

令和元年 12 月 13 日

都道府県医師会
情報システム担当理事 殿

日 本 医 師 会
常任理事 石 川 広 正



マルウェア「Emotet」に関する注意喚起について

拝啓 時下ますますご清祥のこととお慶び申し上げます。日頃より会務運営に対しご高配を賜り深く感謝申し上げます。

さて、日本国内におけるマルウェア「Emotet」の感染被害に関しましては、医療機関の感染も確認され拡大傾向にあります。

日本医師会においては、12月3日付「日医君」だよりにて既に注意喚起を行っておりますが、各医療機関での感染拡大が懸念されることから、改めて注意喚起を行うことといたしました。

本マルウェアの感染について説明いたしますと、主な感染経路はメールとなっています。受信者が添付ファイルを開封したり、メール本文中に記載された URL をクリックしたりすることにより、端末が Emotet に感染します。添付の Word ファイルを開き、コンテンツの有効化を行ってしまうことで感染します(過去には、メール内に記載されたURLにアクセスすることで感染した例もあるようです)。また、特徴の一つとして、感染したPC内のメールソフトの情報を窃取し、その情報を元に、過去にメールのやり取りをしたことがある相手に、発信者の名前を騙ってウイルスメールを送付することが挙げられます。

そのため、送信者が知っている相手であっても、不審な添付ファイルを開いたり、メール内の不審なURLにアクセスしてしまうことがないよう、ご注意ください。また、お願いいたします。メール本文をみただけで感染することはありませんので、不審なメールは速やかに削除していただければ大丈夫です。

このマルウェアに限らず、メールサーバ上のスキャンソフトや、各PCに導入している対策ソフトでは、必ずしも防ぎきれない脅威もありますので、下記 JPCERT/CC の記事も参考にいただければ幸いです。

一方、ウイルス等に感染した場合、あるいはその疑いが有る場合は直ちに医療情報システムの保守会社等に連絡するとともに、「医療情報システムの安全管理に関するガイドライン」に基づき必要な対応を行い、厚生労働省医政局研究開発振興課医療情報技術推進室(03-3595-2430)へ連絡いただきますようお願いいたします。

また、情報処理推進機構情報セキュリティ安心相談窓口ではマルウェアや不正アクセスに

関する技術的なサポート受けられますので、適宜ご利用ください。

敬具

IPA情報セキュリティ安心相談窓口:03-5978-7509 anshin@ipa.go.jp
<https://www.ipa.go.jp/security/anshin/index.html>

マルウェア Emotet の感染に関する注意喚起(JPCERT/CC)
<https://www.jpcert.or.jp/at/2019/at190044.html>

<参考>

Emotet について

Emotet は、「情報窃取機能」、「感染拡大機能」、「自己更新機能」、「耐解析機能」を持つマルウェアです。

Emotet は 2014 年頃に初めて確認されたマルウェアですが、2018 年 10 月に Emotet の新たな機能として、「感染端末に保存されていたメールの件名と本文を窃取する機能」が追加されました。攻撃者は、この機能を悪用し Emotet の感染を拡大させています。

また、Emotet にはコマンドアンドコントロール(C2)サーバーと通信することで、感染端末に別のマルウェアを送り込む機能が存在します。攻撃者が、この機能を悪用し感染端末にバンキングマルウェア TrickBot やランサムウェア Ryuk を送り込むケースも存在します。こういったケースでは、被害が拡大し組織に深刻な影響を与えることも多いため、一層の注意が必要となります。

Emotet の感染を予防するための対策

Emotet の感染を予防し、また、感染被害を最小化するため、以下に示す対策等の実施を検討してください。

- ・組織内への注意喚起の実施
 - ・Word マクロの自動実行の無効化
 - ・メールセキュリティ製品の導入によるマルウェア付きメールの検知
 - ・メールの監査ログの有効化
 - ・定期的な OS 等へのパッチ適用（脆弱性を悪用した感染拡大への対策）
 - ・定期的なオフラインバックアップの取得
- (Emotet 感染後にランサムウェアに感染する恐れがあるため)

このほか、

「主な感染経路」「感染した場合の影響」「感染に気付いた場合の対応」等の詳細については、日医 HP の PDF ファイルを参照ください。

<http://www.med.or.jp/japanese/members/info/ceptoar/pdf/20191129.pdf>