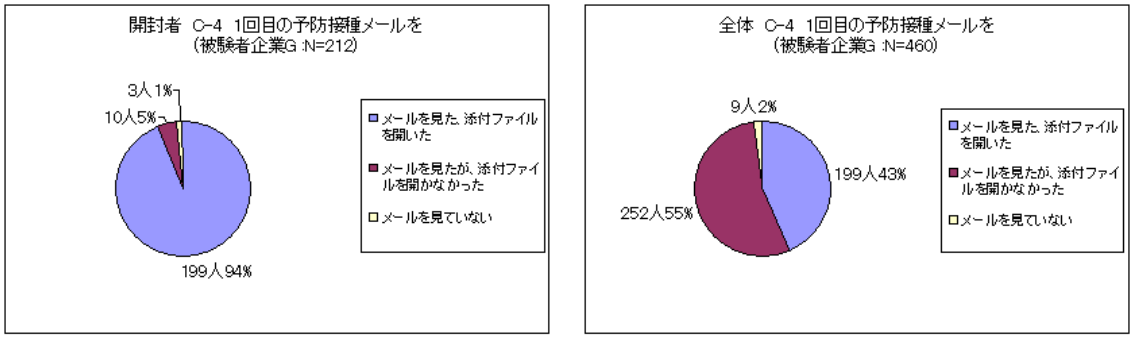
9.8. 被験者アンケートの分析

本節では、被験者企業 G における被験者アンケートの回答内容から、その特徴となる諸点を示す。

9.8.1. 添付ファイル開封の有無とその理由

被験者企業 G における被験者アンケート結果から、設問 C-4 に対する回答の分布は図 61 に示す通りである。

図 61 被験者企業 G：被験者アンケートから見た開封状況(第 1 回配信)



第 1 回配信では、前述のとおり、有効回答者 460 名中の 199 名(43.3%)が添付ファイルを開封したと回答していることがわかる。

これらの開封者が添付ファイルを開封した理由を設問 C-5 から探すと、以下

のような記述を読み取ることができる。

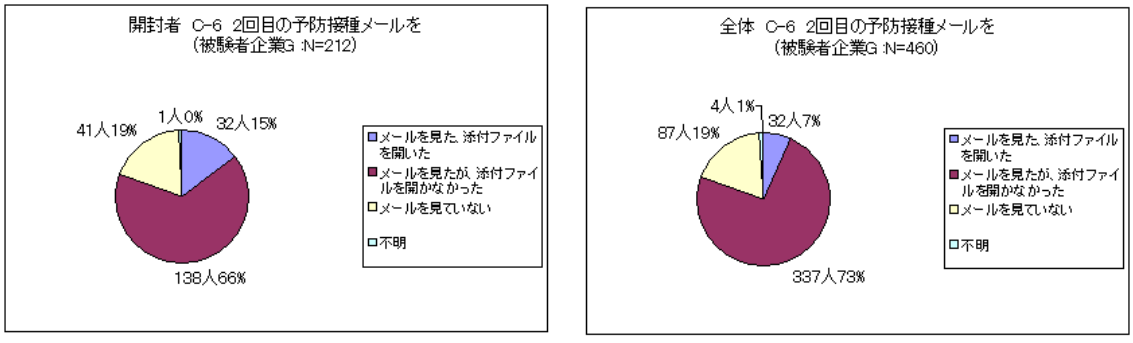
1. あまりにもメールの内容がタイミング的に社内事情に一致したトピックであった。
2. 新サービスについての記載があったので、自分の業務に関連するのか興味があったため。
3. あまりに自然だった。
4. 先に(社内イントラサービス)の特急便で概要を見ており、その後、詳細が記載されたメールが届き、思わず添付ファイルを開いてしまいました。
5. プレスリリースという単語がスパムらしくなかった。
6. 多くのスパムメールを見ているが、そのどれにも当てはまらない通常のメールの書式(書き方)であった為。
7. (被験者企業 G)のネットワークセキュリティを信頼している。

開封理由のひとつには、偶然に社内事情に一致した話題の擬似攻撃メールとなったことが挙げられている。また、はっきりとスパムだと認識したメールではなかったので開封したというものも見られた。

次に、図 62 に、被験者アンケートの設問 C-6 に対する回答から、添付ファイルの開封状況を示す。

第 2 回配信では、前述の通り、有効回答者 460 名中の 32 名(7.0%)が添付ファイルを開封したと回答している。
第 1 回配信と比較すると、開封者は大幅に減少していて、第 1 回配信での体験とその後の周知・教育の効果が読みとれる結果となった。

図 62 被験者企業 G：被験者アンケートから見た開封状況(第 2 回配信)



第 1 回配信における開封者 199 名のうち、第 2 回では添付ファイルを開封しなかったという被験者は 180 名であり、第 1 回開封者の 90.5%を占める。
このような被験者が第 2 回配信で開封しなかった理由を設問 C-7 などから探すと、第 1 回配信での学習効果があったということが読み取れる。

つまり、上記の 180 名うちの半数以上の被験者が、「メールアドレスがフリーメールからで怪しい」などの技術的な観点から、擬似攻撃メールを不審なメールと識別している。これが学習効果である。

しかし、「メールの内容に興味が無かった」為に開封していないという被験者もおよそ半数見受けられる。

したがって、上記の 180 名のうちの約半数には学習効果が認められるが、残り半数は、単に興味の無い内容のメールを最後まで読まなかっただけだと言うことになる。

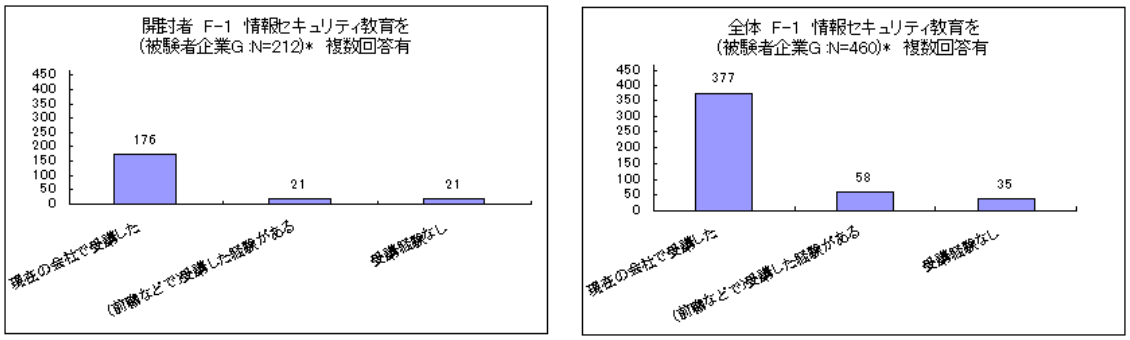
また、設問 C-5 と C-7 の各擬似攻撃メールの対処理由を使って、「送信元のアドレスをチェックする等の技術的な視点からメールを怪しいと判断した」と明らかに記述している被験者が何名いるかを計数した。

その結果、有効回答者 460 名の中で、第 1 回配信では 93 名、第 2 回配信では 123 名が技術的観点からメールを不審と判断していた。すなわち、第 1 回配信から第 2 回配信までに、30 名の被験者が新たにこの観点を身に付けたことになる。なお、この 30 名の全員が、第 1 回配信時の開封者であった。

9.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて検討する。

図 63 被験者企業 G：情報セキュリティ教育の経験

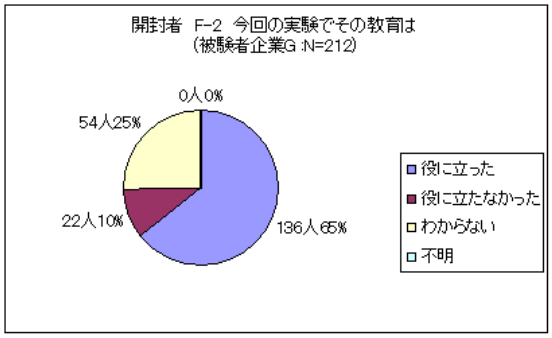


被験者企業 G に付いて、被験者アンケートの設問 F-1 に対する回答の集計結果を図 63 に示す。

被験者アンケートの有効回答者 460 名の中の 377 名(82.0%)は、現在の勤務先で情報セキュリティ教育を受けたと回答している。

このうちの 176 名(377 名に対して 46.7%)が、第 1 回配信と第 2 回配信のいずれかまたは両方で添付ファイルを開封している。

図 64 被験者企業 G：情報セキュリティ教育の有効性



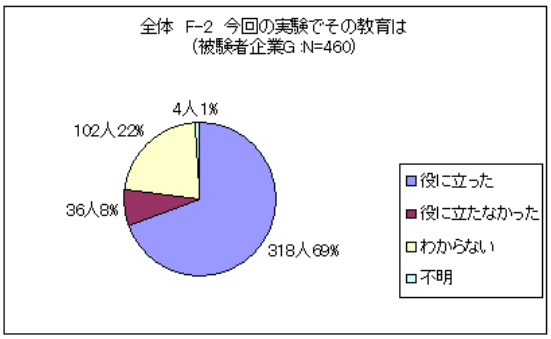


図 64 には、設問 F-2 に対する回答を集計して、自分が受講した情報セキュリティ教育が今回の予防接種に役立ったか否かについて示した。

これを見ると、情報セキュリティ教育が予防接種に役立ったと回答した被験者は、有効回答者 460 名の中の 318 名(69.1%)であることが読み取れる。
他方で、開封者 212 名の中で見ると、136 名(212 名に対して 64.2%)の被験者が役に立ったと回答している。
情報セキュリティ教育は役に立ったけれども、添付ファイルを開封したというのは、少々奇妙で理解に苦しむところである。

9.8.3. 危機管理意識の変化と感想

被験者アンケートの設問 F-4(危機管理意識の変化)と設問 G(感想)への回答をみると、今回の IT セキュリティ予防接種を体験することによって、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したと受け取れる感想が多い。
被験者企業 G では、普段のセキュリティ教育は e ラーニングを使って実施しているとのことだが、予防接種のような体験型の訓練には、知識として理解していた(またはそのつもりになっていた)セキュリティ教育の内容を体得させる効果があると読める回答を多く得ている。

9.8.4. もし標的型攻撃がきたら、どう対処するか

被験者アンケートの設問 C-3・F-3 で、もし標的型メール攻撃がきたらどう対処するかを尋ねた。
設問 C-3 で、「セキュリティ担当者に連絡する」を選択した被験者が 254 名(55.2%)であるのに対し、F-3 で「管理者に連絡する」を選択した被験者は 296 名(64.3%)と約 9%だけ多い結果となっている。
いずれも半数以上の回答者が、インシデント報告の意義と手段を理解しているものと思われる。
また、設問 C-3 と設問 F-3 の間で、擬似攻撃メールに対する自らの反応とそ

の理由を振り返って貰うことで、このような標的型メール攻撃の際にどのように対処するべきかを再認識してもらうことができたと思われる。

なお、F-3 では「ウィルスチェックをする」等その他の項目でも回答数が増えてしまっており、ISO27001 などが要求するインシデント報告義務との兼ね合いでは問題が残る結果となった。

設問 C-3 に対する回答を図 65 に示す。また、設問 F-3 について図 66 に示す。

図 65 被験者企業 G：もし標的型メール攻撃が来たら

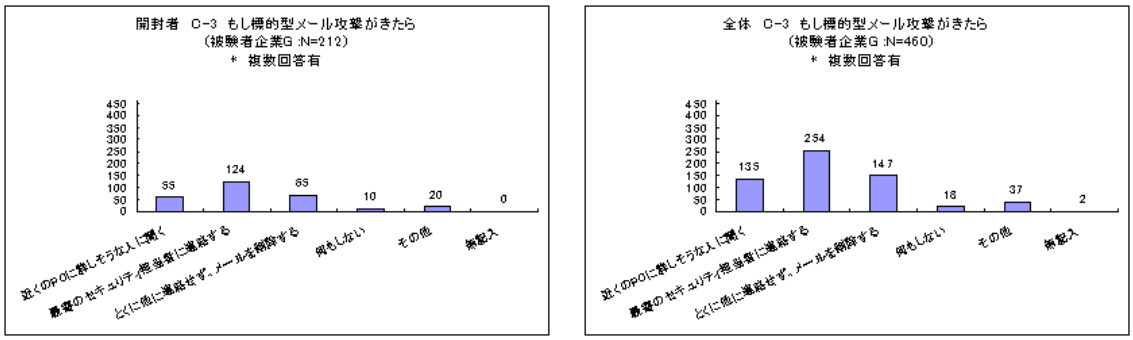
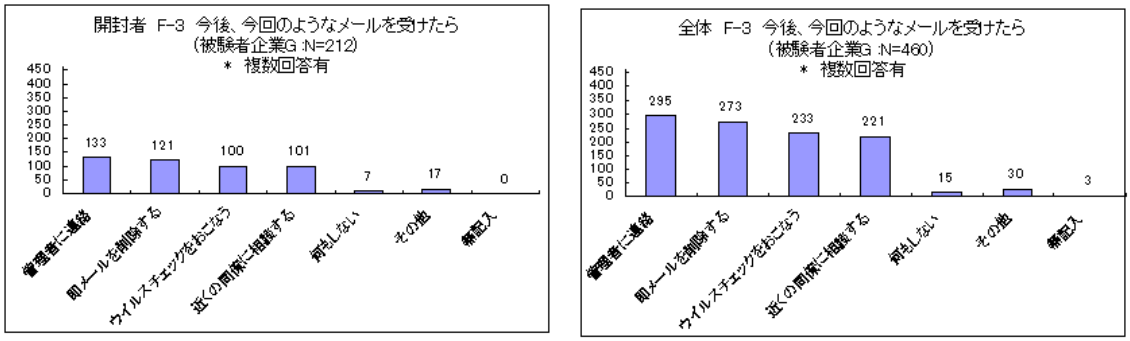


図 66 被験者企業 G：今後、今回のようなメールを受けたら



9.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業インタビューによれば、被験者企業 G では、ISO27001 認証を取得していることもあって、情報セキュリティ関連の組織体制・社内規定・技術的対策などを整備しており、基本的に実施できているという認識であった。

しかし、情報セキュリティ対策の重要性やその方法についてエンドユーザの実感として感じて貰うところまではできておらず、今回の予防接種によって初めて「実感」まで到達したという窓口担当者の感想を得た。

窓口担当者が個々の被験者から話を聞いたところでは、今回初めて添付ファイルの怖さを知ったという感想もあったそうで、そういう実感を持って貰ったことが収穫である。

また、予防接種については、PDCA サイクルの C (Check)に該当するものだと窓口担当者は認識しており、継続的に実施するべきであるとの意見を得た。

9.10. 考察

被験者企業 G は大手のインターネットサービスプロバイダー(ISP)なので、会社全体の IT リテラシーが高いものと予想していた。

しかし、被験者アンケートに対する回答を見ると、擬似攻撃メールをそれと見抜く際の判断材料として、差出人のメールアドレスを確認するなどの技術的な観点を挙げた回答者は、第 1 回配信では約 20%、第 2 回配信では約 25%に過ぎない。

詳細に聞けば技術的観点から判断した被験者の実数は増えると思われるが、ISP 業務を行っている会社としては、予想外に、メールの本文の印象だけで判断している被験者が多い印象を受けた。

この意味では、「今後標的型メール攻撃は来ると思う」と答える回答者が多いにも関わらず、メールの正当性を文面のみの判断に委ねているものが多い状況は、興味深い。

なお、感想などの自由記述欄を見ると、第 1 回配信に素直に騙される形で添付ファイルを開封してしまった被験者ほど、今回の予防接種に関して教育効果が見受けられる結果となった。

また、擬似攻撃メールの配信から開封数の終息までが短時間であるのも被験者企業 G の特徴である。

このような組織では、実際の攻撃が起きた場合には、誰かが攻撃に気づくときには多くの人が既に開封した後である可能性が高い。情報セキュリティ教育を始めとする事前対策に力を入れることが必要である。

被験者アンケートの「自社のネットワークセキュリティを信頼している。」という回答からは、既にネットワーク境界での防御が難しい現状を従業員に伝えていく必要性を感じる。

10. 被験者企業H

10.1. 被験者企業Hの概要

被験者企業 H は、重要インフラ企業の 100%出資のシステム子会社である。同企業グループ内の IT 分野を担当すると共に、一般市場でも IT のプロフェッショナルとして SI 事業を行っている。

表 39 に、被験者企業 H の概要を示す。

表 39 被験者企業 H：概要

業種	情報処理・提供サービス業
設立	1977 年 7 月
資本金	3 億 5 千万円
本社所在地	東京
拠点数	19 箇所
社員数	約 2000 名
認証	プライバシーマーク(全社)、ISO27001(部門単位)

10.2. 被験者企業Hにおける予防接種の概要

表 40 に示す日程と規模で、被験者企業 H に対する予防接種を実施した。

表 40 被験者企業 H：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/13 11:00	2009/1/27 11:00
種明かし	2009/1/14 10:00	2009/1/28 11:30
被験者数	49 名	49 名

被験者企業 H における被験者は、部課長級を中心とする 49 名である。

今回が初めての予防接種ということもあって、予防接種手法を導入すると会社が社員を試しているかのように受け止められる可能性があり、労働組合との折衝には神経を使うとのことである。そこで、今回は組合員を避けて部課長級を中心とした人選となった。

被験者企業 H では、会社としてプライバシーマークを取得しており、一部の部門では ISO27001 認証を取得している。被験者の所属部門は ISO27001 認証を取得していない。

したがって、被験者は、プライバシーマークが要請するヒヤリハット報告の義務を負っているとともに、一般的なセキュリティ教育を受けているはずである。

なお、今回の予防接種に際しては、第 1 回配信の約 2 ヶ月前に、社内の Web 掲示板に標的型メール攻撃への注意喚起の教育文書を掲載した。
ただし、予防接種を実施するということは、特に周知していない。

10.3. 擬似攻撃メールの内容

10.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 H における第 1 回配信の擬似攻撃メールをリスト 26 に示す。

この擬似攻撃メールの文面などは、リスト 2 のサンプル(7)を参考にして作成した。
この擬似攻撃メールは、自社社長がテレビ番組に出演したことを総務部から全社へ周知する形を装い、被験者の興味を惹こうとするものである。緊張を呼ぶ話題ではないので、被験者の油断を誘う要素もある。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人のメールアドレスを moto02501@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
2. 差出人の表示名に実在する組織である「総務部」を用いた。本文中の署名も同様である。
3. 差出人の所属・氏名・連絡先を記した署名が無い点が、標的型攻撃メールの特徴に一致する。
4. 被験者企業 H では、社内のセキュリティポリシーで添付ファイルを自動的に暗号化している。これにも関わらず、この擬似攻撃メールでは、MS-Word 形式のファイルがそのまま添付されている。これは被験者企業 H に特有の気付きのポイントである。

リスト 26 被験者企業 H：第 1 回配信の擬似攻撃メール

```
From: 総務部 <moto02501@(フリーメール B)>
Subject: 先日のテレビ番組出演について

社長の出演した番組をメールに添付しました。
参考までに、閲覧ください。

総務部

添付ファイル名:社長テレビ出演.doc
```

10.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 H における第 2 回配信の擬似攻撃メールをリスト 27 に示す。

この擬似攻撃メールの文面などは、リスト 2 のサンプル(9)を参考にして作成した。

この擬似攻撃メールは、総務部からアンケートへの協力を依頼するものであり、旅行代理店が消費者の旅行動向を調べるのを仲介する態を装っている。「2, 3 日の間でお手すきの際に」とアンケートの回答の締め切りを指定することで、添付ファイルの開封を急がせるものとなっている。

このメールには、以下のような気付きのポイントが含まれている。

1. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
2. 差出人の表示名に実在する組織である「総務部」を用いた。本文中の署名も同様である。
3. 差出人の所属・氏名・連絡先を記した署名が無い点が、標的型攻撃メールの特徴に一致する。
4. 被験者企業 H では、社内のセキュリティポリシーで添付ファイルを自動的に暗号化している。これにも関わらず、この擬似攻撃メールでは、MS-Word 形式のファイルがそのまま添付されている。これは被験者企業 H に特有の気付きのポイントである。

リスト 27 被験者企業 H：第２回配信の擬似攻撃メール

From: 総務部 <censusteam@(フリーメール A)>
Subject: アンケートのご協力

某旅行代理店からの依頼で今年度の消費者の旅行動向についての
アンケート調査を実施しています。社員の皆様からも、是非アン
ケートにご協力いただきたいので、2, 3 日の間でお手すきの際に
ご協力ください。旅行の時期、場所、予算、同行人数といった簡
単な内容なので、数分でお答えいただけると思います。よろしく
お願いいたします。

総務部

添付ファイル名:旅行動向アンケート.doc

10.4. Webビーコンの集計結果

被験者企業 H について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 41 に示す。

被験者企業 H では、添付ファイルを開封した被験者の数と比率は、第 1 回配信の 30 名(61.2%)から、第 2 回配信の 4 名(8.2%)へ、大幅な改善が見られた。

しかし､2回とも開封した被験者が2名(4.1%)おり､絶対数では少数であるが、周知・教育を受けているにもかかわらず、開封するものは開封するという側面も見られる。この 2 名は、第 2 回配信での開封者数 4 名の半分を占める。

表 41 被験者企業 H：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2009/1/13 11:00	2009/1/27 11:00
種明かし	2009/1/14 10:00	2009/1/28 11:30
被験者数	49 名	49 名
Web ビーコンへのアクセス総数	46 回	6 回
開封したと考えられる人数	30 名(61.2%)	4 名(8.2%)
2 回とも開封した人	2 名(4.1%)	

10.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 H における擬似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業 H では、擬似攻撃メール配信の後、約 1 時間でほとんどの開封者が添付ファイルを開封している。

第 1 回配信では、配信後約 2 時間のところにも小さな開封の山があるが、これは昼食休憩の終わりに該当する。午前中にメールを処理しなかった被験者が、昼食後にまとめて処理したのであろう。

図 67に、擬似攻撃メール配信後の3日分の開封数を、1時間刻みのヒストグラムとして示す。また、同様に15分刻みの4時間分のヒストグラムを図 68に示す。

図 67 被験者企業 H：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

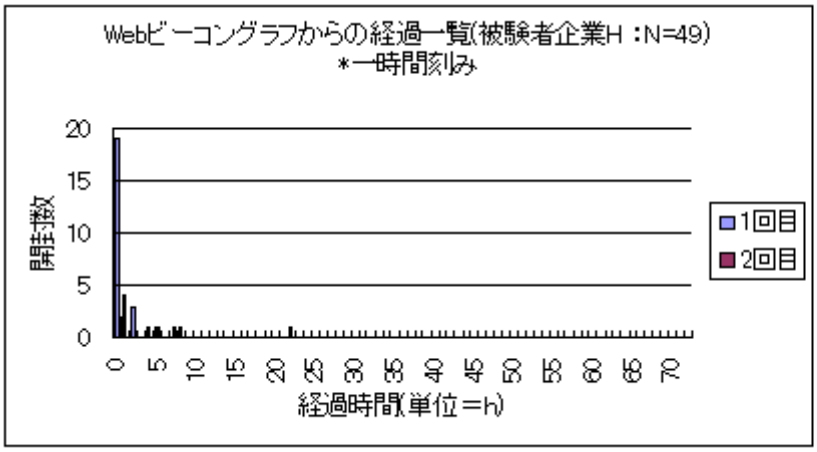
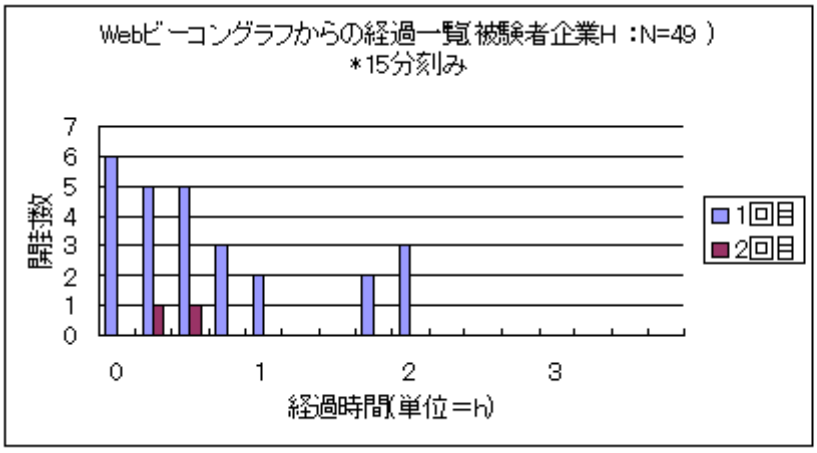


図 68 被験者企業 H：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



10.6. 予防接種実施時の特記事項

特になし。

10.7. 被験者アンケートの集計

被験者アンケートへの回答から見た、被験者企業 H における添付ファイルの開封状況を表 42 に示す。

表 42 被験者企業 H：被験者アンケート回答者の開封状況

有効回答数	29 名	
	第 1 回	第 2 回
開封した人数	21 名(72.4%)	0 名(%)

2 回とも開封した人	0 名(0%)

被験者数 49 名に対し、30 名(61.2%)の被験者から被験者アンケートへの回答があった。アンケートの回答者のうち、1 名が擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答数を 29 名とする。

有効回答数 29 名の中で、第 1 回配信の際に添付ファイルを開封したと回答している被験者は 21 名(72.4%)であり、第 2 回配信では 0 名(0.0%)である。したがって、両方を開封した被験者は 0 名である。

前節で Web ビーコンから開封率を見たが、それと比較すると、第 1 回配信での開封率が約 10%高めに出ており、第 2 回配信での開封率は約 10%低めに出ている。しかし、全体としてはほぼ同様の傾向を示しているものと思われる。

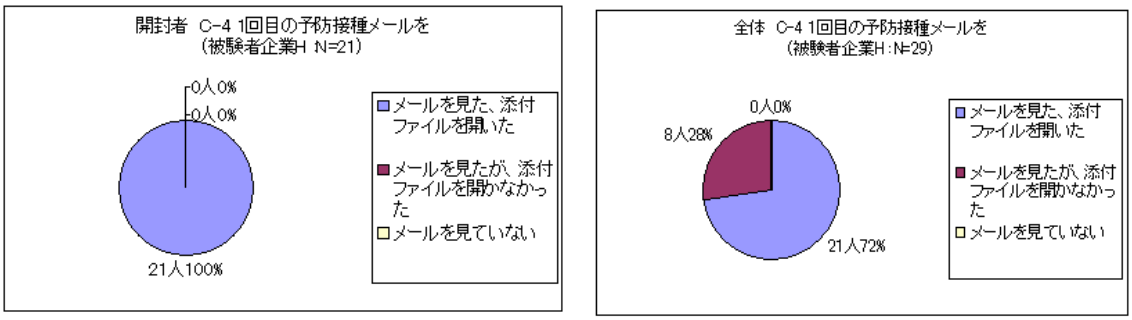
10.8. 被験者アンケートの分析

本節では、被験者企業 H の被験者アンケートの回答内容から、その特徴となる諸点を示す。

10.8.1. 添付ファイルの開封の有無とその理由

被験者企業 H における被験者アンケートの設問 C-4 への回答結果を図 69 に示す。

図 69 被験者企業 H：被験者アンケートから見た開封状況(第 1 回配信)



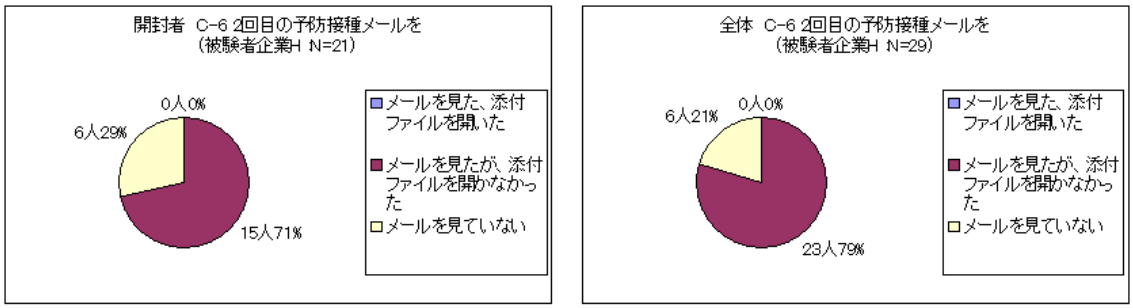
前述の通り、被験者企業 H の第 1 回配信では、21 名(72.4%)の被験者が添付ファイルを開封している。その理由を被験者アンケートの設問 C-5 から探ると、以下のような理由を読み取ることができる。

1. 特に意識することもなく社内からのメールだと信じて、添付ファイルを開いた。
2. 表示名や本文末尾に「総務部」という名前があったので、疑わなかった。

3. 業務上、「総務部」とのメールのやりとりが多く、「総務部」と見た瞬間に反射的に処理してしまった。

被験者企業 H における被験者アンケートの設問 C-6 の回答結果を図 70 に示す。

図 70 被験者企業 H：被験者アンケートから見た開封状況(第 2 回配信)



第 2 回配信では、有効回答者 29 名の中には、添付ファイルを開封したと回答した被験者がいない。Web ビーコンから見た開封率と比較して、開封率が大きく改善したところは同傾向であるが、比率の点ではやや異なった姿となっている。

Web ビーコン側で確認できる開封者は、何らかの理由で被験者アンケートへの回答を躊躇したのであろう。

第 1 回配信での開封者で、第 2 回配信の添付ファイルを開封しなかった被験者が、どういう理由で添付ファイルを開かなかったのかを、設問 C-7 の回答から検討する。

該当する被験者の多くは、差出人の表示名やメールアドレスを仔細に確認したり、メール本文の内容が社内文書の形式と合致するか否か、添付ファイルが暗号化されている[8]か否かを注意深く確認したりしていることがわかる。

これは、第 1 回配信の体験と、その後の周知・教育の効果があったという仮説を支持するものである。

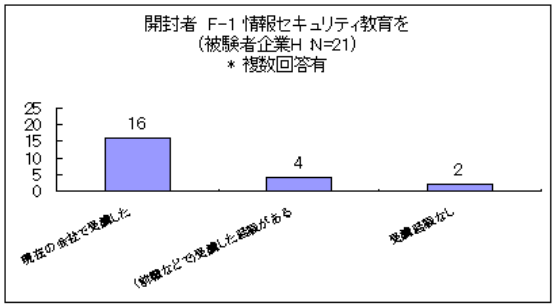
10.8.2. 情報セキュリティ教育の経験

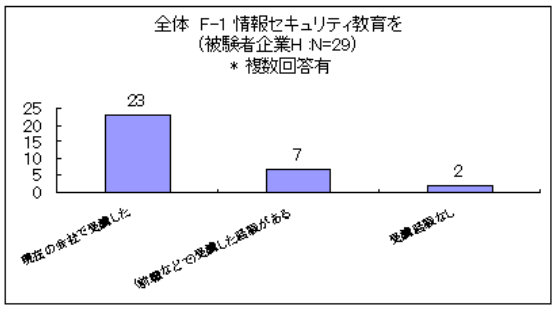
ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

被験者アンケートの設問 F-1 への回答状況を図 71 に示す。

[8] 前述の通り、通常、社内からのメールの添付ファイルは暗号化されている。

図 71 被験者企業 H：情報セキュリティ教育の経験



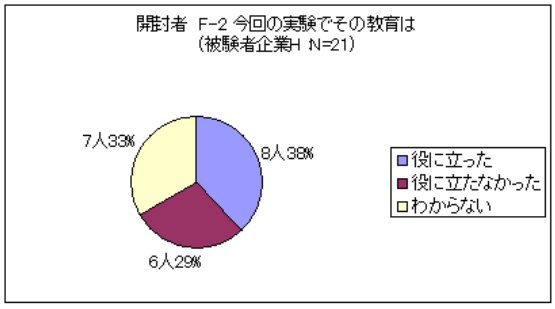


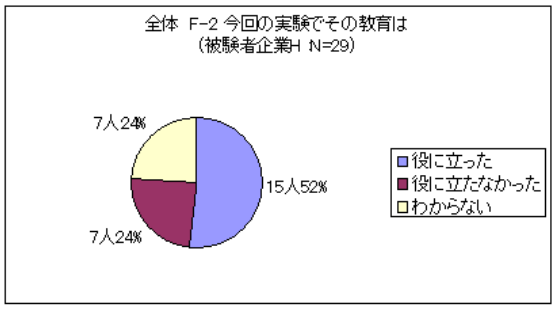
これによれば、被験者アンケート有効回答者 29 名中の 23 名(79.3%)が現在の勤務先で情報セキュリティ教育を受けていることがわかる。
この 23 名中の 16 名(69.6%)が、第 1 回配信で添付ファイルを開封している。
したがって、情報セキュリティ教育を受けていても、添付ファイル開封率がそれほど違わないことがわかる。

なお、情報セキュリティ教育を受けたことがないと回答した被験者 2 名は、その全員が添付ファイルを開封している。

同様に、設問 F-2 の結果を図 72 に示す。

図 72 被験者企業 H：情報セキュリティ教育の有効性





これによれば、情報セキュリティ教育が予防接種の際に役に立ったと回答した被験者は、有効回答者 29 名の中の 15 名(51.7%)であるが、開封者 21 名の中でも 8 名(38.1%)を占める。
被験者にとっては、情報セキュリティ教育は様々な知識を身に付けるという意味では役には立っているが、予防接種の開封率のように実際に我が身を守る際にはあまり関係がないと言うことであろうか。

被験者アンケートの設問 F-4 や設問 G に対する回答を見ると、今回の予防接種を体験することで、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したと受け取れる感想が多い。予防接種のような体験型の訓練には、知

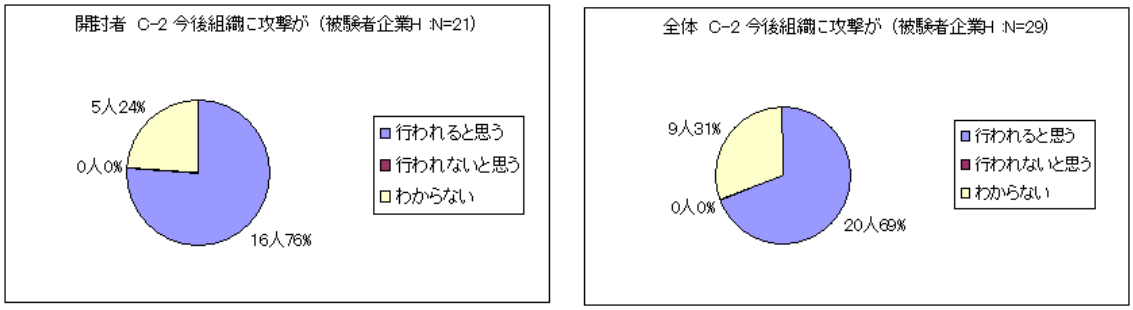
識として理解していた、またはそのつもりになっていたセキュリティ教育の内容を体得させる効果があるといえるのではないか。

10.8.3. もし標的型攻撃がきたら、どう対処するか。

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのような反応を示すと思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答を図 73 に示す。
これを見ると、今後組織に標的型メール攻撃が行われるかもしれないと回答している被験者は、有効回答者 29 名の中の 20 名(69.0%)である。
今回の予防接種で、実際の攻撃とほぼ同様の擬似的攻撃を受けて、あらためて脅威を認識したということであろう。

図 73 被験者企業 H：今後組織に攻撃があると思うか



被験者アンケートの設問 C-3 に対する回答を図 74 に示す。
これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 29 名中の 23 名(79.3%)で、非常に高い割合を占める。
プライバシーマーク制度におけるヒヤリハット報告ルールが、多くの被験者に周知徹底されていると言える。

図 74 被験者企業 H：もし標的型メールが来たら

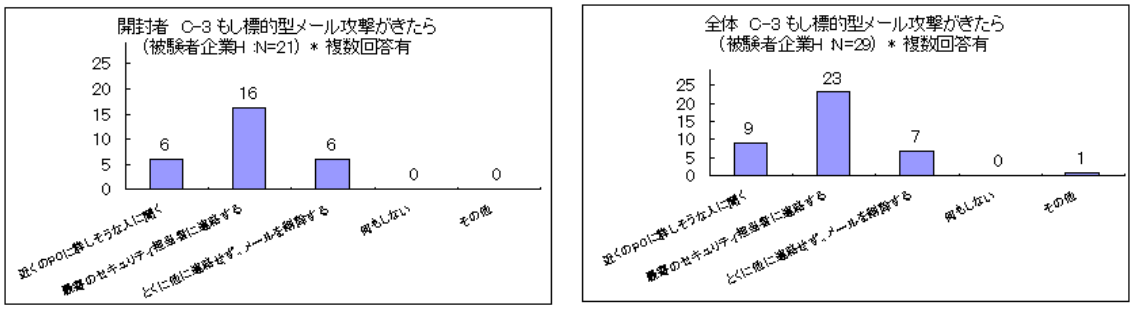


図 75 被験者企業 H：今後、今回のようなメールを受けたら

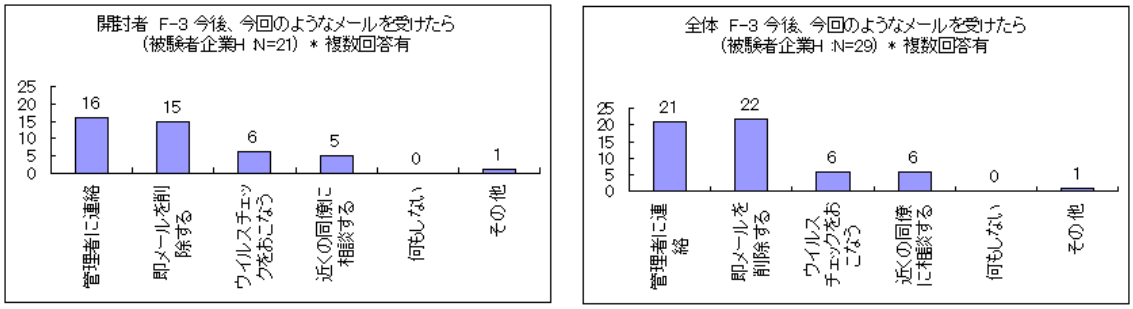


図 75 には、被験者アンケートの設問 F-3 に対する回答状況を示す。設問 F-3 では、先述の設問 C-3 とほぼ同様の内容を、表現を変えて再質問している。

これによれば、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者は、有効回答者 29 名中の 21 名(72.4%)であり、先程の設問 C-3 に比べて 2 名減となっているものの、依然として高い割合を占めている。

しかし、「即メールを削除する」と回答した被験者は、29 名中の 22 名(75.9%)と、設問 C-3 での 7 名(24.1%)から大幅に増加した。

これは、被験者企業 H では、社内掲示板に「心当たりのないメールは、迂闊に開かずに、すぐに削除しましょう」と掲載するなどの指導が普段から行われていることを思い出した結果ではないかと思われる。

プライバシーマーク制度ではインシデントを管理するために報告することが理想とされているが、被験者企業 H では、セキュリティ対策が本来業務の妨げになってはならないという判断のもとに、このような方針を定めて運用しているとのことであった。インシデント報告を行う意識も高いので、不審なメールをすぐに削除することで実害を防ぐことは、現実的な判断であろう。

10.8.4. 危機管理意識の変化

ここでは、被験者アンケートの設問 F-4 に対する回答を用いて、被験者の危機管理意識が変化したか否かについて調べる。

有効回答者 29 名の内、26 名(89.7%)の被験者が、今回の訓練を通して危機管理意識の変化を感じ、もしくは危険・脅威の再認識をし、このような変化の原因となった予防接種を肯定的に捉えている。

被験者アンケートの自由記述欄から、関連するコメントをいくつか拾っておく。

1. 自宅 PC と異なり、ある程度フィルタリングされているので今回のようなメールに対する油断があったと思う。不審な時はアドレスを確認する習慣をつけたい。

2. 当社は、強固なセキュリティで守られているから大丈夫だろうと安心しきっていた部分があったが、脆弱性をついた標的型メール攻撃は、いつ何時されるかわからない危機意識を再認識した。

10.8.5. 感想

ここでは、被験者アンケートの設問 G に対する回答から、メッセージを読みとることを試みる。

有効回答者 29 名のうち、16 名(55.2%)の被験者は、今回の予防接種訓練を肯定的に捉えており、危機意識が変化したことや予防接種再実施の提案などのような前向きの回答を寄せている。
いくつか抜粋しておく。

1. 今回は「総務部」と言うアドレスであり、研修に従いプロパティを開くと確かに外部からのものであった。2 回目はプロパティも確認せず削除した。今後は体裁のおかしさだけで判断できるか疑問であるが、「プロパティまでなら見てよいのか」悩むより、おかしなものは即削除するものとしたい。
2. 普段は十分注意していると思っていても、何らかの外部要因(キーワード、思い込み)で意識が変わってしまうものだと思った。
3. 2 回目のアンケートは、変だと感じたが、、、1 回目の社長 TV 出演は、、、気がつかなかった。いずれにしても、大量にメールが来る中でのチェックポイントがわかった。怪しいと思ったら、確認と、直ぐ削除するように徹底したい。
4. ただ単に社内掲示板で注意を呼びかけるよりも、今回のやり方はるかに効果があったと思います。「もし本当のメール攻撃だったら」と思うと背筋が寒くなります。
5. メールの表題、発送先をチェックすることは、明らかにおかしいという場合を除き開いてしまう。メールの形式が(被験者企業 H)のものであるか、外部からのメールの場合に発送先が認識できるか等開く前にチェックすることを励行しなければならない。

これらのコメントからは、セキュリティ教育で学んだこと(プロパティ確認)の実践・キーワードや思いこみの重要性・社内掲示板での啓発よりも体験の方が効果的・本文に違和感がなければ差出人アドレスなどを確認しない習慣などを読み取ることができる。

10.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 H について、被験者企業アンケートと被験者企業インタビューから以下のことがわかる。

まず、被験者企業アンケートから以下のことがわかるので、被験者企業 H における情報セキュリティ体制は概ね整っていると言える。

1. プライバシーマーク(全社)と ISO27001(一部の部門)の認証を取得している。
2. 情報セキュリティの管理体制はほぼ整備されており、インシデントの連絡体制(窓口)も定められている。
3. 定期的な情報セキュリティ教育を実施している。

なお、被験者企業 H は、重要インフラ系企業の IT 子会社という位置づけであり、グループ企業全体に共通の情報セキュリティ体制の一角を占めている。企業グループ内で統一されたポリシーや対策を持つことはすばらしいので、実務上の困難を乗り越えて、さらに良い体制に進まれることを期待する。

次に、被験者企業インタビューの際に、窓口担当者から以下の意見・感想を得た。

1. 迷惑メール対策・メール添付ファイルの自動暗号化・クライアント PC の情報漏えい防止対策等、システム側でしっかりとした対策を施していることに自信と誇りを感じるが、そのために一般社員の危機意識が薄れている点に危惧を抱く。
2. 社員のセキュリティ意識を保つために、常時携帯できる「セキュリティについての行動カード」を作成・配布するなどの対策を実施している。
3. 被験者アンケートの設問 C-3 と設問 F-3 で、インシデント報告をするという回答が多かった理由は、今回の被験者層が管理職中心であり、現場でのインシデント報告を奨励し、実際に報告先となる立場にあったためではないか。

ここでも、被験者企業 H における情報セキュリティ体制がよく定着している姿を見ることができる。また、その背景に地道な努力があることもわかる。

さらに、予防接種の実施方法について次のような提案があった。

1. 同じ被験者に 2 回送らずに、五月雨式に全員に擬似攻撃メールを送る方が良いのではないか。
2. その結果を定期的にまとめ、社内の情報セキュリティに対する意識度の変化を定常的に見える化しておきたい。

今年度の予防接種では、全被験者に 2 週間間隔で 2 回の擬似攻撃メール配信を行うことを原則としているが、大量一斉配信の限界や被験者相互の情報漏れなどの点で問題がないわけではない。BBSec としても既に五月雨式配信と結果

のグラフ化については検討していたので、同様の提案が被験者企業から出てくることは心強い。

10.10. 考察

被験者企業 H では、労働組合対応の関係で、主に管理職から被験者を選定した。結果的には、標的型メール攻撃メールの主たる攻撃相手であると言われている層に近い被験者を選んだことになった。管理職は、情報セキュリティインシデントの届出連絡体制の窓口役を担っていることもあって、高い報告義務感を示す結果となった。

被験者企業 H では、約 7 割の被験者が標的型メール攻撃が組織に行われると思うと回答しており、また、約 8 割の被験者が標的型メール攻撃を受けたら管理者に報告すると回答している。いずれも非常に高い比率であり、危機意識の点でも報告義務の意識の点でも、被験者企業 H で情報セキュリティ意識がよく定着していることがわかる。

2 度の擬似攻撃メール配信で、差出人の表示名を「総務部」としたが、管理職中心の被験者は、日常業務として総務部とメールをやりとりする機会が多いため、特に第 1 回配信で多くの開封者を生むこととなった。

また、第 1 回配信の擬似攻撃メールは、社長がテレビ番組に出演したという簡単な業務連絡を装うものであったが、この程度の完成度の擬似攻撃メールでも、被験者(管理職)にとっては「総務部からの連絡」「社長の出演」というキーワードから、疑うことなく添付ファイルを開封する傾向があることが浮かび上がった。

第 2 回配信では、被験者の多くは、表示名に惑わされず差出人のメールアドレスを確認している。また、被験者企業 H での添付ファイルのシステムによる自動暗号化の有無も確認している。すなわち、第 1 回配信の体験から、同様のキーワードがあっても、それに惑わされずに様々な確認を行うようになったと言える。

したがって、被験者企業 H のように情報セキュリティ教育・連絡体制が整っている企業においても、予防接種のような体験型の訓練がセキュリティ意識を呼び起こす教育効果を持っていることがわかる。

11. 被験者企業I

11.1. 被験者企業Iの概要

被験者企業 I は、ディーラー事業・システムインテグレーションサービス事業・セキュリティソリューションサービス事業などを提供する企業グループの持株会社である。

なお、実際には、持ち株会社と主要子会社 3 社を対象に予防接種を実施しており、その内の 1 社はセキュリティソリューションサービス事業会社である。

表 43 に被験者企業 I の概要を示す。

表 43 被験者企業 I：概要

業種	複合サービス事業
設立	2007 年 10 月 1 日
資本金	10 億円
本社所在地	東京
拠点数	5 箇所
社員数	約 1400 名
認証	持株会社としては取得していない。子会社ごとに取得の違いがある。

11.2. 被験者企業Iにおける予防接種の概要

表 44 に示す日程と規模で、被験者企業 I に対する予防接種を実施した。

被験者の選定にあたっては、実際の標的型メール攻撃で狙われると思われる管理職層を被験者とし、さらにランダムに選出した一般社員を加えた。

こうして選定した被験者は、合計で 280 名である。

なお、今回、対象とした子会社の中にはセキュリティソリューションサービス事業会社があるが、グループ全体で情報セキュリティ教育を徹底して実施しているわけではない。

また、今回の予防接種に際して、訓練の事前通知や、標的型メール攻撃を取り上げた事前教育は、特に実施しなかった。

表 44 被験者企業 I：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/13 13:00	2009/1/27 13:00
種明かし	2009/1/14 9:24	2009/1/28 10:22
被験者数	280 名	280 名

11.3. 擬似攻撃メールの内容

11.3.1. 第 1 回配信の擬似攻撃メール

被験者企業Ｉにおいて第１回配信に用いた擬似攻撃メールをリスト 28 に示す。

この擬似攻撃メールは、自社のホームページの好感度調査を行うので社員にも協力してほしいと依頼する態を装うものであり、一見したところでは読み手に不審感を与えないものとなっている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を省略しているので、メールアドレスが直接表示されている。日常的にメールを交換する相手からのメールには見えない。
2. 差出人のメールアドレスを moto02501@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
3. 差出人の所属・氏名・連絡先と記した署名(フッター)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 28 被験者企業Ｉ：第 1 回配信の擬似攻撃メール

```
From: moto02501@(フリーメール B)
Subject: 自社 HP に関するアンケート調査

(被験者企業 I)に対するホームページの好感度調査を行います。
参考までに、社員に対してもアンケートを実施したいと思います。
お手すきの際に、添付ファイルの内容に、ご回答ください

添付ファイル名：アンケート.doc
```

11.3.2. 第 2 回配信の擬似攻撃メール

第 2 回配信の擬似攻撃メールをリスト 29 に示す。

この擬似攻撃メールは、自社の Web サイトで発表した件についてマスコミ対応方針を周知する態を装うものである。

記入項目があると本文中で指摘することで、被験者を添付ファイル開封へ誘導している。

なお、読み手に不審感を与えない点は、第 1 回配信の擬似攻撃メールと同様である。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を省略しているので、メールアドレスが直接表示されている。日常的にメールを交換する相手からのメールには見えない。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. このほか、差出人の所属・氏名・連絡先と記した署名(フッター)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 29 被験者企業 I：第 2 回配信の擬似攻撃メール

From: censusteam@(フリーメール A)
Subject: マスコミ対応方針の確認について

宛先各位

本日、(被験者企業 I)の Web サイトで発表した件
について、マスコミ取材への対応方針を添付ファイルのとおりに
まとめました。

一部記入項目がありますので、ご確認の上、返信してください。

よろしくお願いします。

添付ファイル名： マスコミ対応方針.doc

11.4. Webビーコンの集計結果

被験者企業 I における添付ファイルの開封状況を、Web ビーコンのアクセスログから見ると、表 45 の通りとなる。

被験者企業 I では、添付ファイルを開封した被験者数と比率は、第 1 回配信では 61 名(21.8%)で、第 2 回配信では 61 名(21.8%)と、まったく変化が見られなかった。

なお、2 回とも開封した被験者が 17 名(6.1%)であったことから、開封者の大半が入れ替わっていることがわかる。第 1 回配信での開封者のうちの 44 名(15.7%)は第 2 回配信では開封していないし、第 2 回配信で初めて開封した被験者が 44 名(15.7%)いることになる。

また、被験者企業 I では、多数の偵察アクセスを観測した。

これは、今回対象とした企業のひとつがセキュリティソリューションサービス事業会社であるため、技術に詳しい被験者がいたのであろう。

表 45 被験者企業 I：Web ビーコン集計

	第 1 回	第 2 回
被験者数	280 名	280 名
Web ビーコンへのアクセス総数	852 回	128 回
開封したと考えられる人数	61 名(21.8%)	61 名(21.8%)
2 回とも開封した人	17 名(6.1%)	

11.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 I における擬似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業 I では、擬似攻撃メール配信の後およそ 2 時間で、ほとんどの開封者が添付ファイルを開封している。また、その後 1 時間経過した 3 時間後にも開封がみられる。

配信後約 20 時間経過後に開封が見られるのは、配信翌日の始業時にメールを見ていることを示している。ここから、必ずしも常時メールを確認するタイプの被験者ばかりではないことがわかる。

図 76 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 77 に示す。

図 76 被験者企業 I：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

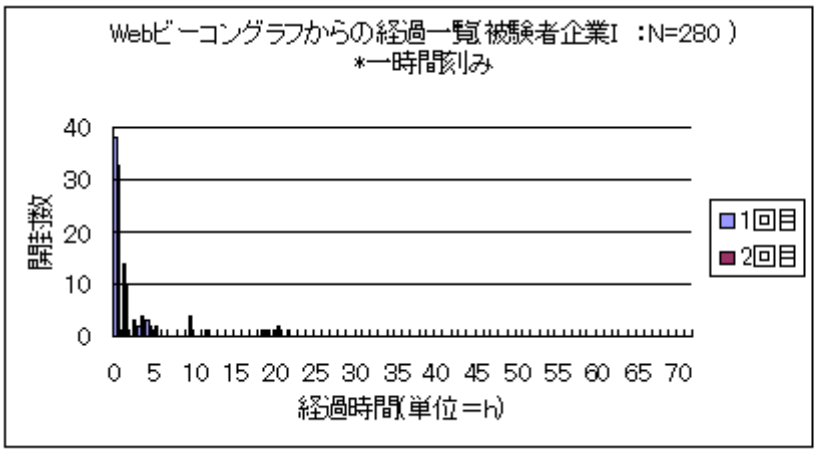
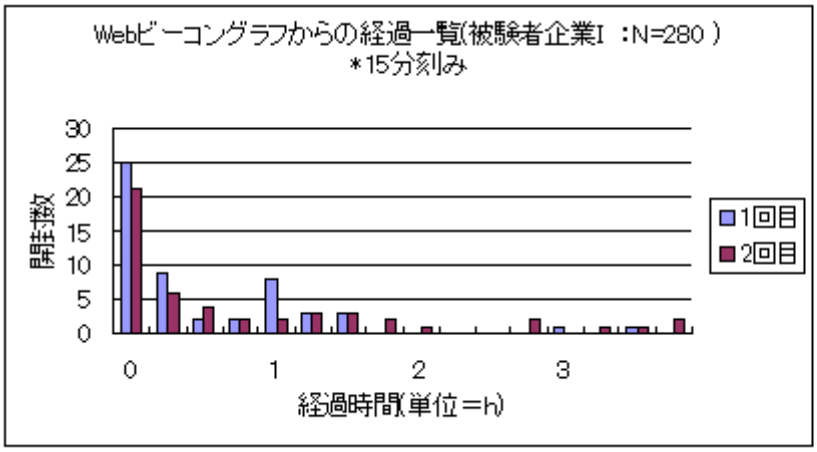


図 77 被験者企業 I：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



11.6. 予防接種実施時の特記事項

11.6.1. 偵察アクセス

被験者企業 I では、非常に多くの偵察アクセスを観測した。第 1 回配信時には総アクセス数 852 回のうちの 566 回(66.4%)が、第 2 回配信では総アクセス数 128 回のうちの 69 回(53.9%)が、偵察アクセスであった。

被験者企業インタビューの際の話では、中には Web アプリケーション用の脆弱性診断ツールを使って脆弱性診断を行った被験者もいたようである。また、他のサイトを経由してアクセスするものなど、巧妙なものも見られた。

お手柔らかに願いたいものである。

11.7. 被験者アンケートの集計

被験者企業 I における被験者アンケートの集計状況について表 46 に示す。

表 46 被験者企業 I：被験者アンケート回答者の開封状況

有効回答数	73 名	
	第 1 回	第 2 回
開封した人数	26 名(35.6%)	14 名(19.2%)
2 回とも開封した人	7 名(9.6%)	

被験者企業 I では、被験者 280 名のうちの 81 名(28.9%)が被験者アンケートに回答している。

このうち 8 名が 2 回とも擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答数を 73 名(被験者数比で 26.1%)とする。

有効回答中で、一度でも添付ファイルを開封した被験者は 33 名(45.2%)であ

り、第 1 回配信で開封した被験者は 26 名(35.6%)、第 2 回で開封した被験者は 14 名(19.2%)、両方を開封した被験者は 7 名(9.6%)であった。

前節の Web ビーコンから見た開封率に比べると、被験者アンケートの回答から見た開封率が異なった傾向を示している。すなわち、前者では第 1 回配信も第 2 回配信もともに 21.8%の開封率であったのに対し、後者では第 1 回配信の 35.6%から第 2 回配信の 19.2%へ改善している状況である。

11.8. 被験者アンケートの分析

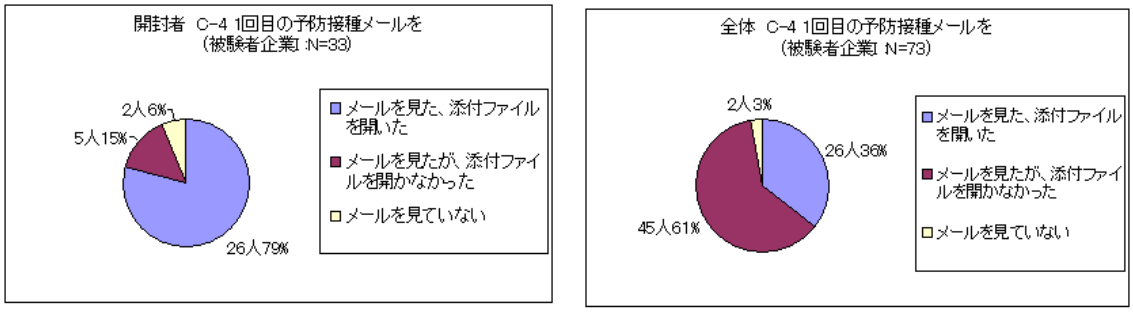
本節では、被験者企業 I の被験者アンケートへの回答内容から、その特徴となる諸点を示す。

11.8.1. 添付ファイル開封の有無とその理由

ここでは、被験者アンケートから見た開封状況とその理由などを調べる。

まず、被験者アンケートの設問 C-4 に対する回答の状況を、図 78 に示す。

図 78 被験者企業 I：被験者アンケートから見た開封状況(第 1 回配信)



これによれば、第 1 回配信では、有効回答 73 名中の 26 名(35.6%)が、添付ファイルを開封したと回答している。

設問 C-5 に対する回答からその理由を探ると、特に不審に思うこともなく社内のメールと思って開封している被験者がほとんどである。しかし、中には、差出人のメールアドレスを不審には思ったが、表題と本文の内容がグループ企業関連の話題であったために、結局は開封したという被験者もいる。

設問 C-5 への回答の具体的な記述をいくつか抜粋しておく。

1. 「文面」のみで判断してしまった。宛先メールアドレスをよく確認していなかった。
2. from:アドレスが怪しいと思ったが、subject:および本文の内容が、(社内システム)関係であったので。

3. 最初に送信されてきた文面の内容を確認したところ、よく知っている会社の同僚からであり、文面の内容も極めて自然なものであったため、無意識に開いてしまった。その後、送信者アドレス等をよくよく見直してみて、初めて不審な箇所があることに気付きました。(ちなみに、同じ人より本アンケート依頼のメールがあったため、逆に罠ではないかと疑ってしまいました)差出人や表題があり得るものだったので、特に疑わずに開けてしまった。
4. 新会社のやり方だと思った。
5. メールの内容を見て、何の事か知るために開けた。
6. 発信元は不明であったが、依頼内容を確認するため開いた。

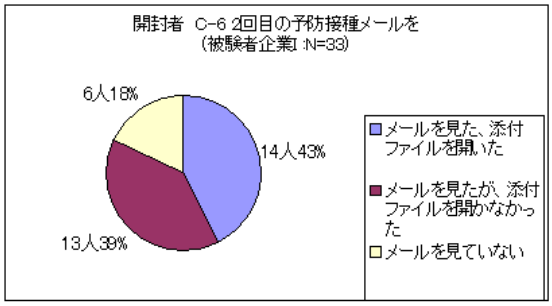
また、少数ではあるが、技術的に危険なメールかどうか確認してから開封した被験者もいる。

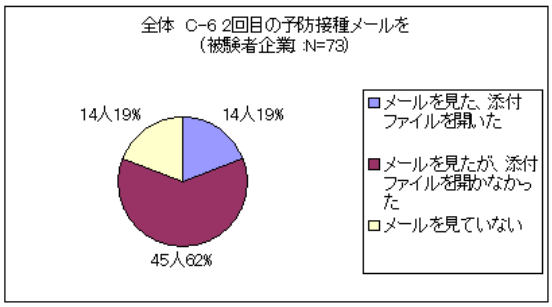
1. セキュリティ担当者へ連絡するための攻撃メールか確認するため。
2. 一旦保存してバイナリエディタで内容を参照し、開いても大丈夫そうだったので開いてみました。

第 1 回配信の非開封者には、差出人のメールアドレスがフリーメールアドレスである点を不審に感じて開封しなかったという被験者が多い。

次に、第 2 回配信について同様に検討する。図 79 に被験者アンケートの設問 C-6 に対する回答状況を示す。

図 79 被験者企業Ⅰ：被験者アンケートから見た開封状況(第 2 回配信)





これによれば、第 2 回配信では、添付ファイルを開封した被験者は有効回答者 73 名中の 14 名(19.2%)であった。このうち 7 名(9.6%)は 2 回とも開封している被験者である。

設問 C-7 に対する回答を見ると、ほとんどの回答者が擬似攻撃メールの本文だけを見て、不審にも思わずに開封していることが読み取れる。
しかし、擬似攻撃メールの内容が被験者の担当業務に関係している場合には、業務上の必要性を感じて開封していることが読み取れる。その具体的記述を、

いくつか抜粋しておく。

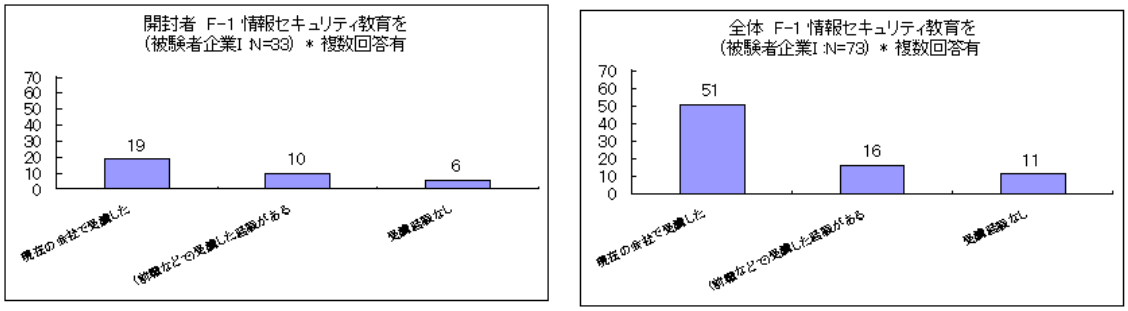
1. 1 回目に準じる。しかも、社内システムの方がテストの為に(フリーメール A)でテストメッセージ送信されたことが以前にもあったため。なお、開く前に HP の IR 情報は確認してから開いた。
2. 業務上の状況にマッチしており、即時対応が必要と判断し、添付ファイルを開いてしまった。
3. 当該メールは取引先と連携業務がある関係で送られたメールであり、小職の役割を知らないと送れないメールだと思った。
4. 送信元に不審を抱いたが、この理由と緊急性を感じ開かないわけにはいかないと思った。
5. 内容が現在の業務に関する事に近い内容であった為。

11.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

図 80 に、被験者アンケートの設問 F-1 に対する回答状況を示す。

図 80 被験者企業 I：情報セキュリティ教育の経験



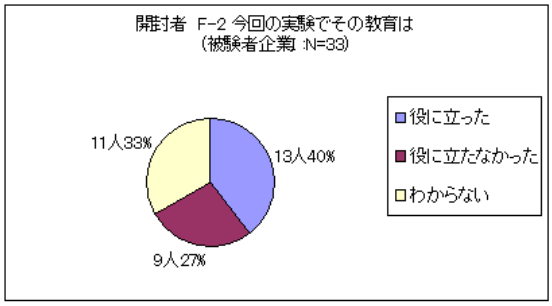
これによれば、被験者アンケートの有効回答者 73 名中の 51 名(69.9%)が現在の勤務先で情報セキュリティ教育を受けたと回答している。前職などで受講した被験者と合わせると、67 名(91.8%)が情報セキュリティ教育を受講した経験があることになる。

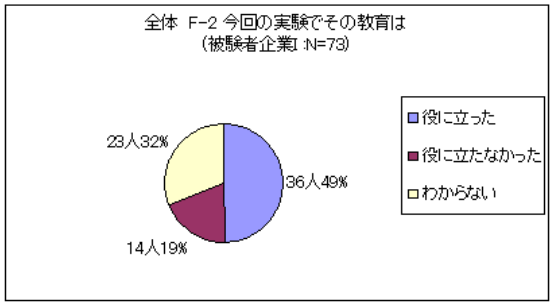
また、開封者 33 名の中の 19 名(57.6%)が現在の勤務先で、前職なども含めると 29 名(87.9%)が情報セキュリティ教育を受けている。

有効回答者全体よりも開封者の方がやや低い値ではあるが、どちらも相当大きな割合の被験者が情報セキュリティ教育を受けていることには変わりがない。

次に、設問 F-2 に対する回答から、情報セキュリティ教育の有効性を考える。図 81 に、設問 F-2 に対する回答状況を示す。

図 81 被験者企業Ｉ：情報セキュリティ教育の有効性





これを見ると、情報セキュリティ教育が予防接種に対して役に立ったと回答した被験者は、有効回答者 73 名中の 36 名(49.3%)であり、開封者 33 名の中では 13 名(39.4%)である。

情報セキュリティ教育を受けた比率が高いのに比べると、それが役に立ったと回答する被験者は明らかに減少している。これは、受講した情報セキュリティ教育では、標的型メール攻撃について強調した形の説明を受けたことがないためではないかと思われる。

設問 F-4(危機管理意識の変化)や設問 G(感想)への回答を見ると、今回の予防接種を体験することによって、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したと受け取れる感想が多い。
また、業務上必要と思われる内容のメールでも送信者の確認をする習慣をつける必要性に気付いた感想もあった。
予防接種のような体験型の訓練には、知識として理解していた(またはそのつもりになっていた)セキュリティ教育の内容を体得させる効果があるといえるのではないか。

11.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-1,C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようなことが起きると思われるかを検討する。

図 82 に設問 C-1 に対する回答状況を示す。

これによれば、標的型メール攻撃を知っている被験者は有効回答者 73 名の中の 42 名(57.5%)であり、開封者 33 名の中では 19 名(57.6%)である。
両者の比率がほとんど同じであることから、「標的型メール攻撃を知っていても、開封している」現実が浮かび上がる。
また、被験者企業Ｉのグループ企業には、セキュリティソリューションサービス事業会社があるにもかかわらず、標的型メール攻撃の認知度が平均程度であったのは意外である。

図 82 被験者企業Ｉ：標的型メール攻撃について

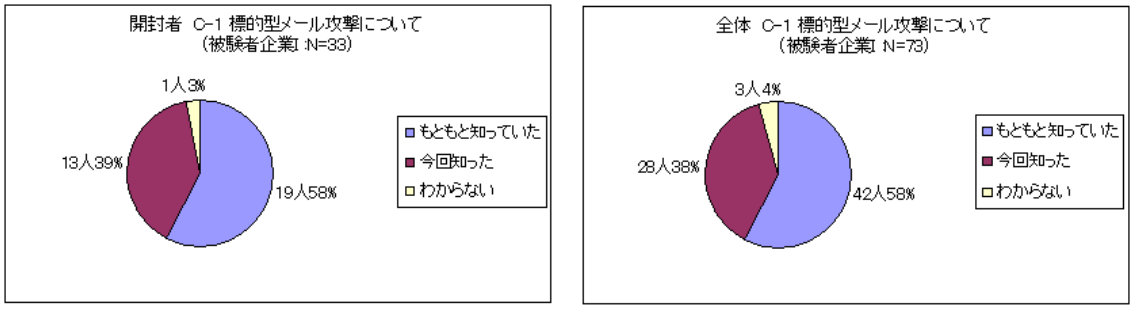


図 83 に設問 C-2 に対する回答状況を示す。

これによれば、有効回答者 73 名の中の 45 名(61.6%)の被験者が、開封者 33 名の中では 19 名(57.6%)の被験者が、今後組織に標的型メール攻撃が行われるかもしれないと回答している。

図 83 被験者企業Ｉ：今後組織に攻撃があると思うか

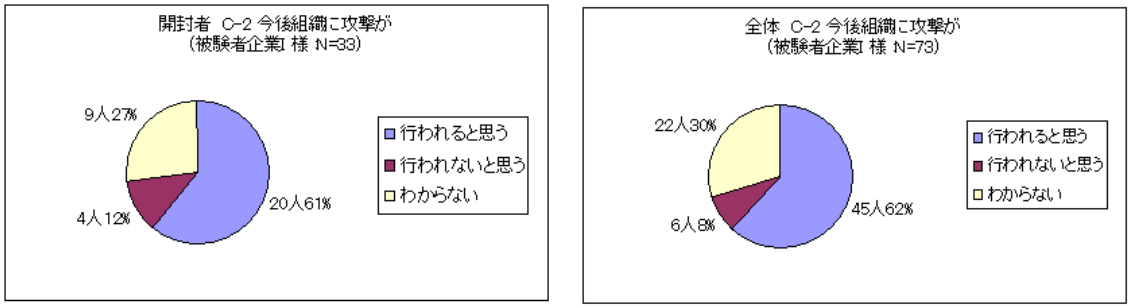


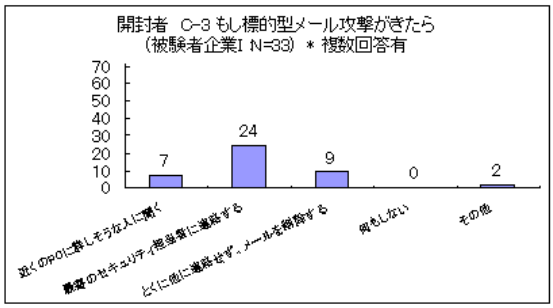
図 84 に、設問 C-3 に対する回答状況を示す。

これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 73 名中の 55 名(75.3%)で、被験者企業Ｉはインシデント報告を行うという回答が比較的多い企業であると言える。

また、「とくに他に連絡せず削除する」と回答した被験者は、17 名(23.3%)で、平均よりも低い。

これらの点は、グループ企業内にセキュリティソリューションサービス事業会社を抱えていることが良い影響を与えているのであろう。

図 84 被験者企業Ｉ：もし標的型メールが来たら



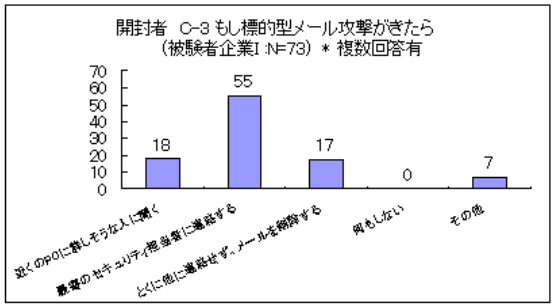
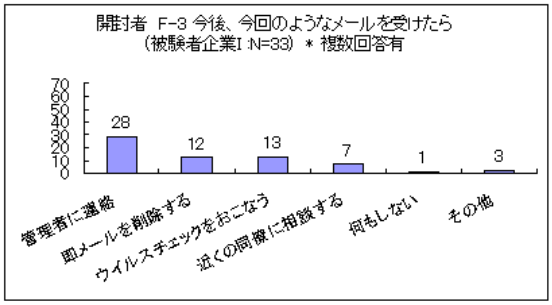


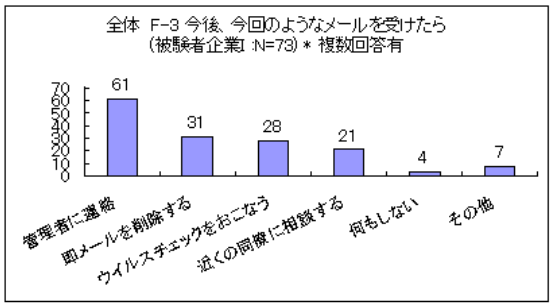
図 85 に、設問 F-3 に対する回答状況を示す。
設問 F-3 では、前述の設問 C-3 とほぼ同様の内容について、表現を若干変えて再度質問している。

ここでは、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者が、有効回答者 73 名中の 61 名(83.6%)となり、先の C-3 での回答よりも増えている。
しかし、「即メールを削除する」と回答した被験者も、31 名(42.5%)と増えている。

インシデント・ハンドリングの観点からは、不審に思ったメールを証拠保全し、管理者に連絡することが理想的である。
しかし､被験者企業Ｉのようなセキュリティソリューションサービス事業会社を抱えるグループであっても、証拠を保全するという意識を定着させることは困難であるようだ。

図 85 被験者企業Ｉ：今後、今回のようなメールを受けたら





11.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4 では､危機管理意識の変化の有無を尋ねている。
被験者企業Ｉにおける設問 F-4 への回答状況を見ると、有効回答者 73 名中の 55 名(75.3%)が、今回の予防接種を体験して、危機管理意識の変化を感じるか、

もしくは危険の再認識をしており、予防接種を肯定的に捉えている。
　また、自由記述欄に「セキュリティ担当者に連絡することが大切である」という回答が多く見られるのは、被験者企業 I の特徴である。

　以下に特徴的な回答を抜粋しておく。

1. かなり無防備だったと感じた。何も考えずにプレビューさせていることがあるし、社外(Oracle や IBM といった企業)からのメールマガジンを受け取っているので、仮に見知らぬ社内以外の人間からメールが来ていても、あまり疑問を持たずに開いてしまうと思った。
2. セキュリティ担当者に報告することを求められていると思った。ただし、報告を受ける側もそのことを日ごろから徹底すべきだと思った。
3. 個人のメールアドレスと違い、会社のメールアドレスは仕事のみで使用しているため今回の攻撃メールを意識していなかった。そのため情報管理者への連絡やメールの削除をしていなかったが、今後は危機意識を持つようにする。

11.8.5. 感想

　被験者アンケートの設問 G(感想)には、67 名の被験者から回答があった。
　この中には、今回の予防接種から教訓を得たという回答が多かったので、以下にいくつか抜粋しておく。

1. 「分かっていてもうっかり」という事はあるので定期的に予防訓練を行うことは効果的だと思いました。
2. メールの送信元アドレスなど、簡単に偽装が可能なので今回のメール程度では不十分。社内のアドレスを偽装されたら、ほぼ全員添付を開くと思う。このようなメールが社内に入ること自体を抑止するシステム的な仕組みの必要性を強く感じる(最低限、電子証明書導入程度は必須か？)
3. 経営陣が、実態を認識するのにとても有効だった。現在の対策では不十分である事、教育の徹底と事故後の対応の手順が不明確であることが認識でき今後の改善につながった。
4. 限りなくビジネスメールに近い形を装って届くメールに関しては、メール自体を開封しないという選択肢を取る事自体が難しく、個人の意識でどうこうというよりは、会社で防衛策を取るのが正しいのでは？と思う。例えば、「ウイルス対策の強化を図る」、「セキュリティの講義を開催する」など会社単位での策も練って欲しいと思う。

11.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業Iに対する被験者企業アンケートや被験者企業インタビューから、以下のことがわかった。

まず、被験者企業Iは持株会社であるが、現時点では、企業グループ全体の情報セキュリティ体制を統括管理しているわけではない。
それゆえ、企業グループ全体を統べるセキュリティポリシーは、比較的大枠で基本的なもののみを定めている状態である。
したがって、グループ内各社の情報セキュリティ体制の整備状況には差がある。
同様に、情報セキュリティ関連の認証取得についてもグループ内各社に委ねられているので、必要に応じて各社が認証を取得している状況である。
これからグループ内のセキュリティ対策を整備していくところなのであろう。

被験者企業Iでは、送信ドメイン認証のひとつであるSPFをDNSに設定していない。JPドメイン名の約3分の1でSPFの設定を実施しているという統計もあるので、検討していただければ幸いである。

11.10. 考察

被験者企業Iはセキュリティサービスを提供する企業のイメージが強く、予防接種の成績は相当良いだろうと予想していた。
しかし、結果としては、予想していたよりも開封者が多かっただけでなく、第2回配信でも開封率が下がらなかった数少ない被験者企業のひとつであった。前後2回の配信で用いた擬似攻撃メールは、ともにフリーメールのアドレスから送信しており、気付きのポイントの難易度は同程度で、あまり難しいものではない。
このような結果になった理由は、おそらく、被験者企業Iがグループ統合からまだ3年足らずという点であろう。それぞれの企業文化をグループ内で共有して共通の理解を得る途上にあるため、業務上あっても不思議ではないメールを受け取ると多少不審に思っても内容を確認しないわけにはいかない状況であるようだ。
最近のM&Aの流行で、多くの企業で同様の状況が生まれていると思われるが、このような過渡期が危険であるという一つの例であろう。

また、被験者企業Iでは、経営層に属する被験者から、予防接種に対する不快の念や(スパム対策のように)情報システムや(予防接種ではない通常の)情報セキュリティ教育などで対応するべきである、とのご意見を頂いた。
これは、経営層を予防接種の被験者とした被験者企業Iの慧眼を示すとともに、経営層の方が情報セキュリティ対策をどのように考えているかの良い例になったのではないかと思う。

12. 被験者企業J

12.1. 被験者企業Jの概要

被験者企業 J は、機械系製造会社である。表 47 に、被験者企業 J の概要を示す。

表 47 被験者企業 J：概要

業種	製造業
設立	(非公開)
資本金	(非公開)
本社所在地	東京
拠点数	(非公開)
社員数	(非公開)
認証	「ISO27001」(部門取得)・「ISO9000」

12.2. 被験者企業Jにおける予防接種の概要

表 48 に示す日程と規模で、被験者企業 J に対する予防接種を実施した。

表 48 被験者企業 J：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/20 13:00	2009/2/3 13:00
種明かし	なし	2009/2/9(事業部毎に違う)
被験者数	94 名	94 名

被験者企業 J における被験者は 94 名であり、管理職を中心として 3 つの事業部門から選定した。

被験者企業 J では、事前に今回の予防接種を実施することを予告した。
また、第 1 回配信後には種明かしを行わず、そのまま第 2 回配信を行った。第 2 回配信実施後には種明かしを行った。

12.3. 擬似攻撃メールの内容

12.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 J において、第 1 回配信に用いた擬似攻撃メールをリスト 30 に示す。

この擬似攻撃メールは、リスト 2 のサンプル(11)を参考にして作成した。
この擬似攻撃メールでは、「本部長から、来期事業計画関連資料を配付するの

で、明日の会議までに目を通すように」という業務指示を装うものである。本部長という権威ある役職からの指示で、しかも「明日の会議までに」という形で添付ファイル開封を急がせている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「本部長」とし、個人を特定していない。
2. 差出人のメールアドレスを moto02501@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
3. 表題と本文に「明日の会議」という表現を使うことで、添付ファイルの開封を急がせている。
4. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する

リスト 30 被験者企業 J：第 1 回配信の擬似攻撃メール

From: 本部長 < moto02501@(フリーメール B)>
Subject: 明日の資料

各部門長から提出いただいた内容をベースに、来期事業計画について
まとめた資料です。明日の会議で検討するので、よく目を通しておい
てください。

添付ファイル名:来年度の事業計画(案).doc

12.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 J における第 2 回配信の擬似攻撃メールをリスト 31 に示す。

この擬似攻撃メールは、被験者企業 J の窓口担当者の原案によって文面を作成した。

この擬似攻撃メールでは、「外交問題研究所」という外部のシンクタンクと思われる組織を差出人として、米国の大統領交代が日本の外交・経済に与える影響について調査報告を送る体裁を装っている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名に設定した「外交問題研究所」は実在しない組織である。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 本文の「急ぎご一読下さい」という表現で、添付ファイルの開封を急がせている。

4. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 31 被験者企業 J：第 2 回配信の擬似攻撃メール

```
From: 外交問題研究所<censusteam@(フリーメール A)>
Subject: 緊急報告)米国の外交政策はこう変わる

米国の新大統領就任が日本外交や経済に与える影響についての調査レポートです。
急ぎご一読下さい

添付ファイル名:調査レポート.doc
```

12.4. Webビーコンの集計結果

被験者企業 J について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 49 に示す。

Web ビーコンから見ると、被験者企業 J における添付ファイルの開封率は、第 1 回配信の 32 名(34.0%)から第 2 回配信の 6 名(6.4%)へと改善が見られた。
しかし、2 回とも開封した被験者が 5 名(5.3%)おり、絶対数では少数ではあるが、開封する者は開封するという側面が見られる。

なお、被験者企業 J では第 1 回配信の後に種明かしを実施しなかったので、Web ビーコンのアクセスログの集計対象期間として、擬似攻撃メール配信日時から 3 営業日目の終わりまでを採用した。

表 49 被験者企業 J：Web ビーコン集計

	第 1 回	第 2 回
被験者数	94 名	94 名
Web ビーコンへのアクセス総数	63 回	39 回
開封したと考えられる人数	32 名(34.0%)	6 名(6.4%)
2 回とも開封した人	5 名(5.3%)	

12.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 J の添付ファイル開封状況は、以下の通りである。

被験者企業 J では、擬似攻撃メール配信の後およそ 1 時間で、ほとんどの開封者が添付ファイルを開封している。

図 86 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 87 に示す。

図 86 被験者企業 J：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

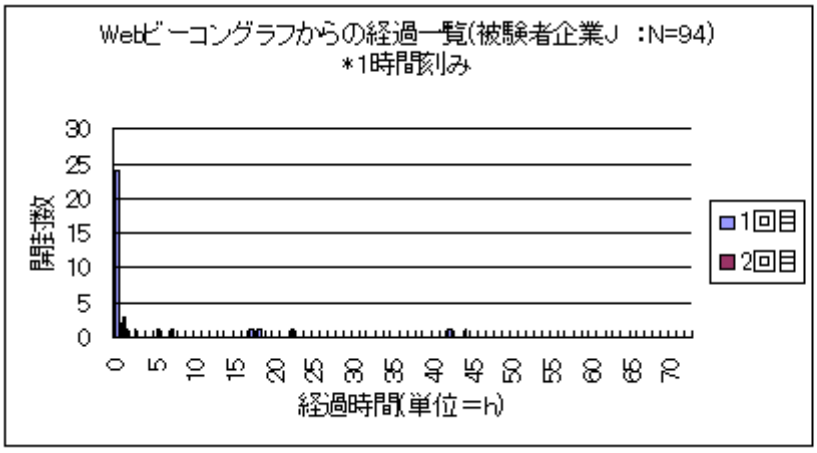
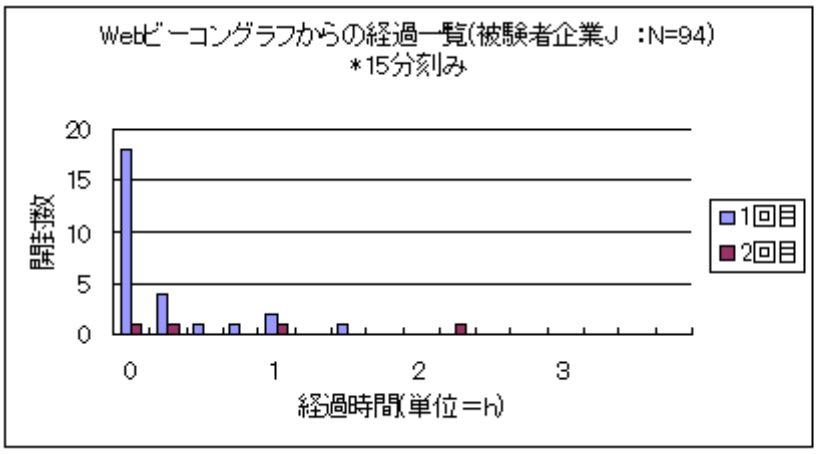


図 87 被験者企業 J：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



12.6. 予防接種実施時の特記事項

12.6.1. 予防接種実施に関する事前予告

被験者企業 J では、予防接種を実施することを事前に被験者に対して周知している。この点は、他のほとんどの被験者企業での状況とは異なる点に注意する必要がある。

被験者企業アンケートの設問 D に該当する記述があるので引用しておく。

1. 弊社内の状況ですが、弊社では社内に予防接種実施を予告しましたが、予告以降、職場内の緊張が高まったり、その他の不審メールへの警戒度も上がったようです。
2. 今回は、対象者にアンケート協力を依頼する都合上、修了宣言を出しましたが、予防接種は修了宣言しない方が、社内の緊張感が維持できて望ましいと思われます。

12.6.2. 偵察アクセス

被験者企業 J では、偵察アクセスを観測しており、一部に専門的な技術知識を有する被験者が存在する。

第 1 回配信の際には、総アクセス回数 63 回のうちの 17 回(27.0%)の偵察アクセスが見られた。また、第 2 回配信の際には、総アクセス回数 39 回のうち 33 回(84.6%)の偵察アクセスが見られた。

この中には、Web ビーコンの URL を多少改変してアクセスするものや、異なる HTTP Method を用いるものなどがある。

通常、偵察アクセスは第 1 回配信時よりも第 2 回配信時の方が少なくなるものだが、被験者企業 J ではアクセス数も比率も逆に増加している。
これは、第 2 回配信の擬似攻撃メールの話題が、その出所に対する好奇心を惹起するものであったのではないかと思われる。

12.7. 被験者アンケートの集計

被験者企業 J の被験者アンケートの集計状況について表 50 に記す。

表 50 被験者企業 J：被験者アンケート回答者の開封状況

有効回答数	32 名	
	第 1 回	第 2 回
開封した人数	11 名(34.4%)	1 名(3.1%)
2 回とも開封した人	1 名(3.1%)	

被験者企業 J では、被験者数 94 名に対して 42 名(44.7%)から被験者アンケートの回答があった。
しかし、このうちの 10 名が擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答数を 32 名とする。被験者アンケート回答率は 34.0%となる。

有効回答者 32 名の中で、一度でも開封した被験者は 11 名(34.4%)であり、第 1 回配信での開封者も 11 名(34.4%)、第 2 回配信での開封者は 1 名(3.1%)である。

また、両方を開封した被験者は 1 名(3.1%)であった。

前節で Web ビーコンから開封率を見たが、本節のアンケート回答者の開封率はよく似ている。すなわち、第 1 回配信については 34.0%対 34.4%、第 2 回配信では 6.4%対 3.1%である。

12.8. 被験者アンケートの分析

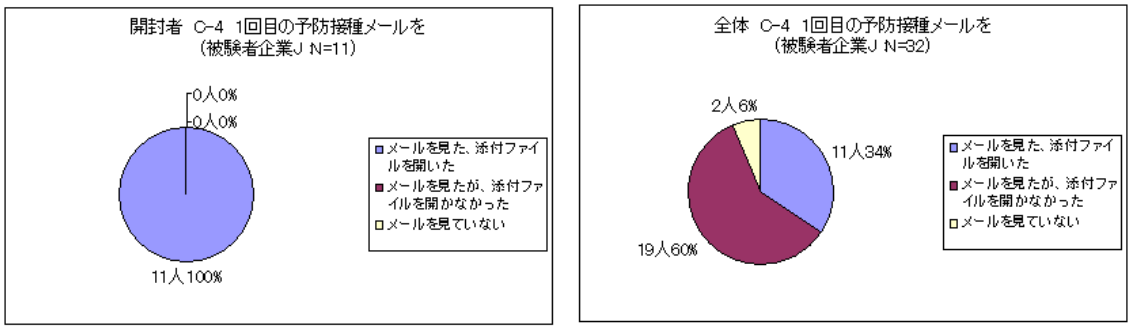
本節では、被験者企業 J の被験者アンケートの有効回答の内容から、その特徴となる諸点を示す。

12.8.1. 添付ファイル開封の有無とその理由

ここでは、被験者アンケートから見た開封状況とその理由などを調べる。

まず、被験者アンケートの設問 C-4 に対する回答を図 88 に示す。

図 88 被験者企業 J：被験者アンケートから見た開封状況(第 1 回配信)



これによれば、第 1 回配信では、有効回答者 32 名中の 11 名(34.4%)が、添付ファイルを開封したと解凍している。

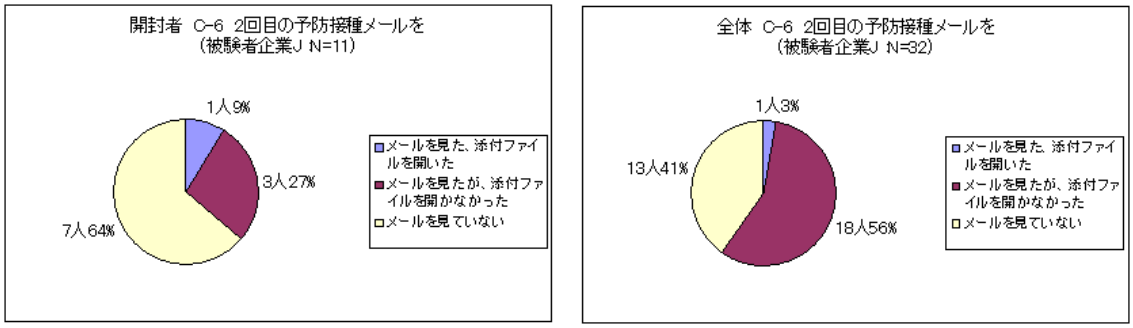
設問 C-5 に対する回答からその理由を探すと、差出人のメールアドレスをよく確認することなく、表題や本文のキーワードに目を奪われて開封している傾向が読み取れる。

設問 C-5 への回答から該当する部分を以下に抜粋しておく。

1. 差出人や表題があり得るものだったので、特に疑わずに開けてしまった。

次に、第 2 回配信について同様に検討する。図 89 に被験者アンケートの設問 C-6 に対する回答状況を示す。

図 89 被験者企業 J：被験者アンケートから見た開封状況(第 2 回配信)



これによれば、第 2 回配信では、有効回答者 32 名中の 1 名(3.1%)が添付ファイルを開封したと回答している。この 1 名は、第 1 回配信の際にも添付ファイルを開封している。

設問 C-7 から開封の理由を探ると、メール処理を急いだあまり本文の「緊急」や「本部長」などのキーワードに気を取られて開封してしまったとある。
これは、メールを常に注意深く取り扱うことがどうしても困難であるという状況を示唆しているだろう。

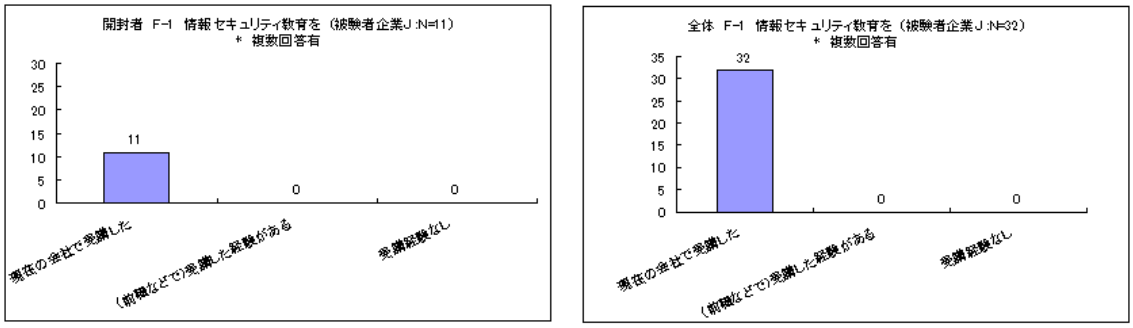
第 1 回配信では添付ファイルを開封し、かつ、第 2 回配信では開封しなかった被験者は、どのような理由で添付ファイルを開かなかったのであろうか。
被験者アンケートの C-7 への回答から検討すると、このような被験者が、差出人の表示名に馴染みがないことに気付いて、さらに差出人のメールアドレスを確認していることがわかる。

12.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

図 90 に、被験者アンケートの設問 F-1 に対する回答状況を示す。

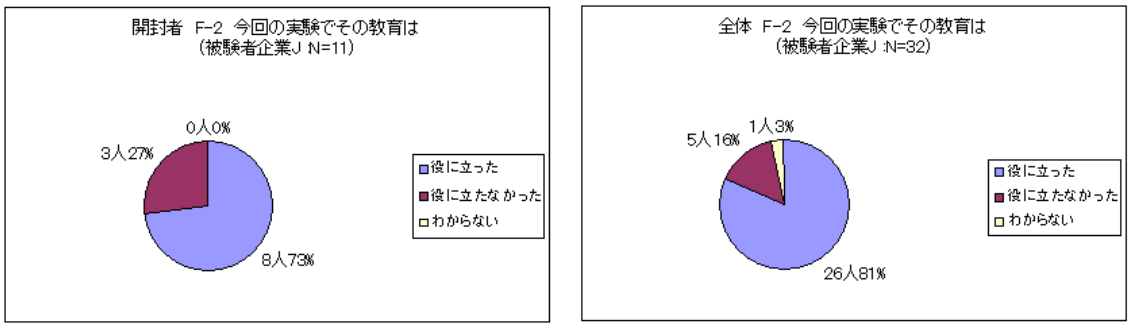
図 90 被験者企業 J：情報セキュリティ教育の経験



これによれば、被験者アンケートの有効回答者 32 名中の全員が現在の勤務先で情報セキュリティ教育を受けている。

次に、設問 F-2 に対する回答から、情報セキュリティ教育の有効性を考える。図 91 に、設問 F-2 に対する回答状況を示す。

図 91 被験者企業 J：情報セキュリティ教育の有効性



これによれば、受講した情報セキュリティ教育が予防接種に対して役に立ったと回答している被験者は、有効回答者 32 名中の 26 名(81.3%)であり、開封者 11 名の中では 8 名(72.7%)を占める。

情報セキュリティ教育が役に立ったけれども、添付ファイルを開いてしまったというのは、相矛盾していて解釈が難しいところである。

被験者アンケートの設問 F-4(危機管理意識の変化)と設問 G(感想)への回答をみると、今回の IT セキュリティ予防接種を体験することによって、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したという感想が多く見られた。

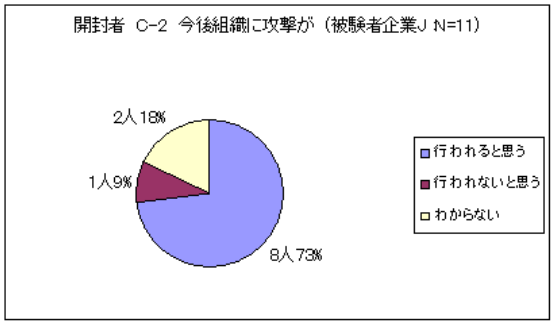
予防接種のような体験型の訓練には、知識として理解していた(またはそのつもりになっていた)セキュリティ教育の内容を体得させる効果があるといえるのではないか。

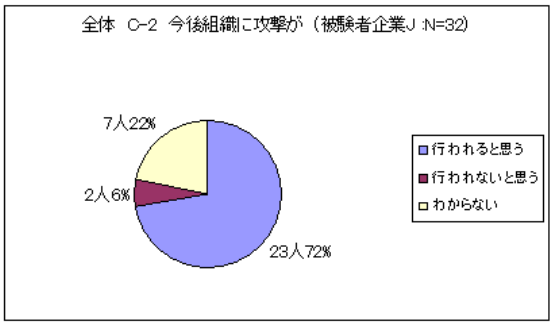
12.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようなことが起きると思われるかを検討する。

図 92 に設問 C-2 に対する回答状況を示す。

図 92 被験者企業 J：今後組織に攻撃があると思うか





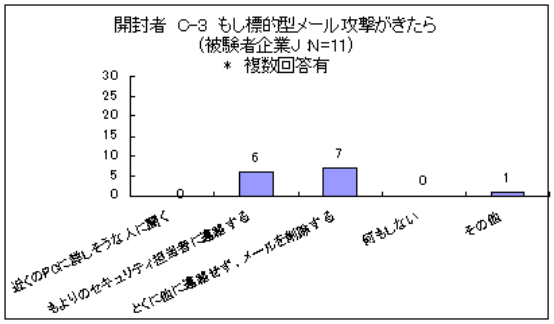
これによれば、有効回答者 32 名の中で、今後組織に標的型メール攻撃が行われると思うと回答している被験者は 23 名(71.9%)である。

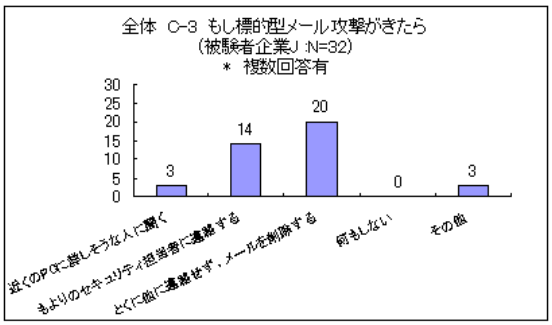
被験者企業 J が日頃から危機意識が高いことを表しているものと思われる。

また、擬似的なものではあっても予防接種の擬似攻撃メールを受け取って、脅威を改めて認識したということであろう。

図 93 に設問 C-3 に対する回答状況を示す。

図 93 被験者企業 J：もし標的型メール攻撃が来たら



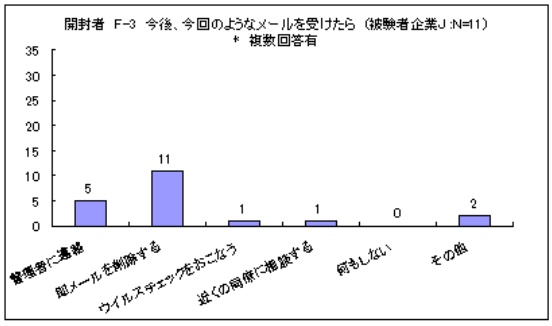


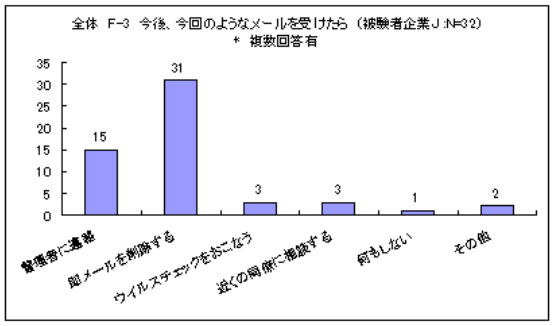
これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 32 名中の 14 名(43.8%)である。

また、「とくに他に連絡せず削除する」と回答した被験者は、有効回答者 32 名中の 20 名(62.5%)である。

図 94 に設問 F-3 に対する回答状況を示す。設問 F-3 は、設問 C-3 とほぼ同じ内容について、表現を変えて再び質問するものである。

図 94 被験者企業 J：今後、今回のようなメールを受けたら





これによれば、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者は、有効回答者 32 名中の 15 名(46.9%)で、設問 C-3 の時とほぼ同じである。しかし、「即メールを削除する」と回答した被験者は、有効回答者 32 名中の 31 名(96.9%)で、設問 C-3 の場合よりも大幅に増加し、ほぼ全員がこの回答を選択した。

12.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4 では、危機管理意識の変化の有無を尋ねている。

被験者企業 J における設問 F-4 への回答状況を見ると、有効回答者 32 名中の 25 名(78.1%)の被験者が、今回の訓練を通して危機管理意識の変化、もしくは危険の再認識をしたと回答しており、予防接種を肯定的に捉えている。

また、自由記述欄に有益な回答が見られたので抜粋しておく。

1. メールを受信した時に、明らかにウイルスメールだと判ったが、なかなか手の込んだ内容だと感心した。
2. 訓練内容と直接関係ないかもしれないが、「メールに具体的かつ適切な表題をつけておく」ことの有意性について気付かされた。(一般的に、表題のつけ方がいい加減すぎ。←教育等で触れられる機会は少ないが、重要なことでは？)。
3. セキュリティには自信がありました。ただし、前述のように、社内のアドレス帳の変更により間違いメールが多発している状況を放置して、セキュリティと言っても片手落ちであることが良く分かりました。

12.8.5. 感想

被験者アンケートの設問 G では、24 名の被験者から予防接種全体についての感想を回答していただいた。

回答には、今回の予防接種訓練からさまざまな教訓を得ている様子がうかが

えるので、いくつか抜粋しておく。

1. ＩＴ専門家も引っかかっており、会社として課題は大きい。
2. 擬似攻撃メールは差出人が通常と異なるので、違和感を感じた。
3. ただの座学や E-ラーニングによる教育だけでなく、このようなショッキング的な試みは良いことだと思います。今後も定期的に、予告なしで実施してはいかがでしょうか？なお、メールを明けさせようとする側と、守る側の攻防はエンドレスです。注意点や見破る方法のフォローを必ず実施してください。それがないと、ただの意地悪に感じてしまうのは私だけでしょうか？
4. それらしいメール表題、メールアドレスだった場合、確実に排除できる自信は無い。ソフトウェアによる排除も強力に推進してください。
5. なぜ、自分にだけ、このような嫌がらせメール(？)が来るのだろうと思った。本当の標的型メールもこのように、本当に捨ててもいいかなと思うような題名で送られてくるのなら、気をつけなくてはいけないと思いました。

12.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 J に対する被験者企業アンケートや被験者企業インタビューから、以下のことがわかった。

被験者企業アンケートから、以下のことが読み取れる。

1. 被験者企業 J は、ISO27001 を部門取得している。
2. 情報セキュリティの管理体制はほぼ整備されており、インシデントの連絡体制(窓口)も定められている。
3. 定期的な情報セキュリティ教育を実施している。

これらのことから、被験者企業 J では、情報セキュリティ体制が概ね整備され、情報セキュリティに対する関心は非常に高いものがあると感じられる。

被験者企業 J における被験者企業インタビューでは、以下のような見解・意見を得た。

1. 被験者企業 J では、予防接種の実施を社内に予告した。この結果、社内の警戒心が高まり、予防接種以外のセキュリティ問題も含めて、大変効果があった。
2. 擬似攻撃メールの本文なども、なるべく現実の実例に即したもので、全員が引っかかってしまうレベルのものが望ましい。
3. 実際に起きた標的型メール攻撃のケーススタディや犯人情報を世間に広報して欲しい。

12.10. 考察

被験者企業 J は、総じて地道なセキュリティ対策を着々と実施している印象を受けた。

被験者企業 J では、被験者アンケートで「標的型メール攻撃が今後来ると思う」と回答した被験者が 4 分の 3 に上る。

セキュリティポリシーを考えるものにとっては、少なくとも、通常の迷惑メールと標的型攻撃メールを区別して、その特性と傾向に応じた情報セキュリティ教育を確立する必要があるだろう。同時に、インシデント報告の重要性を喧伝することもまた必要である。

13. 被験者企業K

13.1. 被験者企業Kの概要

被験者企業 K は、自動車製造の分野で要素技術・システム・製品を提供するメーカーである。

なお、実際には、被験者企業 K およびその情報システム子会社 2 社から被験者を選定した。

表 51 に被験者企業 K の概要を示す。

表 51 被験者企業 K：概要

業種	製造業
設立	(非公開)
資本金	(非公開)
本社所在地	(非公開)
拠点数	(非公開)
社員数	(非公開)
認証	「ISO27001」取得部門あり

13.2. 被験者企業Kにおける予防接種の概要

表 52 に示す日程と規模で、被験者企業 K に対する予防接種を実施した。

表 52 被験者企業 K：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/28 11:00	2009/2/12 11:00
種明かし	なし	2009/2/16
被験者数	65 名	65 名

被験者企業 K における被験者は 65 名であり、被験者企業 K と情報システム系子会社 2 社の計 3 社から選定した。

これらの被験者は、IT 担当の比較的若年層を選んでいる。

また、被験者が周囲の被験者の状況から影響を受けにくいように、机の島に被験者が 1 名だけになるように配慮した。

なお、今回の予防接種に際して、第 1 回配信より前には、予防接種が行われることを特に周知していない。これは、被験者企業 K では、定常的に様々なセキュリティ問題に関する注意喚起を行ってきており、標的型メール攻撃の話題もその中で扱っているので、敢えてもう一度注意喚起を行う必要はないと判断したとのことである。

また、第 1 回配信の後の種明かしも行わなかった。

13.3. 擬似攻撃メールの内容

13.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 K において、第 1 回配信に用いた擬似攻撃メールをリスト 32 に示す。

リスト 32 被験者企業 K：第 1 回配信の擬似攻撃メール

```
From: 案内 < stats_mastor@(フリーメール B)>
Subject: 4 月以降の組織

(被験者企業 K の情報システム部門名)、(子会社名 1)、(子会社名 2) 各位

09 年 4 月からの組織ですが、
以下のファイルのように案を作成しました。
確認ください。

添付ファイル名:組織表 0904.doc
```

この擬似攻撃メールは、新年度に向けた組織変更を案内する風を装うものである。年度末の近い時期でもあり、被験者にとっては興味をそそられる話題であろう。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「案内」とし、個人を特定していない。
2. 差出人のメールアドレスを stats_mastor@(フリーメール B)とした。これは明らかにフリーメールのアドレスである。
3. 他には、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

13.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 K において、第 2 回配信に用いた擬似攻撃メールをリスト 33 に示す。

この擬似攻撃メールでは、マイクロソフト社が Windows やその他の製品について「重要な更新」を配布する月例日に、Windows XP のセキュリティ対策を要請する態を装っており、「至急セキュリティ対策を施」すように求めることで添付ファイルの開封を急がせている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「緊急対策チーム」とし、個人を特定していない。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 他には、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 33 被験者企業 K：第２回配信の擬似攻撃メール

From: 緊急対策チーム <censusteam@(フリーメール A)>
Subject: 至急対策ください

1/31 に windows XP に深刻な脆弱性が見つかりました。
今のところ、マイクロソフトからパッチ提供がありませんが、
暫定対策として以下が有効と思われます。

以下のマニュアルに従い、至急セキュリティ対策を施してください。

添付ファイル名:対策マニュアル.doc

13.4. Webビーコンの集計結果

被験者企業 K について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 53 に示す。

Web ビーコンから見ると、被験者企業 K における添付ファイルの開封率は、第１回配信の 48 名(73.8%)から第２回配信の 11 名(16.9%)へと改善が見られた。

しかし、2 回とも開封した被験者が 10 名(15.4%)おり、絶対数では少数ではあるが、開封する者は開封するという側面が見られる。

に掲げる。

表 53 被験者企業 K：Web ビーコン集計

	第 1 回	第 2 回
被験者数	65 名	65 名
Web ビーコンへのアクセス総数	52 回	13 回
開封したと考えられる人数	48 名(73.8%)	11 名(16.9%)
2 回とも開封した人	10 名(15.4%)	

13.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 K における擬

似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業 K では、擬似攻撃メール配信の後、約 2 時間でほとんどの開封者が添付ファイルを開封している。

図 95 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 96 に示す。

図 95 被験者企業 K：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

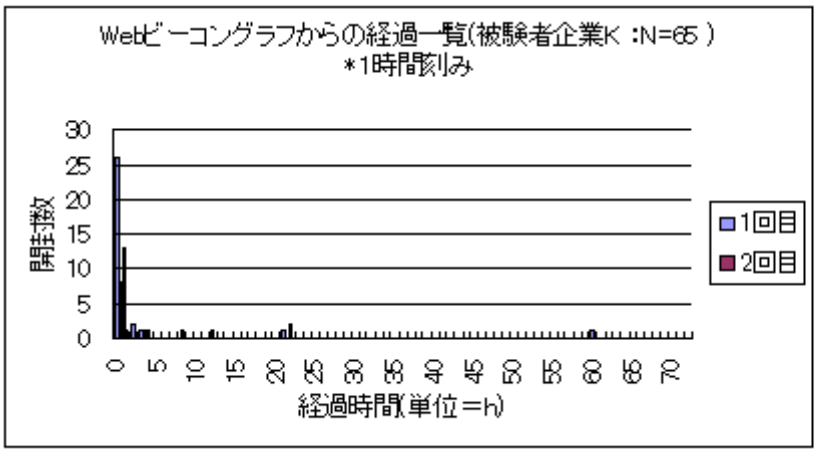
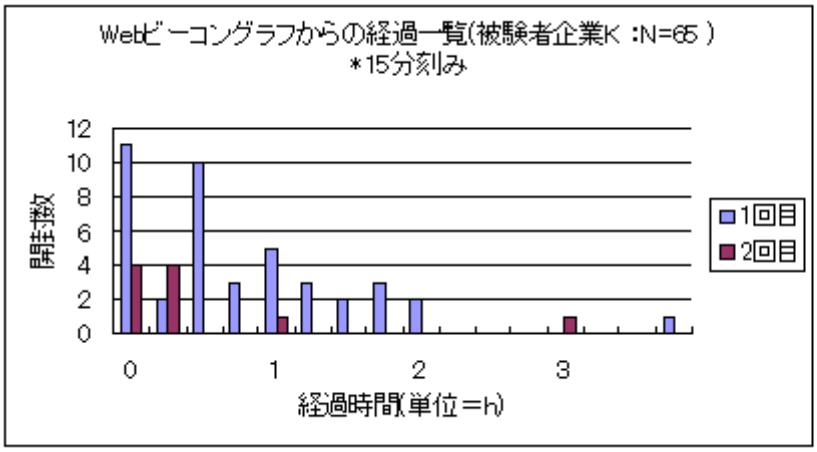


図 96 被験者企業 K：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



13.6. 予防接種実施時の特記事項

特になし。

13.7. 被験者アンケートの集計

被験者企業 K における被験者アンケートの集計状況について表 54 に記す。

表 54 被験者企業 K：被験者アンケート回答者の開封状況

有効回答数	35 名	
	第 1 回	第 2 回
開封した人数	28 名(80.0%)	5 名(14.3%)
2 回とも開封した人	5 名(14.3%)	

被験者数 65 名に対し、37 名からアンケートの回答があったが、このうち 2 名が擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答者数を 35 名(被験者数に対して 53.8%)とする。

被験者アンケートの有効回答者 35 名の中で、第 1 回配信での開封者は 28 名(80.0%)、第 2 回での開封者は 5 名(14.3%)である。両方を開封した被験者は 5 名(14.3%)であり、一度でも添付ファイルを開封した被験者は 28 名(80.0%)である。

前節で Web ビーコンから開封率を見たが、本節のアンケート回答者の開封率と比べてさほどの違いがない。すなわち、第 1 回配信については 73.8%対 80.0%、第 2 回配信では 16.9%対 14.3%である。

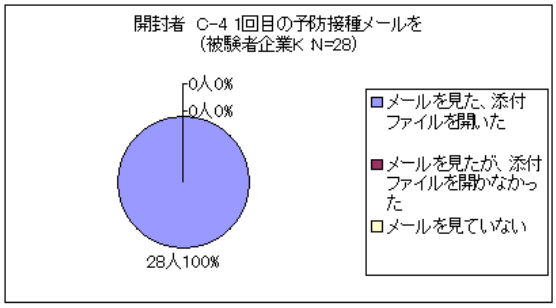
13.8. 被験者アンケートの分析

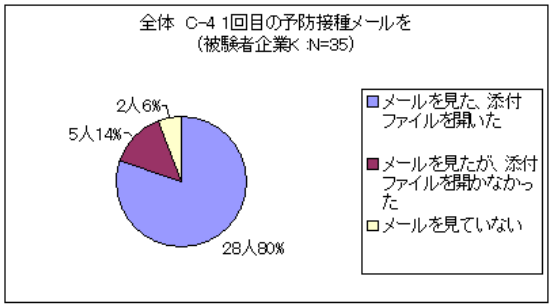
本節では、被験者企業 K の被験者アンケートの回答内容から、その特徴となる諸点を示す。

13.8.1. 添付ファイル開封の有無とその理由

被験者企業 K における被験者アンケートの設問 C-4 に対する回答状況を図 97 に示す。

図 97 被験者企業 K：被験者アンケートから見た開封状況(第 1 回配信)





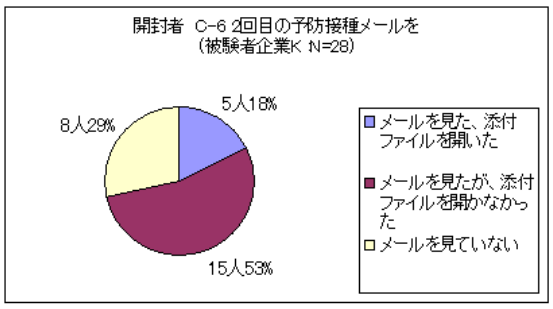
前述の通り、被験者企業 K の第 1 回配信では、有効回答者 35 名中の 28 名(80.0%)が添付ファイルを開封したと回答している。

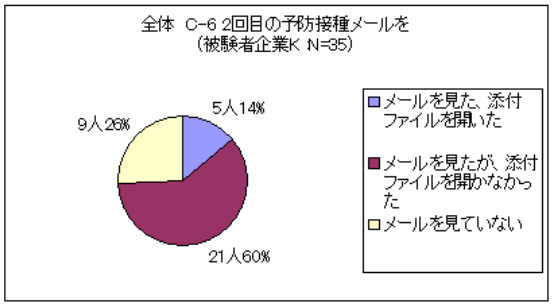
被験者アンケートの設問 C-5 に対する回答から探すと、以下のような理由を読み取ることができる。

1. もっともらしい表題だった。
2. メールのタイトルを見て、内容が気になったため。
3. Notes なので送信元のメールアドレスではなく、表示名が表示される。

被験者企業 K における被験者アンケートの設問 C-6 の回答結果を図 98 に示す。

図 98 被験者企業 K：被験者アンケートから見た開封状況(第 2 回配信)





前述の通り、第 2 回配信では有効回答者 35 名中の 5 名(14.3%)が添付ファイルを開封したと回答している。

第 1 回配信と比較すると開封者は大幅に減少しており、第 1 回配信での体験とその後の周知・教育の効果が読み取れる結果となった。

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が、どういう理由で開封しなかったのかを、被験者アンケートの設問 C-7 に対する回答から検討する。

当該被験者の多くは、差出人の表示名やメールアドレスを仔細に確認したり、メール本文の内容が本当に自分に関係あるのか否かを注意深く確認したりしていることがわかる。

これは、第 1 回配信とその後の周知・教育の効果があったものと思われる。

ただし、第 2 回配信ではメール本文中の呼び掛けが被験者本人宛ではなかったので、これが原因となって第 2 回配信の差出人を細かく確認したのかもしれない。

第 1 回配信と第 2 回配信の両方で添付ファイルを開封した被験者は 5 名(14.3%)であった。

設問 C-7 への回答から、開封の理由をいくつか抜粋する。

1. ウィルス対策のパッチをあてるメールが大体同タイトルであったと記憶している。とくにＸＰは要対応のものが多く、ＰＣに詳しくない私はいつも対応に時間がかかっていた。
2. メールを確認・添付ファイルを開くより、開かない方が業務影響があると考えたため(何かの打合せの際に確認されるなど)
3. 何かよく分からないけど、とりあえず中身を確認した。
4. 社内からのメールと思って特に気にせず開いた。
5. 送信者名は不審に思いましたが、もっともらしい表題だったので開いてしまいました。

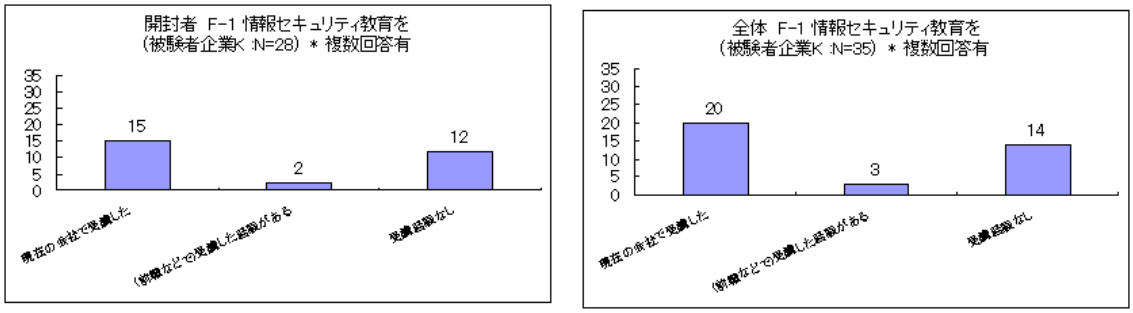
第 2 回配信では、マイクロソフトの月例パッチ配信日に Windows XP のセキュリティ対策の話題を使って擬似攻撃メールを配信したので、もっと開封者が多いものと予想していたが、現実には予想よりも少なかった。

13.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

被験者アンケートの設問 F-1 への回答状況を図 99 に示す。

図 99 被験者企業 K：情報セキュリティ教育の経験



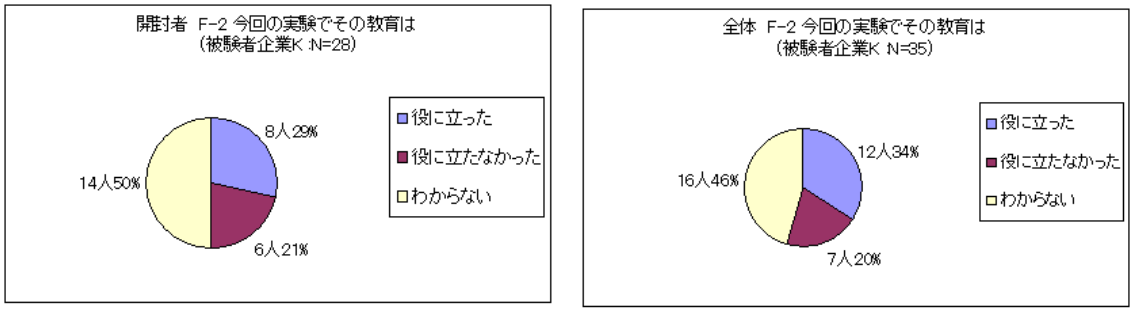
これによれば、被験者アンケート有効回答者 35 名中の 20 名(57.1%)が、現在の勤務先で情報セキュリティ教育を受けたと回答している。

この 20 名の中の 15 名(75.0%)が、第 1 回または第 2 回の擬似攻撃メールの添付ファイルを開封している。

また、現在の勤務先で教育を受けたと答えていない 15 名中の 13 名(86.7%)が、添付ファイルを開封している。

被験者アンケートの設問 F-2 に対する回答状況を図 100 に示す。

図 100 被験者企業 K：情報セキュリティ教育の有効性



これによれば、会社で受けた情報セキュリティ教育が予防接種で役に立ったと回答している被験者は、有効回答者 35 名中の 12 名(34.3%)である。

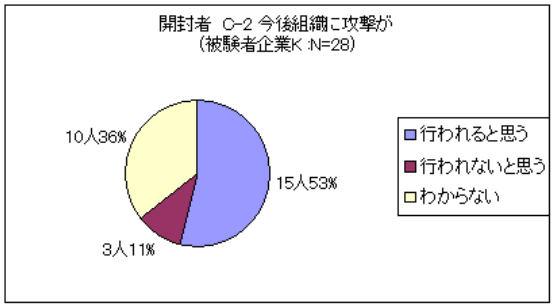
教育が役に立ったかどうかわからないと回答した被験者は、有効回答者 35 名中の 16 名(45.7%)を占めており、開封者 28 名中では 14 名(50.0%)と、ほぼ半数を占めている。

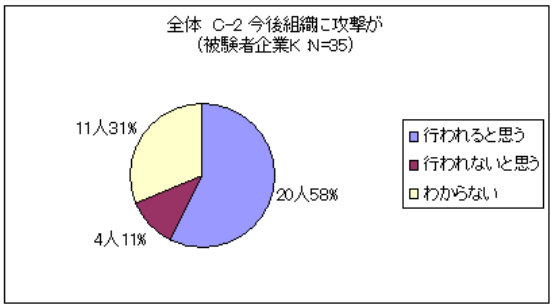
13.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのような反応を示すと思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答状況を図 101 に示す。

図 101 被験者企業 K：今後組織に攻撃があると思うか

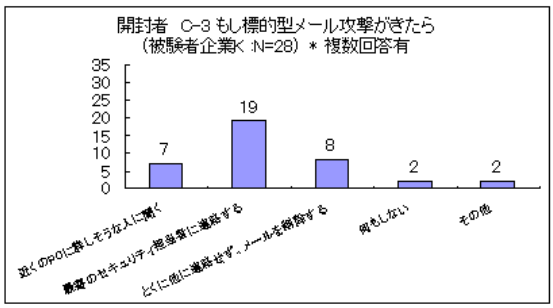


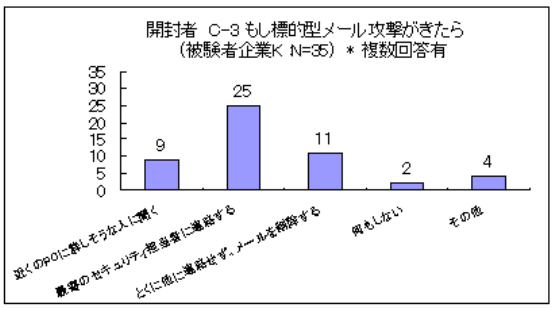


これによれば、有効回答者 35 名の中で、今後組織に標的型メール攻撃が行われるかもしれないと回答している被験者は、20 名(57.1%)である。

被験者アンケートの設問 C-2 に対する回答状況を図 101 に示す。

図 102 被験者企業 K：もし標的型メール攻撃が来たら





これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 35 名中の 25 名(71.4%)である。

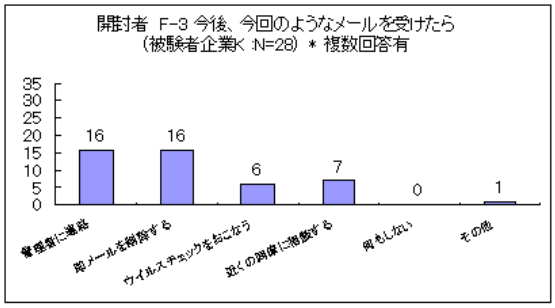
他方で、35 名中の 11 名(31.4%)は、「とくに他に連絡せずに削除する」と回答している。

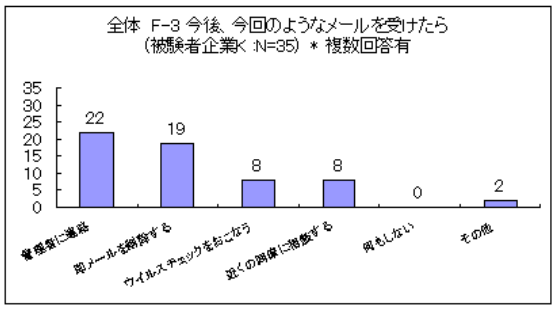
プライバシーマーク制度におけるヒヤリハット届出や、ISO27001 でのインシデント報告の義務は、ここでもあまり浸透していない。

被験者アンケートの設問 F-3 に対する回答状況を図 103 に示す。

この設問では、設問 C-3 と同様の内容を、異なる形で再び尋ねている。

図 103 被験者企業 K：今後、今回のようなメールを受けたら





これによれば、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者は、有効回答者 35 名中の 22 名(62.9%)で、先程の設問 C-3 での回答状況よりも、比率がやや下がっている。

逆に、「即メールを削除する」と回答している被験者は有効回答者 35 名中の 19 名(54.3%)と増加している。

この誘導では、証拠保全し管理者に連絡することの重要性が認識される方向には向かわず、危険なメールは削除すればよいという考え方に流されているようだ。

13.8.4. 危機管理意識の変化

ここでは、被験者アンケートの設問 F-4 に対する回答を用いて、被験者の危機管理意識が変化したか否かについて調べる。

有効回答者 35 名中の 25 名(71.4%)の被験者が、予防接種によって危機管理意識の変化、もしくは、危険の再認識をしており、予防接種を肯定的に捉えている。

また、自由記述欄には以下のような回答があった。

1. 会社のネットワークであれば安全であると思っていました。
2. 表題だけでは不審なメールだと判断できないので、見覚えの無いアドレスだった場合、メールを開かないようにしようと思った。

ひとつはシステム側のスパム対策が成功していることで、標的型メール攻撃に対する警戒心が薄れている例であり、今年度の予防接種でも時々見られる現象である。

もうひとつは、予防接種から非常に素直に教訓を学んでいる様子がうかがえるものである。

13.8.5. 感想

ここでは、被験者アンケートの設問 G に対する回答から、メッセージを読み

とることを試みる。

被験者アンケートの設問 G に対する回答では、有効回答者 35 名中の 15 名(42.9%)が予防接種を肯定的に捉えており、予防接種再実施の提案や、日頃から注意しなければならない等と回答している。

また、被験者企業 K で使っているグループウェアに対して、改善の余地があるとして、以下のような回答があった。

1. Lotus Notes の受信ボックスにて、プリビュー画面を表示していると、受信と同時にメールを自動的に開いてしまうため、表示を見直すきっかけとなった。
2. 現在の Lotus Notes では、メール一覧の画面には発信者のアドレスが表示されません。ひと目でわかるよう、改善の余地ありと思います。
3. メーラーに Notes を使用していますが、Notes のメール受信リストでは送信メールアドレスが分からないため、送信者の名前で判断することになります。受信リストで送信メールアドレスが分かれば、安全なメールであるか即座に把握できると思います。
4. Lotus Notes の仕様か設定かは不明だが、受信ボックス上ではメールアドレスが確認できない(送信者名が表示される)。もっともらしい送信者名、表題を偽装されれば、メールを見るのを防ぐのは困難だと思う。添付ファイルを開かないようにするのは当然だが、セキュリティ強化を優先するなら、メールを見るだけで外部へのアクセスを強要できる HTML 形式のメールは禁止すべきだと考える。

もちろん、差出人のメールアドレスを詐称することも容易にできるが、この部分を確認することは標的型メール攻撃を防ぐ上で基本的な手順である。
したがって、Lotus Notes に限らずメールソフトので、差出人のメールアドレスを表示するように設定変更しておくべきである。もし、そのような機能がないのであれば、そのメールソフトは採用するべきではないかも知れない。

13.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 K について、被験者企業アンケートと被験者企業インタビューから以下のことがわかる。

被験者企業 K では、毎年一度の情報セキュリティの強化月間を設けており、情報セキュリティに対して非常に真摯に取り組んでいる。

被験者企業 K は、人員の規模も地理的な分散も大きいこともあって、情報セキュリティ対策のための組織編成としては、中央のセキュリティ対策チームが

各内部組織の OA 担当者を教育し、その OA 担当者が教育内容を各内部組織に持ち帰る仕組みを取っている。特に製造業では、同様の方法で TQC や ISO9000 シリーズなどに対応してきた歴史もあるので、適切な方法であると言える。
ただし、個々の OA 担当の能力や熱意の多寡によって伝達度合いが変わってしまう欠点があるとのことなので、効果測定などを適切に行うことが必要であろう。

被験者企業 K では、グループウェアとして Lotus Notes を使用しているため、メールソフトとしても Lotus Notes を使用している。
Lotus Notes のメールソフト機能については、被験者アンケートへの回答にもあったように、差出人のメールアドレスを表示する設定にするなど、若干の手当が必要であるようだ。s

13.10. 考察

被験者企業 K における第 1 回配信の開封率は、Web ビーコンから見ても被験者アンケートから見ても 70%から 80%と、非常に高かった。また、約 15%の被験者が 2 回とも開封しており、全体としては、最も開封率の高い被験者企業のひとつである。
その反面で、第 1 回配信から第 2 回配信にかけて非常に大きな改善が見られるので、被験者が標的型メール攻撃に慣れていないのではないかと考えている。

また、被験者企業 K における被験者アンケートでは、「今後組織に攻撃が行われると思う」被験者の割合は 56%程度で、被験者全体の平均に比べてやや低いと言わざるを得ない。被験者が主に 20 歳代から 30 歳代であることが、危機意識の低さにつながっているのであろうか。

14. 被験者企業L

14.1. 被験者企業Lの概要

被験者企業 L は、シンクタンク系の情報セキュリティ専門子会社で、各種の情報セキュリティ関連サービスやコンサルティングなどを取り扱っている。

表 55 に被験者企業 L の概要を示す。

表 55 被験者企業 L：概要

業種	情報通信業
設立	2000 年 8 月 1 日
資本金	4.5 億円
本社所在地	東京
拠点数	2 箇所
社員数	約 120 名
認証	「ISO27001」(全社取得)

14.2. 被験者企業Lにおける予防接種の概要

表 56 に示す日程と規模で、被験者企業 L に対する予防接種を実施した。

表 56 被験者企業 L：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/29 13:00	2009/2/12 13:00
種明かし	2009/1/29 17:20	2009/2/12 17:20
被験者数	124 名	124 名

被験者企業 L における被験者は、ほぼ全社員の 124 名である。

また、被験者企業 L は、全社で ISO27001 を取得しているので、被験者は情報セキュリティ教育を受けているはずである。

14.3. 擬似攻撃メールの内容

14.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 L における第 1 回配信の擬似攻撃メールをリスト 34 に示す。

この擬似攻撃メールは、リスト 2 のサンプル(11)を参考にして作成した。

この擬似攻撃メールでは、全社定例会議で来期事業を検討するので、添付した資料に目を通しておくようにと社長名で指示している。表題に「明日の資料」とあるので、被験者に対して、添付ファイルを急いで開封するように誘導して

いる。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名に社長の姓を使用した。被験者は日常的にこのようなことがあるか否かを考える必要がある。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 他には、差出人の所属・連絡先を記した署名(フッタ)が、中途半端な点が、標的型攻撃メールの特徴に一致する。

リスト 34 被験者企業 L：第 1 回配信の擬似攻撃メール

From: (社長の姓) < censusteam@(フリーメール A)>
Subject: 明日の資料

各事業部長から提出いただいた内容をベースに、来期事業について
まとめた資料です。全社定例で検討するので、よく目を通しておい
てください。

(社長の姓)

添付ファイル名:来期の事業案内(案).doc

14.3.2. 第 2 回配信の擬似攻撃メール

リスト 35 に、被験者企業 L における第 2 回配信で用いた擬似攻撃メールを示す。

この擬似攻撃メールは、リスト 2 のサンプル(4-2)を参考にして作成した。

この擬似攻撃メールでは、個人情報保護法関連の架空のセミナーについての受講希望者募集を装っている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名が部長級の実在人物の姓である。このような案内が日常的にあるか否かを被験者は考える必要がある。
2. 差出人のメールアドレスを censusteam@(フリーメール A)とした。これは明らかにフリーメールのアドレスである。
3. 「個人情報保護法セミナー」と言っているだけで具体的な名称がない。
4. 他には、呼びかけが「各位」となっていて宛先の個人の名前を呼

んでいない点や、差出人の所属・連絡先を記した署名(フッタ)が、中途半端な点が、標的型攻撃メールの特徴に一致する。

リスト 35 被験者企業 L：第 2 回配信の擬似攻撃メール

From: (部長級人物の姓) <stats_mastor@(フリーメール B)>
Subject: 個人情報保護セミナー参加者の募集

各位

添付資料にあるように個人情報保護関連のセミナーを数社から協力をいただいて実施することとなりました。受講希望者は御相談ください。
以上宜しくお願い致します。

＃既に連絡を受けているようでしたら重複をお許しください。

(部長級人物の姓)

添付ファイル名:開催概要.doc

14.4. Webビーコンの集計結果

被験者企業 L について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 57 に示す。

表 57 被験者企業 L：Web ビーコン集計

	第 1 回	第 2 回
被験者数	124 名	124 名
Web ビーコンへのアクセス総数	24 回	2 回
開封したと考えられる人数	17 名(13.7%)	2 名(1.6%)
2 回とも開封した人	0 名(0.0%)	

被験者企業 L では、第 1 回配信での開封者数が 17 名(13.7%)であり、第 2 回配信では 2 名(1.6%)である。また、開封者の中には 2 回とも開封した被験者はおらず、今年度の予防接種で最も開封率の低い被験者企業のひとつである。

また、第 1 回配信の際に Web ビーコンのログ収集サーバへの偵察アクセスが観測されている。

なお、被験者数を考えると、被験者企業 L におけるアクセス総数は開封率と同様に非常に小さい。

14.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 L における擬似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業 L では、擬似攻撃メール配信の後の約 1 時間に添付ファイル開封のアクセスが集中している。

図 104 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 105 に示す。

図 104 被験者企業 L：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

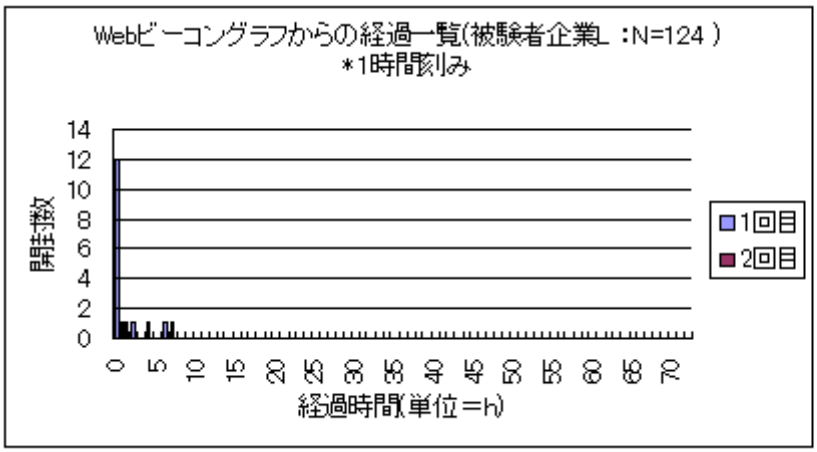
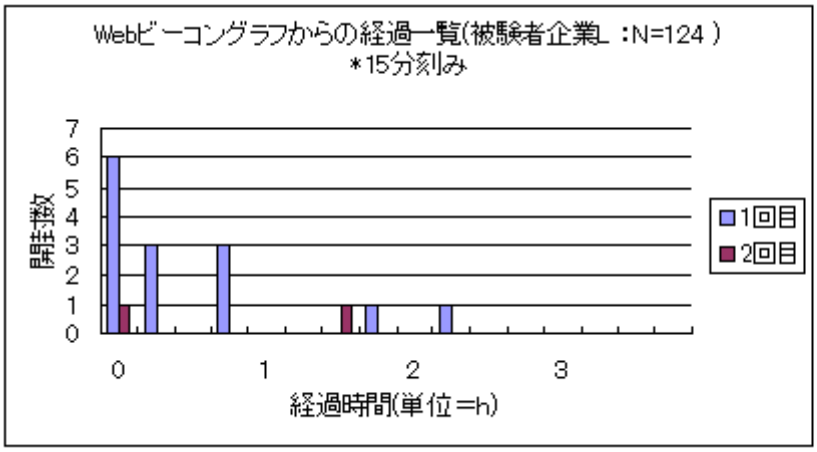


図 105 被験者企業 L：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



14.6. 予防接種実施時の特記事項

14.6.1. インシデントレスポンスの動き

被験者企業 L では、第 1 回配信の擬似攻撃メールを本物の標的型メール攻撃ではないかと疑って、社長への問い合わせや外部のインシデント報告先へ報告しようとするなどの動きが被験者の一部に見られた。

これは、標的型メール攻撃に対する反応としては極めて正しいものだが、予防接種としてはそうなる前に矛を収める必要がある。

そこで、窓口担当者の判断によって配信当日の 17:20(配信時刻から 4 時間 20 分後)に種明かしを行った。

また、窓口担当者の心遣いで第 1 回配信と条件を揃えるために、第 2 回配信でも同時刻に種明かしを行った。

14.6.2. 偵察アクセス

第 1 回配信時に、総アクセス回数 24 回のうちの 6 回の(25.0%)を占める偵察アクセスが見られた。第 2 回配信では偵察アクセスは見られなかった。

被験者企業 L の業種から見て当然優れた技術者を擁しているものと思われるが、偵察アクセスの質・量が意外に少なかった。

14.7. 被験者アンケートの集計

被験者アンケートへの回答から見た、被験者企業 L における添付ファイルの開封状況は表 58 の通りである。

表 58 被験者企業 L : 被験者アンケート回答者の開封状況

有効回答数	36 名	
	第 1 回	第 2 回
開封した人数	19 名(52.8%)	8 名(22.2%)
2 回とも開封した人	5 名(13.9%)	

被験者企業 L では、被験者数 124 名に対し 41 名(33.1%)から被験者アンケートに対する回答があった。このうち 5 名が 2 回とも擬似攻撃メールに気付かなかったと回答しているので、被験者アンケート有効回答数を 36 名とする。

有効回答者 36 名の中で、第 1 回配信での開封者は 19 名(52.8%)、第 2 回配信での開封者は 8 名(22.2%)である。また、一度でも開封した被験者は 22 名(61.1%)、両方を開封した被験者は 5 名(13.9%)であった。

前節で Web ビーコンから見た開封率について述べたが、本節の被験者アンケ

ートから見た開封率と比べると大きな違いがある。
すなわち、第 1 回配信での開封者は、Web ビーコンから見た 17 名(13.7%)に対して被験者アンケートでは 19 名(52.8%)と 4 倍近い割合を占めている。第 2 回配信での開封者でも同様で、2 名(1.6%)に対して 8 名(22.2%)と 10 倍以上の開きがある。
これは、被験者アンケートの設問にある「開封」という言葉を、添付ファイルの開封ではなく、メールソフトによるメール本文の表示と解釈した為であろう。被験者アンケートの設問や選択肢などを誤解の余地の少ないものにする必要があったと反省している。

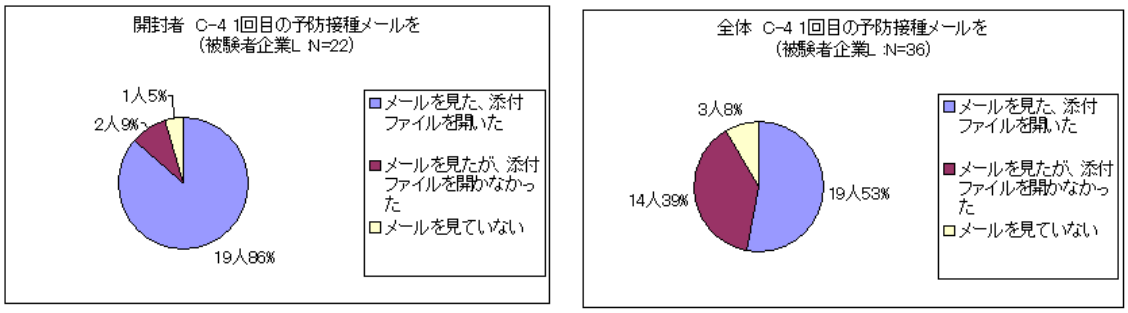
14.8. 被験者アンケートの分析

本節では、被験者企業 L の被験者アンケートに対する有効回答から、その特徴となる諸点を示す。

14.8.1. 添付ファイル開封の有無とその理由

被験者企業 L における被験者アンケートの設問 C-4 の回答結果を図 106 に示す。

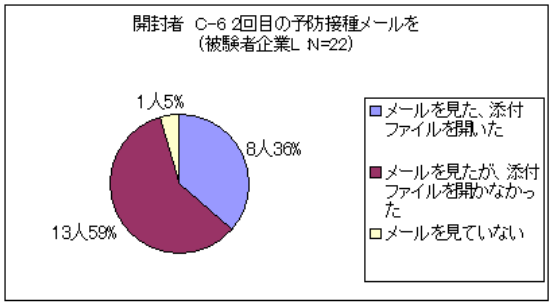
図 106 被験者企業 L：被験者アンケートから見た開封状況(第 1 回配信)

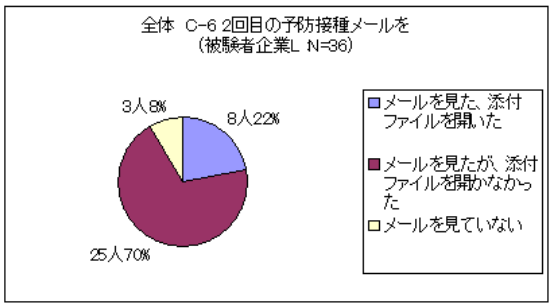


前述の通り、第 1 回配信では、有効回答者 36 名中の 19 名(52.8%)が添付ファイルを開封したと回答している。
被験者アンケートの設問 C-5 に対する回答からその理由を探すと、ほとんどの開封者が一瞥して社内連絡であるものと思い込んで開封していることがわかる。中でも、差出人の表示名が社長の姓であったことで、ほとんど自動的に開封している様子が多数見られた。

同様に、設問 C-6 に対する回答状況を図 107 に示す。

図 107 被験者企業 L：被験者アンケートから見た開封状況(第 2 回配信)





第 2 回配信では、有効回答者 36 名中の 8 名(22.2%)が添付ファイルを開封したと回答している。第 1 回配信と比較すると、開封者は減少している。

第 1 回配信での開封者で、第 2 回配信では添付ファイルを開封しなかった被験者が、どのような理由で添付ファイルを開かなかったのかを、被験者アンケートの設問 C-7 に対する回答から検討する。

すると、多くの当該被験者が、差出人の表示名やメールアドレスを仔細に確認していたり、メール本文の内容が本当に自分に関係あるのか否かを注意深く確認したりしていることがわかった。

これは、第 1 回配信とその後の周知・教育の効果があったということであろう。

いずれにしても、擬似攻撃メールの本文の内容が、配信当時の社内状況とよく一致しているために、開封に結びついたようだ。

この中には、全体としては社内状況に合致しているのに、些細な点が矛盾していると、確認のために開封したくなるという感想もある。人間心理の綾と言えるだろう。

設問 C-7 への回答からいくつか抜粋しておく。

1. そろそろ異動の季節だったから、社長のメール添付ファイルを見てしまった。
2. ちょうど事業計画の最中で必要かつ緊急に対応しなくてはいけないメールだと思ったため。
3. リーダ会などでも事業計画はホットな話題であった。内容がつじつまが合わない(全社定例後に送信されている)ことで、むしろ、何を意図しているのか中身を見て確認しようとしてしまった。
4. 何かがおかしいとは思いつつも、良く確認せず(考えず)に添付ファイルを開いていた。

他方で、開封しなかった被験者は気付きのポイントを的確に指摘している。

1. From がフリーアドレスドメインであったため。

2. 詐称された差出人が書いたにしては、内容が微妙に不自然だったため、From をみたら、フリーメールのアドレスだった。
3. (社長の姓)さんから、直接メールが来ると思いにくかった。また、アドレスが変であることに気づけた From アドレスが変だったため。

第 1 回配信と第 2 回配信の両方で添付ファイルを開封したと回答した被験者は 5 名(13.9%)であるが、その開封理由は、設問 C-7 への回答によれば以下の通りである。

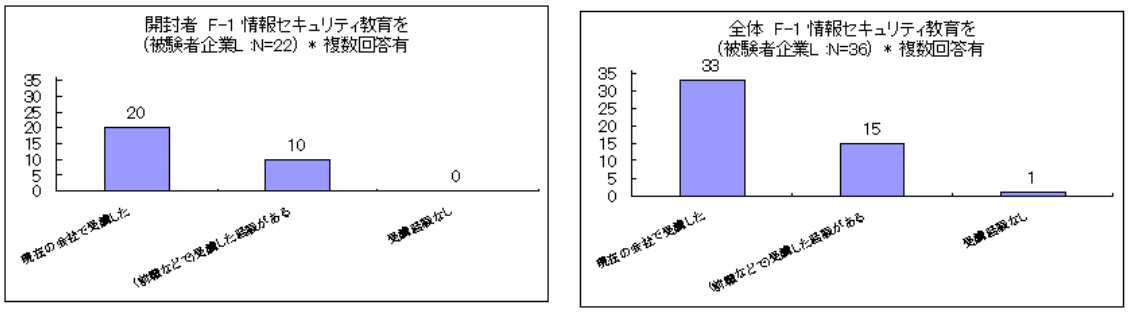
1. (擬似攻撃メールの)本文を読んで添付ファイルを開いてしまった。
2. 取締役メールに対する条件反射。
3. 内容が研修セミナーの企画だったにもかかわらず、私に何の相談・連絡がなかったため、思わず「どういうことだ！」との衝動が沸いて、とっさに開いてしまった。

14.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間にどのような関係が読み取れるかについて調べる。

被験者アンケートの設問 F-1 に対する回答状況を図 108 に示す。

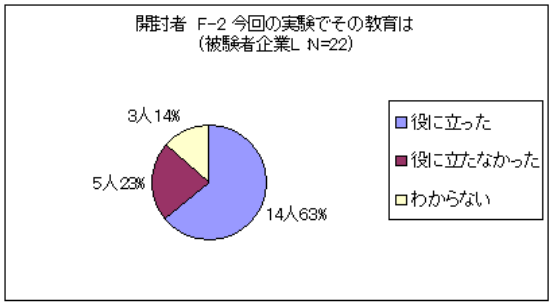
図 108 被験者企業 L：情報セキュリティ教育の経験

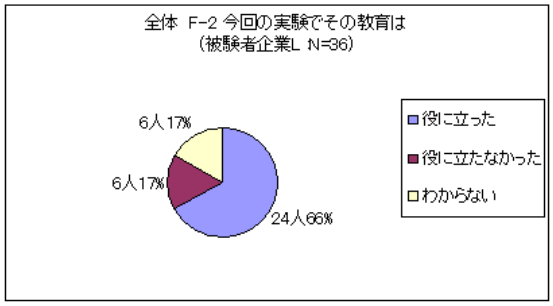


これによれば、被験者アンケート有効回答者 36 名中の 33 名(91.7%)は、現在の勤務先で情報セキュリティを受けたと回答している。

次に、設問 F-2 に対する回答状況を図 109 に示す。

図 109 被験者企業 L：情報セキュリティ教育の有効性





これによれば、有効回答者 36 名中の 24 名(66.7%)の被験者が、今回の予防接種で情報セキュリティ教育が役立ったと回答している。

また、開封者 22 名中の 14 名(63.6%)の被験者も、役に立ったと回答している。

なお、教育が役に立たなかったと回答した被験者 6 名のうちの 5 名は、添付ファイルを開封した被験者である。

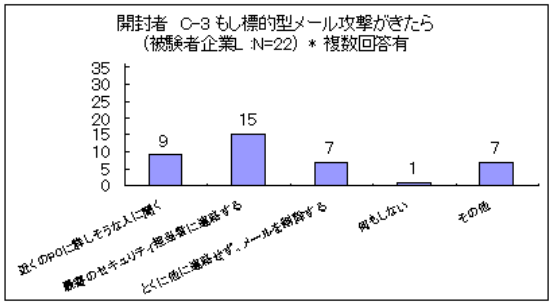
ここでも、知識を得る場所としての情報セキュリティ教育と、実際の(擬似)攻撃体験が別々に意識されていて、統一的な理解を得ていないようだ。

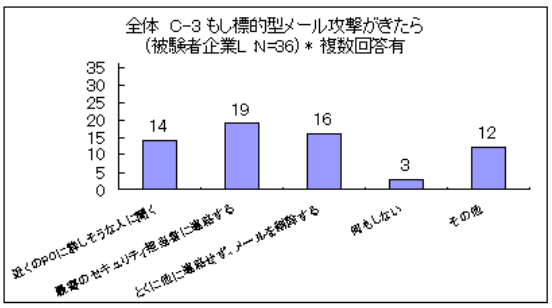
14.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのようになことが起きると思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答状況を図 110 に示す。

図 110 被験者企業 L：もし標的型メール攻撃が来たら





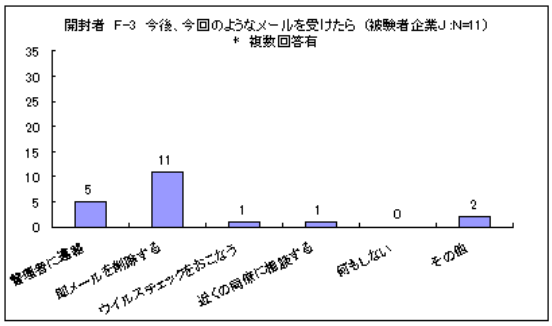
これによれば、標的型メール攻撃を受けた場合の対処方法として「最寄りのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 36 名中の 19 名(52.8%)であった。

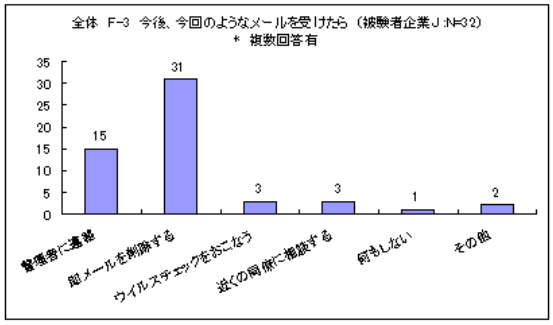
他方で、有効回答者 36 名中の 16 名(44.4%)は、「とくに他に連絡せずに削除する」と回答している。

ここでもインシデント報告をするという回答は約半数に留まり、半数弱の被験者が単に不審なメールを削除するという選択をしている。

図 111 に、被験者アンケートの設問 F-3 への回答状況を示す。設問 F-3 は、設問 C-3 とほぼ同じ内容を別の表現で聞き直している。

図 111 被験者企業 L：今後、今回のようなメールを受けたら





これによれば、標的型メールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者は、有効回答者 36 名中の 24 名(66.7%)となり、設問 C-3 での回答よりもその比率が上がっている。

逆に、「即メールを削除する」と回答している被験者は有効回答者 36 名中の 11 名(30.6%)と減少している。

この誘導では、不審なメールの証拠を保全して管理者に連絡することの重要性が認識される方向に向かっているようだ。

14.8.4. 危機管理意識の変化

ここでは、被験者アンケートの設問 F-4 に対する回答を用いて、被験者の危機管理意識が変化したか否かについて調べる。

有効回答者 36 名中の 17 名(47.2%)の被験者が、危機管理意識の変化や脅威の再認識をしたと回答しており、この訓練を肯定的に捉えている。

また、以下のような回答があり、予防接種による気付きがあったことがわかる。

1. メールの振り分けを見直した。フリーメールアドレスを振り分けるようにして、自身に気付き・警戒を促すようにした。
2. 日頃から、セキュリティ分野を専門としている人間であっても、不完全な部分があるということの自覚が出来たというのは大変、良かったと思います。

14.8.5. 感想

ここでは、被験者アンケートの設問 G(感想意見など。自由記述)に対する回答状況からメッセージを読み取ることを試みる。

有効回答者 36 名中の 15 名(41.7%)は、今回の予防接種訓練を肯定的にとらえて、予防接種の再実施提案や日頃から十分注意しようという回答をしている。
以下のような特徴的な感想があったので抜粋しておく。

1. 「今回の気付きポイント」もあまり効果がないように思える。振り込め詐欺と同じで、危険なものをルール化したとたん、それ以外のものを安心してしまうようになるのでだめだと思う。メールの閲覧、添付ファイルの処理を自分の中で根本的に見直さないと防げないと感じた。
2. あくまでも感想ですが、実際には今回ほど巧妙なものは外部の第三者ではなかなか作れないのではと思いました。というのも、(被験者企業Lの社名略称)の中にいれば、「(社長の姓)さん＝事業計画」「(部長級の実在人物の姓)さん＝個人情報」とピタッとひもづくので、アドレスをよく見ずに本人だと思ってしまいかねません。ただ、ここまでピタッとしたひもづきを外部の第三者が知りうるのかが、やや疑問です。一方で、二人とも役員だし、(被験者企業 Lの社名略称)の社外公開ホームページをはじめとしてある程度の情報は外部に公開されているので、そこから類推して作れなくもないのかなとも思います。
3. イノキュレーションという仕組みについて概念は理解していましたが、実地で状況を見れたのは初めてでした。Security Culture という位置づけで考えると、研修だったり E ラーニングでも身につかないことが、こういった体験を元にして活かしていけるというのは すばらしい取り組みだと思います。巧妙に内部文書をコピーしたタイプの訓練をやられると、かなりの組織で引っかかりそうな気がします。
4. セキュリティに対して強い意識を持っているつもりでも、簡単にトラップにかかってしまうものだと感じました。
5. 怪しいメールは開くわけがないと考えていたが、今回の件のように個人名等に社内の人物が書かれているだけで、警戒心が薄れることがよくわかった。その点に気づけただけでも意味のある訓練だったと思う。

14.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 L について、被験者企業アンケートと被験者企業インタビューからの分析を以下に記す。

まず、被験者企業 L の情報セキュリティ体制は、相当程度に整っていることがわかる。

1. プライバシーマークと ISO27001 を取得している。
2. 情報セキュリティの管理体制はほぼ整備されており、インシデントの連絡体制(窓口)も定められている。
3. 定期的な情報セキュリティ教育を実施している。
4. サーバや通信ログを監視し定期的に報告している。

次に、被験者企業 L では、個々の PC 環境から外部の Web サイトへのアクセスを動的に制限している。擬似攻撃メールの添付ファイルを開封してしまった場合でも、このアクセス制限機構によって Web ビーコンのアクセスが抑止されたケースがある。

このアクセス制限機構は非常に高度かつ柔軟なもので、今年度の被験者企業の中では類例を見ない。

次に、被験者企業インタビューの際に、窓口担当者から以下の意見・感想を得た。

1. 今回の予防接種で、とくに苦情や問題にならなかったので、方法論としてはこれでよいと思う。
2. 時間がたてば人も入れ替わるし、免疫効果も薄れるので、繰り返し実施する必要がある。
3. 繰り返し実施する場合は、徐々に気付きのポイントを減らすか、攻撃手法を多様化する必要がある。
4. メールへファイルを添付する習慣を根絶すべきではないか。常時添付ファイルが入ってくるような状況ならば個々のケースを気にしていられないが、たまに入ってくるならば注意が届きやすくなる。
5. S/MIME や PGP の利用は相手次第で有効であるが、通常は顧客が対応できないため利用は困難である。

14.10. 考察

被験者企業 L は情報セキュリティの専門会社であるから、日頃から情報セキュリティに対する意識が高い。そのためか、非開封者にとっては、この程度の擬似攻撃メールでは明らかに不審で、もっと凝ったものでないと訓練としても効果がないと回答する傾向にある。

それでも、社内の実在人物の姓が表示名やメール本文に記述されているだけで、容易に信じて疑わないものだということを身をもって体験したと自由記述欄に答えている被験者は少なくない。

したがって、被験者企業 L の被験者のような専門家であっても、標的型メー

ル攻撃の被害を受けることがないとは言い切れないのであって、予防接種としては、徒に見破られない擬似攻撃メールを目指す必要はないと考える。

予防接種の学習効果としては、当然ながら、標的型メール攻撃をそれと見抜く眼力を養うことを目的としているが、二次的には万一の事故の際にどのような対処方法を取るべきかを徹底することであろう。

被験者企業 L では、一部の被験者に上司や社内外のインシデント報告窓口に対する報告をしようという動きがあったとのことであるが、この点でも被験者企業 L は今年度の被験者企業の中で抜群の水準にあると言える。

また、このようなインシデント報告機構がどの程度作動するのかを実地に観測できることは、予防接種の副次的な効果のひとつである。

15. 被験者企業M

15.1. 被験者企業Mの概要

被験者企業 M は、エネルギー関連の基礎技術から応用技術までを研究開発する公益法人である。被験者企業 M は、重要インフラ系の組織でもある。

被験者企業 M の概要を表 59 に示す。

表 59 被験者企業 M：概要

業種	公益法人
設立	(非公開)
資本金	N/A
本社所在地	東京
拠点数	6 箇所
社員数	約 800 名
認証	なし

15.2. 被験者企業Mにおける予防接種の概要

表 60 に示す日程と規模で、被験者企業 M に対する予防接種を実施した。

なお、今回の予防接種では 221 名を被験者として実施した。被験者の中には、派遣社員や業務委託社員なども含んでいる。

表 60 被験者企業 M：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/1/30 11:00	2009/2/13 11:00
種明かし	2009/2/3 15:54	2009/2/17 15:56
被験者数	214 名	221 名

被験者企業 M は、およそ 2 年に 1 度程度の頻度でセキュリティ教育を受けている。

被験者企業 M では、今回の予防接種実施に際して、各部門の長に予防接種を実施することを予告したが、被験者に対しては予告していない。

また、第 1 回配信の後、第 2 回配信までの間に、予防接種を実施したことの事後通知・標的型メール攻撃の概要説明・標的型メール攻撃についての注意喚起の 3 点について、連絡担当者から被験者へ周知したとのことである。

15.3. 擬似攻撃メールの内容

15.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 M における第 1 回配信の擬似攻撃メールをリスト 36 に示す。

この擬似攻撃メールは、リスト 2 のサンプルの(12)を参考にして作成した。

この擬似攻撃メールは、「システム担当」からシステムのアップデートを促す態を装うものである。「添付の資料を参照の上、お早めに」と言う記述で、添付ファイルの開封を促す誘導もしている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「システム担当」とした。この組織名は被験者企業 M では普通使用しない名称である。
2. 差出人のメールアドレスを stats_mastor@(フリーメール B)とした。これは明らかにフリーメールアドレスである。
3. 本文に「システムアップデート」と記載しているが、具体的にどのシステムが対象なのかを記載していない等、具体性に欠ける。
4. 他には、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 36 被験者企業 M：第 1 回配信の擬似攻撃メール

```
From: システム担当 < stats_mastor@(フリーメール B)>
Subject: システムアップデートについてのお願い

利用者各位

                                        システム担当

別途お知らせの通り、添付の資料を参照の上、お早めにシステム
アップデートを実施してください。
新しいプログラムのインストールによりコンピュータの状態が安定し、
システム利用時のパフォーマンスが向上します。

添付ファイル名:update.doc
```

15.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 M における第 2 回配信の擬似攻撃メールをリスト 37 に示す。

この擬似攻撃メールは、実在する「厚生労働省の新型インフルエンザ対策行動計画」を参照しつつ、虚構の社内行動計画を作成したので確認しておくよう

にという社内周知を装うものである。「生命に関わる」などの文言で添付ファイルの開封を促している。

また、文中には触れていないが、被験者企業 M の総務部が新型インフルエンザ対策に関するパンフレットを配布したのは事実である。

また、偶然ではあるが、被験者企業 M には、差出人のメールアドレスにある”motok”から連想される人物が実在していたが、インフルエンザに関する周知を行う立場にはなかったとのことである。

したがって、第 2 回配信の擬似攻撃メールは、期せずして判別が非常に難しいものとなっている。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を「総務担当」とした。この組織名は曖昧さを残している。
2. 差出人のメールアドレスを motok2501@(フリーメール A)とした。これは明らかにフリーメールアドレスである。
3. 差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 37 被験者企業 M：第 2 回配信の擬似攻撃メール

```
From: 総務担当 <motok2501@(フリーメール A)>
Subject: 新型インフルエンザ行動計画(案)について

新型インフルエンザ対策について、国民の健康被害を最小限にとどめ、
社会・経済機能の破綻を来すことのないよう、「新型インフルエンザ
対策行動計画」が、11 月 14 日、厚生労働省を中心に取りまとめられ、
同日の関係省庁対策会議において了承されました。

それを受け、当社でも新型インフルエンザの発症が国内で確認された
場合の行動計画の素案を添付資料の通り作成しました。

皆様の生命にも関わることですので、業務実態と照らし合わせて、
いざという時に計画に沿った行動が取れるかどうか必ずご確認頂き
ますようお願いいたします。

---
総務担当

添付ファイル名:新型インフルエンザ行動計画(案).doc
```

15.4. Webビーコンの集計結果

被験者企業 M について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 61 に示す。

表 61 被験者企業 M：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2009/1/30　11:00	2009/2/13　11:00
種明かし	2009/2/3　15:54	2009/2/17　15:56
被験者数	214 名	221 名
Web ビーコンへのアクセス総数	97 回	62 回
開封したと考えられる人数	85 名(39.7%)	56 名(25.3%)
2 回とも開封した人	27 名(12.2%)	

被験者企業 M では、第 1 回配信での開封者が 85 名(39.7%)であり、第 2 回配信では 56 名(25.3%)である。第 1 回配信から第 2 回配信へと若干の改善が見られる。

また、2 回とも開封した被験者は、27 名(12.2%)である。

第 1 回配信の開封者の中で、2 回とも開封した被験者の割合は 31.8%で、この比率は今年度の予防接種の中で一番大きいものとなった。

これは、第 2 回配信で用いた擬似攻撃メールが、偶然が重なって非常に識別困難なものとなった為であろう。

15.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 M における擬似攻撃メールの添付ファイル開封状況は以下の通りである。

被験者企業 M においても、擬似攻撃メールの配信後、約 1 時間でほとんどの開封者が添付ファイルを開封する傾向が見られる。しかし、この傾向は他の被験者企業よりも弱く、その後もしばらくの間は若干の開封が見られる。

図 112 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 113 に示す。

図 112 被験者企業 M：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

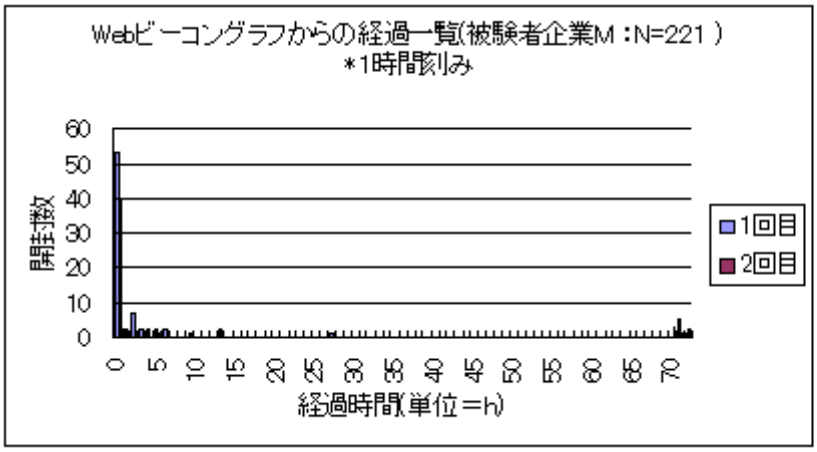
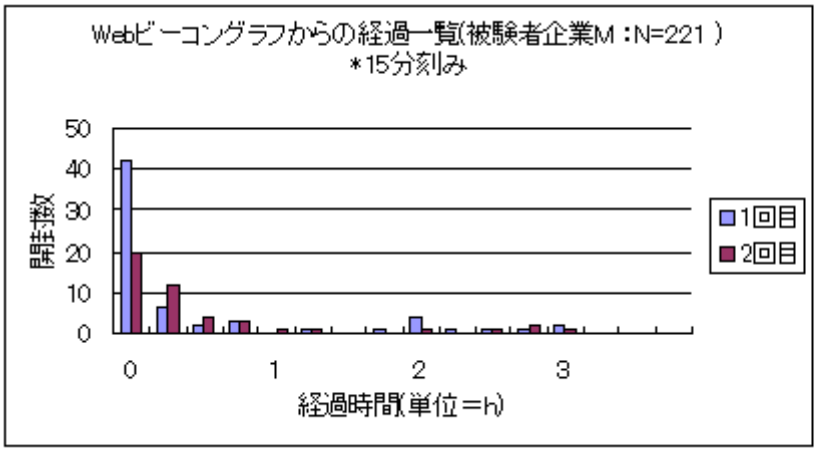


図 113 被験者企業 M：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



15.6. 予防接種実施時の特記事項

15.6.1. 被験者数の変動

被験者企業 M では、第 1 回配信時と第 2 回配信時で被験者数が異なる。

通常、各配信の予行演習では被験者を宛先としない運用であったが、被験者企業 M では、第 2 回配信の被験者に、第 1 回配信の予行演習の宛先とした者の一部を含めたためである。

この結果、第 1 回配信では被験者数は 214 名であり、第 2 回配信では 221 名となった。

各種の集計や比率計算においては、第 1 回配信に限っては母数として 214 名を採用し、その他の場合は 221 名を採用することにした。

15.6.2. 添付ファイルの誤添付

被験者企業 M では、窓口担当者の努力により、擬似攻撃メールの添付ファイルには、当該擬似攻撃メールの気付きのポイントを列挙した。したがって、擬似攻撃メール本文と添付ファイルには対応関係ができていた。

一方、擬似攻撃メールの配信順序を取り違えていることが、第 1 回配信の直前になって発覚したので、急ぎ入れ換え作業を行う事となった。

しかるに、擬似攻撃メールの本文・表題・添付ファイル名などについては正しく入れ換えたにも関わらず、添付ファイルの実体を入れ換えなかったために、第 1 回配信の擬似攻撃メール本文と添付ファイルの対応関係が崩れる結果となった。

また、この時に用いた添付ファイルが第 2 回配信用に準備したものであったため、第 2 回配信の差異の気付きのポイントを周知する結果となった。これでは、第 2 回配信の開封状況が良い方に振れる恐れが強いので、第 2 回配信の擬似攻撃メールの文面を再作成することとなった。

さらに、再作成した文面が、さまざまな偶然によって、非常に識別困難なものとなったのは前述の通りである。

15.7. 被験者アンケートの集計

被験者アンケートへの回答から見た、被験者企業 M における添付ファイルの開封状況を表 62 に示す。

表 62 被験者企業 M：被験者アンケート回答者の開封状況

有効回答数	82 名	
	第 1 回	第 2 回
開封した人	34 名(41.5%)	22 名(26.8%)
2 回とも開封した人	13 名(15.9%)	

被験者数 221 名に対し、86 名(38.9%)から被験者アンケートに対する回答があったが、このうちの 4 名が擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答数を 82 名(37.1%)とする。

有効回答数 82 名の中で、第 1 回配信で擬似攻撃メールの添付ファイルを開封した被験者は 34 名(41.5%)であり、第 2 回配信での開封者は 22 名(26.8%)である。また、両方を開封した被験者は、13 名(15.9%)であり、一度でも添付ファイルを開封した被験者は、43 名(52.4%)である。

前節では Web ビーコンから開封率を見たが、本節の方がやや高い開封率を示している。しかし、両者の傾向は非常によく似ている。

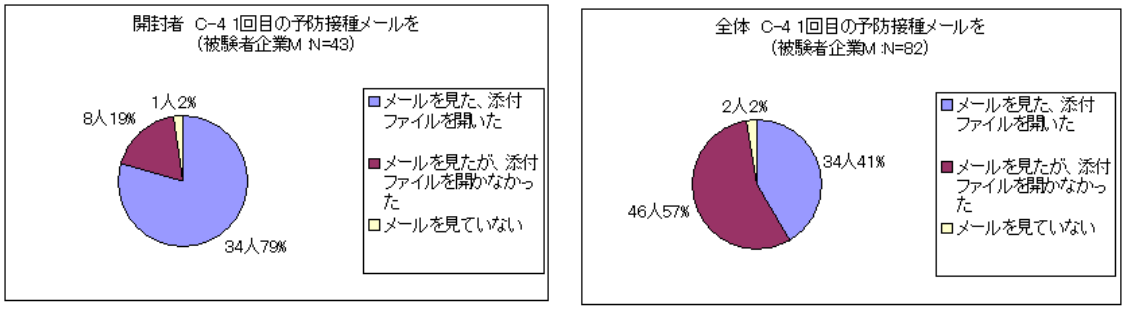
15.8. 被験者アンケートの分析

本節では、被験者企業 M の被験者アンケートへの回答内容から、その特徴となる諸点を示す。

15.8.1. 添付ファイル開封の有無とその理由

被験者企業 M における被験者アンケートの設問 C-4 に対する回答結果を図 114 に示す。

図 114 被験者企業 M：被験者アンケートから見た開封状況(第 1 回配信)



前述の通り、被験者企業 M の第 1 回配信では、有効回答者 82 名の中の 34 名(41.5%)の被験者が添付ファイルを開封したと回答している。その理由を被験者アンケートの設問 C-5 から探すと、以下のようなものが挙げられている。

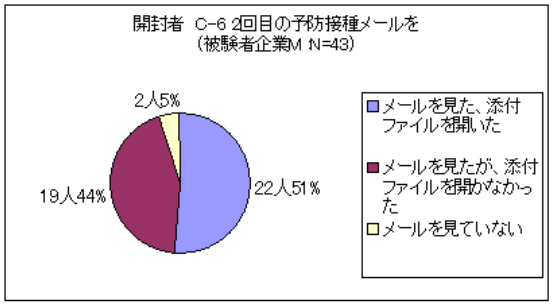
1. ディスプレイ交換のお知らせが来た直後であり、関連するものと思った。
2. システムアップという言葉は、PC を熟知してない者にとって脅迫観念に捕らわれ反射的にメールを開いてしまう。
3. (システム側の)メールフィルタに引っかからなかったため、警戒していなかった。

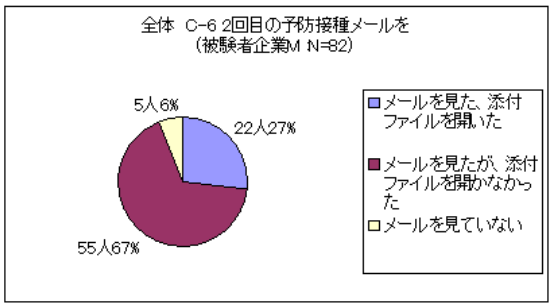
ここでも、被験者自らの置かれた状況に合致していたための無警戒・よくわからない内容を確認するため・既存のスパム対策などへの過信など、他の被験者企業と共通する理由が挙げられている。

なお、第 1 回配信の開封者のうち 5 名は、ウィルスチェックをしたり、Linux のシステムに移して開封したり、予防接種のメールが配信された話を聞いて好奇心から開封したりなど、ある程度見抜いた上で開封している。
このような開封者をどのように扱うべきかは議論のあるところだが、ここでは被験者アンケートへの回答をそのまま採用している。

図 115 に、被験者アンケートの設問 C-6 への回答状況を示す。

図 115 被験者企業 M：被験者アンケートから見た開封状況(第 2 回配信)





前述の通り、第 2 回配信では有効回答者 82 名中の 22 名(26.8%)の被験者が、添付ファイルを開封している。また、この第 2 回配信での開封者 22 名の中の 13 名(59.1%)が 2 回とも開封している。

他の被験者企業と比較して、被験者企業 M における第 2 回配信の開封率は高い部類に入る。

その理由を設問 C-7 への回答から探ると、やはり、第 2 回配信で用いた擬似攻撃メールの文面が偶然社内事情に合致していて識別困難であったようだ。

これは、逆に、巧妙に仕掛けられた標的型メール攻撃が危険であることを示す結果でもある。

以下に、設問 C-7 への回答から特徴的なものを抜粋しておく。

1. インフルエンザのパンデミックについて、所内で注意を呼びかける資料等が最近、配布された。今回、宛名が、私の姓が漢字となっていたこともあり、インフルエンザ関連の周知事項と思い、メール送信者、本文内容を十分確認しないまま不用意に開けた。
2. たまたま、幹部職会議で話題になり、席に戻ったらこのメールが来ており、躊躇なく開いてしまった。このメールは時機を得ており、なんら疑いもなく開いた。まさか２度目の架空メールはないと内心思っており、油断してしまった。１度目不注意、２度目油断、３度目自己責任になりますか。
3. 最近、インフルエンザの対策マニュアルを配布された後だったので、何も疑わなかった。
4. 周りで先に受信した人が怪しいメールがまた来たよ，これも前回と同じテストに違いない，と言っているのを聞いていたにもかかわらず，ちょうど多忙で複数の業務を平行して行っており，かつ，しばらく前にインフルエンザに関する冊子が配布されていたので，当所の総務からと勝手に勘違いして開いてしまった。
5. 総務から新型インフルエンザのリーフレットが配られていて、いかにもその続きのお知らせという感じがしたのでだまされた。発

信者のアドレス motok が所内の実在の人物を思わせ、つい信用してしまった。

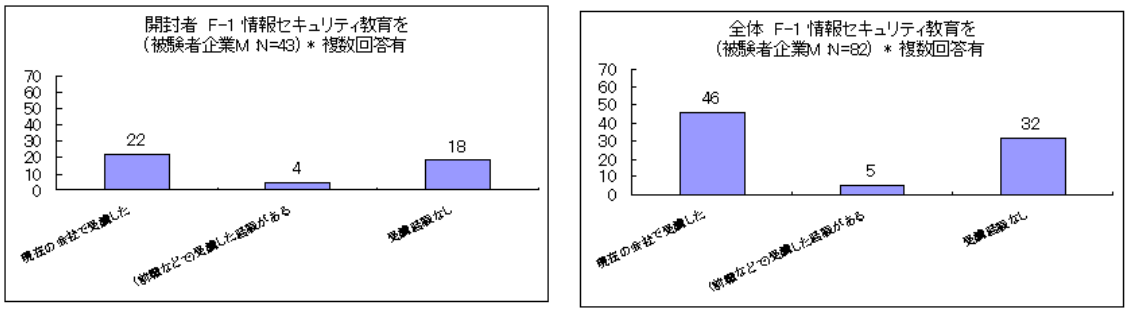
第 1 回配信での開封者のうち、第 2 回配信の添付ファイルを開かなかった被験者が、どういう理由で添付ファイルを開かなかったのかを設問 C-7 の回答から拾うと、その多くは、第 1 回配信の体験から注意をするようになったことや、その結果、差出人のメールアドレスがフリーメールアドレスであることに気付いたとのことである。

15.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

被験者アンケートの設問 F-1 に対する回答状況を図 116 に示す。

図 116 被験者企業 M：情報セキュリティ教育の経験

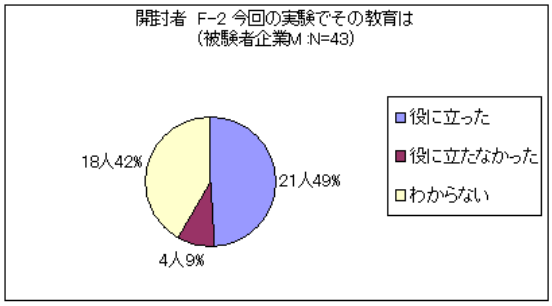


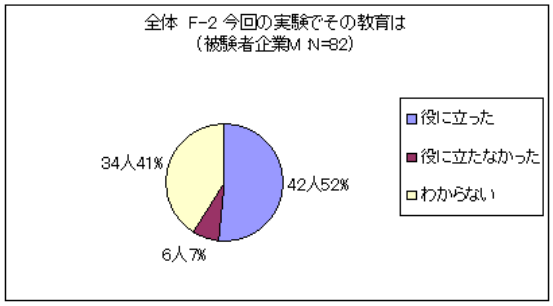
これによれば、被験者アンケートの有効回答者 82 名中の 46 名(56.1%)が、現在の勤務先で情報セキュリティ教育を受けている。一方、受講経験なしと回答した被験者が 32 名(39.0%)で、高い割合を占めている。少なくとも被験者の認知度の点から見ると、情報セキュリティ教育があったことさえ記憶に残っていない場合が多いということであり、組織としての情報セキュリティ教育体制が徹底されていないのではないかと思われる。

なお、開封者 43 名の中の 22 名(51.2%)が、現在の勤務先で情報セキュリティ教育を受けたと回答している。他の被験者企業のケースと同様に、情報セキュリティ教育の受講経験と実際の体験との関係が希薄で、情報セキュリティ教育で学んだ内容を、自らの実際の体験に活かすことができていないようである。

図 117 に被験者アンケートの設問 F-2 に対する回答状況を示す。

図 117 被験者企業 M：情報セキュリティ教育の有効性





これによれば、会社で受けた情報セキュリティ教育が、予防接種に対して役に立ったと回答した被験者は、有効回答者 82 名中の 42 名(51.2%)であるが、開封者 43 名の中でも 21 名(48.8%)を占めている。

教育が役に立ったけれども添付ファイルを開いてしまったというのは、相矛盾していて解釈が難しいところである。

被験者アンケートの設問 F-4(危機管理意識の変化)や設問 G(感想)への回答を見ると、予防接種を体験することによって、日頃のセキュリティ意識の欠如に気付き、その重要性を再認識したと受け取れる感想が多い。

2 回とも開封したことにより、さらなる注意が必要なことを再認識した被験者もいた。

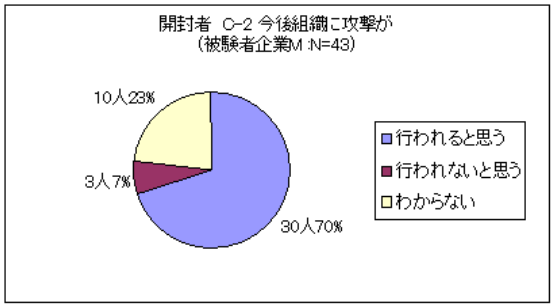
また、既存のスパム対策フィルタをすり抜けるメールがあることを知ったという被験者もおり、予防接種のような体験型の訓練によって、知識として理解していた(またはそのつもりになっていた)セキュリティ教育の内容を体得したと言えるだろう。

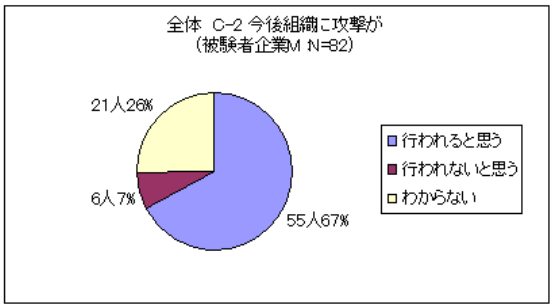
15.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本物の攻撃があった場合にどのような反応を示すと思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答を図 118 に示す。

図 118 被験者企業 M：今後組織に攻撃があると思うか



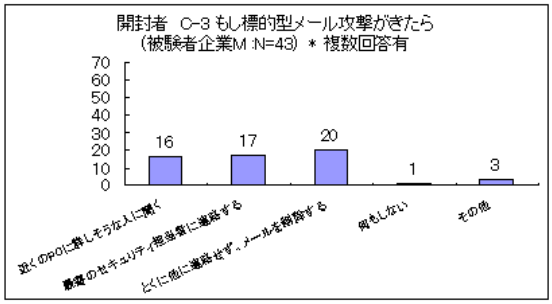


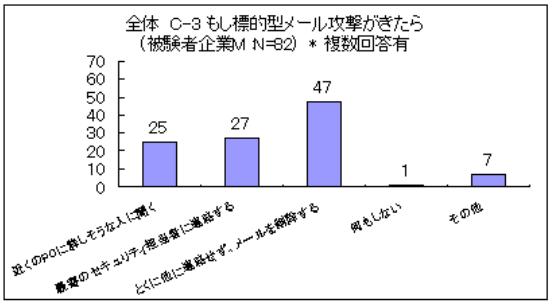
これによれば、有効回答者 82 名の中の 55 名(67.1%)の被験者が、今後組織に標的型メール攻撃が行われるかもしれないと回答している。

これは、被験者企業 M が重要インフラ系の組織であるため、日頃の危機意識が高いことをあらわしているものと思われる。また、予防接種によって擬似的な標的型メール攻撃を受けて、改めて脅威を認識したということであろう。

図 119 に、被験者アンケートの設問 C-3 に対する回答状況を示す。

図 119 被験者企業 M：もし標的型メール攻撃が来たら



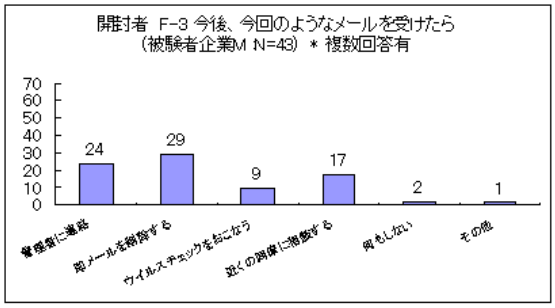


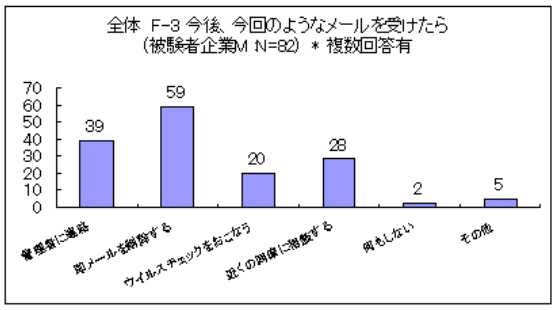
これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 82 名中の 25 名(30.5%)であり、「とくに他に連絡せず削除する」と回答した被験者は同じく 47 名(57.3%)である。

他の被験者企業でもほぼ同様であるが、これは、被験者企業 M においてインシデント報告の体制がまだ確立されていないと言える。

図 120 に、被験者アンケートの設問 F-3 に対する回答状況を示す。設問 F-3 は、設問 C-3 とほぼ同じ内容について文言を変えて再び質問している。

図 120 被験者企業 M：今後、今回のようなメールを受けたら





これによれば、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者は、有効回答者 82 名中の 39 名(47.6%)となり、先の設問 C-3 の場合に比べて 17.1%多い結果となった。

しかし、「即メールを削除する」と回答した被験者は、有効回答者 82 名中の 59 名(72.0%)と、こちらも 14.7%増えている。

理想的には、不審に思ったメールについては証拠保全し、管理者に連絡することが望ましいが、被験者企業 M では、他の被験者企業と同様に、そこまでの体制は構築されていないようである。

15.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4 では、危機管理意識の変化を尋ねた。

有効回答者 82 名中の 52 名(63.4%)の被験者が、今回の訓練を通して危機管理意識の変化や危険の再認識をしており、この訓練を肯定的に捉えている。

以下のような危機管理意識の変化を示す回答があったので、ここに抜粋しておく。

1. 2 回も開いてしまって、危機意識の薄さに気がついた。今後の対策に十分役に立った。
2. アドレスに注意することを覚えました。
3. 自分が対象となるとは思っていなかった。よい体験になった。
4. 特に変化なし。意識が高くてもかかるときはかかる。最悪のシナリオを想定しておくことが肝要。

15.8.5. 感想

被験者アンケートの設問 G では、全体的な感想を尋ねている。

これに対する回答内容には、今回の予防接種訓練から教訓を得た様子を示す回答が多かったので、以下に特徴的な回答を掲げる。

1. 1 回目は何も考えないで添付ファイルを開いてしまいましたが、2 回目は怪しいと思いながらも添付ファイルを開けてしまいました。

2. メールが来たら早く確認しなくてはいけないと思っていましたが、添付ファイル付きなどのメールは特に気をつけて対応したいと思います。
3. まだ自分には訓練が足りない。たぶんまた開く可能性大。そもそも会社のメールは、万全のフィルターにかけられてメールを受信していると信じているから。そこまで気を使っていたら、仕事ができない。
4. 振り込め詐欺にだまされる心理がわかった。

15.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 M について、被験者企業アンケートと被験者企業インタビューから以下のことがわかる。

被験者企業 M は、認証取得が目的となっては本末転倒なのでセキュリティ対策は進めるが認証取得はしない、という姿勢で情報セキュリティに取り組んでいる。

この姿勢を守って認証取得はしていないが、情報セキュリティポリシーを制定しており、その改定も期限を定めて定期的に実施している。

しかし、情報セキュリティ専門の部署はなく、CSO も任命していない。

また、情報セキュリティ教育は、2 年に 1 度程度の頻度で不定期に実施しているが、これは一般的な頻度(3 ヶ月毎から 6 ヶ月毎)よりも間隔が長い。

情報セキュリティ教育の受講者のリテラシーのレベルが様々なので、E-learning や集合研修のような画一的なやり方で適切な教育効果を上げることができるのか否かにやや疑問を感じている、とのことである。

特に、「やらされている」と感じる受講者や、研修内容と実際の体験との関係が希薄であると感じる受講者が多いのではないかと思われ、結果として情報セキュリティ教育の内容が受講者の身に付かないのではないか、という感想も頂いた。

この意味で、今回の予防接種のような実践的な教育方法は、これまで取り組んだことのないものであり、今までの教育方法のギャップを埋めるために良かったのではないかとの事であった。

窓口担当者の感想としては、今回の予防接種での擬似攻撃メール程度のものでも、多くの人が添付ファイルの開封にまで誘導されたことに驚きを覚えているとのことである。

普段から、セキュリティに関するアナウンス等の啓蒙活動は行っているが、実際に職員にどの程度のリスクがあるかが見えていなかった。したがって、

予防接種を実施することでリスクを顕在化できたことは非常に意味があったとのことである。

なお、予防接種への要望として、MS-WORD 以外の添付ファイル形式(例えば、PDF や MS-Excel)でも実施できるとなお良いのではないかとのご意見を頂いた。

15.10. 考察

被験者企業 M では、一般企業に比べて情報セキュリティへの取り組みの緊迫感があまり感じられなかった。

これは、組織形態の特性上、内部統制・委託先管理・個人情報管理などの必要性を強く要求される場面が少ない為であろうか。

しかし、重要インフラ関連の研究を行っているのであるから、情報セキュリティ防護体制を構築する必要があるのではないかと思われる。

実際に、被験者企業 M は、今年度の予防接種の中では、開封率が比較的高いうちの一つである。これは、用意した擬似攻撃メールの文面が、偶然に被験者企業の M の状況に合致したことも原因であると思うが、重要インフラ系企業としては万全を期す必要があるのではないかと思う。

また、被験者企業 M では、認証取得という手段が目的化するのを嫌って、ポリシーとしてセキュリティ関連の認証取得をしない由である。しかし、ISO27001 の認証を取得することで、情報セキュリティ教育の頻度の問題を改善することができるのではないかと思われる。

16. 被験者企業N

16.1. 被験者企業Nの概要

被験者企業 N は、インターネット証券会社であり、設立から 3 年余りの若い企業である。

表 63 に、被験者企業 N の概要を示す。

表 63 被験者企業 N：概要

業種	金融業
設立	2005 年
資本金	約 25 億円(2009 年 1 月現在)
本社所在地	東京
拠点数	1 箇所
社員数	約 100 名
認証	なし

16.2. 被験者企業Nにおける予防接種の概要

表 64 に示す日程と規模で、被験者企業 N に対する予防接種を実施した。

表 64 被験者企業 N：予防接種の実施日時と被験者数

	第 1 回	第 2 回
配信日時	2009/2/5 15:30	2009/2/19 15:30
種明かし	2009/2/5 16:30	2009/2/23 11:00
被験者数	103 名	103 名

被験者企業 N における予防接種では、ほぼ全社員が被験者となっている。

被験者企業 N は会社設立から日が浅く、まだ情報セキュリティポリシーを持っていない。したがって、社員に対する定期的な情報セキュリティ教育も行われていない。

なお、今回の予防接種に際して、第 1 回配信の前には、予防接種が行われることを特に周知していない。
第 1 回配信の後、第 2 回の予防接種が行われることは周知している。
また、第 2 回配信後に種明かしを行った。

16.3. 擬似攻撃メールの内容

16.3.1. 第 1 回配信の擬似攻撃メール

被験者企業 N における第 1 回配信で用いた擬似攻撃メールをリスト 38 に示す。

この擬似攻撃メールでは、被験者企業 N の社長の姓名を騙って大入り袋と称する一時金を配布する態を装って、添付ファイルの開封へ誘導している。
また、メーリングリストに送られたメールを装った表題を設定した。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を被験者企業 N の社長の姓名とした。
2. 差出人のメールアドレスを motok2501@(フリーメール C)とした。これは明らかにフリーメールのアドレスである。
3. 他には、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 38 被験者企業 N：第 1 回配信の擬似攻撃メール

```
From: (社長の姓名) < motok2501@(フリーメール C)>
Subject: [int-all: 427] 大入袋を支給します。

お疲れ様です、(社長の姓)です。

9 月から今月までの収益が予想以上に伸びていることと、12 月の営業収支が
大幅に予想を上回ったため、皆様に感謝の意を込めて大入袋をお渡ししたい
と思います。

金額は添付ファイルを見てください。

(社長の姓)

添付ファイル名:大入り袋の支給額について.doc
```

16.3.2. 第 2 回配信の擬似攻撃メール

被験者企業 N における第 2 回配信で用いた擬似攻撃メールをリスト 39 に示す。

この擬似攻撃メールでは、社長の姓名を騙ってストックオプション付与に関する案内を行う態を装って、添付ファイルの開封へ誘導した。

この擬似攻撃メールには、以下のような気付きのポイントが含まれている。

1. 差出人の表示名を被験者企業 N の社長の姓名とした。
2. 差出人のメールアドレスは takasmaster@(フリーメール C)とした。これは明らかにフリーメールのアドレスである。
3. 他には、差出人の所属・氏名・連絡先を記した署名(フッタ)が無い点が、標的型攻撃メールの特徴に一致する。

リスト 39 被験者企業 N：第 2 回配信の擬似攻撃メール

From: (社長の姓名) <takasmaster@(フリーメール C)>
Subject: ストックオプションのお知らせ

お疲れ様です、(社長の姓)です。

先日の取締役会におきまして、3 月 31 日付で在籍している社員に対し、
ストックオプションを付与することとなりました。

在籍期間、職種により割当数量を確定いたしましたのでご連絡いたします。

詳細は添付の「ストックオプション.doc」をご覧ください。

(社長の姓)

添付ファイル名:ストックオプション.doc

16.4. Webビーコンの集計結果

被験者企業 N について、Web ビーコンのアクセスログから見た添付ファイルの開封状況を表 65 に示す。

表 65 被験者企業 N：Web ビーコン集計

	第 1 回	第 2 回
配信日時	2009/2/5 15:30	2009/2/19 15:30
種明かし	2009/2/5 16:30	2009/2/23 11:00
被験者数	103 名	103 名
Web ビーコンへのアクセス総数	112 回	18 回
開封したと考えられる人数	62 名(60.2%)	16 名(15.5%)
2 回とも開封した人	14 名(13.6%)	

被験者企業 N では、被験者数 103 名に対して、第 1 回配信では 62 名(60.2%)の被験者が添付ファイルを開封しており、第 2 回配信では 16 名(15.5%)が開封している。また、両方を開封した被験者は 14 名(13.6%)である。

第 1 回配信時の開封率は比較的高いが、第 2 回配信で大きく改善している。

16.5. Webビーコンログからの時系列開封状況

Web ビーコンのアクセスログから時系列で見ると、被験者企業 N における擬似攻撃メールの添付ファイル開封状況は、以下の通りである。

被験者企業 N では、擬似攻撃メール配信の後、約 1 時間でほとんどの開封者が添付ファイルを開封している。

図 121 に、擬似攻撃メール配信後の 3 日分の開封数を、1 時間刻みのヒストグラムとして示す。また、同様に 15 分刻みの 4 時間分のヒストグラムを図 122 に示す。

図 121 被験者企業 N：Web ビーコンの時系列開封状況(1 時間刻み 3 日分)

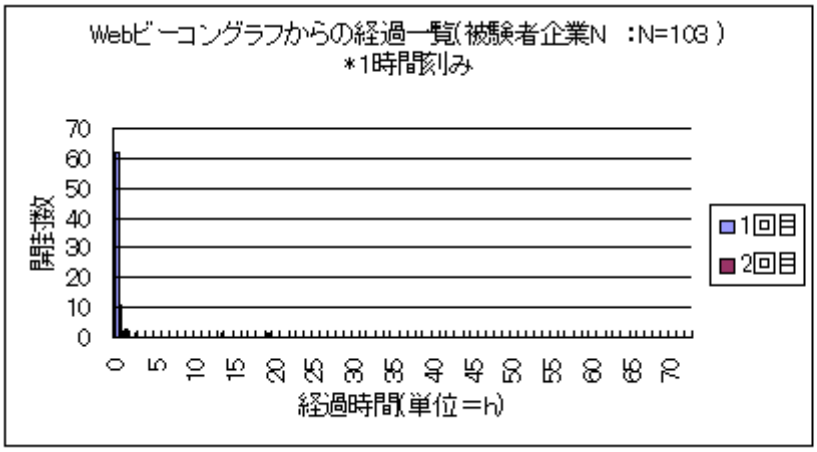
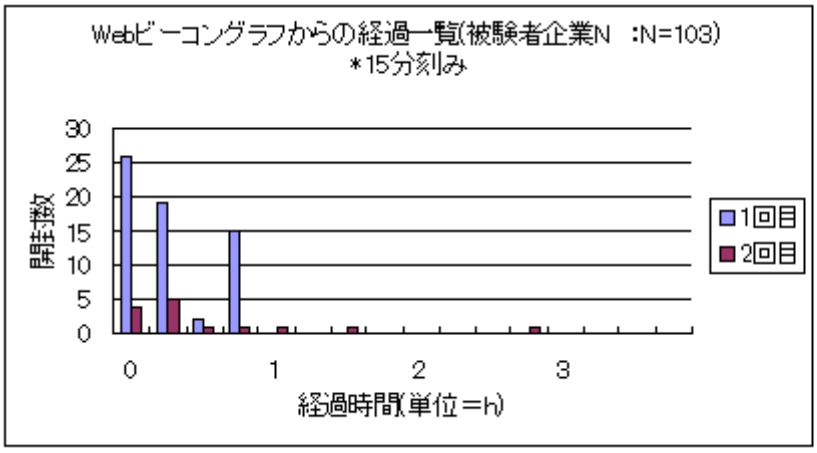


図 122 被験者企業 N：Web ビーコンの時系列開封状況(15 分刻み 4 時間分)



16.6. 予防接種実施時の特記事項

16.6.1. 添付ファイルの再転送

被験者企業 N の第 1 回配信の際に、ある被験者が、擬似攻撃メールの添付ファイルを別のファイル名に変更した上で、社内用メッセンジャー経由で同僚に転送したとのことである。種明かしがこの部分に触れていないのを訝しむコメントが、被験者アンケートの自由記述欄に見られた。

これ自体は単純ないたずらであると思われるが、擬似攻撃メールの添付ファイルを使った「2 次攻撃」を行ったのは、この被験者が初めてである。

本物の標的型メール攻撃でも同様の転送が起きる可能性はあると思われるが、もしこれが起きれば、本物の同僚からファイルを転送されるわけで、攻撃ベクトルとしては非常に危険である。

また、今回の予防接種においては、この転送のために騒ぎが起きかけたとのことで、窓口担当者が急いで種明かしを実施して鎮めた。

16.7. 被験者アンケートの集計

被験者企業 N における被験者アンケートの集計状況について表 66 に示す。

表 66 被験者企業 N：被験者アンケート回答者の開封状況

有効回答数	51 名	
	第 1 回	第 2 回
開封した人数	43 名(84.3%)	9 名(17.6%)
2 回とも開封した人	7 名(13.7%)	

被験者企業 N では、被験者数 103 名に対し、54 名(52.4%)の被験者から被験者アンケートへの回答があった。このうちの 2 名は擬似攻撃メールに気付かなかったと回答しているので、被験者アンケートの有効回答者数を 51 名とする。

被験者アンケートの有効回答者 51 名の中で、第 1 回配信で添付ファイルを開封したと回答している被験者は 43 名(84.3%)であり、第 2 回配信での開封者は 9 名(17.6%)である。また、一度でも添付ファイルを開封したと回答した被験者は 45 名(88.2%)であり、両方を開封した被験者は 7 名(13.7%)である。

前節で Web ビーコンから開封率を見たが、本節のアンケート回答者の開封率の方がやや高めの比率となっている。しかし、全体としてはほぼ同様の傾向を示していると言える。

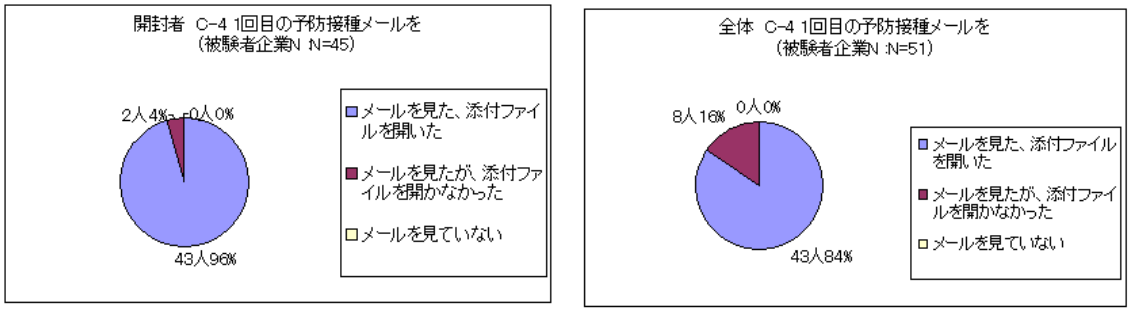
16.8. 被験者アンケートの分析

本節では、被験者企業 N の被験者アンケートの有効回答の内容からその特徴となる諸点を示す。

16.8.1. 添付ファイル開封の有無とその理由

被験者企業 N における被験者アンケートの設問 C-4 に対する回答状況を図 123 に示す。

図 123 被験者企業 N：被験者アンケートから見た開封状況(第 1 回配信)



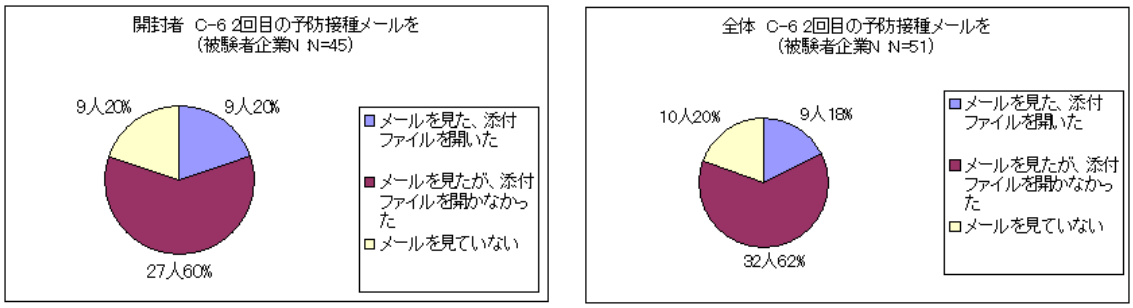
前述の通り、第 1 回配信では有効回答者 51 名中の 43 名(84.3%)が添付ファイルを開封したと回答している。

被験者アンケートの設問 C-5 に対する回答からその理由を探すと、以下のようなものがあった。

1. メールの内容があり得るネタであった。
2. 社長の名前であった。
3. メーリングリストの表題になっていて、かつ、差出人が社長の名前であった。
4. 送信元アドレスがおかしいと思ったが、メール文章が送信者のものと似ていたので。

図 124 に、被験者アンケートの設問 C-6 に対する回答状況を示す。

図 124 被験者企業 N：被験者アンケートから見た開封状況(第 2 回配信)



前述の通り、被験者企業 N の第 2 回配信では、有効回答者 51 名中の 9 名

(17.6%)が添付ファイルを開封したと回答している。第 1 回配信と比較すると、開封者が大幅に減少していることがわかる。

被験者企業 N では、もう一度擬似攻撃メールを配信することを第 1 回配信と第 2 回配信の間に予告したために被験者が警戒心を強め、第 2 回配信での開封率が大幅に改善されたのではないかと思われる。

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が、どのような理由で開封しなかったのかを被験者アンケートの設問 C-7 に対する回答から検討すると、この予告の効果を確認できる。

すなわち、当該被験者の多くは第 1 回配信後の予告によって警戒を強めている上、第 2 回配信の擬似攻撃メールの差出人や内容が第 1 回配信のものと似ていることから不審なメールであると判断している。

なお、今年度の予防接種で重要な気付きのポイントとなっている差出人のメールアドレスを確認して擬似攻撃メールをそれと見破った被験者は、第 2 回配信での非開封者 42 名のうちの 11 名(26.2%)に過ぎない。

第 1 回配信と第 2 回配信の両方で添付ファイルを開封した被験者は 7 名(13.7%)であるが、その開封理由を設問 C-7 への回答から抜粋しておく。

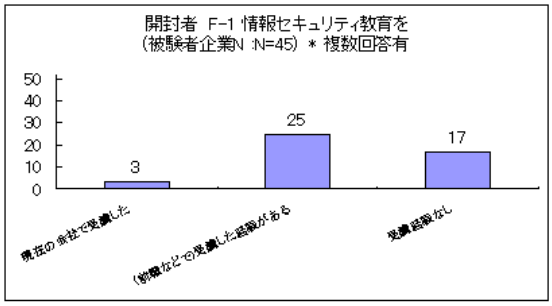
1. あやしいから興味で見た。
2. ストックオプションの内容を確認するために開きました。
3. ひらくとどうなるのかと思い開いた。
4. メールはできるだけ添付ファイルを開いて確認するようにしているから。
5. 以前、同様の内容のメールが来たことがあり、信頼性が高かったため。
6. 休み明けでメール確認を早く終わらせようと焦っていたため標的メールのことは注意していなかった。

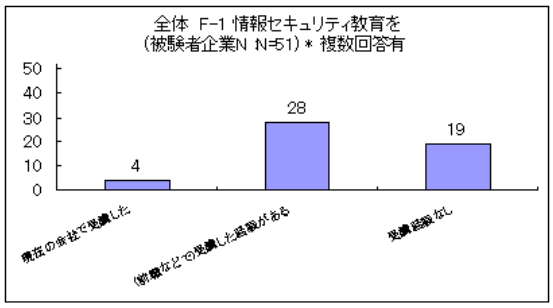
16.8.2. 情報セキュリティ教育の経験

ここでは、情報セキュリティ教育の経験の有無と開封率の間に、どのような関係が読み取れるかについて調べる。

被験者アンケートの設問 F-1 への回答状況を図 125 に示す。

図 125 被験者企業 N：情報セキュリティ教育の経験



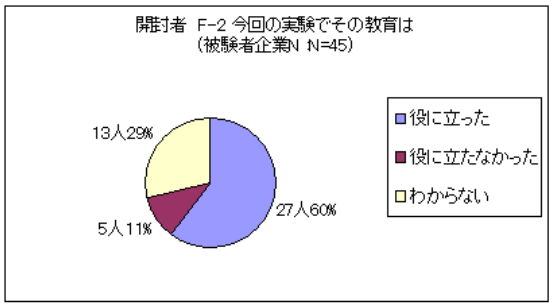


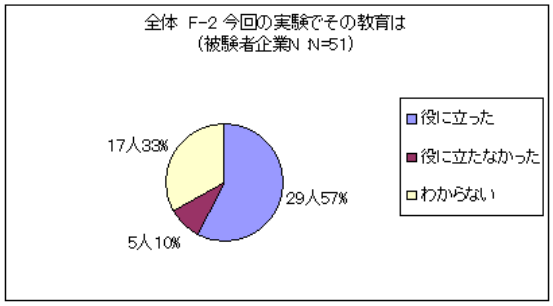
これによれば、被験者アンケート有効回答者 51 名中の 4 名(7.8%)が、現在の勤務先で情報セキュリティ教育を受けたと回答している。前職などで情報セキュリティ教育を受けたことがある被験者は、有効回答者 51 名の中の 28 名(54.9%)であり、受講経験がないと回答した被験者は 19 名(37.3%)である。

被験者企業 N では、定期的な情報セキュリティ教育が事実上行われていないに等しいということであり、早期に改善するべき課題である。

図 126 に被験者アンケートの設問 F-2 に対する回答状況を示す。

図 126 被験者企業 N：情報セキュリティ教育の有効性





これによれば、情報セキュリティ教育が予防接種に対して役に立ったと回答している被験者は、有効回答者 51 名中の 29 名(56.9%)である。教育が役に立ったかどうかわからないと回答した被験者は、有効回答者 51 名中の 21 名(41.2%)である。

一方、開封者 45 名の中では、27 名(60.0%)の被験者が、情報セキュリティ教育が役立ったと回答している。

ここでも、情報セキュリティ教育の受講経験と予防接種の開封率の間には、あまり相関関係がないようである。

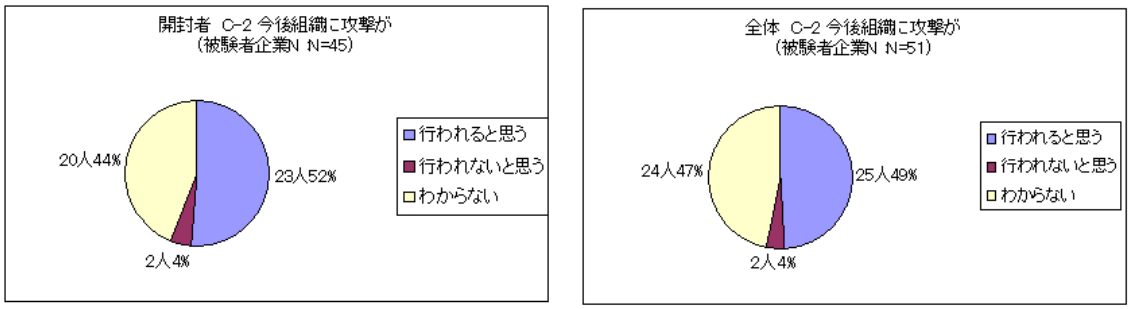
16.8.3. もし標的型攻撃がきたら、どう対処するか

ここでは、被験者アンケートの設問 C-2, C-3, F-3 などに対する回答から、本

物の攻撃があった場合にどのような反応を示すと思われるかを検討する。

被験者アンケートの設問 C-2 に対する回答を図 127 に示す。

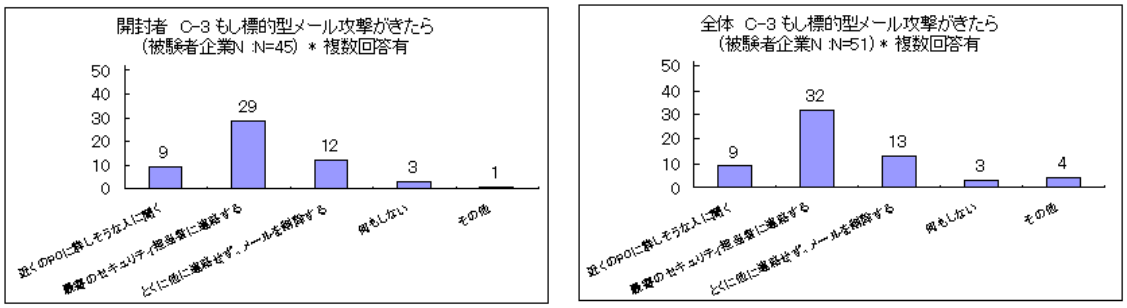
図 127 被験者企業 N：今後組織に攻撃があると思うか



これによれば、有効回答者 51 名の中で、今後組織に標的型メール攻撃が行われるかもしれないと回答している被験者は 25 名(49.0%)である。
予防接種を経験して、改めて脅威を認識したということであろう。
しかし、その比率は例によって半数程度でしかない。

図 128 に、被験者アンケートの設問 C-3 に対する回答状況を示す。

図 128 被験者企業 N：もし標的型攻撃が来たら

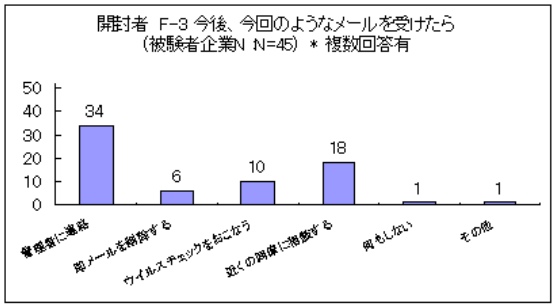


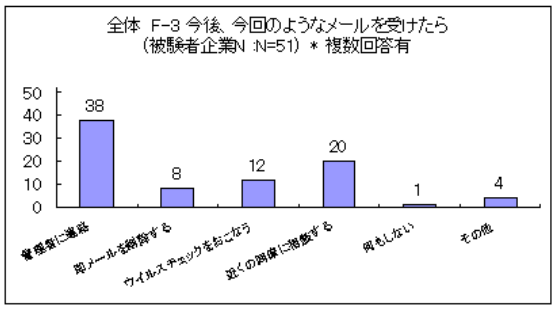
これによれば、標的型メール攻撃を受けた場合の対処方法として、「もよりのセキュリティ担当者に連絡する」と回答した被験者は、有効回答者 51 名中の 32 名(62.7%)である。
他方で、有効回答者 51 名中の 13 名(25.5%)は、「とくに他に連絡せずに削除する」と回答している。
被験者企業 N では、会社としての情報セキュリティポリシーを持っていないにも関わらず、6 割以上の被験者がインシデント報告を行うと回答しているのであるから、素晴らしいというべきであろう。

図 129 に、被験者アンケートの設問 F-3 に対する回答状況を示す。設問 F-3

は、先の設問 C-3 とほぼ同じ内容について、文言を変えて再び尋ねている。

図 129 被験者企業 N：今後、今回のようなメールを受けたら





これによれば、標的型攻撃のメールが来た場合の対処方法として、「セキュリティ管理者に連絡する」と回答した被験者が有効回答 51 名中の 38 名(74.5%)となり、先の設問 C-3 への回答よりも比率が上がっている。

逆に、「即メールを削除する」と回答している被験者は 51 名中 8 名(15.7%)と減少している。

被験者企業 N は証券業を営むと言うこともあって、事故発生時には証拠保全し、管理者に連絡するという文化を持っている様子がうかがえる。

ただし、被験者企業インタビューの際の議論では、情報技術に馴染みがない社員が多く、そのような社員は何かあればすぐにわかる社員に尋ねる習慣を持つと言うことである。結局のところは、「近くの PC に詳しそうな人に訊く」と大同小異であるのかも知れない。

16.8.4. 危機管理意識の変化

被験者アンケートの設問 F-4 では、危機管理意識の変化について尋ねている。この設問への回答を見ると、有効回答者 51 名中の 41 名(80.4%)の被験者が、今回の訓練を通して危機管理意識の変化や危険の再認識を感じるとともに、予防接種を肯定的に捉えている。

被験者アンケートの自由記述欄から関連する回答を抜粋しておく。

1. 会社のネットワークであれば安全であると思っていました。
2. 私は業務委託で様々な会社へ出向しています。ある会社では、日々の業務を行う上で情報漏洩はどのようにしておこるのか、またそれを防ぐためにはどうしたらいいのか、もし情報漏洩が発覚した場合どのように対処すべきか、を電子教材として定期的(3 ヵ月に 1 回ほど)に学習させていました。今回はメールによる注意喚起でしたが、もっとほかにも業務上注意すべき部分はあると思います。たとえば、PC の前から離れるときは必ずロックしてから離れる、

など。
3. 社内イントラだからといってセキュリティー(ソフトや Proxy など)に頼らずに各自の危機管理意識が必要だと感じた。
4. 表題だけでは不審なメールだと判断できないので、見覚えの無いアドレスだった場合、メールを開かないようにしようと思った。
5. 社内事情を知るものからの攻撃は想定外であった。
6. 多少の IT 平和ボケ状態だったので、初歩を振り返る良い機会になった。

16.8.5. 感想

被験者アンケートの設問 G では、有効回答者 51 名中の 15 名(29.4%)の被験者が予防接種を肯定的に捉えており、再実施の提案や日頃の注意意識改善などの回答をしている。

以下に、いくつかの回答を抜粋する。

1. 「全体周知の場合はファイルを添付せずに、共有フォルダの場所を明記するだけにする」とか「メール本文に URL は貼り付けない」とか「フリーメールは排除する」とかルールを明確にすれば、こういう被害を広げなくて済むのではないかと思った。また、実際の被害ではどういうメール内容だったとか、どういう風な対応をしたからまずかったとかそういうことも事前に教えてもらえれば、いざという時の対応で差が出るのではないかと思った。さらに、「フリーメール」とか「外部メールサーバ」とか「宛先がおかしい」
2. メール 2 通とは別に、instantmessenger 経由でファイルが送られてきて、それは開けてしまったんですが、それがアンケートで触れられていないのが気になります。
3. メールの文面はセンスが良すぎて泣きそうであった。
4. 甘い誘い文句に騙されてしまったので、次回以降気をつけたい。
5. 気をつけるというより委縮する。事前告知したほうが、よいと思いました。
6. 事前に知っていたにもかかわらず、引っかかったので、反省しております。
7. 全てのメールの From を確認するわけではないので、怪しいメールに気づく IT リテラシーを教育などによって身につけるべきだと思いました。

ここにもいくつか出現しているが、擬似攻撃メールの話題があまりにも生々しいのではないかという指摘が、一部の被験者から出たと聞く。

標的型メール攻撃を行う立場であれば、そのような話題を好んで使うかも知れないが、予防接種を行う立場からは、自重した方が良いかも知れない。

16.9. 被験者企業アンケートと被験者企業インタビュー

被験者企業 N について、被験者企業アンケートと被験者企業インタビューから以下のことがわかる。

被験者企業 N は、会社設立後 4 年目と若い企業であることもあって、セキュリティポリシーがないなど、情報セキュリティ体制がよく整備されているとは言えない状態である。
しかし、証券業を営むためか、危機意識とインシデント報告への意識には高いものがある。
インシデント報告の義務や手順が社内規定に謳われているわけではないが、特に情報技術に疎い社員は、何かあればインフラチームへ問い合わせるのが慣習となっているとのことである。

被験者アンケートへの回答では、情報セキュリティ教育を被験者企業 N で受講したという回答が 10%未満であり、非常に低い比率であったが、実際には、年 1 回の情報セキュリティ教育を実施しているとのことであった。
在籍 1 年未満の社員も多いようなので、年 1 回の情報セキュリティ教育をこれから受講する社員が多いのかも知れないが、頻度の点でも内容の点でも、情報セキュリティ教育を改善する必要があるのではないかと思われる。

また、被験者企業 N では、ウイルス対策やスパム対策をすべてエンドポイントで実施しているとのことである。これは、顧客からのメールが万一にも誤検知・過検知で排除されることを恐れているためであるとのことである。
セキュリティポリシー的観点からは縦深防御を説きたくなるところであり、また、技術的にも不審なメールをすぐに削除するようなソリューションばかりではないので、今後の改善を望む。

前述の通り、被験者企業 N では、社内用メッセンジャー経由で擬似攻撃メールの添付ファイルを再送信した被験者がいた。
被験者企業 N では、社内用メッセンジャーを除いて、インスタントメッセンジャーの類を禁止しているとのことであったので、ポリシーの強制力や状態監視の点で一考を要する。

16.10. 考察

被験者企業 N は会社設立からの時日も浅く、セキュリティ対策もこれから整備していく状況である。
まず、被験者企業にとってはインターネットが顧客との間の主たるコミュニケーションチャンネルとなっており、したがって、一般企業にも増して情報セキュリティ対策が重要であると言える。
今後はセキュリティポリシーの制定や ISO27001 認証取得などに進むことと

なろうが、スタートアップ企業のスピード感で必ず目的を達成することと思う。

特に、今回の予防接種で社長が見せた決断は賞賛に値する。すなわち、予防接種実施への指示を出すとともに、実行責任を窓口担当者に権限委譲して、みずからは被験者の一人として参加するという決断は、なかなかできるものではない。

この社長のイニシアティブがあれば、情報セキュリティ対策の立案や構築も成功裏に実行可能であろう。

なお、その際には、前節にあるいくつかの注意点を踏まえていただければ幸いである。

17. 被験者全体の傾向分析

今年度の予防接種では、14 の被験者企業にまたがる 2,603 名の被験者を対象とした。本章では、これらすべての被験者企業・被験者について分析を行う。

なお、被験者企業 A は、擬似攻撃メールの配信順序によってグループ A とグループ B のふたつに分割して扱う。以下では、被験者企業 A のグループ A を A(a)、グループ B を A(b)と呼ぶ。

17.1. Webビーコンによる被験者企業別の開封状況

被験者数や Web ビーコンのアクセスログから見た開封者数などは、これまで被験者企業毎に見てきた通りである。

ここでは、さらに、第 1 回配信での開封率から第 2 回配信の開封率を差し引くことで、どの程度事態が改善したかを示す指数を計算しよう。これを改善率と呼び、次のように定義する。

(改善率) ＝ (第 1 回配信での開封率) − (第 2 回配信での開封率)

このような計数や比率を表 67 に示す。

表 67 被験者全体：Web ビーコンから見た開封状況と改善率

被験者企業	被験者数	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(a)	215	119	55.3%	17	7.9%	47.4%
A(b)	213	40	18.8%	93	43.7%	-24.9%
B	83	17	20.5%	6	7.2%	13.3%
C	308	54	17.5%	24	7.8%	9.7%
D	29	4	13.8%	7	24.1%	-10.3%
E	70	49	70.0%	4	5.7%	64.3%
F	25	2	8.0%	1	4.0%	4.0%
G	724	346	47.8%	59	8.1%	39.6%
H	49	30	61.2%	4	8.2%	53.1%
I	280	61	21.8%	61	21.8%	0.0%
J	94	32	34.0%	6	6.4%	27.7%
K	65	48	73.8%	11	16.9%	56.9%
L	124	17	13.7%	2	1.6%	12.1%
M[9]	221	85	39.7%	56	25.3%	14.4%
N	103	62	60.2%	16	15.5%	44.7%
合計	2,603	966	37.1%	367	14.1%	23.0%

[9] 被験者企業 M では、第 1 回配信の際の被験者数が 214 名、第 2 回配信では 221 名であった。そこで、第 1 回配信の開封率および開封者①の開封率の計算には 214 名を採用し、その他の場合は 221 名を採用することにした。以下でも同様である。

例えば、今年度の予防接種の被験者総数は 2,603 名で、第 1 回配信では 966 名(37.1%)が添付ファイルを開封しており、第 2 回配信では 367 名(14.1%)が開封している。被験者全体についての改善率は、23.0%である。

ここで、添付ファイルの開封状況をもう少し詳しく見てみよう。

第 1 回配信時にのみ添付ファイルを開封した被験者を「開封者①」と呼ぶことにする。
同様に、第 2 回配信時にのみ開封した被験者を「開封者②」、第 1 回配信と第 2 回配信の両方で添付ファイルを開封した被験者を「開封者⑫」、第 1 回配信と第 2 回配信の両方で開封しなかった被験者を「非開封者」と呼ぶことにする。

さて、開封者①とは、第 1 回配信では添付ファイルを開封したが、第 2 回配信では見破って開封しなかった被験者のことである。
このような被験者は、予防接種による学習効果があったと判断することができるので、その人数比を学習効果率と呼んで次のように定義する。

(学習効果率) ＝ (開封者①) ÷ (第 1 回配信の開封者数)

このような計数や比率を表 68 に示す。

表 68 被験者全体：Web ビーコンから見た開封状況の詳細

被験者企業	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	構成比	被験者数	構成比	被験者数	構成比	被験者数	構成比	
A(a)	13	6.0%	106	49.3%	4	1.9%	92	42.8%	89.1%
A(b)	14	6.6%	26	12.2%	79	37.1%	94	44.1%	65.0%
B	2	2.4%	15	18.1%	4	4.8%	62	74.7%	88.2%
C	4	1.3%	50	16.2%	20	6.5%	234	76.0%	92.6%
D	0	0.0%	4	13.8%	7	24.1%	18	62.1%	100.0%
E	2	2.9%	47	67.1%	2	2.9%	19	27.1%	95.9%
F	0	0.0%	2	8.0%	1	4.0%	22	88.0%	100.0%
G	39	5.4%	307	42.4%	20	2.8%	358	49.4%	88.7%
H	2	4.1%	28	57.1%	2	4.1%	17	34.7%	93.3%
I	17	6.1%	44	15.7%	44	15.7%	175	62.5%	72.1%
J	5	5.3%	27	28.7%	1	1.1%	61	64.9%	84.4%
K	10	15.4%	38	58.5%	1	1.5%	16	24.6%	79.2%
L	0	0.0%	17	13.7%	2	1.6%	105	84.7%	100.0%
M	27	12.2%	58	27.1%	29	13.1%	107	48.4%	68.2%
N	14	13.6%	48	46.6%	2	1.9%	39	37.9%	77.4%
合計	149	5.7%	817	31.4%	218	8.4%	1,419	54.5%	84.6%

被験者全体の開封者①は 817 名(31.4%)、開封者②は 218 名(8.4%)、開封者⑫は 149 名(5.7%)、非開封者は 1,419 名(54.5%)である。また、この場合の学習効果率は、84.6%である。

第 1 回配信と第 2 回配信のいずれか、または、両方で添付ファイルを開封した被験者(「開封者」と呼んでいる)が、被験者全体では 1184 名(45.5%)であることは、容易に計算できる。

(開封者) ＝ (開封者①) ＋ (開封者②) ＋ (開封者⑫)

各被験者企業と全被験者の平均について、開封者①・開封者②・開封者⑫・非開封者の比率を図 130 に示す。また、改善率と学習効果率のグラフを図 131 に示す。

図 130 被験者全体：Web ビーコンから見た開封状況

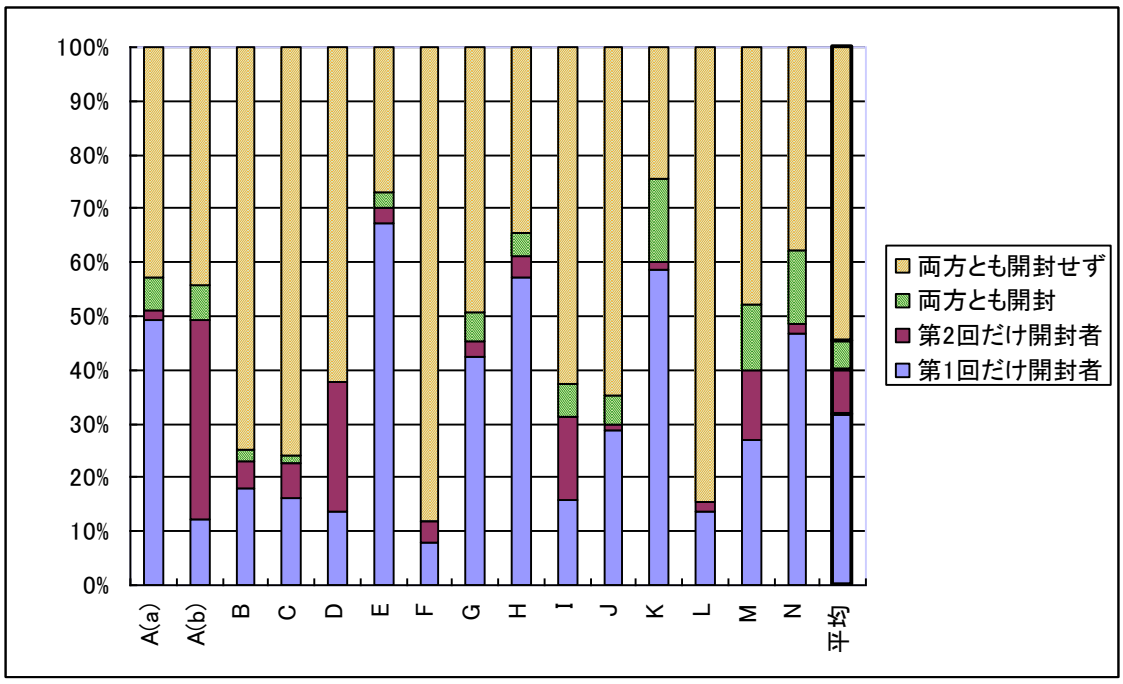
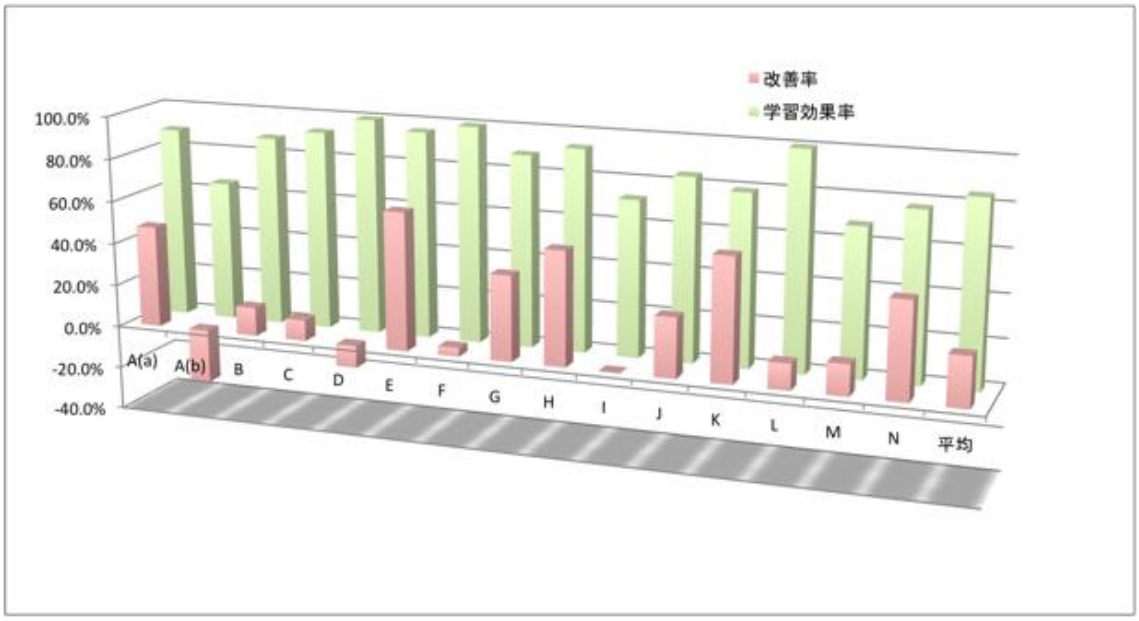


図 131 被験者全体：Web ビーコンから見た改善率と学習効果率



開封者②の比率が高い(10%以上)被験者企業は、被験者企業 A(b)の 37.1%、被験者企業 D の 24.1%、被験者企業 I の 15.7%、被験者企業 M の 13.1%である。

学習率は高いが、開封者②が多いのは被験者企業 D であった。
被験者アンケートの回答とあわせて分析すると、被験者企業 D の開封者は、実際は 1 名で、他は添付ファイルを技術的に安全であると判断しているか、予防接種の訓練だと気付き、好奇心から開封している。

学習率が平均より低く、開封者②が多い被験者企業は、A(b)・I・M である。
被験者企業 A(b)では、第 2 回の擬似攻撃メールが、偽装されていると気付きにくい自組織のドメイン名から送られており、実際に組織内にある部署を騙ったものであった。
被験者企業 I では、通常の業務メールとして違和感のない本文であった。ただし、差出人の表示名は設定されていなかった。
被験者企業 M では、擬似攻撃メールの文面が、たまたま被験者企業 M の状況とタイミングよく合致しており、メールの本文だけを読むと納得できる内容であった。
このことから、擬似攻撃メールは通常サブジェクトと本文の内容が受信者にとって受け入れやすい場合は、特に疑問におもわず開封する確率が高い、ということが確認できた。

17.2. 被験者アンケートから見た被験者企業別の開封状況

被験者アンケートから見た開封者数や開封率についても、前節の Web ビーコンのアクセスログから見た傾向と同様に分析する。

被験者アンケートの設問 C-4, C-6 について被験者企業別に集計して、開封者数や開封率と改善率を得た。これを表 69 に示す。

表 69 被験者全体：被験者アンケートから見た開封状況と改善率

被験者企業	有効回答者数	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(a)	136	73	53.7%	20	14.7%	39.0%
A(b)	117	27	23.1%	32	27.4%	-4.3%
B	42	10	23.8%	4	9.5%	14.3%
C	91	23	25.3%	10	11.0%	14.3%
D	8	2	25.0%	1	12.5%	12.5%
E	46	33	71.7%	2	4.3%	67.4%
F	14	2	14.3%	3	21.4%	-7.1%
G	460	199	43.3%	32	7.0%	36.3%
H	29	21	72.4%	0	0.0%	72.4%
I	73	26	35.6%	14	19.2%	16.4%
J	32	11	34.4%	1	3.1%	31.3%
K	35	28	80.0%	5	14.3%	65.7%
L	36	19	52.8%	8	22.2%	30.6%
M	82	34	41.5%	22	26.8%	14.6%
N	51	43	84.3%	9	17.6%	66.7%
合計	1,252	551	44.0%	163	13.0%	31.0%

今年度の被験者アンケートの有効回答数は全体では 1,252 名で、被験者総数 2,603 名の 48.1%との回答率である。

このうち、第 1 回配信では 551 名(44.0%)、第 2 回配信では 163 名(13.0%)が添付ファイルを開封したと回答している。改善率は 31.0%である。

開封者①・開封者②などの状況を調べると、表 70 の通りである。

表 70 被験者全体：被験者アンケートから見た開封状況の詳細

被験者企業	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	構成比	被験者数	構成比	被験者数	構成比	被験者数	構成比	
A(a)	12	8.8%	61	44.9%	8	5.9%	55	40.4%	83.6%
A(b)	10	8.5%	17	14.5%	22	18.8%	68	58.1%	63.0%
B	1	2.4%	9	21.4%	3	7.1%	29	69.0%	90.0%
C	4	4.4%	19	20.9%	6	6.6%	62	68.1%	82.6%
D	0	0.0%	2	25.0%	1	12.5%	5	62.5%	100.0%
E	1	2.2%	32	69.6%	1	2.2%	12	26.1%	97.0%
F	1	7.1%	1	7.1%	2	14.3%	10	71.4%	50.0%
G	19	4.1%	180	39.1%	13	2.8%	248	53.9%	90.5%
H	0	0.0%	21	72.4%	0	0.0%	8	27.6%	100.0%
I	7	9.6%	19	26.0%	7	9.6%	40	54.8%	73.1%
J	1	3.1%	10	31.3%	0	0.0%	21	65.6%	90.9%

K	5	14.3%	23	65.7%	0	0.0%	7	20.0%	82.1%
L	5	13.9%	14	38.9%	3	8.3%	14	38.9%	73.7%
M	13	15.9%	21	25.6%	9	11.0%	39	47.6%	61.8%
N	7	13.7%	36	70.6%	2	3.9%	6	11.8%	83.7%
合計	86	6.9%	465	37.1%	77	6.2%	624	49.8%	84.4%

被験者アンケートへの有効回答全体では、開封者①は 465 名(37.1%)、開封者②は 77 名(6.2%)、開封者⑫が 86 名(6.9%)、非開封者は 624 名(49.8%)となる。学習効果率は 84.4%である。

前節の Web ビーコンから見た開封状況と比較して、第 1 回配信での開封者数がやや多いなど多少の違いはあるものの、よく似た傾向を示している。

ここで調べた開封者①・開封者②・開封者⑫・非開封者の比率を図 132 に示す。また、改善率と学習効果率のグラフを図 133 に示す。

図 132 被験者全体：被験者アンケートから見た開封状況

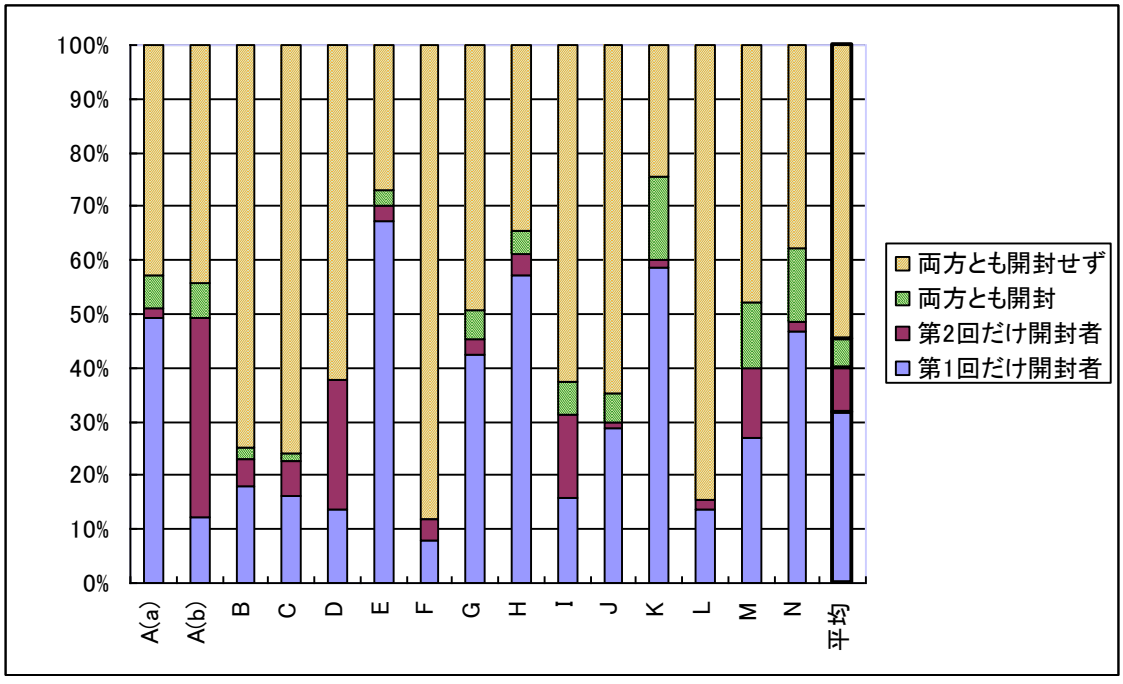
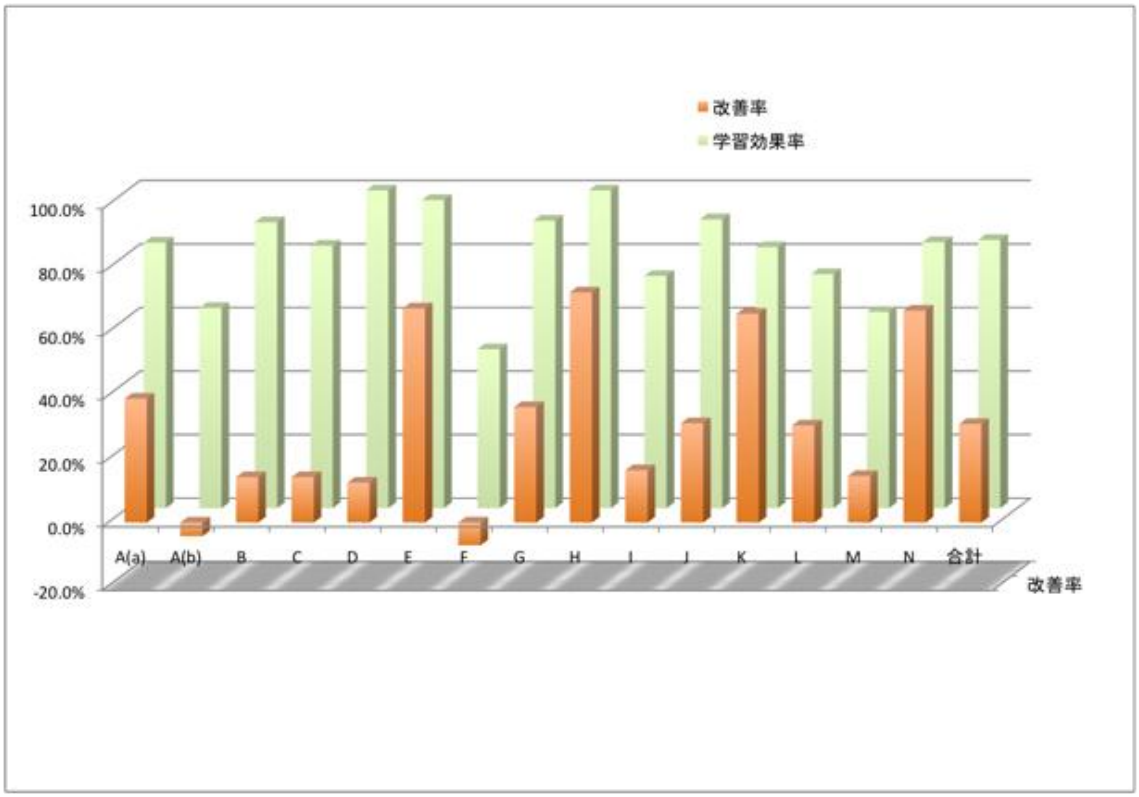


図 133 被験者全体：被験者アンケートから見た改善率と学習効果率



17.3. 被験者企業の属性で分類した開封状況

被験者企業アンケートと被験者企業インタビューの結果から、情報セキュリティ対策の整備状況の指標となる項目を表 71 に掲げる。

表 71 被験者全体：被験者企業の属性

被験者企業名	IT 系企業	ISO27001	ISO 9000	P マーク	BCP	CSO	情報セキュリティ専門部署	情報セキュリティポリシー	電子メールのセキュリティ規定	メールアカウントの即時停止
A	-	-	-	-	-	有	-	有	有	-
B	○	取得済	-	取得済	-	有	有	有	有	有
C	○	取得済	取得済	取得済	取得済	有	有	有	有	有
D	○	取得済	-	-	-	有	有	有	有	有
E	-	取得済	取得済	-	-	有	有	有	有	-
F	○	-	-	-	-	-	有	有	有	-
G	○	取得済	取得済	-	-	有	有	有	有	-
H	○	取得済	取得済	取得済	-	有	有	有	有	-
I	○	-	-	-	-	有	有	有	有	-

J	-	取得済	取得済	-	-	有	有	有	-	有
K	-	-	取得済	-	-	-	-	有	有	-
L	○	取得済	-	取得済	-	有	有	有	有	有
M	-	-	-	-	-	-	-	有	有	有
N	-	-	-	-	-	-	-	-	-	有

以下では、これらの指標によって被験者企業を分類し、被験者企業別の開封状況を調べることにする。

ただし、ISO27001 とプライバシーマークの認定状況はよく似ているのでまとめて傾向を見ることにする。また、ISO9000 シリーズ・BCP・情報セキュリティに関わる専門部署・情報セキュリティポリシー・電子メール関連セキュリティ規定の有無については、被験者企業が片方に偏るので調べなかった。

17.3.1. IT系企業/非IT系企業別の開封状況

今年度の被験者企業の中で、被験者企業 B, C, D, F, G, H, I, L は IT 系企業であると思われる。被験者企業 A, E, J, K, M, N は非 IT 系企業である。

なお、被験者企業 N はいわゆるオンライン証券業で IT 系企業とも言えるが、ここでは本業が IT 系ではないことを重視して、非 IT 系企業に分類した。

この分類にしたがって開封状況と指標を表 72 および表 73 に示す。

IT 系の被験者企業と非 IT 系の被験者企業を比較すると、以下の傾向があることがわかる。

1. 開封率は、全般に IT 系企業の方が非 IT 系企業よりも低い。
2. 改善率には、両者にさほどの違いがない。
3. 学習効果率は、IT 系企業の方が非 IT 系企業よりも高い。

表 72 IT 系/非 IT 系の開封状況と改善率

	被験者企業分類	被験者数	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	
Web ビーコン	IT 系	1,622	531	32.7%	164	10.1%	22.6%
	非 IT 系	981	435	44.3%	203	20.7%	23.6%
被験者アンケート	IT 系	753	302	40.1%	72	9.6%	30.5%
	非 IT 系	499	249	49.9%	91	18.2%	31.7%

表 73 IT 系/非 IT 系の開封状況と学習効果率

	被験者	開封者⑫		開封者①		開封者②		非開封者		学習効果率
	企業分	被験	構成比	被験	構成比	被験	構成比	被験	構成比	

	類	者数		者数		者数		者数		
Web ビーコン	IT 系	64	3.9%	467	28.8%	100	6.2%	991	61.1%	87.9%
	非 IT 系	85	8.7%	350	35.7%	118	12.0%	428	43.6%	80.5%
被験者アンケート	IT 系	37	4.9%	265	35.2%	35	4.6%	416	55.2%	87.7%
	非 IT 系	49	9.8%	200	40.1%	42	8.4%	208	41.7%	80.3%

17.3.2. ISO27001 などの認証取得と開封状況

ISO27001 とプライバシーマークのいずれかまたは両方の認証を取得しているか否かで、被験者企業を分類する。

認証取得済みの被験者企業は、被験者企業 B,C,E,G,H,J,L である。被験者企業 A,D,F,I,K,M,N はこの種の認証を取得していない。

なお、被験者企業 D は部門単位で ISO27001 認証を取得しているが、今回の予防接種の被験者の所属する部門では取得していないので、認証を取得していない側に分類した。

この分類にしたがって開封状況と指標を表 74 および表 75 に示す。

認証を取得している被験者企業と取得していない被験者企業を比較すると、以下の傾向があることがわかる。

1. 第 1 回配信での開封率はさほどの差が無いが、認証取得企業では第 2 回配信での開封率が非認証取得企業よりも低い。
2. 改善率は、認証取得企業の方が、非認証取得企業よりも高い。
3. 学習効果率は、認証取得企業の方が非認証取得企業よりも高い。

表 74 認証取得状況別の開封状況と改善率

	被験者企業分類	被験者数	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	
Web ビーコン	認証有	1,452	545	37.5%	105	7.2%	30.3%
	認証無	1,151	421	36.6%	262	22.8%	13.8%
被験者アンケート	認証有	736	316	42.9%	57	7.7%	35.2%
	認証無	516	235	45.5%	106	20.5%	25.0%

表 75 認証取得状況別の開封状況と学習効果率

	被験者企業分類	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	構成比	被験者数	構成比	被験者数	構成比	被験者数	構成比	
Web	認証有	54	3.7%	491	33.8%	51	3.5%	856	59.0%	90.1%

ビーコン	認証無	95	8.3%	326	28.3%	167	14.5%	564	48.9%	77.4%
被験者アンケート	認証有	31	4.2%	285	38.7%	26	3.5%	394	53.5%	90.2%
	認証無	55	10.7%	180	34.9%	51	9.9%	230	44.6%	76.6%

17.3.3. CSOの有無と開封状況

CSO(最高セキュリティ責任者)を任命しているか否かで、被験者企業を分類する。

CSO を任命している被験者企業は、被験者企業 A, B, C, D, E, G, H, I, J, L である。被験者企業 F, K, M, N は CSO を任命していない。

この分類にしたがって開封状況と指標を表 76 および表 77 に示す。

CSO を任命している被験者企業と任命していない被験者企業を比較すると、以下の傾向があることがわかる。

1. CSO 任命企業の方が非 CSO 任命企業よりも、全般的に開封率が低い。ただし、開封者②だけはほとんど差が無い
2. 改善率は、CSO 任命企業の方が、非 CSO 任命企業よりも低い。
3. 学習効果率は、CSO 任命企業の方が非 CSO 任命企業よりも高い。

表 76 CSO 任命状況別の開封状況と改善率

	被験者企業分類	被験者数	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	
Web ビーコン	CSO 有	2,189	769	35.1%	283	12.9%	22.2%
	CSO 無	414	197	47.6%	84	20.3%	27.3%
被験者アンケート	CSO 有	1,070	444	41.5%	124	11.6%	29.9%
	CSO 無	182	107	58.8%	39	21.4%	37.4%

表 77 CSO 任命状況別の開封状況と学習効果率

	被験者企業分類	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	構成比	被験者数	構成比	被験者数	構成比	被験者数	構成比	
Web ビーコン	CSO 有	98	4.5%	671	30.7%	185	8.5%	1235	56.4%	87.3%
	CSO 無	51	12.3%	146	35.3%	33	8.0%	184	44.4%	74.1%
被験者	CSO	60	5.6%	384	35.9%	64	6.0%	562	52.5%	86.5%

アンケート	有									
	CSO 無	26	14.3%	81	44.5%	13	7.1%	62	34.1%	75.7%

17.3.4. メールアカウント即時停止状況と開封状況

退職者などのメールアカウントを即時停止する社内規定があるか否かで、被験者企業を分類する。

即時停止する被験者企業は、被験者企業 B, C, D, J, L, M, N である。被験者企業 A, E, F, G, H, I, K はそのような規定を持たない。

この分類にしたがって開封状況と指標を表 78 および表 79 に示す。

退職者などのメールアカウントを即時停止する社内規定を持つ被験者企業と持たない被験者企業を比較すると、以下の傾向があることがわかる。

1. 即時停止企業の方が非即時停止企業よりも、全般的に開封率がやや低くなる傾向がある。ただし、開封者⑫のように逆転している部分もある。
2. 改善率は、即時停止企業の方が、非即時停止企業よりも低い。
3. 学習効果率は、即時停止企業の方が非即時停止企業よりも低い。

表 78 メールアカウント即時停止状況別の開封状況と改善率

	被験者企業分類	被験者数	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	
Web ビーコン	即時停止有	962	271	28.2%	117	12.2%	16.0%
	即時停止無	1,641	695	42.4%	250	15.2%	27.1%
被験者アンケート	即時停止有	342	142	41.5%	55	16.1%	25.4%
	即時停止無	910	409	44.9%	108	11.9%	33.1%

表 79 メールアカウント即時停止状況別の開封状況と学習効果率

	被験者企業分類	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	構成比	被験者数	構成比	被験者数	構成比	被験者数	構成比	
Web ビーコン	即時停止有	52	5.4%	219	22.8%	65	6.8%	626	65.1%	80.8%
	即時停止無	97	5.9%	598	36.4%	153	9.3%	793	48.3%	86.0%
被験者	即時停	31	9.1%	111	32.5%	24	7.0%	176	51.5%	78.2%

アンケート	止有									
	即時停止無	55	6.0%	354	38.9%	53	5.8%	448	49.2%	86.6%

17.4. 被験者企業の属性で分類した被験者アンケート項目

さて、ここでは、開封状況以外の被験者アンケート項目のうち注目すべき設問について、被験者企業別の集計・分析を行う。

なお、被験者企業 A では被験者アンケートの設問が大きく異なるため、以下の集計・分析の対象としていない。

注目した設問は、C-1, C-2, C-3, F-1, F-2, F-3 である。これらの設問は、被験者が標的型メール攻撃についてどのような知識を持つのか、どのような行動を取るのか、また、情報セキュリティ教育が有効であるか否かについて尋ねている。

これらの設問について被験者企業別に集計した結果を表 80 に示す。

これによれば、被験者アンケートの有効回答者数 999 名のうち、標的型メール攻撃をもともと知っていた被験者は、527 名(52.8%)である。

今後組織に標的型メール攻撃が行われると思う被験者は668名(63.2%)である。

今後、標的型攻撃メールを受信した場合に管理者に連絡すると回答した被験者は、設問 C-3 では 570 名(57.1%)、設問 F-3 では 625 名(62.6%)である。ほぼ同様の質問に対して約 5%の差が出るのは、両者の中間にある設問で擬似攻撃メールの添付ファイルを開いたか否かとその理由を尋ねたために、インシデント報告の義務を思い出したと言うことだろうか。

標的型攻撃メールを受信した場合にすぐに削除すると回答した被験者は、設問 C-3 では 320 名(32.0%)、設問 F-3 では 539 名(54.0%)である。管理者への連絡と同様に、当該メールの削除を選択する被験者も増加している。これは、被害局限のためにはとにかく削除すれば良いという考え方があるためではないかと思われる。被害局限策としては一定の効果があるが、インシデント・ハンドリングやフォレンジック調査の観点から見ると、攻撃の痕跡を消すことになりかねないという問題もある。

情報セキュリティ教育を現在の会社で受講したと回答した被験者は 758 名(75.9%)である。

情報セキュリティ教育が役に立ったと回答した被験者は640名(64.1%)であり、役に立たなかったと回答した被験者は 109 名(10.9%)である。ここでは情報セキュリティ教育が役に立ったという回答が多数を占めているが、後述するとおり情報セキュリティ教育の受講経験と開封率の間に相関関係はほとんど見られない。一般的なセキュリティ知識を得るためには役に立ったが、擬似攻撃メールを見抜く役には立たなかったと言うことだろうか。

表 80 被験者全体：被験者企業別の被験者アンケート結果

被験者企業	アンケート有効回答数	標的型メール攻撃について、もともと知っていた。	今後組織に攻撃が行われると思う。	もし標的型メール攻撃がきたら「もよりのセキュリティ担当者に連絡する」	今後、今回のようなメールを受けたら「管理者に連絡する」	もし標的型メール攻撃がきたら「とくに連絡せずメールを削除する」	今後、今回のようなメールを受けたら「即メールを削除する」	情報セキュリティ教育現在の社で受講した	情報セキュリティ教育が役に立った	情報セキュリティ教育が役に立たなかった
		C-1(a)	C-2(a)	C-3(b)	F-3(a)	C-3(c)	F-3(b)	F-1(a)	F-2(a)	F-2(b)
B	42	28	26	22	21	14	21	40	34	4
		66.7%	61.9%	52.4%	50.0%	33.3%	50.0%	95.2%	81.0%	9.5%
C	91	40	50	58	58	14	39	80	62	7
		44.0%	54.9%	63.7%	63.7%	15.4%	42.9%	87.9%	68.1%	7.7%
D	8	6	4	6	2	1	3	3	2	2
		75.0%	50.0%	75.0%	25.0%	12.5%	37.5%	37.5%	25.0%	25.0%
E	46	22	28	21	15	13	20	42	29	9
		47.8%	60.9%	45.7%	32.6%	28.3%	43.5%	91.3%	63.0%	19.6%
F	14	14	12	14	14	0	2	7	11	1
		100%	85.7%	100%	100%	0.0%	14.3%	50.0%	78.6%	7.1%
G	460	225	339	254	295	147	273	377	318	36
		48.9%	73.7%	55.2%	64.1%	32.0%	59.3%	82.0%	69.1%	7.8%
H	29	21	20	23	21	7	22	23	15	7
		72.4%	69.0%	79.3%	72.4%	24.1%	75.9%	79.3%	51.7%	24.1%
I	73	42	45	55	61	17	31	51	36	14
		57.5%	61.6%	75.3%	83.6%	23.3%	42.5%	69.9%	49.3%	19.2%
J	32	17	23	14	15	20	31	32	26	5
		53.1%	71.9%	43.8%	46.9%	62.5%	96.9%	100%	81.3%	15.6%
K	35	15	20	25	22	11	19	20	12	7
		42.9%	57.1%	71.4%	62.9%	31.4%	54.3%	57.1%	34.3%	20.0%
L	36	32	21	19	24	16	11	33	24	6
		88.9%	58.3%	52.8%	66.7%	44.4%	30.6%	91.7%	66.7%	16.7%
M	82	43	55	27	39	47	59	46	42	6
		52.4%	67.1%	32.9%	47.6%	57.3%	72.0%	56.1%	51.2%	7.3%
N	51	22	25	32	38	13	8	4	29	5
		43.1%	49.0%	62.7%	74.5%	25.5%	15.7%	7.8%	56.9%	9.8%
合計	999	527	668	570	625	320	539	758	640	109
		52.8%	66.9%	57.1%	62.6%	32.0%	54.0%	75.9%	64.1%	10.9%

表 80 に掲げた比率をそのまま使ってレーダーチャートを描くと、図 134 となる。被験者全体の合計に対する比を取って正規化すると、図 135 のレーダーチャートとなる。

図 134 被験者全体：被験者企業別の被験者アンケート結果(絶対比率)

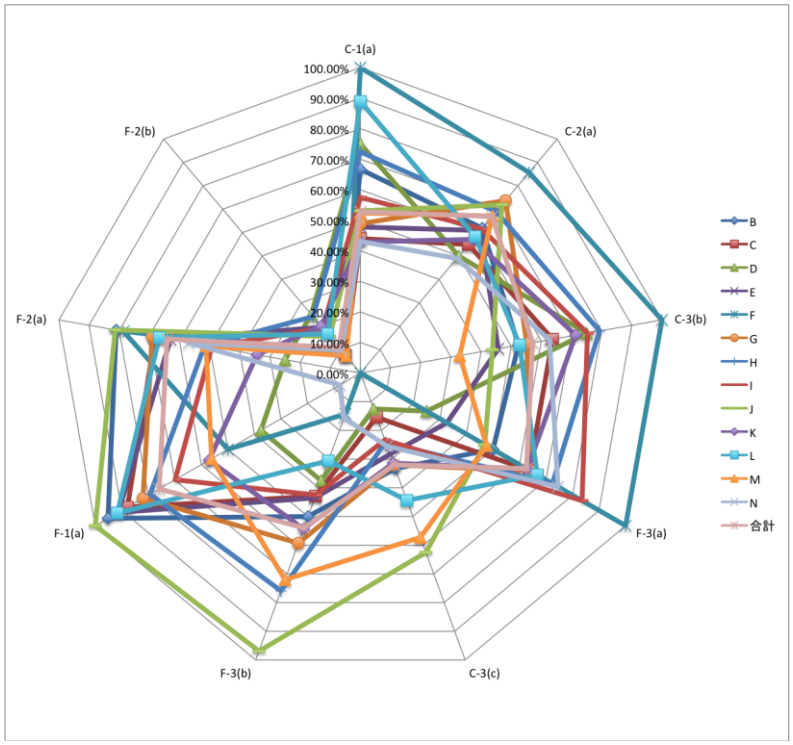
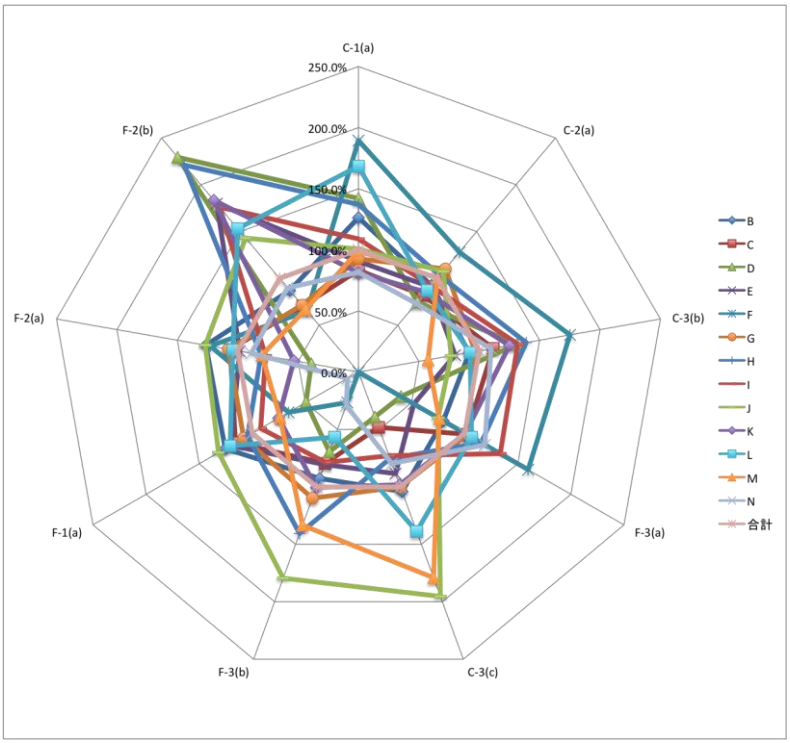


図 135 被験者全体：被験者企業別の被験者アンケート結果(相対比率)



17.4.1. IT 系企業/非 IT 系企業と被験者アンケートの傾向

17.3 節で被験者企業を属性別に分類して開封状況の傾向を探ったが、以下では同様の分類によって被験者アンケートの注目すべき設問にどのような傾向が見いだせるかを検討する。

被験者企業を IT 系企業と非 IT 系企業に分類し、各設問についてそれぞれ平均を取ると、表 81 を得る。

表 81 被験者全体：IT 系/非 IT 系の被験者アンケート分析

	被験者数	C-1(a)	C-2(a)	C-3(b)	F-3(a)	C-3(c)	F-3(b)	F-1(a)	F-2(a)	F-2(b)
IT 系	753	408	517	451	496	216	402	614	502	77
		54.2%	68.7%	59.9%	65.9%	28.7%	53.4%	81.5%	66.7%	10.2%
非 IT 系	246	119	151	119	129	104	137	144	138	32
		48.4%	61.4%	48.4%	52.4%	42.3%	55.7%	58.5%	56.1%	13.0%

これによれば、標的型メール攻撃をもともと知っていた被験者は、IT 系企業の方が非 IT 系企業よりも多く、今後組織に標的型メール攻撃が行われると思う被験者も同様である。

今後、標的型攻撃メールを受信した場合に管理者に連絡すると回答した被験者は、設問 C-3 でも設問 F-3 でも IT 系企業の方が多い。

標的型攻撃メールを受信した場合にすぐに削除すると回答した被験者は、設問 C-3 でも設問 F-3 でも IT 系企業の方が少ない。

情報セキュリティ教育を現在の会社で受講したと回答した被験者は、IT 系企業の方が多い。

情報セキュリティ教育が役に立ったと回答した被験者は IT 企業の方が多く、役に立たなかったと回答した被験者は IT 系の方が少なかった。

結局、全般に IT 系企業の方が望ましい傾向を示しており、ベースラインが高いと言える。

これは、IT 系企業に勤める被験者の方が、IT 技術やセキュリティ情報に触れる機会も多いと思われるので、全般的な技術・意識レベルがある程度高いのであろう。また、社内教育やセキュリティ対策の担当者も人材に恵まれることが多いであろう。このような観点から見れば、上記の結果は驚くに値しないと言える。

17.4.2. ISO27001 などの認証取得と被験者アンケートの傾向

ISO27001 またはプライバシーマークの認証を取得しているか否かによって被験者企業を分類して、その結果を表 82 に示す。

表 82 被験者全体：認証取得状況別の被験者アンケート分析

	被験者数	C-1(a)	C-2(a)	C-3(b)	F-3(a)	C-3(c)	F-3(b)	F-1(a)	F-2(a)	F-2(b)
認証有	736	385	507	411	449	231	417	627	508	74
		52.3%	68.9%	55.8%	61.0%	31.4%	56.7%	85.2%	69.0%	10.1%
認証無	263	142	161	159	176	89	122	131	132	35
		54.0%	61.2%	60.5%	66.9%	33.8%	46.4%	49.8%	50.2%	13.3%

これによれば、標的型メール攻撃をもともと知っていた被験者は、認証取得の有無によらず同程度である。

今後組織に標的型メール攻撃が行われると思う被験者は、認証を取得している被験者企業の方が若干高い比率である。

今後、標的型攻撃メールを受信した場合に管理者に連絡すると回答した被験者は、設問C-3 でも設問F-3 でも認証を取得していない企業の方が多い。

標的型攻撃メールを受信した場合にすぐに削除すると回答した被験者は、設問 C-3 では同程度であるが､設問 F-3 では認証を取得している企業の方が多い。

情報セキュリティ教育を現在の会社で受講したと回答した被験者は、認証を取得している企業の方が多い。

情報セキュリティ教育が役に立ったと回答した被験者は認証を取得している企業の方が多く、役に立たなかったと回答した被験者は同程度であった。

基本的には認証を取得している企業の方が望ましい結果を示しているが、インシデントの報告を行う意識付けの点では認証を取得していない企業の方が良い結果となっており、セキュリティ関連の認証を取得することが直ちに標的型メール攻撃に対する耐性の高さを示すものではないことがわかる。これについては、認証を取得していない企業では、それゆえに「何かあればとにかく管理者・担当者に問い合わせる」という傾向にあるのかも知れない。

また､「不審なメールはすぐに削除する」のようなやや拙速な反応も見られる。

特に ISO27001 ではさまざまな社内規定を作成して周知徹底するところに力点を置いているので、形式的な部分は周知徹底が進んでいるが、血肉の部分はまだこれからの課題というところであろうか。それでも、ISO27001 の認証を取得することがベースラインの底上げにつながることが見て取れるので、PDCA ループを回してよりよいセキュリティ対策・体制を構築して欲しいものである。

17.4.3. CSOの有無と被験者アンケートの傾向

CSO を任命している被験者企業とそうでない被験者企業に分類して、その結果を表 83 に示す。

表 83 被験者全体：CSO 任命状況別の被験者アンケート分析

	被験	C-1(a)	C-2(a)	C-3(b)	F-3(a)	C-3(c)	F-3(b)	F-1(a)	F-2(a)	F-2(b)

	者数									
CSO 有	817	433	556	472	512	249	451	681	546	90
		53.0%	68.1%	57.8%	62.7%	30.5%	55.2%	83.4%	66.8%	11.0%
CSO 無	182	94	112	98	113	71	88	77	94	19
		51.6%	61.5%	53.8%	62.1%	39.0%	48.4%	42.3%	51.6%	10.4%

これによれば、標的型メール攻撃をもともと知っていた被験者は、CSO 任命の有無によらず同程度である。

今後組織に標的型メール攻撃が行われると思う被験者は、CSO 任命企業の方が若干高い比率である。

今後、標的型攻撃メールを受信した場合に管理者に連絡すると回答した被験者は、設問 C-3 でも設問 F-3 でもほぼ同程度である。

標的型攻撃メールを受信した場合にすぐに削除すると回答した被験者は、設問C-3 ではCSOを任命していない企業の方が高いが、設問F-3 ではCSOを任命している企業の方が高いというねじれ現象が起きている。

情報セキュリティ教育を現在の会社で受講したと回答した被験者は、CSO を任命している企業の方が多い。

情報セキュリティ教育が役に立ったと回答した被験者はCSO を任命している企業の方が多く、役に立たなかったと回答した被験者は同程度であった。

CSO 任命の有無で比較すると、情報セキュリティ教育の受講経験については大きな差があり、CSO を任命するほどにセキュリティを重視する企業では、当然、情報セキュリティ教育にも力を入れていると言える。

これ以外の項目ではさほどの違いがあるとは読み取れないが、これらの被験者企業の CSO にとっては、インシデント報告の意識付けと周知徹底が喫緊の課題ではないかと思われる。

17.4.4. メールアカウント即時停止と被験者アンケートの傾向

退職者などに対するメールアカウントの即時停止措置が制度化され運用されているか否かによって被験者企業を分類した結果を表 84 に示す。

表 84 被験者全体：メールアカウント即時停止状況別の被験者アンケート分析

	被験者数	C-1(a)	C-2(a)	C-3(b)	F-3(a)	C-3(c)	F-3(b)	F-1(a)	F-2(a)	F-2(b)
即時停止有	342	188	204	178	197	125	172	238	219	35
		55.0%	59.6%	52.0%	57.6%	36.5%	50.3%	69.6%	64.0%	10.2%
即時停止無	657	339	464	392	428	195	367	520	421	74
		51.6%	70.6%	59.7%	65.1%	29.7%	55.9%	79.1%	64.1%	11.3%

これによれば、標的型メール攻撃をもともと知っていた被験者は、メールア

カウント即時停止措置の有る企業の方がやや高い。
今後組織に標的型メール攻撃が行われると思う被験者は、メールアカウント即時停止措置のない企業の方が高い比率である。
今後、標的型攻撃メールを受信した場合に管理者に連絡すると回答した被験者は、設問C-3 でも設問F-3 でもメールアカウント即時停止措置のない企業の方がやや高い比率である。
標的型攻撃メールを受信した場合にすぐに削除すると回答した被験者は、設問C-3 ではメールアカウント即時停止措置のある企業の方が高いが、設問F-3 ではそうでない企業の方が高いというねじれ現象が起きている。
情報セキュリティ教育を現在の会社で受講したと回答した被験者は、メールアカウント即時停止措置のない企業の方が多い。
情報セキュリティ教育が役に立ったと回答した被験者も、役に立たなかったと回答した被験者も、ほぼ同程度であった。

メールアカウントの即時停止措置の有無で分類すると、どちらかと言えば、そうでない企業の方が望ましい結果となっている。この理由はよくわからないが、規則や運用がきちんと整備された結果として、規則や運用で守られているから大丈夫と過信・誤解して個々の被験者の危機管理意識が後退したのかもしれない。

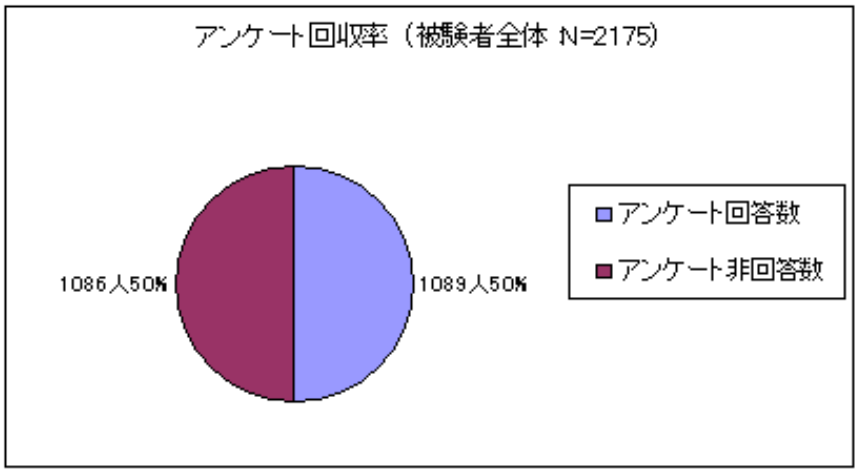
17.5. 被験者アンケートの全体集計

17.5.1. 被験者アンケートから見た被験者全体の開封状況

以下では、被験者企業 B から被験者企業 N までのすべての被験者について、被験者アンケートへの回答内容を集計し、さまざまな指標についてどのような傾向があるかを分析した。

ただし、以下で扱う被験者アンケートは、被験者全体の 2,603 名から被験者企業 A の 428 名を除いた 2,175 名の被験者に対して実施したもので、このうち 1,089 名(50.0%)から回答を得た。この状況を図 136 に示す。
ここで、被験者企業 A を分析の対象から除いたのは、被験者アンケートの設問が相当異なるためである。
なお、設問によっては一部の被験者企業で回答を得られなかった場合があるが、この差は僅少なのでここでの分析の対象としている。

図 136 被験者全体：被験者アンケートの回収率

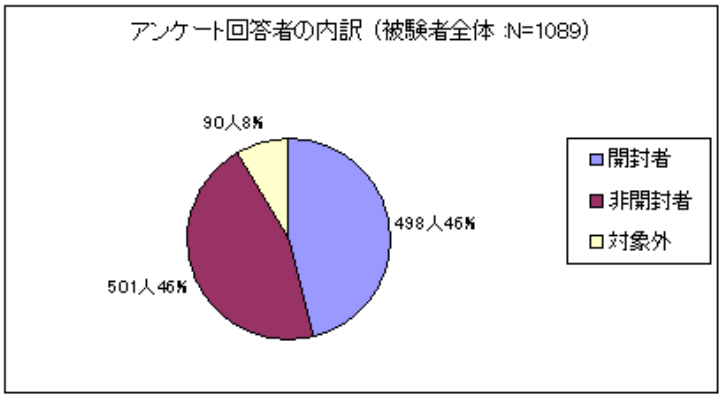


被験者アンケートの回答に有効回答と無効回答があるのは前述の通りである。有効回答を開封者と非開封者に分類した上で、無効回答と併せて図 137 に示す。

この図に見えるように、有効回答者は 999 名(回答全体の 1,089 名に対して 91.7%)であり、このうち開封者は 498 名(回答全体に対して 45.7%、有効回答に対して 49.8%)、非開封者は 501 名(同、46.0%と 50.2%)である。

したがって、有効回答者数の約半分が開封者であり、残り半分が非開封者であることがわかる。

図 137 被験者全体：被験者アンケートによる開封状況



17.5.2. 被験者全体の開封状況と傾向分析

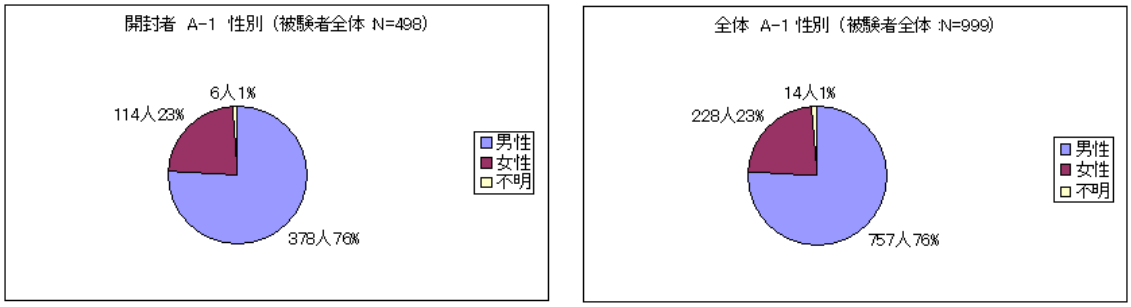
以下では、被験者アンケートの様々な設問について、有効回答者全体での構成比と開封者の構成比を比較して傾向を分析した。

しかし、詳細は後述するが、どの属性を使っても構成比に大きな差が見られなかった。したがって、どのような属性を持つ被験者が標的型メール攻撃に耐性を持つのか、あるいは、耐性がないのかという分析では、今年度の予防接種では確たる結論を得るに到らなかったと言える。

左右に円グラフが並ぶ場合は、右側が有効回答者全体を示し、左側が開封者を示す。積み上げ棒グラフは、検討した属性ごとに開封者と非開封者がどのような割合になるかを示すものである。

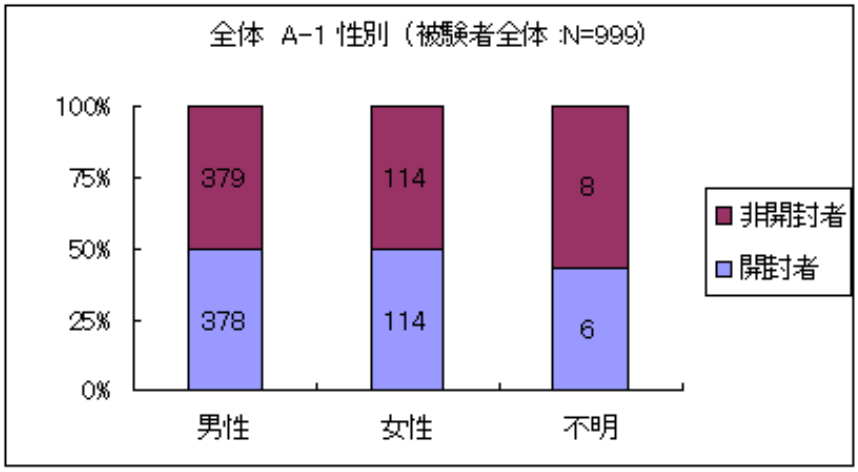
被験者アンケートの設問 A-1 では被験者の性別を訊いているので、その構成比を図 138 に示す。
有効回答者と開封者で構成比がほぼ同じなので、性別によって開封率が異なるとは言えない。

図 138 被験者全体：有効回答者と開封者の性別構成比



男性・女性それぞれについて開封者・非開封者の構成を見ても、図 139 に示す通り、特に偏りがあるとは言えない。

図 139 被験者全体：性別の開封・非開封



同様に、図 140 と図 141 で設問 A-2 から年齢層による開封率の偏りを調べたが、特に偏りがあるとは言えない。

60 歳代で開封率が高いように見えるが、母数が少ないので即断するのは危険である。

図 140 被験者全体：有効回答者と開封者の年齢層別構成比

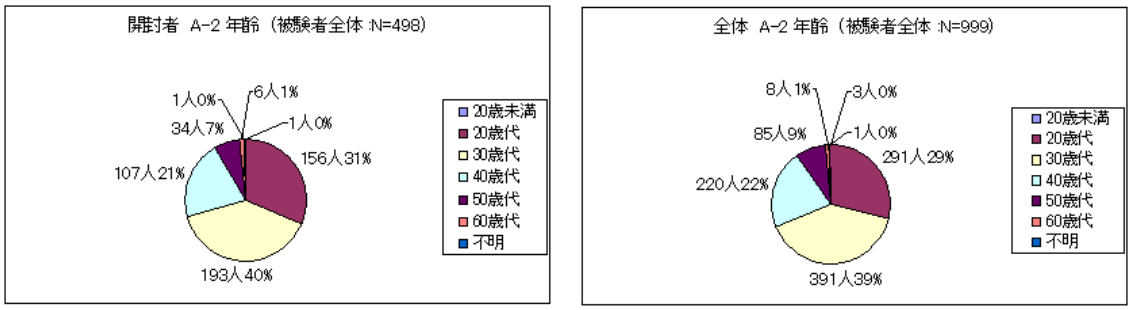
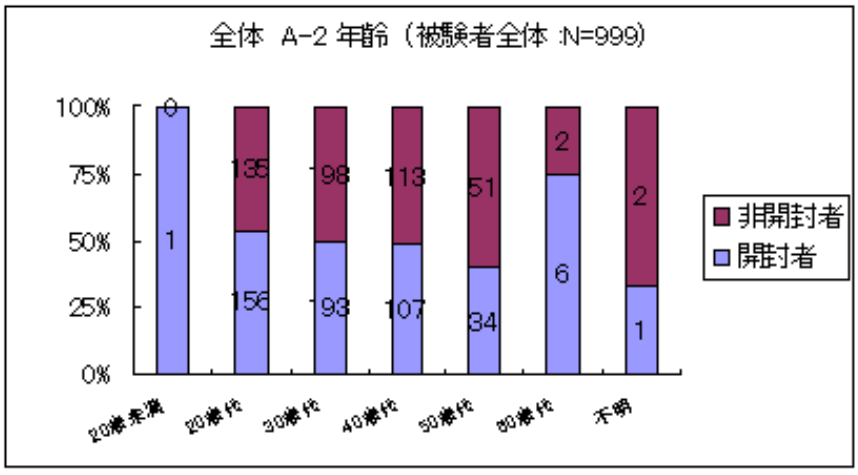
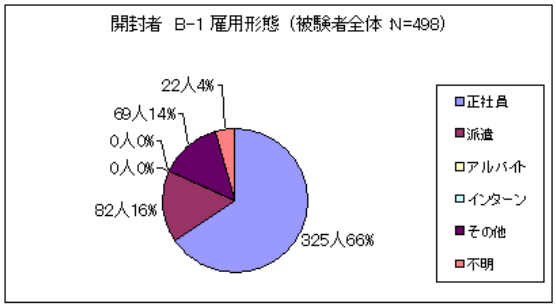


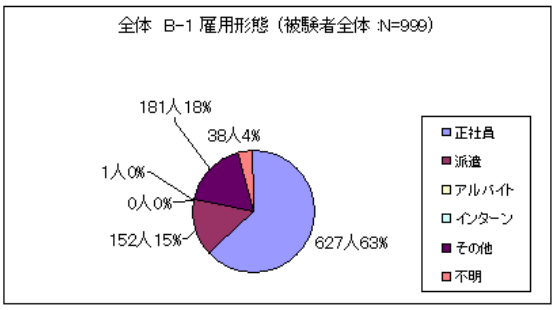
図 141 被験者全体：年齢層別の開封・非開封



正社員や派遣労働者などの雇用形態別では、有効回答者に占める割合が、開封者に占める割合とほぼ同じである。したがって、雇用形態が異なっても開封率に偏りがあるとは言えない。

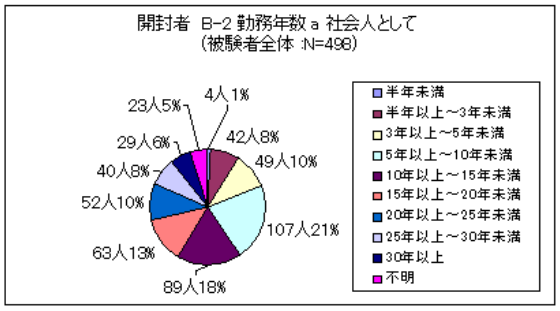
図 142 被験者全体：有効回答者と開封者の雇用形態別構成比

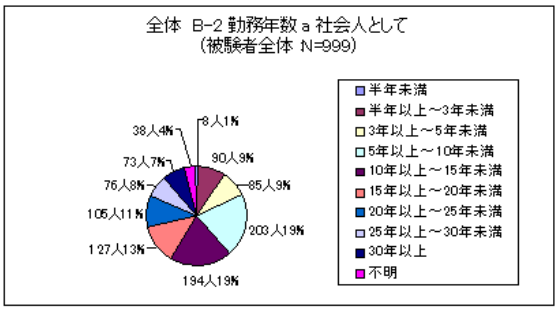




社会人としての勤務年数別で比較しても、有効回答者と開封者の間に、特に偏りは見られない。

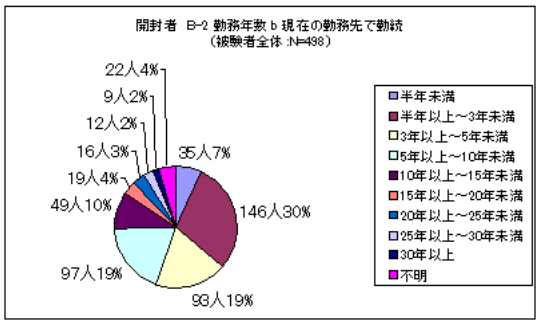
図 143 被験者全体：有効回答者と開封者の社会人勤務年数別構成比

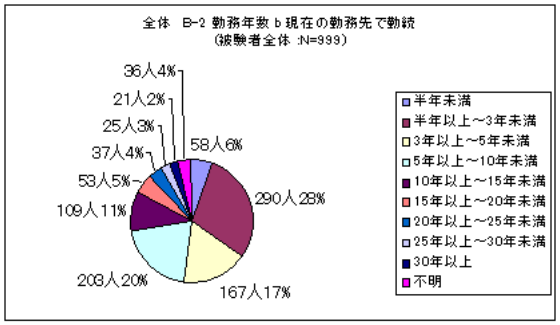




現在の勤務先での勤続年数別で比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 144 被験者全体：有効回答者と開封者の勤続年数別構成比





役職別で比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 145 被験者全体：有効回答者と開封者の役職別構成比

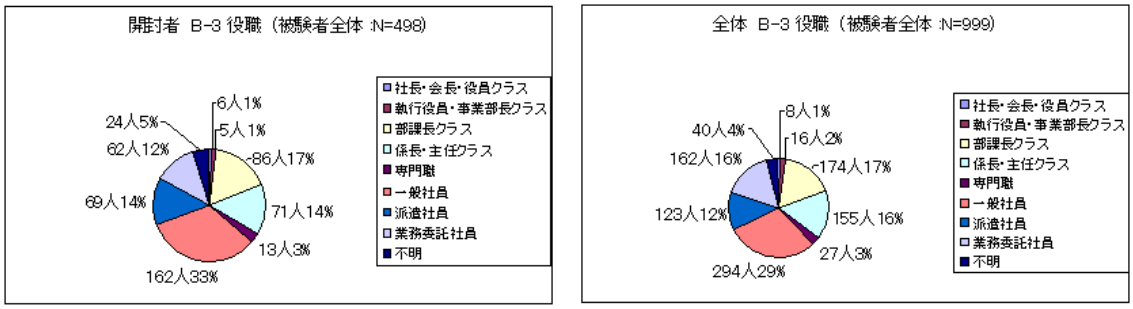
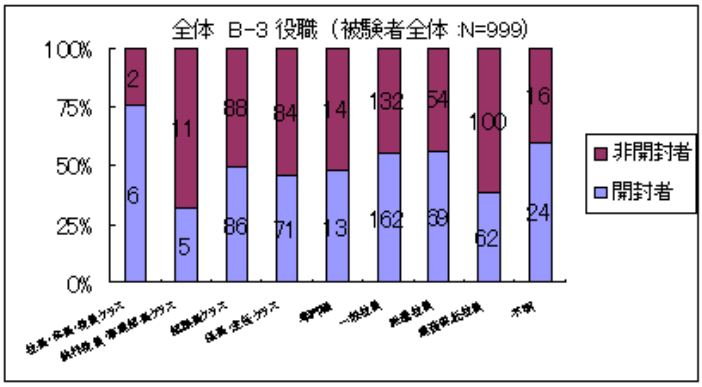


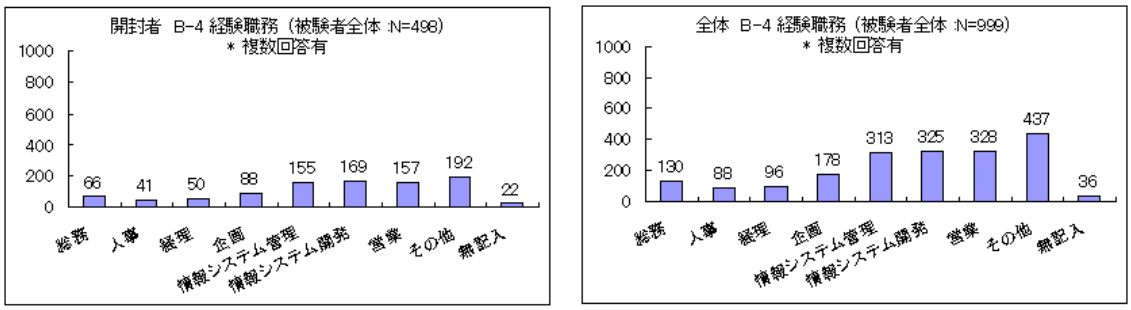
図 146 被験者全体：役職別の開封・非開封



経験職別で比較しても、有効回答者と開封者の間に、特に偏りは見られない。

特に、情報システム関連の職務経験があっても、他の職務経験と比べて開封率に差はない。

図 147 被験者全体：有効回答者と開封者の経験職務別構成比



標的型攻撃メールを知っていたかどうかで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 148 被験者全体：有効回答者と開封者が標的型メール攻撃を知っていたか

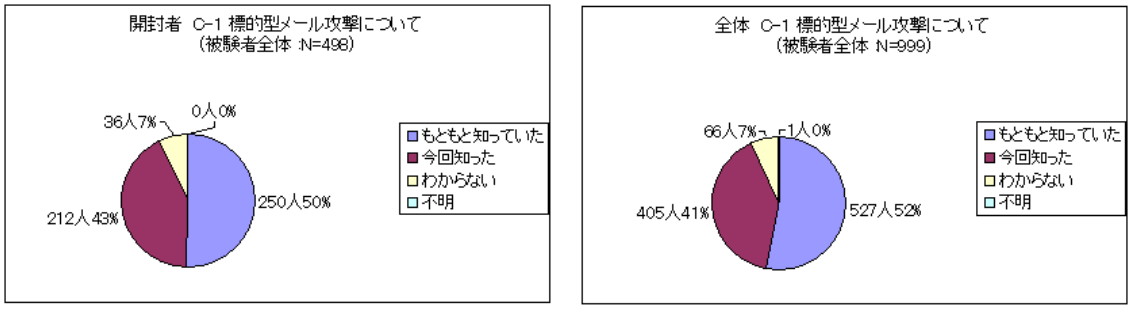
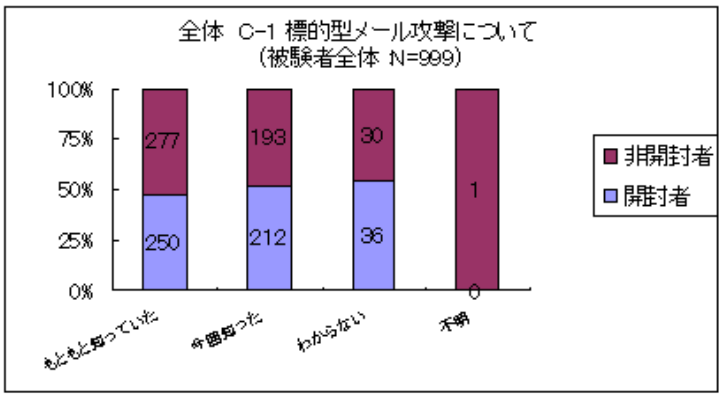


図 149 被験者全体：標的型メール攻撃を知っていたかどうかによる開封・非開封



今後、組織に攻撃があると思うかどうかで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 150 被験者全体：有効回答者と開封者が今後組織に攻撃があると思うか

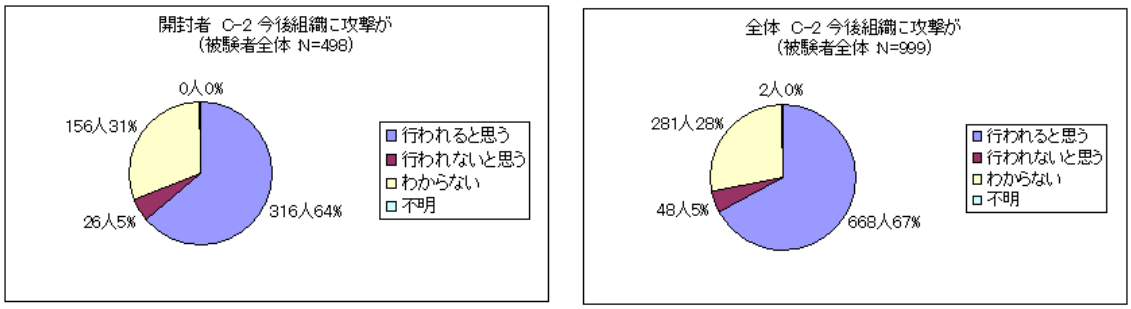
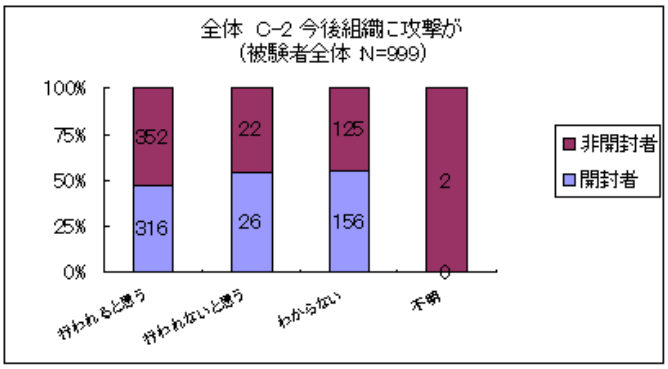
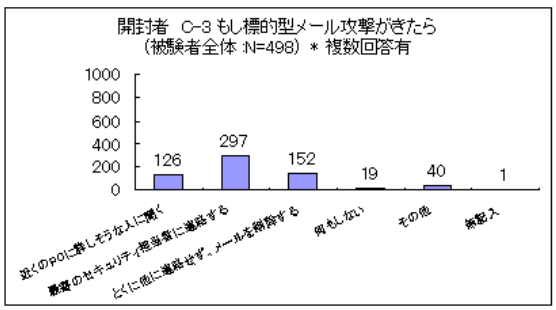


図 151 被験者全体：今後組織に攻撃があると思うか否かによる開封・非開封



もし標的型攻撃メールが来たらどうするかで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 152 被験者全体：有効回答者と開封者は、もし標的型メール攻撃が来たらどうするか



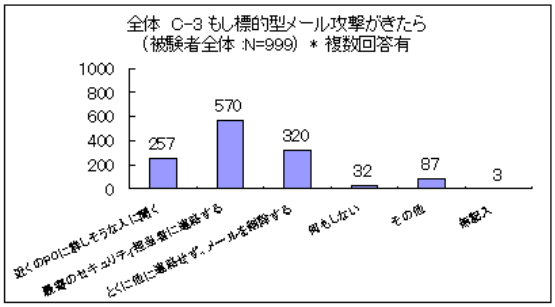
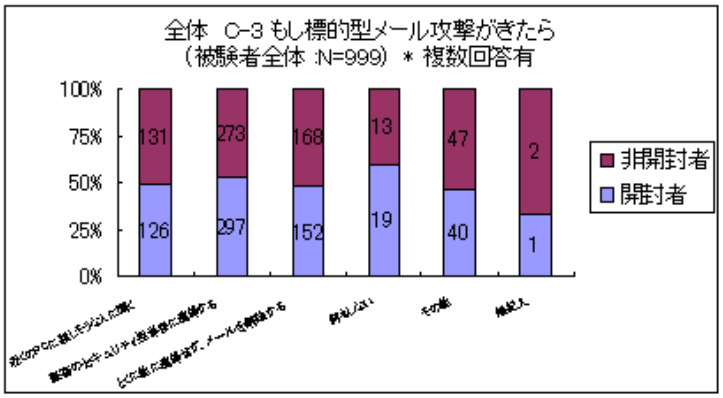


図 153 被験者全体：もし標的型メール攻撃が来たらどうするかによる開封・非開封



PC の利用経験年数で比較しても、有効回答者と開封者の間に、特に偏りは見

られない。

図 154 被験者全体：有効回答者と開封者の PC 利用経験別構成比

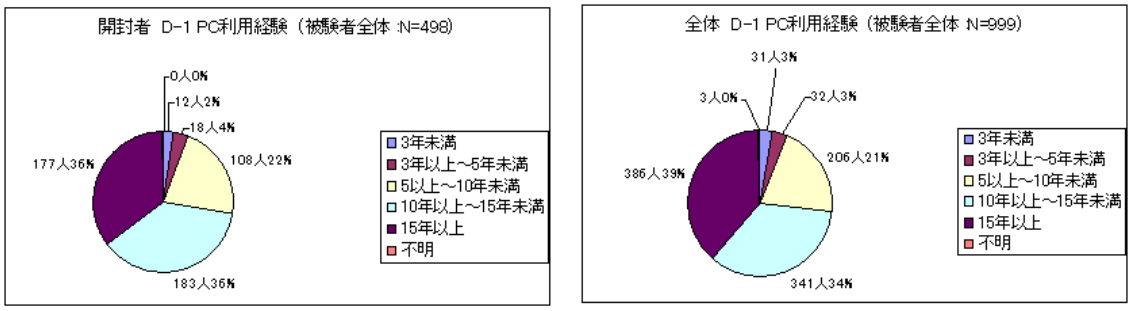
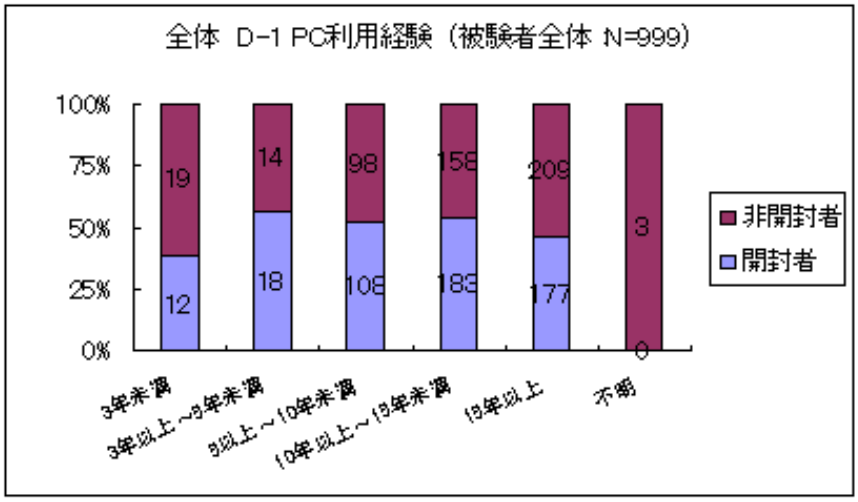


図 155 被験者全体：PC 利用経験別の開封・非開封



使用しているメールソフトで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 156 被験者全体：有効回答者と開封者の使用メールソフト

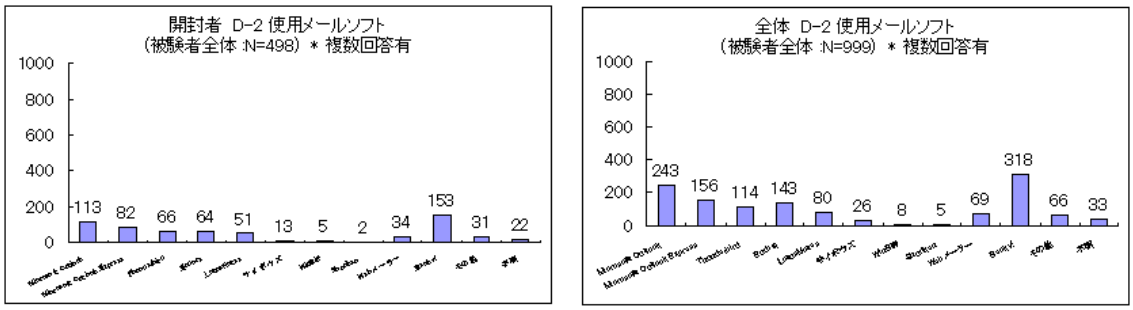
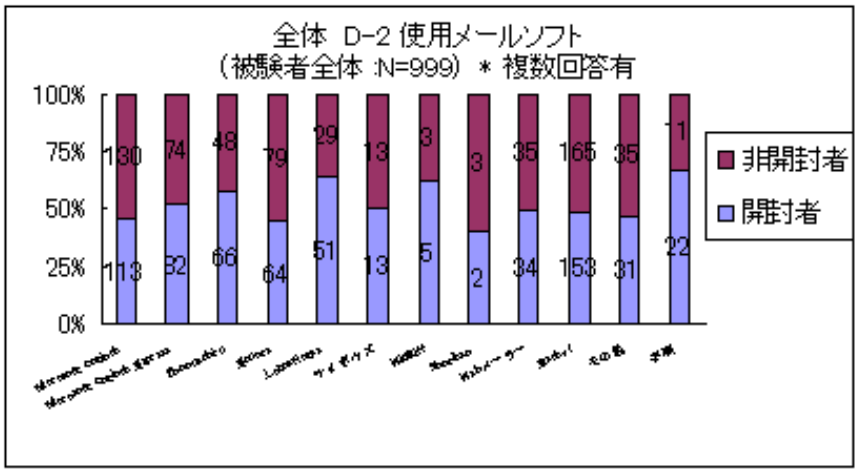
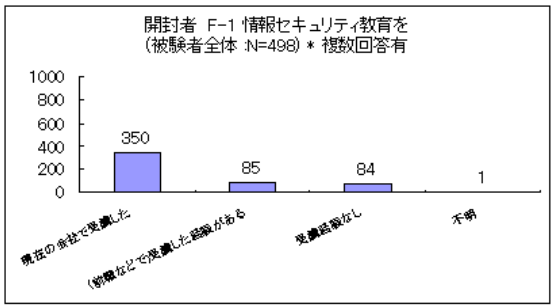


図 157 被験者全体：使用メールソフト別の開封・非開封



情報セキュリティ教育の受講経験で比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 158 被験者全体：有効回答者と開封者の情報セキュリティ教育受講経験



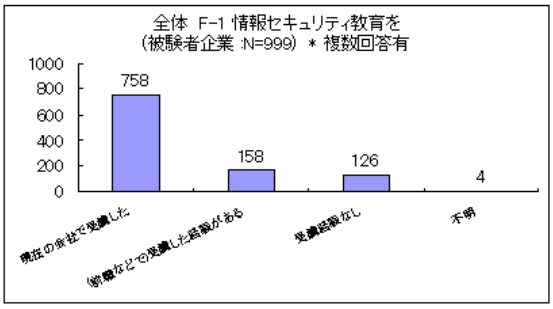
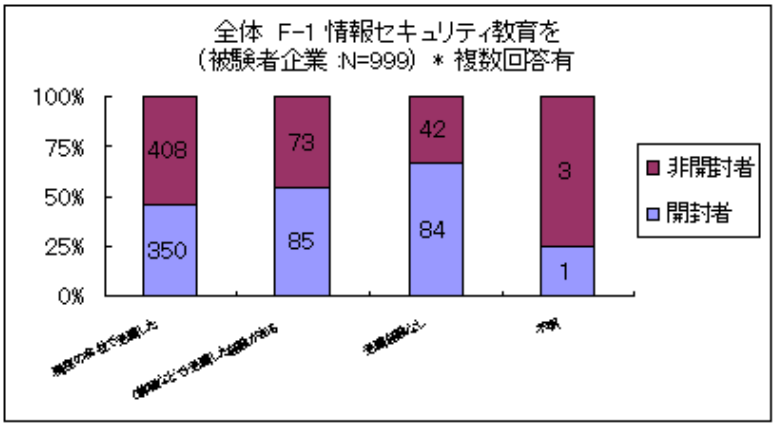


図 159 被験者全体：情報セキュリティ教育の経験別の開封・非開封



情報セキュリティ教育が役に立ったかどうかで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

ただし、開封者では、役に立たなかったと思っている被験者数がやや多いように思われるが、心理的に当然こう思うので傾向としては取り上げないことにした。

図 160 被験者全体：有効回答者と開封者にとって情報セキュリティ教育が役に立ったか

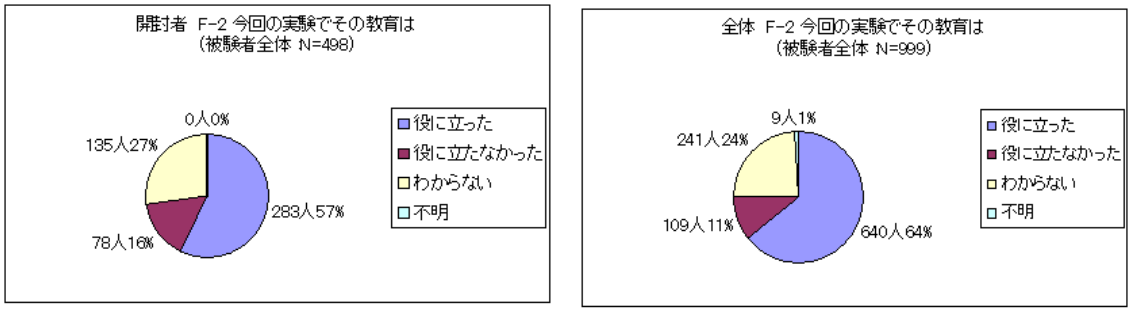
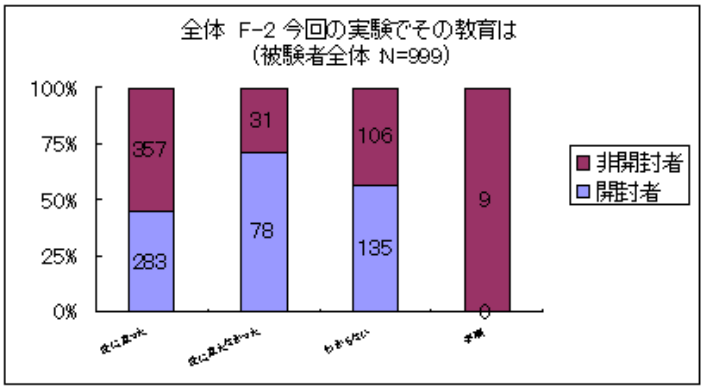


図 161 被験者全体：情報セキュリティ教育が役に立ったか否かと開封・非開封



今後、今回のようなメールを受けたらどうするかで比較しても、有効回答者と開封者の間に、特に偏りは見られない。

図 162 被験者全体 : 有効回答者と開封者は今後このようなメールを受けたらどうするか

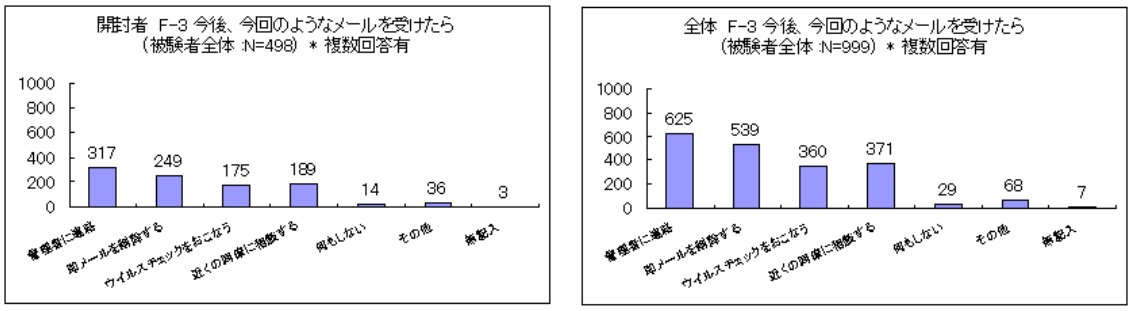
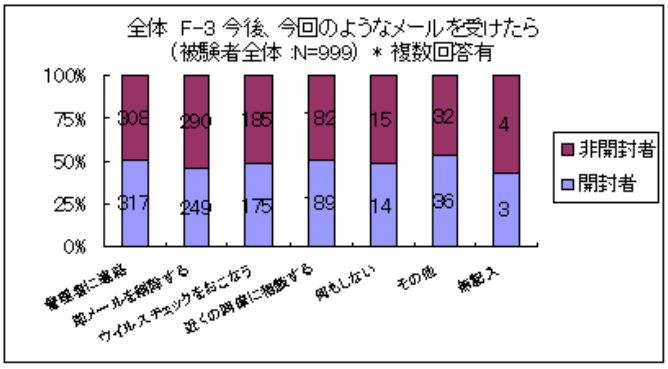


図 163 被験者全体 : 今後このようなメールを受けたらどうするかと開封・非開封



17.6. インシデント報告に関する分析

予防接種を実施するということは、被験者が擬似攻撃メールを受けとるということであり、その被験者企業でのインシデント報告の機序に対して(擬似的な)起動契機を与えることになる。

今年度の予防接種では被験者アンケートおよび被験者企業アンケート・被験者企業インタビューを実施しているので、予防接種の本来の目的とは別に、各被験者企業のインシデント報告が実際にどの程度動作するものかを知ることができる。

以下では、被験者アンケートの設問 F-3 への回答状況から、この点について検討する。

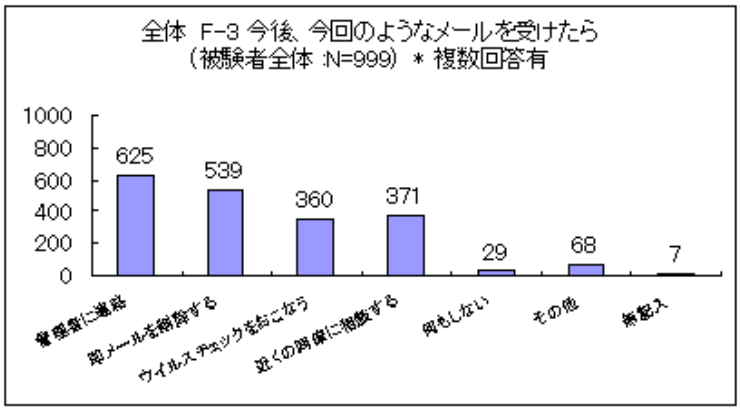
一般に、標的型メール攻撃のような不審なメールを受け取った場合には、それ以上の操作を行わずに証拠を保全し、定められた手順でインシデント報告を行うことが望ましい。

これは、その不審なメールがなんらかの攻撃またはその一部であった場合に、CSIRT もしくは社内でセキュリティ対応を行う担当部門が的確に状況を把握できるようにするためである。

他方で、軽微なものまでインシデント報告を行って証拠保全をしていると、本来の業務に差し障るという現実も無視できない。
こららの相反する条件を調停して、現実的で効果的なセキュリティ対策・体制を築くことが理想ではあるが、なかなかそうも行かないのが実情であろう。

さて、被験者アンケートの設問 F-3 に対する回答は図 164 のようになっている。
なお、ここでの有効回答者数 999 名は、被験者企業 B から被験者企業 N までを集計したものであり、被験者企業 A については被験者アンケートの設問が異なるために分析対象外としている。

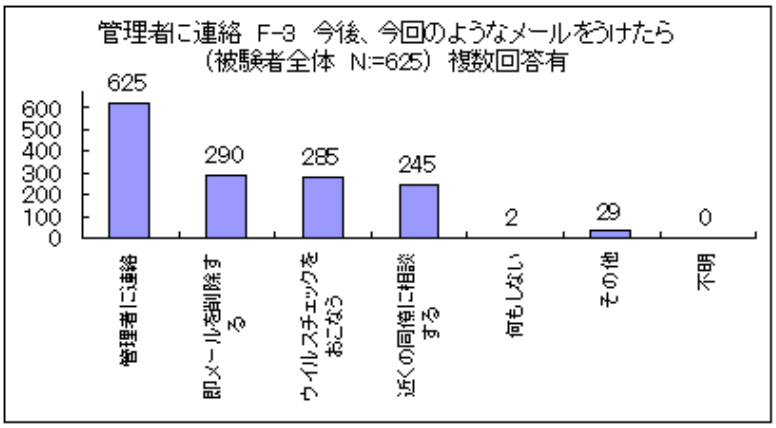
図 164 被験者全体：今回のようなメールを受けたらどうするか



被験者アンケートの有効回答者は 999 名であり、このうち、「今後、今回のようなメールを受けたら管理者に連絡する」と回答した被験者は 625 名(62.6%)である。
設問 F-3 は複数回答を許すので、この他にも多くの被験者が選択した選択肢があり、多い順に「即メールを削除する」の 539 名(54.0%)、「近くの同僚に相談する」の 371 名(37.1%)、「ウイルスチェックを行う」の 360 名(36.0%)である。

ここで、管理者に連絡すると回答した被験者 625 名に注目して、その回答状況を抽出すると、図 165 の通りとなる。

図 165 被験者全体：今後、今回のようなメールを受けたら管理者に連絡する被験者の回答状況



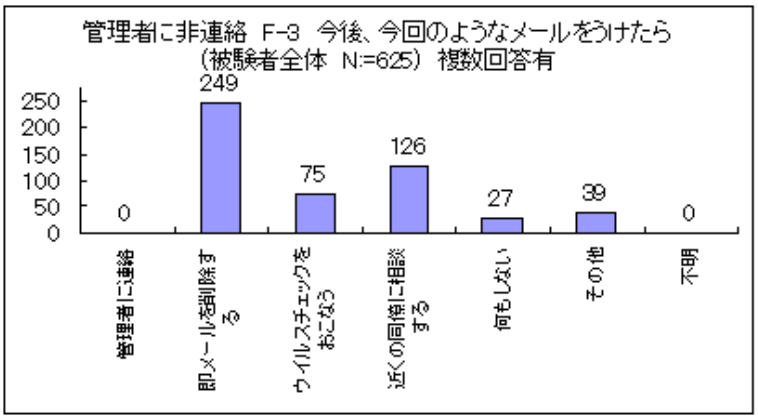
管理者に連絡すると回答した被験者 625 名のうち、290 名(46.4%)が「即メールを削除する」と回答していることがわかる。この他、ウイルスチェックをすると回答した被験者は 285 名(45.6%)、近くの同僚に相談すると回答した被験者は 245 名(39.2%)である。

先述の通り、インシデント・ハンドリングに当たっては証拠保全が重要であるが、この回答状況ではインシデント報告のうちの約半数は既にファイルを削除した後で、証拠となるものが残っていない[10]ことになる。

他方で、管理者に連絡すると回答しなかった被験者 374 名に注目して、その回答状況を抽出すると、図 166 の通りとなる。

[10] 削除されたファイルを復元する手法などを使って証拠を確保することが可能である場合があるが、ここでは深入りしない。

図 166 被験者全体：今後、今回のようなメールを受けても管理者に連絡しない被験者の回答状況



管理者に連絡すると回答しなかった被験者 374 名のうち、249 名(66.6%)が、「即メールを削除する」と回答している。この他、ウイルスチェックをすると回答した被験者は 75 名(20.1%)、近くの同僚に相談すると回答した被験者は 126 名(33.7%)である。

管理者に連絡すると回答した被験者と比べて、そうでない被験者では、「即メールを削除する」の比率が跳ね上がっており、「何もしない」も増えている。逆に「ウイルスチェックを行う」の比率は大きく下がっており、「近くの同僚に相談する」の比率も下がっている。

管理者に連絡すると回答しなかった被験者は、不審なメールだと思えばとにかく削除する傾向にあり、管理者への報告だけでなくウイルスチェック・同僚への相談なども含めて、望ましい反応を示さない傾向がある。

管理者へのインシデント報告義務を周知徹底するということは、不審なメールへの基本的な対応方法についても同様に周知徹底されていることを意味していると言えるだろう。

17.7. 保有情報数に関する分析

17.7.1. 保有情報の状況

ここでは、被験者アンケートの保有情報に関する設問(E-1, E-2, E-3)に対する回答から、各被験者が抱える機密情報の状況を分析する。

ただし、被験者アンケートの設問が異なる被験者企業 A と、諸般の事情でこれらの設問に回答を得られなかった被験者企業 J を分析の対象から除外している。

全被験者について、保有情報の数を平均すると表 85 の通りとなる。

なお、各保有情報の「有効回答数」には、保有数が 0 であると回答した被験

者も含んでいる。同様に、「平均保有数」は保有数 0 の被験者も含めた平均値である。

表 85 被験者全体：保有情報の平均

分類	被験者アンケート有効回答数	個人情報		顧客契約		社内秘密	
		有効回答数	平均保有数	有効回答数	平均保有数	有効回答数	平均保有数
B-N	999	933	553.0	939	1215.3	925	343.2

この中には極端に大きな数値を回答した被験者もいるので、これらの平均保有数をそのまま信じて良いかどうかには議論の余地があるが、それでもなんらかの目安にはなるだろう。

これによれば、被験者一人当たり平均 553 件の個人情報を保有しており、顧客との契約などについては平均 1215 件、社内秘の情報は平均 343 件を保有していることになる。

17.7.2. 保有情報に関する想定損害賠償額試算

さて、仮に本物の標的型攻撃メールによってこれらの保有情報が漏洩したとすれば、その損害賠償額はどのような金額になるだろうか。

ここでは、JNSA[11]の「2007 年度 情報セキュリティインシデントに関する調査報告書」[12]を参考にして、想定損害賠償額を計算する。

まず、同報告書によれば、個人情報が漏洩した場合の 2007 年度の「一人当たり平均想定損害賠償額」は 39,017 円となっている。

被験者一人当たり平均 553 件の個人情報を保有しているので、平均想定損害賠償額は 21,576,401 円となって二千万円を越える金額となる。

また、同報告書では平均想定損害賠償額の算出式を定義しており、これによれば、個人情報漏洩事故における一件当たりの想定損害賠償額は、次のように計算できる。

ただし、保有している個人情報としては名刺程度の情報を想定した。また、計算手法の詳細については同報告書を参照されたい。

(想定損害賠償額) = (基礎情報価値 [500 円/件])
× (機微情報度 [2])
× (本人特定容易度 [3])
× (情報漏洩元組織の社会的責任度 [2])

[11] NPO 日本ネットワークセキュリティ協会 (http://www.jnsa.org/)
[12] http://www.jnsa.org/result/2007/pol/incident/index.html から入手可能。

× (事後対応評価 [1])
＝ 6,000 円/件

これによれば、553 件の個人情報が漏洩した場合には、3,318,000 円の損害賠償額を想定する必要がある。

これらふたつの想定損害賠償額は大きく異なるが、いずれにしても数百万円以上の金額を想定しなければならないことは確かであろう。

その他の保有情報については適当な計算式が見当たらないので、想定損害賠償額を計算することはできないが、少なくとも個人情報の想定損害賠償額よりは大きい金額になるだろう。

標的型メール攻撃によって被験者の PC が乗っ取られれば、このような金額の損失を想定しなければならないのである。

なお、ここでは被験者企業にとっての想定損害賠償額を試算したが、個人のクレジットカード番号やオンライン銀行口座の ID/パスワードなどを狙う標的型メール攻撃も多いので、個人の PC やメールアカウントについても相応の注意が必要である。

17.7.3. 被験者企業の属性別の保有情報数

ここでは、17.3 節での分類にしたがって被験者企業を分類し、保有情報数にどのような傾向が認められるかを分析した。
しかし、一部の被験者が極端に大きな数値を回答していることもあって、整合性のある推論はできなかった。

まず、IT 系被験者企業と非 IT 系被験者企業に分類した。それぞれの保有情報数を表 86 に示す。

表 86 被験者全体：IT 系/非 IT 系別の保有情報数

分類	被験者アンケート有効回答数	個人情報		顧客契約		社内秘密	
		保有者数	平均保有数	保有者数	平均保有数	保有者数	平均保有数
IT 系	753	720	442.1	726	1563.5	719	384.2
非 IT 系	246	214	925.5	213	28.4	206	200.3

個人情報の平均保有数では非 IT 系企業の方が多い結果となっているが、顧客契約や社内秘密では IT 系企業の方が多い。

次に、IS27001 またはプライバシーマークの認証を取得しているか否かで分類した結果を表 87 に示す。

表 87 被験者全体：認証取得状況と保有情報数

分類	被験者アンケート有効回答数	個人情報		顧客契約		社内秘密	
		保有者数	平均保有数	保有者数	平均保有数	保有者数	平均保有数
認証あり	736	674	413.8	677	1676.1	666	347.9
認証なし	263	259	915.3	262	24.3	259	331.3

認証取得の有無で分類した場合も、傾向としては IT 系/非 IT 系別の場合とよく似ている。

さらに、CSO を任命しているか否かで分類した結果を表 88 に示す。

表 88 被験者全体：CSO 任命状況と保有情報数

分類	被験者アンケート有効回答数	個人情報		顧客契約		社内秘密	
		保有者数	平均保有数	保有者数	平均保有数	保有者数	平均保有数
CSO 有り	817	753	429.9	758	1497.7	747	370.5
CSO 無し	182	180	1068.0	181	32.3	178	228.8

CSO 任命の有無で分類した場合も、傾向としては IT 系/非 IT 系別の場合とよく似ている。

最後に、メールアカウント即時停止措置の有無で分類した結果を表 89 に示す。

表 89 被験者全体：メールアカウント即時停止措置の有無と保有情報数

分類	被験者アンケート有効回答数	個人情報		顧客契約		社内秘密	
		保有者数	平均保有数	保有者数	平均保有数	保有者数	平均保有数
即時停止有り	342	294	537.2	296	28.7	292	155.4
即時停止無し	657	639	560.3	643	1761.5	633	429.9

メールアカウントの即時停止措置の有無で分類すると、どの保有情報も同措置のない企業の方が保有情報数が多い結果となった。

17.8. 発見事項と教訓

17.8.1. 事前教育の重要性

予防接種における事前教育とは、前後 2 回の擬似攻撃メール配信よりも前に「標的型メール攻撃とはどのようなものか」・「標的型メール攻撃が流行していること」・「迂闊に添付ファイルを開くと危険な場合があること」を被験者に教育・周知することを指している。
ただし、「予防接種という擬似的な攻撃を行うこと」自体は、被験者には伝えないことを原則としている。

昨年度の予防接種では、ある被験者企業で事前教育を実施しない(以下、抜き打ち)ままに擬似攻撃メールを配信したところ、被験者の心証を害してしまって予防接種を最後まで実施できなかったと聞く。

今年度の予防接種においても、抜き打ちで擬似攻撃メールを配信した被験者企業で同様の事象が発生し、被験者アンケートの実施が大幅に遅れる結果となった。このケースでは、窓口担当者のご尽力で最終的には被験者アンケートを実施できたので事なきを得たが、事前教育の重要性を再確認することとなった。

これらのケースを見ると、抜き打ちの予防接種が問題になる被験者企業には、次のような特徴があるようである。

1. 情報通信や情報技術に関連した業種で、IT やセキュリティに関するスキルの高い被験者が比較的多い。
2. 非常に専門的な業務である。
3. 個々の担当者の業務が比較的独立している。

事前教育を実施することでこのようなリスクを避けることができるだけでなく、予防接種での体験をより深く理解していただくためにも有効である。
今後の予防接種においても、事前教育の重要性を引き続き強調するべきである。

17.8.2. 開封を誘う要因

被験者アンケートの自由記述欄を見ると、開封者も非開封者も、最初に擬似攻撃メールの本文と表題を見て、その印象(だけ)から当該メールの怪しさを判断している場合が多いことがわかる。
したがって、開封率の大小には「メールの本文や表題が被験者のおかれている状況とどれだけ合致するか」が大きく影響する。
また、メールを処理する際に、業務が多忙であれば注意力が散漫となって開封率を大きくする方向に働く。
さらに、差出人の表示名やメールアドレスがメールソフト上でどのように表

示されるかによっては、気付きのポイントをみすみす失う結果となる。すなわち、擬似攻撃メールはほとんどの場合にフリーメールのメールアドレスを送信者として送信したが、メールソフトが表示名だけを表示する場合には気付かないことがほとんどである。

これらを裏付ける記述が、被験者アンケートの自由記述欄にいくつか現れるので、以下にまとめておく。

1. 表題や本文の内容が自分の担当業務に関係があると思い、疑わなかった。
2. 差出人の表示名が自分の知っている人物・部署であったので疑わなかった。(この場合、差出人のメールアドレスを確認していないことが多い。)
3. 宛先の表示名に自分の名前があったので疑わなかった。
4. 標的型メール攻撃などのメールによる攻撃は英文メールだけに気を付けていればよいと誤信していた。

特に、メールソフトによっては差出人のメールアドレスが表示されないという点には、予防接種によって初めて気付いた被験者も多い。

今回の予防接種に出現したメールソフトは、そのほとんどがリスト表示の段階では差出人の表示名だけを表示する。

また、メール本文を表示させると、差出人のメールアドレスを表示するものもあれば、そうでないものもある。例えば、Outlook Express は、メール本文を表示させると、差出人の表示名は表示する者の、そのアドレスは表示しない。Thunderbird は、アドレス帳に登録があれば表示名だけを表示する。Outlook 2007 は「表示名[メールアドレス]」の形で表示する。(いずれも標準設定)

被験者アンケートへの回答の中にも、この点に気付いた被験者の声が散見される。設定変更やメールソフトの入れ換えで対応するべきであるとの声も合った。

また、差出人のメールアドレスと Received:ヘッダを比較して、いわゆる From:詐称の有無を確認しようとしても、多くのメールソフトでは Received:ヘッダの表示に手間がかかり、コンピュータリテラシの低い被験者がこの確認方法を理解し実践することは望むべくもない。

このような傾向から見て、各個人の「見抜く力」を向上させることが重要であるが、差出人のメールアドレスを表示する設定を強制するなどの技術的な対策も必要である。

ソーシャルエンジニアリングを用いた標的型攻撃メールに対しては、技術的解決策やスキル向上だけでは万全とは言えないが、ある程度のレベルまでベースラインを上げていく努力は必須であろう。

被験者アンケートへの回答の中には、業務の都合上、どのようなメールでも対応せざるを得ない場合があるという指摘もあったが、このような場合には、安全にファイルを開くための隔離環境を用意すると良いかも知れない。

17.8.3. 予防接種の限界

標的型メール攻撃に対する耐性を強化するために、今年度も予防接種を実施してその効果を見てきた。

予防接種を行うことで、被験者が標的型メール攻撃の脅威を体感することができ、また、それまでに受けた情報セキュリティ教育の内容を浸透させるのによい機会となることは、この報告書でも見てきたとおりである。

しかし、一方で、多くの被験者が擬似攻撃メールの添付ファイルを開封しており、ある程度の確率で攻撃側の目的が達成できることもまた、事実である。

さらに、今年度の予防接種で使用した擬似攻撃メールよりも「よくできた」攻撃メールを作成することは比較的容易であり、そのような標的型メール攻撃が実行されれば、これを完全に阻止する手段は存在しないだろう。

また、予防接種を実施することである程度の効果は見込めるとしても、あらゆる状況で完璧な対策となっているわけではなく、むしろ、標的型メール攻撃に対する縦深防御の一部をなすと考えるべきである。

さらに、予防接種で学んだことも、時間が経過すれば風化せざるを得ないので、継続的な取り組みが必要である。

さらに、予防接種の教育効果を高めるためには、擬似攻撃メール配信の前後の教育が非常に重要である。予防接種の枠組みの中では事前教育の重要性を強調しているが、もっと詳しい教育プログラムを予防接種の前後に実施することが望ましい。この教育プログラムは、標的型メール攻撃の仕組み・騙しのテクニック・流行の程度・被害の実態・気付きのポイントなどを網羅するべきである。

17.8.4. 予防接種の教育的コンテンツに関する問題点

ここでは、予防接種における教育コンテンツがどれほど有効であるかについて検討する。

今年度の予防接種では、以下のような教育コンテンツを被験者に届けている。それぞれのコンテンツの詳細については、2 章に詳しく記述した。

1. 被験者全員に対して、事前教育を実施する。
2. 開封者は、擬似攻撃メールの添付ファイルの内容を読む機会がある。

3. 被験者全員に対して種明かしメールを配信する。

なお、この他に擬似攻撃メール受信体験が教育コンテンツとして挙げられるが、ここでは問題にしない。また、被験者企業が自ら実施する情報セキュリティ教育についてもここでの検討の対象としない。

さて、この報告書では、添付ファイルの開封状況によって、被験者を開封者⑫・開封者①・開封者②・非開封者に分類した。

このうち、開封者⑫は非常に問題で、次のケースが考えられる。

1. 教育コンテンツを読み飛ばすので、毎回被害を受ける。
2. 教育コンテンツを読むが理解できず、毎回被害を受ける。

前者については、そもそも興味がないか、自分にはわからないと思いこんでいるか、あるいは、予防接種における教育コンテンツを読み始めて訓練だとわかったために以後の解説を読むことを放棄した場合もあるだろう。
いずれにしても、教育コンテンツをただ届けるだけでは足りず、なんらかの方法で被験者本人の意識付けをする必要がある。(以下、意識付けの問題と呼ぶ。)

後者については、標的型メール攻撃について、また、その背景となる IT 技術や IT セキュリティ全般について、さらに教育をしていく必要がある。この場合、当該被験者の知識・能力の問題で理解できない(以下、スキルの問題と呼ぶ)ケースと、それなりのスキルはあったが教育コンテンツが不出来で理解できない(以下、コンテンツの問題と呼ぶ)ケースがあるだろう。

開封者①は、予防接種の被験者としては理想的に見える。
しかし、この中には、「第 2 回配信では、表題や本文だけを見て自分とは関係のないメールだと判断したので、添付ファイルを開封することがなかった」という単に幸運であった被験者が含まれているだろう。開封者①は、事前教育や第 1 回配信時の添付ファイルを呼んでいるはずなので、この場合にも、意識付けの問題・スキルの問題・コンテンツの問題が含まれているだろう。

開封者②は、その多くが第 1 回配信では単に幸運であった被験者であろう。開封者②は、すくなくとも事前教育のコンテンツを読んでいるはずなので、意識付けの問題・スキルの問題・コンテンツの問題を考えざるを得ない。

非開封者は、「標的型メール攻撃について熟知していて、擬似攻撃メールをそれと見破った」のであれば全く問題ないが、単に幸運であった被験者も多く含まれるのではないか。

このような意識付けの問題・スキルの問題・コンテンツの問題があるだろう

と思われる回答が、被験者アンケートへの回答にも散見されるのである。

予防接種で用いる教育コンテンツの改善を図るとともに、被験者企業とともに被験者の意識付けや基礎教育に注力する必要があるだろう。

17.8.5. 被験者アンケートの設問

今年度の予防接種では被験者アンケートを実施して、個々の被験者に対してその属性や擬似攻撃メール受信時にどのように行動したか、また、今後同様のメールを受け取った場合にどのように行動するつもりかなどを尋ねた。
被験者アンケートの結果はこの報告書に記述したとおりであるが、来年度の予防接種に向けて反省するべき点を列挙する。

1. 設問数が多く、回答する側にも集計する側にも負担が大きい。
2. 機械的処理のできない自由記述欄が多く、集計する側の負担が大きい。
3. 解釈の余地が不必要に大きい設問があり、回答する側の迷いを招く。
4. 選択肢が不完全で、回答する側がひとつも選択できない場合がある。
5. 気付きのポイントを列挙して、どのポイントに気付いたかを問うべきである。これは、被験者への教育コンテンツとしての側面も持つことになる。しかし、擬似攻撃メールの定型化が必須となる。
6. Web アンケートのシステム作成が遅れたために、MS-Excel シートで代替した場合がある。被験者企業によっては外部の Web サーバへのアクセスを禁止している場合があるので、結局は両方を準備する必要がある。

いずれも被験者アンケートの設計や運用があまりうまくいかなかったということであり、大いに反省するべきであると認識している。

17.8.6. 攻撃ベクトルの拡充

予防接種では、擬似攻撃メールの表題・差出人の表示名・本文などにソーシャルエンジニアリングの手法を適用し、添付ファイルの開封へ誘導するという攻撃ベクトルを用いた。
予防接種で用いる添付ファイルは開封しても Web ビーコンが作動するだけであるが、本物の標的型メール攻撃ではマルウェアに起動契機を与えてしまうのである。

現時点の予防接種では、添付ファイルとして MS-Word のファイルを採用しているが、ファイル形式の種類を増やすことは重要である。

業務上やりとりするメールに一般的に添付されるファイル形式としては、MS-Excel などの MS-Office 系のものや PDF・ZIP などが多いと考えられる。
したがって、攻撃ベクトルとしてもこれらのファイル形式を使えるようになれば、より多彩なかたちで予防接種を実施できるようになる。

また、広義の標的型メール攻撃では、HTML メールに埋め込んだハイパーリンクから Web サイトへ誘導し、そこからマルウェアをダウンロードさせるという攻撃ベクトルも使われている。プレーンテキストのメールに URL を書いておけば、MUA が自動的にハイパーリンクとして解釈してくれる場合もある。
予防接種手法で、これらの攻撃ベクトルを擬似的に実施することも有望である。

17.8.7. インシデント報告体制の有効性評価

予防接種を実施することで、副次的に、被験者企業内のインシデント報告体制がどの程度実働するのかを確認することができる。

ISO27001 などのセキュリティ関連認証を取得するためには、事実上、インシデント報告を含めたインシデント・ハンドリングの体制を構築・運用する必要がある。さらに、その体制の有効性評価が求められるようになっているので、なんらかの形で実働状況を計測する必要がある。
また、最近では CSIRT 設立の必要性が叫ばれるなど、認証を取得しない場合であってもなんらかのインシデント・ハンドリング体制が求められていることには変わりがない。

予防接種では、擬似攻撃メールを被験者に配信するので、これを受信した被験者がどのようにインシデント報告を行うかを調べれば、インシデント報告体制の実働状況を計測することができる。

今年度の予防接種では、被験者アンケートの中で被験者の意識調査を実施しており、その結果、被験者の 62.6%が管理者へ報告するという回答をしている。
この詳細については、17.6 に述べた。

ISO27001 における有効性評価の方法のひとつとして、予防接種は貴重なデータを作成することができるのではないかと思われる。

18. 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認知を向上し、ひいては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重層防御態勢を構築することが必要である。

今年度の予防接種の経験からは、被験者が往々にしてメールの表題や本文の「おおざっぱな雰囲気」だけを判断材料にしている傾向が読み取れた。
この傾向についての対策の第一歩は、差出人のメールアドレス [13]を確認することである。また、メールそのものを吟味すると同時に、被験者自らの置かれた文脈と照らし合わせて、標的型メールに残る「不自然さ」を見抜くことが必要である。

このような「眼力」を身に付けるためには、単に情報セキュリティ教育が必要であるだけでなく、その前提となる IT リテラシーの向上も重要である。今年度の予防接種で、IT 系企業の方が非 IT 企業よりも良い結果を示したことが、IT リテラシーの重要性を裏打ちしている。

[13] 今年度の予防接種では、差出人のメールアドレスとしてフリーメールのものを使用した。実際の標的型メール攻撃では、自組織や関連組織のアドレスを詐称するものが多いので、さらに難易度が高い。