令和 7 年 3 月 21 日

各位

当社におけるセキュリティインシデントの発生について(第 2 報)

シンク・エンジニアリング株式会社
代表取締役　岡村　勝也

日頃よりシンク・エンジニアリング株式会社をご愛顧いただき、誠にありがとうございます。

このたび、令和 7 年 1 月 8 日付で当社ホームページにて報告させていただきましたとおり、当社内のサーバが不正アクセスを受けました。その際、サーバ内のドキュメント及びファイルが暗号化され使用出来なくなるとともに、一部が窃取されるという被害が生じました。

本文書では、本インシデントに関する当社の現時点での調査結果をご報告申し上げます。皆さまに正確なご報告ができるよう被害の状況把握に時間を要しましたこと、皆さまにご迷惑とご心配をおかけしておりますことを、心より深くお詫び申し上げます。

当社では、このたびの事態を厳粛に受け止め、お客様には誠心誠意、適切な対応をさせていただくとともに、再発防止の対策を徹底して参ります。

記

1. 本インシデントの概要

令和 7 年 1 月 4 日早朝、社内業務システムにシステム障害が発生し、調査を行った結果、社内業務用サーバが不正アクセスを受け、ランサムウェアにより複数のサーバが暗号化されていることが確認されました。直ちに感染拡大防止措置としてネットワークの遮断を実施しましたが、現時点の調査では、一部社内業務システムのファイルが暗号化されると同時に、不正アクセスが行われました事が判明しております。

２. 外部犯罪集団によって閲覧及び窃取された可能性がある情報

専門会社による調査により、お客様サービスに関わる情報の一部において、漏洩した恐れのある痕跡が確認されました。情報が漏洩した可能性のあるお客様には、個別にお知らせさせて頂きます。

３. インシデント対応状況

ランサムウェア感染の発覚以後、対策本部を設置し、原因や影響の範囲、また復旧の見通しについてセキュリティ専門会社と共に調査を進めてきました。

上記調査の結果、ランサムウェア感染の原因となった脆弱性が特定されました。

結果を受け、是正処置及びシステムの更新を行い、一部業務について社内業務システムを仮復旧いたしました。

４. 二次被害及びその内容

漏洩等の可能性がある情報の中に、経済的な二次被害を直接生じさせうる情報は含まれておりませんでした。また、現時点で本インシデントにて漏洩した情報を用いた二次被害については確認されておりません。

５. 再発防止策について

当社はこのたびの事態を厳粛に受け止め、調査結果を踏まえてシステムの更新、セキュリティ対策及び監視体制の強化を行い、再発防止を図ってまいります。

この度は、お客様はじめ関係各位に多大なるご心配、ご迷惑をおかけすることとなり、重ねてお詫び申し上げます。

以　上