事務所News ニュース
2026.11
K-087
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

大規模な個人データ漏えい事例の原因と対策を知りましょう!

「大規模な漏えい等事案を踏まえた対応について(注意喚起)」の公表



個人情報保護委員会では、近年の個人データ漏えい事例を踏まえた注意喚起を行い、今後見直し予定の安全管理措置を公表しました。併せて個人情報保護委員会に報告された個人データ事例を分析し、その原因と対策例も公表しました。

1 「大規模な漏えい等事案を踏まえた対応について(注意喚起)」の公表

昨今の国民に広く普及した、大量の個人情報を取り扱う個人情報取扱事業者が外部からの不正アクセスを受け、その取り扱う大量の個人データが漏えいし、又は漏えいのおそれが生じた漏えい等事案が増えていることから、個人情報保護委員会では、10月7日「大規模な漏えい等事案を踏まえた対応について(注意喚起)」を公表しました※。

個人情報保護委員会が公表した「注意喚起」では、**①安全管理措置の全体像、②今後の見直し予定と現時点における見直し後の技術的安全管理措置の内容、③不要となった個人データの消去、④その他御参考**が記載されており、各項目の内容は以下のようになっています。

① 安全管理措置の全体像

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)別添は、「講じなければならない措置」と、当該措置を実践するための「手法の例示」で構成されており、「講じなければならない措置」は、これらに従わなかった場合、法違反と判断される可能性があります。

「手法の例示」は、必ずしも例示の内容の全てを講じなければ法違反と判断されるというものではなく、また、適切な手法は例示の内容に限られるものではありませんが、具体的な対策をとる上で参考になるものとなっています。

② 今後の見直し予定と現時点における見直し後の技術的安全管理措置の内容

個人情報保護委員会では、今後、ガイドライン(通則編)別添の「手法の例示」等について見直しを予定しており(来年4月を予定)、近時の動向を踏まえて「手法の例示」として、外部からの不正アクセスとの関係で、安全管理措置のうち主に問題となる、技術的安全管理措置の見直し予定内容を記載しています。

安全管理措置には、技術的安全管理措置のほかに、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置及び外的環境の把握もあるため、その点には注意が必要となります。

③ 不要となった個人データの消去

個人情報取扱事業者は、利用目的が達成され、当該個人データを保有する合理的な理由が存在しなくなった場合や、利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等は、当該個人データを遅滞なく消去するよう努めなければなりません。

こうした対応が徹底されず、漏えい等事案がより深刻化するといった事例も発生しているため、保管している個人データの必要性についてその法令等の根拠とともに確認を適切に行うことを含めて、改めて注意することが必要です。

④ その他御参考

個人情報保護委員会では、漏えい等報告を受領した事案を分析し、典型的な事案類型及び問題点について「WARNING~不正アクセスによる個人データ漏えい防止のための注意喚起~」(令和6年12月11日、令和8年10月7日改訂)を公表し、注意喚起を行っています。

2 見直し後の技術的安全管理措置の内容

個人情報保護委員会で、見直しを予定している技術的安全管理措置の内容は、下記のものとなっています。

技術的安全管理措置

個人情報取扱事業者は、情報システム(パソコン等の機器を含む。)を使用して個人データを取り扱う場合(インターネット等を通じて外部と送受信等する場合を含む。)、技術的安全管理措置として、次に掲げる措置を講じなければならない。

裏面へ続く→

⑴ **アクセス制御**
担当者及び個人データを取り扱う情報システムの範囲を限定するために、適切なアクセス制御を行わなければならない。

⑵ **アクセス者の識別と認証**
個人データを取り扱う情報システムを使用する者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。

⑶ **外部からの不正アクセス等の防止**
個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

⑷ **情報システムの使用に伴う漏えい等の防止**
情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。

⑸ **不正アクセス等の検知等**
個人データを取り扱う情報システムに対する不正アクセス等が発生した場合に早期に検知等するための措置を平時から講じ、組織内ネットワークにおける被害拡大を防止できるよう適切に運用しなければならない。

上記の講じなければならない安全管理措置の例示について、特に中小規模事業者における手法の例示としては、下記のものがあげられています。

⑴ **アクセス制御**
- 個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。

⑵ **アクセス者の識別と認証**
- 機器に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

⑶ **外部からの不正アクセス等の防止**
- 個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。
- 個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。

⑷ **情報システムの使用に伴う漏えい等の防止**
- メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

⑸ **不正アクセス等の検知等**
- 個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログ等を一定の期間保管する。

3 「WARNING~不正アクセスによる個人データ漏えい防止のための注意喚起~」

個人情報保護委員会では、報告された事案を分析し、問題点を9つの事例として整理し、その原因と対策例を「WARNING~不正アクセスによる個人データ漏えい防止のための注意喚起~」として公表しています。

脆弱性への対応や強固な認証方式の採用等の情報セキュリティ対策は、どれか一つを講じればよいということではなく、多層的に講ずる必要があります。

これらの事例の多くは、委託先等を含め、個人情報取扱事業者内外における複数の組織・部署が関係することから、その問題点を克服するためには、単純な技術的問題への対応にとどまらず、経営層を交えて現状の組織体制の抱える問題点や漏えい等が発生した場合に生じ得る損害等を評価し、組織的に対応することが必要となります。

公表した事例は、〈事例1〉脆弱性が放置された事例、〈事例2〉脆弱性への対応が遅れた事例、〈事例3〉不正ログインの事例、〈事例4〉グループ会社や海外拠点が狙われた事例、〈事例5〉グループ会社間のアクセス制御不備があった事例、〈事例6〉個人領域に保存したデータの漏えい事例、〈事例7〉グループ会社への監督が不十分な事例、〈事例8〉利用するクラウドサービスからの漏えい事例、〈事例9〉API(Application Programming Interface)が悪用される事例となっています。

これらの事例のうち、税理士事務所でも、近年利用されることが多くなっているクラウドサービスからの漏えい事例と個人領域に保存したデータの漏えい事例と原因、対策例は、右記の図のようなものとなっています。

【図1】利用するクラウドサービスからの漏えい事例

クラウドサービス提供事業者が提供する業務システムが不正アクセスを受け、クラウド環境で管理されていた多数のクラウドサービス利用者である顧客企業の個人データが暗号化され、大量の個人データについて漏えいのおそれが生じた事案。

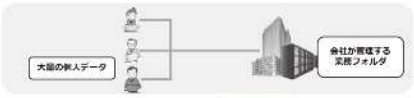


原因
- ✓ クラウドサービスの外部からの不正アクセス等の防止のための措置等の技術的安全管理措置に問題があった。
- ✓ 業務の委託ではないクラウドサービス利用は個人データの取扱いの委託には該当しないと考えていたため、委託先に対する個人データの取扱状況の監督を実施していなかった。

対策例
- ✓ 顧客企業は、利用しようとするクラウドサービスにおいて適切なセキュリティ対策が講じられているかを、サービス利用規約やクラウドサービスの安全性評価に関する資料等により確認し、適切なサービスを選定する。
- ✓ クラウドサービス利用が個人データの取扱いの委託となる場合、利用する顧客企業が適切に取扱状況を把握できるよう、クラウドサービス提供事業者は積極的にセキュリティレポート等の必要な情報を公開することが望ましい。

【図2】個人領域に保存したデータの漏えい事例

個人情報取扱事業者の従業者が、業務で使用する電子ファイル等(個人データを含む。)を個人が管理する領域に保存しており、個人情報取扱事業者の情報システムが不正アクセスを受けた際、個人が管理する領域に保存されていた個人データについても漏えいが生じた。



原因
- ✓ 従業者が業務で使用する電子ファイルについて、組織として管理されておらず、従業者各自のデスクトップ端末等で加工・保存される業務運用が慣例化してしまっており、また、このような管理状況について、定期的な監査等の網にもかからなかった。
- ✓ 組織として管理されていない個人データの中には、本来は消去すべき古いデータ等が含まれているケースがあり、漏えい被害の範囲が大きくなってしまった。

対策例
- ✓ 個人情報取扱事業者における個人データの取扱いは、あらかじめ整備された個人データの取扱いに係る規律・ルールに従う。
- ✓ 個人情報管理台帳等を整備し、定められた保存場所で個人データを作成・加工・保存することを徹底する。
- ✓ 個人データを組織で管理し、取扱職員・管理媒体等を監査部門が把握した上で、定期的な監査等を行う。
- ✓ 従業者に対し、日頃から個人データの取扱いに係る規律・ルールを周知し徹底を促す。

※「大規模な漏えい等事案を踏まえた対応について(注意喚起)」の公表(個人情報保護委員会)(URL:https://www.ppc.go.jp/news/press/2026/261007_houdou/)