（参考書式）

新潟市個人情報取扱委託業務等に関する個人情報取扱状況報告書

※この表において「個人情報」とは、個人情報取扱委託業務等において取り扱う個人情報をいいます。
※確認結果欄の「はい」「いいえ」のどちらかにチェックを入れてください。該当がない項目は「非該当」にチェックしてください。
※今後実施予定がある場合又は実施することを承知している場合は、「はい」にチェックしてください。
※この報告書は、原則、業務履行開始前に提出をお願いします。

契約件名					
No.	措置項目	確認内容	確認結果		
			はい	いいえ	非該当
1	法令の遵守	個人情報の保護に関する法律第４章その他関係法令を遵守していますか。	□	□	
2	規程の整備	個人情報等の適切な管理に関する定めを整備していますか。 （例：組織全体の規定、担当部署の規定、業務マニュアルの整備など）	□	□	
3	管理体制	個人情報を安全に取扱うための組織体制を構築していますか。 （例：個人情報に関する総括責任者、担当部署の責任者の指定など）	□	□	
		責任者は、個人情報を扱う業務に従事する従事者（派遣労働者を含む。以下「従事者」という。）を明確にしていますか。	□	□	
4	教育研修	従事者に対して、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ための啓発等の研修を実施しましたか。	□	□	
5	従事者の責務	従事者は、法の趣旨にのっとり、関連法令及び責任者の指示に従い、個人情報を取り扱わなければならないことを理解していますか。	□	□	
6	アクセス制限	個人情報にアクセスする権限を管理していますか。	□	□	
		個人情報を取り扱うシステムや個人情報が含まれるデータへのアクセスログその他の個人情報の取扱いに係る記録等を保存していますか。	□	□	
		責任者は、従事者に対して、個人情報にアクセスする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個人情報にアクセスしてはいけないこと及びアクセスは必要最小限としなければならないことについて周知していますか。	□	□	
7	複製等の制限	責任者は、次に掲げる行為について、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、新潟市の指示又は承諾に基づき行わなければならないことを従事者に周知していますか。 ①　個人情報の複製 ②　個人情報の送信 ③　個人情報が記録されている媒体の外部への送付又は持ち出し ④　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	□	□	
8	誤りの訂正等	従事者が個人情報の内容に誤り等を発見した場合には、新潟市及び責任者の指示に従い訂正等を行うように周知し、実施していますか。	□	□	
9	媒体の管理等	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、必要に応じて、耐火金庫への保管、施錠等を行っていますか。	□	□	
		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（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じていますか。	□	□	□
10	誤送付等の防止	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、取り扱う個人情報の秘匿性等その内容に応じ、複数の従事者による確認やチェックリストの活用等の必要な措置を講じていますか。	□	□	□
11	廃棄等	個人情報又は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、新潟市及び責任者の指示に従い、当該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うようにしていますか。	□	□	□
		個人情報の消去や個人情報が記録されている媒体の廃棄を再委託（新潟市から見た再委託。以下同じ）する場合（二以上の段階にわたる委託を含む。）には、必要に応じて責任者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など、再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ようにしていますか。	□	□	□

No.	措置項目	確認内容	確認結果		
			はい	いいえ	非該当
12	個人情報の取扱状況の記録	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ていますか。	□	□	□
13	外的環境の把握	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ていますか。	□	□	□
14	アクセス制御	情報システム（パソコン等の機器を含む。以下同じ。）で取り扱う個人情報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ますか。	□	□	□
		上記の措置を講ずる場合は、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ますか。	□	□	□
15	アクセス記録	情報システムで取り扱う個人情報の秘匿性等その内容に応じて、当該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ますか。	□	□	□
		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ますか。	□	□	□
16	アクセス状況の監視	情報システムで取り扱う個人情報の秘匿性等その内容及びその量に応じて、当該個人情報への不適切なアクセスの監視のため、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じていますか。	□	□	□
17	管理者権限の設定	情報システムで取り扱う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ますか。	□	□	□
18	外部からの不正アクセスの防止	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ますか。	□	□	□
19	不正プログラムによる漏えい等の防止	不正プログラムによる個人情報の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。）を講じていますか。	□	□	□
20	情報システムにおける個人情報の処理	情報システムで取り扱う個人情報について、従事者が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していますか。	□	□	□
		責任者は、当該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ますか。	□	□	□
21	暗号化	情報システムで取り扱う個人情報の秘匿性等その内容に応じて、暗号化のための必要な措置を講じていますか。	□	□	□
22	記録機能を有する機器・媒体の接続制限	情報システムで取り扱う個人情報の秘匿性等その内容に応じて、当該個人情報の漏えい、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（当該機器の更新への対応を含む。）等への接続の制限等の必要な措置を講じていますか。	□	□	□
23	端末の限定	情報システムで取り扱う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ますか。	□	□	□
24	端末の盗難防止等	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じていますか。	□	□	□
		従事者は、新潟市の指示又は承諾がある場合で、責任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いませんか。	□	□	□
25	第三者の閲覧防止	端末の使用に当たって、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うことを徹底する等の必要な措置を講じていますか。	□	□	□
26	入力情報の照合等	情報システムで取り扱う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、処理前後の当該個人情報の内容の確認、既存の個人情報との照合等を行っていますか。	□	□	□
27	バックアップ	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ますか。	□	□	□
28	情報システム設計書等の管理	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ますか。	□	□	□

No.	措置項目	確認内容	確認結果		
			はい	いいえ	非該当
29	入退管理	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「情報システム室」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従事者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じていますか。	□	□	□
		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。）を設けている場合は、必要に応じて上記の措置を講じていますか。	□	□	□
		必要に応じて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じていますか。	□	□	□
		情報システム室等及び保管施設の入退の管理について、必要に応じて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（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じていますか。	□	□	□
30	情報システム室等の管理	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じていますか。	□	□	□
		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。	□	□	□
31	業務の委託等	個人情報の取扱いに係る業務を再委託する場合には、新潟市から承諾を得て行っていますか。	□	□	□
		個人情報の取扱いに係る業務を再委託する場合には、再委託先に対して、個人情報の安全管理が図られるよう、必要かつ適切な監督を行っていますか。	□	□	□
		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していますか。	□	□	□
32	サイバーセキュリティの確保	個人情報を取り扱い、又は情報システムを構築し、若しくは利用する場合は、サイバーセキュリティ基本法による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ていますか。	□	□	□
33	事案の報告及び再発防止措置	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に、その事案等を認識した従事者は、直ちに責任者に報告するようになっていますか。	□	□	
		漏えい等事案が発生した場合は、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じるようになっていますか。特に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（従事者に行わせることを含む。）ようになっていますか。	□	□	
		責任者は、漏えい等事案が発生した場合は、直ちに新潟市に報告する体制のフロー等を定めていますか。	□	□	
		責任者は、漏えい等事案が発生した場合は、当該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、組織内に再発防止措置を共有するようになっていますか。	□	□	
34	点検	責任者は、個人情報の記録媒体、処理経路、保管方法等について、定期に点検を行っていますか。	□	□	
35	評価及び見直し	責任者等は、上記34の措置による点検の結果又は新潟市による検査の結果等を踏まえ、実効性等の観点から個人情報の適切な管理のための措置について評価し、必要に応じて、その見直し等の措置を講じていますか。	□	□	

（報告日）　　年　　月　　日

上記のとおり報告します。

受託者（名称及び代表者の氏名）

新潟市保有個人情報の適切な管理のための措置　概要
（委託先に対し市と同等の安全管理措置を求める内容）

※　ここで使用する用語の意義は、法の定めるところによる。

No.	措置項目	内容
1	管理体制	保有個人情報を安全に取り扱うための組織体制を整備する。
2	教育研修	保有個人情報の取扱いに従事する職員に対し、保有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ための啓発その他必要な教育研修を行う。
3	職員の責務	職員は、法の趣旨にのっとり、関連法令及び総括保護管理者等の指示に従い、保有個人情報を取り扱わなければならない。
4	アクセス制限	アクセス権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。
		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。
		職員はアクセス権限を有する場合であっても、アクセスは必要最小限としなければならない。
5	複製等の制限	保護管理者は、次に掲げる行為について、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の外部への送付又は持ち出し ④　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
6	誤りの訂正等	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、保護管理者の指示に従い訂正等を行う。
7	媒体の管理等	職員は、保護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、施錠等を行う。
8	誤送付等の防止	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、当該保有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やチェックリストの活用等必要な措置を構ずる。
9	廃棄等	保有個人情報又は保有個人情報が記録されている媒体が不要となった場合には、保護管理者の指示に従い、復元又は判読が不可能な方法により消去又は当該媒体の廃棄を行う。
		保有個人情報を削除した場合又は保有個人情報が記録されている媒体を廃棄した場合には、削除又は廃棄した記録を保存する。これらの作業を委託する場合には、委託先（再委託先を含む。）が確実に削除または廃棄したことについて、証明書等により確認する。
10	保有個人情報の取扱状況の記録	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、利用及び保管等の取扱状況について記録する。
11	外的環境の把握	保有個人情報が、外国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。
12	アクセス制御	情報システムで取り扱う保有個人情報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
		上記の措置を講ずる場合は、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ずる。
13	アクセス記録	情報システムで取り扱う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ずる。
		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。

No.	措置項目	内容
14	アクセス状況の監視	情報システムで取り扱う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。
15	管理者権限の設定	情報システムで取り扱う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。
16	外部からの不正アクセスの防止	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ずる。
17	不正プログラムによる漏えい等の防止	不正プログラムによる保有個人情報の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。
18	情報システムにおける個人情報の処理	情報システムで取り扱う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。
19	暗号化	情報システムで取り扱う保有個人情報の秘匿性等その内容に応じて、暗号化のための必要な措置を講ずる。
20	記録機能を有する機器・媒体の接続制限	情報システムで取り扱う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。
21	端末の限定	情報システムで取り扱う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ずる。
22	端末の盗難防止等	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。
		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。
23	第三者の閲覧防止	端末の使用に当たって、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うことを徹底する等の必要な措置を講ずる。
24	入力情報の照合等	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、既存の個人情報との照合等を行う。
25	バックアップ	保護管理者は、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。
26	情報システム設計書等の管理	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。
27	入退管理	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「情報システム室」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。）を設けている場合は、必要に応じて上記の措置を講ずる。
		必要に応じて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。
		情報システム室等及び保管施設の入退の管理について、必要に応じて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（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。

No.	措置項目	内容
28	情報システム室等の管理	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、警報装置及び監視設備の設置等の措置を講ずる。
		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。
29	業務の委託等	保護管理者は、必要があると認めるときは、委託先が再委託先に対して保有個人情報の取扱いに関し必要かつ適切な監督を行っていることを検査の実施等により確認する。
		保有個人情報の取扱いに係る業務を再委託する場合には、再委託先について安全管理措置を講じさせていますか。
		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。
		保護管理者は、保有個人情報の取扱に係る業務を派遣労働者に行わせる場合には、労働者派遣契約書に秘密保持義務等の保有個人情報の取扱いに関する事項を明記する。
30	サイバーセキュリティの確保	個人情報を取り扱い、又は情報システムを構築し、若しくは利用する場合は、サイバーセキュリティ基本法による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。
31	事案の報告及び再発防止措置	職員は、保有個人情報の漏えい等安全管理上、問題となる事案の発生又はその兆候を把握した場合は、直ちに保護管理者に報告する。
		報告を受けた保護管理者は、直ちに事実関係を確認したうえで、総括保護管理者に報告するとともに、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。
		保護管理者は、速やかに保有個人情報の漏えい等が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。
32	点検	保護管理者は、保有個人情報の記録媒体、処理経路、保管方法等について、定期に点検を行う。
33	評価及び見直し	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、必要があると認められるときは、その見直し等の措置を講ずる。