

特定個人情報保護評価書(重点項目評価書)

評価書番号	評価書名
4	予防接種に関する事務 重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

函館市は、予防接種に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

評価実施機関名

北海道函館市長

公表日

令和8年1月30日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 変更箇所

システム2	
①システムの名称	団体内統合宛名利用番号連携システム
②システムの機能	1. 中間サーバ連携機能: 中間サーバまたは中間サーバ端末からの要求に基づき、団体内統合宛名番号に紐付く宛名情報等を通知する機能 2. 宛名情報等管理機能: 団体内統合宛名システムにおいて宛名情報を団体内統合宛名番号、個人番号と紐付けて保存し、管理する機能 3. 宛名番号付番機能: 団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番する機能 4. 既存システム連携機能: 既存業務システムからの要求に基づき、個人番号、団体内統合宛名番号に紐付く宛名情報を通知する機能
③他のシステムとの接続	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> その他 (中間サーバシステム等)
システム3	
①システムの名称	中間サーバシステム
②システムの機能	1. 符号管理機能: 情報照会または情報提供に用いる個人の識別情報である「符号」と、市の内部で個人を特定するために利用する「団体内統合宛名番号」を紐付け、その情報を管理する機能 2. 情報照会機能: 情報提供ネットワークを介して、特定個人情報(連携対象)の情報照会および情報提供受領(照会した情報の受領)を行う機能 3. 情報提供機能: 情報提供ネットワークシステムを介して、情報照会要求の受領および、その特定個人情報(連携対象)の提供を行う機能 4. 既存システム接続機能: 中間サーバと団体内統合宛名システムおよび、その他既存システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能 5. 情報提供等記録管理機能: 特定個人情報(連携対象)の照会または提供があった旨の情報提供等記録を生成し、管理する機能 6. 情報提供データベース管理機能: 特定個人情報(連携対象)を副本として保持・管理する機能 7. データ送受信機能: 中間サーバと情報提供ネットワークシステムとの間で情報照会、情報提供符号取得のための情報等について連携するための機能 8. セキュリティ管理機能: 特定個人情報(連携対象)の暗号化および復号や、伝聞への署名付与伝聞および情報提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、情報提供ネットワークシステム(インターフェイスシステム)から受信した情報提供ネットワークシステム配信マスター情報を管理する機能 9. 職員認証・権限管理機能: 中間サーバ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(連携対象)へのアクセス制御を行う機能 10. システム管理機能: バッチの状況管理、業務統計情報の集計、稼働状況の通知、保管期限切れ情報の制限を行う機能
③他のシステムとの接続	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 住民基本台帳ネットワークシステム <input type="checkbox"/> 既存住民基本台帳システム <input type="checkbox"/> 宛名システム等 <input type="checkbox"/> 税務システム <input type="checkbox"/> その他 ()

3. 特定個人情報ファイル名	
予防接種台帳ファイル	
4. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項別表14, 126の項
5. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	(情報提供の根拠) 番号法第19条第8号に基づく主務省令第2条の表25, 26, 27, 28, 29, 153, 154の項 (情報照会の根拠) 番号法第19条第8号に基づく主務省令第2条の表25, 27, 28, 29, 153の項
6. 評価実施機関における担当部署	
①部署	保健福祉部保健予防課・子ども未来部母子保健課
②所属長の役職名	保健福祉部保健予防課長・子ども未来部母子保健課長
7. 他の評価実施機関	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
予防接種台帳ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	市に居住する予防接種の対象者
その必要性	予防接種に関する事務処理の基礎とするとともに、必要な記録の適正な管理を図るため
④記録される項目	[10項目以上50項目未満] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	<ul style="list-style-type: none"> ・識別情報 個人番号:対象者を正確に特定するために保有する。 その他識別情報:当市において、個人を一意に識別するために独自の識別番号を保有する(以降、宛名番号と表記)。 ・連絡先等情報 予診票等の送付先情報として保有する。
全ての記録項目	別添1を参照。
⑤保有開始日	平成28年1月1日
⑥事務担当部署	保健福祉部保健予防課・子ども未来部母子保健課

3. 特定個人情報の入手・使用									
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 () <input type="checkbox"/> 行政機関・独立行政法人等 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 (他の自治体) <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 ()								
②入手方法	<input type="checkbox"/> 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ <input type="checkbox"/> 電子メール [] 専用線 [<input type="checkbox"/>] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ()								
③使用目的 ※	予防接種の実施, 予防接種に関する記録の作成								
④使用の主体	使用部署	保健福祉部保健予防課・子ども未来部母子保健課							
	使用者数	[10人以上50人未満] <table border="0"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	<選択肢>		1) 10人未満	2) 10人以上50人未満	3) 50人以上100人未満	4) 100人以上500人未満	5) 500人以上1,000人未満
<選択肢>									
1) 10人未満	2) 10人以上50人未満								
3) 50人以上100人未満	4) 100人以上500人未満								
5) 500人以上1,000人未満	6) 1,000人以上								
⑤使用方法	<p>・予防接種対象者の情報の登録(更新)および予防接種を接種した者について接種結果の登録(更新)を行う。</p>								
情報の突合	予診票等に記載された住所, 氏名, 生年月日等と突合し接種対象者の該当の有無を確認								
⑥使用開始日	平成28年1月1日								

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[委託する] <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	健康管理システムの保守管理・法制度改正に伴う改修業務	
①委託内容	予防接種法および新型インフルエンザ等対策特別措置法による予防接種事務に関する台帳管理等(予防接種台帳の整備, 予防接種済の記録, 台帳補記, 住民異動の反映, 帳票の出力等)システム内で管理している情報のうち、情報連携を行う必要のある予防接種履歴に関する項目を抽出し、情報連携を行えるようにする。	
②委託先における取扱者数	[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
③委託先名	株式会社エスイーシー	
再委託	④再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[] 提供を行っている () 件 [] 移転を行っている () 件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去

保管場所 ※

・本市と専用線で接続されたデータセンター(入退室管理あり)の本市専用環境に設置したサーバ内に保管しサーバへのアクセスにはID/パスワードによる認証が必要としている。
・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザIDによる識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。

7. 備考

(別添1) 特定個人情報ファイル記録項目

(1) 住民情報ファイル

1. 宛名番号, 2. 氏名, 3. カナ氏名, 4. 清音カナ氏名, 5. 生年月日, 6. 性別, 7. 世帯番号, 8. 世帯員番号, 9. 続柄, 10. 世帯主番号, 11. 世帯主氏名, 12. 世帯主カナ氏名, 13. 行政区コード1(大街), 14. 行政区コード2(小街), 15. 行政区コード3(郵便局), 16. 行政区コード4(母子担当), 17. 行政区コード5(訪問担当), 18. 郵便番号, 19. 住所1, 20. 住所2, 21. 住民となった事由, 22. 住民となった日, 23. 住民となった届出日, 24. 住民でなくなった事由, 25. 住民でなくなった日, 26. 住民でなくなった届出日, 27. 増減異動事由, 28. 増減異動日, 29. 増減異動届出日, 30. 住民区分, 31. 旧氏名, 32. 旧カナ氏名, 33. 旧清音カナ氏名, 34. 旧郵便番号, 35. 旧住所1, 36. 旧住所2, 37. 個人番号

(2) 予防接種台帳ファイル

1. 宛名番号, 2. 予防接種種類, 3. 回数, 4. 接種日, 5. 接種機関, 6. 診察医師, 7. 接種医師, 8. 製造社, 9. ワクチン名, 10. LotNo, 11. 有効期限, 12. 接種量, 13. 接種後状況, 14. 備考, 15. 接種券等発行日, 16. 更新日時, 17. 更新端末名, 18. 更新者名, 19. アクセスログ番号, 20. 検査年月日, 21. 抗体検査方法, 22. 抗体検査結果, 23. 抗体検査番号, 24. 判定結果

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
予防接種台帳ファイル	
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	健康管理システムには、特定個人情報を扱う業務からその他の業務あるいはその逆へのアクセスに制限を行う機能を有する。個人毎に設定するIDで利用可能な業務も制限されている。
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
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	健康管理システムには、特定個人情報を扱う業務からその他の業務あるいはその逆へのアクセスに制限を行う機能を有する。個人毎に設定するIDで利用可能な業務も制限されている。
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	健康管理システムを利用する必要がある職員を特定し、個人毎にユーザIDを割り当てるとともに、利用時にはユーザIDとパスワードで認証を行う。健康管理システムサーバが設置されているデータセンターサーバ室への入退室の際には、ICカード認証を行う。
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

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

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： 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 3) 課題が残されている	2) 十分である

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

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

【目的外の入手が行われるリスク】

＜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では、個人番号利用事務(システム)からの接続には認証を必須とし、個人番号利用事務(システム)以外のアクセスはできない対策を実施する。
- ・団体内統合宛名システムでは、ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施する。

＜中間サーバ・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紹介内容の紹介許可照会リスト(※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する。

2. 中間サーバの職員認証・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制する仕組みとする。

(※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および照会した情報の受領を行う機能。

(※2)番号法別表第2および第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。

(※3)中間サーバ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。

【安全が保たれない方法によって入手が行われるリスク】

＜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では、事前に登録したサーバ(中間サーバ等)のみに、情報入手元を限定する。
- ・団体内統合宛名システムでは、通信路セキュリティとして経路暗号化を実施する。

＜中間サーバ・ソフトウェアにおける措置＞

・中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する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実施できるよう設計されるため、安全性が担保する。

＜中間サーバ・プラットフォームにおける措置＞

・中間サーバと既存システム、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する。

・中間サーバと団体については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する。

【入手した特定個人情報ที่ไม่正確であるリスク】

＜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では、事前に登録したサーバ(中間サーバ等)のみに、情報要求のリクエスト先を限定する。

＜中間サーバ・ソフトウェアにおける措置＞

・中間サーバは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者にかかる特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することを担保する。

【入手の際に特定個人情報が漏えい・紛失するリスク】

＜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では、通信路セキュリティとして経路暗号化を実施する。

＜中間サーバ・ソフトウェアにおける措置＞

・中間サーバは、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する。(※)

・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る。

・情報照会が完了また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する。

・中間サーバの職員認証・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制する。

(※)中間サーバは、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い、照会者の中間サーバでしか復号できない仕組みとする。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する。

＜中間サーバ・プラットフォームにおける措置＞

・中間サーバと既存システム、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する。

・中間サーバと団体については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する。

・中間サーバ・プラットフォーム事業者の業務は、中間サーバ・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。

<p>リスクへの対策は十分か</p>	<p>[十分である] <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>
<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>【不正な提供が行われるリスク】 <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では、個人番号利用事務(システム)からの接続には認証を必須とし個人番号利用事務(システム)以外のアクセスはできない対策を実施する。 ・団体内統合宛名システムでは、ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施する。</p> <p><中間サーバ・ソフトウェアにおける措置> ・情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して情報提供機能により照会許可照会リストに基づき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を実施する。 ・情報提供機能により、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、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領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応する。 ・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付加フラグを設定し、特定個人情報の提供を行う際に送信内容を改めて確認し、提供を行う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する。 ・中間サーバの職員認証・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とする。 (※)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提供の要求の受領および情報提供を行う機能。</p> <p>【不適切な方法で提供されるリスク】 <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では、通信路セキュリティとして経路暗号化を実施する。 ・団体内統合宛名システムでは、中間サーバに接続許可対象システムとして登録することで中間サーバへの提供元を団体内統合利用番号連携システムに限定する。</p> <p><中間サーバ・ソフトウェアにおける措置> ・セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施したうえで提供を行う仕組みとする。 ・中間サーバの職員認証・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とする。 (※)暗号化・復号機能と鍵情報および照会許可照会リストを管理する機能。</p> <p><中間サーバ・プラットフォームにおける措置> ・中間サーバと既存システム、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する。 ・中間サーバと団体については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する。 ・中間サーバ・プラットフォームの保守・運用を行う事業者においては、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を行い、不適切な方法での情報提供を行えないよう管理する。</p> <p>【誤った情報を提供してしまうリスク】 <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では、事前に登録したサーバ(中間サーバ等)のみに、情報提供先を限定する。</p> <p><中間サーバ・ソフトウェアにおける措置> ・情報提供機能により、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、情報提供許可証と情報照会者への経路情報を受領したうえで、情報照会内容に対応した情報提供をすることで、誤った相手に特定情報が提供されるリスクに対応する。 ・情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有する。 (※)特定個人情報を副本として保存・管理する機能。</p>
<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢></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>

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

<中間サーバ・プラットフォームにおける措置>

- ・中間サーバ・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公共団体ごとに区分管理(アクセス制御)しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない仕様とする。
- ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運営を行う事業者における情報漏えい等のリスクを極小化する。

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	<p>[十分である] <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>
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	
<p><函館市における措置></p> <ul style="list-style-type: none"> ・ICカード認証による入退出管理を行っている部屋に設置した大型汎用機(サーバ)に保管する。大型汎用機(サーバ)に接続することができる各業務担当課に設置された端末についてはそれぞれID、パスワード、生体認証(指紋・静脈)を設定し、大型汎用機(サーバ)へのアクセスはパスワードによる認証を必要としている。 ・函館市電子計算機処理に係るデータ保護管理規程に基づき、保護責任者は保存期間の経過等により保管の必要がなくなった磁気ファイルについて、一切アクセスできないよう制限した上、システム上で速やかに消去、排気筒の必要な措置を講じている。 ・保存期限を経過した紙媒体による特定個人情報については、廃棄処分を実施する。 <p><中間サーバ・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館およびサーバ室への入室を厳重に管理する。特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。 	

8. 監査	
実施の有無	[<input type="radio"/>] 自己点検 [<input type="radio"/>] 内部監査 [] 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	<p>・職員等に対しては、配属時(新規事務従事時)および年1回、個人情報保護、特定個人情報の取り扱い、法令等に違反した場合の罰則、情報セキュリティ等に関する研修を実施する。</p> <p>・委託業者に対しては、契約内容に個人情報(特定個人情報を含む)保護に関する条文を規定するとともに、業務に従事する従業員に対して、職員に対する研修と同等の研修の実施の義務づけを行う。</p> <p>※従業者とは、契約形態にかかわらず、特定個人情報保護評価の対象となる事務に現に従事する者の全てが含まれる。行政機関においては、正規職員のほか、会計年度任用職員等も含む。</p>
10. その他のリスク対策	

IV 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	総務部文書法制課 函館市東雲町4番13号 0138-21-3649
②請求方法	個人情報の保護に関する法律および函館市個人情報の保護に関する法律施行条例の規定に基づき、開示・訂正・利用停止請求を受け付ける。
③法令による特別の手続	—
④個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	保健予防課 函館市五稜郭町23番1号 0138-32-1540・母子保健課 函館市五稜郭町23番1号 0138-32-1533
②対応方法	対応について記録を残す。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和7年6月20日
②しきい値判断結果	[基礎項目評価及び重点項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び重点項目評価の実施が義務付けられる 2) 基礎項目評価の実施が義務付けられる(任意に重点項目評価を実施) 3) 特定個人情報保護評価の実施が義務付けられない(任意に重点項目評価を実施)
2. 国民・住民等からの意見の聴取【任意】	
①方法	
②実施日・期間	
③主な意見の内容	
3. 第三者点検【任意】	
①実施日	
②方法	
③結果	

