改正個人情報保護法ニュース第９号

平成 28 年８月 17 日

『改正個人情報保護法Ｑ＆Ａ』
～第９回　安全管理措置とガイドライン～

執筆者：渡邉　雅之
＊　本ニュースレターに関するご相談などがありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士　渡邉　雅之
TEL　03-5288-1021
FAX　03-5288-1025
Email　m-watanabe@miyake.gr.jp

平成 29 年中に施行される個人情報の保護に関する法律の改正法について連載してまいります。

平成 28 年８月２日には、政令の改正・施行規則のパブリックコメント案も公表されました（『「個人情報の保護に関する法律施行令の一部を改正する政令（案）」及び「個人情報の保護に関する法律施行規則（案）」に関する意見募集について』[1]）ので、その内容も踏まえて解説いたします。

1 http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000022&Mode=0

○用語

「個人情報保護法」

個人情報の保護に関する法律のこと。

「現行保護法」

現行の個人情報の保護に関する法律のこと。

「改正法」「保護法」「法」

個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律(平成 27 年9月 9 日法律第 65 号)に基づく改正後の個人情報保護法のこと。

「現行施行令」

現行の個人情報の保護に関する法律施行令

「施行令案」

個人情報の保護に関する法律施行令の一部を改正する政令（案）に基づく改正後の同法施行令のこと。

「規則案」

施行後の個人情報の保護に関する法律施行規則（案）のこと。

「経産省ガイドライン」

「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」のこと。

「番号法ガイドライン」

特定個人情報の適正な取扱いに関するガイドライン（事業者編）（本文及び（別添）特定個人情報に関する安全管理措置）のこと。

Q　改正個人情報保護法の施行により、個人情報取扱事業者に求められる安全管理措置はどのようになりますか。また、個人情報保護委員会は安全管理措置に関してどのようなガイドラインを定めるのでしょうか。

A　現在は、主務大臣である各省庁の長が事業分野ごとにガイドラインを定め、それぞれのガイドラインにおいて安全管理措置も定められています。

改正個人情報保護法の施行後は、個人情報保護委員会が、一元的にすべての事業者に適用されるガイドラインを定め、そのガイドラインにおいて安全管理措置が定められる予定です。

【解説】

1　安全管理措置

個人情報取扱事業者は、個人データについての安全管理措置（保護法 20 条)、従業者の監督（同法 21 条)、委託先の監督（同法 22 条）を講ずる義務を負います。「従業者の監督」と「委託先の監督」は広義の安全管理措置といえます。

改正個人情報保護法においては、これらの規定について改正は全くありません。

（安全管理措置）
第二十条　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。
（従業者の監督）
第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業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。
（委託先の監督）
第二十二条　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。

現行の個人情報保護法の下では、各主務大臣が個人情報保護法に基づく勧告及び命令等の監督権限を有しており、同法８条等に基づき、事業分野ごとの個人情報保護等に関するガイドライン（以下「各省ガイドライン」といいます。）を策定しています。そして各省ガイドラインにおいて安全管理措置も定められています。

例えば、経済産業分野においては、経済産業大臣が「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」を定め、その中で個人情報取扱事業者の

安全管理措置を定めています。

また、金融分野においては、金融庁長官が「金融分野における個人情報保護に関するガイドライン」及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」を定め、これらの中において金融機関が講ずべき安全管理措置を定めています。

２　委員会ガイドラインの一元化

改正保護法の全面施行時（平成 29 年９月８日までの政令で定める日）には監督権限が個人情報保護委員会に一元化されます。これを踏まえて、個人情報保護委員会は、改正保護法４条（国の責務）、８条（地方公共団体「等」への支援）及び 51 条（委員会の任務）に基づき、全ての事業分野に適用される汎用的な個人情報保護委員会ガイドライン（以下「委員会ガイドライン」といいます。）を策定し、告示として公表する予定です。

これに伴って、現行の各省ガイドラインは、原則として委員会ガイドラインに一元化されますが、その際は、事業分野の特性（当該事業において取り扱われる個人情報の性質及び利用方法等の特性を含む。）及び現行の各省ガイドラインの内容等を踏まえるとともに、事業者に混乱が生じないよう留意し、個々に取扱いが検討される予定です。

委員会ガイドラインにおいては、各省ガイドライン等により従来から共通的に示されてきた解釈は基本的に踏襲しつつ、改正法に係る国会審議や直近の社会情勢等も踏まえ、適切な解釈及び事例等を示される予定です。

また、改正法附則 11 条において、「この法律の施行により旧個人情報保護法第２条第３項第５号に掲げる者が新たに個人情報取扱事業者となることに鑑み、特に小規模の事業者の事業活動が円滑に行われるよう配慮するものとする。」とされている点にも留意する必要があります（「第８回　小規模事業者への適用除外の廃止」参照）。

３　委員会ガイドラインで定められる安全管理措置

（１）番号法ガイドラインに準ずる内容[2]

委員会ガイドラインで定められる安全管理措置は、「組織的・人的・物理的・技術的」の観点ごとに「講じなければならない項目」及び「手法例」が示される予定です。

その安全管理措置の内容は、原則、番号法ガイドラインに準ずるものとされる予定です。

その理由は、①番号法で求められる安全管理措置と、個人情報保護法が求める安全管理措置とでは、その基本的な要素（漏えい、滅失又は毀損の防止その他の安全管理のために必要かつ適切な措置）がおおむね共通すること、②番号法ガイドラインの内容は、現在の各省庁の個人情報保護ガイドラインに共通する内容が反映されている（事業者における混乱は少ないものと想定）こと、③番号法ガイドラインの内容は、既に、全ての事業分野の

[2] 個人情報保護委員会「個人情報保護法ガイドラインにおける安全管理措置及び小規模の事業者への配慮に関する基本的な考え方（概要）」参照

事業者に適用されていること、です。

なお、委員会ガイドラインが適用される事業者の規模・事業内容は非常に多様であるため、過剰反応防止等の観点から、汎用的かつ分かり易い内容になる予定です。

その上で、詳細な手法等の例示及び技術的に専門的な内容等については、別途参考となり得る関連規格・指針等（ＩＳＯ・ＪＩＳ・ＩＰＡ等）を示すほか、Ｑ＆Ａその他の解説資料等において必要に応じて示される模様です。

	個人情報保護法の安全管理措置	番号法の安全管理措置
対象情報	個人データ（保護法 20 条）	個人番号（番号法 20 条） 特定個人情報（番号法 33 条）
内容	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 ※具体的な内容及び手法例は、各省庁の事業分野ガイドラインにおいて、組織的・人的・物理的・技術的等の観点で示されている。	個人番号・特定個人情報の漏えい、滅失又は毀損の防止その他の個人番号・特定個人情報の安全管理のために必要かつ適切な措置 ※具体的な内容及び手法例は、番号法ガイドラインにおいて、組織的・人的・物理的・技術的等の観点で示されている。 ※個人情報保護に関する各省庁の事業分野ガイドラインに共通する内容が反映されている。
対象事業者	●現在は、取り扱う個人情報が 5,000 人分以下の事業者は、対象外。 ●改正全面施行後は、個人情報データベース等を事業の用に供する全ての事業者が対象に。（改正法附則第 11 条で小規模の事業者への配慮が求められている。）	●個人番号・特定個人情報を取り扱う全ての事業者（※）（事業者の規模や取扱件数を問わない） ●「中小規模事業者」については、取り扱う個人番号等の数量が少なく、取り扱う従業者が限定的であること等を踏まえて特例的な対応方法が示されている。

（２）小規模事業者への配慮

「第８回　小規模事業者への適用除外の廃止」において改正したとおり、委員会ガイドラインにおいては、番号法ガイドラインを参考に、中小規模事業者に対しては緩和された特例的な安全管理措置を許容する予定です。

特例的な対応の対象となる事業者は、番号法ガイドラインと同様に「中小規模事業者」と称することとし、その範囲は以下のとおり、「従業員の数が 100 人以下の事業者」であって、「取扱う個人情報の数が 5000 人分超の事業者」及び「委託に基づいて個人データを取り扱う事業者」以外の事業者とされる予定です。

個人情報保護法ガイドラインの 「中小規模事業者」	番号法ガイドラインの 「中小規模事業者」
従業員の数が 100 人以下の事業者であって、次に掲げる事業者を除く事業者 ①取り扱う個人情報の数(*)が 5,000 人分超の事業者 ②委託に基づいて個人データを取り扱う事業者	●従業員の数が 100 人以下の事業者であって、次に掲げる事業者を除く事業者 ①個人情報取扱事業者 （≒取り扱う個人情報の数が 5,000 人分超の事業者） ②委託に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者 ③金融分野の事業者 ④個人番号利用事務実施者

＊「取り扱う個人情報の数」：事業の用に供する個人情報データベース等を構成する個人情報により識別される特定の個人の数

（3）番号法ガイドラインにおける安全管理措置

番号法ガイドラインにおいては、以下のとおり安全管理措置について定めています。個人データに関する安全管理措置も、これらと同様の内容が定められることになるでしょう。

ア　安全管理措置の内容

安全管理措置は、①基本方針の策定、②取扱規程等の策定、③組織的安全管理措置、④人的安全管理措置、⑤物理的安全管理措置、⑥技術的安全管理措置からなります。

個人情報（個人データ）に関しては、「基本方針」に相当するのは「個人情報保護方針（プライバシーポリシー）」、「取扱規程等」に相当するのは「個人情報取扱規程」ということになります。

イ　「講じなければならない項目」及び「手法例」

番号法ガイドラインにおいては、以下のとおり、安全管理措置に関して、一般事業者と中小規模事業者に分けて、「講じなければならない項目」及び「手法例」を示しています。

個人情報に関する委員会ガイドラインにおいても、同様の「講じなければならない項目」及び「手法例」が規定されると考えられます。

○一般事業者と中小規模事業者の安全管理措置（参照：内閣官房・個人情報保護委員会作成資料）

<table>
<tr><th>一般事業者における安全管理措置</th><th>中小規模事業者における安全管理措置</th></tr>
<tr><td>A 基本方針の策定
特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。</td><td>同左
→基本方針の策定は義務ではありませんが、作ってあれば従 業員の教育に役立ちます</td></tr>
<tr><td>B 取扱規程等の策定
事務の流れを整理し、特定個人情報等の具体的な取扱いを定める取扱規程等を策定しなければならない。</td><td>○特定個人情報等の取扱い等を明確化する。
○事務取扱担当者が変更となった場合、確実な引継ぎを行い、責任ある立場の者が確認する。
→業務マニュアル、業務フロー図、チェックリスト等に、マイナンバーの取扱いを加えることも考えられます。</td></tr>
<tr><td colspan="2">C 組織的安全管理措置
事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。</td></tr>
<tr><td>a　組織体制の整備
安全管理措置を講ずるための組織体制を整備する。</td><td>○事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分することが望ましい。
→けん制効果が期待できる方法です。</td></tr>
<tr><td>b　取扱規程等に基づく運用
取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。</td><td rowspan="2">○特定個人情報等の取扱状況の分かる記録を保存する。
→例えば、次のような方法が考えられます。
・業務日誌等において、特定個人情報等の入手・廃棄、源泉 徴収票の作成日、本人への交付日、税務署への提出日等の、特定個人情報等の取扱い状況等を記録する。
・取扱規程、事務リスト等に基づくチェックリストを利用し て事務を行い、その記入済みのチェックリストを保存する</td></tr>
<tr><td>c　取扱状況を確認する手段の整備
特定個人情報ファイルの取扱状況を確認するための手段を整備する。
なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。</td></tr>
<tr><td>d　情報漏えい等事案に対応する体制の整備
情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。
情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。</td><td>○情報漏えい等の事案の発生等に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認しておく。
→業務遂行の基本、「ほうれんそう」（報告・連絡・相談） を確認しましょう。</td></tr>
<tr><td>e　取扱状況の把握及び安全管理措置の見直し
特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む。</td><td>○責任ある立場の者が、特定個人情報等の取扱状況について、定期的に点検を行う。
→事業者のリスクを減らすための方策です。</td></tr>
</table>

<table>
<tr><td colspan="2">D　人的安全管理措置
事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。</td></tr>
<tr><td>a　事務取扱担当者の監督
事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。</td><td rowspan="2">同左
→従業員の監督・教育は、事業者の基本です。従業員にマイナンバー４箇条を徹底しましょう。</td></tr>
<tr><td>b 事務取扱担当者の教育
事業者は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。</td></tr>
<tr><td colspan="2">E　物理的安全管理措置
事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。</td></tr>
<tr><td>a　特定個人情報等を取り扱う区域の管理
特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。</td><td>同左
→事業者の規模及び特定個人情報等を取り扱う事務の特性等 によりますが、例えば、壁又は間仕切り等の設置及び覗き見されない場所等の座席配置の工夫等が考えられます。</td></tr>
<tr><td>b　機器及び電子媒体等の盗難等の防止
管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。</td><td>同左
→事業者の規模及び特定個人情報等を取り扱う事務の特性等 によりますが、例えば、書類等を盗まれないように書庫等の カギを閉める等が考えられます。</td></tr>
<tr><td>c　電子媒体等を持ち出す場合の漏えい等の防止
特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる。
「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。</td><td>〇特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
→置き忘れ等にも気を付けましょう。</td></tr>
<tr><td>d　個人番号の削除、機器及び電子媒体等の廃棄
個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。</td><td>〇特定個人情報等を削除・廃棄したことを、責任ある立場の者が確認する。
→事業者のリスクを減らすために大切です。</td></tr>
<tr><td colspan="2">F　技術的安全管理措置
事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。</td></tr>
</table>

a　アクセス制御 情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。	○特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。 ○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、情報システムを取り扱う事務取扱担当者を限定することが望ましい。 →担当者以外の者に勝手に見られないようにしましょう。
b アクセス者の識別と認証 特定個人情報等を取り扱う情報システムは、事務取扱担当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する。	
c 外部からの不正アクセス等の防止 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、適切に運用する。	同左 →インターネットにつながっているパソコンで作業を行う場 合の対策です。例えば、次のような方法が考えられます。 ・ウイルス対策ソフトウェア等を導入する。 ・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 等の活用により、ソフトウェア等を最新状態にする。
d　情報漏えい等の防止 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。	同左 →インターネットにつながっているパソコンで作業を行う場 合の対策です。例えば、データの暗号化又はパスワードによる保護等が考えられます。

（4）個人情報取扱規程の策定・改訂

上記（3）のとおり、委員会ガイドラインにおいては、安全管理措置に関して、番号法ガイドラインと同様の「講ずべき項目」と「手法例」が示される模様です。

したがって、マイナンバー対応の際策定した「取扱規程等」と同様の個人情報取扱規程を（これまで個人情報取扱事業者でなく個人情報取扱規程がない事業者については）新たに策定するか又は（既に個人情報取扱規程を策定している事業者については）それを改訂する必要があります。