Information System Department
情報通
2024.September　9月号
発　行：東京税理士会 情報システム部

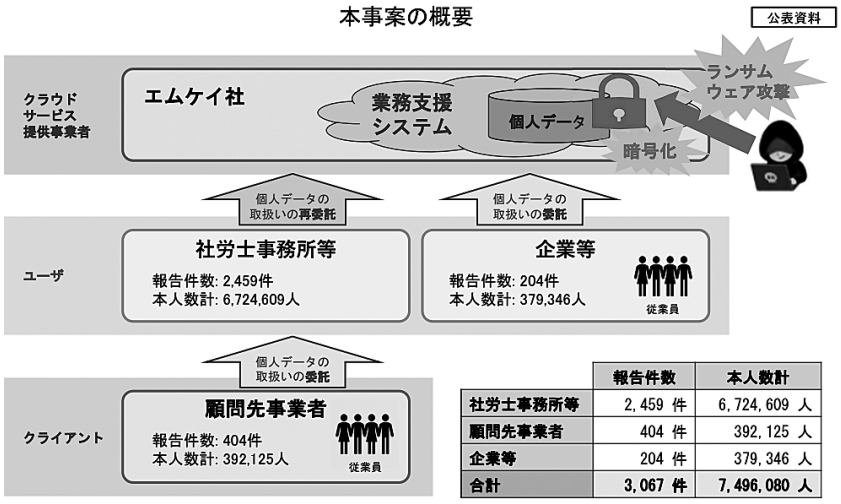
クラウドサービスを利用する場合の個人情報保護法上の留意点

情報システム部　委員　石川　典子

1　はじめに

警察庁が令和６年３月14日に公表した「令和５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」によると、令和５年中におけるランサムウェア被害の報告件数は197件であり、令和４年上半期以降、高い水準で推移していることが報告されています。ランサムウェア攻撃を受けた場合にはデータの毀損及び外部への漏えいが発生する可能性が高いことから、データ内に個人データが含まれる場合は個人データの漏えいとして、本人及び個人情報保護委員会（以下、「個情委」）の報告対象となります。最近では税理士業務にクラウドサービスを利用するケースも増え、自身がセキュリティ対策を施していても、クラウドサービス提供事業者がランサムウェア被害を受ける可能性があります。令和５年６月には、社会保険・人事労務業務支援システムを提供している会社のサーバが不正アクセスを受け、ランサムウェアによりシステム上で管理されていた個人データが暗号化され、漏えいの危険性が生じました（図参照）。同様の事例は、個人データを取り扱う税理士にも十分に起こり得ます。本稿では、現行の個人情報の保護に関する法律（以下、「個情法」）に基づき、クラウドシステム利用者である税理士がとるべき対応についてみていきます。

【図】個情委令和６年３月25日公表資料より



	報告件数	本人数計
社労士事務所等	2,459 件	6,724,609 人
顧問先事業者	404 件	392,125 人
企業等	204 件	379,346 人
合計	3,067 件	7,496,080 人

出典：https://www.ppc.go.jp/files/pdf/240325_houdou.pdf

2　安全管理措置

個人情報取扱事業者は、個情法第23条において、個人データについては安全管理のために必要かつ適切な措置を講じなければならないとされています。

3　クラウドサービスから漏えい等があった場合にとるべき対応

個情法第26条（漏えい等の報告等）は、令和４年４月１日以降、義務規定となりました。個人情報取扱事業者は、取り扱う個人データの漏えい、滅失、毀損など、個人データの安全確保に係る事態で個人の権利利益を害するおそれが大きいものとして一定の事態（具体的には不正アクセスによる個人データの漏えい、マルウェアに感染したことによる個人データの漏えい等）が生じた場合には、速やかに（知った時点から概ね３日～５日以内に）「速報」を行い、事態を知った日から30日以内（不正な目的で行われたおそれがある場合は60日以内）に「確報」を個情委に報告する義務があります。また、個人データの取扱いを委託している場合、委託元と委託先の双方が本人への通知を必要としています（事前に本人の同意を得ていた場合を除く）。

顧問先が税理士に委託し、税理士がクラウドサービスを利用しており、クラウドサービスがランサムウェア攻撃を受けた場合には、税理士及び顧問先は攻撃を受けてから３日～５日以内に個情委と漏えいがあった可能性が高い個人データに係る本人に速報通知をし、30日以内に確報報告の義務があります。

なお、報告等の義務の対象となる「個人データ」と似た用語として「個人情報」「保有個人データ」があります。これらは、個情法における個人情報取扱事業者の義務に関連して使い分けられています。

(1)個人情報：①生存する個人に関する情報で、氏名、生年月日などにより特定の個人を識別できるもの（他の情報と容易に照合して特定の個人を識別できるものを含む）。②個人識別符号（指紋、基礎年金番号等）が含まれるもの。

(2)個人データ：個人情報データベース等を構成する個人情報を指します。これは、コンピュータを使って検索できるように体系的に構成した個人情報を含む情報の集合体、又は紙面で処理した個人情報を一定の規則（例：五十音順、生年月日順など）に従い整理・分類し、特定の個人情報を容易に検索できるようにしたもので、他人によっても容易に検索可能な状態においたもの。

(3)保有個人データ：個人情報取扱事業者が開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行う権限を有する個人データ。ただし、委託を受けて取り扱っている個人データや、体系的に整理されていない個人情報は含まれません。

なお、それぞれの義務規定の差異は下記表を参照してください。

（参考）個人情報、個人データ、保有個人データの義務規定の差異

		個人情報	個人データ	保有個人データ
第17条	利用目的の特定	○	○	○
第18条	利用目的による制限	○	○	○
第19条	不適正な利用の禁止	○	○	○
第20条	適正な取得	○	○	○
第21条	取得に際しての利用目的の通知等	○	○	○
第22条	データ内容の正確性の確保等		○	○
第23条	安全管理措置		○	○
第24条	従業者の監督		○	○
第25条	委託先の監督		○	○
第26条	漏えい等の報告等		○	○
第27条	第三者提供の制限		○	○
第28条	外国にある第三者への提供の制限		○	○
第29条	第三者提供に係る記録の作成等		○	○
第30条	第三者提供を受ける際の確認等		○	○
第32条	保有個人データに関する事項の公表等			○
第33条	開示			○
第34条	訂正等			○
第35条	利用停止等			○
第36条	理由の説明			○
第37条	開示等の請求等に応じる手続			○

出典：https://www.ppc.go.jp/all_faq_index/faq2−q2−3/

4　クラウドサービスを利用する（した）場合の注意点

令和６年３月25日に個情委から出された「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」では、クラウドサービス利用者が個人データを取り扱う際の注意点について述べられています。この中で、クラウドサービスの利用が個人データの取扱いの委託に該当するかどうかを判断する必要があり、委託に該当する場合には、クラウドサービス利用者である個人情報取扱事業者は、委託先に対する必要かつ適切な監督を行わなければならないとしています。サービス選定時には、クラウドサービス提供事業者が個人データを取り扱っているかを確認し、個人データの取扱いがある場合には、監督責任があることを理解した上でサービスを締結する必要があります。また、以下の３点も留意することが求められています。

(1)サービスの選定：サービスに付随するセキュリティ対策について十分に理解し、確認した上でクラウドサービス提供事業者及びサービスを選択すること。

(2)契約の明確化：個人データの取扱いに関する必要かつ適切な安全管理措置として合意した内容を、規約や契約等でできるだけ客観的に明確化すること。

(3)定期的な確認：利用しているサービスに関し、セキュリティ対策を含めた安全管理措置の状況について、例えばクラウドサービス提供事業者から定期的に報告を受けるなどの方法により確認すること。

5　おわりに

個情法は、平成27年改正の際に設けられた「３年ごと見直し」が行われます。来年は改正年となりますので、税理士業務に関わる改正がないか確認しましょう。なお、本会では９月17日（火）に個情法に関する「税理士業務に必要な情報セキュリティ」研修が予定されていますので、是非受講してください。