個人情報取扱事業者の皆様へ

令和８年 10 月７日
個人情報保護委員会

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）

近時、個人情報保護委員会（以下「当委員会」という。）では、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に接しています。

当委員会は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 26 条第１項の規定による漏えい等報告を受領した事案に関して必要な調査を行い、必要に応じて指導等の権限行使等を行うことで、法第 23 条で規定する安全管理措置について、個人情報取扱事業者の自主的な改善を促しています。また、当委員会は、事業者の安全管理措置の検討に資するようガイドラインに手法の例示等を示すとともに、現在その追加、現代化を図っています。

個人情報取扱事業者のうち、特に、国民の多くが利用する事業における業界内で高いシェアを有するサービス又は顧客が事業者を指定し難いサービスを提供することで大量の個人情報を保有している事業者、機微性の高い個人情報、財産的被害につながるおそれのある個人情報又は詐欺などに利用されるおそれのある個人情報を保有している事業者その他の漏えい等が生じた場合に国民の権利利益の侵害の蓋然性が高い個人情報を保有する事業者の皆様におかれましては、下記で提供する情報も踏まえて、個人情報等の適正な取扱いをお願いします。

記

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）「10 （別添）講ずべき安全管理措置の内容」（以下「ガイドライン（通則編）別添」という。）では、法第 23 条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等について示しています。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が、「手法の例示」は、文字どおり例を示したものであって、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ません。この点、ガイドライン（通則編）別添では、「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものである」としています。

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

令和８年９月 16 日に開催した第 369 回個人情報保護委員会で決議したとおり、今後、ガイドライン（通則編）別添の「手法の例示」等については、現代化を含めた見直しを予定しています[1]。見直しの内容の確定は、来年４月を予定していますが、近時の動向を踏まえて、「手法の例示」として、より参考になると考えられるため、見直し予定の内容を先取りする形でお示しします。

外部からの不正アクセスとの関係では、主に安全管理措置のうち技術的安全管理措置が問題になるところ、現時点における見直し後の技術的安全管理措置の内容は別紙のとおりとなります。なお、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がありますので御留意ください。

3　不要となった個人データの消去

法第 22 条は、「個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、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らない。」と規定しています。すなわち、個人情報取扱事業者は、利用目的が達成され当該目的との関係では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（法令の定めにより保存期間等が定められている場合は、この限りではありません。）。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にも接していますので、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、改めて注意喚起します。

---

[1] https://www.ppc.go.jp/files/pdf/260916_shiryou-2.pdf

４　その他御参考

当委員会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）[2]を公表し、注意喚起を行っていますので、こちらも参考にしてください。

以　上

[2] https://www.ppc.go.jp/files/pdf/261007_warning.pdf

（別紙）

10-6　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。

（1）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。

（2）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。

（3）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。

（4）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。

（5）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。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(1) アクセス制御	（情報システムの限定） • 個人データを取り扱う情報システムを限定する。 • 個人データを取り扱う情報システムへのアクセスを最小化する。例えば、事前に許可した特定の IP アドレスからのみに限定する方法が考えられる。 （アクセスできる者の限定） • 個人データを取り扱う情報システムを使用できる従業者については、ユーザーID に付与するアクセス権限を最小化することにより限定する。 • 特権アカウントを割り当てる従業者、利用する端末、利用する場面等を最小限に限定する。 • 組織体制に変更が生じた場合（例えば、人事異動、従業者の退職等）等に、アクセス権限の変更を適切に行う。 • アクセス制御が適切に行われているか確認する。例えば、アクセス権限について定期的に監査するなど、アクセス権限の棚卸しを行う等の方法が考えられる。 • 組織内外からのアクセスについて、アクセス要求ごとにアクセス元の場所、アクセス時間、デバイスのセキュリティ状態等の動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する仕組みを導入する。	• 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。
(2) アクセス者の識別と認証	（情報システムを使用する従業者の識別・認証手法の例） • ユーザーID、パスワード、磁気・IC カード、指紋認証・静脈認証・顔認証等の方法が考えられる。 • ユーザーID・パスワードを利用する場合には、同一のユーザーID・パスワードの使い回しの原則禁止及び類似パスワードの使い回しの制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止等を行う。	• 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。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	• 個人データへのアクセス権限を有する者が使用できる端末又はアドレス等についての識別と認証を実施する。例えば、IP アドレス認証、電子証明書等の方法が考えられる。 • 組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な個人データへのアクセスにおいては、識別・認証手法を複数組み合わせる多要素認証（フィッシングに耐性のあるものを含む。）を導入する。 （情報システムを使用する従業者以外の者の識別・認証手法の例） • 従業者以外の者を適切に識別・認証する方法を採用する。例えば、同一及び類似パスワードの使い回しをしないよう周知、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止、多要素認証（フィッシングに耐性のあるものを含む。）の導入等が考えられる。	
(3) 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と外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 • 個人データを取り扱う情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入して適切に運用（パターンファイルや修正ソフトウェアの更新確認等を行うことを含む。）し、不正ソフトウェアの有無を確認する。 • 機器やソフトウェア等に標準装備されている自動更新機能等の活用、端末及びサーバー等のオペレーティングシステム、ミドルウェア、アプリケーション等に対するセキュリティ対策用修正ソフトウェアの適用により、ソフトウェア等を最新状態とする。 • 個人情報取扱事業者において許可していないソフトウェア等の導入を防止する。例えば、ソフトウェアの導入時の確認のほか、定期的な監査などの方法が考えられる。 • 組織が許可し、セキュリティ基準を満たしたデバイスからのみ個人データへのアクセスを許可する。	• 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。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(4) 情報システムの使用に伴う漏えい等の防止	(情報システムの開発、維持・管理、変更等における安全性確保) • 個人データを取り扱う情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 • 個人データを取り扱う情報システムの動作確認を行う際に、テストデータとして利用する個人データを必要最小限とする。例えば、テストデータとして個人データを利用することを禁止したり、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換えるなどの方法が考えられる。 • 個人データを取り扱う情報システムの変更時に、当該変更によって情報システム又は運用環境のセキュリティが損なわれないことを検証する。 (通信の経路又は内容の暗号化) • 個人データを含む通信の経路又は内容を暗号化する。例えば、インターネットや無線 LAN 等による個人データの送信（例えば、本人又は従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）時に、個人データの暗号化等の秘匿化（例えば、SSL/TLS、S/MIME 等）を行うなどの方法が考えられる。 • 移送する個人データについて、パスワード等による保護を行う。 (クラウドサービスを利用した情報システムの更改・廃棄) • クラウドサービスのサーバ上に保管された個人データを消去する際は、クラウドサービス提供事業者が提供する方法、暗号化消去等、容易に復元できない手段を採用する。	• 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。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(5)不正アクセス等の検知等	（定期的な分析） • 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（例えば、認証ログ、アクセスログ、操作ログ、通信ログ等）等を一定の期間保管する。 • 当該ログ等の漏えい、滅失及び毀損並びに改ざん、不正消去等からの適切な保護を行う。 • 当該ログ等の定期的な分析により、不正アクセス等の発生又は兆候を早期に検知する。 （常時監視による早期検知） • 不正アクセス等の発生又は兆候を早期に検知等するための仕組み（例えば、IDS/IPS、EDR 等）等を導入する。 （組織内ネットワークでの被害拡大の防止） • 不正アクセス等が発生した場合でも個人データを取り扱う情報システムの被害が広がらないよう、必要な対策を講ずる。例えば、侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化などの方法が考えられる。その他必要な対策については、10-6 技術的安全管理措置(1)から(4)の手法の例示も参照されたい。	• 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。