事　務　連　絡
令和４年３月８日

各 都道府県衛生主管部（局）長
　 地方厚生（支）局医事課長　殿

厚生労働省医政局研究開発振興課
医療情報技術推進室

マルウェア「Emotet」の感染拡大について(注意喚起)

日頃より医療分野のサイバーセキュリティ対策に関し、格別の御配慮を賜り、厚く御礼申し上げます。

さて、最近、医療機関においても「Emotet」と呼ばれる、情報の窃取に加え、さらに他のマルウェアへの感染に悪用されるマルウェアに感染したという事例が多数確認されております。Emotet への感染により、医療情報システムが停止するといった、直接的に診療へ影響を及ぼした事例は確認されていないものの、Emotet への感染を契機としたランサムウェアへの感染や、個人情報の流出等が想定されることから、十分に注意いただくことが必要です。

攻撃の手口については、従前と同様で、添付した Excel ファイルのマクロの悪用、パスワード付き ZIP ファイルの悪用が目立っています。

つきましては、下記対策の徹底を管下の医療機関へ御周知いただくとともに、医療機関が職員一人一人に対し、下記対策を周知できるように御協力いただきますよう、何卒よろしくお願い申し上げます。

記

1　身に覚えのないメールの添付ファイルは開かない。また、メール本文中の URL リンクはクリックしない。

2　自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。

不自然な点の例としては、次のものがあります。

(1)「件名」が過去にやり取りされたメールの標題、関係者の氏名である。

例：「RE：関係者氏名」、「Fwd：過去のメールの標題」

(2) 「送信者」が過去メールをやり取りした関係者等に偽装されている。
例：厚労太郎〈abcdef123@xx.xx〉氏名と〈 〉内のアドレスが不一致
(3) 圧縮されたファイルが添付され、本文にパスワードを記載している。
(4) 短いメッセージで添付ファイルの開封を促す記載がある。
例：添付ファイルをご確認ください。

3 OSやアプリケーション、セキュリティソフトを常に最新の状態にする。

4 信頼できないメールに添付されたWord文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。

5 メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。

6 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門やシステムベンダ等へ連絡する。

なお、Emotetへの感染やその疑いがある場合は、厚生労働省医政局研究開発振興課医療情報技術推進室に御一報いただくとともに、システムベンダや独立行政法人情報処理推進機構（IPA）の情報セキュリティ安心相談窓口にも御相談いただきますようお願い申し上げます。

【厚生労働省連絡先】
厚生労働省医政局研究開発振興課医療情報技術推進室
電話：03-3595-2430
メール：igishitsu at mhlw.go.jp
※「 at 」をアットマークに変換してください。

【参考】
「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
(独立行政法人情報処理推進機構)
https://www.ipa.go.jp/security/announce/20191202.html#L18

情報セキュリティ安心相談窓口（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/anshin/index.html

マルウェアEmotetの感染再拡大に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2022/at220006.html
※Emotet感染有無確認ツール「EmoCheck」について記載があります。