平成 27 年 12 月 16 日
総合調整会議　資　料

「栗東市特定個人情報等の安全管理措置に関する基本方針」及び
「栗東市特定個人情報等の保護に関する取扱規程」の策定について

１．現　状

個人番号の利用が平成２８年１月１日に始まることから、本市においても、税や社会保障等の分野である個人番号利用事務及び財務会計や人事給与の分野である個人番号関係事務において、個人番号の収集・取扱を行うところです。

そのため、特定個人情報保護委員会（平成２８年１月１日から個人情報保護委員会に改組）が定める「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体編)」（平成２６年１２月１８日策定（平成２７年１０月５日一部改正））で求められている安全管理措置を実施する必要があります。

また、平成２７年６月に発生した日本年金機構での不正アクセスによる個人情報流出事案等のインターネットからの脅威に対する対策についても求められていることを受け、「栗東市特定個人情報等の安全管理措置に関する基本方針」及び「栗東市特定個人情報等の保護に関する取扱規程」を策定するものです。

２．検討経緯

本市の情報セキュリティに関する全庁的な検討機関である「情報セキュリティ委員会」を１２月１日に開催し、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体編)」に示されている内容に基づき作成した基本方針（案）及び取扱規程（案）の検討を求め、「了」とされました。

※情報セキュリティ委員会とは、栗東市情報セキュリティポリシー（平成１７年４月１日施行）の規定に基づき、情報セキュリティ統括責任者である副市長を委員長とし、部長級で構成される委員会であり、市全体のセキュリティの維持向上に必要な措置について検討する機関とされています。

３．栗東市特定個人情報等の安全管理措置に関する基本方針（案）の概要

これは、特定個人情報等の適正な取扱いの確保について栗東市が組織として取り組むために、策定するものです。

保護方針として、「法令遵守」、「安全管理措置」、「適正な収集・保管・利用・廃棄、目的外利用の禁止」、「委託・再委託」、「組織的改善」の５項目を本市が講ずべき事項として規定し、個人番号の利用が始まる平成２８年１月１日を施行日とするものです。

４．栗東市特定個人情報等の保護に関する取扱規程（案）の概要

これは、上記の「栗東市特定個人情報等の安全管理措置に関する基本方針（案)」で講ずる具体的な内容について定めたものであり、「組織・体制」、「教育研修」、「職員の責務」、「特定個人情報等の取扱い」、「情報システムにおける安全の確保等」、「情報システム室等の安全管理」、「業務の委託等」、「安全確保上の問題への対応」、「監査及び点検の実施」の９項目について具体的に規定し、個人番号の利用が始まる平成２８年１月１日を施行日とするものです。

講ずべき安全管理措置の内容を明確にした上で、具体的な手法を示しています。特に、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」の側面から、その内容を定め、本市が取り組む事項を定めています。

５．今後の対応

１２月２２日に実施する「栗東市社会保障・税番号制度連絡会議作業部会」において主として、利用事務実施関係者に内容を周知します。

また、各職員への教育研修については、１月以降適宜実施し、特定個人情報等の適正な取扱いを図れるよう周知するものとします。

情報セキュリティ委員会での意見を踏まえ、栗東市情報セキュリティポリシーの改正に併せて、栗東市特定個人情報等の安全管理措置に関する基本方針及び栗東市特定個人情報等の保護に関する取扱規程との一本化を図るべく調整します。

栗東市特定個人情報等の安全管理措置に関する基本方針（案）

1　特定個人情報等の保護に関する考え方

栗東市では、「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。）に定められた事務及び「栗東市行政手続における特定個人を識別するための番号の利用等に関する法律に基づく個人番号の利用に関する条例」（平成 27 年栗東市条例第　　号。以下「番号条例」という。）に定められた事務において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。

番号法においては、特定個人情報等の利用範囲を限定する等、より厳格な保護措置を求めていることから、管理体制及び取扱規程等を整備し、職員等に遵守させる等の措置を講じ、適正に特定個人情報を取り扱う。

2　特定個人情報等の保護方針

特定個人情報等を取り扱う全ての事務において、次のとおり適正に取り扱う。

（法令遵守）

①　特定個人情報等の適正な取扱いに関する法令等（注）を遵守する。

（注）法令等には次のものを含む。

- 番号法
- 番号条例
- 栗東市個人情報保護条例（平成 16 年栗東市条例第 29 号）
- 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体編）（平成 26 年特定個人情報保護委員会告示第 6 号）

（安全管理措置）

②　特定個人情報等の漏えい、滅失及び毀損の防止その他の適切な管理のために必要な安全管理措置を講ずる。

（適正な収集・保管・利用・廃棄、目的外利用の禁止）

③　特定個人情報等は、番号法に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内で適正に利用、収集・保管及び提供するとともに、不要となった特定個人情報等は速やかに廃棄する。また、目的外利用を防止するための措置を講ずる。

（委託・再委託）

④　特定個人情報等を取り扱う事務の全部又は一部を委託する場合、委託先（再委託先を含む。）において、番号法に基づき栗東市自ら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。

（組織的改善）

⑤　特定個人情報等の保護に関する取扱規程等及び安全管理措置を継続的に見直し、その改善に努める。

附則

1　本方針は、平成 28 年 1 月 1 日より実施する。

栗東市特定個人情報等の保護に関する取扱規程（案）

1　組織・体制

本市の特定個人情報等の保護に関する体制については、以下のとおりとする。

（1）総括保護管理者

総括保護管理者を一人置くこととし、副市長をもって充てる。

総括保護管理者は、市長を補佐し、本市における個人番号及び特定個人情報（以下「特定個人情報等」という。）の管理に関する事務を総括する。

（2）保護管理者

特定個人情報等を取り扱う各部等に、保護管理者を一人置くこととし、当該部等の長又はこれに代わる者をもって充てる。

保護管理者は、各部等における特定個人情報等を適切な管理を確保する任に当たる。特定個人情報等を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる。

（3）保護担当者

特定個人情報等を取り扱う各課等に、保護担当者を一人置くこととし、当該課等の長をもって充てる。保護担当者は、保護管理者を補佐し、各課等における特定個人情報等の管理に関する事務を担当する。

（4）監査責任者

監査責任者を一人置くこととし、総括保護管理者が指名する者をもって充てる。

監査責任者は、特定個人情報等の管理の状況について監査する任に当たる。

（5）特定個人情報等の適切な管理のための委員会

総括保護管理者は、特定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、保護管理者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。

（6）事務取扱担当者及びその役割の明確化

保護担当者は、特定個人情報等を取り扱う職員（以下「事務取扱担当者」という。）並びにその役割を指定する。

（7）事務取扱担当者が取り扱う特定個人情報等の範囲の明確化

保護担当者は、各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。

（8）組織体制の整備

保護担当者は、次に掲げる組織体制を整備する。

ア）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監査責任者への報告連絡体制

イ）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

ウ）特定個人情報等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

エ）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

２　教育研修

教育研修については、以下のとおりとする。

（１）総括保護管理者は、特定個人情報等の取扱いに従事する職員に対し、特定個人情報等の取扱いについて理解を深め、個人情報及び特定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。

（２）総括保護管理者は、特定個人情報等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、特定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）総括保護管理者は、保護管理者及び保護担当者に対し、課等の現場における特定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）保護担当者は、当該課等の職員に対し、特定個人情報等の適切な管理のために、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。

（５）１～４の措置を講ずる場合には、特定個人情報等の取扱いに従事する職員以外の者（派遣のよる従事者等）についても、職員と同様の措置を講ずる。

３　職員の責務

職員は、「栗東市個人情報保護条例」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。）の趣旨に則り、関連する法令及び規程等の定める事項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、特定個人情報等を取り扱わなければならない。

４　特定個人情報等の取扱い

（１）アクセス制限

ア）保護担当者は、特定個人情報等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職員に限る。

イ）アクセス権限を有しない職員は、特定個人情報等にアクセスしてはならない。

ウ）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特定個人情報等にアクセスしてはならない。

（２）複製等の制限

職員は、業務上の目的で特定個人情報等等を取り扱う場合であっても、次に掲げる行為については、保護担当者の指示に従い行う。

ア）特定個人情報等の複製

イ）特定個人情報等の送信

ウ）特定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

エ）その他特定個人情報等の適切な管理に支障を及ぼすおそれのある行為

（３）誤りの訂正等

職員は、特定個人情報等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。

（４）媒体の管理等

職員は、保護担当者の指示に従い、特定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、必要があると認めるときは、耐火金庫への保管、（キャビネット等の）施錠等を行う。

（５）廃棄等

職員は、特定個人情報等又は特定個人情報等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、保護担当者の指示に従い、当該特定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削除又は当該媒体の廃棄を行う。

（６）特定個人情報等の取扱状況の記録

保護担当者は、特定個人情報等の秘匿性等その内容に応じて、台帳等を整備して、当該特定個人情報等の利用及び保管等の取扱いの状況について記録する。

（７）個人番号の利用の制限

保護担当者は、個人番号の利用に当たり、番号法があらかじめ限定的に定めた事務に限定する。

（８）特定個人情報の提供の求めの制限

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。

（９）特定個人情報ファイルの作成の制限

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。

（10）特定個人情報等の収集・保管の制限

番号法第 19 条各号及び番号条例第 4 条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。

（11）取扱区域

保護担当者は、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、物理的な安全管理措置を講ずる。

5　情報システムにおける安全の確保等

（１）アクセス制御

ア）保護担当者は、特定個人情報等（情報システムで取り扱うものに限る。）の秘匿性等その内容に応じて、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。

イ）保護担当者は、ア）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。

（２）アクセス記録

ア）保護担当者は、特定個人情報等の秘匿性等その内容に応じて、当該特定個人情報等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。

イ）保護担当者は、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。

（３）アクセス状況の監視

保護担当者は、特定個人情報等の秘匿性等その内容及びその量に応じて、当該特定個人情報等への不適切なアクセスの監視のため、特定個人情報等を含むか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。

（４）管理者権限の設定

保護担当者は、特定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。

（５）外部からの不正アクセスの防止

保護担当者は、特定個人情報等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。

（６）不正プログラムによる漏えい等の防止

保護担当者は、不正プログラムによる特定個人情報等の漏えい、滅失又は毀損の防止のため、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。

（７）情報システムにおける特定個人情報等の処理

職員は、特定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。保護担当者は、当該特定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。

（８）暗号化

保護担当者は、特定個人情報等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、その処理する特定個人情報等について、適切に暗号化を行う。（職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。

（９）記録機能を有する機器・媒体の接続制限

保護担当者は、特定個人情報等の秘匿性等その内容に応じて、当該特定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・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。

（10）端末の限定

保護担当者は、特定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するために必要な措置を講ずる。

（11）端末の盗難防止等

ア）保護担当者は、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。

イ）職員は、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。

（12）第三者の閲覧防止

職員は、端末の使用に当たっては、特定個人情報等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。また、窓口端末はディスプレイの方向・設置場所の考慮、斜視防止フィルタの利用及び窓口間の衝立の設置等を行う。

（13）入力情報の照合等

職員は、情報システムで取り扱う特定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、処理前後の内容の確認、既存の特定個人情報等との照合等を行う。

（14）バックアップ

保護担当者は、特定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ずる。

（15）情報システム設計書等の管理

保護担当者は、特定個人情報等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。

（16）特定個人情報等の取扱いに関するシステムログ又は利用実績の記録

保護担当者は、特定個人情報等へのアクセス状況を記録し、その記録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。また、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。

6　情報システム室等の安全管理

（１）入退管理

ア）保護担当者は、特定個人情報等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、特定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。また、特定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。

イ）保護担当者は、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。

ウ）保護担当者は、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。

（２）情報システム室等の管理

ア）保護担当者は、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、監視設備の設置等の措置を講ずる。

イ）保護担当者は、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。

７　業務の委託等

（１）特定個人情報等の取扱いに係る業務を外部に委託する場合には、特定個人情報等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　特定個人情報等に関する秘密保持、目的外利用の禁止等の義務

②　再委託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　特定個人情報等の複製等の制限に関する事項

④　特定個人情報等の漏えい等の事案の発生時における対応に関する事項

⑤　委託終了時における特定個人情報等の消去及び媒体の返却に関する事項

⑥　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

（２）特定個人情報等の取扱いに係る業務を外部に委託する場合には、委託する特定個人情報等の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年１回以上の定期的検査等により確認する。

（３）委託先において、特定個人情報等の取扱いに係る業務が再委託される場合には、委託先に（１）の措置を講じさせるとともに、再委託される業務に係る特定個人情報等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（２）の措置を実施する。特定個人情報等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）特定個人情報等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。

（５）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、番号法に基づき栗東市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。

（６）個人番号利用事務等の全部又は一部の委託をする際には、「委託を受けた者」において、栗東市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。

（７）個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託をする際には、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する。

8　安全確保上の問題への対応

（1）特定個人情報等の漏えい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、その事案等を認識した職員は、直ちに当該特定個人情報等を管理する保護担当者に報告する。（職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。）

（2）保護担当者は、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）保護担当者は、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。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。

（4）総括保護管理者は、（3）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。

（5）保護担当者は、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（公表等）を講ずる。

（6）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、当該事案に係る特定個人情報等の本人への対応等の措置を講ずる。

9　監査及び点検の実施

（1）監査

監査責任者は、特定個人情報等の適切な管理を検証するため、本規程に規定する措置の状況を含む特定個人情報等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を行い、その結果を総括保護管理者に報告する。監査は、特定個人情報等の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。

（2）点検

保護担当者は、各課室等における特定個人情報等の記録媒体、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、その結果を総括保護管理者に報告する。

（3）評価及び見直し

特定個人情報等の適切な管理のための措置については、総括保護管理者、保護管理者、保護担当者等は、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

1　本規程は、平成28年1月1日より実施する。