「セキュリティ」

日本テンプルヴァン（株）井上拓郎

「サイバー攻撃」

９月から１０月にかけて次々と明るみになった情報漏洩（ろうえい）問題。様々な企業が外部から攻撃を受け、氏名、生年月日、メールアドレス、電話番号、住所などの個人情報や、運転免許証の画像が流出した可能性があると、連日の様に発表がありました。情報漏洩を公表した企業の大半はサイバー攻撃によって、個人情報などの漏洩、システム障害による業務停止、信頼低下による株価への影響などの被害を受けました。これらの被害は企業のみならず、政府機関や地方自治体などの委託先企業へも影響を及ぼしました。その一つが、デジタル庁が運用する政府共通のネットワーク基盤「ガバメントソリューションサービス（ＧＳＳ）」で、２３機関の職員や業務関係者などの個人情報(氏名、メールアドレス、電話番号など）が漏洩した可能性があると公表されました。ちなみに一般の国民の個人情報は含まれていない様ですが、約２万４，６００件の情報が漏洩した可能性があるそうです。それ以外でも大阪府のＩＴ関連企業への不正アクセスにより、自治体向けの緊急情報配信システムなどに影響が出たほか、各地の地方自治体や委託事業者でもランサムウェア被害や情報漏洩が報告されております。またこの件の漏洩によって警察官、及び警察職員の氏名、メールアドレスも流出したと発表がありました。これらの被害は第三者（国、個人、団体を問わず）からのサイバー攻撃によって発生している訳ですが、直接的な攻撃によって企業や団体が標的となり、漏洩した個別の個人情報を複合的に統合すると、個人の特定に繋がる重大な個人情報になる恐れがあります。それぞれのデータを統合すると、スマホのアプリや様々なオンライン取引のログイン情報などに結び付く可能性があります。もちろんサービスによってメールアドレスを替える、パスワードの使いまわしを行わない、指紋や顔認証などの生体認証や２段階認証を設定する事によって、ネット空間での個人情報を結び付けにくくし、外部からの侵入や接続を出来なくするなどの対策をとる事によって、ある程度の防衛は出来ますが、１００％万全と言う訳ではありません。今回のサイバー攻撃の主体がＡＩである事が分かってきておりますが、情報は漏洩するものと認識し、最低限の自己防衛を行う事が、現段階での唯一の防衛策なのかもしれません。

「情報セキュリティ基本方針」

ＡＩも使い方によって便利なツールにもなり得ますが、悪意を持って利用するものにとっても都合のいいツールである事は疑いようのない事実です。昨今のサイバー攻撃の主流は、不特定多数の対象へＡＩを使って脆弱性を見つけて攻撃するといったやり方が大半の様ですが、ホームページを持っていてネットに繋がったサーバー環境（パソコンも含む）を利用又は所有していたりすると攻撃の対象となり得る可能性があり注意が必要です。特に長い間様々なアップデートをせずに放置していると、セキュリティホールなる隙間から侵入され、サーバーを乗っ取られる可能性があります。そういった事が原因かは判りませんが、実際にある宗派ではホームページがサイバー攻撃によって閲覧できなくなる事象が発生しました。この様な事が起こらぬ様、情報セキュリティの基本的な考え方、運用体制、運用規定、対策基準などを定めたものに情報セキュリティ基本方針というものが有ります。基本方針を定めて・実行して・検証して・改善までが一サイクルなので、繰り返して継続する事が重要です。ちなみに浄土宗ではこの情報セキュリティ基本方針を定めてホームページで公表しております。皆さんも参考にされてみては如何でしょうか。