福祉事業者様へのお役立ち情報

OMジャーナル

2026年　第4号

For the next solutions
ONWARD MANAGEMENT

平素より格別のご厚情を賜り、心より御礼申し上げます。
昨年から大手企業を狙ったランサムウェア被害が相次いでいます。今回は、法人を取り巻くサイバー攻撃の実態と対策をご紹介します。

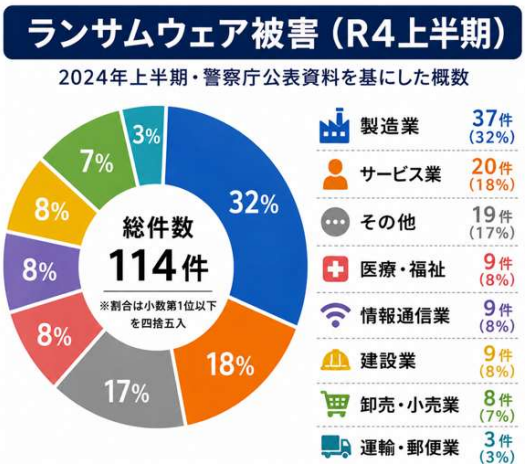
サイバー攻撃の実態と対策

近年、サイバー攻撃は急速に高度化し、その被害は大企業だけでなく、中小企業や福祉施設、医療機関など幅広い組織に広がっています。2025 年には、保険会社や流通業をはじめとする企業で、ランサムウェアによるシステム停止や大規模な情報漏えいが相次ぎました。システムが利用できなくなることで、受発注や顧客対応、社内業務が停止し、復旧費用だけでなく、売上の減少や取引先への補償、社会的信用の低下など、経営全体に大きな影響が及んでいます。

さらには、ニチレイグループがサイバー攻撃を受け、一部のシステム障害により受発注や出荷業務に影響が生じました。このように、一社の被害がグループ会社や取引先、物流、利用者にまで波及する「サプライチェーンリスク」が現実のものとなっています。福祉施設においても、介護記録や請求、勤怠、給与などを外部のクラウドサービスや委託業者に依存しているケースが多く、取引先やシステム会社が攻撃を受けることで、自法人の業務が停止する可能性があります。

攻撃手法も巧妙化しています。AI を悪用して自然な文章を作成した標的型メールや、経営者・取引先になりすました偽の音声や画像、パスワードを盗み取るフィッシング、セキュリティ対策の弱い取引先を経由した侵入などが増えています。IPA でも、ランサムウェアやサプライチェーン攻撃、AI の利用をめぐるサイバーリスクを重大な脅威として位置付けています。

こうした背景を受け、経済産業省は、サプライチェーン全体のセキュリティ対策を共通の基準で評価する**「サプライチェーン・サイバーセキュリティ評価制度（SCS）」**の整備を進めています。
今後は、大企業や自治体などから、取引先や委託先に対して一定水準の対策を求める動きがさらに広がると考えられます。サイバー攻撃は「自社は狙われない」と考えるのではなく、「いつ被害に遭ってもおかしくない」という前提で備えることが重要です。OS やソフトウェアの更新、多要素認証（MFA）の導入、定期的なバックアップ、標的型メール訓練、委託先の管理に加え、万一の際に誰が何を行うのかを定めた初動対応手順や BCP を整備しておくことが、被害を最小限に抑え、事業を継続するための鍵となります。



現在、9 月に「サイバー攻撃の実態と対策」をテーマとした集合研修を企画しております。詳細が決まりましたら、FAX やメールにてご案内いたしますので、ぜひご参加をご検討ください。

令和 8 年熊本地震により被災された皆さまに、謹んでお見舞い申し上げます。また、現地での状況確認や被災地支援にご尽力されているすべての皆さまに、心より敬意を表します。現在ご加入中の地震保険・火災保険などの補償内容に関するご質問・ご相談などがございましたら、どうぞお気軽にお問い合わせください。

HP・インスタ・Xでも情報発信中！フォローもお願いします