情報セキュリティ対策

～ 危険性を正しく認識し、まず取り組むことが重要 ～

業務のデジタル化に伴ってサイバー攻撃の危険性が高まると懸念される一方、規模の小さい企業ほどそのリスクを軽視する傾向がみられます。サイバー攻撃のリスクを軽減して自社の持続可能性を高めるには、適切な情報セキュリティ対策が必要であり、経営者がリーダーシップを発揮して実践しやすい取組からスタートすることが求められます。今回は、企業を取り巻くサイバー攻撃の現状・必要性を紹介するとともに、取り組みやすい具体的な対策を解説します。

サイバー攻撃の現状

近年、企業を狙ったサイバー攻撃が増加しており、情報セキュリティ対策を取る必要性が増しています。

（独法）情報処理推進機構が公表した「情報セキュリティ 10大脅威2024」では「『組織』向け脅威」の上位３つとして「ランサムウェアによる被害・サプライチェーンの弱点を悪用した攻撃・内部不正による情報漏えい等の被害」が挙げられています（図表１）。

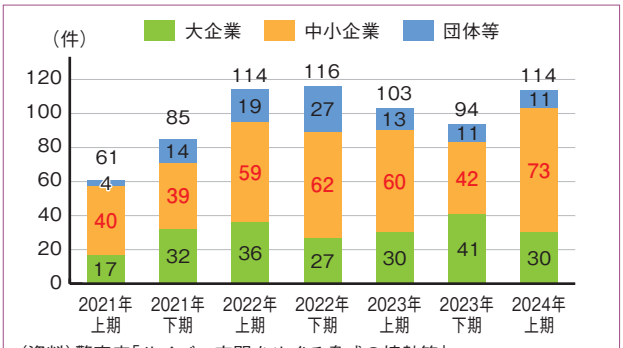
図表１　「組織」向け10大脅威

順位	「組織」向け脅威
1	ランサムウェアによる被害 <データを暗号化し、身代金を要求するウイルスに感染させる>
2	サプライチェーンの弱点を悪用した攻撃 <取引先のシステムを踏み台に、社内ネットワークへ侵入する>
3	内部不正による情報漏えい等の被害 <組織の関係者が、悪意を持って情報漏えいする>
4	標的型攻撃による機密情報の窃取 <特定の組織を狙い、弱点に合わせた手法で攻撃を行う>
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） <ソフトウェアの脆弱性を悪用し、修正される前に攻撃する>
6	不注意による情報漏えい等の被害 <社内の人為的なミスにより、社外に情報が漏えいしてしまう>
7	脆弱性対策情報の公開に伴う悪用増加 <ソフトウェア更新パッチなど、公開された対策情報を悪用する>
8	ビジネスメール詐欺による金銭被害 <社内外の関係者になりすましたメールを通じ、振込をさせる>
9	テレワーク等のニューノーマルな働き方を狙った攻撃 <テレワークに導入された製品等を狙い、社内ネットワークへ侵入する>
10	犯罪のビジネス化（アンダーグラウンドサービス） <企業の情報が、攻撃する目的で不正に取引されてしまう>

（資料）（独法）情報処理推進機構「情報セキュリティ10大脅威 2024」をもとに作成

最上位に挙げられた「ランサムウェアによる被害」の警察庁への報告件数は、年間200件を超えるペースで推移しています。ただし、被害を受けても警察へ報告しない企業も一定存在すると考えられ、実際の被害件数はさらに多いとみられます。直近の半数以上が中小企業の被害であり、規模の大小を問わず、攻撃を受けていることが分かります（図表２）。

図表２　企業・団体等によるランサムウェア被害の報告件数



（資料）警察庁「サイバー空間をめぐる脅威の情勢等」

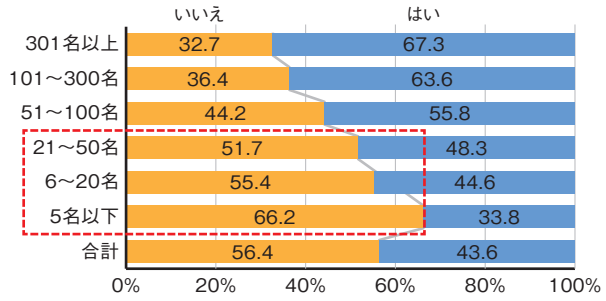
NPO法人日本ネットワークセキュリティ協会によると、ランサムウェア攻撃を受けた組織の被害金額は平均2,385万円、対応に要した内部工数は平均27.7人月とされており、自社の経営に大きな打撃を受けることになります。

自社で取り組む必要性の認識

今後、生産性を向上させるため社内外における業務のデジタル化が進展していくなか、ひとたび攻撃を受けると、自社の業務が滞るだけでなく、取引先の機密情報漏えい等によってサプライチェーンに波及した際の被害は甚大なものになると懸念されます。

サイバー攻撃のリスクが高まっていくと懸念される一方、企業の意識は十分と言えません。自社が情報セキュリティ被害に遭う可能性を感じないとする割合は56.4％と過半数に上り、従業員数が少ない企業ほどサイバー攻撃によるリスクを軽視する傾向がみられます（図表３）。

図表３　自社が情報セキュリティ被害に遭う可能性を感じるか



（資料）三菱UFJリサーチ＆コンサルティング㈱
「中小企業における情報セキュリティ対策の最新動向」

経済産業省は、サイバーセキュリティに関して「経営者が認識すべき３原則」として、下記の内容を掲げています。

①「経営者のリーダーシップが重要」
⇒経営者が情報セキュリティにかかわるリスクを自社の重要な経営課題として捉え、全社的な対策を主導する

②「サプライチェーン全体にわたる対策への目配り」
⇒取引先や委託先等を含めたサプライチェーンの一員としての責任を持ち、セキュリティ対策を徹底する

③「社内外関係者との積極的なコミュニケーション」
⇒普段から、セキュリティ対策に関する情報を社内外で共有することで、緊急時の対応が円滑になる

まずは経営者が、サイバー攻撃を受けた際のリスクを正しく理解し、取り組む必要性を認識することがセキュリティ対策の第一歩であると言えます。

すぐ実践できるセキュリティ対策

（独法）情報処理推進機構の情報セキュリティ白書2024によると、「情報セキュリティ対策を進める上での問題点」は、「必要な知識を持ち、対策を行うための人材不足」「従業員の情報セキュリティ意識の低さ」「セキュリティ対策を行うための予算の確保」に集約されます。

つまり、企業がセキュリティ対策を進めるための課題は「人材不足・社員教育・予算」と言え、このことを前提に、中小企業が実践しやすい対策として、以下の４点が挙げられます。

①守るべき情報の識別
⇒社内で保有する情報の重要度を明確にし、従業員がその重要性を認識できるよう管理する

②堅固なパスワード管理
⇒なるべく文字数の多いパスワードを設定し、定期的な変更を徹底する

③従業員へのセキュリティ教育
⇒従業員のセキュリティ意識を高めるため、研修を定期的に実施する

④情報管理に関する社内規程の策定
⇒従業員が異常を迅速に報告し、早期に対策できるよう、社内ルールを明確にする

こうした基本的な対策を実践するだけでも、自社がサイバー攻撃を受けるリスクを軽減するとともに、攻撃を受けた際の被害を抑制できます。

加えて、セキュリティ対策の実効性を高めるには、経営者またはシステムに関連する権限を持った役員が主導して取り組むことが必要不可欠です。

また、（独法）情報処理推進機構が提供する中小企業向けの無料ツールを用いることも有効です。セキュリティ対策の評価や社内での研修実施等、自社の取組状況に応じて内容を選択し、活用できます。

①「５分でできる！情報セキュリティ自社診断」
⇒自社のセキュリティの現状を客観的に評価し、改善点を把握できる

②「映像で知る情報セキュリティ」
⇒YouTubeで公開された動画を使い、短時間での社内研修を実施できる

③「情報セキュリティ関連規程（サンプル）」
⇒中小企業向けがセキュリティ関連規程を策定する際の叩き台として、自由に編集できる

サイバー攻撃は中小企業にとって他人事でなく、経営者自身がその危険性を認識したうえで、すぐ実践できる情報セキュリティ対策から始めることが重要です。

三十三総研 コンサルティング部
コンサルタント　長井　翔吾

San ju san Institute of Research,Ltd. All rights reserved.