

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

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ェア(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。

——— 以下、6月号「後編」———

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」、「コストが課題、費用対効果が不明確」が過半を超えている。

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。

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（問 1）

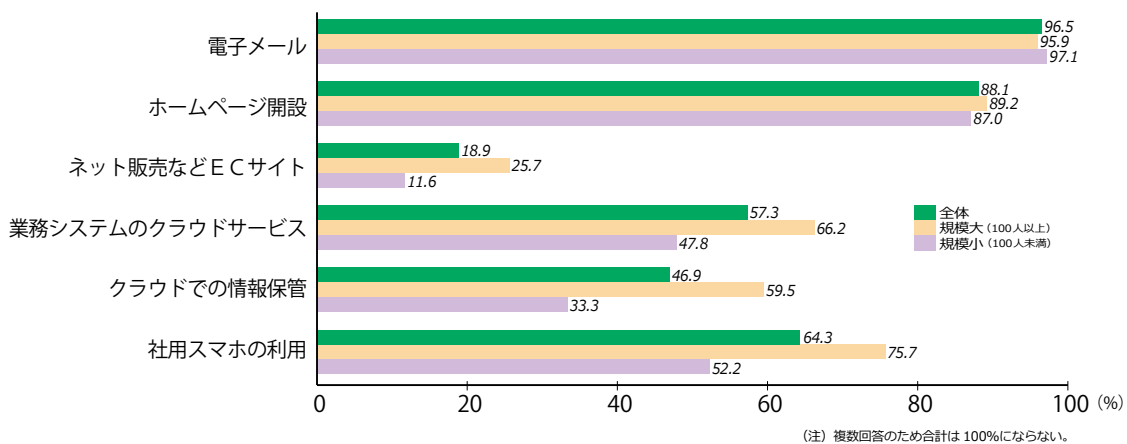
情報セキュリティ・リスクの度合いは、社内システムがインターネット等を介して外部と繋がる機会の多寡に依存すると考えられる。そこで、利用している主な IT についてみると、「電子メール」は 96.5% とほぼ全ての先、「ホームページ開設」も企業規模の大小を問わず 9 割近くの先が利用している。

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、ランサムウェア攻撃等の脅威と決して無縁ではないといえる。

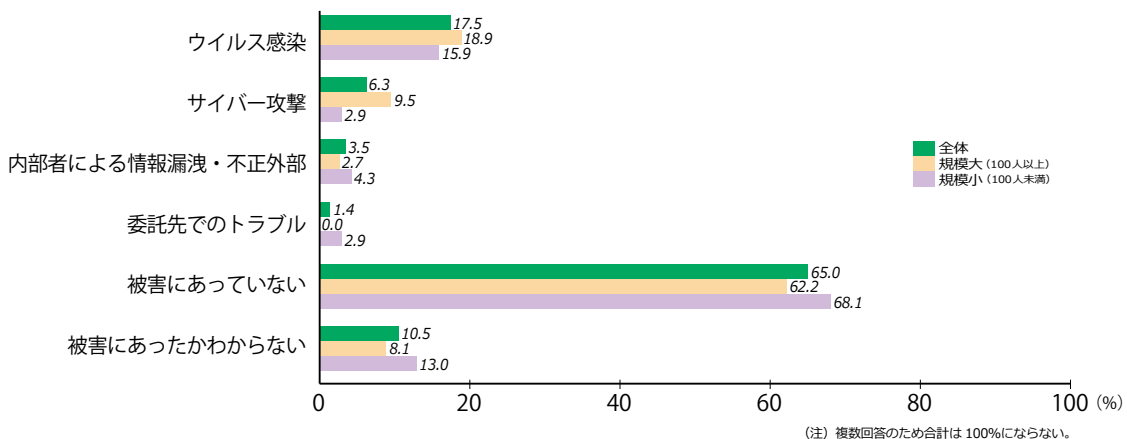
(2) 実際の情報セキュリティ被害（問 2.3）

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

問 1. 主な IT の利用状況



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）

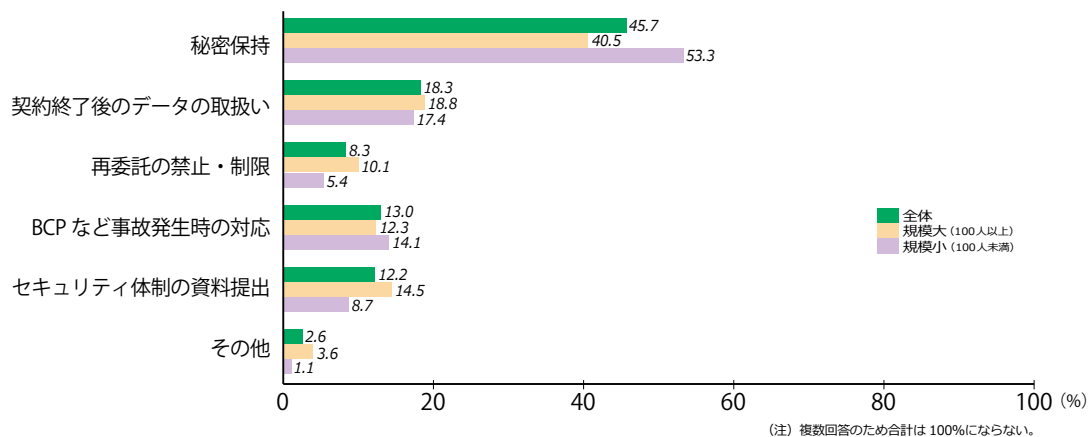




問 3. 情報セキュリティ被害の業務や取引への影響、金銭的な影響

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	業務全搬が滞り、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	外部取引先との通信が丸一日できなくなった。

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）



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。

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、上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。

(3)情報セキュリティに関する取引先からの要請内容(問 4)

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。

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。

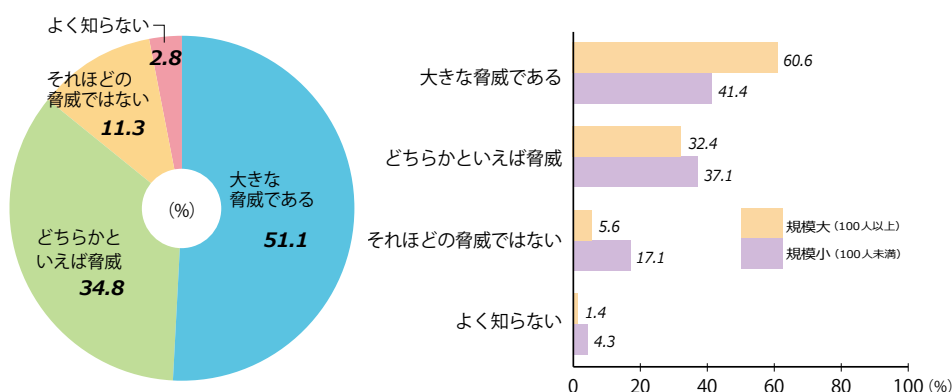
情報セキュリティのリスク認識と リスク管理スタンス

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。

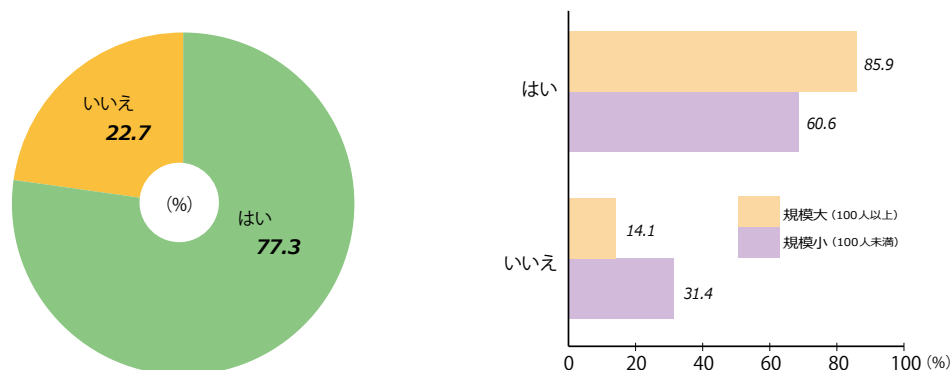
(1)情報セキュリティ被害の受け止め方、被害にあう可能性についての認識（問5~7）

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、「それほど脅威ではない」(11.3%)、「よく知らない」

問5. 情報セキュリティ被害の受け止め



問6. 情報セキュリティ被害にあう可能性を感じるか



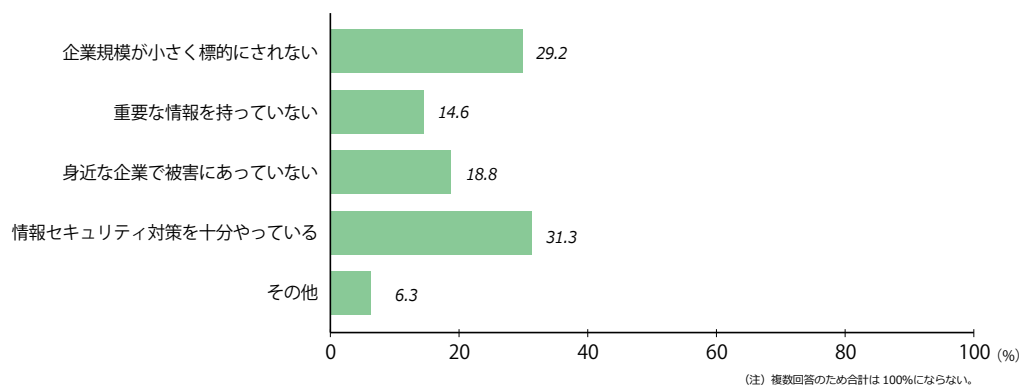


(2.8%) など、必ずしも重く受け止めているわけではない先が合計 14.1%にのぼるなど、気懸りな結果となった。なお、そうした受け止め方は、規模の小さい企業ほど多い。

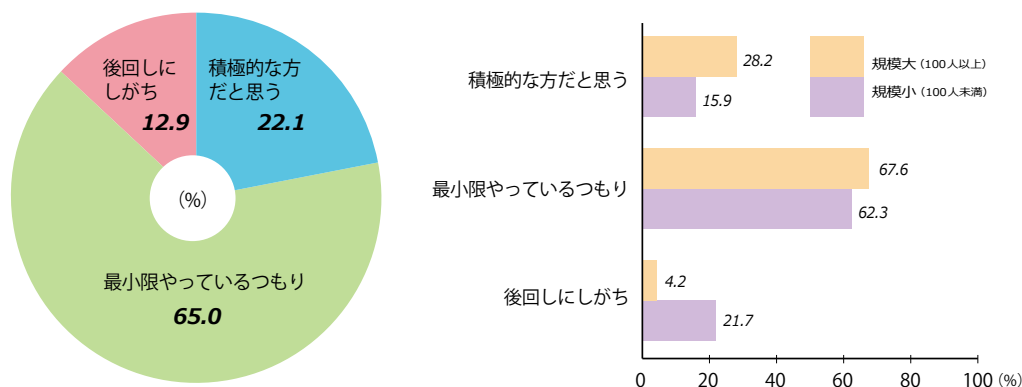
また、情報セキュリティ被害にあう可能性も、

77.3%と大方の企業は感じているものの、22.7%もの先が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

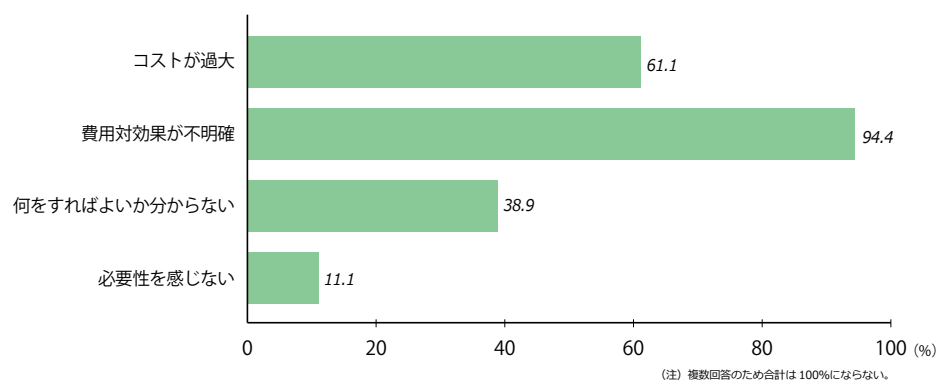
問 7. 情報セキュリティ被害にあわないと感じる理由（問 6 の更問。複数回答）



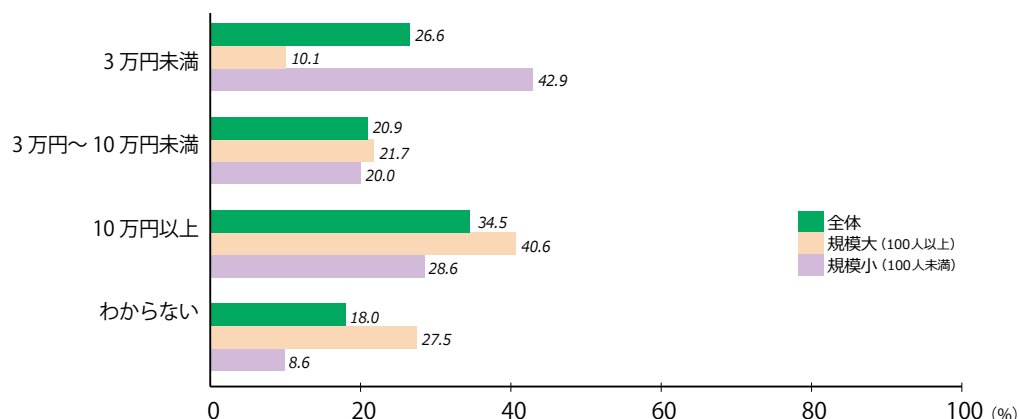
問 8. 情報セキュリティへの取組みに関する自己評価



問 9 「後回しにしがち」になる理由（問 8 の更問。複数回答）



問 10 情報セキュリティ費用（月額）



い」（29.2％）との回答が約3割にのぼった。

(2) リスク管理スタンス（問 8.9）

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「最小限やっているつもり」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。

「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り組み姿勢を見直すことが期待される。

(3) 情報セキュリティのための金銭的負担（問 10）

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。

（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。

（6月号「後編」に続く）