2019 年 2 月 6 日

標的型攻撃メール感染による情報流出についてのお詫びとお知らせ

公益財団法人日本生産性本部

このたび、当本部事務局員が使用しているパソコンが、標的型攻撃メールによるウィルスに感染していたことが判明し、その後、当本部のパソコンからお客様情報が流出した可能性のあることが判明いたしました。

このような事態になり、個人情報をご提供いただいた皆様をはじめ、関係者の皆様に多大なご迷惑とご心配をおかけしましたことを深くお詫びいたします。

今回の事態を厳粛に受け止め、引き続き調査を行い、二次被害の防止を図るとともに再発防止に向けて個人情報の取り扱いに万全を期し、セキュリティ対策を強化するよう努めてまいります。

記

１．経緯

- 2018 年 10 月 3 日：標的型攻撃メール着信。4 日に添付の word ファイルを開き感染。
- 10 月 17 日：10 月 4 日に着信したファイルを別のパソコンにて開く。ウィルス対策ソフトが検知。対象のパソコンを隔離。
- 10 月 22 日：外部調査機関 A に相談。調査を依頼。
- 10 月 25 日：ファイヤーウォールで通信禁止措置実施。
- 10 月 31 日：外部調査機関 A より、「攻撃者によって情報を窃取された可能性があると推察」との連絡を受け、セキュリティベンダと緊急対策開始。
- 11 月　1 日：外部調査機関 A より、「メールアカウント情報が窃取された可能性あり」との連絡を受ける。
- 11 月 2 日：全端末のメールシステムのパスワード変更を実施。
- 11 月 6 日：セキュリティベンダ（外部調査機関 B）によるフォレンジック(事故証跡)調査開始。
- 11 月 16 日：セキュリティベンダ（外部調査機関 B）の調査結果により、新たな事故証跡が判明。
- 2019 年 1 月 28 日：流出の可能性のある情報の件数を特定

２．流出の可能性のある情報

・ 期間（推定）：10 月 4 日～25 日
・ お客様データ：9,288 件、（企業名、所属・役職、住所、氏名）
（9,288 件中、8,427 件は当本部賛助会員データ）

３．原因

当本部への悪意ある標的型攻撃メールの送信による不正アクセス。

４．現在の状況

現在まで、お客様から、上記の流出した情報に対する不審な動きに関するご指摘やご相談は頂戴しておりません。

今後、ご関係の皆様にお知らせすべき新たな情報が判明いたしましたら、随時ホームページ等でお知らせいたします。

５．再発防止策等

・ 全端末のメールシステムのパスワード変更を実施いたしました。
・ 当本部内において、情報セキュリティ管理および個人情報管理の関連規定の再通知再徹底をはかり、全職員に対して、メール開封時の対応や不審メールの取り扱いについて対応を徹底してまいります。
・ 新種のマルウェアの対策、ネットワーク監視の強化など、セキュリティ対策の強化をはかってまいります。

＜本件に対するお問い合わせ先＞

統括本部（総務）　鵜野沢（うのざわ）
TEL：03-3511-4003