

中小規模事業者の安全管理措置に関する実態調査
分析結果

令和5年8月9日

個人情報保護委員会

(はじめに)

令和4年4月1日に全面施行された個人情報の保護に関する法律等の一部を改正する法律(令和2年法律第44号。以下「令和2年改正法」という。)により、個人情報取扱事業者において、個人データの漏えい等が発生し、個人の権利利益を害するおそれがあるとき、個人情報保護委員会への報告及び本人への通知が義務化されることとなった。

こうした中、個人情報保護委員会は、広報・啓発活動として、事業者への講師派遣や多面的な情報発信、ハンドブック等のホームページ掲載等の広報・啓発活動に努めている。令和4年度における主な取組として、以下のものが挙げられる。

①事業者等に対して個人情報保護制度を周知するため、オンラインでの説明会を含め、事業者団体主催の説明会等への講師派遣等を行った。

②個人データ等の漏えい等発生時の対処を周知・啓発するために「個人情報保護委員会シンポジウム」(令和5年2月16日)を開催した。

③令和2年改正法の概要を幅広い国民に周知する動画「個人情報保護法の概要」、安全管理措置についてまとめた動画「個人情報保護法上の安全管理措置」、個人データを取り扱うために整備が必要な規律等や、個人情報保護委員会のホームページに掲載しているツールについて紹介する動画「規律等の整備とお役立ちツールのご紹介」等を作成し、政府インターネットテレビに掲載した。

今般、従業員の数が100人以下の中小規模事業者における個人データの安全管理措置の実態を把握し、個人情報保護委員会における検討及び今後の執務に役立てるとともに事業者の個人情報保護に対する意識の向上につなげることを目的として、アンケート調査を実施し、①個人情報の保有状況、②個人情報保護に関する取組、③令和2年改正法と漏えい等への対応、④不正アクセス、⑤ECサイト等の運営状況、⑥テレワークの実施状況、⑦個人情報保護委員会への要望等について、分析結果を取りまとめた。

(調査の概要)

(1) 調査方法

委託事業者(株式会社アズコムデータセキュリティ)による郵送アンケート調査。

(2) 調査事項

個人情報の保有状況、個人情報保護に関する取組、令和2年改正法と漏えい等への対応、不正アクセス、ECサイト等の運営状況、テレワークの実施状況、個人情報保護委員会への要望等。

(3) 調査対象

国内に本社を置く従業員100人以下(※)の事業者3万先(無作為抽出)。

(※)「個人情報の保護に関する法律についてのガイドライン(通則編)」で、従業員100人以下の個人情報取扱事業者を「中小規模事業者」としている。なお、次に掲げるものを除く。

- ・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6月以内のいずれかの日において、5,000を超える者
- ・委託を受けて個人データを取り扱う者

(4) 回収率等

令和5年1月18日から2月28日までに4,681件を回収(回収率15.6%)。

(5) 回答事業者の属する業種

全体	建設業	製造業	情報通信業	運輸業、郵便業	卸売業、小売業
100.0% (4,681 社)	23.0% (1,076 社)	13.0% (610 社)	2.6% (123 社)	2.9% (138 社)	16.6% (778 社)
不動産業、 物品賃貸業	宿泊業、飲食サ ービス業	教育、学習支 援業	医療・福祉	その他	無回答
4.1% (191 社)	2.4% (111 社)	1.5% (70 社)	9.8% (461 社)	21.5% (1,005 社)	2.5% (118 社)

(※) 図表中の構成比率は、小数点第2位以下を四捨五入しているため、合計しても必ずしも 100.0%とはならない(以下同じ)。

1. 個人情報の保有状況

- ・ 中小規模事業者を対象としているが、保有する顧客情報が1万人超の事業者も一部(4.8%)存在する。
- ・ 保有する個人情報の内容をみると、基本4情報(氏名、生年月日、性別、住所)の保有割合は約4~9割となっている。その他、電話番号は約8割、メールアドレスは約5割、銀行口座情報は約3割、マイナンバー及び健康状態(健康診断情報を含む)はそれぞれ約2割、保有されている。

(1) 顧客情報

全体	100人以下	100人超~1千人以下	1千人超~1万人以下	1万人超~100万人以下	100万人超	無回答
100.0% (4,681社)	51.9% (2,428社)	31.1% (1,456社)	10.7% (500社)	4.6% (216社)	0.2% (8社)	1.6% (73社)

(2) 従業員情報

全体	5人以下	5人超~50人以下	50人超~100人以下	100人超~	無回答
100.0% (4,681社)	37.5% (1,756社)	53.2% (2,488社)	5.6% (261社)	2.8% (133社)	0.9% (43社)

(3) 保有する個人情報の内容(複数回答可)

全体	氏名	生年月日	性別	住所	電話番号	クレジットカード情報	銀行口座情報	メールアドレス	パスワード
(4,681社)	89.1% (4,173社)	43.7% (2,047社)	55.1% (2,577社)	78.2% (3,660社)	83.8% (3,924社)	2.9% (138社)	31.0% (1,449社)	45.1% (2,110社)	3.1% (144社)
パスポート番号	マイナンバー	免許証番号	販売履歴	HP等の閲覧履歴	健康状態(健康診断情報含む)	病歴	顔画像	その他	無回答
1.6% (76社)	17.1% (799社)	11.0% (516社)	16.9% (791社)	1.1% (50社)	17.9% (840社)	8.3% (387社)	8.5% (399社)	2.1% (96社)	6.1% (286社)

2. 個人情報保護に関する取組

- ・ 個人情報の取扱いに関する課題について、「何をしてもよく分からない」、「個人情報保護法等(ガイドラインを含む)の理解不足」との回答が、それぞれ約4割となっており、個人情報の保護に関する法律(平成15年法律第57号)等に係る理解が不足しているため、具体的に何をしてもよく分からない状況にあることがうかがわれる。
- ・ 個人情報保護に関する担当者のいない中小規模事業者が、過半数を占めている。
- ・ 個人情報の管理に当たり参考にしているものとして、「法律・ガイドライン」(約6割)に次いで、「弁護士や税理士、コンサルティング業者への相談」(約3割)が多い。また、「弁護士や税理士、コンサルティング業者への相談」と回答した中小規模事業者の具体的な相談先としては、税理士が最も多く(約7割)、次いで社会保険労務士の比率が高く(約4割)、いずれも弁護士の比率(約2割)を上回っている。中小規模事業者にとって税務や社会保険などで密接な関係性を有する税理士及び社会保険労務士に対して、個人情報の管理等についても相談を寄せていることがうかがわれる。
- ・ 個人情報の安全管理に関する措置に過去1年間に要したコストは、「10万円以下」が約6割、「10万円超～100万円以下」が約3割であり、「100万円超～」は僅少(4.1%)に留まっている。

(1) 個人情報の取扱いに関する課題(複数回答可)

全体	何をしてもよく分からない	個人情報保護法等(ガイドラインを含む)の理解不足	社内規程が不足している	従業員の教育	情報セキュリティ対策	個人情報保護のための資金不足	個人情報保護のための人材不足	電子化による管理の難易度上昇	その他	無回答
(4,681社)	36.1% (1,690社)	38.4% (1,796社)	20.2% (945社)	25.7% (1,201社)	24.8% (1,160社)	13.2% (616社)	14.0% (657社)	24.4% (1,143社)	20% (94社)	8.0% (374社)

(2) 個人情報保護に関する担当者の有無

全体	いる	いない	無回答
100.0% (4,681社)	43.7% (2,047社)	52.6% (2,463社)	3.7% (171社)

(3) 個人情報の管理に当たり参考にしているもの(複数回答可)

全体	法律・ガイドライン	個人情報保護委員会が発信する情報や資料	個人情報保護委員会以外の行政機関が発信する情報や主催する説明会に参加	商工会議所、法人会、認定団体等の民間事業者が発信する情報や主催する説明会に参加	個人情報保護に関する書籍等	弁護士や税理士、コンサルティング業者への相談	親会社・グループ企業からの通達等	その他	無回答
(4,681社)	57.7% (2,701社)	10.1% (471社)	3.1% (145社)	12.2% (572社)	11.9% (559社)	26.3% (1,230社)	12.0% (562社)	5.1% (239社)	5.3% (250社)

(4)「弁護士や税理士、コンサルティング業者への相談」と回答した事業者の具体的な相談先(複数回答可)

全 体	弁護士	税理士	社会保険労務士	行政書士	コンサルティング業者	その他	無回答
(1230社)	17.5% (215社)	74.1% (912社)	38.4% (472社)	8.8% (108社)	10.4% (128社)	1.1% (14社)	3.4% (42社)

(5)個人情報の安全管理に関する措置に過去1年間に要したコスト

全 体	10万円以下	10万円超～ 100万円以下	100万円超～ 1,000万円以下	1,000万円超～ 5,000万円以下	5,000万円 超	無回答
100.0% (4,681社)	60.9% (2,850社)	27.1% (1,270社)	4.0% (185社)	0.1% (7社)	0.0% (1社)	7.9% (368社)

3. 令和2年改正法と漏えい等への対応

- ・ 令和2年改正法への対応について、予定を含めても対応するとの回答は3割に満たず、「改正したことや改正の内容を知らない」との回答が約4割、「改正の内容は把握しているが何をしてもよいか分からない」との回答が約1割であり、多くの中小規模事業者が対応できていないことがうかがわれる。
- ・ 令和2年改正法により個人情報の漏えい等報告が義務化されたことについて、「知らなかった」との回答が約8割を占め、「知っている」との回答は約2割に留まった。
- ・ 漏えい等発生時の規程・マニュアルの整備状況について、「規程・マニュアル等を作成している」との回答は約1割に留まるが、「今はないが、これから作成する予定」との回答が約4割、「今後も作成する予定はない」との回答が約4割を占めている。

(1) 令和2年改正法への対応状況

全体	対応済	今年度中に 対応予定	1年以内に 対応予定	対応の予定 はない	改正したこと や改正の内容 を知らない	改正の内容は 把握しているが 何をしてもよいか 分からない	無回答
100.0% (4,681 社)	7.8% (366 社)	6.6% (308 社)	10.8% (507 社)	15.9% (745 社)	42.3% (1,982 社)	11.1% (518 社)	5.4% (255 社)

(2) 個人情報の漏えい等報告の義務化についての認知状況

全体	知っている	知らなかった	無回答
100.0% (4,681 社)	18.6% (869 社)	78.6% (3,677 社)	2.9% (135 社)

(3) 個人情報の漏えい(紛失も含む)・滅失・毀損があった場合の対応手順を文書化した規程・マニュアルの有無

全体	規程・マニュアル 等を作成している	今はないが、 これから作成 する予定 (1年以内)	今はないが、 これから作成 する予定 (将来的に実施 予定だが、1年 以内の予定はな い)	今もなく、 今後も作成する 予定はない	無回答
100.0% (4,681 社)	14.8% (691 社)	8.0% (374 社)	36.8% (1,721 社)	36.8% (1,723 社)	3.7% (172 社)

4. 不正アクセス

- ・ サーバやサイト等に不正アクセスを受けたことがあると回答した中小規模事業者は、僅少(3.3%)であるが、被害状況としては「システム等の停止」が約4割、次いで「データの改ざん」、「クレジットカード情報等の決済情報の漏えい」が続いている。
- ・ 不正アクセスの原因として、「システムの脆弱性」のほか、「フィッシングメール」、「セキュリティ対策ソフト等を導入していなかった」、「パスワードの設定不備」などが挙げられている。これらは、いずれも情報セキュリティの基本的な対策(脆弱性に対するパッチ適用、ウイルス対策ソフトの導入、ウイルス定義ファイルを最新の状態にすること、従業員に対する教育・注意喚起など)により回避できた可能性がある。
- ・ また、不正アクセスの被害を受けたにも関わらず、「原因不明」との回答が約4割となっており、中小規模事業者における情報セキュリティに関する分析・調査の対応が十分でないことがうかがわれる。

(1) サーバやサイト等に不正アクセスを受けた経験の有無

全体	受けたことがある	受けたことがない	無回答
100.0% (4,681 社)	3.3% (153 社)	91.0% (4,258 社)	5.8% (270 社)

(2) 不正アクセスを受けた事業者の被害状況(複数回答可)

全体	顧客・取引先情報の漏えい	クレジットカード情報等の決済情報の漏えい	システム等の停止	データの改ざん	その他	無回答
(153 社)	7.2% (11 社)	9.8% (15 社)	37.3% (57 社)	11.1% (17 社)	37.3% (57 社)	2.6% (4 社)

(3) 不正アクセスの原因(複数回答可)

全体	セキュリティ対策ソフト等を導入していなかった	システムの脆弱性	パスワードの設定不備	フィッシングメール	その他	原因不明	無回答
(153 社)	11.1% (17 社)	27.5% (42 社)	6.5% (10 社)	22.2% (34 社)	9.2% (14 社)	37.9% (58 社)	2.6% (4 社)

5. ECサイト等の運営状況

- ・ ECサイト等を運営している中小規模事業者の割合は約1割。このうち、ECサイト等の開発方法について、「外部事業者に委託した」との回答が約5割を占めており、保守・運用についても、外部事業者に委託しているとの回答が約5割を占めている。
- ・ ECサイト等の運用・保守の委託先において漏えい等が発生した場合の対応として、「何かあれば連絡があると思っているので、特にルール等は決めていない」との回答が約4割と最も多く、委託先においてインシデントが発生した場合の対応を委託先任せにしている事業者が多いとみられる。

(1) ECサイト等の運営状況

全体	運営している	運営していない	無回答
100.0% (4,681 社)	8.3% (390 社)	88.9% (4,160 社)	2.8% (131 社)

(2) ECサイト等を運営している事業者の EC サイト等の開発方法(複数回答可)

全体	自社開発 (独自でアプリケーションを開発)	自社開発 (EC-CUBE等のパッケージを利用し、構築)	外部事業者 に委託した	クラウド型 サービス (BASE や shopify 等)を 使って構築した	ショッピング モール型 (楽天等) のサービス を利用した	その他	無回答
(390 社)	8.5% (33 社)	9.7% (38 社)	46.9% (183 社)	21.5% (84 社)	31.5% (123 社)	1.0% (4 社)	0.8% (3 社)

(3) ECサイト等の保守・運用の形態

全体	自社	開発・構築を を行った 外部事業者	開発・構築を行っ た外部事業者と は別の事業者	保守・運用は 特に行っていない	無回答
100.0% (390 社)	39.7% (155 社)	46.4% (181 社)	2.3% (9 社)	9.5% (37 社)	2.1% (8 社)

(4) ECサイト等の保守・運営の委託におけるセキュリティに関する状況(複数回答可)

全体	プロの業者なので、セキュリティ対策についても適切に取り扱われていると認識しており、委託先業者に任せている	委託先業者においてどのようなセキュリティ対策が実施されているか把握している	委託契約時にセキュリティに関する事項も契約内容に盛り込んでいる	委託契約時に情報の漏えいした場合の対応や責任の範囲について盛り込んでいる	その他	無回答
(190 社)	68.9% (131 社)	15.8% (30 社)	4.2% (8 社)	9.5% (18 社)	12.6% (24 社)	8.9% (17 社)

(5) ECサイト等の保守・運営の委託先において漏えい等事案が発生した場合の対応(複数回答可)

全体	漏えい等事案発生時のルールを決めている	不正アクセス緊急時には委託先の判断でシステムを止める基準を決めている	詳細は決めていないものの、休日等も含めた緊急時の連絡体制は整えている	何かあれば連絡があると思っているので、特にルール等は決めていない	その他	無回答
(190社)	13.2% (25社)	12.6% (24社)	33.2% (63社)	38.4% (73社)	1.1% (2社)	9.5% (18社)

6. テレワークの実施状況

- ・ テレワークを「実施している」及び「現在は実施していないが過去実施していた」との回答は、合わせて約2割。そのうち、テレワークにおいて個人データを取り扱っていない事業者が約6割となっているが、「テレワークでも、個人データが保管されている社内のサーバやシステムにアクセスできる」との回答は約5割を占めており、個人データにアクセス可能な環境でテレワークを行っていることがうかがえる。
- ・ VPN 機器の導入状況については、導入しているとの回答が約4割であり、そのうちの約9割が VPN 機器の脆弱性情報を確認している又は確認させていると回答している。

(1)テレワークの実施状況

全体	実施している	現在は実施していない (過去に実施していた)	これまで一度も実施 していない	無回答
100.0% (4,681 社)	12.8% (601 社)	8.3% (388 社)	76.4% (3,575 社)	2.5% (117 社)

(2)テレワークにおける個人データの取扱い

全体	取り扱っている	取り扱っていない	無回答
100.0% (989 社)	37.1% (367 社)	60.2% (595 社)	2.7% (27 社)

(3)テレワークにおける社内サーバ・システムへのアクセス可否

全体	テレワークでも、 個人データが保管さ れている社内の サーバやシステム にアクセスできる	テレワークでは、 個人データが保管さ れている社内の サーバやシステムに アクセスできない	テレワークでは 全ての社内の サーバやシステム にアクセスできない	その他	無回答
100.0% (989 社)	48.6% (481 社)	26.3% (260 社)	16.9% (167 社)	4.1% (41 社)	4.0% (40 社)

(4)VPN 機器の導入状況

全体	導入している	導入していない	無回答
100.0% (741 社)	42.2% (313 社)	54.9% (407 社)	2.8% (21 社)

(5)VPN 機器の脆弱性に係る情報の確認状況

全体	確認して(させて) いる	確認していない	無回答
100.0% (313 社)	88.5% (277 社)	10.5% (33 社)	1.0% (3 社)

7. 個人情報保護委員会への要望等

- ・ 個人情報保護委員会のホームページを閲覧したことがあるとの回答は約1割に留まっている。ただし、閲覧したことがある中小規模事業者のうち、「大変参考になった」と及び「まあまあ参考になった」との回答は合わせて約8割であり、掲載資料の内容は有用なものであることがうかがえる。
- ・ 個人情報保護委員会への要望として、「資料の充実」との回答が最も多いものの、上記のとおり、個人情報保護委員会のホームページを閲覧したことがある中小規模事業者は約1割に留まることと、閲覧した中小規模事業者の約8割からは「参考になった」との評価を受けていることから、まずは現在の資料の存在を周知していくことが肝要と考えられる。

(1) 個人情報保護委員会のホームページの閲覧経験

全体	閲覧したことがある	閲覧したことはない	無回答
100.0% (4,681 社)	8.6% (403 社)	88.1% (4,122 社)	3.3% (156 社)

(2) 「閲覧したことがある」と回答した事業者の閲覧内容(複数回答可)

全体	委員会 開催状況	報道発表 資料	法令・ ガイドライ ン等	令和2、3 年度 改正個人 情報保護 法について	漏えい等 の対応	研修資料 ヒヤリハッ トコーナー	その他	無回答
(403 社)	7.2% (29 社)	17.4% (70 社)	69.7% (281 社)	40.2% (162 社)	33.7% (136 社)	17.1% (69 社)	7.4% (30 社)	0.2% (1 社)

(3) 「閲覧したことがある」と回答した事業者の閲覧による参考度合い

全体	大変参考にな った	まあまあ参 考になった	どちらともい えない	あまり参考にな らなかった	全然参考にな らなかった	無回答
100.0% (403 社)	33.7% (136 社)	48.6% (196 社)	13.4% (54 社)	2.5% (10 社)	0.7% (3 社)	1.0% (4 社)

(4) 個人情報保護委員会への要望等(複数回答可)

全 体	資料の充実	説明会の実施	研修会の実施	研修会への 講師の派遣	その他	無回答
(4,681 社)	15.4% (723 社)	9.5% (444 社)	5.7% (269 社)	1.0% (47 社)	4.3% (202 社)	73.6% (3,447 社)

【個人情報保護委員会への要望等(抜粋)】

項目	内容(抜粋)
資料の充実	<ul style="list-style-type: none"> ・ 最低限のやることリスト ・ 個人情報保護に関するすべて(法律、機関の内容等) ・ 規程のひな型 ・ 社内教育用資料 など
説明会の実施	<ul style="list-style-type: none"> ・ 企業がすべき保護内容の説明及び法改正の内容 ・ 法令・ガイドライン等全般の内容について ・ セキュリティ対策の具体的進め方 など
研修会の実施	<ul style="list-style-type: none"> ・ 企業が最低限実施しなければならない事 ・ リモートによる研修会 ・ 法改正内容と最新の企業側義務内容について など
研修会への講師派遣	<ul style="list-style-type: none"> ・ 不正アクセス被害に遭遇した場合の対処法 ・ 中小企業(それも10名未満)の会社での取組の具体例 など
その他	<ul style="list-style-type: none"> ・ 最新情報の周知 ・ 簡単に短時間で分かるようまとめた説明動画の配信 など

以 上