2022 年 6 月 10 日
社会保険労務士法人
経営管理センター

# 弊社を装った不審メールに関するお詫びとご報告

この度、弊社を装った第三者からの不審なメールが複数の方へ発信されている事実を確認し、メールの送受信者・メールアドレス・件名等のデータの一部が外部に流出したことが判明致しました。

本件につきましては、お客様をはじめ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心よりお詫び申し上げます。

弊社ではシステム会社へ調査を依頼し、この度の被害範囲と外部への影響について調査を行ったところ、弊社サーバーへの不正な侵入や事業所管理クラウドへの攻撃などの事実は無かったことを確認致しました。

弊社ではこれまでも個人情報をはじめとするデータ全般の適正な管理とセキュリティ対策に努めて参りましたが、本件の発生を重く受け止め、より一層の再発防止に万全を期して参ります。

【これまでの経緯】

2022 年 5 月 18 日　弊社を装った第三者からの不審なメールが複数の方へ発信されている事実を確認。直ちに東京オフィスの全従業員の PC についてアンチウィルスソフトによるウィルススキャン及び JPCERTCC が提供する「EmoCheck」によるウィルススキャンを二重に実施し、感染が無い事を確認。
お客様に対して第一報をメールにて報告。
被害範囲と外部への影響について、システム会社に調査を依頼。

2022 年 5 月 19 日　大阪オフィス・神戸オフィスについても同様の対応を実施し、全 PC に感染が無い事を確認。
各拠点のメールサーバーのパスワードを変更。

2022 年 5 月 20 日　お客様に対して、従業員 PC へ感染が無い事を確認した旨、続報をメールにて報告。

2022 年 5 月 25 日　改正個人情報保護法に基づき、個人情報保護委員会へ被害を届け出

2022 年 6 月 2 日　システム会社より弊社サーバーへの侵入やクラウドへの攻撃の痕跡は認められなかったとの報告を受理。
これにより今回被害にあった「Emotet」については、メールボックスから情報を抜き取る行為が確認されたが、それ以上の脅威は確認されず、ランサムウェアの脅威も無い事が確認された。

【再発防止策】
・ウィルス対策ソフト製品の強化
・ウィルス対策ソフトによる全 PC へのウィルスチェック
・ファイアーウォール製品の強化
・弊社使用の全メールアカウントのパスワード変更
・社内の情報管理体制の強化
・従業員のセキュリティ教育の徹底

【流出した情報】
・メール送受信者、メールアドレス、件名等のデータの一部

【不審なメールを受信された皆様へのお願い】
差出人や署名・件名の表記で、あたかも弊社社員から送信されたように装っています。
「内容に心当たりがない」「業務に無関係」などのメールを受信された場合は、ウィルス感染のリスクが高いため、メールの開封・添付ファイルの参照、メール本文の URL のクリック等を行うことなく削除して頂きますようお願い致します。
また添付ファイルを開封してしまった場合、お手数ですがシステム管理者に報告の上、ウィルススキャン等の対応をお願い致します。

不審メールの見分け方として、送信者の氏名表示とメールアドレスが異なっているという特徴がございます。弊社からのメールは「*****@kanricenter.com」「*****@kanri-center.jp」を利用しております。
つきましては弊社社員を装ったメールを受信された場合、まずは送信者アドレスのご確認をお願い致します。@マーク以下が上記以外の場合は、添付ファイルの開封または本文中の URL をクリックせずにメールごと削除をお願い致します。

「Emotet」の詳細につきましては、JPCERTCC が公開しているウィルスの特徴を引用致しますので、合わせてご参照下さい。

～以下、JPCERTCC サイトより引用～

Emotet の感染によってメールが送信されるケースは、感染者とその関係者を巻き込む形で複数のパターンに分かれます。

1） 自組織が Emotet に感染し、なりすましメールが配信されるケース
Emotet に感染すると、感染端末に保存されていたメールの情報やアドレス帳に保存されていた担当者名などの情報が窃取されます。
窃取された情報は、その後の Emotet の感染に繋がるなりすましメールで悪用されることがあります。

2） 取引先が Emotet に感染し、なりすましメールが配信されるケース
自組織の職員になりすましたメールが飛んでいるからといって、その職員の端末が Emotet に感染しているとは限りません。
職員が過去にメールのやりとりを行った取引先の端末が Emotet に感染し、その端末から窃取された情報に含まれていた当該職員の情報が悪用されているというケースの可能性があります。

自組織の職員になりすましたメールが送られているという場合でも、送られているメールの内容や状況を関係者間で確認および整理の上、EmoCheck や FAQ の内容などを参考に自組織の感染の有無をご確認頂くことを推奨します。

https://www.jpcert.or.jp/at/2022/at220006.html