事務所ニュース News
2025.7
K-071
発行：村田健二税理士事務所

経営バイタルの強化書 KEIEI VITAL

中小企業が実際に行っている有効な情報セキュリティ対策のポイント

「2024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」報告書

独立行政法人情報処理推進機構（以下「IPA」）は、中小企業等におけるサイバーセキュリティ対策の実態及び課題等を明らかにし、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理することを目的に調査を実施しました。

1 「2024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」報告書

近年、サプライチェーン上の弱点を狙って、攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化しており、サプライチェーンを構成する中小企業等がサイバー攻撃に対する対策が不十分である場合、当該中小企業等の事業活動に支障が生じ得ることに加えて、取引先が提供した重要な情報が流出してしまうおそれや、当該企業を踏み台にして取引先が攻撃されるおそれ等があります。

このような状況を踏まえ、独立行政法人情報処理推進機構（以下「IPA」）では、中小企業等におけるサイバーセキュリティ対策の実態及び課題等を明らかにし、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理することを目的に調査を実施しました。

この調査では、全国の中小企業4191社を対象にウェブアンケートを行い、情報セキュリティ対策への取り組みや被害の状況、対策実施における課題、取引先を含む情報セキュリティ対策の状況などが調査されました。

この調査の結果は2025年2月14日に速報版※1として、サプライチェーン全体でのサイバーセキュリティの不備が取引先にも深刻な影響を及ぼしていることを報告し、今回（2025年5月27日）公表された資料※2で、「2024年度中小企業等実態調査」全体の報告書を取りまとめるとともに、中小企業が実際に行っている対策や効果が見られた対策のポイントを報告しています。

2 中小企業の現状（速報版のポイント）

速報版の主なポイントは下記のとおりとなっています。

① 過去3期内で、サイバーインシデントが発生した企業における被害額の平均は73万円（うち9.4%は100万円以上）、復旧までに要した期間の平均は5.8日（うち2.1%は50日以上）
② 不正アクセスされた企業の約5割が脆弱性を突かれ、他社経由での侵入も約2割
③ サイバーインシデントにより取引先に影響があった企業は約7割
④ 過去3期における情報セキュリティ対策投資を行っていない企業は約6割
⑤ セキュリティ対策投資を行っている企業の約5割が、取引につながった

① 過去3期内で、サイバーインシデントが発生した企業における被害額の平均は73万円（うち9.4%は100万円以上）、復旧までに要した期間の平均は5.8日（うち2.1%は50日以上）

2023年度にサイバーインシデントの被害を受けたと回答した企業（n=975）のうち、サイバーインシデントによる影響として、「データの破壊」と回答した企業が35.7%、「個人情報の漏えい」と回答した企業が35.1%でした。また、過去3期に発生したサイバーインシデントで生じた被害額の平均は73万円であり、100万円以上の被害額であった企業は9.4%（最大で1億円）、過去3期内で10回以上のサイバーインシデント被害に遭った企業が1.7%（最大で40回）、復旧までに要した期間の平均は5.8日であり、50日以上を要した企業が2.1%（最大で360日）でした。サイバーインシデントと聞くと大企業の被害が目立ちますが、中小企業においても実際に甚大な被害が起きていることが窺えます。

② 不正アクセスされた企業の約5割が脆弱性を突かれ、他社経由での侵入も約2割

裏面へ続く→

2023年度にサイバーインシデントの被害を受けた企業のうち「不正アクセス被害を受けた」と回答した企業（n=419）について、サイバー攻撃の手口を聞いたところ、「脆弱性（セキュリティパッチの未適用等）を突かれた」との回答が48.0%で最も多く、次いで、「ID・パスワードをだまし取られた」との回答が36.8%でした。「取引先やグループ会社等を経由して侵入」との回答も19.8%あり、サプライチェーン上のセキュリティリスクが読み取れます。

不正アクセスによる被害の内容については、「自社Webサイトのサービス停止、または機能が低下させられた」が22.9%、「業務サーバのサービス停止、または機能が低下させられた」との回答が20.3%と上位となりました。

③ サイバーインシデントにより取引先に影響があった企業は約7割

2023年度にサイバーインシデントの被害を受けたと回答した企業（n=975）のうち、全体の約3割に相当する「特に無し」を除くと、約7割が「サイバーインシデントにより取引先に影響があった」と回答しました。影響があったと答えた企業のうち、「取引先にサービスの停止や遅延による影響が出た」との回答は36.1%でした。また、「個人顧客への賠償や法人取引先への補償負担の影響が出た」との回答が32.4%、「原因調査・復旧に関わる人件費等の経費負担があった」との回答も23.2%でした。サプライチェーン全体でのサイバーセキュリティの不備が、取引先にも深刻な影響を及ぼし、事業の継続性を脅かす実情を浮き彫りにしています。

④ 過去3期における情報セキュリティ対策投資を行っていない企業は約6割

「情報セキュリティ対策投資をしていない」企業の割合が62.6%でした。2016年度調査の55.2%、2021年度調査の33.1%からさらに増加しています。

情報セキュリティ対策投資を行わなかった理由としては、「必要性を感じていない」の割合が44.3%と最も多く、「費用対効果が見えない（24.2%）」、「コストがかかりすぎる（21.7%）」が続いています。中小企業として資金が限られる中で情報セキュリティ投資に踏み出せない状況が窺えます。

⑤ セキュリティ対策投資を行っている企業の約5割が、取引につながった

取引先（発注元企業）から情報セキュリティ対策に関する要請を受けた経験がある企業（n=511）のうち、取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと回答した企業は、42.1%でした。

また、情報セキュリティ対策投資別に見てみると、過去に情報セキュリティ対策投資を行っている企業の49.8%が、発注元からの要請でサイバーセキュリティ対策を行ったことが取引につながったと回答しているのに対し、情報セキュリティ対策投資を行っていない企業では27.4%に留まっています。

3 中小企業が実際に行っている対策や効果が見られた対策のポイント

中小企業が実際に行っている対策や効果が見られた対策の主なポイントは下記のとおりとなっています。

① OSやウイルス対策ソフトの最新化を実施している企業は約7割
② 情報セキュリティ対策実施によりサイバーインシデント被害が低減した
③ 1割強の企業が取引先から情報セキュリティ対策の要請を受けている
④ セキュリティ体制を整備している企業の約6割が、取引につながった

① OSやウイルス対策ソフトの最新化を実施している企業は約7割

「5分でできる！情報セキュリティ自社診断」（以下「自社診断」）※3の25項目について、「実施している」及び「一部実施している」を合わせた割合は「パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか?」（73.0%）が最も高く、次いで「パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか?」（71.4%）でした。基本的なセキュリティ対策はある程度定着していることが窺えます。

一方、低かったのは「新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか?」（37.9%）、次いで「情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか?」（39.2%）、「セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか?」（39.8%）でした。組織的に取り組む必要のあるセキュリティ対策が進んでいないことが窺えます。

② 情報セキュリティ対策実施によりサイバーインシデント被害が低減した

「自社診断」の25項目を「実施している … 4点」「一部実施している … 2点」「実施していない … 0点」「わからない … −1点」で点数化し、25項目の対策状況を採点したところ、合計点が高い企業ほどサイバーインシデントによる影響を「特になし」と回答した割合が高い傾向が見て取れます。情報セキュリティ対策の実施により、サイバーインシデント被害（影響）の低減が期待されます。

③ 1割強の企業が取引先から情報セキュリティ対策の要請を受けている

発注元企業から情報セキュリティに関する要請を受けた経験がある企業の割合は1割強でした。要請された内容は、8割が「秘密保持のための措置」（79.6%）でした。

要請された対策の実施に向けての課題は、「対策費用（具体的な対策と費用）の用意、費用負担の検討」（51.3%）が最も多く、次いで「情報セキュリティ対策に関する販売先（発注元企業）との契約内容の明確化」（47.0%）、「専門人材の確保・育成」（32.9%）でした。コストや人材不足が課題となっていることが窺えます。

④ セキュリティ体制を整備している企業の約6割が、取引につながった

取引先（発注元企業）から情報セキュリティ対策に関する要請を受けた経験がある企業のうち、セキュリティ体制の整備がされている（専門部署（担当者）がある）企業の59.8%が、発注元からの要請でサイバーセキュリティ対策を行ったことが取引につながったと回答しているのに対し、セキュリティ体制の整備がされていない（セキュリティ対策は各自の対応に任せている）企業は24.2%に留まっています。取引先から要請を受けた企業側の担当者の実感として、セキュリティ体制が整備されている企業の方が、対策の実施が取引上の信頼を得るための重要な要素であることを示しています。

※1「2024年度中小企業等実態調査結果」速報版を公開（IPA）（URL：https://www.ipa.go.jp/pressrelease/2024/press20250214.html）
※2「2024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」報告書について（IPA）（URL：https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html）
※3 5分でできる！情報セキュリティ自社診断（IPA）（URL：https://www.ipa.go.jp/security/guide/sme/5minutes.html）