［報告］

情報セキュリティ意識向上への取り組み ～標的型攻撃メールを想定した防災訓練の実施

東京都赤十字血液センター
太田祐平，辻　由紀，相良智則，照井健良，染谷由美子，西田一雄，加藤恒生

Approach to raising information security awareness Implementation of disaster drills based on targeted attack mail

Tokyo Metropolitan Red Cross Blood Center
Yuhei Ota, Yuki Tsuji, Tomonori Sagara, Kenryo Terui,
Yumiko Someya, Kazuo Nishida and Tsuneo Kato

抄　　録

IT社会の進歩によって業務効率が向上している反面，情報セキュリティに関するリスクは高まっている。こうしたリスクは技術的な対策だけで回避することが難しく，職員一人ひとりの意識を高めることが課題となっている。そこで，情報セキュリティ意識の向上を目的に訓練用偽装メールを各部署・全職員に抜き打ちで一斉送信し，標的型攻撃メールを想定した防災訓練を実施した。結果，１回目の訓練でウイルス感染とみなした部署は30部署中26部署，２回目の訓練では８部署であった。要因は知識不足だけではなく，リスク抑制に繋がる情報共有が部署内でなされていないことが意識調査から判明した。その改善を促したことで２回目の訓練では多くの部署でリスクが回避できており，防災訓練はセキュリティ意識の向上に有効であるという結論を得た。今後も防災訓練を定期的に実施し，継続的に計画・実施・評価・改善していく体制の構築が課題となる。

【はじめに】

通信技術の発達した現代社会においては，情報の発信や収集のためにインターネットの利用は不可欠になっている。その一方でインターネットを悪用してコンピュータネットワーク内のシステムを破壊したり，データが詐取されるなどのサイバー攻撃による被害は世界規模で発生しており，社会的責任のある各企業やその企業を利用する顧客にとって大きな脅威となっている。それはもはや国家の安全保障に影響を及ぼす恐れもあるほどの社会問題になっている。こうしたサイバー攻撃は情報技術の発達に伴い複雑かつ高度に進化しており，サイバー攻撃による被害は増加の一途をたどっている。サイバー攻撃の一種である標的型攻撃メールとは特定の企業や組織の情報の搾取を目的に近年増加している攻撃手法である。攻撃者はターゲットが不審感を持たないような内容の案内メールを送信し，不正プログラムを組み込んだ添付ファイルやURLをクリックしたターゲットのパソコンをウイルスに感染させる。その手法は非常に巧妙であり，世界的に注視されている。近年，標的型攻撃メールの被害は増加傾向にあり，日本

論文受付日：2018年２月28日
掲載決定日：2018年10月23日

国内でも顧客の個人情報や組織の機密情報等の漏えいを許してしまっている事例が多く発生している。警察庁ではサイバーインテリジェンス情報共有ネットワーク[1]により，情報窃取を企図したとみられるサイバー攻撃に関する情報を事業者等と共有しており，同ネットワークを通じて把握した平成28年の標的型攻撃メールの件数は4,046件で，平成27年より218件増加した[2]（**図1**参照）。

標的型攻撃メールはセキュリティソフトでは検知できない場合があるため技術的対策だけでは不十分であり，さらなる情報セキュリティ対策として人的な対策を施す必要がある。そこで，職員一人ひとりが標的型攻撃メールに対応できるようになるため，情報セキュリティ意識の向上と改善を目的に『ITセキュリティ予防接種』と銘打った標的型攻撃メールの防災訓練を実施したので報告する。

【方　　法】

平成28年12月と平成29年1月に各1回ずつ，合計2回の防災訓練を実施した。1回目は内部関係者，2回目は外部関係者を装った訓練メールを各部署･全職員を対象に抜き打ちで一斉送信する。送信メールにはVisual Basic for Applicationsを組み込んだMicrosoft OfficeのExcelファイルやWordファイルを添付する。メール受信者がなりすましの訓練メールに気付くことができずに添付してあるファイルのプログラムを実行してしまった場合は，まずウイルスに感染したかのような画面が表示され，数秒後に訓練メールであることを伝える主管課からの注意喚起画面が表示される。プログラムが実行された端末やユーザーを特定するためのログはグループ内の共有サーバー上に作成した任意のフォルダへ自動送信され，実行状況を集計できる仕組みとした。この2回にわたる訓練をとおしてセキュリティ意識の向上・改善の効果検証を行うこととした。また，訓練実施後に各施設各部署の担当者に意識調査を行い，実施結果を踏まえた原因の分析と改善策についてまとめた資料を全部署の課長級以上が出席する東京都赤十字血液センター情報セキュリティ委員会において報告し全体共有した（**図2**，**図3**参照）。

【結　　果】

30部署220件のメールアドレスへの送付に対し，1回目の訓練ではプログラムを実行した部署が26部署・プログラム実行回数127回，2回目の訓練では8部署・プログラム実行回数12回という実施結果となった（**図4**参照）。

1回目の訓練でプログラム実行回数が多かった要因は大きく分けて2つあった。1つめの要因は，脅威への認識不足である。「メールの文章を見て不審に思わなかった」や「WordやExcelのプログラムを実行するだけでウイルス感染するとは思っ

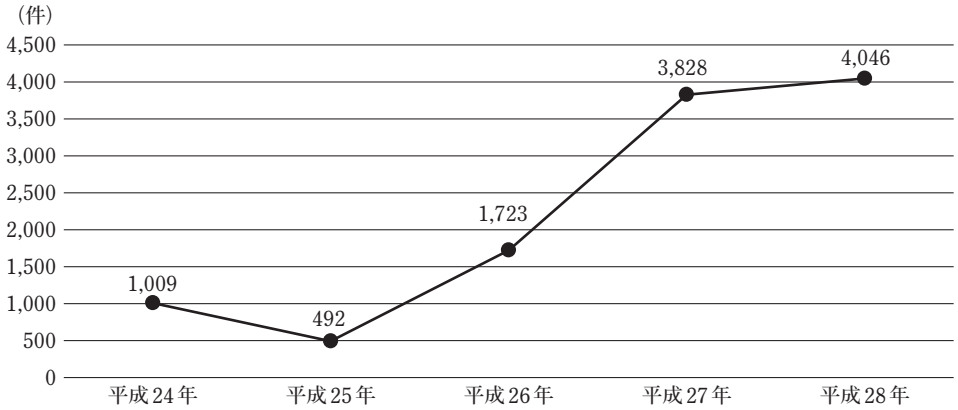


図1　標的型攻撃メールの被害件数の推移

	1回目の訓練	2回目の訓練
訓練対象者	東京都赤十字血液センター 全職員	東京都赤十字血液センター 全職員
メール送信対象アドレス	220アドレス （個人メール・共有メール）	220アドレス （個人メール・共有メール）
訓練用メール送信日	平成28年12月5日 （月曜日）	平成29年1月31日 （月曜日）
メール内容	平成28年の賞与・給与・ 確定申告計算システムに ついての案内	年末調整の過不足額の精算 手続きについて
添付ファイルの形式	エクセル 拡張子[.xls]	ワード 拡張子[.doc]
集計期間	1週間	1週間

参考：「年末調整の過不足額の精算手続きについて.doc」添付ファイル画面キャプチャ

年末調整の過不足額の精算手続きについて（還付金）

関係者各位

総務局　総務部　税務課長

年末調整の過不足額の精算手続きについて以下のとおり進めてください。

はじめに年末調整加過納額還付請求書を記入してください。

請求書を記入するにはこちらをクリックしてください。

クリックしても何も起こらない場合は、

画面上部にある【編集を有効にする】【コンテンツの有効化】を押してください。

記入が終わったらご返信ください。

こちらから残存過納額明細書を添付して、税務局へ代理申請します。

源泉所得税及び復興特別所得税の年末調整過納額還付請求書兼残存過納額明細書

税務署受付印

※整理番号

住所又は所在地　〒　電話　－　－

（フリガナ）

氏名又は名称

個人番号又は法人番号

（フリガナ）

代表者氏名　㊞

平成　年　月　日

税務署長殿

平成　年分年末調整により生じた過納額については、次の事由により還付することができなくなったので、所得税法施行令第313条第2項の規定により、下記のとおり還付を請求します。

図2　標的型攻撃メール防災訓練の概略

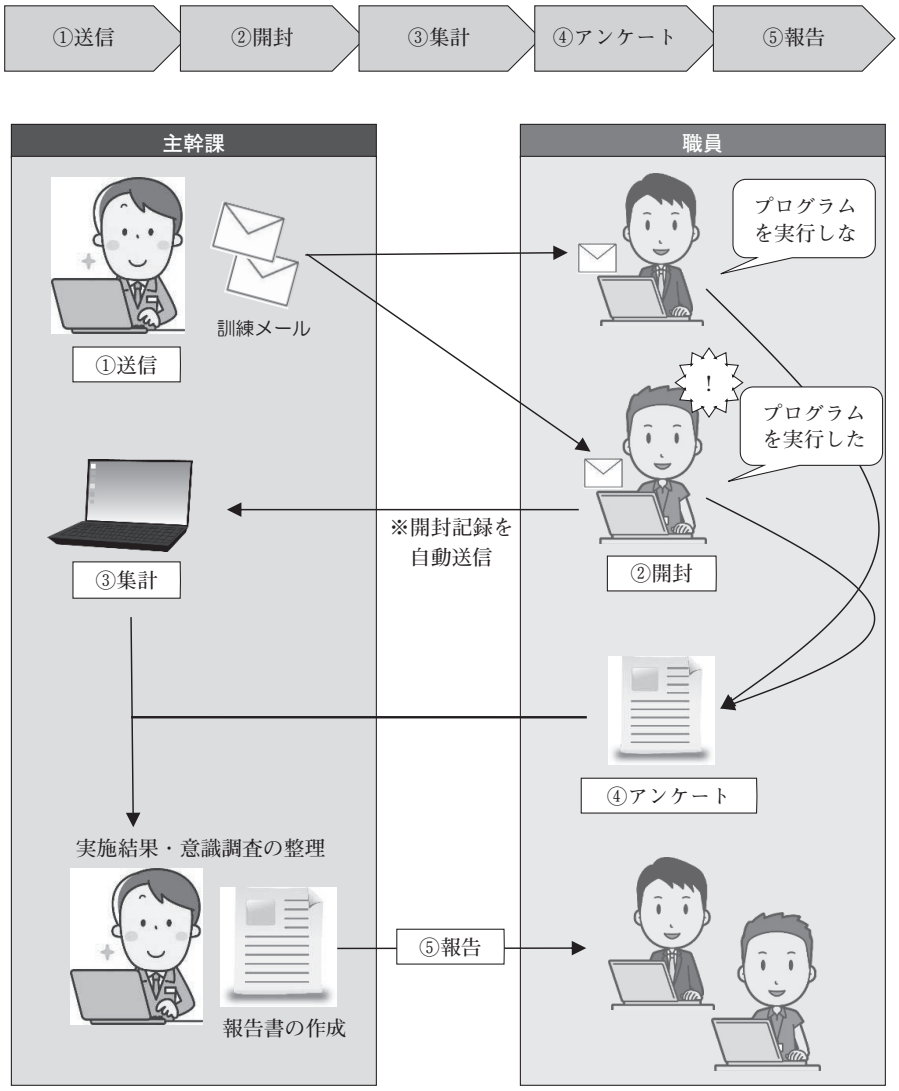


図３　標的型攻撃メール防災訓練の仕組み

ていなかった」等，標的型攻撃メールの特徴である「なりすまし」に気付かず，安易にプログラムを実行してしまっていることが浮き彫りになった。もう１つは，被害を拡大させないために重要である部署内での情報共有が充分になされていなかったことである。不審なメールが届いていることやメールを開いてしまったことの「報告･連絡･相談」が徹底されておらず，被害を最小限に抑えられない状況となっている部署が多かった。このような個人レベル，組織レベルでのセキュリティ意識の現状と訓練結果をまとめ，東京都赤十字血液センター情報セキュリティ委員会において報告し課員へ周知するよう依頼した。そのうえで２回目の訓練を予告することなく実施した。１回目の訓練結果に対して，２回目の訓練では大幅に標的型攻撃メールを回避することができ，大きな改善効果が得られた。

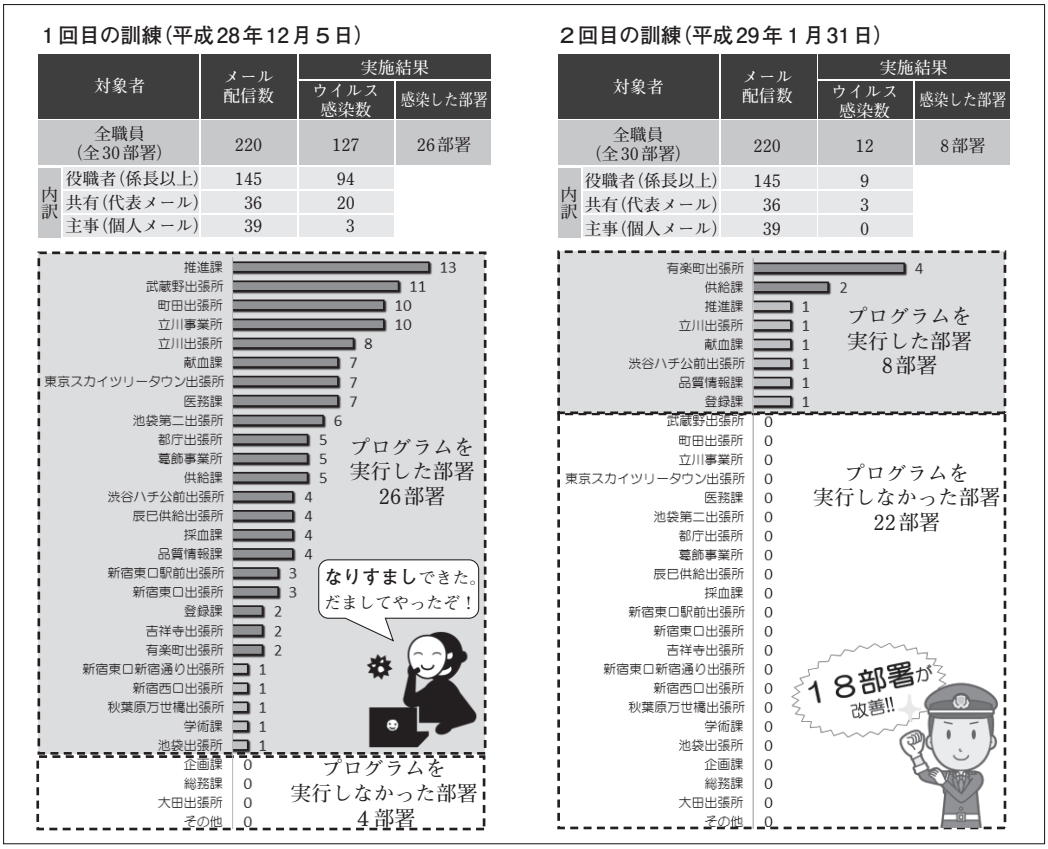


図４　標的型攻撃メール防災訓練の実施結果（部署別）

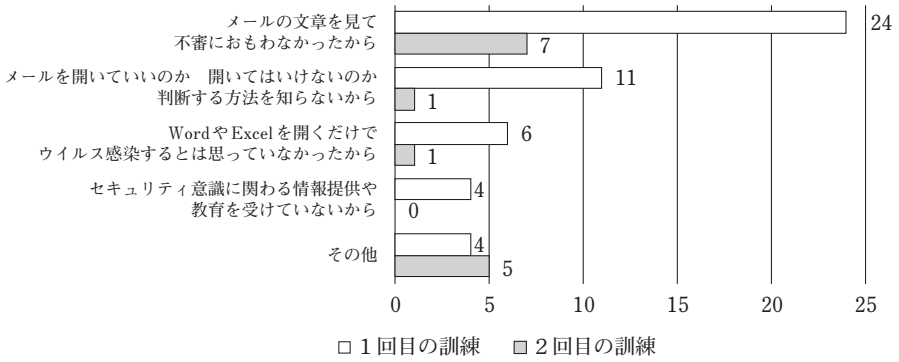
【考　　察】

１回目の訓練では，標的型攻撃メールにより被害を受けている日本年金機構や大手旅行会社の個人情報流出事例の危険性が自らの組織にも存在するという現状を知ることができた。それと同時に知識のない職員に標的型攻撃メールの脅威を身を持って体験させることができた。それを全体に共有したことで２回目の訓練では各部署が問題点を改善し，組織全体のセキュリティ意識が向上する効果を確認できた。

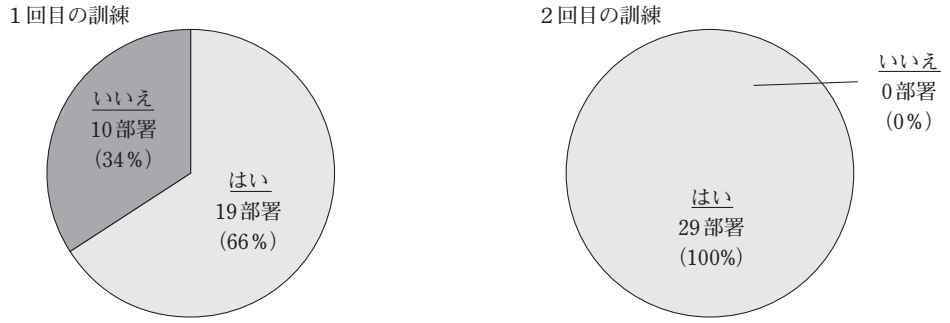
それは標的型攻撃メールの認知度・理解度についての意識調査において，訓練前では「よく知っている」との回答が全体の３割であったのに対して訓練後には全体の８割が「十分に理解した」との回答に変わり，また，１回目の訓練で課題となった部署内の情報共有は，２回目の訓練では全部署において報告・連絡・相談が行われるように改善されたことからも見て取れる（**図５**参照）。

今回，２回にわたる情報セキュリティ防災訓練を実施したことによって，東京都赤十字血液センターにおける現状と人的対策の重要性を認識することができた。しかしながら，継続して情報資産を守り続けていくためには，技術的対策と人的対策の両面におけるセキュリティ対策を実施する必要がある。そのためにはファイル添付形式の攻撃メールやURLリンク形式の攻撃メール，ランサムウェア形式の攻撃メール等の多種多様なサイバー攻撃に対応する防災訓練を定期的に実施し，計画・実施・評価・改善を繰り返していく体制（PDCAサイクル）の構築ができるかが課題となる。また，

〈アンケート〉
標的型攻撃メールだと気付かなかった原因は何ですか？（複数回答可）
プログラムを実行した部署（1回目：26部署・2回目：8部署）から回答



〈アンケート〉
標的型攻撃メールに気付いた人が上司や同僚に相談・報告を行い，情報共有を行っていたか？
調査対象29部署から回答



〈アンケート〉
標的型攻撃メールの認知度・理解度（特徴や対応方法等）について，お答えください。
調査対象29部署から回答

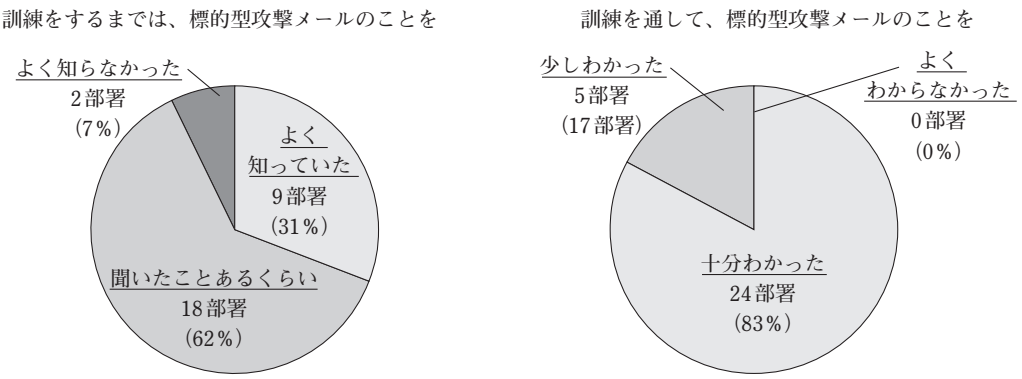


図5　アンケートによる意識調査の結果

今後は地域の垣根を越えて他センターと連携した合同訓練を実施するなど，より組織的かつ効果的な情報セキュリティ対策への取り組みを検討したい。

参考文献

1） 日立ソリューションズ：サイバーインテリジェンス情報共有ネットワークとは
（https://securityblog.jp/words/cyber_intelligence.html）

2） 警察庁：平成28年中におけるサイバー空間をめぐる脅威の情勢等について
（https://www.npa.go.jp/news/release/2017/20170323cyber_jousei.html）