やってみよう！攻撃メール訓練

自分の手で模擬マルウェアプログラムと訓練メールを作成し、従業員に攻撃メールを体感してもらう訓練をやってみましょう

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

このトライアルマニュアルでは、キットを用いて、模擬の攻撃メールを作成する手順をご紹介します。

標的型攻撃メール対応訓練実施キット　トライアルマニュアル

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き、ありがとうございます！

初めまして、こんにちは。
この度は、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き、また、本資料をご覧いただきまして、誠にありがとうございます。
インターネットを通じ、このようなご縁をいただ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、非常に嬉しく思います。

無料モニター版のキットには制限があります

無料モニターへのご参加でお使い頂けるキットにつきましては、試用版としての位置づけとなりますため、以下の制限がございます。この点をご了解いただいた上でご利用ください。

なお、以下の制限はございますが、訓練の実施自体は、製品版をお使いいただく場合と何ら変わりなく行うことができますので、無料モニター版のキット一式にて訓練が実施いただけることをご確認いただけましたら、是非、製品版のご購入について、ご検討をいただけましたら幸いに存じます。

① **ご提供するツールには制限があります**
キットを使って模擬のマルウェアプログラムを作成し、訓練メールとして社内に配布することに制限はございませんが、無料モニター版のキット一式でご提供するツールでは、一度に出力できるデータや、処理できる件数に制限がございます。各ツールにおける制限事項につきましては、各ツールに説明を記載しておりますので、そちらをご参照ください。

② **模擬マルウェアプログラムの作成にあたって、Visual Studio の他に必要となるツールがあります**
無料モニター版では、模擬マルウェアプログラムのメインプログラム部分のソースコードを非開示とさせていただいております関係で、メインプログラム部分を DLL 化しているため、ご利用に際して、Microsoft 社から無償で提供されております、ILMerge.exe というツールが必要となります。
なお、製品版ではメインプログラム部分はソースコードでご提供しますので、ILMerge.exe は不要となります。

では、次のページより、無料モニター版の説明を進めます。

無料モニター版のキットでできること

無料モニター版のキットをお使い頂くと、以下の攻撃メール訓練を実施いただくことができます。

① Exe 実行ファイル添付型の攻撃メール訓練

訓練メールに、模擬のマルウェアプログラムとなる exe 実行ファイルを添付する形式の訓練を実施することができます。

従業員が添付ファイルを開くと、標的型メールに関する教育用コンテンツが表示されると共に、添付ファイルを開いた方の情報がメールで訓練実施担当者宛に送付されます。訓練実施担当者側では、この情報をキットに付属のツールを用いて集計することで、訓練の実施結果をまとめることができます。

② Word 文書ファイル添付型の攻撃メール訓練

訓練メールに、模擬のマルウェアファイルとなる Word 文書ファイルを添付する形式の訓練を実施することができます。

従業員が添付ファイルを開くと、Word 文書の内容が表示されると共に、Word 文書ファイルを開いた方の情報が、Web サーバを経由してメールで訓練実施担当者宛に送付されます。訓練実施担当者側では、この情報をキットに付属のツールを用いて集計することで、訓練の実施結果をまとめることができます。

③ URL リンククリック形式の攻撃メール訓練

訓練メールの本文に URL リンクを設定し、URL リンクをクリックすると不正なサイトに誘導される形式の訓練を実施することができます。

従業員がメール本文中の URL リンクをクリックすると、あらかじめ設定したリンク先のページが表示されると共に、URL リンクをクリックした方の情報が、Web サーバを経由してメールで訓練実施担当者宛に送付されます。訓練実施担当者側では、この情報をキットに付属のツールを用いて集計することで、訓練の実施結果をまとめることができます。

上記①～③については。それぞれ単独で実施することもできますし、組み合わせて実施することもできます。
但し、Gmail のように exe ファイルや zip ファイルをメールで受信することができない環境や、あらかじめ登録されている以外の exe プログラムは実行不可にしている環境では、実施することができない訓練もあります。

無料モニター版のキットでは、自社ではどのような訓練が実施可能で、どのような訓練は実施不可となるかについても、同時にご確認をいただければと存じます。

無料モニター版のキットに含まれているもの

無料モニター版のキットには、攻撃メール訓練を実施する際に必要となる、以下のものが含まれています。

① 模擬のマルウェアプログラムのテンプレート

Microsoft Visual Studio を使用して、設定を変えるだけで模擬のマルウェアプログラムを作成することのできる、プログラムのテンプレートファイルです。

② 訓練用 Word 文書ファイル一括作成ツール

Word 文書ファイル添付型の訓練で使用する、ユーザー毎にユニークとなる Web ビーコンファイルを埋め込んだ Word 文書ファイルを一括して生成することができる Excel ツールです。

③ 訓練メール一括送信ツール

SMTP サーバーを利用して、従業員に訓練メールを一括送信するための Excel ツールです。メール送付先ごとに、添付するファイルを変えたり、メール本文中に埋め込む URL リンクを変えるなど、訓練メールを一括して送付するための機能を有しています。

④ 開封者情報集計ツール

訓練メールに添付されている模擬のマルウェアファイルを開いてしまった人や、メール本文中の URL リンクをクリックしてしまった人の情報を集計する Excel ツールです。開封した方の一覧や、所属部署別の開封率を集計するといったことができます。

⑤ Web サーバー側に設置するプログラム（ASP.NET 版と PHP 版）

Word 文書ファイル添付型や、URL リンククリック型の訓練、また、開封者情報の送付に SMTP サーバーを利用することができないケースにおいては、開封者情報の収集に Web サーバーが必要になります。この Web サーバーに設置するプログラムとして、Windows サーバー用の ASP.NET 版のプログラム、Linux サーバー用の PHP 版のプログラムをご提供します。

⑥ 従業員教育用コンテンツの雛形（Word 文書データ、HTML データ、PDF ファイル）

従業員に対して、攻撃メールの見分け方などを教育するための教育用コンテンツの雛形として、Word 文書、HTML、PDF の 3 種類のコンテンツデータをご提供します。Word 文書添付型の訓練並びに、URL リンククリック型の訓練でご利用頂けます。Word 文書と HTML については編集が可能なデータとなりますので、訓練の実施内容に合わせてお客様側で適宜カスタマイズしてご利用下さい。

⑦ その他のツール

eml ファイルを④のツールで処理できるデータに変換するツール並びに、goo.gl の短縮 URL を一括生成するツールを付属しています。

キットを用いた攻撃メール訓練実施の流れ

P.5～P.10

exe 実行ファイル添付型の訓練実施の流れ

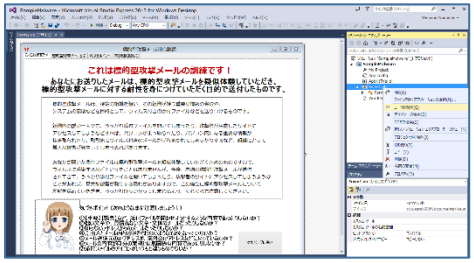
標的型攻撃メール対応訓練実施キットを使用しての Exe 実行ファイル添付型の訓練実施の流れは、おおよそ以下のようになります。
詳しくは、P.11 から始まる「Exe 実行ファイル添付型の訓練実施」を参照して下さい。

STEP1 キットが使えるかどうかを確認する

模擬のマルウェアプログラムを作成する前に、KitCheckTool を用いて、キットが貴社環境で使えるかどうか（開封者情報メールが送信できるかどうか）を確認します。このツールで、キットが使えることを確認できたら、STEP2 に進みます。

STEP2 Visual Studio Express を入手する

訓練メールに添付する模擬マルウェアプログラムを作成するため、Microsoft から提供されている無償の開発ツールである、Visual Studio Express を、Microsoft のサイトから入手します。



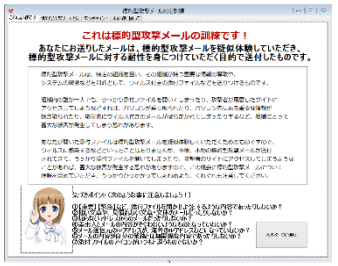
STEP3 模擬のマルウェアプログラムを作成

キットに同梱されている、模擬マルウェアプログラムのテンプレートと、Visual Studio Express を使って、模擬のマルウェアプログラムを作成します。

STEP4 訓練メールを作成してメールを送信

模擬マルウェアプログラムを添付するための訓練メール本文を作成します。キットを使って訓練ができるかどうかのテストなので、メール本文の内容自体はダミーでも構いません。

メールを作成したら、模擬のマルウェアを同梱した zip ファイルを作成してメールに添付し、訓練メールとして送信します。

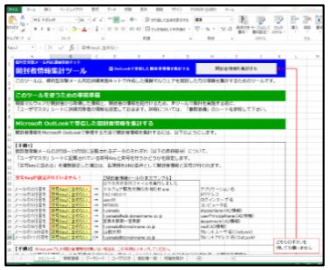


STEP5 模擬マルウェアの実行

訓練対象者が訓練メールを受信し、訓練メールに添付されている、模擬のマルウェアプログラムを実行します。
この行為によって、開封者情報が指定のメールアドレス宛に送付されます。

STEP6 開封者情報メールの受信

Microsoft OutLook などのメールソフトを用いて、開封者情報メールの受信を行います。



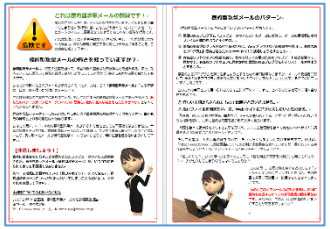
STEP7 開封者情報の集計

キットに同梱の開封者情報集計ツールを用いて、STEP6 で受信した開封者情報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。

STEP7 までを問題なく確認することができたら、キットを使っての訓練実施は可能ということになります。

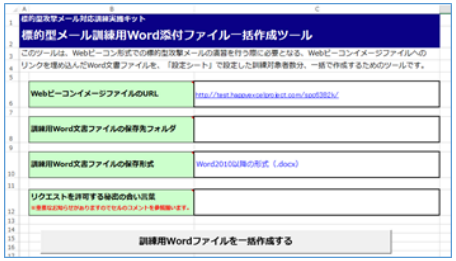
Word 文書ファイル添付型の訓練実施の流れ

Word 文書ファイル添付型の訓練実施の流れは、おおよそ以下のようになります。
詳しくは、P.20 から始まる「Word 文書ファイル添付型の訓練実施」を参照して下さい。



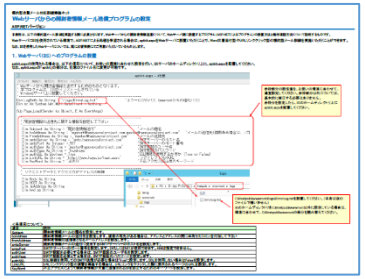
STEP1 添付用の Word 文書を用意する

訓練メールに添付する Word 文書のオリジナルを作成します。これは通常の Word 文書ファイルになりますので、キットに付属の文書をそのまま使用いただいても構いませんし、独自に文書を作成いただいても構いません。



STEP2 個別の Word 文書を作成する

STEP1 で用意した Word 文書を元に、Word 文書一括作成ツールを用いて、訓練対象者ごとの Word 文書ファイルを作成します。



STEP3 Web サーバ側の設定を行う

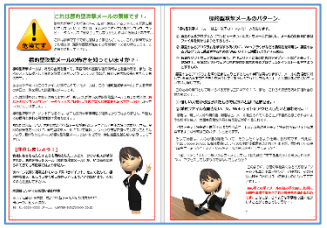
Word 文書ファイル添付型では、Web ビーコンを使用して、開封者の情報取得を行います。

Web ビーコンを使用するには、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 サーバに設置いただきます。

STEP4 訓練メールを作成してメールを送信

Word 文書を添付するための訓練メール本文を作成します。キットを使って訓練ができるかどうかのテストなので、メール本文の内容自体はダミーでも構いません。

本文を作成したら、添付ファイル付きメール一括送信ツールを用いて、STEP2 で作成した Word 文書を添付した、個別の訓練メールの送付を行います。



STEP5 Word 文書を開く

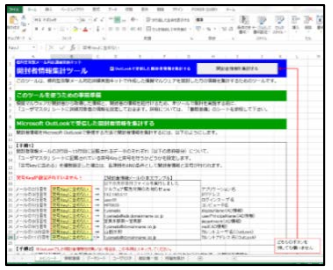
訓練対象者が訓練メールを受信し、訓練メールに添付されている、Word 文書を開きます。

この行為によって、Web サーバへのアクセスが発生し、開封者情報が指定のメールアドレス宛に送付されます。

※但し、Word 文書を開いた際に警告が表示され、インターネットへのアクセスを拒否する選択をユーザが行った場合は、Web サーバへのアクセスは発生せず、開封者情報も送付されません。

STEP6 開封者情報メールの受信

Microsoft OutLook などのメールソフトを用いて、開封者情報メールの受信を行います。



STEP7 開封者情報の集計

キットに同梱の開封者情報集計ツールを用いて、STEP6 で受信した開封者情報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。

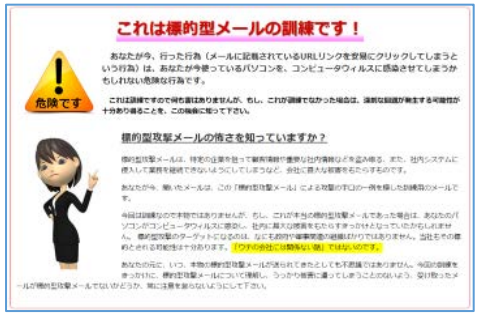
STEP7 までを問題なく確認することができたら、キットを使っての訓練実施は可能ということになります。

URL リンククリック型の訓練実施の流れ

メール本文中に URL リンクを埋め込む、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。
詳しくは、P.25 から始まる「URL リンククリック型の訓練実施」を参照して下さい。

STEP1 Web サーバ側の設定を行う

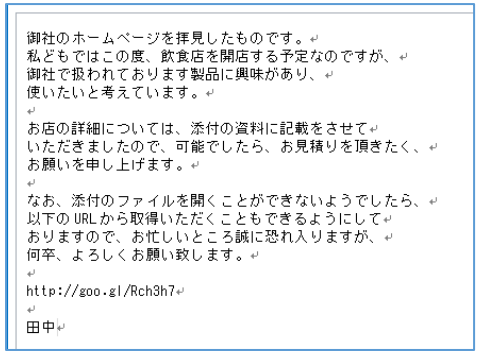
URL リンククリック型では、Word 文書ファイル添付型と同様、お客様側にて Web サーバをご用意いただき、キットに付属の Web サーバ側用プログラムを Web サーバに設置いただきます。



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 サーバに設置いただく、また、既存の Web ページを利用していただくなど、訓練の内容に合わせて選択してください。

用意したページの URL は、STEP1 で設定したプログラムの「LinkURL」の値として設定してください。


御社のホームページを拝見したものです。
私どもではこの度、飲食店を開店する予定なのですが、
御社で扱われております製品に興味があり、
使いたいと考えています。

お店の詳細については、添付の資料に記載をさせて
いただきましたので、可能でしたら、お見積りを頂きたく、
お願いを申し上げます。

なお、添付のファイルを開くことができないようでしたら、
以下の URL から取得いただくこともできるようにして
おりますので、お忙しいところ誠に恐れ入りますが、
何卒、よろしくお願い致します。

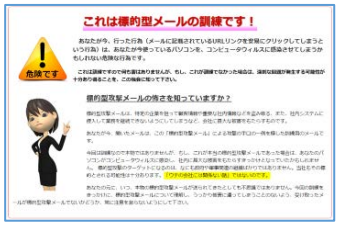
http://goo.gl/Rch3h7

田中

STEP３ 訓練メールを作成してメールを送信

URL リンクを埋め込んだ訓練メール本文を作成します。キットに付属の一括メール送信ツールでは、テキスト形式のメールと HTML 形式のメールを送信することができます。

なお、メール本文に埋め込む URL リンクには、URL リンクをクリックしたユーザを特定するための個別のパラメータ情報を設定してください。実際にアクセスすることになる URL やパラメータ情報を見られたくない場合は、http://goo.gl/ などで提供されている短縮 URL サービスを使う方法があります。



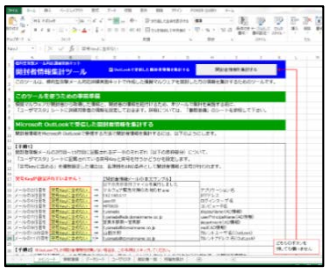
STEP4 リンクがクリックされる

URL リンクがクリックされると、Web サーバに設置したプログラムへのアクセスが発生し、Web サーバから開封者情報のメールが送付されると共に、ユーザには 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。

この間、リンクをクリックしたユーザには、リダイレクト先のページに直接アクセスしているように見えることになります。

STEP5 開封者情報メールの受信

Microsoft OutLook などのメールソフトを用いて、開封者情報メールの受信を行います。



STEP6 開封者情報の集計

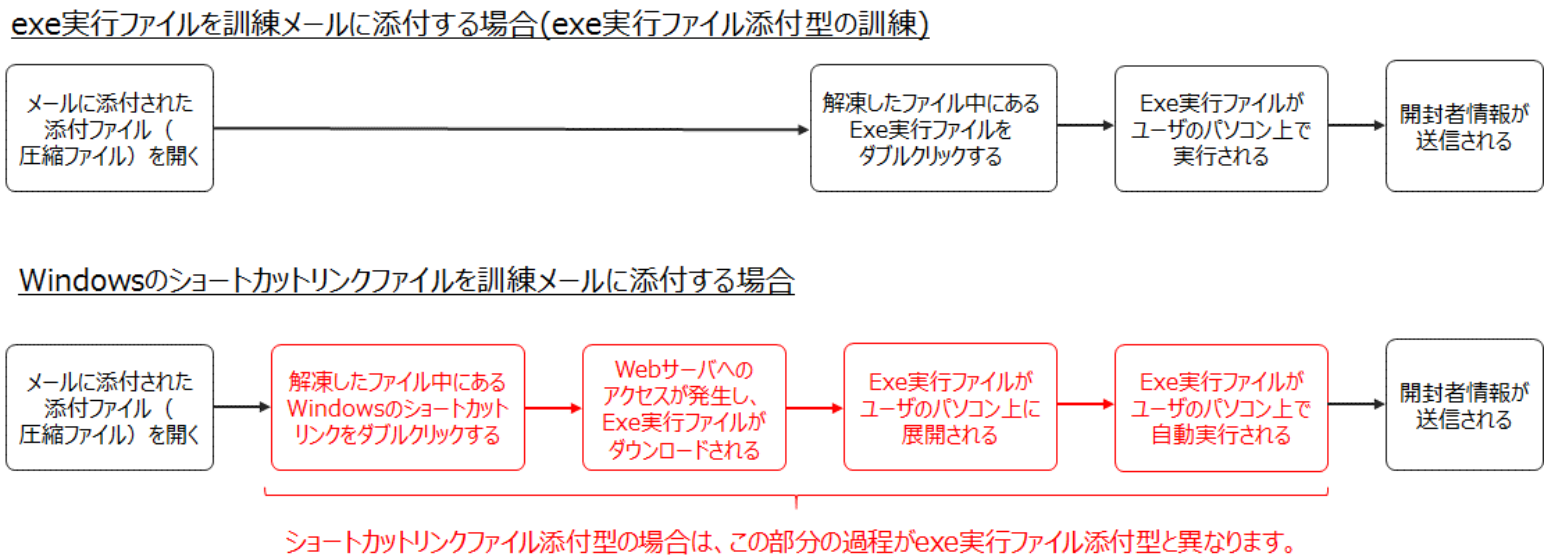
キットに同梱の開封者情報集計ツールを用いて、STEP5 で受信した開封者情報の集計処理を行います。

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。

URL リンククリック型では、リンク先となるページに、訓練対象者に読んでもらうコンテンツをご用意頂くことが必要になります。

（参考）Windows のショートカットリンククリック型の訓練実施の流れ

標的型攻撃メール対応訓練実施キットでは、メールに exe 実行ファイルを添付する代わりに、Windows のショートカットリンクファイルを添付する、「ショートカットリンククリック型の訓練」も実施することができます。実施の流れ自体は exe 実行ファイル添付型の訓練を実施する場合と同様となり、exe 実行ファイル添付型との違いは、exe 実行ファイルをユーザのパソコンにダウンロードさせるための仕組みが追加で必要となる点になります。



Windows のショートカットリンクファイルを添付する形式の訓練を実施するには、exe 実行ファイル添付型での準備に加え、上記の赤枠部分の仕組みを用意するため、以下の作業を追加で行います。

① Web サーバ側に、exe 実行ファイルをダウンロードさせるためのデータ（スクリプトファイルと、exe 実行ファイル）を設置する。
② 製品版のキットに付属のツールを使って、訓練メールに添付する Windows のショートカットリンクファイルを作成する。

無料モニターでお使い頂けるキット一式では、ショートカットリンククリック型の訓練を実施するためのツールは付属していませんので、ショートカットリンククリック型の訓練を実施することはできませんが、無料モニターでお使い頂けるキット一式に付属の「**ショートカットファイル添付型の模擬メール訓練実施の手引き.pdf**」を参照頂くことで、具体的な流れについては、ご確認いただくことができます。

標的型攻撃メール対応訓練実施キットは、開封者情報収集の方法に特徴があります

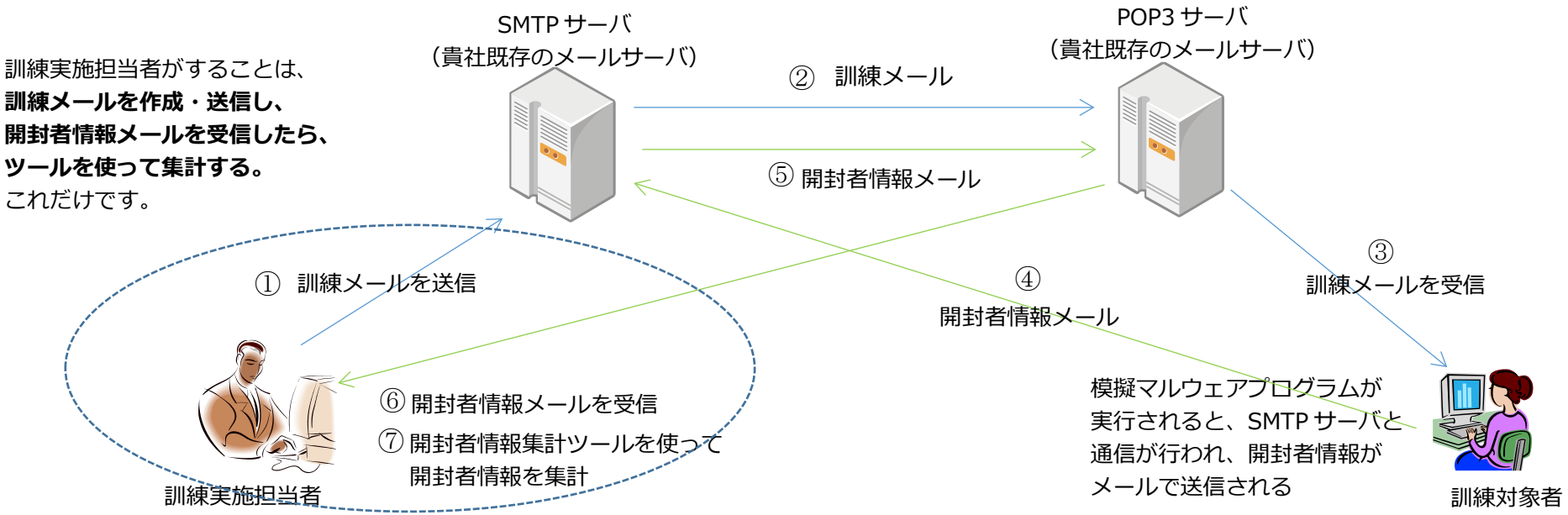
標的型攻撃メール対応訓練実施キットの開封者情報収集は、メールを使った独自の方法を採用しております。
これは、他社の標的型メール訓練サービスをご利用されていたお客様、また、Web サーバのログを解析する方法で訓練を実施されていたお客様からすると、意外な方法に思われるかもしれません。

標的型攻撃メールの演習に関して一般に公開されているドキュメントなどでは、Word 文書や PDF 文書ファイルに画像データを埋め込み、Web サーバのログを解析する方法で開封者情報を集計するといった方法が使われていますが、標的型攻撃メール対応訓練実施キットでは、ログを解析する方法は使わず、「訓練対象者のパソコンから開封者情報のメールを送信させる」もしくは、「Web サーバ側から開封者情報のメールを送信させる」という方法を採用しています。

訓練対象者のパソコンから直接メールで開封者情報を送信する場合は、Web サーバを経由させる必要も、また、Web サーバのアクセスログを解析する必要も無いということになりますので、訓練実施に際して Web サーバをご用意いただく必要がありません。Word 文書ファイル添付型や、URL リンククリック型の訓練を実施される場合は、Web サーバをご用意いただく必要はあるものの（と言っても、普段お使いの Windows7 パソコンがそのままお使い頂けます）、アクセスログの解析は不要なので、アクセスログの解析ができる技術者は必要ありません。サーバなどの専用の機材を用意しなくて良いということは、外注に頼らずに訓練を実施するに際して、大きなポイントになります。

なお、社内の都合で SMTP サーバを用意することができず、訓練対象者のパソコンや、Web サーバからメールを送信することができない場合は、Windows7 などに付属の IIS（Web サーバソフト）をお使い頂ければ、メールを送信する代わりに、Web サーバ内に eml ファイルとしてメールを保存する方法が使えます。この方法を使うと、開封者情報のメールを送信する場合と同様に、キットに付属のツールを使って開封者情報の集計を行うことができます。

◆標的型攻撃メール対応訓練実施キットによる訓練実施の流れ



Web サーバにアクセスさせる形で開封者情報を集計する場合の URL 構成

標的型攻撃メール対応訓練実施キットには、訓練対象者のパソコン上から直接メールを送信することができない場合や、Word 文書ファイル添付型や URL リンククリック型の訓練を実施する際に開封者情報を収集するための仕組みとして、Web サーバ上で動作し、開封者情報をメールにして送信するためのプログラムとして、「aptkit.aspx」（ASP.NET 版）と「aptkit.php」（PHP 版）をご提供しています。

どちらも 1 つのファイルで全ての訓練タイプに対応しており、Web サーバにアクセスする URL によって、使い分けができるようになっています。
各訓練実施タイプにおける URL 構成については、以下のようになります。

【基本構文】

http://web サーバ名/フォルダ名/aptkit.aspx（又は aptkit.php）?（第一パラメータ）&（第二パラメータ）

例：http://192.168.0.250/kunren/aptkit.aspx?apps=user01&kwd=passwd

第一パラメータ： ① apps=xxxx（Word 文書ファイル添付型の訓練実施の場合） ② data=xxxx（exe 実行ファイル添付型の訓練実施の場合）
③ user=xxxx（URL リンククリック型の訓練実施の場合）

※xxxx の部分は、訓練対象者毎に設定する固有の値になります。
※apps=test と指定すると、プログラムの実行結果として、取得できた IP アドレスとホスト名の情報が HTML データとして返却されますので、プログラムの動作確認用として使用頂けます。

第二パラメータ： kwd=yyyy ※yyyy の部分は、aptkit.aspx や aptkit.php で指定する、不正アクセス防止用のキーワード値になります。

【使い方】

Case1 第一パラメータに apps=xxxx と指定すると、Web サーバにアクセスした際に、1 ドット×1 ドットの png 画像が返却されます。
Case2 第一パラメータに data=xxxx と指定すると、Web サーバにアクセスした際に、空の html ページが返却されます。
Case3 第一パラメータに user=xxxx と指定すると、Web サーバにアクセスした際に、aptkit.aspx または、aptkit.php にある「LinkURL」に設定した URL がリダイレクト先として返却されます。なお、user=xxxx の user の部分については、apps と data 以外であれば、user 以外の文字列も使えます。

・Case1 と Case 2 のパターンについては、キットに付属のツールや、模擬マルウェアプログラム内で使われるものとなりますので、訓練対象者が直接 URL をクリックするような形式では通常利用しません。

・URL リンククリック型の訓練を実施される場合は、Case 3 のパターンを、メール本文中に埋め込むリンク先の URL として設定いただくことになります。

※http://192.168.0.250/kunren/aptkit.aspx?apps=user01&kwd=passwd のような URL は、ユーザには見えないようにしたい。という場合は、goo.gl などの短縮 URL のご利用をご検討ください。

Exe 実行ファイル添付型の訓練実施

P.12～P.20

Visual Studio Express 2015 for Windows Desktop を入手しましょう

標的型攻撃メール対応訓練実施キットを使って、模擬のマルウェアプログラム（exe 実行ファイル）を作成するには、Microsoft 社から提供されている無償のプログラム開発ツールである、「Visual Studio Express 2015 for Windows Desktop」を入手し、お手持ちのパソコンで使えるようにすることが必要です。
以下に、Visual Studio の入手方法を記載します。　※Visual Studio Express 2013 や 2012 でも問題なくご利用いただけます。

Word 文書ファイル添付型や URL リンククリック型の訓練を実施される場合は Visual Studio は使用しませんので、Visual Studio に関する説明は読み飛ばしていただいて構いません。

◆Visual Studio について

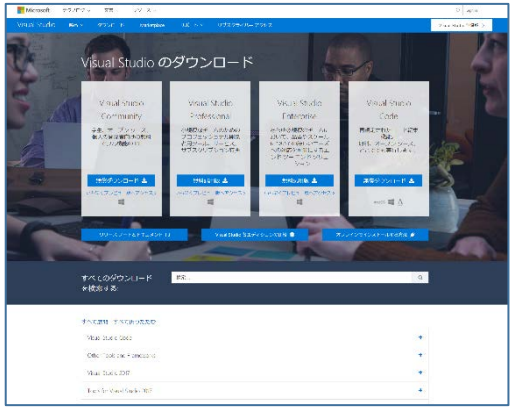
Visual Studio には、無償で使える Express 版と、プロフェッショナル向けの有償版があります。更に、Windows のアプリケーション作成用や、モバイル端末向けのアプリケーション作成用、また、Web サーバ用のアプリケーション作成用など、目的別に細かく分かれているのですが、キットでは、Windows パソコン上で動作する模擬マルウェアプログラムを作成することになりますので、「Windows Desktop 版」を使います。

無償版と有償版では、どちらをお使いいただいても構いませんが、開発者でなければ、無償で使える Express 版を選択いただくことをお奨めします。
なお、現在では Visual Studio Community がメインの製品として提供されていますが、こちらは無償での利用に制限がありますので、無償でのご利用を希望されるお客様は、Visual Studio Express をお選びいただくことをお勧めします。

開発者様などで、既に Visual Studio Professional 版などをお持ちでしたら、そちらをお使い頂く形でも構いません。

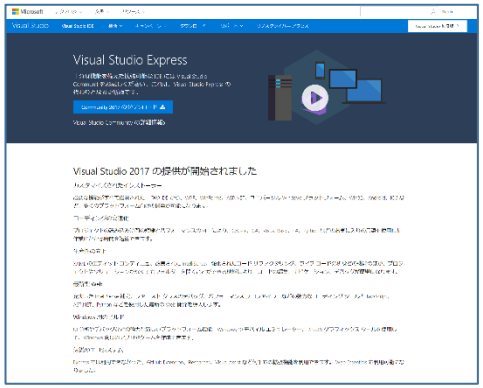
◆Visual Studio の入手方法について

Visual Studio については、以下のサイトより入手することができます。
Visual Studio Express のダウンロード URL：https://www.visualstudio.com/ja/post-download-vs/?sku=xdesk&clcid=0x409&telem=ga
https://www.visualstudio.com/ja/vs/visual-studio-express/



Visual Studio ダウンロード

Visual Studio 2017 のリリースでは、Express 版の提供が行われなくなりました。このため、Visual Studio Express は 2015 までとなり、Visual Studio の Web サイトから辿れるリンクより、Express 2015 for Desktop を選択し、ダウンロードして頂く流れとなります。



Express のページもありますが・・・

Visual Studio の Web サイトには、Express のページもありますが、このページよりダウンロードできるのは、Community 版の Visual Studio となるため、2015 版の Express をダウンロードするには、このページの下部に用意されている、Express 版のリンクからダウンロード頂く形になります。

Visual Studio Express 2015 for Windows Desktop を使えるようにする

Visual Studio Express のインストーラーをダウンロードし、実行する

Visual Studio Express をインストールするには、Visual Studio Express のダウンロードページにアクセスし、インストーラーをダウンロードして実行してください。なお、ネットワーク環境の都合でインストーラーをダウンロードして実行する形式が使えない場合は、「オフラインでインストールする方法」について説明したページ
https://msdn.microsoft.com/ja-jp/library/e2h7fzkw.aspx#bkmk_offline
を参照してください。

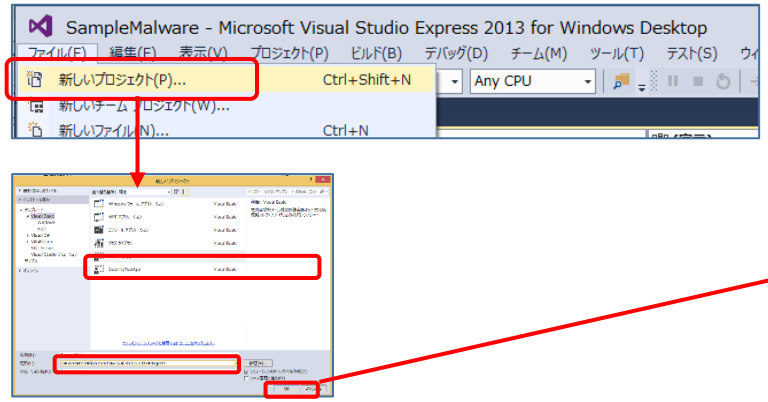
https://www.visualstudio.com/ja/vs/visual-studio-express/のページの下部にある、
Express 2015 for Windows Desktop のリンクをクリックして、インストーラのダウンロードを行います。

Visual Studio Express インストール完了後、Visual Studio Express 2015 for Windows Desktop を用いて模擬のマルウェアプログラムを作成するには、以下の手順で行います。

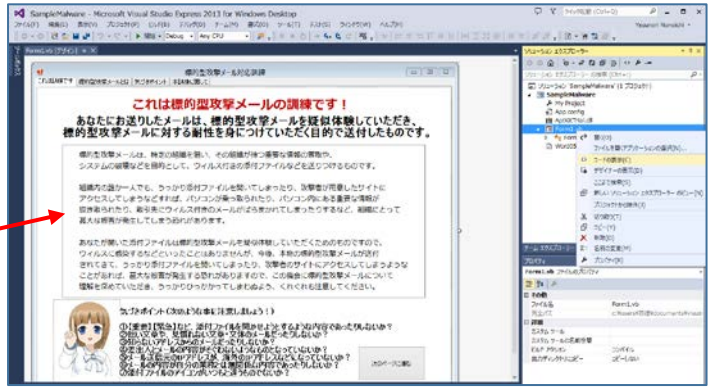
① 模擬マルウェアプログラムのテンプレートファイルを、Visual Studio Express のプロジェクトテンプレートフォルダにコピーします。

キットに同梱されている「SecurityAppTrial-Net40.zip」(.NET4.0 用)または「SecurityAppTrial-Net20.zip」(.NET2.0 用) を、Visual Studio Express の「Visual Studio 2015¥Templates¥ProjectTemplates」フォルダ配下に、丸ごとコピーします。この際、zip ファイルは解凍せずに、そのままコピーを行ってください。

②Visual Studio Express において、「新しいプロジェクト」を選択し、模擬マルウェア作成用テンプレートを選択して、模擬マルウェアプログラムのテンプレートを元に、新しいプロジェクトを作成します。(①の作業の際に、Visual Studio Express を起動している場合は、一旦終了させてください。)



新しいプロジェクトを選択するダイアログに、「SecurityAppTrial～」という名前が表示されているはずなので、これを選択し、プロジェクトの名前を設定して OK ボタンを押します。「SecurityAppTrial～」の名前が出てこない場合は、コピーしたテンプレートの zip ファイルが壊れているか、コピーした場所を間違えている可能性が考えられます。

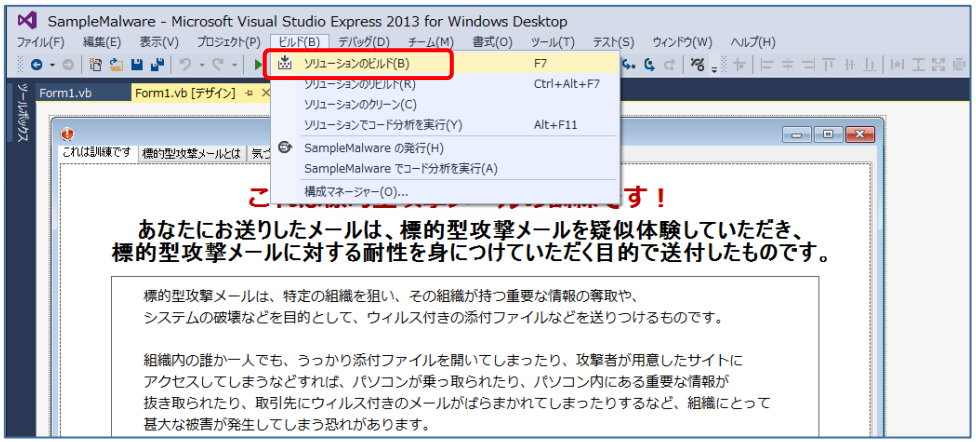


模擬マルウェアプログラムのテンプレートを元に、プロジェクトが生成されます。
これで、模擬マルウェアプログラムを編集する準備が整いました。
※上記の画面が表示されない場合は、Ctrl キー＋ALT キー＋L キーを押して、
「ソリューションエクスプローラー」を表示させてください。

Visual Studio Express を使って模擬のマルウェアプログラムを作成しましょう

では、Visual Studio Express 2015 for Windows Desktop を用いて、模擬のマルウェアプログラムを作成してみましょう。といっても、難しくはありません。まずは作り方に慣れていただくため、ここでは、訓練メールに添付できる、exe 実行ファイルを作ってみます。

◆模擬マルウェアプログラムを編集する準備が整ったら、「ソリューションのビルド」を選択します。



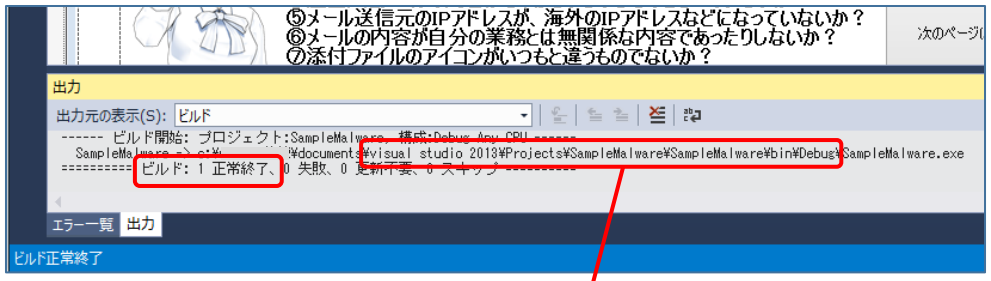
ソリューションのビルド

ソリューションのビルドとは、実行可能なプログラムを生成する作業です。
模擬マルウェアプログラムのテンプレートを使って、模擬のマルウェアプログラムを作るには、ソリューションのビルドにより、実行可能な exe ファイルを生成します。

実際の演習用に使うには、SMTP サーバ情報の設定や、表示される画面などを適宜変更するといった作業が必要になりますが、とりあえず動くものを作成するだけであれば、ソリューションのビルドを行うだけで OK です。

◆ビルドの結果を確認しましょう。

「ソリューションのビルド」を実行すると、実行結果が「出力」表示画面に出力されます。テンプレートから新しいプロジェクトを生成し、プログラムには何も手を加えない状態でビルドを実行すれば、ビルドは正常に終了するはずです。ビルドが正常に終了すると、以下の図のように「1 正常終了」と出力されます。

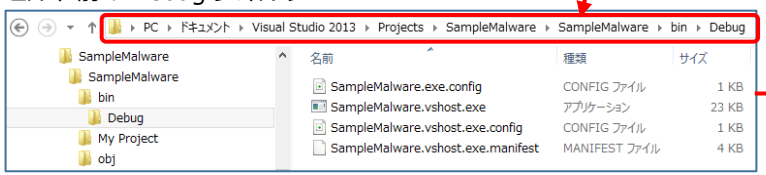


exe 実行ファイルを取り出す

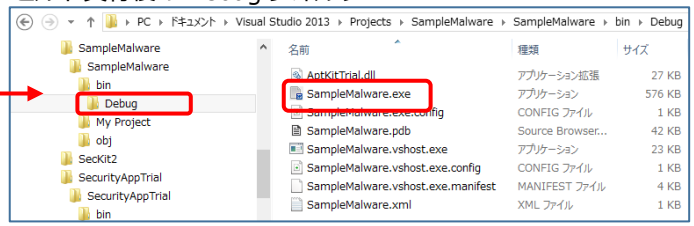
ビルドを実行すると、Debug フォルダ内に、「プロジェクト名+.exe」のファイル名にて、exe 実行ファイルが出力されます。これが、演習用のメールに添付することができる、模擬のマルウェアプログラムになります。

Debug フォルダ内には、pdb ファイルや config ファイルなどがありますが、これらは訓練メールでは使用しませんので無視していただいて構いません。

ビルド前の Debug フォルダ



ビルド実行後の Debug フォルダ

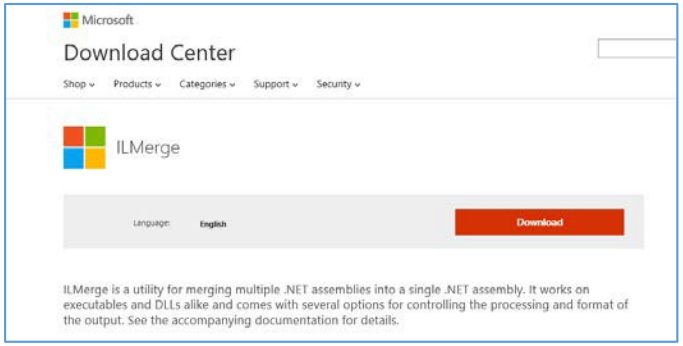


ILMerge.exe を用いて、訓練メールに添付する exe 実行ファイルを作成する

無料モニター版のキットでは、本書の P.1 に記載の通り、模擬マルウェアプログラムのメインプログラム部分のソースコードを非開示とさせていただいております関係で、メインプログラム部分を DLL 化しているため、Visual Studio で生成した exe ファイルを他のコンピュータ上で実行すると、DLL ファイルが無い事に起因するエラーが発生します。

Visual Studio で生成した exe ファイルを、訓練メールに添付して他者に配布が可能な exe 実行ファイルとするには、Microsoft 社から無償で提供されております ILMerge.exe というツールを用いて、Visual Studio で生成した exe 実行ファイルと、DLL ファイルを結合する作業を行い、DLL ファイルが含まれる exe 実行ファイルを生成します。

ILMerge のダウンロードページ
http://www.microsoft.com/en-us/download/details.aspx?id=17630



ILMerge.exe を用いて、Visual Studio で生成した exe ファイルと、
DLL ファイル（AptKitTrial.dll）を結合する手順については、キットに同梱の資料「※初めにお読み下さい－標的型攻撃メール対応訓練実施キット（無料モニター版）について.pdf」の後半部分に、右図の説明書きを掲載しておりますのでご参照下さい。

なお、キットの製品版では、ILMerge.exe による、exe ファイルと DLL ファイルの結合作業は不要で、Visual Studio で生成した exe ファイルをそのまま訓練用の exe 実行ファイルとしてお使い頂けます。

ILMerge による DLL ファイルと exe ファイルの統合方法

1．exe ファイルと DLL ファイルのマージ準備
Visual Studio で生成した exe ファイルと、AptKitTrial.DLL を一本化（マージ）するため、この 2 つのファイルを適当なフォルダにコピーします。

なお、生成した exe ファイルは通常、以下のフォルダに出力されます。
（Visual Studio をインストールしたフォルダ）¥Visual Studio 2013¥Projects¥（設定したプロジェクト名）¥（設定したプロジェクト名）¥bin¥Debug

名前
AptKitTrial.dll
SecurityAppTrial.exe

2．DOS コマンドプロンプトを起動し、ILMerge がインストールされているフォルダに移動します
例：C:¥Program Files (x86)¥Microsoft¥ILMerge¥

3．ILMerge のコマンドをタイプし、exe ファイルを生成します
DOS コマンドプロンプト上で、以下のコマンドをタイプし、リターンキーを押します。（下図の例を参照）

ILmerge /out:"1 本化後の exe ファイル名" "Visual Studio で生成した exe ファイル名"
"結合する DLL ファイル名（AptKitTrial.dll）"
/targetplatform:v2,"C:¥Windows¥Microsoft.NET¥Framework¥v2.0.50727"

※各ファイル名はフルパスで指定して下さい。
以下は、実際のタイプ例になります。

コマンド プロンプト

/targetplatform:v2,"C:¥Windows¥Microsoft.NET¥Framework¥v2.0.50727"の部分は、.Net Framework2.0 の場合の指定になります。ターゲットとなる.Net Framework のバージョンを 2.0 以外のものにするには、この部分の設定を変更します。例えば、.Net Framework4 をターゲットとする場合は、次のようになります。

/targetplatform:v4,"C:¥Windows¥Microsoft.NET¥Framework¥v4.0.30319

訓練メールに exe 実行ファイルを添付して送信する

Visual Studio Express で exe 実行ファイルを生成したら、訓練メールに添付して、訓練対象者に配布することができます。

◆exe 実行ファイルを zip ファイルにする

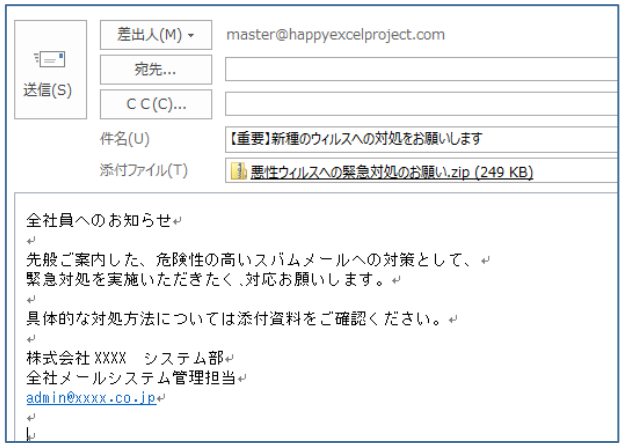
昨今のメールサーバやメールソフトでは、セキュリティ対策のために、exe 実行ファイルをそのままメールに添付することを許可していない、また、メールを送ることができたとしても、exe 実行ファイルが添付されていた場合は、受信側で自動的に削除してしまう等の措置が行われていることがほとんどです。

このため、exe 実行ファイルについては、拡張子を.exe_に変える、また、zip で圧縮ファイルにするといった加工が必要になります。なお、昨今では、標的型攻撃メールに zip ファイルが使われることから、zip ファイルも受信不可としているケースもあります。この場合は、lzh など、他の圧縮形式を使うか、zip ファイルの拡張子を.zip_に変えるなどの加工が必要になります。

zip ファイル化すれば OK なのか、それとも、他の圧縮ファイルを使うか、拡張子を zip_に変更しないといけないのか？といったことについては、貴社のメール環境に依りますので、どのようなセキュリティ対策が施されているかについては、メールサーバの管理者にお尋ねいただくか、実際に試してみていただくことで確認を行ってください。ちなみに、Gmail では exe、zip、lzh などの拡張子を持つ添付ファイルは受信することができません。

◆訓練メールを送信する

訓練メールの送信を行うには、キットに付属のメール送信ツールもしくは、今お使いのメールソフトをお使いいただき、通常のメール送信と同じ方法でメールを送信いただくか、メール送信ツールをお持ちであれば、そちらを使って訓練メールの送信を行っていただくことになります。



訓練メールの作成例

左記は訓練メールの作成例です。実際に訓練メールを作成する際は、以下のような点を考慮の上、本文と添付ファイルの名前をどのようなものにするのが適切か？を検討してください。

①訓練対象者のセキュリティ知識レベルは高い？それとも低い？
②誰から送られたメール（送信元アドレス及び送信者名）だと引っかかりやすいか？
③本文の内容がどのようなものだと、引っかかりやすいか？
④本文のフォーマットがどのようになっていると引っかかりやすいか？
⑤メールのタイトルがどのようになっていると、メールを開いてしまいやすいか？

ちなみにメールの差出人については、有名な団体名に似せたものなど、外部からの送信を装うことを希望される方が多いのですが、社内からのメールを装ったケースも、意外と騙されてしまいやすいパターンです。

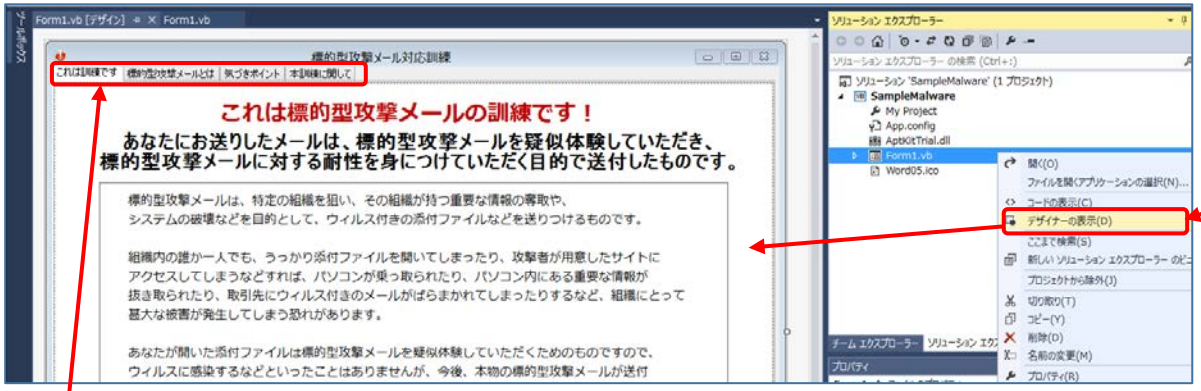
社内からのメールを装うケースでは、アドレスを詐称するといった必要も無く、メールの送信も比較的やりやすいので、訓練を実施されたことがない組織でしたら、まずは社内からのメールを装うケースで訓練を実施されることをお奨めします。

模擬マルウェアファイルの編集

初期の手順では、模擬マルウェアファイルのテンプレートを用いて新規に作成したプログラムは全く加工せずに、ソリューションのビルドを行って、exe 実行ファイルを生成しましたが、この状態では、模擬マルウェアプログラムを実行した方が誰であるのか？を特定するための開封者情報の送信が行われません。
また、模擬マルウェアプログラムを実行した際に表示されるダイアログもデフォルト設定のままであるため、訓練で使用できるよう、編集を行う必要があります。

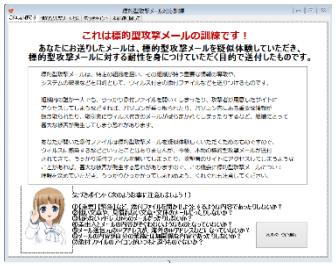
◆ダイアログ表示の編集（表示される画面の編集）

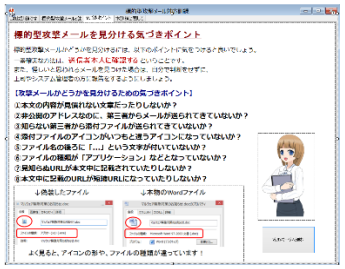
模擬マルウェアプログラムを実行した際に表示される画面を編集するには、Visual Studio Express の画面で「ソリューションエクスプローラー」を表示し、「Form1.vb」を選択してマウスの右ボタンを押し、「デザイナーの表示」を選択します。



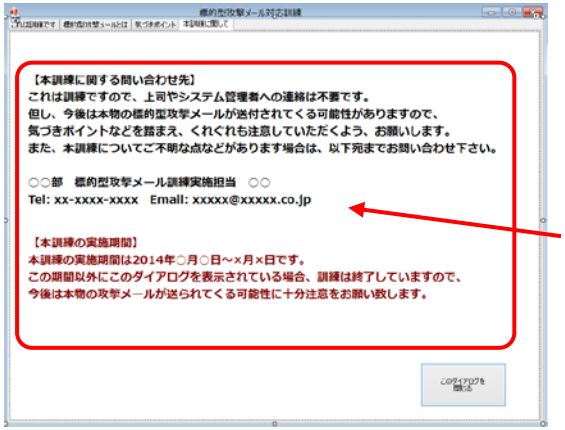
「デザイナーの表示」をクリックすると、
模擬マルウェアプログラムのフォーム画面が
表示され、編集できるようになります。

模擬マルウェアプログラムで用意されている表示画面は４つのタブ画面で構成されており、タブの部分をクリックすることで、それぞれの画面を編集することができます。





３つのタブ画面で、標的型攻撃メールに関する知識と、見分け方のポイントを説明しています。
これらをそのままお使いいただいても構いませんし、使えそうな部分だけ使い、他は独自のコンテンツに入れ替えていただくような使い方をされても構いません。

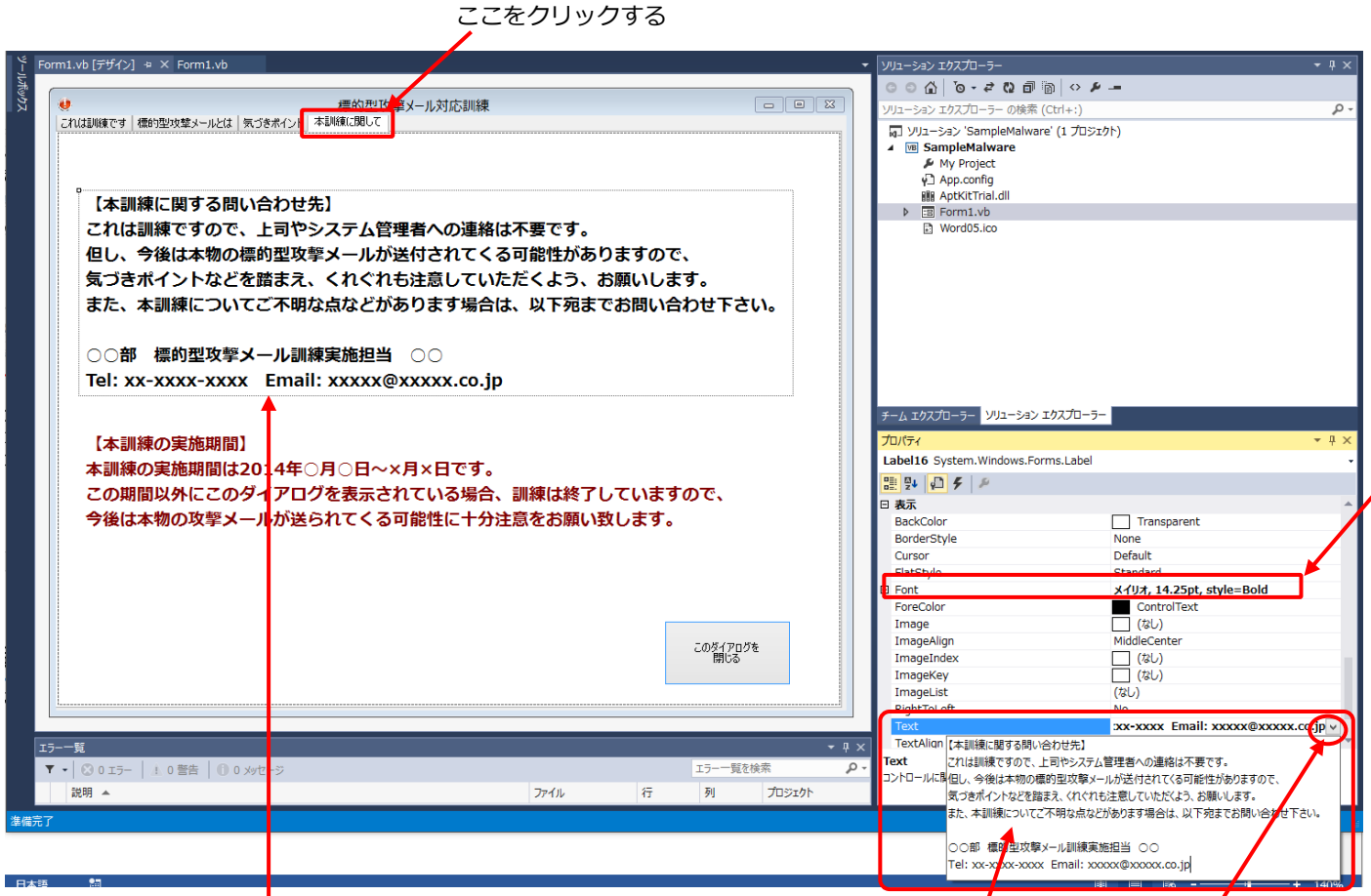


訓練対象者が本物の攻撃メールであると間違えないよう、訓練主催者の情報を表示する画面です。

訓練実施期間や問い合わせ先などを記載する場所となっていますので、最低限、この部分については編集を行っていただくことになります。

模擬マルウェアファイルのタブ画面表示の編集

模擬マルウェアプログラムのタブ画面の表示（フォーム画面の表示）を変更するには、以下のようにします。
Visual Studio Express でのフォーム画面編集の詳細について知りたい方は、関連書籍などをあたられることをお奨めします。
また、少し古いですが、http://www.atmarkit.co.jp/fdotnet/chushin/introwinform_index/index.html も参考になるかと思います。



プロパティの設定を変更することにより、表示形態を変えることができます。

例えば、表示されるフォントの種類や大きさを変えたい場合は、「Font」プロパティを変更します。

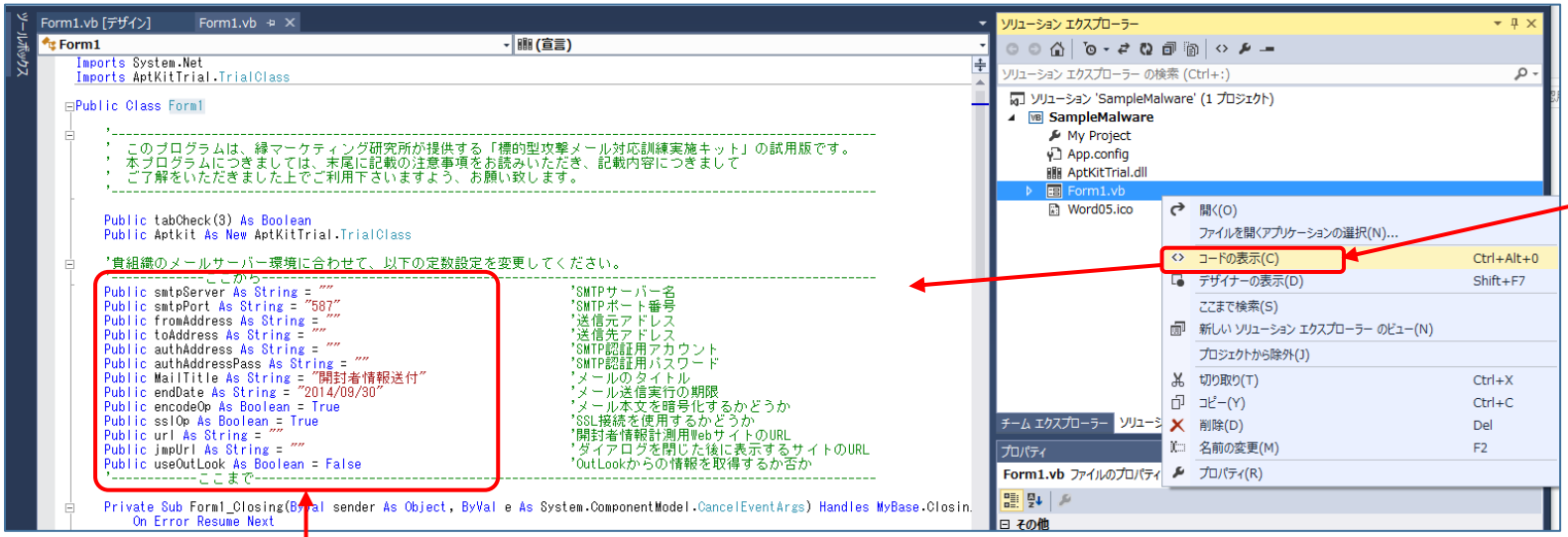
編集を行いたいパーツをクリックします。

編集を行いたいパーツをクリックすると、プロパティが表示されるので、「Text」の部分を選択し、ドロップダウンボタンを押して、設定されているテキストの本文を表示させます。

テキストボックスの部分をクリックすると、編集モードになり、設定されている内容の編集ができるようになるので、設定されている文字列を表示させたい内容に修正します。

模擬マルウェアファイルのプログラムコードの編集

模擬マルウェアプログラムが実行された際に、開封者情報が送信されるようにするには、プログラムコード内に、SMTP サーバの情報などを設定する必要があります。プログラムコードを編集するには、以下のようにします。



「コードの表示」をクリックすると、
模擬マルウェアプログラムの
コード編集画面が表示され、
プログラムコードを編集集できるように
なります。

プログラムコード内の「ここから」「ここまで」の間の部分に、SMTP サーバの情報などを設定します。
赤枠の部分以外については、ご自身でプログラムのカスタマイズを希望されるので無い限りは、変更は不要です。
各変更箇所に設定すべき事項については、キット一式に同梱されている「模擬マルウェアプログラム作成の手引き.pdf」を参照願います。

SMTP サーバの情報などを設定するに際しては、KitCheck ツールをご活用頂けます

KitCheck ツールは、貴社環境において、キットを使って作成した模擬マルウェアが開封者情報を収集できるか？
また、開封者情報を送信することができるかどうか？を確認するためのツールですが、このツールに設定した情報は、
模擬マルウェアプログラムのコードに設定する情報とイコールになります。

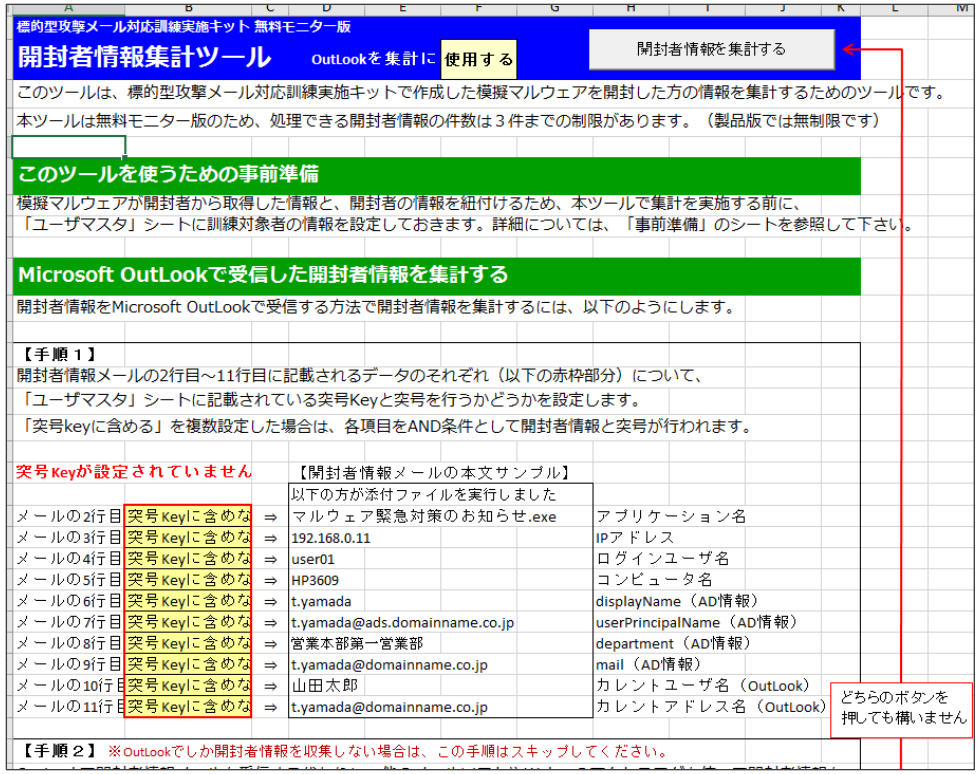
このため、Visual Studio Express を使ってプログラムコードを編集する前に、KitCheck ツールを用いて、SMTP サーバの情報を確認しておくと、プログラムコードの編集をスムーズに行っていただくことができるかと思います。

KitCheck ツールの使い方については、キットに同梱の「キット使用可否判定ツールの使い方.pdf」を参照願います。

開封者情報の集計

模擬マルウェアプログラムに SMTP サーバの情報などを設定し、開封者情報が送信されるようにした exe 実行ファイルを作成したら、訓練メールに添付して、実際に模擬訓練を行ってみましょう。訓練メールに添付された模擬のマルウェアプログラムが実行されると、プログラムコード内に設定した宛先に、開封者情報がメールで送信されます。

Microsoft OutLook を使って開封者情報を受信するようにすると、キットに同梱の「開封者情報集計ツール」を用いて、簡単に開封者情報の集計を行うことができます。なお、社内で使用可能なメールソフトが規定されているなどにより、OutLook が使用できない場合は、お使いのメールソフトが eml 形式ファイルへの出力に対応していれば、「開封者情報集計ツール」を用いて、開封者情報の集計を行っていただくことができます。
例えば、無償で利用できるメールソフト「Thunderbird」は、eml 形式ファイルへの出力に対応しています。



開封者情報集計ツール

開封者情報集計ツールは、Microsoft OutLook と組み合わせて使用していただくことにより、面倒な開封者情報集計作業を、簡単に行うことができるツールです。

このツールを用いての開封者情報の集計手順は、以下のようになります。

①訓練対象者が模擬のマルウェアプログラムを実行する。

②①により、模擬のマルウェアプログラムが開封者情報を指定のアドレス宛に送信する。

③Microsoft OutLook を用いて、指定のアドレス宛に届いた開封者情報のメールを受信する。

④開封者情報集計ツールを実行し、開封者情報を格納した OutLook のメール受信フォルダを選択する。

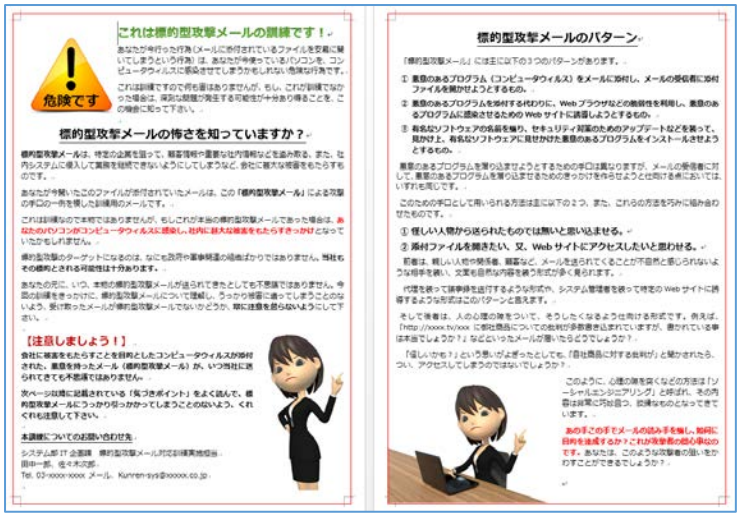
⑤ツールが、選択したフォルダから自動的に開封者情報の収集、解析を行い、集計結果を作成する。

なお、Microsoft OutLook が利用できない場合でも、開封者情報集計は可能です。詳細は、キットに同梱の開封者情報集計ツールに記載の説明を参照願います。

Word 文書ファイル添付型の訓練実施

P.22～P.25

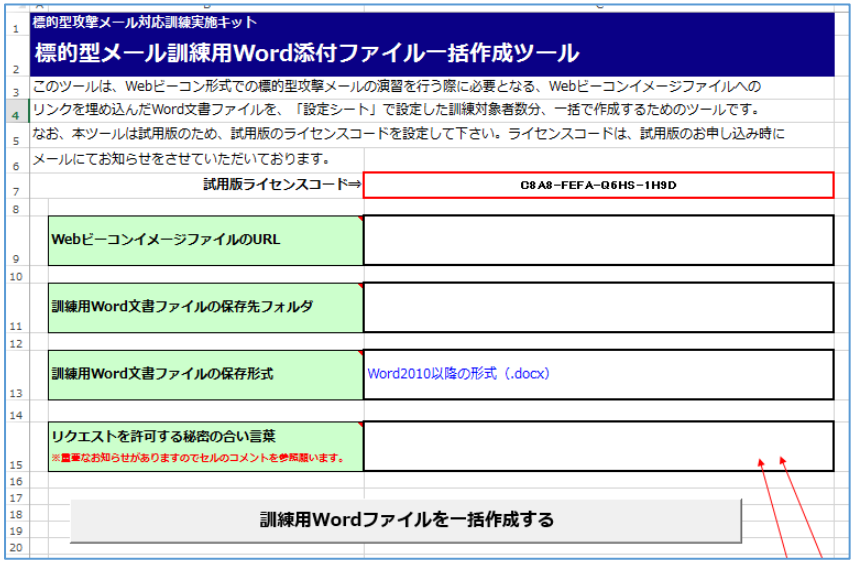
まずは、オリジナルの Word 文書ファイルを用意しましょう



Word 文書ファイル添付型の訓練を実施するには、まず初めに、訓練メールに添付する Word 文書ファイルのオリジナルとなる文書ファイルを作成します。

キットには、ひな形の文書ファイルとして、「template.docx」（左記の図）が付属しています。この文書ファイルをそのまま使用いただいても構いませんし、独自に文書ファイルを作成いただいても構いません。Word 文書ファイル自体は通常の文書ファイルでよいので、内容自体はどのようなものでもお使いいただけます。

個別の Word 文書ファイルの作成を行います



オリジナルとなる文書ファイルを用意したら、Word 添付ファイル一括作成ツールを用いて、訓練対象者毎の Word 文書ファイルを作成します。

添付ファイル一括作成ツールでは、オリジナルの Word 文書ファイルをコピーし、文書末尾に、訓練対象者毎の識別情報を設定した、横 1 ドット×縦 1 ドットの Web ビーコンを埋め込んだ Word 文書を生成します。

ツールの使い方については、添付ファイル一括作成ツールに説明の記載がありますので、そちらをご参照ください。

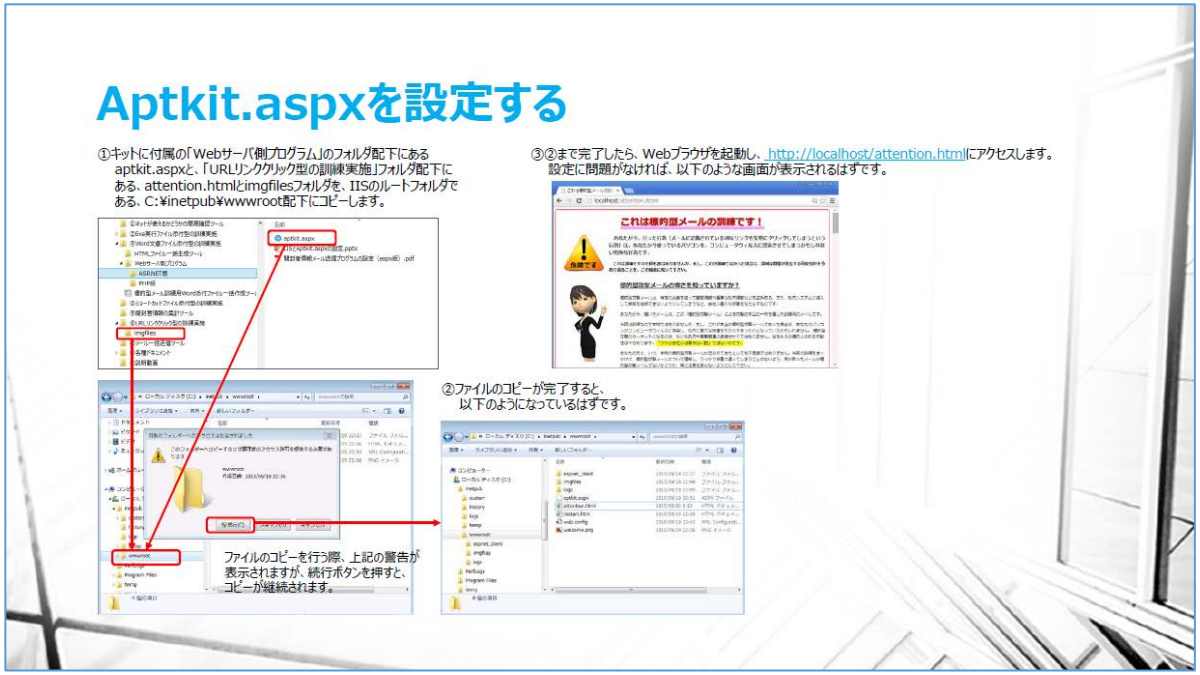
Web サーバ側の設定を行います

Word 文書ファイル添付型の訓練を実施するには、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 ASP.NET 版プログラムもしくは、PHP 版プログラムのどちらかを設置いただく必要があります。

ちなみに Web サーバというと、専用のサーバ用コンピュータと、サーバ用の OS が必要となってしまうのでは？思われるかもしれませんが、Windows7 であれば、標準で IIS という Web サーバソフトをインストールすることが可能です。Windows のクライアント用 OS では、同時接続数に制限がありますが、Windows7 以降の OS でインストールできる IIS は、同時接続数を超える接続があっても、レスポンスが待たされることになるだけで、アクセスエラーにはなりません。レスポンスが待たされるといっても、1 分間に数百人分のアクセスを処理することは十分可能なので、訓練用として使用する分には、同時接続数の制限は実質的に考慮する必要がないとお考え頂いて差し支え有りません。

このため、訓練用にわざわざサーバ用コンピュータとサーバ用 OS を用意いただかなくとも、現在お使いの業務用のパソコンを利用して訓練を実施いただくことが可能です。

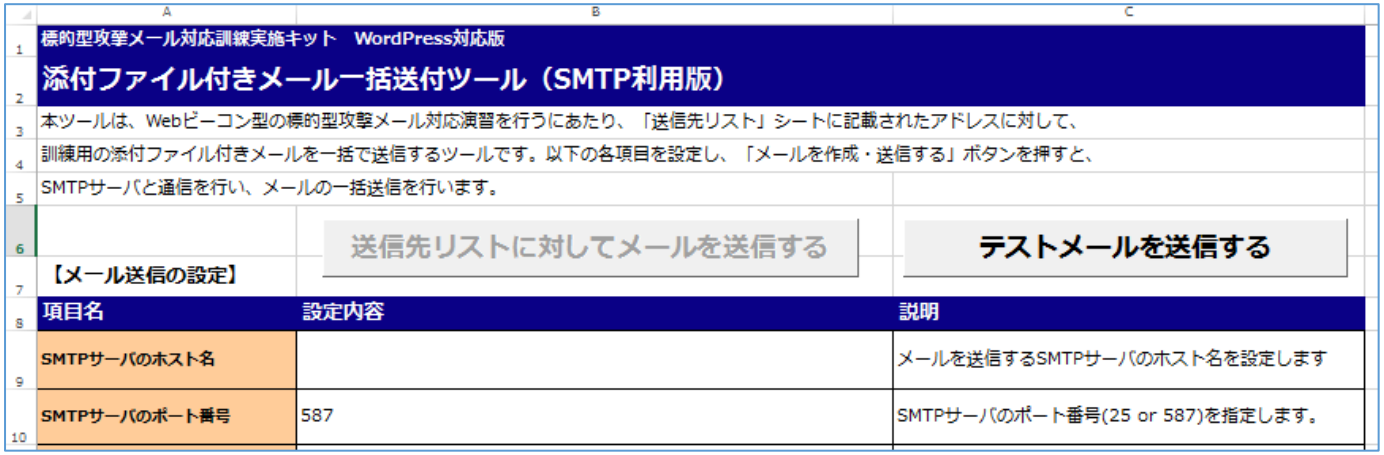
Web サーバ側に設置するプログラムの設定方法については、ASP.NET 版と PHP 版で異なりますので、キットに付属するそれぞれの説明資料をご参照ください。



Word 文書ファイルが添付された訓練メールの送信を行います

キットに付属の、メール一括送付ツール（SMTP 利用版）を使い、訓練対象者に対して、個別の Word 文書ファイルを添付したメールを一括送信します。

なお、メールの一括送付については、必ずしもメール一括送付ツール（SMTP 利用版）をお使いいただく必要はありません。既にお持ちのツールなどがあれば、そちらをお使いいただいても構いません。



標的型攻撃メール対応訓練実施キット　WordPress対応版

添付ファイル付きメール一括送付ツール（SMTP利用版）

本ツールは、Webビーコン型の標的型攻撃メール対応演習を行うにあたり、「送信先リスト」シートに記載されたアドレスに対して、
訓練用の添付ファイル付きメールを一括で送信するツールです。以下の各項目を設定し、「メールを作成・送信する」ボタンを押すと、
SMTPサーバと通信を行い、メールの一括送信を行います。

送信先リストに対してメールを送信する　　テストメールを送信する

【メール送信の設定】

項目名	設定内容	説明
SMTPサーバのホスト名		メールを送信するSMTPサーバのホスト名を設定します
SMTPサーバのポート番号	587	SMTPサーバのポート番号(25 or 587)を指定します。

開封者情報メールが送付されることを確認します

訓練メールが届いたら、添付の Word 文書ファイルを開きます。Web サーバへのアクセスが発生すれば、開封者情報メールが送付されます。

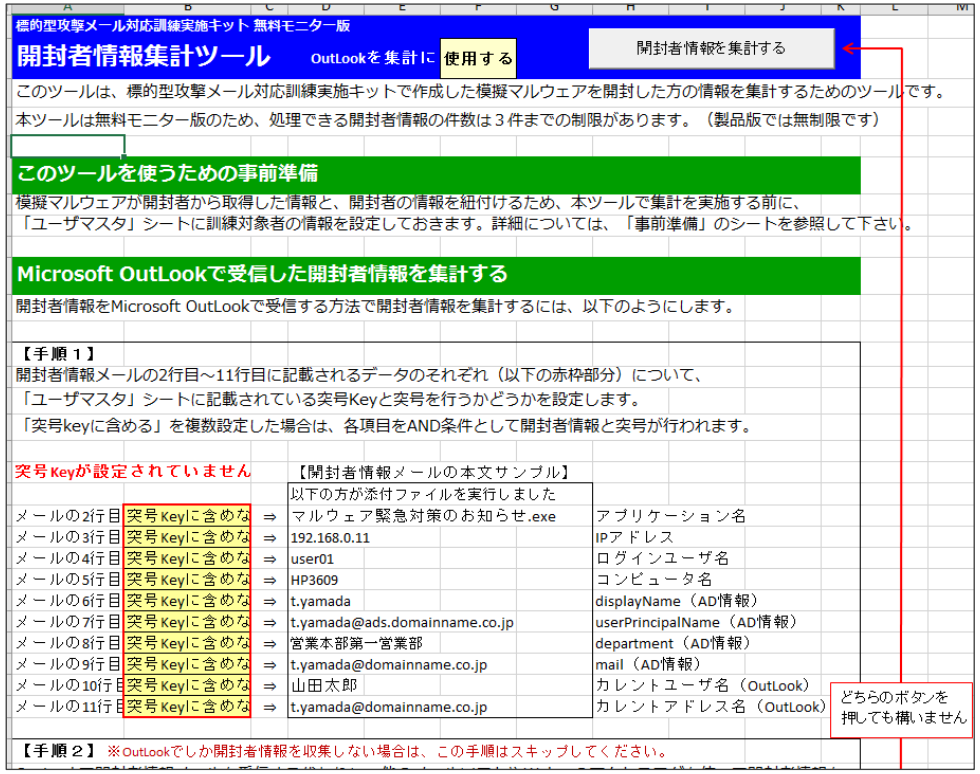
もし、開封者情報メールが届かないようであれば、Web サーバ側の設定と、Word 文書一括作成ツールで設定した情報が一致しているかどうかを確認します。

なお、メールに添付された Word 文書ファイルが開かれる際には、警告が表示される場合があります。この際、文書ファイルを無効化する選択をした場合は、Web サーバへのアクセスが発生せず、開封者情報メールは届かないことになります。

開封者情報の集計を行います

開封者情報メールが送信されることを確認したら、キットに付属の開封者情報集計ツールを使い、メールソフトで受信した開封者情報を元に、開封者情報の集計を行います。

Microsoft OutLook を使って開封者情報を受信するようにすると、キットに同梱の「開封者情報集計ツール」を用いて、簡単に開封者情報の集計を行うことができます。なお、社内で使用可能なメールソフトが規定されているなどにより、OutLook が使用できない場合は、お使いのメールソフトが eml 形式ファイルへの出力に対応していれば、「開封者情報集計ツール」を用いて、開封者情報の集計を行っていただくことができます。
例えば、無償で利用できるメールソフト「Thunderbird」は、eml 形式ファイルへの出力に対応しています。



開封者情報集計ツール

開封者情報集計ツールは、Microsoft OutLook と組み合わせて使用していただくことにより、面倒な開封者情報集計作業を、簡単に行うことができるツールです。

このツールを用いての開封者情報の集計手順は、以下のようになります。

①訓練対象者が模擬のマルウェアプログラムを実行する。

②①により、模擬のマルウェアプログラムが開封者情報を指定のアドレス宛に送信する。

③Microsoft OutLook を用いて、指定のアドレス宛に届いた開封者情報のメールを受信する。

④開封者情報集計ツールを実行し、開封者情報を格納した OutLook のメール受信フォルダを選択する。

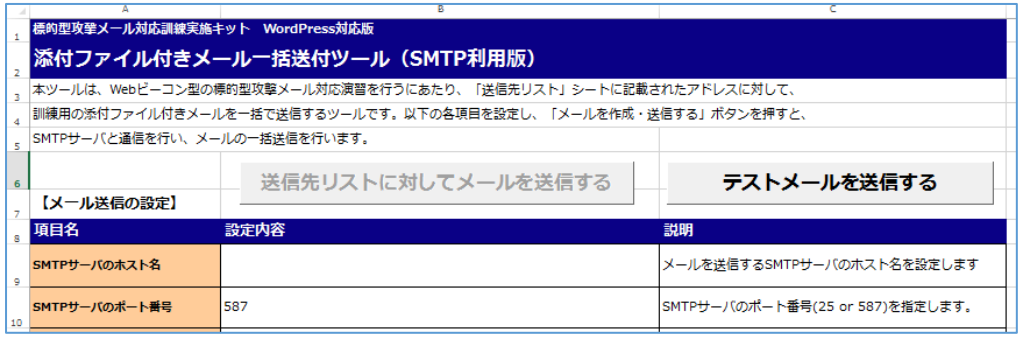
⑤ツールが、選択したフォルダから自動的に開封者情報の収集、解析を行い、集計結果を作成する。

なお、Microsoft OutLook が利用できない場合でも、開封者情報集計は可能です。
詳細は、キットに同梱の開封者情報集計ツールの説明情報を参照願います。

URL リンククリック型の訓練実施

P.27～P.29

メール本文中に URL リンクを埋め込んだ訓練メールを送信する



標的型攻撃メール対応訓練実施キット　WordPress対応版

添付ファイル付きメール一括送付ツール（SMTP利用版）

本ツールは、Webビーコン型の標的型攻撃メール対応演習を行うにあたり、「送信先リスト」シートに記載されたアドレスに対して、
訓練用の添付ファイル付きメールを一括で送信するツールです。以下の各項目を設定し、「メールを作成・送信する」ボタンを押すと、
SMTPサーバと通信を行い、メールの一括送信を行います。

送信先リストに対してメールを送信する　　テストメールを送信する

【メール送信の設定】

項目名	設定内容	説明
SMTPサーバのホスト名		メールを送信するSMTPサーバのホスト名を設定します
SMTPサーバのポート番号	587	SMTPサーバのポート番号(25 or 587)を指定します。

URL リンククリック型の訓練を実施するには、訓練メールの本文中に URL リンクを埋め込んだ訓練メールを送信する必要があります。

キットに付属している「メール一括送付ツール」では、訓練メールの本文中に、メールの送信先毎に異なる URL リンクを埋め込んだ訓練メールを送信することができるようになっています。

URL リンククリック型の訓練では、メール本文中の URL リンクがクリックされたら、Web サーバーに設置した aptkit.aspx（又は aptkit.php）が呼び出され、Web サーバーから指定のメールアドレス宛（一般的には、訓練実施担当者のメールアドレス）に開封者情報メールの送付が行われると同時に、指定の URL にリダイレクトされる流れとなります。

キットでは、リダイレクト先となる Web ページの雛形として、従業員教育用のコンテンツをご用意していますので、この雛形をお使い頂くことで、訓練メール本文中の URL リンクをクリックしてしまった従業員に対しては、標的型メールに関する教育用の Web ページを参照してもらうようにすることができます。

訓練メールの本文中に URL リンクを埋め込むには、メール一括送付ツールの「送信先リスト」シートにおいて、以下のように設定することで、メールの送付先アドレス毎に、異なる URL リンクを埋め込んだ形でメールを送信することができます。設定方法については、メール一括送付ツールに記載の「使い方」の説明をお読み頂くと共に、キットに同梱の資料「URL リンククリック型の訓練実施について.pdf」を参照願います。

G	H	I	J
メールに記載するURL	実際にアクセスするURL	ユーザ特定用キーワード	不正アクセス防止用キーワード
http://hoge.jp/index.html	http://hoge.jp/aptkit.aspx	ret=user001	kwd=passwd

「メール本文①」シートでの本文設定例　その１

先般ご案内した、危険性の高いスパムメールへの対策と
緊急対処を実施いただきたく、対応お願いします。
具体的な対処方法については添付資料をご確認ください。

【本メールに関する詳細はこちらをご参照ください】
%URL%

【添付ファイル名】
緊急対処方法のご案内.zip

実際に送付されるメールの本文

先般ご案内した、危険性の高いスパムメールへの対策と
緊急対処を実施いただきたく、対応お願いします。
具体的な対処方法については添付資料をご確認ください。

【本メールに関する詳細はこちらをご参照ください】
http://www.hoge.jp/aptkit.php?ret=user001&kwd=passwd

【添付ファイル名】
緊急対処方法のご案内.zip

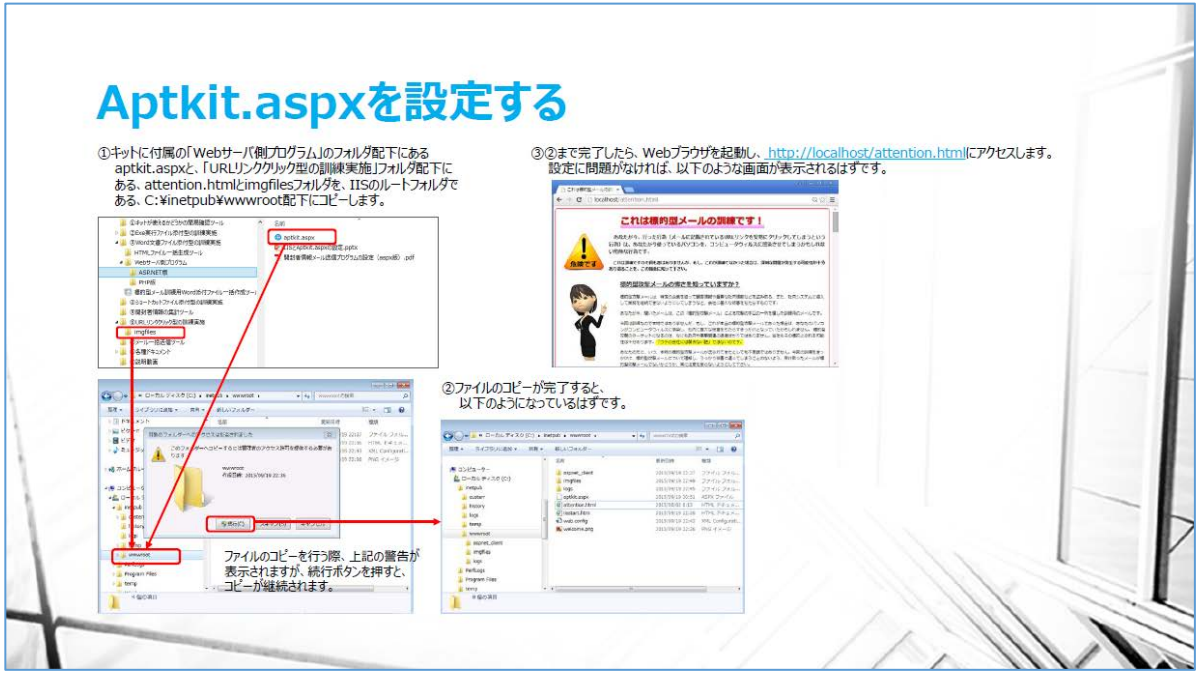
Web サーバ側の設定を行います

URL リンククリック型の訓練を実施するには、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 ASP.NET 版プログラムもしくは、PHP 版プログラムのどちらかを設置いただく必要があります。

ちなみに Web サーバというと、専用のサーバ用コンピュータと、サーバ用の OS が必要となってしまうのでは？思われるかもしれませんが、Windows7 であれば、標準で IIS という Web サーバソフトをインストールすることが可能です。Windows のクライアント用 OS では、同時接続数に制限がありますが、Windows7 以降の OS でインストールできる IIS は、同時接続数を超える接続があっても、レスポンスが待たされることになるだけで、アクセスエラーにはなりません。レスポンスが待たされるといっても、1 分間に数百人分のアクセスを処理することは十分可能なので、訓練用として使用する分には、同時接続数の制限は実質的に考慮する必要がないとお考え頂いて差し支え有りません。

このため、訓練用にわざわざサーバ用コンピュータとサーバ用 OS を用意いただかなくとも、現在お使いの業務用のパソコンを利用して訓練を実施いただくことが可能です。

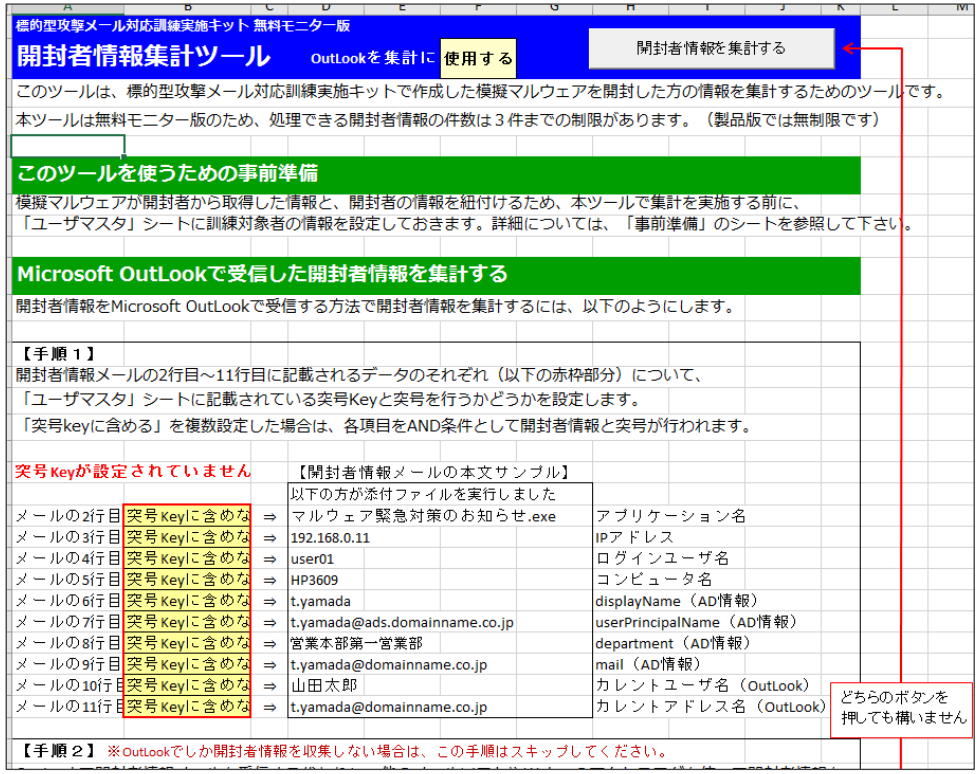
Web サーバ側に設置するプログラムの設定方法については、ASP.NET 版と PHP 版で異なりますので、キットに付属するそれぞれの説明資料をご参照ください。
また、URL リンククリック型の訓練を実施する場合のプログラムの設定については、キットに付属の資料「URL リンククリック型の訓練実施について.pdf」を参照して下さい。



開封者情報の集計を行います

訓練メールの本文中にある URL リンクをクリックすると、Web サーバへのアクセスが発生し、開封者情報のメールが送信されます。開封者情報メールが送信されることを確認したら、キットに付属の開封者情報集計ツールを使い、メールソフトで受信した開封者情報を元に、開封者情報の集計を行います。

Microsoft OutLook を使って開封者情報を受信するようにすると、キットに同梱の「開封者情報集計ツール」を用いて、簡単に開封者情報の集計を行うことができます。なお、社内で使用可能なメールソフトが規定されているなどにより、OutLook が使用できない場合は、お使いのメールソフトが eml 形式ファイルへの出力に対応していれば、「開封者情報集計ツール」を用いて、開封者情報の集計を行っていただくことができます。
例えば、無償で利用できるメールソフト「Thunderbird」は、eml 形式ファイルへの出力に対応しています。



開封者情報集計ツール

開封者情報集計ツールは、Microsoft OutLook と組み合わせて使用していただくことにより、面倒な開封者情報集計作業を、簡単に行うことができるツールです。

このツールを用いての開封者情報の集計手順は、以下のようになります。

①訓練対象者が模擬のマルウェアプログラムを実行する。

②①により、模擬のマルウェアプログラムが開封者情報を指定のアドレス宛に送信する。

③Microsoft OutLook を用いて、指定のアドレス宛に届いた開封者情報のメールを受信する。

④開封者情報集計ツールを実行し、開封者情報を格納した OutLook のメール受信フォルダを選択する。

⑤ツールが、選択したフォルダから自動的に開封者情報の収集、解析を行い、集計結果を作成する。

なお、Microsoft OutLook が利用できない場合でも、開封者情報集計は可能です。
詳細は、キットに同梱の開封者情報集計ツールの説明情報を参照願います。

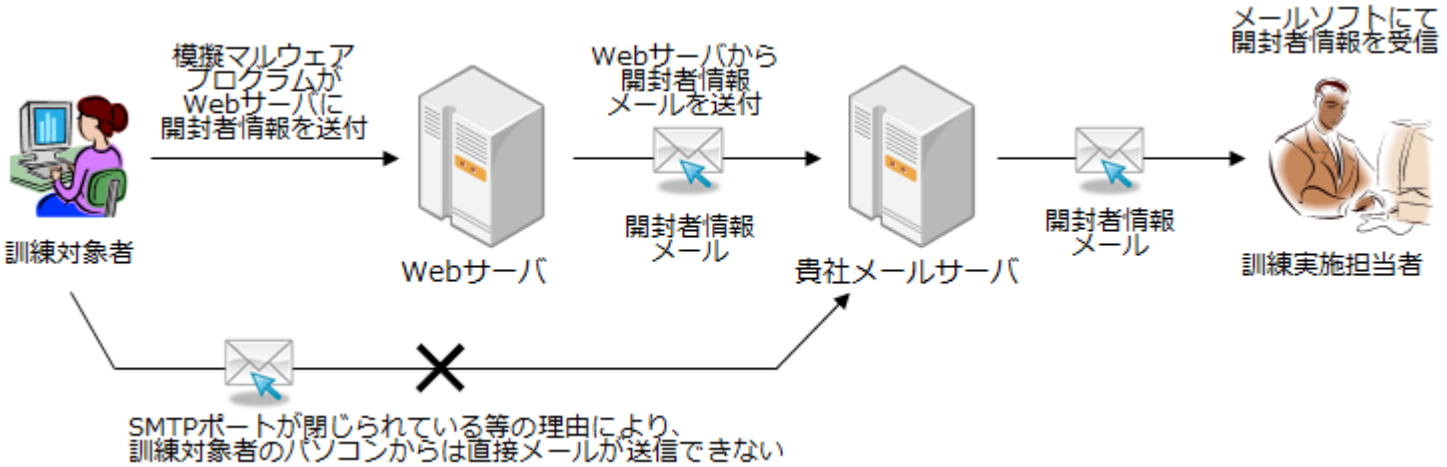
exe 実行ファイル添付型の訓練実施において、

SMTP サーバが利用できない場合の代替策

P.31～P.32

訓練対象者のパソコンからメールが送信できない場合の代替策について

セキュリティ設定の関係で、SMTP ポートを閉じているなど、訓練対象者のパソコンから直接メールを送信することができない場合は、
Web サーバに開封者情報を送付し、Web サーバ側から開封者情報のメールを送付する代替策がご利用いただけます。
但し、この代替策を利用する場合は、訓練対象者のパソコンからアクセスが可能な Web サーバをご用意いただく必要があります。



【ご用意いただく Web サーバの条件】

Web サーバ経由で開封者情報メールを送付する方式をご利用の場合は、以下の条件を満たす Web サーバをご用意下さい。

1．ASP.NET もしくは、PHP のプログラムが動作する
2．SMTP サーバに接続してのメール送信が可能となっている（aptkit.php をお使い頂く場合）

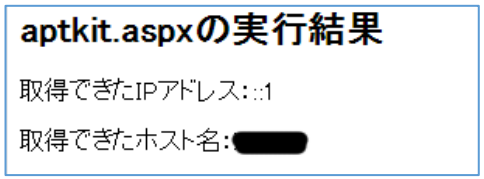
なお、Web サーバとして利用するコンピュータは、サーバ用のコンピュータである必要はありません。
使用可能な Web サーバをお持ちであれば、そちらをご利用いただいてもよいですが、無い場合は、今お使いのパソコンに Web サーバソフトをインストールし、簡易な Web サーバとしてご利用いただく形で十分です。

IIS であれば、Windows7 に標準で付属しており、ASP.NET 版のプログラムがご利用いただけますので、こちらをご利用いただく方法がお手軽です。また、IIS をお使い頂く場合は、Web サーバから送信されるメールを、SMTP サーバには送らずに Web サーバ内に保存する方法も選択頂けます。このため、IIS をお使い頂く場合は SMTP サーバがご利用いただけない環境でも開封者情報を収集することができます。

Web サーバへのプログラムの設置について

Web サーバをご用意いただいたら、Web サーバに開封者情報を送付するためのプログラムを設置します。
キットに付属のプログラムを Web サーバが参照するフォルダ配下にコピーし、Web ブラウザからアクセスできるようにしてください。

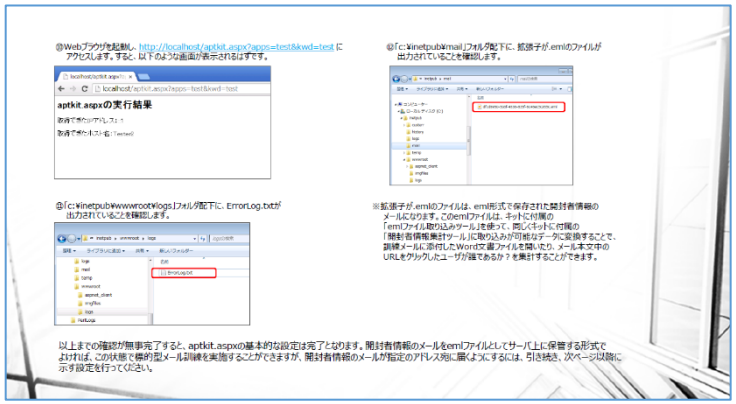
【aptkit.aspx をお使いの場合の動作確認方法】



Aptkit.aspx をお使いの場合は、「http://web サーバのアドレス/aptkit.aspx?apps=test&kwd=xxxx」（xxxx の部分は設定された不正アクセス防止用のパスワードになります）の URL でアクセスすると、左のように、取得できた IP アドレスとホスト名が表示されます。
左のようなページが表示されない場合は、プログラムが正しく動いていないことになりますので、IIS の設定として、ASP.NET が使るようになっているかどうか、また、ErrorLog.txt にエラーメッセージが出力されていないかどうかを確認してください。

【Web サーバ側プログラムの設定変更】
Web サーバに設置したプログラムへのアクセスがエラー無く行えるようであれば、プログラム内の設定を変更し、開封者情報メールが自分宛に届くようにします。設定を変更したら、「http://web サーバのアドレス/aptkit.aspx?apps=user01&kwd=xxxx」のように、パラメータに?apps=user01 と付けてアクセスしてみて下さい。開封者情報メールが届けば、Web サーバ側の設定は完了です。なお、URL リンククリック型の訓練を実施される場合は、リダイレクトされることの確認として、
「http://web サーバのアドレス/aptkit.aspx?user=user01&kwd=xxxx」のような URL でアクセスを行ってみてください。

Web サーバ側に設置するプログラムの設定方法については、ASP.NET 版と PHP 版で異なりますので、キットに付属するそれぞれの説明資料をご参照ください。



キットご利用のフォローアップについて

標的型攻撃メール対応訓練実施キットでは、サポート用 Web サイトによる情報共有型のサポートをご提供しております。

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、まずは以下のサイトにアクセスしていただき、問題解決に役立つ情報があるかどうかをご確認ください。

サポート用 Web サイトにヒントとなる回答がない、また、個別のご質問がございます場合は、サポート用 Web サイトからリクエストを送信いただくか、ask@kunrenkit.jp 宛までメールをお送り下さい。

【本キットのサポート用 Web サイト】

https://support.kunrenkit.jp/