

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
21	こども医療費の助成に関する事務 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

熊谷市は、こども医療費の助成に関する事務の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	なし
------	----

評価実施機関名

熊谷市長

公表日

令和8年1月5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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	こども医療費の助成に関する事務
②事務の内容	<p>熊谷市こども医療費の助成に関する条例及び熊谷市こども医療費の助成に関する条例施行規則に基づき、こども医療費の支給を行う。</p> <p>特定個人情報ファイルを使用する事務の内容</p> <p>①医療費の助成に関する事務</p> <p>②医療費の受給資格の登録に関する事務</p> <p>＜Public Medical Hub (PMH)を活用した情報連携に係る公費医療費助成事務＞</p> <p>・情報連携のため、本市は、Public Medical Hub (PMH)へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報の紐付け及び登録を行う。</p> <p>・住民は、マイナポータルを介して、自身の本事務に係る公費医療費助成の資格情報の取得/閲覧が可能となる。</p>
③対象人数	<div>＜選択肢＞</div> <div>[1万人以上10万人未満] 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満</div>
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	医療助成システム
②システムの機能	こども医療受給資格者の台帳管理、医療費支給情報の作成管理、支給決定通知書等帳票類の発行
③他のシステムとの接続	<div>[] 情報提供ネットワークシステム [O] 庁内連携システム</div> <div>[] 住民基本台帳ネットワークシステム [O] 既存住民基本台帳システム</div> <div>[O] 宛名システム等 [] 税務システム</div> <div>[O] その他 (Public Medical Hub (PMH))</div>
システム2～5	
システム2	
①システムの名称	団体内統合宛名システム
②システムの機能	<p>1. 個人番号管理機能</p> <p>個人番号と団体内統合宛名番号を紐付け、個別業務システムから個人を一意に特定できるように管理する機能。</p> <p>2. アクセス制御機能</p> <p>個人番号利用事務、事務取扱部署及び事務取扱担当者を紐付け、アクセス制御とログ管理を行う機能。</p> <p>3. 個人番号確認機能</p> <p>個別業務システムからの要求に基づき、本人確認のために必要な情報を確認する機能。</p> <p>4. 中間サーバ連携機能</p> <p>情報連携で必要なデータを個別業務システムから受け取り、中間サーバへ連携する機能。</p>
③他のシステムとの接続	<div>[] 情報提供ネットワークシステム [O] 庁内連携システム</div> <div>[] 住民基本台帳ネットワークシステム [O] 既存住民基本台帳システム</div> <div>[] 宛名システム等 [O] 税務システム</div> <div>[O] その他 (中間サーバー、個別業務システム)</div>

システム11～15
システム16～20

3. 特定個人情報ファイル名		
児童手当受給者ファイル		
4. 個人番号の利用 ※		
法令上の根拠	・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 第9条第2項 ・熊谷市個人番号の利用に関する条例第3条第1項 別表第1の1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】 なし(本事務において、情報提供ネットワークシステムによる情報提供は行わない) 【情報照会の根拠】 ・番号法第19条第9号 ・熊谷市個人番号の利用に関する条例第3条	
6. 評価実施機関における担当部署		
①部署	福祉部 こども課	
②所属長の役職名	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		
こども医療費受給者台帳ファイル		
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	[1万人以上10万人未満] ＜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 ※	本市からこども医療を受給している者	
その必要性	こども医療費の適正な支給を実現するために、必要な特定個人情報を保有する必要がある。	
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 ※	・識別情報 [<input type="radio"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="radio"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="radio"/>] 4情報(氏名、性別、生年月日、住所) [<input type="radio"/>] 連絡先(電話番号等) [<input type="radio"/>] 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="radio"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="radio"/>] 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="radio"/>] 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="radio"/>] その他 (医療助成資格情報)	
	その妥当性	・個人番号、その他識別情報(内部番号) 対象者を正確に特定するために保有 ・4情報、連絡先等情報、その他住民票関係情報 受給者・請求者の基準日時点の居住地、世帯情報等を把握するために保有 ・地方税関係情報 所得状況に応じて医療日の支給額が変動するために保有 ・医療保険関係情報 加入保険資格の確認のため保有 ・生活保護・社会福祉関係情報 生活保護受給状況の確認のため保有 ・識別情報(その他識別情報) PMHキー、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 自治体業務ID…PMH内で公費医療の種類を区別するために必要となる。 ・業務関係情報(その他) 医療助成資格情報…(医療費助成事務の適切な実施にあたり必要となる情報を管理し、)PMHが、外部と情報連携するために必要となる。
	全ての記録項目	別添1を参照。
⑤保有開始日	令和6年10月22日	
⑥事務担当部署	福祉部こども課	

3. 特定個人情報の入手・使用		
①入手元 ※		<div><div>[○] 本人又は本人の代理人</div><div>[○] 評価実施機関内の他部署（市民税課）</div><div>[] 行政機関・独立行政法人等（）</div><div>[○] 地方公共団体・地方独立行政法人（市区町村）</div><div>[○] 民間事業者（社会保険診療報酬支払基金、医療機関）</div><div>[○] その他（地方公共団体情報システム機構）</div></div>
②入手方法		<div><div>[○] 紙</div><div>[○] 電子記録媒体(フラッシュメモリを除く。)</div><div>[] フラッシュメモリ</div><div>[] 電子メール</div><div>[] 専用線</div><div>[○] 庁内連携システム</div><div>[○] 情報提供ネットワークシステム</div><div>[○] その他（住民基本台帳ネットワークシステム、医療保険者等向け中間サーバー、医療機関用アプリ、マイナポータル）</div></div>
③使用目的 ※		こども医療費の適正な支給のため
④使用の主体	使用部署	福祉部こども課、大里行政センター、妻沼行政センター、江南行政センター
	使用者数	<div><div><選択肢></div><div>[10人以上50人未満]</div><div>1) 10人未満</div><div>2) 10人以上50人未満</div><div>3) 50人以上100人未満</div><div>4) 100人以上500人未満</div><div>5) 500人以上1,000人未満</div><div>6) 1,000人以上</div></div>
⑤使用方法		<div><div>・こども医療の資格登録申請に対して、収集した情報をもとに資格を付与する。</div><div>・こども医療の支給申請に対して、収集した情報をもとに医療費の支給を行う。</div><div>・情報連携のため、本市は、Public Medical Hub (PMH) へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報の紐付け及び登録を行う。</div><div>・登録後、Public Medical Hub (PMH) は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub (PMH) が運動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hub (PMH) に応答する。</div><div>・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルとPublic Medical Hub (PMH) で共有されることでマイナポータルや医療機関システムから公費資格情報の取得/閲覧を行うといった情報連携が可能となる。</div></div>
	情報の突合	住民からのこども医療費各種請求書等の内容と住基情報・情報照会等により収集した地方税関係情報等を突合する。
⑥使用開始日		平成30年12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 ※		<div> <div>委託する</div> <div> <div><選択肢></div> <div>1) 委託する 2) 委託しない</div> </div> </div> <div>(2) 件</div>
委託事項1		システムの運用・保守業務、法制度改正に伴う改修作業業務
①委託内容		システムの運用・保守業務、法制度改正に伴う改修作業
②委託先における取扱者数		<div> <div>10人未満</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>
③委託先名		株式会社ジーシーシー
再委託	④再委託の有無 ※	<div> <div>再委託しない</div> <div> <div><選択肢></div> <div>1) 再委託する 2) 再委託しない</div> </div> </div>
	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2		こども医療受給者証作成業務委託
①委託内容		こども医療受給者証の作成
②委託先における取扱者数		<div> <div>10人未満</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>
③委託先名		株式会社ジーシーシー
再委託	④再委託の有無 ※	<div> <div>再委託しない</div> <div> <div><選択肢></div> <div>1) 再委託する 2) 再委託しない</div> </div> </div>
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項3		Public Medical Hub(PMH)を活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容		Public Medical Hub(PMH)の利用・情報連携業務及び運用保守業務
②委託先における取扱者数		<div> <div>50人以上100人未満</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>
③委託先名		国(デジタル庁)
再委託	④再委託の有無 ※	<div> <div>再委託する</div> <div> <div><選択肢></div> <div>1) 再委託する 2) 再委託しない</div> </div> </div>
	⑤再委託の許諾方法	書面又は電磁的方法による承諾
	⑥再委託事項	PMHキーの付与、情報連携業務及び運用保守業務
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 [O] 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 [] 電子メール [] フラッシュメモリ [] その他 ()	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度		
提供先2～5		
提供先2		
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 [] 電子メール [] フラッシュメモリ [] その他 ()	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度		
提供先3		
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 [] 電子メール [] フラッシュメモリ [] その他 ()	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度		
提供先4		
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 [] 電子メール [] フラッシュメモリ [] その他 ()	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度		
提供先5		
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 [] 電子メール [] フラッシュメモリ [] その他 ()	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度		

提供先6～10
提供先11～15
提供先16～20

移転先1	こども課	
①法令上の根拠	熊谷市誕生祝金の支給に関する要綱	
②移転先における用途	誕生祝金支給事業において、支給口座の登録のために利用。	
③移転する情報	氏名、住所、生年月日、性別、世帯情報等の住民情報、口座情報	
④移転する情報の対象となる本人の数	[1万人以上10万人未満] <div><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</div>	
⑤移転する情報の対象となる本人の範囲	対象者の熊谷市におけるこども医療の支給情報	
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [<input checked="" type="checkbox"/>] 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	都度	
移転先2～5		
移転先2		
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	[] <div><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</div>	
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3		
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	[] <div><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</div>	
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4		
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	[] <div><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</div>	
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5		
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	[] <div><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</div>	
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 ※	<p>＜熊谷市における措置＞</p> <ul style="list-style-type: none">・サーバは、入退室管理を行っているデータセンターのサーバ室に設置している。・入退室管理は、サーバ室への入室権限を持つ者を事前申請により限定し、サーバ室へ入退室する者が権限を有することを生体認証とICカードで確認することとしている。 <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及びサーバ室への入室を厳重に管理する。・特定個人情報は、データセンターの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。 <p>＜ガバメントクラウドにおける措置＞</p> <ul style="list-style-type: none">・サーバ等はクラウド事業者が保有・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事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ①ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ②日本国内でのデータ保管を条件としていること。・特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。・特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際に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、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 <p>＜Public Medical Hub (PMH)を活用した情報連携に係る公費医療費助成事務＞</p> <p>Public Medical Hub (PMH)は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバー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、政府情報システムのためのセキュリティ評価制度 (ISMAP)において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。</p> <ul style="list-style-type: none">・サーバ設置場所等への入退室記録管理、施錠管理・論理的に区分された当市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(デジタル庁)や医療機関及び住民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。・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。
7. 備考	
<p>＜Public Medical Hub (PMH)を活用した情報連携に係る公費医療費助成事務＞</p> <ul style="list-style-type: none">・本市の領域に保管されたデータのみ、Public Medical Hub (PMH)を用いて消去することができる。・本市の領域に保管されたデータは、他機関から消去できない。 <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p> <ul style="list-style-type: none">・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。・不要となったバックアップファイルは、古いものから順に自動削除される。	

(別添1) 特定個人情報ファイル記録項目

【識別情報】

1.個人番号,2.宛名番号

【連絡先等情報】

1.氏名,2.生年月日,3.性別,4.住所,5.電話番号,6.世帯番号,7.続柄,8.世帯主氏名

【業務関係情報】

1.受給者番号,2.受付年月日,3.資格取得日,4.資格取得事由,5.有効期間開始日,6.有効期間終了日,7.資格喪失日,8.宛名番号,9.世帯番号

10.カナ氏名,11.氏名,12.生年月日,13.性別,14.続柄,15.郵便番号,16.住所,17.方書,18.保護者氏名,19.保護者郵便番号,20.保護者住所
21.保険者番号,21.保険者名,22.保険種別,23.被保険者名,24.保険記号番号,25.保険開始日,26.銀行名,27.支店名,28.預金種別,29.口座番号

30.口座名義人カナ,31.所得額,32.控除後所得額,33.送付先郵便番号,34.送付先住所,35送付先肩書,36送付先宛名

【Public Medical Hub (PMH)を活用した情報連携に係る公費医療費助成事務における追加の記録項目】

(1)対象者情報

- ・個人番号
- ・PMHキー
- ・PMH仮名識別子
- ・基本5情報(カナ・氏名・住所・生年月日・性別)
- ・自治体コード
- ・自治体業務ID
- ・連携ファイル名
- ・連携日時
- ・連携処理ステータス/エラー内容
- ・制御フラグ(不開示/閲覧停止)
- ・その他管理番号・ID等(履歴ID、属性ID)

(2)ユーザー情報

- ・機関マスタID
- ・機関ユーザーID
- ・メールアドレス
- ・ユーザー氏名
- ・ユーザー区分
- ・ユーザー権限ID
- ・個人番号閲覧可能フラグ
- ・ユーザー削除フラグ

(3)医療助成資格情報

- ・受給者証種別ID
- ・受給者証名
- ・受給者証ID
- ・受給者証券面情報
- ・受給者証項目情報
- ・表示順番号
- ・公費ID
- ・区分
- ・公費負担者番号
- ・公費受給者番号
- ・自己負担上限情報(自己負担上限額ID、自己負担上限額種別、負担定義、負担率、金額、回数)
- ・有効期間
- ・強制失効日
- ・医療機関コード
- ・指定医療機関情報

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名		
こども医療費受給者台帳ファイル		
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	<ul style="list-style-type: none">・住基情報の入手については、既存住民基本台帳システムに登録した情報を庁内連携機能で取得するため、対象候補となりうる住民以外の情報を入手することはない。・住民からの申告・申請情報の入手については、本人確認や個人番号の真正性確認を実施している。・市町村CSからの住登外情報については、対象者を確定した上で情報を入手している。・庁内連携機能からの各種照会情報の入手については、個人単位の操作ログを取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。証跡については完全性を担保し、容易に改ざんできない対策を施している。・医療保険者等向け中間サーバーからPublic Medical Hub (PMH) へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステムの的に制御している。・Public Medical Hub (PMH) 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。	
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		
<p><不適切な方法で入手が行われるリスクに対する措置></p> <ul style="list-style-type: none">・庁内連携機能からの住民税賦課情報の入手については、入退室管理をしているデータセンター内のサーバ間通信に限定することで、詐取・奪取が行われないようにしている。・庁内連携機能からの各種照会情報の入手については、アクセス権を有しない職員のなりすましによる入手への対策を施している。また、当該情報に接続可能なシステム及び端末を予め登録し、許可された機器に限定した入手方法とすることで、対象外の機器からの入手が行われないようにしている。 <p><入手した特定個人情報が不正確であるリスクに対する措置></p> <ul style="list-style-type: none">・入手した情報については、窓口での聞き取りや本人確認書類との照合等を通じて確認することで正確性を確保している。・職員にて収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 <p><入手の際に特定個人情報が漏えい・紛失するリスクに対する措置></p> <ul style="list-style-type: none">・庁内連携機能からの住基情報、各種照会情報の入手については、サーバ間通信を限定することで漏えい・紛失を防止している。		
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	<ul style="list-style-type: none">・団体内統合宛名システムのアクセス制御機能により、個人番号利用事務、事務取扱部署及び事務取扱担当者以外が、特定個人情報を参照できない仕組みを講じている。・医療助成システムには、医療助成事務に関係のない情報を保有しない。・医療助成システムでは、特定個人情報を参照できる機能と情報を限定しており、設定された利用権限の範囲を超えてアクセスができないように制御を行っている。・Public Medical Hub (PMH) にアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。・Public Medical Hub (PMH) では、権限のある者しか個人番号にはアクセスできないように制御している。・医療機関システムからは既存の開域網経由でPublic Medical Hub (PMH) に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないよう制御している。・住民からはインターネットからマイナポータルAPI経由でPublic Medical Hub (PMH) に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	
	[十分である]	<選択肢>

リスクへの対策は十分か	<div> <div></div> <div> <div>1) 特に力を入れている</div> <div>2) 十分である</div> </div> <div>3) 課題が残されている</div> </div>
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	<div> <div>[行っている]</div> <div> <div><選択肢></div> <div> <div>1) 行っている</div> <div>2) 行っていない</div> </div> </div> </div>
具体的な管理方法	<div> <div> <ul style="list-style-type: none"> ・医療助成システムへのアクセスにおいて、識別情報(ユーザID/パスワードと生体)による2因子認証を実施している。また認証後は認可機能により、そのユーザが利用できる機能を制限することで、不正利用が行えないよう対策している。 ・パスワードには、有効期限の設定、同一又は類似パスワード再利用制限、最低文字数の設定等を行っている。 ・ユーザID/パスワードの管理者は必要最小限とし、漏えい等が発生しないように厳重に管理している。 ・ユーザID/パスワードを複数人で共有することを禁止している。 </div> <div> <div><Public Medical Hub (PMH)を活用した情報連携に係る公費医療費助成事務における追加措置></div> <div>権限のない者に不正使用されないよう、以下の対策を講じている。</div> <ul style="list-style-type: none"> ・本市は、Public Medical Hub (PMH) のアクセス権限を管理する管理者を定める。 ・Public Medical Hub (PMH) のログインはユーザID・パスワードで行う。 ・Public Medical Hub (PMH) へのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・Public Medical Hub (PMH) における特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)からPublic Medical Hub (PMH) への連携は、アクセス権限を持つ者のみ実施が可能となっている。 </div> </div>

その他の措置の内容	<p><アクセス権限の発効・失効の管理></p> <ul style="list-style-type: none"> ・識別情報(職員カード、ユーザID/パスワード)の発行・更新・廃棄は、人事異動や退職時など、あらかじめ定められたルールに基づいて随時行っている。 ・医療助成システムにアクセスする職員へのアクセス権限は定期的に見直しを行い、適切な者のみがアクセスできるようにしている。 <p><アクセス権限の管理></p> <ul style="list-style-type: none"> ・ユーザID/パスワードの管理者は必要最小限とし、漏えい等が発生しないように厳重に管理している。 ・ユーザIDについては、セキュリティ責任者が定期的にチェックを行い、不要なIDが残存しないようにしている。また、利用期間が明確になったものについては、ユーザIDに有効期限を設定し、期限到来により自動的に失効するようにしている。 <p><特定個人情報の使用の記録></p> <ul style="list-style-type: none"> ・ユーザIDとともに、児童手当システムへのアクセス、操作(登録、更新、印刷、外部媒体への出力等)のアクセス記録をログとして保管している。 ・上記アクセス記録について、確認が必要となった場合には即座に確認できる仕組みを準備しており、また、異常アクセス(休業日や業務時間外のアクセス、ログインエラー等)については定期的にチェックを行っている。
リスクへの対策は十分か	<div> <div>[十分である]</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>
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><従業者が事務外で使用するリスクに対する措置></p> <ul style="list-style-type: none"> ・外部媒体へのデータのコピーや印刷を制御することで、許可なく持ち出せないようにしている。 ・各種ログを取得しているため、業務外利用をした場合には特定可能であることを職員に周知し、事務外の利用を抑止している。 <p><特定個人情報ファイルが不正に複製されるリスクに対する措置></p> <ul style="list-style-type: none"> ・バックアップファイルの取得は入退室管理をしているデータセンタでの作業に限定され、また、バックアップファイルの持ち出しはセキュリティ責任者による承認を必須としている。 ・特定個人情報ファイルの外部媒体への出力は、特定のアクセス権限を持ったユーザのみが、特定の端末及び特定の記録媒体への書き出しのみに限定している。 ・特定個人情報を記録した紙媒体、DVD等の外部記録媒体は施錠保管し、鍵は管理者が厳重に管理している。また、持出し・持込みのルールを定め、遵守している。 ・保管期間が経過した特定個人情報を記録した媒体は、復元不可能な状態で確実に消去・廃棄している。 ・機器を廃棄もしくはリース返却する場合、機器内部の記憶装置からすべての情報を消去し、復元不可能な状態にする措置を講じている。 ・庁内の端末の持ち出しは、業務上どうしても必要な場合、情報セキュリティ管理者の許可を得て記録をとることとしている。 ・職員(非常勤、臨時職員含む)が特定個人情報を取り扱う作業を行う場合は、インターネットへの接続、電子メールの使用、外部記録媒体への出力が不可能な端末によって行っている。 	

4. 特定個人情報ファイルの取扱いの委託		[] 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	<div> <div>[定めている]</div> <div> <div><選択肢></div> <div> 1) 定めている 2) 定めていない </div> </div> </div>	
規定の内容	<p>・情報システムの運用、保守等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結している。</p> <ul style="list-style-type: none"> ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・委託先の責任者、委託内容、作業者、作業場所の特定 ・提供されるサービスレベルの保証 ・従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務 ・再委託に関する制限事項の遵守 ・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等) ・市による監査、検査 <p><Public Medical Hub(PMH)を活用した情報連携に係る公費医療費助成事務における追加措置> 特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)を遵守し、委託契約書に以下の規定を設ける。</p> <ul style="list-style-type: none"> ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・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 ・再委託における条件 ・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 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業員の明確化 ・従業員に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項 	
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	<div> <div>[十分に行っている]</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>	
具体的な方法	<p><Public Medical Hub(PMH)を活用した情報連携に係る公費医療費助成事務における追加措置></p> <ul style="list-style-type: none"> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検(年1回程度又は随時)を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、必要であると認めるときには、デジタル庁に報告を求めることができる。 	
その他の措置の内容	<p><Public Medical Hub(PMH)を活用した情報連携に係る公費医療費助成事務における追加措置></p> <ul style="list-style-type: none"> ・委託契約書に以下の規定を設ける。 <p>委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。</p>	
リスクへの対策は十分か	<div> <div>[十分である]</div> <div> <div><選択肢></div> <div> 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 </div> </div> </div>	
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		
1. 委託先による特定個人情報の不正な取扱いに関するリスクに対する措置		

・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に対する措置

：委託先から他社への提供は認めていない。

：情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明している。

：情報資産を提供する際、必要に応じ暗号またはパスワードの設定を行っている。

：必要に応じて、市職員が現地調査を実施している。

・委託先による特定個人情報の保管・消去、委託契約終了後の不正な使用等に関するリスクに対する措置

：委託先に対して個人情報の複製、送信、持ち出し等の個人情報の適切な管理に支障を及ぼす恐れのある行為を禁止している。

：必要に応じて熊谷市は現地調査・確認を行えることとしている。

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	<div> <div>[定めている]</div> <div> <div><選択肢></div> <div> <div>1) 定めている</div> <div>2) 定めていない</div> </div> </div> </div>	
<div> <div>ルールの内容及びルール遵守の確認方法</div> </div>	<div> <div>・庁内のデータ連携については、あらかじめ定められた仕様に基づくものであり、それ以外の連携はできない。</div> <div>・具体的に誰に対し何の目的で提供できるかを書き出したマニュアルを整備しており、マニュアル通りに特定個人情報の提供を行う。年一度の研修、個人情報保護の理解度チェックを行い、マニュアルを理解しているか確認する。</div> </div>	
その他の措置の内容	<div> <div>・端末から電子媒体への出力は特定の端末に限定しており、出力時の操作ログを取得している。</div> </div>	
リスクへの対策は十分か	<div> <div>[十分である]</div> <div> <div><選択肢></div> <div> <div>1) 特に力を入れている</div> <div>2) 十分である</div> <div>3) 課題が残されている</div> </div> </div> </div>	
<div> <div>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</div> </div>		
<div> <div> <div><不適切な方法で提供・移転が行われるリスクに対する措置></div> <div> <div>・他自治体への提供については、あらかじめ定められた方法でのみ行っており、また、複数職員による確認を行っている。</div> <div>・庁内のデータ連携については、あらかじめ定められた仕様に基づくサーバ間通信に限定している。</div> </div> </div> <div> <div> <div><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に対する措置></div> <div> <div>・庁内のデータ連携については、あらかじめ定められた仕様に基づくサーバ間通信に限定している。</div> <div>・個人情報に正確かつ最新であることを、定期的に確認する手順、不正確または最新ではないことが判明した場合の訂正の手順が明確になっている。</div> </div> </div> </div> </div>		

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	<p>＜医療助成システムのソフトウェアにおける措置＞</p> <ul style="list-style-type: none"> ・中間サーバの仕様(プレフィックス情報等)に基づき、当該事務で必要となる情報以外の入手は不可能。 ・中間サーバへの情報照会処理については、業務システム側で操作ログを記録しており、処理実施者、操作内容を把握可能である。 <p>＜医療助成システムの運用における措置＞</p> <ul style="list-style-type: none"> ・権限を持った職員が上長の承認を得た上で情報照会・入手を行うこととしている。 ・医療助成システムで記録している操作ログは、適宜医療助成システムからリストの出力を行い、目的外の入手が行われていないことを定期的に確認している。 ・定められたルールに基づく入手を職員に周知、徹底している。 <p>＜中間サーバ・ソフトウェアにおける措置＞</p> <ul style="list-style-type: none"> ・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、番号利用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。 ・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止する仕組みになっている。 <p>(※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。</p> <p>(※2) 番号法第19条第8号に基づく利用 特定個人情報の提供に関する命令第2条及び番号法第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。</p> <p>(※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。</p> <p>＜中間サーバの運用における措置＞</p> <ul style="list-style-type: none"> ・不正検知の目的で、ログを定期的に確認する。 ・中間サーバ接続端末の情報照会機能(特定個人情報の情報照会及び情報提供受領)の利用にあたっては、事前に情報照会の内容について、上長の承認を得た上で実施する運用を義務付けている。
リスクへの対策は十分か	<div> <div>[十分である]</div> <div> <div>＜選択肢＞</div> <div> 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 </div> </div> </div>

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

◆入手した特定個人情報が不正確であるリスク

＜医療助成システムのソフトウェアにおける措置＞

・中間サーバの仕様(プレフィックス情報等)に基づき入手するため、入手した特定個人情報の正確性は医療助成システムで担保されている。

・医療助成システムで中間サーバから特定個人情報を入手する際、文字コード、型等の変換の正確性をテストで担保している。

＜中間サーバ・ソフトウェアにおける措置＞

・中間サーバは、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係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が担保されている。

＜中間サーバの運用における措置＞

・中間サーバ接続端末から情報提供を入手し、医療助成システムへ登録する場合、複数の職員によるチェックを行って登録している。

◆入手の際に特定個人情報漏えい・紛失するリスクに対する措置

＜医療助成システムのソフトウェアにおける措置＞

・中間サーバ・医療助成システム間は、データセンター内のサーバ間通信に限定して、漏えい・紛失するリスクを排除している。

＜医療助成システムの運用における措置＞

・権限を持った職員が上長の承認を得た上で情報照会・入手を行うこととしている。

・外部から不正なアクセスがないか、アクセスログ等を確認している。

＜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している(※)。

・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ている。

・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、特定個人情報漏えい・紛失するリスクを軽減している。

・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になっている。

(※) 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っており、照会者の中間サーバ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・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している。

・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している。

・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。

＜中間サーバの運用における措置＞

・中間サーバ接続端末に用いる外部記憶媒体(USB等)を限定する。

・中間サーバ接続端末から外部記憶媒体に特定個人情報を格納する際には暗号化を行っている。

・外部記憶媒体(USB等)の貸出、利用、データ消去、返却等の定められた運用ルールに従い実施し、貸出、返却時には上長の承認を得ている。

◆不適切な方法で提供されるリスク

＜医療助成システムのソフトウェアにおける措置＞

・中間サーバ・医療助成システム間は、データセンター内のサーバ間通信に限定しており、他の経路で提供できない。

・医療助成システムは、ID/パスワードと生体による2因子認証を行い、限られた職員のみ操作可能である。

・医療助成システム以外から情報提供できないようシステム上で担保している。

＜医療助成システムの運用における措置＞

・情報提供内容の自動応答が出来ない場合を想定し、手動で情報提供を行う場合は、上長への確認を行った上で、実施することを運用している。

ルールとして義務付けられている。

＜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上で提供を行う仕組みになっている。

・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になっている。

(※)暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能。

＜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している。

・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している。

・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している。

＜中間サーバの運用における措置＞

・不正検知の目的で、ログを定期的に確認する。

◆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に対する措置

＜医療助成システムのソフトウェアにおける措置＞

・医療助成システムの情報提供機能は、中間サーバの仕様に基づき設計、テストを行っているため、誤った情報を提供してしまうリスクを排除している。

＜医療助成システムの運用における措置＞

・中間サーバに登録する特定個人情報については、登録時に複数の職員によるチェックに加え上長の承認を経た上で登録する。

・中間サーバには可能な限り最新の情報を登録すること、誤った情報を登録した場合などの対応ルールを定め、当該ルールに従って実施している。

＜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上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。

・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内容を確認できる手段を準備することで、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。

・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している。

(※)特定個人情報を副本として保存・管理する機能。

＜中間サーバの運用における措置＞

・中間サーバ接続端末から情報提供内容を登録する場合、上長の承認を得た上で、登録時に複数の職員によるチェックを行う。

・中間サーバ接続端末から誤った情報を修正する場合、事前に修正内容について、上長の承認を得た上で、実施する運用を義務付けている。

・情報提供は自動応答又は中間サーバ接続端末に限定し、実施手順を運用ルールに定め、職員へ運用ルールの周知を徹底している。

◆その他の措置

＜熊谷市における措置＞

・医療助成システム、中間サーバ接続端末での情報照会、情報提供等に係る実施手順を業務マニュアルに記載し、新規従業者に対して、年1回研修を実施している。

＜中間サーバ・ソフトウェアにおける措置＞

・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になっている。

・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。

＜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、安全性を確保している。

・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している。

・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。

・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・運用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	[十分にしている]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
②過去3年以内に、評価実	[発生あり]	＜選択肢＞

<p>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</p>	<p>「元エの」</p> <p>1) 発生あり</p> <p>2) 発生なし</p>
<p>その内容</p>	<ul style="list-style-type: none"> ・データ入力業務において、委託業者が当市の承諾を得ないまま8,170件を再委託し、そのうち6,312件に特定個人情報が含まれていた。 ・職員等の健康診断の委託において、受託者のシステムがランサムウェアによる不正アクセス攻撃を受けた。
<p>再発防止策の内容</p>	<ul style="list-style-type: none"> ・法令に定める安全管理措置を講じることを明記し、委託業者の定める特定個人情報に関する取扱規程等を提出させることとした。また、再委託の有無を事前に書面にて報告させ、かつ、再委託するときには書面にて申請させることとした。 ・受託者がセキュリティ対策の強化を行うことから、作業完了後を目途に実地検査を行い、個人情報の管理状況を確認する。
	<p>▼物理的対策</p> <p>＜熊谷市における措置＞</p> <ul style="list-style-type: none"> ・特定個人情報を保管するサーバ設置場所には、入退室管理を行っている。 ・特定個人情報を保管するサーバに係る脅威に対して、無停電電源装置の設置、室温管理、ケーブルの安全管理、耐震対策、防火措置、防水措置等を講じている。 ・特定個人情報を保有するサーバが設置された専用の部屋への入室はICカードと生体による2因子認証で管理されている。 ・特定個人情報を保有するサーバが設置された部屋には監視カメラ等が設置されている。 ・特定個人情報を保有するサーバが設置されたラックは施錠管理されている。 ・特定個人情報を保有するサーバは定期的に保守点検を実施することで情報の毀損等への対策を図っている。 ・特定個人情報を含む電子データを定期的に電子媒体に保存し、入退室管理された専用の保管場所に保管している。 <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することとしている。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。 <p>＜ガバメントクラウドにおける措置＞</p> <ul style="list-style-type: none"> ・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。 ・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。 <p>◆技術的対策</p> <p>＜熊谷市における措置＞</p> <ul style="list-style-type: none"> ・ウィルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。 ・OSやアプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆるセキュリティパッチ)を適用している。 ・ファイアウォールにより、特定個人情報へのアクセスを制御している。 ・使用されていないポートを閉鎖している。 ・情報漏えい等の防止のため、特定個人情報を保有するサーバをインターネット等の外部ネットワークから隔離されたネットワーク内に設置している。

その他の措置の内容

かつ物理的にサーバ・ネットワーク上に設置している。

- ・盗聴による情報漏えい等の防止のため特定個人情報を保有するサーバとの通信を暗号化している。
- ・内部の部品が2重化された高可用性の外部記憶装置(ストレージ)に特定個人情報を保存することで情報の毀損等への対策を図っている。
- ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。

<中間サーバ・プラットフォームにおける措置>

- ・中間サーバ・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。
- ・中間サーバ・プラットフォームでは、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。
- ・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の適用を行う。

<サービス検索・電子申請機能における措置>

専用線であるLGWAN回線を用いているため、盗聴による情報漏えい等の防止のため特定個人情報を保有するサーバとの通信を暗号化している。

<ガバメントクラウドにおける措置>

- ・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。
- ・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。
- ・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。
- ・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。
- ・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及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。
- ・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。
- ・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。
- ・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。

<Public Medical Hub(PMH)を活用した情報連携に係る公費医療費助成事務における追加措置>

○物理的対策

Public Medical Hub(PMH)は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバー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、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正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。

○技術的対策

Public Medical Hub(PMH)は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバー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、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正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本市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(デジタル庁)や医療機関及び住民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。
- ・本市の端末とPublic Medical Hub(PMH)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。
- ・本市の端末とPublic Medical Hub(PMH)との通信はLGWAN回線又は閉域網VPN等に限定されている。
- ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。
- ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。〇

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		
<p><特定個人情報が古い情報のまま保管され続けるリスクに対する措置></p> <ul style="list-style-type: none"> ・基本的に届出・申請等に基づき、更新を実施しているが、情報に誤りがある場合は、職権により修正を行っている。 <p><特定個人情報が消去されずいつまでも存在するリスクに対する措置></p> <ul style="list-style-type: none"> ・特定個人情報の消去にあたっては、消去の必要性があれば、業務責任者の承認を得た上で実施する。 ・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、NIST 800-88、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(ガバメントクラウドにおける措置)。 		

8. 監査	
実施の有無	<input type="checkbox"/> 自己点検 <input type="checkbox"/> 内部監査 <input type="checkbox"/> 外部監査
9. 従業員に対する教育・啓発	
従業員に対する教育・啓発	<div> <input type="checkbox"/> 十分に行っている </div> <div> <input type="checkbox"/> 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 </div>
具体的な方法	<p><熊谷市における措置></p> <ul style="list-style-type: none"> ・毎年、職員全員と、該当の臨時職員に情報セキュリティ研修を実施している。 ・サーバ室への入退室については、生体情報による認証を実施している。 ・年に1回、所属部署の担当者に対し、教育を実施している。 ・集合教育は必要に応じて実施している。 <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"> ・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・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	
<p><中間サーバ・プラットフォームにおける措置></p> <p>・中間サーバ・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。</p> <p><ガバメントクラウドにおける措置></p> <p>ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。</p> <p>ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。</p> <p>具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。</p>	

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	郵便番号360-8601 熊谷市宮町2丁目47番地1 熊谷市総務部庶務課行政係 電話048-524-1111 内線223
②請求方法	個人情報の保護に関する法律、熊谷市個人情報の保護に関する法律施行条例及び熊谷市個人情報の保護に関する法律施行細則に基づき、請求書に住所、氏名、請求内容等の必要事項を記入し、請求する。 個人情報の本人であることを証明する書類等を持参の上、個人情報保護窓口に提出する。
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	郵便番号360-8601 熊谷市宮町2丁目47番地1 熊谷市福祉部こども課給付係 電話048-524-1111 内線372
②対応方法	問い合わせの受付時に受付票等を記載することにより、対応について記録を残す。 情報漏えい等の重大な事案に関する問い合わせについて、関係先等に事実確認を行うための標準的な処理期間を設ける。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和6年12月25日
②しきい値判断結果	[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)] <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	

(別添2) 変更箇所

[illegible]