コンピューターウイルス「Emotet」に関する注意喚起

コンピュータウイルスEmotet(エモテット)が世界的に猛威をふるっています。

今年の6月ごろ経済学部同窓会や経済学部事務室にもEmotetに感染させようとするメールが添付ファイルとともに多数届きました。また、職員の名前を勝手に語り、他のパソコンに感染させるためのウイルスメールが大量に送信されることもあります。そのため注意喚起を掲載することにいたしました。

コンピュータウイルス Emotetについて

Emotetは、情報の窃取に加え、更に他のウイルスに多重感染させるために悪用されるウイルスであり、メールに添付されるファイルを開くことで感染が拡大します (参考情報サイト: IPA『「Emotet(エモテット)」と呼ばれるウイルスへの感染を狙うメールについて』 を参照)。Emotetに感染すると、他のウイルスへの多重感染も引き起こすことが多く、情報を窃取しさらに暗号化し身代金を要求するランサムウェアを招き入れ、窃取した機密情報を公表すると脅迫してくるケースもあります。

未然に防ぐために

- 差出人メールアドレスが、普段やり取りしているメールアドレスであることを確認する(なりすましの可能性)
- 添付ファイルは、原則として開かない(zipファイルによる攻撃が非常に多い)
- 差出人が見知ったメールアドレスであっても、メールの件名や本文に少しでも不審な点を感じたら添付ファイルは絶対に開かない(差出人が感染している可能性)
- 攻撃手法は日々進化するため、Windows Defenderを含む従来のウイルス対策ソフトでは、Emotetの感染を防止できない可能性が高いので、安心しすぎない
- その他、『標的型攻撃メールの概要と対応』(参考情報サイト: セキュリティ対策掛『標的型攻撃メールの概要と対応』)の内容を改めて確認しておく

怪しいメールの添付ファイルをクリックしてしまったら

Emotetの可能性のあるファイルをクリックしてしまった時、すぐに対応することが重要ですので以下を実施してください。

速やかに実施すべき作業

- 速やかにネットワークから切り離す
  - 有線LANで接続している場合はLANケーブルを抜く
  - 無線LANで接続している場合は無線LANを無効にする

ネットワークに接続せずに実施

- ウイルス対策ソフトで完全スキャンを実施する
  - Emotetは発見できない可能性が高いが、それでも何かを発見するかもしれないので必ず実施する
- 他の安全なパソコンでマルウエアEmotetへの対応FAQからEmoCheckをダウンロードして当該PCで実行し、感染の有無を確認する
  - 感染していたら、パソコンを初期化(工場出荷状態の戻す)する

参考情報サイト

1. IPA 『Emotet(エモテット)」と呼ばれるウイルスへの感染を狙うメールについて』
2. JPCERT『マルウエア Emotet の感染に関する注意喚起』
3. JPCERT『マルウエアEmotetへの対応FAQ』
4. セキュリティ対策掛『標的型攻撃メールの概要と対応』
5. Targeted Email Attacks and How to Deal with Them