サイバーセキュリティの置き薬

2020年
第3号

新型肺炎に便乗した"Emotet"ウイルスに注意！

新型コロナウイルスの感染拡大に伴って、保健所等からの予防対策に関する注意喚起メールを装ったEmotetウイルスの拡散が確認されていますので、注意してください。

保健所等からの正規メールを受診した関係機関の端末が既にEmotetウイルスに感染していたことが原因で、Emotetウイルスが拡散されたと考えられます。Emotetウイルスは、感染端末が過去に送受信した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送信するといった特性があります。

サイバーセキュリティの置き薬（2019年第13号、2020年第2号）では、Emotetウイルスや新型コロナウイルスに乗じた犯罪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、添付ファイルのWord文書ファイル等のマクロ動作を通じて感染するものです。マクロ動作を有効にする旨を要求する添付ファイルには注意が必要です。

端末にインストールされたWordやExcel等の**「マクロを無効にする」**設定にしてください。

≪情報提供（通報）をお願いします≫

今後、社会情勢に乗じたサイバー犯罪の発生が懸念されます。新型コロナウイルスや東京オリンピック・パラリンピック競技大会を装ったフィッシングメールやウイルスメール等のサイバー犯罪等を確認した際は、警察まで情報提供（通報）をお願いします。

【富山県警察サイバー犯罪対策課　076－441－2211】

2月1日～3月18日は「サイバーセキュリティ月間」です。
“サイバーセキュリティは全員参加”