事務所ニュース News
2026.1
K-077

発行：ふじわら税理士事務所　兵庫県高砂市神爪1丁目12番18号 高田ビル2F　Tel.079(433)0030　Fax.079(433)0020

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とは、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 要配慮個人情報が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、従業者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

裏面へ続く→

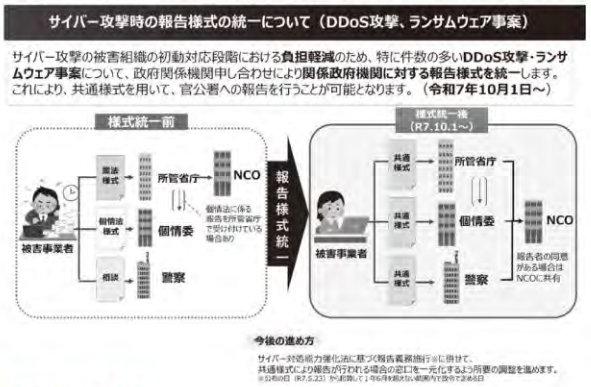
して送信すべきところをCC欄に入力して一括送信した場合が該当します。

個人情報保護委員会への報告は、個人情報保護委員会ウェブサイトの報告フォームより下記の事項について報告を行います※3。

- **報告種別**
- **報告をする個人情報取扱事業者の概要**
- **報告事項**：⑴事態の概要、⑵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の項目、⑶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に係る本人の数、⑷発生原因、⑸二次被害又はそのおそれの有無及びその内容、⑹本人への対応の実施状況、⑺公表の実施状況、⑻再発防止のための措置、⑼その他参考となる事項

令和7年10月1日以降は、ランサムウェア事案による個人データの漏えい等（又はそのおそれ）が発生した場合には、共通様式により報告を行います。

【図1】ランサムウェア事案による個人データの漏えい等の場合の報告※3



3 ランサムウェアの被害報告件数等

警察庁の「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」によれば、令和7年上半期におけるランサムウェアの被害報告件数は116件となっており、半期の件数として令和4年下半期と並び最多となっています※4。

また、組織規模別のランサムウェア被害件数は、前年と同様に中小企業が狙われる状況が継続していて、77件となっており、約3分の2を占め、件数・割合ともに過去最多となっています。

ランサムウェアによる被害に遭った企業・団体等に実施したアンケートの結果によると、令和6年と比較して、ランサムウェアの被害による調査・復旧費用が高額化しており、1,000万円以上を要した組織の割合は、50%から59%に増加しており、中小企業の被害が増える中で費用負担が増加し、被害組織の経営に与える影響は決して小さくないと考えられています。

前述のアンケート結果によると、VPNやリモートデスクトップ用の機器からの侵入が、全体の感染経路の8割以上を占める状況となっており、その原因としては、当該機器のID・パスワード等が非常に安易であったことや、不必要なアカウントが適切に管理されずに存在していたことなどが挙げられています。

攻撃を行うランサムウェアグループは身代金を得るために日々策を講じており、例えば、

- 土日が休業日の企業を狙う場合に、金曜日の営業終了後にシステムに侵入して月曜日の朝までに暗号化を実行する
- 被害企業に侵入口を閉じられた場合でも再侵入できるように、遠隔操作可能なソフトウェアをバックドアとして設置する
- 侵入時の痕跡を消したり、復旧作業をさせないために、被害企業のログやバックアップを消去する

など攻撃手法を巧妙にしています。

【図2】企業・団体における被害報告件数の推移※4

【図3】復旧等に要した期間 調査費用の総額※4

※ノーウェアランサムとは、ランサムウェアと異なり、データの暗号化を行わず、情報の窃取と対価を要求するサイバー攻撃のことを言います。

4 ランサムウェア等の攻撃による個人情報の漏えい原因と対応

個人情報保護委員会「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」によれば、令和7年度第2四半期に指導した案件のうち、不正アクセス事案の原因分析を行ったところ、攻撃別では、ランサムウェアが最多（44件中22件）となっており、原因別では、ソフトウェアの脆弱性、ID・パスワードの脆弱性がそれぞれ、28件、20件と多くなっています※2。

事業者のサーバが不正アクセスを受け、ランサムウェアに感染した結果、ファイルが暗号化され、顧客等の個人データについて、漏えいのおそれが生じた事案の原因としては、

- 侵入口となったサーバやVPN機器の脆弱性が公表されていたにもかかわらず放置していたため、脆弱性を突かれたこと、当該VPN機器の認証情報の強度に問題があったこと
- 侵入に利用された管理者権限を有するVPNアカウントの認証情報を把握できていなかったこと
- 登録されたIPアドレスのみが利用可能な設定とすることができたが、事業者がIPアドレス制限等を実施していなかったこと等推測されやすいID・パスワードの設定をしていたこと

が挙げられており、基本的な対策をしっかり行っていない場合に大きな被害が生じることが示されています。

年末年始が近づき、また、税理士業界の繁忙期が近づく中、ランサムウェア等の攻撃にあわないように、情報セキュリティの基本的な対策を今一度見直しておくことが重要です。

※1「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（PDF）」（個人情報保護委員会）（URL：https://www.ppc.go.jp/files/pdf/251210quarter-report_roueihoukoku.pdf）
※2「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（PDF）」（個人情報保護委員会）（URL：https://www.ppc.go.jp/files/pdf/251210quarter-report_kengenkoushi.pdf）
※3 漏えい等の対応とお役立ち資料（個人情報保護委員会）（URL：https://www.ppc.go.jp/personalinfo/legal/leakAction/#business）
※4「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（PDF）」（警察庁）（URL：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf）