【標的型攻撃メールの対策】(出典：NEC フィールデング(株))を一部、編集　　文責：河東岩夫　　作成日：平成 27 年 10 月 30 日(金)

(1)メールの添付ファイルを開封する場合に、以下の事項を確認する必要がある。

・何の前触れもなく、緊急連絡網の確認を依頼してきたメール

・採用窓口宛てに、添付ファイルの開封を要求してきたメール

・テキストで書ける内容をわざわざ添付ファイルに記しているメール

注)標的型攻撃のしくみとは

・攻撃者は、偽装した「悪意のあるファイル」を電子メール等に添付して標的に送付して来る(メールに記載した URL をクリックさせて「悪意のあるファイル」をダウンロードさせることもある)。

・標的となった担当者が「悪意のあるファイル」を実行すると、攻撃者は社内のシステムを不正に操作する。

(2)「悪意のあるファイル」を実行させる巧妙な騙しのテクニックに注意する必要がある。

1)攻撃する相手を調べている

・攻撃前に、標的とする会社の部門や役員名を電話やホームページで確認している。

・実在する部門を装い、「緊急で添付ファイルの確認をしたい」とのメールを送ってくる。

・送信元のアドレスを社内のアドレスに偽装していたり、「緊急なので家から送ります」と違うアドレスであることの理由を付けていたりする。

・悪意のあるファイルは、「緊急連絡：住所録.xls」や「異動先.pdf」等、普段使っているファイルのように偽装して標的に送付してくる。

2)やり取りをして相手を信用させる

・会社の採用窓口宛てのメールアドレスに、必要書類や連絡先等を何度か問合わせた後に「質問事項を添付ファイルにまとめました」とメールに記載して、添付ファイルの開封を要求してくる。

・製品の問合わせ窓口宛てのメールアドレスに、製品の取扱いに関する質問を何度か問合わせた後に「文書では分かりづらいので、画像ファイルを送ります」として、添付ファイルを開封させる。

(3)標的型攻撃(悪意のあるファイルによる攻撃)を防ぐには以下の６つの対策事例を組み合わせて攻撃に備える必要がある。

対策	安全管理措置(技術的)の事例
1)大事な情報は外にさらさない	・ファイアウオールでアクセス制御 ・内から外へ通信制限
2)怪しい情報を検知する	・不正アクセス、スパムメール対策を導入 ・OS、ウイルス対策、業務 AP は常に最新 ・従業者の訓練・教育
3)情報を攻撃者へ送信しない	・不要なメール、ファイルはクリックしない ・外部へ出る通信はプロキシサーバ経由
4)攻撃を広げない	・ネットワークを分離し、パスワードを変える ・あやしいメールが来たことを周囲に連絡
5)いつ誰が、何をしていたかを知る	・外部への通信を記録
6)盗まれても内容を見せない	・データを暗号化

(4)以下の標的型攻撃メールを開封したと考えられる場合、業務を中断し、関係者と情報を共有して対策を講じる必要がある。

・組織内の不特定多数に対して同時に同様のメールが送信されている。

・通常通信されていない時間帯に通信が発生している。

・特定の端末やサーバが重要ファイルにアクセスして失敗しているログがある。

・勝手にインターネットに接続しようとする。

以上