資料５

検査結果事例集の更新について

１．趣旨

立入検査を通じて得られた知見を基に、地方公共団体等における特定個人情報を適正に取り扱う上で参考となるよう、立入検査で指摘した指摘事例、把握した好事例及びその他参考情報等の検査結果事例を取りまとめ、29 年度に「マイナンバーを適切に取り扱うためのポイント～検査結果を踏まえて～」として公表している。

本資料は、30 年度に事案追加等の更新を行っているが、令和元年度の立入検査においても有用な事例を把握したことから、再度の更新を行うこととしたい。

なお、公表方法は、前回更新時と同様に、委員会ホームページ掲載後、自治体及び行政機関に更新した旨の事務連絡を発出することとしたい。

２．更新概要

⑴　指摘事例：４件（２件追加、２件内容追加）
⑵　好 事 例：１件追加

	更新等件数	更新事例
指摘事例	４件	【事例９】監査の実施③ 【事例10】教育研修の実施① 【事例13】入退室管理及び機器等の持ち込み制限※ 【事例18】委託先の監督※
好事例	１件	【事例７】端末起動時画面の表示による啓発、注意喚起
その他参考事例	０件	（更新なし）

※事例 13 及び事例 18 は、既存の事例に青字部分の内容を追加したもの

以上

○追加・変更事例

1　指摘事例

【事例９】監査の実施③

＜事例＞

⑴　●●機関において、監査の実施については、監査対象課から特定個人情報等の取扱状況に係る自己点検票の提出を受けて結果を集約するにとどまっており、その運用状況等を監査担当課が第三者の目線で検証する手法となっていなかった。

⑵　●●機関において、定期的に監査を行っていたものの、監査結果を総括責任者に報告していなかった。また、監査対象課に監査結果をフィードバックしていなかったことから、問題点が改善されていなかった。

＜チェックポイント！⑴＞

○　被監査部署から提出された自己点検票の回答を基に助言等を行うに留まっており、自己点検票の回答のとおり運用されているのか確認を行っていなかった。

➢　被監査部署から提出された自己点検票について、その運用状況等を、第三者の目線で客観的に確認する必要があります。たとえば、被監査部署に対して、自己点検の回答のとおり適切に運用が行われているのかを、被監査部署の執務室等で目視により確認することや使用簿や管理簿等の提出を求めて確認することなどが考えられます。

＜チェックポイント！⑵＞

○　監査の結果を総括責任者に報告しておらず、また、被監査部署にフィードバックしていなかったことから問題点が改善されていなかった。

➢　監査を実施するだけでなく、監査結果を受けて必要に応じて取扱規程等や安全管理措置を見直す必要があります。そのため、監査責任者は、監査結果を総括責任者に報告し、総括責任者は必要に応じて、番号制度所管課及び特定個人情報等を取り扱う課に対して、取扱規程等や安全管理措置の見直しを指示する必要があります。

　総括責任者への報告の際には、監査で検出された問題点について、どのように改善を図っていくのか、被監査部局以外への波及の有無などを踏まえ、その改善方法等について検討する必要があります。

　なお、被監査部署において検出された問題点については、監査部署からフィードバックするとともに、改善する期日を設けた上で改善の報告を求めるなど、問題点が改善されているかどうかを確認する必要があります。

※参考

○マイナンバーガイドライン安全管理措置2C　組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し

＜事例７※参考を参照＞

≪人的安全管理措置≫

【事例 10】教育研修の実施①

＜事例＞

⑴　●●機関は、教育研修の実施については、取扱規程において、「総括責任者及び保護責任者は、特定個人情報等の適正な取扱いを確保するため、適切に研修を行うものとする」と規定しているが、必要な研修内容やその対象者については明確になっていなかった。

　このため、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て、特定個人情報等の適切な管理のための教育研修の必要性が認識されておらず、当該研修が実施されていなかった。

⑵　●●機関は、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て、特定個人情報等の適切な管理のための教育研修を毎年実施しているが、当該研修の対象者は、基幹系システム及び住基台帳ネットワークシステムを管理するシステム担当課の職員のみとしていた。このため、担当課で個別に管理する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が研修対象者に含まれていなかった。

＜チェックポイント！⑴＞

○　特定個人情報等の適正な取扱いのために必要となる教育研修について、必要となる研修内容や対象者が明確になっていなかった。

➢　総括責任者及び保護責任者は、番号法及びマイナンバーガイドラインが求める４種類の教育研修を行う必要があります。研修対象者や研修内容が明確になっていない場合、役割等に応じて必要となる教育研修が実施されない可能性がありますので、取扱規程や研修実施要領等で明確にして下さい。

【番号法及びマイナンバーガイドラインが求める研修】

教育研修の種類		対象者
①	特定個人情報等の適正な取扱いに関する研修	事務取扱担当者
②	特定個人情報等を取り扱う情報システムの管理、運用、セキュリティ対策に関する研修	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
③	課室等における特定個人情報等の適切な管理のための研修	保護責任者
④	サイバーセキュリティの確保に関する研修	特定個人情報ファイルを取り扱う事務に従事する者

＜チェックポイント！⑵＞

〇　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て行っている研修の対象者に、担当課で個別に管理するシステム等の管理に関する事務に従事する職員が含まれていなかった。

➢　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て行う研修は、特定個人情報等を取り扱うシステムの管理に関する事務に従事する全ての職員を対象に実施する必要があります。たとえば、生活保護に係る事務を取り扱うシステム等を個別に管理する担当課については、当該システムの管理に従事する職員は研修の対象者となります。

※参考

〇マイナンバーガイドライン安全管理措置２　D　人的安全管理措置　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。

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のとすること。

≪物理的安全管理措置≫

【事例 13】入退室管理及び機器等の持込制限

＜事例＞

⑴　●●機関は、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（管理区域）に入室できる権限については、情報システムの運用担当課の職員のＩＣカードのみに付与し、当該ＩＣカードのログから入退室の記録を確認する運用としている。

しかしながら、システム保守等の際に、ＩＣカードが貸与されていない運用保守業者等に対しては、管理区域への入退室を記録していなかった。

⑵　●●機関は、取扱規程において、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（管理区域）に持ち込む機器等を制限する措置を整備していなかった。

そのため、管理区域としているサーバ室に入室する職員等は、ＵＳＢメモリ等の機器を持ち込むことが可能となっていた。

＜チェックポイント！⑴＞

○　情報システムの運用担当課の職員以外の入退室記録が残されていなかった。

➢　管理区域を明確にし、入退室管理等の措置を講ずる必要があります。

入退室管理においては、入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者が入室する場合の職員の立ち合い等の措置が考えられます。ＩＣカードを貸与していない者についても、別途、入退室記録簿を整備する等により、入退室を記録する必要があります。

＜チェックポイント！⑵＞

○　管理区域は定めていたものの、機器等の持込制限等の措置を整備していなかったことから、ＵＳＢメモリ等の機器を持ち込むことが可能となり、入室する職員等の不正による情報漏えいリスクを抱えている状況となっていた。

➢　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（管理区域）を取扱規程等に規定するなど明確にし、管理区域については、入退室管理や機器等の持込制限をするなど、情報漏えいや滅失、毀損リスクを軽減する措置を講ずる必要があります。

※参考

○マイナンバーガイドライン安全管理措置 2 Ｅ　物理的安全管理措置　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。

① 入退室管理

・ 情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。また、情報システム室等に特定個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。

・ 必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。

・ 必要があると認めるときは、入室に係る認証機能を設定し、及び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。

② 情報システム室等の管理

・ 外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

≪委託及び再委託≫

【事例 18】委託先の監督

＜事例＞

⑴　●●機関は、特定個人情報が記載された給与支払報告書等のパンチ入力業務の委託先の選定に当たって、●機関と同等の安全管理措置が講じられるか否かについて、あらかじめ確認を行わず、前年度と同一の委託先と契約を行った。その理由は、委託先とは、例年、同様の契約を締結しており、特定個人情報の取扱状況は確認していないものの、特段の問題が生じた旨の報告を受けたことが無かったというものであった。

⑵　●●機関は、特定個人情報を取り扱うシステムに係る運用及び保守業務について委託している。委託に際し、委託契約を締結していたが、番号制度開始前からの契約内容を見直しておらず、契約書をそのまま使用していたことから、「特定個人情報を取り扱う従業者の明確化」・「契約内容の遵守状況について報告を求める規定」等が盛り込まれていなかった。

　また、取扱規程において、「委託先における特定個人情報の取扱状況を把握するため、委託先に対する実地の調査を行い、状況を確認するものとする」としていたが、委託契約の締結以降、一度も実地の調査を実施していなかった。

⑶　●●機関は、特定個人情報が記載された給与支払報告書等のパンチ入力業務を委託しており、貸与した給与支払報告書等の特定個人情報が記載された資料は、契約終了後に返却する契約内容としている。しかしながら、委託先において入力されたデータの削除については、契約内容に定められていなかった。

　このため、担当部署において、貸与した資料の返却について確認は行っていたものの、委託先のサーバに保存されていたデータの削除については確認を行っていなかった。

＜チェックポイント！⑴＞

○　委託先とのこれまでの契約実績から、委託先における安全管理措置の状況をあらかじめ確認せずに委託契約を行っていた。

➢　委託先の選定を行う際には、委託先において、番号法に基づき行政機関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、あらかじめ確認する必要があります。具体的な確認内容としては、契約書や仕様書等で求める安全管理措置をどのように講じるのか、委託先の設備や従業者に対する監督・教育の状況等を確認することなどが考えられます。

＜チェックポイント！⑵＞

①　番号制度開始に当たり、既存の契約内容の見直しを行っていなかった。

➢　マイナンバーガイドライン行政編で求められている契約内容を、委託契約に盛り込む必要があります。

② 委託先に対して、実地の調査を実施していなかった。

➢ 実地の監査、調査等の実施や、契約内容の遵守状況について報告を求めること等によって、委託先における特定個人情報の取扱状況を把握し、適切に評価する必要があります。

＜チェックポイント！⑶＞

〇 契約終了後に資料の返却は行われていたが、委託先に保存されていたデータの削除は確認していなかった。

➢ 給与支払報告書等のパンチ入力業務を委託した場合、貸与した資料の返却を確認する以外に、委託先においてデータを確実に削除したことを確認する必要があります。確認の方法としては、削除証明書等の受領や委託先への臨場等が考えられます。なお、本事例においては、契約内容にデータの削除についての定めが無かったため、契約内容の見直しも必要です。

※参考

〇番号法第 11 条

個人番号利用事務等の全部又は一部の委託をする者は、当該委託に係る個人番号利用事務等において取り扱う特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなければならない。

〇マイナンバーガイドライン行政編第４－２－⑴

1 委託先の監督

A 委託先における安全管理措置

個人番号利用事務等の全部又は一部の委託をする行政機関等及び地方公共団体等は、「委託を受けた者」において、番号法に基づき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が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。

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。

２　好事例

【事例７】端末の起動時画面の表示による啓発、注意喚起

＜事例＞

●●機関において、全職員の端末の起動時画面に情報セキュリティに係る研修資料、自己点検の分析結果や監査結果を日替わりで表示させることにより、職員の個人情報保護に関する意識の高揚等を図っている。

＜ポイント！＞

○　全職員が必ず確認する画面に、特定個人情報等に係る情報を日々表示することは、特定個人情報等の適正な取扱いについての理解を深め、特定個人情報等の保護に関する意識の高揚を図るために有効です。また、監査結果等を表示させることにより、問題点が共有され、機関全体における特定個人情報等の取扱いの改善が図られることも期待されます。