埼玉県内企業の情報セキュリティの現状に関する調査

■ 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：143 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

（はじめに）

企業の情報セキュリティ・リスクとは、保有する情報資産に対する潜在的な脅威・危険性である。情報資産の機密性（アクセス制限）、完全性（改ざん・破壊の阻止）、可用性（必要な時に利用可能）が損なわれることでリスクは顕在化し、インターネットやデジタル機器を通じた情報や金銭の窃取、システムの破壊・機能妨害への対応のため、企業等は金銭面、業務面で多大な負担を強いられる。

一般に、各種攻撃の標的になるのは、公的機関や大企業が中心であると捉えられがちであるが、実際のところ、リスクの度合いと組織規模の大小との関係は薄い。例えば、令和 6 年（2024 年）におけるランサムウエア（保有データを暗号化して身代金を要求）の被害件数 222 件のうち 140 件（63%）は中小企業が被っている（警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」）。

こうした中、ぶぎん地域経済研究所では、中小企業を中心とする県内企業における情報セキュリティ・リスクに対する認識やリスク管理の実態を把握し、今後の課題を考察するため、定例の企業経営動向調査（2025 年 1－3 月）に付帯してアンケート(注)を実施することとした。

(注)　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）。

（調査結果の総括）

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。本稿の章立てに沿って調査結果を要約すると、以下の通りである。

1．情報セキュリティ・リスクは遠い存在なのか

■ IT 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。実際、過去 3 年間の情報セキュリティ被害については、「被害にあっていない」との回答は 6 割台であることから、4 割弱の企業は被害にあったか、「被害にあったかわからない」。また、情報セキュリティ被害を受けた場合の影響としては、端末の修復・入れ替えや業務停止などが挙げられている。「秘密保持」を中心とする取引先からの要請にも合致したリスク認識とリスク管理が求められている。

2．リスク認識とリスク管理の取組み姿勢

■ もっとも、14.1%の先では情報セキュリティ被害について重くは受け止めておらず、また、被害にあうと感じていない企業も 2 割を超えている（22.7%）。この背景には、「情報セキュリティ対策を十分やっている」とか「規模が小さく標的にされない」といった見方がある。こうした認識の下、リスク管理の取組みについては受け身の姿勢にある企業が大勢であり、さらに 12.9%の企業が「後回しにしがち」としている。「費用対効果が不明確」、「コストが過大」などが主たる理由となっている。

3．リスク管理の実態

■ 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ると、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。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 21.4%が「不明・キーパーソンもいない」と回答。また、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。

4．従業員教育と今後の課題認識

■ 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、この点改善が期待される。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。

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。

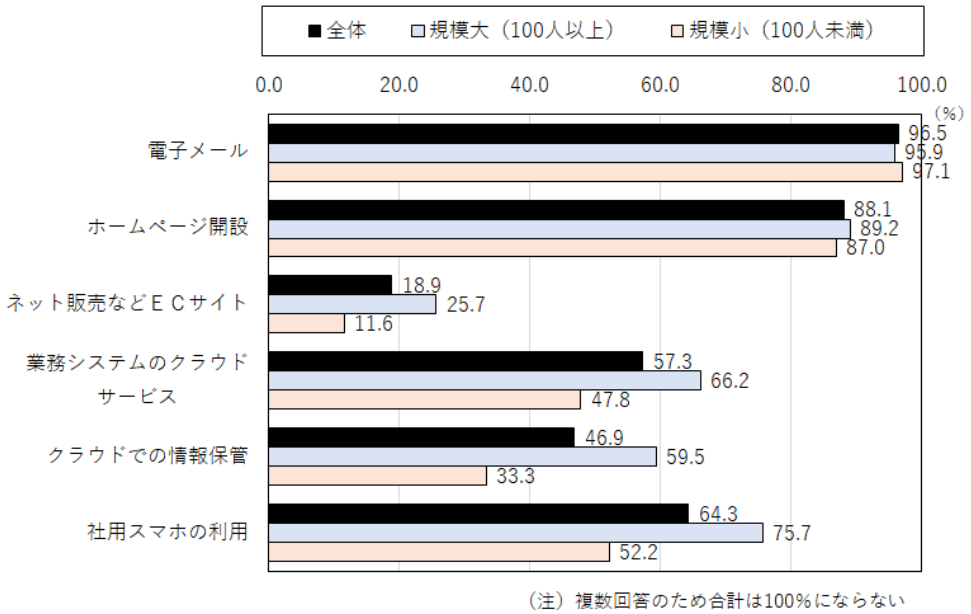
1．情報セキュリティ・リスクは遠い存在なのか

まず、県内企業にとって情報セキュリティ・リスクは遠い存在なのか、それともすぐそばに潜む脅威なのかを、IT の利用状況や最近の被害状況、更に情報セキュリティに関する取引先からの要請内容を通じて確かめる。

(1) 利用している主な IT

情報セキュリティ・リスクの度合いは、社内システムがインターネット等を介して外部と繋がる機会の多寡に依存すると考えられる。そこで、利用している主な IT についてみると、「電子メール」は 96.5%とほぼ全ての先、「ホームページ開設」も企業規模の大小を問わず 9 割近くの先が利用している。次いで多いのが「社用スマホの利用」(64.3%) であり、会計管理・人事管理などの「業務システムのクラウドサービス」(57.3%)、「クラウドでの情報保管」(46.9%) と続く。後二者は規模の大きい企業では半数以上、規模の小さい企業でも 3 割から 5 割が利用している。IT の活用状況を踏まえると、県内企業は、規模の大小にかかわらず、コンピュータ・ウイルスへの感染、不正アクセス、ランサムウエア攻撃等の脅威と決して無縁ではないといえる。

問 1. 主な IT の利用状況



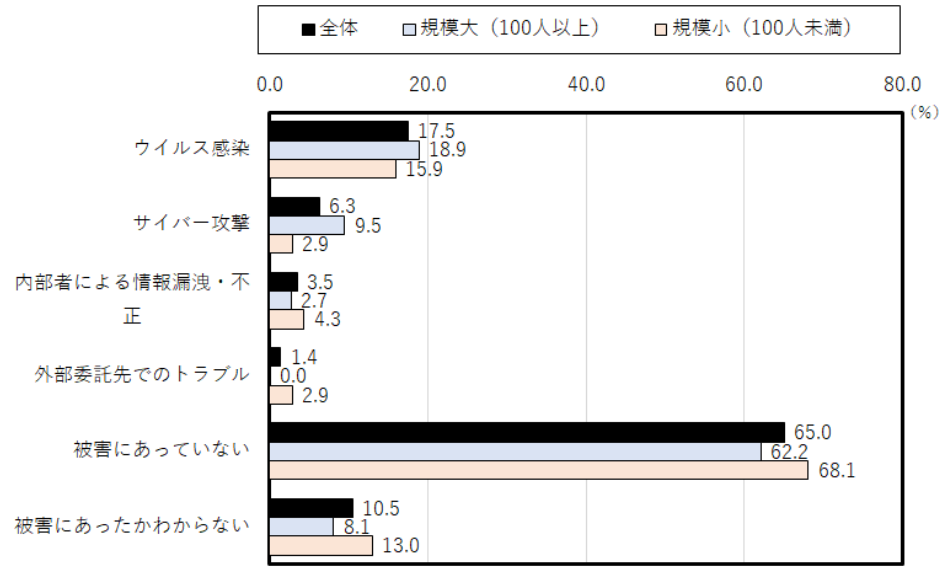
（注）複数回答のため合計は100%にならない

(2) 実際の情報セキュリティ被害

次に、過去 3 年間における実際の情報セキュリティ被害について尋ねると、6 割超の企業では「被害にあっていない」としている。もっとも、これは裏を返せば、4 割弱が被害にあったか、「被害にあったかわからない」(10.5%) ということであり、その点がより重要で

ある。規模別にみると、大きな先では、「ウイルス感染」が 18.9%、「サイバー攻撃」が 9.5%にのぼっており、小さな先でも 15.9%の先が「ウイルス感染」を経験している。規模が小さければ情報セキュリティ被害から免れられるというわけではない。

問 2. 過去３年間での情報セキュリティ被害状況(複数回答)



（注）複数回答のため合計は100%にならない

こうした中、情報セキュリティ被害を受けたとする企業に対して、どのような影響があったかを尋ねると、端末の修復・入れ替えや業務停止など過大な負担を強いられたことがわかる。今回は、限られたサンプル数であるにもかかわらず、下表のとおり少なからぬ回答が寄せられた。改めて情報セキュリティ・リスクへの備えの重要性を感じさせる。

問 3. 情報セキュリティ被害の業務や取引への影響、金銭的な影響

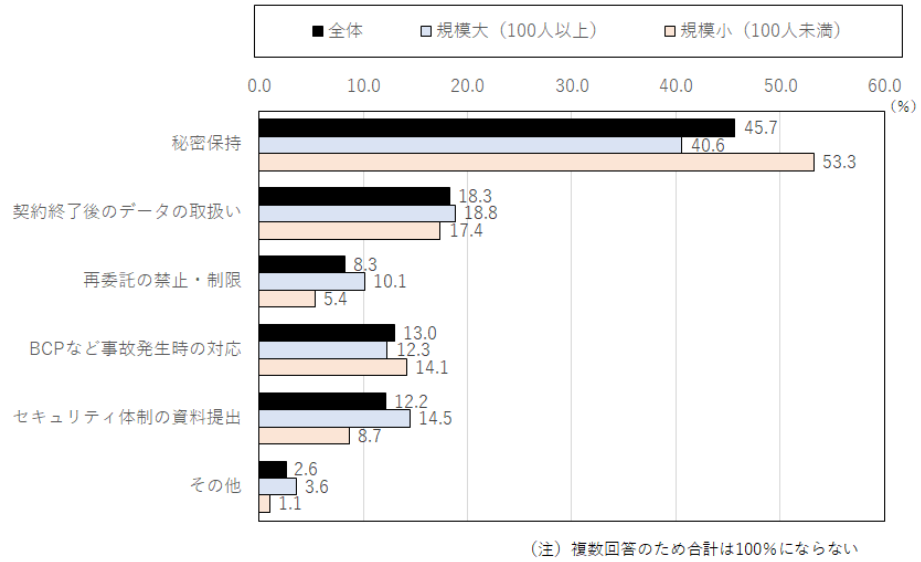
業種	規模	業務や取引への影響や金銭的影響
精密機械	大	Emotet被害あり。感染したPCを修復しつつ、全社員に注意喚起し、大きな影響には至らなかった。
金属製品	大	社用スマホ紛失。取引先へ謝罪の連絡を実施。
輸送用機械	大	業務全般が滞り、多大な損失にみまわれた。
建設	大	取引先のPC が感染。当社社員のメールアドレスが流失する可能性があったが、事なきを得た。
鉄鋼・非鉄金属	大	大きな影響ではないが、パソコン買替え費用を要したほか、暫く業務ができなくなった。
電気機械器具	小	約600万円の調査費用、再発防止対策費用のほか、監督官庁への報告書提出等の事務負担が発生。保険金の補填があったが、業務負荷は大。
窯業・土石	小	外部取引先との交信が丸一日できなくなった。

(3) 情報セキュリティに関する取引先からの要請内容

情報セキュリティに関する取引先からの要請は、取引先自身が意識している重要な情報セキュリティ・リスクを表している。そうした要請に応じられるか否かは、実際の取引量を左右することから、企業にとっては優先度の高い対応事項である。具体的な要請内容をみると、「秘密保持」が 45.7%と最大であり、次いで「契約終了後のデータの取扱い」となっている。これに加えて、規模の大きい企業では、14.5%の先が「セキュリティ体制の資料提出」を求められており、規模の小さい企業では 14.1%の先で「BCP など事故発生時の対応」を整えることが求められている点が特徴的である。

なお、経済産業省は、企業のセキュリティ対策状況を可視化し、対策レベルが適正か判断するために「サプライチェーン強化に向けたセキュリティ対策評価制度」の導入を検討している (2026 年 10 月開始予定)。企業は「ガバナンスの整備」、「インシデントへの対応」等の評価に基づいて格付けされ、今後はこの評価制度が政府の調達要件や企業間取引において実効性を持つ基準となる可能性がある。

問 4. 情報セキュリティに関する取引先からの要請内容(複数回答)



（注）複数回答のため合計は100%にならない

(小括)

業務における IT の活用の拡がりに伴い、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。過去 3 年間の情報セキュリティ被害について窺うと、「被害にあっていない」との回答は 6 割台であることから、4 割弱の企業は被害にあったか、「被害にあったかわからない」。また、情報セキュリティ被害を受けた場合の影響としては、端末の修復・入れ替えや業務停止などが挙げられている。「秘密保持」を中心とする取引先からの要請も、企業にとっては優先度の高い対応事項である。

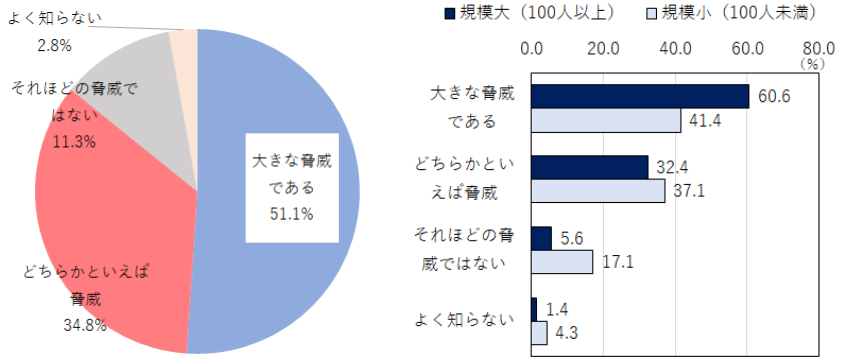
2. 情報セキュリティのリスク認識とリスク管理スタンス

前述のとおり、県内企業にとって情報セキュリティ・リスクは遠い存在ではなく、すぐそばに潜む脅威にほかならないが、企業サイドのリスク認識やリスク管理スタンスはどうなのか、以下、アンケートへの回答により確認する。

(1) 情報セキュリティ被害の認識、被害にあう可能性についての認識

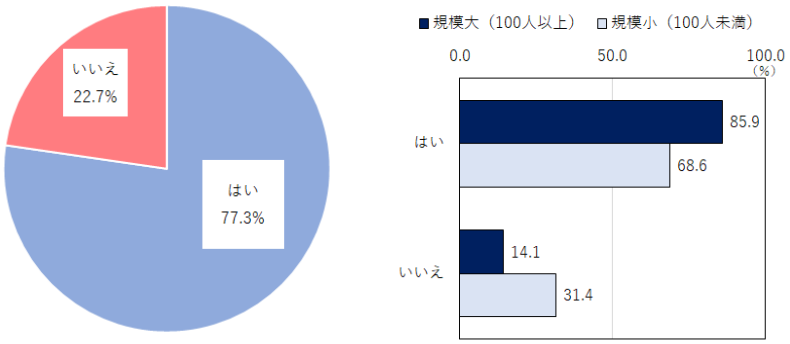
情報セキュリティ被害に関する認識を窺うと、51.1%の先が「大きな脅威である」としているものの、「それほどの脅威ではない」(11.3%)、「よく知らない」(2.8%) など、必ずしも重く受け止めているわけではない先が合計 14.1%にのぼるなど、気懸りな結果となった。なお、そうした受け止め方は、規模の小さい企業ほど多い。

問 5. 情報セキュリティ被害の認識

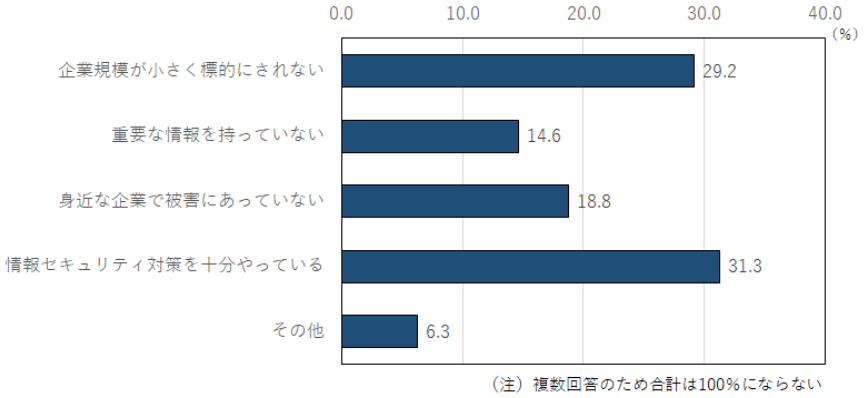


また、情報セキュリティ被害にあう可能性も、77.3%と大方の企業は感じているものの、22.7%もの先は被害にあう可能性を感じないとしている。更に、そう回答した企業に対して被害にあわないと感じる理由を問うと、「情報セキュリティ対策を十分やっている」(31.3%)、「規模が小さく標的にされない」(29.2%) との回答が約 3 割にのぼった。

問 6. 情報セキュリティ被害にあう可能性を感じるか



問 7.　情報セキュリティ被害にあわないと感じる理由（問 3 の更問。複数回答）

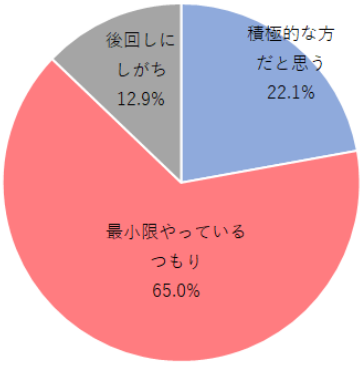


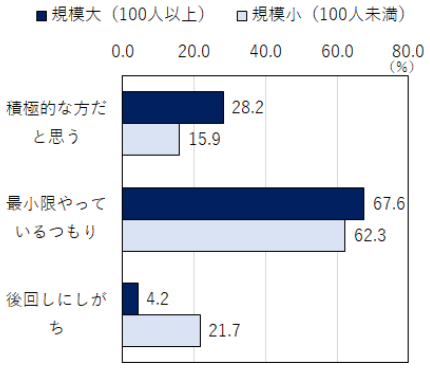
（注）複数回答のため合計は100%にならない

（2）リスク管理スタンス

以上のリスク認識のもとでリスク管理スタンスはどうか。まず、自己評価を尋ねると、全体として、「積極的な方だと思う」と自負する企業は 22.1%にとどまり、大勢（65.0%）は「最低限はやっているつもり」と、どちらかといえば受け身の姿勢にあるのが実情である。さらに、12.9%と相応の数の企業が「後回しにしがち」としていることには課題を感じざるを得ない。企業規模別にみると、規模の小さい企業では、「後回しにしがち」の比率が 21.7%に達するなど、より課題が大きい状況にある。

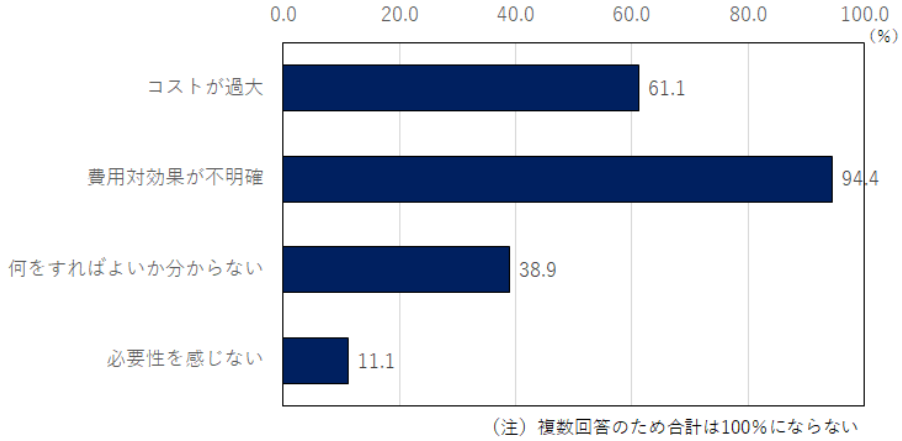
問 8.　情報セキュリティへの取組みに関する自己評価





「後回しにしがち」と回答した企業に対して、その理由を尋ねると、「費用対効果が不明確」が 94.4%と圧倒的で、次いで「コストが過大」が 61.1%となっている。これらに共通するのは、厳しい資金事情のもと、実感できないリスクにコストをかける気になれないという心理であると思われる。ただ、取引先からの要請に応えられず、最悪取引を失う可能性があることも認識し、情報セキュリティへの取組み姿勢を見直すことが期待される。

問 9　「後回しにしがち」になる理由　（問 8 の更問。複数回答）

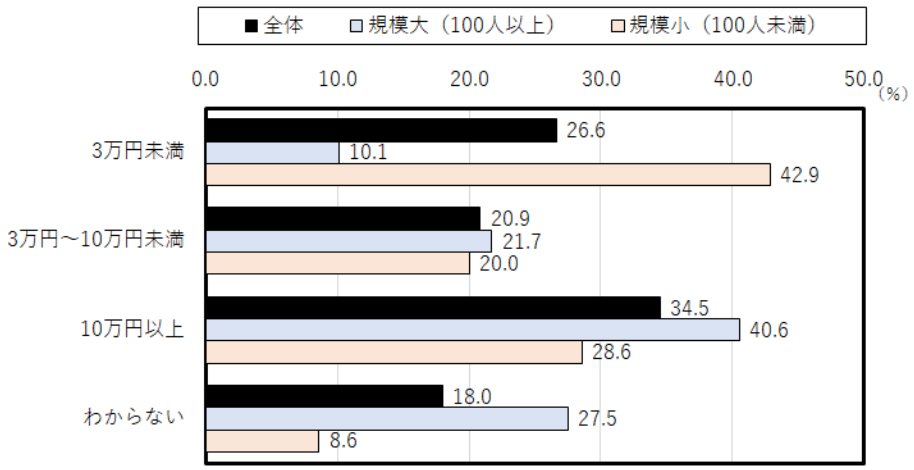


（注）複数回答のため合計は100%にならない

（3）情報セキュリティのための金銭的負担

また、情報セキュリティのための費用について問うと、月額で「10 万円以上」と相応の費用を支払って対応している先と、「3 万円未満」と殆どコストをかけていない先との二極化がみられる。これは専ら規模の小さい企業の回答によるもの。規模が小さくとも、月額「10 万円以上」とする先が 28.6%もある点は心強いが、42.9%の先では「3 万円未満」となっている。因みに、規模の大きい先では「10 万円以上」が 40.6%と最大勢力である。

問 10　情報セキュリティ費用（月額）



（小括）

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、情報セキュリティ被害について重く受け止めていない企業は 14.1%と相応にあり、また、被害にあうと感じていない企業も 2 割を超えている（22.7%）。この背景には、「情報セキュリティ対策を十分やって

いる」とか「規模が小さく標的にされない」といった見方がある。こうしたリスク認識の下、リスク管理の取組みについては、どちらかといえば受け身の姿勢にある企業が大勢であり、さらに 12.9%と相応の数の企業が「後回しにしがち」とするなど、課題は大きい。「費用対効果が不明確」、「コストが過大」などが主たる理由である。

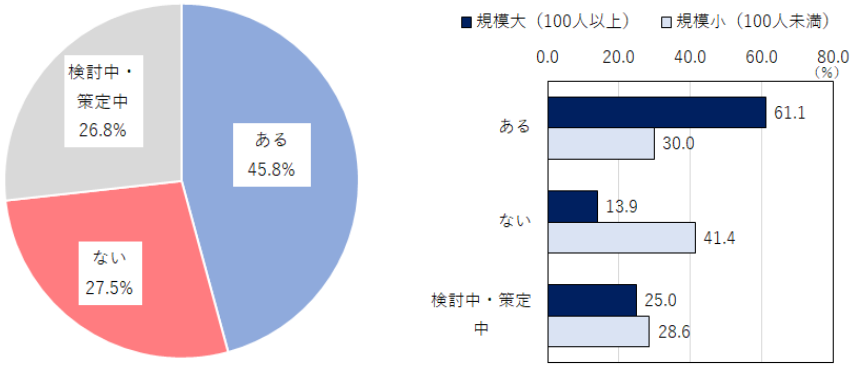
3. リスク管理の実態

上記の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。

(1) セキュリティ・ポリシーと組織体制

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。

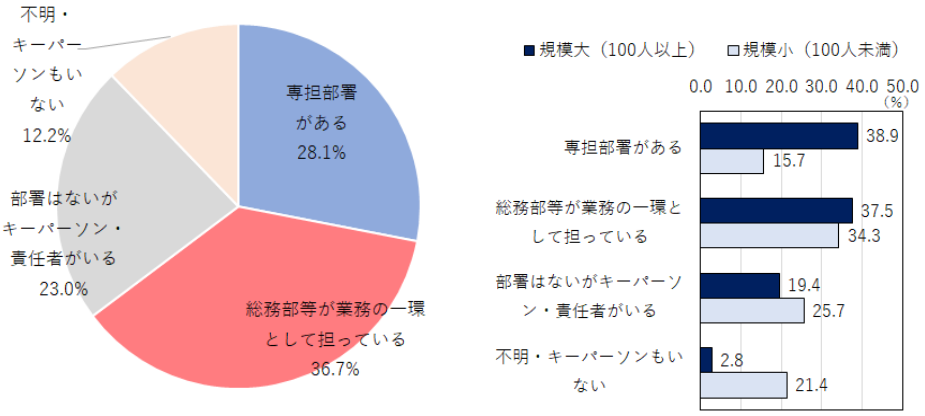
問 11　セキュリティ・ポリシーの有無



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 12　情報セキュリティの組織体制

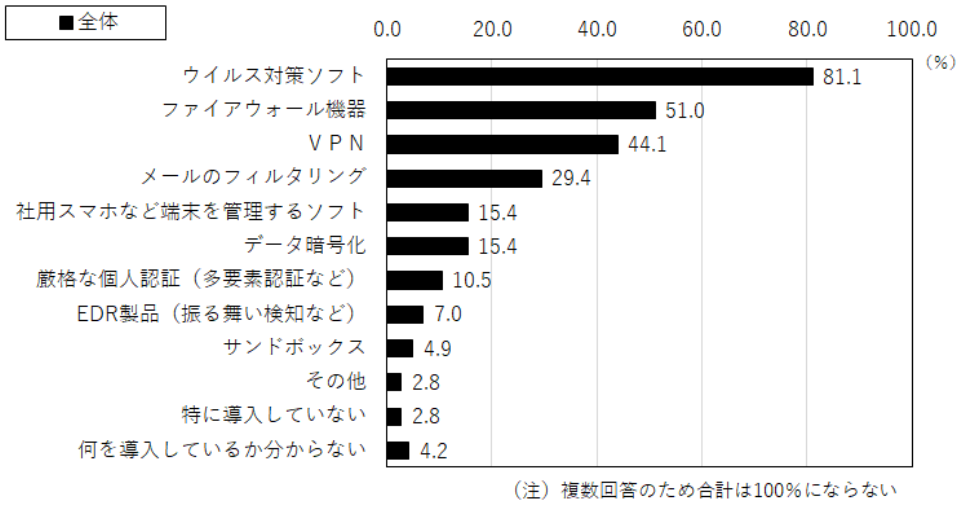


（2）リスク管理ツールの導入状況

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、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、サンドボックス）、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 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。

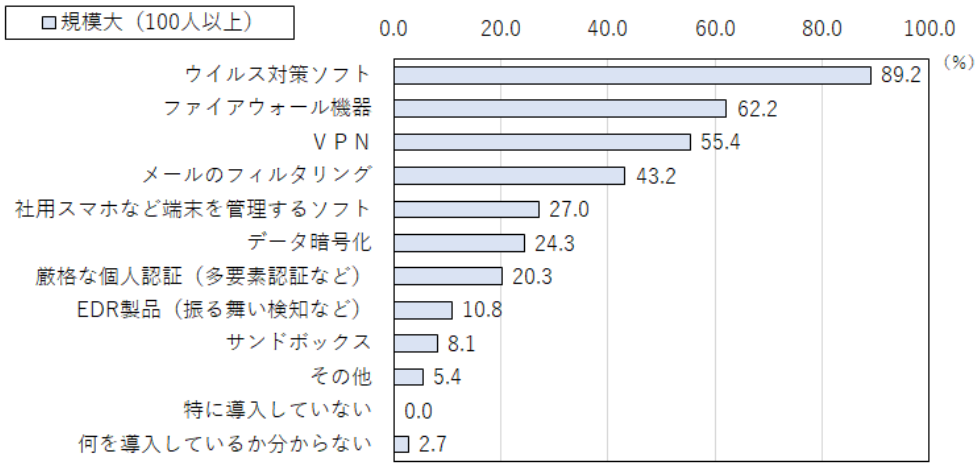
（注 1）ＶＰＮ	バーチャル・プライベート・ネットワーク。社内ネットワークと社外 PC の間に仮想の専用回線を通すサービス（例えばリモートワークで会社のサーバに接続）。
（注 2）ファイアウォール機器	外部インターネットと内部システムの間に設置される機器で、通信の許可・拒否を判断する。
（注 3）サンドボックス	砂場。怪しいメールなどを隔離して、ウイルス感染していないかを検証・分析。
（注 4）EDR 製品	エンドポイント・ディテクション・アンド・レスポンス。PC などの端末（エンドポイント）を監視し、ウイルス感染した際の不審な動きを検知する製品。

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)



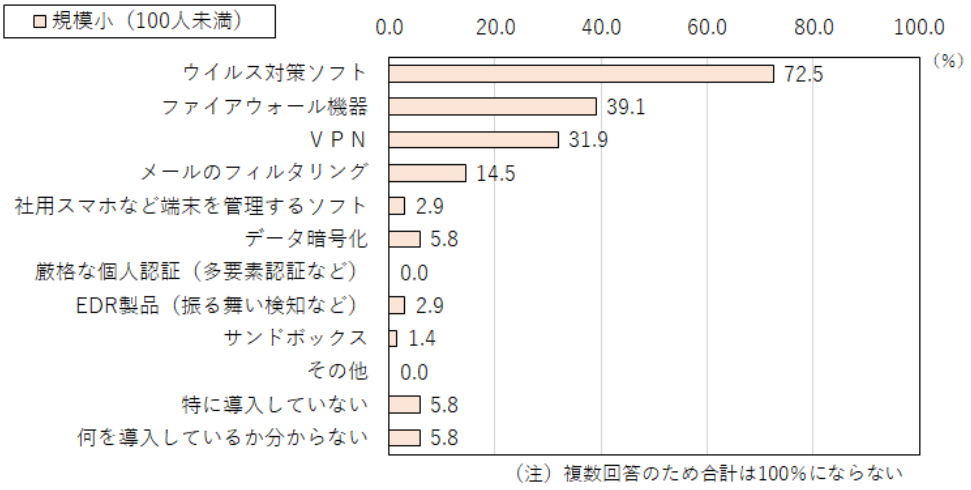
（注）複数回答のため合計は100%にならない

これを企業規模別にみると、規模の大きな企業では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。



（注）複数回答のため合計は100%にならない

一方、規模の小さな企業においては、「ウイルス対策ソフト」は 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重要な課題である。

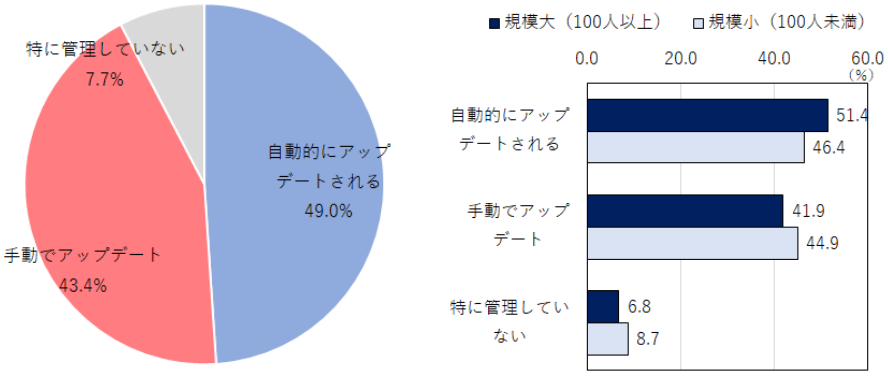


(3) アップデートの仕組み

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。

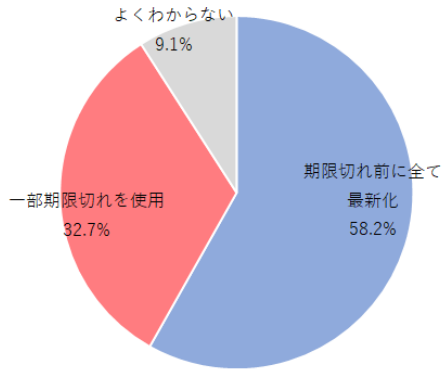
問 14　OS （オペレーティングシステム／基本ソフト）などソフトウエアの最新化



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。

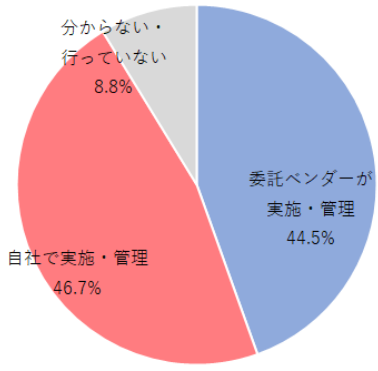
問 15　サポート期限切れの OS の使用

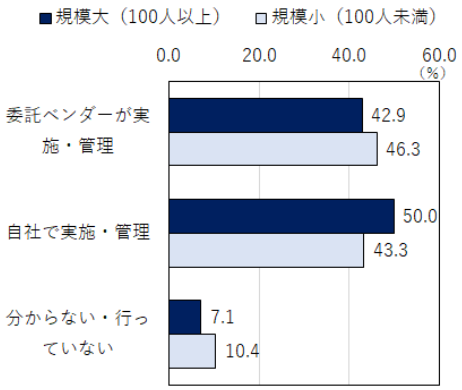


（注）本設問の集計対象は55社。

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 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。

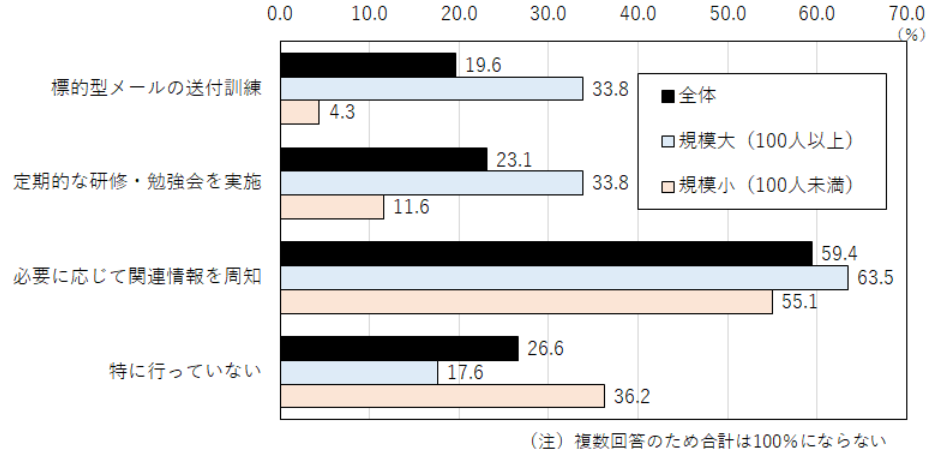
4. 従業員教育と課題認識

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

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 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。

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)



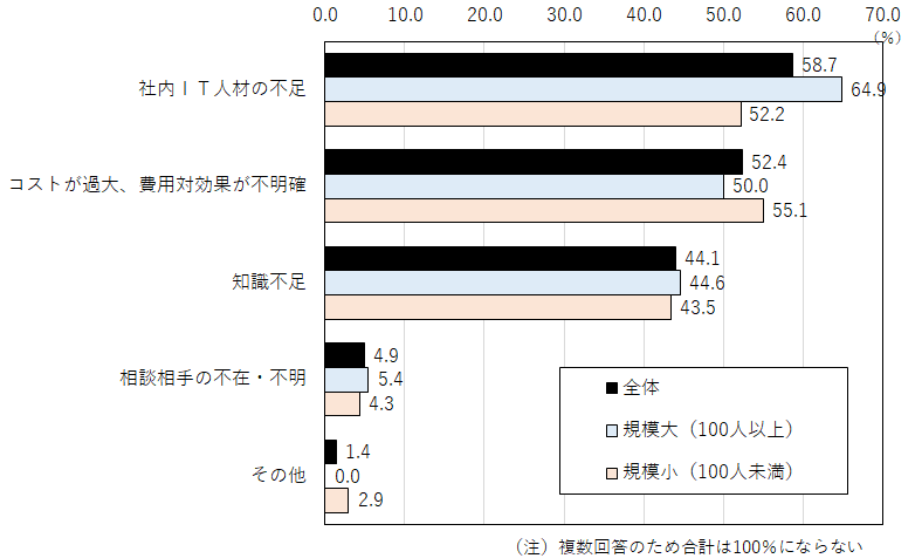
（注）複数回答のため合計は100%にならない

(2) 企業からみた情報セキュリティの課題

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。

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）



（注）複数回答のため合計は100%にならない

（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。

5．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。

以　　上