サイバーセキュリティ通信　【第2号】

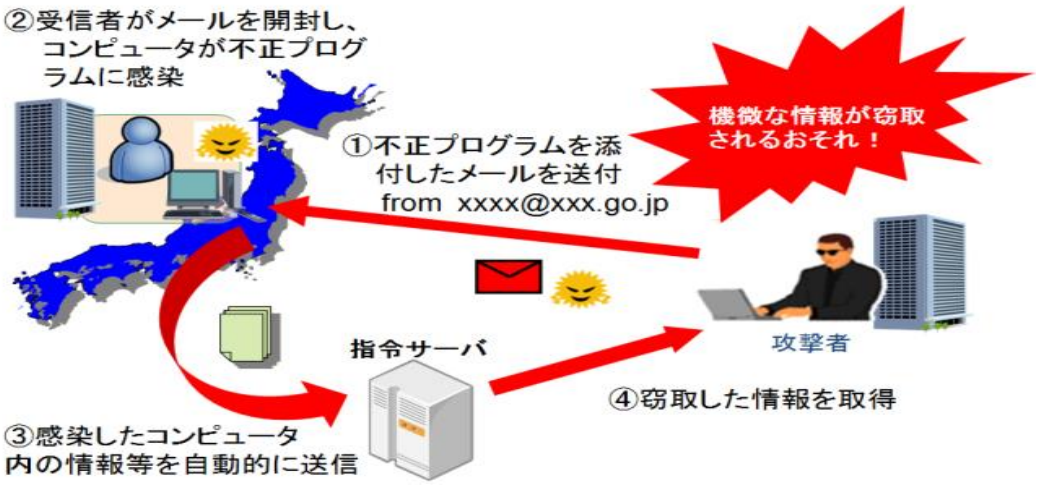
平成28年8月12日
大分県警察本部　生活安全部
生活環境課　サイバー犯罪対策室

不正プログラムが添付された標的型メールに注意を！！

昨年、日本年金機構の職員の端末が不正プログラムに感染したことにより、同機構が保有する個人情報が流出し、今年には大手旅行会社が790万人分の顧客情報が流出したと大きく報道されました。
いずれも、不正プログラムは「標的型メール」により感染をしてしています。
自分は狙われない、うちの会社は攻撃の対象にならないと思っていませんか？
ぜひ、標的型メールの危険性を認識して下さい。

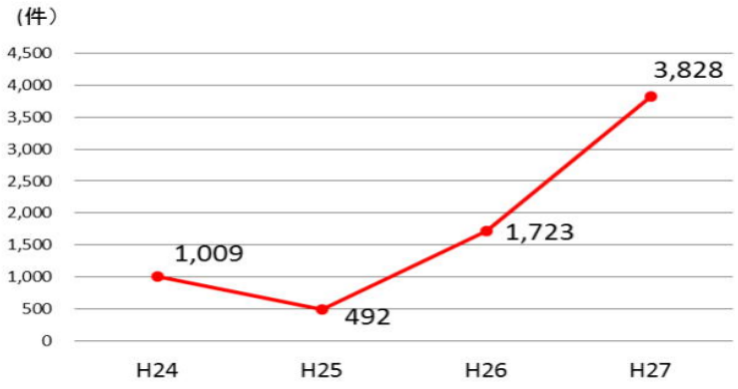
1　標的型メールとは

業務に関連した正当なものであるかのように装いつつ、不正プログラムを添付した電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させることによって情報の盗み取るもの。



2　平成27年中の標的型メールの発生状況と特徴

平成27年中に警察が事業者等から報告を受けた標的型メールは、3，828件と過去最多。
Word文書形式のファイルを添付したものが急増し、過半数を占める。



【標的型メール攻撃の件数】

標的型メールは、ばらまき型が多数発生し、全体の92%を占めています。
その多くは、品物の発送代金の請求等の業務上の連絡を装ったものです。

３　標的型メールを見破るための「６」のポイント

①　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

・新聞社や出版社からの取材申込や講演依頼
・就職活動に関する問合せや履歴書送付
・製品やサービスに関する問合せ、クレーム、アンケート調査
・議事録、講演原稿などの内部文書　　・著名人に関する情報

②　これまで届いたことのない官公庁や有名企業からの連絡

・熊本地震・大雨など災害情報

③　IDやパスワード、口座番号などの入力を要求するメール

・メールボックス、サーバーなどの容量オーバーの警告文
・金融機関からの登録情報の確認や口座凍結防止の案内

④　送信メールアドレスがおかしい

・官公庁や大手企業からのメールなのにフリーメルを使用している
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なっている。

⑤　メール本文の日本語表記がおかしい

・日本で使われていない漢字が表記されている
・使われない言い回し（翻訳ソフト使用）

⑥　実行形式ファイル（exe、scr、cplなど）や圧縮ファイル（ZIP）が添付

・拡張子とアイコンの組み合わせが異なっている
・二重拡張子（***.exe.xls）となって、拡張子が偽装されている

無料アプリの恐怖

４　防止対策

①　パソコンのOS、ソフトウェアを最新の状態にする

標的型メールに添付されている不正プログラムは、パソコンのOSやインストールされている各ソフトのぜい弱な部分を狙って侵入します。
OSやソフトウェアは、常に最新の状態に更新しましょう。

②　ウイルス対策ソフトを導入

標的型メールの添付ファイルに仕掛けられた不正プログラムが既に把握済みのウイルスであれば、ウイルス対策ソフトで検知可能です。
インターネットにアクセスするパソコンには、必ずウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新しましょう。

③　添付ファイルを不用意に開けない

標的型メールの添付ファイルの約50％は実行形式ファイル（Zip形式で圧縮されている場合が多い）でした。アイコンやファイル名を偽造している場合がありますので、注意をして下さい。添付ファイルがあれば、不用意に開かずにまずは拡張子を確認して下さい。
分からないファイルの場合は、送信者に電話で直接確認をして下さい。

④　組織対応と情報共有

企業や団体であれば、セキュリティポリシーを定め、従業員には日頃からセキュリティの意識を高めるための教育、指導が必要です。
また、不審なメールを受け取った場合には、それらのメールの情報をいち速く共有することで、被害の拡大を防止することが出来ます。

サイバー犯罪についての相談をお寄せ下さい。
大分市荷揚町4番35号
大分県警察本部生活安全部生活環境課サイバー犯罪対策室
Tell:097－534－2048