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）

勧　告	説明図表番号
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。	表 2-(1)-①～④
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。	表 2-(1)-⑤
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)。	表 2-(1)-⑥、⑦
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	表 2-(1)-⑧
、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ＬＡＮをオフにすることについて規定しているものがある。	表 2-(1)-⑨
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。	表 2-(1)-⑩、⑪

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。	表 2-(1)-⑫～⑱
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。	表 2-(1)-⑲
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。	表 2-(1)-⑳
【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。	

表 2－(1)－①　「「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」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」」における主な改正点

事項	改正点
初期対応に係る対策強化	○　外部からの不正アクセスが疑われる場合においては、ＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行うことを明記（行政機関指針第 9-2、独法等指針第 9-2） ○　各行政機関は、所管する独立行政法人等に対し、個人情報の保護に関し必要な指導、助言を行うことを明記（行政機関指針第 11） ○　漏えい等事案発生の場合、独立行政法人等は、当該独立行政法人等を所管する行政機関に対し、速やかに情報提供を行うことを明記（独法等指針第 9-5） ○　各独立行政法人等は、当該独立行政法人等を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行うことを明記（独法等指針第 11）
現場における安全管理措置の徹底	○　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（注）は、当該情報システムの管理者と連携して、保有個人情報の適切な管理を確保することを明記（行政機関指針第 2-2、独法等指針第 2-2） （注）課室長級職員。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。 ○　一般職員だけではなく、課室等の現場責任者である保護管理者等にも安全管理の研修を実施することを明記（行政機関指針第 3-3、独法等指針第 3-3） ○　保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去すること等を明記（行政機関指針第 6-9、独法等指針第 6-9） ○　職員が処理する保有個人情報について、適切に暗号化を行うこと（職員が行う暗号化には、適切なパスワードの選択、パスワードの漏えい防止の措置等を含む。）を明記（行政機関指針第 6-10、独法等指針第 6-10）

（注）　総務省（行政管理局）の平成 27 年 8 月 25 日報道発表資料「「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」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」の改正」に基づき、総務省（行政評価局）が作成した。

表２－(1)－②　「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」新旧対照表

（下線部は改正箇所）

改正後	現　行
第１　（略）	第１　（略）
第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、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（注）。 （注）例えば、第６、第７、第９－２、第 10－２、第 10－３その他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、情報システムの管理者と連携して、それぞれの措置を講ずる。 ３～５　（略）	第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。保護管理者は、各課室等における保有個人情報を適切に管理する任に当たる。 ３～５　（略）
第３　教育研修 １　総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者（注）を含む。以下同じ。）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。 （注）保有個人情報の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報の適切な取扱いを行うことに配慮されたものとする必要がある。 ２　（略） ３　総括保護管理者は、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。 ４　（略） （削除）	第３　教育研修 １　総括保護管理者は、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　（略） （新設） ３　保護管理者は、当該課室等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。 ４　１～３の措置を講ずる場合には、保有個人情報の取扱いに従事する派遣労働者についても、職員と同様の措置を講ずる。
第４　（略）	第４　（略）

第５　保有個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。 ２・３　（略） （複製等の制限） ４　職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為 ５～８　（略）	第５　保有個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員に限る。 ２・３　（略） （複製等の制限） ４　職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為 ５～８　（略）
第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（16を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる（注）。 （注）アクセス制御の措置内容は、第５－１により設定した必要最小限のアクセス権限を具体化するものである必要がある。 ２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。 ３・４　（略） （アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要	第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（10を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。 ２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。 ３・４　（略） （アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報への不適切なアクセスの監視のため、一定数以上の保有個人情報がダウンロードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講ずる。

な措置を講ずる。	
６・７　（略）	６・７　（略）
（不正プログラムによる漏えい等の防止）	（不正プログラムによる漏えい等の防止）
８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。	８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置を講ずる。
（情報システムにおける保有個人情報の処理）	
９　職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。	（新設）
（暗号化）	（暗号化）
１０　保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。 職員（注）は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。 （注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。	９　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。
	（記録機能を有する機器・媒体の接続制限）
１１　（略）	１７　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。
	（端末の限定）
１２　（略）	１３　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。
	（端末の盗難防止等）
１３　（略）	１４　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。
１４　（略）	１５　職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。
	（第三者の閲覧防止）

15　（略）	16　職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。
	（入力情報の照合等）
16　（略）	10　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。
	（バックアップ）
17　（略）	11　保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。
	（情報システム設計書等の管理）
18　（略）	12　保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。
第７　（略）	第７　（略）
第８　保有個人情報の提供及び業務の委託等	第８　保有個人情報の提供及び業務の委託等
１　（略）	１　（略）
２　保護管理者は、法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。	２　保護管理者は、法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講ずる。
３～７　（略）	３～７　（略）
第９　安全確保上の問題への対応	第９　安全確保上の問題への対応
（事案の報告及び再発防止措置）	（事案の報告及び再発防止措置）
１　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、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。 （注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。	１　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が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者に報告する。
２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部から	２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。

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等のＬＡＮケーブルを抜くなど、被害拡大防止のため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。）ものとする。	
３～５　（略）	３～５　（略）
（公表等）	（公表等）
６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（注）等の措置を講ずる。 公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行う。	６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。
（注）漏えい等が生じた保有個人情報に係る本人への連絡等の対応	
第 10　監査及び点検の実施	第 10　監査及び点検の実施
（監査）	（監査）
１　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、第２から第９に規定する措置の状況を含む当該行政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（外部監査を含む。以下同じ。）（注）を行い、その結果を総括保護管理者に報告する。	１　監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。
（注）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。	
（点検）	（点検）
２　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。	２　保護管理者は、自ら管理責任を有す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、定期に又は随時に点検を行い、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。
（評価及び見直し）	（評価及び見直し）
３　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。	３　保有個人情報の適切な管理のための措置については、総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずる。
第 11　独立行政法人等に対する指導等 各行政機関は、「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）４に基づき、所管する独立行政法人等に対して、その業務運営における自主性に配慮しつつ、個人情報の保護に関し必要な指導、助言を行う。	（新設）

表 2－(1)－③　「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」新旧対照表

（下線部は改正箇所）

改正後	現　行
第１　（略）	第１　（略）
第２　管理体制	第２　管理体制
１　（略）	１　（略）
（保護管理者）	（保護管理者）
２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、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（注）。 （注）例えば、第６、第７、第９－２、第 10－２、第 10－３その他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、情報システムの管理者と連携して、それぞれの措置を講ずる。	２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、各課室等における保有個人情報を適切に管理する任に当たる。
３～５　（略）	３～５　（略）
第３　教育研修	第３　教育研修
１　総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者（注）を含む。以下同じ。）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。 （注）保有個人情報の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報の適切な取扱いを行うことに配慮されたものとする必要がある。	１　総括保護管理者は、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　（略）	２　（略）
３　総括保護管理者は、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。	（新設）
４　（略）	３　保護管理者は、当該課室等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。
（削除）	４　１～３の措置を講ずる場合には、保有個人情報の取扱いに従事する派遣労働者についても、職員と同様の措置を講ずる。
第４　（略）	第４　（略）

第５　保有個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。 ２・３　（略） （複製等の制限） ４　職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為 ５～８　（略）	第５　保有個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員に限る。 ２・３　（略） （複製等の制限） ４　職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為 ５～８　（略）
第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（16を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる（注）。 （注）アクセス制御の措置内容は、第５－１により設定した必要最小限のアクセス権限を具体化するものである必要がある。 ２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。 ３・４　（略） （アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がな	第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（10を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。 ２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。 ３・４　（略） （アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報への不適切なアクセスの監視のため、一定数以上の保有個人情報がダウンロードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講ず

される機能の設定、当該設定の定期的確認等の必要な措置を講ずる。	る。
６・７　（略）	６・７　（略）
（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。	（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置を講ずる。
（情報システムにおける保有個人情報の処理） ９　職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。	（新設）
（暗号化） 10　保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。 職員（注）は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。 （注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。	（暗号化） ９　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。
11　（略）	（記録機能を有する機器・媒体の接続制限） 17　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。
12　（略）	（端末の限定） 13　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。
13　（略）	（端末の盗難防止等） 14　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。
14　（略）	15　職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。 （第三者の閲覧防止）

15　（略）	16　職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。
	（入力情報の照合等）
16　（略）	10　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。
	（バックアップ）
17　（略）	11　保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。
	（情報システム設計書等の管理）
18　（略）	12　保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。
第７　（略）	第７　（略）
第８　保有個人情報の提供及び業務の委託等	第８　保有個人情報の提供及び業務の委託等
１　（略）	１　（略）
２　保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。	２　保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講ずる。
３～７　（略）	３～７　（略）
第９　安全確保上の問題への対応	第９　安全確保上の問題への対応
（事案の報告及び再発防止措置）	（事案の報告及び再発防止措置）
１　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、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。 （注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。	１　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が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者に報告する。
２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部から	２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。

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等のＬＡＮケーブルを抜くなど、被害拡大防止のため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。）ものとする。	
３・４　（略）	３・４　（略）
５　総括保護管理者は、事案の内容等に応じて、事案の内容、経緯、被害状況等について、当該独立行政法人等を所管する行政機関に対し、速やかに情報提供を行う。	（新設）
６　（略）	５　（略）
（公表等）	（公表等）
７　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（注）等の措置を講ずる。 公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行う。 （注）漏えい等が生じた保有個人情報に係る本人への連絡等の対応	６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。
第 10　監査及び点検の実施	第 10　監査及び点検の実施
（監査）	（監査）
１　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、第２から第９に規定する措置の状況を含む当該独立行政法人等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（外部監査を含む。以下同じ。）（注）を行い、その結果を総括保護管理者に報告する。 （注）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。	１　監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。
（点検）	（点検）
２　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。	２　保護管理者は、自ら管理責任を有す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、定期に又は随時に点検を行い、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。
（評価及び見直し）	（評価及び見直し）
３　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。	３　保有個人情報の適切な管理のための措置については、総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずる。
第 11　行政機関との連携	
各独立行政法人等は、「個人情報の保護に関する	（新設）

基本方針」（平成16年４月２日閣議決定）４を踏まえ、当該独立行政法人等を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行う。	

表 2－(1)－④　「総務省指針改正に伴う規程の見直し等について（依頼）」（平成 27 年 8 月 25 日付け事務連絡）（抜粋）

事　務　連　絡
平成 27 年８月 25 日

行政機関個人情報保護担当官　殿
各独立行政法人等個人情報保護担当者　殿

総務省行政管理局
情報公開・個人情報保護推進室

総務省指針改正に伴う規程の見直し等について（依頼）

平素から当室の業務に御協力いただき、厚く御礼申し上げます。

今般、「「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について」の一部改正について」（平成 27 年８月 25 日総管管第７０号総務省行政管理局長通知）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について」の一部改正について」（平成 27 年８月 25 日総管管第 71 号総務省行政管理局長通知）を発出したことに伴い、下記のとおり、依頼等させていただきますので、よろしくお願いいたします。

記

１．各行政機関・独立行政法人等における規程の見直しについて

「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）では、法の適切な運用のため、行政機関・独立行政法人等が保有する個人情報の適切な管理に関する指針等を総務省が策定するとともに、各行政機関・各独立行政法人等は、その指針等を参考に、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管理に関する定め等（以下「規程」という。）を整備することとされています。

つきましては、各行政機関・各独立行政法人等におかれましては、今般の指針改正を踏まえ、それぞれの規程につきまして平成 27 年中を目途に見直し（改正）いただきますようお願いいたします。

（注）下線は当省が付した。

表 2－(1)－⑤　保護管理規程の見直し（改正）状況

（単位：機関）

区分	機関数	平成 27 年度に見直し(改正)	平成 28 年度に見直し(改正)
行政機関	45 (100%)	44 (97.8%)	1 (2.2%)
独立行政法人等	201 (100%)	194 (96.5%)	7 (3.5%)
計	246 (100%)	238 (96.7%)	8 (3.3%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

3　(　)は、機関数に占める割合を示す。

4　厚生労働省においては、保護管理規程について、本省内部部局とは別に、施設等機関及び地方支分部局の各機関で整備しており、本省内部部局は平成 27 年度に見直し（改正）を実施しているが、施設等機関及び地方支分部局の中には、28 年度に見直し（改正）を実施したものがあるため、「平成 28 年度に見直し（改正)」欄に計上している。

5　検察庁は、行政機関個人情報保護法において、最高検察庁、各高等検察庁、各地方検察庁は、それぞれ一の行政機関とされているが、本報告書においては、まとめて一機関として計上している（以下同じ。)。

6　会計検査院は、行政機関個人情報保護法において、行政機関とされているため、行政機関として計上している（以下同じ。)。

表 2－(1)－⑥　保護管理規程等の見直し（改正）内容（行政機関）

（単位：機関）

行政機関指針の改正内容	機関数	保護管理規程の見直し（改正）	保護管理規程以外の規程による対応	平成 28 年度以降見直し(改正)
①保護管理者とシステム管理者との連携（第 2-2）	45 (100%)	40 (88.9%)	2 (4.4%)	3 (6.7%)
②現場責任者への教育研修（第 3-3）	45 (100%)	41 (91.1%)	2 (4.4%)	2 (4.4%)
③複製等の最小限化、処理後の消去(第 6-9)	45 (100%)	42 (93.3%)	3 (6.7%)	0 (0.0%)
④暗号化(パスワード設定)（第 6-10）	45 (100%)	40 (88.9%)	5 (11.1%)	0 (0.0%)
⑤被害拡大防止措置（第 9-2）	45 (100%)	41 (91.1%)	4 (8.9%)	0 (0.0%)
⑥所管独法等への指導、助言（第 11）	23 (100%)	21 (91.3%)	0 (0.0%)	2 (8.7%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表を参照。

3　(　)は、機関数に占める割合を示す。また、割合は小数点第 2 位を四捨五入しているため、機関数の数値とその内訳の数値の合計が一致しない場合がある。

4　「保護管理規程の見直し（改正)」欄には、保護管理規程の改正（保護管理規程の委任を受けた規則及び細則の改正によるものも含む。）のほか、既に保護管理規程に行政機関指針の改正内容が規定されているものも含む。

5　「保護管理規程以外の規程による対応」欄には、セキュリティポリシー等の改正による対応のほか、既にセキュリティポリシー等に行政機関指針の改正内容が規定されているものも含む。

表 2－(1)－⑦　保護管理規程等の見直し（改正）内容（独立行政法人等）

（単位：機関）

独法等指針の改正内容	機関数	保護管理規程の見直し（改正）	保護管理規程以外の規程による対応	平成 28 年度以降見直し（改正）
①保護管理者とシステム管理者との連携（第 2-2）	201 (100%)	195 (97.0%)	0 (0.0%)	6 (3.0%)
②現場責任者への教育研修（第 3-3）	201 (100%)	191 (95.0%)	0 (0.0%)	10 (5.0%)
③複製等の最小限化、処理後の消去(第 6-9)	201 (100%)	190 (94.5%)	4 (2.0%)	7 (3.5%)
④暗号化(パスワード設定)（第 6-10）	201 (100%)	191 (95.0%)	6 (3.0%)	4 (2.0%)
⑤被害拡大防止措置等（第 9-2、第 9-5）	201 (100%)	198 (98.5%)	2 (1.0%)	1 (0.5%)
⑥所管行政機関との連携（第 11）	201 (100%)	184 (91.5%)	1 (0.5%)	16 (8.0%)

（注）1　当省の調査結果による。

2　詳細は独立行政法人等別内訳表を参照。

3　(　)は、機関数に占める割合を示す。

4　「保護管理規程の見直し（改正)」欄には、保護管理規程の改正（保護管理規程の委任を受けた規則及び細則の改正によるものも含む。）のほか、既に保護管理規程に独法等指針の改正内容が規定されているものも含む。

5　「保護管理規程以外の規程による対応」欄には、セキュリティポリシー等の改正による対応のほか、既にセキュリティポリシー等に独法等指針の改正内容が規定されているものも含む。

表 2－(1)－⑧　保護管理規程においてシステム管理に関する役職を設け、その具体的な責務等を規定している事例

事例の内容
＜システム管理者の設置＞ 保護管理規程が整備された平成 17 年から、インシデント発生時にはシステム管理者にしかできない対応策があるとして、行政機関指針にはないシステム管理者を規定している。 システム管理者は、①保有個人情報等を取り扱う情報システムを整備・管理する課室内に置くこと、②セキュリティポリシーで規定されるシステム管理者を充てること、③システム管理者は、セキュリティポリシーに基づき情報システムに係るセキュリティ対策に関する事務を担うとともに、保護管理規程に定めるシステム管理者の責務等に従い、保有個人情報等の適切な管理のために必要な情報システムに関する事務を行うこととされている。 ＜システム管理者の責務等＞ システム管理者の責務等として、保護管理規程に以下の事項が規定されている。 ① システム管理者は、ソフトウェアの改善に併せ、パスワード等を使用して一定の職員以外は記録された保有個人情報等にアクセスできないようにする機能を設ける等、保護担当者（注）からの協議に応じて、必要な措置を講ずるよう努めるものとする。 ② システム管理者は、ソフトウェアの改善に併せ、保有個人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存できる機能を設ける等、保護担当者からの協議に応じて、必要な措置を講じるよう努めるものとする。 当該機能が整備された後は、アクセス記録の改ざん、窃取又は不正な消去の防止に努めるとともに、保護担当者がアクセス記録を分析することができるよう、アクセス記録を定期に又は随時に保護担当者に提供するものとする。 ③ システム管理者は、保有個人情報等の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する更改された脆弱性の解消、把握された不正プログラムの感染防止及び外部からの不正アクセスの防止等必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずるものとする。 ④ システム管理者は、ソフトウェアの改善等に併せ、通信量を監視し異常を検知した場合に通知がなされる機能等を設ける等、保護担当者からの協議に応じて、必要な措置を講じるよう努めるものとする。当該機能が整備された後は、当該機能の定期的確認等の必要な措置を講じるよう努めるものとする。 ⑤ システム管理者は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等、保護担当者からの協議に応じて、必要な措置を講ずるものとする。 ⑥ システム管理者は、保有個人情報等に係る情報システムの設計書、構成図等の保管、複製、廃棄に当たっては、業務上必要となる者以外に知られることがないよう必要な措置を講ずるものとする。 ⑦ システム管理者は、保有個人情報等が記録された情報システム機器の廃棄に当たっては、その完全な消去等、保有個人情報等を復元することが不可能となる処理を行うものとする。 ⑧ システム管理者は、自らが整備、管理する情報システムに関し、当該情報システムを利用する職員及び保護担当者が個人情報の適正な管理のためとるべき措置を必要に応じて定め（その定期又は随時の見直しを含む。）、通知するものとする。 （注）当該規程における保護担当者は、行政機関指針上の保護管理者に当たる。 ＜システム管理者の責務等に基づく具体的な対応事例＞

今回調査した保有個人情報を取り扱う情報システムの一部において、以下のような対応を行っている。 ⅰ）保護管理規程が整備された平成 17 年 3 月（平成 28 年 3 月に一部改正）に、システム管理者は、上記システム管理者の責務等⑧に基づき、保護管理者に対し、管理する情報システムの個人情報の取扱いについて通知している。 ⅱ）システム管理者は、上記システム管理者の責務等②に基づき保護担当者がアクセス記録を分析することができるよう、アクセス記録を保護担当者に提供し、保護担当者は、ⅰ）の通知に基づき、原則週に 1 度、自己の担当分の管理リストを確認する。その後、アクセス権限を有しない者による不正アクセス等個人情報の流出の可能性が認められる場合は、システム管理者に報告することとしている。

（注）当省の調査結果による。

表 2－(1)－⑨　端末の接続状況を踏まえた被害拡大防止措置を規定している事例

事例の内容
独法等指針第 9-2 では、安全確保上の問題への対応として「保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、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等のＬＡＮケーブルを抜くなど、被害拡大防止のため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。）ものとする。」と定められている。 当該法人では、無線ＬＡＮで接続する端末が全体の 90%以上であることもあり、緊急時に職員が直ちに対応できるよう規定振りを明確化する観点から、平成 28 年 1 月、保護管理規程について、「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、（中略）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無線ＬＡＮをオフにする又はＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行うものとする。」と改正した。

（注）当省の調査結果による。

表 2－(1)－⑩　施設等機関及び地方支分部局における保護管理規程の適用関係等

保護管理規程の適用関係等	行政機関数
①　本府省庁の保護管理規程が適用	19
②　本府省庁の保護管理規程が適用。地方支分部局は当該規程の細則を整備	4
③　施設等機関について、行政機関指針に基づく保護管理規程を整備	2
④　施設等機関、地方支分部局について、行政機関指針に基づく保護管理規程を整備	1 （厚生労働省）
計	26

（注）1　当省の調査結果による。

2　本表は、施設等機関及び地方支分部局を設けている 26 機関の内訳について記載している。

表 2－(1)－⑪　厚生労働省において、本省内部部局とは別に施設等機関及び地方支分部局で保護管理規程を整備する根拠

○　厚生労働省保有個人情報管理規程（平成 17 年厚生労働省訓第 3 号）（抜粋）

（目的）

第１条　この訓令は、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。）第６条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（平成２５年法律第２７号。以下「番号法」という。）第４条の規定に基づき、厚生労働省（内部部局に限る。以下同じ。）の保有する個人番号その他の個人情報の適切な管理のために必要な措置について定め、その漏えい、滅失、毀損等（以下「情報漏えい等」という。）を防止し、適正な管理を図ることを目的とする。

（施設等機関及び地方支分部局）

第５８条　施設等機関及び地方支分部局の保有個人情報の管理については、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。

（注）下線は当省が付した。

表 2－(1)－⑫　厚生労働省本省内部部局における保護管理規程の周知等

総発 1001 第 2 号
平成 27 年 10 月 1 日

内部部局の長
大臣官房各課長　殿

大臣官房総務課長
（公　印　省　略）

厚生労働省保有個人情報管理規程の一部改正について

今般、厚生労働省保有個人情報管理規程の一部を改正する訓令（平成 27 年厚生労働省訓令第 35 号）が別添のとおり制定され、本日から施行されることとされたので通知する。

ついては、貴部局（課）における周知をお願いする。

なお、地方支分部局、施設等機関及び独立行政法人（※）（以下「地方支分部局等」という。）を所管する内部部局の長及び大臣官房各課長においては、所管する地方支分部局等に対し、所管する地方支分部局等が保有する個人情報の適切な管理に関する定め等の整備等の措置を講ずるよう、改めて必要な指導、助言等をお願いする。

（※）　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）第２条第１項に規定する独立行政法人等をいう。

表 2－(1)－⑬　厚生労働省本省内部部局からの施設等機関への周知（試験研究機関）

事　務　連　絡
平成27年8月25日

各試験研究機関　御中

厚生労働省大臣官房厚生科学課

総務省指針改正に伴う規程の見直し等について（依頼）

今般、「「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について」の一部改正について」（平成 27 年 8 月 25 日総管管第 70 号総務省行政管理局長通知）が発出したことに伴い、下記のとおり、依頼等させていただきますので、よろしくお願いいたします。

記

1. 各試験研究機関における規程の見直しについて

「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）では、法の適切な運用のため、行政機関等が保有する個人情報の適切な管理に関する指針等を総務省が策定するとともに、各行政機関等は、その指針等を参考に、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管理に関する定め等（以下「規程」という。）を整備することとされています。

つきましては、各試験研究機関におかれましては、今般の指針改正を踏まえ、それぞれの規程につきまして速やかに見直し（改正）いただきますようお願いいたします。

2. 規程見直し（改正）状況の回報、改正後の規程の提供等について

お手数ですが、規程の見直し（改正）を行い次第、別添様式によりその旨を御回報いただくとともに、その際、改正後の規程を添付いただきますようお願いいたします。

なお、平成 27 年 10 月 31 日時点において、規程の見直し（改正）が終了していない場合は、見直し（改正）状況を別添様式により、平成 27 年 11 月 13 日（金）までに御回報いただきますようお願いいたします。

表 2－(1)－⑭　厚生労働省本省内部部局からの施設等機関への周知（国立ハンセン病療養所）

（厚生労働省医政局医療経営支援課から各国立ハンセン病療養所への連絡（平成27年10月5日））

今般、厚生労働省保有個人情報管理規程の一部が改正されましたので、
別添のとおり送付致します。

各施設におかれましては、各施設ごとの「保有個人情報管理取扱規程」等の
改正が必要と存じますので、つきましては、10月20日（火）　までに
各施設内規程を改正していただき、小職まで御登録頂きますようお願い致します。

なお、改正作業にかかる疑義照会等ございます場合は、適宜ご連絡ください。

表 2－(1)－⑮　厚生労働省本省内部部局からの施設等機関への周知（国立障害者リハビリテーションセンター）

（厚生労働省社会・援護局障害保健福祉部企画課から国立障害者リハビリテーションセンターへの連絡（平成27年10月2日））

年金機構の個人情報流出事案を踏まえ、
総務省「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」
厚生労働省情報セキュリティポリシーの改正、等を受け、
厚生労働省保有個人情報管理規程が改正されました。

同規定では、
（施設等機関及び地方支分部局）
第50条　施設等機関及び地方支分部局の保有個人情報の管理については、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。

と定められていることから、
国リハの個人情報管理規程を改正する等、個人情報の適切な管理に関する定め等の準備等の措置を講ずるよう指示されています。

内容をご確認いただき、
国リハの個人情報管理規程について、改正作業を行っていただきたいと思います。

改正案については、10 月30日まで、当職宛にお送りいただきたいと思います。
その後、こちらで省内関係部局と協議しますので、調整いただくことになると思います。

表 2－(1)－⑯　厚生労働省本省内部部局からの施設等機関への周知（検疫所）

（厚生労働省医薬・生活衛生局 生活衛生・食品安全部企画情報課から各検疫所への連絡（平成28年3月14日））

今年度、厚生労働省保有個人情報保護規程の改正が行われたことから、この改正にあわせて各検疫所の保有個人情報保護規程も改正が必要となっております。
改定する際には、厚生労働審議官への協議が必要となります。

つきましては、年度末のお忙しいところ、短期間の作業依頼で申し訳ございませんが、別添の厚生労働省保有個人情報保護管理規程を沿った形で各検疫所保有個人情報保護管理規程（案）を改正していただき、新旧対照表をつけて 3 月 18 日（金）までに小職あてメールにて登録願います。

協議が終了しましたらお知らせしますので、各検疫所において規程の改正をお願いいたします。

表 2－(1)－⑰　厚生労働省本省内部部局からの地方支分部局への周知（地方厚生（支）局）

事　務　連　絡
平成２７年１２月１４日

各地方厚生（支）局　総務課長　殿

大臣官房地方課
地方厚生局管理室長補佐

地方厚生（支）局における保有個人情報管理規程の一部改正について

平成27年12月4日付け地発1204第2号「厚生労働省保有個人情報管理規程の一部改正について（通知）」による地方課長通知が発出されたところですが、貴局における保有個人情報管理規程について別添を参考に改正するようお願いいたします。

表 2－(1)－⑱　厚生労働省本省内部部局からの地方支分部局への周知（都道府県労働局）

地 発 1204第３号
平成27年12月４日

都道府県労働局長　殿

厚生労働省大臣官房地方課長
（　公　印　省　略　）

厚生労働省保有個人情報管理規程の一部改正に伴う都道府県労働局
保有個人情報管理規程準則の改正について

都道府県労働局における保有個人情報管理規程については、平成17年3月29日付け地発第0329006号「都道府県労働局における個人情報管理規程の策定について」 により策定を指示したところであるが、今般、平成27年12月4日付け地発1204第2号「厚生労働省保有個人情報管理規程の一部改正について（通知）」により通知したとおり、厚生労働省保有個人情報管理規程の一部を改正する訓令（平成27年厚生労働省訓第35号）が制定され、平成27年10月1日から施行されたところである。

このため、改正された厚生労働省保有個人情報管理規程（以下「改正管理規程」という。）に準じて改正した都道府県労働局保有個人情報管理規程準則（以下「改正準則」という。）を別添のとおり示すので、これを参考にしつつ下記に掲げた事項に留意して、本年中に、貴局における保有個人情報管理規程を改正し、非常勤職員を含めた全職員に周知徹底されたい。

記

1　改正管理規程第 50 条に基づく厚生労働審議官との協議については、改正準則を当課から官房総務課へ協議したことをもって、その手続を終えたこととしたので、改正準則に従うものであれば、貴局において改めて協議を行う必要はないこと。

2　改正準則における主な改正の趣旨は以下のとおりであるので、貴局における保有個人情報管理規程の改正に当たっては、これらを踏まえること。

(1) 改正準則第 10 条第 1 項は、保有個人情報を取り扱う課の課長が、保有個人情報の複製等を行うことができる場合を、あらかじめ限定することを示したもの。

また、同条第2項は、前項で限定した範囲内において複製等を必要最小限の範囲で行うことを示したもの。

(2) 改正準則第 21 条は、独自システムの安全確保のため、独自システムを取り扱う課の課長は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損を防止するため、不正プログラム対策ソフトを、随時、最新のものに更新する等の不正プログラムの感染防止に必要な措置を講ずることを示したもの。

(3) 改正準則第 22 条は、同条第 1 項に、保有個人情報の複製等を「必要最小限に限り」、「不要となった情報を速やかに消去する」と示していることを踏まえ、同条第 2 項において、独自システムを取り扱う課の課長が、同条第 1 項の処理終了後速やかに、複製された保有個人情報

が消去されていることを確認することを示したもの。

(4) 改正準則第 23 条は、保有個人情報へのパスワードの設定に当たり、暗号化の要を為さない設定にしないこと、また、当該パスワードの漏えいを防止すべきことを示したもの。

(5) 改正準則第 44 条は、不正アクセスや不正プログラムの感染が疑われる端末等が発生した場合に、システムと遮断すべき旨を具体的に示したもの。

(6) 改正準則第 48 条第 3 項は、保有個人情報の取扱に係る教育研修について、新たに保有個人情報を取り扱う課の課長を対象とした研修を定期的に実施することを示したもの。

(7) 改正準則第 49 条は、保有個人情報の適切な管理に係る監査について、必要と認めるときのみならず定期に行うべきことを示したもの。

表 2－(1)－⑲　厚生労働省における保護管理規程の見直し（改正）状況

区分		規程数	本省（大臣官房総務課（情報公開文書室））からの施設等機関、地方支分部局の所管課等への指示等	施設等機関、地方支分部局に対する所管課等からの指示等	本省（大臣官房総務課（情報公開文書室））との協議日	見直し(改正)規程数	
						平成 27 年度中に見直し（改正）	平成 28 年 4 月に見直し(改正)
本省内部部局		1	H27.10.1 指示 本省内部部局の保護管理規程提示	－	－	1	0
施設等機関	試験研究機関	4	－	H27.8.25 指示（大臣官房厚生科学課）	H27.11.26（規程ごとの協議）	4	0
	国立ハンセン病療養所	13	－	H27.10.5 指示（医政局医療経営支援課）	H27.12.4（規程ごとの協議）	13	0
	国立障害者リハビリテーションセンター	1	－	H27.10.2 指示（社会・援護局障害保健福祉部企画課）	H27.10.23（規程ごとの協議）	1	0
	国立児童自立支援施設	2	－	特段の指示はなし	H28.4.22（規程ごとの協議）	0	2
	検疫所	13	－	H28.3.14 指示（医薬・生活衛生局生活衛生・食品安全部企画情報課）	H28.4.8（規程ごとの協議）	0	13
地方支分部局	地方厚生局	8	－	H27.12.14 雛形提示、改正指示（大臣官房地方課）	H27.11.18（雛形の協議）	7	1
	都道府県労働局	147	－	H27.12.4 準則提示、改正指示（大臣官房地方課）	H27.12.4（準則の協議）	147	0
計		189	－	－	－	173	16

（注）当省の調査結果による。

表 2－(1)－⑳　地方厚生局及び都道府県労働局における本省内部部局の保護管理規程との差異

区分	本省内部部局の保護管理規程との差異
地方厚生局	本省内部部局の保護管理規程に準じた雛形を基に整備しているため、厚生局間で差異はない。
都道府県労働局	都道府県労働局が個別に規程を整備する理由として、都道府県労働局の独自システムがあったことが考えられるが、実際の都道府県労働局における規定内容は本省内部部局規程に準じた準則と同じとなっている。

（注）当省の調査結果による。

(2) 管理体制の状況

調査の結果	説明図表番号
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）。	表 2-(2)-①、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。	表 2-(2)-③
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。	表 2-(2)-④
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）。	表 2-(2)-⑤、⑥
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。	表 2-(2)-⑦ 表 2-(2)-⑧
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。	表 2-(2)-⑨

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）。	表 2-(2)-⑤、⑥
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。	表 2-(2)-⑩
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。	表 2-(2)-⑪
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。	表 2-(2)-⑫ 表 2-(2)-⑬
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。	表 2-(2)-⑭
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。	表 2-(2)-⑮～⑰
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。	表 2-(2)-⑱、⑲
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。	表 2-(2)-⑳～㉒
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。	

表 2－(2)－①　行政機関指針における管理体制の規定（「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））（抜粋）

第２　管理体制

（総括保護管理者）

１　各行政機関に、総括保護管理者を一人置くこととし、官房長等をもって充てる。

総括保護管理者は、行政機関の長を補佐し、各行政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。

（保護管理者）

２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。

保護管理者は、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（注）。

（注）例えば、第６、第７、第９－２、第10－２、第10－３その他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、情報システムの管理者と連携して、それぞれの措置を講ずる。

（保護担当者）

３　保有個人情報を取り扱う各課室等に、当該課室等の保護管理者が指定する保護担当者を一人又は複数人置く。

保護担当者は、保護管理者を補佐し、各課室等における保有個人情報の管理に関する事務を担当する。

（監査責任者）

４　各行政機関に、監査責任者を一人置くこととし、内部監査等を担当する部局の長等をもって充てる。

監査責任者は、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。

（保有個人情報の適切な管理のための委員会）

５　総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする委員会を設け、定期に又は随時に開催する。

（注）下線は当省が付した。

表 2－(2)－②　独法等指針における管理体制の規定（「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））（抜粋）

第２　管理体制

（総括保護管理者）

１　各独立行政法人等に、総括保護管理者を一人置くこととし、総務担当役員等をもって充てる。

総括保護管理者は、各独立行政法人等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。

（保護管理者）

２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。

保護管理者は、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（注）。

（注）例えば、第６、第７、第９－２、第10－２、第10－３その他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、情報システムの管理者と連携して、それぞれの措置を講ずる。

（保護担当者）

３　保有個人情報を取り扱う各課室等に、当該課室等の保護管理者が指定する保護担当者を一人又は複数人置く。

保護担当者は、保護管理者を補佐し、各課室等における保有個人情報の管理に関する事務を担当する。

（監査責任者）

４　各独立行政法人等に、監査責任者を一人置くこととし、監事等をもって充てる。

監査責任者は、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。

（保有個人情報の適切な管理のための委員会）

５　総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする委員会を設け、定期に又は随時に開催する。

（注）下線は当省が付した。

表 2－(2)－③　情報セキュリティ対策の役職との兼務状況

（単位：機関）

区分	機関数	総括保護管理者	保護管理者	監査責任者
行政機関	45 (100%)	36 (80.0%)	44 (97.8%)	30 (66.7%)
独立行政法人等	201 (100%)	113 (56.2%)	144 (71.6%)	76 (37.8%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

3　本表は、各機関の保護管理規程における行政機関指針又は独法等指針に規定される総括保護管理者、保護管理者、監査責任者に当たる役職と情報セキュリティ対策の役職の兼務状況を示したもの。

4　（　）は、機関数に占める割合を示す。

表 2－(2)－④　保護管理者と情報システム管理者の連携に関する取組事例

事例の内容
システム管理者が、アクセス記録を保護担当者（行政機関指針における保護管理者）に提供し、保護担当者が原則週に 1 度、自己の担当分の管理リストを確認。
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。
標的型メール訓練において、情報システムの管理者から、不適切な対応がみられた職員が所属する課室の保護管理者に対し、職員を指導するよう要請。
個人情報と情報システムの担当者会議を随時開催し、標的型メール訓練の方法等の打合せ等を実施。
個人情報が保存されている情報システムがどのようなリスクにさらされる可能性があるかを情報システム管理者だけでなく、保護管理者も把握するため、「システムリスク管理委員会」を設置。
四半期に 1 度、役員、情報システム管理者及び保護管理者が出席する「ＩＴ戦略委員会」で、保有する情報システムの改修等の計画及び進捗状況等を共有。
週 1 回の役員会において、必要に応じ、情報セキュリティに関する議題を取り上げ、保護管理者とシステム管理者が連携。

（注）当省の調査結果による。

表 2－(2)－⑤　行政機関指針における安全確保上の問題への対応の規定（「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））（抜粋）

第９　安全確保上の問題への対応

（事案の報告及び再発防止措置）

１　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、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。

（注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。

２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、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等のＬＡＮケーブルを抜くなど、被害拡大防止のため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。）ものとする。

３　保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。

４　総括保護管理者は、３の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を行政機関の長に速やかに報告する。

５　保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

（注）下線は当省が付した。

表 2－(2)－⑥　独法等指針における安全確保上の問題への対応の規定（「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））（抜粋）

第９　安全確保上の問題への対応

（事案の報告及び再発防止措置）

１　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、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。

（注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。

２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、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等のＬＡＮケーブルを抜くなど、被害拡大防止のため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。）ものとする。

３　保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。

４　総括保護管理者は、３の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を独立行政法人等の長に速やかに報告する。

５　総括保護管理者は、事案の内容等に応じて、事案の内容、経緯、被害状況等について、当該独立行政法人等を所管する行政機関に対し、速やかに情報提供を行う。

６　保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

（公表等）

７　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（注）等の措置を講ずる。

公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行う。

（注）漏えい等が生じた保有個人情報に係る本人への連絡等の対応

（注）下線は当省が付した。

表２－(2)－⑦　保有個人情報の漏えい等事案の発生時の連絡体制の整備状況

（単位：機関）

区分	機関数	連絡体制の整備
行政機関	45 (100%)	45 (100%)
独立行政法人等	201 (100%)	201 (100%)
計	246 (100%)	246 (100%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

表２－(2)－⑧　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の対応

（単位：機関）

区分	機関数	夜間・休日対応	幹部への速やかな報告	所管する行政機関への報告
行政機関	45 (100%)	45 (100%)	45 (100%)	－
独立行政法人等	201 (100%)	201 (100%)	201 (100%)	201 (100%)
計	246 (100%)	246 (100%)	246 (100%)	201 (100%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

表 2－(2)－⑨　情報システムからの保有個人情報の漏えい又は漏えいのおそれがある場合の対応に関する取組事例

事例の内容
全てのインシデント処理について、一律な処理をするのではなく、そのレベルに応じた対応を行うためのマニュアルを作成している。 当該マニュアルでは、レベル 0（セキュリティインシデントに発展するおそれがある状態）からレベル 3（セキュリティインシンデントと認知され、甚大な被害が想定される状態）までの 4 段階の「インシデントレベル」に区分し、区分ごとの「具体的な事例」（不正通信、ホームページ改ざん、メールの誤送信、パソコンやＵＳＢメモリの紛失等）、とこれらの事例に対する「初期対処における留意事項」（関係部署への連絡、外部との通信切断等）について記載している。 全職員に当該マニュアルを周知後、当該マニュアルに従った対応が行われていることを確認している。
平成 27 年度に標的型メールによる攻撃を受けたという仮定でＣＳＩＲＴを招集するなど実践形式でインシデント発生の対応訓練を実施し、立会いの外部専門業者に訓練結果を評価してもらうことで修正すべき点を整理している。 なお、修正すべき点については、迅速に対応し改善を図ることで、組織としてインシデント対応の機能を強化している。

（注）　当省の調査結果による。

表 2－(2)－⑩　被害拡大防止のための注意喚起の実施状況

（単位：機関）

区分	機関数	被害拡大防止のための注意喚起
行政機関	45 (100%)	45 (100%)
独立行政法人等	201 (100%)	201 (100%)
計	246 (100%)	246 (100%)

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

表 2－(2)－⑪　被害拡大防止のための注意喚起に関する取組事例

事例の内容
平成 27 年度に、職員に対し、標的型メールの添付ファイルを開封又はＵＲＬをクリックした者が行う初動対応（ＬＡＮケーブルの抜線、システム管理者への報告等）及び当該法人のＣＳＩＲＴへの報告について訓練を実施。
職員が不審メールと思われる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（「不審メールを提出」ボタン）をメールソフトに設け、日常的に周知。 また、平成 27 年度から、標的型メール訓練において、当該機能による報告の訓練を実施。
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た場合、直ちにＬＡＮケーブルを抜線することができるよう、組織内の端末に接続しているＬＡＮケーブルに非常時に抜線するよう示したテープを貼付。

（注）当省の調査結果による。

表 2－(2)－⑫　行政機関指針における独立行政法人等に対する指導等の規定（「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））（抜粋）

第 11　独立行政法人等に対する指導等 各行政機関は、「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）４に基づき、所管する独立行政法人等に対して、その業務運営における自主性に配慮しつつ、個人情報の保護に関し必要な指導、助言を行う。

（注）下線は当省が付した。

表 2－(2)－⑬　独法等指針における行政機関との連携の規定（「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））（抜粋）

第 11　行政機関との連携 各独立行政法人等は、「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）４を踏まえ、当該独立行政法人等を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行う。

（注）下線は当省が付した。

表 2－(2)－⑭　行政機関と独立行政法人等との連携状況

（単位：機関）

区分	機関数	行政機関と独立行政法人等との連携
行政機関	23 （100％）	23 （100％）
独立行政法人等	201 （100％）	201 （100％）
計	224 （100％）	224 （100％）

（注）1　当省の調査結果による。

2　詳細は行政機関別内訳表及び独立行政法人等別内訳表を参照。

3　本表は、日本年金機構の個人情報流出事案を受けた取組として、①行政機関については、独立行政法人等への指導、助言を行った機関、②独立行政法人等については、所管する行政機関からの指導、助言に対する対応を行った機関を示している。

表 2－(2)－⑮　行政機関と独立行政法人等との連携に係る取組事例（研修・会議関係）

事例の内容
平成 27 年度に当該行政機関が実施した「情報セキュリティ勉強会」及び「情報セキュリティセミナー」に、所管する独立行政法人等の職員も参加。 「情報セキュリティ勉強会」及び「情報セキュリティセミナー」では、日本年金機構の個人情報流出事案を踏まえ、標的型攻撃とセキュリティ対策、官公庁に求められる情報セキュリティ等を議題とした官民の有識者による講演を実施。
平成 27 年度に当該行政機関が実施した情報セキュリティインシデント対応演習に所管する独立行政法人等の職員も参加。 演習は、座学として組織内でインシデントが起きた場合、システム管理者としてどのように判断、行動すべきかを学習するとともに、標的型攻撃による情報漏えい事故を想定した机上演習を実施。
情報セキュリティ強化等に向けた組織・業務改革の一環として、所管する独立行政法人等の役員（理事長及び理事）を対象に、平成 27 年度に 2 回、ＩＴ人材の育成、訓練、脆弱性を突いた攻撃への対応等を議題とした情報セキュリティ対策推進連絡会議を開催。
所管する独立行政法人等と個人情報の取扱いについての情報の共有を行うため、情報公開・個人情報担当課長等会議を定期的に開催。
平成 27 年度に、所管する独立行政法人等のセキュリティ担当者を対象に、個人情報の適切な管理、近年話題となった脅威、インシデント対応等を議題として会議を開催。

（注）当省の調査結果による。

表 2－(2)－⑯　行政機関と独立行政法人等との連携に係る取組事例（点検関係）

事例の内容
所管する独立行政法人等に対し、日本年金機構の個人情報流出事案を踏まえ、①メールの署名がいつもと異なる、②送信元や内容に覚えがないなど、不審な点を感じたら、メールの添付ファイルやＵＲＬを開かず、直ちにセキュリティ担当に連絡することについて、メールの例示や被害拡大防止策も加えた資料を配布し、職員への個人情報を含む重要情報の適切な管理の徹底を依頼。 あわせて、「個人情報を含む重要情報の適正な管理におけるチェック表」を配布し、①標的型メールが確認された場合の注意喚起や教育の実施、②標的型メール攻撃等の事案が発生した場合の連絡体制の構築、③個人情報を含む重要情報が保存されているファイルのパスワード設定、④保護管理規程の整備状況等について、改めて、点検・確認。
日本年金機構の個人情報流出事案を踏まえ、確認項目（複製の制限、個人情報が記録されている媒体が不要となった場合の消去、廃棄状況等）、当該確認項目の保護管理規程上の根拠等を示したチェックリスト（「個人情報ファイルの管理状況」）を作成し、これらにより、所管する独立行政法人等の管理状況を確認。

（注）当省の調査結果による。

表 2－(2)－⑰　行政機関と独立行政法人等との連携に係る取組事例（指導関係）

事例の内容
平成 27 年 10 月に発生した漏えい等事案について、所管の行政機関の担当課に報告した際、同課から当該事案に関する総務省行政管理局への報告の有無について確認を受けたことにより、報告を行うことを失念していたことを認識し、直ちに報告。
所管の行政機関に当該独立行政法人等で発生した漏えい等事案の再発防止策について連絡した際、当該行政機関から注意喚起だけでなく研修を行うよう指示。 このため、平成 27 年度に発生した 2 事案について、発生後速やかに、経緯、原因、被害状況、その後の対策、研修実施の指示があった旨等を具体的に記載した資料を使って緊急研修を実施。

（注）当省の調査結果による。

表 2－(2)－⑱　「個人情報を含む重要情報の適正な管理について」（平成 27 年 6 月 2 日内閣府大臣官房総務課情報公開係）

事　務　連　絡
平成２７年６月２日

各部局個人情報保護担当 各位

大臣官房総務課情報公開係

個人情報を含む重要情報の適正な管理の徹底について

内閣府が保有する個人情報については、「内閣府本府が保有する個人情報管理規程」の規定を遵守すること等により適切に管理していただくようお願いしているところです。

今般、日本年金機構における個人情報の大量流出事案の発生を受けて、平成２７年６月１日、サイバーセキュリティ対策推進会議（CISO 等連絡会議）（第３回）が開催されました。同会議において、サイバーセキュリティ対策推進会議議長より、別添の「点検及び再発防止策の徹底について」の指示がありました。

内閣府における個人情報を含む重要情報の適正な管理について、改めて、必要な措置の徹底を図るようお願いします。

また、万一、個人情報を漏えいしてしまった場合は、被害の拡大防止等の対応を速やかに講じる必要があるので、大臣官房総務課を始め、関係部署への速やかな連絡をお願いします。

独立行政法人等の所管部局におかれましては、所管の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、徹底を指導願います。

【必要な措置例】

・保有個人情報の管理の徹底（アクセスできる職員の範囲の見直し、パスワードの設定、アクセス状況の記録、保有個人情報を保管している執務室等の施錠等）
・重要情報を含む文書の外部への送付は、原則手渡しや親展と記載した上で郵送する。
・電子メールの宛先に外部の者が含まれている場合は、宛先を誤ってＴｏに入力して送信することのないよう、宛先がＢＣＣとなっているかダブルチェック等の誤送信防止を行う。
・ＦＡＸの誤送信防止のため、個人情報を含む重要情報のＦＡＸ送信については、緊急等のやむを得ない場合に限定し、「０」発信かどうかの区別を分かりやすくＦＡＸ機器ごとに明示しておく。
・公用携帯の管理を徹底し、公用携帯に登録する個人情報は必要最小限とし、紛失した場合に備え、他者が操作できないよう暗証番号を設定する。

（注）下線は当省が付した。

表 2－(2)－⑲　「個人情報を含む重要情報の適正な管理について」（平成 27 年 6 月 2 日内閣府大臣官房総務課情報公開係）の独立行政法人等への周知状況

独立行政法人等名	独立行政法人等の所管部局等からの周知状況
国立公文書館	大臣官房公文書管理課から周知なし。
北方領土問題対策協会	北方対策本部から周知なし。
沖縄振興開発金融公庫	沖縄振興局参事官(調査金融担当)から周知。
沖縄科学技術大学院大学学園	沖縄振興局沖縄科学技術大学院大学企画推進室からの周知状況は確認できず。
原子力損害賠償・廃炉等支援機構	原子力損害賠償・廃炉等支援機構担当室から周知なし。
日本医療研究開発機構	通知元である大臣官房総務課情報公開係から所管部局である日本医療研究開発機構担当室に周知せず。

（注）当省の調査結果による。

表 2－(2)－⑳　平成 28 年度に保護管理規程を見直し（改正）した理由

独立行政法人等名	見直し（改正）日	平成 28 年度に見直し（改正）した理由
国立長寿医療研究センター	4 月 1 日改正	平成 27 年度末に見直しする予定であったが、審査作業等が滞ったため年度の切替えに合わせて改正することとしたため。また、所管する行政機関からは独法等指針を示されたのみで、見直しに関する情報提供はされていない。
医薬品医療機器総合機構	4 月 28 日改正	平成 27 年度末に見直しする予定であったが、他の規程等の見直しも重なり、審査作業等が滞ったため。また、所管する行政機関からは独法等指針及び所管する行政機関の改正後の保護管理規程を示されたが、それ以外の見直しに関する情報提供はされていない。
国立国際医療研究センター	4 月 28 日改正	情報セキュリティポリシーの規定で対応しようとしたが、平成 27 年 12 月からの総務省の調査を契機に保護管理規程を改正すべきものと認識したため。
農業・食品産業技術総合研究機構	5 月 26 日改正	平成 28 年 4 月に他機関と統合したことにより、組織全体の規程類の整備をする必要があり作業が滞ったため。また、所管する行政機関からは独法等指針を示されたのみで、見直しに関する情報提供はされていない。
筑波大学	4 月 1 日改正	関連する他の規程と併せて、平成 27 年度中の改正を目指していたが、規程を所管する部署間の調整に時間を要したことに加え、28 年 4 月 1 日からの学内組織の一部改組により、年度の切替えに合わせて改正することとしたため。また、所管する行政機関からは独法等指針及び保護管理規程の見直しに関する事務連絡が送付されたが、それ以外の見直しに関する情報提供はされていない。
京都教育大学	5 月 16 日改正	平成 28 年 1 月に改正案を関係各課に対して協議したが、案に対して多くの意見があり、調整に時間を要することとなったため。また、所管する行政機関からは独法等指針及び保護管理規程の見直しに関する事務連絡が送付されたが、それ以外の見直しに関する情報提供はされていない。
日本年金機構	4 月 30 日改正	平成 27 年 5 月の個人情報流出事案を踏まえ、ハードウェア、ソフトウェア及びその運用に関して根本からの検討を加え、28 年 1 月にセキュリティポリシーを改正するなど、順次実際的な対応を進めてきたが、同年 3 月の総務省の実地調査を契機に保護管理規程上の措置の必要性を認識し、独法等指針以外の改正事項も併せて、同年 4 月に改正を行ったため。

（注）当省の調査結果による。

表 2－(2)－㉑　平成 27 年度に研修が未実施の理由

独立行政法人等名	未実施の理由
航空大学校	研修を実施しようと考えていたが、研修資料やノウハウがなかったため、実施できなかった。

（注）1　当省の調査結果による。

2　平成 27 年度に研修が未実施とは、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）の状況を示す。

表 2－(2)－㉒　平成 27 年度に点検が未実施の理由

独立行政法人等名	未実施の理由
名古屋大学	本件の調査対象期間外の平成 27 年 4 月に既に点検を実施していたため。
山口大学	従来実施していた点検方法について、より効果的な点検を実施するために他機関の実施方法等を参考にするなどして見直していたため。

（注）1　当省の調査結果による。

2　平成 27 年度に点検が未実施とは、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）の状況を示す。