２０２２年２月１０日
株式会社 サンシステム

弊社を装った不審メール発生に関するお詫びとお知らせ

平素は、格別のご高配を賜り厚く御礼申し上げます。
2022 年 2 月 9 日に弊社を装った第三者から複数の方へ不審なメールがあったという事実を確認いたしました。現時点での調査で分かっていることは、弊社を装った不審なメールには、マルウェア「Emotet（エモテット)」というコンピューターウィルスが含まれており、該当日にセキュリティソフトで、不審なプログラムの自動削除が実行されたパソコンが見つかりました。

ユーザー様ならびに関係者の皆様に多大なる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。

現在、影響範囲の調査を通じて二次災害や拡散の防止に努めておりますが、今回の事象を受け、より一層の情報セキュリティ対策の強化に取り組んでまいります。何卒ご理解とご協力を賜りますようよろしくお願い申し上げます。

【 不審メールの見分け方 】

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あります。
※弊社からのメールは「　＊＊＊＊＊＊@sunsystem-web.co.jp　」を利用しております。

また、不審メールには、マクロを含む Word・Excel ファイルや Zip ファイルが添付されており、ファイルを開き「コンテンツの有効化」をすることにより感染や不正アクセスの恐れが生じます。
つきましては、弊社を装った不審なメールを受信された場合、送信者アドレスをご確認いただき＠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いたします。

【 不審なメールへの対策 】

・不審なメールは、すぐに削除とご利用のセキュリティソフトでフルスキャンを実行してください。
・OS・各ソフトウェア・セキュリティソフト等、最新の状態にしてください。
・Office 製品でのマクロの自動実行を無効化する設定にしておくことでリスク軽減できます。

【 参考 】

「 Emotet 」の詳細につきましては、情報処理推機構（IPA）のサイトをご参照ください。
https://www.ipa.go.jp/security/announce/20191202.html

「 Emotet 」に感染しているか確認したいという方は、一般財団法人 JPCERT コーディネーションセンターの GitHub で感染チェックツール「 EmoCheck 」が公開されております。
https://github.com/JPCERTCC/EmoCheck/releases

「 Emotet 」に関する 2022 年 2 月 10 日に発表された YAHOO ニュースのリンク
https://news.yahoo.co.jp/articles/8f016ab8ab8ab8f705fb9421bd389ec480c03fa2