DXお悩み相談室

第7回 「情報セキュリティ」のお悩み

海外からの攻撃も急増 積極的に狙われる中小企業

Gさん（経営者）：最近、企業へのサイバー攻撃が増えているように感じます。これまでは、中小企業は攻撃の標的にはならないと思っていて、当社ではパソコンにセキュリティソフトを入れる程度の対策しかしていませんでしたが、今後もこれで大丈夫なのか、ちょっと不安になっています。

柴山：Gさんの不安は正しいです！　サイバー攻撃については、「中小企業は狙われない」という思い込みが一番危ないと私は考えています。例えば、企業のデータを暗号化して身代金を要求するランサムウェアの被害企業のうち、中小企業の割合はどれくらいだと思いますか？

Gさん：ほぼ大手企業ですよね？　中小企業は多くても2～3割でしょうか。

柴山：IPA（独立行政法人情報処理推進機構）の調査などによると、被害企業の約6割が中小企業ということです。

Gさん：えっ、そんなに!?

柴山：近年、中小企業は効率的な標的として積極的に狙われているんです。その大きな理由が、防御が手薄なこと。IPAでは全国の中小企業4191社にアンケート調査をしているのですが、その約7割で組織的なセキュリティ体制が整備されておらず、約6割が情報セキュリティに積極的な投資をしていない、という実態が浮き彫りになっています。

Gさん：もし標的になって攻撃されてしまったら、どんな被害があるのでしょうか。

柴山：主な被害は、データ破壊と個人情報の漏えいです。被害額の平均は73万円、復旧期間は6日程度ですが、復旧に莫大なコストと期間がかかった企業もあります（図1参照）。また、「サイバードミノ」の脅威もあります。被害の影響が直接攻撃を受けた企業だけにとどまらず、ドミノ倒しのように取引先にまで及んでしまうのです。過去3年間にサイバー攻撃の被害に遭った中小企業のうち、約7割が「取引先にも影響が及んだ」と回答しています。

Gさん：取引先にまで迷惑をかけてしまうのは怖いですね。なぜそんなことに？

柴山：API（Application Programming Interface）というソフトウェア同士がやり取りするための窓口のようなものがあるのですが、これが普及したことによって様々なシステム同士を簡単につなげられるようになったことが挙げられます。サプライチェーンが長く、大企業から中小企業まで多くの企業のシステムがつながっていることで、サイバードミノが起こりやすくなっているのです。そうすると、ハッカーなど攻撃者は、防御が薄くて楽に侵入できるところを入口としてまず狙いますよね。

Gさん：小さいところを狙っても割りに合わないだろうと思っていましたが、そういうことがあるんですね！

柴山：しかも近年は、生成AIの発達によって、海外のハッカーから日本企業への攻撃が急増しているんですよ。

Gさん：えっ!?　どういうことですか？

柴山：従来は、日本語という言語の壁によって、英語圏のハッカーからの攻撃は比較的少なかったのですが、生成AIで簡単に翻訳ができるようになったことで、その壁がなくなってしまった。しかも、ハッカーが自分のハッキングの手順をプログラミングして、24時間働ける分身のようなAIエージェントを大量につくり出すなど、攻撃が効率化・大規模化しているといわれています。そのため、ランサムウェアで侵入されてから実際に被害に遭うまでの潜伏期間が従来は2週間くらいはあったのが、2025年には中央値が4日までに短縮されてしまっているそうです。

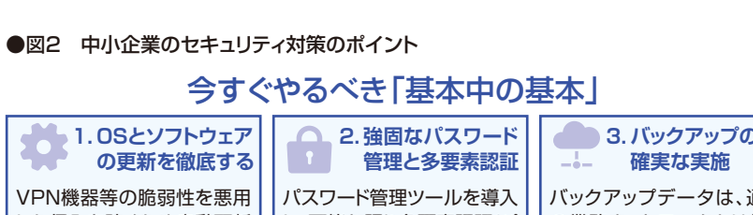
Gさん：気付いた時には手遅れ、ということですね。

柴山：そのとおりです。さらに最近では、クラウド環境への攻撃も増えています。クラウドストレージ上のファイルを直接削除するという新手法が登場し、従来は「クラウドは安全」と思われていましたが、その神話が崩壊しつつあります。

Gさん：今すぐ対策をしないと！　という気持ちになってきましたが、具体的に何をすればいいのでしょうか。

柴山：まずは、最小限の費用で最大の効果が得られる対策から始めましょう。今すぐやるべき「基本中の基本」の対策を図2にまとめましたので、参考にしてください。全部を完璧にできなくてもいいのです。「何もしない」と「最低限でも何かする」の間には、非常に大きな差があります。「セキュリティは経営課題」と捉えて、御社に合ったセキュリティ対策に取り組んでいってください。

●図1　サイバー攻撃によって生じた主な被害



被害の影響　平均被害額：73万円（最大1億円）　復旧期間：平均5.8日（最大360日）

出典：IPA「2024年度中小企業等実態調査（2023年度被害）」

●図2　中小企業のセキュリティ対策のポイント

今すぐやるべき「基本中の基本」

1. OSとソフトウェアの更新を徹底する
VPN機器等の脆弱性を悪用した侵入を防ぐため自動更新を有効にし、常に最新の状態を保つ。特に人材不足の拠点での放置に注意。

2. 強固なパスワード管理と多要素認証
パスワード管理ツールを導入し、可能な限り多要素認証（パスキー認証※を推奨）を設定する。「破られにくい」設定は必須。

3. バックアップの確実な実施
バックアップデータは、通常の業務ネットワークとは切り離したオフラインストレージやクラウドの別環境に保管する。

4. 従業員教育
フィッシング詐欺やソーシャルエンジニアリング対策として、不審なメールやリンク、添付ファイルへの基本的な警戒ルールを共有。

5. 最低限のセキュリティツール導入
ウイルス対策ソフトに加え、ファイアウォールも導入。安価な「サイバーセキュリティお助け隊サービス」等の活用も検討。

※パスワードを使わずにセキュリティと使いやすさを実現させた認証方式。例えば、指紋・顔認証やPINコードといったデバイスのロック解除機能（生体認証・端末固有のセキュリティ情報）を利用してログインする技術

回答者

柴山 治（しばやま・おさむ）
デジタル戦略プランナー／株式会社YOHACK CEO

米国ワシントン大学 経営学修士課程（Global Executive MBA）修了。ITベンチャー、コンサルティングファーム、外資系生命保険会社等を経て、現在は株式会社YOHACK代表。
企業の成長フェーズや課題に応じた、テーラーメイドの支援を提供している。著書に『日本型デジタル戦略』等がある。

※DXに関するお悩みは、どんなことでもお気軽にご相談ください。