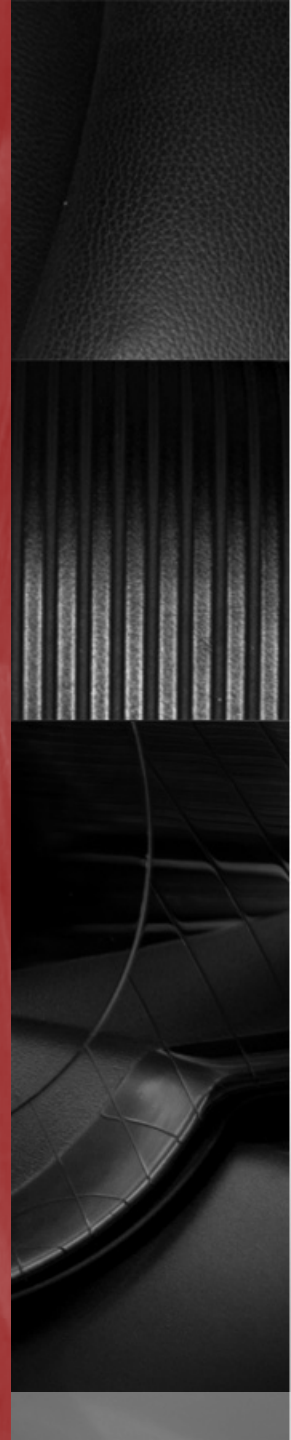
標的型攻撃メール
対応訓練実施キットの概要



縁マーケティング研究所

標的型攻撃メール対応訓練実施キットは、
組織に甚大な被害をもたらす

「悪意のあるプログラム」が埋め込まれたメールを

うっかり開いてしまわないよう、模擬の標的型攻撃メールを
使って実際に体験してもらうことで、

「標的型攻撃メール」

というものがあることを知ってもらい、
悪意のある攻撃者から自分の身と組織を守る術を
身につけてもらうことを目的とするものです。

標的型攻撃メール対応訓練実施キットには、
訓練を実施するために必要な以下のもの一式が含まれています。

1．模擬のマルウェアプログラム

2．訓練用のメール本文の文例（テンプレート）

3．訓練の実施手引書

4．訓練対象者向けの教育用コンテンツ

5．模擬マルウェア開封者の集計用ツール

既に出来上がっているものを利用するので、
面倒な文章を考えたりといった訓練実施の準備の手間を
大幅に軽減できます。

このキットの特徴

1．Webビーコンを使う方法に比べて手間がかからない

2．マクロを使わないのでマクロが禁止されているパソコンも訓練対象とすることができる

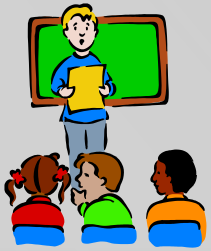
3．既に出来上がっているものを手直しするだけなので準備に手間がかからない

4．模擬マルウェア開封者の情報をメールで受信する形なのでリアルタイムに開封状況を確認できる

5．模擬マルウェア開封者の集計用ツールが用意されているので開封者情報の集計に手間がかからない

このキットを使った訓練実施の流れは以下のようになります。

① 訓練対象者に
事前の教育を実施



② 模擬のマルウェア
プログラムを作成

③ 訓練対象者に訓練
開始をアナウンス

④ 訓練対象者に
訓練メールを送信

⑤ ツールで模擬のマル
ウェアを開いた人の
情報を集計

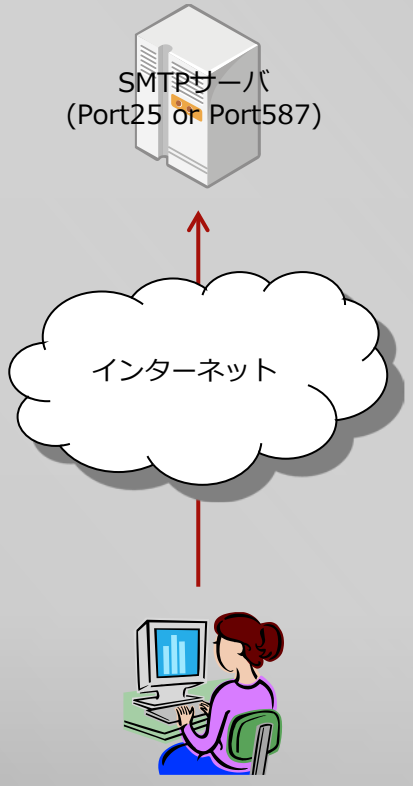
⑥ 訓練対象者に種を
明かして訓練終了

⑦ 効果測定のための
理解度測定を実施

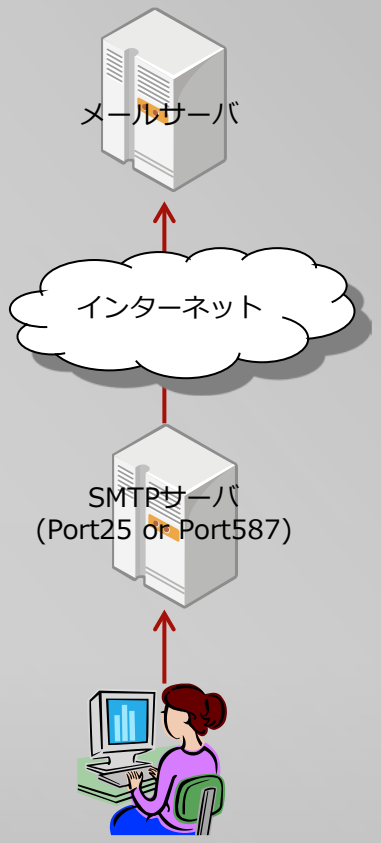
⑧ 実施結果から、
今後のアクション
プランを検討

以下のように、訓練対象者のパソコンがSMTPサーバに接続できる環境が用意できれば、このキットを使って訓練が実施できます。

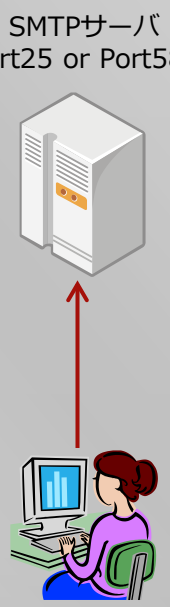
① 外部のSMTPサーバに接続して組織内のメールのやり取りができる



② 社内のSMTPサーバから外部のメールサーバを経由して、組織内のメールのやり取りができる



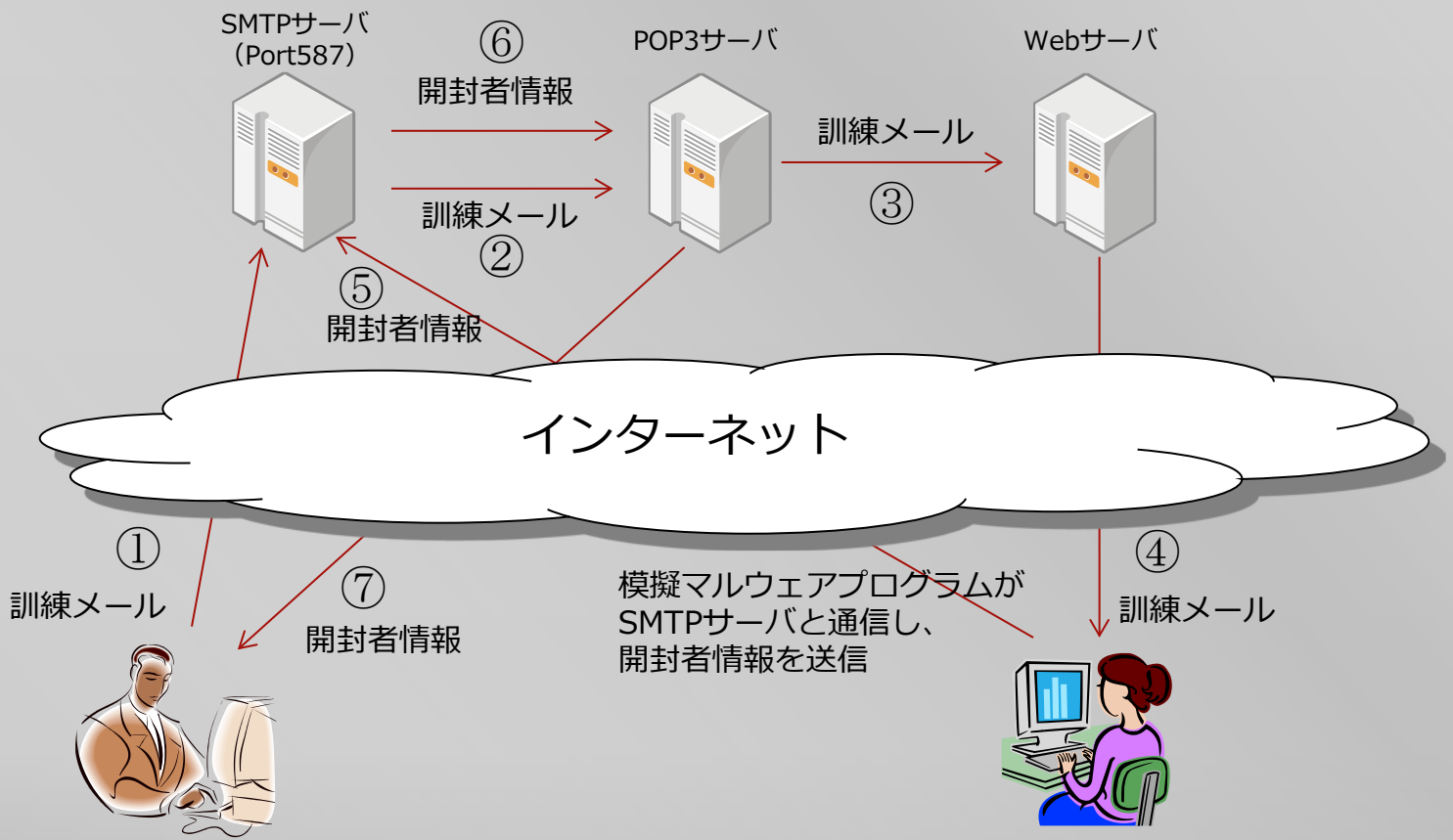
③ 組織内のメールのやり取りに社内のSMTPサーバが使える



訓練対象者がメールソフトに何を使っているかは問いません。

実施例1

サイボウズを使っている組織などでは、この図のようなパターンになります。

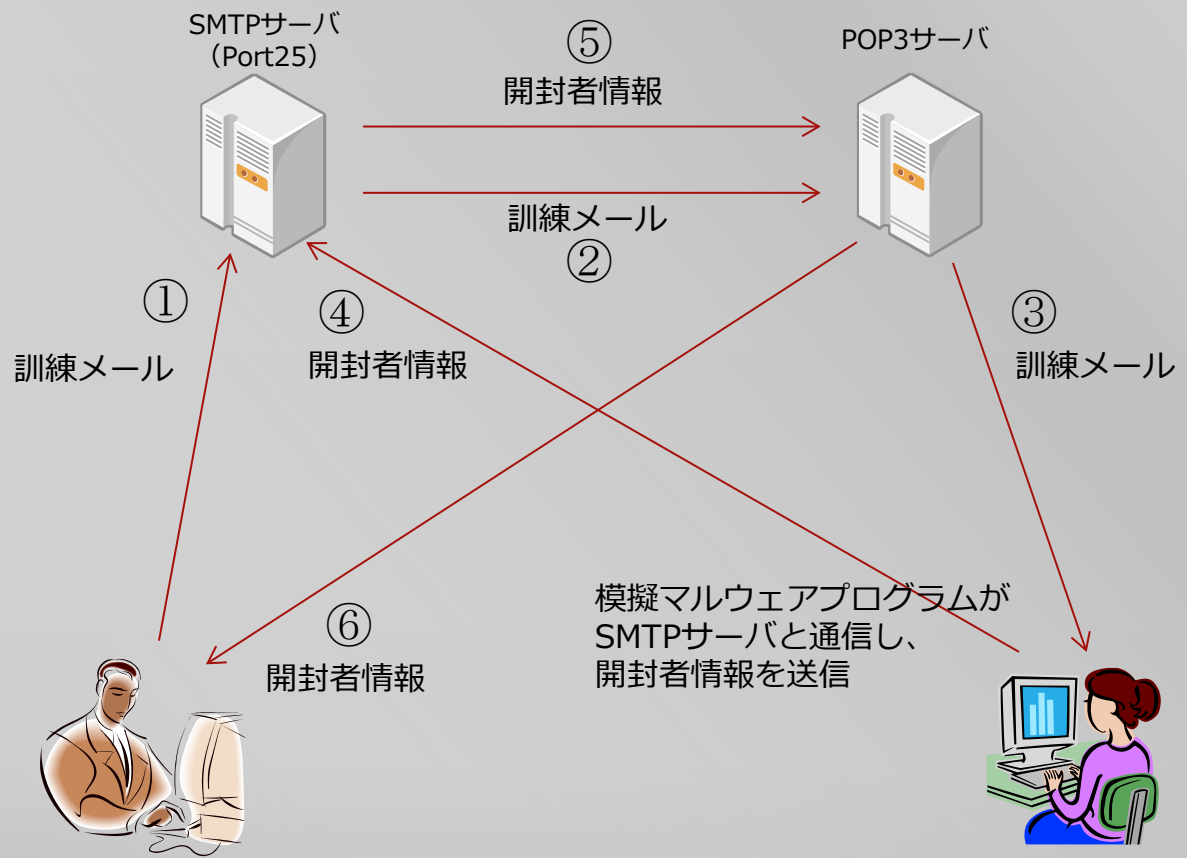


訓練実施担当者はメールサーバに
直接アクセスして一括で訓練メールを送信。
開封者情報はOutLookを使ってPOP3サーバから受信

訓練対象者はWebメーラーでメールを受信
模擬マルウェアを開封すると、開封者情報が
SMTPサーバを経由して訓練実施担当者に送付される。

実施例２

社内LANの中にSMTPサーバとPOP3サーバを置いている組織では、
この図のようなパターンになります。



訓練実施担当者はメールサーバに
直接アクセスして一括で訓練メールを送信。
開封者情報はOutLookを使ってPOP3サーバから受信

訓練対象者はメールソフトでメールを受信
模擬マルウェアを開封すると、開封者情報が
SMTPサーバを経由して訓練実施担当者に送付される。

社内にSMTPサーバが無い場合はどうすればいい？

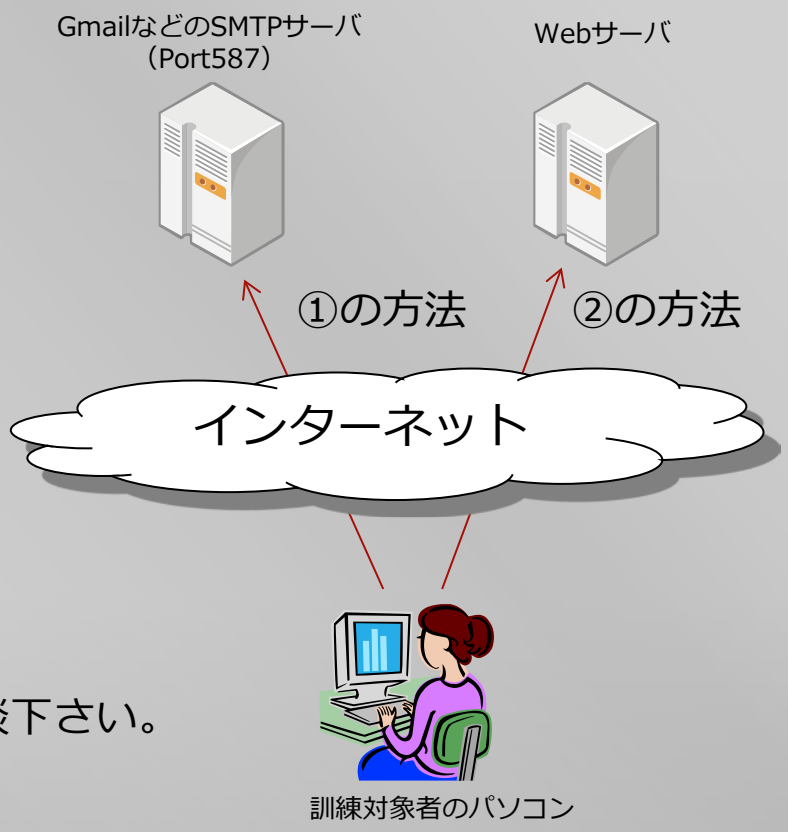
社内ではWebメーラーを使用しているので、使えるSMTPサーバがない。
という場合はどうすればいいでしょうか？

この解決方法は２つあります。

１．訓練対象者のパソコンからインターネット上の
SMTPサーバ（GmailのSMTPサーバなど）に
アクセスできる場合は、そのSMTPサーバを
使ってメールを送信するよう、模擬マルウェアを
設定する方法があります。

２．訓練対象者のパソコンからインターネット上の
Webサーバにアクセスできる場合は、
メール送信の代わりに、Webサーバに
アクセスする形で、開封者情報を送るよう、
模擬マルウェアを設定する方法があります。

※２．の場合はWebサーバの用意が必要になります。
Webサーバをご用意できないお客様については、
訓練用にお貸しするオプションもありますのでご相談下さい。



模擬マルウェアプログラムでは、訓練対象者のパソコンから
以下の順で情報を取得するようになっています。

１．ActiveDirectoryから取得できる情報

２．Microsoft OutLookに設定されているメールアドレス情報

３．パソコンのログイン情報

情報が取得できた段階で開封者情報の送信を行うため、
ActiveDirectoryに参加していない場合は、OutLookの情報を、
OutLookの情報も取得できない場合は、パソコンのログイン
情報を、開封者の情報として取得し、送信することになります。

開封者情報の送信に際しては、模擬マルウェアプログラムが、
SMTPサーバと直接通信を行って送信します。

模擬マルウェアプログラムが、SMTPサーバと直接通信できれば
よいので、訓練対象者が使用しているメールソフトは
何であっても構いません。

逆に、模擬マルウェアプログラムが、SMTPサーバと直接通信
できることが必要となってくるので、モバイル環境など、
模擬マルウェアプログラムが開かれた時に、SMTPサーバと
通信できない場合は、開封者情報を送ることはできません。

但し、画面は表示されるので、模擬マルウェアプログラムを
開封した方に、教育用コンテンツを見せることはできます。

※SMTPサーバと通信はできないが、外部のWebサイトへのアクセスはできるという場合は、
SMTPサーバと通信する代わりに、Webサーバにアクセスする方式にすることもできます。
このようなご希望があります場合はご相談ください。

開封者情報の内容については、暗号化してメール送信することが可能です。（暗号化しないでメールを送信することも可能です）

外部のSMTPサーバを介して開封者情報を受け取る場合、
メールの内容が第三者に知られてしまう可能性を心配されるかもしれませんが、暗号化への対応により、万一、開封者情報の内容が第三者に知られてしまったとしても、どのような内容が書かれているかわからないので、訓練対象者の情報が外部の第三者に知られてしまうことはありません。

【以下は暗号化された開封者情報の例】

TGGGG99D9TGGGG9YCBTGGGG93DDTGGGGY6GCTGGGG93BBTGGGGY46YTGGGGY685TGGGG9485TGGGG9451TGGGG9454TGGGG949CTGGGG93G1TGGGG9FD1TGGGG9E84TGGGG93C6TGGGG93EDTGGGG93C6TGGGG93CETETBTETBT64T76T74T65T76T84T85TETBT77T76T49T41T4BT4BT42T73T75T4BT43T45T74T74T4BT74T44T76T72T4BT73T72T48T44T36T42T45T3DT77T76T49T41T4BT4BT45T77T4BT43T49T42T49T4BT4YT46T45T73T4BT75T48T46T46T36T42T43T3DT42T4YT43T3FT42T47T49T3FT41T3FT49T3DT43T41T41T42T4BT41T4BT4YT75T44T49T4BT4YT41T75T48T4BT45T77T4BT43T49T42T49T4BT4YT46T45T73T4BT75T48T46T46TETBT5GT77T77T7YT74T76T43T41T42T41TETBT84T76T74T85T76T84T85T51T79T72T81T81T8YT76T89T74T76T7DT81T83T7GT7BT76T74T85T3FT74T7GT7E

模擬マルウェアプログラムは、exe実行ファイルです。
ExcelやWordのマクロではないので、訓練対象者のパソコンで
マクロが使えるようになっているかどうかは関係ありません。

exe実行ファイルなので、逆アセンブルしない限りは、
プログラムの内容が訓練対象者に知られることはありません。

また、開封者情報の送信は期限を設けることができますので、
模擬マルウェアプログラムが外部に送信された場合でも、
期限を過ぎてしまえば、画面が表示されるのみとなり、
開封者情報が送信されることはありません。

本キットでは、Excelで作成された以下のツールが提供されます。

１．開封者情報の集計ツール（キットに同梱）

開封者の情報が1通ずつメールで送られてくることになりますので、
このメールをMicrosoft OutLookで受信します。集計ツールを
起動し、メールを受信したOutLookのフォルダを指定すると、
そのフォルダ内に保存されているメールから開封者の情報を
取り出し、Excelのシートに一覧として出力を行います。

フォルダを指定するだけの操作なので集計に手間がかかりません。

２．メールの一括送信ツール（キット購入者特典として提供）

Excelのシートに記載されている訓練対象者のメールアドレスを元に、
メールを個別に自動送信します。Microsoft OutLookによる
メール送信を自動化するツールのため、Microsoft OutLookが
必要になります。

Webビーコンを使う方法と何が違うのか？

１．訓練対象者ごとに添付ファイルと画像を作らなくて良い

Webビーコンを使う場合、開封者情報を特定するには、訓練対象者ごとの
Webビーコンを埋め込んだ添付ファイルを作成する必要があり、Webサーバ側にも
訓練対象者分の画像データをアップロードしなければなりませんが、本キットでは
それらの手間が不要になります。

２．Webサーバを用意しなくて良い

Webビーコンを使う場合は、Webサーバが必要になりますが、本キットでは
Webアクセスを行わないので、Webサーバは不要です。

３．開封者情報を集計するのに手間がかからない

Webビーコンを使う方法では、Webサーバのログをサーバから取り出して
解析ツールに投入し、集計を行うといった手間がかかりますが、本キットでは
集計用のExcelツールを起動し、開封者情報を受信したメールフォルダを指定する
だけで、あとはツールが集計処理を行ってくれるので手間がかかりません。

４．リアルタイムに開封者情報を確認できる

Webビーコンを使う方法では、ログをサーバから取り出さないと集計ができないため、
リアルタイムに開封者情報を確認するにはログをウォッチしないといけませんが、
本キットではOutLookのメールフォルダを確認すればよいので、Webサーバのログを
ウォッチする方法に比べて確認しやすいというメリットがあります。

マクロを使う方法と何が違うのか？

１．マクロが動かない環境でも訓練ができる

WordマクロやExcelマクロを使う方法では、マクロが禁止となっている
パソコンでは動作しません。また、KingOfficeなど、Microsoft製品が
入っていないパソコンではマクロが機能しません。本キットはexeファイルを
用いているため、exeファイルが動作するパソコンであれば、マクロが動くか
どうかに関係なく、訓練ができます。

２．マクロを使わないので警告が出ない

マクロを使うと、訓練対象者のパソコンの設定によっては、警告が表示され、
訓練対象者がファイルを開く前に気づかれてしまい、開封者情報を集計することが
できないというデメリットがあります。

訓練ということを考えれば、ファイルを開こうとした人は開封者として集計したい
ところなので、警告が出てしまうのは、訓練を実施する上ではマイナスになります。

本キットのご利用について

本キットのご利用は、キットをご購入いただいた組織様内でのご利用に限らせていただいておりますが、スタンダードキット及び、プレミアムキットに限り、キットをご購入いただきました組織様を含む2組織様内を対象に、本キットにより生成した模擬マルウェアプログラムとコンテンツの配布・利用を許諾しております。

これにより、クライアント等に訓練サービスを提供されている組織様におかれては、本キット1本につき1社に対し、本キットを利用して商用サービスを提供いただくことが可能です。

なお、グループ会社と共同で訓練サービスを実施される場合等につきましては、ご利用範囲の適用につきましてご相談をお受けしておりますので、お気軽にご相談下さい。

本キットについてご質問やご要望等がございます場合は、
以下宛てまで、お気軽にご連絡ください。

模擬マルウェアプログラムが使えるかどうか試してみたい。
というご要望にもお応えしています。

標的型攻撃メール対応訓練実施キット問い合わせ窓口

sec-kit@happyexcelproject.com