東京都板橋区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基準

（令和５年３月20日総務部長決定）

目次

第１章 総則（第１条・第２条）

第２章 管理体制（第３条～第７条）

第３章 職員の責務（第８条）

第４章 保有個人情報の取扱い（第９条～第１６条）

第５章 情報システムにおける安全の確保等（第１７条～第３１条）

第６章 情報システム室等の安全管理（第３２条・第３３条）

第７章 保有個人情報の提供（第３４条）

第８章 個人情報の取扱いの委託（第３５条）

第９章 サイバーセキュリティの確保（第３６条）

第１０章 安全確保上の問題への対応（第３７条～第３９条）

第１１章 監査及び点検の実施（第４０条～第４２条）

第１２章 補則（第４３条・第４４条）

第１章 総則

（趣旨）

第１条 この基準は、東京都板橋区（以下「板橋区」という。）における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６６条に規定する保有個人情報の安全管理のために必要な措置について定めるものとする。

（定義）

第２条 この基準で使用する用語は、個人情報保護法で使用する用語の例による。

第２章 管理体制

（総括保護管理者）

第３条 板橋区に、総括保護管理者１人を置く。

２ 総括保護管理者は、総務部長をもって充てる。

３ 総括保護管理者は、次に掲げる事務を行うものとする。

(1) 保有個人情報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こと。

なお、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ことができる。

(2) 前号に掲げるもののほか、板橋区における保有個人情報の管理に関する事務の総括に関すること。

４ 総括保護管理者を補佐し、保有個人情報の保護に関する事務を担うため、副総括保護管理者を置き、総務部区政情報課長（以下「区政情報課長」という。）をもって充てる。

５ 前項の副総括保護管理者を補佐し、同項の事務のうち電子計算機等の管理運営及び電子情報処理組織の使用に係るものを担うため、副総括保護管理者補佐を置き、政策経営部ＩＴ推進課長（以下「ＩＴ推進課長」という。）をもって充てるものとする。

（保護管理者）

第４条 課又は所における保有個人情報の適切な管理を確保するため、課又は所（以下「各課等」という。）に保護管理者１人を置く。

２ 保護管理者は、課長又は所長をもって充てる。

３ 保護管理者は、各課等における保有個人情報の適切な管理を確保する任に当たる。

４ 保護管理者は、保有個人情報を情報システムで取り扱う場合、当該情報システムの管理者と連携して、その任に当たる｡

（保護担当者）

第５条 各課等に、保護担当者１人（業務上必要と認められる場合にあっては複数人）を置く。

２ 保護担当者は、課又は所の係長又はこれに相当する主査の中から課長又は所長が指名する者をもって充てる。ただし、地域センター、区民事務所及び幼稚園にあっては所長が指名する者を、学校にあっては副校長をもって充てる。

３ 保護担当者は、保護管理者を補佐し、各課等における保有個人情報の管理に関する事務を担う。

（監査責任者）

第６条 板橋区に、監査責任者１人を置く。

２ 監査責任者は、区政情報課長をもって充てる。

３ 監査責任者は、板橋区における保有個人情報の管理の状況について監査する。

４ 前項の監査責任者を補佐し、同項に規定する監査のうち電算処理ファイル（個人情報保護法第60条第２項に規定する個人情報ファイルであって、同項第１号に掲げるものをいう。）の管理の状況及び電子情報処理組織の使用の状況に係るものを担うため、監査責任者補佐を置き、ＩＴ推進課長をもって充てる。

（研修）

第７条 副総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、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。

２ 副総括保護管理者は、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定期的に実施する。

３ 副総括保護管理者補佐は、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教育研修を行う。

４ 保護管理者は、各課等の職員に対し、保有個人情報の適切な管理のために、副総括保護管理者及び副総括保護管理者補佐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３章 職員の責務

（職員の責務）

第８条 職員は、個人情報保護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（副総括保護管理者及び副総括保護管理者補佐を含む。）、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

第４章 保有個人情報の取扱い

（アクセス制限）

第９条 保護管理者は、保有個人情報の秘匿性等その内容（特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等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。）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る。

２ アクセス権限を有しない職員は、保有個人情報にアクセスをしてはならない。

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にアクセスをしてはならず、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１０条 職員が業務上の目的で保有個人情報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。

(1) 保有個人情報の複製

(2) 保有個人情報の送信

(3) 保有個人情報が記録されている媒体の外部への送付又は持ち出し

(4) その他保有個人情報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。

また、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（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。

（誤送付等の防止）

第１３条 職員は、保有個人情報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、保有個人情報又は保有個人情報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。

特に、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（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。

（保有個人情報の取扱状況の記録）

第１５条 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。

（外的環境の把握）

第１６条 保有個人情報が、外国（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個人データが保存されるサーバが所在する外国が該当する。）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。

第５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（情報システムで取り扱うものに限る。以下第２９条を除き、この章及び次章において同じ。）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（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。

（アクセス記録）

第１８条 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の状況を記録し、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。

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。

（アクセス状況の監視）

第１９条 保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報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の処理）

第２３条 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。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。

（暗号化）

第２４条 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、その暗号化のために必要な措置を講ずる。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。

（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（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、保護管理者が必要で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２８条 職員は、端末機器の使用に当たっては、保有個人情報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。

（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の内容の確認、既存の保有個人情報との照合等を行う。

（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。

第６章 情報システム室等の安全管理

（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「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、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。

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。

（情報システム室等の管理）

第３３条 保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び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７章 保有個人情報の提供

（保有個人情報の提供）

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等以外の者に保有個人情報を提供する場合には、個人情報保護法第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提供先との間で書面（電磁的記録を含む。）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等以外の者に保有個人情報を提供する場合には、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。

３ 保護管理者は、個人情報保護法第６９条第２項第３号の規定に基づき他の行政機関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、個人情報保護法第７０条の規定に基づき、前２項に規定する措置を講ずる。

第８章　個人情報の取扱いの委託

（業務の委託等）

第３５条 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。

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。

(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（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

(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（再委託先の監査等に関する事項を含む。）

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らない。

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。

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、委託先に第１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第３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。

５ 保有個人情報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３６条 保護管理者は、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

（事案の報告及び再発防止措置）

第３７条 保有個人情報の漏えい等安全管理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、直ちに当該保有個人情報を管理する保護管理者に報告する。

２ 保護管理者は、被害の拡大防止、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、事案の発生した経緯、被害状況等を調査し、副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、直ちに副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 副総括保護管理者は、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、保護管理者及び総括保護管理者とともに、東京都板橋区長に速やかに報告する。

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ずるとともに、同種の業務を実施している各課等に再発防止措置を共有する。

（個人情報保護法に基づく報告及び通知）

第３８条 副総括保護管理者は、漏えい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、前条で定める事項と並行して、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。

（公表等）

第３９条 副総括保護管理者及び保護管理者は、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。

第１１章 監査及び点検の実施

（監査）

第４０条 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、第２章から第１０章に規定する措置の状況を含む板橋区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（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４１条 保護管理者は、各課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、その結果を副総括保護管理者に報告する。

（評価及び見直し）

第４２条 副総括保護管理者及び副総括保護管理者補佐、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。

 第１２章 補則

（他の基準との関係）

第４３条 他の基準の規定により、情報システムの管理に関する事項について、この基準と別段の定めが設けられている場合にあっては、この基準に定めるもののほか、当該基準の定めるところによる。

（細則）

第４４条 この基準の施行に関し必要な事項は、別に副総括保護管理者が定める。

２ 保護管理者は、この基準を実施し、又は保有個人情報の適切な管理のため、必要があるときは、細則を定めることができる。

３ 保護管理者は、前項の細則を定め、変更し、又は廃止したときは速やかに副総括保護管理者に報告するものとする。

付　則

この基準は、令和５年４月１日から施行する。