特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
	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　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

本市は，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り扱いにあたり，特定個人情報ファイルの取り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

柏市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［平成30年５月　様式４］

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　※	本市は，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。番号法第19条第8号に基づき，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する。 ①住民基本台帳を基に予防接種対象者の選定 ②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交付申請による転入者・予診票紛失者への予診票発行等 ⑤予防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	[　30万人以上　] ＜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 5) 30万人以上

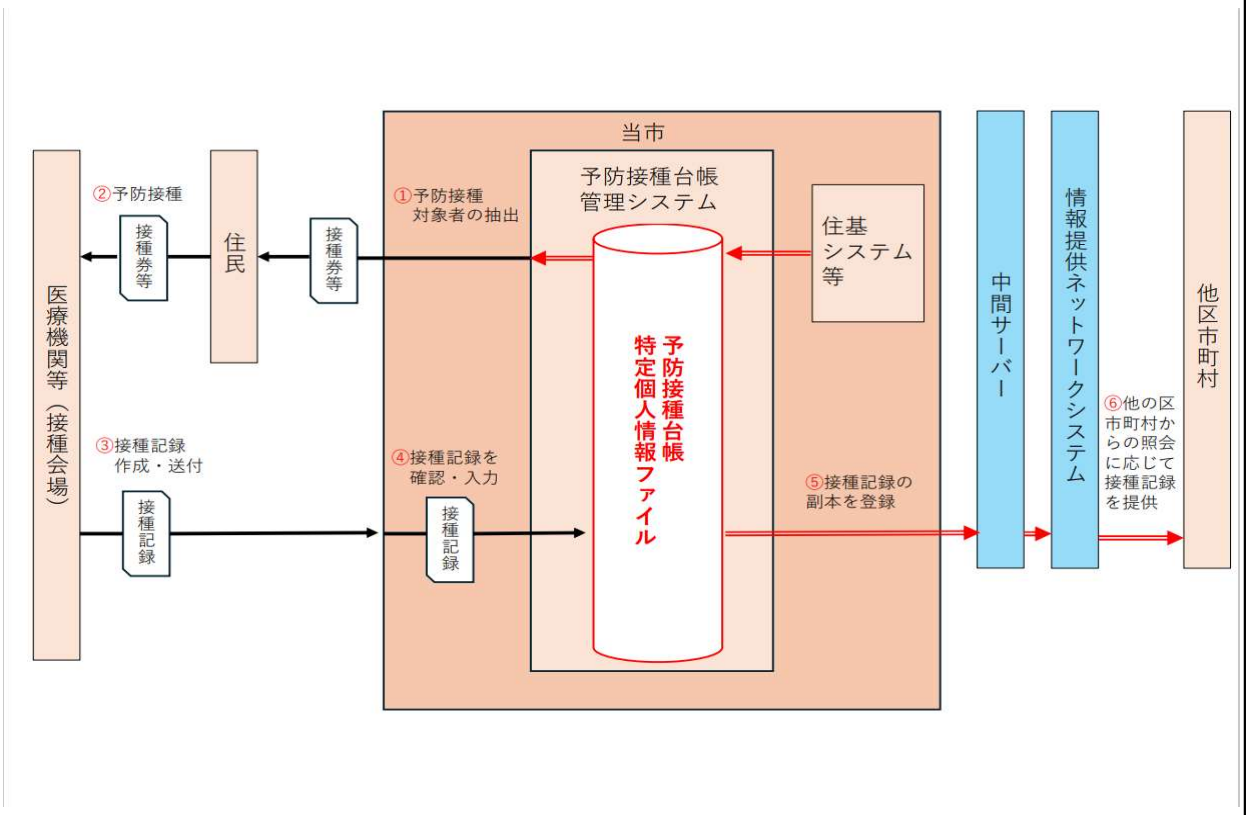
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	保健所情報システム
②システムの機能	・予防接種台帳管理（予防接種履歴の管理，対象者への個別通知，統計処理） ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[ ] 庁内連携システム [ ] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[ ] 税務システム [ ] その他　（　）
システム2～5	
システム2	
①システムの名称	共通宛名システム
②システムの機能	1．宛名管理機能 住民記録システム既存住民基本台帳システムより情報移転を行い4情報（氏名，性別，生年月日，住所），その他住民票関係情報を記録する。住登外者の宛名項目（氏名及び名称，性別，生年月日，住所など）の作成・管理をする。 2．個人番号の保護機能 個人番号の保護を行うため認証の制御や暗号化をする。 3．宛名連携機能 同一人の宛名番号を紐付する機能を有し，宛名番号の関連付けしたデータを作成・管理する。中間サーバーとの連携時には，紐付した宛名番号から団体内宛名番号を取得する。 4．団体内宛名統合機能 提供を行うため税務システム等から提供するデータを受け，中間サーバーへ送信する。情報の照会を行うため税務システム等からの要求情報を受け，中間サーバーへ送信し結果を受信をする。符号付番の際に符号と紐付ける団体内統合宛名番号を中間サーバーへ送信する。団体内宛名番号と4情報（氏名，性別，生年月日，住所）を管理し，中間サーバーからの要求に対応する。 5．中間サーバー連携機能 中間サーバーとの連携によりデータの送信・受信を行う。データの送信・受信を行った結果の情報を取得・管理する。
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 　符号管理機能は，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」とを紐付け，その情報を保管・管理する。 2．情報照会機能 　情報照会機能は，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。 3．情報提供機能 　情報提供機能は，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。 4．既存システム接続機能 　中間サーバーと既存システム，宛名システム及び住民記録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。 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。 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。 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。 8．セキュリティ管理機能 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。 10．システム管理機能 　バッチ処理の状況管理，業務統計情報の集計，稼動状態の通知，保管切れ情報の削除を行う。
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4	
システム5	
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	
予防接種の実施及び履歴管理ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	予防接種の対象者及び接種履歴を正確に把握し，適正な管理を行うため。
②実現が期待されるメリット	新型インフルエンザ等蔓延防止
5. 個人番号の利用　※	
法令上の根拠	1　番号法第9条第1項　別表の126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の主務省令で定める事務を定める命令 （平成26年内閣府、総務省令第5号） ・第67条の2 3　番号法第19条第6号
6. 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　番号法第19条第8号 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第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁、総務省令第9号） ・省令第2条の表　25,26,27,28,29,153,154の項
7. 評価実施機関における担当部署	
①部署	柏市健康医療部健康増進課
②所属長の役職名	次長兼課長
8. 他の評価実施機関	

（別添1）事務の内容

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全体システム



（備考）

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	
予防接種の実施及び履歴管理ファイル	
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 ※	新型インフルエンザ等対策特別措置法に基づく接種対象者
その必要性	予防接種に関する業務実現のために，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	○識別情報 ・個人番号，個人番号対応符号・・・手続時点において同一人の確認・特定をより的確に行うために必要である。 ・その他識別情報（内部番号）・・・庁内連携システムで利用する識別情報（世帯コード・個人コード）についても本人特定の他，庁内他事務のシステムと必要な情報を連携するために必要である。 ○連絡先等情報 ・4情報，連絡先(電話番号等)については，届出(申請)者に対する届出内容の確認，問い合わせのために必要である。 ○業務関係情報 ・健康・医療関係情報・・・予防接種情報は，予防接種の適切な実施及び接種履歴の管理をするために必要である。 ・生活保護・社会福祉関係情報・・・生活保護受給者については，予防接種費用が免除対象となるので，生活保護の受給状況に関する情報が必要である。
全ての記録項目	別添2を参照。
⑤保有開始日	令和8年4月
⑥事務担当部署	柏市健康医療部健康増進課

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　（ 市民生活部　市民課 ） [　] 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　（ ）
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　（ ）
③入手の時期・頻度		住民基本情報： （入手元）市民生活部市民課 （入手頻度・時期）バッチ処理による日時連携 （入手方法）庁内連携システム 接種記録： （入手元）接種を行った医療機関又は本人等 （入手頻度・時期）入手元が医療機関の場合は月1回，入手元が本人等の場合は随時 （入手方法）郵送あるいは持込み 健康被害救済の申請： （入手元）接種を行った本人等 （入手頻度・時期）随時 （入手方法）紙
④入手に係る妥当性		・住民基本情報：庁内連携システムを使用して入手する住民基本情報については，本人等からの申請を受けた都度入力する必要があり，法令等に基づく接種対象者であることの確認を行うものである。 ・接種記録：医療機関や本人等から入手する接種記録については，予防接種法施行規則第3条に示されているとおり，記録・保管することを目的に入手するものである。 ・予防接種による健康被害救済の申請については，予防接種法施行規則第10条及び第11条に基づいて入手している。
⑤本人への明示		・庁内連携システムの場合は，番号法第19条8号及び予防接種法施行規則に基づき取得・利用している。 ・医療機関又は本人から入手する場合は，本人等が記入する予診票にも，市へ接種記録を提出されることを明記し，署名を得ている（予防接種法施行規則第3条）。 ・予防接種による健康被害救済の申請については，予防接種法施行規則第10条及び第11条に明記している。
⑥使用目的 ※		接種対象者の接種要件等を把握する必要があるため
	変更の妥当性	－
⑦使用の主体	使用部署 ※	健康医療部健康増進課
	使用者数	[　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
⑧使用方法 ※		Ⅰ対象者抽出事務：対象者を抽出する。 Ⅱ予防接種管理事務：個人の予防接種の接種情報を入力する。 Ⅲ予防接種情報取込：予防接種の接種情報（パンチデータ）を取込みする。 Ⅳ予防接種照会事務：住民からの問い合わせなど、接種別や接種履歴を照会し，回答する。 Ⅴ転入者処理：転入者があった場合、過去の接種歴などから予防接種の予診票を印刷する。
	情報の突合 ※	・4情報を確認して，対象者を決める。【上記Ⅰ】 ・4情報を確認して，接種済み対象者の情報とシステム上のその他内部番号と突合し，予防接種の接種有無を管理する。【上記Ⅱ，Ⅲ】 ・市民からの問い合わせ時，4情報や住民票関係情報と突合し，接種別や全接種の履歴を照会し，回答する。【上記Ⅳ】 ・住民票関係情報と突合して，転入者の把握，過去の接種歴などから予防接種の予診票を印刷する。【上記Ⅴ】
	情報の統計分析 ※	特定の個人を判別するような情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		令和8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　　] <選択肢> 1）委託する　2）委託しない （　　1）件
委託事項1		健康管理システム運用管理業務
①委託内容		保健衛生システムの運用管理，バッチ処理，障害対応及び軽微な仕様変更等を行うシステム運用維持管理業
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	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
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同様
	その妥当性	システムの運用管理，およびバッチ処理を行う上で，特定個人情報ファイルを扱う必要があるため。
③委託先における取扱者数		[　　50人以上100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
④委託先への特定個人情報ファイルの提供方法		[○]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　（　　）
⑤委託先名の確認方法		下記「⑥委託先名」に記載のとおり。
⑥委託先名		株式会社両備システムズ
再委託	⑦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
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項2		
委託事項3		
委託事項4		
委託事項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 （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	特定個人番号利用事務を処理する者として主務省令で定めるもの
①法令上の根拠	1 番号法第19条第8号 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第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁，総務省令第9号） ・省令第2条の表第26項
②提供先における用途	主務省令で定める用途
③提供する情報	主務省令で定める利用特定個人情報
④提供する情報の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
⑤提供する情報の対象となる本人の範囲	2. ③対象となる本人の範囲」と同上
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	照会を受けた都度
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		
①保管場所 ※		＜本市における措置＞ 1　入退室管理装置及び監視カメラを設置し，かつ専用の室に設置した使用目的別のサーバに保管する。サーバはパスワード等により保護する。 2　予防接種関係届（申出）書等の関係帳票については，入退室管理をする執務室内において鍵付きの書庫等で管理する。 ＜中間サーバ・プラットフォームにおける措置＞ 1　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。 2　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。 ＜ガバメントクラウドにおける措置＞ ①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。 ・ISO/IEC27017，ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②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。
②保管期間	期間	［　　5年　　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	予防接種法施行規則第3条に，予防接種に関する記録は少なくとも5年間保存しなければならないと規定されており，妥当である。
③消去方法		＜システムにおける措置＞ ・ワクチンにより，接種回数及び接種間隔が定まっており，かつ接種対象年齢が幅広いため，問い合わせに対応する必要があることから，接種歴は消去しないが，連携する住民記録台帳システムの情報が消去された場合には，提供できなくなる。 ＜紙媒体における措置＞ ・保管期限を過ぎた紙媒体（予防接種予診票等）は，庁内の機密文書の一斉廃棄により溶解処理をしている。 ＜ガバメントクラウドにおける措置＞ ①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。 ②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。 ③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。
7. 備考		

（別添2）特定個人情報ファイル記録項目

＜予防接種＞
・氏名
・生年月日
・性別
・住所
・年齢
・連絡先（電話番号）
・住民日
・宛名番号
・世帯番号
・団体内統合宛名番号
・接種名称
・期，回数
・接種日

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	
予防接種の実施及び履歴管理ファイル	
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	・情報の入手にあたっては，定型の様式を用いるため，個人番号を含め必要な情報以外を入手することはない。 ・他団体からの情報入手の際は，基本4情報をもとに柏市の対象者と合致するか確認している。
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	届出・申請用紙等について，定められた様式で提出されることから，必要以外の情報が記載できない書式となっている。
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
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	情報の入手にあたっては，定型の様式を用いるため，個人番号を含め必要な情報以外を入手することはない。
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	情報の入手にあたっては，定型の様式を用いるため，個人番号を含め必要な情報以外を入手することはない。
個人番号の真正性確認の措置の内容	・転入時等に，個人番号カード等の提示を受け，本人確認及び個人番号の確認を行う。 ・住民登録外者の場合は，住民基本台帳ネットワークを通して住民登録地である自治体へ個人番号を照会し，本人確認情報との対応付けを行う。
特定個人情報の正確性確保の措置の内容	・窓口での聴聞や添付書類との整合性から正確性を担保する。 ・情報の入力・削除・訂正を行う場合には処理者と点検者を分け，二重チェックを行うことにより正確性を担保する。 ・正確性に疑義が生じた場合は，予防接種法及び同法施行令等に基づき，適宜調査を行い，必要に応じてデータを修正することにより正確性を担保する。 ・入手した特定個人情報について，保持している特定個人情報と突合を行うことにより正確性を担保する。
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
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	・端末には，外部媒体へのデータ出力を制御するためのソフトウェアを導入し，データの外部媒体出力は，予め管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。データ持ち出し時に使用する電子媒体（USBメモリ等）は，施錠管理する保管場所に保管し，持出管理を行い，記録データについては，処理後直ちに消去し，消去したことを複数名で確認する。 ・システム起動に必要なソフトウェアは，端末を限定し，操作に必要なID，パスワード管理することにより，操作権限のない者による不正な操作を防止している。
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	

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		
宛名システム等における措置の内容	その他の事務に用いるファイルにはアクセスできないよう,アクセス制御を行っている。 宛名システムにおいては，個別業務において管理する特定個人情報を保持しない。	
事務で使用するその他のシステムにおける措置の内容	―	
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
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	1）アクセス権限の発効・失効の管理 ①発効管理 正規職員及び非正規職員のユーザIDについては，情報システム担当者が発効し，アクセス権限についても，発効されたユーザIDに基づき，情報システム担当者が一元管理をしている。 ②失効管理 失効管理についても上記と同様であるが，非正規職員のユーザIDについては，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。 2）アクセス権限の管理 ・共有IDは発効せずに個人に対して発行している。 ・アクセス権限を失効した場合は，速やかに情報システム担当者がアクセス権限を削除する。 ・パスワード期限の設定をしており，定期的に新たなパスワードを設定する必要がある。 3）特定個人情報の使用の記録 ・システムへのログイン記録を作成し，必要な場合には，当該ログを確認できる仕組みとしている。また閲覧は，情報システム管理者のみ閲覧できるものとする。 ・当該データにかかる文書保存期間中はアクセスログを保管する。 4）従事者が事務外で使用するリスク ・担当課においては，外部媒体へのデータのコピーは制御されており，伝票起票用のデータ（CSVファイル）を財務会計システムへ移行させる際にUSBを使用する場合を除き，持ち出せないようにしている。 ・職員に対して個人情報保護に関する研修を行う。 ・非正規職員は，契約時に，業務上知り得た情報の業務外利用の禁止に関する条項を含む承諾書に署名する。 ・情報システム管理者がアクセスログ管理を行っており，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。 5）特定個人情報ファイルが不正に複製されるリスク ・バックアップファイルの取得は入退室管理をしているサーバ室での作業に限定されている。 ・特定個人情報を取り扱う端末は，外部媒体を使用させないことにより，漏えいを防止している。 ・正当な理由がなく第三者へ提供した場合の罰則を定めており，研修等により，周知・指導することでリスクを抑制している。	
アクセス権限の発効・失効の管理	[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	・アクセス権限の発行は，管理権限を付与された職員が行う。 ・人事異動等に伴い、随時失効処理を行っている。	

アクセス権限の管理	[　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	アクセス権限については，、定期的に点検を行い，修正を行っている。	
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	システムの操作ログについて，記録している。	
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
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	・職員に対し，個人情報保護の重要性を認識させ，業務外での情報収集の禁止等の指導を徹底することにより，事務外の使用を防止している。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することにより，コンプライアンスの意識を高め，事務外での使用を防止している。	
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	・端末には，大量複製につながるUSBメモリ等の使用について，外部媒体へのデータ出力を制御するためのソフトウェアを導入し，データの外部媒体出力は，管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。 ・データ持ち出し時に使用する電子媒体（USBメモリ）は，施錠管理する保管場所に保管し，持出管理を行う。	
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		

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	委託契約書に「個人情報の保護」について遵守することを記載しており，その実施状況を検査し報告することを受託者に課している。	
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	ユーザーID，パスワード，磁気・ICカード等で正当なアクセス権を有する者であると識別する。	
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	特定個人情報ファイルの利用・出力状況の記録	
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	・再委託の契約の内容を書面により提出させ，当該再委託の契約の内容が，委託契約により委託先に課された全ての義務を再委託先に課すものである場合に限り，再委託の許諾を行う。また，個人情報保護に係る誓約書を提出するように求める。 ・委託契約の報告条項に基づき，必要があれば柏市職員が現地調査を行う。	
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	・委託先に対して，以下の事項を義務付ける「個人情報保護に関する特記仕様書」を提示する。①番号法等の関係法令の遵守②秘密の保持・取扱区域外への情報持ち出しの禁止③目的外利用の禁止・複製の禁止④情報の返却，消去，廃棄・従業員の特定⑤従業員への監督及び教育⑥市の検査，報告の求めへの応諾⑦漏えい等事案に係る損害の賠償⑧再委託の条件，再委託先に対する監督とその履行状況の報告⑨その他柏市個人情報保護条例等に基づき職員が実施する措置に準じた措置の実施⑩特記仕様書に違反する行為の契約解除事由への該当日常運用において，ルールが遵守されていることを定期的にチェックする。	
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
ルールの内容及びルール遵守の確認方法	・ 特定個人情報が記載された書類等を廃棄する場合，焼却又は溶解等の復元不可能な手段を採用する。 ・ 特定個人情報が記録された機器及び電子媒体等を廃棄する場合，物理的な破壊等により，復元不可能な手段を採用する。 ・ 特定個人情報ファイル中の個人番号又は一部の特定個人情報を削除する場合，容易に復元できない手段を採用する。 ・個人情報保護に関する特記仕様書の，提供資料の返還又は廃棄の項において，廃棄方法や，事前に書面で承認を得ること，廃棄完了後の報告，柏市の立会いに応じることを定めている。 ・委託契約の報告条項に基づき，定期的に特定個人情報の取扱いについて書面で，破棄，消去の方法，完了日等報告させ，必要があれば柏市職員が現地調査することも可能とする。	
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	特定個人情報等に係る安全管理措置のとおり	
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	[　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　4）再委託していない
具体的な方法	業務の全部又は主要部分を第三者に委託できないよう制限をかけている。	
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		
―		

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	[ ]	＜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		

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	【中間サーバー・ソフトウェアにおける措置】 ①情報照会機能により，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用照合リスト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。 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なっている。
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
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	＜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を担保する。
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	＜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を担保する。
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	＜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，特定個人情報が漏えい・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・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。
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	＜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。 ・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信し，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。 ・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。 ・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。
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	＜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（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）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，情報照会者から受信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。 ＜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。
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	＜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信した上で，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。
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	
<中間サーバー・ソフトウェアにおける措置> 1)安全が保たれない方法によって入手が行われるリスク ①中間サーバーは，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に設計されるため，安全性が担保されている。 2)入手した特定個人情報が不正確であるリスク ①中間サーバーは，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。 3）入手の際に特定個人情報が漏えい・紛失するリスク 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・紛失のリスクに対応している。 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，不適切な接続端末操作や，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。 4)その他のリスク ①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。 ②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。	

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	[十分に整備している]	<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	[十分に整備している]	<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	[十分に周知している]	<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	[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
具体的な対策の内容	・特定個人情報を記録するサーバは，入退室管理装置及び監視カメラを設置し，使用目的別に物理的に区画，施錠した専用の室に設置する。また，当該室内に別区画を設け，データ，プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する場所を設ける。 ・データセンターに構築し特定個人情報を記録するサーバについては，サーバ設置エリアへの入退室管理，シリンダ錠によるラック施錠，人感センサ付監視カメラによる監視を行う。データセンターは，カメラ監視及び有人監視を常時実施し，事前申請による入館管理を行う。入退館時は，ICカード認証，顔認証及びログ管理を行う。 ・機器更新，交換等に伴い旧機器に保持されているデータを消去する場合は，情報を消去し，その記録をデータ消去証明として残す。 ・予防接種ファイルに関係する帳票のうち，保管する必要がある帳票類は，鍵付きの書庫等で保管する。保管する必要のない帳票類は定期的に裁断処理し，記録に残す。 ・デスクトップ型端末はセキュリティワイヤによる盗難防止を行い，ノート型端末はキャビネットに施錠保管している。 ・システムを利用する者が離席する際には時間経過によるロックが作動する。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・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軽減する。 ＜ガバメントクラウドにおける措置＞ ①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，システムのサーバー等は，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。 ②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。	
⑥技術的対策	[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
具体的な対策の内容	＜不正プログラム対策＞ 端末にウイルス対策ソフトを採用し，ウイルスパターンファイルは最新のものを適用している。 ＜不正アクセス対策＞ LAN及びWAN（インターネット網）からの通信はファイアウォールにより遮断している。 ＜ガバメントクラウドにおける措置＞ ①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。 ②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。 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及びミドルウエアについて，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。	

⑦バックアップ	[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
⑧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
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	生存者の個人番号と死者の個人番号を区別しないため，生存者の個人番号と同様の管理を行う。	
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
リスク2： 特定個人情報が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	本特定個人情報ファイルの個人情報は，住基及び住民登録外者の異動情報を取得し，内部番号を基に最新の情報に反映されるため，古い情報のまま保管され続けるリスクは存在しない。	
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	・保管年限を経過した文書は廃棄を行う。文書として管理しない特定個人情報が記録される作業用の帳票等の書類については，復元が行えないよう裁断の上，廃棄する。 <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。	
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		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	[　　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
具体的なチェック方法	・評価書の記載内容どおりの運用がなされているか，年に1回以上部署内にてチェックする。チェックの結果，不備が生じていることが明らかになった際は，速やかに問題究明にあたり，是正する。	
②監査	[　　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
具体的な内容	定期的に監査を行い，監査結果を踏まえて安全管理体制等を改善する。 ＜ガバメントクラウドにおける措置＞ 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。	
2. 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	・個人情報保護に関する研修会への参加を行っている。 ・eラーニングによる情報セキュリティ研修を受講している。 ・職員に対しては、課内に情報管理者を指名し，随時指導・啓発を行っている。 ・全庁的な個人情報保護に関する研修の受講を積極的に受講している。 ・全庁的な研修として，情報セキュリティを担当する職員については，年に1回以上庁内の集合研修を受講している。 ・正当な理由が無く第三者へ提供した場合の罰則（懲役や罰金など）について，研修等により周知・指導することでリスクを抑制している。 ＜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，セキュリティ研修等を実施することとしている。 ②中間サーバー・プラットフォームの業務に就く場合は，運用規則等について研修を実施することとしている。	
3. その他のリスク対策		
＜ガバメントクラウドにおける措置＞ 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。 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。 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。		

Ⅴ　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277-8505 千葉県柏市柏五丁目10番1号 柏市総務部行政課
②請求方法	指定様式を定め書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	任意の書式においても記載事項を網羅していれば，開示・訂正・利用停止請求を受け付ける。
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　行っていない　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	
公表場所	
⑤法令による特別の手続	
⑥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	「1. ①請求先」と同じ
②対応方法	・問い合わせの受付時に受付票を起票し，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。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	郵便，ファクシミリ，柏市ホームページ（電子申請システム），直接持参による提出
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）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