（情シ 20）F
令 和 2 年 9 月 8 日

都道府県医師会　情報システム担当理事　殿
郡市区等医師会　情報システム担当理事　殿

日本医師会　常任理事
長 島　公 之
（公 印 省 略）

日本医師会事務局におけるコンピュータウイルス感染と それを発端にした関係者への不審メール発生に関するお詫びとご報告（訂正・更新版）

拝啓　時下ますますご健勝のこととお慶び申し上げます。日頃より会務運営に対しましてご高配を賜り深く感謝申し上げます。

さて、令和 2 年 9 月 4 日、日本医師会館内の事務局 LAN に接続しているパソコン端末 1 台がコンピュータウイルス（マルウエア）「Emotet」に感染していることを確認しました。

また、それを発端にして、同端末上のメールソフトで過去にやり取りをした関係者（本会職員、都道府県医師会職員、関係省庁職員など）の名前を騙る不審メールが、日医やこれらの関係者とは全く無関係なサーバより送信されるようになったことを確認しております。

関係者の皆様に多大なご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。本件の経緯等について、下記の通りご報告いたします。

記

１．経緯

9 月 4 日（金）始業後、本会事務局（健康医療第一課）のパソコン端末 1 台において、実在する業務委託先企業（以下、A 社）の担当者からのメールを受信し、添付されていた Word ファイル（.doc）を開いたところ、「作成したデバイスの関係で文書を開くにはこの画像をクリックする必要がある」旨の画像が表示され、それに従ってしまったために、コンピュータウイルス（マルウエア）「Emotet」に感染いたしました。これは本会事務局と A 社共通の関係者を騙る不審メールを受信した A 社担当者が、正常な業務メールと誤認して本会事務局に転送してきたメールでした。なお、日医メールサーバ上では、対策ソフトによるメールチェックを行っており、通常、Word 型の「Emotet」については、各パソコンのメールソフト到達前に駆除できておりますが、今回の原因となったメールについては駆除できずに、Word ファイルが添付された状態で届いておりました（送信元が実在する正常なアドレスであったことが、対策ソフトの挙動に何らかの影響を与えた可能性も考えられますが、原因不明です）。

4 日正午前後から、同端末上のメールソフトで過去にやり取りをした関係者（本会職員、都道府県医師会職員、関係省庁職員など）の名前を騙り、過去のメール本文のコピーを含む内容の不審メールが、無関係な外部のメールサーバより送信されるようになりました。不審メールの宛先は、同端末上のメールソフトで過去にやり取りをした相手先アドレスになります。

なお、送信者名は前述の通り実在の関係者を騙っておりますが、送信元のアドレス自体は架空のアドレスとなっております。

4 日 18 時過ぎに感染したパソコン端末を特定、館内 LAN から切り離した上で、Emotet を駆除いたしました。同端末については、さらに複数のウイルスチェックツールにて確認を実施した後、情報保全のために保管しておりますが、再利用する際にはクリーンインストールを実施するか、もしくは然るべき処理を実施した上で廃棄する予定です。

また、感染端末特定時点では、同部署の他のパソコン端末について、そして、9 月 7 日（月）には、館内 LAN に接続している稼働中のすべてのパソコン端末について、JPCERT CC が提供するチェックツール「EmoCheck」による感染確認を実施し、感染していたのが当該端末 1 台であった旨を確認いたしました（同日に所有者不在で起動できなかった端末についても、順次速やかに実施いたします）。

同ウイルスに関する過去の報告および現時点での不審メールの内容から、感染した端末のメールソフトに履歴の残っていた「送受信した相手のメールアドレスと名前」「メール本文」が漏洩していることは確実ですが、それ以外の漏洩情報を把握することは不可能です。なお、当該端末では会員情報等の個人情報は扱っておりません。

２．本会の関係者を騙る不審メールを受信された皆様へのお願い

本会の職員を名乗るメールを受信し、かつ添付ファイルが付いている場合、メールアドレスをご確認ください。本会職員が業務用に使っているメールにつきましては、基本的に「****@****.med.or.jp」を利用しておりますので、これ以外のアドレスからで、かつ心当たりのないアドレスからのメールにつきましては、削除いただけますよう、よろしくお願い申し上げます。

また、本会の職員以外に、都道府県医師会事務局や、厚生労働省などの関係省庁、関連業者等を名乗っているケースもありますので、添付ファイルを開封する前にメールアドレスが正しいものであるかご確認をお願いいたします。

さらに、今回のケースのように、関係者本人が不審メールを誤って転送してしまう可能性もあり得ますので、併せてご注意をお願いいたします。

なお、「Emotet」の不審メールについては、Word ファイルが添付されているケース以外に、Word ファイルの入ったパスワード付き zip ファイルが添付され、メール本文にパスワードが記載されているという新たなパターンが多く見受けられます。パス付 zip の場合、一般的なメールサーバ上のウイルス対策では防げない可能性が極めて高くなりますので、一層の注意が必要となります。

「Emotet」の詳細につきましては、下記「JPCERT/CC」サイトをご覧ください。

◆マルウェア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

◆上記からリンクされている「マルウエア Emotet への対応 FAQ」
※2019 年 10 月以降の Emotet に感染する Word ファイルの表示例の紹介と共に、チェックツールの説明があり、ダウンロードできるようになっています。
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

３．今後の対策について

今回については、入口対策（メールサーバ上でのウイルスチェック）で侵入を防ぐことができませんでしたが、さらにパスワード付き zip の添付という新たな手口も出てきていることから、従来から実施している入口対策と各端末上での対策に加え、出口対策（漏洩対策）の仕組みについても早期に導入したいと考えております。

また、システム面での対応だけでなく、研修等を通じて各役職員の情報セキュリティに関するリテラシー向上についても図っていく所存です。

今回の件につきましては、引き続き調査を行い、新たな事実が判明しましたらご報告いたします。関係者の皆様に多大なるご迷惑をおかけしましたことを重ねてお詫び申し上げます。

以上

本件に関するお問い合わせ先：日本医師会情報システム課（井川・増子）
TEL：03-3942-6135（課直通）／E-Mail：josys@po.med.or.jp