行政機関等及び地方公共団体等による
特定個人情報の適正な取扱いのためのポイント

～　立入検査における指摘事例と着眼点　～

平成 29 年６月
（令和４年４月改訂）
個人情報保護委員会

＜目次＞

２　その他参考情報

３　好事例

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ます。本資料では、各機関による特定個人情報の適正な取扱いの確保に資するよう、これまでの立入検査において指摘した事例を示し、それぞれについて求められる対応のポイントを着眼点として示しています。併せて、各機関において取り組まれていた好事例なども紹介しています。

＊　指摘事例について、「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「ガイドライン」という。）の「（別添1）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）」の関係箇所に言及しつつ、求められる対応のポイントを着眼点として示しています。

1　指摘事例

≪取扱規程等の見直し等≫

＜ガイドライン＞
・　特定個人情報の具体的な取扱いを定めるために、取扱規程等を策定し、必要に応じて見直し等を行うことが、求められています。
・　その際、①取得、②利用、③保存、④提供、⑤削除・廃棄の管理段階ごとに、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、ガイドラインで記載するすべての安全管理措置を織り込むことが必要です。

【事例1】取扱規程等の見直し等

指摘事例	着眼点
(1)●●機関は、特定個人情報に関する取扱規程等を策定していなかった。また、同機関が従前から策定していた情報セキュリティ対策基準も、全く改正しておらず、特定個人情報に関する取扱いを同対策基準に織り込むといったことも行っていなかった。このため、ガイドラインで求める安全管理措置が講じられていなかった。	・　特定個人情報に関する具体的な取扱いを定めた上で、ガイドラインで求める安全管理措置を講ずる必要があります。
(2)●●機関は、特定個人情報に関する取扱いについて、同機関が従前から策定していた情報セキュリティ対策基準に織り込むことで、同基準を特定個人情報に関する取扱規程等として位置付けていた。しかしながら、同基準の内容としては、「特定個人情報」等の用語の定義に追加するにとどまっており、特定個人情報に関する具体的な取扱いは定められておらず、ガイドラインで求める安全管理措置を網羅した内容となっていなかった。	・　情報セキュリティ対策基準等を特定個人情報に関する取扱規程等として位置付けている以上は、同基準等において特定個人情報に関する具体的な取扱いを定める必要があり、ガイドラインと整合的にし、管理段階ごとにすべての安全管理措置を規定する必要があります。

■参考資料 「地方公共団体等における特定個人情報等取扱要領等」
https://www.ppc.go.jp/files/pdf/chihou_youryou.pdf

≪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

＜ガイドライン＞
- ①個人番号を取り扱う事務の範囲及び②特定個人情報の範囲を明確にした上で、③特定個人情報を取り扱う職員（以下「事務取扱担当者」という。）を明確にしておく必要があります。
- 事務取扱担当者については、①その役割及び②事務取扱担当者が取り扱う特定個人情報の範囲を明確にする必要があります。

指摘事例	着眼点
(1)●●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、特定個人情報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が、非常勤職員、臨時職員等については、事務取扱担当者として指定していなかった。 また、マイナンバーカードの申請・交付の事務について、個人番号を取り扱う事務として認識しておらず、取扱規程において、個人番号を取り扱う事務の範囲に含めていなかった。	・ 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、当該者についても事務取扱担当者に含める必要があります。 ・ マイナンバーの申請・交付の事務についても、個人番号を取り扱う事務になりますので、事務の範囲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、一部の課では非常勤職員、臨時職員等が漏れている場合があります。なお、事務取扱担当者を指定する様式が各課で異なる例が散見されることから、組織として統一的な取扱いとなるよう、委員会が示すひな形をご参考いただきつつ、取扱規程等に具体的な様式を盛り込むことも有効です。
(2)●●機関は、住民基本台帳に関する事務を本庁以外の各支所等でも行っているが、●●区役所●●支所、●●区●●公民館内市民サービス窓口において、取扱規程等に基づく、事務取扱担当者の指定及び「事務取扱担当者一覧」の作成がされていなかった。	・ 本庁以外の支所等についても、特定個人情報を取り扱う職員を事務取扱担当者に指定する必要があります。指定漏れが発生しないよう、支所等の職員も確実に指定できる事務フローを構築する必要があります。なお、対象者が過不足なく特定できるのであれば、事務取扱担当者は個人名での指定ではなく、部署名や事務の名称（「〇〇事務の担当者」等）により指定することも可能です。

【事例3】情報システムの利用状況の分析等

＜ガイドライン＞
- 取扱規程等に基づく運用の状況を確認するため、特定個人情報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必要があります。
- 具体的な方法として、例えば、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）を記録し、定期に及び必要に応じ随時に分析することが、挙げられます。

指摘事例	着眼点
（1）●●機関は、特定個人情報を取り扱う情報システムの利用状況について、取扱規程において、「定期及び随時にアクセスログの分析・確認を実施しなければならない」と規定しているが、実施時期・頻度、分析等作業の具体的な実施方法等を定めず、その点については管理者に任せていたことから、実際には一部のシステムについて、アクセスログの分析等が適切に実施されていなかった。	・ システムの利用状況を定期的に分析・確認するにあたっては、「いつ」、「誰が」、「何を」、「どのように」を明確にし、適切に実施することが重要です。このため、手順書等を定め、毎月又は隔月といった頻度で実施し、分析等結果について取りまとめた際には、問題の有無にかかわらず総括責任者等に報告をすることが望ましいです。 ・ なお、利用状況を分析等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。

■参考資料　「特定個人情報等の利用状況のログ分析・確認について」
https://www.ppc.go.jp/files/pdf/log_bunseki.pdf

【事例4】特定個人情報の持ち運びの記録

＜ガイドライン＞
- 取扱規程等に基づく運用の状況を確認するため、特定個人情報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必要があります。
- 具体的な方法として、例えば、書類・媒体等の持ち運びを記録することが、挙げられます。

指摘事例	着眼点
(1)●●機関は、取扱規程において、「特定個人情報等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」としているが、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ため、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、当該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。	・ 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てもらう、管理者の許可を得てもらうなどして、特定個人情報の取扱状況を把握することが重要です。

【事例5】特定個人情報の取扱状況を確認する手段の整備

＜ガイドライン＞
・ 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必要があります。

指摘事例	着眼点
(1)●●機関は、特定個人情報の取扱状況の記録について、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手段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。	・ 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、各文書ファイルの簿冊数も含めた特定個人情報の取扱状況を把握するため、適切な手段を整備する必要があります。

【事例6】漏えい等事案に対応する体制等の整備

＜ガイドライン＞
・ 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できるように、体制及び手順等を整備する必要があります。

指摘事例	着眼点
(1)●●機関は、取扱規程において、「特定個人情報の漏えい等事案が発生した場合、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ところ、同課は、個人情報保護委員会への報告は不要と判断し、漏えい等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。	・ 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、ガイドライン等に基づき、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報告する必要があります。取扱規程等に適切な内容を規定し、関係部署に周知して下さい。
(2) ●●機関は、取扱規程において、「漏えい等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『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、「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。	・ 漏えい等発生時、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、適切かつ迅速な報告をするための体制を整備する必要があります。

指摘事例	着眼点
(3) ●●機関は、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。	・ 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ルールを整備し、報告ルートを確立する必要があります。

【事例7】監査の実施

＜ガイドライン＞
・ 監査責任者は、特定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に報告する必要があります。
・ 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ことが求められます。

指摘事例	着眼点
（1）●●機関は、取扱規程において、「監査責任者は、特定個人情報等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」と規定しているが、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。	・ 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、具体的な計画や実施方法を策定し、適切に監査を実施することが求められます。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。
（2）●●機関は、内部監査規程において、「監査責任者が、個人番号利用事務を行っている部署を対象に定期的に監査を実施すること」が規定されているが、実際に監査が実施されていたのは一部の課室にとどまっていた。	・ 監査の対象となる全ての課（個人番号利用事務又は個人番号関係事務を実施している課を含め、特定個人情報を取り扱う全ての課）に対して、一定の期間（例えば、3年から5年程度）で監査を一巡して実施できるよう、中期計画を策定することが有効です。
（3）●●機関は、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、その中に、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。	・ 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、監査項目にガイドライン特有の項目や書類の取扱いに関する項目が含まれているか確認する必要があります。なお、特定個人情報等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。

指摘事例	着眼点
(4)●●機関は、監査対象課から特定個人情報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し、助言等を行うにとどまっており、自己点検票の回答どおりに運用されているか、監査担当課が第三者の目線で確認する手法となっていなかった。	・ 監査対象課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。例えば、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。
(5)●●機関は、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。	・ 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、番号制度の所管課及び特定個人情報の担当課に対して、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。 ・ また、総括責任者への報告にあたり、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、被監査部署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。

■参考資料 「地方公共団体等における特定個人情報等に関する監査実施マニュアル」
https://www.ppc.go.jp/files/pdf/kansa_manual.pdf
「地方公共団体等における監査のためのチェックリスト」
https://www.ppc.go.jp/files/pdf/check_list.pdf

≪人的安全管理措置≫

【事例8】教育研修の実施

＜ガイドライン＞

- 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報の適正な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行うことが求められます。
- 総括責任者及び保護責任者は、特定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、特定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ことが求められます。
- 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ことが求められます。
- 上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ことが求められます。
- 総括責任者は、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、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その他の事項に関する研修を行います。

【表：番号法及び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

指摘事例	着眼点
(1)●●機関は、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。	・ 総括責任者及び保護責任者は、番号法及びガイドラインが求める4種類の教育研修(上表の①-④)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する必要があります。 ・ 特定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、特定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必要があります。
(2)●●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。	・ 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。例えば、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おいて、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。

指摘事例	着眼点
(3)●●機関は、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、そのうち 80 名が欠席していたが、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じていなかった。 また、所管課は、同研修の受講者に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。	・ 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。 ・ 所管課は、伝達研修の実施状況について所属課から報告を求めるなどして、実施状況を把握する必要があります。
(4)●●機関は、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等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」としているが、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。	・ 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必要があります。 ・ 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1年ごとに実施する必要があります。

■参考資料 「特定個人情報の適正な取扱いのための各種研修資料」
https://www.ppc.go.jp/files/pdf/mynumber_kensyuu.pdf

≪物理的安全管理措置≫

【事例9】入退室管理及び機器等の持込制限

＜ガイドライン＞
・ 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じます。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必要があります。

指摘事例	着眼点
(1)●●機関は、情報システムの運用担当課職員の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たが、ICカードが貸与されていない運用保守業者等について、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。 ・ 入退室管理等の措置としては、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。
(2)●●機関は、取扱規程において、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ことから、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おり、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。	・ 取扱規程等において管理区域を明確にし、管理区域においては、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ずる必要があります。

【事例 10】特定個人情報が含まれている書類の保管方法

＜ガイドライン＞
・ 特定個人情報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ります。

指摘事例	着眼点
（1）●●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いるが、当該書類の一部が編綴されていない状態で書棚外に放置されているため、書庫に入室した（特定個人情報を取り扱うことができない）他課職員に特定個人情報が記載された書類が容易に見えてしまう状況にあった。	・ 特定個人情報等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、他課所管の書類とは分けて保管するなど、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。

【事例 11】機器及び電子媒体等の盗難等の防止

＜ガイドライン＞
・ 管理区域及び取扱区域における特定個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる必要があります。

指摘事例	着眼点
(1)●●機関は、資料室に設置している情報システムのサーバ及び利用端末について、サーバラックの施錠やセキュリティワイヤー等による固定等の盗難又は紛失等を防止する措置を講じていなかった。	・ サーバ及び利用端末等の機器については、盗難又は紛失等を防止するため、サーバラックの施錠、セキュリティワイヤーの設置等の物理的な安全管理措置を講ずる必要があります。
(2)●●機関は、個人番号が含まれる書類をファイルに編綴してキャビネットで保管していたが、同キャビネットは、事務取扱担当者の目の行き届かない場所に設置されており、かつ、執務時間内は常時施錠されていなかった。	・ 特定個人情報を含む書類を保管するキャビネットは、業務時間外は施錠し、業務時間内であっても、担当者が不在になる時間帯や担当者の目の届かない場所にあるキャビネットは施錠する等の措置が必要です。

【事例 12】電子媒体の使用及び接続制限等

＜ガイドライン＞
・ 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ことが求められます。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ことが求められます。

事例	着眼点
(1)●●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への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。	・ 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。 ・ 電子媒体等について、管理者が管理し、使用時に都度貸し出すことで使用状況を把握する必要があります。

【事例 13】個人番号の削除、機器及び電子媒体等の廃棄記録の整備等

＜ガイドライン＞
- 特定個人情報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必要があります。
- 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必要があります。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、説明書等により確認する必要があります。

指摘事例	着眼点
(1)●●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。 そのため、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等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。	・ 文書の削除・廃棄について、具体的な手順を定め、当該手順に基づいて運用を行うことが重要です。

≪技術的安全管理措置≫

【事例 14】アクセス制御

＜ガイドライン＞
・ 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必要があります。

事例	着眼点
(1)●●機関は、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、アクセス権限を管理するシステム課に対し、速やかに『ユーザー情報変更申請書』を提出し、個人番号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、周知が不徹底であり、担当課が、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」を提出しなかったことから、システム課は、当該職員の人事異動等の情報を把握できず、システムへのアクセス権限についても削除していなかった。	・ 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必要があります。 ・ 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するシステム部門において、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。

【事例 15】不正アクセス等による被害の防止等

＜ガイドライン＞
- 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、適切に運用する必要があります。
- 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必要があります。
- 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必要があります。

事例	着眼点
(1)●●機関は、外部から入手するデータについて、あらかじめセキュリティ対策ソフトウェアにより不正プログラム感染の有無を確認することを求めているが、委託先から納品される電子データ(個人番号を含む)を情報システムに登録する際、不正プログラム感染の有無を確認していなかった。	・ 情報システムの不正な構成変更を防止するために、セキュリティ対策ソフトウェア等を導入し、不正プログラム感染の有無を確認する必要があります。 ・ また、セキュリティ対策ソフトウェアの使用手順書等を整備・周知し、委託先から受領するデータについても安易に信用して直ちに使用するのではなく、まずは不正プログラム感染の有無を確認することが重要であり、こうした取扱いを担当者に徹底させる必要があります。

≪委託及び再委託≫

【事例 16】委託先の監督

＜ガイドライン＞
- 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うことが求められます。
- 「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ます。

指摘事例	着眼点
(1)●●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。その理由としては、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。	・ 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、あらかじめ確認する必要があります。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ます。

事例	着眼点
(2)●●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を委託している。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」等必要な規定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。	・ ガイドラインで求めている契約内容を、委託契約に盛り込む必要があります。具体的には、以下の 10 項目を盛り込んでください。 ①秘密保持義務②事業所内からの特定個人情報の持ち出しの禁止③特定個人情報の目的外利用の禁止④再委託における条件⑤漏えい等事案が発生した場合の委託先の責任⑥委託契約終了後の特定個人情報の返却又は廃棄⑦特定個人情報を取り扱う従業者の明確化⑧従業者に対する監督・教育⑨契約内容の遵守状況について報告を求める規定⑩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 ・ 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。
(3)●●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、契約終了後に返却され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、契約内容に定めていなかった。このため、担当課において、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。	・ 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ことに加え、委託先においてデータが確実に削除され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。

【事例 17】再委託の要件及び監督

＜ガイドライン＞
- 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ます。
- 行政機関等又は地方公共団体等は委託先に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなります。

指摘事例	着眼点
(1)●●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」としているが、再委託について、委託元の許諾を得ないまま、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。 ・ 再委託の許諾の方法について、特にガイドライン等で規定されていませんが、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。
(2)●●機関が委託している個人番号利用事務等の一部について、委託先は別の事業者に再委託しているが、●●機関は、委託先が再委託先に対して必要かつ適切な監督を行っているかどうかの監督が不十分だった。	・ 委託元は、再委託先に対して間接的な監督義務があります。したがって、委託元は再委託先が取り扱う特定個人情報について適切な安全管理が図られるかどうか把握しておく必要があります。 ・ 再委託先における安全管理措置の実施状況について、委託先から報告を受けるほか、必要に応じて実際の取扱状況が分かる資料を提出してもらうなど、再委託先の実態を的確に把握する必要があります。委託先からの報告が形骸化しないように留意してください。

２ その他参考情報

【事例】バックアップの保管

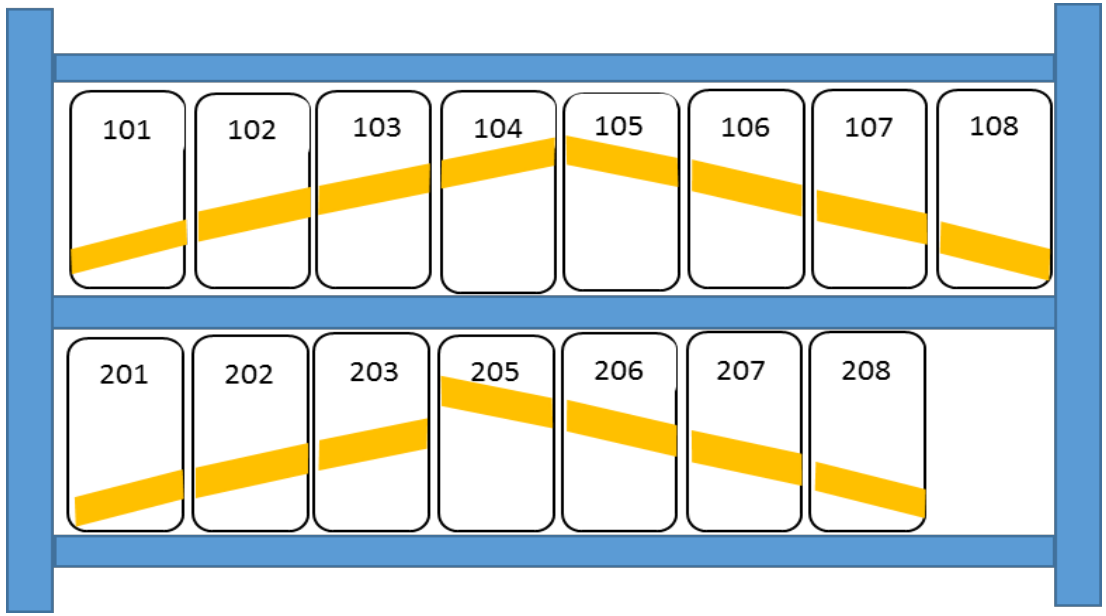
事例	着眼点
・ ●●機関は、取扱規程において、「担当者は、サーバのバックアップを記録媒体に記録する」としており、情報資産の保管については、セキュリティ対策基準等において、「特定個人情報を記録した記録媒体は、鍵のかかる書庫等に適切に保管しなければならない」としている。 しかしながら、バックアップが記録されている記録媒体は、鍵のかかるラックの中に保管されているものの、当該ラックにはサーバ本体も保管されていた。	・ サーバのバックアップを記録している記録媒体が同サーバと同一の場所に保管されており、災害等により双方に被害が及んだ際には、特定個人情報の滅失又は毀損につながるおそれがあります。 ・ 特定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。

３　好事例

【事例１】保管書類の背表紙の模様による検知

好事例	着眼点
・　●●機関は、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。	・　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

好事例	着眼点
・ ●●機関は、システムにおけるアクセス制御について、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、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。	・ 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。

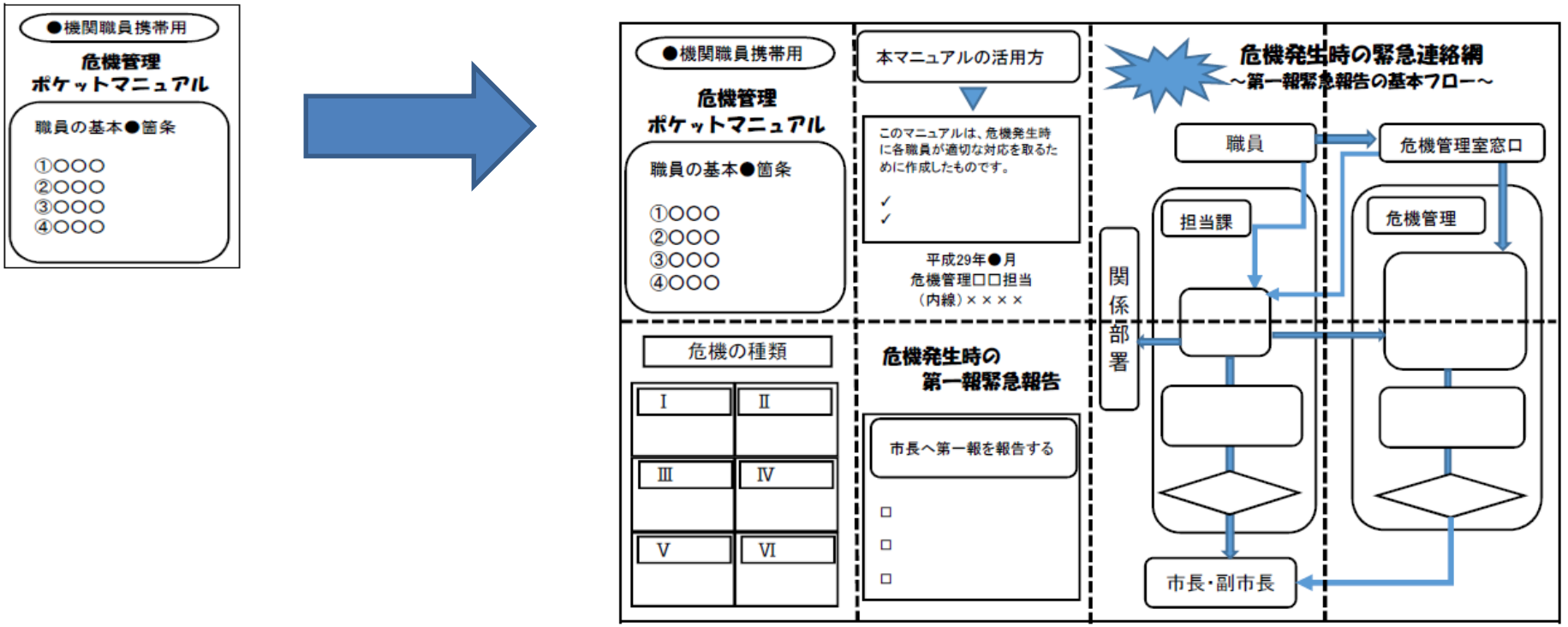
【事例3】アクセス権限の設定

好事例	着眼点
・ ●●機関は、職員の採用、異動、退職等の人事情報について、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。	・ 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に有効です。

【事例4】危機管理ポケットマニュアルの全職員配付

好事例	着眼点
・ ●●機関は、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、漏えい等事案発生時、職員が迅速・的確な対応を図れるよう措置を講じている。	・ 漏えい等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

好事例	着眼点
・ ●●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について協議している。 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。	・ 相互監査の実施により、他機関の特定個人情報の取扱状況の把握もできます。その結果として、監査担当者の理解の向上に繋がり、被監査機関のみならず監査機関の特定個人情報の管理状況についても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

好事例	着眼点
・ ●●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。	・ 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。

【事例7】端末の起動時画面の表示による啓発、注意喚起

好事例	着眼点
・ ●●機関は、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。	・ 全職員が必ず確認する画面に、特定個人情報に係る情報を日々表示することは、特定個人情報の適正な取扱いについて理解を深め、意識の高揚等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の取扱いの改善が図られることも期待されます。