Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
母子保健情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・本市に住民登録がある者の個人番号、基本4情報（氏名、性別、住所、生年月日）、その他の住民基本台帳関係情報は、当市の住基システムよりシステム基盤（個人基本）を経由して取得する方法（システム基盤（個人基本）に反映されない場合は専用端末等による個別確認）によるため、住民またはかつて住民であった者以外の情報を入手することはない。 ・乳幼児精密健康診査の実施については、当市より受診券を発行した上で、受診対象者（保護者）の意志で精密健康診査実施医療機関で精密健康診査を実施し、本市は当該医療機関からの報告に基づいて本件事務を行うため、対象者以外の情報を入手することはない。 ・母子保健法による妊娠届出および母子健康手帳交付に関する事務等について、窓口で個人番号を含む届出書等の受付を行う際は、個人番号カード又は通知カードと身分証明書の提示による本人確認を厳守することで、対象者以外の情報の入手を防止する。
必要な情報以外を入手することを防止するための措置の内容	必要とされる情報以外記載できない書類様式とする。
その他の措置の内容	―
リスクへの対策は十分か	[　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・本市に住民登録がある者の個人番号、基本4情報（氏名、性別、住所、生年月日）、その他の住民基本台帳関係情報は、庁内ネットワーク及びシステム基盤（個人基本）を通じて入手又は権限が認められた職員が専用端末から個別に確認する方法に限定することで、不適切な方法により個人番号が入手されることのないよう、安全を担保している。 ・本市に住民登録がある者及び住民登録がない居住者から入手する母子保健情報は、利用目的を明示した上で入手する。
リスクへの対策は十分か	[　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク3：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・乳幼児精密健康診査の実施については、精密健康診査実施医療機関において、健康保険証等身分証明書の提示などにより、必ず本人確認を行う。 ・母子保健法による妊娠届出および母子健康手帳交付に関する事務等について、窓口で個人番号を含む届出書等の受付を行う際は、個人番号カード又は通知カードと身分証明書の提示による本人確認を行う。
個人番号の真正性確認の措置の内容	上記にて入手した基本4情報（氏名・住所・性別・生年月日）に基づき、システム基盤（個人基本）との連携により、個人番号を入手する。
特定個人情報の正確性確保の措置の内容	1　上記のとおり、入手の各段階で、本人確認のもと、個人情報の正確性を確保する。 2　収集した情報に基づいて、システム基盤（個人基本）との連携により、個人番号を入手することで、正確性を確保する。
その他の措置の内容	―
リスクへの対策は十分か	[　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	＜母子保健情報システムにおける措置＞ 1 システム保守委託業者との契約において、秘密保持の遵守に関する条項を明記して、情報の漏えいを防止する。 2 入手した基本4情報（氏名・住所・性別・生年月日）に基づき、システム基盤（個人基本）との連携により、住民基本台帳から個人番号を入手する際には、外部委託業者には個人番号の表示権限を与えないこととするので、外部に漏れることはない。 3 システム間は専用回線で接続されており、それ以外への接続はできないシステムとするので、外部に漏れることはない。 ＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムは、中間サーバーや各システムとの接続に専用回線を用いるため、外部に漏れることはない。 ＜システム基盤（個人基本）における措置＞ システム基盤（個人基本）との接続に専用回線を用いるため、外部に漏れることはない。 ＜システム外の措置＞ 窓口等で個人番号の提示を受けるときは、法令で定める本人確認を行ったうえで受付を行う。
リスクへの対策は十分か	[特に力を入れている] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	1 母子保健情報システムは、当該事務で使用する部署の職員のみが当該情報にアクセスし、利用できる仕組みとする。 2 システム基盤（個人基本）との連携は、住民基本台帳に関する情報連携に限定する。 3 システム基盤（団体内統合宛名）との連携は、番号制度に伴う、個人特定に必要な範囲に限定する。	
事務で使用するその他のシステムにおける措置の内容	―	
その他の措置の内容	―	
リスクへの対策は十分か	[特に力を入れている]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	システムを利用できる職員を限定し、個人に交付されるICカード及びPINコードによる認証を実施する。 また、業務に応じて各ユーザの操作権限を制限する。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	1 発効管理 ・認証サーバーにおいて、職員ごとに、必要最小限の権限が付与されるよう管理する。 ・アクセス権限の付与を行う際、実施手順に基づき、業務主管部門（Ⅱ．2．⑥事務担当部署）及びシステム保守担当部門（保健福祉局保健所健康企画課）が指定する対象者及び権限について、システム担当者が設定を行うこととする。 2 失効管理 人事異動等によりアクセス権に変更が生じた場合は、実施手順に基づき、業務主管部門の指示のもと、システム担当者が速やかに失効手続きを行うこととする。	
アクセス権限の管理	[行っている]	＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	1 アクセス権限の付与者一覧を作成し、アクセス権限の変更がある都度、更新を行う。 2 機器利用課の職員名簿と、アクセス権限付与者一覧を突合し、その都度、失効手続きを行う。	
特定個人情報の使用の記録	[記録を残している]	＜選択肢＞ 1）記録を残している 2）記録を残していない
具体的な方法	システム操作記録として、いつ、どのユーザーが、誰の情報を、参照・更新したか、アクセスログを記録する。	
その他の措置の内容	1 システムが利用できる端末については、勝手に設定を変更できないよう業務主管部門にて管理する。 2 指定された端末以外からアクセスできないよう、業務主管部門にて制御する。 3 システム使用中以外は必ずログオフを行う旨、実施手順に記載する。	
リスクへの対策は十分か	[特に力を入れている]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク3： 従業者が事務外で使用するリスク	
リスクに対する措置の内容	システム操作記録を取得していることを周知して、定期的に本来の目的以外の用途で使用することのないよう、注意喚起を行う。
リスクへの対策は十分か	[　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	1　システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 2　セキュリティ実施手順に業務主管部門の承認を得なければ、情報の複製は認められない仕組みとする。
リスクへの対策は十分か	[　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
1　一定時間操作が無い場合は、自動的にログアウトする。 2　スクリーンセーバーを利用して、長時間にわたり個人情報を表示させない。 3　端末のディスプレイを、来庁者から見えない位置に置く。 4　画面のハードコピーの取得は、事務処理に必要となる範囲にとどめる。	

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	契約毎に被指名者選考委員会を開いて審議し、指名見積参加者選考調書に記録する。審査基準は札幌市役務契約事務取扱要領および札幌市競争入札参加資格審査等取扱要領による。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法	サーバー室への入退室は従業者に配布するICカードにより制限し、不正な侵入を防止する。 また、端末機の操作者ごとにアクセス権限を設定し、利用可能なファイルを制限する等の方法を定める。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	・システムの改修・保守作業を行う際は、事前に携わる作業要員の氏名及び所属を記載した作業報告を提出する。 ・システム操作記録として、いつ、どの操作者が、誰の情報を参照・更新したかアクセスログを記録する。	
特定個人情報の提供ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	サーバー室および事務室からの情報の持ち出し禁止を仕様書に明記する。また、セキュリティ保全の対策状況について定期的に報告させる。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	サーバー室および事務室からの情報の持ち出し禁止を仕様書に明記する。また、セキュリティ保全の対策状況について定期的に報告させる。	
特定個人情報の消去ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	サーバー室および事務室からの情報の持ち出しは禁止する。 委託先が特定個人情報を消去する場合は、本市の指示に基づき実施する。	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
規定の内容	個人情報取扱注意事項として以下を契約書に明記する。 1　個人情報の保護 2　複写、複製の禁止 3　目的外使用の禁止 4　情報の返還	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	委託先に対し、業務委託契約書における遵守事項を再委託先に周知徹底し遵守させる。 セキュリティ保全状況に関する報告を定期的に提示させる。	
その他の措置の内容	―	
リスクへの対策は十分か	[　特に力を入れている　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
―		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ ]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[ ]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続	[　] 接続しない（入手）　[　] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	＜札幌市における措置＞情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、本市の各業務システムから、情報提供ネットワークシステム側へのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 2　中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法別表第二及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、本市の各業務システムから、情報提供ネットワークシステム側へのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー･プラットフォームにおける措置＞ 1　中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 2　中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、本市の各業務システムから、情報提供ネットワークシステム側へのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 情報提供ネットワークシステムとの情報連携は、システム基盤（市中間サーバー）を通じて、閉鎖された専用回線により通信を行う。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 2　既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 3　情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 4　中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい･紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー･プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、情報提供ネットワークシステム側から、本市の各業務システムへのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 2　情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 3　特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 4　中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、情報提供ネットワークシステム側から、本市の各業務システムへのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 2　中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー･プラットフォームにおける措置＞ 1　中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 2　中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 3　中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜札幌市における措置＞ 1　誤った情報を提供・移転してしまうリスクへの措置 ①　システム操作者は特定個人情報の入力結果に誤りがないか、必ず確認を行う。 ②　情報を提供・移転するファイルはシステム上で形式が定義されており、定義された情報以外は連携されない。 ③　システムによるエラーチェックとして、入力内容や計算内容のチェックが行われている。 2　誤った相手に提供・移転してしまうリスクへの措置 ①　本市の情報システム部門に事前協議を行い、承認を得たうえで、システム機能でどの相手システムと情報連携するかが定義されたもの以外は連携されない。 ②　管理されたネットワーク上で行われる、システム処理による通信により、特定個人情報の提供・移転が行われるため、誤った相手への提供・移転は行われない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 2　情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 3　情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置
＜札幌市における措置＞ 情報提供ネットワークシステムとの連携は、中間サーバー・プラットフォームが行う構成となっており、情報提供ネットワークシステム側から、本市の各業務システムへのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 1　中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 2　情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー･プラットフォームにおける措置＞ 1　中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 2　中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 3　中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 4　特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[特に力を入れて整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[特に力を入れて整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[特に力を入れて周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[特に力を入れて行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜札幌市における措置＞ 1 サーバー室は、必要時以外は常に施錠し、鍵は業務主管部門の所属長が管理している。また、入室できる者を制限することで不正な侵入を防止するとともに、入退室の記録を残す。 2 磁気ディスクやドキュメント類は施錠可能な保管庫で保存している。 3 電気通信装置（ルータ・HUB）は施錠可能なラックに設置している。 ＜中間サーバー・プラットフォームにおける措置＞ 中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
⑥技術的対策	[特に力を入れて行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜札幌市における措置＞ 1 コンピュータウイルス監視ソフトを使用し、サーバー・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。併せて、端末機及びサーバー機のハードディスクドライブの全ファイルのウイルススキャンを毎週1回、自動実行する。 2 本市の情報セキュリティに関する規程に基づき、ネットワーク管理に係る手順等を整備するとともに、機器を設置する際はファイアウォールを敷設することとしている。 ＜中間サーバー・プラットフォームにおける措置＞ 1 中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 2 中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 3 導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	
⑦バックアップ	[特に力を入れて行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[特に力を入れて行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容	－	
再発防止策の内容	－	
⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	生存する市民の個人番号と同様に管理する。	
その他の措置の内容	－	
リスクへの対策は十分か	[特に力を入れている]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	対象者に関する情報は、住基情報と定期的に同期するため、古い情報のまま保管されるリスクはない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	＜選択肢＞ 1）定めている 2）定めていない
手順の内容	1 磁気ディスクの廃棄時は、内容の復元ができないように消去または物理的破砕等を行う。 2 札幌市が定めた保管期間を経過した帳票及び申告書等の廃棄時には、内容が判読できないよう、焼却もしくは裁断することとする。	
その他の措置の内容	－	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
－		