平成 30 年 6 月 6 日

学生皆さま

情報基盤センター

標的型攻撃メールの対策について

1. 標的型攻撃メールとは（IPA：情報処理推進機構より一部引用）

○ 機微な業務・情報を扱う特定の組織に対し、攻撃手段として電子メールに添付したウイルス混入プログラムや、メール本文から誘導する情報窃取ページを通じて、構成員の端末や組織内の情報システムに侵入を図るなど、組織的・持続的な意図をもって行われる、外部からの情報窃取・破壊等の攻撃を目的とした不正な電子メールを指します。

2. 標的型攻撃メールの被害例

○ ウイルス感染（ランサムウェア）すると、感染 PC 内及び感染 PC が接続するサーバー上のデータまでもが暗号化され読み出せなくなる場合があります。さらには、ウイルスがソフトウェアやネットワークの脆弱性を利用し、二次感染、三次感染し、感染が拡大する場合があります。

○ アカウント情報を窃取されると、アカウントの乗っ取りや侵入用の裏口設置（バックドア）により、情報システムに保存されている個人情報や機密情報が窃取される場合があります。

○ その後、暗号化解除や窃取データ返還のための身代金要求のほか、データの改ざん・破壊・情報漏洩を発生させるなど、壊滅的な被害が生じます。

○ 近年の国内発生した個人情報漏洩（特殊法人、大手旅行会社、大手企業、大学、医療機関ほか）の多くは「標的型攻撃メール」が起因しています。

3. 標的型攻撃メールと付帯するウイルスの特徴

○ 次の特徴を有しており、特に（1）（2）により受信者を信用させようとします。

(1) 送信者名として、実在する信頼できそうな組織名や個人名を詐称
(2) 受信者の業務に関係の深い話題や、詐称した送信者が扱っていそうな話題
(3) 巧妙に偽装し、迷惑メールフィルターをすり抜けてくる場合がある
(4) ウイルス対策ソフトを使っていてもウイルスが検知されない場合がある
(5) ウイルス感染しても、挙動が何も変わらず気付き難い場合がある
(6) ウイルスが外部の指令サーバーと裏で通信している場合がある（情報流出）
(7) 巧みな文章で、情報窃取用の不正サイトに誘導するものもある

4. 標的型攻撃メールの見分け方

○ 下記のいずれか一つでも該当するメールは、標的型攻撃メールの可能性が極めて高いため、安易に添付ファイルを開くことや、本文内のリンク情報にアクセスしないようお願いいたします。

標的型攻撃メールを見分けるポイント
① 送信者が日頃受信している実在アドレスと異なる（gmail, yahoo 等のアドレスは疑わしい）
② メール本文に「日本語の言い回しが不自然」、「日本語では使用しない漢字（一部に文字化けや中国語漢字の使用等）」、「署名内容の誤り」などがある
③ ファイル拡張子が「.exe」「.scr」「.cpl」「.js」など、実行形式ファイルが添付されている
④ 受信者の不安や関心を煽る内容（諸手続きや金銭的利害に関すること、身の覚えのない通販決済、アカウント情報ロックなどの警告）で、リンク先ページに誘導しようとしている
⑤ 誘導先ページが送信者メールアドレスドメイン（@以降）と異なるドメインである

○ 例えば、大学関係者や学会及び個人が利用する通販会社などを詐称し、修学や学生生活のほか、決済など諸手続きに関することを理由に、添付ファイル内容の確認や誘導先ページへのアクセスを依頼する内容を受信する場合もあります。この時、安易に信用せず上記の「標的型攻撃メールを見分けるポイント」と次頁の事例を参考に真偽を見分ける必要があります。

（最近の楽天を騙った事例：楽天カードから送信されるメールに似せた巧妙な偽装）

○本事例では、身に覚えのない決済情報から不安を煽り、確認のためにページ内のリンク先に誘導させるものです。
○誘導先ページは「もっと詳しくの情報はこちら.zip」がダウンロードできるものでした。
○本ファイルをダウンロードし、中のファイルを開くとウイルス感染し、知らないうちに裏で各種アカウント情報（情報システムへのログイン、ネットバンキングへのログインなどから）が窃取される可能性があります。開いた場合、直ちに PC をネットワークから切断後、感染確認・駆除が必要となり、あわせて関連アカウント情報の停止や変更など速やかな対応が必要となります。
○または、楽天サイトを偽装したページ（アドレスバーには楽天と異なるドメインページ）に誘導やログイン画面が表示され、楽天 ID・パスワードを入力してしまうと、楽天での不正購入やクレジットカードの不正利用及び個人情報の窃取など、サイバー犯罪に利用される場合があります。
○同様に、Apple や Amazon などを騙る詐欺メールも横行していますのでご注意ください。
○真偽確認が難しい場合は、情報基盤センター（B 棟 2 階）にてご相談ください。
○急を要する内容の場合は、実在の相手に直接の電話（又は正規連絡先メールアドレス）にて、本当に送信されたメールか確認を行ってください。この時、メール本文に記載の連絡先には連絡してはいけません。メール本文内の連絡先に連絡すると、言葉巧みに個人情報（氏名・年齢・住所・電話番号など）を窃取され、犯罪など別トラブルを被る場合もあるため、注意が必要です。

以上