PIMS研究レポート™

サンプル号　2015.06

CONTENTS

特集：マイナンバー制度とプライバシーマーク（201502 号特集より）

マイナンバー制度は、行政を効率化し、国民の利便性を高め、公平かつ公正な社会を実現する社会基盤とするために考えられた制度です。

プライバシーマーク制度を主管する一般財団法人日本情報経済社会推進協会（JIPDEC）は、「番号法施行に併せて、地方公共団体が実施する特定個人情報保護評価実施の支援、民間企業・団体での実務におけるマイナンバー対応のための情報提供」というマイナンバー対応支援を行っています。

主に、地方公共団体向けの PIA（個人情報保護評価）関連事業に力を入れていた JIPDEC でしたが、昨年「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）」が発表された後、民間事業者を対象とするセミナーの開催も積極的に実施しています。2015 年 1 月に実施されたセミナー「マイナンバー事業者ガイドラインから読むこれからの個人情報保護」において JIPDEC 電子情報利活用研究部　部長　マイナンバー対応プロジェクト室主席研究員坂下　哲也氏は*「政府も、「既にプライバシーマークを取得している情報保有機関については、情報保護評価書にその旨を記述することで、個人情報保護に対して適切な体制を採っていることを宣言することができる」（平成 25 年度中間整理など）としている」*と説明しています。

このように説明するということは、今後、プライバシーマークの審査においても、「マイナンバー事業者ガイドライン」に準じた体制・規程等の整備がなされていることを確認する可能性が十分あることを示していると思われます。

法的解釈を審査員が行うことは考えにくいですから、基本的に審査で確認されるのは、「特定」「リスク評価」「対策」「方針・取扱規程の整備」「委託先監督」「取扱者への教育」となるでしょう。

これらのルールは、現在の個人情報保護関連規程に盛り込むこともできますが、個人情報保護法の改正やマイナンバー制度が今後拡張されていくことや、ガイドラインが変更されていくことも鑑みて、個別にルールを作成することを当社ではお薦めしています。

○JIPDEC　坂下氏セミナー「民間事業者におけるマイナンバー対応」
http://www.jipdec.or.jp/project/mynumber_support/20150114-03.html
○JIPDEC　マイナンバーセミナー講演レポート
http://www.jipdec.or.jp/project/mynumber_support/report.html

特集：個人情報保護法改正案概要解説（201502 号特集より）

パーソナルデータの利活用に関する検討会が続けられ、何度もパブリックコメントが実施されましたが、論点が二転三転しながらついに 2015 年 3 月、個人情報保護法改正案が国会に提出されました。この個人情報保護法改正案の概要について解説します。

個人情報保護法改正案の改正ポイント

公表された資料によると個人情報保護法の改正のポイントは以下の通りとなっています。このポイントの中から重要な点について解説していきます。

＜個人情報保護法の改正のポイント＞
個人情報の定義の明確化 個人情報の定義の明確化、要配慮個人情報
適切な規律の下で個人情報等の有用性を確保 匿名加工情報の規定・個人情報保護指針関連規定
個人情報の保護を強化 トレーサビリティの確保、個人情報データベース提供罪の新設
個人情報保護委員会の新設及びその権限
個人情報の取扱いのグローバル化 国境を越えた適用等、外国にある第三者への個人データの提供に関する規定
その他改正事項 本人同意を得ない第三者提供厳格化、利用目的の変更を可能とする範囲、小規模取扱事業者への対応

個人情報の定義の明確化

パーソナルデータの利活用に関する検討会の中でも、「個人情報」をどのように定義づけするかは大きな課題でした。中でも非特定識別情報（どの個人かは特定できないが、ある一人の人物の情報であることが識別できる情報）の取扱について、議論されました。

今回の改正案の中では、同法が対象とする個人情報は、下記のように特定の個人が識別できる情報であることが明記されました。

個人識別符号に関しては、この内容がそのまま個人情報となるわけではなく、「政令」を待たなくてはなりませんが、個人識別符号が個人情報となることで、個人情報の範囲が拡大すると考える事業者はまずは、現状の把握をしておくことが重要になってくるでしょう。

第二条
この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
一当該情報に含まれる氏名、生年月日その他の記述等（略）により***特定の個人を識別することができる***もの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
二***個人識別符号が含まれるもの***
２ この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、***政令で定めるもの***をいう。
一特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該***特定の個人を識別***することができるもの
二個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、***特定の利用者若しくは購入者又は発行を受ける者を識別する***ことができるもの

また、要配慮個人情報が定義されます。

第二条
３ この法律において「要配慮個人情報」とは、**本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等**が含まれる個人情報をいう。

要配慮個人情報については、収集の制限（あらかじめの本人の同意）、第三者提供の制限（同意のない第三者提供の禁止）などが定められました。

要配慮個人情報は、JISQ15001 の特定の機微な個人情報（･思想，信条又は宗教に関する事項/人種，民族，門地，本籍地（所在都道府県に関する情報を除く。），身体・精神障害，犯罪歴その他社会的差別の原因となる事項/勤労者の団結権，団体交渉その他団体行動の行為に関する事項/集団示威行為への参加，請願権の行使その他の政治的権利の行使に関する事項/保健医療又は性生活に関する事項）とは異なった内容であることにも留意します。

適切な規律の下で個人情報等の有用性を確保

今回の法案では、同意なき第三者提供を行える情報として、匿名加工情報が規定されます。どのように加工すれば匿名加工情報として認められるのかについては、個人情報保護委員会が定める基準に基づくとなっていますので、不明瞭のままとなっていますが、取扱いのルールについては以下のようになっています。

（１） 加工の基準は個人情報保護委員会規則で定める

（２） 匿名加工情報を作成する場合、第三者提供する場合には個人情報保護委員会規則が定めた通り公表すること
（３） 削除した記述・加工の方法は漏えい防止すること
（４） 提供する場合には、提供先に匿名加工情報であることを明示すること。
（５） 匿名加工情報を受け取った側は、本人を識別するための以下の行為を禁止
- 作成者が削除した記述等や加工方法を取得すること
- 他の情報と照合

個人情報保護の強化

個人情報保護の強化において、今後事業者に負担になりそうなものは「トレーサビリティの確保」です。この規定は個人データの第三者提供を行う際に記録を保持することを求めるものです。プライバシーマーク取得事業者では、現在でも個人データ等の受け渡しについては記録を保持することになっているかと思いますが、法律で保管義務が定められますので、記録保持方法等については再度ルールを見直す必要が出てくる事業者もあるでしょう。

個人データの提供を受ける事業者についても、取得の経緯等を確認することが定められます。

（第三者提供に係る記録の作成等）
第二十五条個人情報取扱事業者は、個人データを第三者（第二条第五項各号に掲げる者を除く。以下この条及び次条において同じ。）に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第二十三条第一項各号又は第五項各号のいずれか（前条の規定による個人データの提供にあっては、第二十三条第一項各号のいずれか）に該当する場合は、この限りでない。
２ 個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。
（第三者提供を受ける際の確認等）
第二十六条個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第二十三条第一項各号又は第五項各号のいずれかに該当する場合は、この限りでない。
一当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名
二当該第三者による当該個人データの取得の経緯

> 2 前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。

もう一点、大きな変更は「個人情報データベース提供罪の新設」です。これにより個人情報データベース等を取扱う事務に従事する者または従事していた者が、その業務に関して取扱った個人情報データベース等を不正な利益を図る目的で提供し、又は盗用する行為を処罰対象としました。事業者に対する罰則しかなかった個人情報保護法でしたが、不正な行為を行った個人に対しても罰則が作られたのは画期的な変更といえるでしょう。

個人情報保護委員会の新設及びその権限

個人情報保護法の改正の中で制度的に大きく変更される点は、個人情報保護委員会の新設です。新設といっても実際には、現在の特定個人情報保護委員会を改組する予定となっています。

個人情報保護委員会の主な役割は以下の通りです。

- 個人情報及び匿名加工情報の取扱いに関する監督等の権限
- 個人情報保護団体の認定等
- 法律で定められた事務及び基準等の作成

現行では主務大臣が果たす役割よりも大きく個人情報保護委員会は、事業者への立ち入り検査権限が認められています。

認定個人情報保護団体が個人情報保護指針を作成する場合には、消費者の意見を代表する者の意見を聞くように努め、個人情報保護委員会に届出なければならないこととするとともに、個人情報保護指針の変更等も命じることができます。

個人情報の取扱のグローバル化

直接、国内の事業者に関係するものとしては、海外へのデータ移転についての規定の追加です。この改定案のまま成立した場合には、海外の事業者に委託している場合や海外にサーバがあるクラウドサービスの利用においても「本人同意」が必要になる場合があるので留意しておく必要があります。

> （外国にある第三者への提供の制限）
> 第二十四条個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

その他改正事項

その他の改正事項として、下記のようなものがあります。

- 本人同意を得ない第三者提供厳格化
  本人同意を得ない第三者提供を行う場合には、個人情報保護委員会への届出が必要
- 利用目的の変更を可能とする範囲の変更
  「利用目的の変更」に関しては「変更前の利用目的と相当の関連性を有する」から「変更前の利用目的と関連性を有する」となり、「相当の」が削除されます。
- 小規模事業者も個人情報取扱事業者
  小規模事業者に対する除外がなされなくなります。

今後の対応について

実際には、現在はまだ法案の段階ですので、成立するまでは、まだどのようになるか明言できません。また、現状の法案は、「個人情報保護委員会規則」で定めることが多く含まれているため、これだけでは規制の詳細までは分からない状況です。

今回の法案を紐解いてみると、昨年起きた大規模漏えい事故の影響を大きく受け、また海外に対し日本の個人情報保護が十分であることを示すための委員会制度が発足されていることや、事業分野ごとの個人情報保護ガイドラインがなくなることにより特定個人情報保護団体の役割が大きくなる方向性が見えてきています。

これらの背景を念頭に今後の個人情報保護への取り組みを考えておくことは決して無駄にならないのではないかと思われます。

○第 189 回通常国会　提出法案　個人情報保護法改正案等
http://www.cas.go.jp/jp/houan/189.html

201502 号より

プライバシーマーク一問一答

PIMS 研究 WEB のデータベースの一部をご紹介するコーナーです。
「プライバシーマーク一問一答」で回答して欲しい質問を募集しています。PIMS 研究 WEB のご意見・ご要望コーナーより投稿してください。（質問は、当社で再編集し、PIMS 研究レポート、PIMS 研究 web 等に掲載させていただきます）

質問

当社にはシステム管理者が１名しかおらずすべてをまかせきりの状態です。

プライバシーマークの審査においては、最近の大規模な個人データの漏えい事故等により、システム管理者の内部不正対策について確認をされるのではないかと考えています。

当社のような場合には、外部の第三者等の監査を受けるなどの対応を求められるのでしょうか？

回答

昨年の大規模な事故が発端となり、さまざまな情報セキュリティに関する情報提供が行われたり、各省庁ガイドラインが改正されたりしています。

プライバシーマーク事業者に対しては、マネジメントシステムを通じ、このような社会環境をキャッチし、自社の対策の見直し、ルールの見直しにつなげることが期待されています。

そういう意味で、システム管理者が一人しかいないことに対して、新たなリスク認識を持つことができたということ自体が、マネジメントシステムの運用が行われているひとつのエビデンスとなります。まずは、リスク認識が一番大事なことですので、リスク欄に記載しておきましょう。

次にリスクの詳細について考えてみます。

一般的に、管理者が１名しかいないケースでリスクとなりうるのは「内部犯行による情報漏えい」のみとは限りません。管理者が「退職」「怪我・病気・その他の事由での長期休暇」「業務の怠慢」「別業務で多忙で対応不可能になる」などの非常事態が起きた場合に、システム管理業務が不十分になったり、緊急対応が不可能となったりする可能性のほうが、内部犯行よりもリスクが大きい場合も幹がられます。これは、個人情報の漏えい問題にとどまらず、会社の事業継続上のリスクとして捉えるべき問題です。プライバシーマークの審査とは直接関係ないかもしれませんが、大きな問題が発生することが予想されるようでしたら、何らかの対策を講じる必要があるでしょう。これらのリスクに対応する方法として

は、担当者の二重化、マニュアル作成や、業務の一部を外注するなどがあり得ます。

プライバシーマークで意識すべき「内部犯行」に対する対策は、さまざまなものが考えられます。こちらも、通常のリスクに対する対策と同じく個人情報の内容や重要性、事故が起きた際の事業への影響等、係るコストなどから総合的に判断してください。以下に、対策例を記載します。

＜内部不正対策（例）＞※組み合わせも可能

- 外部のシステム監査会社に依頼し、定期的にシステム面のチェックする体制を組む
- システム管理者の操作ログを取り、異常がないか点検している。
- システム管理者の管理者権限の ID/パスワードは、通常業務のものと分けて、管理者権限の使用のログを取り、点検する。作業記録を作成させ、マッチングする。
- システム管理者が、管理者権限を使う際には、二人以上での作業とするという運用にする。（この場合には、作業記録と管理者権限使用ログとマッチングすることで、異常を早く発見できます）
- システム管理者の手順書を作成し、そのように作業させる。
- システム管理者の役割・責任・禁止事項等を明確化し、誓約書を作成する。

内部犯行への対策には下記の「組織における内部不正防止ガイドライン 第 3 版（2015 年 3 月改訂）」が参考になります。

https://www.ipa.go.jp/security/insider/index.html

対策をすぐに講じることができない場合には、「残存リスク」として管理することも選択できます。これは、システム管理者が何らかの問題で不在となってしまう場合のリスクに対しても同様です。

TOPICS

個人情報取り扱いに関する事件・事故情報、JIPDEC 情報、官公庁情報、セキュリティ情報などマネジメントレビューに役立つ情報を掲載しています。

【201502 号に掲載した情報リスト】

- 【経済産業省】個人情報保護法に基づいた報告の求めを実施
- 【官公庁】所轄分野ガイドラインの改正が進む
- 【総務省】電気通信事業ガイドライン等　改正案　意見募集開始
- 【金融庁】金融分野ガイドライン及び実務指針の改正案　意見募集開始
- 【法務省】債権管理回収業分野ガイドラインの改正案　意見募集開始
- 【外務省】外務省所管事業分野ガイドラインの改正案　意見募集開始
- 【農林水産省】農林水産分野ガイドラインの改正案　意見募集開始
- 【経団連】マイナンバー制度への対応準備のお願い
- 【JIPEC】「企業 IT 利活用動向調査 2015」の速報結果を発表
- 【JIPEC】個人情報に関する意識調査を実施し、結果を発表
- 【JIPDEC】「個人情報の適正な取得等について(解説)」の公表について
- 【IPA】Windows Server 2003 のサポート終了に関する注意喚起発表
- 【IPA】情報セキュリティ啓発映像の新作を公開
- 【IPA】IPA テクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」
- 【IPA】情報セキュリティ 10 大脅威 2015　解説資料掲載
- 【IPA】安全なウェブサイトの作り方改訂第 7 版を発表
- 【IPA】組織における内部不正防止ガイドライン　第三版発表
- 【IPA】 ネットワーク対応機器を利用する際のセキュリティ上の注意点
- 【IPA】クラウドサービスに入力した内容の意図しない情報漏えいに注意を発表
- 【IPA】「2014 年度情報セキュリティに対する意識調査」報告書について
- 【事件・事故】株主会員サービスから情報漏えい
- 【事件・事故】ゴルフリゾート運営企業不正アクセスで顧客情報が漏えい
- 【事件・事故】新たにクレジットカード情報の漏えい
- 【事件・事故】オンラインショップでカード情報の漏えい
- 【事件・事故】コールセンター元契約社員より情報持ち出しが発覚
- 【プライバシーマーク取得者数】

PIMS 研究レポートとは？

年間４回　郵送でプライバシーマーク取得事業者に役立つ情報お届けします！

マネジメントシステムの PDCA を踏まえた毎号１～４の特集記事のほか、プライバシーマーク一問一答、官公庁・事故情報等のトピックなど最新情報をお届けしています。

過去の特集

号数	特集内容
201502	特集１：2015 年度に見直したいポイント ～内部犯行対策及び委託先の監督を見直そう～ 特集２：マイナンバー制度とプライバシーマーク 特集３：個人情報保護法改正案概要解説
201501	特集１：経済産業分野ガイドラインの改正 特集２：営業秘密指針から学ぶ「人的管理」
201404	特集１：マネジメントレビュー・インプット情報：2014 年 特集２：事業者による番号法への対応準備～「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）（案）」
201403	特集１：漏えい事件から学ぶ「点検」ポイント 特集２：会見から考える記者会見の教訓
201402	特集１：2014 年度に見直したいリスク対策
201401	特集１：ISO の視点で見た「個人情報保護教育」 特集２：個人情報保護に関する制度の見直し パーソナルデータ利活用に関する制度見直し方針概要 特集３：JIPDEC から発表「(スマートフォン等のアプリケーション配信事業者対象）利用者情報の取扱い、アプリケーション・プライバシーポリシーについて」を考える プライバシーマーク一問一答：従業者のパーソナルクラウドの利用について
201304	特集１：２０１３年個人情報保護関連動向 特集２：マネジメントレビュー･インプット情報 特集３：ISMS 規格 ISO27001 の改訂ポイント 特集４：マネジメントレビュー前に事務局業務の総点検を
201303	特集１：現場の意識向上を図る点検（監査）の視点 特集２：今すぐ見直したい web セキュリティ 特集３：パーソナルデータ利用・流通に関する研究会報告書が発表
201302	特集１：２０１３年度に見直したいリスク対策
201301	特集１：個人情報保護教育、今だからやりたい見直しの視点 特集２：これだけは伝えたい「新人教育」 特集３：教育につかえる資料集

PIMS 研究とは？

マイナンバー制度対策、個人情報保護法制度の改訂に続く JISQ15001 の改正など個人情報保護事務局が対面する課題解決のための情報をお届けするサービスです。

費用は？

年間　38,000 円（初年度のみ登録手数料＋2,000 円）※消費税別

サービス概要

PIMS研究レポート	PIMS研究セミナー	PIMS研究WEB
・年4回最新情報を郵送でお届け ・自社のPIMSの見直しに役立ち、マネジメントレビューで活用できる情報をご提供します ・法・ガイドラインの解説や実務的な対応方法も解説	・年4回　東京で開催 ・法・ガイドライン対応やPIMSの運用課題をテーマにしたセミナーをお届けします。 ・事務局に新たになった方から、ベテランまでに幅広く参加いただけるセミナーです。	・過去のレポート、セミナーがダウンロード可能 ・プライバシーマーク取得事業者のあるあるに一問一答でお答えします。

お申込みは下記の URL から WEB で受け付けています。

http://www.cpdc.co.jp/pims

株式会社シーピーデザインコンサルティングとは？

シーピーデザインコンサルティングは、大日本印刷株式会社の社内ベンチャー制度により 2002 年 4 月に設立された会社です。これまでのプライバシーマーク取得、運用、更新に関するコンサルティングの経験のみならず DNP グループ内での運用情報も踏まえた実践的な情報提供を行います。

代表取締役社長　鈴木靖　プロフィール

（財）日本規格協会 JISQ15001「個人情報保護に関するマネジメントシステム-要求事項」改正原案作成委員会　委員

平成 18 年～　経済産業分野における個人情報保護ガイドライン改正検討委員会　作業部会委員

発行日：2015 年 6 月 11 日
発行：株式会社　シーピーデザインコンサルティング
〒141-8001　東京都品川区西五反田 3-5-20　DNP 五反田ビル
http://www.cpdc.co.jp