# 越前市保有個人情報保護管理規程

目次



## 第１章　総則

（総則）

第１条　この規程は、越前市が保有する個人情報（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２条第１項に規定する個人情報をいう。以下同じ。）の適正な取扱いについて、必要な事項を定めるものとする。

（定義）

第２条　この規程において使用する用語は､法において使用する用語の例による。

## 第２章　保有個人情報の管理体制等

（最高情報セキュリティ責任者）

第３条　市に、最高情報セキュリティ責任者を１人置くこととし、副市長をもって充てる。

２　最高情報セキュリティ責任者は、市における保有個人情報の管理に関する最終決定権限及び責任を有する。

（総括情報セキュリティ責任者）

第４条　市に、総括情報セキュリティ責任者を１人置くこととし、総務部長をもって充てる。

２　総括情報セキュリティ責任者は、最高情報セキュリティ責任者（越前市情報セキュリティ対策基準（令和５年４月１日施行）第２第１項の表に規定する最高情報セキュリティ責任者をいう。以下同じ。）を補佐し、市における保有個人情報の管理に関する事務を総括する任に当たる。

（情報セキュリティ責任者）

第５条　市に、情報セキュリティ責任者を置くこととし、各部局の長をもって充てる。

２　情報セキュリティ責任者は、各部局における保有個人情報の管理に関する事務を総括する任に当たる。

（情報セキュリティ管理者）

第６条　保有個人情報を取り扱う各所属に、情報セキュリティ管理者を１人置くこととし、各所属長をもって充てる。

２　情報セキュリティ管理者は、各所属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。

３　情報セキュリティ管理者は､保有個人情報を情報システムで取り扱うときは、第８条に規定する情報システム管理者と連携して、その任に当たる。

４　情報セキュリティ管理者は、保有個人情報を取り扱う職員（派遣労働者を含む。以下「事務担当者」という。）及びその役割を指定するとともに、保有個人情報が適正に取り扱われるよう、事務担当者に対し必要かつ適切な監督を行う。

５　情報セキュリティ管理者は、各事務担当者が取り扱う保有個人情報の範囲を指定する。

６　情報セキュリティ管理者は、次に掲げる組織体制を整備する。

(1) 事務担当者が本規程等に違反している事実又は兆候を把握した場合の情報セキュリティ責任者への報告連絡体制

(2) 保有個人情報の漏えい、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情報セキュリティ責任者及び情報セキュリティ管理者への報告連絡体制

(3) 保有個人情報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

(4) 保有個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

（情報セキュリティ担当者）

第７条　保有個人情報を取り扱う各所属に、当該所属の情報セキュリティ管理者が指定する情報セキュリティ担当者を１人置く。

２　情報セキュリティ担当者は、情報セキュリティ管理者を補佐し、各所属における保有個人情報の管理に関する事務を担当する。

（情報システム管理者）

第８条　市に、情報システム管理者を１人置くこととし、デジタル政策課長を持って充てる。

２　情報システム管理者は、全庁的な情報システムにおける情報セキュリティについて管理する。

（監査責任者）

第９条　市に、監査責任者を１人置くこととし、人事・法制課長をもって充てる。

２　監査責任者は、保有個人情報の管理の状況について監査する任に当たる。

（保有個人情報の適切な管理のための委員会）

第１０条　総括情報セキュリティ責任者は、保有個人情報の管理に係る重要事項の決定又は連絡、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。

２　前項の委員会の構成員は、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を参加させるものとする。

## 第３章　教育研修

（教育研修）

第１１条　総括情報セキュリティ責任者は、事務担当者に対し、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実施する。

2　総括情報セキュリティ責任者は、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　総括情報セキュリティ責任者は、情報セキュリティ管理者及び情報セキュリティ担当者に対し、各所属の現場における保有個人情報の適切な管理のために必要な教育研修を定期的に実施する。

4　情報セキュリティ管理者は、当該所属の職員に対し、保有個人情報の適切な管理のために総括情報セキュリティ責任者が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

（職員の責務）

第１２条　事務担当者は、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情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報セキュリティ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。

2　職員は、保有個人情報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事務担当者が本規程等に違反している事実又は兆候を把握した場合は、直ちに情報セキュリティ管理者に報告しなければならない。

（厳正な対処）

第１３条　市は、保有個人情報の取扱いに関し、法に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。

## 第５章　保有個人情報の適切な取扱い

（アクセス制限）

第１４条　情報セキュリティ管理者は、保有個人情報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事務担当者に限定し、情報システム管理者に対してアクセス権限の設定を依頼する。

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してはならない。

３　情報セキュリティ管理者は、アクセス制限を事務担当者個人単位で管理し、保有個人情報取扱事務においてID及びICカードの共用をさせてはならない。

４　事務担当者は、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１５条　事務担当者は、業務上の目的以外の目的で、電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。）その他いかなる方法を用いても保有個人情報を複製してはならない。

２　事務担当者は、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、情報セキュリティ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（紙媒体を含む。）の外部への送付又は持出し

(4) 前３号に掲げるもののほか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

３　業務上の目的で複製した保有個人情報は、保有個人情報の原本とみなすものとし、その取扱いについては、この章及び次章の規定を適用する。

（誤りの訂正等）

第１６条　事務担当者は、保有個人情報の内容に誤り等を発見した場合には、遅滞なく情報セキュリティ管理者に報告し、その指示に従い、訂正等を行うものとする。

（媒体の管理等）

第１７条　事務担当者は、情報セキュリティ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（紙媒体を含む。）を定められた場所に施錠保管（鍵の管理については事務担当者が行う。）するとともに、必要があると認めるときは、耐火金庫等への保管を行う。

２　情報セキュリティ管理者は、事務担当者が、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、生体認証等をいう。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１８条　情報セキュリティ管理者は、事務担当者が保有個人情報を含む電磁的記録又は媒体の誤送信若しくは誤送付、誤交付又はウェブサイト等への誤掲載を防止するため、個別の事務又は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、複数の事務取扱者による確認、チェックリスト等の活用等の必要な措置を講ずる。

（廃棄等）

第１９条　事務担当者は、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及び紙媒体を含む。）が不要となった場合には、情報セキュリティ責任者の承認を得た上で、情報セキュリティ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保有個人情報の消去又は当該媒体の廃棄を行う。

２　事務担当者は、前項の規定による保有個人情報の消去又は当該媒体の廃棄の委託（２以上の段階にわたる委託を含む。）をするときは、必要に応じて消去若しくは廃棄に立ち会い、又は写真等を付した消去若しくは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又は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２０条　情報セキュリティ管理者は、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２１条　情報セキュリティ管理者は、保有個人情報が外国において取り扱われる場合にあっては、当該外国の個人情報の保護に関する制度等を把握したうえで､保有個人情報の安全のために必要かつ適切な措置を講じなければならない。

（機器及び電子媒体等の盗難等の防止）

第２２条　情報セキュリティ管理者は、保有個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。

２　事務担当者は、保有個人情報を取り扱う電子媒体及び書類等の庁舎内の移動等において、紛失、盗難等に留意する。

## 第６章　情報システム上における安全の確保等

（アクセス制御）

第２３条　情報セキュリティ管理者は、保有個人情報（情報システムで取り扱うものに限る。以下この章（第３６条を除く。）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　情報セキュリティ管理者は、情報システム管理者の指示に従って、パスワード等の管理が徹底されるよう事務担当者を指導監督するほか、パスワード等の読取防止等を行うために必要な設備等を設置する。

３　アクセス権限を有する事務担当者は、情報セキュリティ管理者の指示に従ってパスワード等を取り扱う。

４　アクセス権限を有する事務担当者は、パスワードの漏えい等が疑われる場合は、遅滞なくパスワードを変更する。

５　情報セキュリティ管理者は、業務上必要がなくなった場合は、遅滞なく事務担当者のアクセス権限を抹消するよう、情報システム管理者に依頼する。

６　情報セキュリティ管理者は、事務担当者のアクセス権限の付与状況をアクセス権限表等で管理し、人事異動又は所属内での担当変更等に即時に対応できるよう適時の見直しを行う。

（アクセス記録）

第２４条　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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２５条　情報セキュリティ管理者は、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恐れの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を行い、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２６条　情報セキュリティ管理者は、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等）

第２７条　情報セキュリティ管理者は、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、情報システム管理者に対して、保有個人情報を取り扱う基幹的なサーバ等をインターネット等の外部のネットワークに接続しないほか必要に応じてファイアウォールの設定による経路制御を行う等の措置を依頼する。

（不正プログラムによる漏えい等の防止）

第２８条　情報セキュリティ管理者は、不正プログラムによる保有個人情報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。

（情報システムにおける保有個人情報の処理）

第２９条　事務担当者は、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。

２　情報セキュリティ管理者は、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３０条　情報セキュリティ管理者は、保有個人情報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ずるものとし、事務担当者はこれを踏まえ、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。

２　事務担当者は、保有個人情報を機器又は電子媒体等に保存する必要がある場合は、原則として、暗号化又はパスワードにより秘匿する。

３　事務担当者は、車両等により保有個人情報を運搬する場合には、当該保有個人情報を暗号化又はパスワードの設定を行う。

（記録機能を有する機器及び媒体の接続制限）

第３１条　情報システム管理者は、保有個人情報の秘匿性等その内容に応じて、保有個人情報の情報漏えい等の防止のため、スマートフォン、デジタルカメラ、ICレコーダ並びにUSBメモリ等の記録機能を有する機器及び媒体について、保有個人情報を処理する端末等への接続を制限（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３２条　情報セキュリティ管理者は、保有個人情報の処理を行う端末を限定し、情報システム管理者に対して、端末へのソフトウェアの導入、端末の認証等の設定を依頼する。

（端末の盗難防止等）

第３３条　情報セキュリティ管理者は、前条の規定により限定された保有個人情報を処理する端末（以下「限定処理端末」という。）の盗難又は紛失の防止のための対策を講じる。

（端末の外部持ち出し等）

第３４条　事務担当者は、情報セキュリティ管理者が必要があると認めるときを除き、限定処理端末を外部へ持ち出し、又は限定処理端末以外の端末を外部から持ち込んではならない。

（第三者の閲覧防止）

第３５条　事務担当者は、限定処理端末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い、又は離席時に端末をロックする。

２　情報セキュリティ管理者は、限定処理端末の画面が第三者に窃視されることがないよう、覗きこみを防止するための対策を講じる。

（入力情報の照合等）

第３６条　事務担当者は、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３７条　情報セキュリティ管理者は、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。

（情報システム開発、導入、保守、廃棄等）

第３８条　情報セキュリティ管理者及び情報システム管理者は、保有個人情報に係る情報システムの調達、開発、導入、保守、廃棄等にあたっては、越前市情報セキュリティ対策基準（令和５年４月１日施行）に従う。

２　情報セキュリティ管理者は、保有個人情報に係る情報システムの開発、導入、保守、廃棄等の作業を担当する職員が保有個人情報の閲覧、複製その他の操作を行う場合には、当該担当者を事務担当者として指定し、行うことのできる操作の範囲及び操作することのできる保有個人情報の範囲を限定し、漏えい、滅失、毀損等の事故がないよう指導し、及び監督する。この場合において、指導及び監督に際しては、情報システム管理者に必要かつ十分な協力をするよう依頼する。

３　情報セキュリティ管理者は、保有個人情報に係る情報システムの開発、導入、保守、廃棄等の作業を委託する事業者が保有個人情報の閲覧、複製その他の操作を行う場合には、当該事業者を保有個人情報取扱事務の委託先とし、第９章を適用して、当該委託先を監督する。この場合において、情報システム管理者に必要かつ十分な協力をするよう依頼する。

（情報システム設計書等の管理）

第３９条　情報セキュリティ管理者は、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、定められた場所で施錠保管を行い、複製を制限し、廃棄する場合には復元不能な方法で廃棄する。

## 第７章　サーバ室等の安全管理

（入退管理）

第４０条　情報システム管理者は、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「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。保有個人情報を記録する媒体を保管するための施設（以下「保管施設」という。）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　情報システム管理者は、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　情報システム管理者は、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４１条　情報システム管理者は、外部からの不正な侵入に備え、サーバ室等に施錠装置、警報装置及び監視設備の設置等の措置を講ずる。

２　情報システム管理者は、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　保有個人情報の提供

（保有個人情報の提供）

第４２条　情報セキュリティ管理者は、法第６９条第２項第３号及び第４号の規

定に基づき市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（電磁的記録を含む。）を取り交わす。

２　情報セキュリティ管理者は、法第６９条第２項第３号及び第４号の規定に基づき市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　情報セキュリティ管理者は、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ずる。

## 第９章　保有個人情報の取扱いの委託

（業務の委託等）

第４３条　情報セキュリティ管理者は、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。

２　職員は、委託先を選定するときは、諸条件を調査及び検討のうえ、その結果を情報セキュリティ管理者に届け出て、承認を得る。

３　情報セキュリティ管理者は、業務の委託契約書には、次に掲げる事項を明記するものとし、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により確認する。

(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。）である場合を含む。第１項及び第６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) 委託契約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

4　情報セキュリティ管理者は、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でなければならない。

5　情報セキュリティ管理者は、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、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。

6　情報セキュリティ管理者は、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自らが前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。

7　情報セキュリティ管理者は、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。

8　情報セキュリティ管理者は、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１０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４４条　情報セキュリティ管理者及び情報システム管理者は、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年法律第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１１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４５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(以下「事案」という。）又は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情報セキュリティ管理者に報告する。

２　情報セキュリティ管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセス又は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は直ちに行う（職員に行わせることを含む。）ものとする。

３　情報セキュリティ管理者は、事案の発生した経緯、被害状況等を調査し、総括情報セキュリティ責任者、情報セキュリティ責任者及びネットワーク管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに最高情報セキュリティ責任者及び総括情報セキュリティ責任者に当該事案の内容等について報告する。

４　統括セキュリティ責任者は、前項による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。

５　情報セキュリティ管理者は、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部局等に再発防止措置を共有する。

６　最高情報セキュリティ責任者は、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（法第１３０条第１項に規定する個

人情報保護委員会をいう。以下この項及び次条において「委員会」という。）への報告及び第６８条第２項の規定による本人への通知を要するときは、前各項と並行して、速やかに所定の手続を行うとともに、委員会による事案の把握等に協力する。

（公表等）

第４６条　最高情報セキュリティ責任者は、法第６８条第１項の規定による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。

２　最高情報セキュリティ責任者は、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、速やかに委員会へ情報提供を行う。

## 第１２章　監査及び点検の実施

（監査）

第４７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１１章までに規定する措置の状況を含む当該行政機関等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、その結果を総括情報セキュリティ責任者に報告する。

（点検）

第４８条　情報セキュリティ管理者は、各所属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、その結果を総括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム管理者に報告する。

（評価及び見直し）

第４９条　総括情報セキュリティ責任者、情報セキュリティ責任者及び情報セキュリティ管理者は、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。

附　則

この規程は、令和５年４月１日から施行する。