標的型メール攻撃対策訓練における 訓練メール自動生成のための受信メール分析手法の検討

岩田一希[1] 中村嘉隆[2] 稲村浩[2] 高橋修[2]

概要：近年，標的型メール攻撃の被害が増大している．現状の対策における課題として使用されるマルウェアは既存の対策ソフトでは検知できない場合が多いという点，またマルウェアへの防御システムは基本的に既知の攻撃にしか対応できない点があげられる．この課題に対して，「人間」に擬似的に攻撃を受けさせ，攻撃に対する訓練をすることで，標的型メール攻撃への耐性をつけるという手法が考えられている．しかし現在行われている訓練手法では訓練を受ける組織に適した訓練にはなっているが，訓練を受ける個々の従業員に対して有効な訓練にはなっていない．そこで本研究では受信 BOX にある受信メールをローカルで分析して普段受信するメールに類似した擬似メールを受信メールのように表示することで，効果の高い訓練を行うことが出来るシステムを提案した.訓練メール生成には受信 BOX のメールを用いており，被訓練者に適した訓練メールを生成出来るようになっている．評価として，この手法を使って，訓練メールを作成し訓練効果が向上するかどうかを検証した．

An e-mail analysis method for automatic generation of training mail in the training against advanced persistent threat

KAZUKI IWATA[1]
YOSHITAKA NAKAMURA[2] HIROSHI INAMURA[2] OSAMU TAKAHASHI[2]

1. はじめに

近年，企業の一個人を対象として，マルウェアを添付したメールや, 悪性サイトの URL を添付したメールを送信し，マルウェアをダウンロード・実行させて感染させる標的型メール攻撃の被害が増大している．標的型メール攻撃の特徴としては，攻撃されている事に気付きにくいことが挙げられる．これらの攻撃メールはそれが攻撃メールであることを悟られないように，受信者にメールを送る可能性の高い他者になりすまされていたり，もしくは受信者の業務内容に沿ったメールを生成･送信しているという特徴がある．また，マルウェアを実行してしまったあとも，アンチウイルスソフトウェアでの検知が難しい上に，通常業務に影響が出ないように動作するため，攻撃に気づきにくい．よって，情報漏洩などの被害にあってから初めて標的型メール攻撃を受けていたことに気づくケースが多い．

標的型メール攻撃の攻撃手順には，準備段階を 1 段階目とすると，図 1 のような 6 つの段階がある．

1 段階:攻撃者が標的の組織の情報を入手
2段階:攻撃者は組織の人間に攻撃メールを送信
3段階:メールを開封し組織内にマルウェアが侵入
4段階:マルウェアが外部との不正な通信路を確立
5段階:確立した通信路を用いて攻撃者は情報収集
6 段階:目的の情報へアクセスして窃取

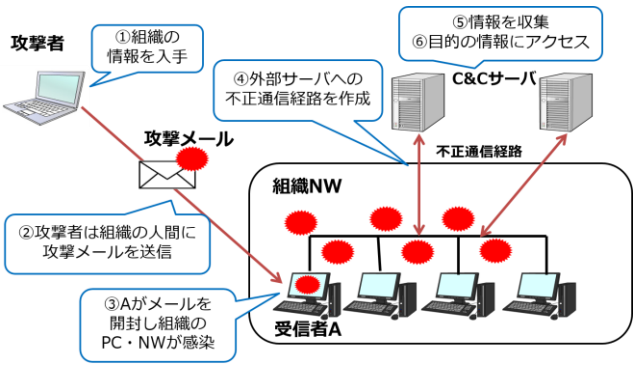

図 1 標的型メール攻撃の攻撃手順

IPA によると標的型メール攻撃による被害状況は図 1 のようになっている. 2011 年度はサイバー攻撃全体の 20%が標的型メール攻撃だったが, 2013 年度は 30%に増えている[1][2]. さらに，2015 年 6 月にも日本年金機構が標的型メール攻撃による大規模な情報漏洩を起こしている[3]. 以上のことから，今日，標的型メール攻撃への対策が求められている．

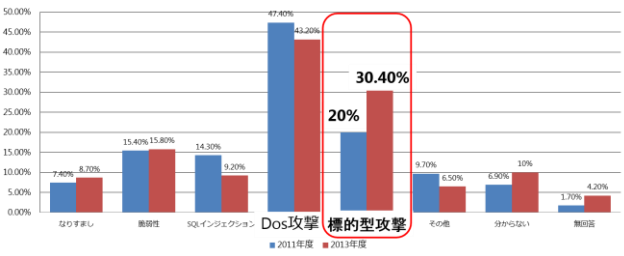

図 2:標的型メール攻撃の被害状況

1 公立はこだて未来大学大学院 システム情報科学研究科
2 公立はこだて未来大学 システム情報科学部

標的型メール攻撃において，マルウェアが侵入しないようにする対策を「入口対策」と呼び，外部へ不正な通信が行われないようにする対策を「出口対策」と呼ぶ.「入口対策」の課題として，この攻撃に使用されるマルウェアは既存のアンチウイルスソフトウェアでは検知できない場合が多いという点，またマルウェアへの防御システムは基本的に既知の攻撃にしか対応できない点がある．この課題に対する解決手段として,「人間」に擬似的に攻撃を受けさせる，つまり攻撃されることへの訓練を行うことで，標的型メール攻撃への耐性をつけるという手法がある．人間にはシステムと違い対応力が存在するため，訓練を経て耐性を持つことができれば，未知の標的型メール攻撃にも対応できると考えられている．実際に 2008 年、2009 年に標的型攻撃対策訓練が行われた結果を JPCERT/CC[4][5]が残している．その資料によると、IT 関連業界だけではなく、地方自治体などの組織でも、訓練による効果を確認することができている．さらに、内田[6]は，標的型メール攻撃対策訓練を以下の 1~4 の条件で実施した場合に，表のような結果を得ている．

1. 事前の情報提供をせず訓練を実施
2. 事前に情報提供を行って訓練を実施
3. 訓練実施 2 年後，事前の情報提供をせず実施
4. 訓練実施 2 年後事前に情報適用し実施

表 1:訓練条件と添付ファイル開封割合

条件	添付ファイル開封割合
1	約 40%
2	約 10%
3	約 12.5%
4	約 6.3%

この表 1 より，標的型メール攻撃訓練には，標的型メール攻撃対策として有効であることがわかる．しかし現在行われている訓練手法では繰り返すことが考えられておらず，次第に効果が薄れてしまう．また，継続されないため訓練内容が改善されない点，さらに訓練メールは被訓練組織に一斉送信されていて，個々人が置かれている状況においては，訓練効果が薄い可能性がある点が課題となっている．

2. 研究目的

本研究は「人間」に擬似的に標的型メール攻撃を継続して体験させる事によって標的型メール攻撃への対策訓練を行うことを目的とする．

3. 先行研究

先行研究として、上記のような標的型攻撃対策訓練の課題を解決するために「人間」に擬似的に標的型メール攻撃を継続して体験させる事によって標的型メール攻撃への対策訓練を行うことを目的とした自動訓練システムを提案した[7].

3.1 システム構成

提案システムは以下の図 3 のように、訓練を実施するメールクライアント部分と訓練データを保存するサーバで構成されている．提案システムのユーザを「ユーザ A」とした時，ユーザ A が直接操作するのはメールクライアントの部分である．その他には訓練データを蓄積するサーバが別にあり，一定のタイミングでメールクライアントとデータの送受信をしている．下記では提案システムの機能について説明する．

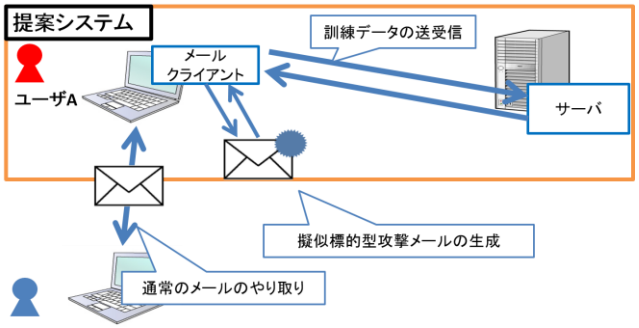

図 3:システム構成図

3.2 メールクライアント

メールクライアントでは，通常のメールのやり取りや，メールの閲覧が可能になっている．また訓練用の標的型攻撃メールをクライアント側で生成し，それをメールとして配信するのではなく，クライアントで表示して訓練をする機能や，訓練データ蓄積サーバに訓練の結果を送信する機能を持つ．

3.2.1 メール分析ツール

受信 BOX のメールを分析し，訓練用の標的型攻撃メールを生成するのに活用する．受信メール分析を行うことにより，ユーザがどのようなメールを信頼して開封しているかを確認できる．

3.2.2 訓練メール生成ツール

訓練メール自動生成ツールでは，クライアント側でメールの分析を行ったデータと，サーバ側で分析を行ったデータを使って，訓練メールを自動生成する．訓練メールを生成する際には上記のデータの他に，標的型攻撃メールだと気づくことができるポイントをメールに盛り込む[8]．このようにメールを自動生成することによって，繰り返し訓練を行う際に訓練メールを一から生成する手間を省くことが

できる．さらに個々人のメール情報や訓練のデータを利用して訓練メールを生成しているため，個々人に特化した訓練を行うことができる．これによってユーザは，自分の弱点への対策を行いながら，似たようなメールが送られてきた時に注意をしながら開封することができるようになる．

3.3 訓練データ蓄積サーバ

訓練データ蓄積サーバでは，メールクライアントから送られてきた訓練データを蓄積する．一人のユーザについて以下の 6 種類のデータを蓄積する．

1. 訓練メール開封の有無
2. 訓練の総計回数
3. 前回訓練時からの経過日時
4. 訓練メールのマルウェアの侵入源
5. 訓練メールである気づくポイントの位置
6. 訓練メールである気づくポイントの数

3.3.1 訓練データ分析ツール

このツールでは，2.3 節で挙げた訓練データ蓄積サーバで蓄積した 6 種類のデータを分析する．1, 2 のデータを分析すると，このツールを使った訓練の効果を検証することができる．1, 3 のデータを分析すると，訓練と訓練の間をどれくらい空けると，最も効果的な訓練の間隔を検証することができる．1, 4, 5, 6 のデータを分析すると，ユーザが開封しやすい標的型メールの傾向を調べることができる．分析したデータは 2.2.2 項で述べた訓練メール自動生成ツールに送信し，自動メール生成に活用する．

3.4 自動訓練システムを活用した訓練手法

このシステムを導入した場合の訓練手法について JPCERT/CC が 2009 年度に行った訓練を参考に下記の図のように提案した．

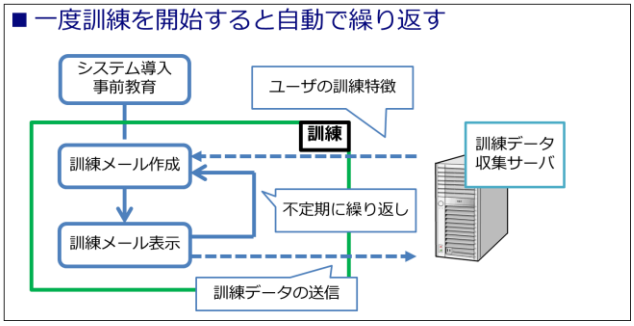

図 4:提案システムを使った訓練手順

1 ユーザに提案システムの導入が伝わる
2 ユーザが標的型メール攻撃についての教育を受ける
3 提案システムの受信 BOX 上に訓練メールが表示される
3.1 訓練メールの添付ファイルを開いた場合は，刺激文や，標的型メール攻撃の特徴が載った Web サイトや文章が表示される
4 3, 3-1 を不定期に繰り返す

手法の 1~2 に関しては，導入する各組織で独自に行うことになるが，手段 3 からは提案システムを導入し，普段と同様にメールの閲覧や送受信を行ってもらうことで，訓練が継続されることになる．一度でも，訓練メールの添付ファイルの開封が行われた場合，刺激文や標的型メール攻撃の特徴がわかるような Web サイトや文章が表示されるため，今後は引っかかってしまわないように気をつけることができる．このような過程で継続してメールクライアントの通常利用や訓練を行うことで，自動的にメールの分析データや訓練データが貯まり，訓練メールの生成に使用されることで，個々のユーザに適した訓練が実施できる．

3.5 先行研究における課題

先行研究では，自動訓練システムとそれを用いた訓練手法について提案した．しかしメールの自動生成時に，利用者が騙されるようなメール文章の機械的な生成は非常に困難であると予想される．よって文章の自動生成を簡易にする方法の考案が課題となる．また，訓練メールを生成するにあたり，実際の標的型攻撃メールにありがちな，通常やり取りするメールとは違う「不自然な点」をどう再現し，どう訓練メールに埋め込むのかを検証することも課題となっている．

4. 提案手法

本稿では，先行研究の課題として挙げた下記の 3 点について解決する．

1. 訓練メールの文章を自動生成手法
2. 攻撃メールの「不自然な点」の再現
3. 訓練メールへの「不自然な点」の反映

4.1 訓練メールの文章を自動生成手法

先行研究の課題にもある通り，利用者が騙されてしまうようなメール文章を一からの自動生成は困難である．また，被訓練者ごとに状況に応じた訓練メールを生成することが本研究の目的であるため，単純に文章を生成するだけではなく，被訓練者に適した文章を生成する必要がある．そこで，受信 BOX の中身にある普段やり取りするメールを分析して，文章生成に反映する手法を提案する．

4.1.1 受信 BOX のメール分析

まず受信 BOX にあるメールを送信者アドレスごとに分割する，その後，新しいメールから順にメールヘッダを分析し，添付ファイルがあるかどうかを調べる．添付ファイ

ルがあるメールは，ある程度の定型文＋添付ファイルとなっている場合が多いと考えられるので，その定型文を送信者アドレスごとの特徴と捉える事ができる．この送信者アドレスごとの特徴を「送信者特徴」と定義する．

例として下記の表のようなメールが同一アドレスから定期的に送られてきていると仮定する．

表 2 添付ファイル付定型文のメール

Subject	今週のゼミの日程について
From	G1111111<g1111111@xxx.co.jp>
Message	XX(実在名)研究室の皆様 M1 の□□(実在名)です. 今週のゼミに関する日程を調整しましたのでお知らせします. 詳細は添付したファイルをご覧ください. よろしくお願いします. 博士（前期）課程 1 年　□□
Attach	今週のゼミの日程.txt

この場合，メール本文の構成として

1. 挨拶
2. 内容
3. 添付ファイル確認促し
4. ㌢の挨拶
5. 署名

となっている．この構成のメールが連続して届いているため，この送信者アドレスの送信者特徴は上記の 1~5 の定型文になると捉えることができる．また，ある送信者アドレスから送られてきているメールがある程度違う文章である場合．行ごとに頻出する文を数え，それを特徴とすることが出来ると考える．

4.1.2 訓練メールの生成

3.1.1 の方法で送信者特徴をとらえた後，最新の送信者特徴が現れている，メールの定型文部分を切り取り，メール本文に貼り付けることで，訓練メールが生成できる．手法として，ある送信者アドレスから送られてきている添付ファイル付きのメールが，3.1.1 項の例文のように簡単な定型文に添付ファイルが付いているようなメールだった場合，送信者特徴と，受信メールの文章が一致するため，訓練メールも同一の文章を用いる．それとは別に，ある送信者アドレスから送られてきている添付ファイル付きのメールが毎回ある程度違う文章である場合は 3.1.1 項を参考に行ごとの特徴を用いて，行ごとに生成することで，ある程度それらしさを持つ訓練メールの自動生成が可能であると考えられる．

4.2 攻撃メールの「不自然な点」再現

攻撃メールの「不自然な点」とは，通常やりとりするメールには現れないはずの特徴である．このような特徴が現れる理由として，攻撃者は，送信者になりすますための必要な情報がすべて入手出来ていない可能性があり，その状態でメールを作成しているためであると考えられる．さらには日本人に向けての攻撃メールを海外の攻撃者が作っている場合もあるため,言葉遣いが不自然な場合も存在する．提案システムでは，3.1 節で説明した通り，過去のメールを参照してメールを生成するため，送信者になりすますための情報は全て手に入れており，それをすべて活用して，訓練メールを生成してしまうと，外部の攻撃者では作成し得ない高度なりすましメールを生成できてしまう．それでは見分ける箇所がなくなってしまい，訓練の度に被訓練者が騙されることになり，改善の余地もなくなってしまうため，攻撃者が起こしそうなミスを「不自然な点」として訓練メールに挿入し，訓練メールを見分けるためのヒントとする.これによって,被訓練者は訓練を繰り返すにつれ，訓練メールを注意深く見るようになって「不自然な点」を見つけるようになり，騙されないようになることができると考える．

「不自然な点」を再現するにあたって，IPA の「標的型攻撃メールの例と見分け方」[8]を参考にする．

4.3 訓練メールへの「不自然な点」反映

実際に訓練メールに「不自然な点」を挿入する際に 3.1 節の手法で訓練メールを生成したあと，3.2 節の IPA の資料を参考に「不自然な点」とする部分を選び挿入する．最初は,「不自然な点」を多く挿入した訓練メールを生成する．ある程度訓練を繰り返し，サーバに被訓練者が見分けづらい苦手な「不自然な点」の情報が溜まってくると，苦手な点を多く挿入した訓練メールを生成するようになる.また，訓練メールを見分けることに成功するようになってくると，挿入される「不自然な点」が少なくなるようになる．

5. 基礎評価実験

従来の訓練手法の訓練継続回数を増やし，提案手法のように被験者の状況に適した訓練メールを，被験者の受け取っているメールに合わせて生成することで，従来と同様，もしくは従来以上の訓練効果を得ることができるのかを検証することを目的とし実験を行った．被験者は公立はこだて未来大学の情報アーキテクチャ学科の学部 3 年生 3 名に対して行った．

5.1 基礎評価実験の手順

JPCERT/CC の 2009 年度の資料を参考として，標的型メール攻撃対策訓練を以下の図 5 のような手順で実施した．

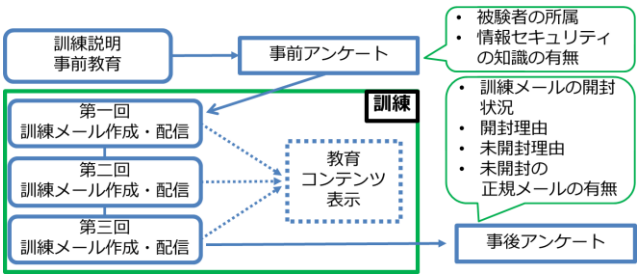

図 5：訓練手順

事前説明では，実験の目的や手順だけではなく，標的型メール攻撃の攻撃手段や，攻撃メールの見分け方の説明を行い，攻撃への理解を深めてもらった．事前アンケートではメールアドレスや所属，セキュリティ知識の有無などを確認した．事前説明で攻撃についての理解は深めてもらっているが，元々のセキュリティ知識の有無が添付ファイルの開封に関与すると考え，項目として追加した．

5.2 実験に使用した訓練メール

訓練用のメールは提案手法に則り，被験者が普段受け取っているメーリングリストのメールの添付ファイルが付いているメールを参考に 3件生成した．1, 2 件目に関しては，JPCERT/CC が実験で使用したメールに被験者の受信 BOX のメールに存在する送信者の名前と，簡単な送信者特徴を合わせて生成している．3 件目に関しては，被験者の所属している狭いコミュニティに向けたメールの送信者特徴を模倣したメールに攻撃メールに表れやすい「不自然な点」を合わせて生成している．実際に使用したメールは以下の 3 通である．

表 3　実験に使用したメール 1

Subject	**保健だより No.7 の配布(医務室)**
From	Abcdefg(実在名)<abcdefg@excite.co.jp>
Message	学生の皆さん こんにちは，医務室の○○(実在名)です． 寒さが厳しくなってきました． ついに強毒型の新型インフルエンザが出現し、急速に罹患者を拡大している模様です． 保健だよりＮｏ．７を添付します． 「すぐできるインフルエンザ対策」を参考に、改めてインフルエンザ対策を強化していただきますようにお願いいたします． 内容：◆強毒型の新型インフルエンザについて ◆すぐできるインフルエンザ対策 医務室　○○(実在名)
Attach	保健だより No.7.pdf

このメールにおける「不自然な点」は，

1. 送信元アドレスのドメインがフリーメールのものである点
2. 署名がなりすまされた人が普段つける署名とは違っている点
3. 危険性を強調して添付ファイルを開かせようとしている点

である．

表 4　実験に使用したメール 2

Subject	至急：Windows の脆弱性暫定回避策
From	xxxxxxx(実在名)<xxxxxxx@yahoo.co.jp>
Message	皆様 昨日、Windows に極めて深刻な脆弱性が発見されました． 現時点ではパッチが出ておりませんが、暫定回避策がありますので、添付のマニュアルにしたがって、各自で至急に対策してください． 今回の脆弱性はリモートから PC を乗っ取られる可能性のあるものですので、今すぐに対策していただきますようにお願いします． システム委員会　情報・施設管理担当
Attach	暫定回避マニュアル.pdf

このメールにおける「不自然な点」は,

1. 送信元アドレスのドメインがフリーメールのものである点
2. 危険性を強調して添付ファイルを開かせようとしている点

である.

表 5　実験に使用したメール 3

Subject	春休みのゼミの日程について
From	G1111111<g1111111@yahoo.co.jp>
Message	XX(実在名)研究室の皆様 M1 の□□(実在名)です. 春休みのゼミに関する日程を調整しましたのでお知らせします. 詳細は添付したファイルをご覧ください. よろしくお願いします. 博士（前期）課程 1 年　□□
Attach	春休みのゼミの日程

このメールにおける「不自然な点」は,

1. 送信元アドレスのドメインがフリーメールのものである点
2. 署名がなりすまされた人が普段つける署名とは違っている点
3. 添付ファイルの確認を促している点

である.

5.3 訓練効果

実験の結果としては以下の表のようになった.

表 6 実験結果

被験者	1 件目	2 件目	3 件目
A	未開封	未開封	未開封
B	未開封	未開封	開封
C	開封	未開封	未開封

訓練の結果としては，被験者 C については，1 件目のメールの添付ファイルを開封したあと，2 件目，3 件目に関しては未開封だったため，訓練の効果があったと言える．また，メールの開封理由は以下の表のようになった.

表 7 未開封理由

被験者	1 件目	2 件目	3 件目
A	危険と判断	危険と判断	危険と判断
B	通常と違うと判断	危険と判断	-
C	-	危険と判断	危険と判断

アンケートの結果，訓練メールを開かなかった理由として「危険なメールだと思ったから」というのが多数で，2 件目のメールと 3 件目のメールの未開封者において，すべての理由となった．1 件目のメールに関しては，理由が 2 つに割れ，片方は「危険なメールだと思ったため」だったが，もう片方は「普段見ないメールだったため」という理由だった． また，3 件目のメールの添付ファイルを開いた被験者 B に開封理由を尋ねたところ，「自身に関連が深いメールだったため，正規メールだと判断してしまった」と回答した.

6. 考察

この実験の結果から，被験者 C に関しては 1 件目の訓練メールの添付ファイルを開封後，2 件目，3 件目では未開封のため，訓練効果が現れていると考えられる．被験者 B に関して，1, 2 件目の送信者特徴をあまり重視していないメールにおいては「通常送られてくるメールと違う」,「攻撃に現れる不自然な点を確認した」と言った理由で開封を回避したが，3 件目の送信者特徴と，被験者の置かれている状況を重視したメールの添付ファイルを開封してしまっている．このことから，訓練は繰り返すだけでも効果が見込めるかもしれないが，提案手法のように被訓練者の受信 BOX から送信者アドレスごとに送信者特徴を取得し，訓練メール生成に活用し，この手法で生成された訓練メールを使って，訓練を繰り返すことで，訓練効果の上昇を図ることができるのではないかと考える.

7. まとめ

標的型メール攻撃対策として，「人間」に対して訓練を行う手法がある.この手法の課題として,従来の手法では,訓練メールは一斉送信されていて，個々人の状況によって効果に個人差が出てしまうという課題がある．本研究ではこの課題を解決するために個々人に適した訓練を継続的に行ってくれる自動訓練システムを提案した．提案システムでは普段受信するメールに似たような訓練メールを作成するために,受信 BOX の中身を送信者アドレス後に分割し，その中の添付ファイル付きのメールから，送信者特徴を割り出し，訓練メール生成に用いる．訓練メール生成の際には送信者特徴を元に，訓練メールを以前受信しているメー

ルからコピーする形で生成する．さらに，訓練メールは送信者になりすますための情報をすべて持っていない攻撃者から送られてきている想定で生成するため，通常のメールには起こりえない「不自然な点」を挿入する．訓練を繰り返す度に，被訓練者に適した「不自然な点」の挿入位置や，個数へと切り替わっていくような仕組みになっている．このようなシステムを使って訓練を行うことで実際に効果が現れるのかどうかを検証するために，基礎実験として，一斉送信されるような訓練メールと被訓練者の状況に合わせて関連の高いメールを受信 BOX のメールを使って作成し訓練を行った結果，関連の高いメールを利用したほうが訓練効果が高まる可能性が高いことがわかった．今後の課題として，さらに多くの被験者に対して，多くの訓練をこの手法で実施することで，訓練効果の確認を行い，さらなる改善点を見つけることが課題である．

参考文献

[1] IPA, “2014 年度情報セキュリティ事象被害状況調査報告書,” http://www.ipa.go.jp/files/000043418.pdf, 2015/01, 最終アクセス:2015/11/10

[2] IPA, “2013 年度情報セキュリティ事象被害状況調査報告書,” http://www.ipa.go.jp/files/000036465.pdf, 2014/01, 最終アクセス:2015/8/10

[3] “年金機構の 125 万件情報流出 職員，ウイルスメール開封,” 日本経済新聞, 2015/6/1, 最終アクセス:2015/11/10

[4] JPCERT/CC, “2008 年度 IT セキュリティ予防接種調査報告書,” http://www.jpcert.or.jp/research/inoculation2008.html, 2009, 最終アクセス:2015/11/10

[5] JPCERT/CC, “2009 年度 IT セキュリティ予防接種調査報告書,” http://www.jpcert.or.jp/research/inoculation2009.html, 2011, 最終アクセス:2015/11/10

[6] 内田勝也, “大規模情報漏えいにおけるセキュリティマネジメントからの考察”, http://www.uchidak.com/IPSJ/20160311_CSEC.pdf, 2015, 最終アクセス:2016/05/11

[7] 岩田一希，中村嘉隆, 高橋修, “標的型メール攻撃対策のための自動訓練メールクライアントシステム,”情報処理学会第 78 回全国大会論文集, pp3-561-pp3-562, 2016

[8] IPA, “IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」,” https://www.ipa.go.jp/files/000043331.pdf, 最終アクセス:2015/11/18