Vol.2013-CSEC-63 No.4
2013/12/9

メール攻撃危険予知訓練システムの開発

木村壮太[†1]

近年，中小企業への標的型攻撃の件数が増加している．その一方で，中小企業でも BYOD が普及しつつあり，会社統制しにくい端末を介した情報漏えいの増加が考えられる．
情報セキュリティへの投資額を考慮すると，中小企業では従業員の意識向上が最も効果的で，座学よりも演習・体験型教育が有効と考える．また，標的型攻撃だけではなく多様な攻撃に対する意識向上が必要となる．
そこで，我々はソーシャルエンジニアリングの観点を導入した攻撃方法の統合マップと，それに基づいた体系的な演習が可能な教育訓練用システムを開発した．現在，このシステムを用いて社内での試験運用を実施中である．今回は統合マップ，教育訓練用システムの構成，実施済みの演習の結果について報告する．

1. はじめに

近年，中小企業への標的型攻撃の件数が増加している[1][2]．これは，大企業や政府機関のサプライチェーンの構成要素のうち情報セキュリティ対策が不十分な箇所を突き，攻撃の踏み台とするためと考えられる[3]．また，コスト削減，利便性の面からか中小企業でも BYOD が普及しつつある[4]が，情報セキュリティのポリシーが未整備あるいは周知されていない状況で BYOD を運用している企業が相当数あり[5]，今後携帯型端末を標的とした攻撃が増加していくことが予想される．
なお，政府は中小企業に対し「リスク認識に基づく対応の強化」（事故前提社会）を提言しており，今後，中小企業は情報セキュリティに対する自発的な対応を法的に求められるようになると考えられる[6]．
しかし，ウィルス対策ソフトなどの技術的対策ではサイバー攻撃を容易に防ぎきれるものではなく，まして社内インフラ再構築など大がかりな対策はコスト的に中小企業には非現実的である．したがって，とりわけ中小企業では入口対策としての従業員の意識向上が最も重要であり，座学よりも演習・体験型教育が有効である．

そこで，我々は「顧客企業の従業員のセキュリティ意識向上により，業務不能化（社内情報インフラ停止）や情報漏えい（外部サーバへの不正送信）を防止する」ことを狙いとして，ソーシャルエンジニアリングの観点を導入した攻撃方法の統合マップと，それに基づいた体系的な演習が可能な教育訓練用システムを開発した．現在，このシステムを用いて社内での試験運用を実施中である．
そこで，今回は統合マップ，教育訓練用システムの構成，実施済みの演習の結果について報告する．

†1 (株)アストジェイ
Advanced Solutions Technology Japan, Ltd.

2. 教育対象擬似攻撃

従業員に対し効果的に教育を行うためには，想定される攻撃パターンを網羅し且つ勤務先の業務形態に合った疑似攻撃コンテンツを用いる必要がある．
そこで我々は，業務利用シーン毎に攻撃方法を想定し，それらの攻撃方法を体系化した統合マップを作製した．更に統合マップにおける攻撃の型に着目して攻撃シナリオを全体マップとしてまとめ，攻撃コンテンツを網羅的に導出できるようにした．

2.1 業務利用シーン別攻撃方法の統合マップ

従業員の執務中に想定される攻撃方法を把握するため，業務利用シーン毎に想定脅威，攻撃の型，攻撃・偽装方法を体系的にまとめた．

(1) メール利用時

メールを利用している従業員に対する攻撃の型は，偽装メール送付型のフィッシング攻撃と標的型攻撃が挙げられる． どちらの攻撃も，メールの送信元およびアドレス，タイトル，内容文等を URL のクリックや添付ファイルの開封を強く促す内容とし，偽サイトへ誘導あるいはマルウェアに感染させることで情報を詐取する．

業務での利用シーン	想定脅威	攻撃の型	攻撃・偽装方法		
			攻撃方法タイプ	偽装箇所	偽装方法
メールの利用時の添付ファイルの開封/登録返信とURLの参照	・機器内の機密情報や個人情報の窃取 ・当該端末を踏み台とした会社の情報システムへの不正アクセス	フィッシング攻撃（偽装メール送付型）	フィッシングメールで偽サイトへ誘導	・送信元/メールアドレス	・信頼できる組織を偽装
				・メールタイトル	・興味を引く/アラートタイトル ・ありえるタイトル（更新・確認依頼等）
				・内容文（組織ロゴ、誘導URL）	・ありえる内容 ・注意や警告の対応促進内容 ・ロゴコピー ・正規に見えるURL
				・偽サイト構築	・正規に見えるURL ・正規に見えるHPコンテンツ
			空メールで偽サイトへ誘導	・手当配布等不正登録用メールアドレス	・興味を引く登録誘導やキャンペーン（クーポン）提供等）
				・偽サイト構築	・正規に見えるURL ・正規に見えるHPコンテンツ
	・マルウェア感染 ・窃取した機密情報や個人情報を再利用した反復攻撃	標的型攻撃	標的型メールを攻撃対象に送付	・送信元/メールアドレス	・信頼できる組織を偽装 ・フリーメール アドレス利用
				・メールタイトル	・興味を引く/アラートタイトル ・ありえるタイトル（更新・確認依頼等）
				・内容文（組織ロゴ、誘導URL）	・ありえる内容 ・注意や警告の対応促進内容 ・ロゴコピー ・正規に見えるURL
				・偽添付ファイル	・正規に見える添付ファイルアイコン ・正規に見える添付ファイル名

図 1「メール利用時」の攻撃方法統合マップ

(2) ブラウザ利用閲覧時

ブラウザを利用している従業員に対する攻撃の型は，不正コンテンツ，マルウェア，アドレス改ざん利用型のフィッシング攻撃と不正アプリ攻撃が挙げられる．

業務での利用シーン	想定脅威	攻撃の型	攻撃・偽装方法		
			攻撃方法タイプ	偽装箇所	偽装方法
ブラウザ利用閲覧時のURL参照	・機器内の機密情報や個人情報の窃取 ・当該端末を踏み台とした会社の情報システムへの不正アクセス ・マルウエア感染 ・窃取した機密情報や個人情報を再利用した反復攻撃	フィッシング攻撃　（不正コンテンツ、マルウエア、アドレス改ざん利用型）	検索リンクから偽サイトへ誘導	・検索リンク	・正規に見える記述項目
				・偽サイト構築	・正規に見えるURL ・正規に見えるHPコンテンツ
			DNSサーバに偽サイトのIPアドレスを書込み偽サイトへ誘導	・DNSサーバのIPアドレス	・偽サイトのIPアドレスへ書き換え
				・偽サイト構築	・正規に見えるURL ・正規に見えるHPコンテンツ
			汚染サイトアクセス時に不正プログラムを送付して偽サイトへ誘導	・検索リンク	・興味を引く記述項目 ・偽サイトのIPアドレスへ書き換え
				・偽サイト構築	・正規に見えるURL ・正規に見えるHPコンテンツ
			本物サイトに不正コンテンツ(不正画面表示)を注入しサイトを乗っ取り情報搾取	・本物サイトのHP or ・利用者ブラウザ(ウイルス)	・HPに不正コンテンツ注入 or ・ブラウザ表示の内容を一部置き換え

図 2「ブラウザ利用閲覧時」の攻撃方法統合マップ(1/2)

業務での利用シーン	想定脅威	攻撃の型	攻撃・偽装方法		
			攻撃方法タイプ	偽装箇所	偽装方法
ブラウザ利用閲覧時のSNSの利用	・機密情報や個人情報の窃取を目的とした悪意あるアプリケーション(マルウエア)の取り込み ・悪意のあるアプリケーションへの感染 ・機器内の機密情報や個人情報の窃取 ・当該端末を踏み台とした会社の情報システムへの不正アクセス	不正アプリ攻撃	■FacebookやTwitterなどのメッセージを通じて詐欺サイトやマルウェア感染サイトに誘導	SNSのメッセージ	大きなニュースに便乗してメッセージを流し、詐欺サイトやマルウェア感染サイトに誘導

図 3「ブラウザ利用閲覧時」の攻撃方法統合マップ(2/2)

フィッシング攻撃では，偽サイトの設置（検索エンジンで検索されるようにする），DNS サーバの書き換え，汚染サイトへのアクセス，改ざんされた正規サイトへのアクセスを通じて，偽サイトへ誘導あるいはマルウェアに感染させることで情報を詐取する．
不正アプリ攻撃では，SNS のメッセージにより感染サイトへ誘導してマルウェアに感染させることで情報の詐取，踏み台化を行う．

(3) アプリケーションダウンロード及びインストール時

アプリケーションのダウンロードおよびインストールを行っている従業員に対する攻撃の型は，不正アプリが挙げられる．

業務での利用シーン	想定脅威	攻撃の型	攻撃・偽装方法		
			攻撃方法タイプ	偽装箇所	偽装方法
アプリケーションのダウンロード＆インストール時	・機密情報や個人情報の窃取を目的とした悪意あるアプリケーション(マルウエア)の取り込み ・悪意のあるアプリケーションへの感染 ・機器内の機密情報や個人情報の窃取 ・当該端末を踏み台とした会社の情報システムへの不正アクセス	不正アプリ攻撃	■機密情報の窃取マルウェアを配布し、利用者が気付かぬように個人情報を窃取	チェックの甘いアプリストアサイト	ユーティリティやゲーム、アダルトアプリを偽装したマルウェア
			■不正課金/請求マルウェアを配布し、勝手に課金用のIDにSMSを送信	スパムメールによる告知広告	ユーティリティやゲーム、アダルトアプリを偽装したマルウェア
			■第一段階のマルウェアが第二段階のマルウェア(ボット等)を勝手にダウンロードし、端末を乗っ取る(遠隔操作)	著名人気アプリの外観	・Skype,Google Maps, Mozilla,Firefox等の著名ソフトの外観を偽装した不正ソフト
				偽の配布サイト	・正規のサイトに酷似したサイトで上記の不正アプリを配布 ・フリー画像ファイルにマルウェアを混入
				有償アプリケーションの海賊版を偽装(混入)	有償アプリの海賊版に不正コードを混入、またはパッケージ化して配布

図 4「アプリケーションのダウンロードおよびインストール時」の攻撃方法統合マップ

不正アプリ攻撃では，機密情報詐取（キーロガー等），不正課金/請求，遠隔操作用等のマルウェアに感染させることで情報を詐取する．

2.2 攻撃シナリオの全体マップ

前項で述べた攻撃方法統合マップの攻撃の型に注目し，攻撃目標，入口，攻撃プロセス，出口，企業へのダメージについて攻撃シナリオの全体マップとして整理した．

図 5 業務利用 PC およびスマホ向け攻撃シナリオの全体マップ

全体マップの「入口」に注目すると，従業員の執務中に想定すべき攻撃の型としては，標的型攻撃のみならず，フィッシング攻撃，不正アプリ攻撃についても網羅的に取り扱う必要があると言える．
なお，攻撃の入り口となるのは Web ブラウザとメールであるが，本教育訓練用システムでは先ず入り口としてメールを扱うこととした．

3. サービス設計

本サービスでは，従業員の BYOD や業務用 PC に対し，模擬サイバー攻撃の演習型教育サービスを提供する．
特徴は以下の 3 点である．

①攻撃シナリオの全体マップと業務利用シーン別攻撃方法の統合マップに基づく体系化された模擬攻撃コンテンツ

②攻撃の種類は，標的型攻撃（従来）
＋フィッシング（新規）＋不正アプリ攻撃（新規）

③攻撃の対象は，PC（従来）
＋スマホ・タブレット（BYOD）（新規）

なお，演習の実施にあたっては，先ず前項の攻撃方法統合マップの業務での利用シーンを顧客企業での業務形態に合わせて選び，次に共通類型化記述を用いて模擬攻撃メールを導出する．
共通類型化記述は，メールの構成要素の「差出人」「件名」「本文」「添付ファイル」について，心理的要因[7]に則っ

た偽装方法を示したものである．権威，好意，希少性，コミットメントと一貫性，返報性，社会的証明の６心理的要因を応用して，偽装メールコンテンツを添付ファイルの開封，URL へのアクセスを強く誘導する内容とすることで教育対象顧客に応じた（罠にかかり易い）不審メールのバリエーション作りを行うことができる．

メールコンテンツ　偽装箇所	【特徴分析】主に効果的な心理的要因：例（偽装方法）
差出人	権威：監督官庁、社内の上長、管理部門
	好意：恩師、旧知の他社の知り合い
件名	権威：警告・注意、更新依頼
	希少性：受信者が興味を引くテーマ（標的に応じて）
	好意：確認依頼、ご参考、助言
本文	ｺﾐｯﾄﾒﾝﾄと一貫性(ﾛｰﾎﾞｰﾙ・ﾃｸﾆｯｸ)：限定商品紹介
	ｺﾐｯﾄﾒﾝﾄと一貫性(ﾄﾞｱｲﾝｻﾞﾌｪｲｽ・ﾃｸﾆｯｸ)：商品の価格交渉
	ｺﾐｯﾄﾒﾝﾄと一貫性(ﾌｯﾄｲﾝｻﾞﾄﾞｱ・ﾃｸﾆｯｸ)：お尋ね
	権威：正規の組織ロゴ不正コピー
	返報性：招待、案内
	社会的証明：他社情報提供
	好意：時事のあいさつ、お礼
	希少性：受信者が興味を引くテーマの内容（標的に応じて）
添付ファイル	社会的証明：正規に見えるアイコン・ファイル名形式

図 6 心理的要因による共通類型化記述

4. 訓練システムについて

本システムは「メール送信用サーバ」「アクセス用 Web サーバ」および「解析用サーバ」で構成される．
各サーバの機能は次のとおりである．

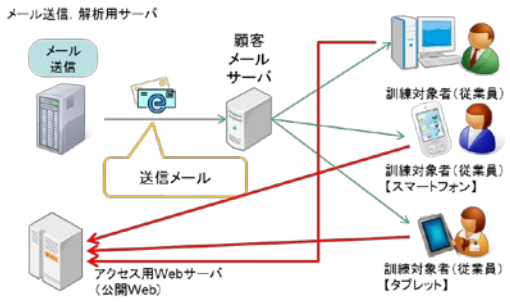

図 7 教育訓練用システムの構成

4.1 メール送信用サーバ，解析用サーバ

メール送信用サーバにより，訓練のパターン（標的型，フィッシング，不正アプリ）に即したメールを作成，顧客メールサーバを介して訓練対象者に送信する．アクセス用 Web サーバのログ（メール開封，URL クリック，アプリダウンロード，アプリ起動時に収集）を基に，解析用サーバで訓練結果を分析する．

4.2 アクセス用Ｗｅｂサーバ

メールによって誘導される Web ページを提供する．メールに反応した訓練対象者を把握するため，BYOD や業務用 PC からのアクセスログを記録する．Android 端末に対する不正アプリ型シナリオではプログラムダウンロードを提供する．

5. 訓練シナリオ

5.1 標的型シナリオ

業務利用シーンとしては「メール利用時」を想定し，共通類型化記述を用いて擬似攻撃メールを作成する．
添付ファイルは，アクセス用 Web サーバへの HTTP アクセス用スクリプトを埋め込んだ PDF とする．
メールに添付された PDF を開くと，アクセス用 Web サーバに準備された説明用 HTML 文書がブラウザに表示されるとともに，アクセスログが記録される．

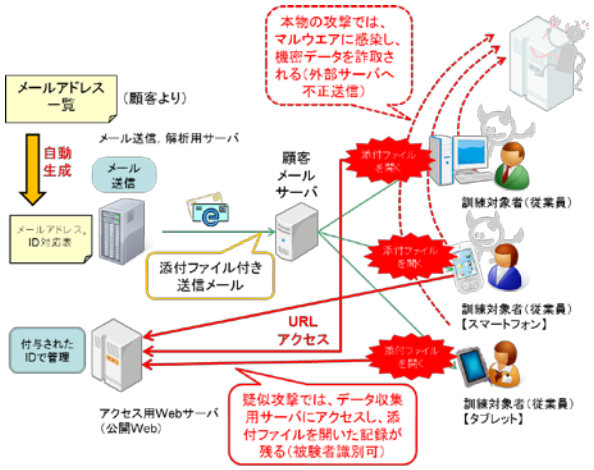

図 8 標的型シナリオ

5.2 フィッシング型シナリオ

業務利用シーンとしては「メール利用時」を想定し，共通類型化記述を用いて擬似攻撃メールを作成する．
本文には，アクセス用 Web サーバ上の CGI スクリプトの URL を記述する．
メールに記述された URL を開くと，アクセス用 Web サーバに準備された説明用 HTML 文書がブラウザに表示されるとともに，アクセスログが記録される．

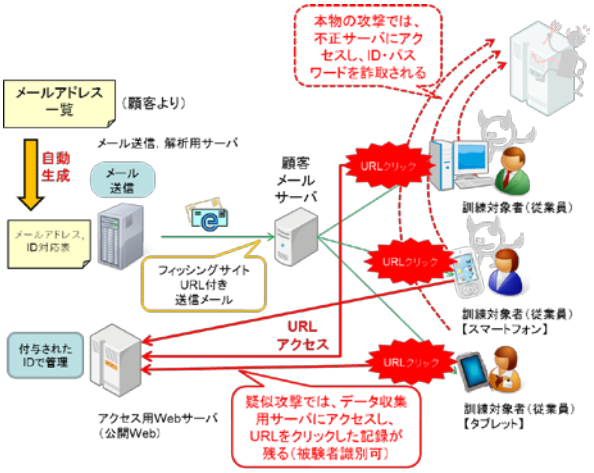

図 9 フィッシング型シナリオ

5.3 不正アプリ型シナリオ

業務利用シーンとしては「アプリケーションのダウンロードおよびインストール時」を想定し，共通類型化記述を用いて擬似攻撃メールを作成する．

本文には，アクセス用 Web サーバ上の CGI スクリプトの URL を記述する．

メールに記述された URL を開くと，アクセス用 Web サーバに準備された模擬不正アプリのインストーラがダウンロードされる．インストールを行った後，メッセージに従ってアプリを起動すると，説明用 HTML 文書がブラウザに表示される．なおインストーラダウンロード，アプリ起動ともに，アクセスログが記録される．

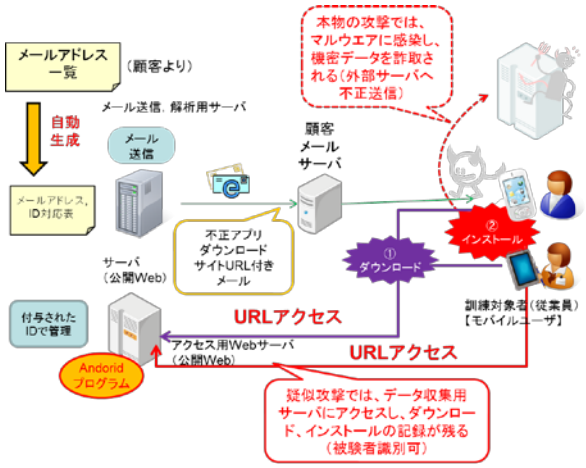

図 10 不正アプリ型シナリオ

6. 評価試験

標的型シナリオとフィッシング型シナリオを用いた演習が社内で実施済みで，ここではその結果について報告する．なお，不正アプリ型シナリオおよび被験者へのアンケートは今後実施する予定である．

6.1 演習の実施スケジュール

教育対象者には，前事教育[8]としてメール攻撃に対する注意喚起と危険予知訓練の予告を行った．なお，模擬標的型攻撃メールは前事教育の 2 週間後，模擬フィッシング型メールはさらにその約 2 ヶ月後に配信した．

表 1 演習の実施スケジュール

実施項目	実施内容	備考
前事教育	注意喚起の文書を配布，危険予知訓練の予告	演習の 2 週間前
演習 1 回目	模擬標的型攻撃メールの配信	
演習 2 回目	模擬フィッシングメールの配信	演習 1 の約 2 ヶ月後

6.2 模擬攻撃コンテンツの作成

(1) 模擬攻撃コンテンツの導出

弊社の業務形態では，取引先および社内での連絡に電子メールを多用するので，業務利用シーンは「メール利用時」とした．攻撃の型は「標的型攻撃」，「フィッシング」を選択した．

なお，模擬標的型攻撃に用いる添付ファイルの種類は PDF とした．

(2) 共通類型化記述による不審メールの作成

不審メールの添付ファイル開封や URL へのアクセスは送信者名，文面内容に依存すると考えられる．演習による学習の効果をできるだけ判別できるようにするため，1 回目配信の模擬標的型攻撃メールと 2 回目配信の模擬フィッシングメールの文面から受ける印象が同程度になるよう配慮した．

模擬標的型攻撃メールについては，送信者を「総務部」（権威），件名を「風疹に関する注意喚起」（権威，希少性），本文を風疹に関する説明（希少性）とし，文面は地方都市の市役所の Web サイトを参考とした，添付ファイルは風疹に関する連絡を偽装するためファイル名称を Fuusin.pdf とした．

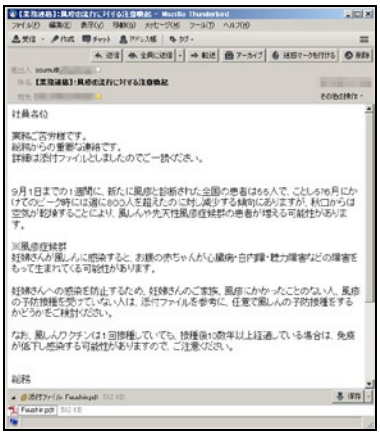

図 11 模擬標的型攻撃メール

模擬フィッシングメールについては，送信者を「IT 管理グループ」（権威），件名を「【業務連絡】：社内認証基盤のパスワードを変更して下さい」（権威），本文を風疹に関する説明（権威）とし，文面はサーバ等から自動発信されたものに似せるよう意識して作成した．

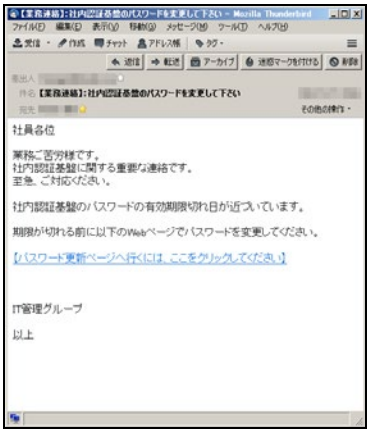

図 12 模擬フィッシングメール

なお，模擬標的型攻撃メール，模擬フィッシングメールとも，架空の差出人名および差出人メールアドレスを使い，実在の部署，社員に問い合わせが行われないよう配慮した．

(3) 添付ファイルと説明用 HTML の作成

添付ファイルを開封した被験者を特定するため，PDF には開封時「アクセス用 Web サーバ」の CGI に被験者 ID をパラメータとしてアクセスする JAVA スクリプトを組み込んだ．

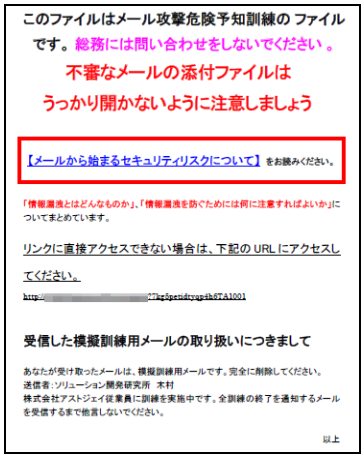

図 13 **PDF 文面**

また，CGI にアクセスすると「アクセス用 Web サーバ」内のログファイルに ID が記録されるとともに，不審メールの添付ファイルを開封することによる情報漏えいのリスクについて述べた HTML が Web ブラウザに表示される．なお，スマホ・タブレットの PDF ビューアには JAVA スクリプトに対応していないものがあるので，PDF 本文に「アクセス用 Web サーバ」の CGI の URL とともに，URL へのアクセスを促す文章を入れている．

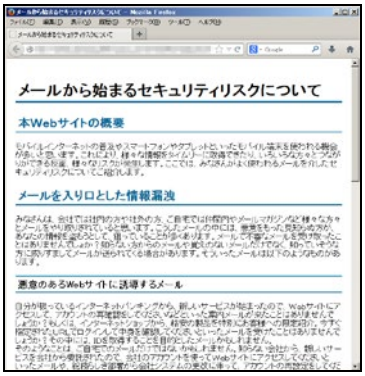

図 14 アクセス用 Web サーバ HTML 文面

6.3 模擬攻撃の結果

演習 1 回目の模擬標的型攻撃メールの配信後，アクセス用 Web サーバには 4 件のアクセスログが記録された．4 件とも PC からのアクセスであった．

表 2 模擬標的型メール攻撃の結果

番号	メール配信後の経過時間（分）	開封件数	アクセス端末
1	63	1	PC
2	147	1	PC
3	238	1	PC
4	7744	1	PC

なお，演習 2 回目の模擬フィッシングメールの配信後，アクセス用 Web サーバへのアクセスは無かった．

7. 考察

演習 1 回目の模擬標的型攻撃メールについては，開封がアクセス用 Web サーバに記録されている 4 件中 3 件までが当日の日中に開封が行われており，実際に攻撃を受けた場合は，直ちに社内へ注意喚起を行う等の処置が必要であると言える．

なお，模擬標的型攻撃メールの配信の後に行った模擬フィッシングメールの配信では，アクセス用 Web サーバへのアクセスがなかったことから，演習により不審メールに対する危険予知能力の向上に効果があったと考えられる．

8. まとめ

サイバー攻撃は容易に防ぎきれるものではなく，入口対策としての従業員の意識向上が最も重要である．セキュリティ対策への設備投資がままならない中小企業ではなおさらである．加えて，コスト削減，利便性の面から，情報セキュリティ対策が未整備，あるいは情報セキュリティポリシーが整備・周知されていない状況下で個人所有の携帯端末を業務に使用する顕著な動向が見られる． そのため，今後は携帯型端末を標的とした攻撃が増加していくことが予想される．セキュリティへの意識向上には，座学よりも演習・体験型教育が有効である．このことから，「顧客企業の従業員のセキュリティ意識向上により，業務不能化（社内情報インフラ停止）や情報漏えい（外部サーバへの不正送信）を防止する」ことを狙いとして，ソーシャルエンジニアリングの観点を導入した攻撃方法の統合マップとそれに基づいた体系的な演習が可能な教育訓練用システムを開発した．これまで社内で実施した模擬標的型メール攻撃と模擬フィッシングメール攻撃の演習を通じて，本メール攻撃危険予知訓練システムの有効性が確認された．

以上を要するに，本システムは不審メールに対する危険予知能力の向上に資するものであることが推断できる．

謝辞 評価試験にご協力いただいた弊社社員の皆様に，謹んで感謝の意を表する．

参考文献

[1] シマンテック: インターネットセキュリティ脅威レポート 2012 第 17 号, http://www.symantec.com/ja/jp/security_response/publications/archives.jsp
[2] シマンテック: インターネットセキュリティ脅威レポート 2013 第 18 号, http://www.symantec.com/ja/jp/security_response/publications/threatreport.jsp
[3] 経済産業省商務情報政策局: サイバーセキュリティに関する課題と取組について, http://www.meti.go.jp/policy/netsecurity/downloadfiles/120615kumamotoken-koen.pdf
[4] 株式会社インプレス R&D: スマートフォン利用動向調査報告書 2013, http://www.impressrd.jp/news/121204/smartphone2013
[5] トレンドマイクロ株式会社: 2012 年 6 月 企業におけるスマートフォン，タブレット端末の BYOD 実態調査, http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20130821051937.html
[6] 総務省: 新たなＩＴ戦略の策定に向けて,平成２５年４月２４日, http://www.kantei.go.jp/jp/singi/it2/kisou/dai2/siryou4.pdf
[7] 内田勝也 et al.: 情報セキュリティ心理学の提案, 情報処理学会研究報告. CSEC, 2007(16), 327-331, 2007-03-01
[8] 一般社団法人 JPCERT コーディネーションセンター: 2009 年度 IT セキュリティ予防接種調査報告書, 2011 年 3 月 9 日