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～

平成 29 年６月
（平成 30 年 10 月改訂）
個人情報保護委員会

＜目次＞

２　好事例

３　その他参考情報

はじめに

個人情報保護委員会は、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 29 条の３第１項及び第 35 条第１項に基づき、行政機関等及び地方公共団体等に対して立入検査を実施している。

立入検査においては、主に①個人情報保護委員会が特定個人情報の適正な取扱いを確保するための具体的な指針として策定した「特定個人情報の適正な取扱いに関するガイドライン」（以下「マイナンバーガイドライン」という。）及び特定個人情報の漏えいその他の事態を発生させるリスクを自ら分析し、そのリスクを軽減するための適切な措置について、対外的に明らかにする特定個人情報保護評価書（以下「保護評価書」という。）に沿って、各機関で規程等が適切に整備されているか、②各機関で定めた規程、マイナンバーガイドライン及び保護評価書に基づき、適切な運用がなされているかなどを確認している。

今般、各機関が特定個人情報を取り扱う上で参考となるよう、立入検査で指摘した事例、把握した好事例及びその他参考情報について、「マイナンバーを適切に取り扱うためのポイント」として公表することとした。

行政機関等及び地方公共団体等のみならず、特定個人情報を取り扱う各機関において、本資料が特定個人情報の適正な取扱いを確保するための一助となることを期待している。

なお、事例の理解を深めるため、マイナンバーガイドラインを一読の上、本資料を参照されたい。

また、今後の立入検査等において、有用と思われる事例が生じた場合は、随時追加等を行っていく予定である。

（※）指摘事例、好事例及びその他参考情報は、事例の理解を深めるため、立入検査の結果を一部抽象化するなどしている。

１　指摘事例

以下において、具体的な事例について、＜チェックポイント！＞を記載することで着眼点を示すとともに、参考として、「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）」（以下「マイナンバーガイドライン行政編」という。）の「（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）」（以下「マイナンバーガイドライン安全管理措置」という。）の関係箇所等を記載しています。

≪取扱規程等の見直し等≫

【事例１】取扱規程等の見直し等

＜事例＞

⑴　Ａ機関は、取扱規程等の見直しとして、情報セキュリティ対策基準の改正を行っていた。

しかしながら、当該改正は、「特定個人情報」等を用語の定義に追加するにとどまり、マイナンバーガイドライン安全管理措置で求められている事項を網羅した内容になっていなかった。

⑵　Ｂ機関は、特定個人情報の具体的な取扱いを定めた取扱規程等を策定しておらず、情報セキュリティ対策基準についても、平成 18 年に策定以降、一度も改正していなかった。

このため、事務取扱担当者の明確化、教育研修、漏えい時等の対応体制、監査、削除・廃棄の記録等の安全管理措置が講じられていなかった。

＜チェックポイント！⑴＞

○　情報セキュリティ対策基準の改正が必要だという認識はあったものの、マイナンバーガイドライン安全管理措置との整合性を確認していなかった。

➢　特定個人情報の取扱いについて、情報セキュリティ対策基準等で対応している場合は、特定個人情報の取得から削除・廃棄までの各段階の具体的な事務の流れを念頭に入れ、書類の取扱いも含めて適切に規定する必要があります。

＜チェックポイント！⑵＞

○　取扱規程等を策定していなかったことから、マイナンバーガイドライン安全管理措置で求められている事項について、具体的な実施方法等が定められていなかった。

➢　取扱規程等の見直しに当たっては、マイナンバーガイドライン安全管理措置で求められている事項が網羅された内容になっているか確認する必要があります。

※参考

〇マイナンバーガイドライン安全管理措置[1]A　個人番号を取り扱う事務の範囲の明確化

　行政機関等及び地方公共団体等は、個人番号利用事務等の範囲を明確にしておかなければならない。

〇マイナンバーガイドライン安全管理措置[1]B　特定個人情報等の範囲の明確化

　行政機関等及び地方公共団体等は、Ａで明確化した事務において取り扱う特定個人情報等の範囲を明確にしておかなければならない。

〇マイナンバーガイドライン安全管理措置[1]C　事務取扱担当者の明確化

　行政機関等及び地方公共団体等は、Ａで明確化した事務に従事する事務取扱担当者を明確にしておかなければならない。

〇マイナンバーガイドライン安全管理措置[1]E　取扱規程等の見直し等

　行政機関等は、個人情報の保護に関する管理規程等の見直し等を行わなければならない。また、行政機関等及び地方公共団体等は、Ａ～Ｃで明確化した事務における特定個人情報等の適正な取扱いを確保するために、個人情報の保護に関する取扱規程等の見直し等を行わなければならない。

〇マイナンバーガイドライン安全管理措置[2]B　取扱規程等の見直し等

　[1]Ａ～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要である。

※「地方公共団体等における特定個人情報等取扱要領等」

　（個人情報保護委員会ウェブサイトに掲載）

≪組織的安全管理措置≫

【事例２】事務の範囲及び事務取扱担当者の明確化

＜事例＞

Ｃ機関は、特定個人情報に関する取扱規程を定め、事務分掌表に基づき、個人番号を取り扱う事務に従事する職員を事務取扱担当者として定めている。

しかしながら、マイナンバーカードの申請・交付の事務及びその事務を行っている担当課の非常勤職員、臨時職員等については、当該事務及び当該者を、特定個人情報を取り扱う事務及び事務取扱担当者としていなかった。

＜チェックポイント！＞

① 「マイナンバーカードの申請・交付の事務」について、特定個人情報を取り扱う事務と認識しておらず、個人番号を取り扱う事務の範囲を明確にしていなかった。

➢ 個人番号を取り扱う事務の範囲を明確にし、事務取扱担当者を明確にする必要があります。

② 個人番号を取り扱う事務の範囲を明確にしていなかったことから、当該事務に従事する非常勤職員、臨時職員等を事務取扱担当者としていなかった。

➢ 非常勤職員、臨時職員等に特定個人情報を取り扱わせる場合は、当該者も事務取扱担当者の対象に含める必要があります。

事務の範囲や事務取扱担当者の明確化について、総括責任者が全体を把握せず、所管課任せになっている場合、非常勤職員、臨時職員等が一部の課で対象から漏れている場合等があります。組織として統一的な取扱いとなるよう、規程等に具体的な様式を盛り込むことも有効です。

※参考

〇マイナンバーガイドライン安全管理措置 1 A　個人番号を取り扱う事務の範囲の明確化

〇マイナンバーガイドライン安全管理措置 1 B　特定個人情報等の範囲の明確化

〇マイナンバーガイドライン安全管理措置 1 C　事務取扱担当者の明確化

＜事例１※参考を参照＞

〇マイナンバーガイドライン安全管理措置 2 C　組織的安全管理措置　a　組織体制の整備

安全管理措置を講ずるための組織体制を整備する。

行政機関等は、組織体制の整備として、次に掲げる事項を含める。地方公共団体等は、次に掲げる事項を参考に、適切に組織体制を整備する。

- 総括責任者（行政機関等に各１名）の設置及び責任の明確化
- 保護責任者（個人番号利用事務等を実施する課室等に各１名）の設置及び責任の明確化
- 監査責任者の設置及び責任の明確化
- 事務取扱担当者及びその役割の明確化

・　事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
・　事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制の整備
・　個人番号の漏えい、滅失又は毀損等（以下「情報漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制の整備
・　特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

【事例３】利用状況等の記録

＜事例＞

Ｄ機関において、特定個人情報ファイルへのアクセス記録の確認については、取扱規程において、「管理者は特定個人情報ファイルへのアクセス記録を定期的に確認すること」とし、さらに管理規程において、「監査責任者は、定期的にアクセス記録の確認が行われているか否かを監査し、その結果を個人情報保護管理者に報告すること」としている。

しかしながら、アクセス記録の確認の頻度については、取扱規程において定められていなかったことから、管理者の判断によって実施されている状況であった。そのため、確認の頻度にばらつきがある状況となっていた。

また、アクセス記録の確認方法についても、管理者が特定個人情報ファイルへのアクセス記録を画面閲覧にて確認していたが、確認結果を記録していなかったことから、監査責任者はアクセス記録の確認状況を監査できない状況となっていた。

＜チェックポイント！＞

○　「定期的に」と規定しているが、実施時期や確認頻度を定めず、管理者に任せたままとしていたことから、アクセス記録の確認が適切に行われていなかった。

また、アクセス記録の具体的な確認方法を定めていなかったことから、管理者は確認結果を記録しておらず、監査責任者による適切な監査が実施できない状況となっていた。

➢　監査責任者による適切な監査を実施できるよう、所管課は、アクセス記録の具体的な確認方法（「いつ」、「誰が」、「何を」、「どのように」）を明確に定め、管理者に周知することが重要です。

なお、アクセス記録を保存することは、取扱規程等に基づく確実な事務の実施、情報漏えい等の事案発生の抑止、監査及び情報漏えい等の事案に対処するための有効な手段です。記録として保存する内容及び保存期間は、システムで取り扱う情報の種類、量、システムを取り扱う職員の数、監査の頻度等を総合的に勘案し、適切に定めることが重要です。また、アクセス記録を確認していることを職員へ周知することにより、不正アクセスを防止するけん制効果が期待されます。

※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　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。

○「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関するＱ＆Ａ　Q14－１

【事例４】特定個人情報の持ち運びの記録

＜事例＞

Ｅ機関は、取扱規程において、「特定個人情報を庁舎外へ持ち出す場合については、管理者の許可を得た上で、持出記録簿に記録する」としている。

しかしながら、管理者は取扱規程に基づく手続を担当者に周知していなかったことから、担当者は、当該書類の持ち運びについて、委託先に持ち出しているにもかかわらず、持出記録簿に記録していなかった。

また、管理者は、持出許可の申請が全くなかったことから、個人番号が記載された書類の持ち出しが行われていることを認識していなかった。

＜チェックポイント！＞

○　持出記録簿への記録については規程が整備されていたものの、管理者はその周知をしていなかったことから、担当者は持出記録簿へ記録することなく事務を行っていた。また、管理者が、委託先に個人番号が記載された書類が持ち運ばれていることを認識していなかった。

➢　管理者は、取扱規程に定められた手続を担当者に確実に周知した上で、取扱規程に基づき持出記録簿へ記録し、管理者の許可を得るなど、特定個人情報の取扱状況を把握することが重要です。

※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　ｂ　取扱規程等に基づく運用

＜事例３※参考を参照＞

○マイナンバーガイドライン安全管理措置２Ｅ　物理的安全管理措置　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。

【事例５】特定個人情報の取扱状況の記録の整備

＜事例＞

Ｆ機関は、特定個人情報の取扱状況の記録については、取扱規程において、「特定個人情報等は、適正に収集、保管、利用及び提供すること」としている。

所管課は、文書規程に基づき保存文書目録を作成し、各課室が保有している全ての文書ファイル（簿書）名及び保存期間満了年月について管理していたが、各文書ファイルの簿冊数を記録する仕組みを整備していなかった。また、担当課においては、簿冊数を把握していなかった。

＜チェックポイント！＞

○　所管課は、保存文書目録を作成し、各課室が保有している文書ファイルを管理していたが、文書ファイルの簿冊数を記録する仕組みを整備していなかった。

また、簿冊数を記録する仕組みがないことから、担当課では、簿冊数を把握していなかった。

➢　簿冊の背表紙に番号を振り、保存文書目録等を作成するなど、特定個人情報の取扱状況を把握するために、適切な手段を整備することが重要です。

※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　ｃ　取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況を確認するための手段を整備する。

行政機関等は、次に掲げる項目を含めて記録する。地方公共団体等は、次に掲げる項目を参考に、適切な手段を整備する。

なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

【事例６】情報漏えい事案等に対応する体制等の整備

＜事例＞

⑴　Ｇ機関は、特定個人情報の漏えい事案等が発生した場合の対応については、取扱規程において、「特定個人情報の漏えい事案等が発生した場合、特に重大と認める事案のみを個人情報保護委員会に報告するもの」とし、関係部署に周知していた。

　担当課において、個人番号が記載された転出証明書の誤交付事案が発生し、所管課に対して当該事案が報告されたが、同課は、個人情報保護委員会への報告は不要と判断し、漏えい事案が発生した旨を個人情報保護委員会に対して報告しなかった。

⑵　Ｈ機関は、特定個人情報の漏えい事案等が発生した場合の対応については、取扱規程において、「情報漏えい事案が発生した場合、職員は速やかに管理者に報告する。その報告を受けた管理者は、速やかに『情報漏えい担当窓口』に報告すること」としている。

　担当課において、個人番号が記載された申請書類の誤交付事案が発生し、担当課の職員から報告を受けた同課管理者は、「情報漏えい担当窓口」に報告しようとしたが、同窓口が設置されている部署や担当者が明確になっていなかったことから、報告先が分からず、報告すべき部署への報告に時間を要した。

⑶　Ｉ機関は、特定個人情報の漏えい事案等が発生した場合の対応については、取扱規程において、具体的な報告先を規定し、明確にしていた。

　担当課において、個人番号が記載された申請書類の紛失事案が発生し、担当課の職員が報告先となっている同課管理者に報告を行おうとしたところ、同課管理者が休暇を取得し不在となっていた。管理者が不在時の対応についてルールが定められていなかったことから、担当課の職員は、同課管理者が出勤するまで誰にも報告を行わず、その結果、同課管理者の上位者である幹部までの報告に時間を要した。

＜チェックポイント！⑴＞

○　行政機関等及び地方公共団体等は、個人情報保護委員会が策定した規則、告示等に基づき、漏えい等した特定個人情報の本人の数が１人であっても個人情報保護委員会への報告が必要となるが、認識が誤っていた。

➢　番号法違反の事案又は番号法違反のおそれのある事案を把握した場合には速やかに、重大事態に該当する事案又はそのおそれのある事案は発覚した時点で、直ちに個人情報保護委員会へ報告する必要があります。

　個人情報保護委員会規則、告示等の内容を踏まえて、取扱規程等に適切な内容を規定し、関係部署に周知しましょう。

＜チェックポイント！⑵＞

○　所管課は、報告先となる「情報漏えい担当窓口」の具体的な部署や担当者について、明確にしていなかった。

➢　情報漏えい時の報告体制については、職員が報告先を正確に把握できるよう窓口を明確にし、関係部署に周知することで、迅速かつ適切な報告をするための体制を整備する必要があります。

＜チェックポイント！⑶＞

〇　報告先となっている者が不在時の対応についてルールが定められていなかった。

➢　指定された報告先に該当する者が不在であっても、幹部まで迅速な報告がなされるよう報告ルートを確立する必要があります。

※参考

〇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　d　情報漏えい等事案に対応する体制等の整備

　情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制及び手順等を整備する。

　情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。

〇特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則（平成 27 年特定個人情報保護委員会規則第５号）

〇独立行政法人等及び地方公共団体等における特定個人情報の漏えい事案等が発生した場合の対応について（平成 27 年特定個人情報保護委員会告示第１号）

〇行政機関における特定個人情報の漏えい事案等が発生した場合の対応について

【事例７】監査の実施①

＜事例＞

Ｊ機関において、監査の実施については、取扱規程において、「監査責任者は、特定個人情報の適正な管理の状況を検証するため、定期に及び必要に応じ随時に監査を実施し、その結果を総括責任者に報告すること」としている。

しかしながら、監査担当課が具体的な計画、実施方法を定めていないことから、監査が実施されていなかった。

＜チェックポイント！＞

○　「定期に及び必要に応じ随時に監査を実施し」と規定しているが、具体的な計画や実施方法を定めていなかったことから、監査が実施されていなかった。

➢　監査は、実施することはもちろん、実施した上で問題点の洗い出しや改善策の検討を行うことが必要ですので、具体的な実施方法や計画を策定し、適切に監査を実施しましょう。

また、総括責任者は監査の報告を受け、問題点のフォローアップをする必要があります。

なお、監査と関連させて自己点検を実施することは、被監査部署における特定個人情報の取扱状況を事前に把握することができ、また、自己点検の結果を基に随時の監査を実施するなど、実効性のある監査を実施することができるため有効です。

※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

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。

※「地方公共団体等における監査のためのチェックリスト～マイナンバーの適正な取扱いのために～」（個人情報保護委員会ウェブサイトに掲載）

【事例８】監査の実施②

＜事例＞

Ｋ機関において、監査の実施については、情報セキュリティ対策基準に基づく情報セキュリティ監査は実施されていたものの、特定個人情報の取扱いに関する監査項目（事務取扱担当者の明確化、個人番号が記載された書類の保管等）が含まれていなかった。

＜チェックポイント！＞

○　情報セキュリティ監査を実施していることで、特定個人情報の取扱いに関する監査を実施できているものと誤認していた。

➢　特定個人情報の取扱いに関する監査を情報セキュリティ監査に含めて実施する場合は、監査項目に書類の取扱いに関する項目やマイナンバーガイドライン特有の項目が含まれているか確認する必要があります。

なお、特定個人情報の取扱いに関する監査と情報セキュリティ監査を同時に実施することは、効率化の観点から有効です。

※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９】教育研修の実施①

＜事例＞

Ｌ機関は、教育研修の実施については、取扱規程において、「取扱責任者は、所属する職員等に対し、特定個人情報の取扱いについて理解を深め、特定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定期的に行うこと」としている。

所管課は、事務取扱担当者に該当する職員 400 名を対象に「マイナンバー制度研修」を実施したが、そのうち 80 名が欠席していた。

また、所管課は、同研修の受講者が所属課内で伝達研修を実施するように指示していたが、その実施状況を把握していなかったほか、一部の課では、伝達研修の受講実績を記録しておらず、未受講者を把握していなかった。

＜チェックポイント！＞

① 所管課は、研修を実施して、欠席者を把握していたが、欠席者へのフォローアップをしていなかった。

また、所属課では、伝達研修を実施したが、伝達研修の実施状況の記録を残しておらず、受講者を特定することができなかったことから、欠席者へのフォローアップをしていなかった。

➢ 事務取扱担当者に該当する全職員（非常勤職員、臨時職員等を含む。）に対して研修を確実に実施し、特定個人情報を適正に取り扱うための正確な知識を習得させる必要があるため、研修の実施状況を記録して出欠を的確に把握するとともに、未受講者に対してフォローアップを行うなど、研修を確実に実施するための措置を講じる必要があります。

② 所管課より所属課に対し、研修を踏まえた課内伝達研修を実施するよう指示をしていたが、所管課においては、全職員に対して、確実に研修を実施する措置を講じていなかった。

➢ 所管課は、伝達研修の実施状況について担当課から報告を求めるなどして、実施状況を把握することが重要です。

※参考

〇マイナンバーガイドライン安全管理措置２Ｄ　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。

　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。

（以下、略）

【事例 10】教育研修の実施②

＜事例＞

M機関は、教育研修の実施については、取扱規程において、「総括責任者は、保護責任者に対し、課室等における特定個人情報の適切な管理のために必要な教育研修を行う、また、毎年度、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、サイバーセキュリティの確保に関する研修を行う」としている。

しかしながら、所管課は、事務取扱担当者に対する研修は実施していたものの、保護責任者に対する研修は実施していなかった。

また、サイバーセキュリティの確保に関する研修については、特定個人情報ファイルを取り扱う事務に従事する全ての者に対して、昨年度は実施していたものの、今年度は実施していなかった。

＜チェックポイント！＞

① 所管課は、保護責任者に対する研修が必要なことを認識していなかった。

➢ 特定個人情報の適切な管理のためには、保護責任者に対する研修を実施する必要があります。

② サイバーセキュリティの確保に関する研修を、毎年度実施する認識がなかった。

➢ サイバーセキュリティの確保に関する研修については、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実施する必要があります。

※参考

〇マイナンバーガイドライン安全管理措置２D　人的安全管理措置　b　事務取扱担当者等の教育

（中略）＜事例９※参考を参照＞

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 11】機器等の持込制限

＜事例＞

Ｎ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！＞

○　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２Ｅ　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。

【事例 12】特定個人情報が含まれている書類の保管方法

＜事例＞

○機関は、取扱規程において、「特定個人情報が記録された書類及び電磁的記録媒体を施錠可能な場所に保管するなどの方法により適正に管理すること」としている。

担当課では、特定個人情報が記載された書類を施錠された書庫で保管しており、当該書庫には、登記情報が記載された書類も保管されているが、特定個人情報が記載された書類の一部が編てつされていない状態で書棚外に放置されており、書庫に入室した他課職員に特定個人情報が記載された書類が見えてしまう状況にあった。

＜チェックポイント！＞

○　特定個人情報を取り扱うことができない職員が、書庫内に入室した際に、特定個人情報が容易に閲覧等できてしまう状況にあった。

➢　特定個人情報が記載された書類を保管する書庫は、取扱区域に該当することから、当該書類を書庫で保管する際のルールを定めるなど、事務取扱担当者等以外の者が容易に閲覧等できないよう、保管方法を見直す必要があります。

※参考

○マイナンバーガイドライン安全管理措置2E　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

＜事例 11※参考を参照＞

【事例 13】電子媒体の接続制限等

＜事例＞

Ｐ機関は、電子媒体の取扱いについて、組織としての統一的なルール等を定めていなかった。

このため、所管課は、特定個人情報を取り扱う業務端末に電子媒体の接続を制限しておらず、許可されていない電子媒体により特定個人情報が取り出せる状態となっていた。

また、電子媒体の管理について、担当者に電子媒体を常時所持させ、管理者が使用状況を管理していなかった。

＜チェックポイント！＞

① 電子媒体の取扱いについて、組織としての統一的なルール等を定めておらず、特定個人情報を取り扱う業務端末への電子媒体の接続を制限していなかった。

➢ 電子媒体等の取扱いに関する組織としての統一的なルール等を定めた上で、特定個人情報を取り扱う業務端末について、記録機能を有する機器の接続を制限する必要があります。

② 管理者が電子媒体を管理しておらず、使用状況も把握していなかった。

➢ 電子媒体等について、管理者が管理し、使用時に貸し出すことで使用状況を把握することが重要です。

※参考

〇マイナンバーガイドライン安全管理措置２Ｅ　物理的安全管理措置　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。

【事例 14】削除・廃棄記録の整備等

＜事例＞

Q機関は、文書（電子データを含む。）の削除・廃棄について、記録、報告等の具体的な手順を定めていないことから、各部署において特定個人情報が記録・記載された文書の削除・廃棄の記録が保存されておらず、文書管理者への報告も行われていなかった。

＜チェックポイント！＞

○　文書の削除・廃棄の手順が明確になっていなかったことから、削除・廃棄の記録が保存されておらず、削除・廃棄の詳細（「いつ」、「誰が」、「何を」、「どのように」）が確認できる体制となっていなかった。

➢　文書の削除・廃棄について、具体的な手順等を定め、当該手順等に基づいて運用を行うことが重要です。

※参考

○マイナンバーガイドライン安全管理措置２Ｅ　物理的安全管理措置　ｄ　個人番号の削除、機器及び電子媒体等の廃棄

特定個人情報等が記録された電子媒体及び書類等について、文書管理に関する規程等によって定められている保存期間を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除又は廃棄する。

→マイナンバーガイドライン第４－３－⑷Ｂ参照

個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

≪技術的安全管理措置≫

【事例 15】アクセス制御

＜事例＞

Ｒ機関は、システムの利用者に係るユーザー情報の登録又は変更については、システム管理規程等において、「人事異動等により個人番号を取り扱う職員に変更が生じる場合には、速やかに『ユーザー情報変更申請書』をアクセス権限を管理しているシステム担当課に提出し、個人番号事務を取り扱うシステムのアクセス権限の付与又は削除を行うこと」としている。

しかしながら、担当課において、人事異動等により個人番号を取り扱う事務を行わないこととなった職員の「ユーザー情報変更申請書」をシステム担当課に提出していなかったことから、当該職員のシステムへのアクセス権限が削除されていなかった。

＜チェックポイント！＞

○　アクセス権限を管理する部署が、人事異動等の情報を把握しておらず、アクセス権限について適切な管理を行っていなかった。

また、人事異動時に個人番号事務権限の付与又は削除を行う手続の職員への周知が不十分であった。

➢　システム、ファイル等の使用について、部門ごとに業務区分をマトリックス表等で管理を行うなどして対象者を限定し、適切な者にアクセス権限を付与する必要があります。

なお、人事異動等に際しては、人事異動等の手続にアクセス権限の登録、変更、削除に係る事項を盛り込むなど、人事部門とアクセス権限を管理するシステム部門で連携を図ることが有効な手段と考えられます。

また、アクセス権限を管理している部署において、定期的にユーザー情報の登録状況を確認することも有効です。

※参考

○マイナンバーガイドライン安全管理措置２Ｆ　技術的安全管理措置　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。

≪委託及び再委託≫

【事例 16】委託先の監督

＜事例＞

Ｓ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。

＜チェックポイント！＞

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。

※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－(1)

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。

【事例 17】再委託の要件

＜事例＞

Ｔ機関は、個人番号利用事務等の一部を委託している。委託契約書において、再委託の制限又は条件に関する事項として、「再委託する場合は、委託元の書面による許諾を得なければならない」としている。

しかしながら、再委託について、許諾を行わないまま、再委託先に特定個人情報を取り扱わせていた。

＜チェックポイント！＞

① 委託元が、再委託の諾否を判断しないまま、再委託先に特定個人情報を取り扱わせていた。

➢ 再委託の要件として、委託元の許諾を得ることが必要です。

なお、委託先が委託元に無断で再委託することもあることから、委託元は委託先に対して実地の監査、調査等を行うこと等により、委託先の特定個人情報の取扱状況を把握する必要があります。

② 再委託について、委託契約に基づく書面による許諾を行っていなかった。

➢ 再委託の許諾の方法について、特段の制限はありませんが、安全管理措置について確認する必要があることに鑑み、書面等により記録として残る形式を取ることが望ましく、口頭の許諾の場合であっても、メモを作成するなどにより証跡を残しておくことが有効です。

※参考

〇番号法第 10 条第１項

個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）の全部又は一部の委託を受けた者は、当該個人番号利用事務等の委託をした者の許諾を得た場合に限り、その全部又は一部の再委託をすることができる。

〇番号法第 11 条

＜事例 16※参考を参照＞

〇マイナンバーガイドライン行政編第４－２－(1)

2 再委託

Ａ 再委託の要件

個人番号利用事務等の全部又は一部の「委託を受けた者」は、当該個人番号利用事務等の委託をした者の許諾を得た場合に限り、再委託をすることができる。

Ｂ 再委託の効果

再委託を受けた者は、個人番号利用事務等の全部又は一部の「委託を受けた者」とみなされ、再委託を受けた個人番号利用事務等を行うことができるほか、最初に当該個人番号利用事務等の委託をした者である行政機関等又は地方公共団体等の許諾を得た場合に限り、その

事務を更に再委託することができる。

　このように、行政機関等又は地方公共団体等が許諾を与えることが個人番号利用事務等の再委託の要件とされていることから、行政機関等又は地方公共団体等は、委託をす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適切な安全管理が図られることを確認した上で再委託の諾否を判断しなければならない。

２　好事例

【事例１】保管書類の背表紙の模様による検知

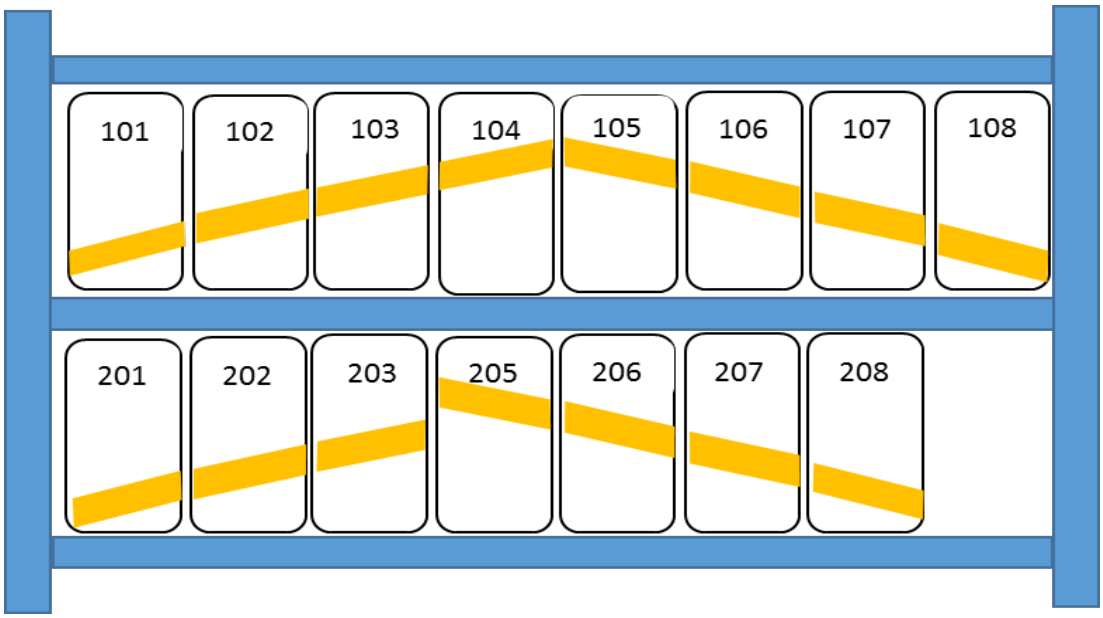
＜事例＞

Ｕ機関において、書庫に保管されている書類の背表紙に連続した模様を付すことにより、簿冊が全てそろっていることを容易に確認できるように取り組んでいる。

＜ポイント！＞

○　簿冊の不足を一目で把握でき、特定個人情報等が記載された書類の適切な保管・管理に有効です。

＜保管書類の背表紙の模様（イメージ図）＞



【事例２】システムのＩＤ管理

＜事例＞

Ｗ機関において、職員の採用、異動、退職等の人事情報については、人事部門が一元管理している。

情報システムに係るアクセス権限の設定は、システム部門が人事部門から提供される人事データを情報システムに取り込むことにより、自動的に必要な権限が付与され、不要となった権限が削除される仕組みとなっている。

＜ポイント！＞

○　年に１度、ＩＤを更新することは、異動した職員等のアクセス権限の削除漏れや、異動先におけるＩＤの不正使用、業務に必要なアクセス権限の見直し等に有効です。

【事例３】アクセス権限の設定

＜事例＞

Ｖ機関において、システムにおけるアクセス制御については、個人ごとに付与するＩＤ及びパスワードにより行っており、当該ＩＤの付与又は削除は所管課が一元的に管理している。

この運用の下で、所管課は、異動又は退職した職員に付与されたアクセス権限の削除漏れを防止するため、年に１度、利用者全員のＩＤを全て削除した上で、新たなＩＤを利用者に付与する措置を講じている。

＜ポイント！＞

○　アクセス権限の設定のために人事部門が作成した人事データを情報システムに取り込むことは、設定作業の効率化、手作業による設定誤りの防止等のための有効です。

【事例４】危機管理ポケットマニュアルの全職員配付

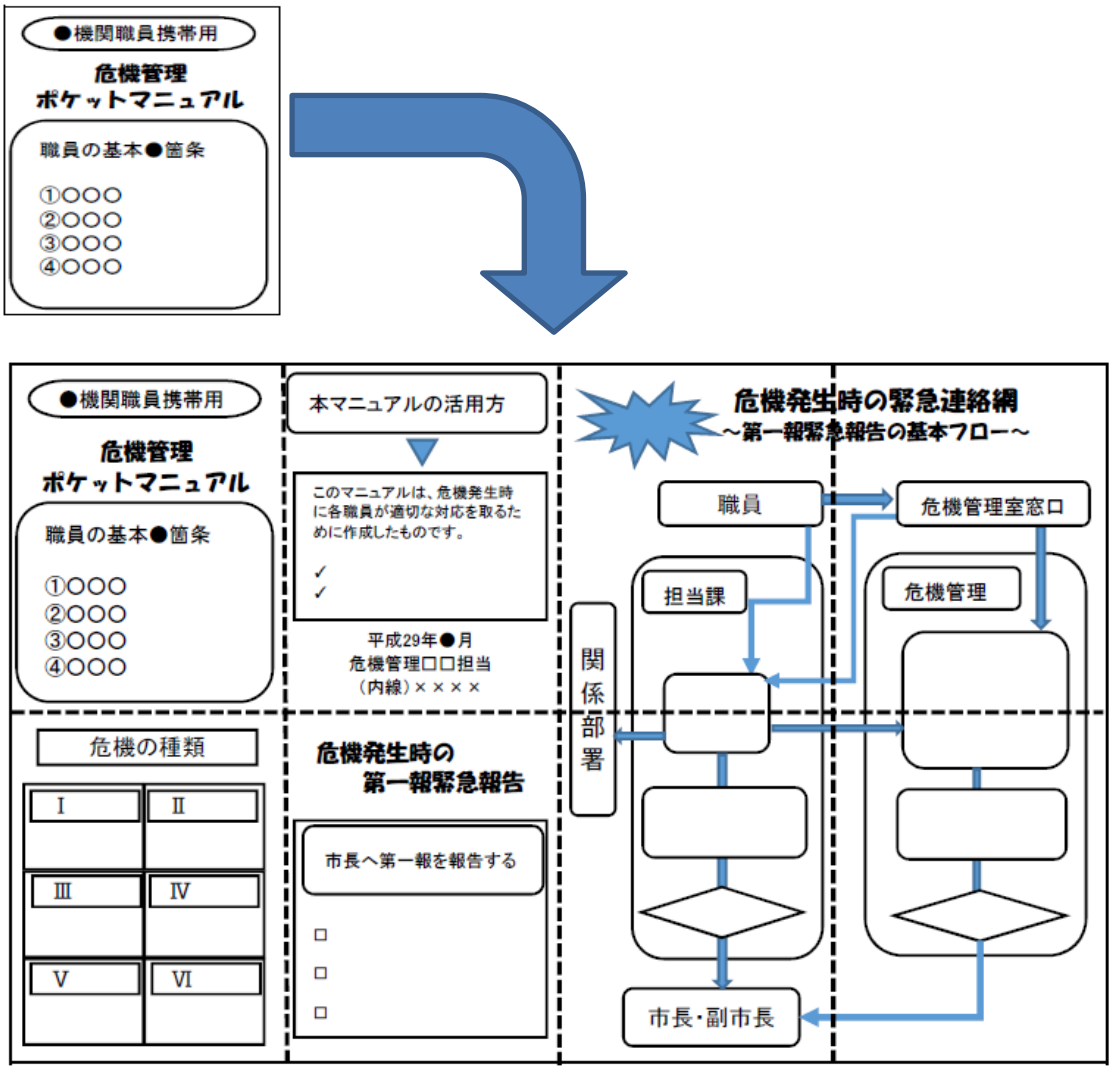
＜事例＞

Ｘ機関において、全職員にカードサイズの危機管理ポケットマニュアルを配付し、身分証ケースに入れるなどして常時携帯させ、情報漏えい事案発生時、職員が迅速・的確な対応を図れるよう措置を講じている。

＜ポイント！＞

○　情報漏えい事案発生時の対応体制等を全職員に常時携帯させることは、報告体制の意識付け及び事案発生時の適切かつ迅速な対応のために有効です。

＜危機管理ポケットマニュアル（イメージ）＞



【事例５】相互監査の実施

＜事例＞

Ｙ機関は、近隣の他機関と定期的に協議会を開催しており、システムの共同調達等を協議している。

当該協議会においてセキュリティの向上対策について検討した結果、監査における外部の視点を取り入れる趣旨から、協議会内で、相互監査を実施している。

＜ポイント！＞

○　相互監査の実施により、他機関の特定個人情報等の管理状況を把握することで、監査担当者は特定個人情報等に関する理解の向上を図ることができ、また、監査結果を活用し、被監査機関のみならず監査機関の特定個人情報等の管理状況を改善することができるため有効です。

【事例６】情報セキュリティ研修の共同調達

＜事例＞

Ｚ機関は、予算を節約し、効率的な執行に努めるため、他機関と共同で情報セキュリティ研修を業務委託している。

研修への参加は、各機関のシステム管理者を必須とし、システム担当者については、できる限り多くの希望者を参加させている。

＜ポイント！＞

○　共同調達は、予算の節約はもとより、各機関が重要としている項目を盛り込むことができるなど、単独での実施に比べ研修内容を充実させることができるほか、研修へ参加した各機関の職員の情報交換等の契機となるため有効です。

３　その他参考情報

【事例１】バックアップの保管

＜事例＞

甲機関は、バックアップの取得について取扱規程において、「担当者は、サーバのバックアップを記録媒体に記録する」としており、情報資産の保管については、セキュリティ対策基準等において、「特定個人情報を記録した記録媒体は、鍵のかかる書庫等に適切に保管しなければならない」としている。

しかしながら、バックアップが記録されている記録媒体は、鍵のかかるラックの中に保管されているものの、当該ラックにはサーバ本体も保管されていた。

＜ポイント！＞

○　サーバのバックアップを記録している記録媒体が同サーバと同一の場所に保管されており、災害等により双方に被害が及んだ際には、特定個人情報の滅失又は毀損につながるおそれがあります。

○　特定個人情報は災害時にも活用されるため、業務の継続性を考慮した上で、バックアップされたデータの保管場所等を検討することが重要です。

※参考

○「市町村のための業務継続計画作成ガイド（内閣府（防災担当））」より抜粋

４．業務継続計画の特に重要な６要素

業務継続計画の中核となり、その策定に当たって必ず定めるべき特に重要な要素として以下の６要素がある。

⑸　重要な行政データのバックアップ

業務の遂行に必要となる重要な行政データのバックアップを確保する。

・災害時の被災者支援や住民対応にも、行政データが不可欠。

【事例２】利用状況等の記録に関する分析等

＜事例＞

乙機関は、システムへのログイン実績及びアクセスログについて、毎月、当該実績等を出力し、管理者が、勤務時間外や休日等の利用状況及び担当業務以外へのアクセスの有無、照会件数等の急増等を確認している。

＜ポイント！＞

○　特定個人情報を取り扱うシステムの利用状況（ログイン実績、アクセスログ等）を、定期的に確認（「いつ」、「誰が」、「何を」、「どのように」）することが重要です。

※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　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。

（中略）

・　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