特集

見えない脅威から会社を守る

～情報セキュリティ対策～

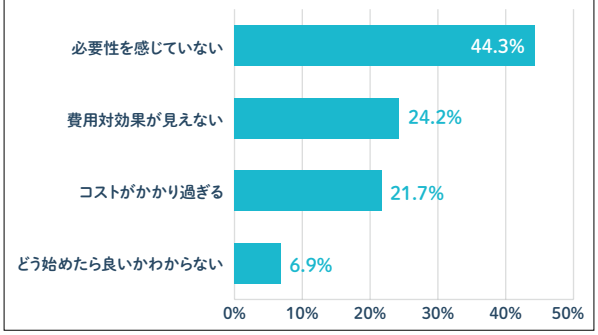
情報化の進展とともに、企業活動における「情報」の重要性や漏洩のリスクも高まっている。大手メーカーや通販事業者がサイバー攻撃を受けて企業経営に大きな影響が出るなど、あらゆる企業で、情報セキュリティ被害が起こることを前提に、必要な対策を取ることが求められている。深刻な影響を及ぼす代表的な攻撃手法は次の通り。

ランサムウェア	Emotet（エモテット）
感染したＰＣやサーバー内のデータを暗号化して使用を制限し、解除と引き換えに金銭を要求してくる。被害者側が金銭の支払いを拒むと盗んだ情報をネット上で公開すると脅す「二重恐喝」や、取引先にも連絡して圧力をかける「三重恐喝」など、手口が高度化している。	メールの添付ファイルを主な感染経路とする悪意のあるソフトウェアの一種。ワードやエクセルのマクロ機能（作業の自動化に役立つ機能）を悪用し、感染すると、個人情報や機密情報が窃取されたり、気づかないうちに他人へ攻撃メールを送信するなど、深刻な被害を引き起こす。

一方で、（独）情報処理推進機構が実施したサイバーセキュリティ対策に関する実態調査では、約6割の企業は過去3期にわたって情報セキュリティ対策に投資を行っておらず、十分な情報セキュリティ対策が行われていない実態が浮き彫りとなった。

情報セキュリティ対策に投資をしていない理由としては、「必要性を感じていない」が44・3％と最も多く、「費用対効果が見えない」24・2％、「コストがかかりすぎる」21・7％という回答が続いている（図1参照）。回答者は中小規模の企業者が多いため、情報セキュリティ対策の必要性が十分に理解されていないことや、コストに見合う投資なのか確信が持てずに投資が躊躇されている実態が分かる。

図1 情報セキュリティ対策に投資をしていない理由



出典「2024 年度中小企業における情報セキュリティ対策に関する実態調査報告書」（独立行政法人情報処理推進機構 調査）

そこで今回の特集では、情報セキュリティの強化に向けて、積極的に対策に取り組む企業や、その活動をサポートする事業者、専門家から取り組みの重要性を紹介する。

TOPIC 01

INTERVIEW
with ホーコーズ

顧客と社員を守る情報セキュリティ

株式会社ホーコーズ
システム担当 野中 達也 氏（右）
管理部 齊藤 昌代 氏（左）

福井市光陽で大型印刷物やＷｅｂサイトなどの製作を手掛ける（株）ホーコーズで、社内の情報セキュリティ対策を担う野中達也氏、齊藤昌代氏に取り組み内容をうかがった。

ECサイトの立ち上げを契機に

同社は昭和48年に創業し、主に官公庁からの注文を受け建設工事の図面の印刷や製本業務を担ってきた。

時代の変化と共に大型印刷物の注文が増え、平成19年にはＥＣサイト「大型出力屋」を立ち上げた。紙素材に加えアクリルパネルなど20種類以上の素材への印刷を手掛け、現在ではタペストリーや懸垂幕、壁紙、展示パネルなど多種多様な大型印刷物を製作している。「小ロット、多品種、短納期」をモットーに取引先は1万件、製作実績は43万件を超えている。

ＥＣサイトを立ち上げたことで多くの顧客情報を扱うことになり、情報管理を徹底させるため、番場光太郎社長の指示で、２００７年に「ＩＳＭＳ／ＩＳＯ２７００１」（国際情報セキュリティマネジメントシステムの国際認証規格）を取得した。

認証取得から社員意識の浸透へ

取得に合わせて、社員一人一人のセキュリティ意識の向上を図るため、情報セキュリティを管理・運営する社内委員会として「ＩＳＯチーム」を組織した。現在では野中氏と齊藤氏が中心となり、情報セキュリティに関する社内研修を年2回開催したり、他社におけるトラブル事例を社員と共有して、同様の被害に遭わないように啓発活動に取り組んでいる。

また、情報漏洩を防ぐため、社内ネットワークのアクセス権限を社員ごとに管理したり、休日や夜間はログインを禁止しているほか、ファイル共有サービスへのアクセスも禁止している。

外部からの攻撃で、システムの脆弱性を突かれないために、サーバーのアップデートを徹底しており、ＥＣサイトも月2回の頻度でアップデートを行っている。万が一、サイバー攻撃を受けた場合に備え、半年に1回はデータのバックアップを取り、データの区分や隔離などの対策も実施している。

更なる意識の向上に向けて

野中氏によれば、同社のＥＣサイトには1日あたり1万件以上の悪意を持ったアクセスが行われているという。これまでもＷＥＢ広告を経由した攻撃を受け、社員から即座に報告を受けて被害が広がる前に対処した経緯が有り、社員の報連相意識の高まりに手応えを感じている。

一方で、サイバー攻撃の手口も巧妙化しており、「お客様と社員を守るためという初心を忘れずに、対策の更なる強化に取り組んでいきたい」と意気込みを語ってくれた。

ECサイト「大型出力屋」は1万件以上の取引先と 43 万件を超える製作実績を持つ

INTERVIEW
with 福井キヤノン事務機

TOPIC 02

企業に寄り添う伴走型サポートで サイバー攻撃被害を無くしたい

福井キヤノン事務機株式会社
代表取締役社長 玉木 啓介 氏（左）
デジタルイノベーション執行役員 宇佐美裕亮 氏（右）

各種情報機器の販売・保守やソフトウェア開発、ネットワーク・情報セキュリティなどを幅広く手掛ける福井キヤノン事務機㈱の玉木啓介社長と執行役員の宇佐美裕亮氏に、県内企業の情報セキュリティ対策の現状や同社のセキュリティ事業について話しを伺った。

サイバー攻撃の多様化に対応し 網羅的なセキュリティ対策へ

県内の中小企業では情報セキュリティに対して「ウチのような規模の会社に情報セキュリティ対策なんて必要ない」という考えを持つ企業が未だに多くを占めるのが実情だという。

ところが、大企業でのランサムウェア感染やサプライチェーン攻撃のニュースが連日報道され、「対策したいが、具体的にどうすればいいか分からない」という相談が確実に増加。こうした変化に合わせ、同社でもセキュリティへの向き合い方を大きく変え、単に機器の納品だけでなく、顧客の「分からない」を解消し、組織全体を守るための網羅的なセキュリティ対策を伴走して支援するスタイルへと、根本からの転換を進めている。

支援先企業に寄り添う 伴走型サポートを展開

情報セキュリティに取り組む前提として、単に「サイバー攻撃からIT資産（PCやサーバー）を守る」のではなく、「あらゆる脅威から企業の情報資産を守る」という、より網羅的な視点を持つことが重要であるとクライアント企業に呼び掛けている。広い視点で捉えると、UTM（統合脅威管理）などの導入はあくまで侵入を防ぐ「玄関の鍵」に過ぎず、守るべきは中にある情報資産と企業の存続となる。そこで、侵入後の内部対策やデータのバックアップ、情報を扱う「人」への教育に加え、万が一の事態に備えた「サイバーリスク保険」による金銭面（ファイナンス）の担保まで含めた、網羅的な備えが不可欠となる。

ただ、守るべき資産やリスクは企業ごとに異なるため、同社では顧客に寄り添って現状を紐解く「伴走型」のサポートを重視している。具体的には「セキュリティの専門会社によるセキュリティ診断」を用いて、技術面だけでなく社内ルールや従業員の意識までを含めた「組織の健康状態」を可視化し、その企業にとって過不足なく、最善なサポート策を提案・構築している。

啓発活動を通じた意識改革

同社では情報セキュリティの啓発活動にも積極的に取り組んでいる。2025年10月には、情報セキュリティ専門家の那須慎二氏㈱CISOを講師に招きセミナーを開催。「ITベンダーの言う通りにセキュリティ商材を買うな」という挑戦的なテーマを掲げ、経営者が主体的に判断できる知識を持つことの重要性を解説。会場では「ベンダー任せでなく、自分たちが組織として備えることが必要だと痛感した」などの声が聞かれたという。

「私たちの願いは、県内企業から理不尽なサイバー攻撃の被害企業が出ないこと」と語る宇佐美氏。一方で玉木氏は「複雑化・多様化するサイバー攻撃の脅威に屈せず、お客様の成長に不可欠なパートナーであり続けたい」と今後への思いを語ってくれた。

福井キヤノン事務機の本社 SL∞p（エスループ）で開催したセミナーでは多くの受講者が熱心に耳を傾けた

TOPIC 03

INTERVIEW with EXPERT

専門家に聞く

あなたの会社も狙われている

企業向けにITの導入・活用、社内教育などに取り組む傍ら、福井県情報化支援協会の理事として、企業からの相談や啓発活動に取り組んでいる佐藤宏隆氏に、情報セキュリティ対策のポイントについて話をうかがった。

有限会社詩季（flow Nexus）
代表取締役　**佐藤 宏隆** 氏

システムの脆弱性が狙われる

コロナ禍を契機にリモートワークが普及し、企業ではＶＰＮなどで入口を設けたものの、その後アップデートが行われず、システムの不備を狙われるケースが増えている。また、「エモテット」と呼ばれる機密情報の搾取を目的とした悪意を持ったプログラムがメールに添付され、ファイルや広告を偽装したリンクを通じて被害を広げるケースも多発した。最近では企業のシステムに侵入して、情報を搾取したりデータやシステムを暗号化させて人質に取り、解放と引き換えに身代金を要求する利益目的の「ランサムウエア」が登場している。

情報リスクは「気が付かないうちに被害が広がる」ため、システムが脆弱な中小企業を入口にサプライチェーンのネットワークに入り込み、大企業が狙われるケースも増えており、被害者である中小企業が加害者になるケースも有る。電子ツールが持つ「即時性」「顔が見えない」という特性も、被害の拡大につながっている。

企業が取るべき対応

事業の継続・発展には取引先や顧客との信頼関係、協力関係が不可欠であり、情報の漏洩は企業の存続に関わる重要な問題となる。一方で中小企業は経営資源や人材に限りが有り、コスト面でも取り得る対応には限界が有るため、自社の事業内容やセキュリティ対策の現状を精査し、優先順位を付けて取り組んでいく必要が有る。対応のポイントは3つ。

●自社も狙われているという意識の下で、社内の啓蒙・啓発を行う
●もしも狙われた場合に対応できるＢＣＰ（事業継続計画）の策定
●ＢＣＰに沿った定期的な訓練とマネジメント強化、対策意識の浸透

セキュリティ対策は会社の保険

セキュリティ対策は「コストがかさむ」と捉える経営者も少なくないが、病気やケガと同様に万が一に備える「保険」と考えてもらいたい。

経営にＩＴを活かすには使う側の意識やスキルを高く持つ必要がある。特殊詐欺でも言われるように「自分の会社は大丈夫」という思い込みが最も怖い。システムの更新やＢＣＰの策定、運用、そして外部の相談機関の活用などを通じて、自社のセキュリティ対策を強化してもらいたい。福井県情報化支援協会（ＦＩＳＡ）でもＩＴの活用やセキュリティの強化に向けたサポートを行っているので、ぜひ相談してもらいたい。

日頃の備えで顧客の信頼を獲得

情報セキュリティ対策は、サイバー攻撃の脅威が増大する現代において不可欠である。被害を受ければ事業停止や顧客情報の流出につながり、企業イメージや信用問題に直結する。従業員一人ひとりが危機管理意識を持ち、会社全体で定期的な教育や訓練を行い、注意点や対策を確認することが重要である。また、最新技術の導入に加えて、被害発生時の迅速な対応体制（ＢＣＰ）を整えることも必要だ。

企業は豊富な知識を持ったＩＴベンダーや専門家などへの相談や外部機関との連携により、対策の構築と継続的な改善を図ることで、顧客や社会からの信頼度を高め、持続的な成長が実現できる。他社への攻撃を「対岸の火事」とせず、自社にも起こり得るリスクと捉えて対応していただきたい。

当所では、専門家による相談制度を設けている。自社のセキュリティに不安が有る方や課題の解決をお考えの方は利用していただきたい。

ＩＴ無料専門家相談
（申込）創業・経営支援課
0776・33・8283