

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
子ども・子育て支援新制度教育・保育給付認定等情報ファイル	
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： 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	個人番号カード等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。
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、事務に必要なない情報との紐付けが行われるリスク	
リスクに対する措置の内容	1 子ども・子育て支援新制度業務に関する宛名情報の保存は、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 子ども・子育て支援新制度業務以外との情報連携が行われるためには、札幌市個人情報保護審議会による承認など札幌市個人情報保護条例に基づく手続きを行わなければならないこととなっている。 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。 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	[<input type="checkbox"/> 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、顔認証、ID及びパスワードによる認証を行っており、一定時間操作が行われない場合、自動的にログアウトする。また、業務に応じてユーザの操作権限を制限する。
その他の措置の内容	1 職員マスタの登録・変更・削除は、保育推進課長が指定する職員に限定している。 2 指定された端末以外からアクセスできないよう、システム部門にて制御している。 3 システム使用中以外は必ずログオフを行う旨、実施手順に記載している。
リスクへの対策は十分か	[<input type="checkbox"/> 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 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 [<input type="checkbox"/>] 委託しない	
リスク： 委託先における不正な使用等のリスク	
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	[<input type="checkbox"/> 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担保	[<input type="checkbox"/> 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。

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

<p>リスクに対する措置の内容</p>	<p><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照会リスト(※2)との照会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、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。 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。 (※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。 (※2)番号法別表及び第19条第7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。 (※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。</p>
<p>リスクへの対策は十分か</p>	<p>[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</p>
<p>リスク2： 不正な提供が行われるリスク</p>	
<p>リスクに対する措置の内容</p>	<p style="background-color: #cccccc;"></p>
<p>リスクへの対策は十分か</p>	<p>[] <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</p>

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制している。

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： 特定個人情報の漏えい・滅失・毀損リスク

①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
②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	-	

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		
-		
8. 監査		
実施の有無	[<input type="radio"/>] 自己点検	[<input type="radio"/>] 内部監査 [<input type="checkbox"/>] 外部監査
9. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[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
具体的な方法	<札幌市における措置> 子ども・子育て支援新制度事務にかかわる職員(臨時職員等を含む。)に対して、初任時及び一定期間ごとに、必要な知識の習得に資するための研修(個人情報保護、セキュリティ対策に関する内容を含む。)を実施するとともに、その記録を残している。 <中間サーバー・プラットフォームにおける措置> IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。	
10. その他のリスク対策		
<札幌市における措置> 情報システム部門が管理するサーバ室にて、統一した設備環境による高レベルのセキュリティ管理(入退室管理等)、情報システム部門と委託業者による均一的で安定したシステム運用・監視を実現する。 <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活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。		