建設業技術者センターにおけるコンピュータウイルス感染と
それを発端にした申請者及び関係者への不審メール発生に関するお詫びとご報告

令和２年９月１８日
一般財団法人建設業技術者センター

時下ますますご健勝のこととお慶び申し上げます、
日頃より当センターの事業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17日、当センター事務局のLANに接続しているパソコン端末のコンピュータウイルス（マルウエア）「Emotet」への感染と関係者の名前を騙る不審メールが確認されておりますのでご報告いたします。
このことにより、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。

１．経緯及び確認された事象

① ９月１７日（木）午前１１時頃、当センター事務局のパソコン端末１台が、受信したメールに添付されていたWordファイル（.doc）を開いたことにより、コンピュータウイルス（マルウエア）「Emotet」に感染しました。

② 同日の正午前後から、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（当センター職員、監理技術者資格者証申請者、関係会社など）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。

③ 同日の１３時過ぎには当センター内のすべてのパソコン端末をインターネットから遮断し、同日１５時過ぎに感染したパソコンを特定するため、事務所内で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、感染していたのは当該端末を含む２台であった旨を確認致しました。

④ 当センターでは、対策ソフトによるメールチェックを行っており、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ファイル又はパスワード付zipファイルが添付された状態で届いておりました。

⑤ 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無関係なアドレスとなっております。

⑥　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、漏洩した情報は、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」と確認しております。それ以外の個人情報の漏洩は現時点では確認されておりません。

⑦　当センターの監理技術者資格者証交付システム及び発注者支援データベースと事務所内 LAN は別のネットワークとなっており、メール以外の業務への支障及びサーバ上の情報流出はありません。

２．不審メールを受信された皆様へのお願い

当センター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。当センターが業務用に使っているメールにつきましては、基本的に「****@cezaidan.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、削除いただきますよう、よろしくお願い申し上げます。特に、当センターとメールの送受信の履歴のある方におかれましては、当該コンピュータウイルスに感染したメールが送信される可能性があります。

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 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。このような場合、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．当センターにおける今後の対策について

当センターでは、従来より、メールサーバによるウイルスチェックを実施しておりますが、今回は侵入を防ぐことができず、更にパスワード付き zip の添付という新たな手口も出てきていることから、引き続き研修を強化する等によって、各役職員の情報セキュリティに関するリテラシー向上を図り万全を期してまいります。更に、システム上の対応強化の可能性に

ついても検討してまいります。

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

本件に関するお問合せ先：一般財団法人建設業技術者センター管理部管理課
TEL：03-3514-4711