HIROTA
電子機器 設計・製造・販売
# HIROTA News Letter
Vol.59
2026年1月13日発行

新年あけましておめでとうございます。本年も変わらぬご支援を賜りますよう、よろしくお願い申し上げます。今回は、近年社会的にも重要性が高まっている「サイバーセキュリティ」についてお伝えいたします。

## サイバー攻撃の現状

企業を取り巻くサイバー脅威は、近年、質・量の両面で高度化・多様化しています。昨年後半には、大手飲料メーカーがランサムウェア攻撃を受け、生産管理システムが停止し、製造ラインの操業中断を余儀なくされました。こうしたサイバー攻撃による被害は単一企業にとどまらず、サプライチェーン全体へ波及し、関連企業のみならず社会基盤にも深刻な影響を及ぼしたことは記憶に新しいところです。

## サイバー攻撃が急増している背景

### １．デジタル化の進展

各企業のDX推進に伴い、業務システム・生産設備・IoTデバイスが広範にネットワーク接続されるようになりました。これにより、従来は閉域ネットワークで保護されていた領域が外部と接続され、結果として攻撃対象領域が拡大しています。

### ２．攻撃手法の高度化・サービス化

標的型攻撃（APT）、ビジネスメール詐欺（BEC）、サプライチェーン攻撃など、攻撃手法は高度化・巧妙化しています。加えて、ランサムウェアが犯罪者向けに“サービス”としてネット上で提供されており、専門的知識を持たない者でも攻撃を容易に実行できる環境が形成されています。

### ３．組織の脆弱性を突く手法の増加

精巧なフィッシングメールやスピアフィッシングにより、従業員の認証情報が窃取され、それを足掛かりとして企業システムへ侵入する事案が増加しています。これらは、相応の注意力を払わなければ判別が困難なレベルに達しています。

## 長野県内における被害例

県内製造業者がランサムウェアに感染し、設計データが暗号化されて生産が停止した事例、取引先を装ったBECにより不正送金が発生した事案、さらにはVPN機器の脆弱性を突かれ社内ネットワークが侵害されたケースなどが報告されています。中小企業は情報システム部門のリソースが限定的であることから、攻撃者にとって“侵入しやすい標的”と認識されやすい状況にあります。

## サイバーセキュリティ対策

### １．企業レベルでの対策

（１）OS・アプリケーションの最新化：脆弱性を突く攻撃が多いため、更新プログラムの適用は最も基本的な対策です。脆弱性を放置しない継続的な管理体制が求められます。
（２）高度防御ソリューションの活用：端末レベルでの侵害検知・封じ込めを可能とするEDRや、より広範な脅威可視化を実現するXDRを活用し、攻撃の早期発見につなげます。
（３）アクセス権限の適正化：“信頼を前提としない”アクセス制御を基本とし、最小権限による運用を徹底します。必要な人だけが必要なデータにアクセスできるよう権限設定を適正化します。
（４）レスポンス体制の整備：サイバー攻撃事案発生時の初動対応手順を明確化し、訓練（演習）を通じて組織としての対応能力を強化します。
（５）バックアップ戦略の強化：オフラインバックアップやクラウドバックアップを併用し、ランサムウェア感染時であっても迅速なデータ復旧を可能とする体制を整備します。
（６）専門業者との連携：セキュリティサービスを提供する専門業者の支援を受け、自社のセキュリティレベルの診断、改善策の構築、定期的な訓練を実施し、継続的なセキュリティ強化を図ります。

### ２．個人レベルでの対策

（１）不審メールの開封および不審リンクへのアクセスを禁止します。
（２）パスワードを強固化し、多要素認証（MFA）を積極的に活用します。
（３）公衆Wi-Fi等、自社ネットワーク以外の利用を制限します。
（４）異常兆候を感知した際は、即時に担当部門への報告を徹底します。


出典：ChatGPT

サイバー攻撃は、企業規模や地域性を問わず発生し得る重大な経営リスクであり、事業継続性を根底から揺るがす要因となります。当社としても、情報セキュリティ対策の継続的な強化を推進するとともに、取引先の皆様との連携を一層深め、安全かつ強靭なサプライチェーンの維持に努めてまいります。

発行 ：株式会社 広田製作所　(執筆:黒岩 信吉 / 文責:広田 文雄)　☎ 026-245-1212
〒382-0901 長野県須坂市大字小河原 3954-13　https://www.hirotass.co.jp