

白岡市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方針
(案)

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32条）

第6章 情報システム室の安全管理（第33条・第34条）

第7章 保有個人情報の提供及び業務の委託等（第35条・第36条
）

第8章 安全管理上の問題への対応（第37条―第39条）

第9章 監査及び点検の実施（第40条―第42条）

第10章 補則（第43条・第44条）

第1章 総則

(趣旨)

第1条 この方針は、市（議会を除く。以下同じ。）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「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 この方針で使用する用語は、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 市に、総括保護管理者1人を置く。

2 総括保護管理者は、副市長の職にある者をもって充てる。

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

イ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、市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。

(保護管理者)

第4条 各課に、保護管理者1人を置く。

2 保護管理者は、課長の職にある者をもって充てる。

3 保護管理者は、各課における保有個人情報の管理に関する事務を総括する。

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、前項の事務を行う。

(保護担当者)

第5条 各課に、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、保護管理者が指定する者をもって充てる。

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

(監査責任者)

第6条 市に、監査責任者1人を置く。

2 監査責任者は、総務部長の職にある者をもって充てる。

3 監査責任者は、市における保有個人情報の管理の状況について監査する。

(研修)

第7条 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、保有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 総括保護管理者は、保護管理者及び保護担当者に対し、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実施する。

3 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、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、各課の職員に対し、保有個人情報の適切な管理のため、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る。

第3章 職員の責務

(職員の責務)

第8条 職員は、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、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（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（情報に接する行為をいう。以下同じ。）をする権限（以下「アクセス権限」という。）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ものとする。

- 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 保護管理者は、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、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ものとする。

- (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として保護管理者が定めるもの
- (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、訂正等を行うものとする。

(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、当該媒体の耐火金庫への保管、保管場所への施錠等の保有個人情報の漏えい等を防止するための措置を講じるものとする。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じるものとする。

(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じるものとする。

(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（端末機器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、保有個人情報の消去又は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（2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ものとする。

（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、当該保有個人情報の利用、保管等の取扱いの状況について記録するものとする。

（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ー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25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当該保有個人情報へのアクセスを制御するために必要な措置を講じるものとする。

2 保護管理者は、前項の措置を講じる場合には、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じるものとする。

（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じるものとする。

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じるものとする。

(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じるものとする。

(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じるものとする。

(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じるものとする。

(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。）を講じるものとする。

(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を行う場合には、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。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ものとする。

(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じるものとする。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じるものとする。

(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るものとする。

(端末機器の限定)

第28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処理を行う端末機器を限定するために必要な措置を講じるものとする。

(端末機器の盗難防止等)

第29条 保護管理者は、端末機器の盗難又は紛失の防止のため、端末機器の固定、執務室の施錠等の必要な措置を講じるものとする。

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

(閲覧防止)

第30条 職員は、端末機器の使用に当たっては、保有個人情報が当該職員以外の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じるものとする。

(記録機能を有する機器・媒体の接続制限)

第31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じるものとする。

（サイバーセキュリティに関する対策の基準等）

第32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（平成26年第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6章 情報システム室の安全管理

（入退管理）

第33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ー等で保護管理者が指定する機器を設置する室その他の区域（以下「情報システム室」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じるものとする。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、同様の措置を講じるものとする。

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情報システム室の安全を管理するための措置を講じるものとする。

3 保護管理者は、情報システム室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、身分証明書の提示を求めるとともに、立入りに係る認証機能を設定し、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。）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じるものとする。

（情報システム室の管理）

第34条 保護管理者は、外部からの不正な侵入に備え、情報システム室に制御機能、施錠装置、警報装置及び監視設備の整備等の措置を講じるものとする。

2 保護管理者は、災害等に備え、情報システム室に、耐震、防火、防煙、防水等の必要な措置を講じるとともに、サーバー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じるものとする。

第7章 保有個人情報の提供及び業務の委託等

(保有個人情報の提供)

第35条 保護管理者は、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、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を取り交わすものとする。

2 保護管理者は、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、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うことにより当該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じるものとする。

3 保護管理者は、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、法第70条の規定に基づき、前2項に規定する措置を講じるものとする。

(業務の委託等)

第36条 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、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、必要な措置を講じるものとする。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ものとする。

- (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3号に規定する子会社をいう。）である場合も含む。以下この号及び第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
- 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、委託先における責任者及び業務従事者の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を行うものとする。
- 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前項の措置を講じるものとする。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保有個人情報の取扱いに関する

る事項を明記するものとする。

- 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若しくは一部を削除し、又は別の記号等に置き換える等の措置を講じる。

第8章 安全管理上の問題への対応

(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の事案の発生又は兆候を把握した場合等、安全管理の上で問題となる事案の発生又は発生のおそれを認識した場合に、その事案の発生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ものとする。

- 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じるものとする。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端末ネットワーク遮断スクリプトの実行等によるネットワークからの遮断など、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、総括保護管理者に報告するものとする。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ものとする。また、白岡市情報セキュリティ対策基準（以下「対策基準」という。）における情報セキュリティインシデントに該当する場合には、対策基準を踏まえた対応を行うものとする。
- 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、被害状況等を市長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るとともに、同種の業務を実施している部局に当該措置を共有するものとする。

(法に基づく報告及び通知)

第38条 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 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対応等の措置を講じるものとする。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、速やかに個人情報保護委員会事務局に情報提供を行うものとする。また、対策基準における情報セキュリティインシデントに該当する場合には、対策基準を踏まえた対応を行うものとする。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の市民の不安を招きかねない事案については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会事務局へ情報提供を行うものとする。

第9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8章までに規定する措置の状況を含む市における保有個人情報の管理の状況について、定期及び必要に応じ随時に監査（外部監査の委託を含む。以下同じ。）を行い、その結果を総括保護管理者に報告するものとする。

(点検)

第41条 保護管理者は、各課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。

る。

(評価及び見直し)

第42条 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じるものとする。

第10章 補則

(他の規定との関係)

第43条 情報システムの管理に関する事項について、この方針と別段の規定が設けられている場合にあつては、この方針に定めるもののほか、当該規定の定めるところによる。

(細則)

第44条 この方針の施行に関し必要な事項は、別に総括保護管理者が定める。

2 保護管理者は、この方針を実施し、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総括保護管理者に報告しなければならない。

附 則

この方針は、デジタル社会の形成を図るための関係法律の整備に関する法律（令和3年法律第37号）附則第1条第7号に掲げる規定（同法第51条の規定に限る。）の施行の日から施行する。