行政機関等による
保有個人情報の適正な取扱いのためのポイント

～　実地調査における指摘事例と着眼点　～

令和７年３月
個人情報保護委員会

＜目次＞

指摘事例

はじめに

個人情報保護委員会は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 156 条に基づき、行政機関等に対して実地調査を実施しています。本資料では、各機関による保有個人情報の適正な取扱いの確保に資するよう、これまでの実地調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。

＊　指摘事例について、「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」（以下「事務対応ガイド」という。）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。

指摘事例

≪規程の整備等≫

【事例1】取扱規程等の見直し等

＜事務対応ガイド＞　4-8-1　指針の意義
- 事務対応ガイド「4-8（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」を参考として、個人情報の適切な管理に関する規程等を整備することが求められています。
- 規程等の整備に当たっては、事務対応ガイドで求められている安全管理措置を織り込むとともに、個人情報保護法等が改正された際には、改正内容に合わせて行政機関等が定めた規程を改正する必要があります。

指摘事例	着眼点
（1）●●機関において、改正個人情報保護法の施行に伴う「●●規程」の改正が行われていなかった。	・ 個人情報保護法等の改正があった際には、内部規程の見直しを行い、規程の整合性を保つ必要があります。

≪管理体制≫

【事例2】総括保護管理者等の明確化

＜事務対応ガイド＞　4－8－2　管理体制
- 行政機関等では、管理体制として総括保護管理者、保護管理者、保護担当者、監査責任者を置くことが定められています。
- 総括保護管理者及び監査責任者は行政機関等に1人、保護管理者は保有個人情報を取り扱う各課室等に1人、保護担当者は保有個人情報を取り扱う各課室等に1人又は複数人設置します。

指摘事例	着眼点
（1）●●機関において、それぞれ比較的小規模の部署であった××部の△△室及び〇〇室に、保護担当者を指定していなかった。	・ 保護担当者は、小規模の部署であっても、保有個人情報を取り扱う各課室等に1人以上指定する必要があります。
（2）●●機関は、××事務所△△課において、保護担当者を指定していなかった。	・ 本庁以外の支所等についても、保護担当者を指定する必要があります。また、異動の際などに保護担当者の指定が漏れることがないように注意してください。

≪教育研修≫

【事例3】保有個人情報の取扱いに従事する職員に対する研修

＜事務対応ガイド＞　4－8－3　教育研修
・ 総括保護管理者は、保有個人情報の取扱いに従事する職員に対して、保有個人情報の取扱いについての研修を実施する必要があります。
・ 正規職員だけでなく、非常勤職員、臨時職員なども対象ですので、これら全ての職員への研修が漏れないように注意してください。

指摘事例	着眼点
（1）●●機関は、集合研修で開催する研修の受講対象者を役員及び正規職員のみとしており、臨時職員については集合研修の受講対象者としていなかった。	・ 保有個人情報の取扱いに従事する職員は、採用形態にかかわらず、漏れなく研修を実施する必要があります。職場環境等の事情により、当該研修が未受講となった職員等がいる場合は、別途伝達研修の実施等により、確実に研修を受講できるよう代替手段を講じてください。
（2）●●機関は、保有個人情報の取扱いに従事する職員に対する研修について、受講対象者を新規採用職員や新任管理職員等のみとしていた。さらに、受講対象者としている新規採用職員や新任管理職員等についても、未受講者に対しては次年度に受講すればよいことにするなど、一部の職員が受講していなかった。	・ 保有個人情報の取扱いに従事する職員に対しては、漏れなく研修を実施する必要があります。事前に受講対象者を漏れなく把握するとともに、受講対象者の受講状況を確認し、未受講者に対してフォローアップするようお願いします。
（3）●●機関は、研修を受講すべき職員を把握しておらず、希望者に対してのみ研修を行っていたため、受講すべき職員のうち一部しか研修を受講していなかった。	・ 希望者だけでなく、保有個人情報の取扱いに従事する職員全員に対しては、漏れなく研修を実施する必要があります。
（4）●●機関は、保有個人情報の取扱いに従事する職員に対し、サイバーセキュリティの確保に関する研修を実施していたものの、保有個人情報の取扱い等に関する事項を含	・ 研修の内容として、保有個人情報の取扱い等に関する事項を含んでいる必要があります。研修計画を作成する際に、研修内容の妥当性を検討することが重要です。

んでおらず、研修内容が不十分であった。	

【事例4】保有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する研修

＜事務対応ガイド＞　4－8－3 教育研修

・ 総括保護管理者は、保有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、保有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研修を行う必要があります。

指摘事例	着眼点
（1）●●機関は、情報システムの管理、運用及びセキュリティ対策に関する研修を行っていなかった。	・ 全職員に保有個人情報の取扱いに関する研修等を実施していても、その内容に情報システムの管理、運用及びセキュリティ対策に関するものが含まれていない場合には、情報システムの管理に関する事務に従事する者に対し、別途それらを網羅する内容の研修を実施する必要があります。

【事例5】保護管理者及び保護担当者に対する研修

＜事務対応ガイド＞　4－8－3 教育研修
- 総括保護管理者は、保護管理者及び保護担当者に対し、課室等の現場における保有個人情報の適切な管理のための教育研修を実施する必要があります。
- 本研修は、定期的に実施する必要があります。

指摘事例	着眼点
（1）●●機関は、幹部昇任者に対する研修は実施されているものの、全ての保護管理者及び保護担当者が対象となっていなかった。また、当該研修は定期的に実施されていなかった。	・ 全ての保護管理者及び保護担当者に対して研修を実施する必要があります。 ・ 保護管理者及び保護担当者は、定期的に研修を受講する必要があります。 ・ 昇任時の1回限りの研修では、研修を定期的に実施しているとはいえません。
（2）●●機関は、保護管理者及び保護担当者に対し、保有個人情報の取扱いに関する研修は実施していたものの、課室等の現場における保有個人情報の適切な管理に関する事項を含んでおらず、研修内容が不十分であった。	・ 保護管理者及び保護担当者に対する研修は、課室等の現場における保有個人情報の適切な管理に関する内容を含んでいる必要があります。一般職員向けの内容と同一の研修を保護管理者及び保護担当者に対して実施しただけでは、研修内容が不足している場合があるので注意してください。

【表：事務対応ガイドが求める研修】

教育研修の種類		対象者
①	保有個人情報の取扱いに関する研修	保有個人情報の取扱いに従事する職員
②	保有個人情報を取り扱う情報システムの管理、運用及びセキュリティ対策に関する研修	保有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
③	課室等の現場における保有個人情報の適切な管理のための研修	保護管理者及び保護担当者

≪保有個人情報の取扱い≫

【事例6】アクセス制限

＜事務対応ガイド＞　4－8－5 保有個人情報の取扱い 【アクセス制限】
・ 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定する必要があります。

指摘事例	着眼点
（1）●●機関は、委託先事業者に〇〇システムへのアクセス権を付与しているが、同アクセス権を使用してデータのやり取りをするのは数回程度であるにもかかわらず、数年間にわたって継続してアクセス権限を付与したままにしており、アクセス権限を必要最小限に限定する等の措置が講じられていなかった。	・ システムにアクセスできる職員の範囲と権限の内容については、保有個人情報の秘匿性等その内容に応じて、必要最小限に限定する必要があります。 ・ 秘匿性が高い保有個人情報を取り扱うシステムについては、特に厳格に管理することが重要です。
(2)●●機関は、〇〇システムについて、異動等により不要となったユーザIDを無効化又は削除していなかった。	・ 異動等によりアクセスする必要がなくなったユーザ ID については、確実に無効化又は削除するなど、適時、漏れなく管理してください。
(3)●●機関は、〇〇課の職員のみがアクセス可能な共有フォルダに保有個人情報を保存していたが、長期休職中の職員のアクセス権限が付与されたままの状態になっていた。	・ 長期休職中など、一部の職員のみがアクセス可能な共有フォルダやシステムへのアクセス権限が不要となっている職員のアカウントは一時的に利用停止にするなど、アクセス権限を常に必要最小限にする措置を講ずることが重要です。
(4)●●機関は、課内に〇〇システムを使用しない者がいるにもかかわらず、システムのアクセス権限を課単位で設定しており、アクセス権限を必要最小限の範囲に限っていなかった。	・ 部署内でシステムにアクセスする必要がない職員にまでアクセス権限を付与することがないよう、適切なアクセス権限を設定する必要があります。

【事例7】媒体の管理等

＜事務対応ガイド＞　4－8－5　保有個人情報の取扱い【媒体の管理等】
・ 保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置を講ずる必要があります。

指摘事例	着眼点
(1)●●機関は、保有個人情報を記録した外部電磁的記録媒体(CD－R)を委託先に交付し、作業終了後に直接返却を受けているが、その外部電磁的記録媒体に記録されたデータについて、パスワードの設定や暗号化などの適切なアクセス制御が行われていなかった。	・ 保有個人情報が記録されている媒体の送付、持ち出しをする際には、原則として、パスワード等の認証機能を設定するなど、適切なアクセス制御を行う必要があります。

【事例8】廃棄等

＜事務対応ガイド＞　4－8－5 保有個人情報の取扱い 【廃棄等】

・ 保有個人情報又は保有個人情報が記録されている媒体が不要となった場合は、保護管理者の指示に従い、復元又は判読できない方法によって当該情報の消去又は当該媒体の廃棄を行う必要があります。

・ 保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合には、必要に応じて職員が立ち会い、又は写真等を付した廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認する必要があります。

指摘事例	着眼点
（1）●●機関は、〇〇システムに電子データとして保存された保有個人情報について、保存期間が満了し不要となったシステム導入以降の全てのデータを保存していた。	・ システム内に保存されている保有個人情報について、保存期間が満了し、不要となった場合は、当該保有個人情報の消去を行う必要があります。
（2）●●機関は、〇〇課において、保存期間が 10 年である××に係る文書について、保存期間が大幅に超過しているにもかかわらず、適切な保存期間延長手続を実施することなく書庫に保管し続けていた。	・ 保有個人情報を含む文書のうち、行政文書としての保存期間が満了したものについては、速やかに廃棄又はあらかじめ適切な延長措置をとっておく必要があります。

【事例9】保有個人情報の取扱状況の記録

＜事務対応ガイド＞　4－8－5 保有個人情報の取扱い 【保有個人情報の取扱状況の記録】
・ 保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する必要があります。

指摘事例	着眼点
（1）●●機関は、要配慮個人情報を含む保有個人情報を記録した外部電磁的記録媒体（CD－R）を委託先である民間事業者に職員が直接交付し、作業終了後に直接返却を受けているところ、その受渡しに関する管理簿、受払簿等がなく、保有個人情報の利用及び保管等の取扱状況について記録がなされていなかった。	・ 保有個人情報の秘匿性等その内容に応じて、保有個人情報の利用及び保管等の取扱いの状況の記録を残す必要があります。
（2）●●機関は、××業務における機密性情報2の書類の持ち出しについて、年に1度の包括的な許可で年間を通じて自由に持ち出せるようになっており、持ち出しを記録する台帳を作成していなかった。	・ 保有個人情報の秘匿性等その内容に応じて、持ち出しを記録する台帳を作成するなど、取扱いの状況について適切に記録を残す必要があります。

≪情報システムにおける安全の確保等≫

【事例 10】アクセス制御

＜事務対応ガイド＞　4－8－6 情報システムにおける安全の確保等 【アクセス制御】

・ 保護管理者は、保有個人情報の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずる必要があります。

・ 保護管理者は、上記措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、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必要があります。

指摘事例	着眼点
（1）●●機関において、〇〇システムの管理者権限を有する共用IDのパスワードが記載されたシステム作業手順書が、システムの管理を行う者以外の者もアクセスすることができる共有フォルダに保存されていた。また、そのパスワードは、当該IDと同一かつ容易に推測可能なものとなっていた。	・ やむを得ず共用 ID を使用する場合は、当該 ID のパスワードを適切に管理する必要があります。認証情報はシステムを使用する最小限の職員にのみ伝えるほか、職員の異動等があった場合は、パスワードを変更するなどの対応が考えられます。なお、共用 ID を利用する場合は、利用者を記録するなど、利用状況を特定できるようにしておくことが求められます。
（2）●●機関において、〇〇システムへログインする際に課内共通のパスワードを使用しており、当該パスワードは人事異動等があった場合も更新されておらず、パスワードの管理が不適切であった。また、〇〇システムのIDは、後任者に前任者のIDを割り当てているため、前任者は人事異動等の後も当該IDを用いてシステムにログインできる状態であった。	・ 前任者の ID をそのまま後任者に使用させるのではなく、利用者ごとに ID を発行して管理することが望ましいです。パスワードについても、安易に共通パスワードを使用するのではなく、利用者ごとに ID を発行した上で、それぞれ異なるパスワードを設定し、他人がログインできないようにすることが求められます。

【事例 11】アクセス記録の定期的な分析

＜事務対応ガイド＞　4－8－6 情報システムにおける安全の確保等 【アクセス記録】
・ 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報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、及びアクセス記録（ログ）を定期的に分析するために必要な措置を講ずる必要があります。

指摘事例	着眼点
（1）●●機関は、〇〇システムについて、アクセス記録は取得・保存していたものの、その定期的な分析が実施されていなかった。	・ アクセス記録については、取得・保存するだけでなく、定期的に分析を行う必要があります。不正アクセス等の問題が発覚した場合だけ分析を行うのではなく、定期的に分析を行う必要がある点に注意してください。
（2）●●機関において、アクセス記録の取得及び点検を行う対象がサーバやファイアウォール等の稼働状況等に係るログに限定されており、保有個人情報を取り扱う〇〇システムにおいては、保有個人情報へのアクセス状況の監視が実施されていなかった。	・ アクセス記録の分析内容には、保有個人情報への不適切なアクセスを監視するための内容を含んでいる必要があります。

■ **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
本参考資料は特定個人情報（マイナンバーをその内容に含む個人情報）等に関する資料ですが、分析手法はおおむね同じと考えられますので、参考資料として御活用ください。

【事例 12】不正プログラムによる漏えい等の防止

＜事務対応ガイド＞ 4－8－6 情報システムにおける安全の確保等 【不正プログラムによる漏えい等の防止】
・ 保護管理者は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる必要があります。

指摘事例	着眼点
（1）●●機関は、〇〇システムで利用するソフトウェアについて、数年前のセキュリティパッチの適用を最後に、それ以降現在に至るまで、セキュリティパッチの適用を実施していなかった。	・ 保有個人情報を管理するシステムについては、セキュリティパッチを適用し、ソフトウェアを常に最新の状態に保つことが必要です。

【事例 13】情報システムにおける保有個人情報の処理

＜事務対応ガイド＞　4－8－6　情報システムにおける安全の確保等　【情報システムにおける保有個人情報の処理】

・　職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する必要があります。

・　保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する必要があります。

指摘事例	着眼点
（1）●●機関は、モバイル端末を用いて複製された保有個人情報の記録を持ち出しているところ、処理終了後に、当該端末に保存されたデータの消去を確認していなかった。	・　一時的な加工等のために保有個人情報の複製等を行った場合は、処理が終了した後に速やかに消去するとともに、保護管理者がその実施状況を確認する必要があります。

【事例 14】記録機能を有する機器・媒体の接続制限

＜事務対応ガイド＞　4－8－6 情報システムにおける安全の確保等 【記録機能を有する機器・媒体の接続制限】
・ 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい等の防止のため、スマートフォン、USB メモリ等の記録機能を有する機器・媒体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必要があります。

指摘事例	着眼点
（1）●●機関において、保有個人情報を取り扱う端末について、許可された外部電磁的記録媒体以外の接続を制限する等の措置が講じられておらず、私物の USB メモリ等が接続できる状態となっていた。	・ 保有個人情報の秘匿性等その内容に応じて、USB メモリ等の外部電磁的記録媒体の接続制限等の措置を講ずる必要があります。

【事例 15】端末の盗難防止等

＜事務対応ガイド＞　4－8－6　情報システムにおける安全の確保等 【端末の盗難防止等】
・　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる必要があります。

指摘事例	着眼点
（1）●●機関は、○○システムの運用保守を行うための運用管理端末（ノートパソコン）について、セキュリティワイヤー等による固定を行っておらず、また、同端末が設置されている部屋は書庫兼職員休憩室として使われていた。 その部屋は物理鍵による施錠が可能であるものの、鍵は執務室入り口に置かれており、○○システムを使用する職員だけでなく、××課に在籍する職員であれば誰でも入室できる状態であった。	・　端末の管理については、盗難や紛失を防止するための措置が必要です。端末をセキュリティワイヤー等で固定する、執務室の施錠を徹底する、端末を使用しないときには施錠できるキャビネット等で保管する等の対応が考えられます。

≪個人情報の取扱いの委託≫

【事例 16】業務の委託等

＜事務対応ガイド＞　4－8－9 個人情報の取扱いの委託【業務の委託等】

（1） 個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講ずる必要があります。また、契約書に、次の事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する必要があります。

① 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
② 再委託の制限又は事前承認等再委託に係る条件に関する事項
③ 個人情報の複製等の制限に関する事項
④ 個人情報の安全管理措置に関する事項
⑤ 個人情報の漏えい等の事案の発生時における対応に関する事項
⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項

（2） 保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければなりません。

（3） 保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年１回以上、原則として実地検査により確認する必要があります。

（4） 委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に上記（1）の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが上記（3）の措置を実施する必要があります。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様です。

指摘事例	着眼点
（1）●●機関は、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項を書面により確認していなかった。	・ 委託先の選定を行う際には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、委託先の管理体制等を書面で確認する必要があります。
（2）●●機関は、法令に基づき事務を委託しているが、契約内容に、事務対応ガイドで規定された事項のうち、以下の項目を明記していなかった。 ・ 利用目的以外の目的のための利用の禁止等の義務 ・ 個人情報の複製等の制限に関する事項 ・ 個人情報の安全管理措置に関する事項 ・ 個人情報の漏えい等の事案の発生時における対応に関する事項 ・ 委託終了時における個人情報の消去及び媒体の返却に関する事項 ・ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項 ・ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項	・ 事務対応ガイドで求めている事項（上記（1）①～⑧の項目）を、委託契約書に明記する必要があります。

（3）●●機関は、保有個人情報の秘匿性等その内容や量等に応じて実地検査で確認することとなっている委託作業において、定期的な実地検査等により、当該委託作業の管理体制及び実施体制や個人情報の管理の状況について確認していなかった。	・ 個人情報の管理の状況等について、委託する業務に係る保有個人情報の秘匿性等その内容や量等に応じて、少なくとも年１回以上、原則として実地検査により確認しなければならないことに留意する必要があります。 ・ 通知書のパンチ入力業務等を委託した場合、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。また、その確認方法としては、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。
（4）●●機関は、業務の委託先に対し、再委託先等における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項を書面により確認させていなかった。	・ 再委託等する場合の要件として、事前承認等の条件がありますが、委託先が委託元に無断で再委託等することもあることから、委託元は委託先に対して実地検査を行うこと等により、委託先の個人情報の取扱状況を把握する必要があります。 ・ 再委託等の許諾の方法について、特に事務対応ガイド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とすることが望ましく、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。

≪安全管理上の問題への対応≫

【事例 17】事案の報告及び再発防止措置

＜事務対応ガイド＞　4－8－11　安全管理上の問題への対応【法に基づく報告及び通知】
・ 漏えい等が生じた場合であって法第 68 条第１項の規定による委員会への報告及び同条第２項の規定による本人への通知を要する場合には、速やかに所定の手続を行うとともに、委員会による事案の把握等に協力する必要があります。

指摘事例	着眼点
（1）●●機関において、法第 68 条第１項の規定による委員会への報告及び同条第２項の規定による本人への通知について、その手順等が整備されていなかった。	・ 行政機関等は、漏えい等報告の対象となる事態が生じた場合には、個人情報保護委員会が策定した規則、事務対応ガイド等に基づき、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。 ・ 漏えい等発生時、職員が報告先を正確に把握できるよう対応手順等を明確にし、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。
（2）●●機関は、個人情報保護法の改正を踏まえた漏えい時等の対応手順については、研修において職員に周知しているものの、その対応手順を規定する手引等について、個人情報保護法の改正を踏まえた見直し、整備を行っていなかった。	

≪監査及び点検の実施≫

【事例 18】監査及び点検

＜事務対応ガイド＞　4－8－12　監査及び点検の実施

【監査】

・ 監査責任者は、保有個人情報の適切な管理を検証するため、4-8-2（管理体制）から 4-8-11（安全管理上の問題への対応）までに記載する措置の状況を含む当該行政機関等における保有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を行い、その結果を総括保護管理者に報告する必要があります。

【点検】

・ 保護管理者は、各課室等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に、及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する必要があります。

【評価及び見直し】

・ 総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる必要があります。

指摘事例	着眼点
（1）●●機関において、保有個人情報の取扱いがあるにもかかわらず、 実地確認等による監査を一度も実施したことがない課室が存在するなど、実地確認等による監査対象課室が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室（保有個人情報を取り扱う全ての課室）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。
（2）●●機関は、毎年度監査計画を策定し、監査対象課室を選定の上で監査を実施しているものの、書面監査を犯罪歴・病歴等の秘匿性が高いもの、秘匿性は高くないが 1,000 人以上の個人情報を含むものを保有する課室のみ	

を対象としており、その他の個人情報ファイルを保有する課室については、過去に漏えい等が発生しているにもかかわらず、監査対象としていなかった。	
（3）●●機関は、監査対象課室が個人情報ファイル簿に掲載されている個人情報ファイルを保有する課室の一部のみとしており、その他の個人情報を保有している課室を監査対象としていなかった。 また、支所等の窓口業務において、個人情報を取得し、個人情報ファイル簿に掲載されている個人情報ファイルを保有している同支所等も監査対象としていないなど、監査対象が一部の課室のみとなっていた。	
（4）●●機関は、一部の部局等における監査の際に、監査対象課室が作成、提出する「監査調査票」を取りまとめて総括保護管理者に報告するにとどまっており、制度所管部署等、被監査部門以外の部署が実地監査する体制になっていなかった。	・ 監査は、単に実施するだけではなく、独立した立場で、かつ客観性・網羅性を担保することや監査結果に対する改善策の検討等を行うことが重要です。具体的な計画や実施方法を策定した上で、適切に実施することが求められます。また、総括保護管理者は監査の報告を受け、問題点の改善状況についてフォローアップをする必要があります。 ・ 保有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、監査項目に事務対応ガイド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ことを確認する必要があります。
（5）●●機関は、実施した内部監査の結果を踏まえた改善要請事項の一部について、フォローアップが不十分であった。	・ 監査において検出された問題点については、総括保護管理者から監査対象課室にフィードバックするとともに、期日を設けた上で改善状況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。 ・ 検出された問題点が、他の課室でも発生し得るものである場合、同機関内に注意喚起することが望ましいです。