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

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

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。	表 3-(1)-⑧
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。	表 3-(1)-⑨
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。	表 3-(1)-⑩
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。	表 3-(1)-⑪
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。	表 3-(1)-⑫、⑬
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。	表 3-(1)-⑭

表 3－(1)－①　行政機関指針における教育研修の規定（「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　総括保護管理者は、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　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　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。

（注）下線は当省が付した。

表 3－(1)－②　独法等指針における教育研修の規定（「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　総括保護管理者は、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　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　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。

（注）下線は当省が付した。

表 3－(1)－③　教育研修の実施状況

（単位：機関）

区分	機関数	平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	45 (100%)	0 (0.0%)
独立行政法人等	201 (100%)	200 (99.5%)	1 (0.5%)
計	246 (100%)	245 (99.6%)	1 (0.4%)

（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　「平成 27 年度に実施」とは、日本年金機構の個人情報流出事案が発生後の平成 27 年 6 月から 28 年 3 月までの実施状況を記載している（以下同じ。）。

表 3－(1)－④　教育研修の対象

（単位：機関）

区分	機関数	保護管理者	保護担当者	情報システム従事者	独法等の職員	派遣労働者	その他
行政機関	45	39 (86.7%)	43 (95.6%)	39 (86.7%)	13 (28.9%)	23 (51.1%)	37 (82.2%)
独立行政法人等	201	170 (84.6%)	167 (83.1%)	164 (81.6%)	190 (94.5%)	118 (58.7%)	90 (44.8%)
計	246	209 (85.0%)	210 (85.4%)	203 (82.5%)	203 (82.5%)	141 (57.3%)	127 (51.6%)

（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。

表 3－(1)－⑤　教育研修の内容

（単位：機関）

区分	機関数	法律・訓令等の周知	標的型メールへの対応		漏えい等事案発生時の初期対応		情報システムの管理・運用	点検・監査結果を踏まえた個人情報の取扱い	その他
			座学	訓練	座学	訓練			
行政機関	45	37 (82.2%)	38 (84.4%)	43 (95.6%)	38 (84.4%)	9 (20.0%)	34 (75.6%)	21 (46.7%)	14 (31.1%)
独立行政法人等	201	167 (83.1%)	166 (82.6%)	83 (41.3%)	151 (75.1%)	39 (19.4%)	145 (72.1%)	68 (33.8%)	62 (30.8%)
計	246	204 (82.9%)	204 (82.9%)	126 (51.2%)	189 (76.8%)	48 (19.4%)	179 (72.8%)	89 (36.2%)	76 (30.9%)

（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。

表 3－(1)－⑥　標的型メール訓練の方法等

区分	具体的な内容
対象範囲	・日常業務において端末を利用する全職員
	・全役職員（役員・常勤職員・非常勤職員）
	・教員、職員、派遣職員
	・事業者を含む組織のネットワークを利用する者全員
メールの送付方法	・無予告、無作為抽出
	・実在の職員名で送付
	・ＵＲＬ誘導型と添付ファイル型の 2 種類を送付
	・1 回目は全職員。2 回目は 1 回目に開封した職員を中心に実施。2 回目に開封した場合は、ＬＡＮケーブルの抜線、事後対応までの訓練を実施
	・難易度を段階的に高めながら 3 回実施。1 回目は見慣れないアドレスから送付。2 回目は見分けにくいアドレスから組織内のメール形式に則した形式で送付。3 回目は実在する組織が実際に公表している情報を使い、当該組織と似た名称の組織名で送付
実施時期	・夏季休暇及びお盆休みの直後
メールの内容	・インフルエンザ対策の周知 ・実在する課からの作業依頼
	・緊急時の報告体制の周知 ・健康保険制度改正の周知
	・年末年始の長期休暇における注意事項 ・標的型メールへの注意喚起
	・実際に使用しているソフトの脆弱性への緊急対応の依頼
	・情報セキュリティに関する注意喚起
	・至急のウィルスチェックを実施するため、添付の対応手順書を確認するよう促すもの
	・パスワードの変更を促す自動配信メールを装うもの
メール受信後の対応	・メールソフトに設けられた不審メール通報機能により、システム管理者に連絡
メール開封後の対応	・開封者には訓練であることを口外しないよう指示するとともに、別途、教育コンテンツを提示
	・添付ファイル等を開封した職員に開封理由などを調査するアンケートを行うとともに、訓練結果の報告等を含めた研修を実施
	・1 回目に添付ファイル等を開封した職員を教育用コンテンツに誘導し学習させた上で、無予告で再度実施。2 回目も開封した職員に対しては、講義形式の集合研修を実施
訓練結果の活用	・地方支分部局において、本省及び地方支分部局全体の添付ファイル等の開封率と自局の開封率を比較した結果、自局の開封率が高いことが判明。このため、管理職を中心に配布している自局の定期作成資料に、本省及び地方支分部局全体と自局の開封率の比較結果を図示

（注）当省の調査結果による。

表 3－(1)－⑦　漏えい等事案発生時の初期対応の訓練

事例の内容
サイバー攻撃の可能性があることを認知した状況を想定し、異常通信端末の特定、被害状況の確認、関係各所への通報・報告体制の確認、緊急対策会議の開催などの初期対応の訓練を実施。
不審な通信が確認されたとの想定の下、全役職員において、端末のＬＡＮケーブルを抜線し、あわせて、手動でのウィルス対策ソフトのフルスキャン手順を確認。

（注）当省の調査結果による。

表 3－(1)－⑧　保護管理者等に対する研修

事例の内容
個人情報の取扱いが多く、漏えい等事案も発生している部局に赴任前の保護管理者に対し、研修を実施。
地方支分部局の管理者研修（保護管理者を含む。）の１コマを利用して、情報セキュリティ等に関する研修を実施。
保護管理者を対象に、①情報セキュリティの最新動向、②情報セキュリティにおける管理者の役割、③個人情報の適切な取扱い、④行政文書の適切な管理について、研修を実施。

（注）当省の調査結果による。

表 3－(1)－⑨　情報セキュリティ及び文書管理に関する研修との同時開催

事例の内容
本省庁では、管理者向け（保護管理者等）、一般職員（全職員）向けに、①情報セキュリティの最新動向、②情報セキュリティにおける管理者の役割、③個人情報の適切な取扱い、④行政文書の適切な管理について、同時に研修を実施。 また、地方支分部局等でも、事務運営指針により、年度当初の早い段階で全職員（非常勤職員を含む。）を対象に、文書管理、情報セキュリティの確保に関する研修と、個人情報の保護に関する研修を同時に行うことを指示。

（注）当省の調査結果による。

表 3－(1)－⑩　職務・個人情報の取扱いに応じた研修

事例の内容
・新任教員に対し「新任教員職員研修」を義務付け。 ・医療系の部局で実施している e-ラーニング研修では、研修後に習熟テストを実施。基準点を超えなければ、インターネットへの接続を認めない運用。 ・学生に対して、入学時にパンフレットで情報倫理や情報セキュリティについて周知。
・専門職員に対しては、赴任前及びキャリアアップの機会に応じて研修を実施し、専門職員をサポートする職員に対しては毎年度研修を実施。 ・専門職員や専門職員をサポートする職員の個人情報の取扱いの実態を踏まえた研修資料を作成。 ・座学だけではなく、ディスカッションを実施し、職員の意識を高揚。 ・研修後アンケートでは、9 割以上の職員から「意識が変わった」等の意見。
・実際の業務を遂行する際の個人情報の取扱いについて事例を示し、当該事例にどのような問題点があるかについてケーススタディによる討論を実施。

（注）当省の調査結果による。

表 3－(1)－⑪　幹部職員等に対する研修

事例の内容
日本年金機構の個人情報流出事案を受け、ＣＩＯ補佐官から、政務三役、指定職職員、各課室長等に対し、情報セキュリティに関する研修を実施。

（注）当省の調査結果による。

表 3－(1)－⑫　意識の高揚を図るための啓発の実施状況

（単位：機関）

区分	機関数	意識の高揚を図るための啓発の実施
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。

3　(　)は、機関数に占める割合を示す。

表 3－(1)－⑬　組織の長による意識の高揚を図るための啓発

事例の内容
情報セキュリティ月間において、組織の長から職員に対し訓示を実施。
組織の長から全職員に対し、複数回にわたる注意喚起を実施。

（注）当省の調査結果による。

表 3－(1)－⑭　事務用端末の起動時を利用した啓発

事例の内容
従来から、職員の事務用端末の起動時に公務員倫理に関する啓発のページを表示していたが、官公庁に対するサイバー攻撃の増加を受け、個人情報の管理や情報セキュリティに関するページを追加し、複数種類からランダムに表示。啓発ページ全 47 種類のうち個人情報の管理や情報セキュリティに関するものは 7 種類が該当。
日本年金機構の個人情報流出事案を始めとする全国的なサイバー攻撃の発生を受けて、職員の事務用端末を起動した際、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。導入時は無予告で行い、職員からの反響大。

（注）当省の調査結果による。

(2) 点検・監査の実施状況

調査の結果	説明図表番号
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)。	表 3-(2)-①、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)。	表 3-(2)-①、②
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。	表 3-(2)-③
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。	表 3-(2)-④～⑦
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。	表 3-(2)-⑧
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。	表 3-(2)-⑨
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。	表 3-(2)-⑨
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	表 3-(2)-⑩

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。	表 3-(2)-⑪
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。	表 3-(2)-⑫

表 3－(2)－①　行政機関指針における監査・点検の規定（「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10　監査及び点検の実施

（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。

（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）

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。

（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。

（注）下線は当省が付した。

表 3－(2)－②　独法等指針における監査・点検の規定（「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10　監査及び点検の実施

（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。

（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。

（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。

（注）下線は当省が付した。

表 3－(2)－③　点検の実施状況

（単位：機関）

区分	機関数	平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	45 (100%)	0 (0.0%)
独立行政法人等	201 (100%)	199 (99.0%)	2 (1.0%)
計	246 (100%)	244 (99.2%)	2 (0.8%)

（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　(　)は、機関数に占める割合を示す。

表 3－(2)－④　点検内容（複製の最小限化・処理後の消去）

（単位：機関）

区分	機関数	複製の最小限化・処理後の消去					
		複製ルールの遵守			共有フォルダ等への複製の保存		
			平成 27 年度に実施	平成 28 年度に実施予定		平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	45 (100%)	43 (95.6%)	2 (4.4%)	45 (100%)	45 (100%)	0 (0.0%)
独立行政法人等	201 (100%)	195 (97.0%)	154 (76.6%)	41 (20.4%)	191 (95.0%)	138 (68.7%)	53 (26.4%)
計	246 (100%)	240 (97.6%)	197 (80.1%)	43 (17.5%)	236 (95.9%)	183 (74.4%)	53 (21.5%)

（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。また、割合は小数点第 2 位を四捨五入しているため、内訳の計と合計が一致しない場合がある。

表 3－(2)－⑤　点検内容（パスワードの設定、不要な個人情報の廃棄）

（単位：機関）

区分	機関数	パスワードの設定			不要な個人情報の廃棄		
			平成 27 年度に実施	平成 28 年度に実施予定		平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	45 (100%)	44 (97.8%)	1 (2.2%)	45 (100%)	44 (97.8%)	1 (2.2%)
独立行政法人等	201 (100%)	198 (98.5%)	171 (85.1%)	27 (13.4%)	200 (99.5%)	163 (81.1%)	37 (18.4%)
計	246 (100%)	243 (98.8%)	215 (87.4%)	28 (11.4%)	245 (99.6%)	207 (84.1%)	38 (15.4%)

（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。また、割合は小数点第 2 位を四捨五入しているため、内訳の計と合計が一致しない場合がある。

表 3－(2)－⑥　点検内容（漏えい等事案が発生した場合の報告手順等の整備、被害拡大防止のための対処方法）

（単位：機関）

区分	機関数	漏えい等事案が発生した場合の報告手順等の整備			被害拡大防止のための対処方法		
			平成 27 年度に実施	平成 28 年度に実施予定		平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	45 (100%)	44 (97.8%)	1 (2.2%)	45 (100%)	44 (97.8%)	1 (2.2%)
独立行政法人等	201 (100%)	192 (95.5%)	157 (78.1%)	35 (17.4%)	187 (93.0%)	150 (74.6%)	37 (18.4%)
計	246 (100%)	237 (96.3%)	201 (81.7%)	36 (14.6%)	232 (94.3%)	194 (78.9%)	38 (15.4%)

（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。

表 3－(2)－⑦　点検内容（行政機関と独立行政法人等との連携体制の整備）

（単位：機関）

区分	機関数	独立行政法人等との連携体制の整備			当該独立行政法人等を所管する行政機関との連携体制の整備		
			平成 27 年度に実施	平成 28 年度に実施予定		平成 27 年度に実施	平成 28 年度に実施予定
行政機関	23 (100%)	23 (100%)	22 (95.7%)	1 (4.3%)	－	－	－
独立行政法人等	201 (100%)	－	－	－	181 (90.0%)	140 (69.7%)	41 (20.4%)

（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。また、割合は小数点第 2 位を四捨五入しているため、内訳の計と合計が一致しない場合がある。

表 3－(2)－⑧　点検結果による改善例

点検項目	改善内容
複製ルールの遵守	「保護管理者（課室長等）は、職員が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に複製等を行った場合は、処理終了後は不要となった情報を速やかに消去するよう注意喚起を行う。」という規定改正が認識されていなかったため、対象者に周知徹底した。
共有フォルダ等への複製の保存	共有フォルダの不要な個人情報の廃棄を実施した。
	端末のＵＳＢポートへの使用制限措置の設定をした。
パスワードの設定	パスワードを設定すべき保有個人情報に設定されていなかったものがあったため、パスワードの設定を徹底した。
不要な個人情報の廃棄	保存期間が満了し、廃棄すべき個人情報が廃棄されていなかったため、直ちに廃棄した。
漏えい等事案が発生した場合の報告手順等の整備状況	漏えい等事案が発生した場合の報告手順等が整備されていなかったため、緊急連絡体制を整備し、問題事案があった場合の対応や情報セキュリティに関する情報を共有することとした。
	漏えい等事案が発生した場合の連絡体制が整備されていなかったため、整備した。
被害拡大防止のための対処方法	被害拡大防止措置を認識していない者がいたため、再認識させるとともに、事例に応じたマニュアルを整備した。

（注）当省の調査結果による。

表 3－(2)－⑨　点検に係る取組事例

事例の内容
本省庁において、以下のとおり点検を実施。 ①各職員は、チェックシートにより点検。 ②各職員がチェックシートを各係担当課長補佐に提出。 ③担当課長補佐は、各係の点検結果について、各職員への質問や目視により文書等の状態を確認し、その結果を点検票に集約した上で、チェックシートとともに、総括担当課長補佐等に提出。 ④総括担当課長補佐等は、点検結果について、各職員への質問や目視により文書等の状態を確認し、その結果を点検票に集約した上で課長（保護管理者）に説明。 ⑤課長（保護管理者）は、点検結果について、各職員への質問や目視により文書等の状態を確認し、取りまとめられた点検結果について確認。
日本年金機構の個人情報流出事案を受け、9 分野 70 項目のチェックリストによる一斉自己点検を実施。1 件でも不適切な状況がみられた場合は、具体的な改善策を記載した点検結果票を作成するよう指示。
日本年金機構や他の機関の個人情報流出事案を受け、個人情報等を多く取り扱っている部署に対して 4 項目の点検を指示し、同月内に他の部署による目視点検を実施。問題のあった事項について改善を指示するとともに、2 か月後に抜き打ちで同様の目視点検を実施。要改善とされた事項の改善状況等を確認。
支部等の現場において、点検を実施する際は、保護管理者である課長（独法等指針における保護担当者）が全職員分の事務用端末内に保存されているデータを全て表示させて確認し、課長自身の点検は各課長間相互で確認することにより、不要な個人情報が保存されていないか確認を徹底。
業務適正化推進月間のテーマを「日本年金機構への不正アクセスによる情報流出事案を踏まえた業務適正化」として、各自のパソコンや共有フォルダの現状を確認し、不要なデータを消去するよう指示。
本省庁では、文書管理、情報セキュリティの確保及び個人情報の保護に関する点検事項を整理し、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。 また、地方支分部局でも、事務運営指針で示された文書管理、情報セキュリティの確保及び個人情報の保護について、整理した統一的な点検項目により保護管理者が点検を実施。
個人情報と情報セキュリティの担当が各部局に示す点検項目について、個人情報の保護の点検と情報セキュリティの点検で重複している項目を調整。点検結果についても、互いに情報共有。
情報セキュリティの点検・監査の一項目として、個人情報の保護の点検・監査を実施。点検・監査のチェックシートは、情報セキュリティ及び個人情報の保護を含む内容。
地方支分部局に設けられた委員会において、点検で把握した問題点等（発生原因、改善措置、再発防止策）、分析・評価（問題点の分析、過去の点検による改善効果、今後焦点を当てるべきリスクの高い点検項目）を審議。審議された改善策・再発防止策を実施するとともに、本省庁等に報告し、監査で活用。

（注）当省の調査結果による。

表 3－(2)－⑩　監査の実施状況

（単位：機関）

区分	機関数	平成 27 年度に実施	平成 28 年度に実施予定
行政機関	45 (100%)	38 (84.4%)	7 (15.6%)
独立行政法人等	201 (100%)	177 (88.1%)	22 (10.9%)
計	246 (100%)	215 (87.4%)	29 (11.8%)

（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　独立行政法人等では 2 機関が「平成 27 年度に実施」及び「平成 28 年度に実施予定」に該当していないため、両欄の計は独立行政法人等の「機関数」の 201 と合致していない。

表 3－(2)－⑪　監査の実施方法等

取組内容
日常において、個人情報に関する書類等が鍵付きのキャビネット等に保管されているか、退勤時に職員の端末が確実にシャットダウンされているかを確認するため、無予告で対象部署の職員の始業前に監査を実施。
実地監査において、共有フォルダへのアクセス制限の設定状況及び外部記録媒体の管理状況を確認するとともに、個人情報に関する書類等の廃棄状況については、溶解処理証明書などで確認。
監査実施担当職員が、全課室の共有ファイルサーバーの個人情報の保存状況を確認。
文書管理、情報セキュリティの確保及び個人情報の保護に関する監査について、行政文書等の事務監査として、統一的な事務監査表により実施。
個人情報と情報セキュリティの監査は別々に行うものの、準備段階から両担当が連携。個人情報保護担当と情報セキュリティ担当で重複している監査項目を調整。監査結果についても、互いに情報共有。
点検の結果を踏まえて、監査により個人情報の適切な管理がなされているか確認。

（注）当省の調査結果による。

表 3－(2)－⑫　行政機関指針の情報システムにおける安全の確保等の規定（「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６　情報システムにおける安全の確保等

１～６　（略）

７　保護管理者は、保有個人情報を取り扱う情報システムへの外部からの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必要な措置を講ずる。

８　（略）

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。

10　（略）

11　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。

（注）下線は当省が付した。