個人情報の保護に関する実態調査
結果に基づく勧告

平成 28 年 7 月

総　　務　　省

前　書　き

ＩＴを活用した個人情報の取扱いの拡大等は、多様化する行政需要に対応した行政サービスの向上や行政運営の効率化に大きく寄与しているが、その一方で、個人情報の処理の特性（大量・高速処理等）から個人の権利利益の侵害のおそれが指摘されている。平成15年5月、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号。以下「行政機関個人情報保護法」という。）及び独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号。以下「独法等個人情報保護法」という。）は、このようなＩＴ社会に対する権利利益の侵害等のおそれに対応するため制定され、17年4月から施行された。

行政機関個人情報保護法及び独法等個人情報保護法では、行政機関の長及び独立行政法人等は、保有個人情報の漏えい等の防止等のために必要な措置を講ずることとされ、これを受け、総務省行政管理局では、保有個人情報の適切な管理のために講ずべき措置として最小限のものを示した「行政機関の保有する個人情報の適切な管理のための措置に関する指針」（平成16年9月14日総務省行政管理局長通知。以下「行政機関指針」という。）及び「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針」（平成16年9月14日総務省行政管理局長通知。以下「独法等指針」という。）を各機関に通知し、行政機関及び独立行政法人等は、これらを踏まえ、個人情報の適切な管理に関する定めを整備し、個人情報の適切な管理に必要な措置の徹底を図ってきたところである。

しかしながら、法施行後10年以上経過しているものの、平成26年度には、行政機関で696件、独立行政法人等で1,377件の漏えい等事案が発生し、平成27年5月には、日本年金機構において約125万件の個人情報流出事案が発生している。

この実態調査は、以上のような状況を踏まえ、個人情報の管理に関する国民の不安の解消を図るとともに、個人情報の適切な管理のための取組を促進させる観点から、行政機関及び独立行政法人等における個人情報の管理の状況について、その実態を把握し、関係行政の改善に資するために実施したものである。

目　　次

1　行政機関、独立行政法人等における個人情報の管理に関する制度の概要

(1)　行政機関における個人情報の管理に関する制度

行政機関の保有する個人情報の取扱いについては、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号。以下「行政機関個人情報保護法」という。）により規律されている。

行政機関個人情報保護法では、行政機関の長は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならないこととされている（第6条）。

これに関し、個人情報の保護に関する法律（平成15年法律第57号）第7条に基づく「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定。以下「基本方針」という。）において、行政機関個人情報保護法の適切な運用のため、総務省は、「行政機関の保有する個人情報の適切な管理のための措置に関する指針」（平成16年9月14日総務省行政管理局長通知。以下「行政機関指針」という。）を策定するとともに、各行政機関は、行政機関指針等を参考に、その保有する個人情報の取扱いの実情に即した個人情報の適切な管理に関する定め（以下「保護管理規程」という。）等を整備することとされている。

(2)　独立行政法人等における個人情報の管理に関する制度

独立行政法人、国立大学法人、大学共同利用機関法人、特殊法人（独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号。以下「独法等個人情報保護法」という。）の対象法人に限る。）及び日本司法支援センター（以下これらを総称して「独立行政法人等」という。）の個人情報の取扱いについては、独法等個人情報保護法により規律されている。

独法等個人情報保護法では、独立行政法人等は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならないこととされている（第7条）。

これに関し、基本方針において、独法等個人情報保護法の適切な運用のため、総務省は、「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針」（平成16年9月14日総務省行政管理局長通知。以下「独法等指針」という。）を策定するとともに、各独立行政法人等は、独法

等指針等を参考に、その保有する個人情報の取扱いの実情に即した保護管理規程等を整備することとされている。

2　個人情報の保護に関する規程及び体制の整備状況

(1)　保護管理規程の見直し（改正）

総務省は、日本年金機構の個人情報流出事案を受け、平成27年8月、行政機関指針及び独法等指針について、ⅰ）初期対応に係る対策強化、ⅱ）現場における安全管理措置の徹底を内容とする改正を行うとともに、行政機関、独立行政法人等に対し平成27年中を目途に、行政機関にあっては行政機関指針を、独立行政法人等にあっては独法等指針を参考に、その保有する個人情報の取扱いの実情に即した保護管理規程の見直し（改正）を依頼している。

これらを受け、行政機関45機関中44機関(97.8%)、独立行政法人等201機関中194機関（96.5%）は、平成27年度中に保護管理規程の見直し（改正）を行い、残りの行政機関1機関、独立行政法人等7機関は、平成28年5月までに見直し（改正）を行っている。

また、保護管理規程等の見直し（改正）内容についてみると、日本年金機構の個人情報流出事案を受けて行政機関指針又は独法等指針に盛り込まれた①保護管理者とシステム管理者との連携（行政機関指針第2-2、独法等指針第2-2)、②保護管理者等現場責任者への研修(行政機関指針第3-3、独法等指針第3-3)、③複製等の最小限化、処理後の消去（行政機関指針第6-9、独法等指針第6-9)、④暗号化(パスワード設定)(行政機関指針第6-10、独法等指針第6-10)、⑤被害拡大防止措置（行政機関指針第9-2、独法等指針第9-2)、⑥独立行政法人等から所管行政機関への速やかな情報提供（独法等指針第9-5)、⑦行政機関の所管法人への指導、助言（行政機関指針第11)、⑧独立行政法人等と所管行政機関との緊密な連携(独法等指針第11)の各項目について、行政機関及び独立行政法人等では、保護管理規程の見直し（改正）又は保護管理規程以外の規程による対応を行っている（一部は平成28年度以降に見直し（改正）予定)。

これらの中には、保護管理規程に、①システム管理に関する役職を設け、その責務等として、保護管理者からの協議に応じて必要な措置を講ずることなどを規定しているもの、②当該機関の端末の接続状況を踏まえ、保有個人情報の漏えい等安全確保の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、ＬＡＮケーブルを抜くこと以外に無線Ｌ

ＡＮをオフにすることについて規定しているものがある。

一方、保護管理規程の適用範囲についてみると、一般に本府省庁が定めた保護管理規程が当該機関全体で適用される場合が多いが、厚生労働省は、厚生労働省保有個人情報管理規程（平成 17 年 3 月 23 日厚生労働省訓第 3 号）第 1 条において、当該規程の適用は、本省内部部局に限るとしており、施設等機関及び地方支分部局については、同保護管理規程第 58 条において、「その長が、それぞれこの訓令に準じて厚生労働審議官と協議して制定するものとする」とされ、施設等機関及び地方支分部局の各機関で保護管理規程を定めることとなっている。

厚生労働省では、施設等機関及び地方支分部局における保護管理規程の整備に当たり、①見直し（改正）例として、本省内部部局の保護管理規程を示していること、②地方厚生局（支局を含む。）には雛形、都道府県労働局には準則を示すなど、保護管理規程を的確に作成することができる措置を講じているとしている。

しかしながら、厚生労働省本省において、①雛形や準則を示していない施設等機関の所管課があること、②地方支分部局への雛形や準則の提示は、本省内部部局の保護管理規程の提示から 2 か月以上の期間を要していること、③施設等機関において保護管理規程の改正状況を確認していない例があるなど、確認・支援が不十分であることなどから、他の行政機関では、遅くとも平成 27 年度中には見直し（改正）作業を終えているにもかかわらず、厚生労働省では、189 の保護管理規程のうち、平成 28 年 4 月に見直し（改正）したものが 16 規程あるなど、他の行政機関に比べ保護管理規程の見直し（改正）作業に長期を要している。

これについて、厚生労働省は、施設等機関及び地方支分部局の数が多く、その規模や組織形態も様々であり、さらに、これらの施設等機関及び地方支分部局においては多くの個人情報を取り扱っていることから、保護管理規程を本省内部部局等と別に施設等機関、地方支分部局で定めていたとしているものの、施設等機関や地方支分部局の保護管理規程は、厚生労働省本省内部部局の保護管理規程に準じて整備しているため、本省内部部局の保護管理規程と大きな差異はないとしている。

【所見】

したがって、厚生労働省は、日々起こり得るサイバー攻撃等、個人情報漏えい等の脅威に迅速かつ的確に対応するため、組織全体の統一的なルールの下、速やかに個人情報の安全確保措置を行う観点から、個人情報の適切な管理のためのルールである保護管理規程を速やかに改正することができるよう、厚生労働省全体で保護管理規程を定める等の措置を講ずる必要がある。

(2) 管理体制の状況

ア 保護管理規程に基づく管理体制

行政機関指針及び独法等指針においては、管理体制として、①各機関における保有個人情報の管理に関する事務を総括する任に当たる総括保護管理者、②各課室等における保有個人情報の適切な管理を確保する任に当たる保護管理者、③保有個人情報の管理の状況について監査する任に当たる監査責任者を設けることとされている（行政機関指針第2、独法等指針第2）。

また、両指針では、保有個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たることとされている（行政機関指針第2-2、独法等指針第2-2）。

今回、行政機関独立行政法人等における管理体制の状況を調査したところ、全ての機関で保護管理規程により管理体制の整備を行っていた。

管理体制としてその設置が求められている上記の各役職と情報セキュリティ対策の役職との兼務状況をみると、総括保護管理者については、行政機関45機関中36機関（80.0％）、独立行政法人等201機関中113機関（56.2％）、保護管理者については、行政機関45機関中44機関（97.8％）、独立行政法人等201機関中144機関（71.6％）、監査責任者については、行政機関45機関中30機関（66.7％）、独立行政法人等201機関中76機関（37.8％）となっている。

また、保護管理者と情報システムの管理者が連携した取組として、①システム管理者が、アクセス記録を保護管理者に提供し、保護管理者が原則週に1度、自己の担当分の管理リストを確認すること、②職員が情報システム上の個人情報ファイルを複製等した場合、情報システム管理者が当該操作を検知し、当該職員が所属する部署の保護管理者に対し、複製等の処理状況について、通知メールを送付するなどの措置を講じている機関があった。

イ 漏えい等事案発生時の連絡体制及び被害拡大防止措置

行政機関指針及び独法等指針においては、安全確保上の問題となる事案又は問題となる事案の発生のおそれを認識した場合の対応について、その事案等を認識した職員から保護管理者への報告及び保護管理者から

総括保護管理者への報告を行うこととされている（行政機関指針第 9-1、9-3、独法等指針第 9-1、9-3）。

今回、各行政機関、各独立行政法人等における保有個人情報の漏えい等事案発生時の連絡体制を調査したところ、全ての機関で、漏えい等事案発生時の連絡体制を整備していた。また、情報システムから保有個人情報が漏えい又は漏えいのおそれがある場合には、夜間・休日対応、幹部への速やかな報告を行うこととなっていた。

また、漏えい等事案発生時における取組として、①インシデントレベルに応じた基本的な初動対応のマニュアルを策定している機関、②インシデント発生時の対応訓練を実践形式で行い、訓練の事後評価を行っている機関があった。

こうした連絡体制の整備に加え、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末のＬＡＮケーブルを抜くなど、被害拡大防止措置のために直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）こととされている（行政機関指針第 9-2、独法等指針第 9-2）。

今回、行政機関及び独立行政法人等における被害拡大防止のための注意喚起の実施状況について調査したところ、全ての機関でＬＡＮケーブルを抜くことなどの注意喚起が行われていた。

また、被害拡大防止のための注意喚起に関する取組として、①不審メールを受信した場合、システム管理者に通報できる機能を日常的に周知している機関、②標的型メールを開封した場合における初動対応等の訓練を実施している機関があった。

ウ　行政機関と独立行政法人等との連携等

行政機関指針においては、行政機関は、所管する独立行政法人等への指導、助言（行政機関指針第11）を、独法等指針においては、独立行政法人等は、所管する行政機関との緊密な連携（独法等指針第11）を行うこととされている。

今回、各行政機関と独立行政法人等における連携等の状況を調査したところ、日本年金機構の個人情報流出事案を受けた取組として、独立行政法人等を所管する行政機関においては、全ての機関で独立行政法人等

への指導、助言を行っており、また、独立行政法人等においても、全ての機関で、所管する行政機関からの指導、助言を受け、関係部局等に通知を発出するなど、当該独立行政法人等の保有する個人情報の適切な管理のための措置を行っていた。

行政機関から所管する独立行政法人等に対する具体的な指導、助言としては、①独立行政法人等の役職員を対象とした会議、演習等を実施、②独立行政法人等に対し点検項目を示し、点検結果の報告を励行、③漏えい等事案の総務省への報告を励行するなどの取組がみられた。

一方、内閣府では、日本年金機構の個人情報流出事案を受け、府内の各部局個人情報保護担当宛てに「個人情報を含む重要情報の適正な管理の徹底について」（平成27年6月2日付け事務連絡）を発出し、独立行政法人等の所管部局において、所管する独立行政法人等に対し、重要情報の適正な管理について、改めて、徹底を指導するよう周知したものの、当該文書について、独立行政法人等の所管部局から独立行政法人等に周知されていないなど、連絡が不十分な状況がみられた。

また、平成27年度中に保護管理規程の見直し（改正）、教育研修及び点検を実施していない独立行政法人等の中には、情報やノウハウがないことなどを理由としているものがあった。

エ　今後の課題

内閣府と所管する独立行政法人等の間で連絡が不十分である状況や、平成27年度中に保護管理規程の見直し（改正）、教育研修及び点検を実施していない独立行政法人等の中には、情報やノウハウがないため実施できなかったとしているものもあったことに鑑み、今後、独立行政法人等を所管する行政機関においては、他の行政機関の取組を参考に、独立行政法人等の保有する個人情報が適切に管理されるよう、なお一層、独立行政法人等に対し、個人情報の保護に関する連絡や支援を的確に行うことが求められる。

3　個人情報の適切な管理を行うための取組状況

(1)　教育研修の実施状況

行政機関指針及び独法等指針において、総括保護管理者は、①保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う、②保有個人情報を取り扱う情報システムの管理に関する事務に従事する職員に対し、保有個人情報の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う、③保護管理者及び保護担当者に対し、課室等の現場における保有個人情報の適切な管理のための教育研修を実施することとされている（行政機関指針第3、独法等指針第3)。

今回、各行政機関、各独立行政法人等における日本年金機構の個人情報流出事案発生後（平成27年6月以降）の教育研修の実施状況を調査したところ、以下のような状況がみられた。

ⅰ） 行政機関では全ての機関が、独立行政法人等では201機関中200機関(99.5%)が平成27年度中に教育研修を実施。平成28年度実施予定の独立行政法人等1機関（0.5%）を含め、全ての機関で教育研修を実施又は実施する予定となっている。

ⅱ）教育研修の対象については、行政機関では、保護担当者が 45 機関中43機関（95.6%）と最も多く、次いで保護管理者及び情報システム従事者が39機関（86.7%)、独立行政法人等の職員が13機関（28.9%）となっている。

一方、独立行政法人等では、職員が201機関中190機関（94.5%）と最も多く、次いで保護管理者が 170 機関（84.6%)、保護担当者が 167 機関（83.1%）となっている。

ⅲ）教育研修の内容については、行政機関では、標的型メールへの対応の訓練が45機関中43機関（95.6%）と最も多く、次いで標的型メールへの対応の座学及び漏えい等事案発生時の初期対応の座学が 38 機関（84.4%)、法律・訓令等の周知が37機関（82.2%）となっている。

一方、独立行政法人等では、法律・訓令等の周知が201機関中167機関（83.1%）と最も多く、次いで標的型メールへの対応の座学が166機

関(82.6%)、漏えい等事案発生時の初期対応の座学が 151 機関(75.1%)、情報システムの管理・運用が 145 機関（72.1%）となっている。

ⅳ）標的型メールへの対応の訓練について、①幹部職員も含めた訓練を実施、②不審メール通報訓練も併せて実施、③メール開封者に対する教育研修を実施、④ＬＡＮケーブルの抜線などの被害拡大防止措置の訓練なども併せて実施している機関がある。

ⅴ）漏えい等事案発生時の初期対応の訓練として、通報・報告体制の確認、緊急連絡会議の開催などの訓練を実施している機関がある。

ⅵ）保護管理者等の課室等の責任者に対する教育研修を実施している機関の中には、個人情報の取扱いが多い部局の保護管理者について、赴任前に個人情報の取扱いに関する研修を実施しているものがある。

ⅶ）効率的・効果的に情報管理の徹底を図る観点から、個人情報の保護に密接に関係する情報セキュリティ及び文書管理に関する研修を同時に開催している機関がある。

ⅷ）職員の職務・個人情報の取扱いに応じた研修を実施している機関がある。

ⅸ）幹部職員等を対象とした研修を実施している機関がある。

ⅹ）全ての行政機関及び独立行政法人等において、日本年金機構の個人情報流出事案を受け、個人情報の保護に関する意識の高揚を図るための啓発を行っており、中には組織の長による訓示を行っている機関がある。

また、事務用端末の起動時に個人情報の管理や標的型攻撃等のサイバー攻撃に関する啓発ページを表示させている機関がある。

(2) 点検・監査の実施状況

行政機関指針及び独法等指針において、保護管理者は、各課室等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告することとされている（行政機関指針第 10-2、独法等指針第 10-2)。

また、監査責任者は、保有個人情報の適切な管理を検証するため、当該機関における保有個人情報の管理の状況について、定期に及び必要に応じ随時に監査を行い、その結果を総括保護管理者に報告することとされてい

る（行政機関指針第 10-1、独法等指針第 10-1）。

今回、各行政機関、各独立行政法人等における日本年金機構の個人情報流出事案発生後（平成 27 年 6 月以降）の点検・監査の実施状況を調査したところ、以下のような状況がみられた。

ⅰ）行政機関では全ての機関が、独立行政法人等では 201 機関中 199 機関（99.0%）が平成 27 年度に点検を実施。また、平成 28 年度に実施予定の独立行政法人等 2 機関（1.0%）を含め、全ての機関で実施又は実施する予定となっている。

ⅱ）日本年金機構の個人情報流出事案において問題とされた①複製ルールの遵守、②共有フォルダ等への複製の保存、③パスワードの設定、④不要な個人情報の廃棄、⑤漏えい等事案が発生した場合の報告手順等の整備、⑥被害拡大防止のための対処方法、⑦行政機関と独立行政法人等との連携体制の整備については、おおむね全ての機関で点検を平成 27 年度に実施又は 28 年度に実施する予定となっている。

ⅲ）点検実施後、①複製ルールの周知徹底、②共有フォルダ内の不要な個人情報の廃棄、③ＵＳＢポートへの使用制限措置の設定、④パスワードを設定すべき保有個人情報へのパスワード設定の徹底、⑤漏えい等事案が発生した場合の報告手順の整備等の改善措置を講じている機関がある。

ⅳ）職員がチェックシートにより自己点検を行った後、補佐、総括補佐及び課長の各段階で各職員への質問や目視によって文書等の状況を確認している機関がある。

ⅴ）効率的・効果的に情報管理の徹底を図る観点から、個人情報の保護に密接に関係する情報セキュリティ及び文書管理に関する点検の項目を整理し、これらを統一的に行うためのチェックシートを示し、当該チェックシートに基づき保護管理者が点検を実施している機関がある。

ⅵ）行政機関では 45 機関中 38 機関(84.4%)が、独立行政法人等では 201 機関中 177 機関(88.1%)が平成 27 年度に監査を実施しており、残りの行政機関 7 機関(15.6%)、独立行政法人等 22 機関（10.9%）は 28 年度に監査を実施する予定となっている。監査周期が到来していないなどの理由から平成 28 年度に監査を実施する予定のない独立行政法人等 2 機関（1.0%）を除き、平成 27 年度に監査を実施又は平成 28 年度に実施する

予定となっている。

なお、平成28年度に実施する予定のない独立行政法人等2機関のうち、1機関については、平成28年4月に統合されたため、当面監査を実施する予定がないとしており、1機関は平成29年度に監査を実施する予定としている。

ⅶ）端末がシャットダウンされているか確認するため、無予告で始業前に監査するなどの取組を行っている機関がある。

なお、上記のような点検・監査の状況を踏まえ、保有個人情報を取り扱う情報システムの一部を抽出して、安全の確保等の状況を確認したところ、調査したシステムでは、①不正アクセスを防止するため、ファイアウォールの設定による経路制御等の措置を実施、②職員が保有個人情報を自由に複製できないよう、上司の許可が必要、③複製後、不要となった情報の消去の状況について点検で確認といった措置を講じている。