資料5

個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正

平成27年1月

経済産業省
商務情報政策局　情報経済課

ガイドライン改訂の工程

○ ベネッセからの最終報告書を踏まえ、内閣官房（IT室）及び消費者庁に加え、学識者、消費者団体、中小企業団体を含む経済界の有識者から意見を聴取しつつ、ガイドラインを改訂。

○ 併せて、（独）情報処理推進機構（IPA）による「組織における内部不正防止ガイドライン」も改訂（9月26日付けで公表・施行）。

工程

○ 8月15日：経産大臣から、ガイドラインを改訂する方針を対外説明。

○ 8月18日：経団連等主要経済団体に対し、個人情報の管理徹底に関し、経産大臣名の要請文を発出。

○ 9月17日：ベネッセによる最終報告書の提出。

○ 9月26日：パブリックコメントを開始（～10月28日）。

○ 12月12日：ガイドライン（告示）公表。

○ 12月以降：広報・周知活動を実施。

ガイドライン改訂のポイント

○　個人情報を取り扱う事業者に望まれる新たな行為規範を追加することにより、広く産業界に対し、個人情報の管理に万全を期すことを促す。

○　改訂のポイントは、ベネッセ事案を踏まえ、個人情報保護法における以下の規定に関し、それぞれ取組の充実・強化を図る。

（1）社内の安全管理措置の強化

（安全管理措置）
第20条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの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。

（2）委託先等の監督の強化

（委託先の監督）
第22条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（3）第三者からの適正な情報取得の徹底

（適正な取得）
第17条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

（1） 社内の安全管理措置の強化

問題点

○ 個人情報のダウンロードを監視するシステムが、設定されていなかった。
○ 個人情報を取り扱う部屋へ、私物であるスマートフォンを持ち込むことができた。また、個人情報のデータベースに、そのスマートフォンが接続できる状態になっていた。
○ 個人情報のダウンロードのログ（記録）について、定期的な確認が行われておらず、長期間にわたり、漏えいの事実を把握できていなかった。
○ 「性善説」に立った、不十分な社内管理体制になっていた。

ガイドライン主な改訂事項

①技術的安全管理

○ 個人情報の**監視システム**について、その動作を**定期確認**。

○ 個人情報への**アクセスやダウンロードのログ**（記録）について、不正が疑われる異常な記録の存否を**定期確認**。

②物理的安全管理

○ 業務上許可を得ていない**記録機能を有する媒体・機器の持ち込み・持ち出しの禁止**又は検査の実施。

○ カメラや立ち会い等によるモニタリングの実施。

○ 個人情報を取り扱う部屋への入退室記録の保存。

③組織的安全管理

○ **個人情報保護管理者**（CPO）への**役員の任命**など、社内体制の整備。

○ 情報セキュリティ等に十分な知見を有する者による社内の監査体制の構築。

○ スマートフォン等の**記録機能を有する機器の接続制限**を行う社内規程の整備。

（2）委託先等の監督の強化

問題点

○ システム開発・管理の委託先（子会社）における安全管理措置が十分でなく、そこから個人情報が不正に持ち出された。

○ 委託業務の一部が、委託先から他の企業へ再委託、再々委託されていることを十分に把握できておらず、委託先等を適切に監督していなかった。

ガイドラインの主な改訂事項

①委託先の監督

○ 委託先の選定に当たり、委託先の安全管理措置を確認し、CPO等が評価。

○ 定期的に、委託業務の監査を実施し、その結果について、CPO等が評価。

○ 委託契約等において、委託先で個人データを取り扱う者の役職又は氏名、損害賠償責任を盛り込む。

②再委託先の監督

○ 委託元は、委託先が再委託を行う場合には、委託先から、事前報告又は承認の申請を求める。

○ 委託元は、委託先を通じて、又は必要に応じて自らが、再委託先に対し、定期的な監査を実施。

○ 再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

（3）第三者からの適正な情報取得の徹底

問題点

○　個人情報を取得した者は、提供元がそれを適法に入手したことを十分に確認しないまま（提供元から「誓約書」を取得するという形式的な対応）、当該情報を入手していた。

ガイドライン主な改訂事項

○　第三者から個人情報を取得する場合（※）には、
- 提供元の選定に当たり、その個人情報保護法の遵守状況を確認。
- 個人データの取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、適法に入手されていることを確認。

（※）不特定かつ多数の者が購入することができるものから取得する場合、法令に基づき提供される場合、承継、共同利用、委託等の場合を除く。

○　第三者から個人情報を取得する場合において、当該個人情報が適法に入手されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応。

中小企業への対応／広報・周知

中小企業への対応

○　中小企業を始めとする事業者には、個人情報の管理に当たり、画一的な対応ではなく、その規模、実態に応じ、必要かつ適切な措置を講じることが期待される。

○　ガイドライン改訂では、以下のとおり、「事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じる」という基本原則の中で、中小企業への「一定の配慮」を規定。

(1) 社内の安全管理措置の強化
　特に、中小企業者においては、その事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

(2) 委託先等の監督の強化
　特に、委託先が中小企業者になる場合においては、その事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。
　優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

広報・周知（予定）

○　改訂ガイドラインの内容については、わかりやすいパンフレット等を作成。経済産業省HP等を通じて、広くPRを行う。

○　併せて改訂する「IPA内部不正防止ガイドライン」の内容とともに、全国主要都市8箇所において、地方説明会を開催。説明会の様子は、インターネットで動画を配信。