サイバーニュース

2022年6月
第６号

Emotetの手口と対応について

1　Emotet（エモテット）の添付ファイルについて

最近のEmotetメールに添付されているショートカットファイル（サイバーニュース第４号でも紹介）に関して、**ショートカットファイルの拡張子「.lnk」**については、パソコンで拡張子を表示する設定にしていたとしても、**拡張子が表示されません。**

最近の事例（**県内でも確認**）では、ショートカットファイルのファイル名を

〇〇〇.doc.lnk

とし、Emotetメールの受信者のパソコンで

〇〇〇.doc

と表示させることにより、**Word文書ファイルへの偽装を狙った手口**も確認されています。

2　EmoCheck（エモチェック）について

自組織の職員になりすましたメールが送信されているからといって、その職員の端末がEmotetに感染しているとは限りません。

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、Emotetの対応方法について

マルウェアEmotetへの対応FAQ
（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）

で紹介しているほか、感染が疑われるパソコンがEmotetに感染しているかどうかをチェックするための

Emotet感染有無確認ツール「EmoCheck」
（https://github.com/JPCERTCC/EmoCheck/releases）

を無償提供しています。

EmoCheckをダウンロードして実行する際は、

- 提供されている**最新のバージョン**を実行
- OSが**64ビットの場合**は「Emocheck_〇_x64.exe」を実行
  OSが**32ビットの場合または分からない場合**は「Emocheck_〇_x86.exe」を実行
- 感染が疑われる際に**ログインしていたアカウントでログイン**して実行

するようにして下さい。

サイバー犯罪に関する通報や相談は警察までお願いします！

石川県警察本部生活安全部サイバー犯罪対策課
０７６－２２５－０１１０　cyber@police.pref.ishikawa.lg.jp