

個人情報保護委員会の保有する個人情報管理規程（平成28年個人情報保護委員会訓令第8号）の全部を改正する訓令を次のように定める。

平成28年1月12日
個人情報保護委員会訓令第8号
最終改正令和4年3月30日

個人情報保護委員会の保有する個人情報等管理規程

第1章 総則

（目的）

第1条 この規程は、個人情報保護委員会（以下「委員会」という。）の保有する個人情報、個人番号及び特定個人情報（以下「保有個人情報等」という。）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 委員会に、総括保護管理者1人を置き、事務局長をもって充てる。

2 総括保護管理者は、委員会における保有個人情報等の管理に関する事務を総括する任に当たる。

（副総括保護管理者）

第3条の2 委員会に、副総括保護管理者1人を置き、事務局次長をもって充てる。

2 副総括保護管理者は、前条第2項の事務について総括保護管理者を補佐する任に当たる。

（公文書監理官）

第3条の3 委員会に置く公文書監理官は、総括保護管理者の職務を助け、委員会における保有個人情報等の管理の実質責任者としての任に当たる。

(保護管理者)

第4条 各課等に、保護管理者1人を置き、各課等の長をもって充てる。

- 2 保護管理者は、当該課等におけ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。
- 3 保護管理者は、次に掲げる事項を指定する。
 - 一 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者」という。）並びにその役割
 - 二 特定個人情報等取扱者が取り扱う特定個人情報等の範囲

(保護担当者)

第5条 各課等に、保護担当者を置き、当該課等の保護管理者が指名する職員をもって充てる。

- 2 保護担当者は、保護管理者を補佐し、当該課等における保有個人情報等の管理に関する事務を担当する。

(監査責任者)

第6条 委員会に、監査責任者1人を置き、事務局総務課長をもって充てる。

- 2 監査責任者は、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。

(保有個人情報等の適切な管理のための会議)

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があると認めるときは、関係職員を構成員とする会議を定期的に又は随時に開催する。

- 2 総括保護管理者は、必要に応じて情報セキュリティ等について専門的な知識及び経験を有する者等の参加を求めるよう努めるものとする。

第3章 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、保有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を目的として必要な教育研修を実施する。

- 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関して必要な教育研修を実施する。

- 3 総括保護管理者は、保護管理者及び保護担当者に対し、各課等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定期的実施する。
- 4 保護管理者は、当該課室等の職員に対し、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のっとり、関連する法令及び規程等の定め並びに総括保護管理者、副総括保護管理者、保護管理者及び保護担当者（以下「総括保護管理者等」という。）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。
- 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必要最小限に限定し、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。
- 2 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。
- 3 職員は、保有個人情報等が記録されている媒体を庁舎内で移動させる場合には、紛失・盗難等に留意するものとする。

(誤送付等の防止)

- 第13条の2 職員は、保有個人情報等を含む電磁的記録又は媒体の誤送信・誤送付、誤交付、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。

(廃棄等)

- 第14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。
- 2 保有個人情報等の消去や保有個人情報等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15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必要に応じて、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。

(外的環境の把握)

- 第15条の2 保有個人情報等が、外国において取り扱われる場合、当該外国の個人情報等の保護に関する制度等を把握した上で、保有個人情報等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。

(個人番号の利用の制限等)

第16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。

2 特定個人情報等取扱者は、個人番号関係事務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。

3 特定個人情報等取扱者は、個人番号関係事務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。

4 特定個人情報等取扱者は、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個人情報を収集し、及び保管してはならない。

5 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区域を明確にし、物理的な安全管理措置を講ずる。

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17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29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。

2 保護管理者は、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定めを整備するとともに、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。

(アクセス記録)

第18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。）を一定の期間保存し、及びアクセス記録を効率的かつ確実に分析するために必要な措置を講ずる。

2 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等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19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20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21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22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、滅失又は毀損の防止のため、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23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。

(暗号化等)

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、その暗号化のために必要な措置を講ずる。

2 職員は、前項の措置を踏まえ、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、適切に暗号化又はパスワードの付与を行う。

(記録機能を有する機器・媒体の接続制限)

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。

(端末の限定)

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、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27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서는ならない。

(第三者の閲覧防止)

第28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に、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。

(入力情報の照合等)

第29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30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31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に、その保管、複製、廃棄等について必要な措置を講ずる。

第7章 サーバ室等の安全管理

(入退管理)

第32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等の機器を設置する室その他の区域（以下「サーバ室等」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。

- 2 保護管理者は、必要があると認めるときは、サーバ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。
- 3 保護管理者は、サーバ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。

（サーバ室等の管理）

第33条 保護管理者は、外部からの不正な侵入に備え、サーバ室等に施錠装置の設置等の措置を講ずる。

- 2 保護管理者は、災害等に備え、サーバ室等に、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34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、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を取り交わす。

- 2 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、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。
- 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、法第70条の規定に基づき、前2項に規定する措置を講ずる。
- 4 職員は、番号法で限定的に明記された場合を除き、特定個人情報等を提供してはならない。

（業務の委託等）

第35条 保有個人情報等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（特定個人情報等を含む。以下この条において同じ。）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に、必要な措置を講ずる。また、契約書に、次

に掲げる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。

- 一 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
 - 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。本項及び第4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
 - 三 個人情報の複製、持出し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 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
 - 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。）
- 2 保有個人情報等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。
 - 3 保有個人情報等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等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。
 - 4 委託先において、保有個人情報等の取扱いに係る業務が再委託される場合には、委託先に第1項に規定する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等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項に規定する措置を実施する。保有個人情報等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。
 - 5 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する。
 - 6 保有個人情報等を提供し、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、保有個人情報等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 安全確保上の問題への対応

(事案の報告及び再発防止措置)

第36条 保有個人情報等の漏えい等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を認識した場合に、その事案等を認識した職員は、直ちに個人情報保護委員会情報セキュリティポリシー（令和3年11月4日個人情報保護委員会最高情報セキュリティ責任者決定）に定める委員会CSIRT（以下「CSIRT」という。）に報告し、指示に従う。

- 2 保護管理者は、CSIRTと連携し、関係省庁等への報告及び被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。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ケーブルを抜く又は無線LANを無効化した上でCSIRTへ連絡することなど、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。
- 3 保護管理者は、CSIRTと連携し、事案の発生した経緯、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事案の内容等について報告する。
- 4 総括保護管理者は、CSIRTと連携し、前項の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を委員長に速やかに報告する。
- 5 保護管理者は、CSIRTと連携し、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とともに、同種の業務を実施している部局等に再発防止措置を共有する。

(法に基づく報告及び通知)

第36条の2 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項から第5項の規定と並行して、速やかに所定の手続を行うとともに、監視・監督室による事案の把握等に協力する。

(公表等)

第37条 保護管理者は、法第68条第1項の規定による報告及び同条第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等の本人への対応等の措置を講ずる。

- 2 国民の不安を招きかねない事案（例えば、公表を行う漏えい等が発生したとき、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、公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに監視・監督室に情報提供を行う。

第10章 監査及び点検の実施

(監査)

第38条 監査責任者は、保有個人情報等の適切な管理を検証するため、第2章から前章までに規定する措置の状況を含む各課等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。）を行い、その結果を総括保護管理者に報告する。

(点検)

第39条 保護管理者は、各課等におけ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。

(評価及び見直し)

第40条 総括保護管理者等は、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講ずる。

第11章 その他

(サイバーセキュリティに関する対策の基準等)

第41条 個人情報を取り扱い、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。

(細則)

第42条 この規程に定めるもののほか、この規程の実施のための手続その他について必要な事項は、総括保護管理者が別に定める。

附 則

この訓令は、平成28年1月1日から適用する。

附 則（令和元年9月30日個人情報保護委員会訓令第5号）

この訓令は、令和元年9月30日から施行する。

附 則

この訓令は、令和4年4月1日から施行する。