資料３－３

特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成 26 年特定個人情報保護委員会告示第６号）の一部改正案の新旧対照表

〇平成 26 年特定個人情報保護委員会告示第６号（特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編））

（赤字傍線部分は改正部分）

<table>
<tr><th>改正案</th><th>現行</th></tr>
<tr><td>

特定個人情報の適正な取扱いに関するガイドライン
（行政機関等・地方公共団体等編）

目次
（略）

第１　（略）

第２　用語の定義等
本ガイドラインで使用する用語の定義等については、法令上の定義等に従い、次の表のとおりとする。

<table>
<tr><th>項番</th><th>用語</th><th>定義等</th></tr>
<tr><td>①</td><td>（略）</td><td>（略）</td></tr>
<tr><td>②</td><td>保有個人情報</td><td>行政機関の職員及び独立行政法人等の役員又は職員が職務上作成し、又は取得した個人情報であって、当該行政機関の職員及び当該独立行政法人等の役員又は職員が組織的に利用するものとして、当該行政機関及び独立行政法人等が保有しているものをいう。</td></tr>
</table>

</td><td>

特定個人情報の適正な取扱いに関するガイドライン
（行政機関等・地方公共団体等編）

目次
（略）

第１　（略）

第２　用語の定義等
本ガイドラインで使用する用語の定義等については、法令上の定義等に従い、次の表のとおりとする。

<table>
<tr><th>項番</th><th>用語</th><th>定義等</th></tr>
<tr><td>①</td><td>（略）</td><td>（略）</td></tr>
<tr><td>②</td><td>保有個人情報</td><td>行政機関の職員及び独立行政法人等の役員又は職員が職務上作成し、又は取得した個人情報であって、当該行政機関の職員及び当該独立行政法人等の役員又は職員が組織的に利用するものとして、当該行政機関及び独立行政法人等が保有しているものをいう。</td></tr>
</table>

</td></tr>
</table>

改正案			現行		
		【行政機関個人情報保護法第２条第５項、独立行政法人等個人情報保護法第２条第５項】			【行政機関個人情報保護法第２条第３項、独立行政法人等個人情報保護法第２条第３項】
③・④	（略）	（略）	③・④	（略）	（略）
⑤	個人情報ファイル	＜行政機関等＞ 保有個人情報を含む情報の集合物であって次に掲げるものをいう。 Ⓐ　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの Ⓑ　Ⓐに掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの ＜地方公共団体等＞ 個人情報保護法第２条第１項に規定する個人情報を含む情報の集合物であって、次に掲げるものをいう。 Ⓒ　特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもの Ⓓ　Ⓒに掲げるもののほか、特定の個人情報を容易に検索することができるよ	⑤	個人情報ファイル	＜行政機関等＞ 保有個人情報を含む情報の集合物であって次に掲げるものをいう。 Ⓐ　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの Ⓑ　Ⓐに掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの ＜地方公共団体等＞ 個人情報保護法第２条第１項に規定する個人情報を含む情報の集合物であって、次に掲げるものをいう。 Ⓒ　特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもの Ⓓ　Ⓒに掲げるもののほか、特定の個人情報を容易に検索することができるよ

改正案			現行		
		うに体系的に構成したものとして「個人情報の保護に関する法律施行令」（平成15年政令第507号。以下「個人情報保護法施行令」という。）で定めるもの 【番号法第２条第４項、行政機関個人情報保護法第２条第６項、独立行政法人等個人情報保護法第２条第６項、個人情報保護法第２条第４項、個人情報保護法施行令第３条】			うに体系的に構成したものとして「個人情報の保護に関する法律施行令」（平成15年政令第507号。以下「個人情報保護法施行令」という。）で定めるもの 【番号法第２条第４項、行政機関個人情報保護法第２条第４項、独立行政法人等個人情報保護法第２条第４項、個人情報保護法第２条第２項、個人情報保護法施行令第１条】
⑥～⑱	（略）	（略）	⑥～⑱	（略）	（略）

第３　（略）

第４　各論

第４－１　（略）

第４－２　特定個人情報の安全管理措置等

第４－２－(1)　委託の取扱い

（関係条文）
（略）

1　委託先の監督（番号法第11条、行政機関個人情報保護法第６条、独立行政法人等個人情報保護法第７条）

Ａ　（略）

改正案	現行
B　必要かつ適切な監督 「必要かつ適切な監督」には、①委託先の適切な選定、②委託先に安全管理措置を遵守させるための必要な契約の締結、③委託先における特定個人情報の取扱状況の把握が含まれる。 委託先の選定については、個人番号利用事務等を行う行政機関等及び地方公共団体等は、委託先において、番号法に基づき当該行政機関等及び地方公共団体等が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。具体的な確認事項としては、委託先の設備、技術水準、従業者（注）に対する監督・教育の状況、その他委託先の経営環境等が挙げられる。 委託契約の締結については、契約内容として、秘密保持義務、事業所内からの特定個人情報の持ち出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、特定個人情報を取り扱う従業者の明確化、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定を盛り込むとともに、行政機関等及び地方公共団体等において必要があると認めるときは委託先に対して、実地の監査、調査等を行うことができる規定等を盛り込まなければならない。 委託先における特定個人情報の取扱状況の把握については、前記の契約に基づき報告を求めること、委託先に対して	**B　必要かつ適切な監督** 「必要かつ適切な監督」には、①委託先の適切な選定、②委託先に安全管理措置を遵守させるための必要な契約の締結、③委託先における特定個人情報の取扱状況の把握が含まれる。 委託先の選定については、個人番号利用事務等を行う行政機関等及び地方公共団体等は、委託先において、番号法に基づき当該行政機関等及び地方公共団体等が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。具体的な確認事項としては、委託先の設備、技術水準、従業者（注）に対する監督・教育の状況、その他委託先の経営環境等が挙げられる。 委託契約の締結については、契約内容として、秘密保持義務、事業所内からの特定個人情報の持出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、特定個人情報を取り扱う従業者の明確化、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定を盛り込むとともに、行政機関等及び地方公共団体等において必要があると認めるときは委託先に対して実地の調査を行うことができる規定等を盛り込まなければならない。

改正案	現行
実地の監査、調査等を行うこと等により、委託契約で盛り込んだ内容の実施の程度を把握した上で、委託の内容等の見直しを検討することを含め、適切に評価する。 （注）「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいう。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。	（注）「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいう。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。
2　（略）	2　（略）
第４－２－(2)　（略）	**第４－２－(2)　（略）**
第４－３～第４－５　（略）	**第４－３～第４－５　（略）**
第４－６　行政機関個人情報保護法等の主な規定 （略）	**第４－６　行政機関個人情報保護法等の主な規定** （略）
Ａ～Ｃ　（略）	**Ａ～Ｃ　（略）**
Ｄ　個人情報ファイル簿の作成及び公表（行政機関個人情報保護法第11条） **ａ　個人情報ファイル簿の作成及び公表**（第１項） 行政機関の長は、行政機関個人情報保護法施行令第10条で定めるところにより、当該行政機関が保有している個人情	**Ｄ　個人情報ファイル簿の作成及び公表**（行政機関個人情報保護法第11条） **ａ　個人情報ファイル簿の作成及び公表**（第１項） 行政機関の長は、行政機関個人情報保護法施行令第７条で定めるところにより、当該行政機関が保有している個人情

改正案	現行
報ファイルについて、それぞれ次に掲げる事項を記載した帳簿（以下「個人情報ファイル簿」という。）を作成し、公表しなければならない。 一　個人情報ファイルの名称 二　当該行政機関の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称 三　個人情報ファイルの利用目的 四　個人情報ファイルに記録される項目（以下Ｄにおいて「記録項目」という。）及び本人（他の個人の氏名、生年月日その他の記述等によらないで検索し得る者に限る。ｂにおいて同じ。）として個人情報ファイルに記録される個人の範囲（以下Ｄにおいて「記録範囲」という。） 五　個人情報ファイルに記録される個人情報（以下Ｄにおいて「記録情報」という。）の収集方法 六　記録情報に要配慮個人情報が含まれるときは、その旨 七　記録情報を当該行政機関以外の者に経常的に提供する場合には、その提供先 八　開示、訂正又は利用停止の請求を受理する組織の名称及び所在地 九　訂正又は利用の停止、消去若しくは提供の停止について他の法律又はこれに基づく命令により特別の手続が定められているときは、その旨 十　その他行政機関個人情報保護法施行令第11条で定める事項	報ファイルについて、それぞれ次に掲げる事項を記載した帳簿（以下「個人情報ファイル簿」という。）を作成し、公表しなければならない。 一　個人情報ファイルの名称 二　当該行政機関の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称 三　個人情報ファイルの利用目的 四　個人情報ファイルに記録される項目（以下Ｄにおいて「記録項目」という。）及び本人（他の個人の氏名、生年月日その他の記述等によらないで検索し得る者に限る。ｂにおいて同じ。）として個人情報ファイルに記録される個人の範囲（以下Ｄにおいて「記録範囲」という。） 五　個人情報ファイルに記録される個人情報（以下Ｄにおいて「記録情報」という。）の収集方法 （新設） 六　記録情報を当該行政機関以外の者に経常的に提供する場合には、その提供先 七　開示、訂正又は利用停止の請求を受理する組織の名称及び所在地 八　訂正又は利用の停止、消去若しくは提供の停止について他の法律又はこれに基づく命令により特別の手続が定められているときは、その旨 九　その他行政機関個人情報保護法施行令第８条で定める事項

改正案	現行
ｂ・ｃ　（略）	**ｂ・ｃ　（略）**
Ｅ・Ｆ　（略）	**Ｅ・Ｆ　（略）**
（別添）特定個人情報に関する安全管理措置 （行政機関等・地方公共団体等編）	**（別添）特定個人情報に関する安全管理措置 （行政機関等・地方公共団体等編）**
【目次】 **（略）**	**【目次】** **（略）**
１　（略）	**１　（略）**
２　講ずべき安全管理措置の内容 （略）	**２　講ずべき安全管理措置の内容** （略）
Ａ　（略）	**Ａ　（略）**
Ｂ　取扱規程等の見直し等 １Ａ～Ｃで明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定めるために、取扱規程等の見直し等を行わなければならない。 特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持ち出し等については、責任者の指示に従い行うことを定めること等が重	**Ｂ　取扱規程等の見直し等** １Ａ～Ｃで明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定めるために、取扱規程等の見直し等を行わなければならない。 特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持出し等については、責任者の指示に従い行うことを定めること等が重要

改正案	現行
要である。 **≪手法の例示≫** ＊　取扱規程等は、次に掲げる管理段階ごとに、取扱方法、責任者・事務取扱担当者及びその任務等について定めることが考えられる。具体的に定める事項については、C～F に記述する安全管理措置を織り込むことが重要である。 ①　取得段階 ②　利用段階 ③　保存段階 ④　提供段階 ⑤　削除・廃棄段階 ＊　個人番号利用事務の場合、例えば、次のような事務フローに即して、手続を明確にしておくことが重要である。 ①　住民等からの申請書を受領する方法（本人確認、個人番号の確認等） ②　住民等からの申請書をシステムに入力・保存する方法 ③　個人番号を含む証明書等の作成・印刷方法 ④　個人番号を含む証明書等を住民等に交付する方法 ⑤　申請書及び本人確認書類等の保存方法 ⑥　保存期間を経過した書類等の廃棄方法 **C　組織的安全管理措置** （略）	である。 **≪手法の例示≫** ＊　取扱規程等は、次に掲げる管理段階ごとに、取扱方法、責任者・事務取扱担当者及びその任務等について定めることが考えられる。具体的に定める事項については、C～F に記述する安全管理措置を織り込むことが重要である。 ①　取得段階 ②　利用段階 ③　保存段階 ④　提供段階 ⑤　削除・廃棄段階 ＊　個人番号利用事務の場合、例えば、次のような事務フローに即して、手続を明確にしておくことが重要である。 ①　住民等からの申請書を受領する方法（本人確認、個人番号の確認等） ②　住民等からの申請書をシステムに入力・保存する方法 ③　個人番号を含む証明書等の作成・印刷方法 ④　個人番号を含む証明書等を住民等に交付する方法 ⑤　申請書及び本人確認書類等の保存方法 ⑥　保存期間を経過した書類等の廃棄方法 **C　組織的安全管理措置** （略）

改正案	現行
a　（略） **b　取扱規程等に基づく運用** 取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。 **≪手法の例示≫** ＊　記録する項目としては、次に掲げるものが挙げられる。 ・　特定個人情報ファイルの利用・出力状況の記録 ・　書類・媒体等の持ち運びの記録　→「持ち運び」については、2Ｅｃ参照 ・　特定個人情報ファイルの削除・廃棄記録 ・　削除・廃棄を委託した場合、これを証明する記録等 ・　特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録 ＊　情報システムの利用状況等の記録に関する分析等としては、ログイン実績、アクセスログ等を定期に及び必要に応じ随時に分析することが考えられる。また、ログと関連する書面の記録を照合し、確認することが考えられる。→2Ｆｃ参照	**a　（略）** **b　取扱規程等に基づく運用** 取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等へのアクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずる。また、記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずる。 **≪手法の例示≫** ＊　記録する項目としては、次に掲げるものが挙げられる。 ・　特定個人情報ファイルの利用・出力状況の記録 ・　書類・媒体等の持ち運びの記録 ・　特定個人情報ファイルの削除・廃棄記録 ・　削除・廃棄を委託した場合、これを証明する記録等 ・　特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録 （新設）

改正案	現行
c・d　（略） **e　取扱状況の把握及び安全管理措置の見直し** 監査責任者（地方公共団体等においては相当する者）は、特定個人情報等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（外部監査及び他部署等による点検を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。 総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。 **D　人的安全管理措置** （略） **a　（略）** **b　事務取扱担当者等の教育** 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等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。 また、特定個人情報等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、特定個人情報等の適切	**c・d　（略）** **e　取扱状況の把握及び安全管理措置の見直し** 監査責任者（地方公共団体等においては相当する者）は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に点検又は監査（外部監査を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。 総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。 **D　人的安全管理措置** （略） **a　（略）** **b　事務取扱担当者等の教育** 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等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。 また、特定個人情報等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、特定個人情報等の適切

改正案	現行
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。 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。 前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。 なお、サイバーセキュリティの研修については、番号法に基づき特定個人情報ファイルを取り扱う事務に従事する者に対して、次に掲げるところにより、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティ（「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保に関する事項その他の事項に関する研修を行う（番号法第 29 条の２、番号法施行令第 30 条の２）。 ・　研修の計画をあらかじめ策定し、これに沿ったものとすること。 ・　研修の内容は、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威及び当該脅威による被害の発生又は拡大を防止するため必要な措置に関するものを含むものとすること。 ・　特定個人情報ファイルを取り扱う事務に従事する者の全てに対して、おおむね一年ごとに研修を受けさせるも	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。 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適正な管理のために必要な教育研修を行う。 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、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。 なお、サイバーセキュリティの研修については、番号法に基づき特定個人情報ファイルを取り扱う事務に従事する者に対して、次に掲げるところにより、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティ（「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保に関する事項その他の事項に関する研修を行う（番号法第 29 条の２、番号法施行令第 30 条の２）。 ・　研修の計画をあらかじめ策定し、これに沿ったものとすること。 ・　研修の内容は、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威及び当該脅威による被害の発生又は拡大を防止するため必要な措置に関するものを含むものとすること。 ・　特定個人情報ファイルを取り扱う事務に従事する者の全てに対して、おおむね一年ごとに研修を受けさせるも

改正案	現行
のとすること。	のとすること。
c　（略）	**c　（略）**
E　物理的安全管理措置 （略）	**E　物理的安全管理措置** （略）
a　特定個人情報等を取り扱う区域の管理 特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。 また、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。 行政機関等は、管理区域のうち、基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。地方公共団体等は、次の①及び②に掲げる項目を参考に、適切な措置を講ずる。	**a　特定個人情報等を取り扱う区域の管理** 特定個人情報等の情報漏えい等を防止するために、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。 特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。 行政機関等は、管理区域のうち、基幹的なサーバ一等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。地方公共団体等は、次の①及び②に掲げる項目を参考に、適切な措置を講ずる。

改正案	現行
①・②　（略） **b　（略）** **c　電子媒体等の取扱いにおける漏えい等の防止** 許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。 取扱規程等の手続に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。 「持ち運ぶ」とは、特定個人情報等を管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、庁舎内での移動等であっても、特定個人情報等の紛失・盗難等に留意する必要がある。 **≪手法の例示≫** ＊　特定個人情報等が記録された電子媒体を安全に持ち運ぶ方法としては、持ち出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 ＊　特定個人情報等が記載された書類等を安全に持ち運ぶ方法と	**①・②　（略）** **b　（略）** **c　電子媒体等の取扱いにおける漏えい等の防止** 許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。 取扱規程等の手続に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。 **≪手法の例示≫** ＊　特定個人情報等が記録された電子媒体を安全に持ち運ぶ方法としては、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 ＊　特定個人情報等が記載された書類等を安全に持ち運ぶ方法と

改正案	現行
しては、封緘、目隠しシールの貼付を行うこと等が考えられる。 **d　（略）** **F　技術的安全管理措置** （略） **a　アクセス制御** 情報システムを使用して個人番号利用事務等を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。 **≪手法の例示≫** ＊　アクセス制御を行う方法としては、次に掲げるものが挙げられる。 ・　特定個人情報ファイルを取り扱うことのできる情報システム端末等を限定する。 ・　各情報システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。 ・　ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。 ・　特定個人情報ファイルへのアクセス権を付与すべき者を最	しては、封緘、目隠しシールの貼付を行うこと等が考えられる。 **d　（略）** **F　技術的安全管理措置** （略） **a　アクセス制御** 情報システムを使用して個人番号利用事務等を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。 **≪手法の例示≫** ＊　アクセス制御を行う方法としては、次に掲げるものが挙げられる。 ・　個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。 ・　特定個人情報ファイルを取り扱う情報システム等を、アクセス制御により限定する。 ・　ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。 ・　特定個人情報ファイルへのアクセス権を付与すべき者を最

改正案	現行
小化する。 ・　アクセス権を有する者に付与する権限を最小化する。 ・　情報システムの管理者権限を有するユーザーであっても、情報システムの管理上特定個人情報ファイルの内容を知らなくてもよいのであれば、特定個人情報ファイルへ直接アクセスできないようにアクセス制御をする。 ・　特定個人情報ファイルを取り扱う情報システムに導入したアクセス制御機能の脆弱性等を検証する。	小化する。 ・　アクセス権を有する者に付与する権限を最小化する。 ・　情報システムの管理者権限を有するユーザーであっても、情報システムの管理上特定個人情報ファイルの内容を知らなくてもよいのであれば、特定個人情報ファイルへ直接アクセスできないようにアクセス制御をする。 ・　特定個人情報ファイルを取り扱う情報システムに導入したアクセス制御機能の脆弱性等を検証する。
b　（略）	**b　（略）**
c　不正アクセス等による被害の防止等 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。 **≪手法の例示≫** ＊　特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断することが考えられる。	**c　不正アクセス等による被害の防止等** 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。 **≪手法の例示≫** ＊　特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断することが考えられる。

改正案	現行
＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認することが考えられる。	＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入することが考えられる。
（削除）	＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認することが考えられる。
＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすることが考えられる。	＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすることが考えられる。
＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知することが考えられる。→2Cb参照	＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知することが考えられる。
＊　不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用することが考えられる。	＊　不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用することが考えられる。
＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。	＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。
d　（略）	**d　（略）**
（巻末資料）　（略）	**（巻末資料）　（略）**