

標的型攻撃メール 対応訓練実施キット

やってみよう！標的型メール訓練

自分の手で訓練メールを作成し、実際に標的型メール訓練が
自社内製でも十分にできることを実感して下さい！

標的型攻撃メール対応訓練実施キットを使えば、自分の手で模擬の標的型攻撃メールを作成し、標的型攻撃メールの見分け方などについて、実際の体験を通じて従業員に学習してもらうことができる「標的型メール訓練」をすぐにでも実施することができます。

このマニュアルでは、キットを用いて、標的型メール訓練を実施する例をご紹介します。



キット活用による標的型メール訓練実践マニュアル
自社サーバでの訓練実施編 ver.2024.06.10.01



この度は標的型攻撃メール対応訓練実施キットをご検討頂き、誠にありがとうございます

この度は、標的型攻撃メール対応訓練実施キットをご検討いただきまして、誠にありがとうございます。インターネットを通じ、このようなご縁を頂くことができましたことを大変嬉しく思います。これを機に、今後とも長いお付き合いができましたら、非常に嬉しい思います。

本マニュアルについて

本マニュアルでは、お客様側で Web サーバ及び SMTP サーバを用意し、キットを活用して標的型メール訓練を実施する方法についてご案内します。キットが提供する「訓練メール送信サービス」及び「URL 転送」の機能を利用し、お客様側でサーバを用意すること無しに訓練を実施される場合は、「訓練メール送信サービスご利用マニュアル」及び「標的型攻撃メール対応訓練実施キットスタートアップガイド」をご参照ください。

標的型メール訓練を実施する上で必要となるもの

標的型メール訓練の実施について、ひと通りの流れを確認するだけであれば、今お使いの Windows パソコン 1 台があれば十分です。別途、新たな機材をご用意頂く必要はありませんが、キットに付属のツールを動作させるために Microsoft Excel が、また、キットに付属の従業員教育用ドキュメントを編集するには Microsoft Word が必要となります。

また、標的型攻撃メール対応訓練実施キットでは標準で、訓練メールを送信する「訓練メール送信サービス」及び、標的型メール訓練を実施する上で必要となる「Web サーバ」の機能を提供する「URL 転送サービス」機能の提供も行っております。

キットに付属のツールとプログラム、また、「訓練メール送信サービス」「URL 転送サービス」をご利用いただく事で、訓練実施用の Web サーバ及び、SMTP サーバを自社で用意し、完全に自社内に閉じた形で訓練を実施したいと考えるお客様はもちろんのこと、諸々の事情から、自社でサーバを用意することは難しいというお客様でも、業者に頼ることなく、標的型メール訓練を実施頂けるようになっております。

では、次のページより、標的型メール訓練実施方法についての説明を進めます。

本書には「Web サーバ」「IP アドレス」「localhost」「ホスト名」といった用語が登場しますが、これらの用語の意味についてよくわからないという方は、まずは本書の記載の手順通りに進めて頂ければと存じます。

また、急がば回れ。ではないですが、スムーズに設定を進めて頂くには、ご面倒でも、本書の記載に沿って進めて頂くことをお奨めします。

「正しく動作しない」「思っていたのと違う結果になる」といった場合、本書の記載通りに順を追って進めて頂いていれば、問題の発生個所が明確になり、どこに原因があるのか？が特定しやすくなるためです。

なお、本書に記載されている内容 자체がわからないので自分だけでは進められそうにない、また、自分で設定するのは面倒という方には、有償にはなりますが、[導入支援サービス](#)もご用意しておりますので、プロにサポートしてもらいながら迅速に準備を進めたいとお考えの場合は、ぜひご検討下さい。

※ 「標的型攻撃メール対応訓練実施キット」導入 & 運用支援サービス <https://kit.happyexcelproject.com/installsvc/>

キット活用による標的型メール訓練実践マニュアル 目次

内容

URL リンククリック型の訓練を実施しよう	4
STEP1 Web サーバ側の設定を行う	5
STEP1-1 Web サーバ（IIS）をパソコンにインストールする	6
STEP1-2 Web サーバ（IIS）を設定する	7
STEP1-3 aptkit.aspx を設定する	8
STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する①	9
STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する②	10
STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する③	11
STEP1-5 aptkit.aspx にリダイレクト先を設定する	12
STEP1-5（補足）GrpName の設定について	13
STEP1-6 開封者情報のメールを指定の宛先に送信するよう設定する	14
STEP1-7 他のパソコンから Web サーバへのアクセスについて	15
STEP1-補足 Windows 以外の OS で Web サーバを構成する	16
STEP2 リンク先のページを用意する	17
STEP3 訓練メールを送信する（訓練メールを送信する 2 つの方法）	18
STEP3-1 自社で用意した SMTP サーバを利用して訓練メールを送信する	19
STEP3-1 自社で用意した SMTP サーバを利用して訓練メールを送信する（続き）	20
STEP3-1（補足）BlackJumboDog のインストール	21
STEP3-1（補足）BlackJumboDog の SMTP 機能のセッティング①	22
STEP3-1（補足）BlackJumboDog の SMTP 機能のセッティング②	23
STEP3-1（補足）BlackJumboDog の SMTP 機能のセッティング③	24
STEP3-2 送信先リストデータの設定	25
STEP3-3 送信先リストデータの訓練メール作成支援ツールへの取り込み	26
STEP3-4 訓練メール送信サービスを利用して訓練メールを送る	27
STEP4 訓練メール本文中の URL リンクがクリックされる	28
STEP5 開封者情報の取得	29
STEP6-1① 開封者情報集計ツールによる開封者情報の集計	30
STEP6-1② 開封者情報集計ツールによる開封者情報データの取り込み	31
STEP6-1③ 開封者情報集計ツールにマスタデータを取り込む	32
STEP6-1④ 開封者情報集計ツールによる開封者情報の集計	33
STEP6-1⑤ アクセス元 IP アドレスについて	34
STEP6-2 開封者情報集計の仕組み	35
STEP6-3 ユーザマスタ情報の作成	36
STEP6-4 開封者情報集計ツールで出力した集計結果データの整形	37

訓練メールに記載される実際の URL リンク先を隠ぺいする方法	38
添付ファイルを用いての訓練実施	39
添付ファイルの作成（キットに付属のツールで添付ファイルを作成する）	40
Office 文書ファイルを開く際の警告表示について	41
Office 文書ファイルにおけるマクロの実行について	42
添付ファイルを用いる場合の開封者情報集計	43
オフライン環境もしくはツールが対応していない環境下でのツール起動方法	44
フィッシング詐欺対応訓練の実施①	45
フィッシング詐欺対応訓練の実施②	46
フィッシング詐欺対応訓練の実施③	47
フィッシング詐欺対応訓練用コンテンツのカスタマイズ	48
フィッシング詐欺対応訓練用コンテンツの種類	49
その他の注意事項について	50
キットご利用のフォローアップについて	51

【訓練実施の進め方について】

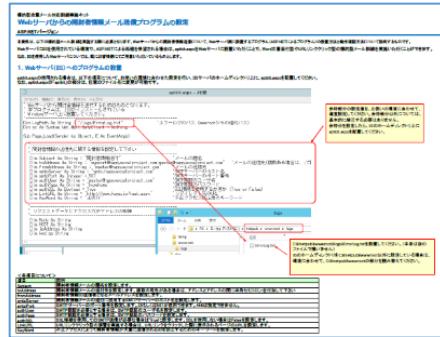
キットを用いると、以下の 4 タイプの訓練が実施できますが、本実践マニュアルでは、最も手軽に始めて頂きやすい「URL リンククリック型」の訓練実施から説明を進めています。他のタイプの訓練は、URL リンククリック型の訓練実施方法についてご理解頂くことで、容易に進めて頂くことができるかと思いますので、まずは、「URL リンククリック型」の訓練を試してみることから始めてみて頂ければと存じます。

1. URL リンククリック型の標的型メール訓練
2. 添付ファイル型の標的型メール訓練
3. フィッシング詐欺対応訓練
4. ファイルダウンロード型の訓練

また、本書では、お客様側でご用意いただいた Web サーバ及びメールサーバ（SMTP サーバ）を利用するパターンについてご案内をしておりますが、お客様側で Web サーバを用意する代わりに、キットが提供する「URL 転送」サービスを利用する、また、お客様側でメールサーバ（SMTP サーバ）を用意する代わりに、キットが提供する「訓練メール送信サービス」を利用して訓練を実施頂くことも可能です。「URL 転送」サービス並びに、「訓練メール送信サービス」については、別冊のマニュアル「訓練メール送信サービスご利用マニュアル」をご参照ください。

URL リンククリック型の訓練を実施しよう

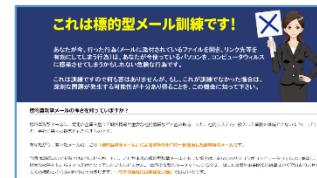
手始めにキットを使用して URL リンククリック型の訓練を実施してみましょう。URL リンククリック型の訓練実施の流れは、おおよそ以下のようになります。本書では訓練実施の仕組みをご理解頂くため、ここでは、Web サーバはお手持ちの Windows パソコンを使って行うやり方についてご案内します。



STEP1 Web サーバ側の設定を行う

URL リンククリック型では、URL リンクのクリック先となる Web サイトが必要となります。

このため、URL リンククリック型の訓練では、お客様側にて Web サーバをご用意いただき、キットに付属の Web サーバ側用プログラムを Web サーバに設置頂くことになります。



STEP4 URL がクリックされる

訓練メールに記載されている URL リンクがクリックされると、Web サーバへのアクセスが発生し、Web サーバから開封者情報が出力されます。

この時、ユーザーには STEP2 で設定したリンク先のページがリダイレクト先として返され、Web ブラウザに表示されます。



STEP2 リンク先のページを用意する

URL リンクがクリックされた際に表示される Web ページを用意します。キットには Web ページの雛形がありますので、これを適宜編集して Web サーバに設置して頂くか、既存の Web ページを流用して頂くなど、訓練の内容に合わせて Web ページを設定頂きます。

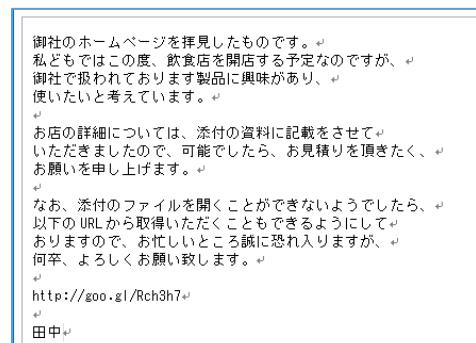


STEP3 訓練メールを送信する

URL リンクを埋め込んだ訓練メール本文を作成します。

キットにはメール本文に個別の URL リンクを埋め込んで訓練メールを作成・送信することができる「訓練メール作成支援ツール」が付属しており、このツールを使うことで、テキスト形式のメールや HTML 形式の訓練メールを作成することができます。

作成した訓練メールは、キットが提供する「訓練メール送信サービス」を利用して送信する、もしくは、貴社でご用意頂いた SMTP サーバを利用して送信することができます。



STEP5 開封者情報の取得

訓練実施担当者側では、Web サーバから出力される開封者情報データを取得します。

開封者情報データは Web サーバ上に出力する方法と、メールデータとして受信する方法の 2つがあります。



STEP6 開封者情報の集計

キットに付属の開封者情報集計ツールを用いて、STEP5 で取得した開封者情報メールの集計処理を行います。

集計作業はツールが行ってくれるので、誰が模擬マルウェアプログラムを実行したかは、リアルタイムに集計することができます。

STEP1 Web サーバ側の設定を行う

URL リンククリック型の訓練実施では、訓練メール本文中の URL リンクがクリックされたことを以って、標的型メールに騙されてしまったとみなします。

URL リンクがクリックされたことを検知するには、URL リンクのクリック先となる Web ページ側に仕掛けを施しておき、この仕掛けが呼び出されることによって、誰が標的型メールに騙されてしまったのか？をキャッチすることになります。

このため、URL リンククリック型の訓練実施では、仕掛けを設置するための Web サーバが必要となり、**お客様側にて Web サーバをご用意頂くか、キットが提供する「URL 転送」サービスをご利用頂くか**のどちらかのご選択となります。

【ご用意頂く Web サーバについて】

Web サーバというと、高価なサーバ設備を用意しないといけないのではないか？と思われるかもしれません、標的型メール訓練を実施するのに、専用のハードウェアをご用意頂く必要はありません。Windows10 や Windows11 など、今お使いの普通のパソコンが 1 台あれば、十分に訓練を実施することができます。もう何年も前の話にはなりますが、2 万人の従業員を対象とした訓練でも、使用したのは中古の Windows7 パソコン 1 台のみという実績があります。

もちろん、既に Web サーバをお持ちで、それらを使うことができるのであれば、そちらをご利用いただいても構いません。

Windows パソコンをお使いになる場合は、IIS という Web サーバソフトが標準で使えるようになっていますので、IIS と、キットに付属のプログラムを組み合わせてお使い頂くのが、最も簡便です。

なお、レンタルサーバやクラウドサービスなどをを利用して Web サーバを用意される場合は、Windows Server OS が使える VPS サーバレンタルサービスなどをご利用頂くか、さくらインターネットのレンタルサーバサービスなど、PHP がお使い頂ける Web サーバのどちらかをご用意下さい。

ちなみに、ASP.NET もしくは、PHP のどちらも使うことができない Web サーバは、キットではご利用いただけませんのでご注意ください。

標的型メール訓練では何故、パソコンが 1 台あれば十分なのか？

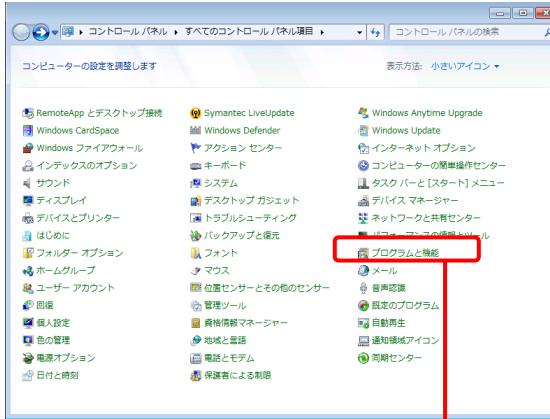
Windows OS に詳しい方であれば、Windows10 などのクライアント OS では、同時接続数に制限があるのだから、Web サーバとして使うのは適切でない。と思われるかもしれません。確かに、サーバ OS ではない Windows10 や Windows11 では、ネットワークの同時接続数に制限が設けられていますが、標的型メール訓練を実施した際に、実際に URL リンクがクリックされるのは訓練実施対象者の 10% 前後くらいなので、例えば、1,000 名が対象の訓練では、Web サーバにアクセスしてくるのは 100 名前後ということになります。

しかし、この数はある瞬間での同時アクセス数ではなく、訓練実施日当日中を通じてのアクセス数になりますので、瞬間での同時アクセス数ということになると、かなり少ない数になります。また、Windows10 や Windows11 に付属の IIS では、処理しきれなかったアクセスについてはキューに溜めて順次処理を行うような仕組みになっていますので、1 日 100 名程度のアクセスでは、同時接続数の制限がネックとなってしまうようなことはまずありません。このため、標的型メール訓練という用途に限って言えば、中古のパソコンなどでも十分使えるということになります。

STEP1-1 Web サーバ (IIS) をパソコンにインストールする

ここでは、お手持ちのパソコン（Windows10 以降の Windows パソコン）に IIS をインストールする手順について説明します。と言っても、難しくはありません。マウスで操作していくだけですので、作業はすぐに終わります。

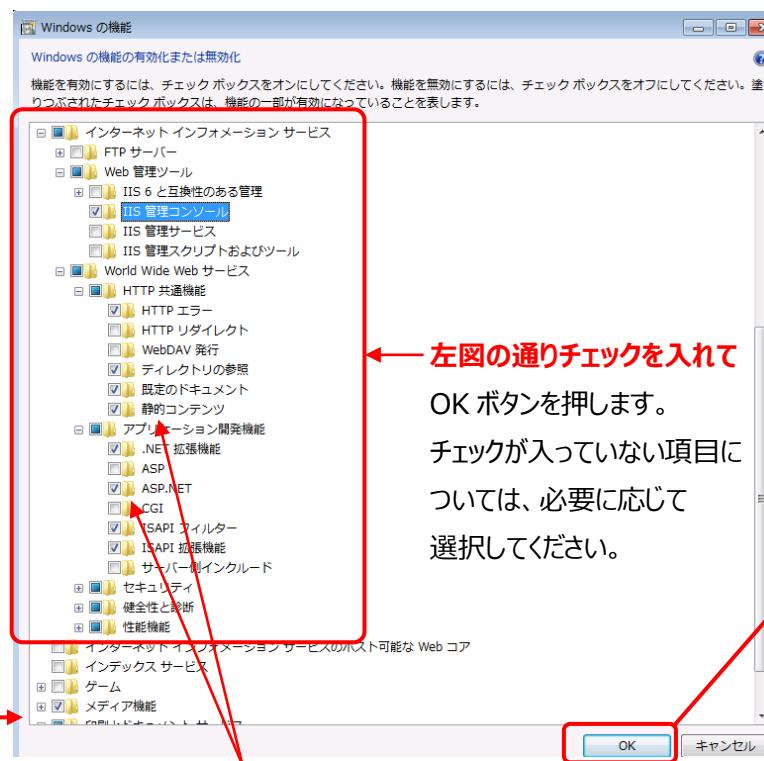
- ①コントロールパネルから「プログラムと機能」を選択します。



- ②「Windows の機能の有効化または無効化」を選択します。



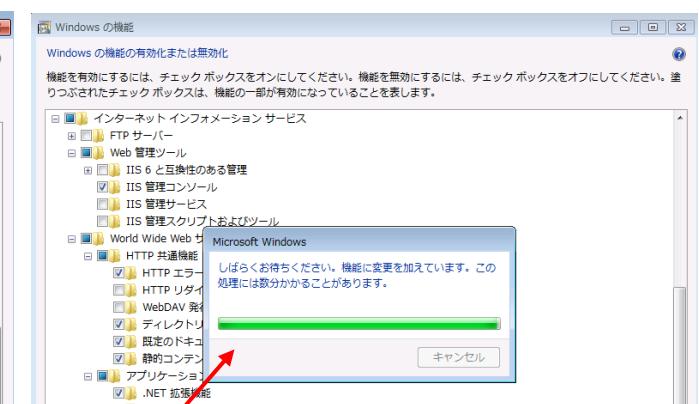
- ③インターネットインフォメーションサービスに関する項目を選択して OK ボタンを押します。



※特に、ASP.NET 及び、静的コンテンツについては、チェックを入れ忘れないようにして下さい！

- ④OK ボタンを押すと IIS がインストールされます。

※マシンの性能によってインストールにかかる時間は異なります。



IIS は Windows に標準で付属している
Web サーバソフトです。
新たに購入する必要はありませんから、
今すぐお使い頂くことができます。



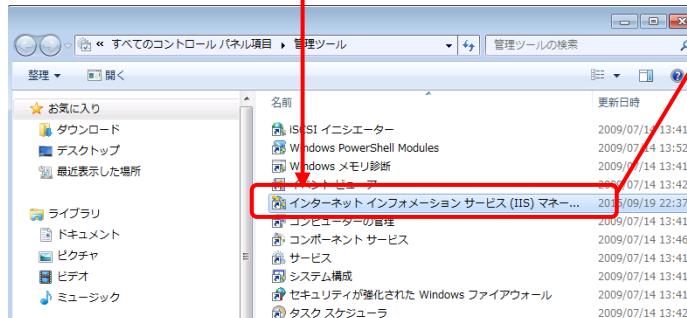
STEP1-2 Web サーバ (IIS) を設定する

IIS のインストールが完了したら、以下の手順に従って IIS の設定を行います。

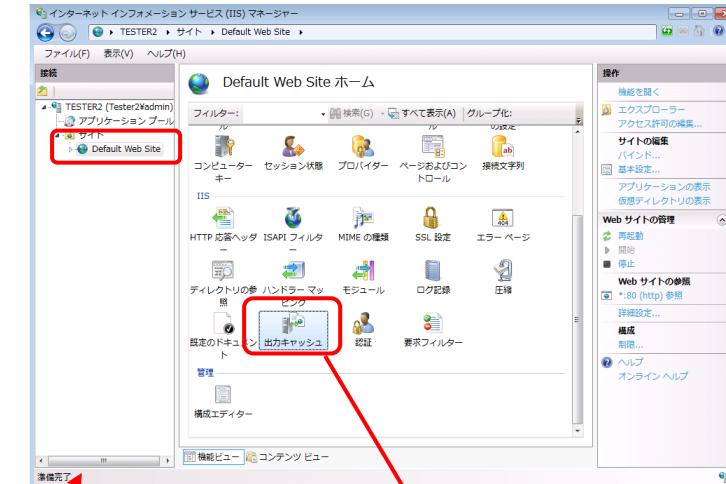
- ⑤IIS のインストールが完了したら、コントロールパネルから「管理ツール」を選択します。



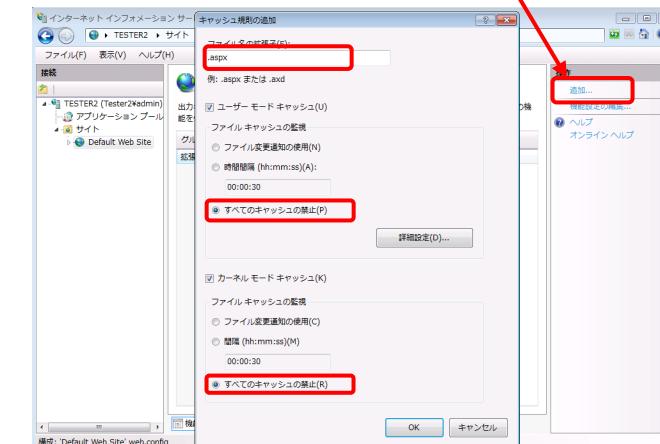
- ⑥管理ツールの一覧の中から「IIS マネージャー」を選択します。



- ⑦「IIS マネージャー」の管理コンソール画面が表示されますので、「Default Web Site」を選択し、さらに「出力キャッシュ」を選択します。



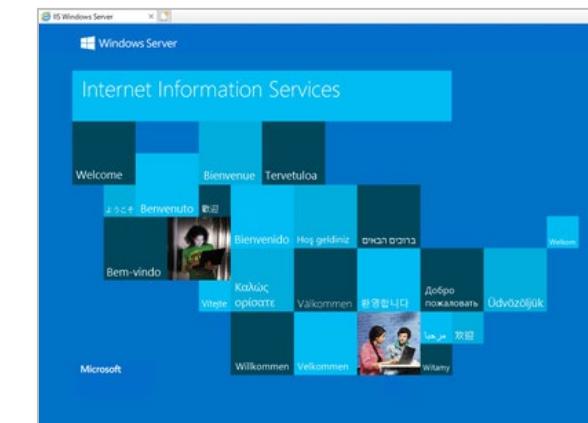
- ⑧「出力キャッシュ」の設定画面で「追加」をクリックすると、「キャッシュ規則の追加」ダイアログが表示されますので、ファイル名の拡張子に「.aspx」とに入力し、ユーザーモードキャッシュ、カーネルモードキャッシュのどちらも、「すべてのキャッシュの禁止」を選択して OK ボタンを押します。



- ⑨出力キャッシュが以下のように追加されます。



- ⑩出力キャッシュの設定まで終れば、IIS の設定は完了です。IIS が正しく設定されているかを確認するため、Web ブラウザを起動し、<http://localhost/> にアクセスしてみてください。以下の画面が表示されるはずです。



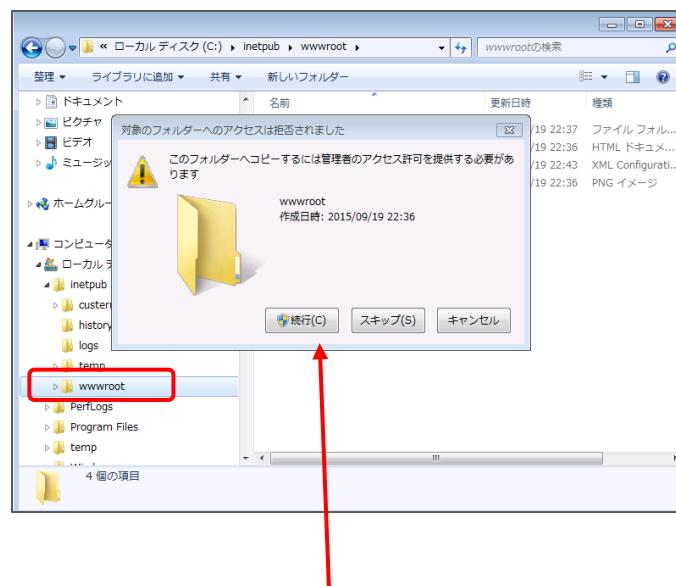
以上で IIS の設定は完了です。
続いて、開封者情報を取得するための仕組みとなる
プログラムを Web サーバに設置するため、
キットに付属の aptkit.aspx の設定を行います。

STEP1-3 aptkit.aspx を設定する

IIS の設定が完了したら、キットに付属の Web サーバ側に設置するプログラム「apkit.aspx」を Web サーバに設置し、動作するよう設定を行います。

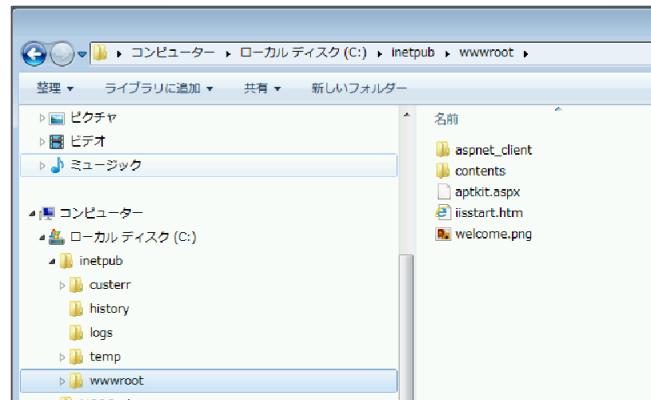
- ① キットに付属の「Web サーバ用プログラム」のフォルダ配下にある apkit.aspx を、IIS のルートフォルダである C:\inetpub\wwwroot 配下にコピーします。

また、C:\inetpub\wwwroot\contents フォルダを作成し、Web サーバ用プログラム¥HTML ファイル¥自社サーバ用¥種明かしページ 1 フォルダ配下にある html ファイルと画像データを、contents フォルダ配下にコピーします。

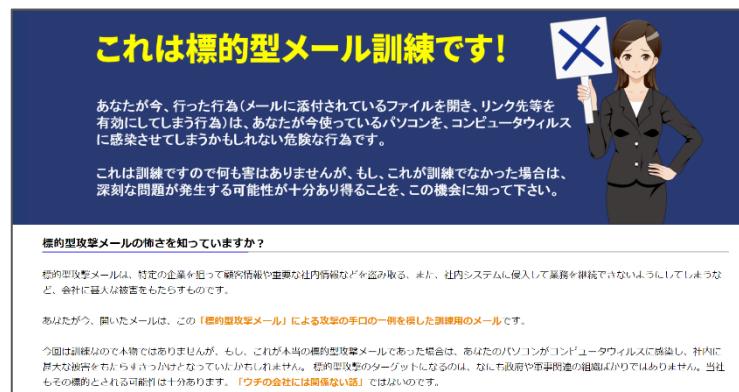


ファイルのコピーを行う際、上記の警告が表示されますが、続行ボタンを押すと、コピーが継続されます。

- ② ファイルのコピーが完了すると、以下のようにになっているはずです。



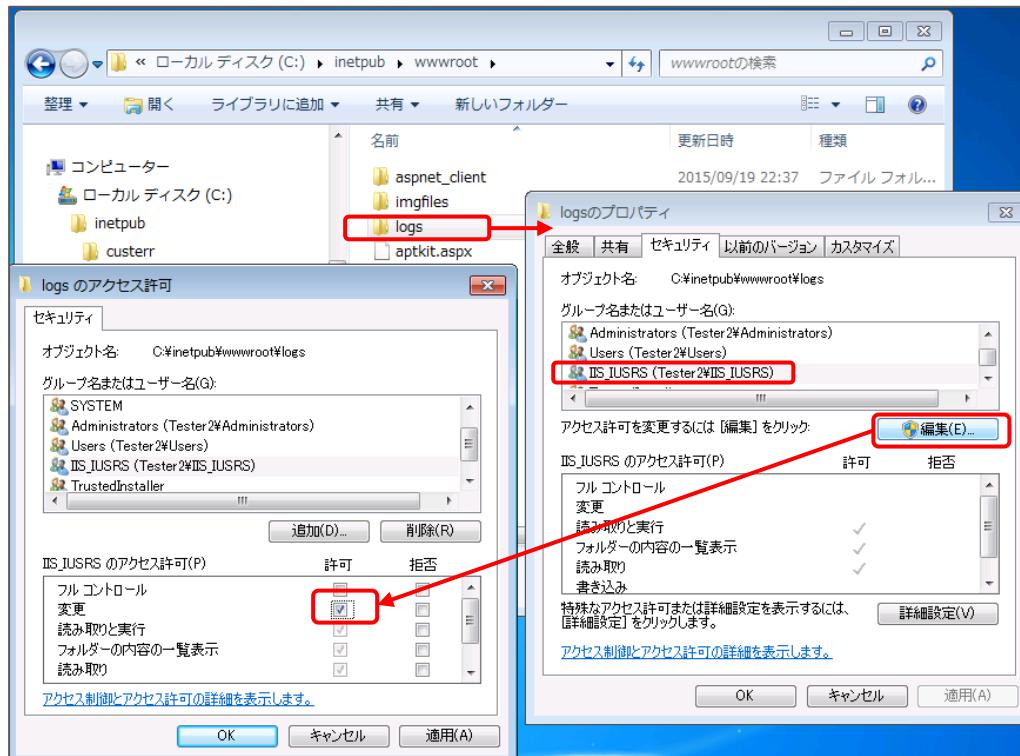
- ③ ②まで完了したら、IIS をインストールしたパソコン上で Web ブラウザを起動し、<http://localhost/contents/top.html> にアクセスします。設定に問題がなければ、以下のようないい画面が表示されるはずです。



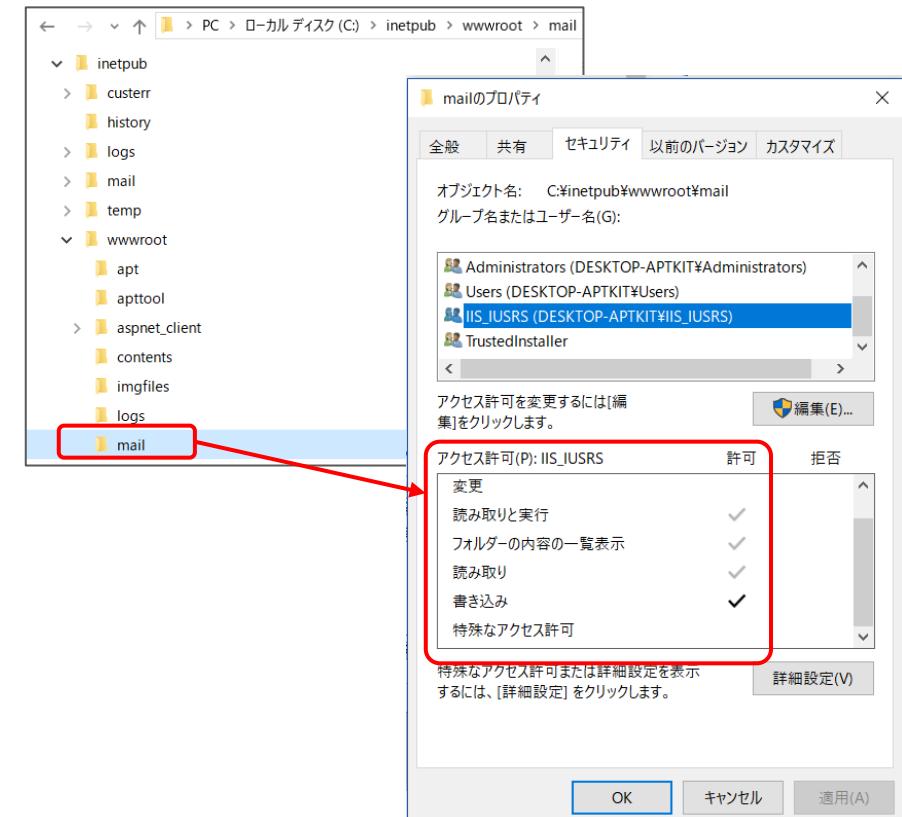
STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する①

aptkit.aspx の動作確認を完了したら、エラーログ記録用のフォルダと、Web サーバに eml 形式のメールデータを保存するためのフォルダ設定を行います。

- ④STEP1-3 の作業を完了したら、c:\inetpub\wwwroot フォルダ配下に「logs」ディレクトリを作成し、フォルダのプロパティ設定ダイアログ画面を表示させて、IIS_IUSRS に変更権限を付与します。

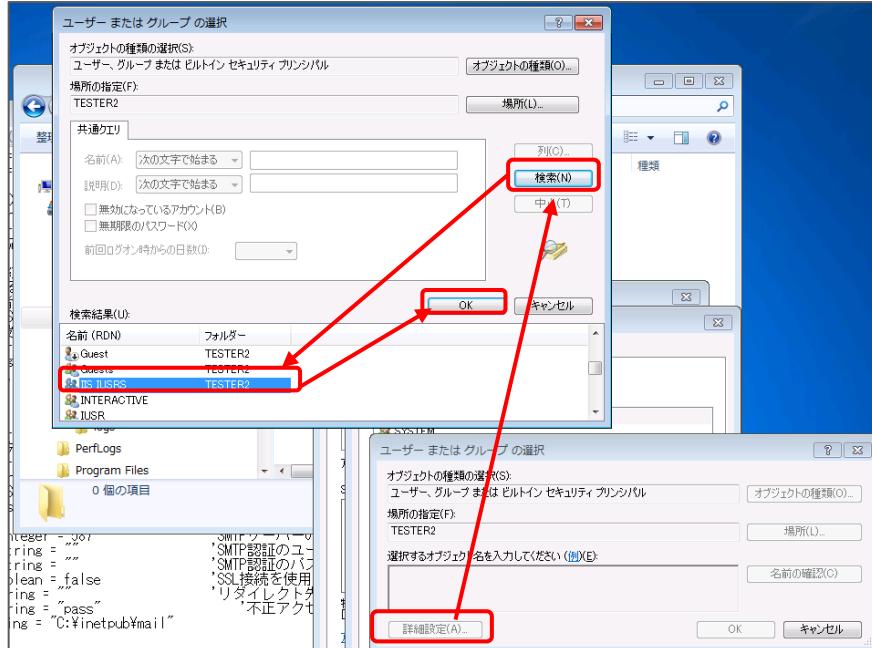


- ⑤④と同様にして、c:\inetpub\wwwroot フォルダ配下に「mail」ディレクトリを作成し、フォルダのプロパティ設定ダイアログ画面を表示させて、IIS_IUSRS に書き込み権限を付与します。

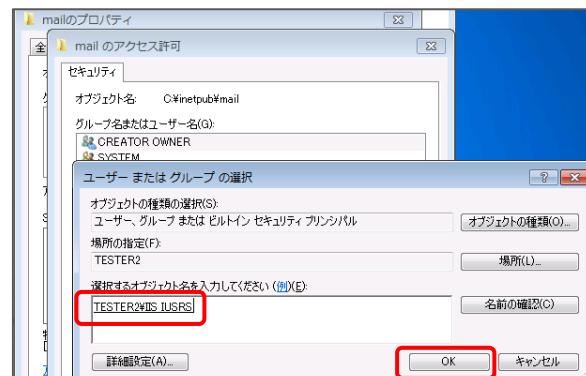


STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する②

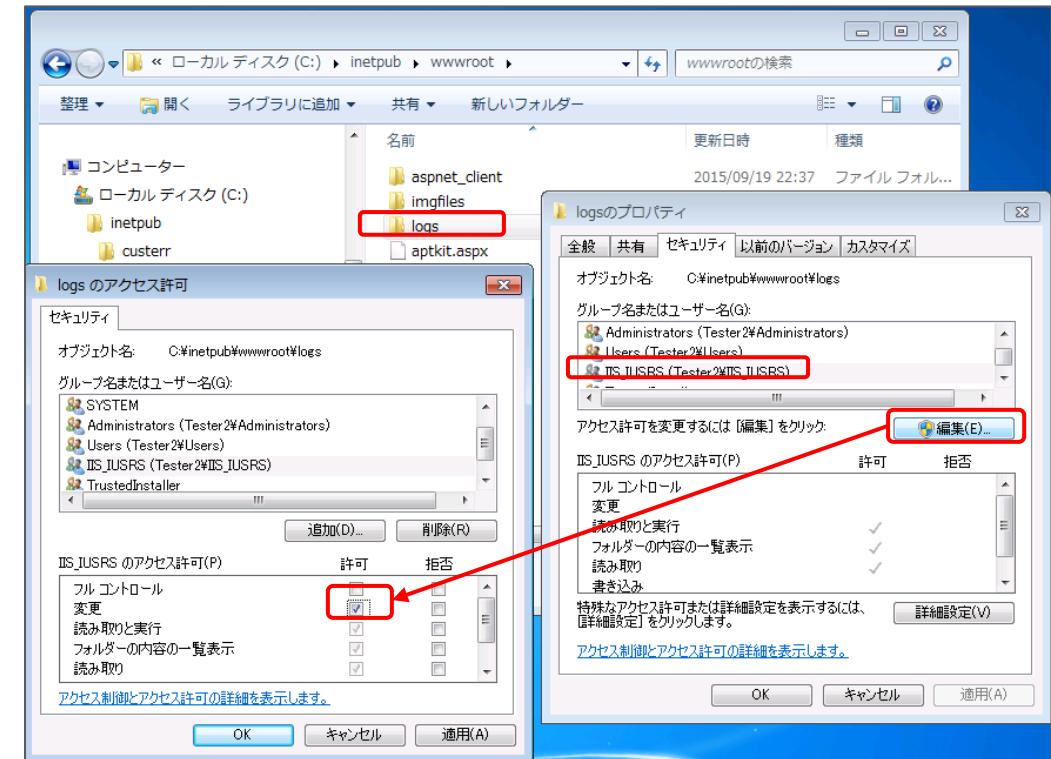
⑥④⑤の手順において、IIS_IUSRS が表示されない場合は、フォルダにアクセス可能なユーザーとして追加されていないため、IIS_USRS を追加するには、「ユーザーまたはグループの選択」ダイアログで「詳細設定」ボタンを押し、「検索」ボタンを押します。すると、検索結果の一覧に IIS_IUSRS が表示されるので、これを選択して OK ボタンを押します。



⑦以下のように、IIS_IUSRS がダイアログに追加されたら、OK ボタンを押します。



⑧④と同様の手順で、IIS_IUSRS に変更権限を付与します。



⑨apkkit.aspx をメモ帳などのテキストエディタで開き、smtpServer の値が空欄となっていることを確認します。

```
-----  
: 開封者情報の送信先に関する情報を設定して下さい  
-----  
Dim GrpName As String = "第1回メール訓練" ' 開封者情報集計用のグループ名  
Dim Subject As String = "開封者情報送付" ' メールの題名  
Dim toAddress As String = "test@hoge.jp" ' メールの送信先(複数ある場合は、;で区切る)  
Dim fromAddress As String = "test@hoge.jp" ' メールの送信元  
Dim smtpServer As String = "" ' SMTPサーバーのホスト名  
Dim smtpPort As Integer = 587 ' SMTPサーバーのポート番号  
Dim authUser As String = "test@hoge.jp" ' SMTP認証のユーザ名  
Dim authPass As String = "password" ' SMTP認証のパスワード  
Dim authSSL As Boolean = true ' SSL接続を使用するか否か (True or False)  
Dim LinkURL As String = "./contents/top.html" ' リダイレクト先のURL  
Dim emlID As String = "C:\Inetpub\wwwroot\mail" ' ローカルにメールを保存する場合の出力先
```

STEP1-4 ログ記録用フォルダとメール保存用フォルダを設定する③

⑨までの設定を完了したら、エラーログファイルの出力と、eml 形式のメールデータ出力の確認を行います。

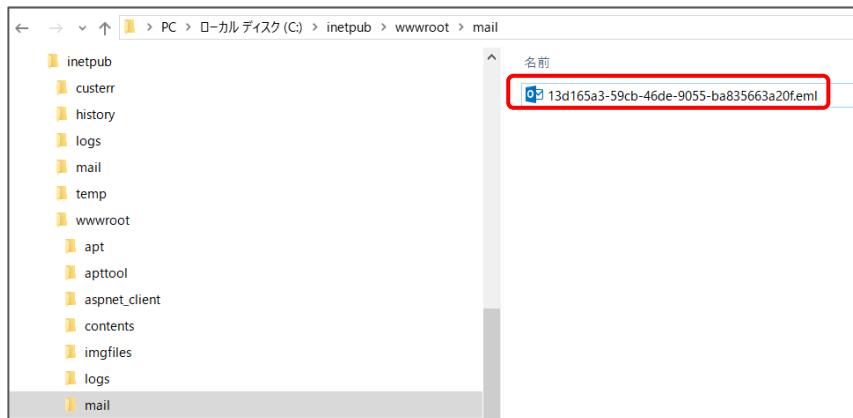
※本作業は Web サーバ(IIS)を設定したパソコン上で行う作業になります。

- ⑩IIS を設定したパソコン上で Web ブラウザを起動し、
<http://localhost/aptkit.aspx?apps=test> にアクセスします。
すると、以下のような画面が表示されるはずです。



※表示されない場合は、STEP1-1③で ASP.NET にチェックを入れているかどうかを確認して下さい

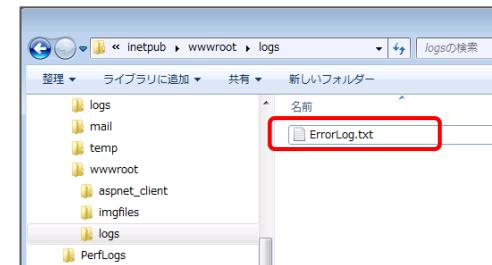
- ⑪<http://localhost/aptkit.aspx?apps=001> にアクセスします。
「c:¥inetpub¥wwwroot¥mail」フォルダ配下に、拡張子が.eml のファイルが出力されていることを確認します。



※拡張子が.eml のファイルは、eml 形式で保存された開封者情報のメールになります。この eml ファイルは、キットに付属の「開封者情報集計ツール」を用いることで、訓練メールに添付したファイルを開いたり、メール本文中の URL をクリックしたユーザが誰であるか？を集計することができます。

- ⑫aptkit.aspx 内の smtpServer の値を hoge に設定し、
<http://localhost/aptkit.aspx?apps=001> にアクセスします。
この後、「c:¥inetpub¥wwwroot¥logs」フォルダ配下に、ErrorLog.txt が
出力されていることを確認します。

```
Dim GrpName As String = "第1回メール訓練" ' 開封者情報集計用のグループ名
Dim Subject As String = "開封者情報送付" ' メールの題名
Dim toAddress As String = "test@hoge.jp" ' メールの送信先(複数ある場合は、;で区切る)
Dim fromAddress As String = "test@hoge.jp" ' メールの送信元
Dim smtpServer As String = "hoge" ' SMTPサーバーのホスト名
Dim smtpPort As Integer = 887 ' SMTPサーバーのポート番号
Dim authUser As String = "test@hoge.jp" ' SMTP認証のユーザ名
Dim authPass As String = "password" ' SMTP認証のパスワード
Dim authSSL As Boolean = _true ' SSL接続を使用するか否か (True or False)
Dim LinkURL As String = "./contents/top.html" ' リダイレクト先のURL
Dim emlFld As String = "C:¥inetpub¥wwwroot¥mail" ' ローカルにメールを保存する場合の出力先
```



※ ErrorLog.txt は、SMTP サーバーとの接続がエラーとなるなど、aptkit.aspx の実行にエラーがあった場合に出力されるファイルとなります。
ここでは、SMTP サーバーとの接続がエラーになるよう、あえて smtpServer の値を設定することで、ErrorLog.txt の出力が行われるようにしています。
開封者情報が出力される場合はエラーが発生していないことになりますので、ErrorLog.txt は出力されないのが正解となります。

STEP1-5 aptkit.aspx にリダイレクト先を設定する

⑫までの設定を完了したら、リダイレクト先として <http://localhost/contents/top.html> を、apkit.aspx の LinkURL に設定します。

リダイレクト先には任意の URL を設定できますので、自社で用意した Web ページや、e-Learning のサイトの URL なども指定できます。

⑬apkit.aspx 内の LinkURL の値を以下の図の通り設定します。

<http://localhost/contents/top.html> の URL にアクセスができる事は事前に Web ブラウザを用いて確認しておいてください。

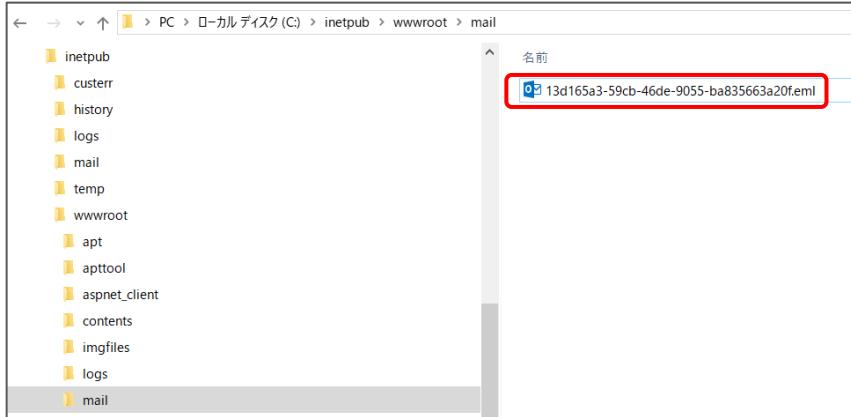
```
' 開封者情報の送信先に関する情報を設定して下さい
Dim GrpName As String = "第1回メール訓練"
Dim Sender As String = "開封者情報送付"
Dim toAddress As String = "test@hoge.jp"
Dim fromAddress As String = "test@hoge.jp"
Dim smtpServer As String = ""
Dim smtpPort As Integer = 587
Dim authUser As String = "test@hoge.jp"
Dim authPass As String = "password"
Dim authSSL As Boolean = true
Dim LinkURL As String = "./contents/top.html"
Dim emlId As String = "C:\inetpub\wwwroot\mail\" & ローカルにメールを保存する場合の出力先
```

⑭apkit.aspx 内の GrpName には、実施する訓練を識別する名称を設定します。
開封者情報集計ツールでは、GrpName に設定した名称の単位で開封者情報を集計することができます。

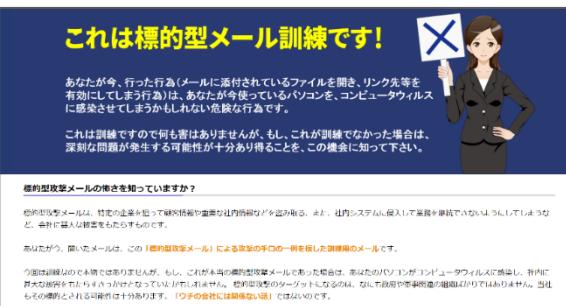
例えば、期間を空けて 2 回の訓練を実施する場合、GrpName に「第 1 回メール訓練」「第 2 回メール訓練」と設定して訓練を実施すると、開封者情報集計ツールでは、「第 1 回メール訓練」「第 2 回メール訓練」の別に集計結果が作成されます。

※詳しくは「開封者情報の集計」を参照して下さい。

⑮Web ブラウザから、<http://localhost/apkit.aspx?u=001> にアクセスします。
この時、inetpub\mail フォルダ配下に、拡張子が.eml のファイルが outputされることを確認します。



⑯<http://localhost/apkit.aspx?u=001> にアクセスすると、<http://localhost/contents/top.html> にページが自動的に切り替わることを確認します。設定に問題がなければ、以下の画面が表示されるはずです。



以上までの確認が無事完了すると、apkit.aspx の基本的な設定は完了となります。開封者情報のメールを eml ファイルとしてサーバ上に保管する形式でよければ、この状態で標的型メール訓練を実施することができますが、開封者情報のメールが指定のアドレス宛（例えば自分宛）に届くようにするには、引き続き、次ページ以降に示す設定を行ってください。

STEP1-5（補足）GrpName の設定について

前ページ⑭で設定する GrpName と、「開封者情報のデータ」「開封者情報集計ツール」「開封者情報集計用ユーザマスター CSV データ生成ツール」の関係は以下の通りです。

開封者情報は GrpName（グループ名）に設定した値の単位で集計されますので、「第 1 回目訓練」や「2024 年 7 月実施訓練」など、訓練の実施単位にグループ名を設定してください。

【aptkit.aspx】

```
Sub Page_Load(Sender As Object, E As EventArgs)
    ' 開封者情報の送信先に関する情報を設定して下さい
    Dim GrpName As String = "以下の方が添付ファイルを実行しました" '開封者情報集計用のグループ名
    Dim Subject As String = "開封者情報実行" 'メールの題名
    Dim toAddress As String = "test@hoge.jp" 'メールの送信元
    Dim fromAddress As String = "test@hoge.jp" 'SMTPサーバーのホスト名
    Dim smtpServer As String = "587" 'SMTPサーバーのポート番号
    Dim authUser As String = "test@hoge.jp" 'SMTP認証のユーザ名
    Dim authPass As String = "password" 'SMTP認証のパスワード
    Dim authSSL As Boolean = true 'SSL接続を使用するか否か (True or False)
    Dim LinkURL As String = "/contents/top.html" 'リダイレクト先のURL
    Dim fishOp As Boolean = false 'フィッシング・詐欺訓練モードにするか否か (True or False)
    Dim fishPage As String = "/LoginForm.html" 'フィッシング・ページのURL
    Dim emlId As String = "C:\inetpub\wwwroot\mail" 'ローカルにメールを保存する場合の出力先
```

【開封者情報のメールデータ】

以下の方が添付ファイルを実行しました
Web ピーチンク
::1
GrpName に設定した値が
開封者情報データの
1 行目に表示されます。
DESKTOP-AptKit
user01

aptkit.aspx（又は aptkit.php）の GrpName に
設定した値を、「開封者情報集計用ユーザマスター
CSV データ生成ツール」の「グループ名」に設定します。

【開封者情報集計用ユーザマスター CSV データ生成ツール】

A	B	C	D	E	
開封者情報集計用ユーザマスター CSV データ生成ツール Ver.2019.02.18.01					
1					
2	本ツールは、標的型攻撃メール対応訓練実施キットに付属の「開封者情報集計ツール（AptAggregationTool.exe）」に取り込む「ユーザマスター用CSVデータファイル」				
3	本ツールの8行目から下にデータを記載し、「ユーザマスターCSVファイルを作成する」ボタンを押すと、本ツールが保存されているフォルダと同じ場所にユーザマ				
4					
5	8行目の項目名のうち、セル背景色が薄黄色（E列～I列）のセルの項目名については、自由な項目名に変更することができます。				
6					
7					
8	グループ名	突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名
9	以下の方が添付ファイルを実行しました	0001	古川慶彦	役員	
10	以下の方に添付ファイルを実行しました	0002	大林政	役員	
11	以下の方に添付ファイルを実行しました	0003	磯野敬子	役員	
12	以下の方に添付ファイルを実行しました	0004	神山栄月	役員	
13	以下の方に添付ファイルを実行しました	0005	難波灯	役員	

開封者情報は、開封者情報データの 1 行目に表示される値の単位に集計されます。

【開封者情報集計ツールのユーザマスター情報】

メールアドレス	第二所属部署名	第一所属部署名	訓練実施対象者氏名	突合キー情報	メールアドレス
kunihiko309@ttulib.			古川慶彦	役員	kkikimprvatsush25
Keiko_Isono@wdr			大林政	役員	akari44334@nevbbf
Rumi_yamada@yataki			磯野敬子	役員	akukase@umrgvvr
shinji435@yderyo			神山栄月	役員	mitsumasakosug@p
Kouichi_Sakamoto@			難波灯	役員	Kouichi_Sakamoto@
			以下の方に添付ファイルを実行しました	0001	
			以下の方に添付ファイルを実行しました	0002	
			以下の方に添付ファイルを実行しました	0003	
			以下の方に添付ファイルを実行しました	0004	
			以下の方に添付ファイルを実行しました	0005	
			以下の方に添付ファイルを実行しました	0006	
			以下の方に添付ファイルを実行しました	0007	
			以下の方に添付ファイルを実行しました	0008	
			以下の方に添付ファイルを実行しました	0009	

【開封者情報集計ツールが表示する Result.csv のデータ】

突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス	役員	ユーザー権限	ユーザー権限	ユーザー権限
a003	2016/10/27 22:06	w003	後藤達也	営業部	kirotaka521@kunren.jp	社員		
a010	2016/10/27 22:06	w010	西岡耕夫	第一営業部	hiroyuki.Nishi-oka@kunren.jp	社員		
a002	2016/10/27 22:06	w002	大森悠	第一営業部	haruka.Otani@kunren.jp	社員		
【以下の方に添付ファイルを実行しました】								
集計結果データ	登録者数	開封者数	開封率					
第一組織名								
役員	11	8	9.0%					

グループ名に設定した値が
開封者情報ツールの
グループ名として取り込まれます。

開封者情報のデータは、開封者情報データの 1 行目に表示される値と、突合キー情報の AND 条件で突合が行われ、グループ名に設定した値の単位で開封者情報データが集計されます。

STEP1-6 開封者情報のメールを指定の宛先に送信するよう設定する

aptkit.aspx では、SMTP サーバを利用して、開封者情報のメールを指定のアドレス宛に送信することができます。開封者情報のメールが指定のアドレス宛に届くようにするには、aptkit.aspxにおいて、以下の設定を行います。設定を完了したら、IIS を設定したパソコン上で Web ブラウザを起動し、<http://localhost/apkit.aspx?apps=001> にアクセスします。SMTP サーバへの接続設定に間違いが無ければ、c:¥inetpub¥mail フォルダ配下に eml ファイルが作成される代わりに、開封者情報のメールが、指定した宛先に送信されます。

```
'-----  
'; 開封者情報の送信先に関する情報を設定して下さい  
  
Dim GrpName As String = "第1回メール訓練"  
Dim Subject As String = "開封者情報送付"  
Dim toAddress As String = "test@hoge.jp"  
Dim fromAddress As String = "test@hoge.jp"  
Dim smtpServer As String = "  
Dim smtpPort As Integer = 587  
Dim authUser As String = "test@hoge.jp"  
Dim authPass As String = "password"  
Dim authSSL As Boolean = true  
Dim LinkURL As String = "./contents/top.html  
Dim emlID As String = "C:¥inetpub¥wwwroot¥mail" 'ローカルにメールを保存する場合の出力先  
  
'-----  
'開封者情報集計用のグループ名  
'メールの題名  
'メールの送信先(複数ある場合は、;で区切る)  
'メールの送信元  
'SMTPサーバーのホスト名  
'SMTPサーバーのポート番号  
'SMTP認証のユーザ名  
'SMTP認証のパスワード  
'SSL接続を使用するか否か (True or False)
```

この部分の設定を変更します。設定する情報については、メールソフトで設定している情報と同じものを指定します。

なお、wwwroot 配下のファイルについては、Windows のセキュリティ機能により、デフォルトでは直接編集して保存することができないようになっていますので、編集した aptkit.aspx については別のフォルダに保存し、ファイルエクスプローラーで wwwroot フォルダ配下の aptkit.aspx に上書きコピーします。

Subject	開封者情報のメールの題名を設定します。変更する必要がなければデフォルトのままで結構です。
toAddress	開封者情報メールの送信先となるメールアドレスを設定します。複数の宛先に送付する場合はアドレスをセミコロン「;」で区切ってください。
fromAddress	開封者情報メールの送信元となるメールアドレスを設定します。
smtpServer	メール送信に使用するSMTPサーバーのホスト名を設定します。
smtpPort	メール送信に使用するSMTPサーバーのポート番号（25、465、587など）を設定します。
authUser	メール送信にSMTP-AUTHが必要となる場合は、SMTP-AUTHに使用するUser名を設定します。
authPass	authUserで設定したUser名に対するパスワードを設定します。
authSSL	メール送信にSSL接続が必要である場合は「True」にします。メール送信に失敗する場合は、この設定を変えてみて下さい。

もしメールが届かない場合は、c:¥inetpub¥wwwroot¥logs¥ErrorLog.txt にエラーが出力されているかどうかを確認してください。

【よくある間違い】

- authSSL の設定で、「true」とすべきところを「false」に設定している。（もしくはこの逆）
- smtpPort に設定すべきポート番号を間違えている。（587と指定すべきところを 25 に設定しているなど）
- SMTP サーバ側で、外部アプリケーションからのメール送信を許可する設定をしていない。（Gmail を使う場合など）
- fromAddress に、SMTP サーバ側では受け入れできないアドレスを設定している。
- SMTP-AUTH の設定（authUser、authPass）を間違えている。

※開封者情報メールの送信がどうしてもうまくいかない場合は、まず、apkit.aspx を設置している PC 上で、OutLook や Thunderbird などの通常のメールソフトを使って、メール送信が正しくできることを確認してください。通常のメールソフトでのメール送信が正しく行えるのであれば、メールソフトの設定画面で設定した内容と同じ情報を apkit.aspx に設定すれば、メール送信が行えるはずです。

STEP1-7 他のパソコンから Web サーバへのアクセスについて

前ページまでの設定については、Web サーバを設定したパソコンでの作業を想定しているため、URL を「<http://localhost/aptkit.aspx?~>」としましたが、実際の訓練では、他のパソコンから Web サーバにアクセスが発生することになるため、「<http://localhost/aptkit.aspx?~>」は使うことができません。（localhost は自己自身のパソコンを表すため）

このため、他のパソコンから Web サーバにアクセスするには、IP アドレスでアクセスさせる、もしくはホスト名（DNS や WINS によって、ホスト名で Web サーバにアクセスすることができるようになっている場合）でアクセスするようにします。なお、Web サーバを設定したパソコンの IP アドレスがわからない場合には、以下の手順で調べることができます。

ちなみに、通常の業務でお使いのパソコンを Web サーバとして使用する場合、お使いのパソコンの IP アドレスが、DHCP によって動的に割り当てられているケースが多いと思います。

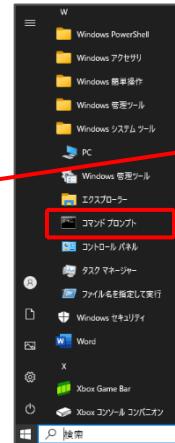
パソコンの電源を入れなおすことで、パソコンに割り当てられる IP アドレスが変わってしまうと、訓練実施前は Web サーバにアクセスできたのに、訓練を実施したら Web サーバにアクセスができなくなってしまった。ということが起こりますので、DHCP によって動的に IP アドレスが割り当てられるパソコンを Web サーバとしてお使いになられる場合は、この点にご留意ください。

- ① コマンドプロンプトを起動します。

↓ Windows8.1

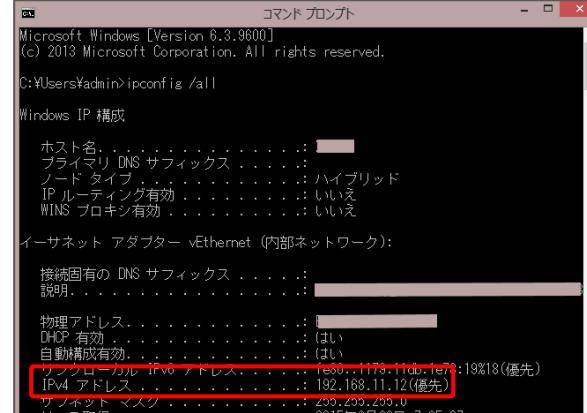


↓ Windows10、11



- ② ipconfig とタイプしてリターンキーを押します。

↓ 下記赤枠部分が、割り当てられている IP アドレスになります。



【自分のパソコンからは <http://localhost/aptkit.aspx?~> にアクセスできるのに、他のパソコンからアクセスできない場合】

P.12 の⑯までは問題なく確認できたのに、他のパソコンの Web ブラウザからは <http://localhost/aptkit.aspx?u=001> にアクセスができない。という場合は、以下の設定を確認してください。

1. Windows のコントロールパネルの設定から Windows ファイアウォールを選択し、アクセス元のパソコン及び、IIS を設定したパソコンの双方において、80 番ポートの受信と送信のどちらかがブロックされていないかどうかを確認して下さい。
2. IIS の設定で、外部からの接続を拒否していないかどうかを確認して下さい。
3. アクセス元のパソコンの Web ブラウザの設定において、プロキシサーバーを経由してアクセスを行うような設定となっている場合は、プロキシサーバーを経由しないよう設定して下さい。



STEP1-補足 Windows以外のOSでWebサーバを構成する

Windows OS に付属の IIS を用いると、最も手軽に Web サーバを構成することができますが、インターネット上に Web サーバを設置せざるをえない、また、既に設置されている Web サーバを使用したいなど、諸事情により Windows OS 以外の OS で構成される Web サーバを使用したいというケースもあります。この場合、PHP が使用できる Web サーバであれば、キットに付属の aptkit.aspx の代わりに、PHP 版のプログラムである aptkit.php を用いて、Web サーバを構成することができます。

なお、apkit.php では eml ファイルの代わりに、txt ファイルが出力されますが、php.ini を編集し、sendmail_path の設定を以下のように変更できる場合は、送信するメールの内容を eml ファイルとして出力することもできます。

```
sendmail_path = /bin/cat > `mktemp -p /tmp XXXXXXXX.eml`
```

手順1 aptkit.phpの編集

メモ帳などのテキストエディタを用いて、キットに付属の aptkit.php を開き、以下の赤枠部分を編集します。

```
// 標的型攻撃メール対応訓練実施キット 開封者情報メール送信プログラム
// 本プログラムは、訓練対象者のパソコンから直接、開封者情報を送付
// することができない場合の代替策。また、Webビューコン形式にて訓練を
// 実施する場合の開封者情報取得用として、Webサーバから開封者情報を
// 送付するプログラムとなります。
// PHPのMailコマンドは使用できるが、Pearモジュールを使えないような
// 場合は、apkit.phpの代わりにこちらをお使いください。
// 本プログラムを利用するには、以下の条件を満たす必要があります。
// 1. Webサーバ側でPHPが使用できること
// 2. PHPのMailコマンドが使用できるようになっていること
// 3. リダイレクト先となるWebページがあること
// 4. GDモジュールが利用可能となっていること
// -----
// 値の設定
// $to= に設定すると、開封者情報をファイルに書き出します。
$URL = "./contents/top.html"; // リダイレクト先のURL
$to = ""; // 開封者情報メールの送信先アドレス
$from = "hoge@hoge.jp"; // 開封者情報メールの送信元アドレス
$subject = "開封者情報送付"; // メールのタイトル
$filepath = "/mail/"; // ファイルの出力先
$GrpName = "第1回メール訓練"; // 開封者情報集計用のグループ名
```

1. \$URL の「サーバ名」の部分を、貴社で用意したサーバのドメイン名もしくは IP アドレスに変更します。
2. \$to には、開封者情報のメールを受信するメールアドレスを記載します。（例： \$to = "myname@hoge.co.jp"）
3. \$from には、開封者情報メールの差出人メールアドレス（Web サーバからのメール送信に使用可能なメールアドレス）を記載します。（例： \$from = "sender@hoge.co.jp"）
4. \$subject については、開封者情報メールのメールタイトルになりますので、必要であれば適宜変更して下さい。
5. \$filepath については、開封者情報をメールで送信する代わりに、ファイルに書き出す運用とする場合に、ファイルの出力先パスを記載します。（出力先のフォルダには書き込み権限を必ず設定しておいて下さい）
6. \$GrpName については、実施する訓練を識別する名称を設定します。開封者情報集計ツールでは、GrpName に設定した名称の単位で開封者情報を集計することができます。

手順2 手順1で保存した aptkit.php を、キットに付属の top.html 及び、imgfiles フォルダと共に Web サーバにアップロードし、apkit.php のパーミッションを 755 に設定します。

手順3 手順2が完了したら、Web ブラウザから、http://サーバ名/apkit.php?u=001 にアクセスし、top.html が表示されること、また、開封者情報のメールが \$to で設定したメールアドレス宛に届くことを確認して下さい。また、\$filepath を設定している場合は、指定した出力先パスに開封者情報の txt ファイルが出力されることを確認して下さい。

訓練メール送信に使用できる SMTP サーバが社内にない、また、ネットワーク環境が異なる拠点が複数あるなど、訓練実施対象者全員からアクセス可能な Web サーバを用意するとなると、インターネット上に Web サーバを用意せざるをえないといった場合は、Sakura インターネット (<https://www.sakura.ad.jp/>) などの事業者が提供するレンタルサーバサービスや VPS サーバサービスを利用する方法があります。

STEP2 リンク先のページを用意する

STEP1 では、Web サーバにアクセスした際に表示される Web ページとして、キットに付属の HTML ファイルを使用しましたが、訓練実施の目的や内容によっては、キットに付属の Web ページではなく、他の Web ページが表示されるようにしたい。というケースもあるかと思います。キットに付属の HTML ファイル以外は使うことができない。といった制限はありませんので、他の HTML ファイルなどを使用したい場合は、リンク先となる Web ページのデータを別途ご用意頂いた上で、以下を参考に、aptkit.aspx 内の「LinkURL」に、アクセス先となる Web ページの URL を設定して下さい。

```
23 :-----↓  
24 ; 開封者情報の送信先に関する情報を設定して下さい↓  
25 -----↓  
26 Dim Subject As String = "開封者情報送付" ;メールの題名↓  
27 Dim toAddress As String = "test@hoge.jp" ;メールの送信先(複数ある場合は、;で区切る)↓  
28 Dim fromAddress As String = "test@hoge.jp" ;メールの送信元↓  
29 Dim smtpServer As String = "" ;SMTPサーバーのホスト名↓  
30 Dim smtpPort As Integer = 587 ;SMTPサーバーのポート番号↓  
31 Dim authUser As String = "test@hoge.jp" ;SMTP認証のユーザ名↓  
32 Dim authPass As String = "password" ;SMTP認証のパスワード↓  
33 Dim authSSL As Boolean = true ;SSL接続を使用するか否か (True or False) ↓  
34 Dim LinkURL As String = "http://hoge.co.jp/kunren.html" ;リダイレクト先のURL↓  
35 Dim emlFile As String = C:\inetpub\wwwroot\mail ;一括でメールを保存する場合の出力先↓  
36 -----↓
```

メモ帳や HTML エディタなどで、LinkURL の値に、アクセス先としたい URL を設定します。

※URL リンククリック型の訓練では、URL リンクをクリックした際に表示する Web ページや、ダウンロードファイルが必要になりますが、これを全く何もない状態から用意するのは面倒です。そこで基本キットでは、URL リンクがクリックされた際に表示する Web ページ画面として、標的型メールに関する教育用のコンテンツの雛形をご提供しています。

雛形では、訓練についての問い合わせ先を記載する箇所を設けてありますので、雛形を利用される際は、メモ帳や HTML エディタなどを使って、問い合わせ先の部分を適宜修正した上でご利用下さい。
なお、雛形の内容については、自由に改編してご利用いただけますが、著作権フリーではありませんので、ご利用いただける範囲は、貴社内でのご利用に限定されますことをご留意ください。



メモ帳や HTML エディタなどでこの部分を適宜書き換えます。

STEP3 訓練メールを送信する（訓練メールを送信する2つの方法）

標的型メール訓練では、誰が訓練メールを開封したかどうか（訓練メールに添付されたファイルを開いたかどうか、また、訓練メール本文中の URL リンクをクリックしたかどうか）を特定できるようにするために、**送信先毎に内容が異なる**訓練メールを送信することになります。

送信先毎に内容が異なるメールを送信することは、Bcc に送信先を設定して訓練メールを一斉送信するといった方法は使えず、送信先ごとに訓練メールを送る必要が生じることになりますが、これを1通ずつ手作業で送信するのは無理があります。

そこで、標的型攻撃メール対応訓練実施キットでは、訓練メールを送信する方法として、以下の2つの方法をご提供しています。

1. 自社で用意した訓練メール送信用のメールサーバ（SMTP サーバ）を使用して訓練メールを送る

キットに付属の「訓練メール作成支援ツール」では、SMTP サーバに接続して訓練メールを一斉送信することができますので、訓練メールを送信することができるメールサーバ（SMTP サーバ）を自社で用意することができる場合は、こちらの方法で訓練メールを送信することができます。

インターネットに接続できない環境で標的型メール訓練を実施される場合や、送信元（From アドレス）として設定するドメイン名の正規のメールサーバから訓練メールを送信したい場合（例えば、Gmail の SMTP サーバからメールを送信したい場合）など、特定の SMTP サーバから訓練メールを送信したい場合は、こちらの方法を利用することになります。

2. 訓練メール送信サービス（<https://mss.kunrenkit.jp/SMTPUpload.aspx>）を利用して訓練メールを送る

キットでは、以下①や②などの理由から、自社内の環境からは訓練メールを送信することが難しい場合の代替として、訓練メールを送信するサービスもご提供しています。

1. の方法で訓練メールを送信することは難しいというお客様は、こちらの方法をご利用ください。

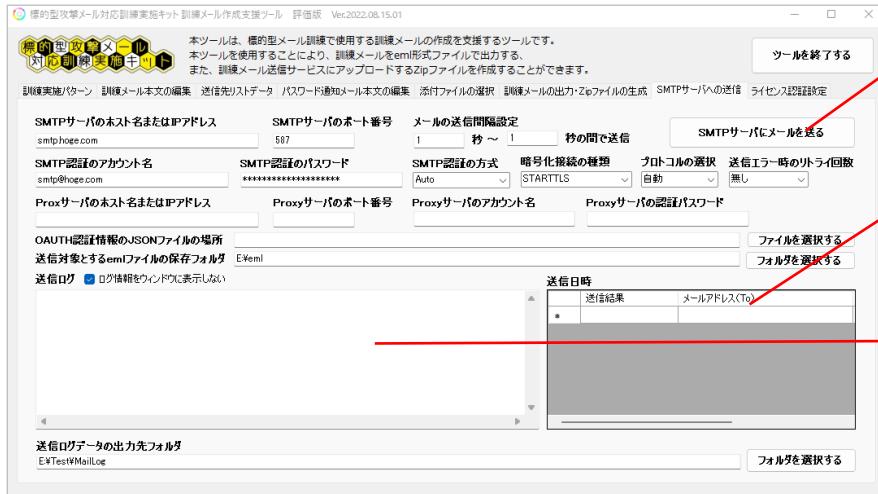
- ① 自社で利用できる SMTP サーバではセキュリティ対策の設定が厳しくて、訓練メールの差出人アドレスを希望するアドレスに設定することができないような場合（例えば、Office365 で提供される outlook.com のメールサーバでは、自分のアドレス以外のアドレスを差出人として設定できません）
- ② 自社の環境ではファイアウォールが設定されており、自社内のパソコンからは、インターネット上にある SMTP サーバ（レンタルサーバサービスで提供される SMTP サーバや、Gmail など始めとするフリーで利用できる SMTP サーバなど）に接続することができない場合

但し、標準の契約の範囲内では、ライセンス有効期間中に送信できる訓練メールの通数に制限が設けられているため、制限を超えて訓練メールを送信したい場合は、送信を希望される通数分の追加送信チケット（有償）を別途ご購入頂く必要があります。

ご契約の種類	標準のご契約の範囲内で送信できる訓練メールの通数
キット 評価版	100 通まで
キット Basic 版	1,000 通まで
キット Standard 版	3,000 通まで
キット Group A 版	5,000 通まで
キット Group B 版	10,000 通まで
追加の送信チケット	100 通/5,000 円（税別）～

STEP3-1 自社で用意した SMTP サーバを利用して訓練メールを送信する

自社で用意した SMTP サーバを利用して訓練メールを送信する場合は、キットに付属している「訓練メール作成支援ツール（KunrenkitTool.exe）」の「訓練メールの出力」機能で eml ファイルを生成した後、「SMTP サーバへの送信」機能を利用することで、訓練メールを送信することができます。本節では、自社で用意した SMTP サーバを用いて訓練メールを送信する際のポイントについて記載します。



「SMTP サーバにメールを送る」ボタンを押すと、ボタン名が「送信処理を中止する」に切り替わり、「送信対象とする eml ファイルの保存フォルダ」で指定したフォルダ配下にある eml ファイルが、順次 SMTP サーバに送信されます。なお、メールの送信順はファイル名順となります。「送信処理を中止する」ボタンを押すと、送信処理が中断されます。

送信完了時の時刻と、送信先のアドレスが表示されます。本欄に出力されたデータについては、SendLog.txt として、送信ログデータの出力先フォルダで指定したフォルダ配下に出力されます。

送信ログ（SMTP サーバとの通信ログ）が、本欄に出力されます。

本欄に出力された情報は、SMTPlog.txt として、送信ログデータの出力先フォルダで指定したフォルダ配下に出力されます。

なお、接続先の SMTP サーバ内でエラーとなったメールに関するエラーについては、本ツールではキャッチすることができないため、出力されません。（例：SMTP サーバ側のセキュリティ対策ルールに基づいて送信拒否となった場合など）

◆各項目の説明

SMTP サーバのホスト名または IP アドレス	訓練メールを送信する SMTP サーバのホスト名又は IP アドレスを設定します。
SMTP サーバのポート番号	SMTP サーバのポート番号（25,465,587）を設定します。
メールの送信間隔設定	間隔を空けてメールの送信を行いたい場合は、間隔を空ける秒数を指定します。開始と終了に同じ秒数を指定すると等間隔で、異なる秒数を設定した場合は、設定した秒数の間でランダムな間隔が適用されます。間隔を設定しない場合（連続で送信する場合）は 0 秒の設定とします。
SMTP 認証のアカウント名・パスワード	SMTP サーバに接続するに際して、SMTP 認証が必要となる場合は、SMTP 認証のアカウント情報を設定します。
SMTP 認証の方式・暗号化接続の種類・プロトコルの選択	SMTP サーバに接続するに際して、SMTP 認証が必要となる場合は、SMTP 認証の方式等を設定します。 Gmail のメールサーバを利用してメールを送信する場合は、OAuth 認証を利用することができます。
送信エラー時のリトライ回数	SMTP サーバへの接続に失敗するなど、送信エラーが発生した場合に再送を行う回数を指定します。指定した回数の再送を行ってもエラーとなる場合は、エラーメールとして処理されます。
Proxy サーバに関する設定 (Proxy サーバのホスト名又は IP アドレスなど)	SMTP サーバに接続するに際して、Proxy サーバを経由する必要がある場合は、Proxy サーバに関する情報を設定します。
送信対象とする eml ファイルのフォルダ	SMTP サーバに送信を行う eml ファイルが保存されているフォルダのパスを指定します。 通常は、訓練メール作成支援ツールの「訓練メールの出力」機能で出力した eml ファイルが保存されているフォルダのパスを指定します。

◆「SMTP サーバへの送信」機能によって送信されるメールについて

「SMTP サーバへの送信」機能では、「送信対象とする eml ファイルの保存フォルダ」で指定したフォルダ配下にある eml ファイルを対象にメールの送信が行われます。このため、訓練メール作成支援ツールで訓練メールの送信を行うには、「訓練メールの出力」機能によって、一旦、拡張子が.eml のファイルを出力し、eml ファイルの内容が意図した通りの内容であることを確認した上で、「SMTP サーバへの送信」機能を用いてメールの送信を行う流れとなります。

なお、eml ファイルの先頭に（送信完了）もしくは（エラー）の文字列が設定されている場合は、送信対象から除外されますのでご注意ください。

STEP3-1 自社で用意した SMTP サーバを利用して訓練メールを送信する（続き）

◆送信結果の出力について

訓練メール作成支援ツールの「SMTP サーバへの送信」機能で送信したメールの結果出力については、送信対象となった eml ファイルの先頭に以下の文字列を付加することによって行われます。

・送信が完了した場合 → eml ファイルの先頭に（送信完了）の文字が付加されます。

・送信エラーとなった場合 → eml ファイルの先頭に（エラー）の文字が付加されます。

なお、eml ファイルの先頭に（送信完了）もしくは（エラー）の文字列が設定されている場合は、送信対象から除外されます。

eml ファイルの先頭に（エラー）の文字が付加されているメールについては、SMTP サーバへの送信が完了していないことになりますので、訓練メールの宛先指定に誤りがないかなど、エラーの原因を確認の上、メールの内容を修正して再送を行うなどのご対応をお願いします。

◆エラーとなったメールの再送について

「送信エラー時のリトライ回数」の設定が 0 以上に設定されている場合、送信エラーとなったメールについて、指定した回数だけ再送が行われます。

なお、エラーとなったメールの再送については、全てのメールの送信処理が完了した後、約 3 分の間隔を置いて、再送処理が実施されます。

◆より柔軟な送信処理を行うために

訓練メール作成支援ツールでは、SMTP サーバとの接続がエラーとなった場合に、指定した回数、再送を行う機能が用意されていますが、SAPPOROWORKS という会社が提供している BlackJumboDog というソフトウェアをはじめとする、再送機能を持つ簡易 SMTP サーバと組み合わせると、より柔軟に訓練メールを送信することができます。

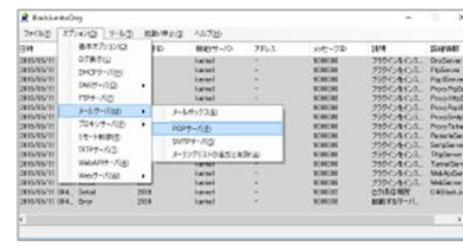
BlackJumboDog のインストールと設定については、「STEP3-1 補足」の説明を参照願います。

なお、BlackJumboDog では STARTTLS で接続する SMTP サーバには対応しておりませんので、ご注意ください。

訓練メール作成支援ツール（SMTP サーバへの送信機能）



BlackJumboDog のSMTPサーバ機能



送信エラーが発生した場合はBlackJumboDogが再送を実施



STEP3-1（補足） BlackJumboDog のインストール

BlackJumboDog をインストールするには、SAPPOROWORKS のサイトから BlackJumboDog をダウンロードしてインストールします。

msi 形式のファイルなら、ダウンロードしてダブルクリックするだけでインストーラが起動しますので簡単です。アーカイブサイトからソースコードをダウンロードし、ご自身でコンパイルを行うこともできますが、以下の URL から msi インストーラをダウンロードし、ダウンロードした msi 形式ファイルをダブルクリックしてインストールを行うのが早道です。

BlackJumboDog のインストールが完了したら、BlackJumboDog (BJD.exe) をダブルクリックして起動します。図は Windows10 での例ですが、Windows11 でも BlackJumboDog は問題なく利用できます。

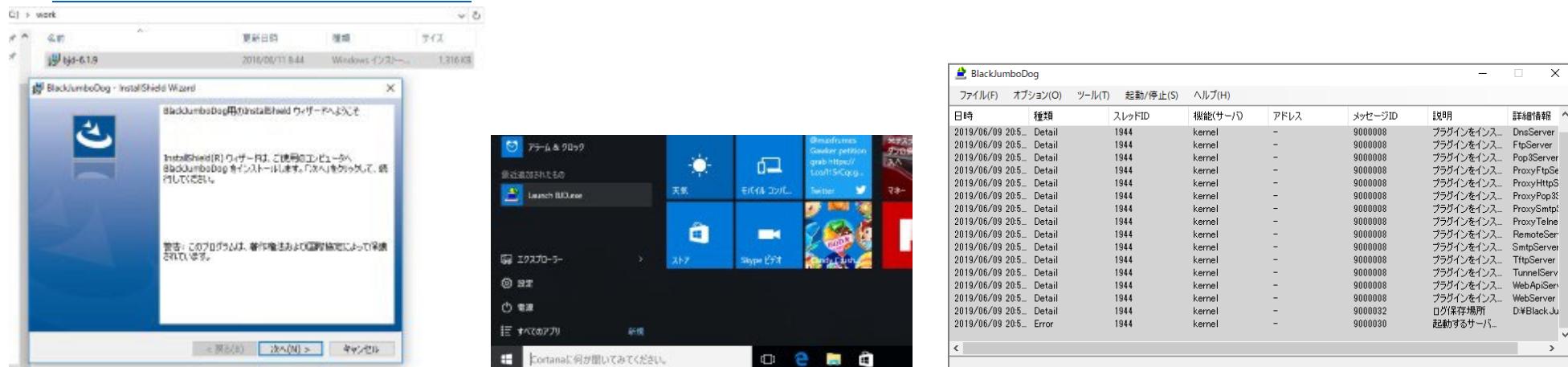
■ BlackJumboDog のダウンロード用 URL

Ver.6.2.0 msi インストーラ <https://forest.watch.impress.co.jp/library/software/blackjmbdog/>

ソースコード <https://codeplexarchive.blob.core.windows.net/archive/projects/blackjumbodog/blackjumbodog.zip>

■ BlackJumboDog の Web サイト

<http://www.sapporoworks.ne.jp/spw/>



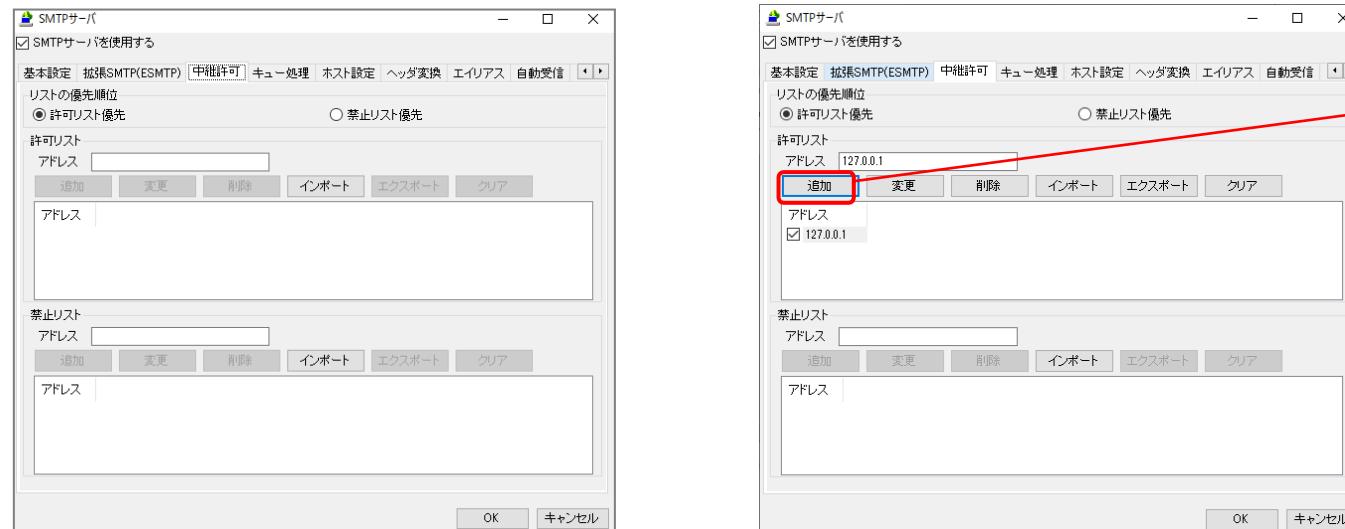
STEP3-1（補足） BlackJumboDog の SMTP 機能のセッティング①

BlackJumboDog の SMTP 機能を設定するには、以下の手順で設定を行います。

STEP1 : BlackJumboDog のメニューから「オプション」→「SMTP サーバ」を選択します。SMTP サーバの設定画面が表示されたら、「SMTP サーバを使用する」のチェックを ON にします。



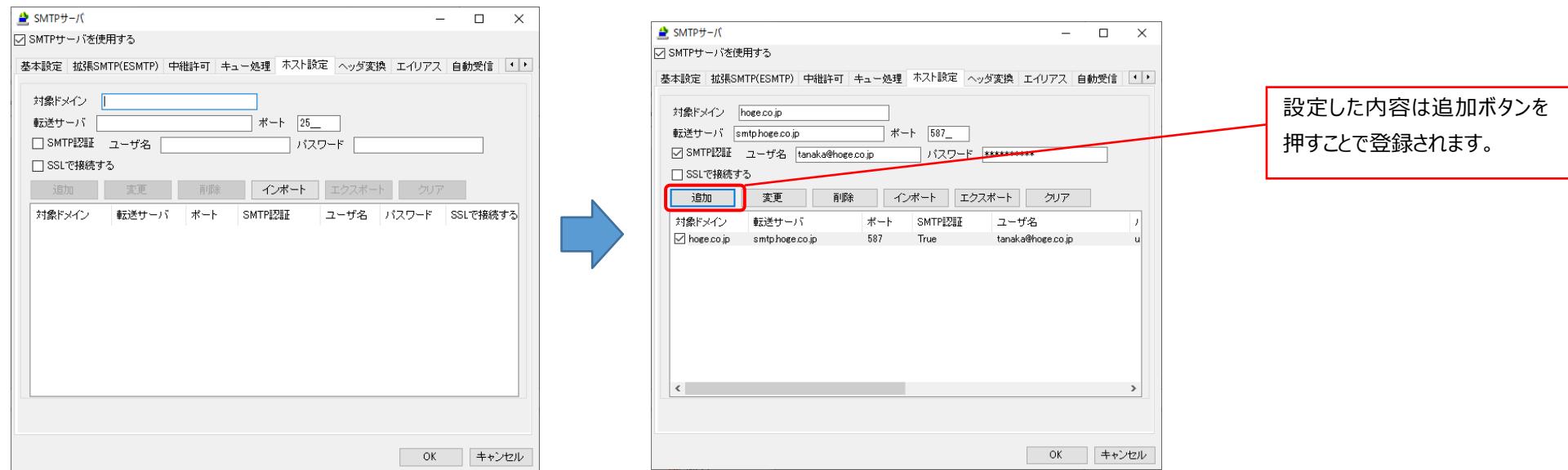
STEP2 : 「中継許可」のタブをクリックし、許可リストに「127.0.0.1」を追加します。他のパソコンからも BlackJumboDog の SMTP サーバを利用してメールを送信する場合は、BlackJumboDog への接続を許可するパソコンのアドレスを追加します。



STEP3-1（補足） BlackJumboDog の SMTP 機能のセッティング②

STEP3：中継許可を設定し終えたら、続けて「ホスト設定」のタブをクリックし、訓練メール送信用に利用する SMTP サーバの情報を登録します。

この例では、訓練メールの送信先が xxxx@hoge.co.jp である場合に、SMTP サーバとして smtp.hoge.co.jp を利用してメールを送信する場合の設定例を記載します。なお、smtp.hoge.co.jp では SMTP 認証による利用者制限を行っているものとします。



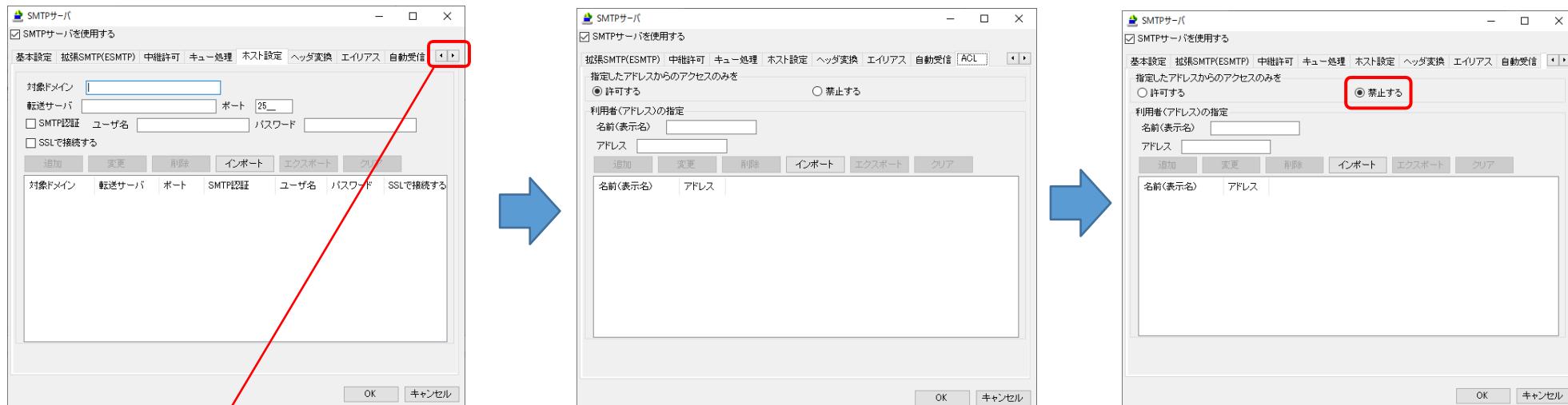
※「訓練メール送信用に利用するSMTP サーバ」とは、貴社でご用意頂いている、訓練メール送信用に使用するSMTP サーバの事を指します。

対象ドメイン	訓練メールの送信先となるメールアドレスのドメイン名（@マークより右側の部分）を指定します。
転送サーバ	訓練メールの送信に使用するSMTP サーバのホスト名（サーバ名）を指定します。
ポート	転送サーバのポート番号として指定されているもの（通常は 25、465、587 のいずれか）を設定します。
SMTP 認証	転送サーバがSMTP 認証を行っている場合は、認証情報として指定されているものを設定します。
SSL で接続する	転送サーバへの接続に際して SSL が必要である場合は、チェックを ON にします。

ご注意とお断り事項： BlackJumboDog には、Office365 で提供されるSMTP サーバなど、TLS 接続を必須とする SMTP サーバへの接続を行う機能ないため、Office365 のSMTP サーバは転送先として使用することができません。

STEP3-1（補足）BlackJumboDog の SMTP 機能のセッティング③

STEP4：ホスト設定を設定し終えたら、続けて「ACL」のタブをクリックし、「指定したアドレスからのアクセスのみを」「禁止する」に設定します。



ACL のタブは、▶ボタンを押すことで表示されます。

※ 「中継許可」の設定で、訓練メール送信用の SMTP サーバに対してメールを転送できるパソコンを制限しているため、 ACL の設定では「禁止する」を選択するのみで構いませんが、セキュリティをより強固にしておきたい場合は、「許可する」を選択し、BlackJumboDog を利用できるパソコンのアドレスを登録して下さい。

STEP5：ACL を設定し終えたら「OK」ボタンを押して設定を終了し、訓練メール作成支援ツールから BlackJumboDog に接続して訓練メールを送信できるかどうかのテストを行います。訓練メールが問題なく届けば、設定は完了です。もし、送信エラーとなるような場合は、ツールの送信結果欄及び、BlackJumboDog の送信ログにエラーの原因が表示されているはずですですので、こちらを確認して下さい。なお、訓練メール作成支援ツールで訓練メールを送信する際の設定は以下の通りです。

■ SMTP サーバのホスト名

localhost（又は、BlackJumboDog を設定したパソコンの IP アドレス）

■ SMTP サーバのポート番号

25（BlackJumboDog のSMTP サーバの基本情報で設定している番号）

■ SSL 接続を行うか否か

行わない

■ SMTP 認証に用いるアドレスとパスワード

いずれも空欄

STEP3-2 送信先リストデータの設定

訓練メール作成支援ツールに取り込む訓練メールの送信先リストデータは、キットに付属のツール「訓練メール作成支援ツール用メールマスタ CSV ファイル作成ツール.xlsm」を使用して作成することができます。

以下の図に記載の例のようにデータを記述し、「メールマスタ CSV ファイルを作成する」ボタンを押すと、ツールが保存されているフォルダと同じ場所に、ユーザマスタ用 CSV データファイル (MailMaster.csv) が出力されます。

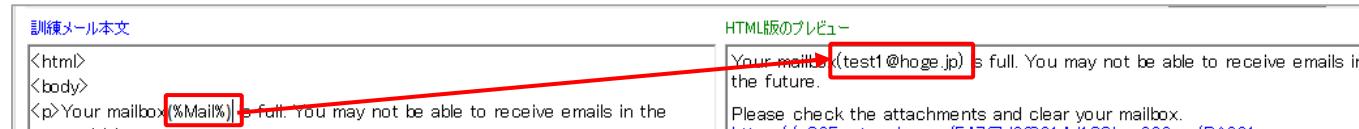
A	B	C	D	E	F	G	H	I	J	K	L	
1	訓練メール作成支援ツール用メールマスタCSVファイル作成ツール					Ver.2022.10.18.01	既存のマスタファイルを取り込む	メールマスタCSVファイルを出力する				
2	本ツールは、標的型攻撃メール対応訓練実施キットに付属の「訓練メール作成支援ツール (KunrenkitTool.exe)」に取り込む「メールマスタCSVデータファイル」を生成するツールです。											
3	本ツールの7行目から下にデータを記載し、「メールマスタCSVファイルを出力する」ボタンを押すと、指定したフォルダにユーザマスタ用CSVデータファイルを出力します。											
4	なお、ファイル出力時の文字コードはUTF-8形式としてください。また、メモ帳など、本ツールとは異なるアプリケーションで編集を行われる際は、ファイルの保存形式にご注意ください。										ファイルの文字コード	
5	マスタファイル出力先フォルダ										UTF-8	
6	メールアドレス	Ccメールアドレス	Bccメールアドレス	出力順	本文パターン	氏名	突合キー	埋込文字1	埋込文字2	埋込文字3	埋込文字4	添付ファイルのパス（複数ある場合は、各ファイルパスを;で区切ってください）
7												

項目名	説明
メールアドレス	訓練メールの送信先となるメールアドレスを設定します
出力順	訓練メールの出力順を半角数字で設定します。
本文パターン	訓練メールの本文として採用する、訓練メール作成支援ツールの本文パターン番号を（本文パターン1～本文パターン7のいずれか）を指定します。
氏名	訓練メールの送信先メールアドレスに紐づく氏名を設定します。
突合キー	訓練メールの送信先メールアドレスごとにユニークな値となる突合キーの情報を設定します。 ベーシック版のライセンスをご利用の場合、突合キー情報は0001から始まる連番となり、突合キー情報として任意の値を設定しても無視されますのでご注意ください。
埋込文字1	訓練メール作成支援ツールの「訓練メール本文の編集」欄もしくは、「パスワード通知メール本文の編集」欄に %Data1% パラメータが設定されている場合、訓練メール作成時に、%Data1%の部分は、本欄に設定した値（例：リンク先 URL など）に置き換えられて訓練メールがOutputされます。
埋込文字2	埋込文字1と同様に、%Data2% の部分は、本欄に設定した値（例：解凍パスワードなど）に置き換えられて訓練メールがOutputされます。
埋込文字3	埋込文字1と同様に、%Data3% の部分は、本欄に設定した値に置き換えられて訓練メールがOutputされます。
埋込文字4	埋込文字1と同様に、%Data4% の部分は、本欄に設定した値に置き換えられて訓練メールがOutputされます。
添付ファイルのパス	既存のファイルを訓練メールに添付する場合、添付するファイルのパス（フルパス）を記載することで、パスで指定したファイルが訓練メールに添付されてOutputされます。添付するファイルが複数ある場合は、フルパスとフルパスの間を、半角セミコロン「;」で区切ってください。

STEP3-3 送信先リストデータの訓練メール作成支援ツールへの取り込み

キットに付属の「訓練メール作成支援ツール用メールマスタ CSV ファイル作成ツール.xlsxm」を使用して作成した、ユーザマスタ用 CSV データファイル（MailMaster.csv）については、訓練メール作成支援ツールの「送信先リストデータ」タブにて、「メールアドレスデータ（CSV データ）を取り込む」ボタンを押して、訓練メール作成支援ツールに取り込みを行います。

メールマスタデータ（CSV データ）のファイルパスを指定して、訓練メール作成支援ツールを終了すると、ファイルパスで指定したファイルが、次回の起動時に自動的にツールに取り込まれます。また、送信先リストデータにデータが取り込まれている状態で訓練メール本文の編集を行うと、以下の図の例のように、「HTML 版のプレビュー」欄に表示されるデータに、送信先リストデータに設定されているデータが反映されます。



標的型攻撃メール対応訓練実施キット 訓練メール作成支援ツール 評価版 Ver.2021.11.01.01

本ツールは、標的型メール訓練で使用する訓練メールの作成を支援するツールです。
本ツールを使用することにより、訓練メールをeml形式ファイルで出力する、
また、訓練メール送信サービスにアップロードするZipファイルを作成することができます。

ツールを終了する

訓練実施パターン 訓練メール本文の編集 送信先リストデータ パスワード通知メール本文の編集 添付ファイルの選択 訓練メールの出力・Zipファイルの生成 SMTPサーバへの送信 ライセンス認証設定

メールマスタデータ(CSVデータ)のファイルパス E:\Test\MailMaster.csv メールアドレスデータ(CSVデータ)を取り込む

出力結果	メールアドレス	出力順	本文パターン	氏名	突合キー	埋込文字1	埋込文字2	埋込文字3
▶	test1@hoge.jp	1	本文パターン1	田中一郎	a0001	https://o365network.com/637f7d6f8614d183bac022ce	jhehG34ed@3	
	test2@hoge.jp	2	本文パターン2	鈴木次郎	a0002	https://o365network.com/637f7d6f8614d183bac022ce	jhehG34ed@3	
	test3@hoge.jp	3	本文パターン2	山田三郎	a0003	https://o365network.com/637f7d6f8614d183bac022ce	jhehG34ed@3	
	test4@hoge.jp	4	本文パターン3	太田史郎	a0004	https://o365network.com/637f7d6f8614d183bac022ce	jhehG34ed@3	
*	test5@hoge.jp	5	本文パターン3	加藤五郎	a0005	https://o365network.com/637f7d6f8614d183bac022ce	jhehG34ed@3	

訓練メールの出力が成功した場合は、訓練
メールファイル（eml ファイル）が出力された
時刻が、エラーが発生した場合は、エラーメッ
セージが本欄に出力されます。

このボタンを押して、CSV データの取り込みを行います。

各欄のデータは、セルをクリックすることで編集することができます。

STEP3-4 訓練メール送信サービスを利用して訓練メールを送る

自社で用意した SMTP サーバを利用する代わりに、訓練メール送信サービス (<https://mss.kunrenkit.jp/SMTPUpload.aspx>) を利用して訓練メールを送信する場合は、「[標的型メール訓練実施用サーバご利用ガイド.pdf](#)」に記載の手順に従って、送信したい訓練メールをサーバにアップロードしていただくことで、訓練メールを送信することができます。なお、訓練メール送信サービスを利用するメリットとして、以下の点があります。

1. 訓練メール送信サービスで用意・提供している独自ドメインを使ったメールアドレスを差出人アドレスとして使える。

訓練メール送信サービスで送信できるメールの From アドレスには、インターネット上に実在するドメイン名（DNS 参照が可能なドメイン名）を用いたメールアドレスを設定することができます。また、SPF (Sender Policy Framework)レコード（SPF とは電子メールの送信元ドメインが偽称されていないかを検査するための仕組みです）が設定されているドメイン名として、以下のドメイン名を用いたメールアドレスを、送信元のメールアドレスとして使用することができます。

【SPF レコードが設定されているドメイン名】(2022 年 9 月時点)

- 1) stresscheck.work 2) o365network.com 3) ux1.co 4) tstrading.biz 5) Office365microsoft.com 6) efaxprint.com 7) 0365microsoft.com
- 8) securitysystemcenter.com 9) 7ejd4ked95sak983ncvys847fhe4wjzuyt3s94jr64dsq2763.com 10) jcb-cards.com 11) smbc-banks.com
- 12) paypay-banks.com 13) rakuten-cards.com 14) doropbox-online.com 15) newdocs.zip 16) announce.zip

2. 指定の時間に訓練メールを送信できる。

訓練メール送信サービスでは、訓練メールの送信時刻を指定することができます。例えば、早朝に訓練メールを送りたいような場合、早朝の送信時刻を指定して訓練メールを送るようにすれば、早朝に訓練メールを送るために、わざわざ前の晩から会社に泊まり込んで対応するといった必要はなくなります。

3. SMTP サーバを自社で用意しなくともよい。

訓練メール送信サービスを利用すれば、訓練メールの送信を行うための SMTP サーバを自社で用意する必要がなくなります。

自社で使えるメールサーバは Office365 で提供されるメールサーバしか無いなど、訓練メール送信用に利用できる SMTP サーバを持っていない組織でも、訓練メール送信サービスを利用することで、自分で訓練メールを送信することができます。

4. ファイアウォールの穴あけをする必要が無い。

自社内に訓練メールの送信に利用できる SMTP サーバが無い場合、社外の SMTP サーバを利用して訓練メールを送信することになりますが、社内から社外へのアクセスはファイアウォールによって制限されていて、社内のパソコンから社外の SMTP サーバに対しては接続することができないという環境でも、訓練メール送信サービスを利用すれば、お手持ちの Web ブラウザを使って訓練メールの送信を設定することができます。

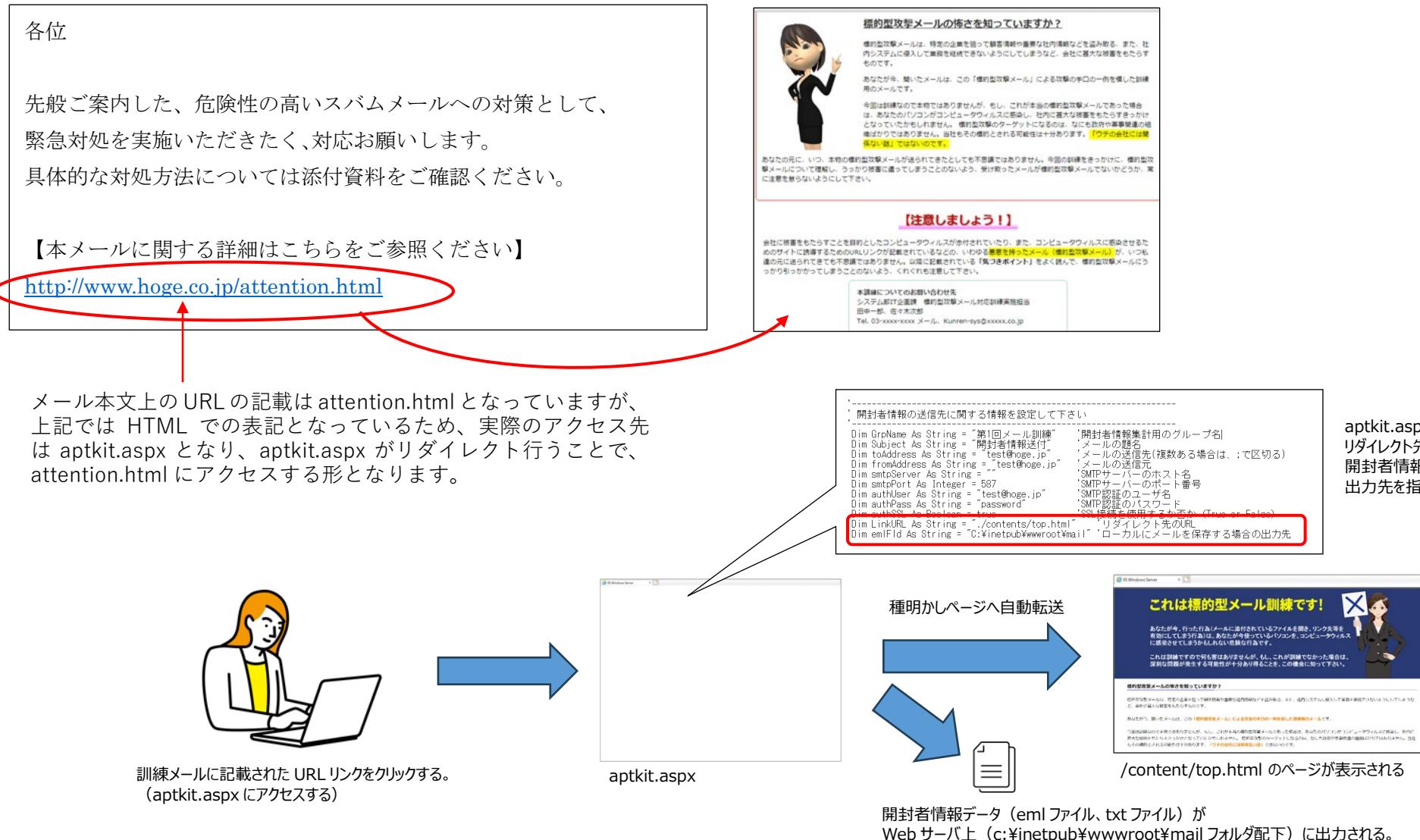
訓練メール送信サービスでは、Web ブラウザを用いて、送信を行う訓練メールをサーバにアップロードする形となるため、ファイアウォールの設定変更を行うといった面倒な作業を行わなくとも、訓練メールの送信を行うことができます。

訓練メール送信サービスの具体的な利用方法については、キットに付属の「[訓練メール送信サービスご利用マニュアル.pdf](#)」をご参照ください。

STEP4 訓練メール本文中の URL リンクがクリックされる

STEP3 で送付した訓練メールの本文中に記載された URL リンクがクリックされることで、STEP1 で設定した Web サーバへのアクセスが発生し、URL リンクをクリックした方の情報が「開封者情報」データとして出力されます。aptkit.aspx もしくは、aptkit.php を利用される場合は、開封者情報のデータについては、データとして出力する以外に、メールとして指定のアドレス宛に送信することもできます。

メール本文中に記載されている URL がクリックされると、訓練対象者のパソコン上で Web ブラウザが起動し、リンク先に設定された aptkit.aspx が呼び出されますが、aptkit.aspx は LinkURL で指定した URL にリダイレクトを行うので、訓練対象者はリダイレクト先の URL に指定されたページを参照することになります。



STEP5 開封者情報の取得

STEP4 で Web サーバから出力、または送信された開封者情報のデータを取得します。STEP6 で行う開封者情報の集計は、ここで取得する開封者情報のデータを元に行うことになります。

キットに付属の「開封者情報集計ツール」では、Web サーバから出力される、eml 形式 (aptkit.aspx を使う場合) または、テキスト形式 (aptkit.php を使う場合) の開封者情報データを取り込む形で集計を行います。開封者情報のデータを Web サーバ内に出力せず、メールで受信する運用としている場合は、メールで受信した開封者情報データを eml 形式のデータに出力することで、開封者情報集計ツールを用いて開封者情報の集計を行うことができます。

【開封者情報をメールで受信する設定】

```
'-----  
' 開封者情報の送信先に関する情報を設定して下さい  
Dim GrpName As String = "第1回メール訓練"  
Dim Subject As String = "開封者情報送付"  
Dim toAddress As String = "test@hoge.jp"  
Dim fromAddress As String = "test@hoge.jp"  
Dim smtpServer As String = ""  
Dim smtpPort As Integer = 587  
Dim authUser As String = "test@hoge.jp"  
Dim authPass As String = "password"  
Dim authSSL As Boolean = true  
Dim LinkURL As String = "/content/top.html"  
Dim emlFld As String = "C:\inetpub\wwwroot\Mail" ' ローカルにメールを保存する場合の出力先  
'-----  
' 開封者情報集計用のグループ名  
' メールの題名  
' メールの送信先(複数ある場合は、;で区切る)  
' メールの送信元  
' SMTPサーバーのホスト名  
' SMTPサーバーのポート番号  
' SMTP認証のユーザ名  
' SMTP認証のパスワード  
' SSL接続を使用するか否か (True or False)
```

aptkit.aspx (または aptkit.php) 内にある、SMTP サーバーに関する情報 (左図の赤枠部分) を設定すると、開封者情報を指定のメールアドレス宛に送信することができます。

toAddress に指定できるメールアドレスは 1 つのみとなるため、複数のアドレス宛に開封者情報のメールが送信されるようにしたい場合は、メーリングリストのアドレスを指定頂くか、複数のメールアドレス宛にメールが送信されるよう、ご自身でプログラムを書き換えるなどしてください。

開封者情報をメールで受信する必要が無い場合は、smtpServer の値を空欄にします。

開封者情報をファイルとして出力する場合は、emlFld に、開封者情報データの出力先フォルダを指定します。

なお、キットが提供する「URL 転送」機能を利用される場合は、開封者情報データ (Zip ファイル) は、「URL 転送」機能の設定ページからダウンロードすることになります。詳しくは、「訓練メール送信サービスご利用マニュアル」をご参照ください。「URL 転送」機能を利用される場合は、開封者情報をメールで送信することはできません。

【開封者情報をメールで受信するようにする際の注意点】

開封者情報をメールで受信する場合、以下のようなことが起きうることが想定されますので、開封者情報をメールで受信する設定にするかどうかは、事前にご検討頂くことをお勧めします。

1. UTM やセキュリティ対策ソフトなどによる訓練メールの検閲 (スキャニング) により、訓練メール内や添付ファイル内に記載されている URL に対し、アクセスが行われる事があります。製品によっては、機器を通過する全ての訓練メールを対象にアクセスを発生させることができますので、例えば、1,000 通の訓練メールを送付した場合、1,000 通の開封者情報メールが送られてくるといった結果となることがあります。
2. メールサーバによっては、一定時間内に受信できるメールの通数を制限している場合があり、制限を超える開封者情報のメールが送られてきた場合、受信ができなくなってしまうことが想定されます。例えば、Exchange Online では、スパムメール対策のため、それぞれのメールボックスに対して受信制限が設けられており、受信数が 1 時間に 3,600 通を超えるとブロックされ、1 時間経過をしないと受信ができないといった制限が設けられています。

開封者情報をメールで受信できるようにすることは、リアルタイムに開封者を確認することができるということで、便利ではありますが、UTM やセキュリティ対策ソフトなどによるメールのスキャニングが当然のように行われるようになった現在では、開封者情報をメールで受信するようにすることは、大量の開封者情報メールが送られてきてしまう可能性があり得るため、あまりお勧めできないというのが実状なので、開封者情報については、ファイルに出力する設定とされることをお勧めします。

STEP6-1① 開封者情報集計ツールによる開封者情報の集計

STEP5で受信した開封者情報のメールについては、キットに付属の「開封者情報集計ツール」を利用して集計を行います。

開封者情報集計ツールでは、aptkit.aspxが出力する eml 形式の開封者情報データ、もしくは、aptkit.phpが出力する txt 形式の開封者情報データを取り込んで集計を行います。開封者情報をメールソフトで受信する方法を選択されている場合は、開封者情報のメールを eml 形式のファイルに出力して「開封者情報集計ツール」で集計を行う流れとなります。

開封者情報集計ツールによる開封者情報の集計については、次のようにします。

① 開封者情報データが保存されているフォルダを指定する

集計対象とする開封者情報データが保存されているフォルダを指定します。

② 開封者情報データを開封者情報集計ツールに取り込む

開封者情報集計ツールの「フォルダ選択」ボタンを押して、URL 転送機能のページからダウンロードした、開封者情報が含まれる zip ファイルが保存されているフォルダを選択します。

③ ユーザマスタデータを開封者情報集計ツールに取り込む

開封者情報集計ツールの「ユーザマスタ情報を取り込む」ボタンを押して、前ページの手順で作成したマスタデータを開封者情報集計ツールに取り込みます。

④ 集計結果データを出力する先となるフォルダを設定する

開封者情報集計ツールの「出力先フォルダ選択」ボタンを押して、集計結果データを出力する先となるフォルダを選択します。

⑤ 開封者情報の開封時刻を補正する場合は、補正する時刻を設定する

URL 転送サービスで記録される開封時刻は日本時間となるため、海外の拠点に居る方を対象に訓練を行う場合など、集計結果データに出力される「開封時刻」の情報を、現地の時間に合わせて補正する必要がある場合は、補正する時間を選択します。日本国内を対象とした訓練の場合は補正を行わ必要はありません。

⑥ 開封者情報の集計を実行する

「開封者情報の集計を行う」ボタンを押して、開封者情報の集計を行います。

この際、URL 転送機能のページからダウンロードした、開封者情報が含まれる zip ファイルは解凍する必要はありません。

「開封者情報の集計を行う」ボタンを押すことで出力される集計結果データ（ResultData.csv）は、**標的型攻撃メール対応訓練実施キットに付属の ResultData 整形ツール.xlsxm** に取り込むことで、Excel のシート上に、整形された集計結果データとして出力することができます。



STEP6-1② 開封者情報集計ツールによる開封者情報データの取り込み

標的型攻撃メール対応訓練実施キットに付属の開封者情報集計ツール（AptAggregationTool.exe）に開封者情報データを取り込むには、集計対象とする開封者情報データが保存されているフォルダを指定し、「開封者情報データを取り込む」ボタンを押してください。この際、集計対象とする開封者情報データファイルの中に、同一時刻に同一内容の開封者情報データが存在する場合、「重複している開封者情報データ（同一時刻・同一内容の開封者情報データ）を除外する」にチェックを入れておくことで、重複するデータがツールに取り込まれてしまうことを防ぐことができます。（デフォルトではチェックが入っています）

開封者情報集計ツールに取り込むことのできるデータは以下の4種類です。

1. ファイルの拡張子が.eml であるファイル（キットに付属の aptkit.aspx ファイルで出力される開封者情報データファイル）
2. ファイルの拡張子が.txt であるファイル（キットに付属の aptkit.php ファイルで出力される開封者情報データファイル）
3. ファイルの拡張子が.zip であるファイル（URL 転送サービスよりダウンロードできる開封者情報データファイル）
4. メールソフトで受信した開封者情報データ（ファイルの拡張子が.msg であるファイル）

開封者情報データを取り込むと、「開封者情報データ」タブに、取り込んだデータが出力されます。

取り込んだデータは「開封者情報取得日時」の順に表示されます。

グループ名	交換キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス	役職	ユーザー情報3
2020年度第1回目訓練	001	古河国彦	役員		kunihiko300@tuliba.jpw	社長	
2020年度第2回目訓練	002	米山吉太郎	役員		seitarou2326@tuliba.jpw	取締役	
2020年度第3回目訓練	003	川田結羽	製造部	第一工場	yuu610@yjdworks.jp	工場長	

取り込んだデータに合わせて、「集計設定」タブにある開封時刻の開始点と終了点の時刻が自動で設定されます。

■集計対象期間の指定
開封時刻が 2021/01/18 10:29:14 ~ 2021/01/20 10:29:14 の期間内にあるものを対象に集計を行う。
同一内容の開封者情報について、時間差が右欄で指定した分数以内である場合は同一の開封者情報とみなす 3 分以内

開封者情報集計ツールの使い方

開封時刻の補正設定
開封者情報に記録される開封時刻を、現地の時間に補正したい場合は以下の選択肢から、補正したい時間を選択してください。

補正しない(記録された時刻そのまま使う)

取り込んだ開封者情報データには、UTM やウィルス対策ベンダーのサーバからのアクセスなど、セキュリティ対策機器が機械的にアクセスを行ったことで発生してしまう開封者情報データが含まれることがあるため、「開封者情報データ」タブに出力されている開封者情報のアクセス元の IP アドレスなどを確認し、集計対象から除外すべきデータが無いかどうかを確認してください。

なお、前ページ⑤に記載の通り、開封者情報取得日時に表示される時刻を補正したい場合は、補正したい時刻を選択することで、「開封者情報データ」タブに表示されるデータの開封者情報取得日時を補正することができます。

STEP6-1③ 開封者情報集計ツールにマスタデータを取り込む

標的型攻撃メール対応訓練実施キットに付属の開封者情報集計ツール（AptAggregationTool.exe）で開封者情報の集計を行うには、取り込んだ開封者情報データと、開封者の情報（氏名や所属情報など）を紐づけるためのマスタデータをツールに取り込んでおきます。

マスタデータ（MasterData.csv）は、**キットに付属の開封者情報集計ツール用ユーザマスタ CSV ファイル作成ツール.xlsxm** を用いて作成することができます。

The screenshot shows the 'User Master CSV File Creation Tool' interface. The main window title is '開封者情報集計用ユーザマスタCSVデータ生成ツール' and the version is 'Ver.2020.09.04.01'. A blue header bar contains the text 'ユーザマスタCSVファイルを作成する'. Below the header, there is a note in Japanese explaining the tool's purpose: '本ツールは、標的型攻撃メール対応訓練実施キットに付属の「開封者情報集計ツール（AptAggregationTool.exe）」に取り込む「ユーザマスタ用CSVデータファイル」を生成するツールです。' and '本ツールの8行目から下にデータを記載し、「ユーザマスタCSVファイルを作成する」ボタンを押すと、本ツールが保存されているフォルダと同じ場所にユーザマスタ用CSVデータファイル（MasterData.csv）を出力します。' A red box highlights the note 'これらの各項目については、自由な項目名を設定できます。' (The names of these items can be freely set). The main table has columns: グループ名 (Group Name), 突合キー情報 (Match Key Information), 訓練実施対象者氏名 (Trainee Name), 第一所属部署名 (First Department Name), 第二所属部署名 (Second Department Name), メールアドレス (Email Address), 役職 (Position), ユーザー情報3 (User Information 3), ユーザー情報4 (User Information 4), and ユーザー情報5 (User Information 5). The table contains 14 rows of data. To the right, a separate window titled 'ユーザマスタ情報の設定' (User Master Information Settings) shows a note about importing user master data from a CSV file and a button labeled 'ユーザマスタ情報を取り込む' (Import User Master Data).

マスタデータ（MasterData.csv）は、開封者情報集計ツール用ユーザマスタ CSV ファイル作成ツール.xlsxm の「ユーザマスタ CSV ファイルを作成する」ボタンを押すことで出力することができます。

出力したマスタデータ（MasterData.csv）は、開封者情報集計ツールの「ユーザマスタ情報を取り込む」ボタンを押して、取り込む対象とするマスタデータを選択することで、ツールに取り込みを行うことができます。

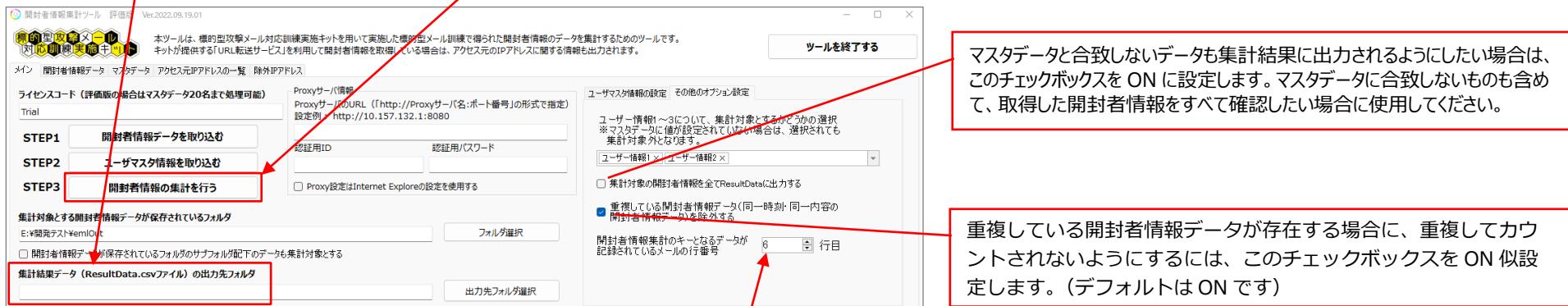
取り込んだデータはツールの「マスタデータ」タブに表示されます。取り込んだデータについては、セルを選択することで修正することもできます。

The screenshot shows the 'AptAggregationTool' interface. The main window title is '開封者情報集計ツール 製品版 Ver.2021.03.02.01'. A note in the center says: '本ツールは、標的型攻撃メール対応訓練実施キットを用いて実施した標的型メール訓練で得られた開封者情報のデータを集計するためのツールです。' A button 'ツールを終了する' (Exit Tool) is visible. The bottom navigation bar includes tabs: メイン (Main), 開封者情報データ (Open Envelope Data), マスタデータ (Master Data), and アクセス元IPアドレスの一覧 (List of Access Source IP Addresses). The 'Master Data' tab is selected, showing a table with columns: グループ名 (Group Name), 突合キー情報 (Match Key Information), 訓練実施対象者氏名 (Trainee Name), 第一所属部署名 (First Department Name), 第二所属部署名 (Second Department Name), メールアドレス (Email Address), 役職 (Position), ユーザー情報3 (User Information 3), and ユーザー情報4 (User Information 4). The table contains 4 rows of data.

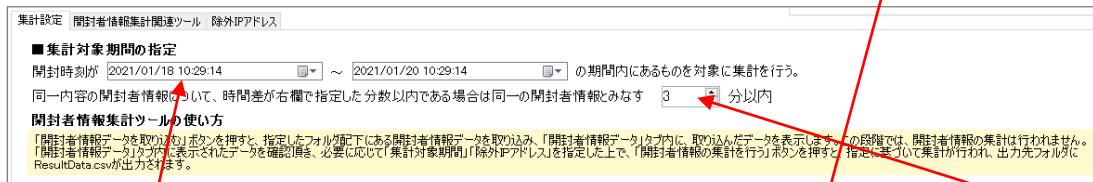
「マスタデータ」タブ上で修正したデータは、「ユーザマスタ情報を出力する」ボタンを押すことで、MasterData.csv ファイルとして出力することができます。

STEP6-1④ 開封者情報集計ツールによる開封者情報の集計

標的型攻撃メール対応訓練実施キットに付属の開封者情報集計ツール（AptAggregationTool.exe）で開封者情報の集計を行うには、「開封者情報データを取り込む」ボタンを押して開封者情報データを取り込んだ上で、「開封者情報の集計を行う」ボタンを押してください。「開封者情報の集計を行う」ボタンを押すと、「出力先フォルダ選択」で指定したフォルダ配下に、集計結果ファイルとして、ResultData.csv ファイルが出力されます。



集計結果データ（ResultData.csv）は、**標的型攻撃メール対応訓練実施キットに付属の ResultData 整形ツール.xlsxm** に取り込むことで、Excel のシート上に、整形された集計結果データとして出力することができます。



なお、「開封者情報の集計を行う」ボタンを押す前に、以下の作業を行って下さい。

① 集計対象期間の設定

集計対象期間を設定することで、ツールに取り込んだ開封者情報のうち、指定した期間内にあるデータのみを集計対象とすることができます。また、同一の開封者が複数回添付ファイルを開いたりした場合など、同一人物による開封者情報データが、一定時間内に複数出力されている場合は、「〇分以内」の数値を設定することで、最初に見つかった開封者情報データの開封時刻から指定した分数以内にあるデータを集計対象から除外して集計を行うことができます。

② 突合キー情報が記録されている行番号の設定（デフォルトは 6 に設定されています）

開封者情報とマスタデータの紐付けに際しては、突合キー情報を元に行われます。マスタデータの「突合キー情報」に相当するデータが、開封者情報データの何行目に表示されているかを指定します。URL 転送サービスを利用して開封者情報を取得している場合、及び、キットに付属の aptkit.aspx 及び aptkit.php 内のプログラムを修正されていない限りは、この値は「6」に設定して下さい。

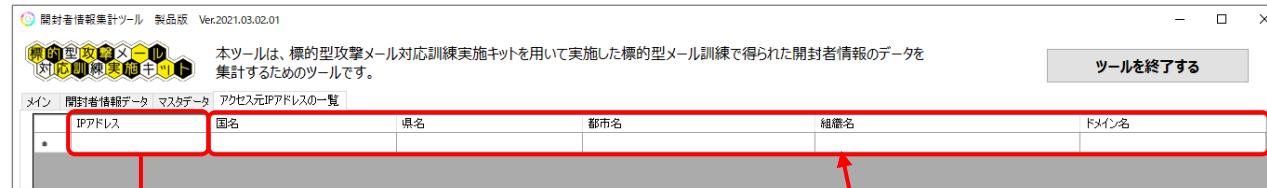
STEP6-1⑤ アクセス元 IP アドレスについて

開封者情報に含まれる「アクセス元 IP アドレス」情報については、開封者情報集計ツールの「アクセス元 IP アドレスの一覧」タブに出力されます。

訓練を実施した環境によっては、UTM やウィルス対策ソフトなどに代表されるセキュリティ対策製品やセキュリティ対策サービスが、リンク先が不正な Web サイトでないかどうかを調べるために、リンク先にアクセスを行う場合があります。このようなケースでは、訓練実施対象者がリンク先にアクセスしていないのにもかかわらず、開封者情報が出力されるという事象が発生することになります。

このため、訓練実施対象者がリンク先にアクセスしたのか？それとも、セキュリティ対策製品などによってアクセスが行われたのか？については、開封者情報に出力されたアクセス元 IP アドレス情報を元に判別を行い、セキュリティ対策製品などによってアクセスされたことによって出力されたと思われる開封者情報については、前ページの記述にある通り、「除外 IP アドレス」を指定することによって、開封者情報の集計から除外を行います。

ちなみに、「URL 転送サービス」を利用して開封者情報を収集した場合は、米国マサチューセッツ州に本社を置く MaxMind 社が提供する GeoIP2 PrecisionWeb サービス (<https://www.maxmind.com/en/geoip2-precision-city-service>) との連動により、アクセス元の具体的な情報も併せて出力されます。



この部分の情報については、「URL 転送サービス」を利用して収集した開封者情報を集計した場合に出力されます。

aptkit.aspx もしくは、aptkit.php を利用して開封者情報を出力した場合は、IP アドレス情報のみ出力されます。

アクセス元 IP アドレスが、セキュリティ対策製品やセキュリティ対策サービスの IP アドレスと思われる場合は、該当の IP アドレスを「除外 IP アドレス」欄に記載することで、開封者情報の集計対象から除外して集計を行うことができます。

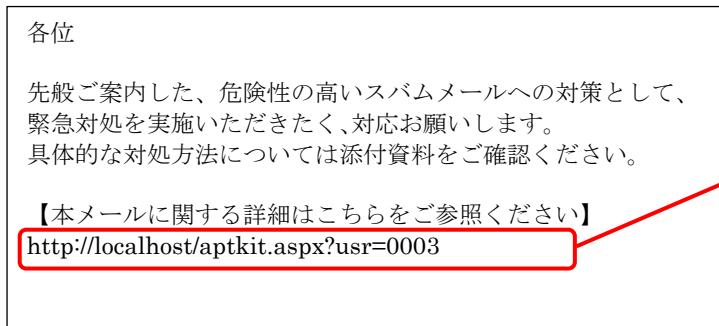


STEP6-2 開封者情報集計の仕組み

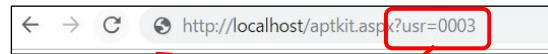
メールソフトの仕組みでは、訓練メール内の URL リンクがクリックされても、そのリンクをクリックした人が誰であるか？を示す個人情報を取得することはできません。このため、誰が URL リンクをクリックしたか？の情報を得るには、訓練メール内に記載される URL リンク自体に特定のキーワードを設定しておき、そのキーワードが含まれる URL リンクをクリックできるのは、その URL リンクを含む訓練メールを受け取った人だけ。となるようにすることで、URL リンクをクリックした人の特定を行います。

例えば、URL リンククリック型の訓練では、図のように usr=xxx の xxx の部分を集計用のキーワードとして扱うことで、例えば、0003 のキーワードを含む開封者情報メールを受信したら、それは、役員の磯野さんがクリックしたものだ。というように解釈し、集計を行います。

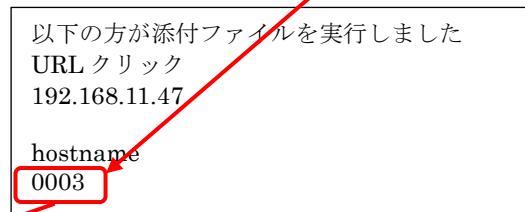
【ユーザーに送付される訓練メール】



【Web サーバへのアクセス】



【Web サーバから送付される開封者情報メール】



【開封者情報集計ツールの「ユーザマスタ」情報】

ユーザマスタ情報					
グループ名	突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス
以下の方が添付ファイルを実行しました	0001	古河国彦	役員		kunihiko306@ftlib.jp
以下の方が添付ファイルを実行しました	0002	大林敦	役員		scklmpvrvatsushi2@
以下の方が添付ファイルを実行しました	0003	磯野敬子	役員		Keiko_Isono@owhdrl
以下の方が添付ファイルを実行しました	0004	神山菜月	役員		ikamiyama@bytahk
以下の方が添付ファイルを実行しました	0005	難波灯	役員		akari44334@neivbbf
以下の方が添付ファイルを実行しました	0006	加藤祐夫	役員		ikuokase@umrqvvsr
以下の方が添付ファイルを実行しました	0007	坂新治	役員		shinji4358@yder.ryo
以下の方が添付ファイルを実行しました	0008	小杉光政	役員		mitsumasakosug@q
以下の方が添付ファイルを実行しました	0009	坂元功一	役員		Kouichi_Sakamoto@

開封者情報メールの 6 行目に記載される 0003 というキーワードを役員の磯野さんに紐づけておき、0003 が開封者情報のメールに含まれていたら、磯野さんがクリックをしたと判断します。

ユーザマスタに記載した第一所属部署名と第二所属部証明の情報を元に、所属部署毎の集計結果一覧が作成されます。

集計結果一覧					
第一所属名	対象者数	開封回数	開封率	開封者数	開封率
役員	11	2	18.18%	0	0.00%
製造部	400	7	1.75%	0	0.00%
営業部	100	2	2.00%	1	0.01%
企画部	12	0	0.00%	0	0.00%
人事部	12	0	0.00%	0	0.00%
総務部	17	0	0.00%	0	0.00%
音楽部	1	0	0.00%	0	0.00%
開発部	50	1	2.00%	1	1.98%
企画部	1	0	0.00%	0	0.00%
材料部	47	0	0.00%	0	0.00%
難波部	1	0	0.00%	0	0.00%
磯野部	1	0	0.00%	0	0.00%
益田部	1	0	0.00%	0	0.00%
佐野部	29	0	0.00%	0	0.00%
宮川部	12	0	0.00%	0	0.00%
熊谷部	13	0	0.00%	0	0.00%
上西野部	1	0	0.00%	0	0.00%
村木部	14	0	0.00%	0	0.00%
鈴木部	50	0	0.00%	0	0.00%
合計	1000	17	1.70%	4	0.40%
第二所属名	対象者数	開封回数	開封率	開封者数	開封率
役員	11	2	18.18%	0	0.00%
製造部一工場	130	4	3.08%	0	0.00%
製造部第二工場	145	1	0.7%	0	0.00%
製造部第三工場	150	2	1.33%	0	0.00%
営業部	1	0	0.00%	0	0.00%
企画部	1	0	0.00%	0	0.00%
人事部	1	0	0.00%	0	0.00%

STEP6-3 ユーザマスタ情報の作成

開封者情報集計ツールに取り込む「ユーザマスタ情報」については、キットに付属の「開封者情報集計ツール用ユーザマスタ CSV ファイル作成ツール.xlsm」を用いて作成することができます。開封者情報ツールへのユーザマスタデータの取り込みについては、以下の手順で行います。

手順1 「開封者情報集計ツール用ユーザマスタ CSV ファイル作成ツール.xlsm」を起動し、ツールの 8 行目に項目名、9 行目以降に、各突合キー情報に紐づける個人場情報を設定します。

なお、8 行目の項目名のうち、A 列～E 列は固定となります、F 列～I 列の項目名については、任意の項目名を設定することができます。

A	B	C	D	E	F	G	H	I	J	K
1	開封者情報集計用ユーザマスタ用CSVデータ生成ツール								Ver.2019.02.10.01	ユーザマスタCSVファイルを作成する
2	本ツールは、標的型攻撃メール対応訓練実施キットに付属の「開封者情報集計ツール（AptAggregationTool.exe）」に取り込む「ユーザマスタ用CSVデータファイル」を生成するツールです。									
3	本ツールの8行目から下にデータを記載し、「ユーザマスタCSVファイルを作成する」ボタンを押すと、本ツールが保存されているフォルダと同じ場所にユーザマスタ用CSVデータファイル（UserMaster.csv）を出力します。									
4	8行目の項目名のうち、セル背景色が薄黄色（E列～I列）のセルの項目名については、自由な項目名に変更することができます。									
5	これらの各項目については、自由な項目名を設定できます。									
6	グループ名	突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス	役職	ユーザー情報 3	ユーザー情報 4	ユーザー情報 5
7	以下の方が添付ファイルを実行しました	0001	古河国彦	役員		kunihiko306@ftluliba.lw	社長			
8	以下の方が添付ファイルを実行しました	0002	大林敦	役員		scklvmpvatsushi236@xttghg.az	副社長			
9	以下の方が添付ファイルを実行しました	0003	磯野敬子	役員		Keiko_Isono@owhdlnzczn.rvv	副社長			
10	以下の方が添付ファイルを実行しました	0004	神山菜月	役員		Ikamiyama@bytahkybiu.ka	専務取締役			
11	以下の方が添付ファイルを実行しました	0005	難波灯	役員		akari44334@neivbbfr.ao	常務取締役			
12	以下の方が添付ファイルを実行しました	0006	加瀬郁夫	役員		ikuokase@umrqvvsr.esc	常務取締役			
13	以下の方が添付ファイルを実行しました	0007	坂新治	役員		shinji4358@yder.ryo	取締役			
14	以下の方が添付ファイルを実行しました	0008	小杉光政	役員		mitsumasakosugi@piluz.nf.wy	取締役			
15	以下の方が添付ファイルを実行しました	0009	坂元功一	役員		Kouichi_Sakamoto@umdmblurp.rxrax.vj	取締役			
16	以下の方に添付ファイルを実行しました	0010	西島政成	役員		naoya_nishimura@umdmblurp.rxrax.vj	取締役			

※「開封者情報集計ツール用ユーザマスタ CSV ファイル作成ツール.xlsm」に初期設定されているデータは参考用のダミーデータです。

グループ名：開封者情報の集計単位を指定する名称を設定します。（例：第 1 回メール訓練）

ユーザマスタ内には、異なるグループ名を混在させることができますので、例えば、複数の会社を対象に訓練を実施するような場合、グループ名の情報を会社名にすることで、会社名の単位に集計結果をまとめることができます。

突合キー情報：突合キー情報には、訓練メール作成支援ツールが生成する連番（0001 など）、また、URL リンクに設定していると突合キー情報を設定します。

訓練実施対象者氏名：突合キー情報に設定した情報を含む URL リンクや添付ファイルを送付する先となる方の氏名情報を記載します。

第一所属部署名：訓練実施対象者氏名に指定した方が所属する組織の 1st 組織名（営業部や総務部など）を記載します。

第二所属部署名：訓練実施対象者氏名に指定した方が所属する組織の 2nd 組織名以降（第一営業部、第二営業部など）を記載します。組織の階層が 2 階層以上あり、第三組織や第四組織といった単位に細かく分かれている場合は、2nd 組織名以降の名称を合算した名称を記載します。

※メールアドレス以降の項目については、項目名も含め、任意のデータを設定できます。なお、開封者情報集計ツールでは、第一所属部署名の単位と、第一所属部署名 + 第二所属部署名の単位で集計を行います。

手順2 データを設定したら、「ユーザマスタ CSV ファイルを作成する」ボタンを押します。ボタンを押すと、ツールが保存されているフォルダと同じ場所にユーザマスタ用 CSV データファイル（MasterData.csv）が出力されますので、開封者情報集計ツールにこのデータを取り込みます。

STEP6-4 開封者情報集計ツールで出力した集計結果データの整形

開封者情報集計ツールで生成される集計結果は CSV データとして出力されます。これは、Microsoft Excel を使用していない組織でも開封者情報の集計ができるようになりますが、Excel をお持ちの場合は、「ResultData 整形ツール.xls」を用いることで、開封者情報集計ツールが生成した集計結果データ（ResultData.csv）を取り込み、Excel シート上に整形した結果を出力することができます。

※Excel で CSV データを開くと、先頭が 0 で始まるデータ（例:0001）は数値に自動的に変換されて「1」と表示されてしまうため、「ResultData 整形ツール.xls」をお使い頂くことで、先頭 0 の問題を回避できます。

A	B	C
1 開封者情報集計結果データ整形ツール		Ver.2019.02.12.01
2 本ツールは、標的型攻撃メール対応訓練実施キットに付属の「開封者情報集計ツール（AptAggregationTool.exe）」で出力したResultData.csvデータを取り込み、		
3 シートに展開するツールです。データの取り込みを開始すると、ResultData.csvの内容に基づき、グループ名ごとに集計結果を記録したシートが生成されます。		
4		
5 ResultData.csvの保存先フォルダ C:\Work\Test\0001\ResultData.csv		データの取り込み開始
6		
7		

手順 1 「ResultData 整形ツール.xls」を起動し、ResultData.csv が保存されているフォルダを指定して「データの取り込み開始」ボタンを押すと、開封者情報集計結果が、グループ名単位にシート化されて、ツール内に作成されます。

手順 2 作成されたデータについて、更に加工が必要な場合は、ご自身で任意の加工を行ってください。

なお、開封者情報集計ツールで作成できる集計結果データは、「開封者情報の一覧」と、「第一組織別、第一組織 + 第二組織別の開封者数と開封率の一覧」になります。

開封者情報	開封者情報名	第一組織番号	第二組織番号	ドメイン	セッション番号	ユーザID	組織名	ユーザ名	接続IP	開封者情報登録日時
1	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
2	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
3	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
4	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
5	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
6	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
7	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
8	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
9	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
10	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
11	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
12	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
13	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
14	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
15	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
16	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
17	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
18	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
19	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
20	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
21	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
22	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
23	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
24	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
25	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
26	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
27	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
28	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
29	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
30	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
31	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
32	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
33	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
34	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
35	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
36	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
37	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
38	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
39	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
40	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
41	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
42	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
43	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
44	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
45	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
46	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
47	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
48	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
49	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
50	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
51	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
52	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
53	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
54	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
55	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
56	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
57	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
58	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
59	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
60	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
61	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
62	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
63	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
64	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
65	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
66	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
67	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
68	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
69	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
70	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
71	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
72	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
73	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
74	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
75	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
76	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
77	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
78	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
79	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
80	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
81	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03:42
82	日本法人	0001	0001	日本法人	0001	0001	日本法人	0001	192.168.1.10	2019/02/28 12:03

訓練メールに記載される実際の URL リンク先を隠ぺいする方法

URL リンクリック型の訓練で用いる「`http://web サーバのアドレス/aptkit.aspx?user=xxxx`」形式の URL を訓練メールに記載したのでは、メールを見る人によっては、この URL を見ることで、訓練であるとすぐに感づかれてしまう懸念が考えられます。HTML 形式のメールを用いることで、見かけ上の URL を変えることはできますが、URL にマウスオーバーすると、実際にアクセスする先の URL がわかつてしまうため、実際の URL リンク先を隠ぺいするための方法として、短縮 URL サービスを使う、もしくは、キットが提供する「URL 転送サービス」を使うという方法があります。

短縮 URL サービスは幾つかありますが、転送先の URL として、ローカル IP アドレスが使用されている URL は指定できないなどの制限や、サービスの提供が 100% 確実に保証されるものではないこと、また、実際の攻撃メールでも利用されることから、導入しているセキュリティ対策によっては、短縮 URL 自体が、不審なサイトへのアクセスである可能性が高いと判断され、アクセス時に警告が表示される、また、サイトへのアクセスが遮断されてしまうといったこともあり得る点にご留意ください。

※短縮 URL 利用時の注意事項

短縮 URL は、実際の URL にリダイレクトするサービスであるため、短縮 URL が使えるのは、インターネットに接続できる環境のみとなります。

インターネットに接続できない環境下で訓練を実施する場合は、短縮 URL をクリックしても短縮 URL を処理するサーバにアクセスすることができず、リダイレクトができないため、実際の URL にアクセスさせることができませんのでご注意ください。

また、短縮 URL でのリダイレクトでは POST データは欠落してしまいますので、フォームから入力されたデータをリダイレクト先に渡したい場合は GET 形式にして URL にデータを含めるようにしてください。

キットの「URL 転送」機能を利用する場合は、URL 転送機能で取得した転送用 URL を訓練メールに記載する URL とし、転送用の URL から、

「`http://web サーバのアドレス/aptkit.aspx?user=xxxx`」形式の URL にリダイレクトさせるという流れとなります。

URL 転送サービスのリダイレクト機能（指定の URL に転送する機能）では、?から後の部分は、転送用 URL 取得時に設定するリダイレクト先の URL に引き継がれてリダイレクトが行われる仕様となっていますので、例えば、転送用 URL のリダイレクト先を、`http://192.168.10.11/aptkit.aspx` と設定した上で、訓練メールに記載する URL を、

`https://stresscheck.work/8ab0f5863b2d61a1ad410aa1/001?user=0001` のように設定すると、訓練メール本文中の URL をクリックしたユーザーを、

`http://192.168.10.11/aptkit.aspx?user=0001` という URL に誘導するすることができます。

添付ファイルを用いての訓練実施

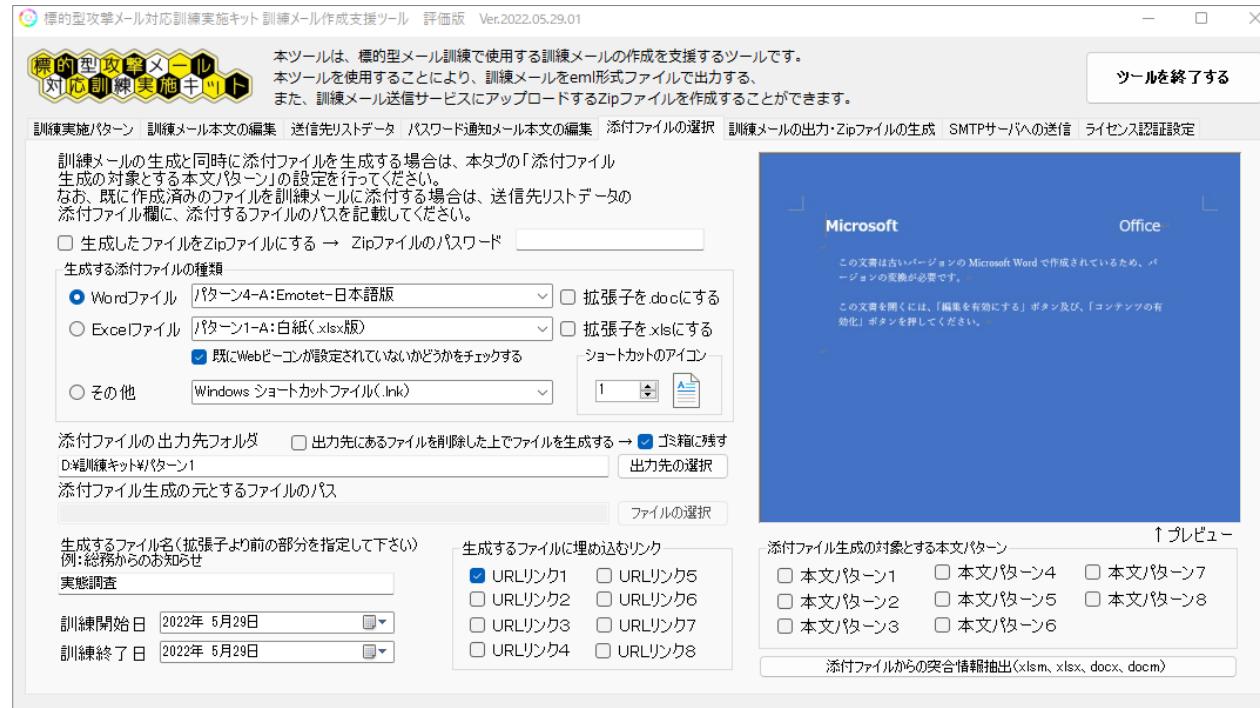
URLリンククリック型の訓練が実施できたら、次のステップとして、キットに付属のツールで作成した模擬のマルウェアファイルを、訓練メールに添付する形式の訓練を実施してみましょう。

但し、キットで作成した模擬のマルウェアファイルを添付した訓練メールを受信できるかどうか、また、受信ができたとしても、添付ファイルを開いた際に開封者情報を取得できるかどうかは、訓練を実施する環境によって異なります。

例えば、Gmailを利用しているような環境では、Gmail自体が圧縮ファイルや、特定の拡張子を持つファイルの添付を許容していないため、ファイルを添付したメールを受信できない。といったことがあります。また、添付ファイルを画像に変換してしまうようなセキュリティ対策製品を導入しているような環境では、添付ファイルを開いても開封者情報を取得できないといったことがあります。開封者情報が集計できるかどうかなど、具体的にどのような動きになるかについては、実際にやってみることで確認して下さい。

キットに付属の「訓練メール作成支援ツール」(KunrenkitTool.exe)を用いると、添付ファイル付きの訓練メールを作成することができます。

「訓練メール作成支援ツール」(KunrenkitTool.exe)の具体的なご利用方法につきましては、付属のマニュアル「[訓練メール作成支援ツールご利用ガイド](#)」をご参照ください。



添付ファイルの作成（キットに付属のツールで添付ファイルを作成する）

訓練メール作成支援ツールでは、訓練メール本文を作成するだけでなく、訓練メールに添付する模擬マルウェアファイルを作成することができます。

訓練メールに添付する模擬マルウェアファイルを作成するには、「添付ファイルの選択」タブにて、生成する添付ファイルの種類、添付ファイル内に設定するリンク先の設定などを行います。

なお、**添付ファイルの生成は、訓練メールの生成と同時に行われます。**

訓練メール作成支援ツールで作成できる添付ファイル内には、URLリンク1～8の8種類のWebビーコンリンクを設定することができますので、例えば、インターネット用のWebサーバとインターネット用のWebサーバの2箇所にアクセスするWebビーコンを設定するといったことができます。



Office 文書ファイルを開く際の警告表示について

訓練メールに添付した Word ファイルや Excel ファイルを開くと、「編集を有効にする」かどうか尋ねる警告表示と、「コンテンツの有効化」を尋ねる警告が表示されることがあります。標的型メール訓練において、訓練メールの受信者が添付ファイルを開いたかどうかを確認するための「開封者情報」を得られるのは、「編集を有効にする」かどうか尋ねる警告表示において、「編集を有効にする」ボタンを押した場合となり、添付ファイルを開いたけれど、「編集を有効にする」ボタンを押さなかった場合や、Outlook のプレビュー機能で文書の内容を閲覧しただけの場合は、「開封者情報」を得ることはできません。

訓練実施担当者からすると、添付ファイルを開いても開封したことがキャッチできないのでは意味がないということで、「警告表示が表示されないようにすることはできないか？」といった質問を頂くことは多いのですが、結論から申し上げると、**外部から意図的に警告が表示されないよう操作することはできません**。警告が表示されるのは、Microsoft Office のセキュリティ対策機能によるものなので、外部から意図的に警告を表示する・しないをコントロールできてしまったのでは、セキュリティ対策機能としての意味がないからです。

訓練実施担当者として、警告が表示されないようにしたいと思う気持ちはよくわかるのですが、現実の問題として、警告が表示される仕組みについてきちんと理解できている人はあまり多くありません。警告が表示される仕組みについてきちんと理解ができていないために、**警告が表示されても無視してボタンを押してしまったり、マクロが実行されるのは「コンテンツの有効化」ボタンを押した時だけだから、「編集を有効にする」ボタンを押してもマルウェアに感染したりしない**。と思い込んでいたりする人も少なくないというのが現実です。

Microsoft Office にセキュリティ対策機能が備わっていても、利用する人がその仕組みをきちんと理解できていないことで、折角の警告表示も無意味なものとしてしまうのでは、それは**「人的なセキュリティホール」**以外の何物でもありません。折角訓練を実施されるのであれば、警告表示が何故行われるのか？また、「編集を有効にする」かどうか尋ねる警告表示と、「コンテンツの有効化」を尋ねる警告表示のそれぞれの違いについて、利用者に正しく理解してもらえるよう、訓練実施前や実施後に行う研修の場や、訓練実施後の告知の機会などをを利用して、解説・教育する機会を持たれることを強くお勧めします。

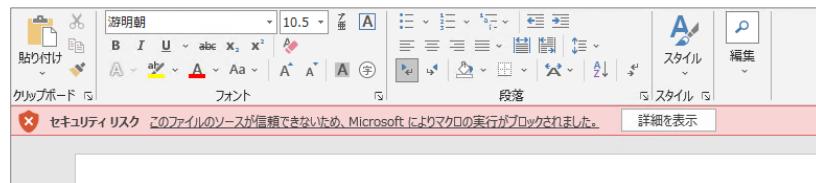
なお、本件についてはキットのサイト (<https://kit.happyexcelproject.com/keikokukaihi/>) でも解説をしていますのでご参照ください。また、Microsoft のサイト ([https://docs.microsoft.com/ja-jp/previous-versions/office/office-2013-resource-kit/ee857087\(v=office.15\)?redirectedfrom=MSDN](https://docs.microsoft.com/ja-jp/previous-versions/office/office-2013-resource-kit/ee857087(v=office.15)?redirectedfrom=MSDN)) も併せて参考されることをお勧めします。

The screenshot shows two Microsoft Office applications. On the left is Microsoft Word, displaying a document named 'becon.docx' with a warning message about potential viruses. A red arrow points from this message to a callout box on the right. The callout box contains the text: '「編集を有効にする」ボタンと、「コンテンツの有効化」ボタンが表示される仕組み、また、2つのボタンの違いについて、あなたは従業員の方々にきちんと説明できるでしょうか？' (What are the differences between the 'Enable Editing' button and the 'Enable Content' button, and can you explain them clearly to your employees?). On the right is Microsoft Excel, showing a warning that macros are disabled. The bottom of the Excel window has a note about compatibility with old versions.

Office 文書ファイルにおけるマクロの実行について

2022年7月以降、Microsoft Office のセキュリティ対策措置として、インターネットから入手した Office ファイルについては、デフォルトでマクロを実行することができないようになりました。このため、VBA マクロが設定された Word や Excel ファイルを訓練メールに添付した場合、訓練メールに添付されているファイルを開いても「コンテンツの有効化」ボタンは表示されず、マクロを実行するには、ファイルのプロパティを開いて、セキュリティ設定を許可する必要があります。

マクロの実行可否を外部からコントロールすることはできませんので、デフォルトでマクロが実行できないよう、Office のバージョンアップが適用されている環境では、強制的にマクロを実行させるようにすることはできることになります。



デフォルトでは、このようにマクロの実行がブロックされます。



「許可する」にチェックを入れないと
マクロを実行することは不可になります。

ファイルのプロパティにおいてセキュリティを許可する
設定にすると、「コンテンツの有効化」ボタンが表示
されるようになります。

なお、「編集を有効にする」ボタンは表示されますので、「編集を有効にする」ボタンを押したかどうか？については、開封者情報として記録することは可能です。

ファイルのプロパティにおいて、セキュリティを許可する設定にしても、「コンテンツの有効化」ボタンを押さない限りは、マクロは実行されません。マクロを実行するには、「ファイルのプロパティ設定でセキュリティを有効にする」→「編集を有効にする」→「コンテンツの有効化」のステップが必要になります。

添付ファイルを用いる場合の開封者情報集計

キット評価版及び、ベーシック版のライセンスでは、添付ファイルに設定される突合キー情報は 0001～9999 までの固定値となり、任意の ID は設定できません。

添付ファイルに設定される突合キー情報は、「訓練メール作成支援ツール」(KunrenkitTool.exe) が生成したフォルダ名（0001、0002 などのフォルダ名）と同じものが設定されますので、訓練メールに「訓練メール作成支援ツール」で作成したファイルを添付する場合、開封者情報集計ツールの突合キー情報には、0001、0002、0003 というように、0001 から始まる ID を設定します。

ユーザマスタ情報

グループ名	突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス
以下の方が添付ファイルを実行しました	0001	古河国彦	役員		kunihiro306@ftliliba.lw
以下の方が添付ファイルを実行しました	0002	大林敦	役員		scklvmpvatsushi236@xttghg.az
以下の方が添付ファイルを実行しました	0003	磯野敬子	役員		Keiko_Isono@owhldnzcqnn.vv
以下の方が添付ファイルを実行しました	0004	神山葉月	役員		ikamiyama@bytahkybiu.ke
以下の方が添付ファイルを実行しました	0005	難波灯	役員		akari44334@neivbbf.rao
以下の方が添付ファイルを実行しました	0006	加瀬郁夫	役員		ikuokase@umrqvvsr.esc
以下の方が添付ファイルを実行しました	0007	坂新治	役員		shinji4358@yder.ryo
以下の方が添付ファイルを実行しました	0008	小杉光政	役員		mitsumasakosugi@pilzuz.nf.wy
以下の方が添付ファイルを実行しました	0009	坂元功一	役員		Kouichi_Sakamoto@umdbclurp.rxarx.vj

※Excel では 0001 と入力すると、自動的に数値に変換されて 1 に置き換わってしまうため、セルに 0001 と入力する場合は、先頭にシングルクオーテーションを付け、「'0001」と入力するようにして下さい。「'0001」と入力することで、文字列での入力と判断され、数値に変換されてしまうのを防ぐことができます。

開封者情報集計用ユーザマスタ用CSVデータ生成ツール						ユーザマスタCSVファイルを作成する					
1	Ver.2019.02.10.01										
2	本ツールは、標的型攻撃メール対応訓練実施キットに付属の「開封者情報集計ツール（AptAggregationTool.exe）」に取り込む「ユーザマスタ用CSVデータファイル」を生成するツールです。										
3	本ツールの8行目から下にデータを記載し、「ユーザマスタCSVファイルを作成する」ボタンを押すと、本ツールが保存されているフォルダと同じ場所にユーザマスタ用CSVデータファイル（UserMaster.csv）を出力します。										
4	8行目の項目名のうち、セル背景色が薄黄色（E列～I列）のセルの項目名については、自由な項目名に変更することができます。										
5	これらの各項目については、自由な項目名を設定できます。										
6	グループ名	突合キー情報	訓練実施対象者氏名	第一所属部署名	第二所属部署名	メールアドレス	役職	ユーザー情報 3	ユーザー情報 4	ユーザー情報 5	
7	以下の方が添付ファイルを実行しました	0001	古河国彦	役員		kunihiro306@ftliliba.lw	社長				
8	以下の方が添付ファイルを実行しました	0002	大林敦	役員		scklvmpvatsushi236@xttghg.az	副社長				
9	以下の方が添付ファイルを実行しました	0003	磯野敬子	役員		Keiko_Isono@owhldnzcqnn.vv	副社長				
10	以下の方が添付ファイルを実行しました	0004	神山葉月	役員		ikamiyama@bytahkybiu.ke	専務取締役				
11	以下の方が添付ファイルを実行しました	0005	難波灯	役員		akari44334@neivbbf.rao	常務取締役				
12	以下の方が添付ファイルを実行しました	0006	加瀬郁夫	役員		ikuokase@umrqvvsr.esc	常務取締役				
13	以下の方が添付ファイルを実行しました	0007	坂新治	役員		shinji4358@yder.ryo	取締役				
14	以下の方が添付ファイルを実行しました	0008	小杉光政	役員		mitsumasakosugi@pilzuz.nf.wy	取締役				
15	以下の方が添付ファイルを実行しました	0009	坂元功一	役員		Kouichi_Sakamoto@umdbclurp.rxarx.vj	取締役				
16	以下の方が添付ファイルを実行しました	0010	坂元功一	役員		koichi.sakamoto@umdbclurp.rxarx.vj	取締役				

オフライン環境もしくはツールが対応していない環境下でのツール起動方法

キットに付属の「訓練メール作成支援ツール」及び、「開封者情報集計ツール」については、インターネットに接続してライセンスの有効性確認が行われます。インターネットへの接続が禁止されている環境下、また、Socks プロキシなど、ツールが対応していない環境下ではインターネットへの接続に失敗するため、ライセンスの有効性確認が行えません。このため、インターネットに接続ができない環境下において製品版のツールをご利用になられる場合は、以下の方法にてツールを起動願います。

※評価版としてツールを起動する場合は、インターネットに接続しているか否かに関係なく起動が可能です。

【オフライン環境下でのツールの起動手順】

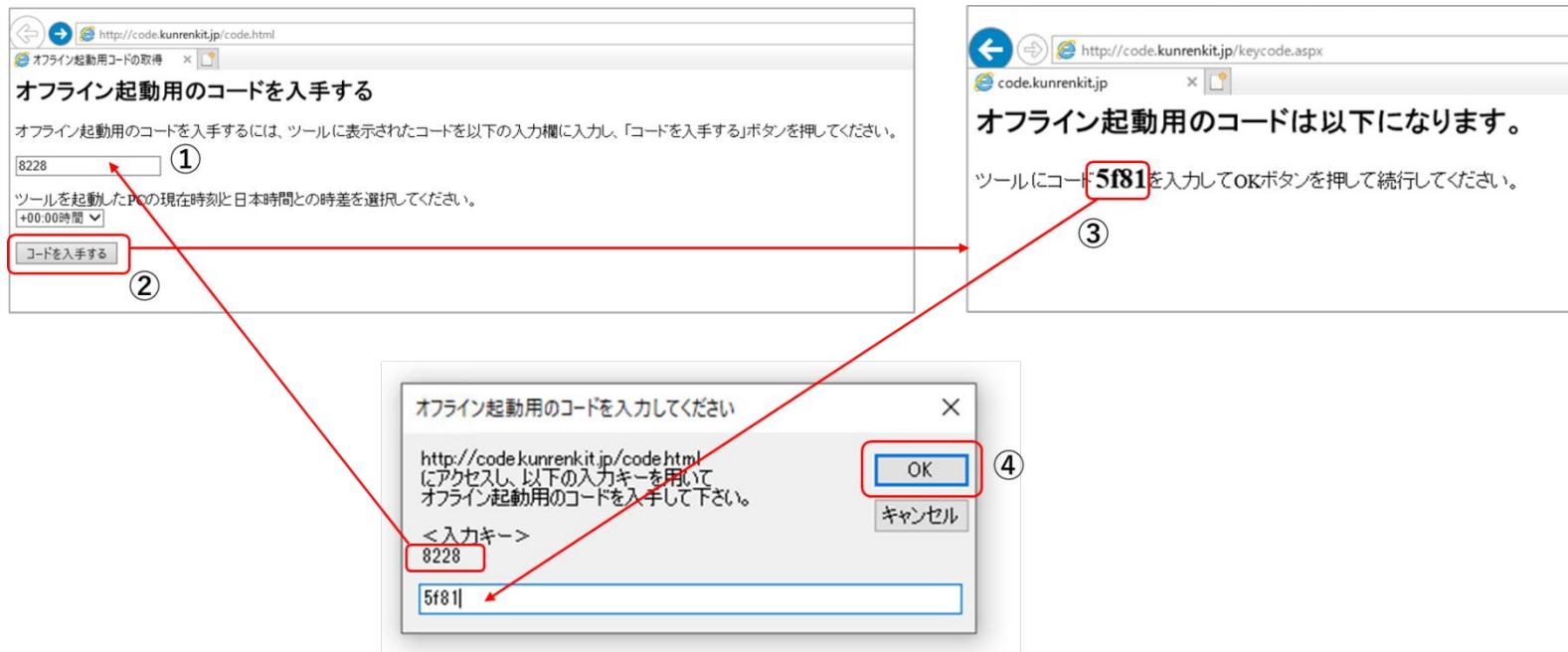
STEP1 : ask@kunrenkit.jp宛に、オフライン起動用のライセンスコードファイル（KitLicense.lcx）をリクエストしてください。折り返し、KitLicense.lcx ファイルをお送りさせて頂きます。

STEP2 : KitLicense.lcx ファイルを受領されたら、ツールが保存されているフォルダと同じフォルダ内に KitLicense.lcx ファイルを置いてください。

STEP3 : ツールをダブルクリックして起動します。（評価版として起動してしまった場合は、ライセンスコードをツールに設定して「ツールを終了する」ボタンを押し、一旦終了後に再起動してください）

STEP4 : ライセンスコードファイルの認証が通過すると、オフライン起動用のコード入力ダイアログが表示されますので、スマートフォンなどを使って <https://code.kunrenkit.jp/code.html> にアクセスし、オフライン起動用のコード入力ダイアログに表示される「入力キー」を用いて、オフライン起動用のコード入手してください。（以下の図の①②の手順）

STEP5 : 入手したオフライン起動用のコードをダイアログに入力（以下の図の③の手順）すると、コードの確認が行われ、コードの認証が完了すると、ツールが起動します。この際、コードの確認に3回失敗すると、評価版としてツールが起動されます。



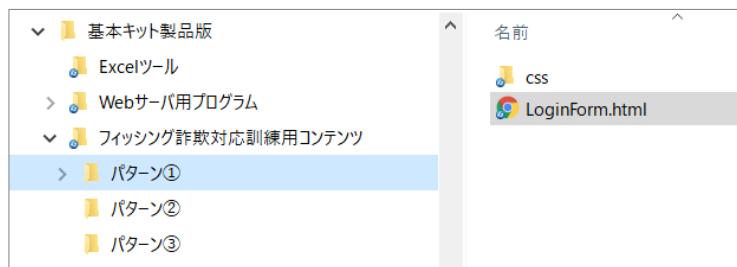
フィッシング詐欺対応訓練の実施①

キットでは、標的型攻撃メール（添付ファイルを開かせようしたり、メール本文中の URL リンクをクリックさせようとするメール）に対応する訓練だけでなく、偽のログインページにアクセスさせ、ログイン ID やパスワードを窃取しようとするフィッシング詐欺に対応する訓練も実施することができます。

フィッシング詐欺対応訓練の実施は、URL リンククリック型の訓練の応用パターンとなり、aptkit.aspx（又は aptkit.php）の設定変更と、フィッシング詐欺対応訓練用の Web コンテンツファイルを Web サーバに設定することで実施することができます。

手順 1 フィッシング詐欺対応訓練用の Web コンテンツファイルを編集する。

キットにはフィッシング詐欺対応訓練用の Web コンテンツファイルとして、標準で 3 種類のコンテンツが付属しています。これらのコンテンツの中から、訓練で使用したいパターンを選び、フォルダ内にある「LoginForm.html」について、以下の編集を行います。



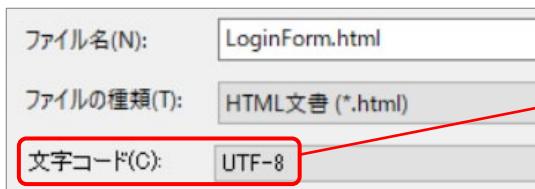
```
1 <!DOCTYPE html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
4 <link href="/css/bootstrap.css" rel="stylesheet" id="bootstrap-css">
5 <link href="/js.maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
6 <script src="/cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
7 <script src="/cdnjs.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
8 </head>
9 <body>
10 <script>
11 function setFormData(f) {
12     var key = localStorage.getItem('key');
13     f.uid.value = key;
14     return true;
15 }
16 </script>
17 <div class="wrapper fadeInDown">
18     <div id="formContent">
19         <form action="http://localhost/aspkit.aspx" method="post" onsubmit="return setFormData(this)">
20             <h2 style="margin-top:20px">ログイン</h2>
21             <input type="text" id="pass" class="fadeIn third" name="login" placeholder="login">
22             <input type="hidden" name="uid" value="1" />
23             <input type="submit" class="fadeIn fourth" value="次へ" />
24         </form>
25     </div>
26 </div>
```

この部分を編集します。

```
18 <div class="wrapper fadeInDown">
19     <div id="formContent">
20         <form action="http://localhost/aspkit.aspx" method="post" onsubmit="return setFormData(this)">
21             <h2 style="margin-top:20px">ログイン</h2>
```

LoginForm.html をメモ帳などのテキストエディタで開き、「<http://localhost/aspkit.aspx>」の部分を、aptkit.aspx もしくは、aptkit.php を設置した Web サーバの URL に変更します。

LoginForm.html の<form action="～"の部分の編集を完了したら、UTF-8 の文字コードでファイルを保存します。



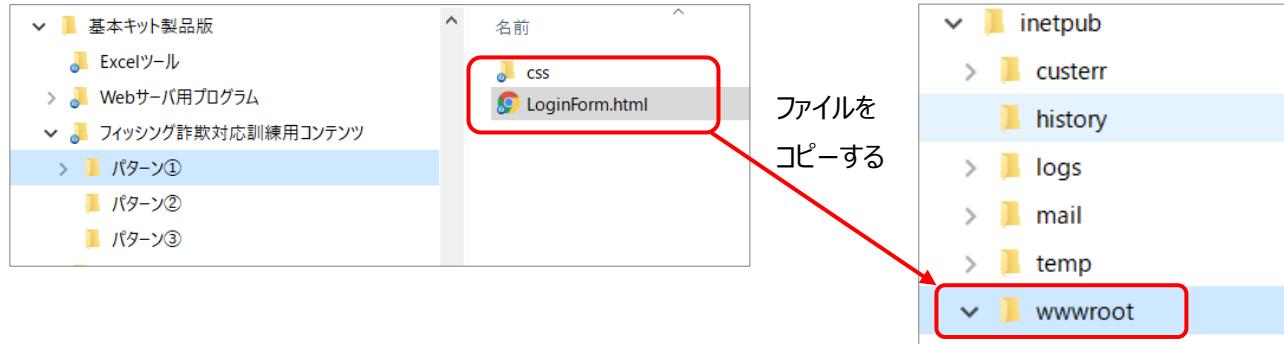
ファイルは必ず、UTF-8 で保存して下さい。

フィッシング詐欺対応訓練の実施②

手順2 手順1で編集した LoginForm.html と、css フォルダを Web サーバにコピーする。

手順1で編集した LoginForm.html と、同じフォルダ内にある css フォルダを、Web サーバにコピーします。（IIS であれば、C:\inetpub\wwwroot フォルダ配下、Apache 等の Web サーバであれば、public_html 配下）

なお、LoginForm.html のファイル名については、任意のファイル名に変更して Web サーバに設定頂いても構いません。（例：login.html）



手順3 aptkit.aspx（又は aptkit.php）の設定をフィッシング詐欺対応訓練用に変更する。

フィッシング詐欺対応訓練を実施するには、apkit.aspx（又は apkit.php）の設定を以下のとおり変更します。

【apkit.aspx の場合】

```
'-----  
' 開封者情報の送信先に関する情報を設定して下さい  
-----  
Dim GrpName As String = "第1回メール訓練" '開封者情報集計用のグループ名  
Dim Subject As String = "開封者情報送付" 'メールの題名  
Dim toAddress As String = "test@hoge.jp" 'メールの送信先(複数ある場合は、;で区切る)  
Dim fromAddress As String = "test@hoge.jp" 'メールの送信元  
Dim smtpServer As String = "" 'SMTPサーバーのホスト名  
Dim smtpPort As Integer = 587 'SMTPサーバーのポート番号  
Dim authUser As String = "test@hoge.jp" 'SMTP認証のユーザ名  
Dim authPass As String = "password" 'SMTP認証のパスワード  
Dim authSSL As Boolean = true 'SSL接続を使用するか否か (True or False)  
Dim LinkURL As String = "./contents/top.html" 'リダイレクト先のURL  
Dim fishOp As Boolean = true 'フィッシング詐欺訓練モードにするか否か (True or False)  
Dim fishPage As String = "/LoginForm.html" 'フィッシングページのURL  
Dim emlFid As String = "C:\inetpub\wwwroot\mail" 'ローカルにメールを保存する場合の出力先
```

①「fishOp」の値を true に設定します。

②「fishPage」の値に、フィッシング詐欺ページの URL 又は、Web サーバの相対パスを設定します。

以上の設定を行うことにより、訓練メール本文中の URL リンクをクリックした際には fishPage で指定したページが表示され（同時にリンククリックの開封者情報データも出力されます）、fishPage で指定したページで ID やパスワードを入力すると、LinkURL で指定したページにリダイレクトされるようになります。（同時にフィッシングマクロ実行の開封者情報データも出力されます）

フィッシング詐欺対応訓練の実施③

【aptkit.php の場合】

```
<?php  
// 標的型攻撃メール対応訓練実施キット 開封者情報メール送信プログラム  
// 本プログラムを利用するには、以下の条件を満たす必要があります。  
// 1. Web サーバ側で PHP が使用できること、  
// 2. PHP の Mail コマンドが使用できるようになっていること  
// 3. リダイレクト先となる Web ページがあること  
// 4. GD モジュールが利用可能となっていること  
  
//-----  
// 値の設定  
// $to="" に設定すると、開封者情報をファイルに書き出します。  
$URL = "./contents/top.html"; // リダイレクト先の URL  
$to = ""; // 開封者情報メールの送信先アドレス  
$from = ""; // 開封者情報メールの送信元アドレス  
$subject = "開封者情報送付"; // メールのタイトル  
$filepath = "./mail"; // ファイルの出力先  
$groupname = "第1回メール訓練"; // 開封者情報集計用のグループ名  
$fishOp = true; // フィッシング詐欺訓練モードにするか否か (True or False)  
$fishPage = '/LoginForm.html'; // フィッシングページの URL
```

aptkit.php の場合も、aptkit.aspx と同様に、「fishOp」「fishPage」の値を設定します。

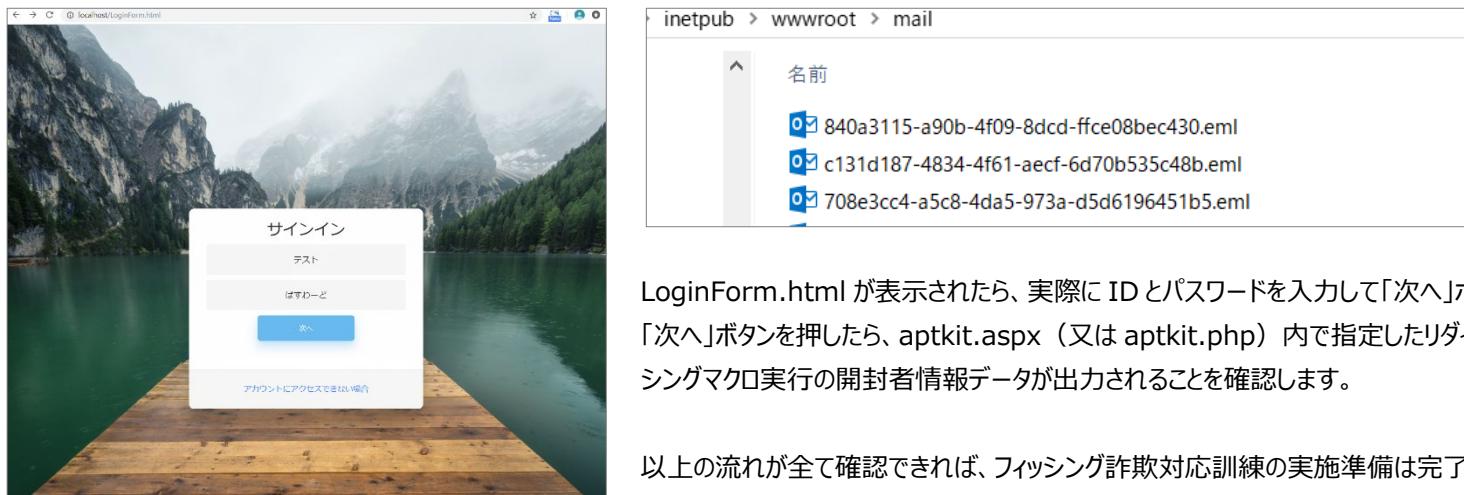
①「fishOp」の値を true に設定します。

②「fishPage」の値に、フィッシング詐欺ページの URL 又は、Web サーバの相対パスを設定します。

※添付ファイル型の標的型メール訓練を実施する場合、また、訓練メール本文内の URL リンクをクリックしたら、教育用コンテンツを表示させるような場合は、**fishOp の値は必ず false に設定**して下さい。

手順 4 URL リンクをクリックして aptkit.aspx (又は aptkit.php) にアクセスし、フィッシング詐欺訓練用コンテンツが表示されることを確認する。

手順 1 ~ 3 の設定に誤りがないかどうかを確認するために、aptkit.aspx (又は aptkit.php) への URL リンク (例 : http://www.hoge.co.jp/aptkit.aspx?u=001) をクリックすると、LoginForm.html のページが表示されること、また、URL リンクがクリックされたことを表す、開封者情報データが出力されることを確認します。



LoginForm.html が表示されたら、実際に ID とパスワードを入力して「次へ」ボタンを押して下さい。
「次へ」ボタンを押したら、aptkit.aspx (又は aptkit.php) 内で指定したリダイレクト先の URL が表示されると同時に、フィッシングマクロ実行の開封者情報データが表示されることを確認します。

以上の流れが全て確認できれば、フィッシング詐欺対応訓練の実施準備は完了です。

フィッシング詐欺対応訓練用コンテンツのカスタマイズ

フィッシング詐欺対応訓練用のログインフォームについては、HTML／CSS／JavaScript から構成される有名な WEB フレームワークである、BootStrap を用いて構成しています。BootStrap のフレームワーク自体は、BootStrap の公開サーバから取得する設定としてありますので、フィッシング詐欺対応訓練用コンテンツを表示するためには、訓練実施対象者のパソコンからインターネットにアクセスができる状態であること、また、JavaScript が実行可能であることが必要になります。

なお、インターネットに繋がっていないクローズドな環境で訓練を実施される場合は、訓練用の Web サーバ上に、BootStrap を動作させるために必要となるファイル（bootstrap.min.css、bootstrap.min.js、jquery.min.js）を設置して下さい。

フィッシング詐欺対応訓練用のログインフォームについて、キットで提供しているパターンでは不都合がある場合（自社システムのログインフォームとは見た目が異なっている等）は、ご自身でコンテンツをカスタマイズすることで、希望のフォームを使用することができます。コンテンツをカスタマイズされる場合は、以下の事項を踏まえてカスタマイズを行ってください。

なお、有償（1 案件 5 万円～）にてコンテンツをカスタマイズするサービスもご提供しておりますので、ご希望のお客様は ask@kunrenkit.jp 宛までお問い合わせ下さい。

1. コンテンツ内には、以下の hidden タグと、JavaScript を必ず含めて下さい。

```
<script>
function setFormData(f) {
    var key = localStorage.getItem('Key');
    f.uid.value = key;
    return true;
}
</script>
<input type="hidden" name="uid" value="">
```

2. Form タグの設定は以下のようにしてください。（method は post、また、onsubmit の設定を以下のようにして下さい）

```
<form action="http://localhost/aptkit.aspx" method="post" onsubmit="return setFormData(this)">
```

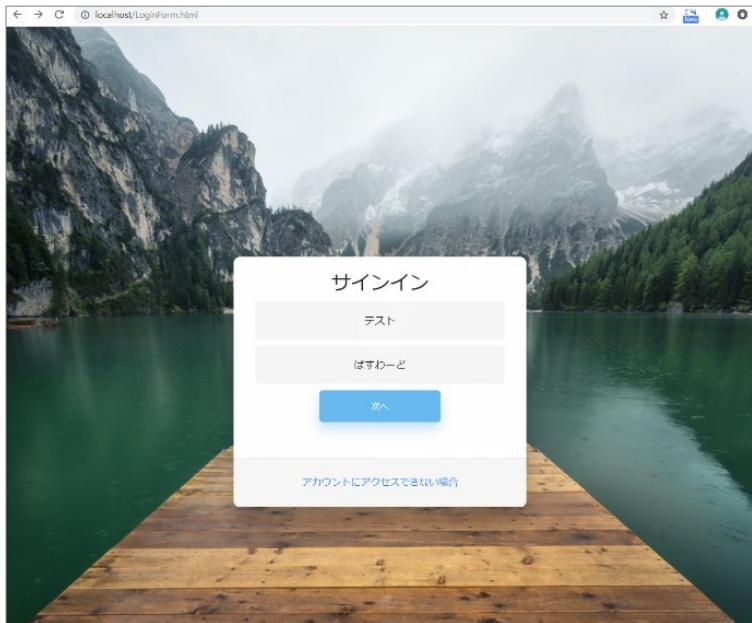
3. ログイン ID、パスワードの input タグ設定は以下のとおりとして下さい。

- ①ログイン ID については、name="login"として下さい。
- ②パスワードについて、name="pass"として下さい。

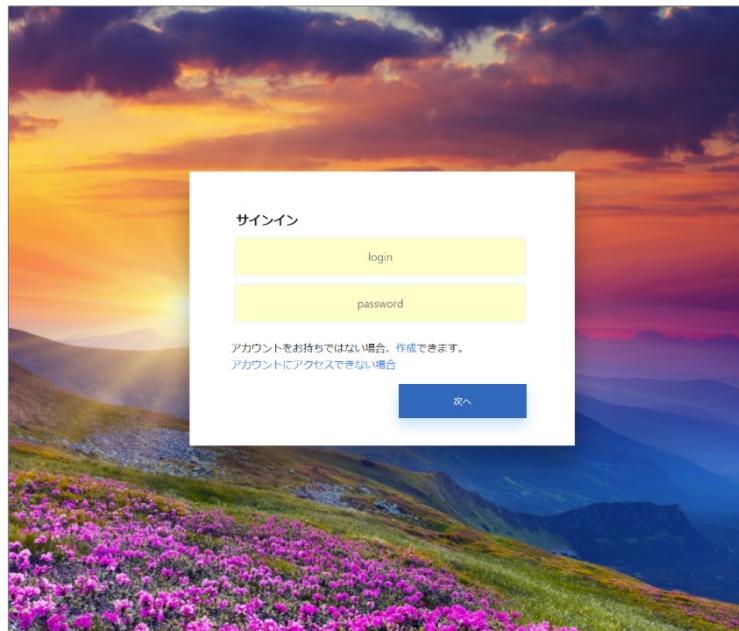
フィッシング詐欺対応訓練用コンテンツの種類

フィッシング詐欺対応訓練用のコンテンツについては、標準で以下 3 つのパターンをご用意しています。実際のイメージについては、各パターンのフォルダに収録されている LoginForm.html を実際に表示して確認してください。なお、コンテンツについてはそのままでもご利用頂けますが、ロゴを追加するなど、細かい部分をカスタマイズされると、よりリアル感のある訓練が実施できます。

パターン① 動きのあるログインフォーム



パターン③ Office365 風のログインフォーム



パターン② ウィルス感染通知



なお、コンテンツの種類については、今後、随時追加を行っていく予定です。

その他の注意事項について

SSLによる接続について

Web サーバへの接続について、SSL による接続を行いたいというご要望を頂くことがあります。

この場合、Let's Encrypt による SSL など、正式な証明書を用いての SSL 接続であれば問題はありませんが、自己証明書による SSL 接続はお使い頂いただけません。

自己証明書による SSL 接続では、SSL 接続を行うに際して、接続を継続するかどうかのダイアログが表示されることになるため、接続をキャンセルされると aptkit.aspx (又は aptkit.php) へのアクセスが発生せず、開封したことを記録することができなくなってしまうためです。

認証プロキシが設置されている環境について

Web サイトへのアクセスに際しては認証プロキシを経由して行う環境となっていて、Web サイトにアクセスするかどうかを尋ねるダイアログを表示するようになっている環境の場合も、自己証明書による SSL 接続と同様、接続をキャンセルされると、aptkit.aspx (又は aptkit.php) へのアクセスが発生しないことになります。

セキュリティ対策ソフトによっては、警告が表示されるなどの動作となる場合があります

セキュリティ対策ソフトによっては、プログラムが Web サイトにアクセスを行うに際して警告を表示するようになっているものがあります。

これはセキュリティ対策ソフトが外部との通信を監視していることによって発生するものなので、警告が表示されないようにすることはできません。

訓練実施担当者の「訓練メールを開かせたい」という想いから、警告が表示されないようにできないか? というご要望を頂くことは多いのですが、**警告が表示されることの意味について、訓練を受ける側が正しく理解しているかどうか**はとても重要なことです。警告の意味を正しく理解できていないために、警告を無視して実行を継続してしまう人がいれば、それは組織にとって**人的なセキュリティホール**となってしまいます。

警告が表示されることを前提に訓練を実施し、警告が表示されても無視して実行を継続してしまう人がいるかどうかを確認することも重要なポイントです。

また、訓練の一環として、実際に添付ファイルを開いてみる。ということをやってみてもらうのも一案です。例えば、PowerPoint プレゼンテーションファイルを利用した模擬マルウェアファイルでは、マウスオーバーによってスクリプトが実行される仕組みとなっていますが、こうしたことは、実際にファイルを開いてみると体験できません。犯罪者がマルウェアを実行させようとする手口を実際に体験することで知り、その仕組みを理解することは、犯罪者の手口にまんまと騙されないようにするためにも、とても大事な事です。

訓練メールが閲覧されたのかどうか？の確認について

訓練の実施に際して、訓練メール自体を見たのかどうかを知りたい。というご要望は多く頂きます。結論から申し上げますと、このようなご要望に沿える万能的な方法はありません。但し、インターネット内に Web サーバが設置されていること。という条件は付きますが、訓練メールを HTML 形式のメールにし、メール内に Web ビーコン画像を埋め込むことで、メールが閲覧されたことをキャッチするという方法はあります。

しかしながら、そもそもの話として、従業員がメールを閲覧しているかどうか？を会社が知ろうとする行為は、法的には許容されてはいるものの、自分がいつ、どのようなメールを閲覧しているか？が会社に知られていると従業員が知ることによって、従業員のモチベーションに影響を与えてしまいかねない点は、考慮の余地はあるかと思われます。

キットご利用のフォローアップについて

本資料並びに、キットに付属の他の資料を読まれてもよくわからない部分がある、また、各ステップにおいて何らかの問題が発生し、先に進むことができないようなことがありました場合は、お気軽に以下宛までご連絡ください。

また、キットの使い方に限らず、訓練実施に関してご不明な点などが生じた場合も、以下宛にご連絡をいただければ、できうる限り迅速に対応をさせていただきます。

【メールでのご連絡先】

ask@kunrenkit.jp

※電話によるサポートは行っておりません。メールでのお問い合わせにご協力をお願い致します。

メールでのご連絡以外にも、キットの Web サイトにありますフォーム画面、また、訓練メール送信サービスのお問い合わせフォーム画面から、お問い合わせをお送り頂く方法もございます。

<https://kunrenkit.jp/support/>

This screenshot shows the 'Contact Us' form on the KunrenKit support website. The form includes fields for company name, department, contact person, and phone number. A yellow box highlights the 'Recipient Mail Address' field, which is currently empty. Below the form, a note states that the recipient's address must be entered.

This screenshot shows the 'Training Mail Submission Registration Page' on the KunrenKit website. It features a large background image of a server room. The registration form includes fields for recipient mail address, subject, message body, and attachments. Buttons for 'Send' and 'Logout' are at the bottom.