特集
標的型メール

SECURE SKETCH BOOKS
VOLUME 2

標的型メール
攻撃訓練の
新たなカタチ

なぜ開く？！
ウイルスメールを
開く社員の傾向と
組織的な対策

あらためて考える
標的型メールへの
セキュリティ対策

EDITED BY
SECURE SKETCH MARKETING TEAM

目次

本資料は、過去にNRIセキュアがお客様に対して送付をした「NRIセキュアニュースレター」にて掲載された記事を基に再構成したものです。

標的型メール攻撃訓練の新たなカタチ

サイバーセキュリティサービス一部　吉田 直子

本記事は2017 年 5 月に発行したNRIセキュア ニュースレターで掲載されたレポートを基に再構成しています。

はじめに

組織としての標的型メール攻撃の耐性を高めたいという多くのご要望から、弊社では標的型 メール攻撃訓練を実施しておりますが、昨今、標的型攻撃による詐欺の手口は時間と共に巧 妙になっています。

標的型メール攻撃訓練の実施に際し「このまま同じ訓練を続けても良いのであろうか」というお客様からの声をよく耳にします。 本稿では、標的型メール攻撃訓練の意義を振り返りつつ、新しい標的型メール攻撃訓練のカタチを考察します。

標的型メール攻撃訓練における３つの種類

2017 年 4 月、警視庁より平成２8 年度標的型メールの件数が公表されました。ばらまき型は全体の90%を占め、依然としてメール攻撃の主流となっています。

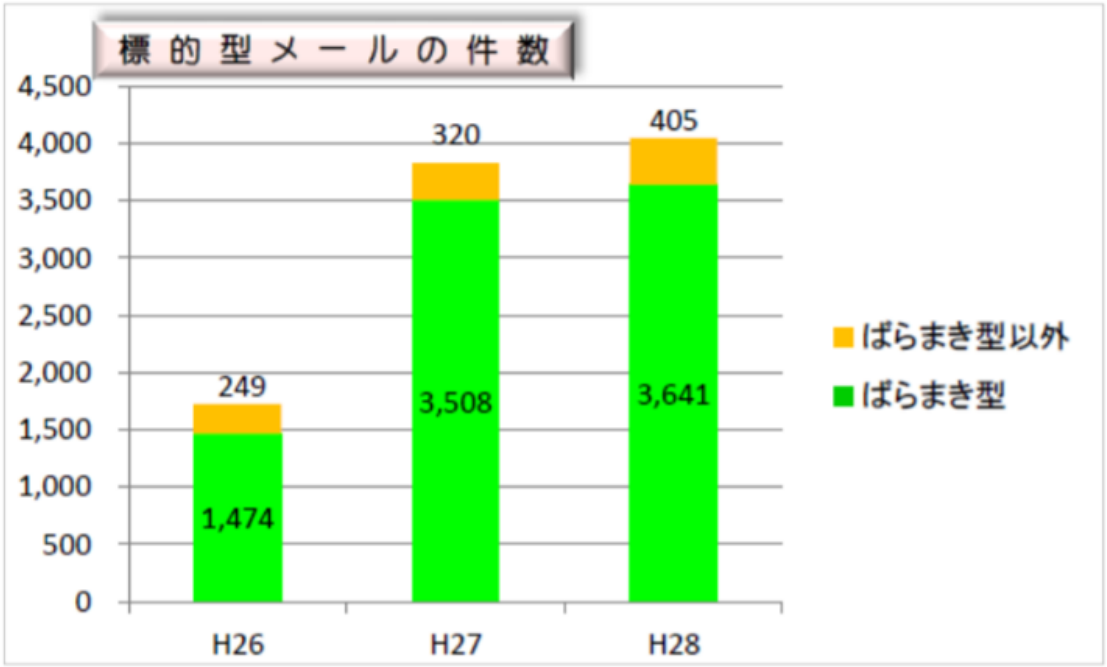


図. 標的型メールの件数

出所）警視庁：平成 28 年におけるサイバー空間をめぐる脅威の情勢について
http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/info_security.files/graph.pdf

上の表からは昨年度からの大きな変化が見られないことから、標的型メール攻撃の耐性を高める対策として、トレンドの攻撃手法の学習も交えつつ引き続き標的型メール攻撃訓練を行うことが肝要であると考えます。

弊社「標的型メール攻撃訓練シミュレーションサービス」（以下標的型メール攻撃訓練） では、お客様の実施目的に沿った訓練をご提供しています。そのうち本稿では、３つの訓練を取り上げます。以下に ３つの訓練の実施目的と効果の概要をまとめます。

＜標的型メール攻撃に対する３つの訓練＞

1. 従来型訓練

訓練対象者に訓練メールの受信を通して標的型メール攻撃を学習する。 これだけでも繰り返せば下がる。開封率は 0 にはならない。

2. エスカレーション型訓練

万が一、訓練メールを開いた場合に報告することを体験するための訓練。報告者は未開封者のみ。これによって標的型メール攻撃から生ずる被害が拡大することを防ぐことにつながる。

3. 拡張版エスカレーション型訓練

実施目的は訓練メールだと気づいたら報告すること を体験するための訓練。報告者は、開封・未開封者。これにより、攻撃者が攻撃を成立させるまでの時間を短縮することが期待できる。

弊社がご提供する標的型メール攻撃訓練サービスにおいて、「従来型訓練」という呼称は 本来使っていませんが、他の２つの訓練と区別するために本稿内に限り利用しています。 それでは、それぞれの訓練について、次章以降でご紹介します。

従来型訓練とは

「従来型訓練」とは、擬似攻撃メール（以下訓練メール）を訓練対象者に送信し、標的型攻撃メールであるかを見抜けるか否かという訓練です。一般的には、全訓練対象者に占める開封者の割合「開封率」という指標を用いることが多いと思います。標的型メール攻撃訓練では、訓練メールの添付ファイルを開いたか、訓練メール本文中の URL をクリックした場合 を「開封した」とみなします。訓練の回数を重ねることで開封率が下がることが弊社統計より分かっています。

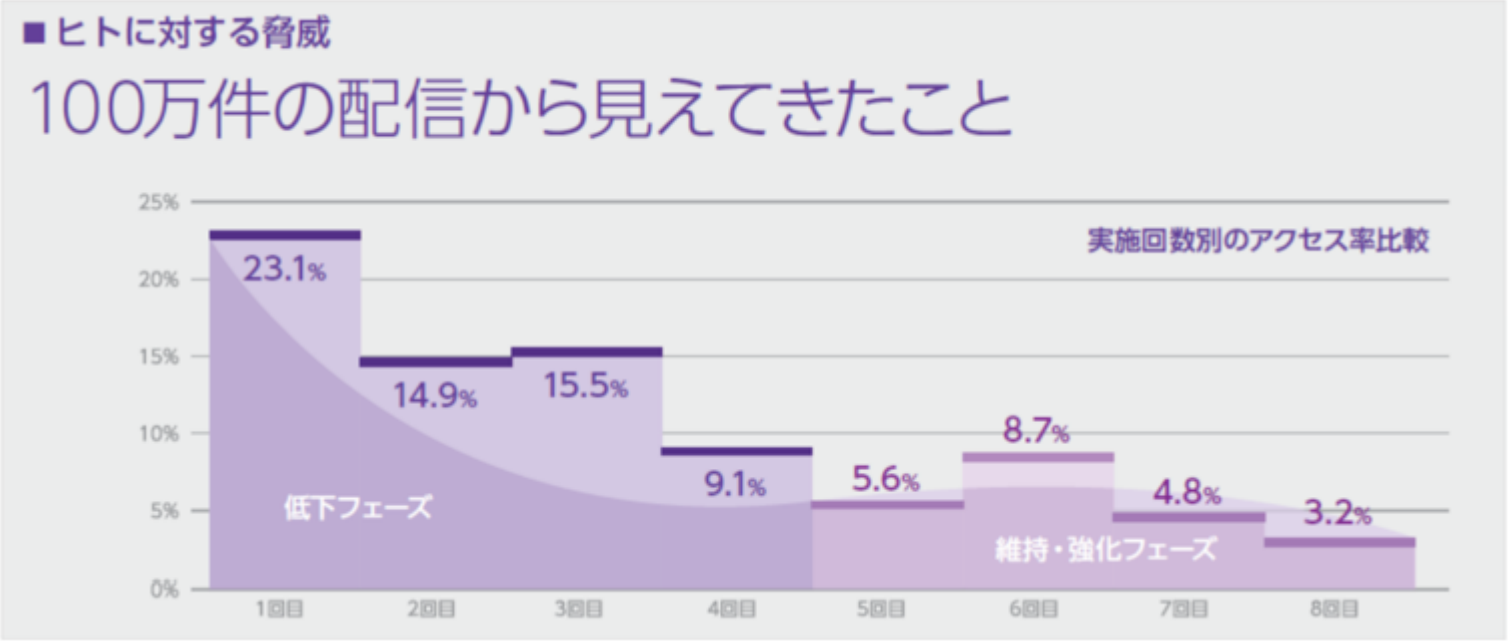


図. 訓練メールの配信件数と開封率

出所）NRIセキュア：サイバーセキュリティ傾向分析レポート2016

「従来型訓練」では、訓練対象者が標的型メール攻撃の存在や実際に攻撃に使われている 手法を知り、自分にも起こり得ることだと認識できるよう教育啓発することで標的型メール 攻撃に対する耐性の向上を図ります。

エスカレーション型訓練とは

「エスカレーション型訓練」とは、訓練メールを開封してしまった場合、訓練対象者が自組 織の所定のルールに即した行動を取れるか、を組織内で確認することを目的とした訓練で す。この訓練では、訓練メールの添付ファイルを開封もしくはメール本文の URL のリンクを クリックした場合、添付ファイルやリンク先の Web ページ上に各実施企業で定める所定のルールに則して行動するように促した文言等を掲載したりします。

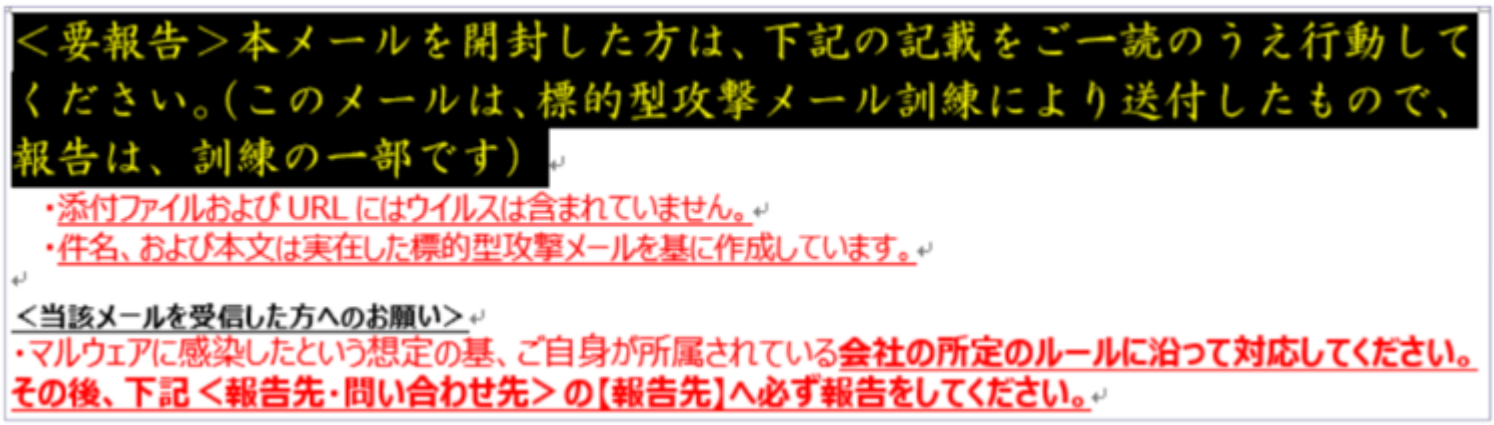


図. エスカレーション型訓練メールの添付ファイル・URLリンク先ページイメージ

開封者がこの文言を見て、所定の連絡先に報告します。もし、開封者がルールに則った行動を取らなかった場合でも、事前に開封状況を連絡先の従業員が把握しておけば、所定のルールに則して行動を取るよう開封者に促し、開封者が所定のルールで定めた事項を全て完了 するまでフォローする、これが「エスカレーション型訓練」の一連の流れとなります。

果たして「エスカレーション型訓練」は有効な訓練となり得るのか、次の章では弊社の統計データを交え考察します。

未開封の多くは「訓練メール」だと気づいている

弊社統計に「開封された訓練メールの約 95%」は配信後 1 日以内に開かれているというデータがあります。

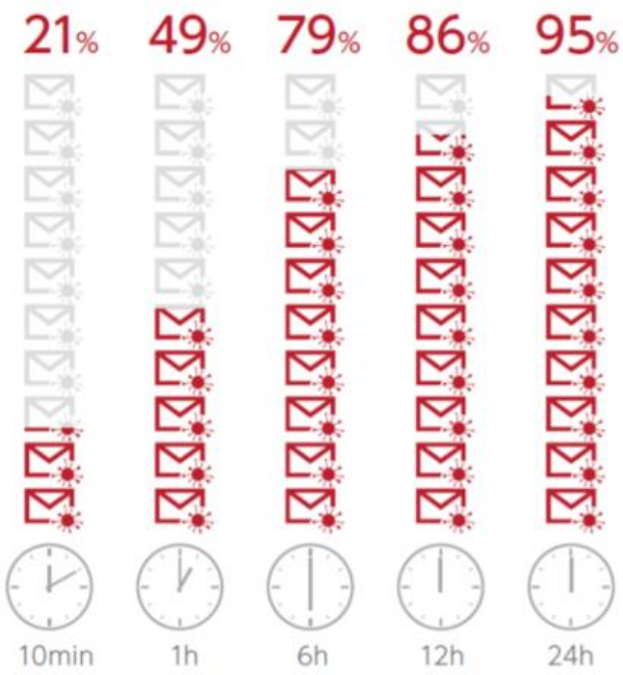


図. 開封された標的型メールにおける開封率推移（時間別）
出所）NRIセキュア：サイバーセキュリティ傾向分析レポート2015

また、訓練メールを「開かなかった」またはクリックしなかった理由として「不審なメー ルであると判別できた」とした人は 、筆者の経験上70%を超えると考えています。 もし、訓練メールを不審なメールだと気づいてアクセスしなかった人（以下、「未開封 者」）も、「標的型攻撃メールを受信した旨」を然るべき自組織内の報告先にエスカレーシ ョンさせることができれば、リスク管理部門が組織の標的型メール攻撃に対する耐性を、より具体的に把握できる可能性があります。また、組織全体としてエスカレーションしやすい 環境や、組織内ルールの認知率向上を図れることが予想されます。

そこで、開封の有無にかかわらず訓練対象者からの報告までを一連のプロセスとした標的型メール攻撃訓練（以下拡張版エスカレーション型訓練）の意義について考察します。

従来型＋拡張版エスカレーション型訓練のすすめ

前述のとおり「エスカレーション型訓練」で想定される報告者は「開封者」のみですが、「拡張版エスカレーション型訓練」は「未開封者」をも含む点が異なります。

図. 各訓練における報告の流れ

種別	避難訓練に例えた例	指標	メール訓練対象者	
			開封者	未開封者
従来型訓練	火災発見時の対応方法確認（机上訓練）	開封率	●	●
		報告率		
エスカレーション型訓練	火災発生時の対応方法確認と、避難訓練（一部参加）	開封率	●	●
		報告率	●	
拡張版エスカレーション型訓練	火災訓練（避難あり、全員参加）	開封率	●	●
		報告率	●	●

図. 標的型メール攻撃訓練の実施イメージ

「エスカレーション型訓練」は「開封者」だけが報告までの訓練を実施するので、「未開封者」の中には報告先や手順などを把握していない可能性もあります。危機管理の教訓では「普段できないことは絶対できない」と言われており、「未開封者」を含む全員に対して報告する訓練を行わなければ、有事の際に期待する動きができない場合が予想されます。「拡 張版エスカレーション型訓練」は、「未開封者」「開封者」双方から報告されるという効果 を得られるように意図した訓練です。

一方で拡張版を含むエスカレーション型訓練には三つの課題があります。

＜エスカレーション型訓練の３つの課題＞

１．　報告先の体制確保
２．　開封率に影響を及ぼす事前告知を避けたい
３．　標的型メール攻撃訓練の際は、報告先を本来の報告先と変えたい

初めて標的型メール攻撃訓練を行う企業の「開封者」の割合は、弊社の統計では約 21.3%です（2017 年 4 月現在）。一つ目の課題は、訓練対象者が数万人規模の大企業ともなると「開封者」は数千人となるため、予想されるエスカレーションに見合った報告先の体制を確保できていないと、対応しきれなくなることが考えられます。

「エスカレーション型訓練」では、訓練対象を絞って実施するということに加え、報告先を本来の報告先・報告手段ではなく、訓練用の報告先として所属の上司・代替の組織に報告することで、小規模のエスカレーションスキームにしている事例もあります。

前述のような実施上の工夫を踏襲したとしても「拡張版エスカレーション型訓練」の場 合、添付ファイルを開かないもしくはメール本文中の URL リンクを開かない為、「エスカレーション型」の伝達方法では訓練用の報告先等の情報が訓練対象者に伝わりません。

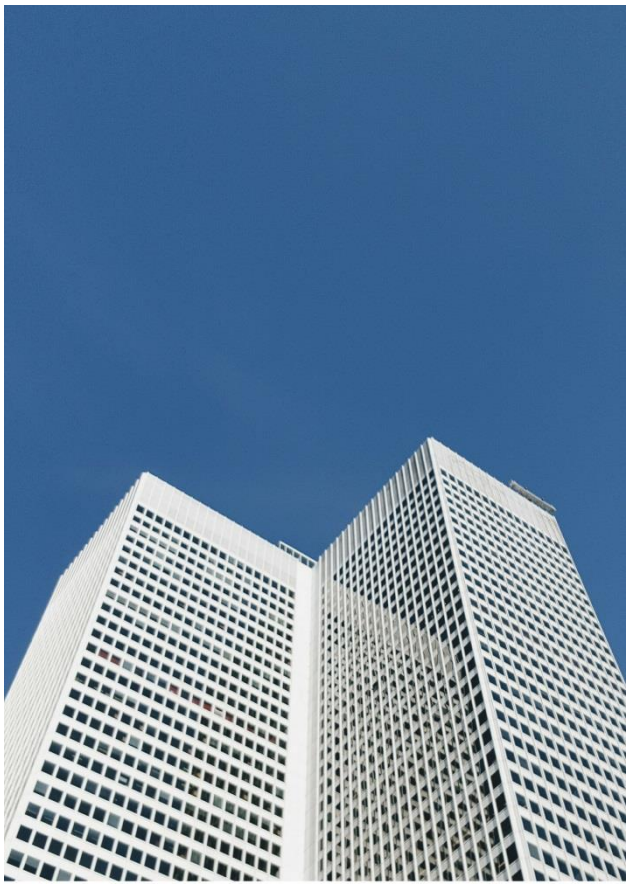
これに 対して「拡張版エスカレーション型訓練」は、標的型メール攻撃訓練の実施期間より先立って訓練の告知をし、その際に訓練用の報告先を訓練対象者に伝えておくことを「エスカレーション型訓練」の実施手順に加えることで解決することができます。告知の際に、本来の報 告先・報告手順も併せて伝達しておくことで、訓練対象者が情報の整理をしたうえで落ち着 いて訓練に望め期待した行動が取られると期待できることから、併せて伝達することをお勧 めします。

二つ目と三つ目の課題は、関係者への事前調整を行うことで解決が可能です。

「拡張版エスカレーション訓練」の主たる目的は、「エスカレーション訓練」より多くの訓練対象者に報告を実戦してもらう点にありますが、もし、事前告知による開封率への影響を避ける点を重視するのであれば、前述の告知は行えないことから、本来の報告先・報告手段のまま「拡張版エスカレーション型訓練」を実施する前提で、その報告先が対応可能な報告者人数や時間帯等の関係者と事前に調整します。

この際、訓練対象者の所属組織の上司等 も訓練内容や報告先を把握しておく必要があるので併せて調整できるとよいでしょう。な お、事前告知の有無にかかわらず、本来の報告先とする場合は同様の調整が必要となると考えます。

おわりに



皆様の組織において、「標的型メール攻撃」への耐性を高めつつ、多層防御の一助となる よう、もう一段上の「拡張版エスカレーション型訓練」を盛り込むことを検討されてみては いかがでしょうか。

本稿が貴社の標的型攻撃の対策検討の一助となれば幸いです。もし、本稿でご紹介した 「拡張版エスカレーション型訓練」へのご関心や、その他標的型メール攻撃訓練におけるお悩みやご興味がありましたら、ＮＲＩセキュアに是非ご相談ください。

関連サービス：

標的型メール攻撃被害シミュレーション

https://www.nri-secure.co.jp/service/assessment/cyberattacksimulation.html

お問い合わせ先：

info@nri-secure.co.jp

なぜ開く？！ ウイルスメールを開く社員の傾向と組織的な対策

マネジメントコンサルティング部　櫻井 宏樹

本記事は2015 年 2 月に発行したNRIセキュア ニュースレターで掲載されたレポートを基に再構成しています。

特集　標的型メール

はじめに

「ウイルスメール が届いていたので、注意喚起のために部内に転送しようとしたら、感染しちゃいました」

「怪しいメールが届いたので、標的型攻撃訓練のメールだと思って、開いたらホンモノだったみたいです」

思わず、「えっ！？」と言いたくなるような報告ですが、ウイルス対応のご支援をしていると少なからず見かける報告でもあります。システム部門であれば、“ウイルスメールは開かず、削除”が当たり前になっているかと思いますが、ユーザ部門では、こうした“ウイルスメールだと分かっているにも関わらず開く人”が実際に存在します。

本稿では、“なぜこの人たちは、ウイルスメールだと分かった上で開くのか”、そして、“それらに対して、どう対策していけばよいか”について解説します。

そもそも、ウイルスメールが届いた場合にどうすればよいか決められているか

“ウイルスメールが届いたら、開かずに削除する”。システム部門の方であれば、当たり前のことだと認識されていると思います。しかしながら、そのことがルールとして明文化されているでしょうか。「わざわざ規定しなくとも、社員も分かっているだろう」と、明文化していない状態になっていないでしょうか。

企業の中には、セキュリティ意識が高く「そんなことは当たり前だ」と思っている社員もいる一方で、「そもそもウイルスって何？」と思っているような、セキュリティ意識がそれほど高くない社員も一定数存在します。

セキュリティ意識の高くない社員にとっては、この“ウイルスメールは開かず、削除”という基本動作が当たり前にはなっていないことが多いです。そのため、まずは“ウイルスメールは開かず、削除”をルールとして明文化し、周知する必要があります。

そして、ルール化・周知を行い、社員がルールを認識していたとしても、残念ながら守られないケースが発生します。“なぜウイルスメールだと分かった上で開くのか”、次章では、その事例を紹介します。その上で、次々章で、“どうルール・手順化し、周知していくべきか”を解説します。

なぜウイルスメールと分かっていても、開くのか？

ウイルスメールだと分かった上で開く理由として、これまでのコンサルティングの現場で多く見かけたケースを、まとめると以下のようになります。

＜ウイルスメールを開いてしまう理由の３つのパターン＞

1. 操作ミス型
2. 興味本位型
3. 業務要件型

それでは、一つひとつを事例を交えながら、問題点と対策を整理していきましょう。

１．操作ミス型

「ウイルスメールのため、開いてはいけない」と認識はできているものの、操作ミス等によりウイルスメールを開いてしまうケースです。

＜事例＞

① ウイルスメールが届いていたので、情報システム部門への報告（あるいは、部内への注意喚起等）を目的として転送しようとした。その際に、誤って添付ファイルを開いてしまった。

② PCの入れ替えに合わせてメール環境の移行をしている際に、新環境でプレビュー機能を無効に設定しないままデータ移行作業を実施していため、ウイルスメールが（プレビュー機能により）開かれてしまった。

問題点と対策

ウイルスメールを再利用しようとしていることや、そもそも削除していないことが問題です。こうした感染を出さないためには、“ウイルスメールは、削除する”ことを周知徹底する必要があります。

また、その際には、「後で消せばいい」、「最終的には消せばいいのだから、報告に使ってから」といった考え方をしないように、**“削除以外の操作を実施せずに、速やかに削除する”**ことを合わせて伝える必要があります。

2.　興味本位型

ウイルスメールだと認識しているものの、本人の操作により意図してウイルスメールを開いているケースです。

＜事例＞

① 知らないアドレスからのメールであり、添付ファイルも付いていたので、ウイルスメールかなと思ったが、件名やメール本文中の記載内容に興味があったため、添付ファイル（あるいは、メール中のURL）を開いてしまった。

② 標的型攻撃メール訓練の実施期間中に来ていた怪しいメールだったので、標的型攻撃メール訓練用の偽ウイルスメールだと判断した。その際に、訓練メールの中身が気になり、訓練メールだから開いても大丈夫だろうと思って、興味本位でメールを開いたところ、実際に送られてきていた本物のウイルスメールだった”。

問題点と対策

ウイルス感染のリスクについて軽視していることが問題であり、ウイルス感染のリスクについて教育することが対策になります。

また、ウイルス感染のリスクについて教育が行われていても、自分の問題、現実的な問題として認識できておらず、対岸の火事となっている場合にも、当該事例が発生する可能性があります。

教育を実施する際には、具体的に“開いた本人にどういったことが起こるのか(単に、”ウイルスに感染しPCが使えなくなる“だけではなく、懲戒処分や損害賠償も起こりうること)”を伝え、自社、他社、そして**自分自身にも被害が及ぶ問題であることの認識を持たせる必要があります**。

また、このケースの場合、「ウイルスメールを開いたとしても、ウイルス対策ソフトがウイルスを駆除してくれるから感染しない」と、ユーザがウイルス対策ソフトを過信していることも多いです。そのため、“昨今のウイルスは、ウイルス対策ソフトであっても駆除できない場合がある。ウイルス対策ソフトを導入していても感染することがある”等も併せて伝えることが望ましいです。

例として記載した後者の事例は、標的型攻撃メール訓練を実施している企業で起こりやすいケースでもあります。標的型攻撃メール訓練を実施する際には、こうした事故を併発しないように、訓練メールであっても開いてはいけないという意識を持ってもらうことに留意しつつ実施することが望ましいです。

3.　業務要件型

業務の性質上、ウイルスメールだと見分けられたとしても開く必要のあるケースです。

＜事例＞

① ウェブサイトに問い合わせ用として公開しているメールアドレスに届いたメールだったが、ウェブサイトを見た上での問い合わせメールであるかは不明瞭だった（例えば、“関係がない製品に関する問い合わせ”や“日本語でしか公開していないサイトへの英語での問い合わせ”など）。しかしながら、問い合わせ用のメールアドレスに届いている以上、確認せずに削除するわけにはいかないので、メール及び添付ファイルを開いて確認したところ、ウイルス感染してしまった。

問題点と対策

ウイルス感染のリスクの観点からは”開かない”ことが大原則ですが、ユーザの業務を遂行するために、ユーザとしては開かなければならない場合があります。

これは、ルールとして“開かず、削除”を規定する一方で、その例外事項として対応する必要があるケースです。その上で、ウイルス感染のリスク（あるいは、感染した後の被害）を低減することを目的とした対策を実施する必要があります。

例えば、例とした記載したケースでは、“不特定多数の外部から届くメールを開くための、適切な対策がなされた専用PCを用意する”こと等が対策となります。また、システム部門によって、こうした“**ウイルスメールを開かなければならない業務”が把握された上で、適切な対策が検討されている状態となっていることが望ましいです**。

上記のうち、”操作ミス型”、”興味本位型”は、いずれも、ユーザの意識・知識向上によって発生を低減できるケースですが、一方で、”業務要件型”は、その性質上、”開かず、削除”とすることが難しく、補完的な対策に頼らざるを得ないケースです。

このケースは、該当する業務としては、多くないと想定されますので、該当業務を洗い出した上で、対策を検討することも可能かと思います。もし、洗い出し及び対策がなされていないのであれば、この機に実施することを推奨します。

どうルール・手順化し、周知していくべきか

前述の内容を踏まえて、どのようにルール・手順化し、周知していくべきなのでしょうか。本章では、ルール・手順・周知の仕方の３つの観点でのポイントを例示します。

＜ルール＞

以下を明記する。

●ウイルスメールが届いた場合は、“開かずに速やかに削除する”。

●やむを得ず(業務上の要件等により)ウイルスメールを開く場合は、事前にシステム(もしくは、セキュリティ)部門の承認（承諾）を得る。

＜手順＞

ルールに定めたことを実施するために、以下のような手順を策定する。

“開かずに安全に削除するための手順”

“やむを得ずウイルスメールを開く場合の申請手順” 等

＜周知＞

上記ルール・手順の周知に加えて、以下の関連事項も合わせて周知する。

【削除する際の留意点】

- **“削除するための手順”に従って、安全に削除する。**
- **後になって誤って開封することのないように、確実に削除する。**
- **再利用をしない（注意喚起や報告等のために再利用しない）。**

【ウイルスメールを開くことのリスク】

- **ウイルスメールを開くことによって、“情報が漏洩する”、“端末が乗っ取られ、外部の攻撃に利用される”等の被害が発生しうる。**
- **被害によって社の信用失墜や（賠償補償などによる）金銭的被害が発生しうる。**
- **結果として、ウイルスメールを開いた人自身の責任が追及される可能性もある。**

【昨今のウイルスメール事情】

- **ウイルス対策ソフトウェア等のシステム対策を導入していても、ウイルス対策 ソフト等に検知されないように作りこまれているウイルスの場合、駆除されずに感染してしまう場合がある。**
- **ウイルス対策ソフトによりウイルスの駆除等が行われていても、完全に駆除されず、ウイルスが残存する場合がある。**

どれも当たり前のことであり、システム部門の方からすれば、「そんなことは既にやっている」、あるいは、「そこまで丁寧に解説する必要があるのか？」と感じる内容かと思います。

しかしながら、実際に事故が発生している状況があるのであれば、対策に不十分な点があったと言わざるを得ません。そして、その不十分となってしまった原因に、“当たり前”との思い込みが潜んでいる場合があります。システム部門とユーザ部門では、“当たり前”と思う内容に差異があります。

まずは、“その当たり前の差異”をご認識いただいた上で、改めて見直してみることを推奨します。

おわりに

本稿では、“なぜウイルスメールだと分かった上で開くのか”を解説した上で、“どうルール・手順化し、周知していくべきか”を解説しました。どの対策も実施すること自体は難しくありませんが、“ユーザの意識”に働きかける必要がある以上、継続的な実施が不可欠となっています。

多くの企業では、新人研修等でこうしたセキュリティに関する研修が行われている一方で、以降、そうした研修は行われてないのではないのでしょうか。ウイルスメール等を含む、新たなセキュリティの脅威とその対策を社員に周知するためにも、配属以降の定期的なセキュリティ研修の実施（例えば、全員社員に対して年1回実施、役職昇格時研修の1コマとして実施等）をご検討されることをお勧めします。

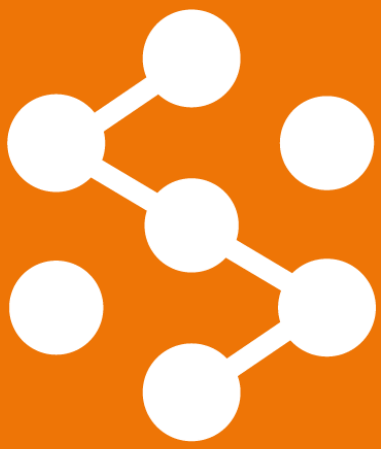
関連サービス：

標的型メール攻撃被害シミュレーション

https://www.nri-secure.co.jp/service/assessment/cyberattacksimulation.html

お問い合わせ先：

info@nri-secure.co.jp



Secure SketCH

セキュリティ経営をシンプルに

https://www.secure-sketch.com