国家社会機能継続性確保施策・副首都整備推進本部保有個人情報等管理規程

（令和８年10月30日
国家社会機能継続性確保施策・
副首都整備推進本部長決定）

第１章　総則

（目的）

第１条　この規程は、国家社会機能継続性確保施策・副首都整備推進本部（以下「本部」という。）の保有する個人情報、個人番号及び行政機関等匿名加工情報等（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121条第２項に規定する「行政機関等匿名加工情報等」をいう。以下同じ。）の適切な管理に関して必要な事項を定めることを目的とする。

（用語の定義）

第２条　この規程における用語の定義は、個人情報保護法第２条及び第60条並びに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２条の定めるところによる。

第２章　管理体制

（総括保護管理者）

第３条　本部に、総括保護管理者１人を置き、国家社会機能継続性確保施策・副首都整備推進本部事務局長をもって充てる。

２　総括保護管理者は、国家社会機能継続性確保施策・副首都整備推進本部長を補佐し、本部における保有個人情報、個人番号及び行政機関等匿名加工情報等（以下「保有個人情報等」という。）の管理に関する事務を総括するとともに、保有個人情報等の管理の状況について監査する任に当たる。

（保護管理者）

第４条　本部に、保護管理者を置き、総括保護管理者が指名する参事官をもって充てる。

２　保護管理者は、参事官としてつかさどる事務に係る保有個人情報等の適切な管理を確保する任に当たる。保有個人情報等を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる（注）。

（注）例えば、第23条から第39条まで、第44条、第46条及び第47条その他保有個人情報等を情報システムで取り扱う場合、保護管理者は、情報シス

テムの管理者と連携して、それぞれの措置を講ずる。

（保護担当者）

第５条　本部に保護担当者を置き、保護管理者が指名する国家社会機能継続性確保施策・副首都整備推進本部事務局の職員（以下「職員」という。）をもって充てる。

２　保護担当者は、保護管理者を補佐し、保有個人情報及び行政機関等匿名加工情報等の管理に関する事務を担当する。

（特定個人情報等取扱担当者）

第６条　保護管理者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う職員（以下「特定個人情報等取扱担当者」という。）を指名するとともに、当該特定個人情報等取扱担当者が取り扱う特定個人情報等の範囲を指定する。

（国家社会機能継続性確保施策・副首都整備推進本部個人情報等管理委員会）

第７条　総括保護管理者は、保有個人情報等の管理に係る重要事項の決定、連絡・調整等を行うため、必要に応じて保護管理者等を構成員とする国家社会機能継続性確保施策・副首都整備推進本部保有個人情報等管理委員会を開催することができる。

第３章　啓発・教育研修

第８条　総括保護管理者は、保有個人情報等の取扱いに従事する職員（派遣労働者（注）を含む。以下同じ。）に対し、保有個人情報等の取扱いについて理解を深め、個人情報及び特定個人情報等の保護に関する意識の高揚を図るため、啓発に努めなければならない。

（注）派遣労働者についても、従事者の義務（個人情報保護法第 67 条）が適用されるところであり、保有個人情報等の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報等の適切な取扱いを行うことに配慮されたものとする必要がある。

２　総括保護管理者は、保有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、保有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ついて、必要に応じて教育研修を実施する。

３　総括保護管理者は、保護管理者、保護担当者及び特定個人情報等取扱担当者に対し、部局の現場における保有個人情報等の適切な管理のための教育研修を実施する。

４　保護管理者は、職員に対し、保有個人情報等の適切な管理のために、総括保

護管理者の実施する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。

第４章　職員の責務

第９条　職員は、個人情報保護法及び番号法の趣旨に則り、関連する法令及びこの規程並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報等を取り扱わなければならない。

第５章　保有個人情報等の取扱い

（アクセス制限）

第10条　保護管理者は、保有個人情報等の秘匿性等その内容（注）に応じて、当該保有個人情報等にアクセスする（紙等に記録されている保有個人情報等に接する行為を含む。以下同じ。）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る。

（注）個人識別の容易性（匿名化の程度等）、要配慮個人情報の有無、漏えい、滅失又は毀損（以下「漏えい等」という。）が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。

２　アクセス権限を有しない職員は、保有個人情報等にアクセスしてはならない。

３　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報等にアクセスしてはならず、アクセスは必要最小限としなければならない。

（複製等の制限）

第11条　職員が業務上の目的で保有個人情報等を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報等の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従い行う。

一　保有個人情報等の複製

二　保有個人情報等の送信

三　保有個人情報等が記録されている媒体の外部への送付又は持ち出し

四　その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第12条　職員は、保有個人情報等の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

（媒体の管理等）

第13条　職員は、保護管理者の指示に従い、保有個人情報等が記録されている媒体

を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。保有個人情報等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（パスワード、ICカード、生体情報等をいう。以下同じ。）を使用してアクセス権限を識別する機能（以下「認証機能」という。）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。

（誤送付等の防止）

第14条　職員は、保有個人情報を含む電磁的記録又は媒体（注）の誤送信・誤送付、又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認やチェックリストの活用等の必要な措置を講ずる。

（注）文書の内容だけでなく、付加情報（PDFファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。

（廃棄等）

第15条　職員は、保有個人情報等又は保有個人情報等が記録されている媒体（端末及びサーバーに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行うものとする。特に、保有個人情報等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（二以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び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。

（保有個人情報等の取扱状況の記録）

第16条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録する。

２　保護管理者は、特定個人情報ファイルを保有する場合は、台帳等を整備して、当該特定個人情報等の利用及び保管等の取扱いの状況について記録する。

（外的環境の把握）

第17条　保有個人情報が、外国（※）において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

（※）近年、行政機関等においても民間事業者が提供するクラウドサービスを利用する場合があり得るところであり、こうした場合においてはクラウドサービス提供事業者が所在する外国及び保有個人情報が保存されるサーバーが所在する外国が該当する。

（個人番号の利用の制限）

第18条　保護管理者は、個人番号の利用に当たり、番号法があらかじめ限定的に定めた事務に限定する。

（個人番号の提供の求めの制限）

第19条　職員（国家社会機能継続性確保施策・副首都整備推進本部員を含む。以下次条及び第21条において同じ。）は、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。）を処理するために必要な場合その他番号法で定める場合を除き、個人番号の提供を求めてはならない。

（特定個人情報ファイルの作成の制限）

第20条　職員は、個人番号利用事務等を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。

（特定個人情報の収集・保管の制限）

第21条　職員は、番号法第19条各号のいずれかに該当する場合を除き、他人の個人番号を含む特定個人情報を収集又は保管してはならない。

（物理的な安全管理措置）

第22条　保護管理者は、特定個人情報等を取り扱う事務を実施するに当たり、物理的な安全管理措置等を講ずる。

第６章　情報システムにおける安全の確保等

（アクセス制御）

第23条　保護管理者は、保有個人情報等（情報システムで取り扱うものに限る。以下第32条を除き、この章において同じ。）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（注）。

（注）アクセス制御の措置内容は、第10条により設定した必要最小限のアクセス権限を具体化するものである必要がある。

２　保護管理者が前項の措置を講ずる場合には、パスワード等の管理に関する規程を定める（その定期又は随時の見直しを含む。）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。

（アクセス記録）

第24条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存する。

２　保護管理者は、アクセス記録を定期に及び必要に応じて分析するものとする。

３　保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

４　保護管理者は、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、必要に応じて分析するための措置を講ずる。また、アクセス記録の改ざん、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。

（アクセス状況の監視）

第25条　保護管理者は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能等の設定、当該設定の定期的確認等の必要な措置を講ずる。

（管理者権限の設定）

第26条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

（外部からの不正アクセスの防止）

第27条　保護管理者は、保有個人情報等を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。

（不正プログラムによる漏えい等の防止）

第28条　保護管理者は、不正プログラムによる保有個人情報等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。

（情報システムにおける保有個人情報等の処理）

第29条　職員は、保有個人情報等について、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。保護管理者は、当該保有個人情報等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。

（暗号化）

第30条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。

２　職員は、前項を踏まえ、その処理する保有個人情報等について、当該保有個人情報等の秘匿性等その内容に応じて、適切に暗号化（注）を行う。

（注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。

（入力情報の照合等）

第31条　職員は、情報システムで取り扱う保有個人情報等の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認、既存の保有個人情報等との照合等を行う。

（バックアップ）

第32条　保護管理者は、保有個人情報等の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。

（情報システム設計書等の管理）

第33条　保護管理者は、保有個人情報等に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。

（端末の限定）

第34条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。

（端末の盗難防止等）

第35条　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。

２　職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

第36条　職員は、端末の使用に当たっては、保有個人情報等が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

（記録機能を有する機器・媒体の接続制限）

第37条　保護管理者は、保有個人情報等の秘匿性等その内容に応じて、当該保有個人情報等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（当該機器の更新への対応を含む。）等の必要な措置を講ずる。

第７章　情報システム室等の安全管理

（入退管理）

第38条　保護管理者は、保有個人情報等を取り扱う基幹的なサーバー等の機器を設置する室その他の区域（以下「情報システム室等」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保

有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ものとする。

2　保護管理者は、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の管理の容易化、所在表示の制限等の措置を講ずるものとする。

3　保護管理者は、情報システム室等及び保管施設の入退の管理について、必要があると認めるときは、立入りに係る認証機能の設定、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。）及び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。

（情報システム室等の管理）

第39条　保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

2　保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。

第８章　保有個人情報等の提供及び業務の委託等

（保有個人情報等の提供）

第40条　保護管理者は、個人情報保護法第69条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、同法第70条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面（電磁的記録を含む。以下同じ。）を取り交わすものとする。

2　前項の場合において、保護管理者は、個人情報保護法第70条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずるものとする。

3　保護管理者は、個人情報保護法第69条第２項第３号の規定に基づき行政機関又は独立行政法人等に保有個人情報を提供する場合において、必要があると認めるときは、同法第70条の規定に基づき、前二項に規定する措置を講ずるものとする。

4　番号法で限定的に明記された場合を除き、特定個人情報等の提供をしてはならない。

5　次のいずれかに該当する場合を除き、行政機関等匿名加工情報を提供してはならない。

一　法令に基づく場合

二　保有個人情報を利用目的のために第三者に提供することができる場合にお

いて、当該保有個人情報を加工して作成した行政機関等匿名加工情報を当該第三者に提供するとき。

6　法令に基づく場合を除き、利用目的以外の目的のために個人情報保護法第107条第４項に規定する削除情報（保有個人情報に該当するものに限る。）を自ら利用し、又は提供してはならない。

（業務の委託等）

第41条　保有個人情報等の取扱いに係る業務を外部に委託（注１）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（注２）を講ずる。また、契約書に、次に掲げる事項を明記する（予算決算及び会計令（昭和22年勅令第165号）第100条の２の規定により契約書の作成を省略する場合にあっては、次に掲げる事項を遵守する旨を委託先に誓約させる。）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。

一　個人情報に関する秘密保持、目的外利用の禁止等の義務

二　再委託（再委託先が委託先の子会社（会社法（平成17年法律第86号）第２条第１項第３号に規定する子会社をいう。）である場合も含む。本号及び第５項において同じ。）（※）の制限又は事前承認等再委託に係る条件に関する事項

（※）委託先との契約書に、再委託に際して再委託先に求める事項は、再委託先が子会社である場合も、同様に求めるべきことを明記すること。

三　個人情報の複製等の制限に関する事項

四　個人情報の安全管理措置に関する事項

五　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

六　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

七　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（注３）

八　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（再委託先の監査等に関する事項を含む。）

（注１）「委託」とは、契約の形態・種類を問わず、行政機関等が他の者に個人情報の取扱いを行わせることをいう。具体的には、個人情報の入力（本人からの取得を含む。）、編集、分析、出力等の処理を行うことを委託すること等が想定されるが、これらに限られない。

（注２）例えば、次条に記載したサイバーセキュリティに関する対策の基準等を参考に、委託先によるアクセスを認める情報及び情報システムの範囲

を判断する基準や委託先の選定基準を整備すること等が挙げられる。

（注３）準拠法や裁判管轄について日本国内法令とすべきかについてもあらかじめ検討する必要がある。

2　個人番号利用事務等の全部又は一部を委託する場合には、委託先において、番号法に基づき本部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。

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、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らない。

4　保有個人情報及び行政機関等匿名加工情報の取扱い等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、委託先における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。

5　個人番号利用事務等の全部又は一部を委託する際には、委託を受けた者において、本部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。

6　委託先において、保有個人情報及び行政機関等匿名加工情報の取扱い等に係る業務が再委託される場合には、委託先に第１項及び第２項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前二項の措置を実施する。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とする。

7　個人番号利用事務等の全部又は一部の委託を受けた者が再委託をする際には、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する。

8　保有個人情報等の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

9　保有個人情報等を提供又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。

第９章　サイバーセキュリティの確保

（サイバーセキュリティに関する対策の基準等）

第42条　保護管理者は、保有個人情報を取扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法（平成26年法律第104号）第26条第１項第２号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報等の性質等に照らして適正なサイバーセキュリティの水準を確保する。

第10章　安全確保上の問題への対応

（事案の報告）

第43条　保有個人情報等の漏えい等の事案の発生若しくは兆候を把握した場合又は特定個人情報等取扱担当者がこの規程等に違反している事実若しくは兆候を把握した場合その他安全確保の上で問題となる事案又は問題となる事案の発生のおそれ（以下「漏えい事案等」という。）を認識した場合に、当該漏えい事案等を認識した職員は、直ちに当該漏えい事案等に係る保有個人情報等を管理する保護管理者に報告するものとする。（注）

（注）職員は、漏えい事案等の発生を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。また、保護管理者が不在等により直ちに報告することが困難な場合には、漏えい事案等を認識した職員は、総括保護管理者に直ちに報告し、その後、保護管理者に報告しなければならない。

２　保護管理者は、前項の規定により報告を受けた場合には、当該漏えい事案等の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該漏えい事案等の内容等について報告するものとする。

３　保護管理者は、個人情報保護法第107条第１項及び同法第113条の規定（同法第116条の規定により同法第113条の規定を準用する場合を含む。）に基づき行政機関等匿名加工情報の利用に関する契約を締結した者（以下「契約相手方」という。）から、当該契約相手方が講じた行政機関等匿名加工情報の適切な管理に支障を及ぼすおそれがある旨の報告を受けたときは、当該報告に係る漏えい事案等の内容、経緯、被害状況等及び当該契約相手方がその是正のために講じた措置を確認しなければならない。この場合において、確認の結果、特に重大と認める内容である場合には、直ちに総括保護管理者に当該内容等について報告するものとする。

４　総括保護管理者は、第２項又は前項の規定に基づく報告を受けた場合には、必要に応じて、当該漏えい事案等の内容、経緯、被害状況等を国家社会機能継続性確保施策・副首都整備推進本部長に速やかに報告しなければならない。

（再発防止等）

第44条　保護管理者は、前条第１項の規定により報告を受けたときは、当該漏えい

事案等に係る被害の拡大防止又は復旧等のための措置を速やかに講ずるとともに、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のLANケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。

２　前条第１項に規定する漏えい事案等が生じた場合であって、個人情報保護法第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、前条第１項、第２項及び第４項並びに前項と並行して、速やかに所定の手続きを行うとともに、委員会による事案の把握等に協力する。

３　前条第１項に規定する漏えい事案等が生じた場合であって、個人情報保護法第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しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への連絡等の措置を講ずる。

４　総括保護管理者は、前二項の場合を除くほか、国民の不安を招きかねない事案が生じた場合（例えば、公表を行う漏えい事案等が発生したとき、個人情報保護に係る内部規程に対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等）については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会へ情報提供を行うことが望ましい。

第11章　監査及び点検の実施

（監査）

第45条　総括保護管理者は、保有個人情報の適切な管理を検証するため、第３条から前条までに規定する措置の状況を含む本部における保有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（外部監査を含む。以下同じ。）（注）を行うものとする。

（注）保有個人情報等の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。

（点検）

第46条　保護管理者は、自ら管理責任を有する保有個人情報等の記録媒体、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ものとする。

（評価及び見直し）

第47条　この規程等については、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等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行うものとする。

第12章　補則

（個人情報保護委員会事務局への報告）

第48条　保護管理者は、行政機関等匿名加工情報等に係る事案について次に掲げるときは、個人情報保護委員会事務局に報告を行うものとする。

一　第43条第２項又は第３項の報告をしたとき

二　第44条第１項の再発防止のための必要な措置を講じたとき

三　契約相手方が個人情報保護法第118条各号に該当すると認められ契約を解除しようとするとき及び解除したとき

四　契約相手方が個人情報保護法違反その他の契約違反を行ったと判断した時その他必要と判断したとき

附　則

この規程は、令和８年10月30日から施行する。