特集　2022年を振り返る

第３章
情報セキュリティリスクへの警鐘

佐々木　剣太
神奈川県中小企業診断協会

2022年２月，大手自動車メーカーのサプライチェーンに連なる，ある部品メーカーがランサムウェアによるサイバー攻撃を受けた。

このサイバー攻撃により，この部品メーカーの保有する受発注システムが停止。その結果，部品供給がとまり，自動車メーカーのすべての工場で，生産が１日停止する事態に陥った。この攻撃により最終的に，全国14ヵ所の工場，28ラインの製造が停止し，約１万3,000台の生産に影響が出た。

調査の結果，部品メーカーの子会社が保有するリモート接続機器の脆弱性を利用した攻撃であったことが判明した。大手自動車メーカーのサプライチェーンは全体で数万社規模といわれている。そのうち１社の情報セキュリティ対策が不十分であることが原因で，チェーン全体に損害を与えたのである。

これらのことからわかるように，企業の規模に関係なく，チェーンにかかわる全企業で，継続的な情報セキュリティ強化が求められる。

本章では，サイバー攻撃の特徴や情報セキュリティに対する中小企業の取組み，そして，中小企業診断士の役割について紹介する。

１．情報セキュリティとは

情報セキュリティとは，社内に保有する流出の許されない情報資産を安全に企業活動に使用するため，「情報セキュリティのCIA」と呼ばれる３つの機能を維持することである。

⑴　機密性（Confidentiality）

アクセス権の設定やパスワード管理，データの暗号化などにより，情報へのアクセスを制限し，意図しない情報開示や流出を防ぐことである。

⑵　完全性（Integrity）

デジタル署名の利用やアクセス・改変の履歴の管理などの仕組みにより，サイバー攻撃による機密情報の破壊，改ざんまたは消去を防ぐことである。

⑶　可用性（Availability）

システム障害発生時においても，継続利用できる仕組みなどにより，いつでも情報を利用できることである。

２．ランサムウェアの現状

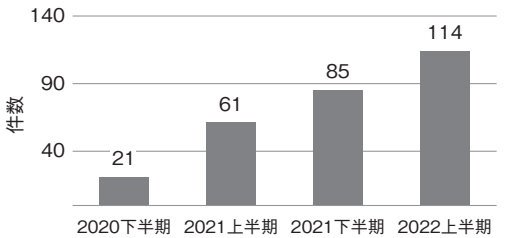
⑴　ランサムウェアとは

「ランサム（＝身代金）＋ウェア（＝ソフトウェア）」から名づけられ，ウイルス感染によりデータを暗号化し，データを人質に取って身代金を要求するサイバー攻撃である。

近年では，データを公表するとして金銭を要求する「二重脅迫型ランサムウェア」へと手口を変化させている。これにより，暗号化によって可用性を低下させる従来の手口に加えて，機密性を脅かすことで被害が甚大化しているといえる。

国内におけるランサムウェア被害の報告件数からも，増加の一途をたどっていることがわかる（**図表１**）。

図表１　ランサムウェア被害の報告件数の推移

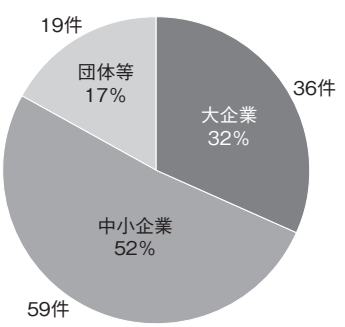


出所：警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2022）をもとに筆者作成

⑵　狙われる中小企業

警察へのランサムウェアの被害報告件数の半数以上を中小企業が占めており，被害は中小企業にも及んでいる（**図表２**）。

図表２　ランサムウェア被害の企業・団体等の規模別報告件数



出所：警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2022）をもとに筆者作成

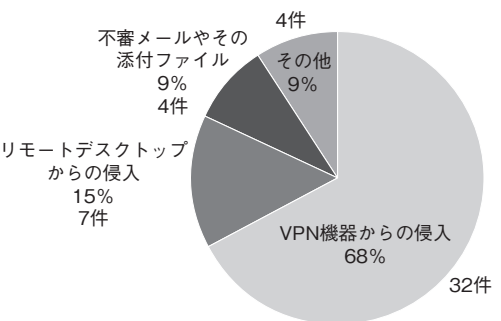
これまでは，「標的型攻撃」という，標的企業に対して，直接的に攻撃を仕掛ける手口が用いられていた。近年では，企業単独ではなく，サプライチェーン全体を狙った「サプライチェーン攻撃」が増えている。その結果，大企業に比べ，情報セキュリティ対策の甘い中小企業へと標的が変わりつつある。

部品メーカーに対するサイバー攻撃も，子会社を経由してシステムに侵入し，結果として，サプライチェーン全体に被害を与えた。まさに，サプライチェーン攻撃の代表的事例といえる。

⑶　サイバー攻撃の経路と対策

次に，ランサムウェアの感染経路について説明する。ランサムウェア被害のうち，８割以上が，リモートデスクトップや仮想的に専用回線を構築するVPN機器の設定の不備や，脆弱性を悪用した攻撃である（**図表３**）。

図表３　感染経路の割合



出所：警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2022）をもとに筆者作成

VPNは，可用性を損なわずに，機密性を高める手段であり，情報セキュリティ強化のために用いられる。しかしながら，脆弱性が見つかったにもかかわらず，セキュリティパッチ（OSやソフトウェアの脆弱性などを解消する更新プログラム）の適用が不十分であると，攻撃のきっかけを与えてしまうことになる。つまり，情報機器の管理を確実に実施できる体制の構築が重要であることがわかる。

３．中小企業の動向

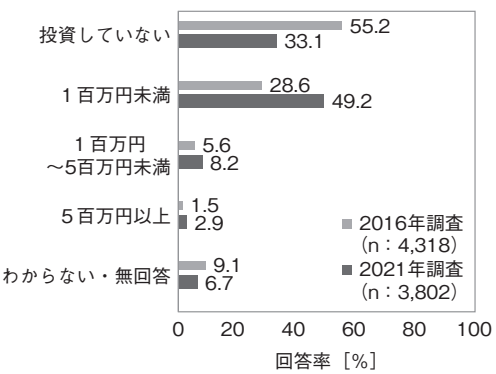
次に，中小企業の情報セキュリティに対する取組みについて紹介する。独立行政法人情報処理推進機構（IPA）が取りまとめた「2021年度中小企業における情報セキュリティ対策に関する実態調査―調査報告書―」より，次の３つの観点から解説する。

⑴ 投資に対する動向

調査年以前の３年間での情報セキュリティに対する投資額を集計した結果より，2016年調査時に比べて，「投資していない」と答える企業は22.1ポイント低減し，情報セキュリティ投資を行う企業は，全体で24.6ポイント増加した（**図表４**）。

2016年に比べて情報セキュリティへの関心は高まっているといえる。

図表４　情報セキュリティ投資額



出所：独立行政法人情報処理推進機構「2021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―調査報告書―」（2022）をもとに筆者作成

⑵ 情報機器管理体制

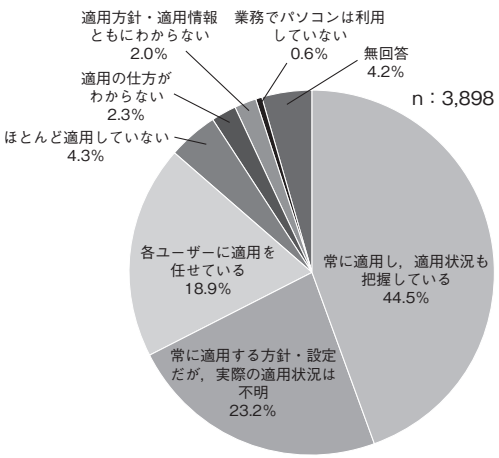
感染経路の調査結果からも，サイバー攻撃を防ぐためには，セキュリティパッチの適用により脆弱性を塞ぐことが重要である。しかしながら，中小企業における Windows Update などのセキュリティパッチの適用状況の調査では，半数以上の企業で適用状況が把握できていない結果となっている（**図表５**）。

⑶ 社員教育に対する動向

情報セキュリティレベルを高く保つためには，従業員が重要性を認識してルールを守ることが必要となるため，教育も重要である。

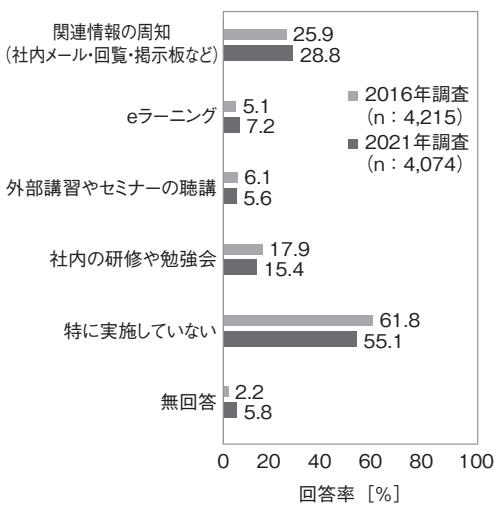
中小企業の従業員への教育は，2016年調査時に比べ，「特に実施していない」と回答する企業は低減しているものの，まだ55%が実施していないという結果となった（**図表６**）。

図表５　パソコンへのセキュリティパッチの適用状況



出所：独立行政法人情報処理推進機構「2021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―調査報告書―」（2022）をもとに筆者作成

図表６　情報セキュリティ教育の実施状況



出所：独立行政法人情報処理推進機構「2021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―調査報告書」（2022）をもとに筆者作成

４．中小企業の対策事例

上記の調査結果からは，情報機器管理や教育面で課題のある結果となった。また，サプライチェーン攻撃の拡大により，チェーン全体の情報セキュリティ強化が求められている。

これらの状況に対して，中小企業にて実践可能な取組み事例をIPAが取りまとめた「2021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―事例集―」より，２つ紹介する。

⑴　従業員教育による対策

山梨県で保険代理店を営むA社は，外部ベンダに委託してシステム構築・メンテナンスを行っている。また，リモートワークやオンライン面談に対応した社内規定の整備や端末・設備の準備を行うことで時流の変化にも対応してきた。

現状でも，情報セキュリティレベルに問題はないが，従業員の不注意による情報流出の懸念は払拭できないことから，従業員教育に力を入れている。具体的には，モバイル端末の取り扱いなどをテーマとして取り上げ，経営者と従業員が参加して毎週定例で勉強会を行っている。ほかにも，動画配信サイトのコンテンツの活用や，外部の研修やセミナーへの参加，標的型攻撃への訓練の実施によりリテラシー向上に励んでいる。

A社は，情報セキュリティ対策への取組みにより顧客からの信頼が得られることで，今日まで取引が継続できていると認識している。

⑵　委託先を巻き込んだ対策

神奈川県で印刷業を営むB社は，印刷物の製作のために公開前の情報を預かる機会が多いことから，情報セキュリティ強化の重要性を認識していた。そのため，情報セキュリティマネジメントシステム（ISMS）認証を取得し，総合的な情報管理を行っている。また，従業員の情報セキュリティに対する意識を常に高く保つため，情報セキュリティに関するメッセージを継続して発信している。

近年では，業務委託を行う協力会社へ，情報セキュリティ対策の要請や，その重要性の周知を行っている。また，業務委託先の選定の際には，付き合いの長さや品質に加え，実際に協力会社に出向いて情報セキュリティレベルを確認している。具体的には，ISMS認証の取得状況や，情報資産の管理方法，部外者の立ち入りの有無などを確認し，守秘義務を守れる環境であるかの確認を行っている。

取引先からの情報セキュリティ上の要請は年々増加傾向にある。情報セキュリティ対策を徹底することのメリットは，取引先からの信頼が得られることにあると感じている。

５．中小企業診断士に求められる役割

ランサムウェアの被害拡大の背景には，コロナ禍でのテレワークの急拡大も一因と考えられている。急な生活様式の変化により生じた機器管理面の不備が狙われたのである。

今後も社会の潮流の変化に合わせて，サイバー攻撃は巧妙に手口を変えてくるだろう。特に，近年ではデジタルトランスフォーメーション（DX）の実現に向け，さまざまな企業が業務プロセスのデジタル化に取り組んでいる。その半面，業務プロセスの急な変化によりほころびが生じる可能性がある。

このような社会の変化に対して，中小企業診断士に求められる役割は，中小企業経営者に対して情報セキュリティリスクの警鐘を鳴らすことである。情報機器管理体制や教育の仕組みの構築など，情報セキュリティの強化は経営者がリーダーシップを発揮して推進する必要がある。そのため，経営者が情報セキュリティの重要性を認識することが活動の第一歩となる。

佐々木　剣太
（ささき　けんた）
奈良先端科学技術大学院大学卒業後，精密機器製造業にて，CAEやAIによる設計・開発のDX化の推進を担当。2022年中小企業診断士登録。