標的型攻撃対策訓練 事前資料

標的型攻撃とは？

特定の組織や人から機密情報を窃取することを目的として行われるサイバー攻撃を標的型攻撃といいます。多くの場合、フィッシングメール（偽装メール）から不正プログラムの実行を促し、実行することによって不正プログラムをインストールします。この不正プログラムはウイルス対策ソフトでは検出できないものが多く、技術的対策だけでは防ぐことが出来ません。

不審なメール受信時の適切な対応方法

1．標的型攻撃メールに引っ掛からないようにする。

- 怪しいと感じたメール（タイトル、送信者、アドレス等）は開封しないでください。
- 開封した上で怪しいと感じたら、添付ファイルや URL リンクにはアクセスせず、破棄してください。
  （業務や組織を騙っている、心当たりのない組織からのメール、など。詳細は下記を参照してください。）

2．組織の感染可能性の芽を早期に摘む。

- 開封した上で怪しいと感じたら、添付ファイルや URL リンクにはアクセスせず、**システム管理者またはシステム管理部門（以下、『管理者』）**へ報告してください。
- 管理者は分析し、**組織内に注意喚起を行い、報告を呼び掛け**てください。

3．問題を早期に発見し、初動対応を取る。

- 誤って添付ファイルや URL リンクにアクセスしてしまった場合、**速やかに管理者へ報告**してください。
- 管理者は初動対応（ネットワークからの切り離し等）を取り、被害の拡散防止に努めてください。
- 管理者は**組織内へ注意喚起、報告の呼び掛け**を行い、状況の調査を行ってください。

4．組織として、被害を低減、最終甚大被害を回避する。

- 管理者は調査・分析を行い、今後の攻撃を回避する為の対策を取ってください。

個々人のセキュリティ意識向上を行い、標的型攻撃に引っ掛からないようにすることも重要ですが、組織にとってはだれか一人でも引っ掛かってしまえば侵入を許してしまうこととなります。このため、感度の高い人の「気付き」を活用し、組織内で共有することにより被害を回避する方法を推奨します。また、引っ掛かってしまったとしても、組織としてできるだけ早く対策を取れるようにすれば被害の低減に役立ちます。

標的型攻撃メールを見分けるためのポイント

差出人 ：松本商工会議所 情報事業部 <jyouhou@example.com>
件名　 ：【重要】マイナンバー変更のお願い
添付　 ：個人の番号漏洩確認リスト.docx　…

あなたはマイナンバーが漏えいしているという連絡がありました。
マイナンバーは安全管理措置を講じる義務があり、これを放置しますとマイナンバー法の違反となります。
この場合、関係省庁からの調査が入る可能性があります。
速やかな以下のウェブサイトにアクセスし、マイナンバーを変更手続きを行ってください。
12 月 31 日までに変更が確認できない場合、法的措置を取ります。

http://www.cas.go.jp/jp/seisaku/bangoseido/ <http://www.cas.com/jp/seisaku/bangoseido/>

松本商工会議所 情報事業部 <jyouhou@example.or.jp>

※：下波線部が疑わしいポイントです。注意して見逃さないようにしましょう。

以下の特徴を持つメールは標的型攻撃メールの可能性が高い為、注意して対応してください。

件名・テーマ

- 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容（取材申込、クレームなど）
- 心当たりのないメールだが、興味をそそられる内容（議事録、演説原稿などの内部文書送付など）
- これまで届いた事の無い公的機関からのお知らせ（情報セキュリティに関する注意喚起、感染症流行情報など）
- 組織全体への案内（人事情報、新年度の事業方針、内部イベント情報など）
- 心当たりのない決裁や配送通知（航空券の予約確認、荷物の配送通知など。英文の場合が多い。）
- ID やパスワード等の入力を要求するメール（メールボックス容量オーバーの警告、銀行からの登録情報確認など）
- 件名や本文に『緊急』『重要』『必ず確認』などの文言が入っている。

差出人及びメールアドレス

- フリーメールアドレス（上記例では『@example.com』）から送信されている。
- 差出人のメールアドレスと本文の署名に記載されたメールアドレスが異なる。
- 企業・公的機関などの場合、本来使用されないメールアドレスを使用している。（ドメインが違う、など）

本文

- 言い回しが不自然（文法がおかしい、など）、日本語では使用されない漢字（繁体字、等）が使われている。
- 実在する名称を一部に含む URL が記載されている。
- 表示されている URL と実際のリンク先の URL が異なる。HTML メールの場合、偽装が可能
- 署名の内容が誤っている。（名前が異なっている、存在しない部署となっている、など）

添付ファイル

- ファイルが添付されている。特に実行形式ファイル（exe／scr／cpl など）やショートカットファイル（lnk など）
- アイコンが偽装されている。（実行形式ファイルなのに文書ファイルのアイコンとなっている、など）
- ファイルの拡張子が偽装されている。（二重拡張子、空白文字の挿入、RLO の使用など）

実施目的を明確化し、効果的な訓練を

標的型攻撃対策訓練は、不審なメールを実際に受信した場合、適切な対処が行えるかどうかを確認する目的で実施されるものです。不審メールの実行率を下げる（不審メールに気付くポイントを学習、体験する）ことは代表的な目的の一つですが、他にも不審メールの受信者が適切な対処ができるか、有事の際にきちんと機能する体制であるかを確認し、組織として改善、強化を図っていく等を目的とした訓練も重要です。

実施目的と訓練内容の例

個々のセキュリティ意識の向上を目的とする場合

- 実行率等を評価対象としてください。管理者への報告率や報告時間（※1）も計測すると良いでしょう。

巧妙な標的型攻撃を受けた際の組織的対応を訓練する場合

- 事前に訓練の告知を行うことを推奨します。訓練対象者及び管理者は対応手順を確認してください。
- 訓練時には管理者への報告から組織内への注意喚起、必要に応じて初動対応までを行ってください。
- 実行率だけではなく管理者への報告率、報告にかかった時間なども評価対象としてください。

標的型攻撃に引っ掛かってしまった際の被害低減を目的とする場合

- メールに内部情報（組織内に実在する部門や役職者氏名等）が記載された訓練メールを使用します。（※2）
- 事前に訓練の告知を行い、訓練対象者及び管理者は対応手順を確認してください。
- 訓練時には管理者への報告から組織内への注意喚起、初動対応までを行ってください。
- 実行率よりも、対処時間と対処内容を評価対象としてください。また、作業フローに問題が無いかをご確認ください。

※1：当サービスでは管理者への報告率、報告時間などは集計されません。必要な場合は別途集計を行ってください。
※2：当サービスをご利用頂く場合、文面は事前にお伝えください。『当サービスにおける訓練メールのカスタマイズ』もご参照ください。

当サービスにおける訓練メールのカスタマイズ

当サービスでは訓練メールのカスタマイズが可能です。ご希望が御座いましたら訓練実施前にお伝えください。（但し、内容によってはご希望に添えない場合も御座います。ご了承ください。）

- 送信者：　任意の表示名に変更が可能です。（※）
  メールアドレスについて、アカウント部（@より前）は変更が可能です。（存在しないものでも構いません。）
  独自ドメインをお持ちの場合は、ドメイン部（@より後）も独自ドメインのものに変更が可能です。
  詳細はお問い合わせください。
- 件名：　任意の件名に変更が可能です。
- 本文：　任意の文面に変更が可能です。URL リンクについては表示されるアドレスを変更することが出来ます。
- 添付ファイル：ファイル名のみ変更可能です。
- 送信日時：送信日程を指定して頂くことも可能です。訓練期間内の日時をご指定ください。
  （日時によってはお引き受けできない場合も御座います。）

※：但し、実在する第三者を装った訓練メールを送ることはできません。酷似する組織名などを使用することもできません。

よくある質問と回答

標的型攻撃訓練一般

- Q1：訓練対象者には事前に知らせた方が良いか？

  A1：訓練の告知などは事前に行った方が良いとのことです。訓練対象者が標的型攻撃に対する知識がない状態では警戒できず、知識があったとしても反発が高まり素直に受け止められず、訓練の効果が下がるという結果が出ています。

- Q2：不審なメールが来た場合は、送信者に直接電話で確認して良いか？

  A2：個人の対応としては間違っていませんが、基本的には**まず管理者に連絡**してください。感度の高い人の「気付き」を活用し、組織内で共有することによって被害を回避することが出来ます。

- Q3：実行率が低ければ、組織のセキュリティは問題ないのか？

  A3：いいえ、**決してそんなことはありません**。標的型攻撃に 1 件でも引っかかってしまえば機密情報は持ち去られてしまいます。標的型攻撃を受けた時、被害を最小限にする体制作りも必要となります。

- Q4：リアリティを追求したいので、実在する（第三者）組織を騙った訓練メールを送りたい。

  A4：フィッシングメールには実在する組織を騙ったものも数多く存在します。
  ですが、第三者組織に影響を与えてしまう為、標的型攻撃訓練では実在する（又は酷似している）組織名を使用して訓練を行うことはできません。具体的には、次の様な影響が考えられます。
  ・訓練メールの内容を問い合わせることで、当該組織が事実確認に追われることとなる。
  ・メール受信者が SNS などに訓練メールを投稿することによって当該組織への風評被害が発生する。

当サービスについて

- Q5：訓練実施までに必要な準備時間は？

  A5：お申し込みから 1 週間程度の準備時間が必要です。
  この 1 週間でテストメールの開封確認や文面の確認、対象メールアドレス一覧の送付を行って頂きます。
  文面の変更を行う場合もこの期間内で行います。

- Q6：一部の訓練が行えない場合、その分の訓練はどうなるか？

  A6：当サービスでは、実行形式ファイル添付型、Word ファイル添付型、URL リンク型の三通の訓練メールを送信します。
  これらの内、一部で訓練が行えない場合は別タイプの訓練に差し替えることが出来ます。
  例えば、実行形式ファイル添付型で訓練が行えない場合、これを Word ファイル添付型に差し替えて Word ファイル添付型 2 回と URL リンク型 1 回の訓練を行うことが出来ます。