お客様各位

2020 年 8 月 27 日
株式会社オザワ

弊社になりすましたマルウェア感染を伴う不審なメールに関するお詫びとお知らせ

この度、弊社より不審な添付ファイルが送られてくるとのご指摘を外部から受け、
事実関係を調査いたしましたところ、弊社のパソコンがコンピューターウイルス（Emotet）に感染し、外部より不正アクセスされ、メールボックス内に残っていたお客様情報が漏洩した可能性が判明いたしました。

本件でお客様には、多大なるご迷惑とご心配をおかけしましたこと、深くお詫び申し上げます。

１．情報漏洩の概要

８月 25 日弊社内のパソコン１台がマルウェア「Emotet」に感染。実在する取引先を名乗るメールだったために、添付ファイルを開封してしまったことが原因と考えられます。
これにより弊社にて利用しておりましたメールサービスにおいて、特定のメールアカウントに第三者が不正アクセスをし、お客様情報等メールボックス内のデータが漏洩いたしました。

２．漏洩が確認されている情報項目

2020 年 8 月 25 日迄にお客様の氏名（法人名含む）、住所、電話番号、メールアドレス、送受信メール本文

３．経緯と対応状況

① 経緯

8 月 25 日 弊社より不審なメールが送られてくるとのお客様よりご指摘を受け、社内調査を行ったところ、弊社社員のメールアカウントが外部より不正にアクセスされたことが確認されました。

② 対応状況

弊社では更なる情報漏洩を防ぐため、当該アカウントを使用しておりましたパソコンのオフライン化した上で初期化、当該メールアカウントのパスワードを強化し変更、社内ネットワークのセキュリティシステムの強化を行いました。

４．再発防止策

上記②に記載の対応に加え、セキュリティの強化に取り組み、新たな被害が無いよう注視してまいります。

弊社を騙る不審なメールが届いておりましたら、本文中に記載されている URL を開いたり、添付されているファイルなどを開たりせずに、メールごと削除していただきますようお願いいたします。

「なりすましメール」は弊社社員名を名乗ってメール本文中に弊社のメールアドレスを記載しておりますが、送信メールアドレスは弊社とはまったく関係のないメールアドレスになっています。不審メールを受信の際には送信元メールアドレスをご確認ください。

万が一、不審なメール上のリンクや添付ファイルを開いた場合は、下記情報をご覧の上、ご対応をお願い致します。

<JPCERT/CC マルウェア 「Emotet」への対応 FAQ>
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

引き続き調査の上、新たな事実が判明しましたらご報告いたします。
関係者各位に多大なるご迷惑をおかけしたことを重ねてお詫び申し上げます。