

経営バイタル の強化書 KEIEI VITAL

個人情報漏えいの対策と万一の 時の対応・報告に備えましょう!

ランサムウェア等の攻撃による個人情報の漏えい対応



近年被害が増加しているランサムウェア等の被害状況と被害に遭遇したときの対応・報告について確認しておきましょう!

1 ランサムウェア等の攻撃による個人情報の漏えい対応

個人情報保護委員会は、12月10日「令和7年度第2四半期における漏えい等報告の処理状況」※1「令和7年度第2四半期における監視・監督権限の行使状況の概要」※2を公表しました。

また、12月4日「漏えい等の対応とお役立ち資料」「特定個人情報の漏えい等事案が発生した場合の対応について」ページのランサムウェア事案に関する共通様式についての記載事項を更新したことを公表しました※3。

令和4年4月1日から、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は、個人情報保護委員会への報告及び本人への通知が必要となっています。個人の権利利益を害するおそれがあるときは、具体的には、①要配慮個人情報が含まれる事態、②財産的被害が生じるおそれがある事態、③不正の目的をもって行われた漏えい等が発生した事態、④1,000人を超える漏えい等が発生した事態を意味します※3。

このような事態が発生した場合は、速やか（概ね3～5日以内）に速報として、また、確定報告（続報）として30日以内に（不正な目的で行われたおそれがある場合は、発覚日から60日以内に）個人情報保護委員会へ報告することが必要になっています。漏えい等報告の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う個人情報取扱事業者と定められており、個人データの取扱いを委託している場合においては、原則として委託元と委託先の双方が報告をする義務を負っています。

税理士は、個人事業者であっても個人情報取扱事業者に該当し、また、クラウドによるデータ保管等を利用している場合に、クラウドサービス提供事業者が不正アクセスにより個人データが漏えいした場合やランサムウェア等により個人データが暗号化され、復元できなくなった場合には、上述の報告が必要となる点には注意が必要です。

2 漏えい等の報告が必要な場合

下記に該当する場合は、個人情報保護委員会へ上述の漏えい等報告が必要となります。

① 要配慮個人情報に含まれる個人データの漏えい等（又はそのおそれ）がある場合

ここで、「要配慮個人情報」とは、人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実、その他政令で定めるもの（身体障害、知的障害、精神障害等の障害があること、健康診断その他の検査の結果、保健指導、診療・調剤情報、本人を被疑者又は被告人として、逮捕、捜索等の刑事事件に関する手続が行われたこと、本人を非行少年又はその疑いがある者として、保護処分等の少年の保護事件に関する手続が行われたこと）になり、例えば、従業員の健康診断等の結果を含む個人データが、漏えいした場合が該当します。

② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等（又はそのおそれ）がある場合

例えば、送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合

やECサイトからクレジットカード番号を含む個人データが漏えいした場合が該当します。

③ 不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等（又はそのおそれ）がある場合

例えば、ランサムウェア等により個人データが暗号化され、復元できなくなった場合や不正アクセスにより個人データが漏えいした場合、従業員が顧客の個人データを不正に持ち出して第三者に提供した場合が該当します。

④ 個人データに係る本人の数が1,000人を超える漏えい等（又はそのおそれ）がある場合

例えば、システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が1,000人を超える場合や自社の会員（1,000人超）にメールマガジンの配信を行う際、本来メールアドレスをBCC欄に入力

