

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
8	予防接種の実施, 給付の支給又は実費の徴収事務 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

本市は予防接種に関する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事を認識し、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]

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。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）は，特定個人情報の適切な取扱いに関するガイドライン，政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており，情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお，以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは，暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国，都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 ＜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	＜選択肢＞ <table border="1"> <tr> <td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr> <tr> <td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr> <tr> <td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr> <tr> <td>10) 定められていない</td><td></td><td></td></tr> </table> 期間 [5年] その妥当性 予防接種法施行令第6条の2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。	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	
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													
③消去方法		＜システムにおける措置＞ ・定期予防接種は，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ことから，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。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ・自機関の領域に保管されたデータのみ，ワクチン接種記録システム（VRS）を用いて消去することができる。 ・自機関の領域に保管されたデータは，他機関から消去できない。 ※クラウドサービスは，IaaSを利用し，クラウドサービス事業者からはデータにアクセスできないため，消去することができない。 ＜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. 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た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。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は，特定個人情報の適切な取扱いに関するガイドライン，政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており，情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため，特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理，施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 <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
<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)からの通信はファイアウォールにより遮断している。 <ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は，特定個人情報の適切な取扱いに関するガイドライン，政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており，情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため，特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された当市の領域にデータを保管する。 ・当該領域のデータは，暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国，都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため，外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより，通信内容の秘匿及び盗聴防止の対応をしている。		

具体的な対策の内容	＜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。
------------------	--

予防接種の実施，給付の支給又は実費の徴収事務 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バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
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	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
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。 <令和5年度以前に実施した新型コロナウイルス感染症予防接種に係る事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ，第9条(市区町村の責任)に則し，適切に職員等の当該システムの利用を管理し，必要な監督をする。	
②監査	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
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。 <令和5年度以前に実施した新型コロナウイルス感染症予防接種に係る事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ，第9条(市区町村の責任)に則し，適切に職員等の当該システムの利用を管理し，必要な監督をする。 <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. 従業員に対する教育・啓発		
従業員に対する教育・啓発	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な方法	・個人情報保護に関する研修会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行っている。 ・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。 ・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。 <令和5年度以前に実施した新型コロナウイルス感染症予防接種に係る事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ，第9条(市区町村の責任)に則し，適切に職員等の当該システムの利用を管理し，必要な指導をする。	
3. その他のリスク対策		
<令和5年度以前に実施した新型コロナウイルス感染症予防接種に係る事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ，第7条(情報到達の責任分界点)，第8条(通信経路の責任分界点)，第9条(市区町村の責任)に則し，適切に当該システムを利用し，万が一，障害や情報漏えいが生じた場合，適切な対応をとることができる体制を構築する。		

＜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。