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	
後期高齢者医療事務情報ファイル	
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	＜広域連合からの入手＞ 1　窓口端末における措置 ①入手元は、広域連合標準システムに限定されており、配信されるデータは広域連合及び本市において関連性や整合性のチェック(※)が行われていることが前提となるため、対象者以外の情報を入手することはない。 ②窓口端末における対象者の検索結果は、同一画面上に氏名、生年月日及び住所（以下「個人識別情報」という。）と個人番号を表示することによって、個人識別情報の確認を促し個人番号のみによる対象者の特定を行うことを抑止することで、誤った対象者を検索するリスクを軽減している。 ※ここでいう関連性・整合性チェックとは、既に個人番号が紐付いている(宛名番号が同じ)人に、以前と違う個人番号を紐付けようとした場合、又は個人番号が空欄の場合に、広域連合標準システムから確認リストが出力され、本市がその内容を確認することを指す。 ＜本人及び関係機関等（広域連合を除く）からの入手＞ 1　個人番号カード又は通知カード及び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。 2　他の行政機関等より特定個人情報を含む情報（被保険者資格情報、所得情報等）を入手する際、必要とされる対象者以外記載できない書類様式で照会等を行う。
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	＜広域連合からの入手＞ 1　窓口端末における措置 ①入手元は、広域連合標準システムに限定されており、配信されるデータは広域連合においてあらかじめ指定されたインターフェイス(※)によって配信されることが前提となるため、必要な情報以外を入手することはない。 ②被保険者等が申請書等に必要以上の情報を記載しないように、必要最低限の適切な項目のみを記載する様式としており、必要以上の情報を入手するリスクを軽減している。 ※指定されたインターフェイスとは、「後期高齢者医療広域連合電算処理システム外部インターフェイス仕様書」に記載されている広域連合標準システムと市町村の窓口端末間でやりとりされるデータ定義のことをいい、その定義に従った項目(法令等で定められた範囲)でなければ、広域連合標準システムからデータ配信ができない仕組みになっている。 ＜本人及び関係機関等（広域連合を除く）からの入手＞ 必要な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	＜窓口端末における措置＞ 1　特定個人情報の入手元は、広域連合標準システムに限定されており、指定されたインターフェイスでしか入手できないようシステムで制御している。 ＜後期高齢システムにおける措置＞ 1　手続に当たっては、個人番号の記載が必要であることを認識してもらった上で、申請書等を提出してもらう。これにより、本人が知らぬ間に個人番号を提出してしまうことを防止している。 2　紙媒体の申請等情報は、本人等が来庁して提出するか、直接札幌市に郵送するため、中間で詐取・奪取が行われるリスクは低い。 3　システムへアクセスできる職員と端末を限定している。 ＜国保・介護・後期　収納管理／滞納整理システムにおける措置＞ システムへアクセスできる職員と端末を限定している。 ＜システム基盤における措置＞ システムへアクセスできる職員と端末を限定している。 ＜住民基本台帳ネットワークシステム統合端末における措置＞ システムへアクセスできる職員と端末を限定している。 ＜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

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	＜広域連合からの入手＞ 窓口端末において広域連合から入手する情報は、本市において以下のとおり本人確認を行った上で広域連合に送信した情報に、広域連合が事務処理等を行った結果を付加して配信された情報である。 ＜本人及び関係機関等（広域連合を除く）からの入手＞ 個人番号カード又は通知カード及び身分証明書の提示などにより、必ず本人確認を行う。 他市町村等からは、他市町村等が番号法第16条に基づく本人確認を行って入手した情報が提供される。
個人番号の真正性確認の措置の内容	＜広域連合からの入手＞ 窓口端末において広域連合から入手する情報は、本市において以下のとおり真正性の確認を行った上で広域連合に送信した情報に、広域連合が事務処理等を行った結果を付加して配信された情報である。 ＜本人及び関係機関等（広域連合を除く）からの入手＞ 個人番号カード又は通知カード及び身分証明書の提示を受け、登録済みの宛名情報の基本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	＜広域連合からの入手＞ 広域連合においては本市の後期高齢システムと同様の宛名番号をキーとして個人識別情報を管理しており、宛名番号をキーとして必要なデータが配信されることをシステム上で担保することで正確性を確保している。 ＜本人及び関係機関等（広域連合を除く）からの入手＞ 1　入手の各段階で本人確認を行う。 2　職員が収集した情報に基づいて、不正確な情報があれば修正している。
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	＜窓口端末における措置＞ 1 本市の窓口端末は、広域連合標準システムにのみ接続され、接続にはLGWAN及び専用線を用いる。 2 本市の窓口端末と広域連合標準システムとの通信には、認証・通信内容の暗号化を実施している。 3 本市の窓口端末と広域連合標準システムとの専用ネットワークは、ウィルス対策ソフト、ファイアウォール等によって安全なシステム稼働環境を確保することにより、不適切な方法によってデータが漏えい・紛失することのリスクを軽減している。 4 ウィルス対策ソフトは自動でアップデートを行い、ファイアウォール等の設定変更が必要となった際は、広域連合が迅速に実施する。 5 窓口端末へのログイン時の職員認証において、個人番号利用事務の操作権限が付与されていない職員がログインした場合には、個人番号の表示、検索、更新ができない機能により、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 6 ログインを実施した職員・時刻等が記録されるため、その抑止効果として、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 ＜後期高齢システムにおける措置＞ 1 紙媒体及び電子媒体により提出された申請等情報は、鍵付きの保管庫で保管する。 2 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している。 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なっているので、外部に漏れることはない。 ＜国保・介護・後期 収納管理／滞納整理システム＞ 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なっているので、外部に漏れることはない。 ＜システム基盤における措置＞ 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なっているので、外部に漏れることはない。 ＜住民基本台帳ネットワークシステム統合端末における措置＞ 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なっているので、外部に漏れることはない。
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 後期高齢者医療業務に関する宛名情報は、システム基盤（社会保障宛名）に保存しており、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。 2 後期高齢者医療業務以外との情報連携は、番号法や条例などの関係法令で定められた必要な範囲に限定される仕組みとなっている。 3 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される仕組みとなっている。 4 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、個人の特定に必要な範囲に限定される仕組みとなっている。
事務で使用するその他のシステムにおける措置の内容	システム基盤（市中間サーバー）との連携は、番号法や条例などの関係法令で定められた団体間の情報連携に必要な範囲に限定される仕組みとなっている。
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： 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	＜窓口端末における措置＞ 1 窓口端末を利用する必要がある事務取扱担当者（※）を特定し、個人ごとにユーザIDを割り当て、パスワードによるユーザ認証を実施する。 2 なりすましによる不正を防止する観点から、共用のIDは利用しない。 3 窓口端末へのログイン時の認証において、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号の表示、検索、更新ができない機能により、不適切な操作等がされることのリスクを軽減している。 4 ログインしたまま放置せず、離席時にはログアウトすることやログインID、パスワードの使いまわしをしないことを徹底している。 ※事務取扱担当者とは、実際に窓口端末を操作し、特定個人情報等を取り扱う職員等を指す。 ＜後期高齢システム・国保・介護・後期 収納管理／滞納整理システムにおける措置＞ 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	＜窓口端末における措置＞ 1 発効管理 窓口端末を利用する必要がある事務取扱担当者を特定し、担当者ごとのアクセス権限の付与及びユーザIDの割当を、本市から広域連合に対して申請する。 2 失効管理 人事異動等によりアクセス権限に変更が生じた場合は、担当者ごとのアクセス権限及びユーザIDの削除を、本市から広域連合に対して速やかに申請する。 ＜後期高齢システム・国保・介護・後期 収納管理／滞納整理システムにおける措置＞ 1 発効管理 ① 認証サーバにおいて、職員の所属及び業務によりアクセス権限をパターン化することによって、必要最小限の権限が付与されるよう管理している。 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）から情報システム部門に対して申請を行う。 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情報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	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、更新を行っている。 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	＜窓口端末における措置＞ ・ログインを実施した職員・時刻・操作内容等を記録している。 ・広域連合において定期的に、記録の内容を確認し、不正な運用が行われていないかを点検する。 ・当該記録は一定期間保存する。 ＜後期高齢システム・国保・介護・後期　収納管理／滞納整理システムにおける措置＞ 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情報システム部門にて管理している。 2　指定された端末以外からアクセスできないよう、情報システム部門にて制御している。 3　システム使用中以外はログオフを行う。
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		1　外部記憶媒体へデータのコピーを原則禁止している。例外については、実施手順により定められている。 2　システムにより操作記録を取得していることを周知して、定期的に事務外で使用することに対する注意喚起を行っている。 3　会計年度任用職員等は、業務上知り得た情報の業務外利用禁止に関する条項を含む承諾書に署名する。
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		＜窓口端末における措置＞ 1　GUI（Graphical User Interface）によるデータ抽出機能(※)を窓口端末に搭載しないことにより、個人番号利用事務以外でデータが抽出されないようにしている。 2　ログインを実施した職員・時刻・操作内容等が記録され、広域連合において定期的に記録の内容が確認され、不正な運用が行われていないかが点検される。 ※　GUIによるデータ抽出機能とは、後期高齢者医療事務情報ファイルのデータベースからデータを抽出するに当たっての抽出条件等を、端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で端末上のハードディスク等にファイルを出力する機能のことを指す。 ＜後期高齢システム・国保・介護・後期　収納管理／滞納整理システムにおける措置＞ 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　情報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		[　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　事務処理に必要のない画面のハードコピーは取得しない。		

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あらかじ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。 また、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。 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	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		[　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　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あらかじ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		[　　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	[　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	＜広域連合への移転＞ ログインを実施した職員・時刻・操作内容等が記録される。 ＜広域連合以外への提供・移転＞ 特定個人情報の提供・移転が行われるシステム処理の実行記録が保管される。
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	＜広域連合への移転＞ 窓口端末における措置 （内容） 本市の窓口端末から広域連合標準システムへのデータ送信については、「一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について（通知）」において、同一部署内での内部利用の取扱いとするとされている。 （確認方法） 広域連合は本市の窓口端末から広域連合標準システムへのデータ送信に関する記録を確認し、不正なデータ配信が行われていないかを点検する。 ＜広域連合以外への提供・移転＞ （内容） 特定個人情報の提供・移転は、番号法や条例などの関係法令で定められた必要な範囲に限定される。 （確認方法） 個人番号利用事務監査を実施し、提供・移転が適切であるか確認している。
その他の措置の内容	1 「サーバー室等への入室権限」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・移転を行う作業等においては、情報システム部門の職員が立会う。 3 外部記憶媒体へデータのコピーを原則禁止している。例外については、実施手順により定められている。
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	＜広域連合への移転＞ 窓口端末における措置 ①本市の窓口端末からのデータ送信は、広域連合標準システム以外には行えない仕組みとなっている。また、窓口端末へのログインIDによる認可により、データ送信処理が可能な職員等を事務取扱担当者に限定している。 ②窓口端末へのログインを実施した職員・時刻・操作内容等及びデータ配信されたデータが広域連合標準システムに記録されるため、広域連合において広域連合標準システムの記録を調査することで、操作者個人を特定できる。 ③本市の窓口端末と広域連合標準システムとの接続にはLGWAN及び専用線を用いる。 ④本市の窓口端末と広域連合標準システムとの専用ネットワークは、ウィルス対策ソフト、ファイアウォール等によって安全なシステム稼働環境を確保している。 ＜広域連合以外への提供・移転＞ 1 誤った相手への提供・移転しないように、管理されたネットワーク上の通信を用いる。 2 システム処理によらない特定個人情報の提供・移転を行う必要がある場合は、業務主管部門からの事前手続きに基づいて、情報システム部門の管理の下に実施する。
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： 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	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、定義された形式の情報以外は連携されない。 ③ システムによって入力内容や計算内容のエラー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 誤った相手へ提供・移転しないように、管理されたネットワーク上の通信を用いる。 ＜広域連合への移転＞ 窓口端末における措置 ①本市の窓口端末と広域連合標準システムとの専用ネットワークは、ウィルス対策ソフト、ファイアウォール等によって安全なシステム稼働環境を確保することにより、誤った相手に移転するリスクを軽減している。 ②情報の移転先にあたる広域連合については、本市の後期高齢システムと同様の宛名番号をキーとして個人識別情報を管理しており、従来からその宛名番号で業務データと個人の紐付けを行っているため、本市から送信したデータが広域連合で誤って他人に紐付けされることはない。
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　情報提供ネットワークシステムが照会内容を照会許可用照合リストと照合し、情報提供許可証を発行した後で、情報照会を行う仕組みになっている。この仕組みにより、番号法上認められた情報連携以外の照会を拒否している。 2　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	[　　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： 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＞ 情報提供ネットワークシステムは、個人情報保護委員会との協議を経て総務大臣が設置・管理している。中間サーバーは、この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しか入手できない設計になっており、安全性を保っている。 ＜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、安全性を確保している。 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。
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	
リスクに対する措置の内容	情報提供ネットワークシステムは、個人情報保護委員会との協議を経て総務大臣が設置・管理している。中間サーバーは、この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しか入手できない設計になっている。そのため、正確な照会対象者の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	[　　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	＜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みを入手するため、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中間サーバーと地方自治体等については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が、運用、監視・障害対応等の業務をする際に、特定個人情報へ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　情報提供ネットワークシステムが照会内容を照会許可用照合リストと照合し、情報提供許可証を発行した後で、情報照会を行う仕組みになっている。この仕組みにより、番号法上認められた情報連携以外の照会を拒否している。 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　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保守・運用を行う事業者が、特定個人情報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。 ③ システムによる入力内容や計算内容のエラー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、承認を得る必要がある。また、情報連携が認められた相手システムとしか連携されない仕組みになっている。 ② 誤った相手へ提供・移転しないように、管理されたネットワーク上の通信を用いる。 ＜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	[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、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＞ 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	＜窓口端末における措置＞ ①窓口端末には、ウィルス対策ソフトを導入し、ウィルスパターンファイルは適時更新する。 ②不正アクセス防止策として、ファイアウォールを導入している。 ③オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。 ＜後期高齢システム・国保・介護・後期　収納管理／滞納整理システムにおける措置＞ 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、端末及びサーバー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。 ＜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		＜窓口端末における措置＞ 窓口端末に保管されるデータはない。 ＜後期高齢システム・国保・介護・後期　収納管理／滞納整理システムにおける措置＞ 保有する情報は異動があった場合に随時更新しており、更新していない場合は他の職員から判別可能にして複数人で確認できる体制をとっている。
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	＜窓口端末における措置＞ 窓口端末に保管されるデータはない。 ＜後期高齢システム・国保・介護・後期　収納管理／滞納整理システムにおける措置＞ 1　一定の保管期間を経過するなど業務上不要と判断される情報に関して、システムにて自動判別し、情報を消去する。 2　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又は物理的破砕等を行う。 3　本市及び広域連合が定めた一定の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、焼却又は裁断する。
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		
―		