

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	
予防接種情報ファイル	
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	<p>1 窓口対応では、個人番号カード又は通知カード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。</p> <p>2 他の地方公共団体等から特定個人情報を含む情報を入手する際は、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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <p>・新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。</p>
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	<p>1 必要な情報以外記載できない書類様式とする。</p> <p>2 情報提供ネットワークシステムの連携によるデータも、必要な情報以外を入手できないフォーマットとする。</p>
その他の措置の内容	-
リスクへの対策は十分か	<p>[特に力を入れている] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	<p><予防接種システムにおける措置></p> <p>1 被接種者情報については、予防接種実施医療機関を経由して入手することから個人番号の記載欄は無く、不適切に個人番号を入手することはない。</p> <p>2 システムへアクセスできる職員と端末を限定している。</p> <p><団体内統合宛名システムにおける措置></p> <p>システムへアクセスできる職員と端末を限定している。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。</p>
リスクへの対策は十分か	<p>[特に力を入れている] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>・予防接種の実施については、予防接種実施医療機関において、健康保険証等の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。</p> <p>・予防接種法による給付の支給に関する事務等について、窓口で個人番号を含む申請書等の受付を行う際は、個人番号カード又は通知カード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。</p>
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通知カード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	<p>1 入手の各段階で本人確認を行う。</p> <p>2 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。</p> <p>3 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。</p>
その他の措置の内容	-
リスクへの対策は十分か	<p>[特に力を入れている] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

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	<p><予防接種システムにおける措置></p> <ol style="list-style-type: none"> 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。 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。 入手した基本4情報(氏名・住所・性別・生年月日)に基づき、システム基盤(個人基本)との連携により、住民基本台帳から個人番号を入手する際には、システム保守委託業者には個人番号の表示権限を与えないので、外部に漏れることはない。 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。 <p><システム基盤(団体内統合宛名)における措置></p> <p>システム基盤(団体内統合宛名)は、中間サーバー・プラットフォーム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。</p> <p><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></p> <p>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ているため、外部に漏れることはない。</p> <p><システム基盤(個人基本)における措置></p> <p>システム基盤(個人基本)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。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。</p>
リスクへの対策は十分か	<p>[特に力を入れている]</p> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	
<p><ワクチン接種記録システム(VRS)における追加措置></p> <p>・入手した特定個人情報については、限定された端末を利用して札幌市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。</p>	

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	
宛名システム等における措置の内容	<p>1 予防接種に関する事務に係る宛名情報は、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。</p> <p>2 予防接種に関する事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第三者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)に基づく手続を行わなければならない。</p> <p>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。</p> <p>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。</p>
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	<p>[特に力を入れている] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>[行っている] <選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<p>システムを利用できる職員を限定し、個人に交付されるICカード及び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。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>権限のない者によって不正に使用されないよう、以下の対策を講じている。</p> <ul style="list-style-type: none"> ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LGWAN端末による操作に限り可能になるように制御している。 ・LGWAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、札幌市が指定する管理者が認めた者に限定して発行される。
アクセス権限の発効・失効の管理	<p>[行っている] <選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<p>1 発効管理</p> <p>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。</p> <p>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(保健福祉局保健所健康企画課)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。</p> <p>2 失効管理</p> <p>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システム部門に対して、速やかに失効の申請を行う。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、札幌市が指定する管理者が必要最小限の権限で発効する。また、VRSに接続できるパソコンを業務に必要な最小限の台数に限定する。</p> <p>札幌市が指定する管理者は、定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。</p> <p>やむを得ず、複数の職員が共有するID(以下「共用ID」という。)を発行する場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動/退職等のイベントが発生したタイミングで確認し、当該事由が生じた際には速やかに把握している内容を更新する。</p>
アクセス権限の管理	<p>[行っている] <選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<p>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、更新を行う。</p> <p>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、失効手続きを行う。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、札幌市が指定する管理者が必要最小限の権限で発効する。</p> <p>札幌市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。</p>

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	システム上の操作のログを取得しており、操作ログを確認できる。ログは定期に及び必要に応じ随時に確認する。	
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	・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。 ・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	[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	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 実施手順に業務主管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。 <新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 住民基本台帳システムや予防接種台帳システムから特定個人情報を抽出したCSVファイルを、ワクチン接種記録システム(VRS)へ登録する際には、以下のようになっている。 ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化又はパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。 ・管理簿に消去の記録を記載する等、消去履歴を残す。	
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		
<p><予防接種に関する事務に関係のない職員や来庁者等によるのぞき見のリスク></p> <ol style="list-style-type: none"> 一定時間操作が無い場合は、自動的にログアウトする。 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。 端末のディスプレイを、来庁者から見えない位置に置く。 事務処理に必要な画面のハードコピーは取得しない。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <ol style="list-style-type: none"> 特定個人情報を使用する場面を必要最小限に限定している。具体的には、接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために個人番号を入手し、使用する場面に限定している。 ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。 		

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。 <新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 札幌市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 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 ・ 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	・ 特定個人情報を取り扱う従業者の名簿を提出させる。 ・ 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。 ・ 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) 当該委託業務においては、「特定個人情報等の取扱いに関する特記事項」又は「ワクチン接種記録システムの開発・運用保守業務一式契約書に関する覚書」を遵守するよう定めている。 (確認方法) これらの中で、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) 当該委託業務においては、「特定個人情報等の取扱いに関する特記事項」又は「ワクチン接種記録システムの開発・運用保守業務一式契約書に関する覚書」を遵守するよう定めている。 (確認方法) これらの中で、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
ルール内容及びルール遵守の確認方法	(内容) 当該委託業務においては、「特定個人情報等の取扱いに関する特記事項」又は「ワクチン接種記録システムの開発・運用保守業務一式契約書に関する覚書」を遵守するよう定めている。 (確認方法) これらの中で、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	<p>当該委託業務においては、「特定個人情報等の取扱いに関する特記事項」又は「ワクチン接種記録システムの開発・運用保守業務一式契約書に関する覚書」を遵守するよう定めており、以下の事項を規定している。</p> <ol style="list-style-type: none"> 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及び教育並びに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	<p>当該委託業務においては、「特定個人情報等の取扱いに関する特記事項」又は「ワクチン接種記録システムの開発・運用保守業務一式契約書に関する覚書」を遵守するよう定めている。これらの中で、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。</p>	
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	[]	<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	[] <input type="checkbox"/> 接続しない(入手) [] <input type="checkbox"/> 接続しない(提供) <input type="checkbox"/> 特に入力している <input type="checkbox"/> 十分である <input type="checkbox"/> 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 [] <input type="checkbox"/> 接続しない(入手) [] <input type="checkbox"/> 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	<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。</p> <p><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。</p>
リスクへの対策は十分か	[<input type="checkbox"/> 特に入力している] <input type="checkbox"/> 十分である <input type="checkbox"/> 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	<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。</p> <p><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。</p> <p><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。</p>
リスクへの対策は十分か	[<input type="checkbox"/> 特に入力している] <input type="checkbox"/> 十分である <input type="checkbox"/> 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	<p><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。</p>
リスクへの対策は十分か	[<input type="checkbox"/> 特に入力している] <input type="checkbox"/> 十分である <input type="checkbox"/> 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	<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。</p> <p><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、漏えい及び紛失のリスクに対応している(※7)。 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。 ※7 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。</p> <p><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。</p>
リスクへの対策は十分か	<p>[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</p>
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	<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、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。</p> <p><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 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。</p>
リスクへの対策は十分か	<p>[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</p>

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	<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、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。</p> <p><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。</p> <p><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、特定個人情報に係る業務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。</p>
リスクへの対策は十分か	<p>[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</p>
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	<p><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。</p> <p><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(※8)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。 ※8 特定個人情報を副本として保存・管理する機能。</p>
リスクへの対策は十分か	<p>[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</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> 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> 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。 2 事前に申請し承認されてない物品、記憶媒体、通信機器等を所持若しくは持出又は持込することがないよう、警備員等により確認している。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。
⑥技術的対策	[特に力を入れて行っている]	<選択肢> 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、端末及びサーバ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。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LGWAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。

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
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 予防接種関係法令に定められた保管年数を経過した情報は、データを調査した上で消去する。 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。	
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		
-		