

経営視点からのサイバーセキュリティと企業責任

教学大介氏

東京海上日動火災保険 サイバー室専門次長

東京海上ディーアール サイバーセキュリティ事業部チーフコンサルタント

近年では企業を標的とするサイバー攻撃が頻発し、その被害は自社のみならず取引先や顧客まで巻き込み拡大する危険性をはらみます。ひとたび発生すれば企業経営の根幹を揺るがしかねないサイバーリスクに企業はどのように対処すべきなのか。経営者が知るべき最新情報や対策法をうかがうため、日本の損害保険会社として初のサイバーリスク保険開発に携わり、サイバー攻撃対策の最前線で活躍する教学大介さんを講師にお迎えしました。

企業を取り巻くサイバーリスクの実態

情報セキュリティの「10大脅威」が毎年、情報処理推進機構から発表されますが、2026年版では第1位が「ランサム攻撃による被害」、2位が「サプライチェーンや委託先を狙った攻撃」で、いずれも毎年上位に挙がる脅威です。3位には今年初めて「AIの利用をめぐるサイバーリスク」が選出されました。ハッカーはシステムの穴を見つけ、パッチで塞がれる前に攻撃を仕掛けますが、AIでより早くシステムの脆弱性を特定できるようになり攻撃頻度も上がっています。

サイバー攻撃を受けた企業は被害額が10億円単位にのぼることもあります。サイバー攻撃を受けた企業が被る損害は、業務停止に伴う売上損失、取引先に被害が及んだ場合の賠償責任、サイバー攻撃に対処するための調査やシステム再構築に要する費用などとなります。たとえば2024年に



攻撃を受けた KADOKAWA は決算で数十億円の特損失を計上しました。

ランサム攻撃では身代金が要求され、拒否する企業に対しては第2段階として窃取

した情報をバラ撒くと脅してきます。顧客や取引先への影響を恐れる企業に要求をのませるのが狙いです。

サイバー攻撃の話をする「大手企業は狙われてもウチは大丈夫でしょ」と楽観する中堅・中小企業の経営者もいます。しかし実際には従業員数が50～200名規模の企業の被害報告も多く見られます。セキュリティが厳重な大手企業に時間と資金を投じて侵入し多額の身代金交渉をするよりも、とにかく侵入しやすい企業を狙う方向に戦略を変えてきたと考えられます。

そもそもサイバー攻撃は攻撃側に有利で、システム上にひとつでも侵入口を見つければ彼らの勝ち。最新の AI の活用や未知のウィルス等の武器も保持している。対する防御側企業は IT 部門が片手間でセキュリティ対応しているのが現実であり、侵入口が存在する領域はシステムに限らず社員の行動、取引先などさまざまな場所に及んでいます。しかも 100%完璧に防いでやっとな引き分けです。

いまやサイバー攻撃は、if つまり「万が一起きたら」ではなく、when「いつ起きるか」という時間の問題になりました。

覚えておくべき来年末開始の新制度

サイバーセキュリティに関し、意識しておくべき新制度が 2027 年末より開始される予定です。経済産業省が定めた「サプライチェーン強化に向けたセキュリティ対策評価制度 (SCS 評価制度)」がそれです。自社内だけでなく取引先や業務委託先にも求めるべきセキュリティ対策の指針とガイドラインが明確化され、「標準的に

目指すべき対策」や「到達点として目指すべき対策」等の内容が定められました。

つまりセキュリティ対策は自社内だけでは済ませられなくなり、取引相手や業務の受委託先に対して、セキュリティ対策を求めたり求められたりする段階に入るわけですが。ここで注意すべきは、川上側に位置する発注者の立場でセキュリティ対策を強く求めすぎると取引条件や費用負担のあり方によっては、取適法（旧下請法）上の問題となる可能性があること。対策を要望するに際しては、取引先が何をすべきかの説明会を開催し、公的な支援制度の紹介、対策による原価上昇に伴う価格交渉にも応じる必要があります。こうした配慮を通じてパートナーシップを構築し、取適法違反に問われない対策を施すことも重要なポイントです。

サイバー攻撃で企業に何が起こるのか

サイバー攻撃はある日突然に起きます。発覚までの時間稼ぎのため金曜夕方から週末にかけて攻撃が仕掛けられ、多くは週明けに事態が明るみ出ます。ところが専任担当者を置く企業は少なく、社内に何からどう指示すればよいのか、対処法が分からない経営者は少なくありません。しかも早期の事業再開や被害拡大防止など短時間で対処すべき要素が多く、身代金の期限への対応も迫られるという、二重三重の時間的プレッシャーにさらされます。個人データの漏えい等が発生し、個人情報保護法上の報告対象となる場合には、速報、確報について法令上の期限も意識する必要があります。また、外部公表やマスコミ対応

など通常は経験のない事象にもさらされます。

加えてシステム復旧や対外対応をおこなう前提として原因調査が必須となりますが、被害状況の見極めや原因究明のためのデジタルフォレンジック調査を委託できる業者探しが困難です。最近は各業者とも多くの仕事を抱えているのが実情です。やっと業者を見つけても彼らが与信調査を終え契約締結までに1週間はかかります。

ようやく見積もりを取れば費用の大きさに驚くでしょう。パソコン1台の調査に200万円ほどかかるのが相場です。調査だけで数千万円単位になることも珍しくありません。これでは保険に入っていなければ多額の費用負担が迅速な復旧の制約となる場合があります。保険に入っていれば、デジタルフォレンジック業者も与信を軽減できる可能性がありますし、保険会社が無料でサイバーセキュリティの専門家から契約企業に対してアドバイスもします。ちなみに当社ではサイバーリスク保険を発売以来、約3000件の実績があり、数少ないグローバル資格を持ったサイバーセキュリティ専門家とのパイプもあります。

企業責任問われるサイバーセキュリティ

サイバー攻撃を受けた企業は被害者の立場ですが、一定の責任が生じます。第一に、流出した中に個人情報が含まれれば個人情報保護法上の責任があり、法令上の報告義務については先ほど説明した通りです。第二に、取引先に迷惑をかけた際の責任です。自社の過失で取引先に損害を与えれば民法上の不法行為責任や、契約上の債

務不履行責任が生じるケースもあります。

契約関係がない取引先企業へ送ったメールが原因で相手がサイバー攻撃の被害を受けた場合は責任の所在を判断するのが難しい面はありますが、こういう事例がありました。大阪の救急病院がサイバー攻撃を受け数カ月間にわたり診療がストップ。給食納入業者のVPN機器の脆弱性が原因であることが後日判明しました。病院側は給食業者等を相手取り損害を訴え、最終的に給食業者等が和解金を支払うことで和解決着しました。責任の有無や程度は、個々の事案における予見可能性や講じていた対策などを踏まえて判断されます。SCS評価制度そのものに強制力や罰則があるわけではありませんが、今後広く普及すれば、企業に求められるセキュリティ対策の水準を考えるうえで、一つの参考となる可能性があります。その意味でも、自社や取引先に求められる対策水準を確認しておくことが重要です。

サイバーセキュリティは、もはやIT部門だけの課題ではなく、経営者自身がセキュリティを重視する姿勢を明確に示し、必要な人材・時間・予算を確保することが重要です。そうした経営者の意思が、組織全体の対応力を高め、万一の際の早期復旧にもつながります。

<Profile>

きょうがく・だいすけ●1997年東京海上火災保険に入社。2005年より商品開発部門へ異動し2015年にサイバーリスク保険を開発。2022年経団連サーバーセキュリティWGコアメンバー、2024年からは経済産業省産業サイバーセキュリティ研究会委員も務める。