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
個人情報保護委員会

＜目次＞

まずは、「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）」を一読の上、本事例集を参照していただきますようお願いします。

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、行政機関及び地方公共団体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、立入検査で把握した指摘事例、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。

行政機関及び地方公共団体のみならず、特定個人情報を取り扱う機関において、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。

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、内容を御理解いただくため、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、＜何がいけなかった？＞及び＜チェックポイント！＞といった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）（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。）の関係箇所を記載しています。

≪組織的安全管理措置≫

【事例１】事務の範囲及び事務取扱担当者の明確化

＜事例＞

Ａ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、担当課の非常勤職員が、特定個人情報が記載された申請書・届出書等を含む郵便物を開封し、内容を確認して担当者に配付しているにもかかわらず、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。

また、担当課の臨時職員が、マイナンバーカードの申請及び交付の事務に携わっているにもかかわらず、当該事務及び当該者を、特定個人情報の取り扱う事務及び事務取扱担当者としていなかった。

＜何がいけなかった？＞

✓　担当課の認識不足により、特定個人情報を取り扱う事務を把握しておらず、事務の範囲を明確にしていなかった。

✓　事務の範囲を明確にしていなかったことから、誰が何を行うか明確にできず、事務取扱担当者と認識できなかった。

＜チェックポイント！＞

✓　特定個人情報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ことが重要です。

✓　例えば、受付窓口での収受事務、廃棄事務の担当者も、その事務において特定個人情報等を取り扱う場合には、事務取扱担当者になりますので、事務の流れに当てはめて、事務取扱担当者に漏れや誤りがないか確認しましょう。

※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1B　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1C　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2C　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２】アクセスの記録

＜事例＞

Ｂ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。

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いことから、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。

＜何がいけなかった？＞

✓　「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。

✓　アクセス記録の具体的な確認方法を示し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されていなかった。

＜チェックポイント！＞

✓　具体的な確認方法（「いつ」、「誰が」、「何を」、「どのように」）を明確に規定しましょう。

✓　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を定め、管理者に周知することが重要です。

✓　アクセスの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、点検・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、点検・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働きます。

※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　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。

〇「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　Ｑ14－２

【事例３】特定個人情報の取扱状況の記録の整備

＜事例＞

Ｃ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。

＜何がいけなかった？＞

✓　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。

✓　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。

＜チェックポイント！＞

✓　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

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　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４】情報漏えい事案等に対応する体制等の整備

＜事例＞

Ｄ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。

＜何がいけなかった？＞

✓　行政機関及び地方公共団体等は、個人情報保護委員会が策定した告示に基づき、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。

＜チェックポイント！＞

✓　当委員会の規則及び告示の内容を踏まえて、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。

✓　個人情報保護委員会への報告は、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、直ちに報告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）

【事例５】情報漏えい時の報告体制の整備

＜事例＞

①Ｅ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。

②Ｆ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誤交付事案が発生し、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。

＜①何がいけなかった？＞

✓　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。

＜①チェックポイント！＞

✓　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整備をすることが重要です。

＜②何がいけなかった？＞

✓　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。

＜②チェックポイント！＞

✓　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）

【事例６】自己点検及び監査

＜事例＞

Ｇ機関において、自己点検の実施については、取扱規程において、「取扱責任者は、自ら管理責任を有する特定個人情報の管理状況について定期又は随時に点検を行い、その結果を総括責任者に報告すること」とし、監査の実施については、同規程に基づき、「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、定期又は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、自己点検については、所管課が具体的な実施方法及び報告方法の検討並びに各課への周知を行っておらず、監査については、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、自己点検及び監査が実施されなかった。

＜何がいけなかった？＞

✓ 「定期に又は随時に点検を行い」と規定しているが、自己点検については、具体的な実施方法、報告方法の検討を行っておらず、監査については、具体的な計画や実施方法を定めていなかったことから、自己点検及び監査が実施されなかった。

✓ 所管課から各課への周知が行われなかったことから、各課の自己点検に対する認識が不十分であり、実施されなかった。

＜チェックポイント！＞

✓ 自己点検は、各事務の共通点検項目と個別点検項目があることが考えられるので、関係各課で協力して、自己点検チェックシートを作成するなど具体的な実施方法を定め、実施時期を含めて周知しましょう。

✓ 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。

✓ 自己点検又は監査の報告を受け、問題点のフォローアップを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。

≪人的安全管理措置≫

【事例７】教育研修の実施①

＜事例＞

Ｈ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、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、各所属長は、所管課から、所属職員に対して同研修を踏まえた課内研修を実施するように指示を受けていたが、一部の所属長は、欠席した所属職員に対して研修を実施していなかった。

＜何がいけなかった？＞

✓　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。

✓　所管課より各課に対し、研修を踏まえた課内研修を実施する旨の指示はあったが、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。

＜チェックポイント！＞

✓　全職員（非常勤職員や臨時職員を含む。）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ことが重要です。

✓　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しましょう。

※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。

【事例８】教育研修の実施②

＜事例＞

Ｉ機関は、教育研修の実施については、取扱規程において、「特定個人情報の取扱いに従事する職員に対し、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こと」としている。

所管課は、特定個人情報を取り扱う担当者を対象にマイナンバー制度に関する研修を実施し、また、各課に対して、当該研修受講者が講師となって、事務取扱担当者に伝達研修を実施するように指示していたが、各課において、伝達研修の受講実績を記録していなかった。

＜何がいけなかった？＞

✓　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することができなかった。

✓　所管課より各課に対し、伝達研修を実施する旨の指示は行ったが、伝達研修の実施状況を把握する措置を講じていなかった。

＜チェックポイント！＞

✓　全職員（非常勤職員や臨時職員を含む。）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ことが重要です。

✓　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ましょう。

✓　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しましょう。

※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。

≪物理的安全管理措置≫

【事例９】機器等の持込制限

＜事例＞

Ｊ機関は、特定個人情報の取扱いについて定めている取扱規程において、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に関する規定は定められていなかった。

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。

＜何がいけなかった？＞

✓　管理区域は定めていたものの、機器等の持込制限等の規定を取扱規程に定めていなかった。

✓　当該規定を定めていないことから、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漏えいリスクを抱えている状況となっていた。

＜チェックポイント！＞

✓　特定個人情報等を取り扱う事務を実施する区域（取扱区域）と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ましょう。

✓　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、漏えいや滅失、毀損リスクを軽減する措置を講じましょう。

※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　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、基幹的なサーバー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 10】特定個人情報が含まれている書類の保管方法

＜事例＞

Ｋ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、過去からの登記情報が記載された書類も保管されている。当該登記情報が記載された書類は、他課の職員も利用することから、当該書庫には、特定個人情報を取り扱わない他課職員が入室する場合がある。その際、書庫で保管している書類等の情報の漏えいを防止するために、担当課職員が立ち会うこととなっているものの、特定個人情報が記載された書類は、書庫内の開放された書棚に保管されているため、書庫に入室した他課職員は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。

＜何がいけなかった？＞

✓　書庫内の開放されている書棚に「特定個人情報が記載された書類」と「登記情報が記載された書類」とが分別されずに管理されていた。

✓　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！＞

✓　特定個人情報が記載された書類が今後増加した場合に職員の立ち会いのみでは漏えいリスクの軽減に限界があります。特定個人情報が記載された書類を保管するための鍵付きの書棚を用意するなど、保管方法を見直しましょう。

※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　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。

≪技術的安全管理措置≫

【事例 11】アクセス制御

＜事例＞

Ｌ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。

＜何がいけなかった？＞

✓　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。

✓　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。

＜チェックポイント！＞

✓　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。

✓　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しましょう。

✓　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

〇マイナンバーガイドライン安全管理措置 2 Ｆ　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。

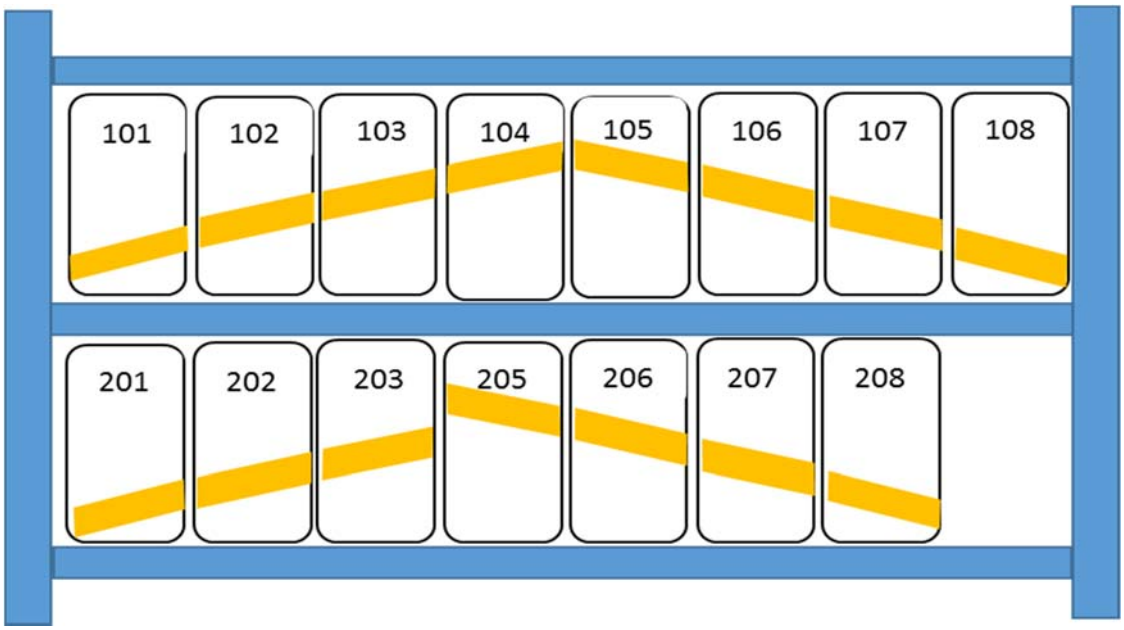
２　好事例

【事例１】保管書類の背表紙の模様による検知

＜事例＞

Ｍ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。

＜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管理について

＜事例＞

Ｎ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。

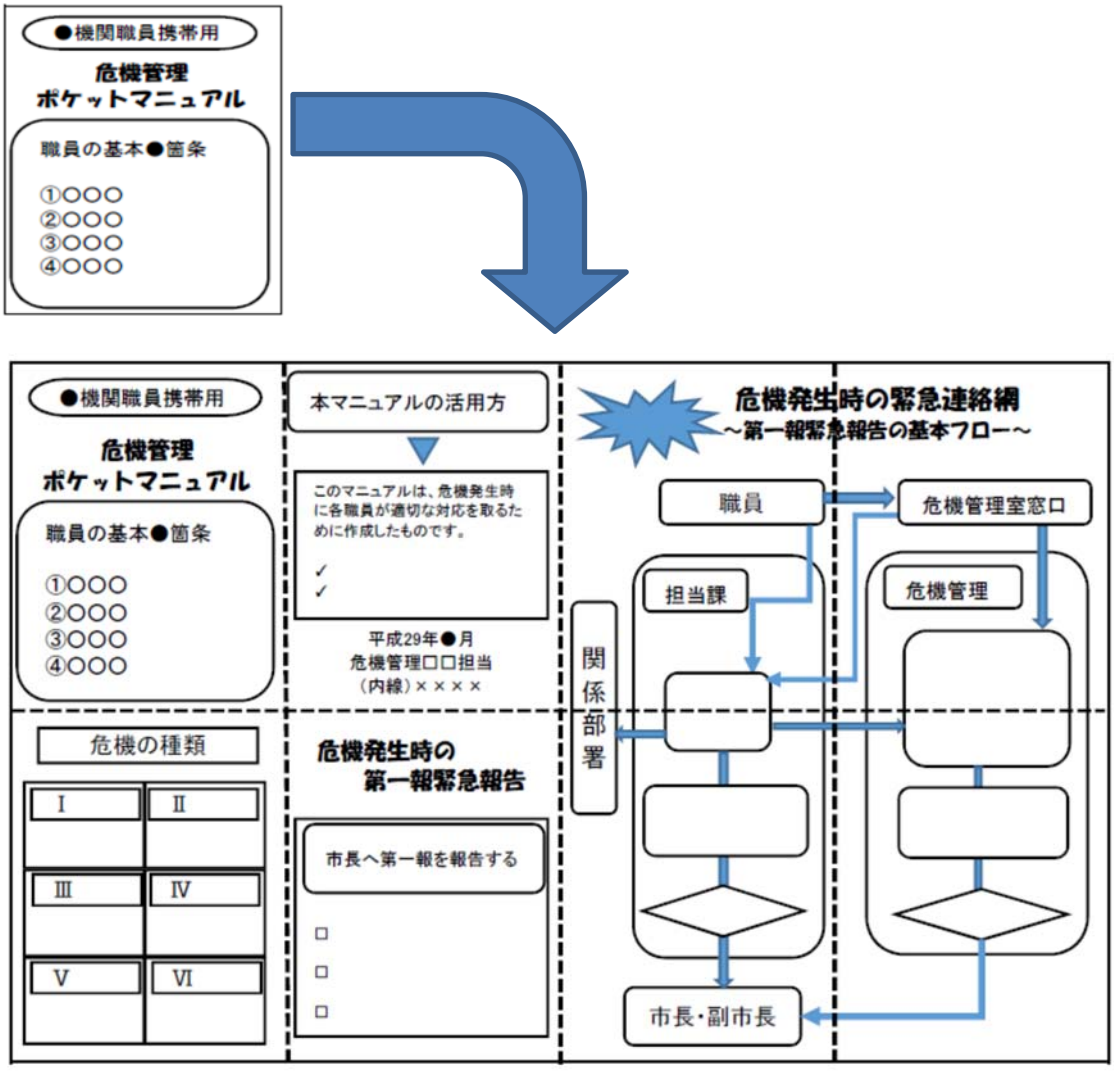
この運用の下で、所管課は、異動又は退職した職員に付与されたアクセス権限の削除漏れを防止するため、年に１度、利用者全員の ID を全て削除した上で、新たな ID を利用者に付与する措置を講じている。

【事例３】危機管理ポケットマニュアルの全職員配布

＜事例＞

　○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布し、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・適確な対応を図れるよう措置を講じている。

＜危機管理ポケットマニュアル（イメージ）＞



３　その他参考情報

【事例１】業務継続

＜事例＞

Ｐ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」旨規定されている。

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。そして、当該ラックの施錠状況を確認したところ、前扉は施錠されていたが後扉は施錠されていなかった。

また、入退室状況を確認したところ、同サーバ室の管理区域には、外部委託業者を含む職員等が入室できることとなっていた。

＜何がいけなかった？＞

✓　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る。

✓　後扉が施錠されていなかったことから、外部委託業者を含む職員等が入室した際にサーバに直接触れることができる状態にあった。

＜チェックポイント！＞

✓　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必要があります。

✓　ラックの施錠に関する点検を徹底するなどして施錠漏れがないように措置を講じましょう。

※参考

〇「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。

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　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。