# 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 | |
|---|---|
| 令和6年度札幌市定額減税補足給付金（調整給付）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 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 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 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 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　　] ＜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 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 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 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 個人番号の真正性確認の措置の内容 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 特定個人情報の正確性確保の措置の内容 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 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　　] ＜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 | 情報提供ネットワークシステム以外を通じて特定個人情報を入手することはない。 |
| 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 |
| 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 給付金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。<br>2 給付金業務以外との情報連携を行うためには、札幌市情報公開・個人情報保護審議会による点検など札幌市情報公開・個人情報保護審議会及び札幌市情報公開・個人情報保護審査会条例（平成16年条例第36号）に基づく手続きを行わなければならない。<br>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。<br>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 | [ 特に力を入れている ] | ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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＞<br>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＞<br>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<br>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。<br>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。<br>2 失効管理<br>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＞<br>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。<br>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＞<br>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 | － | |
| リスクへの対策は十分か | [ 特に力を入れている ] | ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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 | ・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。<br>・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。 | |
| リスクへの対策は十分か | [ 十分である ] | ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>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。<br>・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 | [　　特に力を入れている　　] ＜選択肢＞<br>1）特に力を入れている　　2）十分である<br>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 | |
| ― | |

| 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<br>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<br>委託先による特定個人情報の保管・消去に関するリスク<br>委託契約終了後の不正な使用等のリスク<br>再委託に関するリスク | | |
| 情報保護管理体制の確認 | | |
| 特定個人情報ファイルの閲覧者・更新者の制限 | [ ] | <選択肢><br>1）制限している　2）制限していない |
| 具体的な制限方法 | | |
| 特定個人情報ファイルの取扱いの記録 | [ ] | <選択肢><br>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ルール | [ ] | <選択肢><br>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 | | |
| 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 | | |
| 特定個人情報の消去ルール | [ ] | <選択肢><br>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 | | |
| 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 | [ ] | <選択肢><br>1）定めている　2）定めていない |
| 規定の内容 | | |
| 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 | [ ] | <選択肢><br>1）特に力を入れて行っている　2）十分に行っている<br>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 | [ ] | <選択肢><br>1）特に力を入れている　2）十分である<br>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＞<br>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。<br><br>＜中間サーバー・ソフトウェアにおける措置＞<br>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、行政手続における特定の個人を識別するための番号の利用等に関する法律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。<br>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。<br>※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。<br>※2　行政手続における特定の個人を識別するための番号の利用等に関する法律別表及び第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。<br>※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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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。<br><br>＜中間サーバー・ソフトウェアにおける措置＞<br>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。<br><br>＜中間サーバー・プラットフォームにおける措置＞<br>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。<br>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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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、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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>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。<br><br>＜中間サーバー・ソフトウェアにおける措置＞<br>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（※）。<br>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。<br>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。<br>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。<br>※　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。<br><br>＜中間サーバー・プラットフォームにおける措置＞<br>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。<br>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。<br>3　中間サーバー事業者が運用、監視・障害対応等の業務をする際に、特定個人情報に係る業務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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）特に力を入れている　2）十分である<br>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＞<br>1）特に力を入れている　2）十分である<br>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保守・運用を行う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＞<br>1）特に力を入れて遵守している　2）十分に遵守している<br>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＞<br>1）特に力を入れて整備している　2）十分に整備している<br>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＞<br>1）特に力を入れて整備している　2）十分に整備している<br>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＞<br>1）特に力を入れて周知している　2）十分に周知している<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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。<br>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。<br>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。<br><br>＜中間サーバー・プラットフォームにおける措置＞<br>1　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。<br>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。 | |
| ⑥技術的対策 | [ 特に力を入れて行っている ] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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。<br>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。<br><br>＜中間サーバー・プラットフォームにおける措置＞<br>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。<br>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。<br>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。 | |
| ⑦バックアップ | [ 特に力を入れて行っている ] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>1）特に力を入れて行っている　2）十分に行っている<br>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＞<br>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><br>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同様の方法にて保管している。 | |
| その他の措置の内容 | ー | |
| リスクへの対策は十分か | [ 特に力を入れている ] | <選択肢><br>1）特に力を入れている 2）十分である<br>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 | [ 特に力を入れている ] | <選択肢><br>1）特に力を入れている 2）十分である<br>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><br>1）定めている 2）定めていない |
| 手順の内容 | 情報提供ネットワークシステムの情報照会内容、情報照会結果は、保存期間後に市中間サーバーが自動で削除する。 | |
| その他の措置の内容 | ー | |
| リスクへの対策は十分か | [ 十分である ] | <選択肢><br>1）特に力を入れている 2）十分である<br>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 | | |
| ー | | |