TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2020年 第26号

Emotetウイルスが感染拡大中！感染の有無を確認する方法について

Emotetウイルスの感染が疑われる事案が、県内外で発生しています。このウイルスは、情報の窃取に加え、更に他のウイルス感染のために悪用され、感染の拡大が試みられています。

Emotetウイルスの感染経路は、メールです。攻撃者（差出人）は、正規のメールへの返信を装うことで取引先等になりすまし、実際のメール内容を用いて、ほぼ同じ内容の文面や件名でメールを送信します。メールの添付ファイルやURLリンクを開き、ウイルスに感染させられてしまう可能性は誰にでもあり得ます。

OSやウイルス対策ソフトは、常に最新の状態に更新しましょう。
サイバーセキュリティの置き薬（2019年第13号、2020年第3号）では、Emotetウイルスについて注意喚起をしています。次の点に注意してください。

1．不審なメールは開かない

2．添付ファイル、URLリンクに注意する

3．マクロ動作を有効にしない

Emotetウイルスは、Microsoft Officeファイル（Word文書ファイル等）のマクロ動作を通じて感染します。メールの添付ファイルはMicrosoft Officeファイルだけでなく、パスワード付きzipファイルのケースが確認されています。また、メールに記載しているURLリンクをクリックすることで、Emotetへの感染を狙うファイルをダウンロードさせる手口も確認されています。

感染を確認する方法

JPCERTコーディネーションセンターのサイトにおいて、Emotetウイルス感染の有無を確認するツール「EmoCheck」が公開されています。感染が疑われる場合はツールの活用をお願いします。

○　引用元：JPCERT コーディネーションセンター
「マルウェアEmotetへの対応FAQ」
https://blog.jpcert.or.jp/ja/2019/12/emotetfaq.html

【参考】IPA　「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html