調査レポート

- 後編 -

埼玉県内企業の情報セキュリティの現状に関する調査

ぶぎん地域経済研究所 専務取締役／チーフエコノミスト **大西 浩一郎**

■ 調 査 対 象 ：県内企業535社　　■ 調査方法(期間)：アンケート方式（1月18日~2月26日）
■ 回 答 企 業 ：153社（回答率26.7%）
■ 規 模 別 内 訳 ：規模の大きい企業（100人以上）74社、規模の小さい企業（100人未満）69社
（参考）業種別内訳 ：製造業71社、非製造業72社

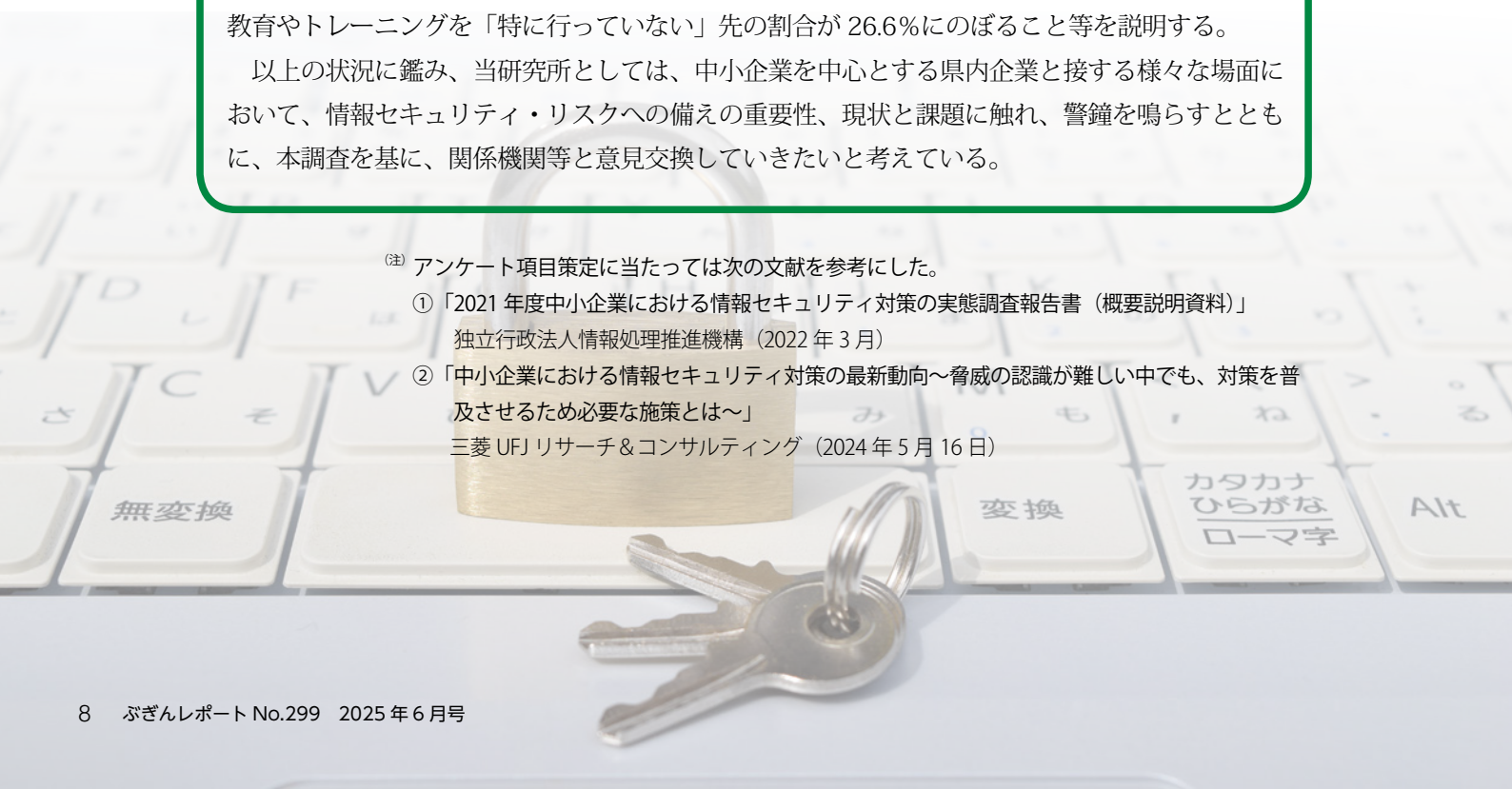
県内企業においては、情報セキュリティに関するリスク認識、リスク管理体制の整備と実効性の確保のいずれにおいても課題があり、企業各社の自助努力と各方面からの手厚い支援が求められている。

ぶぎんレポート５月号に掲載した前編のエッセンスは、①ITの普及に伴い、県内企業にとって情報セキュリティ・リスクはすぐそばにある脅威となっていること、②もっとも、被害にあうと感じていない企業は２割を超えており、リスク管理の取組みも受け身または「後回しにしがち」とする企業が大勢を占めること、の２点であった。

後編では、**「リスク管理の実態」**において、規模の小さい企業での社内体制、リスク管理ツールの導入状況および運用に関して、21.4%が「不明・キーパーソンもいない」と回答するなど遅れが目立つことを説明する。**「従業員教育と今後の課題認識」**では、従業員に対するセキュリティ教育やトレーニングを「特に行っていない」先の割合が26.6%にのぼること等を説明する。

以上の状況に鑑み、当研究所としては、中小企業を中心とする県内企業と接する様々な場面において、情報セキュリティ・リスクへの備えの重要性、現状と課題に触れ、警鐘を鳴らすとともに、本調査を基に、関係機関等と意見交換していきたいと考えている。

㈱ アンケート項目策定に当たっては次の文献を参考にした。
①「2021年度中小企業における情報セキュリティ対策の実態調査報告書（概要説明資料）」
独立行政法人情報処理推進機構（2022年３月）
②「中小企業における情報セキュリティ対策の最新動向～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～」
三菱UFJリサーチ＆コンサルティング（2024年５月16日）



リスク管理の実態

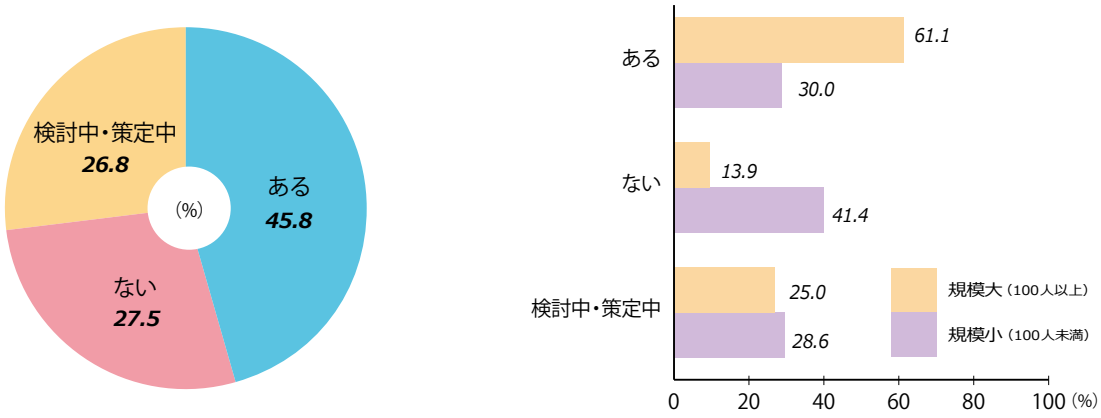
前章までにみた情報セキュリティを巡るリスク認識やリスク管理スタンスの下で、実際のリスク管理はどうなっているのか。以下、社内体制面、リスク管理ツールの導入状況および運用をみることとする。

⑴セキュリティ・ポリシーと組織体制（問 11、12）

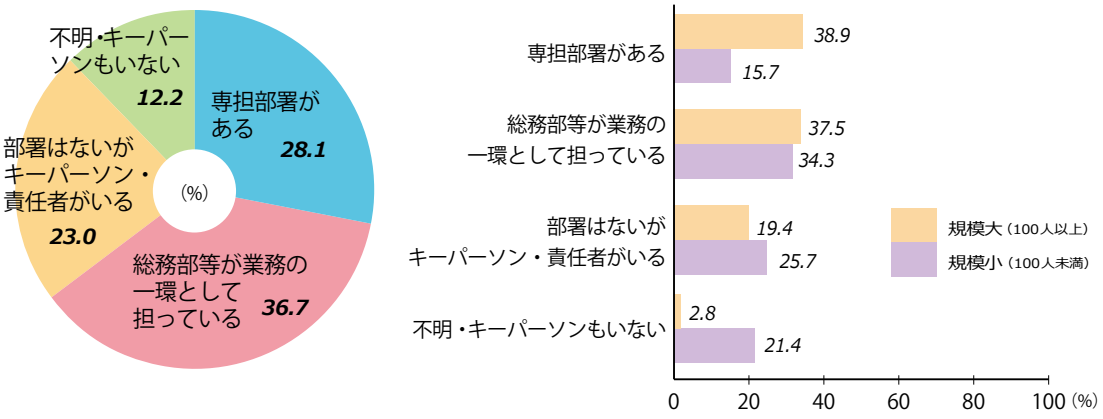
セキュリティ・ポリシーとは、組織としての情報セキュリティへの対応指針と各種手順で構成される文書である。リスクへの備えや何らかの事態が発生した場合の対応が従業員によってまちまちであってはならず、セキュリティ・ポリシーはそのような目線を合わせる上でも重要である。今回、セキュリティ・ポリシーの策定状況を尋ねたところ、「ある」は 45.8％にとどまり、「ない」（27.5％）と「検討中・策定中」（26.8％）が上回った。本設問結果は企業規模の違いが鮮明であり、規模が小さくなるほど策定状況は不調となる。規程の必要性は企業規模に比例する面は否定しないが、足並みを揃えた対応のため、規模の大小にかかわらず策定に向けて歩を進めることが期待される。

次に情報セキュリティのための組織体制について窺うと、「総務部等が業務の一環として担っている」先が 36.7％で最大勢力であり、「専担部署がある」（28.1％）、「部署はないがキーパーソン・責任者がいる」（23.0％）と続いている。企業規模別にみると、規模の大きい企業では「専担部署がある」、「総務部等が業務の一環として担っている」がそれぞれ 4 割弱と相応の体制を有している。規模の小さい企業に関しては、万全の体制を敷くのは難しいとは思われるものの、21.4％もの企業が「不明・キーパーソンもいない」と回答している点は課題として意識せざるを得ない。対応が急がれるテーマであると思われる。

問 11　セキュリティ・ポリシーの有無



問 12　情報セキュリティの組織体制



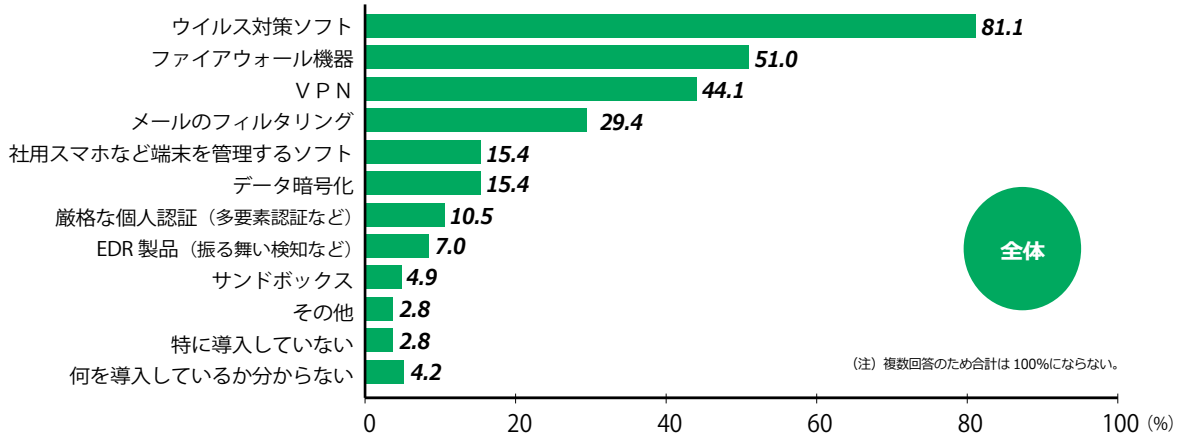
⑵リスク管理ツールの導入状況（問 13）

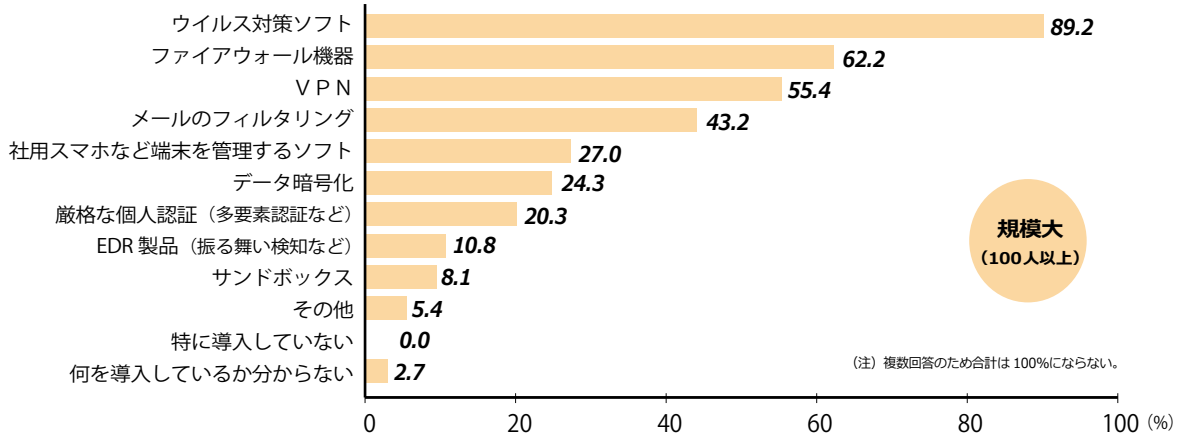
続いて、情報セキュリティのためのリスク管理ツールの導入状況をみる。リスク管理ツールは、アクセスを限定するためのツール（VPN (注1)、厳格な個人認証など）、攻撃を跳ね返すためのツール（ファイアウォール機器 (注2)、サンドボックス (注3)）、ウイルスを検知するためのツール（ウイルス対策ソフト、EDR(注4)製品）など多岐にわたるが、これらを万遍なく整備することが望ましい。県内企業の導入状況をみると、「ウイルス対策ソフト」は 81.1％と最も高い導入率となっており、次いで「ファイアウォール機器」（51.0％）、「VPN」（44.1％）がポピュラーである。さらに、「メールのフィルタリング」（29.4％）、「データ暗号化」（15.4％）、「社用スマホなど端末を管理するソフト」（15.4％）も一定の割合を占めている。一方、振る舞い検知などで攻撃をいち早く感知するための「EDR 製品」の導入は 7.0％にとどまった。万一感染した際の被害を最小限にとどめる観点から、導入拡大が期待される。

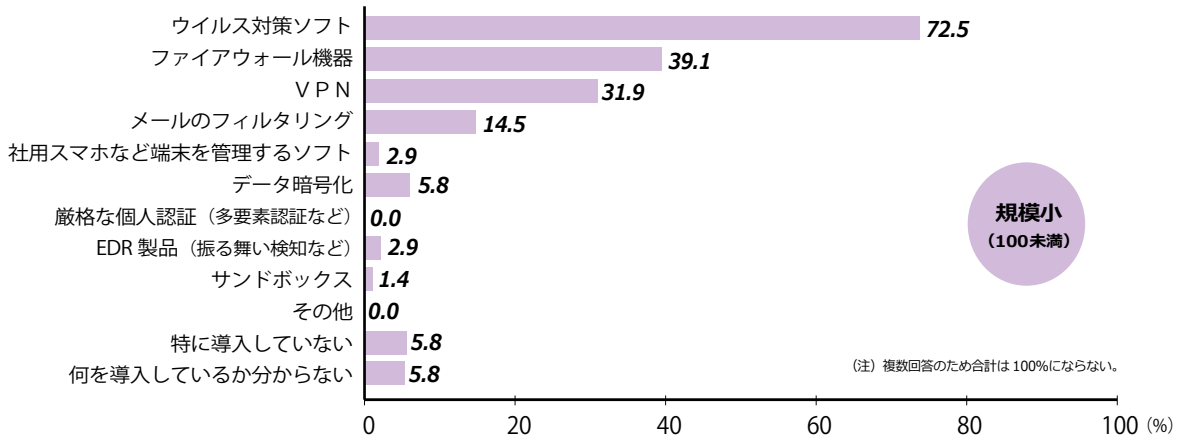
これを企業規模別にみると、規模の大きな企業では

(注 1) **ＶＰＮ**	バーチャル・プライベート・ネットワーク。社内ネットワークと社外 PC の間に仮想の専用回線を通すサービス（例えばリモートワークで会社のサーバに接続）。
(注 2) **ファイアウォール機器**	外部インターネットと内部システムの間に設置される機器で、通信の許可・拒否を判断する。
(注 3) **サンドボックス**	砂場。怪しいメールなどを隔離して、ウイルス感染していないかを検証・分析。
(注 4) **ＥＤＲ製品**	エンドポイント・ディテクション・アンド・レスポンス。PC などの端末（エンドポイント）を監視し、ウイルス感染した際の不審な動きを検知する製品。

問 13　導入している情報セキュリティ対策・製品・サービス (複数回答)







リスク管理ツールの導入状況が相対的に充実しており、多要素認証など厳格な個人認証の導入も 20.3％となっている。もっとも、「EDR 製品（振る舞い検知など）」（10.8％）の導入は 1 割にとどまっている。

一方、規模の小さな企業においては、「ウイルス対策ソフト」（72.5％）、「ファイアウォール機器」（39.1％）、「VPN」（31.9％）の 3 点に限られているのが実情である。規模が小さくてもサイバー攻撃は免れないことを念頭に、情報セキュリティ・リスクの管理の実装を強化することが重要な課題である。

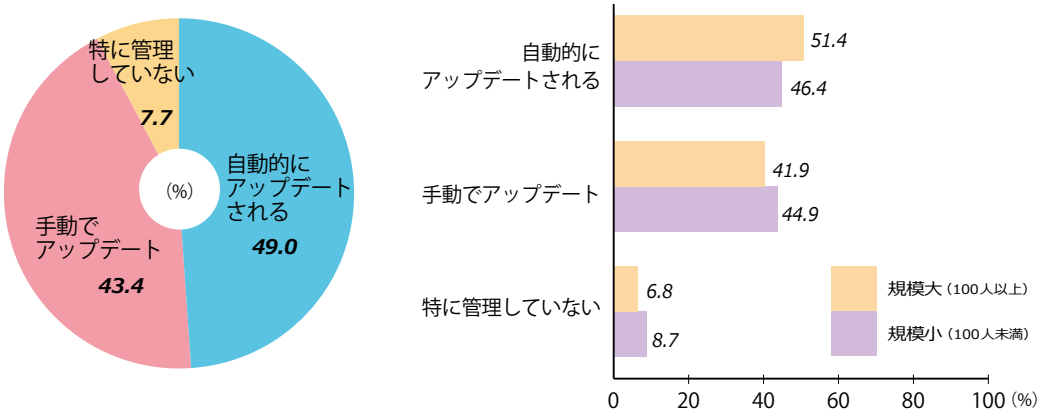
⑶アップデートの仕組み（問 14 ～ 16）

OS（オペレーティングシステム／基本ソフト）にせよ、上記のリスク管理ツールにせよ、サイバー攻撃等に対する脆弱性はゼロにはならない。情報セキュリティへの備えの十分性を保つためには、導入したソフトを適時適切にアップデートする必要がある。アップデートは、手動よりは自動、また、専門家が限られているなら自前で管理するよりは専門業者に託す方がより確実である。

この点、まず、OS の最新化について窺うと、「自動的にアップデートされる」が 49.0％と半数にとどまっており、「手動でアップデート」している先が 43.4％を占める。なお、本設問への回答に関しては、規模の大小に大きな違いはみられなかった。

次に、サポート期限切れの OS の使用状況（本設問の集計対象は 55 社）についてみると、「期限切れ前に全て最新化」している企業は 58.2％であり、「一部期限切れを使用」している先が 32.7％、「よくわからない」が 9.1％となった。サポート期限切れ OS を使用している機器を外部インターネットに接続することは禁じられていると思われるが、そうした運用は、個々

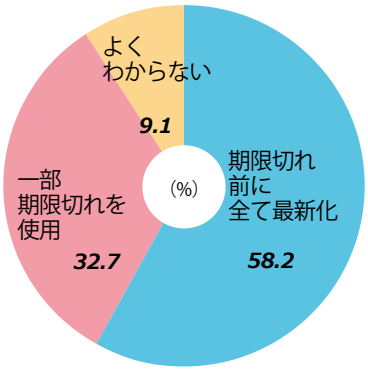
問 14　OS（オペレーティングシステム）などソフトウエアの最新化



人の行動にかかっているという点で常にリスクを伴う。サポート期限切れ OS のリスクを今一度認識することが重要である。

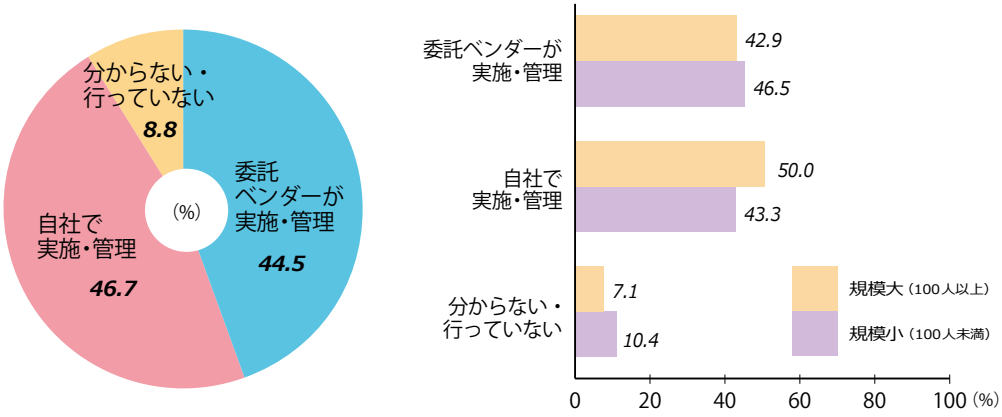
最後に、情報セキュリティ対策に係るソフトの最新化、脆弱性を補完するための修正プログラムの適用状況についてみると、「自社で実施・管理」（46.7％）と「委託ベンダーが実施･管理」（44.5％）がほぼ拮抗した。なお、企業規模別にみると、規模の大きな企業では自社管理の方が多く、規模の小さい企業では委託ベンダーによる管理に委ねている先の方が多い。専担部署の有無など組織体制を背景としたものであると思われる。

問 15　サポート期限切れの OS の使用



（注）本設問の集計対象は 55 社。

問 16　情報セキュリティ対策ソフトの最新化や修正プログラムの適用



小括

以上、情報セキュリティに関するリスク管理の実態について、社内体制面、リスク管理ツールの導入状況および運用からみてきた。いずれについても、規模の大きい企業は相応に進んでいる一方、規模の小さい企業では遅れが目立つ結果となった。特に、情報セキュリティのための組織体制について、規模の小さい企業のうち 21.4％もの先が「不明･キーパーソンもいない」と回答した点は無視できないほか、相対的にリスク管理ツールの導入の拡がりがみられない点も課題であると見受けられた。なお、振る舞い検知などで攻撃をいち早く感知するための「EDR 製品」に関しては、規模の大きな企業を含めて導入拡大が期待される。

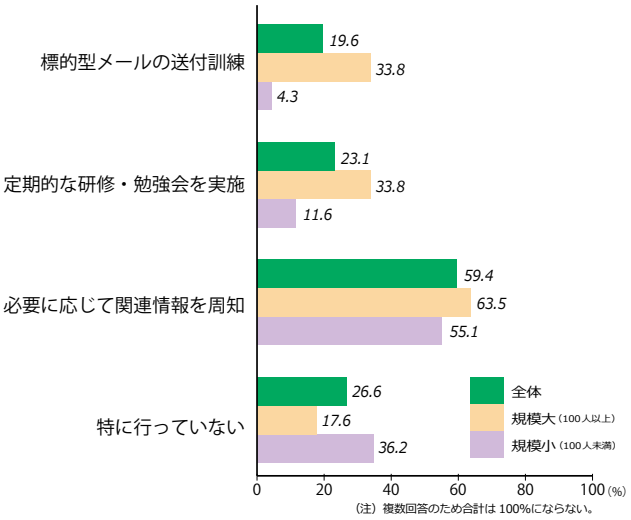
従業員教育と今後の課題認識

どんなに高度なツールを導入しても、それを使用する従業員全員が情報セキュリティに関する危機感を共有し、厳格な運用を履行しなければリスク管理は形骸化する。こうした事態を防ぐためには継続的な従業員教育が必要である。以下では、まずこの点を確認した後、最後に県内企業が課題として認識する事項をみることとする。

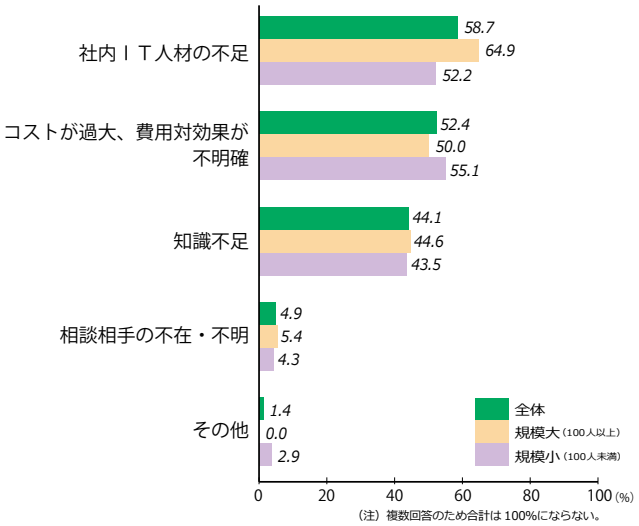
(1)従業員教育（問 17）

従業員に対するセキュリティ教育やトレーニングの状況について窺うと、「標的型メールの送付訓練」は

問 17　従業員に対するセキュリティ教育やトレーニング (複数回答)



問 18　情報セキュリティ対策で課題と感じていること（複数回答)



19.6％、「定期的な研修・勉強会を実施」は 23.1％にとどまり、「特に行っていない」が 26.6％にのぼるなど、大きな課題を残していることがわかった。「特に行っていない」と回答した企業は、設問構成からみて、関連情報の周知も行っていないとみられる。規模別にみた場合、規模の大きい企業では、「標的型メールの送付訓練」などのトレーニング、「定期的な研修・勉強会を実施」はいずれも 33.8％となったが、「特に行っていない」も 17.6％あるなど、二極化が生じている。また、規模の小さい企業では「特に行っていない」が 36.2％に達する。従業員教育の強化は優先度の高い課題であると言える。

⑵企業からみた情報セキュリティの課題（問 18）

最後に情報セキュリティ対策で課題と感じていることについて尋ねると、「社内 IT 人材の不足」が 58.7％と最大で、これは規模の大きい企業での回答がより多い。次いで、「コストが過大、費用対効果が不明確」が 52.4％となっており、こちらは規模の小さい企業での回答がより多くなっている。また、「知識不足」が 44.1％を占めたが、「相談相手の不在・不明」は 4.9％にとどまった。

小括

従業員に対するセキュリティ教育やトレーニングは、情報セキュリティに関するリスク管理の実効性の裏付けとなるが、県内企業では、「特に行っていない」先の割合が 26.6％にのぼっており、大きな課題を抱えている。また、各社が課題とする事項としては、「社内 IT 人材の不足」、「コストが過大、費用対効果が不明確」が過半となっている。

まとめ

県内企業にとって情報セキュリティ・リスクはすぐそばにある脅威であるが、県内企業は、情報セキュリティに関するリスク認識、リスク管理体制の整備と実効性の確保のいずれにおいても少なからぬ課題を抱えている。企業各社の自助努力と各方面からの手厚い支援が求められている。こうした状況に鑑み、当研究所としては、中小企業を中心とする県内企業と接する様々な場面において、情報セキュリティ・リスクへの備えの重要性、現状と課題に触れ、警鐘を鳴らすとともに、本調査を基に、関係機関等と意見交換していきたいと考えている。