昨今の標的型攻撃メール訓練の実施課題

みずほリサーチ&テクノロジーズ株式会社
伊藤　聡司

1. はじめに

コロナ禍を起因としてここ数年で働き方も大きく変わり、企業に求められるセキュリティ対策も在宅などのリモートワークを考慮したものにシフトをしている。昨今の状況の変化に合わせて犯罪者側も未成熟状態の業務スタイルの隙を突き被害者の認識の甘さの利用や、企業側の対策未整備箇所の脆弱性を突き攻撃を変化させてきている。企業がセキュリティ対策に力を入れても、ばらまき型や標的型に代表される不審メールついては最終的には人間の判断で開いてしまう事が太宗となっている。このため各企業は標的型攻撃メールの訓練を行い社員のリテラシー向上を図る対応を迫られている。しかし、この標的型攻撃メール訓練は実際の効果を定量的に図りにくく、費用を含めた運用コストが掛かるものとなっている。

本稿は、現在の環境での標的型攻撃メール訓練の効果を上げる考え方、訓練担当者が直面する課題、結果の分析などに対する考えを述べていく。現在訓練を検討している担当者、既に実施している担当者の方に活用頂ければ幸いである。

2. 標的型攻撃メール訓練での指標

標的型攻撃メール訓練の実施で用いられる指標は主に２種類ある。一般的には「開封率」「報告率」と呼ばれている訓練結果を評価する際に用いられているものである。

開封率は、訓練対象者の中で、メール本文内にあるURLや添付ファイルを開いた人の割合だ。つまり「訓練用のメールに引っかかってしまった人」の割合と言える。

報告率は、訓練内容に応じて２つの指標があると私は考えており、過去に別媒体での記事※にて以下のように定義したので本稿においてもこの定義を用いていきたい。

受信報告率： 訓練メールを開封せずに「不審メールの受信を報告した人」の割合

開封報告率： 訓練メールの開封後に「不審メールの開封を報告した人」の割合

また、これらに加えて標的型攻撃メール訓練の自社の数年後の目標到達点を定義し、現在の立ち位置を分析した上で訓練を計画する事が望ましい。

3. 訓練指標の測定方法

これらの指標について、開封率はセキュリティベンダーが提供しているサービスの利用、又は自社で同様の仕組みを作る事で自動的に集計をするものが大半である。しかし、報告率については被訓練者が自主的に報告する何らかのアクションが必要となり、利用するベンダーのサービスによっては一部を自動化する方法は存在するが、被訓練者の動きも含めて完全に自動化して集計を行う事はできない。尚、この報告率を集計する訓練は組織が定めている規定に従い報告対応が出来ているかを評価する事が一般的である。この規則には自社環境を管理する部門への連絡タイミングや感染したと考えられる端末の扱いについて定められている事が太宗となっている。そのため被訓練者が自社の規則を何処まで把握し対応する事ができるかというものが報告率から得られるものである。

4. 訓練実施の課題

昨今の標的型攻撃メール訓練は、訓練担当者が計画時に考慮すべき検討事項が増加傾向にある。特に訓練を成立させるための環境面の技術的な事前確認、設定に掛かる工数見積り、訓練用文面・運用の工夫などは解決していないと十分な訓練成果を見込

※ https://www.itmedia.co.jp/enterprise/articles/1908/01/news004.html

む事が出来なくなる。そのため訓練を実施する上での課題を技術面、信頼度、経営理解の３つの視点で述べていきたい。

4.1　環境面における技術的な課題

昨今のリモートワーク環境促進により周囲に相談せず個人の判断で受信した不審メールを開封するような攻撃側優位の状況がより整ってきている。その対策として企業側がセキュリティ強化を講じた結果、訓練用メールが期待動作をしない場合がある。同様に添付ファイルに使われる Office 製品のセキュリティ対策も近年では強化されており訓練を成立させる上での考慮点となっている。これらは事前に確認をしていない場合、実際の訓練時に判明しコストを掛けてやり直すという事態も想定される。

それぞれ「メールセキュリティ対策製品」「外部アクセス制御」「Office 製品」の３点に分けて説明し最後に設定箇所を述べたい。

4.1.1　メールセキュリティ対策製品

メール対策ソフトでの注意点は、対策ソフトが不審メールとして判断し被訓練者にメールが届かないといったものが代表的である。これに加えて最近の対策ソフトは事前にメール内容をサンドボックスのように検証する機能が存在しており URL や添付ファイルを疑似的にチェックする事ができる。この過程でクリックした事となり被訓練者に届く前に開封などをした通知がサービス側に届くといったケースがある。尚、後者の場合は開封率がほぼ同一時刻に 100% となる結果が確認できるため判別がつきやすい。

4.1.2　外部アクセス制御

企業によっては社内環境から外部へのアクセスを制限している場合もある。メール本文の URL クリックや添付ファイル開封時の集計の仕組みは http 通信を利用した外部アクセスである。よって、外部アクセス制御が掛けられている場合は URL 型・添付ファイル型は共に通信が遮断され結果の集計をする事が出来ない。

4.1.3　Office 製品の挙動

添付ファイルについては､「編集を有効にする」「コンテンツの有効化」などの所謂、保護ビューに関わる端末の設定状況によっては開封の通知が動作しない事がある。これは添付ファイルが外部に通信する際に許可されていないといけない権限などが関係する。更に外部通信をするという事自体が通常では発生しない事なので Office 製品が保護をしているものとなっている。近年はこのセキュリティ強化が起因で Office 製品を使った添付ファイルでの訓練を期待通りに行う事が難しくなっている。

4.1.4　設定箇所と必要な情報

メールセキュリティ対策、外部アクセス制御などは製品の仕様としてホワイトリスト登録など例外設定が可能な事が一般的である。訓練担当者は事前にこの設定が可能な事と、設定に必要な情報を把握している事が望ましい。特に訓練担当者自身の所属と別組織に依頼する時などは経緯説明などを含めて想定以上の期間が掛かる事がある。また、これらの設定に必要な情報は環境や製品毎に異なるため一概にこれが全てという事ではないが対策箇所と設定事項を図１に纏めた。訓練の運用担当者は自社の環境を精査した上で計画を立てなければならない。

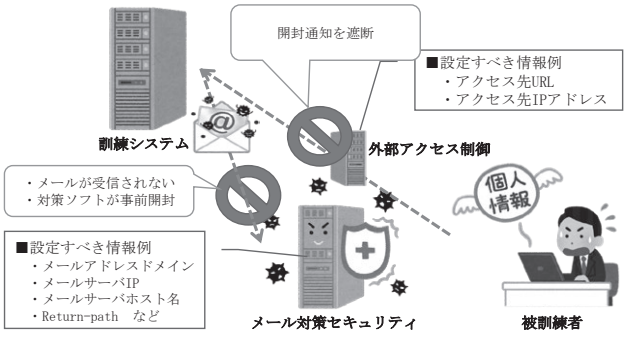

図1：セキュリティ対策箇所

4.2　訓練実施における信頼度の課題

環境面の課題と並行して取り組むべき事は、訓練の質についての検討となる。特に訓練結果の信頼度に関わる主な課題は２点存在する。

これらの課題に対し訓練担当者は対策を立てる、方針を決めるなどして割り切るなど計画を立てていく必要がある。

１：訓練メールであることが周知される
２：報告率を測る際の開封率が低い

１つ目は開封する可能性のある社員が周知された事で引っかからず結果に集計されない図２に示したような状況となる。対策としては訓練を細かく分割し同一組織内で共有されないように訓練日を分ける、異なる文面を用意するなどがあるが、これは訓練関係者の人件費やサービスの利用料など工数に直結するため自組織の予算や体力を勘案する必要がある。

２つ目は報告率を評価するための標本数として少ない場合を意味する。極端な例だが 1000 人の会社で 10 名開封し、その中で 8 名が報告した場合、開封率は 1% であり、報告率は 80% となる。この 10 人の報告率の結果をもって自社全体の状況を正確に測れるとは言い難い。対策としては事前に開封率の目標を定め、自社の被訓練者のリテラシーや文化を分析する。その結果から一定程度開封すると想定される訓練メールの文面を作り込む事が必要となる。ここはある意味訓練担当者の腕の見せ所となる。

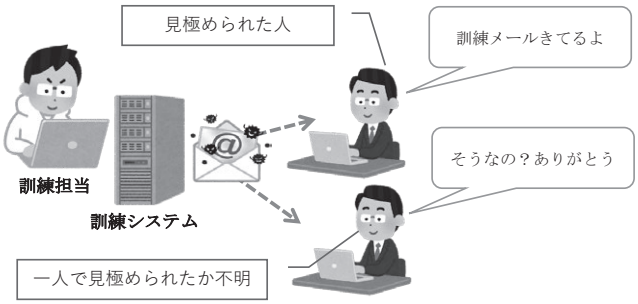

図2：訓練時の組織内共有の例

4.3 経営層への説明課題

訓練担当者は経営層に報告する際に自社社員の標的型攻撃メールに対するリテラシーがどの段階であるか説明し数年に渡るロードマップを示した説明をする必要がある。これを行わない場合、結果だけを見た経営層が過剰に反応し過度な対応を指示する場合などがある。

そのため事前にその年の訓練の位置づけを説明し理解を得た上で実施するのが望ましい。特に開封率については報告率の精度を上げるために一定の開封者が必要となる。よって開封率の高さは参考値であり、本当に見るべきものは報告率と自社の現在のリテラシーの成熟具合である事を説明し理解してもらう事が必要となる。

5. 訓練結果報告の考慮点

5.1　経営層が気にする事

訓練担当者は訓練の実施後に結果を経営層に報告する必要がある。経営層への報告は自社の客観的な結果を示し、次年度以降に向けた方針と必要な予算の了承を取り付けるという重要なものとなる。体制も予算も据え置きという結果では自社のリテラシー向上は望めない。

ここで担当者が考慮すべき点は経営層が求めている報告内容は自社の客観的な状況であるという点だ。よって報告は開封率や報告率などの客観的な指標を用いた報告を行う必要があるが、単年の自社報告のみだと経営層が判断出来ず十分な報告とならない。そのため、過去の自社との変化、他社との比較など縦横の客観的差異を示す事で説得力を持たせる必要がある。ただし、他社との比較は訓練の前提条件や使っている指標の差などを明確にした上で比較報告をしないと見た目の数値で優劣を判断されてしまうので十分な分析をした上で報告に臨む事が必要となる。

5.2　比較に必要な他社の情報入手

経営層へ報告する際の準備として、「過去の自社

との比較」「他社との比較」など縦横の軸を用いて報告を組み立てる事が出来るように準備をする必要がある。特に訓練初年度は過去の自社との比較が不可能なため、横の比較が重要となる。比較対象としては「他業種との比較」「同業種との比較」といった業種全体のものから「同業種のA社」や「同グループ会社B」のような個別のものがある。業種全体については、例えば利用している標的型攻撃メール訓練サービスを提供しているセキュリティベンダーから提供を受ける事が考えられるが、「開封率」の情報のみとなり、守秘義務の関係上個別の情報開示は難しいだろう。また、「報告率」についてはサービスを提供しているセキュリティベンダーが顧客から収集しているケースが少なく情報を得る事は難しい。

他社の情報を得るために訓練担当者には通常の業務から1歩踏み込んだ対応が求められる。常日頃から同様の立場の他社の訓練担当者やセキュリティベンダー担当者と交流・意見交換をし、「開封率」「報告率」の情報交換ができる関係を築く事が必要となる。

6. 訓練の質向上に向けた取り組み

最後に標的型攻撃メール訓練を行う上で訓練担当者の工数・コストに見合った成果を出すために計画段階で検討すべき事を述べて本稿を終わりとしたい。

6.1　訓練目的を明確にする

訓練目的を明確にする必要がある。例えば、「不審なメールの見極め」を目的とする訓練と、「不審なメールが届いたときの社員の対応力を測る」ことを目的とする訓練とでは、使用するメールの文面や訓練の実施体制が異なる。

6.2　訓練の割り切り事項を見極める

4.2で前述した通り標的型攻撃メール訓練における課題の一つに、「意図しない周知によって結果の信頼度が損なわれること」がある。この課題解決は訓練の分割などで対応は可能であるが、予算や人的リソースといったコストとのトレードオフになるため、訓練担当は計画時に「どこまで割り切るか」を見極めておく必要がある。

6.3　関係部門との調整は十分に行う

規模の大きい組織において効果の高い訓練を行うには、関係部門を交えた準備が必要となる。特に報告率を求める訓練では、報告先の部門に負担がかかるため、事前の調整が必要である。また、訓練を受ける各部社員は通常の業務を行っているため繁忙期を見極めた上での実施が求められる。

6.4　メール文面は受け取り手の立場で作る

高い訓練成果を挙げるためには不審なメールと思わせず高い開封率を促すメール文面を作成し、信頼できる報告率を測定するために十分な開封者を確保する事が望ましい。そのため内容については被訓練者の心理に付け込んだ内容のメール文面を作る必要がある。特に「相手の立場で受け取る可能性のあるもの」「時期がある程度限定されているもの」は比較的開封率が高い結果となる事が多い。