マイナンバー制度で必要な安全管理措置
―特定個人情報保護に関するガイドラインの動向―

マイナンバー制度では、特定個人情報（特定の個人を識別できる情報）を扱うことから、これまでの機密情報管理よりも高いセキュリティレベルが求められる。本稿では、特定個人情報保護に関する各種ガイドラインの動向を概観し、高レベルの安全管理措置に必要なポイントについて考察する。

野村総合研究所 金融ITイノベーション事業本部
金融システムリスク管理部長
堤（つつみ）　順（じゅん）
専門はリスクマネジメント全般、ITガバナンスの構築・運営

求められる安全管理措置

「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」（以下、番号法）に基づいてマイナンバーの利用が2016年1月に始まるのを前に、金融機関および事業会社では準備を急がなければならない時期に入っている。

内閣府の特定個人情報保護委員会は、金融機関および事業会社が特定個人情報を適切に取り扱うための具体的な指針を定めた「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）」（以下、「特定個人情報保護ガイドライン」）を2014年12月に公表した。

「特定個人情報保護ガイドライン」はその第1ページに「本ガイドラインの中で、「しなければならない」及び「してはならない」と記述している事項については、これらに従わなかった場合、法令違反と判断される可能性がある」とし、「「望ましい」と記述している事項については、これに従わなかったことをもって直ちに法令違反と判断されることはないが、番号法の趣旨を踏まえ、事業者の特性や規模に応じ可能な限り対応することが望まれるものである」としている。

そして「各論」とされた部分で「個人番号利用事務実施者である事業者は、個人番号及び特定個人情報の漏えい、滅失又は毀損の防止等、特定個人情報管理のために、必要かつ適切な安全管理措置を講じなければならない」（一部略）とし、「別添」の部分で安全管理措置の記述に多くのページを割いている。

「講ずべき安全管理措置の内容」には、基本方針の策定と取扱規程の策定に続けて、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、技術的安全管理措置の4つを挙げている（表1参照）。ここではこの4つの措置について触れる。

講ずべき措置の内容は、手法の例までを示した具体的なものとなっている。例えば人的安全管理措置では、「秘密保持に関する事項を就業規則に盛り込むこと」などが示され、物理的安全管理措置の「特定個人情報等を取り扱う区域の管理」では、「ICカード、ナンバーキー等による入退室管理システムの設置等」「壁又は間仕切り等の設置及び座席配置

表1 「特定個人情報保護ガイドライン」に示された4つの安全管理措置

組織的安全管理措置	組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、情報漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直し
人的安全管理措置	事務取扱担当者の監督、事務取扱担当者の教育
物理的安全管理措置	特定個人情報等を取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち出す場合の漏えい等の防止、個人番号の削除、機器及び電子媒体等の廃棄
技術的安全管理措置	アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報漏えい等の防止

の工夫等」などの手法が例示されている。また「機器及び電子媒体等の盗難等の防止」の方法としては「特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等」などと記されている。技術的安全管理措置の「情報漏えい等の防止」については、「通信経路の暗号化」や「データの暗号化又はパスワードによる保護等」などが挙げられている。

このように、「特定個人情報保護ガイドライン」は具体的な方策を立てやすいものになっている。

金融機関向けガイドラインの動向

2014年12月には、経済産業省により、「個人情報の保護に関する法律」（個人情報保護法）についての経済産業分野を対象とするガイドラインが改訂された。これを受け、金融庁も個人情報保護の新しいガイドラインを告示することが予想される。消費者庁からはガイドライン共通化の考え方が示されているため、経済産業省のガイドラインと金融庁のガイドラインの内容は、ある程度共通化されたものになるであろう。

経済産業省のガイドラインを見ると、「特定個人情報保護ガイドライン」と同様、4つの安全管理措置（組織的、人的、物理的、技術的）が例示とともに記載されている。両者の構成は同じではあるが、例示については、経済産業省のガイドライン改訂が実際のセキュリティ事案を受けての対応ということもあり、過去のセキュリティ事案に基づいた部分については、より具体的な例示が含まれている。

例えば、「個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）」と書かれている。過去の事案に基づき、スマートフォンという具体的な機器の種類まで示されていることが、そのあたりの事情をよく示している。

前述のように、経済産業省のガイドラインと「特定個人情報保護ガイドライン」は構成がほぼ同じであるため、双方の例示を合わせた形で社内の安全管理措置を講じるのが分かりやすい方法であろう。

ただし両者には大きく違う点もある。経済産業省のガイドラインでは「個人情報を取り

扱う作業責任者を明確にする」としているのに対して、「特定個人情報保護ガイドライン」では「特定個人情報を取り扱う人を個々人まで把握・管理していること」を求めている。これは、仮に特定個人情報が漏えいした際に、原因や経緯の調査をより厳格にできるようにしなければならないからであろう。

2015年1月には、FISC（金融情報システムセンター）より、「金融機関等コンピュータシステムの安全対策基準・解説書」（FISC安全対策基準）の改訂案が示された。また、同年2月には、金融庁より「主要行等向け総合的な監督指針」および「金融検査マニュアル」の情報システムに関連する改訂案も公表されている。それぞれ、昨今のセキュリティ事案への対応、サイバー攻撃に関する国際的な動き、クラウドサービスという新しい技術・契約形態に関連した改訂となっている。これらのガイドラインに共通するのは、態勢の整備、運用の徹底、モニタリング、改善という、いわゆるPDCAの対象を従業員のみならず外部委託先（2次委託先以降を含む）にまで広げることを求めている点である。

以上、各種のガイドラインの動向について示したのは、マイナンバー制度の施行に合わせて、情報漏えいなどへの備えについて全体的に見直す必要があるからである。

特定個人情報保護と委託先管理

特定個人情報を取り扱う業務で求められる安全管理措置は、企業内で行われる業務だけでなく、外部委託先の業務にも区別なく当てはまる。従って、企業内の各組織に業務の責任を持たせるのと同様に、外部委託先にも業務の責任を持たせ、適切で十分な安全管理措置を実施させ、それをモニタリングしなければならない。

外部委託先管理を社内部署（役職員）の管理と比較すれば、外部委託先との間でサービス水準を定義するSLAの締結が、部署の業務の責任を明確にする業務分掌に相当する。そのSLAに安全管理措置を盛り込む必要がある。その上で、外部委託先で設計・実装する安全管理措置が、リスクに鑑みて適切であるかを確認する必要がある。そのために、社内部署に自己点検させるのと同様に、外部委託先には内部監査の実施を求める。その際には、委託元の内部監査部門がそれを行えるように契約書に盛り込むべきである。

このように、委託先の管理では、企業内の安全管理措置と比較してポイントを洗い出し、それを委託先選定時の評価ポイントとすること、委託元のポリシーを順守させるために必要な条項を契約書に盛り込むこと、委託を開始した後は継続的にモニタリングすることが必要である。

「特定個人情報保護ガイドライン」の別冊として、金融機関向けに「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」も公表されている。この中で、特定個人情報の利用制限、提供制限などとともに、金融機関が業務委託を行う際に必要な安全管理措置について記載されている。

具体的な安全管理措置については「特定個人情報保護ガイドライン」を参照するよう求めているが、これに加えて、すでに述べた委託先の選定、SLAの締結、取り扱い状況のモ

ニタリングを「必要かつ適切な監督」とし、金融機関は委託先の監督を行わなければならないと定めている。さらに、「再委託（2次委託以降を含む）については委託元の金融機関に許諾を得た場合のみ許す」とあるので、特定個人情報を取り扱う業務を委託先が再委託することがあるかどうか、委託元の金融機関は十分に注意する必要がある。

継続的・横断的な安全管理措置の態勢づくりが必要

「特定個人情報保護ガイドライン」および経済産業省のガイドラインの安全管理措置は、例示を多くし、非常に分かりやすくまとまっている。しかしそれだけに、そこに示された安全管理措置さえ守っていればよいという誤解が生じやすい面もある。例示が分かりやすいのは、昨今の事案に即した具体的な方策が記載されているからである。しかし、それらは過去に発生した事案への対応にほかならず、新たなリスクへの備えは例示することが難しい。

また、情報セキュリティに関してJISやISOなどによって規定されている「機密性」「完全性」「可用性」の維持という観点で見れば、2つのガイドラインとも「機密性」が中心になっている。これもまた、過去に発生した事案に着眼しているからである。仮に、将来的に「完全性」に問題が発生し（例えばマイナンバーが本人と正しくひも付けられないようなケース）、何らかの被害が出た場合には、「完全性」に関連する事例が安全管理措置に追加されることになるであろう。

リスクマネジメントのポイント

それでは、マイナンバー制度で企業に求められるリスクマネジメントは何がポイントになるだろうか。それは特定個人情報保護に限らず全てのリスクマネジメントに共通していることではあるが、リスクマネジメントは経営がその役割を全うするために欠かせない道具であり、その道具を継続的に機能させるための態勢づくりは経営の責任であることを再認識する必要があるという点だ。具体的には、以下のようなPDCAサイクルの態勢を整備することが求められる。

①社内および他社における“ヒヤリハット”事案の情報を収集する態勢
②収集した情報を分析する態勢
③分析の結果を受けて自社の対応を検討する態勢
④その対応内容を社内に伝達する態勢
⑤対応が確実に遂行されているかをモニタリングする態勢

経営は、このようなリスクマネジメントのPDCAサイクルが適切に機能していることを利害関係者に説明しなければならない。従って、上記の態勢に説明責任能力を組み込むことも必要である。

経営は、「特定個人情報保護について自社の安全管理措置は十分か」と問うよりは、「自社は安全管理措置が十分であり続けるための態勢を確保できたか」と問うべきである。そして業務委託をするのであれば、経営が委託元の管理態勢をモニタリングでき、直接議論することができる委託先を選ぶことが大切であろう。■