

○神奈川県町村情報システム共同事業組合保有個人情報
等取扱規程

(令和6年3月26日)
(訓令 第1号)

目次

- 第1章 総則 (第1条・第2条)
- 第2章 管理体制 (第3条—第6条)
- 第3章 教育研修 (第7条)
- 第4章 職員の責務 (第8条)
- 第5章 保有個人情報等の取扱い (第9条—第15条)
- 第6章 情報システムにおける安全の確保等 (第16条—第30条)
- 第7章 情報システム等の安全管理 (第31条)
- 第8章 保有個人情報等の提供及び業務の委託等 (第32条・第33条)
- 第9章 安全確保上の問題への対応 (第34条—第36条)
- 第10章 監査及び点検の実施 (第37条—第39条)
- 第11章 その他 (第40条)

附則

第1章 総則

(趣旨)

第1条 この規程は、個人情報の保護に関する法律(平成15年法律第57号。以下「保護法」という。)、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。)、神奈川県町村情報システム共同事業組合個人情報の保護に関する法律施行条例(令和5年条例第4号。以下「保護法施行条例」という。)、に定めるもののほか、本組合における保有個人情報及び個人番号(以下「保有個人情報等」という。)の適正かつ円滑な運用管理及び情報保護の安全管理対策に関し、必要な事項を定めることを目的とする。

(定義)

第2条 この規程における用語の意義は、保護法、番号法及び保護法施行条例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 本組合に、総括保護管理者を置くこととし、事務局長をもって充てる。

2 総括保護管理者は、保有個人情報等の管理を総括する任に当たる。

(保護管理者)

第4条 保有個人情報等を取り扱う課等に、保護管理者を置くこととし、主幹又は副主幹若しくは主査をもって充てる。

- 2 保護管理者は、課等における保有個人情報等を適切に管理する任に当たる。
- 3 保護管理者は、保有個人情報等を取り扱う職員(以下「保護担当者」という。)、その役割及び各保護担当者が取り扱う保有個人情報等の範囲を指定する。

(監査責任者)

第5条 本組合に、監査責任者を置くこととし、内部監査等を担当する事務局次長をもって充てる。

- 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。

(保有個人情報等の管理に係る委員会)

第6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委員会を設け、定期に又は随時に開催するものとする。

第3章 教育研修

(教育研修)

第7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必要な教育研修を行うものとする。

- 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行うものとする。
- 3 保護管理者は、当該課等の職員に対し、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じなければならない。

第4章 職員の責務

(職員の責務)

第8条 職員は、保護法、番号法及び保護法施行条例の趣旨にのっとり、関連する法令及び規程等の定め及び総括保護管理者、保護管理者の指示に従い、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

(アクセス制限等)

第9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権限を有する者をその利用目的を達成するために必要最小限の職員に限定する。

- 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ない。

(複製等の制限)

第10条 職員は、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、次に掲げる行為については、保護管理者の指示に従わなければならない。

- (1) 保有個人情報等の複製

- (2) 保有個人情報等の送信
- (3) 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出し
- (4) 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 11 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 12 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、施錠等を行うものとする。また、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じなければならない。

(誤送付等の防止)

第 13 条 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ぐため、事務において取り扱う保有個人情報等の秘匿性等その内容に応じ、複数の職員による確認、チェックリストの活用等の必要な措置を講じなければならない。

(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わなければならない。

(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ものとする。

2 職員は、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。

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 16 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をするために必要な措置を講じなければならない。

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(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。

(アクセス記録等)

第 17 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定期的に分析するために必要な措置を講ずるものとする。

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の防止のために必要な措置を講ずるものとする。

3 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、当該保有個人情報への不適切なアクセスの監視のため、監査機能の設定、当該機能の定期的確認等の必要な措置を講ずるものとする。

(アクセス状況の監視)

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み、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ものとする。

(管理者権限の設定)

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に応じて、情報システムの管理者権限の特権を不正に搾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ものとする。

(外部からの不正アクセスの防止)

第 20 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ものとする。

(不正プログラムによる漏えい等の防止)

第 21 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、不正プログラムの感染防止等に必要な措置を講ずるものとする。

(情報システムにおける保有個人情報の処理)

第 22 条 職員等は、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は、その対象を必要最小限とし、処理終了後は不要となった情報を速やかに消去するものとする。

2 保護管理者は、前項の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ものとする。

(暗号化)

第 23 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ものとする。

(記録機能を有する機器・媒体の接続制限)

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の漏えい、滅失又は毀損の防止のため、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ものとする。

(入力情報の照合等)

第 25 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ものとする。

(バックアップ)

第 26 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ものとする。

(情報システム設計書等の管理)

第 27 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じなければならない。

(端末の限定)

第 28 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ものとする。

(端末の盗難防止等)

第 29 条 保護管理者は、前条に規定する端末について、個人情報等が記録可能な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てはならない。

(第三者の閲覧防止等)

第 30 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ものとする。

第 7 章 情報システム等の安全管理

(情報システム等の管理)

第 31 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じなければならない。

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ものとする。

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 32 条 保護管理者は、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等以外の者に保有個人情報等を提供する場合には、保護法第 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、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以外の者に保有個人情報等を提供する場合には、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、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、保護法第 69 条第 2 項第 3 号の規定に基づき他の行政機関等に保有個人情報等を提供する場合において、必要があると認めるときは、前 2 項に規定する措置を講ずる。

(業務の委託等)

第 33 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。

- (1) 個人情報等に関する秘密保持、目的外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) 個人情報等の複製等の制限に関する事項
- (4) 個人情報等の漏えい等の事案の発生時における対応に関する事項
- (5) 委託終了時における個人情報等の消去及び媒体の返却に関する事項
- (6) 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

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 34 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が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報等を管理する保護管理者に報告しなければならない。

- 2 保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずるものとする。
- 3 保護管理者は、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しなければならない。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ものとする。
- 4 総括保護管理者は、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、被害状況等を管理者に速やかに報告するものとする。
- 5 保護管理者は、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じなければならない。

(法に基づく報告及び通知)

第 35 条 総括保護管理者は、保有個人情報の漏えい等の事案が発生した場合であって、個人情報保護法第 68 条第 1 項の規定による個人情報保護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、前条の規定による措置の実施等と並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力するものとする。

(公表等)

第 36 条 前条に規定する場合その他事案が発生した場合において、総括保護管理者は、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、当該事案に係る本人への対応等の措置を講ずるものとする。

第 10 章 監査及び点検の実施

(監査)

第 37 条 監査責任者は、保有個人情報等の管理の状況について、定期に又は随時に監査(外部監査を含む。)を行い、その結果を総括保護管理者に報告しなければならない。

(点検)

第 38 条 保護管理者は、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、定期に又は随時に点検を行い、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 39 条 保有個人情報等の適切な管理のための措置については、総括保護管理者、保護管理者は、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、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ものとする。

第 11 章 その他

(その他)

第 40 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、管理者が別に定める。

附 則

この訓令は、令和 6 年 4 月 1 日から施行する