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
17	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務　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、新型インフルエンザ等対策特別措置法による予防接種の実施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2年11月16日

［平成30年５月　様式３］

項目一覧

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	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務
②事務の内容	熊谷市は、新型インフルエンザ等対策特別措置法及び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（以下「番号利用法」という。）の規定に従い、特定個人情報を以下の事務で取り扱う。 新型インフルエンザ等が発生した場合に、特定接種や、住民に対する予防接種、予診票の発行等を行う。番号利用法別表第二に基づき、新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。情報提供に必要な情報を「副本」として中間サーバーへ登録する。 具体的には、特定個人情報ファイルを次の事務に使用している。 ①住民基本台帳をもとに、予防接種対象者の選定 ②個人番号を用い、予防接種実施の登録（予防接種の種類、実施日、実施場所等） ③照会申請による予防接種履歴の照会 ④委託料の支払い ⑤交付申請による転入者・予診票紛失者への予診票配布等 ⑥定期接種により健康被害が生じた場合の給付金の支給
③対象人数	[　10万人以上30万人未満　]　＜選択肢＞ 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

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	健康情報システム
②システムの機能	予防接種 ・医療機関から送付された予診票を基に予防接種の接種実績の登録を行う。 ・接種種別、接種区分、宛名番号、生年月日、性別、LotNo、接種量、接種医療機関、接種年月日、請求月、実施場所、予診区分、予診医療機関、予診医師、接種医師、ワクチン会社等の管理を行う。 ・個人毎の予防接種の実績情報、接種可能範囲等の参照を行う。 ・指定した検索条件に該当した住民情報の表示とファイル出力を行う。
③他のシステムとの接続	[　]情報提供ネットワークシステム　[○]庁内連携システム [　]住民基本台帳ネットワークシステム　[　]既存住民基本台帳システム [○]宛名システム等　[　]税務システム [　]その他　（　）
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	1. 個人番号管理機能 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。 2. アクセス制御機能 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。 3. 個人番号確認機能 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。 4. 中間サーバー連携機能 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、中間サーバーへ連携する機能。
③他のシステムとの接続	[　]情報提供ネットワークシステム　[○]庁内連携システム [　]住民基本台帳ネットワークシステム　[○]既存住民基本台帳システム [○]宛名システム等　[○]税務システム [○]その他　（中間サーバー、健康情報システム、個別業務システム）

システム3	
①システムの名称	中間サーバー
②システムの機能	1．符号管理機能 情報照会・情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐づけ、その情報を保管・管理する機能。 2．情報照会機能 情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報提供受領（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及び当該特定個人情報（連携対象）の提供を行う機能。 4．既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住民基本台帳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、又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 中間サーバーと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）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 セキュリティを管理するための機能。 9．職員認証・権限管理機能 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（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 処理状況の管理、業務統計情報の集計、稼働状態の通知、保管期限切れ情報の削除を行う機能。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [○] 宛名システム等　　[　　] 税務システム [　　] その他　（　　）
システム4	
①システムの名称	共通基盤システム（庁内連携システム）
②システムの機能	1．統合データベース機能 個別業務システム間で必要となる連携データを一括管理し、個別業務システムへ提供する機能。 2．共通管理機能 各業務システムを利用する際に必要となる認証やアクセス制御等の管理機能を一元化した機能。
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [○] 宛名システム等　　[○] 税務システム [○] その他　（ 健康情報システム、個別業務システム　　）
システム6～10	
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
1. 予防接種ファイル	
4. 個人番号の利用 ※	
法令上の根拠	1. 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（番号利用法） （平成25年5月31日法律第27号） ・番号利用法第9条第1項　別表第一の93の2の項 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第一の主務省令で定める事務を定める命令（別表第一省令） （平成26年内閣府・総務省令第5号） ・別表第一省令第67条の2
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	1. 番号利用法第19条第7号（特定個人情報の提供の制限）及び別表第二 （別表第二における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（特定個人情報）に「新型インフルエンザ等対策特別措置法（平成二十四年法律第三十一号）による予防接種の実施に関する情報であって主務省令で定めるもの」が含まれる項（115の2の項） （別表第二における情報照会の根拠） ：第一欄（情報照会者）が「市町村長」の項のうち、第二欄（事務）に「新型インフルエンザ等対策特別措置法（平成二十四年法律第三十一号）による予防接種の実施に関する事務であって主務省令で定めるもの」が含まれる項（115の2の項） 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第二の主務省令で定める事務及び情報を定める命令（別表第二省令） （平成26年内閣府・総務省令第7号） （別表第二主務省令における情報提供の根拠） ・別表第二省令（第59条の2） （※別表第二の115の2の項） （別表第二主務省令における情報照会の根拠） ・別表第二省令（第59条の2） （※別表第二の115の2の項）
6. 評価実施機関における担当部署	
①部署	市民部　健康づくり課
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		
1. 予防接種ファイル		
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 ※		当該市町村の区域内に居住する予防接種の対象となる者
	その必要性	予防接種に関する業務の実現のために、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 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[○] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	＜個人番号、その他識別情報（内部番号）＞ ・本人確認等、対象者を正確に特定するために保有 ＜4情報、その他住民票関係情報＞ ・予防接種対象者の居住地を把握するために保有 ＜健康・医療関係情報（予防接種に関する情報）＞ ・予防接種の接種実績、接種料金等を把握するために保有
	全ての記録項目	別添1を参照。
⑤保有開始日		令和3年4月1日
⑥事務担当部署		市民部　健康づくり課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署　（　　） [○] 行政機関・独立行政法人等　（　　） [○] 地方公共団体・地方独立行政法人　（　　） [　　] 民間事業者　（　　） [○] その他　（ 住民基本台帳ネットワークシステム　　）
②入手方法		[○] 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 [　　] 電子メール　[　　] 専用線　[○] 庁内連携システム [○] 情報提供ネットワークシステム [○] その他　（ 住民基本台帳ネットワークシステム　　）
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	市民部　健康づくり課
	使用者数	[　　10人以上50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		・予防接種の実施、予防接種に関する記録の作成等に使用する。
	情報の突合	・住民からの費用助成申請書等の内容と地方税関係情報を突合する。
⑥使用開始日		令和3年4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] （ 1 ） 件	<選択肢> 1）委託する 2）委託しない
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		[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		株式会社ジーシーシー	
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　※	＜熊谷市における措置＞ ・サーバーは、入退室管理を行っているデーターセンターのサーバー室に設置している。 ・入退室管理は、サーバー室への入室権限を持つ者を事前申請により限定し、サーバー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。 ＜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ー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ー室に設置された中間サーバー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。
7. 備考	

（別添1）特定個人情報ファイル記録項目

1．予防接種ファイル

【識別情報】
1.個人番号,2.宛名番号

【連絡先情報】
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.接種種別、2.接種区分、3.宛名番号、4.生年月日、5.性別、6..Lot No、7.接種量、8.接種_医療機関id、9.接種年月日、10.請求月、
11.実施場所id、12.予診区分、13.予診_医療機関id、14.予診_医師id、15.接種_医師id、16.合併前市町村、17.ワクチン会社、
18.二混合区分、19.初回ワクチン区分、20.ツベルクリン判定、21.ツベルクリン判定（大きさ：縦）、22.ツベルクリン判定（大きさ：横）、
23.ツベルクリン判定（状態）、24.エラーコード、25.備考

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	・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、職員2名以上でダブルチェックを行って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。
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	

＜不適切な方法で入手が行われるリスクに対する措置＞
・庁内連携機能からの住基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。

＜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＞
・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。

＜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＞
・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、事務に必要の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	・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。 ・健康情報システムには、健康管理事務に関係のない情報を保有しない。 ・健康情報システムでは、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。 ・特定個人情報を使用できる事務については、業務マニュアルに記載し、定期的に職員研修を実施している。
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
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	・健康情報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。
その他の措置の内容	＜アクセス権限の発効・失効の管理＞ ・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。 ・健康情報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。 ＜アクセス権限の管理＞ ・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。 ＜特定個人情報の使用の記録＞ ・ユーザIDとともに、健康情報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	[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

＜従業者が事務外で使用するリスクに対する措置＞
・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。

＜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＞
・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	[　　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	・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。 ・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	
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	[　　再委託していない　　]	＜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		
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		
＜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、熊谷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＞		

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	[　　定めている　　]	＜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	・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。 ・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。	
その他の措置の内容	・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。	
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		
＜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＞ ・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。 ・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。 ＜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＞ ・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。 ・個人情報が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。		

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	＜健康情報システムのソフトウェアにおける措置＞ ・中間サーバーの仕様（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。 ・中間サーバー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。 ＜健康情報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。 ・健康情報システムで記録している操作ログは、適宜、健康情報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。 ＜中間サーバー・ソフトウェアにおける措置＞ ・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、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。 ・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）番号法の規定によ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に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※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。 ＜中間サーバー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。 ・中間サーバー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	[　　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： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜健康情報システムのソフトウェアにおける措置＞ ・中間サーバーの仕様に基づき提供するため、不正に特定個人情報が提供されないよう健康情報システムで担保している。 ・特定個人情報の提供は健康情報システムでの連携に限定しており、人の手を介在できない。 ＜健康情報システムの運用における措置＞ ・健康情報システムで記録している操作ログは、適宜リストの出力を行い、不正な提供が行われていないことを定期的に確認している。 ・提供に制限のある特定個人情報は、適切に不開示設定を行う実施手順を運用ルールに定め、当該ルールに従い実施している。 ・自動応答不可の特定個人情報の提供に当たっては、上長の承認を得た上で、提供を実施する運用を義務付けている。 ＜中間サーバー・ソフトウェアにおける措置＞ ①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用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合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している。 ②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している。 ③機微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及び情報提供を行う機能。 ＜中間サーバー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。 ・中間サーバー接続端末の情報提供機能の利用にあたっては、事前に情報提供の内容について、上長の承認を得た上で、提供を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	[　　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

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

◆安全が保たれない方法によって入手が行われるリスク
＜健康情報システムのソフトウェアにおける措置＞
・中間サーバー－健康情報システム間は、データセンタ内のサーバ間通信に限定して安全性を確保している。

＜中間サーバー・ソフトウェアにおける措置＞
・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。
・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。
＜中間サーバー･プラットフォームにおける措置＞
・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。
・中間サーバーと団体については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、中間サーバー・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、中間サーバー･プラットフォームの事業者における情報漏えい等のリスクを極小化する。

◆入手した特定個人情報が不正確であるリスク
＜健康情報システムのソフトウェアにおける措置＞
・中間サーバーの仕様（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健康情報システムで担保されている。
・健康情報システムで中間サーバー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。

＜中間サーバー・ソフトウェアにおける措置＞
・中間サーバーは、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。

＜中間サーバーの運用における措置＞
・中間サーバー接続端末から情報提供を入手し、健康情報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が漏えい・紛失するリスク
＜健康情報システムのソフトウェアにおける措置＞
・中間サーバー－健康情報システム間は、データセンタ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。
＜健康情報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。
＜中間サーバー・ソフトウェアにおける措置＞
・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（※）。
・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、特定個人情報が漏えい・紛失するリスクを軽減している。
・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。
（※）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。
＜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。
・中間サーバーと団体については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。
・中間サーバー･プラットフォーム事業者の業務は、中間サーバー・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。
＜中間サーバーの運用における措置＞
・中間サーバー接続端末に用いる外部記憶媒体（USB等）を限定する。
・中間サーバー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
＜健康情報システムのソフトウェアにおける措置＞
・中間サーバー－健康情報システム間は、データセンタ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。
・健康情報システムは、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。
・健康情報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。

＜健康情報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ルールとして義務付けている。
＜中間サーバー・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。
（※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。
＜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。
・中間サーバーと団体については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。
・中間サーバー・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。
＜中間サーバー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。
・情報提供は自動応答又は中間サーバー接続端末に限定し、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。

◆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
＜健康情報システムのソフトウェアにおける措置＞
・健康情報システムの情報提供機能は、中間サーバー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。
＜健康情報システムの運用における措置＞
・中間サーバー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。
・中間サーバー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。
＜中間サーバー・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。

＜中間サーバーの運用における措置＞
・中間サーバー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。
・中間サーバー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。

◆その他
＜熊谷市における措置＞
・健康情報システム、中間サーバー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。
＜中間サーバー・ソフトウェアにおける措置＞
・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。
・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。
＜中間サーバー･プラットフォームにおける措置＞
・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。
・中間サーバーと団体については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、中間サーバー・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、中間サーバー・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

◆物理的対策
＜熊谷市における措置＞
・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。

＜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。
・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、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。

◆技術的対策
＜熊谷市における措置＞
・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(いわい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、パターンファイルの更新を行う。
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の適用を行う。

8. 監査	
実施の有無	[○] 自己点検　　[　　] 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	＜熊谷市における措置＞ ・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OA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。 ＜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材を作成し、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
＜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。

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 熊谷市宮町二丁目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	熊谷市個人情報保護条例に基づき、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360-0014 埼玉県熊谷市箱田一丁目2番39号 熊谷市市民部健康づくり課 電話048-528-0601
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3年11月10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	

（別添2）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明