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	
税情報ファイル	
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、個人番号カードなど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。 2　電子申請時は、利用届出の情報と申告時に添付する電子証明書による本人確認を行うか、又は公的個人認証による電子署名が付与された申告データを受領することで、なりすましではないかの検証を行う。また、利用届出や申告データ等に記載された提出先のみが情報を入手できるようシステムで制御しており、対象者以外の情報を入手することはできない。
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とする。 2　審査システム（eLTAX）、国税連携システム（eLTAX）及び団体内統合宛名システムでは、各入手元からの情報に設定された提出先により、対象者以外の情報が入手できないようシステムで制御するとともに、法令等により定められた様式を用いることで、必要な情報以外を入手できないようシステムで制御している。
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：　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	＜税システム、国税連携システム、審査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告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　電子データで提出される申告情報等は、国税連携及び電子申告の専用回線を介して入手するため、中間で詐取・奪取が行われるリスクは低い。 3　紙媒体や電子記録媒体の申告等情報は、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。 ＜税宛名システム、税収納システム、税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。 ＜団体内統合宛名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。 マイナポータルから、届出先が本市である申請情報のみ取得するよう制御している。 ＜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	［　　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	個人番号カードなど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。 電子申告の場合には、公的個人認証等による電子署名が付与されたデータを受領し、署名検証を行う。 ※　国税庁等からは、当該団体等が番号法第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	個人番号カードなど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　審査システム（eLTAX）は、受領した情報をそのまま保管する。 3　システム基盤（団体内統合宛名システム）は、取得した情報をそのまま連携する。 4　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。 5　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	＜税システム、国税連携システム（eLTAX）、審査システム（eLTAX）における措置＞ 1　電子データで提出される申告情報等は、国税連携システム（eLTAX）及び審査システム（eLTAX）の専用回線を介して暗号化通信により入手しており、入手した電子データは庁内連携システムを通じて税システムに取り込むことで漏えい・紛失を防止している。 2　紙媒体及び電子媒体により提出された申告等情報は、鍵付きの保管庫で保管する。 3　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。 ＜税宛名システム、税収納システム、税滞納整理システムにおける措置＞ 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、マイナポータル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。 ＜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＞ 住民基本台帳ネットワークシステムとの接続に専用回線を用いるため、外部に漏れるリスクはことはない。
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　税業務に関する宛名情報は、システム基盤（税宛名）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　税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する。 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する。 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	システム基盤（市中間サーバ）との連携は、番号制度に伴う、他の地方公共団体等との情報連携に必要な範囲に限定する。
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	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い、一定時間端末を操作しなかった場合は再度パスワード認証を要求する設定としている。	
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： 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　外部記憶媒体へのコピーを禁止している。また、外部記憶媒体利用制御システムにより外部記憶媒体が作動しないようにすることで、情報の不正な持ち出しを禁止している。 2　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　臨時職員等に、業務上知り得た情報の業務外利用禁止と、違反した場合の罰則について周知している。	
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	［　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。 5　特定個人情報の目視が不要なシステム（税収納、税証明、税滞納整理）については、システム画面に個人番号を表示しない。		

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等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。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。 ＜システム基盤（税宛名）および各税システムの運用保守業務における措置＞ 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。 ＜eLTAXシステム認定委託先事業者における措置＞ システムを操作した履歴を記憶媒体に記録し、法令を順守していることを監査する等、その利用の正当性について確認することが技術基準に定められている。	
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		[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等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	特定個人情報の提供・移転の実行記録をシステムに保管する。紙で提供・移転を行う場合も、紙をシステム出力した時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	（内容） 札幌市内部の税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する。 （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。 3 外部記憶媒体へのコピーを禁止している。また、外部記憶媒体利用制御システムにより外部記憶媒体が作動しないようにすることで、情報の不正な持ち出しを禁止している。
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。
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。また、システム操作者によるオンラインでの誤入力を防止するため、入力が必要な業務をシステム化して減らしたほか、入力を誤りやすい業務については入力結果を後日に抜き出して再確認できるようにしている。更に研修やマニュアルを充実させるとともに、マニュアルを順守するよう徹底している。 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 誤った相手に情報を提供・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、相手システムとの情報連携について承認を得る必要がある。また、承認された相手システムとしか情報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。
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　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有しており、目的外の入手が行われないように備えている。 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内閣総理大臣が設置・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	＜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内閣総理大臣が設置・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、照会対象者の正確な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）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、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。 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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。
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
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（支援措置対象者情報等）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
その他のリスク①：不正なアクセスがなされるリスク ＜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することにより、システムの仕組みとして、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が不可能となるようにしている。 ＜中間サーバー・ソフトウェアにおける措置＞ 　ログイン時の職員認証のほか、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機能を有することにより、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している。 その他のリスク②：情報提供用符号が不正に用いられるリスク ＜中間サーバー・ソフトウェアにおける措置＞ 　システム上、情報連携時にのみ符号を用いる仕組みになっており、不正な名寄せが行われることのないよう、安全性を確保している。 その他のリスク③：通信中の情報に対する不正なアクセスにより情報が漏えいするリスク ＜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ことにより、通信中の情報に不正なアクセスを受けることのないよう、安全性を確保している。 ＜中間サーバー・プラットフォームにおける措置＞ 1　中間サーバーと情報提供ネットワークシステムとの間における通信は、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、通信中の情報が不正なアクセスを受けることのないよう、安全性を確保している。 2　中間サーバーと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、自治体ごとに通信回線を分離することで、通信中の情報が不正なアクセスを受けることのないよう、安全性を確保している。 3　中間サーバーと情報提供ネットワークシステムとの間における通信は暗号化されており、万が一通信中の情報に不正なアクセスがあったとしても容易に情報漏えいが起こらないよう対応している。 その他のリスク④：情報提供データベースに保存される情報が漏えいするリスク ＜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、特定個人情報を管理するデータベースを地方自治体ごとに区分管理（アクセス制御）しており、他の地方自治体が管理する情報には一切アクセスできない仕組みとすることで、保存された情報が漏えいすることのないよう、安全性を確保している。 2　地方自治体のみが特定個人情報の管理を行う仕組みとし、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アクセスできないようにしているため、事業者における情報漏えい等のリスクを極小化している。

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	[　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＞ 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。 ＜eLTAXシステム認定委託先事業者における措置＞ 技術基準及び認定要綱に定められた基準を満たすデータセンターにサーバを設置するとともに、これらの基準に沿ってサーバの管理を行っている。 ＜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　コンピュータウイルス監視ソフトを使用し、サーバ・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、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。 ＜eLTAXシステム認定委託先事業者における措置＞ 　技術基準及び認定要綱に沿って、ファイアウォールによる通信制御やコンピュータウイルス混入防止などのセキュリティ対策を実施している。 ＜標準準拠システム連携基盤における措置＞ ①共通機能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管理し、保管年数経過後に消去する。
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
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であるなど複数人で確認できる体制にあることから、古い情報のまま保管されるリスクは小さい。
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　保管年数を経過した情報は消去する。 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　帳票及び申告書等の廃棄時は、内容が判読できないよう、焼却又は裁断する。 4　標準準拠システム連携基盤においては、格納期限が経過した連携ファイルは消去する。 5　ガバメントクラウドにおいては、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、NIST800-88、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		
―		