村澤社会保険労務士法人
令和４年５月号

不正プログラム「エモテット」にご注意！

◆「エモテット（Emotet）」の脅威

2022 年に入り「Emotet（エモテット）」によるサイバー犯罪被害が激増しています。エモテットとは、主にメールを介して感染を広げるマルウェア（不正プログラム）で、取引先に対してマルウェアに感染した「なりすましメール」を勝手に送りつけるほか、ＰＣ内の機密データを知らぬ間に操作･窃取されたり、ランサムウェア（社内データ等を人質に金銭を脅し取ることを目的とした不正プログラム）がダウンロードされ、社内ネットワーク内のＰＣに感染を拡げたりするなどの被害をもたらします。実際のメールの件名を利用するなど、なりすましの手口も巧妙化しています。

◆対応策

政府はこうした事態を受け、次のような対策を講じるよう企業に注意喚起しています。

１．リスク低減のための措置

○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○ＩｏＴ機器を含む情報資産の保有状況を把握する。特にＶＰＮ装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○メールの添付ファイルを不用意に開かない、ＵＲＬを不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知

○サーバ等における各種ログを確認する。

○通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復

○データ消失等に備えて、データのバックアップの実施および復旧手順を確認する。

○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

被害を受けた場合、その影響は自社にとどまらず、サプライチェーン全体の事業活動に及ぶ可能性があります。積極的な対策を講じていきましょう。

【経済産業省「サイバーセキュリティ対策の強化について注意喚起を行います」】

https://www.meti.go.jp/press/2021/03/20220324008/20220324008.html

【警視庁「サイバーセキュリティ ad 資料」】

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/CS_ad.html