

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
14	健康増進法に関する事務 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、健康増進法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7年5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

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) 成人保健ファイル	
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 ※	熊谷市に居住する健康増進法による健康増進事業の対象となる者
その必要性	健康増進法による健康増進事業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	[100項目以上] <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="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="checkbox"/>] 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="checkbox"/>] 地方税関係情報 [<input type="radio"/>] 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="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	<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> ・検診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(検診に関する情報)、医療保険関係情報> ・検診の受診履歴、検診の一部負担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	平成30年12月
⑥事務担当部署	市民部 健康づくり課 熊谷保健センター

3. 特定個人情報の入手・使用		
①入手元 ※	<input checked="" type="checkbox"/> 本人又は本人の代理人 <input checked="" type="checkbox"/> 評価実施機関内の他部署 (市民部市民課) <input type="checkbox"/> 行政機関・独立行政法人等 () <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 (他市区町村) <input checked="" type="checkbox"/> 民間事業者 (検診実施医療機関) <input type="checkbox"/> その他 ()	
②入手方法	<input checked="" 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 checked="" type="checkbox"/> 庁内連携システム <input checked="" type="checkbox"/> 情報提供ネットワークシステム <input checked="" type="checkbox"/> その他 (住民基本台帳ネットワークシステム)	
③使用目的 ※	健康増進法に基づく検診の適正な実施をし、検診結果及び受診歴を管理するため。	
④使用の主体	使用部署	市民部 健康づくり課 熊谷保健センター
	使用者数	<input type="checkbox"/> 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	①検診対象者の特定 ②検診結果の登録 ③検診結果について、情報提供ネットワークシステムを介して本人への情報提供	
情報の突合	健康情報システムへの検診結果データ登録時に内部識別番号である宛名番号(氏名、生年月日)と住基情報を突合する。	
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 ※	[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	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 ※	[再委託する] <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	再委託先及び再々委託先から承諾申請書の提出があり、内容を審査したところ適正であると認められたため承諾している。
	⑥再委託事項	システムの運用・保守業務、法制度改正に伴う改修作業全般
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

(別添1) 特定個人情報ファイル記録項目

1. 成人保健ファイル

【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】

(共通管理項目)

1. 西暦年度、2. 受診日、3. 受診日年齢、4. 年度末年齢、5. 受診番号、6. 特記事項、7. 検診方式、8. 実施医療機関、9. 実施区分、10. 登録日、11. 請求日(月)、12. 紹介先医療機関、13. 実施場所

(胃がん検診_一次)

14. 検査方法、15. 受診歴、16. 診断名、17. 内_検査結果、18. 総合指導区分

(肺がん検診_一次)

14. 胸部エックス線判定、15. 喀痰判定、16. 喫煙本数、17. 喫煙年数、18. 喫煙指数、19. 受診歴、20. 喀痰容器配布、21. 喀痰受診歴、22. 喀痰検体提出、23. 喫煙指数該当、24. 総合指導区分

(大腸がん検診_一次)

14. 便潜血反応1日目、15. 便潜血反応2日目、16. 受診歴、17. 総合指導区分

(子宮頸がん検診_一次)

14. 頸部ベセスダ区分、15. 体部区分、16. 体部判定、17. 診断名、18. 体部受診歴、19. 検診種別、20. 検体の適否、21. 頸部ベセスダ判定、22. 無料クーポン利用、23. 1次検診日、24. HPV検査、25. 総合指導区分

(乳がん検診_一次)

14. マンモグラフィーカテゴリ、15. X線_所見・判定、16. 受診歴、17. クーポン区分、18. 総合判定、19. 総合指導区分

(前立腺がん検診_一次)

14. PSA、15. 判定

(骨粗しょう症検診_一次)

14. 方法、15. 骨量値、16. 検査判定、17. 総合指導区分

(肝炎ウイルス検診_一次)

14. B型肝炎_判定、15. C型肝炎_判定

(歯と口の健康診査_一次)

14. 健全歯数、15. 未処置歯数、16. 処置歯数、17. 要補綴歯数、18. 欠損補綴歯数、19. 現在歯数、20. 歯肉出血BOP(17または16)、21. 歯肉出血BOP(11)、22. 歯肉出血BOP(26または27)、23. 歯肉出血BOP(47または46)、24. 歯肉出血BOP(31)、25. 歯肉出血BOP(36または37)、26. 歯肉出血BOP(最大値)、27. 歯周ポケットPD(17または16)、28. 歯周ポケットPD(11)、29. 歯周ポケットPD(26または27)、30. 歯周ポケットPD(47または46)、31. 歯周ポケットPD(31)、32. 歯周ポケットPD(36または37)、33. 歯周ポケットPD(最大値)、34. 歯石の付着、35. 口腔内の状態、36. 粘膜所見、37. 総合指導区分

(胃がん検診_精密)

14. 医療、15. 診断名、16. がんの深達度、17. がんの内訳【旧】、18. 診断・所見

(肺がん検診_精密)

14. 診断名、15. 切除の根治性、16. 組織分類、17. 病期、18. がん内訳、19. 医療

20. 喀痰検査による要精検、21. 診断・所見

(大腸がん検診_精密)

14. その他疾患【旧】、15. 検査、16. 医療、17. その他の疾患、18. がんの深達度、19. 検査【旧】、

20. がんの深達度【旧】、21. がんの内訳、22. 診断・所見

(子宮頸がん検診_精密)

14. がんの内訳【旧】、15. 医療、16. HPV検査、17. 診断・所見、18. 進行期、19. 判定

(乳がん検診_精密)

14. 医療、15. 病期、16. がん内訳、17. 診断・所見

(前立腺がん検診_精密)

14. 診断・所見、15. 医療

(歯と口の健康診査_精密)

14. 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	
(1)成人保健ファイル	
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。 ・業務上認められた内容以外は照会できないよう、システムで制限をかけている。 ・操作者に対しては個人ごとのID及びパスワードでアクセス制限をかけ、目的外の入手を行うことはできない。
リスクへの対策は十分か	<p style="text-align: center;">[十分である] <選択肢></p> <p style="text-align: center;">1) 特に力を入れている 2) 十分である</p> <p style="text-align: center;">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><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。 <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。 ・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	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[十分である]</div> <div> <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> </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 style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[行っている]</div> <div> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p> </div> </div>
具体的な管理方法	<ul style="list-style-type: none"> ・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	<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。 ・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。 <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、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	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[十分である]</div> <div> <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> </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

<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ー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。

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
ルール内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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		
<p><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></p> <ul style="list-style-type: none"> ・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。 <p><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></p> <ul style="list-style-type: none"> ・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。 		

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

◆ 女直が採たイロない方法によつ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た特定個人情報入手のみ実施できるよう設計されるため、安全性が担保されている。

<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。

◆ 入手した特定個人情報に不正であるリスク

<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制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会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、ログを定期的を確認する。
- ・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、新規従業員に対して、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

を行う。

③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。

④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。

⑤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。

⑥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。

⑦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。

⑧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。

<p>リスクへの対策は十分か</p>	<p>[十分である]</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>
<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>		
<p>◆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。</p> <p><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。</p> <p>◆技術的対策 <熊谷市における措置> ・ウイ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。</p> <p><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。 ・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。</p> <p><ガバメントクラウドにおける措置> 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。</p>		

8. 監査

実施の有無	<input checked="" type="checkbox"/> 自己点検 <input type="checkbox"/> 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	<input type="checkbox"/> 十分に行っている <input type="checkbox"/> 十分にいない
具体的な方法	<p><選択肢></p> <p>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</p> <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。 <p><中間サーバー・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・運用規則等に基づき、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、定期的に自己点検を実施することとしている。

10. その他のリスク対策

<p><中間サーバー・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。 <p><ガバメントクラウドにおける措置></p> <p>◆監査</p> <p>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、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。</p> <p>◆その他</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	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、個人情報保護窓口へ提出する。
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 熊谷市箱田一丁目2番39号 熊谷市市民部熊谷保健センター 電話048-526-5737
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	—

