参考資料 11

保有個人情報に関する
内部監査実施マニュアル

久喜市

目次

１　目的

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。）に基づき、久喜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規程（令和5年訓令第13号。以下「規程」という。）を定めています。

規程第42条では、「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章から前章までに規定する措置の状況を含む久喜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。」と規定されており、監査の実施が求められています。

また、規程第44条では、「総括保護管理者及び保護管理者は、監査又は点検の結果等を踏まえ、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、その見直しその他の措置を講ずるものとする。」と定めていることから、本マニュアルにおいて、その内部監査の実施方法について定めるものです。

２　監査体制の構築

規程の規定により、総括保護管理者は副市長とし、保護管理者は保有個人情報を取り扱う各課等の長とし、監査責任者は、総務部長とします。

３　監査の対象所属

保有個人情報を取扱う所属を対象とすることから、原則、全ての所属を対象とします。

４　監査計画の策定

監査は、5年計画で行います。

監査を効率的かつ効果的に行うために、「中期監査計画（様式1）」及び「年度監査計画（様式2）」を策定し、総括保護管理者の承認を得た後、被監査所属に通知します。

（1）中期監査計画

監査担当課は、全ての監査の対象所属について、単年度内で監査を実施することは困難であることから、5年で全ての監査の対象所属に対する監査が実施できるよう「中期監査計画（様式1）」を策定します。

（2）年度監査計画

監査担当課は、中期監査計画を基に、年度内での被監査所属、実施時期、監査範囲等を明示した「年度監査計画（様式2）」を策定します。

５ 自己点検の実施

自己点検については、保護管理者及び保護担当者自らが保有個人情報の取扱いの見直しを図ることを意識付けること及び被監査所属における保有個人情報の取扱状況を効率的に把握することを目的として、毎年度、全ての所属に対し実施します。

監査担当課は全ての所属に対し、保有個人情報の取扱いに関する自己点検チェックリスト（以下、「自己点検チェックリスト」という。（様式3））に基づく自己点検の実施を依頼します。

全ての所属は、自己点検チェックリストに基づき、自己点検を実施し、その回答を監査担当課に提出します。

６ 監査の実施

監査担当課は、年度監査計画に基づき監査の対象となる被監査所属に対し、自己点検チェックリストの回答のとおり運用が行われているかどうか、組織の体制や事務の運用状況等を考慮して適宜、適切な運用がおこなわれているかどうか、被対象所属の職員に対するヒアリングや現地において目視にて、独立した立場で、かつ客観的な視点で監査を実施します。

※令和5年度は、全ての対象所属が書面による自己点検を実施することをもって、監査を実施したものとします。

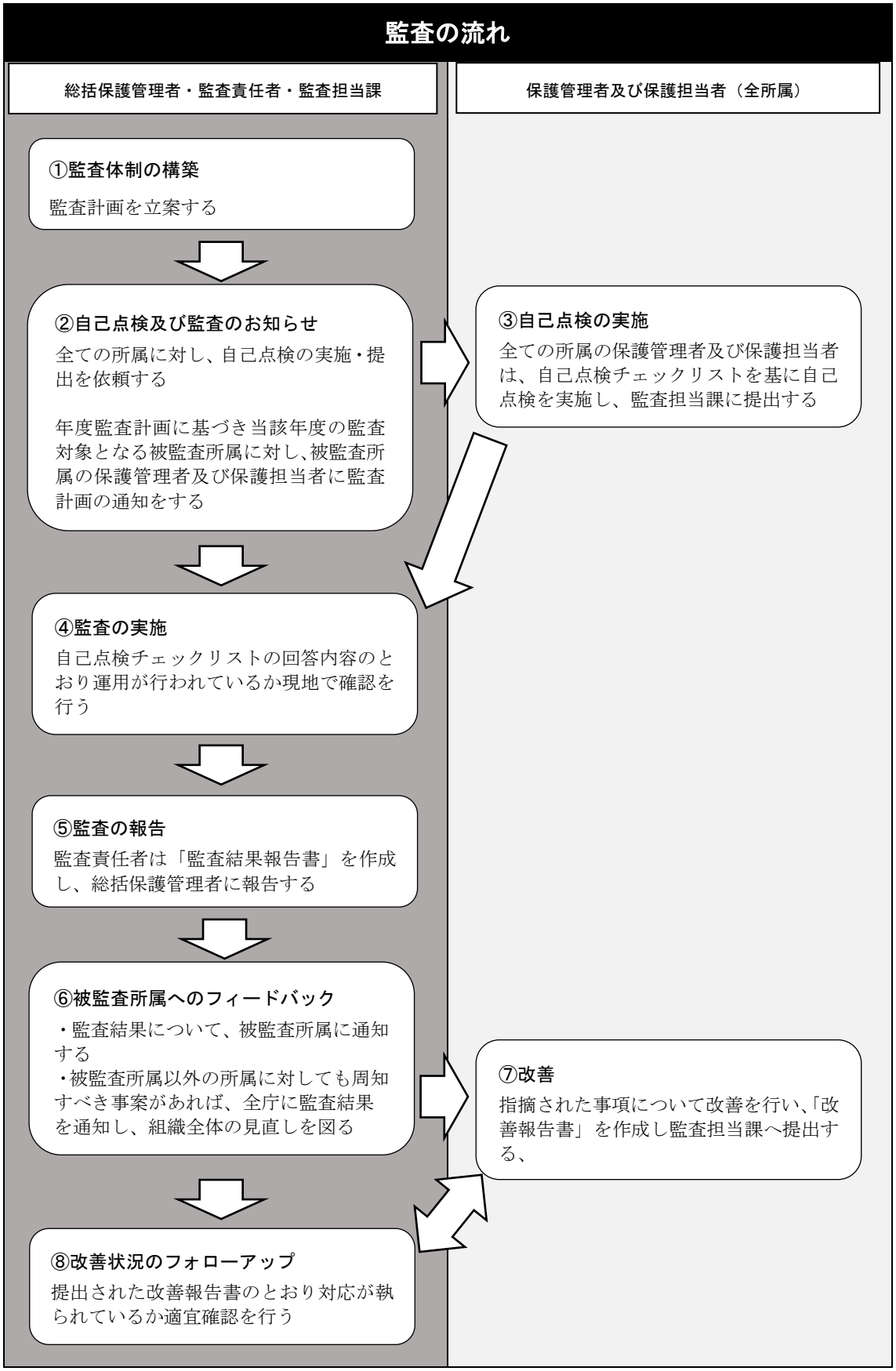
７ 監査実施後

（1）監査結果報告書の作成

監査責任者は、監査実施後、「年度監査結果報告書 （様式4）」を作成し、総括保護管理者へ報告します。

（2）改善状況のフォローアップ

監査担当課は、監査で指摘した事項について、被監査所属から提出された「監査改善報告書（様式5）」のとおり対応が執られているか、適宜、必要に応じて現地に赴く等により確認します。


監査の流れ
総括保護管理者・監査責任者・監査担当課
保護管理者及び保護担当者（全所属）
①監査体制の構築
監査計画を立案する
②自己点検及び監査のお知らせ
全ての所属に対し、自己点検の実施・提出を依頼する
年度監査計画に基づき当該年度の監査対象となる被監査所属に対し、被監査所属の保護管理者及び保護担当者に監査計画の通知をする
③自己点検の実施
全ての所属の保護管理者及び保護担当者は、自己点検チェックリストを基に自己点検を実施し、監査担当課に提出する
④監査の実施
自己点検チェックリストの回答内容のとおり運用が行われているか現地で確認を行う
⑤監査の報告
監査責任者は「監査結果報告書」を作成し、総括保護管理者に報告する
⑥被監査所属へのフィードバック
・監査結果について、被監査所属に通知する
・被監査所属以外の所属に対しても周知すべき事案があれば、全庁に監査結果を通知し、組織全体の見直しを図る
⑦改善
指摘された事項について改善を行い、「改善報告書」を作成し監査担当課へ提出する、
⑧改善状況のフォローアップ
提出された改善報告書のとおり対応が執られているか適宜確認を行う

８ 様式

（様式１）

年　月　日

保有個人情報に関する中期監査計画

監査計画

年度	被監査所属
年度	
年度	
年度	
年度	
年度	

なお、監査責任者は、上記の監査に加えて、漏えい事案の発生等を踏まえ、必要に応じて随時監査を実施することとする。

以　上

（様式２）

年　月　日

年度　保有個人情報に関する監査計画

１　監査計画

1	監査目的	【例】○○業務に関して、久喜市の保有する個人情報等の適切な管理のための措置に関する規程に基づく運用状況及び保有個人情報の管理状況について確認する。
2	監査範囲	【例】○○業務、○○システム
3	被監査所属	
4	監査方法	【例】自己点検結果の確認、○○システムの取扱規程に基づく運用状況の確認、執務室の状況確認
5	監査実施日程	年　月　日～　年　月　日
6	監査実施体制	監査責任者　総務部長 監査人　庶務課公文書館職員
7	適用基準	【例】久喜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規程

２　監査結果のフォローアップ

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ずるものとする。

以　上

（様式３）

保有個人情報の取扱いに関する
自己点検チェックリスト

記入 年月日　　年　月　日	所属 （機関:　　）	保護管理者 （課等の長）	保護 担当者

NO.	確認事項	回答欄	参考条文等
1	保有個人情報のアクセス権限（情報に接する行為をいう。以下同じ。）について必要以上に付与していないか。	□　はい □　いいえ	・規程 （アクセス制限） 第10条第1項、 第2項関係
2	業務上必要な範囲を超えて保有個人情報にアクセスできるようになっていないか。	□　はい □　いいえ	・規程 （アクセス制限） 第10条第1項、 第2項関係
3	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いないか。	□　はい □　いいえ	・規程 （アクセス制限） 第10条第3項、 第4条関係
4	職員が保有個人情報を必要以上に複製、送信、持出し、その他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をしないように措置を講じているか。 講じている場合、どのような内容か。 【例】 ・許可された外部記憶媒体のみ端末への接続を許可されている。 ・許可された端末以外では USB メモリや HDD 等の外部記憶媒体へのデータの書き出しができないようにされている。	□　はい □　いいえ （措置の内容）	・規程 （複製等の制限） 第11条関係
5	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、訂正等を行っているか。	□　はい □　いいえ	・規程 （誤りの訂正等） 第12条関係
6	職員は、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、耐火金庫への保管、保管場所への施錠等、個人情報の漏えい等を防止するための措置を講じているか。 【例】 ・個人情報については、施錠できるキャビネットや金庫に保管している。	□　はい □　いいえ （措置の内容）	・規程 （媒体の管理等） 第13条第1項関係

7	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、パスワード等（パスワード、ICカード、生体情報等をいう。）を使用して権限を識別する機能を設定する等、アクセス制御のために必要な措置を講じているか。 【例】 ・USB メモリにパスワードを設定している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （媒体の管理等） 第13条第2項関係
8	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、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ているか。講じている場合、どのような方法であるか。 【例】 ・必ず 2 人以上でのダブルチェックをするフローとしている。	□　はい □　いいえ （措置の内容）	・規程 （誤送付等の防止） 第14条関係
9	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、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っているか。	□　はい □　いいえ □　該当なし	・規程 （廃棄等） 第15条第 1 項関係
10	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。）は、職員が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若しくは廃棄が確実に行われていることを確認しているか。	□　はい □　いいえ □　該当なし	・規程 （廃棄等） 第15条第 2 項関係
11	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、秘匿性等その内容に応じて、管理台帳を作成するなどして記録しているか。	□　はい □　いいえ □　該当なし	・規程 （保有個人情報の取扱状況の記録） 第16条関係
12	保有個人情報（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、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じているか。 【例】 ・取り扱う必要のある職員にのみ権限を付与している。 ・秘匿性の高い情報が含まれる文書については暗号化している。 ・二要素認証を取り入れている。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （アクセス制限） 第18条第1項関係
13	(12)の措置を講ずる場合、パスワード等の管理に関する定め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じているか。 【例】 ・アクセス権が必要なくなった職員については遅滞なくその権限を削除している。 ・推測困難な複雑なパスワードを設定している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （アクセス制限） 第18条第2項関係

14	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ているか。 【例】 ・アクセスログを1年間以上保存している。 ・6か月以上の間隔でアクセスログの分析を行っている。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （アクセス記録） 第19条第1項関係
15	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ているか。 【例】 ・アクセスログにアクセスできる職員を少数に限定している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （アクセス記録） 第19条第2項関係
16	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じているか。 【例】 ・定期的に委託先から運用報告を受けている。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （アクセス状況の監視） 第20条関係
17	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ているか。 【例】 ・管理者権限をシステムごとに細分化している。 ・管理者権限はごく限られた少数者にのみ付与している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （管理者権限の設定） 第21条関係
18	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ているか。 【例】 ・ファイアウォールを設置している。 ・ファイアウォールの設定を定期的に見直している。 ・ネットワークに適切なアクセス制御を施している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （外部からの不正アクセスの防止） 第22条関係
19	不正プログラムによる保有個人情報の漏えい、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。）を講じているか。 【例】 ・脆弱性情報を定期的に確認している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （不正プログラムによる漏えい等の防止） 第23条関係

20	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の複製等を行う場合は、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しているか。	□ はい □ いいえ □ 該当なし	・規程 (情報システムにおける保有個人情報の処理) 第24条第1項関係
21	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しているか。	□ はい □ いいえ □ 該当なし	・規程 (情報システムにおける保有個人情報の処理) 第24条第2項関係
22	当該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行っているか。 暗号化している情報がある場合は、その情報の内容を記載。 【例】 ・HDDを暗号化している ・特に秘匿性の高い情報を抽出し、その情報が保存されているデータベースを暗号化している。 ・情報システムへのアクセス権限を付与した者のパスワードを暗号化している	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (暗号化) 第25条第1項、第2項関係
23	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、滅失又は毀損の防止のため、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ているか。 【例】 ・端末には利用許可された媒体のみ接続可能としている。 ・利用媒体は、全て管理し利用履歴を残している。 ・データの受渡しには、必ず情報セキュリティ管理者の承認を受けることとし、その記録を残している。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (記録機能を有する機器又は媒体の接続制限) 第26条関係
24	保有個人情報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じているか。 【例】 ・秘匿性の高い保有個人情報を取り扱うための専用端末を設けている。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (端末の限定等) 第27条第1項関係
25	端末を外部へ持ち出し、又は外部から持ち込んでいないか。	□ はい □ いいえ □ 該当なし	・規程 (端末の限定等) 第27条第2項関係
26	端末の盗難又は紛失の防止のための措置を講じているか。 講じている場合、どのような方法であるか。 【例】 ・端末をセキュリティワイヤーで固定している。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (端末の盗難防止) 第28条関係

	・退庁時は端末を施錠できる机やキャビネット等の中に保管している。		
27	職員は、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、使用状況に応じて必要な措置を講じているか。 講じている場合、どのような方法であるか。 【例】 ・端末の画面に覗き見防止フィルムを貼っている。 ・一定時間端末を操作しないときは自動的にロックがかかる設定にしている。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (閲覧防止) 第29条関係
28	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っているか。	□ はい □ いいえ □ 該当なし	・規程 (入力情報の照合等) 第30条関係
29	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ているか。 【例】 ・オンラインでバックアップデータを収集し分離したネットワークに保存している。 ・磁気テープを使用してバックアップをしている。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (バックアップ) 第31条関係
30	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じているか。 【例】 ・アクセスできる者を必要最小限に限定している。 ・暗号化もしくは鍵のかかるキャビネット等で保管している。 ・保管又は保存場所を一定の範囲の者にのみ伝えている。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (情報システム設計書等の管理) 第32条関係
31	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を行っているか。	□ はい □ いいえ □ 該当なし	・規程 (入退管理) 第33条第1項関係
32	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じていますか。 【例】 ・配線の損傷防止等の措置を講じている。 ・代替機を用意している。	□ はい □ いいえ □ 該当なし (措置の内容)	・規程 (情報システム室等の管理) 第34条関係

33	保護管理者は、個人情報保護法第69条第2項第4号の規定に基づき他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人以外の者に保有個人情報を提供する場合に、同法第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。）を取り交わしているか。	□　はい □　いいえ □　該当なし	・規程 （保有個人情報の提供） 第35条第1項関係・
34	保有個人情報の取扱いに係る業務を外部に委託（再委託も含む）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、必要な措置を講じているか。 講じている場合は、その内容を記載。 【例】 ・委託業者の選定に当たっては、個人情報取扱業務委託が適正に履行できるか、「遵守確認表（契約前）」を活用するなどして確認している。	□　はい □　いいえ □　該当なし （措置の内容）	・規程 （業務の委託等） 第36条第1項、第5項関係
35	個人情報の取扱いに係る業務を外部に委託するときは、契約書に「個人情報の取扱いに関する特記仕様書」を設け、委託先における責任者及び業務従事者の管理体制、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確認しているか。	□　はい □　いいえ □　該当なし	・規程 （業務の委託等） 第36条第2項関係
36	保有個人情報の取扱いに係る業務を外部に委託するときは、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ているか。	□　はい □　いいえ □　該当なし	・規程 （業務の委託等） 第36条第3項関係
37	保有個人情報の取扱いに係る業務を外部に委託（再委託も含む）する場合には、「久喜市個人情報取扱事務の外部委託及び指定管理に係る個人情報保護基準」に基づき必要な措置を講じているか。 ※基準 ①指定管理業者の場合 年1回、作業所へ赴き確認する。 ②長期継続契約の場合 年1回、書面で確認するとともに、契約期間中に少なくとも1回は作業所に赴き確認する。 ③1年契約の場合 年1回、書面で確認する。 （毎年、同じ業者へ継続している場合は 3 年に 1 回は作業所に赴き確認する。） ④1年未満の契約の場合 履行期間中に、書面で確認する。	□　はい □　いいえ □　該当なし	・規程 （業務の委託等） 第36条第4項、第5項関係
38	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又は問題となる事案の発生のおそれを認識した場合、責任者への報告連絡体制は取られているか。	□　はい □　いいえ	・規程 （事案の報告及び再発防止措置） 第39条関係

（様式４）

年　　月　　日

監査責任者

年度　保有個人情報の取扱いに関する監査結果報告書

「　　年度保有個人情報の取扱いに関する監査計画」に関する監査結果は、次のとおりである。

１　監査の対象

２　監査の実施日

年　　月　　日～　　月　　日

３　監査担当課

４　指摘事項等

（様式５）

年　　月　　日

保護管理者

年度　保有個人情報の取扱いに関する監査
改善報告書

「　　年度保有個人情報の取扱いに関する監査」において指摘を受けた事項について、次のとおり改善しましたので報告します。

１　監査の対象

２　監査の実施日
　　年　　月　　日～　　月　　日

３　監査担当課

４　指摘事項等

５　改善内容

令和6年2月16日（初版）

令和6年7月（改訂版）

総務部　庶務課公文書館