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
2	個人住民税の賦課事務　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，個人住民税の賦課事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］

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	＜住民税システムにおける措置＞ ・サーバ設置箇所については、入退室管理を行っている。 ・庁内情報用端末については、特定個人情報を保管していない。 ・業務用端末は，盗難防止用ワイヤーを設置している。 ・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メモリ等の外部媒体を使用できない状態にしている。 ＜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	＜住民税システムにおける措置＞ ・住民税システムは，庁内のみの独立したネットワークにのみ搭載されており，外部接続していない。 ・eLTAXシステム等，外部接続のシステムには，ファイアウォールを設置している。 ・アクセスの監視とアクセスログの取得・点検について規定をしている。 ＜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。 ＜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及び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及び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	・データセンタ内のサーバで管理しており、生存者の個人番号と同様の方法にて安全管理措置を実施している。	
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	・住民税システムに存在する賦課情報は，各種申告情報に基づき，更新・賦課を行った上で，住民に対して税額通知を行い，住民側でも確認を行うため、古い情報のまま保管され続けることはない。	
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：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	・保存期間を過ぎたシステム上の特定個人情報については，当該事務所管部署の所属長の責任で消去を行う。また，当該消去を行った旨を文書主管課長に報告する。 ・消去の際には，規定に基づき対象のデータを特定し，消去漏れのないよう所管部署が確認をする。消去前にデータバックアップを行い，誤った消去が判明した場合は当該バックアップデータより復元する。バックアップデータは作業完了後に消去する。確認は消去完了報告書で行う。 ・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，当該事務所管部署の所属長が文書主管課長に廃棄を依頼する。文書主管課は当該文書について，外部業者による溶解処理を行い廃棄する。 <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	・評価書の記載内容通りの運用ができているかについて、国のチェックリスト等を活用し，年に1回の頻度で各業務主管課でチェックを実施する。 ＜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、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。 ・評価書の記載事項と運用形態のチェック ・個人情報保護に関する規定，体制準備 ・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	・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。 ・委託事業者に対しては、秘密保持に関する条項を含んだ契約を締結している。 ・違反行為を行った者に対しては，都度指導の上，違反行為の程度によっては懲戒の対象となりうる。 ・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。 ・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）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。 ＜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。	