2022 年 5 月 13 日

【重要】当機構役職員、関係者を装った迷惑メール（なりすましメール）について

2022 年 5 月 13 日（金）、当機構役職員や関係者を装った迷惑メールが、不正に送信されている事案を確認しました。

当機構の PC ウイルス感染等を確認したところ、該当する感染はない状況です。

不審なメールを受信された皆さまには、多大なご迷惑をお掛けしましたことをお詫び申し上げます。

これらのメールは、当機構役職員や関係者になりすまして送信された悪質なメールであり、当機構が送信したメールではありません。

つきましては、当機構とのやりとりに心当たりのないメールの場合、ウイルス感染や不正アクセスなどの危険がありますので、添付ファイルの開封や記載された URL へのアクセス、当該メールへの返信や記載された電話番号・FAX への返信等は行わず、メールを削除いただきますよう、お願いいたします。

不審なメールの見分け方は、多くの場合は送信者のメールアドレスが偽られているため、当機構からのメールを受信した際には、御手数ですが送信者のアドレスをご確認願います。

不審なメールは、送信者名に当機構の役職員の氏名が表示されていますが、当機構が利用している「〇〇〇〇@bousaisi.jp」のドメインとは異なるメールアドレスとなっております。

当機構におきましては、サーバーのセキュリティチェック、ファイアーウォールの設置、セキュリティソフトの導入等、情報セキュリティには十分注意しておりますが、引き続き対策を強化して参ります。

ご理解とご協力をいただきますようお願い申し上げます。

※マルウェア「Emotet」について（参考）
近年、世界中でメールによるマルウェア「Emotet」の感染が脅威を広げています。
これは、メールに添付されたファイルを開いてしまうと、コンピューターがウイルスに感染し、メールアカウント情報やアドレス帳の情報が抜き取られてしまうものです。
アドレス帳から抜き取った情報を利用して他人になりすまし、さらに感染を拡大させる特徴を持ちます。送信元が皆さまのお知り合いになりすましてメールを送信してくるため、騙されやすく、厄介なものです。
もし、皆さま及びご関係者の情報が入った、どなたかの端末が Emotet に感染した場合にもこのなりすましメールが届いてしまう可能性がございます。
「Emotet」というマルウェアは、そのなりすましメールに添付されたファイルを開かないことで感染を防ぐことが可能ですので、お知り合いになりすました不審なメールが届いた時には、まず添付ファイルを開かない、送信元に書かれた名前のお相手に電話等で確認する、などの対策が推奨されています。

※警視庁　Emotet（エモテット）感染を疑ったら（参考）
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html

特定非営利活動法人
日本防災士機構　総務課
電話　03-3234-1511