入善町保有個人情報等の取扱いに関する安全管理規程

制定　平成27年12月28日
一部改正　平成30年４月１日
一部改正　令和５年４月１日
一部改正　令和７年12月１日

（定義）

第１条　この規程における用語の意義は、「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。）及び「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。）の定めるところによる。

（管理体制）

第２条　町に、総括責任者を一人置くこととし、副町長をもって充て、町長を補佐し、町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。）の管理に関する事務を総括する任に当たる。

２　保有個人情報等を取り扱う各課（室及び局を含む。以下同じ。）に、保護責任者を一人置くこととし、当該所属の長又はこれに代わる者をもって充て、各所属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。この場合において、保有個人情報等を情報システムで取り扱うときは、保護責任者は、当該情報システムの管理者と連携して、その任に当たるものとする。

３　保有個人情報等を取り扱う各課に、当該所属の保護責任者が指定する保護担当者を置くものとし、保護責任者を補佐し、各所属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。

４　町に、監査責任者を一人置くこととし、総務課長をもって充て、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。この場合において、保有個人情報等を情報システムで取り扱う場合の監査については、財政課長の協力を得て、その任にあたるものとする。

５　総括責任者は、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ことができる。この場合において、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。

6　保護責任者は、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（臨時的な雇用による者を含む。以下「特定個人情報等事務取扱担当者」という。）及びその役割を指定するものとする。

7　保護責任者は、それぞれの特定個人情報等事務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ものとし、次に掲げる組織体制を整備する。

⑴　特定個人情報等事務取扱担当者が、取扱規程等に違反している事実又は兆候を把握した場合の保護責任者への報告連絡体制

⑵　特定個人情報等の漏えい、滅失又は毀損等（以下「情報漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制

⑶　特定個人情報等を複数の所属で取り扱う場合の各所属の任務分担及び責任の明確化

⑷　特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の対応体制

（教育研修）

第３条　総括責任者は、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必要な教育研修を行うものとする。

2　総括責任者は、保有個人情報等を取り扱う情報システム（以下「情報システム」という。）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。

3　総括責任者は、保護責任者及び保護担当者に対し、各所属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　保護責任者は、当該所属の職員に対し、保有個人情報等の適切な管理のために、総括責任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。

（職員の責務）

第４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、規則等の規定並びに総括責任者、保護責任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。

（保有個人情報等の取扱い）

第５条　保護責任者は、保有個人情報等を取り扱う権限（以下「アクセス権限」という。）を有する職員とアクセス権限の内容を、必要最小限の範囲に限る措置を行なうものとする。

２　アクセス権限を有しない職員は、保有個人情報等を取り扱ってはならないものとする。

３　職員は、アクセス権限を有する場合であっても、業務上の目的外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。

４　職員が業務上の目的で保有個人情報等を取り扱う場合は、保護責任者は、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、保護責任者の指示に従い行わなければならない。

⑴　保有個人情報等の複製

⑵　保有個人情報等の送信

⑶　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

⑷　その他保有個人情報等の適切な管理に支障をきたすおそれのある行為

５　職員は、保有個人情報等の内容に誤りその他訂正が必要な事項を発見した場合には、保護責任者の指示に従い、訂正、修正その他必要な措置を行う。

６　職員は、保護責任者の指示に従い、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、保護責任者が必要と認めるときは、耐火性のある金庫その他の設備に保管し、又は施錠等を行うものとする。この場合において、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ものとする。

７　職員は、保有個人情報等を含む電磁的記録若しくは媒体の誤送信、誤送付及び誤交付又はウェブサイト等への誤掲載を防止するため、個別の事務及び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、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。

８　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（電子情報処理組織における個人の情報端末又はサーバーに内蔵されている電子媒体を含

む。）が不要となった場合には、保護責任者の指示に従い、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。この場合において、保有個人情報等の消去及び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（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等、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。

９　保護責任者は、保有個人情報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、当該保有個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

10　保護責任者は、特定個人情報ファイル（紙媒体を含む。以下同じ。）を保有する場合は、特定個人情報ファイルの取扱状況を確認する台帳を整備し、次に掲げる事項を記録し、特定個人情報等の利用及び保管の取扱状況を記録するものとする。この場合において、当該記録には、特定個人情報等は記載しないものとする。

⑴　特定個人情報ファイルの名称

⑵　特定個人情報ファイルが利用に供される事務を担当する所属の名称

⑶　特定個人情報ファイルの利用目的

⑷　特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲

⑸　特定個人情報ファイルに記録される特定個人情報等の収集方法

11　保護責任者は、個人番号の利用を、番号法があらかじめ定めた事務に限定するものとする。

12　保護責任者は、保有個人情報等が、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。

13　職員は、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。

14　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。

15　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個人情報を収集又は保管してはならない。

16　保護責任者は、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全措置を講ずるものとする。

（情報システムにおける安全の確保等）

第６条　保護責任者は、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、この条において同じ。）について、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ものとする。

２　保護責任者は、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規定を整備し、又は当該規定の定期若しくは随時の見直しを行い、パスワード等の読取防止を行うために必要な措置を講ずるものとする。

３　保護責任者は、保有個人情報等の秘匿性等その内容及び必要に応じて、当該保有個人情報等の取扱い状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及び定期に又は随時に分析するために必要な措置を講ずるものとする。

４　保護責任者は、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じなければならない。

５　保護責任者は、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じなければならない。

６　保護責任者は、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場合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なければならない。

７　保護責任者又は財政課長は、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。

８　保護責任者は、不正プログラムによる保有個人情報等の情報漏えい等の防止の

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。）を講ずるものとする。

9　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ものとする。この場合において、保護責任者は、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ものとする。

10　保護責任者は、保有個人情報等の秘匿性等その内容に応じて、暗号化のために必要な措置を講じなければならない。この場合において、職員は、これを踏まえ、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、適切に暗号化を行うものとする。

11　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。

12　保護責任者は、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じなければならない。

13　保護責任者は、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ものとする。

14　保護責任者は、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しなければならない。

15　保護責任者は、情報端末の盗難又は紛失の防止のため、情報端末の固定、執務室の施錠等の必要な措置を講ずる。

16　職員は、保護責任者が認める場合を除き、情報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。

17　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しなければならない。

18　保護責任者は、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情報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及び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。

（保有個人情報等の保管区域の保全）

第７条　保護責任者又は財政課長は、保有個人情報等を取り扱う基幹的なサーバ等で保護責任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若しく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ものとする。この場合において、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　保護責任者又は財政課長は、認証機能の設定、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ことができる。

３　保護責任者は、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、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ものとする。

４　保護責任者又は財政課長は、災害等に備え、情報システム室等に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。

（保有個人情報の提供）

第８条　保護責任者は、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、個人情報保護法第70条の規定に基づき、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さなければならない。

２　保護責任者は、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、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じることができる。

３　保護責任者は、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、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じることができる。

（特定個人情報の提供）

第９条　保護責任者は、番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

（保有個人情報の取扱いに係る業務の委託等）

第10条　保護責任者は、保有個人情報の取扱いに係る業務の全部又は一部を委託する場合には、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ものとする。また、当該委託にかかる契約書に、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を書面で確認するものとする。

⑴　個人情報に関する秘密保持、目的外利用の禁止等の義務

⑵　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、第８号、第３項及び第11条第３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

⑶　個人情報の複製等の制限に関する事項

⑷　個人情報の安全管理措置に関する事項

⑸　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

⑹　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

⑺　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

⑻　契約内容の遵守状況についての定期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　保護責任者は、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とし、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、

年１回以上の定期的な検査により確認するものとする。

３　保護責任者は、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実施するものとする。この場合において、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。

４　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ものとする。

５　保有個人情報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、又は別の記号に置き換える等の措置を講ずるものとする。

（特定個人情報等の取扱いに係る業務の委託等）

第11条　保護責任者は、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、番号法に基づき町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ものとする。

２　保護責任者は、個人番号利用事務等の全部又は一部の委託をする場合には、委託先において、町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。

３　保護責任者は、個人番号利用事務等の全部又は一部の委託先が再委託をする場合には、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しなければならない。

（サイバーセキュリティに関する対策の基準等）

第12条　保護責任者は、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。

（安全確保上の問題への対応）

第13条　保有個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合及び特定個人情報等事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合等、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、その事案等を知った職員は、直ちに当該保有個人情報等を管理する保護責任者に報告しなければならない。

２　保護責任者は、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ＬＡＮケーブルを抜く等、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　保護責任者は、事案の発生した経緯、被害状況等を調査し、総括責任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、直ちに総括責任者に当該事案の内容等について報告しなければならない。

４　総括責任者は、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、被害状況等を町長に速やかに報告するものとする。

５　保護責任者は、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ものとする。

６　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ものとする。

７　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並びに番号法第29条の４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の４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連絡等の措置を講ずるとともに、必要に応じて当該事案の内容、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ものとする。

（監査及び点検の実施）

第14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条から第13条までに規定する措置の状況を含む町における保有個人情報等の管理の状況について、監査（外部監査を含む。以下同じ。）を行い、その結果を総括責任者

に報告するものとする。

２　保護責任者は、各所属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、点検を行い、必要があると認めるときは、その結果を総括責任者に報告する。

３　総括責任者、保護責任者等は、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。

（その他）

第15条　この規程の施行にあたり必要な事項は、別に定める。

附　則

この規程は、平成28年１月１日から施行する。

附　則

この規程は、平成30年４月１日から施行する。

附　則

この規程は、令和５年４月１日から施行する。

附　則

この規程は、令和７年12月１日から施行する。