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	
（1）住民基本台帳ファイル	
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	・窓口における届出人の本人確認を厳格に行う。 ・住所異動届の際に、届書の記載内容、対象者の特定に誤りがないか、窓口で確認を行う。また、市外転入時には、転出証明書の記載内容も併せて確認を行う。 ・住基法第９条第２項に基づく通知（※）等、職権で住民票に記載・修正・消除を行う際に、事前に書類審査を行い、対象者、記載内容に誤りがないか確認する。 ※住基法第９条第２項に基づく通知　…　市町村の住民以外の者について戸籍に関する届書の受理等をしたことにより、住所地で住民票の記載等が必要になった場合、当該市町村長からその者の住所がある市町村長に対して行う当該記載等をすべき事項の通知 ・届書の内容を既存住基システムに入力後、審査者が、異動届の記載と入力内容に相違がないか、対象者に誤りがないかについて、出力された審査リストに基づき、照合を行う。また、入力内容が多い処理（市外転入等）については、複数の職員によって審査を行う。
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	・届書に記載されている項目以外は、既存住基システムの入力を行えない仕組みとなっている。
その他の措置の内容	・窓口の受付、入力方法についての運用を、全市共通のマニュアルで定めている。
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	・住所異動届（郵送での転出届を除く。）は統一様式を使用し、住基法に基づく届出であることを明らかにする。 ・届書の内容を既存住基システムに入力後、適切な届出による入力であるか、審査者が照合を行う。 ・システムを利用できる職員を限定し、ユーザIDによる識別と認証用トークンに表示されたパスワード（約30秒ごとに変化する）、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。
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	
入手の際の本人確認の措置の内容	個人番号カード又は通知カードと身分証明書の提示を受けることなどにより、必ず本人確認を行う。
個人番号の真正性確認の措置の内容	個人番号カード又は通知カードと身分証明書の提示を受け、登録済みの基本4情報（氏名・住所・性別・生年月日）と差異がないか比較することにより、個人番号の真正性を確認する。
特定個人情報の正確性確保の措置の内容	1　入手の各段階で本人確認を行う。 2　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。 3　業務に関係のない職員が特定個人情報を変更したりすることがないよう、システムを利用できる職員を限定する。
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
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	・住民からの届書等は、入力・審査が完了したら、鍵付の書庫に保管する。 ・既存住基システムは、連携を行うシステム間において閉鎖された専用回線により通信を行うため、回線に接続されていない相手先への情報の提供・移転は行われないことがシステム上担保される。
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
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	・庁内における情報連携及び宛名情報の保存は、システム基盤において行うこととなっており、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なっている。 ・システム基盤で保存される情報は、本市内部で共通して使用する最低限の項目のみとしている。
事務で使用するその他のシステムにおける措置の内容	・既存住基システムと市町村CS間では、法令に基づく事務で使用する情報以外のものとの紐付けは行わない仕様となっている。 ・本市内部の他システムについても、システム基盤を介して連携することとし、既存住記システムと直接のネットワーク接続を行わない。 ・本市で策定している既存住基システムにおけるセキュリティ実施手順（以下「実施手順」という。）により、不要なネットワークとの接続が禁止されている。
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
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、ユーザIDによる識別と認証用トークンに表示されたパスワード（約30秒ごとに変化する）、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 ① 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。 ② 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」の所属長）及びシステム保守担当部門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。 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はシステム部門に対して、速やかに失効の申請を行う。
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	・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、更新を行っている。 ・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、失効申請を行っている。
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している。
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システム部門で管理している。 2 指定された端末以外からアクセスできないよう、システム部門で制御している。 3 システム使用中以外は必ずログオフを行う。
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： 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	アクセスログを記録していることを周知し、定期的に事務外で使用しないよう注意喚起を行っている。
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： 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なっている。 2 セキュリティ実施手順にシステム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なっている。
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

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
・一定時間操作が無い場合は、自動的にログアウトする。 ・スクリーンセーバを利用して、長時間にわたり本人確認情報を表示させない。 ・端末のディスプレイを、来庁者から見えない位置に置く。 ・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	札幌市が規定する特定個人情報取扱安全管理基準に適合しているか予め確認して委託契約を締結している。	
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	①特定個人情報を取り扱う従業者の名簿を提出させる。 ②電子計算機等のアクセス権限を設定し、アクセスできる従業者を限定させる。 ③サーバ室や事務室の入退室を従業者に配布しているICカードにより制限し不正な侵入を防止している。 ④端末機の操作者ごとにフォルダへの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	特定個人情報を取り扱う電子計算機等では、従業者の利用状況をアクセスログとして記録し、保管している。 また、システム操作記録による記録を残している。また、データベースへの接続監視を行い、30分毎に担当職員へメールで監視状況が通知されるようになっており、いつ・だれが・どのデータベースに・どのようなアクセスをしたかを把握できるようになっている。	
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	（内容） 当該委託業務の契約書では、「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めている。 （確認方法） この特記事項の中で、第三者への提供の禁止を規定している。また、遵守内容について定期的に報告させている。	
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	（内容） 当該委託業務の契約書では、「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めている。 （確認方法） この特記事項の中で、札幌市の指定する手段で特定個人情報等の受渡しや確認を行うことを規定している。また遵守内容について定期的に報告させている。	
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	（内容） 当該委託業務の契約書では、「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めている。 （確認方法） この特記事項の中で、札幌市の指定する手段で消去し、その内容を記録した書面で報告することを規定している。	
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	（内容） 当該委託業務の契約書では、「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めている。 （確認方法） この特記事項の中で、札幌市の指定する手段で消去し、その内容を記録した書面で報告することを規定している。	
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	当該委託業務の契約書では、「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めている。この特記事項の中で、再委託するときは必ず札幌市の許諾を得ることと規定している。その際には、再委託先が札幌市の規定する特定個人情報取扱安全管理基準に適合しているか予め確認して許諾することと規定している。 また、再委託先における特定個人情報等の取扱状況についても定期的に報告させている。	
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	[　　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	・特定個人情報（個人番号・4情報等）の提供・移転を行う際に、全ての提供・移転記録（提供・移転日時、操作者等）をシステム上で管理し、7年間保存する。	
特定個人情報の提供・移転に関するルール	[　　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	・個人情報（特定個人情報を含む。）の提供・移転に当たり、デ）デジタル企画課に事前協議を行い、承認を得たもののみ情報提供及び移転を認める旨、本市の住民基本台帳ファイル利用要領（平成5年3月3日総務局長決裁）によって定めている。 ・個人情報の提供・移転を行う場合は、デ）デジタル企画課の事前協議において、本市住民基本台帳ファイル利用要領を遵守した提供・移転であるか、審査・確認を行っている。	
その他の措置の内容	1 「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を管理し、情報の持ち出しを制限する。 2　システムにより自動化されている情報の提供・移転処理以外で、情報の提供・移転を行う場合は、情報システム部門の職員が立会う。	
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：　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	・札幌市CS、システム基盤ともに、閉鎖された専用回線により通信を行うため、回線に接続されていない相手先への情報の提供・移転は行われないことがシステム上担保される。 ・実施手順及び運用作業・申請手順書に基づいて、特定個人情報を含む全ての個人情報の提供・移転の際には、依頼文による事前手続きを必要とするとともに、総）システム管理課長の承認を受けている。	
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：　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	（誤った情報を提供・移転してしまうリスクへの措置） ・既存住基システムに入力した特定個人情報の内容に相違がないか、必ず審査を行う。 ・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、定義された形式の情報以外は連携されない。 ・論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする。）により不正と判断された情報については、連携処理がストップするような仕組みとなっている。 （誤った相手に提供・移転してしまうリスクへの措置） ・札幌市CS、システム基盤ともに、閉鎖された専用回線により通信を行うため、回線に接続されていない相手先への情報の提供・移転は行われないことがシステム上担保されている。	
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
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	
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： 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	
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： 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	
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	
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　情報提供の要求があった際には、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する機能が備わっている。 2　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、照会内容に対応した情報のみを自動で生成して送付する機能が備わっている。また、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け取ってから提供する機能が備わっている。これらの機能により、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　機微情報（DV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することで、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　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、操作内容が記録されるため、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。
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・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 情報提供ネットワークシステムに情報を送信する際は、情報が暗号化される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、操作内容が記録されるため、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･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 中間サーバーと地方自治体等との間については、VPN（仮想プライベートネットワーク）等の技術を利用し、地方自治体等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・プラットフォームの事業者及びクラウドサービス事業者が、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することで、不適切な方法での情報提供を行えないようにしている。
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、決められたファイル形式以外では情報を提供・移転できない仕組みになっている。 ③ システムが、入力内容や計算内容に誤りがないかチェックしている。 2 誤った相手に提供・移転してしまうリスクへの措置 ① 札幌市の情報システム部門に事前協議を行い、承認を得た情報連携先とだけ連携できる仕組みになっている。 ② 誤った相手へ提供・移転しないよう、特定個人情報の提供・移転は管理されたネットワーク内で行う。 ＜中間サーバー・ソフトウェアにおける措置＞ 1 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、照会内容に対応した情報のみを自動で生成して送付する機能が備わっている。また、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け取ってから提供する機能が備わっている。これらの機能により、誤った相手へ特定個人情報を提供するリスクに対応している。 2 情報提供データベースへ情報が登録される際には、決められた形式のファイルであるかをチェックする機能が備わっている。また情報提供データベースに登録された情報の内容は端末の画面で確認することができる。これらにより、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内の副本データを既存業務システム内の正本データと照合するためのデータを出力する機能を有しており、提供する特定個人情報に誤りがないか確認することができる。 （※）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	
－	

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	[十分に整備している]	＜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	[十分に整備している]	＜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	[十分に周知している]	＜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	[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
具体的な対策の内容	＜札幌市における措置＞ 1　サーバ室は、機械による入退室管理設備を設置し、入退室カード（ICカード）を貸与された者でないと入室できない。また、入退室の記録は保存され、監視カメラも設置している。 2　磁気ディスクや書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＞ 1　中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 2　事前に申請し承認されてない物品、記憶媒体、通信機器などを所持し、持出持込することがないよう、警備員などにより確認している。 ＜標準準拠システム連携基盤における措置＞ ガバメントクラウドへの接続は閉鎖された専用線であり外部からの侵入は物理的に不可能となっている。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。	

⑥技術的対策		[　　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
	具体的な対策の内容	＜札幌市における措置＞ 1　サーバ室は、機械による入退室管理設備を設置し、入退室カード（ICカード）を貸与された者でないと入室できない。また、入退室の記録は保存され、監視カメラも設置している。 2　磁気ディスクや書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＞ 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、ウイルスパターンファイルを更新する。 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を適用する。 4　中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 5　中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 6　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。 7　中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ＜標準準拠システム連携基盤における措置＞ ①共通標準仕様書で定められた通信のセキュリティレベルを実現する。 ②ファイル連携においてはオブジェクトストレージを利用し、暗号化と複合化を行い管理する。 ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDoS対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、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。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ		[　　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
⑧事故発生時手順の策定・周知		[　　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
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保管し、死亡による消除後は住民基本台帳法施行令第34条第1項に基づき、150年間保管する。
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

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	・住民票に対する修正等が発生する場合、複数の職員によるチェックを行うことにより、処理漏れを防止する。 ・住基法第14条第1項（住民基本台帳の正確な記録を確保するための措置）の規定に基づき調査等の必要な措置を実施することにより、住民基本台帳の正確な記録を確保する。
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： 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	・除票は住民基本台帳法施行令第34条第1項に定める保存期間（消除から150年間）、異動データは当該異動処理から1年間を経過した情報を、毎年1回システム上消去する仕組みを作っている。 ・磁気ディスクの廃棄時は、要領・手順書に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、物理的粉砕等を行うことにより、内容を読み出すことができないようにする。 ・届書及び帳票の紙媒体の情報については、法令及び例規に基づき、保管及び廃棄を行うこととしている。廃棄時には、要領・手順書等に基づき、裁断、溶解等を行うとともに、帳票管理簿等にその記録を残す。 ＜標準準拠システム連携基盤における措置＞ 格納期限が経過した連携ファイルは消去する。 ＜ガバメントクラウドにおける措置＞ データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。
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	
―	

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	
（2）本人確認情報ファイル	
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	本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。
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	・平成14年6月10日総務省告示第334号第6－6（本人確認情報の通知及び記録）により札幌市CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ等）の指定を必須とする。
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
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	本人確認情報の入手元を既存住基システムに限定する。
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	
入手の際の本人確認の措置の内容	特定個人情報の入手元である既存住基システムへの情報の登録の際、個人番号カード又は通知カードと身分証明書の提示を受けることなどにより、必ず本人確認を行う。
個人番号の真正性確認の措置の内容	個人番号カード又は通知カードと身分証明書の提示を受け、登録済みの基本4情報（氏名・住所・性別・生年月日）と差異がないか比較することにより、個人番号の真正性を確認する。
特定個人情報の正確性確保の措置の内容	・既存住基システムに特定個人情報の入力を行った場合、入力を行った者以外の職員により審査を行う。また、入力内容が多い処理（市外転入等）については、複数の職員によって審査を行う。 ・既存住基システムで入力を行った異動情報は、事後の検証のため、一定期間保存される。
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
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	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※札幌市CSのサーバ上で稼動するアプリケーション。札幌市CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、札幌市CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する。）を内蔵している。
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
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	札幌市CSと宛名管理システム（システム基盤の各宛名システム）間の接続は行わない。
事務で使用するその他のシステムにおける措置の内容	・庁内システムにおける札幌市CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと札幌市CS間では、法令に基づく事務で使用する情報以外のものとの紐付けは行わない仕様となっている。 ・札幌市CSのサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず、また、札幌市CSが設置されたセグメントにある通信機器は入退室者を制限したマシンルーム内にあり、さらに、施錠可能なラック内に設置している。 ・システム管理部門が、ラックの鍵の厳格な利用手順を定め、別に管理している。
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
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	住基ネットへアクセスするための端末（統合端末）は、生体認証による操作者認証を行っている。
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	照合ID（統合端末内のアプリケーションにログインするためのID）と操作者ID（統合端末内の各アプリケーションを利用するために付与された権限の管理ID）の発行・失効については、デ）住民情報課が一元的に管理することとしており、区の戸籍住民課で異動・退職等が発生した場合には、デ）住民情報課に申請を行った上で発行・失効処理が行われる仕組みとしている。また、照合IDと操作者IDを操作権限管理簿で管理し、随時チェックを行っている。
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	・操作者の業務内容に応じた操作権限を付与している。 ・不正アクセスや不正利用を分析するために、札幌市CS及び統合端末の操作履歴を7年間保管している。
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	・本人確認情報を扱うシステム（札幌市CS及び統合端末）のアクセスログを記録する。 ・システム管理部門が、週に1回、時間外の不正アクセスがないかをチェックし、適切な機器利用を確保している。また、調査・確認が必要な場合にはヒアリング等の実地調査を実施する。
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
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	・本人確認情報を扱うシステム（札幌市CS及び統合端末）のアクセスログを記録する。 ・総）システム管理課が、週に1回、時間外の不正アクセスがないかをチェックし、適切な機器利用を確保している。また、調査・確認が必要な場合にはヒアリング等の実地調査を実施する。 ・システム利用職員への研修において、目的外利用の禁止等について指導する。 ・業務委託契約書で「特定個人情報等の取扱いに関する特記事項」を規定し、委託先にセキュリティ対策を講じさせている。
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： 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	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なっている。
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

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
・長時間にわたり本人確認情報を表示させないため、5分間入力がなかった場合、スクリーンセーバが起動し、解除にもパスワード入力を求めるようOSを設定している。 ・統合端末から離席する際には業務アプリケーションをログオフする。 ・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・業務目的以外の画面のハードコピーを禁止している。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得ることとしている。

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	札幌市が規定する特定個人情報取扱安全管理基準に適合しているか予め確認して委託契約を締結している。	
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	①特定個人情報を取り扱う従業者の名簿を提出させる。 ②電子計算機等のアクセス権限を設定し、アクセスできる従業者を限定させる。 ③サーバ室や事務室の入退室を従業者に配布しているICカードにより制限し不正な侵入を防止している。 ④端末機の操作者ごとにフォルダへの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	・操作履歴を7年間保存している。（委託する特定個人情報ファイルを取り扱う業務は、すべて操作履歴が残る作業である。）	
特定個人情報の提供ルール	[　定めていない　]	＜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	特定個人情報を委託先に提供することはない。	
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	特定個人情報を委託先に提供することはない。	
特定個人情報の消去ルール	[　定めていない　]	＜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	特定個人情報を委託先に提供することはない。	
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	当該委託業務の契約書では「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めており、以下の事項を規定している。 1　秘密保持義務 2　事業所内からの特定個人情報の持ち出しの禁止 3　特定個人情報の目的外利用の禁止 4　再委託における条件 5　漏えい事案等が発生した場合の委託先の責任 6　委託契約終了後の特定個人情報の返却又は廃棄 7　特定個人情報を取り扱う従業者の明確化 8　従業者に対する監督・教育、契約内容の遵守状況についての報告 9　必要があると認めるときは実地の監査、調査等を行うこと	
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	[　再委託していない　]	＜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	－	
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	[　　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	特定個人情報（個人番号、4情報等）の提供・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、7年分保存する。なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。
特定個人情報の提供・移転に関するルール	[　　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	・提供先は都道府県及び機構に限られる。 ・相手方（都道府県サーバ）と札幌市CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。
その他の措置の内容	・「サーバ室等への入室権限」及び「特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を適切に管理する。 ・都道府県サーバとの整合性検査時、媒体を用いて情報を連携する場合には、権限を有する職員が行う。
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： 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	・提供先は都道府県及び機構に限られる。 ・相手方（都道府県サーバ）と札幌市CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。 ・また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。
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： 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	・提供先は都道府県及び機構に限られるため、システム上、提供すべき情報のみを出力することを担保する。 ・また、本人確認情報に変更が生じた際には、札幌市CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・相手方（都道府県サーバ）と札幌市CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。
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
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	
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： 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	
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： 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	
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	
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	
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	
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	
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
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	

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	[十分に整備している]	＜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	[十分に整備している]	＜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	[十分に周知している]	＜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	[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
具体的な対策の内容	・札幌市CSが設置されているサーバ室は、機械による入退室管理設備を設置し、入退室カード（ICカード）を貸与された者でないと入室できない。また、入退室の記録は保存され、監視カメラも設置している。 ・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。 ・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。	
⑥技術的対策	[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
具体的な対策の内容	・ファイアウォールを設置し、必要最小限の通信のみ許可されるように設定し、毎月通信ログをチェックしている。なお、インターネットとは物理的に分離している。 ・ウィルス対策ソフトを使用し、機構からのセキュリティ情報（脆弱性情報、セキュリティ更新プログラムの適用、ウィルスパターンファイルの適用等）に従い、必要な措置を講じている。	
⑦バックアップ	[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
⑧事故発生時手順の策定・周知	[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
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	生存する個人の個人番号とともに、死亡による消除後、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）保管する。	
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

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	既存住基システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
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： 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	・システム上、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）を経過した住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報を消去する仕組みとする。 ・磁気ディスクの廃棄時は、情報セキュリティ技術対策基準、情報セキュリティ実施手順に基づき、専用ソフトウェアによる消去又は媒体の物理的破壊を行うとともに、磁気ディスクの管理台帳にその記録を残す。 ・帳票の廃棄時には、帳票管理要領に基づき、内容が判読できないよう、焼却又は裁断することとし、帳票管理簿にその記録を残す。	
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		
―		

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	
（3）送付先情報ファイル	
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	送付先情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出／申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。なお、統合端末から直接情報を登録する際にも同様の措置を講ずる。
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	・平成14年6月10日総務省告示第334号第6－6（本人確認情報の通知及び記録）により市町村CSにおいて既存住基システムを通じて入手することととされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ等）の指定を必須とする。
その他の措置の内容	－ ＜選択肢＞
リスクへの対策は十分か	[　十分である　] 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	送付先情報の入手元を既存住基システムに限定する。
リスクへの対策は十分か	[　十分である　] 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	特定個人情報の入手元である既存住基システムへの情報の登録の際、個人番号カード又は通知カードと身分証明書の提示を受けることなどにより、必ず本人確認を行う。
個人番号の真正性確認の措置の内容	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応する個人番号を適切に取得できることを、システムにより担保する。
特定個人情報の正確性確保の措置の内容	既存住基システムにおいて正確性が確保された送付先情報を適切に受信できることをシステムにより担保する。 なお、送付先情報ファイルは、既存住基システムから入手後、個人番号カード管理システムに送付先情報を送付した時点で役割を終える（不要となる）ため、送付後速やかに札幌市CSから削除する。 そのため、入手から削除までのサイクルがごく短期間であることから、入手から削除の間の正確性を維持するための特段の対策は講じない。
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　] 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	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※札幌市CSのサーバ上で稼動するアプリケーション。札幌市CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、札幌市CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
リスクへの対策は十分か	[　十分である　] 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	札幌市CSと宛名管理システム（システム基盤の各宛名システム）間の接続は行わない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムにおける札幌市CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと札幌市CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。 なお、札幌市CSのサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず、また、札幌市CSが設置されたセグメントにある通信機器は入退室者を制限したマシンルーム内にあり、さらに、施錠可能なラック内に設置している。なお、ラックの鍵も厳格な利用手順を定め別に管理している。	
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
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	住基ネットへアクセスするための端末（統合端末）は、生体認証による操作者認証を行っている。	
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	照合ID（統合端末内のアプリケーションにログインするためのID）と操作者ID（統合端末内の各アプリケーションを利用するために付与された権限の管理ID）の発行・失効については、デ）住民情報課が一元的に管理することとしており、区の戸籍住民課で異動・退職等が発生した場合には、デ）住民情報課に申請を行った上で発行・失効処理が行われる仕組みとしている。また、照合IDと操作者IDを操作権限管理簿で管理し、随時チェックを行っている。	
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	・操作者の業務内容に応じた操作権限を付与している。 ・不正アクセスや不正利用を分析するために、札幌市CS及び統合端末の操作履歴を7年間保管している。	
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	・送付先情報を扱うシステム（札幌市CS及び統合端末）の操作履歴（操作ログ）を記録する。 ・システム管理部門が、週に1回、時間外の不正アクセスがないかをチェックし、適切な機器利用を確保している。また、調査・確認が必要な場合にはヒアリング等の実地調査を実施する。	
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
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	・送付先情報を扱うシステム（札幌市CS及び統合端末）のアクセスログを記録する。 ・システム管理部門が、週に1回、時間外の不正アクセスがないかをチェックし、適切な機器利用を確保している。また、調査・確認が必要な場合にはヒアリング等の実地調査を実施する。 ・システム利用職員への研修において、目的外利用の禁止等について指導する。 ・業務委託契約書で「特定個人情報等の取扱いに関する特記事項」を規定し、委託先にセキュリティ対策を講じさせている。	
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： 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	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なっている。	
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

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
・長時間にわたり本人確認情報を表示させないため、5分間入力がなかった場合、スクリーンセーバが起動し、解除にもパスワード入力を求めるようOSを設定している。 ・統合端末から離席する際には業務アプリケーションをログオフする。 ・統合端末のディスプレイを、来庁者から見えない位置に置く。 ・業務目的以外の画面のハードコピーを禁止している。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得ることとしている。

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	札幌市が規定する特定個人情報取扱安全管理基準に適合しているか予め確認して委託契約を締結している。	
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	①特定個人情報を取り扱う従業者の名簿を提出させる。 ②電子計算機等のアクセス権限を設定し、アクセスできる従業者を限定させる。 ③サーバ室や事務室の入退室を従業者に配布しているICカードにより制限し不正な侵入を防止している。 ④端末機の操作者ごとにフォルダへの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	・操作履歴を7年間保存している。（委託する特定個人情報ファイルを取り扱う業務は、すべて操作履歴が残る作業である。）	
特定個人情報の提供ルール	[　定めていない　]	＜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	特定個人情報を委託先に提供することはない。	
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	特定個人情報を委託先に提供することはない。	
特定個人情報の消去ルール	[　定めていない　]	＜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	特定個人情報を委託先に提供することはない。	
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	当該委託業務の契約書では「特定個人情報等の取扱いに関する特記事項」を遵守するよう定めており、以下の事項を規定している。 1　秘密保持義務 2　事業所内からの特定個人情報の持ち出しの禁止 3　特定個人情報の目的外利用の禁止 4　再委託における条件 5　漏えい事案等が発生した場合の委託先の責任 6　委託契約終了後の特定個人情報の返却又は廃棄 7　特定個人情報を取り扱う従業者の明確化 8　従業者に対する監督・教育、契約内容の遵守状況についての報告 9　必要があると認めるときは実地の監査、調査等を行うこと	
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	[　再委託していない　]	＜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	－	
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	［　　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	特定個人情報（個人番号、4情報等）の提供・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、7年分保存する。なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。	
特定個人情報の提供・移転に関するルール	［　　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	・提供先は機構に限られる。 ・相手方（個人番号カード管理システム）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。	
その他の措置の内容	・「サーバ室等への入室権限」及び「特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を適切に管理する。	
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	・提供先は機構に限られる。 ・相手方（個人番号カード管理システム）と札幌市CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。	
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：　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	・システム上、既存住基システムから入手した情報の内容に編集を加えず、適切に個人番号カード管理システムに提供することを担保する。 ・相手方（個人番号カード管理システム）と札幌市CSの間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上担保される。	
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
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	
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： 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	
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： 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	
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	
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	
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	
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	
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
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	

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	[十分に整備している]	＜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	[十分に整備している]	＜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	[十分に周知している]	＜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	[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
具体的な対策の内容	・札幌市CSが設置されているサーバ室は、機械による入退室管理設備を設置し、入退室カード（ICカード）を貸与された者でないと入室できない。また、入退室の記録は保存され、監視カメラも設置している。 ・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。 ・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。	
⑥技術的対策	[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
具体的な対策の内容	・ファイアウォールを設置し、必要最小限の通信のみ許可されるように設定し、毎月通信ログをチェックしている。なお、インターネットとは物理的に分離している。 ・ウィルス対策ソフトを使用し、機構からのセキュリティ情報（脆弱性情報、セキュリティ更新プログラムの適用、ウィルスパターンファイルの適用等）に従い、必要な措置を講じている。	
⑦バックアップ	[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
⑧事故発生時手順の策定・周知	[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
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	[保管していない]	＜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		
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

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	本特定個人情報ファイル（送付先情報ファイル）は、送付先情報の連携を行う必要が生じた都度作成／連携することとしており、システム上、連携後速やか（1営業日後）に削除する仕組みとする。 そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは少ない。
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	システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。
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	
送付先情報ファイルは、機構への特定個人情報の提供後、速やかに札幌市CSから削除される。その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない。	