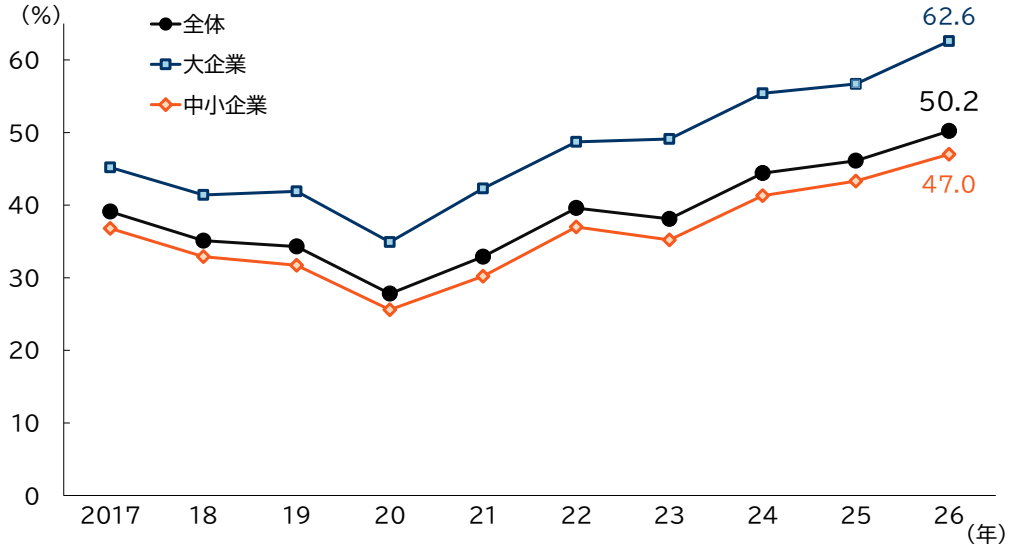
なぜ今、セキュリティは経営課題なのか――攻撃の進化と企業の備え

企業経営においてサイバーリスクは、もはや専門部署だけが扱う技術課題ではありません。近年では、国内外の製造業や流通業、金融機関といった大企業がランサムウェア攻撃を受け、操業停止や物流混乱に追い込まれる事例が相次ぎました。こうした被害は大企業だけではなく、中堅・中小企業、さらには個人にまで攻撃対象が広がっています。サイバー攻撃は「いつか起きる可能性のある事故」ではなく、「常に起きている前提で備えるべき経営リスク」に変化しています。

こうした認識の広がりは、調査データにも表れています。帝国データバンクが毎年実施している「事業継続計画（BCP）に対する企業の意識調査」によると、2026 年は「情報セキュリティ上のリスク」が過去最高となりました。サイバーリスクは上昇傾向にあり、企業規模を問わず脅威と認識されていることがうかがえます。すでに一部の先進企業だけの課題ではなく、すべての企業が備える必要がある共通課題となっています。

事業の継続が困難になると想定しているリスク
「情報セキュリティ上のリスク」の推移



攻撃が急増している背景には、いくつかの構造的要因があります。ひとつは、デジタル化の進展です。クラウドやリモートワークの普及により、企業の情報資産が外部ネットワークに広く接続され、攻撃対象領域が拡大しました。加えて、攻撃の「産業化」が進んでいます。攻撃ツールやノウハウが闇市場で流通し、専門知識を持たない個人でも容易に参入できるようになりました。いわゆる「RaaS（ランサムウェア・アズ・ア・サービス）」はその象徴といえます。

攻撃の手口も多様化しており、代表的なのは、巧妙化したフィッシングメールによる認証情報の窃取です。従来の不自然な日本語ではなく、業務連絡を装う自然な文面が増えて

おり、その精巧な内容が従業員の判断を惑わせています。さらに、VPN 機器やソフトウェアの脆弱性を突く侵入、サプライチェーン経由の攻撃も増加しています。一度侵入を許せば、内部ネットワークを横断的に移動して最終的にはデータの暗号化や窃取へと至るのが典型的な流れとなっています。

重要なことは、こうした攻撃が企業規模を問わないということです。セキュリティ投資が十分でない中小企業は、むしろ標的になりやすく、結果として取引先である大企業への侵入経路として悪用されるケースもあります。また、個人に対しても、ネットバンキングやオンラインサービスの普及により、日常的にリスクにさらされています。

多くの企業がセキュリティ製品を導入していますが、それだけでは十分と言えません。課題の中心はむしろ運用にあります。全社的なリスク認識が不足していると、重大な事故が発生した際の初動対応が遅れ、被害が拡大します。専門人材の不足も大きな制約となっており、監視や分析が不十分な体制のまま運用されているケースも少なくありません。さらに、ルールと実態の乖離も問題です。規程は整備されていても現場で徹底されていない場合、対策は形骸化します。さらに、サプライチェーン全体での管理が不十分な場合、自社の対策だけでは防ぎきれないリスクが残ります。

実効性のある対策には、まず、継続的な教育が重要です。単発の研修ではなく、疑似攻撃を取り入れた訓練などを通じて、従業員の判断力を日常的に鍛える必要があります。多くの攻撃が人の操作を起点としている以上、現場のリテラシー向上は不可欠です。次に、ルールの明確化と運用の徹底です。パスワード管理や多要素認証の導入、端末利用の基本ルールなど、基本的な統制を確実に実行することが出発点となります。また、インシデント発生時には迅速に報告できる体制を整え、早期対応につなげることが重要です。さらに、経営主導による文化づくりも欠かせません。セキュリティ対策をコストではなく投資と位置付け、経営層が主体的に関与することで、組織全体の優先度が高まります。個人レベルでも、パスワードの使い回しを避け、多要素認証を活用すること、不審なリンクやメールを安易に開かないことが重要であり、基本的な対策の徹底が求められます。

サイバー攻撃の進化は著しく、今後も進化し続けることが予想されます。完全な防御を前提とするのではなく、「侵入される可能性を前提に備える」という考え方への転換が重要です。迅速な検知と対応、被害の最小化を重視した体制を整えることで、リスクは管理可能なものとなります。経営層と現場、企業と個人がそれぞれの役割を果たすことで、サイバーリスクへの耐性は着実に高まっていくでしょう。

情報統括部　情報統括課
中村駿佑