LAC

セキュリティ診断レポート

2018 秋

特集

700組織の事例に学ぶ
標的型攻撃メール訓練「成功の秘訣」

【特集】

700組織の事例に学ぶ
標的型攻撃メール訓練「成功の秘訣」

ラックが提供している「ITセキュリティ予防接種」は、標的型攻撃メールの防災訓練です。
組織のITセキュリティにおいて、ますます重要度を増している標的型攻撃メールへの対策。
ラックが蓄積してきた知見やノウハウをご紹介します。

目 次

はじめに

「サイバー攻撃を疑似体験する」標的型攻撃メール訓練という選択

木 村 雅 弘
セキュリティ診断部　部長

Webアプリケーションセキュリティの研究、ソースコード診断、インシデントレスポンス支援、ラックのJSOC監視システム開発を経て、2013年4月よりセキュリティ診断事業に従事。2018年4月からセキュリティ診断部の責任者を務める。

サイバー攻撃はメールから始まる

近年、頻発するサイバー攻撃では、特定の組織や個人をターゲットにして、情報窃取やデータの改ざん、破壊を行う標的型攻撃が増加しています。

警察庁がまとめた「平成29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」と題されたレポートによると、2017年のメールを使った標的型攻撃の件数は、2016年と比較して、1.5倍となる6,027件を観測しています（下図参照）。

このグラフからは標的型メールによるサイバー攻撃件数が過去5年を通して増加し続けていることがわかります。これは、攻撃者にとってメールが攻撃の起点として悪用できるとともに、守る側では対策が十分に行き届いていない状況の証左でもあると認識しています。

標的型メール攻撃に備えるには、技術的な対策と人的・組織的な対策を組み合わせる必要があります。技術的対策では、ウイルス対策ソフトの導入やネットワーク監視、最新パッチ適用、管理者権限の最小化など様々な方法がありますが、完璧に対応することは難しく、メールが使える環境では防御をすり抜けることがあります。防げない部分は、人的・組織的対策が必要です。標的型攻撃メールを開封してマルウェアに感染した場合は、被害を最小化するためなるべく早く気付き、実害が発生する前に組織的に封じ込めることが重要となります。

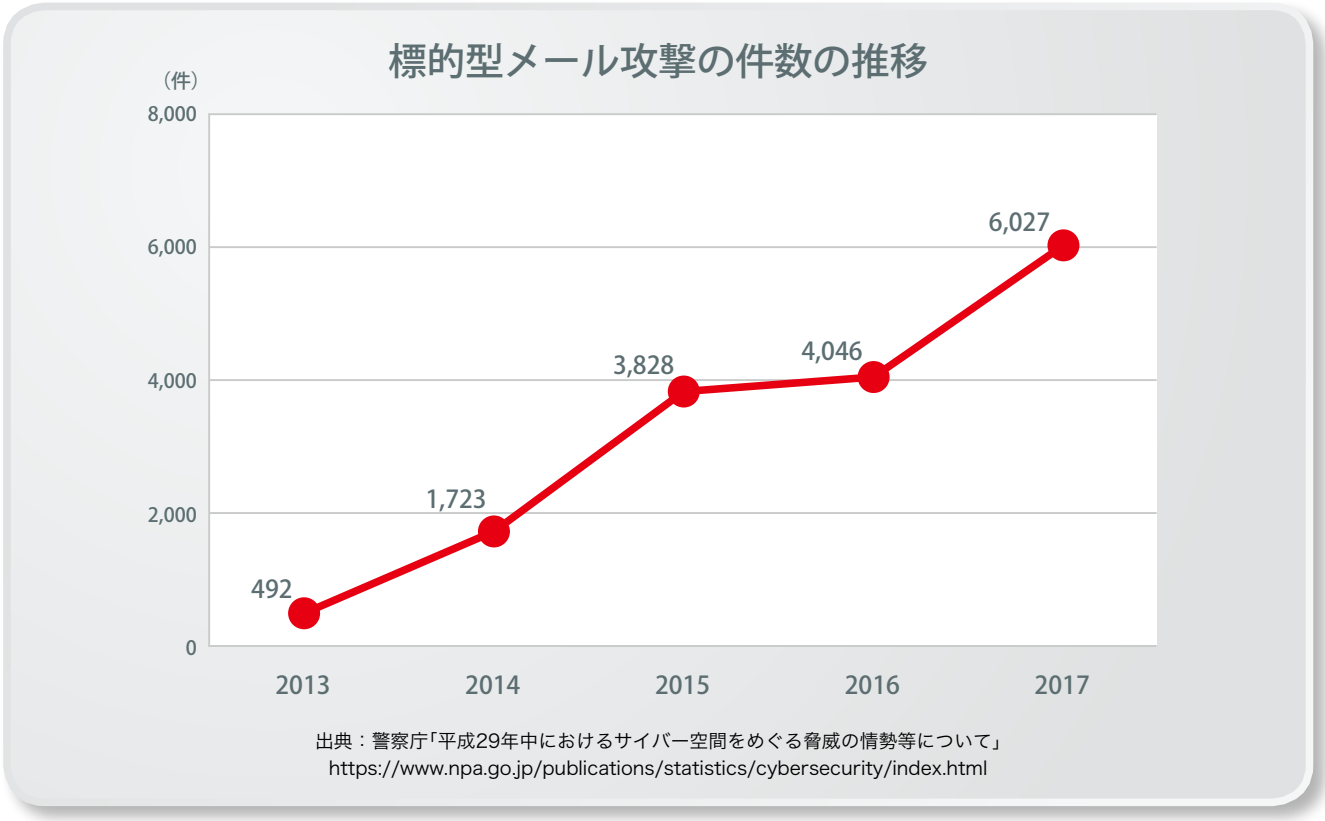
標的型攻撃を疑似体験する

標的型攻撃メールが届く可能性のある社員一人一人の意識を高め、対応に習熟してもらう方法として、標的型攻撃メール訓練があります。

「不審なメールが来たら報告すること」と定期的にアナウンスしても、どんなメールが不審であるかを的確に判断したり、気付いた時に具体的に行動に移すのは難しいことです。防災訓練と同様に、実際に体験することで、社員の理解度や組織的な防衛が正しく機能するかを評価できます。

ラックでは、標的型攻撃を疑似体験し、社員の意識の向上や不審なメールに気付いた際の適切な対応方法を訓練する「ITセキュリティ予防接種」サービス(※a)を2011年から提供し、これまで多くのお客様に利用いただいています。

本レポートでは、ITセキュリティ予防接種の実績を元に大きく2つの成果を報告します。1つは訓練時のメール開封率やアンケートから見えてきた分析結果、もう1つは、標的型攻撃メールの訓練に使えるノウハウや注意点です。自組織で訓練を実施する際にも、セキュリティベンダーに訓練を依頼する場合にも使えるバイブルとなるようまとめましたので、今後の標的型攻撃対策の1つとしてご活用ください。



出典：警察庁「平成29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/publications/statistics/cybersecurity/index.html

※a「ITセキュリティ予防接種」で検索：https://www.lac.co.jp/service/education/inoculation.html

傾向分析

700組織の訓練事例が示す「メール訓練の効果」と「組織の改善点」

森 田 義 礼
セキュリティ診断部
ITセキュリティ予防接種担当
新規顧客への提案活動やリピート顧客に対する効果的なメール訓練のアドバイスを行っている。現在はサービス提供だけでなく、案件全体の管理やサービス担当者の育成にも力を入れている。

相 沢 航 太
セキュリティ診断部
ITセキュリティ予防接種担当
様々な業種の顧客に対するITセキュリティ予防接種サービスを担当。その経験を基に大規模案件のリーダーや提案活動、セキュリティ研修の講師など幅広く活動する。

Point 1

標的型攻撃対策の1つとしてメール訓練が定着

ラックでは2013年度から2017年度までの5年間で、約700組織の標的型攻撃メール訓練を実施。
訓練の有効性を感じ、定期的に実施するユーザーが増えています。

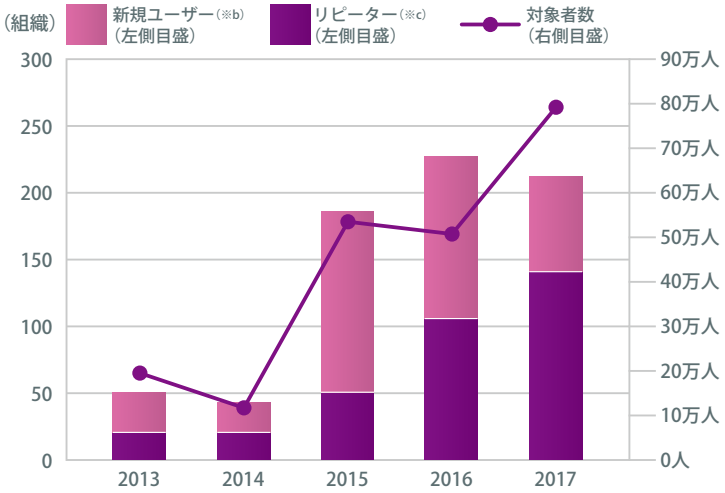
図1は2013年度から2017年度にかけてラックに標的型攻撃メール訓練(以下メール訓練)を依頼した組織数および訓練対象者数(疑似攻撃メール配信人数)の推移です。

標的型攻撃メールは2015年の日本年金機構の事件以降、注目度が高まりました。この事件を機に対策の一環としての「メール訓練」に関心が集まり、ラックでメール訓練を実施するお客様も多くなりました。

その後も、メール訓練を実施する組織数は増加傾向にあり、特にリピーターが増加しています。また、訓練範囲の拡大にともない、2017年度の訓練対象数は約80万人となっています。

このような需要動向からメール訓練は瞬間的なブームではなく、標的型攻撃メールへの対策として定着したといえます。

図1 「標的型攻撃メール訓練」実施組織数と対象者数



Point 2

訓練継続により社員の理解度が向上

メール訓練を繰り返すことによって、組織としてのセキュリティ能力を維持。
訓練内容にひと工夫加えて実施している事例もあります。

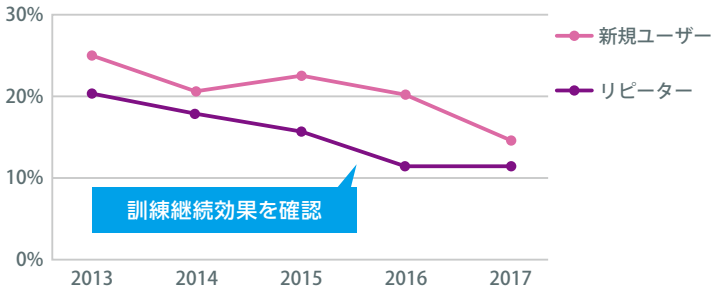
疑似攻撃メールの開封率は下降傾向

メール訓練では、訓練対象者が疑似攻撃メールの添付ファイルを開封、またはURLリンクをクリックした割合を「開封率」としています。図2は新規ユーザーとリピーターの平均開封率の推移を示しています。

訓練の効果はもちろん、標的型メール攻撃をはじめとしたサイバー攻撃の認知度の高まりから、新規ユーザーおよびリピーターともに開封率は近年下降傾向にあります。

特にリピーターは新規ユーザーに比べ低い開封率を維持しており、訓練の効果を得てきたといえます。

図2 過去5年間における新規ユーザーとリピーターの平均開封率



※b **新規ユーザー**：ラックに初めて標的型攻撃メール訓練を依頼した組織のこと。
※c **リピーター**：ラックに標的型攻撃メール訓練を2回以上依頼した組織のこと。訓練回数は、2013年度より前の依頼も含む。

訓練実施回数から見る訓練継続効果

図3は2013年度から2017年度にラックにてメール訓練を実施した組織（延べ722組織）における、訓練実施回ごとの開封率の平均を示しています。

初回の開封率は20.4%、2回目は13.6%で、7ポイントほどの開きがあります。これは、訓練対象者が標的型攻撃メールを認知しているかどうかによる違いといえます。

3回目の開封率は11.8%で、2回目から3回目の間でも、平均開封率は2ポイントほど開きがあります。

複数回の訓練では内容をひと工夫

図4は継続して訓練を行っている組織Aの開封率推移を示しています。

このケースでは、単純に開封率が減少していくのではなく、何度か増加していることがわかります。これは訓練の効果が下がっているわけではなく、疑似攻撃メールの配信方法や内容を、より高度なものに変更したためです。

組織Aでは2回目の訓練で一定の効果が出たと感じたため、今まで対象者に一斉に配信していた疑似攻撃メールを、3回目の訓練ではタイミングを分散して配信しました。その結果、今まで発生していた対象者同士の声掛けや注意喚起などの情報共有が減り、結果として2回目よりも開封率が高くなっています。

7回目の訓練では、疑似攻撃メールの送信元を自組織のメールアドレスに偽装した「なりすましメール」を使用して訓練を行いました。すると低い数値に留まっていた開封率が再び高くなっています。また8回目の訓練終了後に社員教育を行った結果、9回目は開封率が低くなりました。

組織Aではこの後も、開封率がある程度下がったタイミングで、業務メールを模したものを使用する、不審な点の少ないメールを使用するなど、判別の難易度を高めたメール訓練を続けています。

現在の訓練内容ではもの足りないという場合は、この事例のような「ひと工夫」を加えることが有効です。

定期的な訓練で社員の理解度を維持

図5は、継続して訓練を行っている組織Bの開封率推移を示しています。

こちらは組織Aとは異なり、初回訓練から訓練内容を大きく変更していません。このため図の通り4回目訓練以降の開封率は10%以下にとどまっています。

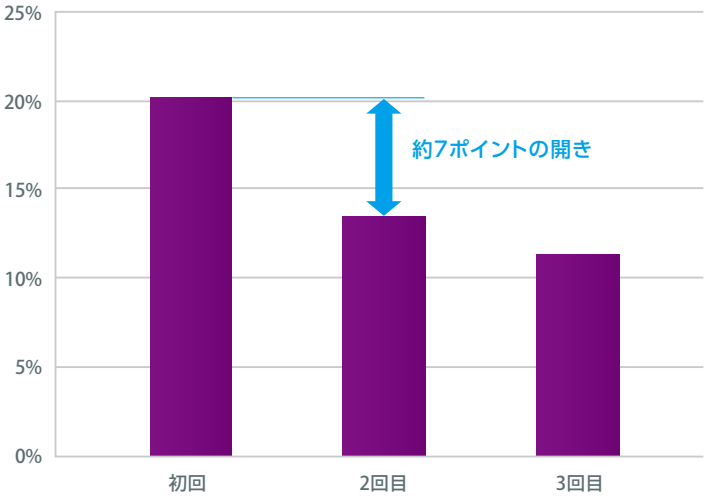
開封率が下げ止まりとなっているお客様から「開封率が下がりきった今、訓練を継続する意味はあるのか」との質問を受けることがあります。その答えは、「イエス」です。

社員一人一人が不審なメールへの対応を継続して意識するためには、継続的な訓練が必要です。

また、新規採用や中途入社など、不審メールの取り扱い手順に慣れていない人が毎年一定数増えるため、それらの人にメール訓練を経験させるためにも継続していく必要があります。

以上を踏まえると、組織Bの開封率が一定の水準を維持していること自体が、訓練を継続していることによる効果といえます。

図3 訓練実施回数別開封率の平均



※回数=ラックでメール訓練を実施した回数
初回=新規ユーザー

図4 組織Aの訓練継続による開封率推移

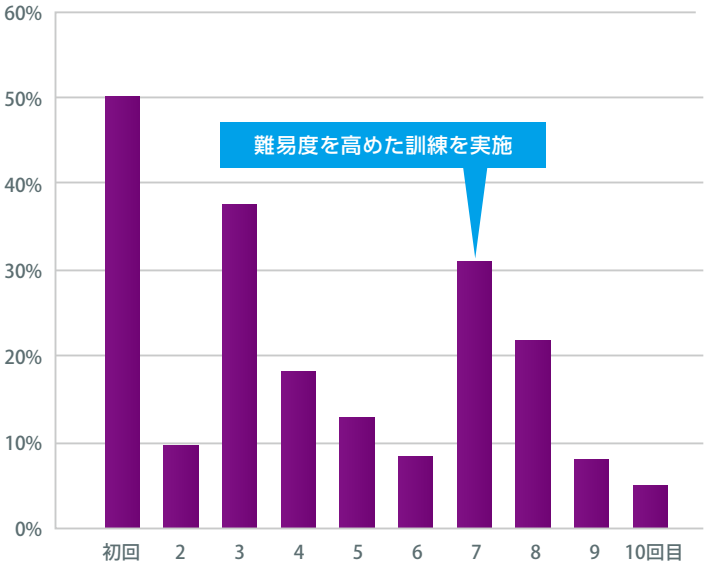
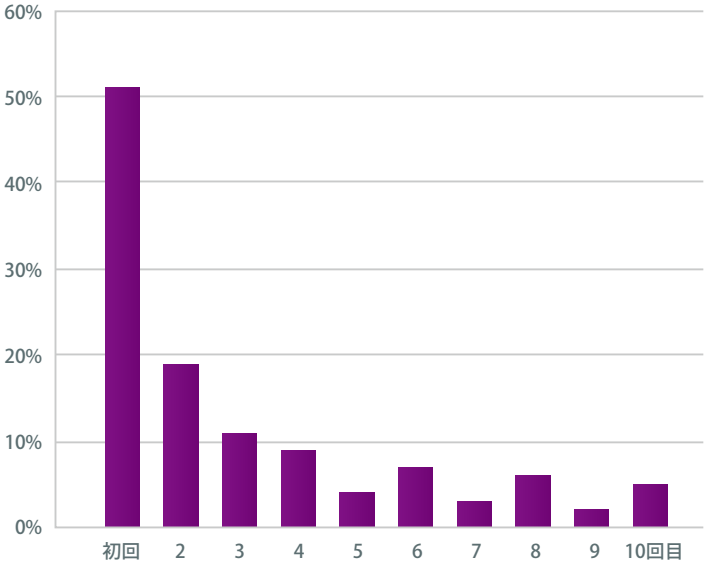


図5 組織Bの訓練継続による開封率推移



Point 3

訓練有効との意見多数　課題は社内ルールの整備と浸透

標的型攻撃について理解を深めることが、被害を未然に防ぐための第一歩。
メール訓練とともにアンケートを実施することが、訓練対象者の理解度と意識、セキュリティリテラシーの把握につながります。

9割以上が訓練は有効と回答

訓練結果といえば開封率に注目しがちですが、ラックではメール訓練後に対象者へのアンケートを推奨しています。訓練に対する対象者の声を聞くことにより、今後の訓練・社員教育計画につながります。

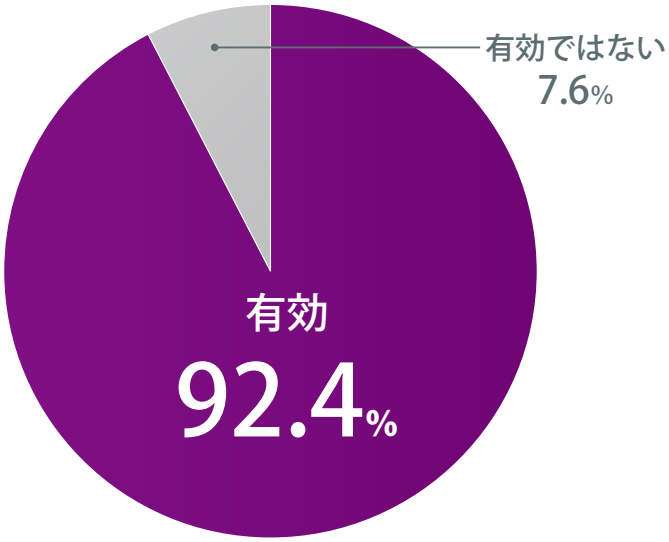
ラックで実施するアンケートには、メール訓練を有効と感じたかどうかの設問があります。過去3年間(※d)のデータを集計したところ、回答者の9割以上がメール訓練の有効性を認めているという結果(図6)が得られました。

有効性に関する感想として最も多くみられるのは、「実際に標的型攻撃メールの受信を体験できたため」という内容です。

一般的に、組織における情報セキュリティ教育は、座学やEラーニングが大半を占めます。知識として聞いたことがあり、知っているつもりになっている人も、実際に自分のメールボックスに巧妙な標的型攻撃メールが届くと、うっかり開封してしまうケースは少なくありません。

メール訓練によって「体験を通した実感」が得られると、対象者が標的型攻撃メールへの正しい対策や対処を理解する大きな助けとなります。

図6　訓練後アンケートにおけるメール訓練の有効性について



対象期間：2015～2017年度(回答者数131,768名・単一回答)

標的型攻撃メールへの理解度が向上

体験を通した標的型攻撃メールへの理解度の向上はアンケート結果からも確認できます。

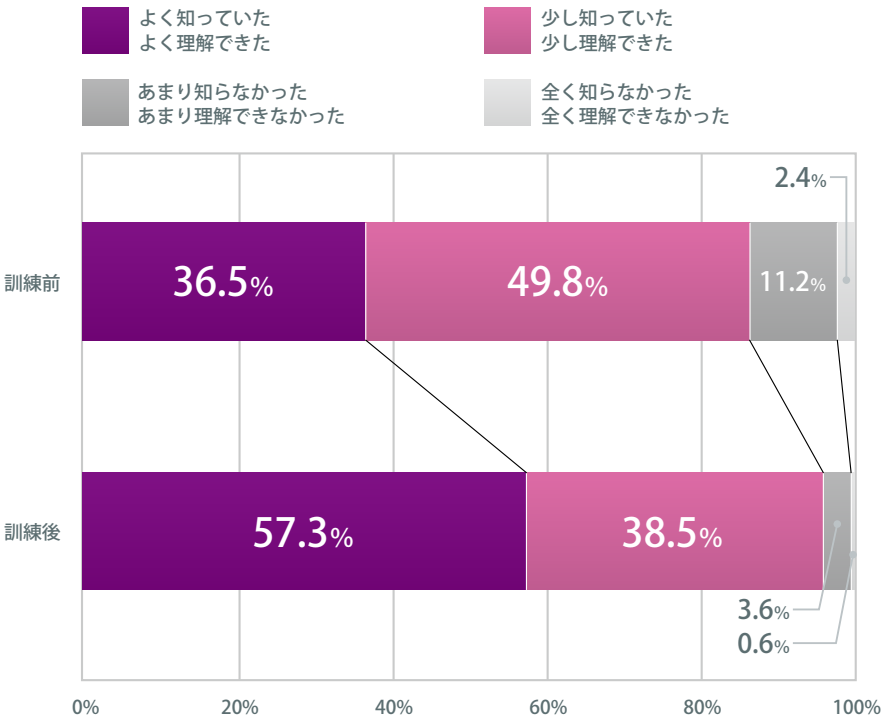
図7は「標的型攻撃メールの攻撃方法や脅威についての理解度」を尋ねる設問に対する、過去3年間の回答を示しています。

訓練実施後は、回答者の9割以上が理解できた(※e)と回答しています。

なかでも注目すべき点は、訓練前は36.5%だった「よく知っていた・よく理解できた」が、訓練後には半数を超えていることです。

標的型攻撃への対処は、組織全体、一人一人のリテラシーを向上させることが最も大切なポイントです。このアンケート結果は、メール訓練の有効性を実証しています。

図7　訓練後アンケートにおける訓練前後の標的型攻撃メールへの理解度推移



対象期間：2015～2017年度(回答者数92,908名・単一回答)

※d **過去3年間**：「メール訓練の有効性」をアンケートの共通項目とした2015年以降のデータを集計対象としている。
※e **「理解できた」**：「よく知っていた・よく理解できた」「少し知っていた・少し理解できた」の計。

報告は少数、初動対応に課題

図8は、疑似攻撃メールを受信した際にどのような対応を行ったかを尋ねる設問について、過去3年分の回答を示しています。

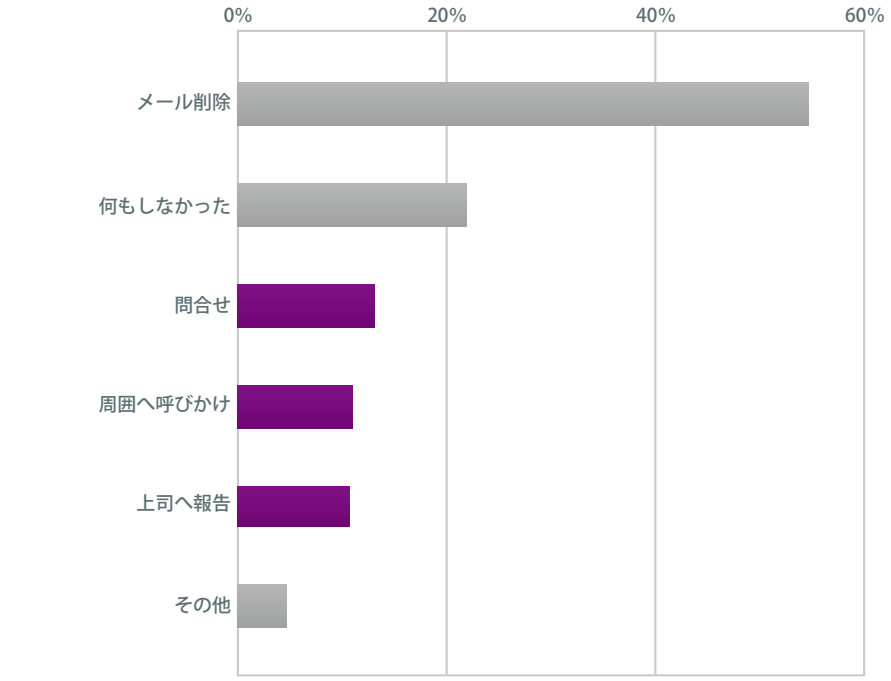
その結果、「何もしなかった」という回答が一定数ありました。何もしなかった理由は、「対応方法がわからなかった」場合と、「訓練であると気付いた」場合の大きく2つに分けられます。

メール受信後に関係者へ連絡したかという点に着目すると、「問合せ」「周囲へ呼びかけ」「上司へ報告」が、いずれもアンケート回答者の1割程度になっています。1割という数字は、標的型攻撃メールの攻撃方法や脅威について理解できた9割とは開きがあります。

これは、攻撃方法の理解度は高まったものの、報告するといった対応手順は十分に浸透していない組織が多いためです。この状況を改善するには、対応手順を整備・周知していく必要があります。

開封率を出して終わりとせずにアンケート結果を分析し、具体的な課題が何かに気付き、改善につなげることが重要です。

図8 メール受信後の行動



対象期間：2015～2017年（回答者数131,768名・複数回答有）

組織全体のリテラシー向上を目指す

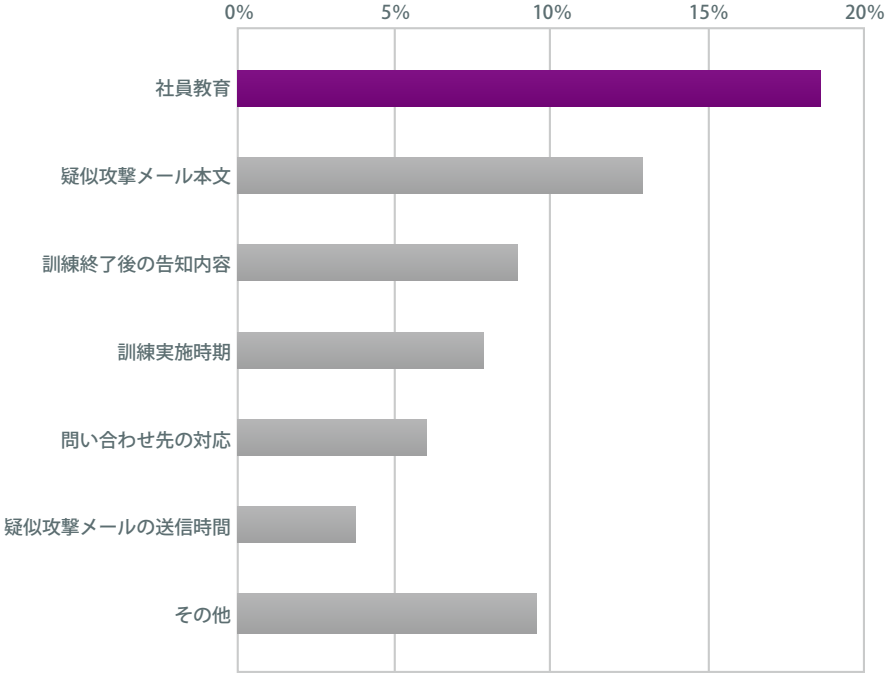
図9はメール訓練への改善要望を尋ねる設問について、過去3年分の回答結果を示しています。

この結果から回答者の5人に1人は社員教育について改善要望を抱いていることがわかりました。具体的な要望の内容としては、「訓練後に改めてフィードバックが必要である」「不審メール受信時の見分け方はわかったが、その後の報告などの対応をどうすればよいのかわからない」などの意見が多く寄せられています。

このような意見の通り、単にメール訓練を実施するだけでは、社員が不審なメールを受信した際の対応手順を十分に理解できるようになるとはいえません。

メール訓練実施後の次のステップとして、訓練結果に基づいた社員教育や、組織内の対応手順を見直すことが、組織全体のリテラシー向上において重要かつ効果的な施策となります。

図9 訓練後アンケートにおける改善要望



対象期間：2015～2017年（回答者数131,768名・複数回答有）

知見の整理

自組織で実施するための訓練担当者が知るべき「メール訓練のコツ」

川 島 夏 海
セキュリティコンサルティング部
コンサルタント

金融業の顧客を中心としたセキュリティコンサルティング業務に従事。ITセキュリティ予防接種サービスにも過去5年間携わり、200社以上の訓練を担当。日本ネットワークセキュリティ協会（JNSA）の活動にも参画。

坂 本 智 幸
セキュリティ診断部
サービスマネジメントグループ
グループリーダー

2015年から3年間、ITセキュリティ予防接種サービスのグループリーダーを務めた。現在は予防接種サービスをはじめとする診断サービス全体の企画立案などに従事している。

Knowledge [Phase1]

目的／メール訓練をやっても意味がない!?

訓練に対する理解が年々向上

2018年6月で、ラックが標的型攻撃メール訓練サービス「ITセキュリティ予防接種」を開始してから7年が経ちました。

当初のお客様の反応は「標的型攻撃メールの訓練?? なにそれ？」であったものの、標的型攻撃メールによる被害の増加とともにメール訓練の認知度も高まり、今ではラックのセキュリティサービスの一端を担う存在となりました。

お客様と会話するたびに、世の中全体で標的型攻撃メールに対する理解が進んでいることを実感しています。

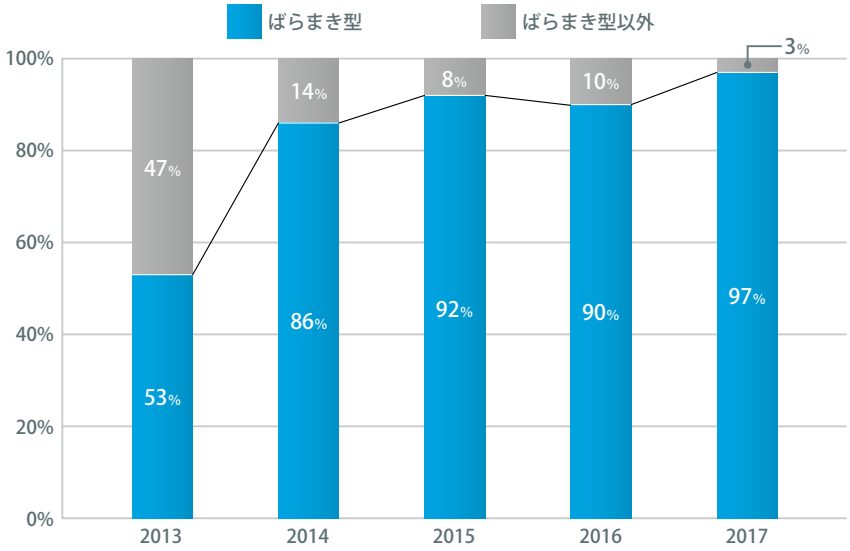
メール訓練には意味があるのか？

サービスの提供を開始してしばらく経つと「メール訓練は本当に意味があるのか」という声をたびたび聞くようになりました。また「最近の標的型攻撃メールは巧妙だから、人の目で見分けるのは無理だ」、このような声もよく耳にします。

たしかに、ここ数年、攻撃メールの巧妙化はますます進み、普段の業務メールをコピーしたかのような巧妙な標的型攻撃メールの事例が、これまでに複数報じられています。しかし、巧妙でないものを見抜けるようになると、攻撃メールの大半を見抜けることにつながるため、メール訓練には大きな意義があるのです。

警察庁が公表しているデータ（図10）では、観測された標的型攻撃メールの約9割が、多くのターゲットに対して同じ内容の攻撃メールを使う「ばらまき型」であるとされています。こういったメールは不特定多数を対象としているため、自身に心当たりがなければ、不審メールだと見抜ける可能性があります。

図10 「ばらまき型」(※f)とそれ以外の標的型攻撃メールの割合



出典：警察庁「平成29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」(※g)

近年では、約9割が不特定多数を対象とした
「ばらまき型」のメール

内容に心当たりがないなど
見抜ける可能性が高い

※f **はらまき型**：警察庁では、「標的型メール攻撃」のうち、同じ文面や不正プログラムが10か所以上に送付されていた標的型メール攻撃を「ばらまき型」としている。
※g **警察庁「平成29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/publications/statistics/cybersecurity/index.html

メール訓練は標的型攻撃メールの「防災訓練」

適切な対応によって被害を防ぐ

メール訓練の意義についてお客様へ説明をするときに、必ず例として挙げるのが「防災訓練」の話です。

防災訓練は「災害を起こさない」ためではなく、「災害が発生したときにどう動くか」を体験・学習するために実施します。実際の災害を想定し、「机の下にもぐる」「避難経路に従って避難する」という対処を防災訓練の中で体験することで、災害時に取るべき行動を学習できます。

メール訓練では、防災訓練と同じように「標的型攻撃メールを受信したときにどう動くか」を社員一人一人が体験することが目的の1つとなります。標的型攻撃メールの添付ファイルを開いてしまったとしても、その後に「端末をインターネットから切断する」「社内の担当部門に報告する」など、社内のルールを知っているだけの場合と、訓練で実際に対応したことがある場合では、大きな違いがあります。社員一人一人がルールに従った適切な対応を取ることで、何もしなかった場合と比較して、標的型攻撃メールによる被害を低減できる可能性が大幅に高まります。

目的意識を明確にした訓練の実施が重要

疑似攻撃メールは目的に合わせる

訓練の意義を高めるには、企画する側が目的意識を持つことが重要です。

サービスを提供する中で、お客様から「訓練に使用するメールの難易度はどの程度にするのがよいのか？」といった質問をいただきます。疑似攻撃メールの難易度は「難しいほどよい」といったものではありません。目的に合わせた疑似攻撃メール（図11）を使用することが重要です。

不審なメールを見極める力を養わせたい場合

社員に「不審なメールを見極める力」を養わせたいのであれば、あえて「気付かせる」ための疑似攻撃メールを使用します。

実際の攻撃に使用された標的型攻撃メールの内容を活用する方法もあります。攻撃事例は公的機関が公表しているものが参考になります。例えば、一般財団法人日本サイバー犯罪対策センター（JC3）では、不審メールの事例を公開しています。（ラックでは、実際にラックが観測した攻撃メールの内容を基に疑似攻撃メールのテンプレートを作成しています）

これまでに訓練を実施したことがなく、社員の知識レベルがわからない場合には、実際の攻撃例に近い内容の疑似攻撃メールを使用することで、実際に攻撃を受けた場合の開封率や、社員のリテラシーレベルを把握できます。

「気付かせる」疑似攻撃メールを使用した場合は、訓練後に社員に対して「気付きのポイント」を周知し答え合わせをすることで、標的型攻撃メールについて、社員の理解がさらに深まります。

不審なメールを受信した場合の対応力を養わせたい場合

見抜けないほど巧妙な標的型攻撃メールを受信したり、見抜くポイントを理解していてもうっかり開封したり、ということが起こる可能性は十分にあります。そういった、万が一の場合の「対応力」を養うのであれば、あえて「気付かせない」メールを使用する方法もあります。

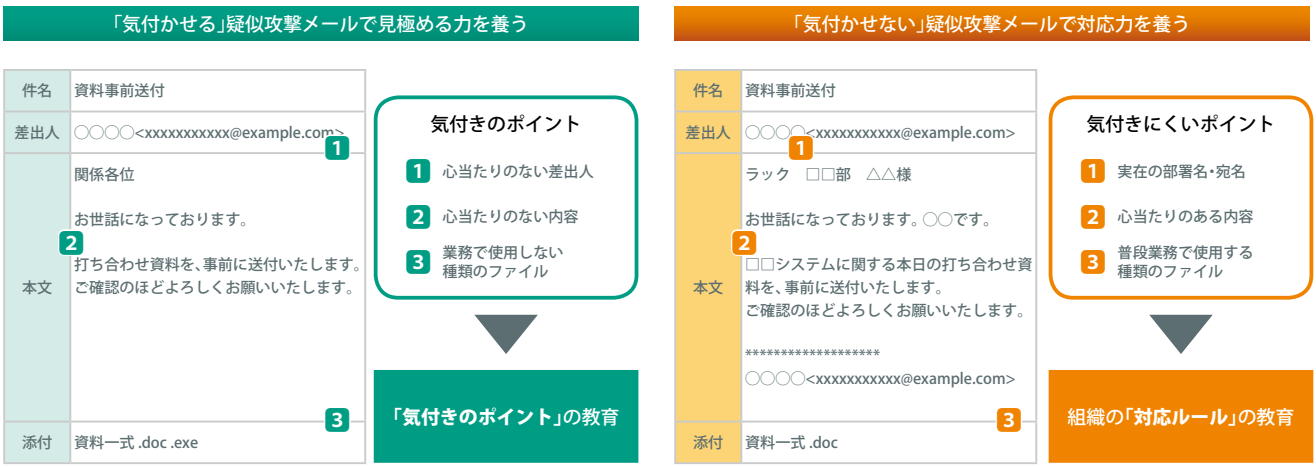
実在の部署名を利用するなど、実際の組織の情報を活用して作成した疑似攻撃メールは見抜くのが困難です。このような「気付かせない」メールを使用して訓練を実施したお客様では、半数以上の訓練対象者が添付ファイルを開封する例もありました。「気付かせない」メールを使用する場合は、どれくらいの人が、開封後に組織内のルールに従った適切な対応を取ったかの「対応状況」に着目するのがポイントになります。

添付ファイル開封時には、訓練である旨と合わせて「組織のルールに従って行動してください」というアナウンスを表示し、開封した人は実際の組織のルールに従った行動（LANケーブルの抜線、担当部門への電話報告など）を体験することになります。

また、実際の攻撃に近づけ、訓練である旨を表示せずに、自発的に報告させる例もあります。この方法では、疑似攻撃メールの難易度がより高まるだけでなく、慣れてきた社員が訓練の際は初動対応を実施しなくなるなど、訓練の継続実施から生じる「訓練慣れ」による影響を軽減し、より実践的な訓練を実施することが可能です。

このように、疑似攻撃メールの内容1つをとっても、その訓練を行うことで何を得たいのか、訓練の目的を意識した上で十分に検討することで、訓練を意味あるものにすることができます。

図11 「気付かせる」疑似攻撃メールと、「気付かせない」疑似攻撃メールの例



疑似攻撃メールの難易度は本文の内容だけではなく、送信元メールアドレスや添付ファイルなどの要素にも依存する。「気付きのポイント」が少ないほど難易度は高い。

Knowledge [Phase2]

準備／訓練成功につなげる「5つ」の準備

準備1. 訓練実施時期とメール配信タイミングの決定

メール訓練は、実際の攻撃メールに似せて作成した疑似攻撃メールを訓練対象者に送るだけのシンプルなトレーニングです。

それだけに、訓練が成功するか失敗に終わるかは、事前の入念な準備を行うかどうかが重要になります。準備不足のまま訓練を実施しても、訓練対象者の業務に大きな支障をきたすなど、予想外のトラブルが発生することがあり、十分な効果が得られません。そこで、自組織で訓練を実施する際に、メール訓練の担当者（以下訓練担当者）が事前に準備すべきポイントを5項目に整理して、順にお伝えしていきます。

実施時期

メール訓練は、対象者が最も多く参加できる時期に実施するのがお勧めです。一人でも多くの人が疑似攻撃メールを見分け、事前に決めた報告先に報告するという手順を経験すると、より高い教育効果が得られます。そのため、休暇を取る人が多い休業日（ゴールデンウイーク、夏季休暇、年末年始など）は避けたほうがよいでしょう。

配信時刻

先ほども述べた通り、疑似攻撃メールはできるだけ多くの対象者の目に触れることが大事です。また、対象者からの連絡が訓練担当者やヘルプデスクに来ることになるため、業務時間内に疑似攻撃メールを配信するのが望ましいでしょう。

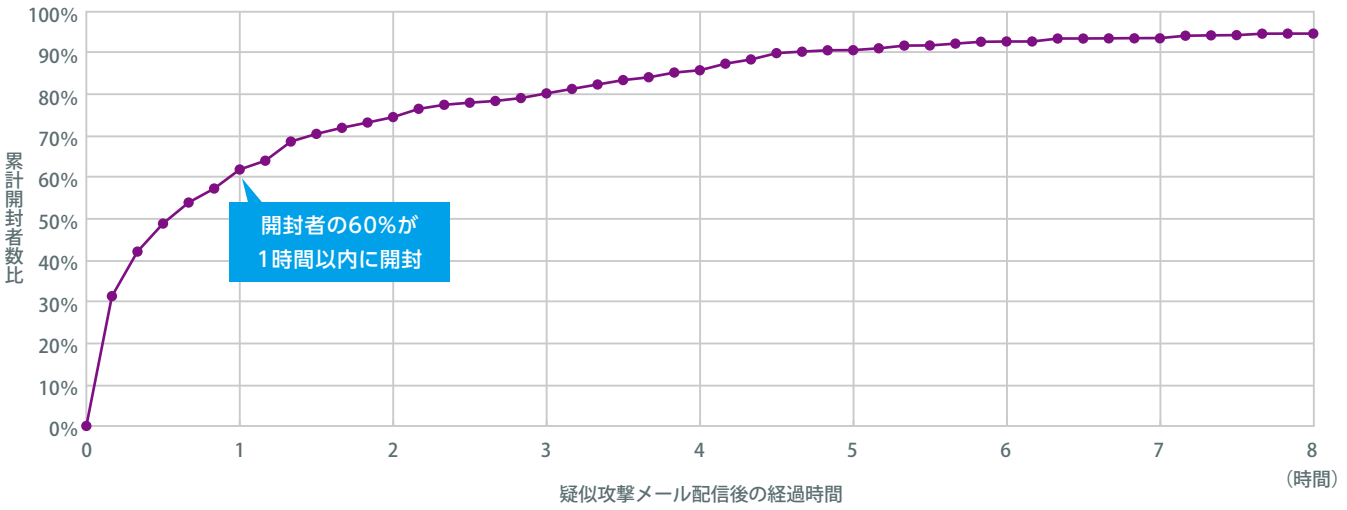
図12は、業務時間内に疑似攻撃メールを配信し、メールを受け取った人が添付ファイルを開くまでの経過時間を示しています。ラックの過去の訓練実績では、開封者の約60%が配信直後から1時間以内に添付ファイルを開いています。教育効果を期待する場合は、業務終了後の時間は避けましょう。疑似攻撃メールの配信時刻は訓練効果を左右する重要な要素といえます。

注意点

配信時刻を決める際は、メール訓練によるメールサーバーやネットワークへの負荷も忘れずに考慮に入れましょう。メール訓練の性質上、回避できないこと（数千通の疑似攻撃メールを一斉配信する場合など）もありますが、疑似攻撃メールを分割して配信し、システムが高負荷となるタイミングを分散させるなど、可能な手立てを検討しておくことが大切です。

図12 メール受信からの経過時間と添付ファイルの開封状況

ラック実績（2017年度）



準備2. メールを配信する対象者の決定

訓練未経験者を中心にする場合

次に、訓練の対象者を選定します。

基本的には全員を対象とするのが望ましいメール訓練ですが、特に新入社員や中途採用社員などの訓練未経験者を優先的に対象とします。

初めて訓練を受けた人のメール開封率が、継続的に訓練を受けている人に比べて高いことは、3ページ（Point2 訓練継続により社員の理解度が向上）で紹介した通りです。メール訓練を実施したことのある組織と実施したことがない組織にも、開封率には大きな開きがあります。

訓練未経験者に「体験」させることは、メール訓練の大切なポイントです。

対象者を限定して実施する場合

一方で、訓練を継続して実施している組織では、対象者をあえて一部の社員に絞るケースがあります。

全社員を対象に継続的に実施していると、訓練慣れが生じたり、職場内で訓練情報が共有されて、疑似攻撃メールが無視されるなど、教育効果が見えにくく想定した効果を上げられないことがあります。

標的型攻撃メールが本物だった場合は関係者が情報を共有することは好ましいのですが、訓練では参加する一人一人に警戒心を持ってもらうことが重要です。そのためには、対象者を絞って実施するのも一案ということになるのです。

また、全社員を対象とする場合でも、同時に疑似攻撃メールを配信するのではなく、日時を分散して配信したり、内容を変えるなどの工夫を加えることも有効です。

準備3. メール内容の決定

3つめのポイントはメールの内容です。訓練で使う疑似攻撃メールの文面は、対象者の訓練経験の有無などに合わせて、レベルを変えて使い分けると、リテラシー向上に効果的です。

●初級編／実際の攻撃に使われた不審メールを、疑似攻撃メールの文面作成の参考にするとよいでしょう。自組織へ実際に届いたもののほか、一般財団法人日本サイバー犯罪対策センター(JC3)に届け出があったメール例が参考になります。

●応用編／訓練経験者には、日頃、実際にやり取りするメールに似せたメールで理解度を試す方法が有効です。この場合、所属する組織内でよく使われる用語や言い回しなどを含むメールに、不審メールと気付くべきポイント(不自然な日本語、署名が無いなど)を紛れ込ませて疑似攻撃メールを作成します。業務メールだけでなく、セミナー案内など業務外の内容に気付きのポイントを入れるケースもあります。

注意点

疑似攻撃メール作成時、リアリティを追求するあまり、実在する会社などの情報を含めてしまうことがあります。疑似攻撃メールを受け取った対象者がメールに記載された組織や人物に対して問い合わせをしてしまうと、第三者の業務を妨げる恐れがあります。疑似攻撃メールには、実在する組織や人物名など固有の存在をイメージさせる事柄を盛り込むことは避けましょう。

テスト配信

疑似攻撃メールの文案が完成したら必ずテスト配信を行い、次の2点を確認します。

●問題なく受信できるか／最近では、メールの閲覧方法として、メールソフトウェアに加え、Webブラウザやスマートデバイスを使うことも増えてきました。テスト配信では、メールソフトウェアや各デバイスで疑似攻撃メールが迷惑メールフォルダに振り分けられることなく受信フォルダに届いているか確認します。

●開封者の集計機能が正しく働くか／疑似攻撃メールに設定した、開封者の集計機能(Webビーコンなどの動作)を確認します。組織のネットワーク要件で外部通信が不可となっていて開封したことを知らせる通信が届かない場合や、セキュリティ製品(クラウドのセキュリティサービスなど)が検知し開封したことを知らせる通信が誤って送られてしまう場合があるためです。

テスト配信後は、開封者の状況が正しく集計できているか、開封者のIPアドレスが訓練担当者の組織のものであるかなどを確認しておきます。

準備4. 不審メール受信時の初動対応手順の整備

初動対応手順とは、不審メールを受信した際にどのように行動するかを定めた指針です。訓練対象者向けと、問い合わせ対応に当たる訓練担当者向けの両方を準備して、メール訓練で実際に使って有効性を確認しましょう。

対象者向け対応手順

不審メールを受信したり開封したりした場合の連絡先や連絡方法をまとめたもので、常に社員が簡単に閲覧できる場所に保管します。

＜手順例＞

①不審なメールを受信した場合は、差出人や件名、本文、署名などの情報をもとに標的型攻撃メールかどうかを判断する。少しでも不審に感じたときや、判断できない場合は上司やヘルプデスクなど関係者に報告を上げる

②標的型攻撃メールと判断した場合は、添付ファイルを開いたり、URLをクリックしたりせずに、迅速に担当部門へ報告する

③標的型攻撃メールや添付ファイルを開封したり、URLリンクをクリックした場合はそのPCをネットワークから切断する

訓練担当者向け対応手順

訓練担当者が使用する対応手順は、問い合わせをしてきた社員からヒアリングする方法を示したものです。

＜ヒアリング項目例＞

①不審メールの受信日時

②メールの内容(件名・差出人・差出人のメールアドレス・添付ファイルなど)

③添付ファイルの開封やメール本文中のURLリンクのクリックの有無

④添付ファイルの開封やURLリンクをクリックした日時

メール訓練中に本物の標的型攻撃メールを受信する可能性もあるため、訓練担当者はヒアリングした内容が疑似攻撃メールなのかどうかを判断できるポイントを疑似攻撃メール内に盛り込んでおくと良いでしょう。また、問い合わせをしてきた社員は、ウイルスに感染したかもしれないと焦っている可能性がありますので、訓練担当者は落ち着いてヒアリングを行いましょう。

準備5. 評価項目の決定

メール訓練で判明した課題を整理し、今後取り組むべき改善内容を提言するため、あらかじめ評価項目を設定しておきます。項目によっては、訓練が終了してしまうと収集が難しくなる情報もあります。

そのため、訓練中に記録を付ける、アンケートを実施するなど情報の収集方法も決めておきます。

表1で、設定する評価項目の例を紹介します。なお、全ての評価項目を網羅する必要はありません。報告目的、また自組織の事情やシステム環境などに合わせて適切な評価項目を選びましょう。

表1 設定する評価項目の例

① 疑似攻撃メール開封者における弱点を確認したい場合
●疑似攻撃メールの開封率、開封スピード ●疑似攻撃メール開封者にみられる傾向の有無 (部門／職種／職位、訓練経験有無別、不審メール受信時の初動対応手順の未読／既読など)
② 疑似攻撃メール受信者が適切に初動対応したかを確認したい場合
●疑似攻撃メール受信時の対応　●担当部門への報告率や報告スピード ●疑似攻撃メールの開封(非開封)の理由 ●報告率にみられる傾向の有無(初動対応手順の利用度／訓練参加回数／職種など)
③ その他(今後のメール訓練への考慮点として)
●訓練結果を踏まえた次回の訓練の疑似攻撃メール案 ●訓練実施中の業務影響などの改善事項の有無 ●初動対応手順について改善事項の有無　●次回訓練に向けた意見の収集

Knowledge [Phase3]

実施／訓練中に起こる「3つの問題」への対処

問題1. 訓練対象者の業務が混乱

次に、メール訓練中に発生しやすい問題と、問題発生時の影響を減らすための対策のポイントを整理してご紹介します。

最初に、業務の混乱という問題です。メール訓練は、時として訓練対象者の業務に混乱をもたらします。訓練で使う疑似攻撃メールには、不審メールと気付いてもらうための「気付きポイント」を設定します。例えば、実在しない部署を署名に使ったりします。

訓練対象者がこのようなメールを不審に感じ、周囲に相談や報告をすることが多くあります。不審メールが本物だった場合、情報を共有することは同じようなメールを受け取った人への注意喚起にもなるため、対処法として正しいのですが、訓練ではこの行為が裏目に出ることがあります。

ある組織の事例で、不審メールを受信した社員が情報を周囲と共有するうち、同じ部署に所属する社員全員が不審メールを受信していることが判明。マルウェア感染を疑った一部の社員が自身のPCをネットワークから切断し、ウイルス対策ソフトでフルスキャンを実行したのです。フルスキャン実行中はPCが利用できないために、複数の社員の業務に支障をきたしました。

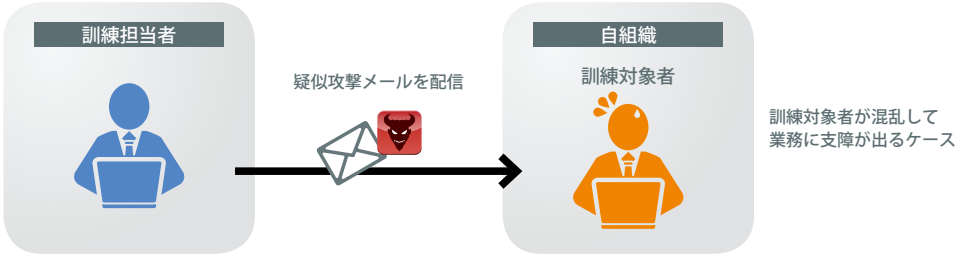
また、疑似攻撃メールの添付ファイルを開封したり、メール本文に記載されたURLをクリックした際に、訓練だと気付けなかった訓練対象者はPCをネットワークから切断してしまいがちです。この場合も、開封者の人数は限定的とはいえ、少なからず業務に支障をきたします。

＜対策のポイント＞

訓練対象者や報告先への案内

実施前に、不審メール受信時の対応手順や報告フローを再周知しておきます。また、受信報告を受ける現場の上司やセキュリティ担当者にも、訓練を実施することや疑似攻撃メールの配信時間、訓練対象者などをあらかじめ知らせておきます。

添付ファイルを開封したりURLリンクをクリックしたりした人に対しては、その先に表示する画面にこのメールが訓練であることや、取るべき行動を明記して、混乱を最小限に抑えましょう。セキュリティ担当部門に連絡をしてきた訓練対象者には、訓練だということを個別に告げて、業務への影響の拡大を防ぎます。



問題2. セキュリティ担当部門がパンク

不審メールが訓練用と気付かず、対象者が一斉に報告を上げてくることで生じるのがセキュリティ担当部門のパンクです。

多くの組織では、不審メール受信時の初期対応としてセキュリティ担当者への報告を定めています。スピードを求める組織では、電話報告を必須としているところもあります。セキュリティ担当部門のパンクは、初期対応手順が訓練対象者に浸透しているからこそ発生する問題です。

ラックが提供するメール訓練では、疑似攻撃メールに添付するファイルやメール本文に記載するURLリンク先に、そのメールが訓練だと知らせる文面を用意します。セキュリティ担当部門への報告が集中しないように工夫をする場合もあります。

セキュリティ担当部門のパンクとは別の問題として、疑似攻撃メールを計画通り早朝に配信したものの、セキュリティ担当部門が業務時間外で不在だったため、訓練対象者からの報告に対応できず、クレームに発展したケースがありました。

早朝の配信はメールの不審さを高める意図があり、対象者が不審に感じたところまでは狙い通りでしたが、配信直後に対象者がセキュリティ担当部門に連絡を入れることまでは想定されていませんでした。

＜対策のポイント＞

配信範囲やタイミングを考慮

業務への影響を小さくするには、疑似攻撃メールの配信範囲を縮小したり、タイミングを分散するのが有効です。

また、セキュリティ担当部門のキャパシティと訓練当日に発生する負荷を考慮し、態勢を整えておくことが重要です。

問題3. 他組織の業務を妨害

メール内容の決定の項で前述した通り、疑似攻撃メールに使う送信元メールアドレスや署名が不適切で、実在する会社や組織をイメージさせるケースでは、他組織の業務を妨げてしまう恐れがあります。

訓練対象者が心当たりのないメールを受信した際、内容を確認するために疑似攻撃メールの差出人に問い合わせをするのはよくあることです。

送信元メールアドレスに他組織に似たドメイン名を利用したり、メール文面に他組織に実在、もしくは類似する部署や人物の名称を記したりしていると、訓練対象者が誤解して、悪気なく問い合わせをしてしまう恐れがあります。当然、問い合わせを受けた他組織の人は事実確認などに追われることになり、結果としてその組織の業務に悪影響を生じさせることになります。場合によっては、訓練担当者の謝罪だけで済む問題でなくなってしまう可能性もあります。

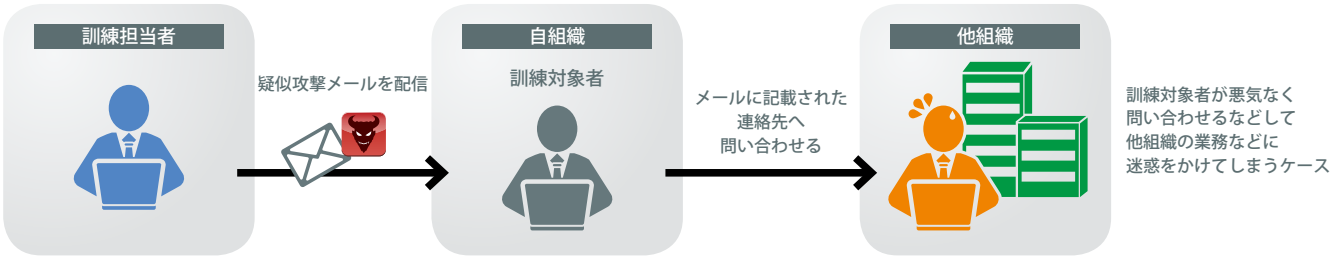
メール文面作成時や、訓練の実施に当たっては十分に注意を払い、万が一にもそのようなことが起こらないように留意することが大事です。

＜対策のポイント＞

実在の組織名などは使わない

疑似攻撃メールに使用する組織や人物の名称は、自組織のものを利用することをお勧めします。その場合でも、必要に応じて関係する部署に事前に許可を得ておきましょう。また、送信元メールアドレスも他組織のものではなく、自身もしくは訓練を実施するベンダーが管理しているものにしておくべきです。

疑似攻撃メールは、開封しても実害はありませんが、訓練対象者にとっては不審なメールに他なりません。また、いずれの問題も起きてからでは手遅れとなります。訓練担当者としてメール訓練を成功させるためには、訓練中に起こりうる問題を予測し、事前に対策を練ることが重要です。



Knowledge [Phase4]

改善／「メール訓練」結果を活かすために

開封率だけではない。
訓練結果への向き合い方

ラックのメール訓練サービス「ITセキュリティ予防接種サービス」では、ラックのエンジニアがお客様に寄り添いながら2〜3か月間、訓練の準備から結果報告までを実施します。最後の報告会では「やりきった！」と言わんばかりに晴れ晴れしたお客様の表情に出会えることもありますが、訓練はそこで終わりではありません。むしろ、本番はその後です。訓練結果を社員の意識と運用プロセスの改善に活かすことで、訓練の価値はさらに高まります。

訓練を複数回実施したお客様から「開封率の考え方」について相談が寄せられることがあります。典型的な相談内容が、「訓練を継続しても、これ以上開封率は下がらないように思われる。教育効果が乏しいということではないか」という懸念です。

訓練を導入して間もないお客様は、開封率の低減を訓練の目的と捉えています。しかし、開封率に捉われすぎないことが大事です。

どんなに頑張って開封率を下げようと試みても、人の入れ替わりなどもあり、開封率0%を目指すことは難しいのが現実です。たとえ開封率0%を実現しても、それは訓練上の結果に過ぎず、実際の標的型攻撃メールまで『絶対に開封しない』と保証しているわけではありません。

本当に向き合うべきなのは、開封率の背景にある開封理由や開封後の行動です。つまり、結果を「改善」に結びつけてこそ、訓練の意義があるのです。

メール訓練には、組織全体のセキュリティを強化するさまざまな効果（図13）があります。次ページでは、訓練の成果をより有意義なものにするための、訓練結果の活用方法をご紹介します。

図13　メール訓練のさまざまな効果

活用方法1. 訓練対象者のレベルに合わせた社員教育

訓練結果から社員のリテラシーを把握することは、必要な情報セキュリティ教育を検討する一助となります。ラックではこれまでに約700組織の訓練を実施してきた経験から、リテラシーのレベルを大きく3段階に分類しています(図14)。

STEP1. 不審な点に気付かず開封する

「気付きポイント」を含んだ疑似攻撃メールを多くの訓練対象者が開封してしまう場合、標的型攻撃メールに関する社員の知識と意識の底上げが必要です。訓練後に結果を踏まえた社員教育を行うと、その効果がさらに高まります。使用した疑似攻撃メールに含まれる「気付きポイント」を解説することで、開封者の理解を深めることができます。

「開封者には、一定期間メールの利用を禁止するなどペナルティを課すようにしたい」といった意見がお客様から出ることがありますが、ラックでは訓練対象者にペナルティを課すことは推奨していません。社員が「開封＝悪」という認識を持ってしまうと、実際に標的型攻撃メールの添付ファイルを開封してしまった際に、叱責を恐れ、事実を隠蔽する懸念が生じるためです。

STEP2. 気付いても報告しない

訓練を繰り返すことによって徐々に開封者が減ってくると、着目すべきポイントは、セキュリティ担当部門への「報告率」に移ります。

報告率を向上させるには、訓練終了後に実施するアンケートが有効です。アンケートの回答からは、セキュリティ担当部門への報告が行われなかった理由を見出すことができます。セキュリティ担当部門では、対応手順を策定し、十分に社員へ周知していると考えていたにもかかわらず、訓練後のアンケートで、実は社員の認知度が高くないことに初めて気が付くようなケースは少なくありません。

訓練対象者からの意見や改善要望を踏まえ、対応手順を整備・周知し、次回以降の訓練で手順が順守されているかを確認しましょう。

STEP3. 手順に沿った報告ができる

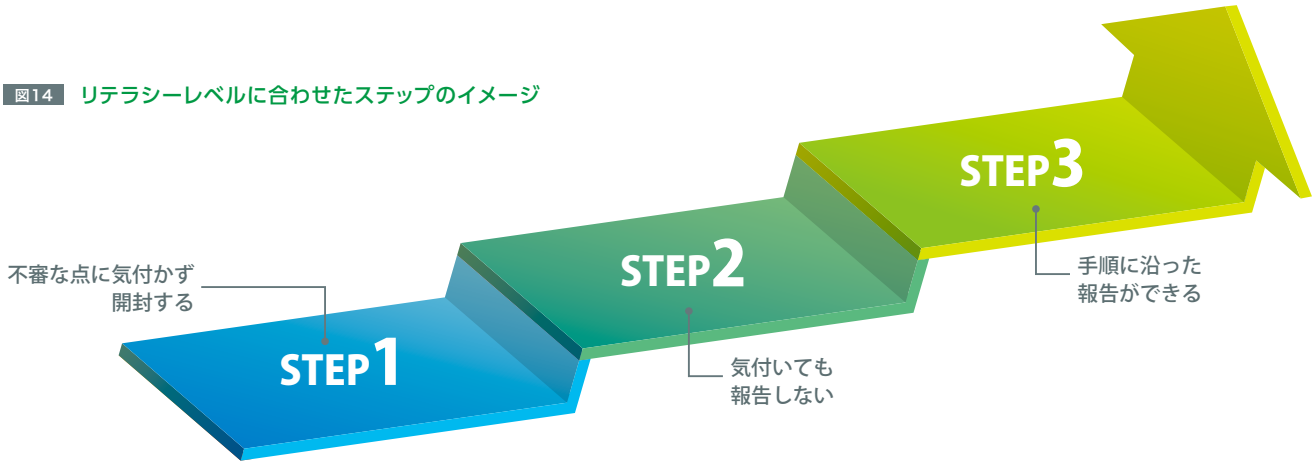
訓練を繰り返し実施すると、対応手順が定着した良い状態に近づいていきます。現実の標的型攻撃メールの傾向は常に変化し続けていることに注意しましょう。

例えば、数年前までは、標的型攻撃メールに添付されているのはほとんどが実行ファイル(exeファイル)でした。そのため、実行ファイルにさえ気を付けていれば、多くの攻撃を防ぐことができました。

しかし最近では、実行ファイルを使用した攻撃は減少し、Excelファイルなど、普段の業務でも使用されることが多いOfficeファイルに不正なマクロを組み込む方法や、メール本文にURLリンクを記載する方法を使用した攻撃が多く観測されています。

このことからも、最新の攻撃事例を反映した訓練を、継続して繰り返すことが大切です。

図14 リテラシーレベルに合わせたステップのイメージ



活用方法2. 社内ルール・運用プロセスの改善

社員のリテラシーが向上しても、標的型攻撃メールは一層巧妙になり、添付ファイルを開く可能性は常に存在します。開封してしまっても致命的な事態に至ることのないよう、社内ルールや運用プロセスの見直しを続けることが大切です。

社内ルールの改善

訓練を実施すると、社内のルールそのものに改善すべき点が見つかる場合があります。形骸化していたり、いざ実際に実行してみると手順が煩雑であったりといった問題です。

「不審な添付ファイルを開封したらすぐにLANケーブルを抜き、担当部門へメールで報告すること」という社内ルールがあり、訓練で添付ファイルを開封した人がLANケーブルを抜いたところ、インターネット接続が切断されてメールを送れなかったという事例もありました。

机上で定めた社内ルールが適切かどうか、実際に運用してみないとわからない部分もあります。その点でもメール訓練は大変有用です。

セキュリティ担当部門の改善

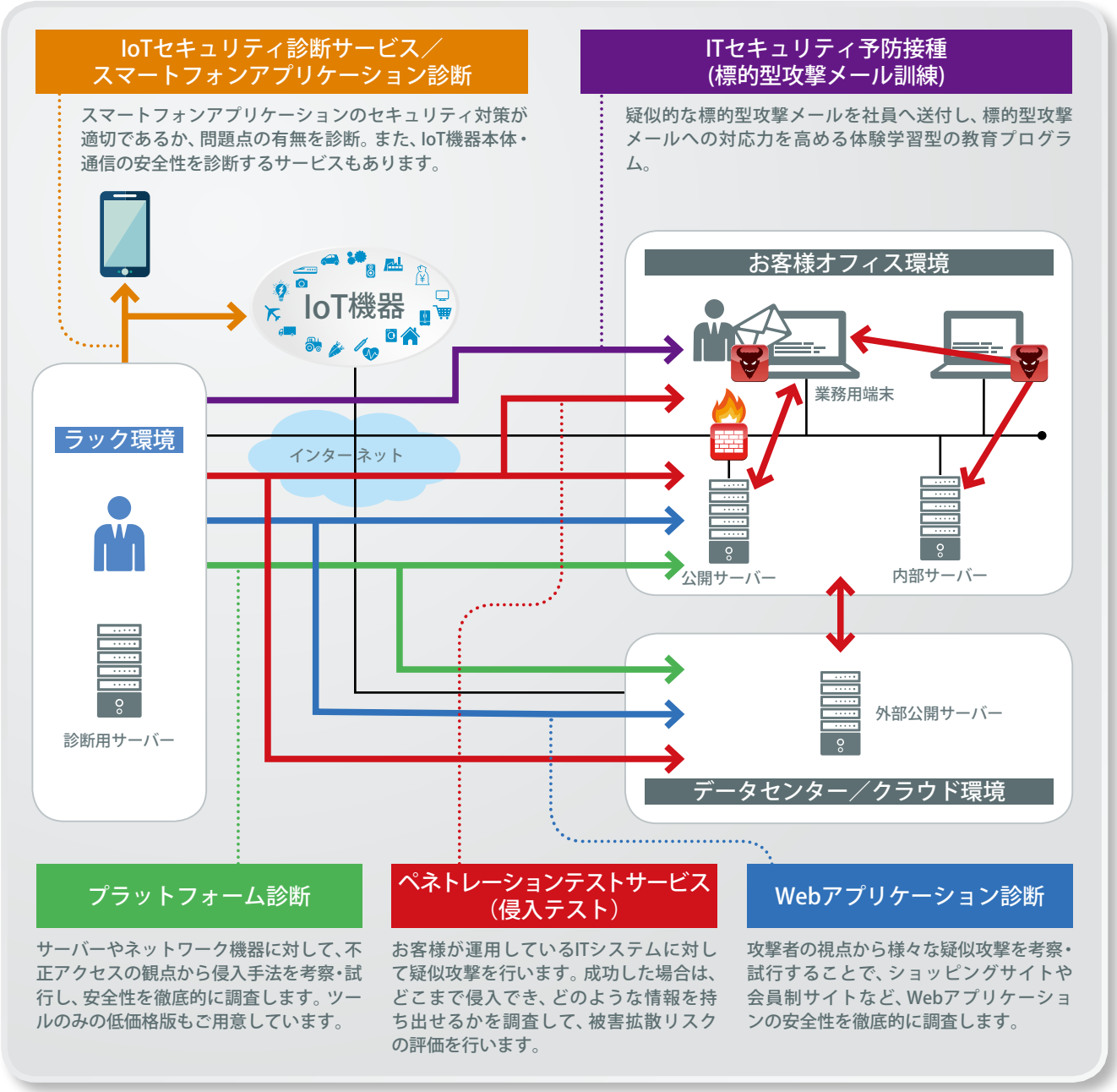
セキュリティ担当部門の改善もメール訓練の重要なポイントです。日頃、担当者が社員から問い合わせを受ける機会が少ないと、適切な対応ができないケースも想定されます。

メール訓練はセキュリティ担当部門の訓練でもあります。社員が報告しやすい環境づくりにも役立てましょう。

標的型攻撃メール対策は、組織にとって重要度を増しています。ぜひ、実績豊富なラックの知見をお役立てください。

ラックの「セキュリティ診断」ラインナップ

巧妙化するサイバー攻撃のリスクから組織を守るために。
進化を続ける最高峰の技術で、さまざまなセキュリティ診断をご提供しています。



セキュリティ診断とは、お客様のITシステムに対して攻撃者の視点から考察した疑似攻撃を試行することでリスクや脆弱性を見出し、対策を進めるためのサービスです。

ITシステムは多様な機器や製品、サービスを複雑に組み上げて構築されています。そのため、ラックではそれぞれの分野に細分化して、最高峰の技術によるセキュリティ診断サービスを提供しています。

上の図は、ラックが提供しているセキュリティ診断サービスを、ネットワーク上の経路に落とし込んだイメージ図です。

1995年、ラックは「セキュリティ診断サービス」を日本で初めてスタートしました。当初は、コンピュータ機器のオペレーティングシステムの脆弱性や、利用しているソフトウェアの脆弱性を発見するサービスが中心でしたが、ITサービスの多様化や、サイバー攻撃の巧妙化によって、セキュリティ診断へのニーズも広がってきました。

それぞれのサービスは、お客様が懸念しているサイバー攻撃被害を想定して用意しているもので、的確なサービスを選択、または複数サービスを組み合わせることにより、効率的にサイバー攻撃の脅威への耐性を調べることができます。

サイバー攻撃のリスクは、ますます高まっています。ぜひ、定期的なセキュリティ診断の実施をお勧めします。

株式会社ラック セキュリティ診断部

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
E-MAIL：sales@lac.co.jp　https://www.lac.co.jp