個人情報の安全管理に関する
ガ　イ　ド　ラ　イ　ン

令和７年６月

刈　　谷　　市

目　　次

第１章　基本事項・・・・・・・・・・・・・・・・・・・・・・・・・・・・・１
　１　取扱管理要領及び本ガイドラインの適用範囲
　２　罰則

第２章　管理体制・・・・・・・・・・・・・・・・・・・・・・・・・・・・・２
　１　管理体制の全体像
　２　責務・役割等

第３章　安全管理措置・・・・・・・・・・・・・・・・・・・・・・・・・・・５
　１　市の機関が講ずべき安全管理措置
　２　安全管理のために必要かつ適正な措置

第４章　個人情報を取り扱う事務の委託・・・・・・・・・・・・・・・・・・９
　１　委託等先における安全管理措置
　２　委託先の選定
　３　契約
　４　委託先の監督
　５　再委託等

第５章　漏えい等の報告及び通知・・・・・・・・・・・・・・・・・・・・・１１
　１　問題発生時の対応の基本的な流れ
　２　委託先・再委託先で漏えい等が発生した場合

第６章　教育研修・・・・・・・・・・・・・・・・・・・・・・・・・・・・１５
　１　教育研修の実施根拠
　２　実施内容等について

第７章　監査・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・１６
　１　教育研修の実施根拠
　２　実施内容等について

第１章　基本事項

１　取扱管理要領及び本ガイドラインの適用範囲

（取扱管理要領第１条、第３４条）

（１）市の機関（市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会及び固定資産評価審査委員会）

（２）委託先・再委託先（再々委託以降を含む。）

個人情報を取り扱う事務の全部又は一部を委託する場合は、市の機関が果たすべき安全管理措置と同等の措置を講じられるよう必要かつ適切な監督が必要となる。

（３）指定管理者

公の施設（地方自治法第２４４条第１項に規定する公の施設をいう。）の管理の業務を行う場合における個人情報の取扱いについて市の機関が果たすべき安全管理措置と同等の措置を講じられるよう必要かつ適切な監督が必要となる。

２　罰則

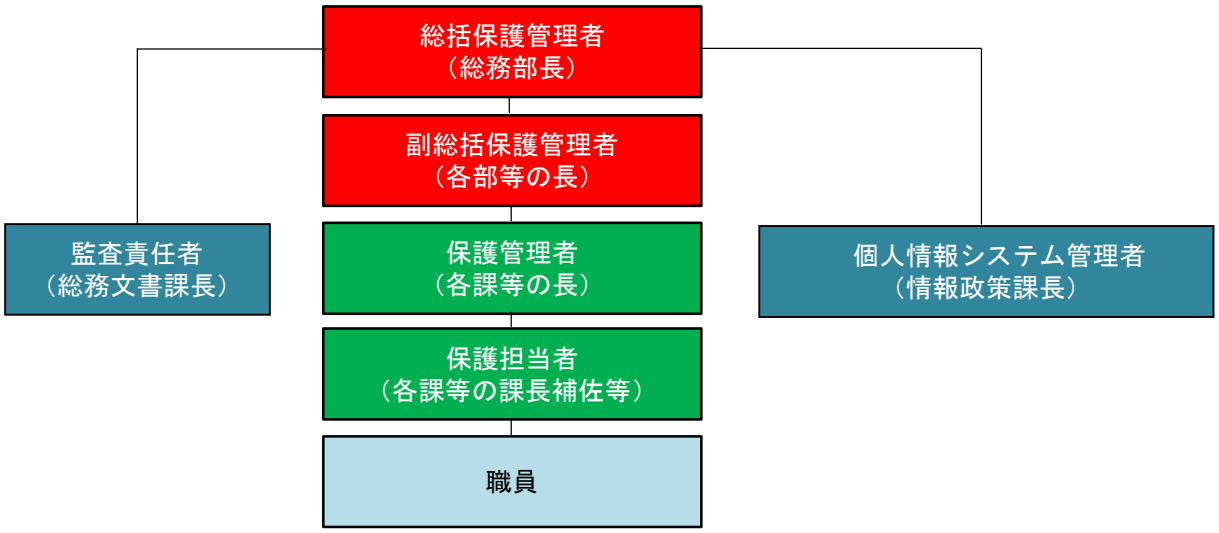
個人情報保護法では、個人情報の取扱いを厳しく制限しており、罰則についても関連する他の法律（地方公務員法等）に比べ重い罰則が科される。（個人情報保護法第１７６条から第１８５条まで）

	行　為	対 象 者	罰　則
１	個人情報の取扱いに従事し、又は従事していた者が正当な理由がないのに、個人の秘密に属する事項が記録された個人情報ファイル（加工したものを含む。）を提供したとき 【第１７６条】	職員（特別職を含む。）、委託先・再委託先（再々委託以降も含む。）、派遣労働者	２年以下の拘禁刑又は１００万円以下の罰金
２	個人情報の取扱いに従事し、又は従事していた者がその業務に関して知り得た保有個人情報を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したとき 【第１８０条】	職員（特別職を含む。）、委託先・再委託先（再々委託以降も含む。）、派遣労働者	１年以下の拘禁刑又は５０万円以下の罰金
３	行政機関等の職員がその職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集したとき 【第１８１条】	職員（特別職を含む。）	１年以下の拘禁刑又は５０万円以下の罰金

第２章　管理体制

１　管理体制の全体像

本市における個人情報の適正な取扱いを確保するため、管理体制を下記のとおり整備する。



２　責務・役割等

（１）総括保護管理者（取扱管理要領第２条、第１０条）

総務部長とし、その役割は次のとおり。

ア　本市が保有する個人情報の管理に関する事務の総括

イ　管理体制の整備

ウ　職員に対する啓発その他個人情報の適切な管理を推進するため必要な研修の実施

エ　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する情報システムの管理・運用及びセキュリティ対策に関する教育研修の実施

（２）副総括保護管理者（取扱管理要領第３条、第３６条）

各部等の長とし、その役割は次のとおり。

ア　総括保護管理者（総務部長）の補佐

イ　保有個人情報の漏えい等の事案の発生又はその兆候その他の安全管理上の問題（以下「問題」という。）が発生した場合における保護管理者からの報告事項の市の機関の長及び総括保護管理者（総務部長）への報告

（３）保護管理者、保護担当者（取扱管理要領第４条、第５条、第１１条～第１６条、第２２条、第２

５条、第２６条、第２９条、第３０条、第３３条～第３５条、第３７条、第３８条、第４１条）

保護管理者は個人情報を取り扱う各課等の長、保護担当者は個人情報を取り扱う各課等の課長補佐等とし、その役割は次のとおり。

ア　各課等において保有する個人情報にアクセスする権限を有する職員及びその権限の内容の指定

イ　当該所属の職員に対する個人情報の取扱いに関する教育研修への参加機会の付与

ウ　保有個人情報の適正な管理（提供、保管、訂正、廃棄等）

エ　物理的安全管理措置の実施及び外的環境の把握

オ　情報システム設計書等の適正な管理（保管、複製、廃棄等）

カ　個人情報を取り扱う業務を委託する場合における委託契約の締結、委託先の監督等

キ　問題が発生した場合における被害の拡大防止等に必要な措置の実施及び当該問題が不正アクセス等による場合における個人情報システム管理者への報告

ク　問題が発生した経緯、被害状況等を調査及び原因の究明並びに総括保護管理者（総務部長）及び副総括保護管理者（各部等長）への報告

ケ　問題が発生した原因を分析及び再発防止措置の実施

コ　問題が発生した場合における事実関係及び再発防止策の公表

サ　各課等において保有する個人情報の管理に関する点検及び総括保護管理者（総務部長）への報告

（４）個人情報システム管理者（取扱管理要領第６条、第１４条、第１７条～第２１条、第２４条、第２９条～第３２条、第４１条）

情報政策課長とし、その役割は次のとおり。

ア　保護管理者からの依頼に基づく、保有個人情報を取り扱う端末、電磁的記録媒体等に記録された保有個人情報の削除等

イ　情報システムで取り扱う保有個人情報のアクセス制御、アクセス状況の記録等及びアクセス記録の改ざん等の防止

ウ　暗号化、管理者権限の最小化その他不正操作等防止のための措置の実施

エ　外部からの不正アクセス防止

オ　不正プログラムによる漏えい等防止

カ　記録機能を有する機器等の端末等への接続制限

キ　バックアップの作成及び情報の分散保管

ク　情報システム設計書等の適正な管理（保管、複製、廃棄等）

ケ　保有個人情報を取り扱う基幹サーバ等の管理区域の管理及び当該管理区域に立ち入る権限を有する者の指定

コ　情報システムで取り扱う保有個人情報の管理に関する点検及び総括保護管理者（総務部長）への報告

（５）監査責任者（取扱管理要領第７条、第３８条）

総務文書課長とし、その役割は次のとおり。

ア　保有個人情報の管理状況に係る定期又は随時の監査の実施

イ　監査結果の総括保護管理者（総務部長）へ報告

第３章　安全管理措置

１　市の機関が講ずべき安全管理措置

市の機関は、個人情報保護法第６６条第１項の規定により、保有個人情報の漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の保有個人情報の安全管理のために必要な措置を講じなければならない。求められる安全管理措置の内容は、保有個人情報の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況（保有個人情報の量及び性質を含む。）、保有個人情報を記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすること。

２　安全管理のために必要かつ適正な措置

（１）組織的安全管理措置

ア　個人情報の取扱いに係る規律に従った運用（取扱管理要領第１１条）

保有個人情報の秘匿性等その内容に応じて、保有個人情報にアクセスする権限を有する職員の範囲及び権限を業務上必要最小限の範囲に限定し、保護管理者（各課等長）は、随時に業務上必要のない権限が付与されていないことを確認する。

イ　個人情報の取扱状況を確認する手段の整備（取扱管理要領第１５条、第１８条）

各課等において保有する個人情報の総量を把握し、適切に管理するため、個人情報が記載された簿冊については、記録簿等を整備し、保管等の状況を記録するなどの措置を講じる。

その措置の例として、参考様式１「個人情報記録文書等管理記録簿」を参照して各課において保有する個人情報が記録された簿冊の量、その利用する事務、保管場所等を記録した上で、**電子媒体で記録しているものは当該ファイルのファイル名に「(個情)」の表記**を、**紙媒体で記録されているものは背表紙にテプラ等で「個人情報記録文書」の表記**をすることで、個人情報の誤廃棄、必要以上の閲覧を防止する。

ウ　漏えい等の事案に対応する体制の整備（取扱管理要領第３６条）

保有個人情報の漏えい等の事案の発生又はその兆候を把握した場合は、**直ちに当該保有個人情報を管理する保護責任者（各課等長）に報告するとともに、保護責任者（各課等長）の指示のもと被害の拡大を防止する措置を講じた上で、総務文書課長に問題の内容等を報告する。**

なお、外部からの不正アクセスや不正プログラムの感染によるものである場合は、上記の対応に加え、直ちに個人情報システム管理者（情報政策課長）に報告する。

総括保護管理者（総務部長）等及び個人情報保護委員会への報告等については、後述する「第５章　漏えい等の報告及び通知」を参照すること。

エ　個人情報の取扱状況の把握及び安全管理措置の見直し（取扱管理要領第４０条、第４１条）

保護管理者（各課等長）は、当該各課等における保有個人情報の保管方法等について、定期に点検を行う。また、監査責任者（総務文書課長）は、定期的に監査を行う。

監査の実施内容等については、後述する「第７章　監査」を参照すること。

（２）人的安全管理措置

ア　職員の責務（取扱管理要領第９条）

保有個人情報を取り扱う職員は、個人情報保護法の趣旨にのっとり、関連する法令及び規定等の定め並びに保護管理者（各課等長）及び保護担当者（各課等の課長補佐等）の指示に従い、保有個人情報を取り扱うこと。

イ　職員の教育（取扱管理要領第１０条）

職員に対して個人情報の保護に関する研修等を実施する。

研修の内容等については、後述する「第６章　教育研修」を参照すること。

（３）物理的安全管理措置

ア　書面及び電子媒体等を持ち運ぶ場合の漏えい等の防止（取扱管理要領第１１条、第１３条）

保有個人情報が記録されている書面及び電子媒体等を外部に送付し、又は持ち出す場合は、パスワードの設定等アクセス制御のための必要な措置を講じる。

その措置の例として、参考様式２「個人情報記録文書等持出記録簿」を参照して外部送付又は持出しの状況を管理する。

イ　書面及び電子媒体等の盗難等の防止（取扱管理要領第１３条、第２６条）

保有個人情報が記録されている書面及び電子媒体等は、定められた施錠可能な場所に保管する。また、情報システムの画面のハードコピー等の保有個人情報が記録された廃棄文書については、保有個人情報を取り扱うことができる職員以外の者が容易に閲覧等できない場所に集約し、廃棄を実施するまでの間、施錠可能な場所に

保管する。

ウ　個人情報の削除及び機器、電子媒体等の廃棄（取扱管理要領第１４条）

不要となった保有個人情報が記録された書面及び電子媒体等は、当該書面及び電子媒体等の保存期間満了後、速やかに廃棄する。

エ　個人情報を取り扱う区域の管理（取扱管理要領第２７条）

保有個人情報を取り扱うことができる職員以外の者が容易に閲覧等できないよう情報システムからのログオフの徹底、間仕切り等の設置、のぞき込みの防止等の必要な措置を行うこと。

（４）技術的安全管理措置

ア　アクセス者の識別と認証（取扱管理要領第１７条）

保有個人情報にアクセスする権限を有する職員以外の者のアクセスを制御するため、認証機能を設定し、パスワード等の読取防止等のため必要な措置を講ずる。

イ　外部からの不正アクセス等の防止（取扱管理要領第２０条）

保有個人情報を取り扱う情報システムへの不正アクセスを防止するため、ファイアウォール等による外部ネットワークとの通信制限、当該情報システムへのセキュリティ対策ソフトウェア等の導入等の必要な措置を講ずる。

ウ　情報システムの使用に伴う漏えい等の防止（取扱管理要領第２１条～第２３条）

保有個人情報の秘匿性等その内容に応じて、滅失又は毀損の防止のためバックアップの作成、分散保管等を行い、不正に保有個人情報を入手した者が容易に復元できないよう、当該保有個人情報が記録されているデータベース等の暗号化を適切に行う等必要な措置を講ずる。

エ　アクセス制御（取扱管理要領第２５条）

保有個人情報の秘匿性等その内容に応じて、業務上必要最小限の範囲で取り扱うことができる情報システムの端末及びデータベースを限定する。

（５）外的環境の把握（取扱管理要領第１６条）

保有個人情報が外国において取り扱われる場合（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、当該事業者が外国に所在する場合及び保有個人情報が保存されるサーバが外国に所在する場合を含む。）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上で、保有個人情報の安全管理のために必要な措置を講じなければならない。

なお、外国の個人情報の保護に関する制度等は、個人情報保護委員会のＨＰ（https://www.ppc.go.jp/enforcement/infoprovision/laws/）を参照すること。

第４章　個人情報を取り扱う事務の委託

１　委託等先における安全管理措置（取扱管理要領第３４条）

個人情報を取り扱う事務の全部又は一部を委託する場合は、その委託先においても市の機関が果たすべき安全管理措置と同等の措置が講じられなければならない。そのため、委託先の定期的な監査等必要かつ適切な監督を行う必要がある。

なお、委託する保有個人情報の取扱いに係る事務について委託先が再委託等（再々委託以降を含む。）をする場合も同様の措置が必要となる。

２　委託先の選定

委託先の選定に当たっては、その候補となる事業者における設備、技術水準、従業者に対する監督、教育の状況等を契約前に書面又は実地調査により確認することとする。書面による確認については、基本的に参考様式３「個人情報に係る安全管理措置に関する報告書」を用いることとするが、当該委託事務の性質に合わせて確認項目を精査すること。

３　契約

業務委託契約の締結に当たっては、契約書に次の内容を規定する。契約書を作成する際には、基本的に参考様式４「個人情報の取扱いに係る特記事項」を用いること。

（１）個人情報に関する秘密保持

（２）個人情報の利用目的以外の目的のための利用の禁止

（３）再委託等（再委託等先が子会社である場合を含む。）に係る条件

（４）個人情報の複製等の制限

（５）個人情報の安全管理措置

（６）個人情報の漏えい等の事案の発生時における対応

（７）委託終了時における個人情報の返却又は廃棄

（８）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

（９）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（再委託等先の監査等を含む。）

４　委託先の監督

委託期間においては、契約内容に基づき安全管理措置が講じられるよう適切な監督を行う必要がある。

個人情報の取扱状況については、月に１回程度書面により報告させ、把握すること。書面による報告については、基本的に参考様式５「個人情報に関する契約内容の遵守状況に係る報告書」を用いること。

適切な安全管理措置の実施状況については、少なくとも年に１回以上、書面又は実地調査により確認すること。安全管理措置の実施状況の確認については、基本的に参考様式６「個人情報管理状況監査チェックシート」を用いること。

なお、適切な安全管理措置の実施状況の確認については、指定管理者に対しても同様に行うこと。

５　再委託等

委託先が個人情報を取り扱う事務の全部又は一部を再委託しようとする場合も同様に、再委託先の候補となる事業者における設備、技術水準、従業者に対する監督、教育の状況等を書面又は実地調査により確認した上で適当と認めた場合に限り承認すること。また、再委託先における個人情報の取扱いについては、保護管理者（各課等長）が監督し、又は委託先に監督させ、その結果を書面により報告をさせること。

なお、再々委託以降についても再委託と同様とする。

第５章　漏えい等の報告及び通知

１　問題発生時の対応の基本的な流れ（取扱管理要領第３６条）

（１）市の機関内部における報告及び被害の拡大防止

問題を把握した場合は、その事実を知った職員は、直ちに当該保有個人情報を管理する保護管理者（各課等長）に報告するとともに、保護管理者（各課等長）の指示のもと被害の拡大を防止する措置を講じた上で、総務文書課長に問題の内容等を報告する。

なお、当該問題が外部からの不正アクセスや不正プログラムの感染によるものである場合は、直ちにパソコンのＬＡＮケーブルを外す等被害拡大防止のための措置を講じ、個人情報システム管理者（情報政策課長）に報告を行う。

（２）事実関係の調査及び原因の究明（副総括保護管理者、総括保護管理者及び市の機関の長への報告）

別記様式「個人情報の漏えい等報告書（内部用）」に記載している事項を参考に、次の場合の区分に応じ、必要事項を報告する。

ア　個人の権利利益を害するおそれが大きい問題（要配慮個人情報若しくは財産被害が生じるおそれのある保有個人情報又は本人の数が１００人を超える保有個人情報が漏えい等した場合、当該問題が不正な目的による場合等個人情報保護委員会規則第４３条各号に該当するものをいう。）に該当しない場合

保護管理者（各課等長）は、発生の経緯、被害状況等の事実関係を調査し、その原因の究明を行い、副総括保護管理者（各部等長）に報告する。また、副総括保護管理者（各部等長）は、当該問題の内容、経緯、被害状況等を総括保護管理者（総務部長）及び市の機関の長に報告する。

イ　個人の権利利益を害するおそれが大きい問題に該当する場合

アと同様の手順により、当該問題の発生について報告を行う。この場合において、副総括保護管理者（各部等長）に報告するときは、併せて総務文書課担当者にも報告を行うこと。

なお、漏えい等した保有個人情報に特定個人情報が含まれる場合は、特定個人情報の漏えい等への対応（個人番号の取扱いに関するガイドライン第８章を参照）が別に必要となる。また、上記対応とは別に情報漏えい発生時の事案報告として、「危機管理マ

ニュアル（企画財政部情報政策課作成）」の連絡体制に従った報告が必要となる。

（３）再発防止策の検討及び実施

保護管理者（各課等長）、副総括保護管理者（各部等長）及び総括保護管理者（総務部長）は、問題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。

（４）個人情報保護委員会への報告

個人の権利利益を害するおそれが大きい問題に該当する場合は、個人情報保護委員会への報告（「速報」（５日以内）及び「確報」（３０日以内））が必要となる。

なお、個人情報保護委員会への報告は、報告専用ページの入力フォーム（https://roueihoukoku.ppc.go.jp/incident/?top=r2.gyousei）から、別記様式「個人情報の漏えい等報告書（内部用）」により報告された内容を基に総務文書課が行う。

（５）本人への通知等

保護管理者（各課等長）は、問題の内容等に応じ、二次被害の防止、類似の問題の発生回避等の観点から、問題の概要、再発防止策等について速やかに本人へ通知し、又は本人が容易に知り得る状態にする。

なお、当該問題が個人の権利利益を害するおそれが大きい問題に該当する場合は、本人への通知が困難な場合、代替措置（問い合わせ窓口の設置、事案の公表など）を講ずる場合を除き本人への通知を行う。

（６）事実関係、再発防止策等の公表

保護管理者（各課等長）は、問題の内容等に応じ、二次被害の防止、類似の問題の発生等の回避の観点から、事実関係、再発防止策等について速やかに公表する。

別記様式

個人情報の漏えい等報告書（内部用）

年　　月　　日

問題発生部署			
副総括保護管理者名		保護管理者名	

次のとおり報告します。

問題の類型	【個人の権利利益を害するおそれが大きい問題の該当の有無】 □　該当する　　□　該当しない
	【個人の権利利益を害するおそれが大きい問題の類型】※複数選択可 □　要配慮個人情報が含まれる保有個人情報の漏えい等が起こった。 □　不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が起こった。 □　不正の目的を持って行われたおそれがある保有個人情報の漏えい等が起こった。 □　保有個人情報に係る本人の数が１０１人以上である。
問題の概要	【発覚日】　　年　月　日 【発生原因】 □紛失・盗難　　□誤送信・誤公開　　□内部犯行 □不正プログラム　　□不正アクセス □その他（　　） 【概要（問題が発生した原因を含む。）】
漏えい等した保有個人情報の内容	
漏えい等した保有個人情報の本人の数	人 ※発覚した時点の把握した概数を記載
想定される二次被害	□　なし □　あり　※下記にその内容を記載 （　　）
本人への対応	□　実施済み【実施日：　　年　月　日】 □　未実施
公表の実施状況	□　公表済み又は予定【実施（予定）日：　　年　月　日】 □　公表しない
再発防止のための措置	

２　委託先・再委託先で漏えい等が発生した場合

委託先、再委託先等で漏えい等の事案が発生した場合も、上記と同様の流れで委託元である市の機関が状況を取りまとめ、報告及び公表を行わなければならない。

第６章　教育研修

１　教育研修の実施根拠

個人情報保護委員会発出の「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」において、個人情報保護法第６６条第１項の規定に基づく安全管理措置の一環として職員に対する教育研修の実施が定められている。本市においては、取扱管理要領第１０条において教育研修の実施を定めている。

２　実施内容等について

総括保護管理者（総務部長）は、毎年度当初に当該年度の研修実施計画を定め、それに基づき研修を実施する。研修の内容や区分については、概ね以下のとおりとするが、毎年度その内容及び頻度について見直しを行い、必要に応じて変更を行うこととする。

内　　容	目　的	対　象　者
１　個人情報の適正な取扱いのための研修	制度の周知徹底	・全正規職員 ・職務において個人情報を取り扱う会計年度任用職員
２　課等における個人情報の適正な管理のための研修	保護管理者及び保護担当者への注意喚起	・保護管理者 ・保護担当者
３　個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項	パソコンを使用する職員への注意喚起	・全正規職員 ・ＬＧＷＡＮ接続系端末を利用する会計年度任用職員
４　個人情報を取り扱う情報システムの管理に関する事項	情報システムの適切な管理・運用、セキュリティ対策に係るスキル向上	・情報政策課情報システム係に属する職員

※　年度途中に対象者となった職員（新規採用・異動・産休育休から復帰）に対しては、全体の実施時期にかかわらず、個別に実施することとする。

第７章　監査

１　教育研修の実施根拠

個人情報保護委員会発出の「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」において、個人情報保護法第６６条第１項の規定に基づく安全管理措置の一環として監査の実施が定められている。本市においては、取扱管理要領第４０の規定により、監査責任者（総務文書課長）が各課等における保有個人情報の管理状況について、定期に又は随時に監査を行い、その結果を総括保護管理者（総務部長）に報告することとしている。

２　実施内容等について

（１）実施目的

保有個人情報の適切な管理を検証し、安全管理措置の有効性及び現行の事務方法における残存リスクを把握するとともに、問題点の改善や事務方法の見直しを行うため。

（２）内容

安全管理措置の取組状況について

（３）実施方法

各課執務室における総務文書課職員による聴取及び実地確認

（４）対象事務

保有個人情報を取り扱う事務

（５）実施頻度

毎年１回、保有個人情報を取り扱う課等の中から５課程度抽出して課等単位で実施（各課等の監査対象頻度が概ね５年に１回になるように設定）

（６）実施機関

原則として、毎年度上半期に実施する（対象課宛てに個別に通知）。

（７）監査結果の取扱い

ア　当該年度実施分を集約の上、総括保護管理者（総務部長）に書面報告

イ　庁内の情報共有として、職員ポータルサイトに監査結果の概要を掲載

（８）指摘事項に対する対応報告

監査において指摘事項があった課等の保護管理者（各課等長）は、当該指摘事項に

係る対応状況を監査責任者（総務文書課長）に報告する。

（９）監査結果に基づく勧告

同一事項に関する指摘内容が繰り返され改善に向けての対策がなされる兆候がない場合は、当該課等宛てに文書勧告等を行う。

参照様式１

個人情報記録文書等管理記録簿

	保有個人情報利用事務	簿冊名	作成年度	保有期間	保管場所	担当係名	廃棄年月日
1							
2							
3							
4							
5							
6							
7							
8							
9							
１０							
１１							
１２							
１３							
１４							
１５							
１６							
１７							

参照様式２

個人情報記録文書等持出記録簿

	持出年月日	記録媒体	文書又は記録媒体の名称	個人の数	持出先	持出方法	持出事由	担当者名
１		紙 ・ 電子						
２		紙 ・ 電子						
３		紙 ・ 電子						
４		紙 ・ 電子						
５		紙 ・ 電子						
６		紙 ・ 電子						
７		紙 ・ 電子						
８		紙 ・ 電子						
９		紙 ・ 電子						
１０		紙 ・ 電子						
１１		紙 ・ 電子						
１２		紙 ・ 電子						
１３		紙 ・ 電子						
１４		紙 ・ 電子						
１５		紙 ・ 電子						
１６		紙 ・ 電子						
１７		紙 ・ 電子						

参考様式３

個人情報に係る安全管理措置に関する報告書

年　　月　　日

刈谷市長

受託者　所　在　地

名　　称

代表者氏名

業務の受注に当たり、次のとおり報告します。

１　設備及び技術水準

２　従業者に対する監督・教育の状況

３　経営環境・組織体制

４　漏えい等事案に対応する体制等の整備状況

参考様式４

個人情報の取扱いに係る特記事項

（秘密保持）

第１条　受注者は、本業務の履行のために知り得た個人情報に関する秘密を漏らし、又は盗用してはならない。本業務の委託終了後においても同様とする。

（事業所内からの個人情報の持出しの禁止）

第２条　受注者は、発注者の書面による承諾なく、個人情報が記録された書類、機器等を発注者の事業所から持ち出してはならない。

２　受注者は、本業務の履行上、やむを得ず、発注者の承諾を得て、発注者の事業所から個人情報が記録された書類、機器等を持ち出す場合は、その日時、持出先及び実施した者の氏名を記録し、保存しなければならない。

（目的外利用の禁止）

第３条　受注者は、本業務の履行のために知り得た個人情報を、本業務の履行以外の目的で使用してはならない。

（再委託等に係る条件）

第４条　受注者は、個人情報を取り扱う業務の全部又は一部を第三者に再委託等しようとする場合（再委託等先が受注者の子会社である場合を含む。）は、あらかじめ書面により発注者に申請し、承諾を得なければならない。

２　受注者は、個人情報を取り扱う業務の全部又は一部を第三者に再委託等する場合は、再委託等先においても本特記事項に基づく個人情報の取扱いが遵守されるよう、毎月、取扱状況を書面又は実地調査により確認し、発注者にその結果を報告しなければならない。

（複製等の制限）

第５条　受注者は、発注者の同意又は指示がある場合を除き、業務を処理するために発注者から提供された個人情報を複製し、又は複写してはならない。

（安全管理措置）

第６条　受注者は、個人情報の漏えい、滅失、毀損（以下「漏えい等」という。）の防止その他個人情報の安全管理のため必要な措置を講じなければならない。

（個人情報の管理）

第７条　受注者は、本業務の履行のために知り得た個人情報が記録された書面、機器等を施錠可能な場所に保管しなければならない。

２　受注者は、本業務の履行のために知り得た個人情報の管理状況について台帳等を整備して記録しなければならない。

（漏えい等事案の発生時における受注者の責任）

第８条　受注者は、漏えい等の事案の発生又はその兆候その他の安全確保上で問題となる事実を把握した場合は、直ちに発注者に報告し、発注者による事態の把握に協力しなければならない。

（委託終了時における個人情報の返却又は廃棄）

第９条　受注者は、発注者から要求があった場合又は本業務の履行を完了した場合は、遅滞なく個人情報が記録された書面、機器等を返却し、又は廃棄しなければならない。

（個人情報を取り扱う役員及び従業員の明確化）

第１０条　受注者は、本業務において個人情報を取り扱う役員及び従業員を、書面により発注者に報告しなければならない。

（従業者に対する監督及び教育の実施）

第１１条　受注者は、前条の役員及び従業員に対し、本特記事項の内容を遵守させるとともに、個人情報の適正な取扱いのため必要な教育を行わなければならない。

（法令等違反時の契約解除及び損害賠償責任）

第１２条　発注者は、受注者が法令等に違反した場合又は本特記事項に基づく個人情報の取扱いを履行しない場合は、本業務に係る契約を解除することができる。

２　受注者は、法令等に違反し、又は本特記事項に基づく個人情報の取扱いを履行しないこ

とにより発注者に損害を与えた場合は、両者協議の上、損害額等について賠償責任を負うものとする。

（個人情報に関する契約内容の遵守状況についての報告）

第１３条　受注者は、個人情報に関する本特記事項の遵守状況について、毎月、書面により発注者に報告しなければならない。

（個人情報の取扱いに関する実地の調査）

第１４条　発注者は、本業務の適正な執行のため、受注者及び再委託等先の事業所その他の個人情報を取り扱う実地を、年１回以上、調査するものとし、本業務の履行に係る指示を行うことができる。

２　受注者は、前項の規定による指示があった場合は、その指示に従い、対応状況について発注者に報告しなければならない。

参考様式５

個人情報に関する契約内容の遵守状況に係る報告書

年　　月　　日

刈谷市長

受託者　名　　称

業務担当責任者氏名

年　　月の個人情報の取扱状況について、次のとおり報告します。

１　個人情報の取扱状況

業務実施日	業　　務　　内　　容
月　　日	
月　　日	
月　　日	

２　契約内容の遵守状況

項目	遵守状況	（問題等ありの場合）対応等の状況
秘密保持	□問題なし □問題あり	
持出しの禁止	□持出なし □持出あり	
目的外利用の禁止	□問題なし □問題あり	
複製等の制限	□複製なし □複製あり	
再委託等の状況	□変更なし □変更あり	
情報漏えい等事案の発生	□問題なし □問題あり	
情報の返却又は廃棄	□問題なし □問題あり	
従業者の明確化	□変更なし □変更あり	
監督及び教育	□問題なし □問題あり	
実地調査の実施	□要請なし □要請あり	

参考様式６

個人情報管理状況監査チェックシート

事業者名

業務名

番号	大分類	小分類	確認項目	達成度（該当に○）			特記事項
				【基準点】概ね達成できている	一部が達成できていない	ほとんど達成できていない	※その具体的内容をご記入ください。達成度が基準点未満の場合は、改善計画等を記入してください。
1	安全管理措置 ※個人情報の取扱状況	個人情報の管理状況確認	①この業務の履行のため知り得た個人情報の秘密保持、目的外利用の禁止の措置が適切になされている。				
			②個人情報が記録された書類、機器等を外部へ持ち出す際のマニュアル、事務フロー等が整備されている。				
2	安全管理措置 ※個人情報の範囲明確化	保有している個人情報確認	①この業務の履行のため知り得た個人情報の範囲が明確になっている。				
			②この業務の履行のため知り得た個人情報の取扱件数を把握している。				
3	安全管理措置 ※取扱担当者の明確化	個人情報を取り扱う者の範囲確認	①この業務の履行のため知り得た個人情報を取り扱う役員・従業員を書面等により明確になっている。				
4	安全管理措置 ※監督及び教育の実施	監督及び教育の実施状況確認	①この業務の履行のため知り得た個人情報の管理・取扱状況について適切に監督を行っている。				
			②この業務の履行のため知り得た個人情報を取り扱う役員・従業員に対し、必要な教育を行っている。				
5	再委託の取扱い ※再委託の実施の確認	再委託の状況について	①この業務の一部又は全部について第三者（子会社を含む。）に委託しているか。				
			（委託している場合） ②委託について発注者に申請し、承諾を得ている。				
			（委託している場合） ③委託先における個人情報の取扱いについて適切に監督している。				
			（委託している場合） ④委託先が再委託等しているか。再委託等している場合、発注者の承認を得ている。また、再委託先等における個人情報の取扱いについて適切に監督している。				
6	安全管理措置 物理的安全管理措置 ※機器及び電子媒体等の盗難等の防止	盗難防止に係る措置について	①機器、電子媒体及び書類等の盗難防止に係る手引書等を整備している。				
			②機器、電子媒体及び書類等の盗難防止に係る運用は手引書等のとおり行っている。				
7	安全管理措置 物理的安全管理措置 ※電子媒体等の取扱いにおける漏えい等の防止	漏えい防止に係る措置	①電子媒体や書類等を持ち運ぶ際は漏えい等の防止の措置を適切に講じている。				
			②漏えい等の事案の発生又はその兆候その他の安全確保上で問題となる事実を把握した場合は、直ちに発注者に報告する体制を整備している。				
8	安全管理措置 技術的安全管理措置 ※アクセス制御	システムへのアクセス制御	①情報システムへのアクセス権の付与と参照できる個人情報は適切に制御されている。				

刈谷市個人情報取扱管理要領

（目的）

第１条　この要領は、市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会及び固定資産評価審査委員会（以下「市の機関」という。）における個人情報（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。）について、その適切な管理に必要な事項を定めることにより、本市の行政の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

（総括保護管理者）

第２条　市の機関における個人情報の管理に関する事務を総括するため、総括保護管理者を置き、総務部長をもって充てる。

（副総括保護管理者）

第３条　総括保護管理者を補佐し、部等における個人情報の適切な管理を確保するため、個人情報を取り扱う部等に副総括保護管理者を置き、当該部等の長をもって充てる。

（保護管理者）

第４条　課等における個人情報の適切な管理を確保するため、個人情報を取り扱う課等に保護管理者を置き、当該課等の長をもって充てる。

（保護担当者）

第５条　保護管理者を補佐し、課等において、個人情報を取り扱う事務における個人情報の適切な管理を確保するため、個人情報を取り扱う課等に保護担当者を置き、当該課等の課長補佐又はこれに相当する職の職員をもって充てる。

（個人情報システム管理者）

第６条　個人情報を取り扱う情報システムに関し、安全の確保に必要な措置を講ずるため、個人情報システム管理者を置き、企画財政部情報政策課長をもって充てる。

（監査責任者）

第７条　個人情報の管理の状況について監査するため、監査責任者を置き、総務部総務文書課長をもって充てる。

（個人情報の適切な管理のための会議）

第８条　総括保護管理者は、個人情報の管理に係る重要事項の決定及び連絡、調整等を行うため個人情報管理運営会議（以下「会議」という。）を定期に又は随時に開催するものとす

る。

２　会議は、次に掲げる者をもって組織する。

（１）総括保護管理者

（２）個人情報システム管理者

（３）総務部総務文書課長

（４）保護管理者のうち、総括保護管理者が指名した者

３　会議の庶務は、総務部総務文書課において処理する。

（職員の責務）

第９条　個人情報の取扱いに従事する職員は、法の趣旨にのっとり、関連する条例、規程等の定め並びに総括保護管理者、副総括保護管理者、保護管理者及び保護担当者の指示に従い、個人情報を取り扱わなければならない。

（教育研修）

第１０条　総括保護管理者は、個人情報の取扱いに従事する職員に対し、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とともに、個人情報の適切な管理を推進するため、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、保護管理者及び保護担当者に対し、課等における個人情報の適切な管理のため教育研修を行うものとする。

３　総括保護管理者は、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、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ものとする。

４　保護管理者は、当該所属の職員に対し、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ずるものとする。

（保有個人情報の取扱い）

第１１条　保護管理者は、各課等における保有個人情報（法第６０条第１項に規定する「保有個人情報」をいう。以下同じ。）の秘匿性及びその内容に応じて、当該保有個人情報にアクセスする権限を有する職員及びその権限の内容を、事務を行う上で必要最小限の範囲に限るものとする。

２　アクセスする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　職員は、アクセスする権限を有する場合であっても、事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ない。

４　職員が事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及びその内容に応じて、当該行為を行うことができる場合を限定するものとする。

（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た文書（電磁的記録を含む。以下同じ。）、端末又は電磁的記録媒体（以下「保有個人情報記録文書等」という。）の外部への送付又は持ち出し

（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

（保有個人情報の訂正）

第１２条　職員は、保有個人情報の内容に誤り等を発見した場合は、保護管理者の指示に従い、速やかに訂正しなければならない。

（保有個人情報の管理等）

第１３条　保有個人情報が記録された文書は、刈谷市文書管理規程（平成６年訓令第４号）第２８条の規定により定めた期間（関係法令に保存期間の定めがある場合にあっては、その定め以上の期間）保存するものとする。

２　保護管理者は、保有個人情報記録文書等を施錠可能な場所に保管しなければならない。

３　保護管理者は、保有個人情報記録文書等を外部へ送付し、又は持ち出す場合は、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。）を使用した権限を識別する機能（以下「認証機能」という。）の設定その他アクセス制御のために必要な措置を講ずるものとする。

（保有個人情報の廃棄等）

第１４条　保有個人情報が記録された文書は、前条第１項に規定する期間を満了したときは、速やかに廃棄し、又は削除するものとする。

２　保有個人情報記録文書等を廃棄し、又は削除しようとする場合は、文書にあっては保護管理者が、端末及び電磁的記録媒体にあっては保護管理者からの依頼に基づき個人情報システム管理者が容易に復元又は判読ができない方法により適切に行うものとする。

（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及びその内容に応じて、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ものとする。

（外的環境の把握）

第１６条　保護管理者は、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上で、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。

（アクセス制御）

第１７条　個人情報システム管理者は、保有個人情報（情報システムで取り扱うものに限る。次条から第３２条まで（第２８条を除く。）において同じ。）の秘匿性及びその内容に応じて、認証機能の設定その他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　個人情報システム管理者は、前項の措置を講ずるに当たっては、パスワード等の管理に関する規程を整備するとともに、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ものとする。

（アクセス記録）

第１８条　個人情報システム管理者は、保有個人情報へのアクセス状況を記録し、その記録した情報（以下「アクセス記録」という。）を一定の期間保存し、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。

２　個人情報システム管理者は、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ずるものとする。

３　個人情報システム管理者は、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ものとする。

（管理者権限の設定）

第１９条　個人情報システム管理者は、保有個人情報の秘匿性及びその内容に応じて、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、当該特権の最小限化その他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　個人情報システム管理者は、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その他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　個人情報システム管理者は、不正プログラムによる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。

（情報システムにおける保有個人情報の処理）

第２２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は、その対象を必要最小限に限り、処理終了後、不要となった情報を速やかに削除しなければならない。

２　保護管理者は、前項の複製等を行った保有個人情報の秘匿性及びその内容に応じて、削除等の実施状況を随時確認するものとする。

（暗号化）

第２３条　職員は、保有個人情報の秘匿性及びその内容に応じて、適切に暗号化を行うものとする。

（記録機能を有する機器等の接続制限）

第２４条　個人情報システム管理者は、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等の保有個人情報を取り扱う端末等への接続の制限（当該端末等の更新への対応を含む。）その他必要な措置を講ずるものとする。

（端末の限定）

第２５条　保護管理者は、保有個人情報の秘匿性及びその内容に応じて、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２６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、執務室の施錠その他必要な措置を講ずるものとする。

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２７条　職員は、保有個人情報を取り扱う端末の使用に当たっては、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その他必要な措置を講ずるものとする。

（入力情報の照合等）

第２８条　職員は、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２９条　保護管理者及び個人情報システム管理者は、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ものとする。

（情報システムの設計書等の管理）

第３０条　保護管理者及び個人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。

（入退管理）

第３１条　個人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区域（以下「管理区域」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合い、持込機器の制限その他の必要な措置を講ずるものとする。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ものとする。

２　個人情報システム管理者は、必要があると認めるときは、管理区域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必要な措置を講ずるものとする。

３　個人情報システム管理者は、管理区域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の設定等の必要な措置を講ずるものとする。

（管理区域の管理）

第３２条　個人情報システム管理者は、外部からの不正な侵入に備え、管理区域に施錠装置、警報装置及び監視設備の設置等の必要な措置を講ずるものとする。

２　個人情報システム管理者は、災害等に備え、管理区域に耐震、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。

（保有個人情報の提供）

第３３条　保護管理者は、法第６９条第２項第３号及び第４号の規定に基づき保有個人情報を当該保有個人情報を保有する市の機関以外の者に提供する場合には、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、利用する事務の根拠法令、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号の規定に基づき保有個人情報を当該保有個人情報を保有する市の機関以外の者に提供する場合には、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ものとする。

（事務の委託等）

第３４条　保護管理者は、必要があると認めるときは、個人情報の取扱いに係る事務の全部又は一部を外部に委託することができる。

２　保護管理者は、前項の規定により委託する場合は、委託先において、法に基づき市が果たすべき安全管理措置と同等の措置（以下この条において「安全管理措置」という。）が講じられているか否かについて、あらかじめ書面又は実地調査により確認するものとする。

３　保護管理者は、第１項の規定により委託する場合は、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事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その他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

（２）個人情報の利用目的以外の目的のための利用の禁止

（３）再委託等（再委託等先が子会社である場合を含む。）に係る条件

（４）個人情報の複製等の制限

（５）個人情報の安全管理措置

（６）個人情報の漏えい等の事案の発生時における対応

（７）委託終了時における個人情報の返却又は廃棄

（８）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

（９）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（再委託等先の監査等を含む。）

４　保護管理者は、第１項の規定により委託する場合には、取扱いを委託する個人情報の範囲は、委託する事務の内容に照らして必要最小限でなければならない。

５　保護管理者は、第１項の規定により委託する場合には、委託先において安全管理措置が講じられるよう必要かつ適切な監督を行うものとする。

６　保護管理者は、委託先が個人情報の取扱いに係る事務の一部を再委託しようとする場合は、再委託先において安全管理措置が講じられるか否かを書面又は実地調査により、委託先に確認させるものとする。

７　保護管理者は、委託先が個人情報の取扱いに係る事務の一部を再委託する場合は、再委託先において安全管理措置が講じられるよう必要かつ適切な監督を行い、又は委託先に監督させ、その結果を報告させるものとする。

８　前２項の規定は、個人情報の取扱いに係る事務の一部の再々委託等について準用する。この場合において、第６項中「委託先が」とあるのは「再委託等先が」と、「再委託先」とあるのは「再々委託等先」と、「委託先に」とあるのは「再委託等先に」と、前項中「委託先が」とあるのは「再委託等先が」と、「再委託先」とあるのは「再々委託等先」と、「又は委託先」とあるのは「又は委託先若しくは再委託等先」と読み替えるものとする。

（提供又は委託時の措置）

第３５条　保護管理者は、保有個人情報を提供し、又は個人情報の取扱いに係る事務の一部若しくは全部を委託する場合は、必要に応じ、特定の個人を認識することができる記載の全部若しくは一部の削除又は別の記号等への置換えその他必要な措置を講ずるものとする。

（サイバーセキュリティに関する対策の基準等）

第３６条　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しなければならない。

（安全確保上の問題への対応及び再発防止措置）

第３７条　漏えい等の事案の発生又はその兆候その他の安全確保上で問題となる事実を把握した場合において、その事実を把握した職員は、直ちに当該保有個人情報を管理する保護管理者に報告しなければならない。

２　保護管理者は、前項の規定により報告を受けた場合は、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。この場合において、発生した安全管理上の問題（以下この条及び次条において「問題」という。）が外部からの不正アクセス又は不正プログラムの感染によるものであるときは、直ちに対象の端末装置等に被害拡大防止のための措置を講じ、個人情報システム管理者に報告しなければならない。

３　保護管理者は、問題が発生した経緯、被害状況等を調査し、及び発生した原因を究明し、

その内容を副総括保護管理者に報告するものとする。ただし、特に重大と認める問題が発生した場合には、直ちに副総括保護管理者に当該問題が発生した事実について報告しなければならない。

４　副総括保護管理者は、前項の規定による報告を受けた場合は、当該報告の内容を問題に係る保有個人情報を保有する市の機関の長及び総括保護管理者に速やかに報告するものとする。

５　保護管理者は、問題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。

（法に基づく報告及び通知）

第３８条　保護管理者は、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は、前条の規定による安全確保上の問題への対応及び再発防止措置と並行して、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問題の把握等に協力するものとする。

（公表等）

第３９条　保護管理者は、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に加えて、問題の内容、影響等に応じて事実関係及び再発防止策の公表、当該問題に係る保有個人情報の本人への対応その他必要な措置を講ずるものとする。

２　保護管理者は、前項の規定による公表等を行う場合は、問題の内容、経緯、被害状況等について速やかに個人情報保護委員会に情報提供を行うものとする。

（監査）

第４０条　監査責任者は、個人情報の適切な管理を検証するため、第２条から前条までに規定する措置の状況を含む本市における個人情報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。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　保護管理者及び個人情報システム管理者は、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４２条　総括保護管理者、保護管理者及び個人情報システム管理者は、監査又は点検の結果を踏まえ、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ものとする。

（雑則）

第４３条　この要領に定めるもののほか、必要な事項は、別に定める。

附　則

この要領は、令和５年４月１日から施行する。