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	
国民健康保険事務情報ファイル	
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	1　窓口対応では、個人番号カード又は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　他の行政機関等から特定個人情報を含む情報(被保険者資格情報、所得情報等)を入手する際は、必要な対象者以外記載できない書類様式で照会等を行う。 3　国保連合会からデータ連携で入手する情報は情報集約システムの情報に限定されており、配信される情報(データ)は国保連合会において対象者との関連性、妥当性及び整合性のチェックを行うことで対象者以外の情報の入手を防止する 4　オンライン申請では、身分証明書の画像添付により、対象者の本人確認を厳守し、また、対象者の被保険者番号の入力を必須とすることで、対象者以外の情報の入手を防止する。なお、対象者以外からの申請により入手した場合は、本人へ連絡し削除のうえ記録を残す。
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	1　必要な情報以外記載できない書類様式または申請フォームとする。 2　国保連合会からデータ連携で入手する情報は情報集約システムの情報に限定されており、配信される情報は国保連合会においてあらかじめ指定された情報(データ定義されている情報)であり、必要な情報以外は入手できない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	[　　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	＜国保業務における措置＞ 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。 4　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する。 ＜庁内各業務システムとの連携における措置＞ システムへアクセスできる職員と端末を限定している。また、本書において、事務ごとに特定個人情報の利用目的を詳細に定義し、これを公表することで、入手元が事前に使用目的を認識できる措置を講じている。 ＜国保連合会とのデータ連携における措置＞ 国保連合会からデータ連携で入手する情報は情報集約システムの情報に限定されており、情報のやり取りには専用線を用いるとともに、指定された情報しか入手できないよう制御されている。また、データ連携に使用するデータ連携用PCは、自動で処理される仕組みとなっており、端末は、施錠可能なラックで保管し、制限された利用者しかアクセスできない。
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身分証明書の提示や署名用電子証明書等により、必ず本人確認を行う。 他市町村等からは、他市町村等が法令で定める本人確認を行って入手した情報が提供される。 国保連合会からデータ連携で入手する情報は、本市において事前に本人確認を行った情報が情報集約システムから送信されるものである。
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身分証明書の提示を受け、既に登録された宛名情報の基本5情報(氏名、氏名の振り仮名、性別、生年月日、住所)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。なお、国保連合会からデータ連携で入手する情報に個人番号は記録されていない。
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　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。また、担当者以外の職員による再確認を行うことで、入力誤りを未然に防止する。 3　国保連合会からのデータ連携で入手する情報は、被保険者の異動前の市町村及び異動後の市町村で確認を行う。
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	＜国保業務における措置＞ 1 紙媒体及び電子媒体により提出された申請等情報は、鍵付きの保管庫や権限を付与された職員のみがアクセス可能なID・パスワード管理により保管する。 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。国保システム標準化後はガバメントクラウド上の閉域ネットワークでシステム間連携を行うため、外部に漏れることはない。 ＜業務間連携システムにおける措置＞ インターネットから隔離された専用回線を用いているため、外部への情報漏えいを防止している。 ＜国保連合会とのデータ連携における措置＞ データ連携用PCと情報集約システムの接続及びデータ連携用PCと国保システムの接続は専用線を用いているため外部に漏れることはない。
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
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 国民健康保険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。国民健康保険システム標準化後は、ガバメントクラウドに保存し、システム基盤（社会保障宛名）は使用しない。 2 国民健康保険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（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、番号制度に伴う、団体間の情報連携に必要な範囲に限定される仕組みになっている。
その他の措置の内容	＜国保連合会とのデータ連携＞ 情報集約システムからデータ連携用PCを通して受信する情報は、データ定義されており不要な情報を入手することはなく、かつ、国保システムで確認の上、情報を取り込む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
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	＜国保システム及び国保・介護・後期　収納管理／滞納整理システムにおける管理方法＞ 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。 ＜標準化後の国保システム及び統合収納・統合滞納システムにおける管理方法＞ システムを利用できる職員を限定し、ユーザIDによる識別とパスワード及びMFAデバイス等を利用した多要素認証を実施する。また、業務に応じて各ユーザの操作権限を制限する。 ＜国保連合会とのデータ連携＞ 1 データ連携用PCは、施錠可能なラックで保管し、アクセスできる職員を限定する。 2 国保総合PCは、利用できる職員を限定し、ユーザーIDとパスワードによる認証を実施する。 3 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。 4 国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことによって、特定個人情報が不正に使用されることのリスクを軽減している。 5 ログインしたまま端末を放置せず、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。 6 パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。
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	＜国保システム及び国保・介護・後期　収納管理／滞納整理システムにおける管理方法＞ 1　発効管理 ①　認証サーバーにおいて、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こととしている。国保システム標準化後は国保統括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こととしている。国保システム標準化後は国保統括部門に対して申請を行う。 ＜国保連合会とのデータ連携＞ 1　データ連携用PCのアクセス権限は、実施手順に基づき、業務主管部門が管理を行う。 2　国保総合PCのアクセス権限は、国保連合会の指示に基づき、業務主管部門が管理を行う。
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、失効させる。
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	1　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。 2　情報システム管理者は定期的又はセキュリティ上の問題が発生した際に、記録の内容と関連する書面の記録を照合して確認し、不正な運用が行われていないかを監査する。
その他の措置の内容		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　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。国民健康保険システム標準化後は国保統括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。 ＜国保連合会とのデータ連携＞ 1　データ連携用PCは、施錠可能なラックに保管されているため、不正に複製されにくい。 2　国保総合PCは、個人番号を利用しない仕組みであるため、不正に複製されにくい。 3　国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容が記録され、国保連合会においても定期的又はセキュリティ上の問題が発生した際に、記録の内容を確認し、不正な運用が行われていないかが監査される。
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：　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　外部記憶媒体へのデータのコピーを原則禁じている。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		［　　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　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。国保システム標準化後は国保統括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 3 住民が行ったオンライン申請のデータ等は、アクセス権限の設定により特定の職員のみがアクセスできるようシステムで管理する。 4 外部媒体へのデータのコピーを禁じている。仮にコピーしようとしたとしても、外部記憶媒体の利用制御システムにより、事前に登録した外部記憶媒体以外は書き込みができない。なお、業務上やむを得ずコピーする場合は、事前に所属長の承認を得たうえで行う。 5 外部記憶媒体内のデータは暗号化する。 ＜国保連合会とのデータ連携＞ 1　データ連携用PCは、施錠可能なラックに保管されているため、不正に複製されにくい。 2　国保総合PCは、個人番号を利用しない仕組みであるため、不正に複製されにくい。 3　国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容が記録され、国保連合会においても定期的又はセキュリティ上の問題が発生した際に、記録の内容を確認し、不正な運用が行われていないかが監査される。

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	【全事務共通】 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。 【国民健康保険業務の場合】 ①閲覧/更新権限を持つものは必要最小限とし、アカウント管理を行い、システム上で操作を制限している。 ②ログを取得し、必要に応じ不正な使用がないことを確認している 【情報集約システムの場合】 アクセス権限を付与する従業員数を必要最小限に制限し、付与するアクセス権限も必要最小限とすることを委託業者に遵守させる。 【医療保険者等向け中間サーバー等の場合】 ①取りまとめ機関の職員に許可された業務メニューのみ表示するよう制御している。 ②運用管理要領等にアクセス権限と事務の対応表を規定し、職員と臨時職員、取りまとめ機関と委託事業者の所属の別等により、実施できる事務の範囲を限定している。 ③アクセス権限と事務の対応表は随時見直しを行う。 ④パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。 【ガバメントクラウド移行作業時に関する措置】 ・移行作業に従事する者は、事前に指定された取扱従業者に限定し、付与するIDの権限及び数は当該業務に必要最小限とし、部外者のアクセスを制限することを委託先に遵守させることとしている。 ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている。
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	・システム操作の記録を残している。また、データベースへの接続監視を行い、一定時間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、誰が、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。 ・情報集約システムについては、アクセスログを記録し、定期的な点検を徹底させる。 医療保険者等向け中間サーバー等については、操作ログを中間サーバーで記録している。 操作ログは、セキュリティ上の問題が発生した際、又は必要なタイミングでチェックを行う。 【ガバメントクラウド移行作業時に関する措置】 ・移行作業に従事する者は、事前に指定された取扱従業者に限定し、付与するIDの権限及び数は当該業務に必要最小限とし、部外者のアクセスを制限することを委託先に遵守させることとしている。 ・移行作業にあたって、作業者以外は対象ファイルにアクセスできないようにし、リスク範囲を限定することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとして

		いる。 ・特定個人情報ファイルにアクセスする移行作業は二人で行う相互牽制の体制で実施することを委託先に遵守させることとしている。 ・特定個人情報等の取扱いに使用する電子計算機等については、アクセスログ等から従業者の利用状況を適切に記録し、保管することを委託先に遵守させることとしている。（再委託及び再々委託する場合も同様とする。）
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	（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。 ＜ガバメントクラウド移行作業時に関する措置＞ ・委託先で作成・使用したデータを削除した場合は、その日時及び消去の内容を記録した書面を作成させ、本市に報告させることとしている。
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	【全事務共通】 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		[　　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	【全事務共通】 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委託先から報告させている。 ・情報集約システムを、クラウド事業者が保有・管理する環境に設置する場合、設置場所のセキュリティ対策はクラウド事業者が実施することになるため、クラウド事業者は、次を満たすものとする。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 ・クラウド事業者が提供するクラウドサービスは、政府情報システムのためのセキュリティ評価制度（ISMAP）に基づくクラウドサービスリストに掲載されているものとする。 ・情報集約システムを、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ（OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc）をどのように確保したかを書面にて示した上で、許諾を得ること。 【医療保険者等向け中間サーバー等の場合】 医療保険者等向け中間サーバー等に係るデータセンター、ハードウェア、OS及びミドルウェア（以下「開発・運用環境」という。）は、取りまとめ機関等が自ら用意・設置するのではなく、開発・運用環境を賃貸する事業者（以下「クラウド事業者」という。）から借り受ける。クラウド事業者は以下の要件を満たしており、最先端のセキュリティ対策を講じている。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 クラウド事業者から借り受けた開発・運用環境内に、取りまとめ機関から委託された開発・運用保守業者が、医療保険者等向け中間サーバー等を構築する。 開発・運用保守業者は、①クラウド事業者が提示する責任共有モデル（クラウド事業者が保有・管理する開発・運用環境についてのそれぞれの責任の範囲を示したもの）を理解し、②OS、ミドルウェア及びシステムに対して、システム構築上及び運用上のセキュリティ（OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc）をどのように確保したかを書面にてクラウド事業者と取り交わし、③書面の内容についてさらに取りまとめ機関から許諾を得る。 なお、クラウド事業者が保有・管理する開発・運用環境を利用できる者は、取りまとめ機関及び開発・運用保守業者のみである。利用に当たっては、専用端末からのみ利用可能となる仕様としており、担当者ごとに必要最小限度の利用範囲を定め、ID・パスワード・生体認証によりログインを行い、さらにアクセスログの管理を徹底する。また、取りまとめ機関とクラウド事業者との契約は、個人情報の電子データを取り扱わない契約とする。 【ガバメントクラウド移行作業時に関する措置】 ・移行作業に従事する者は、事前に指定された取扱従業者に限定し、付与するIDの権限及び数は当該業務に必要最小限とし、部外者のアクセスを制限することを委託先に遵守させることとしている。 ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとしている。 ・特定個人情報等の取扱いに使用する電子計算機等については、アクセスログ等から従業者の利用状況を適切に記録し、保管することを委託先に遵守させることとしている。
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
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		

＜国保連合会における措置＞
・情報集約システムにおいて保有する特定個人情報が、インターネットに流出することを防止するため、情報集約システムはインターネットには接続できないようシステム面の措置を講じている。
・情報集約システムではUTM(コンピュータウイルスやハッキング等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。
・情報集約システムでは、ウイルス対策ソフトウェアを導入し、パターンファイルの更新を行う。
・導入しているOS及びミドルウェアについて、必要なセキュリティパッチの適用を行う。
・情報集約システムを国保連合会に設置し、設置場所への入退室記録管理、監視カメラによる監視及び施錠管理を行う。
・特定個人情報等を取扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。
・情報集約システムを使用して特定個人情報ファイルの複製等の操作が可能な職員を最小限に限定する。
・特定個人情報ファイルを電子記録媒体に複製する際には、不必要な複製を制限するため、事前に個人情報保護管理者の承認を得る。
・許可された電子記録媒体又は機器等以外については、使用又は接続を制限する。
・電子記録媒体は、媒体管理簿で管理し、保管庫に施錠保管する。電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。保管する必要がない使用済の電子記録媒体はシュレッダーで粉砕し破棄する。

＜取りまとめ機関における措置＞
支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。

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	特定個人情報の提供・移転の実行記録をシステムに保管する。 ＜ガバメントクラウドにおける措置＞ 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ついて【第3.0版】」(令和7年3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。
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	(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。国保システム標準化後は国保統括部門の職員が立ち会う。 3 外部記憶媒体へ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。 ＜ガバメントクラウドにおける措置＞ 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。外部ネットワークへの提供・移転は発生しない。
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	1 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。 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に基づいて、情報システム部門の管理の下に実施する。国保システム標準化後は、国保統括部門の管理の下に実施する。
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	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。
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	<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、本市の庁内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	[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、本市の庁内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	[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	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	[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、本市の庁内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、本市の庁内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	[　　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。 4 データ連携用PCは施錠可能なラックに設置している。 5 国保システム標準化後は、ガバメントクラウド上に保存される。 ＜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。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。 ＜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から調達し、サーバ等はクラウド事業者が保有・管理する環境に設置し、認可されたものだけが設置環境にアクセスできるよう適切な権限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 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。 ＜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。 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。 ＜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又はガバメントクラウド運用管理補助者は、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管理する。	
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	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。 データ連携用PCにある情報は、処理後、速やかに削除する。	
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	1 一定の保管期間を経過するなど札幌市が事務処理上不要と判断した情報は、システムにて自動判別し、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 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、焼却又は裁断する。 ＜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		
＜取りまとめ機関における措置＞ 支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務（オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供）」の特定個人情報保護評価を実施している。		