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
1	住民基本台帳に関する事務　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，住民基本台帳に関する業務における特定個人情報ファイルの取扱いにあたり，特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し，特定個人情報の漏えいその他の事態を発生させるリスクを低減させるために十分な措置を行い，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］

「住民基本台帳に関する事務　全項目評価」を例とする，具体的な「重要な変更」の内容

資料1ページ

Ⅱ 特定個人情報ファイルの概要

6. 特定個人情報の保管・消去

		・申請書・帳票等紙媒体は鍵のかかる書庫，倉庫に保管している。 ・入退館管理やコンピュータ室への入退室に対する厳重なセキュリティ，システムやファイルに対する厳しいアクセス権限を設定した運用が徹底されている。 ＜中間サーバー・プラットフォームにおける措置＞ ①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。 ②特定個人情報は，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。
①保管場所 ※		＜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	［　定められていない　］ ＜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	・住民票の記載の修正前の本人確認情報（履歴情報）及び削除者の本人確認情報は，住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）保管する。 ・届出書類は，柏市公文書管理規程第36条により3年保存としている。
③消去方法		・保存期間を過ぎた申請書・帳票等紙媒体の特定個人情報については，外部業者による溶解処理を行い廃棄する。 ・特定個人情報等の重要な情報資産については，物理的破壊またはデータ消去ソフトの使用により，情報資産を復元できないように消去を行うことをルール化している。 ＜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ため，通常，中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は，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，保存された情報が読み出しできないよう，物理的破壊又は専用ソフト等を利用して完全に消去する。 ＜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

Ⅲ 特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 ※

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	・IDカード及び生体認証によりコンピュータ室への入室を許可している。 ・建物の各所に監視カメラを設置している。 ・自家発電装置を設置している。 ・バックアップ媒体は，施錠管理されている場所で保管している。 ・システムに繋がる端末数を必要最小限とする。 ・管理権限を持つ者の端末を除き，USBの挿入口を物理的に塞いでいる。 ・LANケーブルとシステムが簡単に外れないようにカバーをかけている。 ＜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。 ＜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	・ウイルス対策ソフトについて定期的にパターン更新をしている。 ・インターネット等外部ネットワークとは完全に分離し，不正アクセス防止をしている。 ・一度に一定数以上の項目にアクセスがあった場合に，管理者端末に警告のサインが出るよう措置を講じている。 ＜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。 ＜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。）及び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	生存する個人の個人番号とともに，死亡による削除後，住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）保管する。
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

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	・評価書の記載内容通りの運用ができているか，年1回市民課内でチェックを実施 ・運用状況の変更などによる各種マニュアルの見直しを定期的に実施 ＜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，定期的に自己点検を実施することとしている。	
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	情報セキュリティ監査計画書に基づき，以下の観点で情報政策担当課による内部監査を定期的に実施し，監査結果を踏まえて体制や規定を改善する。 なお，監査は，情報セキュリティに関する研修を受けた職員が実施する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定，体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化，安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 ＜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・プラットフォームについて，定期的に監査を行うこととしている。 ＜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	・研修計画を立て，研修を実施している。 ・人事異動等により新たに配属された職員に対し，研修マニュアルにより研修を実施している。 ・研修した内容については，職員の理解度をチェックする。理解度が達していない場合には，繰り返し研修を行い，理解度を高めている。 ・研修に参加した職員とその理解度を記録している。 ・セキュリティ事故の情報を課内で共有するため，全員に回覧している。 ・情報管理者が全員に対してセキュリティチェックを行い，チェックシートにて確認している。 ・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実施している他，所属長等についても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。 ・違反行為を行った者に対しては，指導を行うほか，その行為の程度により懲戒の対象とする。 ＜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行うこととしている。	

3. 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＞
①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。

＜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及び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及び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。