投資育成主催
投資先向け「標的型メール合同訓練」結果報告

中堅企業ほど引っかかりやすいって本当?!
訓練から見えた被害傾向と対策

中小企業のIT活用が進む一方で、情報セキュリティ分野では日々、新たな脅威が出現しています。ひとたび情報漏えいなどの事故が発生してしまうと、自社の業務に影響が及ぶだけではなく、取引先に対しても大きな迷惑をかけるリスクがあります。特に、「標的型攻撃による被害」は、独立行政法人情報処理推進機構（以下、IPA）が発表している「組織における情報セキュリティ10大脅威」の第1位に選ばれるなど、各組織で対策の必要性が高まっています【図1】。このような背景から、投資先企業向けに標的型メールに対する合同訓練を実施しましたので、その結果をご報告します。

東京中小企業投資育成
株式会社
総務企画部主任
平沼 優

大企業に迷惑をかけるかも
標的型メールにご用心

そもそも標的型攻撃とは、メールの添付ファイルを開かせたり、悪意あるウェブサイトにアクセスさせたりすることで、パソコンにウイルスを感染させ、業務上の重要情報や個人情報を盗み取る攻撃のことです。特に注意したいのは、情報窃取の本命である「大企業を狙うための踏み台」として、中小企業が狙われるケースです。セキュリティレベルが低くなりがちな中小企業に、標的型攻撃でウイルスを感染させて、大企業との取引内容や担当者名などを盗み出します。その情報をもとに巧妙な偽メールを作り、大企業に攻撃を仕掛け重要情報を盗み出す手口であり、中小企業のセキュリティ不備により、取引先の大企業に迷惑がかかる可能性があります。

規模が大きくなるほど
開封率は高い傾向に

今回の標的型メール合同訓練には、168社1万5425名にご参加いただきました。全体の結果は、第1回目の開封率が18・5%、2回目が13・5%となりました。2回目の訓練メールは1回目と比べ、難易度の高いものでしたが、1回目の訓練効果があったためか、168社中104社に改善が見られました。

売上高別の開封率では、「売上高が大きくなるほど開封率が高くなる」という傾向があり、特に売上高50億~200億円、同200億円以上の会社では、1回目、2回目ともに全体平均を上回る結果となりました【図2】。売上高が大きくなるほど、顧客情報などの機密情報を多く扱うようになり、情報漏えい時のリスクが高まります。そのため本来であれば、売上高の大きな会社ほどセキュリティ対策に力を入れていると思われますが、標的型メールへの対応は、まだまだこれからという会社が多いようです。

従業員数別に分析した結果において

図1●情報セキュリティ10大脅威 2018

順位	組織における育成	昨年順位
1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺による被害	ランク外
4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
5位	脅威に対応するための セキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービスの 停止	4位
10位	犯罪のビジネス化 （アンダーグラウンドサービス）	9位

独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2018」より引用
https://www.ipa.go.jp/security/vuln/10threats2018.html

図2●売上高別開封率

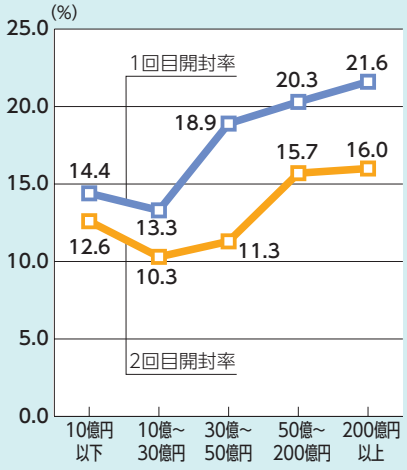
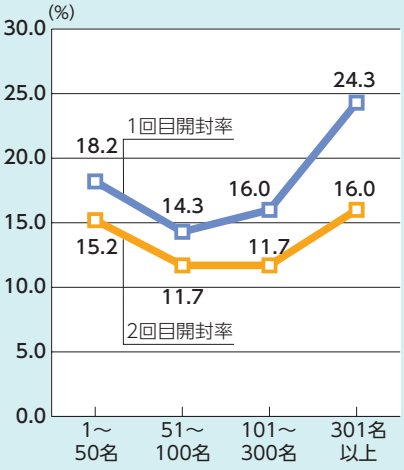


図3●従業員数別開封率



も、「301名以上の会社がもっとも開封率が高く」、規模が大きくなると開封率が高くなる結果となりました【図3】。小規模企業に比べ、複数の拠点があることが多く、全社的に従業員のセキュリティ意識を向上させることが難しいのが理由の一つではないかと考えられます。

不動産業、サービス業、運輸業は「要注意」！

次に業種別に分析すると、「不動産業、サービス業、運輸業の開封率が高い」結果となりました【図4】。特に1回目の訓練では、訓練メールの送信者欄に会社名の記載がなく、個人名のみの記載であったことから、BtoCビジネスの多い不動産業やサービス業の開封率が高くなったのではないでしょうか【図5】。一方で、日頃からセキュリティ分野への意識が高いと考えられる情報通信業については、1回目が2・1%、2回目が6・8%と非常に低い結果となりました。

システム対策では不十分！全従業員の意識向上がカギ

標的型攻撃への対策として、セキュリティベンダ各社から次々に製品やサービスが発表されており、システムを最新のものに更新することも有効な対策の一つです。しかし、攻撃者も日々攻撃手法を進化させていることから、ただシステムで防ぐのみならず、受信者である各従業員が自身で不審なメールを見分けることも重要です。標的型メールによるウイルス感染は、パートやアルバイトであっても、メールを利用する従業員であれば誰でも起こり得るものであるため、「全従業員のセキュリティ意識向上」が課題となります。2回目の訓練で開封率が0%であった、株式会社シンクスコーポレーション（神奈川県愛甲郡）では、不審なメールに対する従業員への注意喚起策として、標的型メールの事例を定期的に社内掲示板にアップしているようです。今回の訓練で開封率の高かった会社では、従業員のセキュリティ意識向上の第一歩として、まずは同様に取り組まれてみるのもいいかもしれません。標的型メールの事例については、IPAが公表している「標的型攻撃メールの例と見分け方」*に記載がございますので、活用されてみては如何でしょうか。

次回のメール訓練は、2018年秋ごろを予定しております。ぜひ、従業員の皆様のセキュリティ意識の向上にお役立てください。ご参加、お問い合わせは投資育成担当者まで。お待ちしております。

【訓練の概要】
日　時：2018年3月8日（1回目）、同20日（2回目）
参加数：168社、1万5425名
開封率：18・5%（1回目）、13・5%（2回目）
参加費：無料

参加企業の声

株式会社村井（東京都豊島区）

お客様の大事な個人情報を扱っているので、日頃から「不要な添付ファイルは開かないように」との注意喚起はしている。次回訓練にも引き続き参加していきたい。

株式会社明輝（神奈川県厚木市）

これまでメール訓練サービスがあることは知っていたが、費用面等を検討した結果、訓練をするにはいたらなかった。今回のような合同訓練は非常にありがたい。

マイナンバーの取り扱いが始まるころから、セキュリティ対策には力を入れてきた。仕組みで防げることもあるが、やはり重要なのは各社員の意識だと思う。今回の訓練でセキュリティ意識を高めるきっかけになったのではないか。

株式会社シンクスコーポレーション（神奈川県愛甲郡）

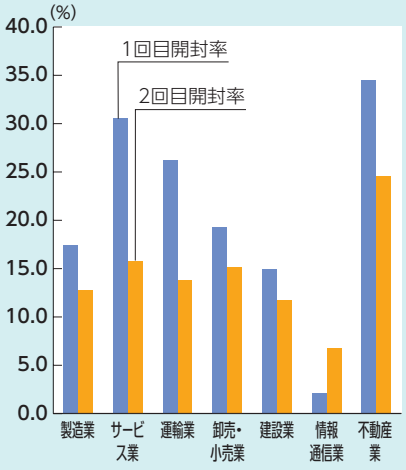
「身に覚えのないメールは開かないように」というアナウンスを周知徹底している。標的型メールの事例を定期的に社内掲示板にアップすることで、社員のセキュリティ意識向上を図っている。

第1回目の訓練では、添付ファイルを開いてしまった社員もいましたが、ほとんどの社員がシステム担当宛てに連絡をくれたので、開いてしまった後の二次対応の訓練にもなった。

図5●訓練メールの内容

	1回目	2回目
送信者名 <メールアドレス>	佐藤和子 <kazuko-sato@qmeil.jp>	日本医療センター機構 総務 <japan-medicalcenter@yehoo.jp>
件名	さきほどの写真の件	医療費通知のお知らせ
本文	お世話になっております。 の写真送らせて頂きます。 宜しくお願い致します。 佐藤	各位 以前よりアナウンスさせていただいているとおり、 今月より、 「医療費のお知らせ」が配信されるようになりました。 内容についてご確認をお願いします。 また、医療費通知のお知らせは、適正な保険診療の啓蒙、医療機関による診療報酬の不正請求の抑止効果等、医療費適正化の取り組みの一つとして実施しています
添付ファイル名	写真.doc	医療費通知のお知らせ_2月分.doc
不審さを見破るポイント	●これまで受信したことがない、自分の業務とは関係のないメールドメインから来ている。 ●心当たりのない内容だが興味をそそる内容 ●日本語が不自然。　など	●これまで受信したことがない、公的機関からのお知らせがきている。 ●こうした通知がメールで送られてくることはない。　など

図4●業種別開封率



＊独立行政法人情報処理推進機構「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/security/technicalwatch/20150109.html