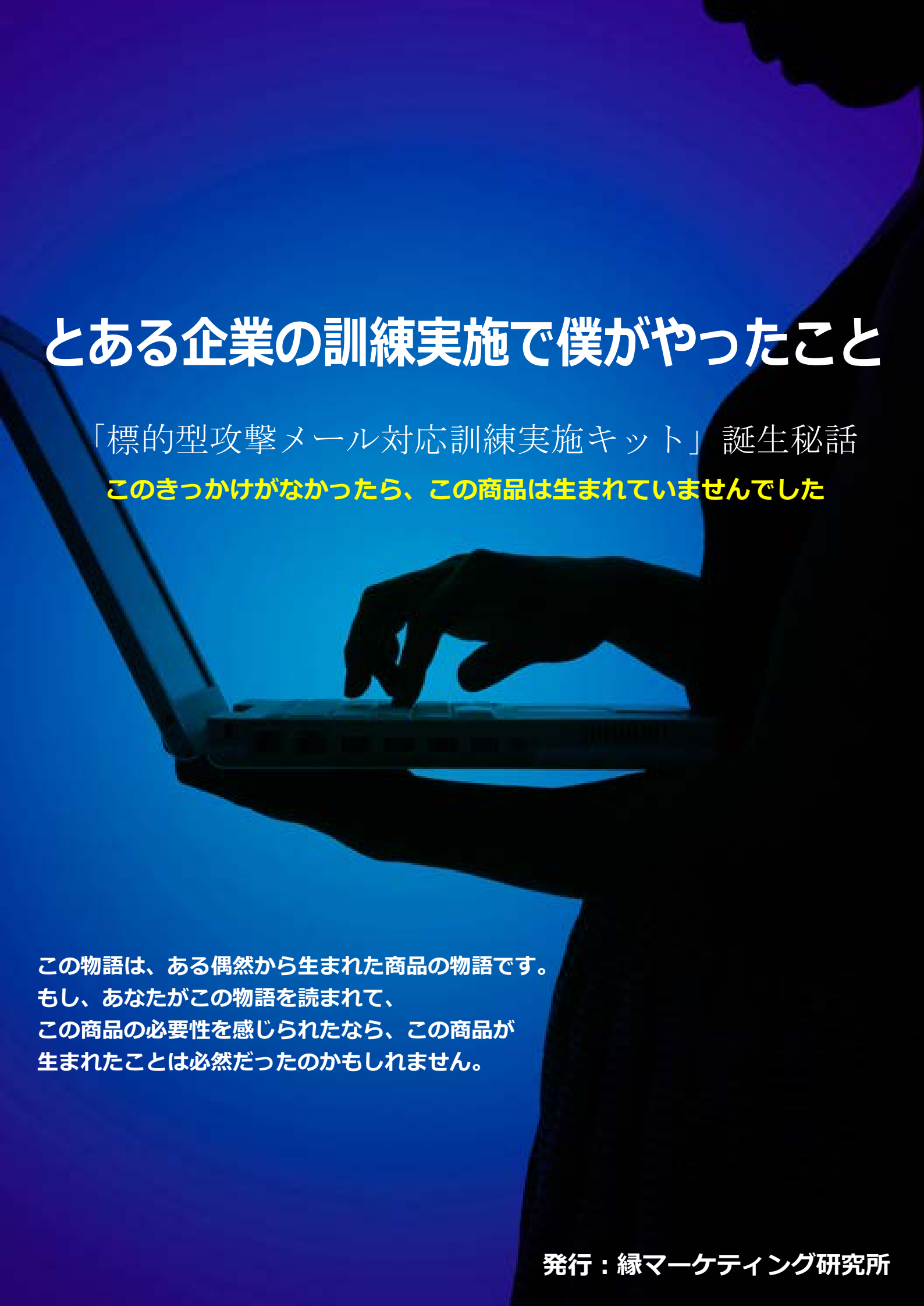


とある企業の訓練実施で僕がやったこと

「標的型攻撃メール対応訓練実施キット」誕生秘話

このきっかけがなかったら、この商品は生まれていませんでした

この物語は、ある偶然から生まれた商品の物語です。
もし、あなたがこの物語を読まれて、
この商品の必要性を感じられたなら、この商品が
生まれたことは必然だったのかもしれません。

発行：縁マーケティング研究所

はじめに！

本書を読むと
こんなことが分かります

本書は、ベンダーによる訓練サービスを利用することなく、模擬のマルウェアの作成も含めて、自社で「標的型攻撃メール」に対応するための訓練を実施することを可能にした商品が生まれることになったきっかけをお伝えするものですが、本書をお読みいただくことで、以下の４つの知識も併せて得ることができます。

1 **ベンダーによる訓練サービスで使用される、訓練で使用する添付ファイル（模擬のマルウェア）を作成する方法と、添付ファイルを開いた人が誰か？を特定する仕組みについて知ることができます。**

2 **ベンダーによる訓練サービスを利用しなくとも、訓練の実施は自分達で行う方法があることを知ることができます。**

3 **ベンダーによる訓練サービスを利用するとした場合、どのような観点に基づいてベンダーを選べば良いのか？ベンダーを選択する際に抑えておきたい７つのポイントについて知ることができます。**

4 **「標的型攻撃メール対応訓練実施キット」がどのような想いで作られた商品であるのか？そして、どのような商品であるか？について知ることができます。**

初めまして、こんにちは。

本書をダウンロードいただき、誠にありがとうございます。

縁マーケティング研究所 代表の 野々市 恭 徳（ののいちやすのり） と申します。

縁マーケティング研究所？聞いたことがない名前だなあ。この名前を見て、きっと、そう思われたのではないでしょうか？なんでこんな名前を聞いたこともないようなところが、「標的型攻撃メール対応訓練実施キット」を手がけているのだろう？そう思われたかもしれません。

「標的型攻撃メール」に対応するための製品やサービスについて Google で検索を行えば、それらを手がけているのは、セキュリティ対策に関するハードウェアやソフトウェアの販売を生業とする、いわゆる「セキュリティベンダー」と呼ばれるところばかりです。セキュリティベンダーが標的型メール訓練に関するサービスを手がけていても何ら不思議でないと思いますが、「縁マーケティング研究所」という名前も知らないようなところが何故に「標的型攻撃メール対応訓練実施キット」なんていうものを手がけているのか？

本書ではその理由をお話しすると共に、ベンダーが提供する訓練サービスが幾つも存在するなかで、何故「標的型攻撃メール対応訓練実施キット」を世に出すことにしたのか？本書を読んでいただくと、その理由がきっとおわかりいただけると思います。

本書をお読みいただければ、「標的型攻撃メール対応訓練実施キット」がどのような方に向けた商品であるか、また、標的型攻撃メール訓練が、どのような仕組みで実施されるのか？そして、既にベンダーが提供する訓練サービスをご利用になられていらっしゃる方であれば、かかるコストを抑えるための方法について、知っていただく事ができると思います。

本文中には難しい用語も登場するかもしれませんが、楽しみながらじっくりお読みいただけると幸いです。

本書の筆者：縁マーケティング研究所 代表　野々市恭徳

1965 年東京生まれ埼玉育ち。システムエンジニア、プロジェクトマネージャーの経験を経て現職に。

Excel と他のアプリケーションを連携させての業務効率化・自動化を得意とするが、サーバ構築などのシステム構築から、ドキュメントライティング、企画書作成、お客様サポートなど、オールラウンダーでこなせるということで、クライアントからは様々な場面で頼られることが多い。

セキュリティ関連業務は 2009 年から。「標的型攻撃メール対応訓練実施キット」を開発したことをきっかけに、現在では、セキュリティ教育のあり方（特に標的型メール訓練のあり方）を追求する日々を送っている。

目次

お話しを始める前に
ちょっとだけ
自己紹介をさせてください

キットの生い立ちについての話をする前に、まず、少しだけ自己紹介をさせて下さい。
自分は 1965 年に東京で生まれ、3 歳になった頃から以降、埼玉で育ちました。

パソコンはタレントのタモリ氏が富士通のパソコンの CM に登場していた時代（これをご存じの方はきっと同世代ですね）から触っていましたから、プログラミングの経歴はずいぶん長いです。あの時は NEC が日本のパソコン市場のほとんどを占めていた時代ですから、今から思えば隔世の感があります。

子供の頃からプログラミングをやっていたので、ひねくれ者の私は、大学卒業後はプログラマ以外の職業に就きたいと考えていたのですが、インターネットブームがやってきたのをきっかけにネットビジネスの世界に足を踏み入れることとなり、プログラミングが得意だったことから、結局、開発者としての道を歩むこととなりました。

今にして思えば、やはりシステム開発の仕事が好きだったということなのだと思います。インターネットビジネスに足を踏み入れた最初の頃は、知り合いと一緒に立ち上げた小さなホスティングサービス会社で、サーバの構築・運営・ユーザサポートなど、開発から運営まで、一通りのことを手がけていました。

当時は楽天やサイバーエージェントなど、今では日本を代表するネット企業がまだ無名とも言えるような存在だった頃で、当時松山を拠点にされていたサイボウズの社長さんが、ホスティングサービス会社であった私どものところにわざわざ協業の申し出に来られたり、サイバーエージェントの創業メンバーの方々が何か一緒にできることはないか？と話に来られるなど、ネットビジネスに将来性を見出し、精力的な活動をされていた方々とお会いする機会が得られたことは、今にして思えば、貴重な体験だったと思います。

あいにく、その時の自分は時流を掴み損ねてしまい、ネット長者にはなれませんでしたが、その後システム開発コンサルティング会社に転職をし、そこで出会ったのが VBA（Visual Basic for Applications）でした。

VBA とは、Microsoft Excel や Word などの Office 製品群をプログラムによって操作できるというもので、Excel などの Office 製品に標準で備わっている機能です。Excel・Word だけでなく、OutLook や Access、Visio といったアプリケーションを横断してデータの連係や処理ができるため、面倒な手作業を自動化することができます。

データ入力のフロントエンドとして Web ブラウザを使うケースは多いですが、実際の業務ではシステムにデータを登録するために手作業が発生してしまうというケースはありがちなため、そういった手作業を自動化・効率化するために、Office 製品を活用するということをよくやりました。

そんなこんなで、様々な事例を通じて VBA に関わるうちに、自然と経験を積むこととなり、今では、VBA やインターネット技術を活用しての業務改善、自動化・効率化支援を仕事としてするようになった。というのが、自分のこれまでの経緯になります。

で、そんな自分が何故、「標的型攻撃メール対応訓練実施キット」なんていうものを手がけるようになったのか？という話に戻るわけですが、このきっかけは、ある大手企業様から、「標的型メール攻撃」の訓練用に使う、Web ビーコンが埋め込まれた Word ファイルを作って欲しいという依頼を受けたことでした。

標的型攻撃メール対応訓練実施キットは、

・訓練実施の手段として「Web ビーコン」を使う方法が使われていなかったら、
・その「Web ビーコン」を使うために大量の Word ファイルを作成する必要がなかったら、
・そして、大量の Word ファイルを作成するために VBA というツールがなかったら、

きっと生まれなかっただろうと思います。これらの条件が重なったことは全くの偶然なだけに、世の中、何がどう転ぶかわからないものです。それでは、話の続きを始めましょう。

そもそも、「標的型メール攻撃」の訓練って何でしょう？

「標的型メール攻撃」の訓練は、座学によるセキュリティ教育とは違い、実際の標的型攻撃メールに似せた模擬のメール（訓練メール）を従業員に送り、身をもって体感してもらう形で行われる、**セキュリティ教育手法**のひとつです。

座学ではわかった気になっても、聞くと見るでは大違い。座学による研修では満点を取った従業員ですら、模擬の標的型メールにはあっさりひっかかってしまうこともしばしば。

パソコンやネットワークに侵入して情報を外部に流出させようとするような、悪意ある目的を持ったプログラムが仕込まれたファイルを、従業員がそれと知らずにうっかり開いてしまえば、会社に与える被害は甚大なものとなる可能性もあるだけに、従業員一人一人が、標的型メールに常に注意を払うよう、意識付けをすることは必須と言えます。

そのため、訓練実施においては、模擬のメールとはいえ、誰がうっかり開いてしまったのかを把握することは必須となるわけですが、そのための方法としてよく使われるのが、**「Web ビーコン方式」**と呼ばれる方法です。

Web ビーコンとは、見た目に目立たないよう、横 1 ドット×縦 1 ドットのサイズに設定した「画像ファイルへの URL リンク」のことで、これを文章ファイルに設定すると、その文章ファイルを開いた人が誰であるか？を特定することができる仕組みです。

元々は Web サイトを閲覧した人を追跡するための仕組みですが、Word 文書ファイルにも応用できるということで、Web ビーコンを仕込んだ Word 文書ファイルを作成し、訓練メールに添付することで、メールに添付された Word 文書ファイルを誰が開いたのか？つまり、標的型攻撃メールにひっかかってしまった人は誰か？を特定することができる。というのが、**「Web ビーコン方式」**による訓練実施の方法になります。

「標的型攻撃メール」が具体的にどのようなものかを知ってもらうための方法として、体験型の訓練を実施することは、訓練を受ける側に強い印象を与えるには最適の方法ですが、

「何もそこまで大袈裟なことをやる必要はないんじゃないか？」
「ウィルスの危険性は誰もが知っていることだから、訓練なんてしなくてもみんなわかっている」

という意見に加え、訓練をやったとしても、標的型攻撃メールにひっかかってしまう人がゼロになる保証が得られるわけではないということで、訓練なんてやってもしょうがないんじゃないか？と考える方も多いようです。

これは、訓練が**「セキュリティ教育のための方法のひとつ」**としてのみ捉えられている事が原因ではないかと思うのですが、訓練実施による効用は、何も怪しいメールを開かないようにすることだけではありません。

毎年訓練を実施している大手企業でも、怪しいメールをうっかり開いてしまう人をゼロにすることは実現できていません。標的型攻撃メールは手口が巧妙なだけに、どれだけ訓練をしようとも、うっかり開いてしまう可能性はありうるわけです。

では、大手企業は何故、毎年訓練を実施しているのでしょうか？
訓練をやっても、ひっかかってしまう人をゼロにすることはできないのに・・・。

この問いに対する答えとなるキーワードが、

うっかり開いてしまった後の対応はどうすればいいのか？

ということです。

誤って標的型攻撃メールに添付されていたファイルをうっかり開いてしまったら、その瞬間、悪意を持ったプログラムが社内ネットワーク内に侵入し、顧客情報を外部に送信したり、自社を踏み台に、取引先にウィルス付きのメールを送ってしまうかもしれません。

しかし、何の確証もないのに、ファイルをうっかり開いてしまったというだけで、慌てて取引先等に連絡をすれば、却って混乱し、信用をなくすような事態に発展してしまうだけです。とはいえ、ウィルスに感染してしまっているかもしれない状況で何もしなければ、被害が拡大していくことになるかもしれません。そんな状況の中、従業員、そしてあなたが取るべき対応は？

標的型攻撃メールへの対処として、そもそもそういった類いのメールにひっかからないようにすることは、根本的な対策として必要ですが、万一、ひっかかってしまったことに気がついた時の対処として、従業員一人一人がどのような行動を取ればよいのか？ということについて、あなたの組織では対処策がしっかり考えられているでしょうか？そして、その対処策を、誰もが迷うことなく、また、まごつくことなく実行できる体制・ルール作りができているでしょうか？

ちょっとした油断などから、ウィルスに感染してしまう可能性はどの企業でもありうることです。感染しないようにすることも大事ですが、企業として本当に大事なのは、万一、感染してしまった場合にどう対処するか？です。対応をひとつ間違えれば、重大な損失や信用の失墜に繋がるだけでなく、対処に追われる従業員の士気低下にも繋がります。

顧客情報が漏洩してしまったことで損害賠償を求められるようなことにでもなれば、中小企業であれば、会社として存続できるかどうかといった問題にまで及んでしまう可能性もあります。

対処に追われたことで従業員が疲弊してしまい、会社のリスクマネジメント姿勢に疑問を感じて優秀な社員が辞めていってしまうということだって、考えられないことではありません。

リスクマネジメントの一つとして、標的型攻撃メールにひっかかってしてしまったことに気づいた場合の対処策を決めておき、訓練実施によって、実際にその通りできるかどうかを試すというのは大事なことであり、また、有益な方法です。

ウィルスに感染しないようにすることも必要ですが、感染してしまった場合でも混乱することなく対処ができ、被害を最小に抑えることができるようになっていれば、まさに言うこと無しでしょう。

本当にできるかどうかは、実際にやってみることです。
実際にやってみると、意外とできないことがよくわかるはずです。

あなたがもし、「訓練なんて大袈裟」「そんなものやらなくても、みんなわかっている」と思われていらっしゃるなら、御社の従業員が万一、標的型攻撃メールにひっかかってしまったと気づいた場合、次のアクションとして、その従業員は何をするだろうか？を考えてみて下さい。

もし、「想像できない」という答えになるのであれば、御社は今、何の保険もかけずに車を運転しているのと同じ状態にあるのかもしれません。

「だろう運転」が危険な行為であることは、車を運転されている方なら、運転免許センターの講習でしつこいくらいに聞かされていることと思います。

「ウィルスが会社にとって危険なことくらい、みんなわかっている**だろう**」
「さすがに、不審な添付ファイルを開いてしまうことなんてない**だろう**」
「誤って開いてしまっても、ちゃんと対処はできる**だろう**」

というのは、ただの思い込みに過ぎません。「だろう」を「かもしれない」に置き換えたら、あなたはきっと不安になるはずです。

「ウィルスが会社にとって危険なことを、わからない人がいる**かもしれない**」
「不審な添付ファイルときづかずに、開いてしまう人がいる**かもしれない**」
「ウィルスに気づいても、ちゃんと対処ができずに被害を拡大させてしまう人がいる**かもしれない**」

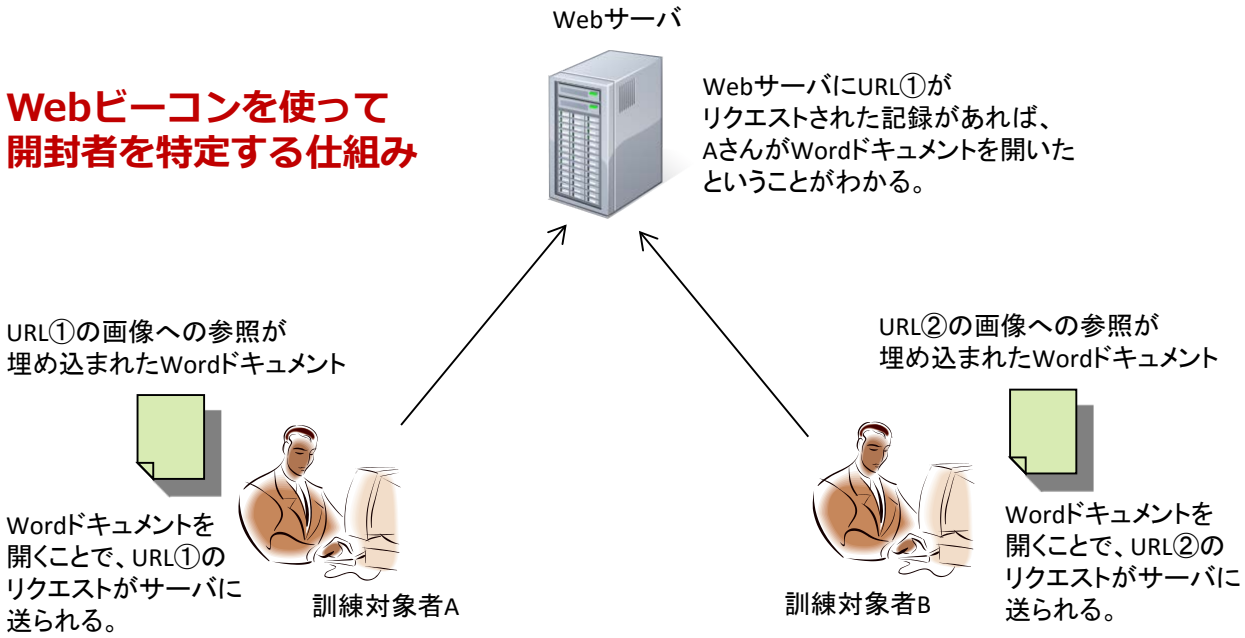
不安に思うあなたの心配を解消する確実な方法は、**実際に試してみること。**そう、座学による教育ではなく、訓練の実施によって、実際にできるかどうかを確認することです。

だから、大企業は毎年、訓練を実施するのです。

訓練実施の目的は、ウィルスに感染しないようにすることだけではありません。万一感染してしまった場合にどうするべきか？を、従業員一人一人にしっかり認識してもらうようにすることも目的の一つです。
机上で設計した対応フローは「絵に描いた餅」になりがちです。また、座学による学習だけでは、実際にはその通りにはできなかったりするものです。
実際にやってみることで、机上の検討だけでは見えなかったことを洗い出せるのも、訓練実施の効用です。

Web ビーコンを使った訓練実施は、
意外に大変です
どこが大変なのでしょう？

私が依頼を受けたその上場企業様では、悪意のあるマクロが仕込まれた Word の添付ファイルが、社内のシステム管理者を装った第三者から送付されてきた。というシナリオで訓練を実施することを考えていたのですが、誰が Word の添付ファイルを開いてしまったかを知るために、送付対象となるユーザごとに、異なる URL への参照を埋め込んだ Word ファイルを作る必要がありました。



Web ビーコンを使う方式では、ユーザが Word ファイルを開くと、Word ファイル内に埋め込まれた横 1 ドット×縦 1 ドットの画像を表示するために、その画像に設定されている URL リンクが自動的に呼び出されます。

例えば、その URL リンクが埋め込まれた Word ファイルは A さんにしか送らないようにすれば、その URL リンクが呼び出されている記録がサーバ側に残っていることを確認することで、A さんが Word ファイルを開いた。と判断できるということになります。

Web ビーコンを使う方式では、添付ファイルを開いた人を特定するために、以下の作業を行う必要が生じます。

Web ビーコン方式を使う場合に必要となる作業

① ユーザ数分の画像ファイルを作成する作業

② ①で作成した画像へのリンクをそれぞれ埋め込んだファイルを作成する作業

③ ①で作成した画像ファイルを Web サーバにアップロードする作業

これが 10 通や 20 通といった程度なら、手作業でも頑張ればどうにでもなるのですが、くだんの企業様の訓練対象者は数千人の規模でした。さすがに数千個の Word ファイルを作るとなると、もはや手作業では無理になります。訓練を実施するためには、短時間で数千個の Word ファイルを作らなければならないということで、VBA に精通した私に依頼すれば、一気にファイルを作ってもらえると考えた。というわけです。

ここでようやく、縁マーケティング研究所なんていうところが、何故「標的型攻撃メール対応訓練実施キット」なんていうものを売っているのか？という話に繋がってきます。

VBA（Visual Basic for Applications）を使うと、Microsoft Word や Excel の操作を自動化することができますが、VBA でできることはそれだけではありません。Windows Script Host（通称 WSH）などと組み合わせることで、ユーザ数分の画像ファイルを作成し、Web サーバにアップロードすることも自動化することができます。

システム管理者はこのような方法を使って作業の省力化を図りますが、通常のビジネスの現場ではあまり使われていません。通常のビジネスの現場でも省力化できることは沢山あるだけに、勿体のないことです。

ちょっと横道にそれますが、Web ビーコンを含んだ Word ファイルの作成方法はご存じでしょうか？意外に知らないという方もいらっしゃるので、本書をお読みいただいている御礼も兼ねて、Web ビーコンを含んだ Word ファイルの作成方法についてご紹介します。

実際に自分でやってみると、Web ビーコンを含んだ Word ファイルをユーザ数分作成する作業の大変さと、その作業を自動でできるようにしたいと思われた企業様の気持ちを実感していただけると思います。

【Web ビーコンを含む添付ファイルの作り方】

手順１　画像ファイルへのリンクを含んだ簡単な HTML データファイルを作成します。この時、画像ファイルのサイズを横 1 ドット、縦 1 ドットに指定するのがポイントです。

以下は作成する HTML データファイルの例になります。

```
<HTML>
<BODY>
<IMG SRC=”http://happyexcelproject.com/bcon.gif “ width=”1” height=”1”>
</BODY>
</HTML>
```

手順２　手順 1 で作成した HTML データファイルを「index.html」としてパソコンに保存します。

手順３　手順 2 で保存した index.html を Word で開きます。

手順４　index.html を Word で開くと、「Web レイアウト」モードでファイルが開かれるので、Word のリボンタブから「表示」を選択し、文章の表示モードを「印刷レイアウト」モードに切り替えます。

手順５　Word ファイルに加えたい文書を設定します。手順 1 で設定した画像ファイルのサイズの大きさは横 1 ドット、縦 1 ドットとしているため、Word で開いた際には点として表示されることになり、見た目には気づきません。手順 4 の時点で「矢印キー」を使ってカーソルを左右に動かしてもらうとわかりますが、文章内に 1 ドットの点が設定されているのがわかるはずです。

Word に文章を追加する際、この 1 ドットの点を誤って削除しないようにして下さい。

手順６　作成した文書を Word ファイルとして保存します。これで、Web ビーコンが埋め込まれた Word ファイルの作成が完了です。

私が素直だったら、
この商品が生まれることは
なかったと思います。

この時、私がクライアントからのリクエスト通りに数千個の Word ファイルを作っていたら、「標的型攻撃メール対応訓練実施キット」が生まれることはなかったと思います。

クライアントからのリクエストを聞いて、この時、私がまず思ったことは、

「メールが転送されたら、その人が開いたのかどうかわからないよなあ」

ということでした。また、

「Word ファイルを作るのはいいけど、1 通ずつ送るのも面倒だよなあ」

ということも思いました。リクエスト通りにやることはできるけれど、それでは効率が悪く、訓練実施の方法としてはあまりよい方法だとは思わなかったのです。仕事を請ける側としては、クライアントがリクエストしてもいないようなことをする。なんていうことはせず、クライアントからのリクエスト通りに作業を行って納品すれば、それで良かったのかもしれません。しかし、明らかに効率が悪いということがわかっていながら、改善策の一つも提示しないというのは、どうにも我慢がなりませんでした。

Web ビーコン方式を使った場合、面倒になるのは画像ファイルや Word ファイルを作る作業だけではありません。作成した各 Word ファイルをそれぞれのユーザに個別に送付する作業も必要になります。しかし、そのような苦労を経て作業を完遂したとしても、ファイルが別の人に転送され、転送先で開かれたら、誰が開いたかわからなくなってしまうという可能性があります。

やりたいことは
誰がファイルを開いたか？
を知りたいということ

実際に添付ファイルを開いた人は誰か？を特定するのが目的なのだから、その情報を確実に取得できる方法はないだろうか？それも、個別に添付ファイルを作るなんていう面倒なことをしなくて済む方法で。

ということを考えたときに気がついたのが、その会社では ActiveDirectory（Microsoft Windows で使われる、ユーザーとパソコンを管理する仕組み）を使っており、パソコンへのログインなどは、あらかじめ決められたユーザ ID が使われる仕組みになっていたということでした。

ActiveDirectory を使っているなら、添付ファイルが開かれたら、そのパソコンから ActiveDirectory の情報を取得すれば、その添付ファイルを開いた人を特定できるのではないか？また、ActiveDirectory を使っていないケースでも、OutLook に設定されているメールアドレスや、パソコンのログイン情報・IP アドレスといったものを取得できれば、やはり、その添付ファイルを開いた人を特定できるのではないか？

このことに気づいた私は、早速 VBA を使って、ActiveDirectory の情報や、OutLook に設定されているメールアドレス情報などを取得してみました。そうしたらドンピシャです！ログインしているユーザの名前や所属部署名、メールアドレスといった情報が取得できるではないですか。

ユーザの名前や所属部署名がわかれば、どこの誰であるかが一発でわかります。これが Web ビーコンを使う方法だと、わかるのはどの URL がリクエストされたか？だけなので、どこの誰であるかを特定するには、その URL を参照するよう設定した Word ファイルを誰に送ったか？を調べなければなりません。

しかも、特定できたとしても、Word ファイルは別の人に転送されているかもしれないので、必ず

しもその人が開いたとは限らないということも考えられます。しかし、ActiveDirectory の情報なら、ログイン ID の使い回しでもされていない限り、別の人ということはありません。

この方法なら、Web ビーコン方式のように、ユーザ数分だけファイルを作成する必要もなく、添付ファイルを開いた人も確実に特定することができます。作るファイルは１つで済むのですから、大きなメリットです。

そして、メールアドレスを取得できていることから、開封者の情報をメールで送るようにすれば、Web サーバも不要になるではないか。ということにも気がつきました。

小さな会社なら、Web サーバを用意して社内に設置するのは、技術者さえいれば、それほど大変なことではありませんが、規模が大きな会社や、拠点が複数に分かれていたりする会社では、全社員がアクセス可能な Web サーバを用意することは気軽にできることではありません。

訓練実施を企画する部署と、サーバを管理する部署は異なっていることが多いので、サーバを用意するには部署間での調整が必要となり、Web サーバを使うというだけで、準備に結構な手間と時間が必要になったりするものです。

訓練を実施するのに Web サーバが不要となれば、部署間の調整事項がなくなるので、実施がし易くなるという大きなメリットが生まれます。メールで開封者情報を送る方法なら、既存のメールサーバを使えばいいので、訓練のためだけにシステムを準備する必要もありません。

Web サーバであれ、メールサーバであれ、サーバを用意するのは面倒なものです。サーバ本体やサーバの置き場所、そしてサーバをセッティングする技術者など・・・これらが不要になれば、その分、準備にかかる時間も費用も、そして手間も軽減されることは言うまでもないことです。

こうして、
キットの基本となるモデルが
生まれました

Web ビーコンを使った方法では、添付ファイルを開いた人が誰かを特定するのに、

Web サーバからアクセスログを取り出し、
誰にどの URL 情報を送ったかの情報との突き合わせを行って、
初めて誰が添付ファイルを開いたか？がわかる

ので、結果がわかるまでに結構な時間を必要とします。しかし、メールで送る方法なら、メールが届いた瞬間に誰が開いたかがわかるので、訓練開始と同時に結果を知ることができます。これだけ良い条件が揃うのですから、もはや Web ビーコン方式を採用する理由はありません。
このことに気がついた私は早速サンプルを作成して、クライアントに提案を行いました。

もともとは Web ビーコンを埋め込んだ Word ファイルをユーザ数分作成して欲しい。という依頼だったので、それとは全く異なる提案を見せられた時は、クライアントも面食らったに違いありませんが、

誰が添付ファイルを開いたのかを確実に特定できる。
ユーザごとに添付するファイルを変えてメールを送らなくても良い。
Web サーバが要らない。
添付ファイルを開いたのが誰であるかがリアルタイムにわかる。

というメリットを聞かされれば、納得しないわけがありません。すぐに話は決まり、添付ファイルが開かれたら ActiveDirectory の情報を取得し、メールでその情報を送付する。という方式で作業を進めることになりました。これが「標的型攻撃メール対応訓練実施キット」が生まれるきっかけとなったわけですが、話はまだ続きます。

さて、方式は決まったものの、添付ファイルを Word にするかどうか？という点が、その時はまだ決まっていませんでした。ActiveDirectory の情報を取得し、メールでその情報を送付するということは、Word のマクロ（VBA）でもできます。Word ファイルに Web ビーコンを埋め込む代わりに、マクロを記述することにしてもよかったわけです。

しかし、Word のマクロを使う場合、次のデメリットがありました。

マクロの実行が禁止されている環境ではマクロが動かない。
マクロを有効にするかどうかを尋ねる警告が表示されるので、マクロの実行を無効にされる可能性がある。
Word のドキュメントにセキュリティ教育のための情報を記載しても、読まないでファイルが閉じられてしまう可能性がある。

さすがにマクロが動かないのは致命的です。これでは添付ファイルを開いていても、開いたという情報が取得できません。

また、うっかり添付ファイルを開いてしまった人には、セキュリティに注意してもらうよう、その場で学習してもらうようにしたいのですが、学習用のコンテンツを読むことなく Word ファイルを閉じられてしまったのでは意味がありません。

そこで、訓練メールに添付するファイルを、Word ファイルから、VB.NET で作成した実行ファイル（exe ファイル）に変更することにしました。Word の文章を表示する代わりに、標的型攻撃メールに関する注意事項が記載されたダイアログボックスを表示し、それをユーザに読んでもらうという形式です。さらには、ダイアログボックスが閉じられたら、確認を促す意味で、セキュリティ教育用の Web ページを自動的に表示するようにもしました。

exe ファイルであれば、マクロの実行が禁止されているかどうかに関係なく動くので、マクロが動かない問題はクリアです。また、学習用のコンテンツが読まれない問題も、exe ファイルならユーザが勝手にダイアログを閉じることができないようにすることができるので、この問題もクリアです。

実際、exe ファイルを添付した標的型攻撃の手法は存在するので、実際のケースとほぼ同じものをユーザに体験してもらえるのは良いことです。また、exe ファイルを作る方法なら、アイコンを Word や Excel などに似せたアイコンに偽装することもできるので、より実際に近い訓練が実施できます。

ただ、exe ファイルを作成するには、プログラムをコンパイルして exe ファイルを生成することができる開発環境が必要になります。この開発環境を用意するのに、システムを別途用意しなければならないとなると大変です。

日頃から開発業務を行っているような部署であれば何と言うことはないかもしれませんが、そうではない部署となると、年に数えるくらいしか実施しない訓練のためだけに、開発用のシステムを用意するのはハードルが高くなります。

しかし、この点を払拭してくれたのが、Microsoft 社から提供されている無償の開発ツール「Visual Studio Express for Windows Desktop」の存在です。
費用ゼロで使えて、しかも、普通のデスクトップパソコンにインストールできるので、新たにシステムを用意する必要がありません。開発作業なんて行っていない担当者のパソコンでも良いのですから、訓練を年に数回しか実施しないとしても全く問題ないわけです。

こうして、exe ファイルの作成に Visual Studio を活用することにより、「標的型攻撃メール対応訓練実施キット」の原型となる訓練実施のモデルが生まれました。

「Visual Studio」は開発者向けのツールですが、Express 版は無償で提供されているので誰にでも使うことができます。無償版といっても、お試し版のように一部の機能しか使えないといったものではなく、本格的なプログラムを作ることができるほど、申し分のない機能が揃っています。このようなツールが無償で使えるのですから、使わない手はありません。しかし、見方を変えれば、誰にでも悪意のあるマルウェアを作ることができる環境が簡単に手に入るということで、企業側はますます油断できない状況になっていると言えます。

自分でやるのであれば、
作業はシンプルであること
手間がかからないのはとっても大事

これで添付ファイルの基となるプログラムは完成し、次回からは添付ファイルを開いた際に表示される文面だけを変えていけばいいという状態になりました。文面を変えるには、プログラム開発者用のツールである「Visual Studio」を使って行うことになりますが、表示される文面を変えて exe ファイルを生成するだけなら、プログラミングの知識など全くない人にでも行うことができます。

わかれば良いのは以下の 2 つなので、手順書さえ用意しておけば、異動などで新しく担当になった方でも迷うことなく作業ができるでしょう。以下の 2 つであれば、教材となる動画やドキュメントを幾つもインターネット上で見つけることができるので、それらを参照するだけでも基本的な操作は十分理解できると思います。

・添付ファイルを開いた際に表示される文面を Visual Studio 上で変更する方法
・exe ファイルを生成する方法

自分で作業をするのは良いけれど、工程が幾つもあったり、面倒な作業ばかりだったりすると、自分でやるより外注した方がいいかもしれないと考えてしまいますが、シンプルな作業であれば、自分でやってもいいかもしれないと思えるはずです。訓練は定期的に実施を行ったほうが良いものだけに、必要な作業がシンプルであるということはとても重要なことであると思います。

上長や役員への報告は必須、だから、
報告のとりまとめも簡単に
集計もツールで自動化

これで訓練メールに添付するファイルの作成も済み、晴れて訓練を実施してメデタシ、メデタシ。となれば良いのですが、この話にはまだ続きがあります。次に解決すべき課題となったのは、開封者の情報をどのようにして集計するか？という問題です。

誰が添付ファイルを開いたか？というのは、届いたメールを見れば一目瞭然でわかります。Web ビーコン方式の場合も、どの画像ファイルへのアクセスがあったかを調べればわかります。しかし、開封者が一番多かったのはどの部署か？とか、全体として何割くらいのユーザが添付ファイルを開いてしまったのか？といった情報はそれだけではわかりません。

最終的には、訓練実施の結果報告書をまとめないといけないので、開封者の一覧や、開封率の集計などが必要となります。では、これをどうやってまとめるか？添付ファイルを開いた人の情報をメールで受信できるようにしたのはよいとしても、届いたメールの内容を 1 通ずつコピー＆ペーストして Excel に貼り付け、手作業で集計を行っていたのでは大変です。

そこで登場するのが、OutLook と Excel を連動させ、VBA（Visual Basic for Applications）を使って、自動で集計結果を作成する方法です。ここはまさに私が得意とする分野です。

Excel や Word の VBA について知っている方はとても多いのですが、OutLook も VBA でコントロールできることをご存じの方は意外と少なかったりします。OutLook と VBA を組み合わせると、メールの受信と連動して自動で業務処理を行わせたり、メールの送信を自動化するなど、面倒な手作業を自動化・省力化することができます。御社の現場でも活用できるシーンは結構あるかもしれません。

VBA を使うと、OutLook に保存されているメールの本文やタイトル、受信日時などの情報を取り出すことができるだけでなく、メールを自動で送受信するなど、様々な操作を行うことができるので、Excel から OutLook のメールフォルダを参照し、必要なデータだけ Excel に持ってくるということができます。Excel にデータを持ってきてしまえば、後は好きなように集計・加工するだけですから、開封者の情報を集計し、報告書として一気にまとめることができるというわけです。

Web ビーコンを使った方法でも、VBA を使って一気にファイルを作ったり、Web サーバのアクセスログと添付ファイルの送付先リストとの突き合わせを行う作業を自動化し、報告書として一気にまとめたりすることは可能です。これらの作業をツール化してしまえば、作業を実施するのにそれほど手間はかからないと思います。

しかし、Web ビーコン方式の場合は、どの画像ファイルにアクセスがあったか？の記録（アクセスログ）を Web サーバから取り出さないといけないため、集計対象のデータを入手するのにどうしても時間がかかってしまいます。上役の方々は、訓練実施の結果を早く知りたがるものです。訓練を実施したらその日のうちに集計結果をまとめられれば、上役の方にも満足してもらえることでしょう。ちょっとしたことですが、開封者情報をメールで受け取れることにはこうしたメリットもあります。

こうして訓練実施に必要な添付ファイルと、集計用のツールが完成し、晴れて訓練実施となりました。

Web ビーコンを使って訓練を実施していた時に比べれば、遙かに手間が軽減され、添付ファイルを開封した人の情報を収集するための Web サーバを用意する必要もなくなったので、クライアントからは、「これ、売れるんじゃない？」とお褒めの言葉をいただきました。この時はさすがに売れるほどのものじゃあないだろうなとは思いましたが、仕事を請けた者として、お褒めの言葉をいただいたことはとても嬉しいことでした。

「標的型攻撃メール対応訓練実施キット」を
何故？
販売しようと思ったのか？

クライアントから「これ、売れるんじゃない？」とお褒めの言葉をいただいたツール類でしたが、標的型攻撃メールに対応した商品やサービスを提供する会社には、セキュリティ対策の専門家を揃えた大手の名だたる企業が名を連ねているので、さすがに、そんな市場に分け入ったところで、相手にされるはずがないのはあきらかだと思っていました。

ですから、クライアントからお褒めの言葉をいただいたからといって、じゃあ、早速売り出そう！という気にはなりませんでした。では何故、販売を始めるに至ったのか？

それは、標的型攻撃メールの訓練について色々と調べていくうちに、各会社から提供されている商品・サービスと、実際に訓練を実施している現場の間に、ギャップがあると感じたからです。

標的型攻撃メールの模擬訓練で Google 検索を行うと、幾つもの会社が「訓練実施代行サービス」を提供しているのを見つけることができます。中には、ASP サービスとして提供し、自分で訓練を実施することができるようになっているものもあります。

ベンダー側で全て代行して実施してくれる「訓練代行サービス」は、経験のあるプロに作業を任せることで、失敗のない訓練を実施できる点がポイントですが、訓練実施は模擬の攻撃メールを送付し、誰が誤って添付ファイルを開いてしまったか？を集計することが全てではありません。もし、ベンダーに訓練実施を委託される機会があるようでしたら、訓練実施によって何を最大化するか？まで踏み込んで提案できるかどうか、質問をしてみることをお薦めします。

これらのサービスの価格を見ると、1 回の訓練ごとに費用が必要になり、しかも、訓練対象者の数によって、かかる費用が上がっていく構造となっているものがほとんどです。さらには、最低価格も定められているため、依頼しようとすると、結構な費用が必要になります。

しかし、これは考えてみれば当然な話です。訓練実施に必要な作業を、セキュリティの専門家が行うのですから、そういった方々の人件費を考えれば、それなりの費用が積み上がることになります。作業に関わる担当者は一人だけということもないでしょうから、人数分の人件費を考えても、何十万円という金額がかかってしまうというのは、致し方ないと思います。

ですが、訓練実施を依頼する側からすると、致し方ないとはいえ、毎回数十万円～数百万円もの費用が出て行くというのは厄介です。訓練サービスを委託するには決済を通す必要がありますが、この時、必ずと言っていいほど、費用対効果の説明を求められることになります。

初めて訓練を行うのであればともかく、2 回目、3 回目ともなってくると、明確な費用対効果を出すのも難しくなってくるので、説得がしづらくなります。ましてや、訓練を実施したからといって、それで被害がゼロになることが保証されるわけでもないので、訓練なんてやらなくてもいいのではないか？といった意見も出てきます。

訓練を企画・実施する担当者の立場に立つと、訓練はやった方がいいとは思うけれど、訓練を実施するにはマルウェアを模した添付ファイルを用意する必要があるので、専門家に頼らないと実施できない。しかし、専門家にお願いするとなると、費用が結構かかるので、決済を通さないといけないが、部長が納得するだけの説明をするとなるとハードルが高い。

ということで、見積もりは取ってみたけれど、結局依頼を見送ったといったケースは、調べてみると意外と多そうだということがわかりました。私に Word ファイルの生成を依頼してきたクライアントも、自力で訓練を企画・実施している口で、外部に作業を委託するという考えは持っていないようでした。

ベンダーの訓練サービスには
Web ビーコン方式
のものが多かった

よほど会社が儲かっていない限りは、コスト削減を求められるのは当然のことなので、担当者からすれば、劇的な効果が得られるわけでもないのに、わざわざ苦労して部長を説得し、毎回委託費用を捻出するなんて面倒なことをしようとは思わないのが普通でしょう。

自力で作業を行うのは面倒でも、決済を通すなんて面倒なことをしなくて済むのなら、そちらの方がいいと思うのは自然なことです。

そして、様々な会社が提供する訓練サービスについて調べていく中で、もう一つ気がついたことは、添付ファイルを開いたことを特定する方式として、**Web ビーコン方式を使ったものが多かった**ということです。

Web ビーコン方式のデメリットは前述したとおりですが、Web ビーコン方式を採用しているが故に、作業実施にかかる時間が多くなっているのだとしたら、委託費用の中には、その分の作業費用が乗っていることになります。

訓練サービスを委託する費用が高いのは、単純に作業にかかる時間が多いからだとすると、単価の高いエンジニアにわざわざ作業をお願いするのは、何だか無駄なように感じます。

作業を委託することによって、セキュリティの専門家が持っている知見を提供してもらえるのなら価値があると思いますが、専門家の知見を得ることが目的なら、講演を依頼する、また、調査レポートを依頼するといった方法もあるので、作業を委託するためだけの費用として何十万円もかかってしまうのだとしたら、やはりどうか？と思うわけです。

もちろん、自分で訓練を企画し、実施するのが不安だとか、その作業をする余裕がないという状況であれば、全ての作業を専門家にお願いすれば間違いはないので、あえて訓練サービスの代行をお願いするというのは、選択としては有りだと思います。

外部に訓練実施作業を委託するのであれば、かかる費用を何に対して支払うのか？

この点が重要で、例えば、「訓練メールを送信して開封者情報を集計する作業」に 50 万円を払うのか？それとも、「訓練実施によって得られる効果」に 50 万円を払うのか？では、費用対効果の評価ポイントも変わるでしょうし、ベンダーを選定する際の着目点も変わってくることになります。

その点、「標的型攻撃メール対応訓練実施キット」は、「訓練メールを送信して開封者情報を集計する作業」にかかるコストと手間を最小化することを実現するものであるので、非常に明確です。

同じコストをかけるのであれば、「訓練メールを送信して開封者情報を集計する作業」よりも、「訓練実施によって得られる効果」の方にコストをかけたいと考える企業が居て、それに応えられるソリューションを提案できるだけのベンダーが存在しないのであれば、「標的型攻撃メール対応訓練実施キット」を出すことは一つの意味があると思ったのです。

「訓練代行サービス」を選ぶ際の７つのポイント

1. **何に幾らのコストがかかるのか？をベンダーが明確にしているか？**
2. **何を目的に訓練を実施するか？を提案できるベンダーか？**
3. **作業に関わるベンダー側の各担当者の役割が明確になっているか？**
4. **訓練実施についてベンダー側が明確な考えを持っているか？**
5. **訓練実施の目的を共有した上で行動してくれるベンダーか？**
6. **他社サービスの長所を把握した上で、自社の特徴を語れるベンダーか？**
7. **要望に対して迅速に応えてくれるスピード感を持っているか？**

外部のサーバを使うため、訓練実施を
あきらめざるをえない
そんな企業もあるのでは？

そして、これは技術的な話になりますが、Web ビーコン方式の場合は、添付ファイルを開いた方の情報を収集するための Web サーバが必要になります。訓練サービスを利用する場合、この Web サーバはベンダー側が用意しているものを使うケースが多いのですが、この Web サーバはインターネット上に置かれているため、訓練実施に際して、会社のパソコンからインターネット上の Web サーバへのアクセスが発生するということになります。

会社のパソコンの場合、インターネットへのアクセスは各パソコンから直接行うのではなく、Proxy サーバを経由して行うようになっていることが多いと思います。そして、社内のサーバへのアクセスは自由だけれど、インターネットにアクセスするには認証が必要な設定としているというケースも多いかと思います。このような場合は、添付のファイルを開いた瞬間、インターネットにアクセスするための認証ダイアログが表示されるということが発生することになります。

ユーザはインターネットにアクセスするつもりはないのに、インターネットにアクセスするための認証ダイアログが表示されれば、当然違和感を覚えます。なので、認証ダイアログが表示されても、キャンセルボタンを押してしまう人が出てきます。そうなると、Web サーバにリクエストが送られないことになるため、添付ファイルを開封したという情報が取れないことになります。

訓練実施の仕組み自体は良いのですが、社内セキュリティの仕組みの関係で訓練を実施することができないケースもあるということで、訓練の実施をあきらめざるを得なかった方もいらっしゃるのではないかと思ったことも、このキットを販売することにしたもう一つの理由です。

結局、色々と調べていくうちに、名だたる会社が、標的型メール攻撃に対する訓練実施のサービスを提供しているけれど、訓練を実施する側の現場としては、

毎回、訓練実施費用を捻出するための説明・説得を上長にするのはハードルが高い。
技術的な問題であきらめざるを得ないケースもある。

といったギャップがあると感じたのです。そして、私がクライアントに提供した方法は、偶然ではありましたが、まさにそのギャップを乗り越えられるものでした。

訓練サービスを提供する業者として参入するのは難しいだろうけれど、自力で訓練を企画し、実施をしている担当者の方、また、訓練を実施したいとは思っているけれど、様々な理由で実施をあきらめている担当者の方に、私がクライアントに提案したモデルを提供することは、もしかして意味があるのではないだろうか？

訓練実施サービスについて調べていくうちに、そう考えるようになりました。

私がクライアントに提案したモデルを実現するためのプログラムは既にあり、作業を効率化するためのツールも既にある。そして、私が提供するのは、セキュリティ対策そのものではなくて、自力での訓練実施を効率的に実現するための方法であるから、セキュリティの専門家と同じ土俵で張り合うものではなく、作業の実施においてはむしろ、VBA のエキスパートであるという私の専門性が逆に活かされるものであるということにも気がつきました。

実際に訓練を実施しているクライアントが、「これ、売れるんじゃない？」と言って実際に喜んでくれているものなら、他社でも同様の事をされている方がいれば、その方にもこのモデルを提供することで喜んでもらえるかもしれない。

そして、はなから、高額な費用は出せないと、訓練実施をあきらめていた中小企業でも、訓練を実施していただくことができるかもしれない。例えちっぽけな存在でも、多くの人に役立ち、喜んでいただけるのであれば、商品として提供することの意義はあるはず。

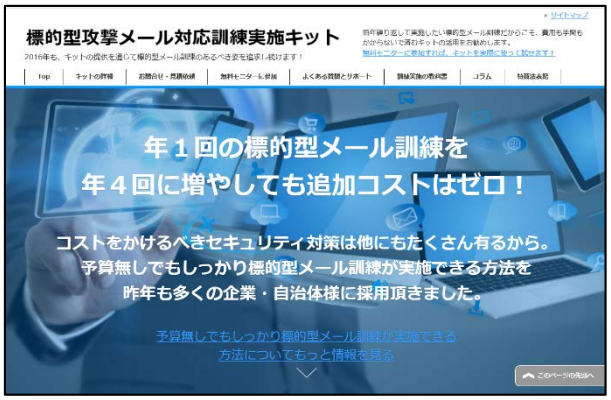
そう思い至った結果、買い切り型の「標的型攻撃メール対応訓練実施キット」という形で、私の考えた訓練実施のモデルと、そのモデルを実現するのに必要なツール類を提供することにしたのです。

こうして、「標的型攻撃メール対応訓練実施キット」が商品として誕生した。というわけです。

「標的型攻撃メール対応訓練実施キット」の紹介ページ

http://kit.happyexcelproject.com/

↑2014 年当時のホームページ



↑2016 年現在のホームページ

キットというモデルを提供することで、
訓練をやったほうがいい
と思えるものにしよう

こうして、「標的型攻撃メール対応訓練実施キット」という商品を販売することにしたのですが、実際に訓練を実施しようとすると、色々と面倒な課題が生じます。

訓練で送付するメールの文面をどうするか？
標的型メール攻撃について、ユーザにどうやって教育するか？
訓練実施による効果をどうやって調べたらいいか？
訓練実施の作業計画をどのように立てたらいいか？
訓練実施にどれくらいの期間と手間を見積もったらいいか？
などなど・・・

標的型攻撃に関する情報はインターネットを調べれば、結構な数の情報が得られます。しかし、実際に訓練を実施するとなると、その具体的な方法については、あまり情報は得られません。
セキュリティ教育を実施しているということを公には謳っていても、訓練の実施に関する実務レベルの情報を公にしている会社はないので、具体的にどうやって訓練を実施するのか？といった情報となると、グッと少なくなるというのが現実です。

そこで、訓練実施のモデルを商品として提供するのなら、実際の訓練実施を通じて自分が得た知見などもまとめて提供すれば、訓練実施の経験がない担当者の方でも、スムーズに訓練を実施していただくことができるはず。はなから訓練実施をあきらめているような中小企業などであれば、訓練なんてやったことがないのですから、実際に訓練をやった人の経験を知ることができるというのは、とても助かるのではないか？

そう思った私は、訓練を企画・実施する担当者向けには「訓練実施の手引書」、そして、訓練を受けるユーザ向けには、標的型攻撃メールに関する知識とリスクを伝える「教育用コンテンツ」という形で冊子をまとめ、キットを構成するパーツの一つとして付けることにしました。

訓練メールに添付するメール本文のサンプルをテンプレートという形で用意したのも、この考えからで、ゼロからアイデアを考えなくてもよいというのは、訓練を企画し、実施しなければならない担当者からすると、大変助かるものだと思います。

ちなみに、御社には標的型攻撃メールが送られてくることはあるでしょうか？

標的型攻撃メールが送られて来たのを見たことがない。という方もいらっしゃれば、結構送られてくるんだよね。という方もいらっしゃる。というのが、現状だと思います。

実際に送られてきた経験をお持ちの方であれば、訓練実施の必要性を実感されているのではないかと思いますが、そうでは無い方の場合は、訓練実施の必要性をあまり感じないということはあるかと思います。

訓練を実施しても、セキュリティの重要性に関心を示さず、イザ、標的型攻撃メールが送られてきたらあっさりひっかかってしまうという方や、セキュリティの重要性についてはわかっていても、うっかりひっかかってしまうという方は、少なからず存在します。

訓練を実施しても、ひっかかる人をゼロにできないのなら何の意味もない。という考えは、それはそれで納得できるものです。訓練実施に毎回何十万円～何百万円もの費用がかかるのであれば尚更だと思います。

実際に被害が発生していない、また、攻撃メールなんて目にしたこともない組織からすれば、あるかどうかもわからないことに毎年費用を投資するのはムダ以外の何物でもないと考えたとしても、致し方ない事だと思います。

しかし、毎回費用が発生するということがなくなり、費用ゼロで訓練が実施できるのなら、訓練をやらないより、やった方がいいんじゃないか？という考えに立つことができるのではないでしょうか？

確かに、訓練を実施しても被害をゼロにすることができるわけではありませんが、セキュリティ教育をしっかりやっておくことで、被害が発生する確率を少しでも下げることができるなら、やらないよりはやったほうがいいはずです。最初の１回目こそは費用が必要でも、２回目以降は費用がかからずにできるのだったら、やらないよりやったほうがいいよね。と思えるはずです。

ましてや、訓練の実施を戦略的に捉え、セキュリティ対策の一環としてのみ考えるのではなく、組織全体としての連絡体制の整備や、企業ブランドの構築・維持のための道具としても活用することを考えれば、費用や手間がかからないで済むということは、より積極的に訓練実施を活用していくための原動力となり得るはずです。

訓練サービスの利用だと、毎回費用の捻出が必要となってしまいますが、買い切り型ならそれは不要です。買い切り型ではリピート需要が発生しないので、商売のモデルとしては上手なやり方ではありませんが、訓練を実施する事に躊躇している方にはきっと喜んでもらえるはずです。

だから、あえて、買い切り型の商品として世に送り出すことにしたのです。

買い切り型で商品を提供することには、「ビジネスとしてはニッチすぎる」といったご指摘もいただいています。このご指摘は確かにその通りかもしれません。
しかし、このような商品を提供することで喜んでいただける方がいるのなら、それはそれで意義があることであり、私のようなちっぽけな存在が考えたモデルが、誰かが喜んでいただけることに繋がり、ご利用いただいた企業様の繁栄に繋がるのなら、この商品を買い切り型として世に送り出すことにした意味があるのだろうと思います。

終わりに
あなたの心に響いた話はありましたでしょうか？

お忙しい中、最後までこのレポートをお読みいただきましてありがとうございます。
もし、このレポートを読まれて、「標的型攻撃メール対応訓練実施キット」が生まれた背景に共感いただけた、また、あなたの心に響いた話がありましたら、大変嬉しく思います。

もし、あなたの周りにこうした訓練の実施にかかるコストや手間をどうにかしたい、また、コストや手間に頭を悩ませること無しに訓練を実施したい、と思われている方がおられましたら、是非、このレポートを共有してください。

幸い、「標的型攻撃メール対応訓練実施キット」は、この商品が生まれた背景に共感いただいた企業様から、ご購入のお申し込みをいただけているので、やはり勇気を出して販売を開始してよかったなと思っています。

大手の会社がひしめく市場だからということで、相手にされないだろうとハナからあきらめていたら、喜んでいただけるお客様に出会うこともなかったと思います。キットの方は、実際に使っていただいているお客様からの要望を採り入れ、日々改良を続けているので、今後も様々なお客様の事例を通じて、良いと思えることは積極的に採り入れ、お客様により喜んでいただけるものにしていきたいと考えています。

標的型メール攻撃はどの企業においてもあり得ることであるだけに、どの企業においても備えは必要だと思います。実際に被害に遭う確率を減らすため、そして、お客様にセキュリティ対策がしっかりしている会社であることを示すため、そして、いざという時に、訓練を実施していなかったということで社会からバッシングを受けることがないようにするため。

目的は様々あれど、やらないよりやったほうがいいと思えるなら、それはやったほうがいいことだと思います。

以前、新聞紙上を賑わしたバイドゥの仮名漢字変換ソフト「Simeji」は、それ自体は悪意のあるソフトではなかったのですが、仕組み的に、重要な情報も外部に流出してしまうようになっていたために、大きな問題になりました。マルウェアが「Simeji」のように、それ自体は悪意のあるソフトではないかのような振る舞いをしていた場合、ウィルス対策ソフトでは悪意のあるソフトとして検知することができないので、気がつかないうちに重要な情報が盗まれてしまっていたという事態も発生し得ます。

また、コンビニのショーケースに店員が寝そべった写真がネットに投稿されたことで、店が廃業に追い込まれたという話は、まだ、記憶に新しいかと思います。写真がネットに投稿されたこと自体は些細なことです。しかし、それによって店舗を閉めざるを得ないような事態にまで発展してしまったことは、標的型攻撃による被害においても、当てはまりうることだと思います。

従業員がそれと気づかずにうっかり開いてしまった 1 通のメールから情報漏洩が始まり、ネット上にその情報が流れてしまうことで大きな問題に発展し、結果として、謝罪会見を開かなければならないような事態となってしまったり、事業所を閉鎖せざる追えない状況に追い込まれてしまったりする。果たして、このような話はフィクションの中だけの話でしょうか？

「訓練サービスを利用される」「ご自身で独自に訓練を実施される」「キットを利用して訓練を実施する」、選択肢は色々ありますが、すぐにでも実践できることがあるようでしたら、是非実践していただければと思います。そしてもし、キットを利用することで「できそうだ」と思える事があるようでしたら、是非、キットを使っていただければと思います。

「標的型攻撃メール対応訓練実施キット」やこのレポートについてご意見やご感想があれば、お気軽にメールをお送り下さい。生の声をいただけるのは励みにもなり、また、嬉しくもあるので、ご連絡は下記までお願い致します！

件名：「標的型攻撃メール対応訓練実施キット」レポートについて
宛先：master@happyexcelproject.com

また、この PDF に書き切れなかったことや、様々な事例などを見聞きする中で思ったこと、そして、セキュリティ対策に関わる方々にシェアしたいことなどを Web サイト上で書き綴っています。ご興味をお持ちいただけましたら、引き続き、サイトの方にもお越しください。

標的型攻撃メール対応訓練実施キットの Web サイト URL

http://kit.happyexcelproject.com/

そして、これは宣伝になってしまいますが、本レポートに登場しました「標的型攻撃メール対応訓練実施キット」にご興味をお持ちいただけるようでしたら、Web サイトにあります詳細資料なども併せてお読みいただけましたら嬉しく思います。

以上をもちまして、このレポートの結びとなりますが、最後に、貴重な時間を割いて、このレポートをお読みいただけましたことに、今一度、深く感謝を申し上げます。

それでは、今後ともよろしくお願い致します。

縁マーケティング研究所　代表　野々市（ののいち）恭徳（やすのり）

標的型攻撃メール対応訓練の実施に関して話を聞いてみたい。
といったご要望がありましたら・・・

縁マーケティング研究所では、「標的型攻撃メール対応訓練実施キット」の開発元としての知見を活かし、訓練実施に関するご相談にお応えすることも可能です。もし、訓練の企画や実施についてお困りのようでしたら、お気軽にご相談下さい。

訓練に関する相談のお申し込み