福県医発第2399号（地）
令和元年12月19日

各 医 師 会 長　殿

福 岡 県 医 師 会
会長　松　田　峻一良
（公　印　省　略）

マルウエア「Emotet」に関する注意喚起について

今般、日本医師会より、日本国内におけるマルウエア「Emotet」の感染被害が医療機関においても確認され拡大傾向にあることから、改めて注意喚起がありました。

本マルウエアの主な感染経路はメールとなっており、受信者が添付ファイルを開封したり、メール本文中の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。

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ることから、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封したり、メール内の不審なURLにアクセスしないよう注意が必要とのことです。なお、メール本文を見ただけでは感染することはありません。

ウイルス等に感染した場合、あるいはその疑いがあ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）へご連絡いただきたいとのことです。

つきましては、貴会におかれましても本件についてご了知いただくとともに、貴会会員への周知方につきよろしくお願い申し上げます。

小郡三井医師会より　　医療情報システム担当理事　田中泰之
会長　島田昇二郎

（情シ 59）
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 己

マルウエア「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エア「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。

本マルウエ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、ご注意いただきますよう、お願いいたします。メール本文を見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。

このマルウエアに限らず、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 の記事も参考にして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エ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

マルウエア 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」を持つマルウエアです。

Emotet は 2014 年頃に初めて確認されたマルウエアですが、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エ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エア TrickBot やランサムウエア 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エ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エ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

令和元年 11 月 29 日

内閣サイバーセキュリティセンター
重要インフラグループ

マルウエア「Emotet」に関する注意喚起

日本国内においてマルウエア「Emotet」の感染被害拡大が確認されています。

本マルウエアの主な感染経路はメールです。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。

こうした状況を踏まえ、対応を実施し、感染が疑われる場合は必要な措置を講じるとともに、速やかに所管省庁に報告してください。

１．概要

日本国内においてマルウエア「Emotet」の感染被害拡大が確認されています。Emotet は、感染した端末のメールの情報を窃取し、それを悪用してメール経由で感染を拡大するマルウエアです。特に実在の組織や人物になりすましたメールに Word ファイルを添付する手口で、感染を拡大させています。

本注意喚起に記載した攻撃の手口や対策、感染時の対応をよく読み、各組織で必要な対応を実施してください。また、感染が疑われる場合は必要な措置を講じるとともに、速やかに所管省庁に報告してください。

２．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」を持つマルウエアです(表 1)。

Emotet は 2014 年頃に初めて確認されたマルウエアですが、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エ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エア TrickBot やランサムウエア 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。

表 1　Emotet が持つ主な機能

機能分類	詳細
情報窃取機能	・端末情報 －　コンピュータ名、動作中プロセスの一覧 ・メール関連情報(Outlook、Thunderbird 等から情報窃取) －　送受信したメールに含まれるメールアドレスと表示名 －　**メールの件名と本文 [2018 年 10 月に新たに追加された機能]** －　メールサーバー情報(通信先、ポート番号、認証情報等) ・認証情報

機能分類	詳細
	- ネットワーク認証情報の窃取 - 端末に保存されたパスワード等の認証情報の窃取
感染拡大機能	・メールによる感染拡大 - 窃取したメールアドレスを使って、他者へ悪性メールを拡散 - 悪性な Office ドキュメントを開くことによる感染 - メール本文中の URL をクリックすることによる感染 ・一般的によく使われるパスワードの一覧を用いたログイン試行による感染拡大
自己更新機能	・コマンドアンドコントロール(C2)サーバーとの通信により、機能拡張モジュールや他のマルウエアをダウンロード ・C2 サーバーとの通信により、自身を最新バージョンに更新
耐解析機能	・感染端末上で特定のアプリケーション(デバッガ、パケットキャプチャソフト、仮想マシン等)の動作を検知し、Emotet の挙動を停止

3. Emotet の主な感染経路

Emotet の主な感染経路はメールです。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。以前は、請求書を騙ったメールやシステム管理者を装ったメール等、一般的にユーザーが開きやすいメールを送ることで感染拡大を狙っていました[1]が、2018 年 10 月に Emotet にメールを窃取する機能が追加され、2019 年に Emotet の新たな感染拡大の手口が観測されるようになりました。2019 年に観測された Emotet の新たな感染拡大の手口を以下にまとめます(図 1)。

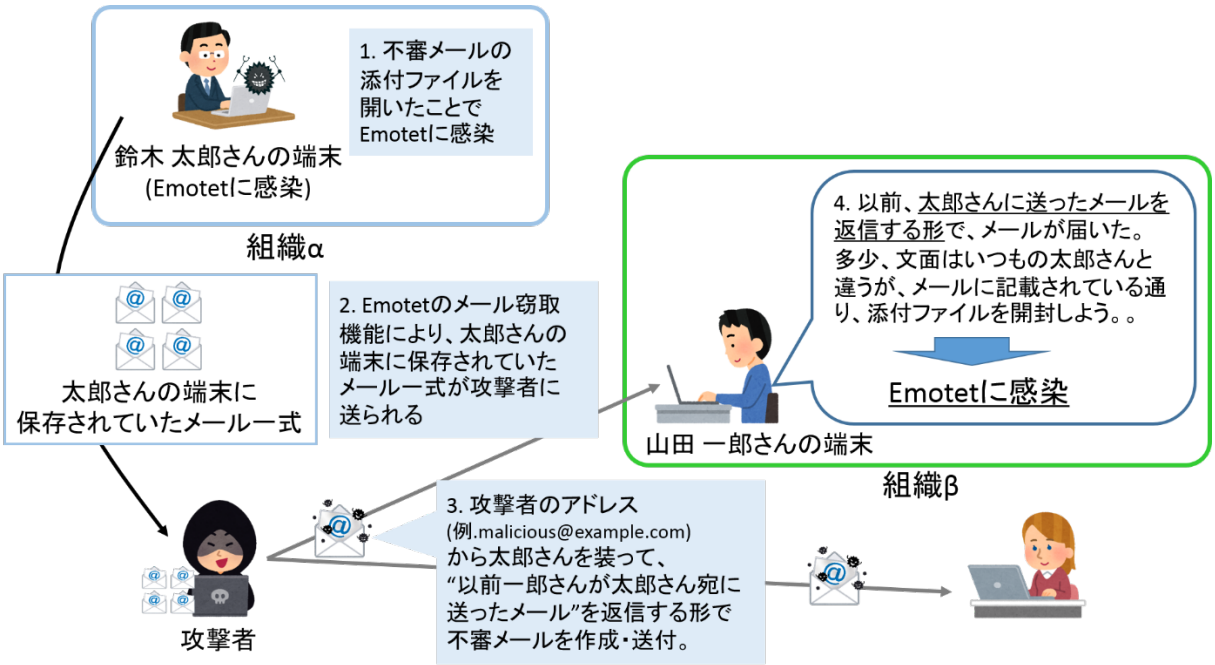

図 1　2019 年に観測された Emotet の新たな感染拡大の手口

本攻撃の手口には、以下の特徴がみられます。

- 攻撃者は、Emotet に感染した端末に保存されていたメールの件名と本文を窃取する。
- 攻撃者は、窃取したメールの本文を引用したメールを作成する。
- 攻撃者は、**攻撃者自身のアドレス** から、攻撃対象に「窃取したメールの本文を引用したメール」を送信し、あたかも以前のメールの返信であるかのように装う。

[1] *請求書を騙ったメールやシステム管理者を装ったメールを用いて Emotet の感染を拡大させる手口は、本注意喚起発出時点(2019/11/29 時点)でも確認されておりますので、ご注意ください。*

メール(図 2)の受信者は、以前のメールが引用されていることから、メールの記載内容を信用し、メールの添付ファイル等を開いてしまいます。その結果、端末が Emotet に感染します。攻撃者はこれを繰り返すことで Emotet の感染を拡大しています。

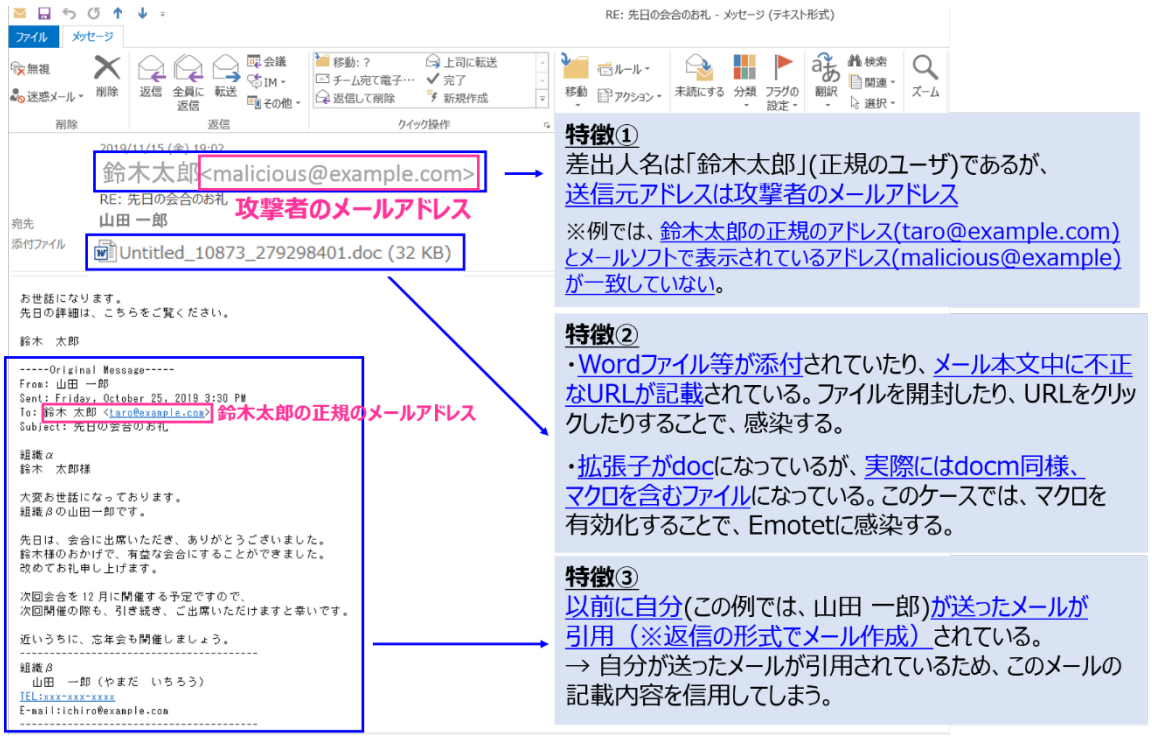

図 2 Emotet 感染者から窃取したメールを利用した不審メールの例

4. Emotet に感染した場合の影響

Emotet に感染した場合、以下のような影響が発生する可能性があります。

- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- 攻撃者が、窃取したパスワードを悪用し SMB[2]によりネットワーク内に Emotet の感染を拡大させる
- メールサーバーの認証情報が窃取される
- メールの件名や本文が窃取される
- メールクライアントソフトのアドレス帳の情報が窃取される
- 窃取されたメールのアカウントや本文が悪用され、攻撃者が Emotet の感染を拡大するメールを送信する

前述のとおり、Emotet に感染した場合、感染端末から情報が窃取された後、その情報を攻撃者が利用して、取引先や顧客に対して感染を拡大するメールが送信される恐れがあります。また、感染したままの端末が組織内に残留すると、感染を広げるメールの配信元として攻撃者に悪用され、組織外に大量の不審メールを送信してしまうことになります。

Emotet には他のマルウエアをダウンロードする機能が存在するため、Emotet に感染した端末がランサムウエア等をダウンロードし、その結果、ランサムウエアに感染して端末に保存されているデータが暗号化されてしまったといった事例も存在します。

[2] *ネットワーク(LAN)上の複数の Windows コンピュータの間でファイル共有等を行うためのプロトコル及び通信サービス*

５．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（図 3[3]）
- メールセキュリティ製品の導入によるマルウエ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エアに感染する恐れがあるため）

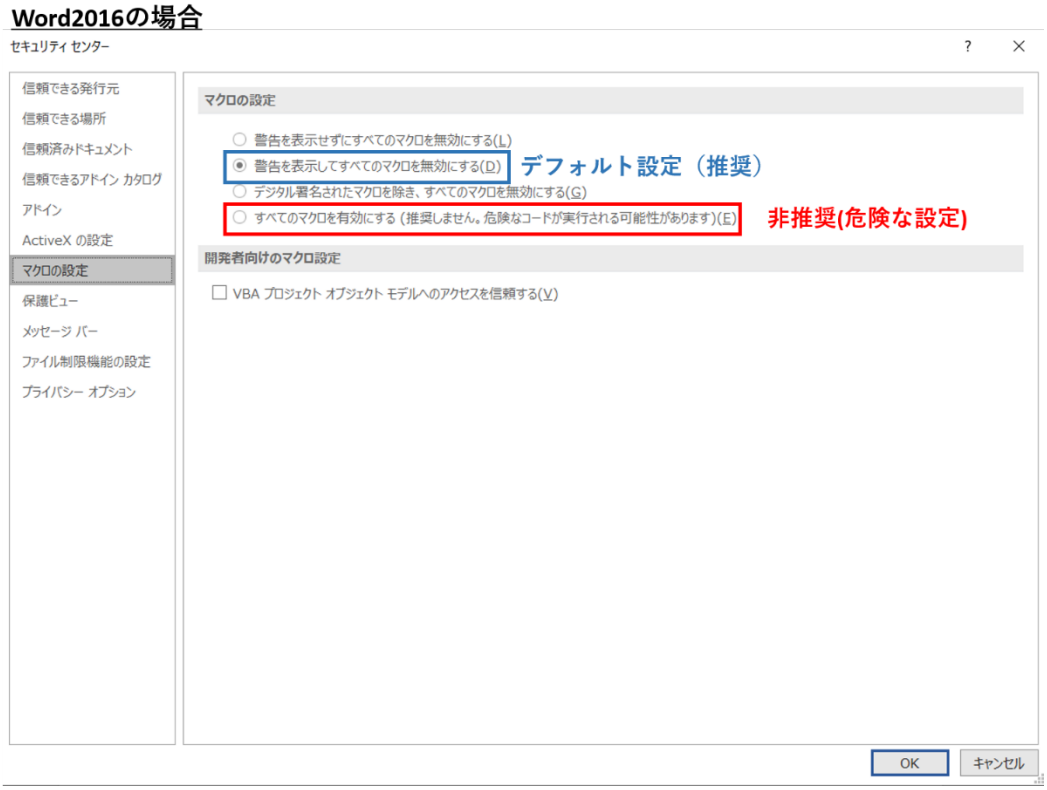

図 3　Word マクロ設定の無効化（推奨設定）

６．Emotet の感染に気付いた場合の対応

以下の事象を確認した場合は、自組織の端末が Emotet に感染している恐れがあります。

- 自組織で使用するウイルス対策ソフトが Emotet を検知した場合
- 自組織のメールアドレスになりすまし、Word 形式のファイルを送るメールが届いたと外部組織から連絡を受けた場合
- 自組織のメールサーバー等を確認し、Word 形式のファイルが添付されたメールやなりすましメールが大量に送信されていることを確認した場合

自組織の端末やシステムにおいて Emotet の感染が確認された場合、被害拡大防止の観点より、初期対応として以下の対処を行うことを推奨します。

---

[3] *Word のマクロ設定変更手順は、https://support.office.com/ja-jp/article/office-ドキュメントのマクロを有効または無効にする-12b036fd-d140-4e74-b45e-16fed1a7e5c6#__toc311698312 に記載されています。*

- 感染した端末をネットワークから隔離する
- 感染した端末が利用していたメールアカウントのパスワードを変更する
- 取引先、顧客等への注意喚起を実施する
  (取引先や顧客等に Emotet の感染が拡大する恐れがあるため)
- 所管省庁へ迅速に報告する

その後、必要に応じて、セキュリティ専門ベンダ等と相談の上、以下の対処等を行うことを推奨します。

- 組織内の全端末に対して、ウイルス対策ソフトによるフルスキャンを実施
- 感染した端末を利用していたアカウントのパスワードを変更
- ネットワークトラフィックログを監視
- 調査後に感染した端末を初期化

参考 URL

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

・Advisory 2019-131a: Emotet malware campaign (Australian Cyber Security Centre)
https://www.cyber.gov.au/threats/advisory-2019-131a-emotet-malware-campaign

・変化を続けるマルウェア「EMOTET」の被害が国内でも拡大 (トレンドマイクロ社)
https://blog.trendmicro.co.jp/archives/22959