

藤沢市個人情報保護制度運営審議会答申第1185号

2025年（令和7年）2月13日

藤沢市長 鈴木 恒夫 様

藤沢市個人情報保護制度
運営審議会会長 飯島 奈津子

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、特定個人情報保護評価に関する規則及び特定個人情報保護評価指針に基づく特定個人情報保護評価書（新型コロナウイルス感染症対策に係る予防接種に関する事務 全項目評価書）について（答申）

2025年（令和7年）1月24日付けで諮問（第1185号）された特定個人情報保護評価書について点検を行ったため、次のとおり答申します。

1 審議会の結論

特定個人情報保護評価書（新型コロナウイルス感染症対策に係る予防接種に関する事務 全項目評価書）については、適当であると認められる。

2 実施機関の説明要旨

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「番号利用法」という。）、特定個人情報保護評価に関する規則（以下「規則」という。）及び特定個人情報保護評価指針（以下「指針」という。）に基づく特定個人情報保護評価書（新型コロナウイルス感染症対策に係る予防接種に関する事務 全項目評価書）に係る実施機関の説明は、次のとおりである。

(1) 諮問に至る経過

2013年（平成25年）5月31日に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。）等、関連法が公布され、導入された番号制度は、社会保障制度、税制、災害対策等の分野における行政運営の効率化を図り、国民にとって利便性の高い、公平・公正な社会を実現するための社会基盤として導入されたものです。

これら関連法により国民一人一人に付番された個人番号を基に2

017年（平成29年）1月から社会保障、税及び災害対策分野における各種行政手続に際し、住民基本台帳の情報、税に関する情報及び他の給付状況等の情報連携が行政機関間において行われています。当該情報連携は地方公共団体情報システム機構が運営する情報提供ネットワークシステムを介して行われています。

番号法は、特定個人情報不正に利用された際に、個人のプライバシー等の権利利益が侵害されるおそれがあるため、その保護措置の一つとして、特定個人情報ファイルを保有しようとする者に対し、特定個人情報の漏えいやその他の事態が発生する危険性及び影響に関する評価を、当該特定個人情報ファイルを保有する前に自ら実施することを義務付けています。この評価を特定個人情報保護評価といい、特定個人情報ファイルを取り扱う事務について特定個人情報保護評価を実施するに際しては、評価対象の事務の対象人数、特定個人情報ファイルの取扱者数、過去の特定個人情報に関する重大事故発生の有無によるしきい値判断を行います。

新型コロナウイルス感染症対策に係る予防接種に関する事務のしきい値判断については、対象人数は住民登録を有する者のうち、予防接種法等関連法令に基づく対象者約44万人、特定個人情報ファイルの取扱者数は、健康づくり課健診・予防接種担当の職員約10人であり、過去に特定個人情報に関する重大事故は発生していないことから、当該事務の特定個人情報保護評価は全項目評価に該当します。

このため、番号法第27条、第28条及び「特定個人情報保護評価に関する規則」並びに「特定個人情報保護評価指針」に基づき、パブリックコメントを経て、当審議会において第三者機関による点検（諮問）をお願いし、2022年（令和4年）3月10日に答申第1126号において「適当である」との答申をいただき、内閣府個人情報保護委員会に提出しました。

本評価書につきましては、これまで、2022年（令和4年）11月10日に国が開発したワクチン接種記録システム（VRS）における接種履歴の一括照会機能の追加及び接種証明書のコンビニエンスストアでの自動交付の開始に伴う再評価（答申第1169号）を実施しています。また、2024年（令和6年）12月16日に見直しを行い、ワクチン接種記録システム（VRS）の停止および接種証明書のコンビニエンスストアでの自動交付終了に伴う変更を行いました。

新型コロナウイルス感染症対策に係る予防接種に関する事務は、地方公共団体ごとに基幹業務システムを構築・運用していますが、2021年（令和3年）9月1日施行の「地方公共団体情報システムの標準化に関する法律」において、当該システムを国の定める標準基準に適合させ、国が地方公共団体に対し提供するガバメントクラウド上に構築した標準準拠システムへ移行することが義務付けられました。

同法に基づき標準化の推進を図るための基本方針として策定された「地方公共団体情報システム標準化基本方針」では、令和7年度までに当該ガバメントクラウドの標準準拠システムへ移行するための環境整備を行うこととされております。本市の健康管理システム（保健所・保健センター業務情報システム）を標準準拠システムに移行するためには、令和7年度当初からシステム改修に着手する必要があることから、このたび新型コロナウイルス感染症対策に係る予防接種に関する事務について再評価を実施しましたので、藤沢市個人情報保護制度運営審議会に諮問するものです。

(2) 評価書の概要

ア 対象ファイルの概要

予防接種対象者台帳は、住民基本台帳に記録されている者及び転出等で削除した者についての情報を蓄積したファイルです。当該ファイルは個人番号、4情報（氏名、性別、生年月日及び住所）、その他住民票関係情報並びに健康・医療関係情報が記録されるものであり、特定個人情報ファイルとして保有するものです。

住民票関係情報は、住民記録システムから、本人確認情報に係る変更又は新規作成が発生した都度入手するものです。なお、住民票関係情報を取り扱う担当課は、市民窓口センター及び各市民センターであり、住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、当該ファイルにおいて区域内すべての住民情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新、管理及び提供するものです。

また、予防接種関係情報（予防接種実施回数、予防接種実施日等）は、住民が予防接種を受けた医療機関から提出される予防接種券・予診票情報から入手するものであり、接種実施時には本人確認が実施されています。なお、転入者等の予防接種関係情報は、同様の手順を経て情報提供ネットワークシステムを介して他自治体から入手するものです。

住民票関係情報を基に予防接種関係情報を追記した予防接種対象者台帳の取扱いについては、保健所・保健センター業務情報システムの保守業務を委託しています。なお、保健所・保健センター業務情報システムに登録された予防接種対象者台帳の情報は、他自治体に情報提供ネットワークシステムを介した提供を行う上で必要であるため、庁内連携システムを介した情報の移転が行われます。

予防接種対象者台帳の情報の保管及び消去については、予防接種法施行令第6条の2において、5年間保管すると定められていますが、接種記録確認等の事務のため20年以上の長期間保管する必要があるものです。ディスク交換やハード更改等の際は、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すことができないよう、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とともに、必要に応じて職員が当該措置の完了まで立合いを行う等、確実な履行を担保します。

ガバメントクラウド移行後においても、国及びクラウド事業者はデータにアクセスすることはできません。

イ しきい値判断の結果

(ア) 評価対象の事務の対象人数

約 44 万人（区域内の住民のうち新型コロナウイルス感染症対策に係る 予防接種対象者）

(イ) 特定個人情報ファイルの取扱者数

約 10 人（健康づくり課 健診・予防接種担当）

(ウ) 過去の特定個人情報に関する重大事故発生の有無
発生なし

ウ 評価実施機関

藤沢市長（所管部署 健康医療部健康づくり課）

エ 公表しない部分の有無

なし

オ 特定個人情報ファイルの保有時期

2021年（令和3年）5月17日から

カ リスク対策

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は、大きく分けて、特定個人情報の入手、特定個人情報の使用、特定個人情報ファイルの取扱いの委託、特定個人情報の提供・移転、情報提供ネットワークとの接続及び特定個人情報の保管・消去の6項目であり、それ以外のリスク対策については監査、従業員に対する教育・啓発及びその他の対策の3項目について明記しています。

(3) 特定個人情報保護評価書の主な変更点

ア 「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 住民基本台帳ファイル 6. 特定個人情報の保管・消去」に次の項目を追加します。

① 保管場所

<ガバメントクラウドにおける措置>

- ・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/IEC 27017、ISO/IEC 27018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。
- ・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消去方法

＜ガバメントクラウドにおける措置＞

- ・特定個人情報の消去は地方自治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。
- ・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/IEC 27001等にしながら確実にデータを消去する。
- ・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に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。

イ 「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 1. 特定個人情報ファイル名 住民基本情報ファイル 7. 特定個人情報の保管・消去」に次の項目を追加します。

リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤ 物理的対策

＜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。
- ・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。

リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥ 技術的対策

＜ガバメントクラウドにおける措置＞

- ・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。

- ・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15「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営管理補助者（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。
- ・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。
- ・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。
- ・地方公共団体が委託したASP又はガバメント運用管理補助者は、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。
- ・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。
- ・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。
- ・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。

リスク3：特定個人情報が消去されずにいつまでも存在するリスク
消去手順 手順の内容

＜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。

ウ 「IVその他のリスク対策1. 監査②監査」に次の項目を追加します。

＜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

エ 「Ⅳその他のリスク対策3. その他のリスク対策」に次の項目を追加します。

＜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なる。具体的な取扱いについて、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。

(4) 住民に対する意見聴取の内容

ア 意見聴取期間

2024年（令和6年）12月25日から2025年（令和7年）1月23日まで

イ 意見聴取の結果

意見あり（1件）

ウ 意見の内容

ワクチン接種事業に対する反対意見

エ 評価書への反映

なし

(5) 提出書類

ア 特定個人情報保護評価書（案）

イ 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（抜粋）

ウ 特定個人情報保護評価に関する規則

エ 特定個人情報保護評価指針

オ 地方公共団体情報システムの標準化に関する法律（抜粋）

3 審議会の判断理由

当審議会は、次に述べる理由により、「1 審議会の結論」のとおり判断をするものである。

(1) 適合性について

実施機関では、本評価の実施手続等について、次のように述べて

いる。

ア 令和4年に藤沢市個人情報保護制度運営審議会に諮問し（答申第1169号）、再評価を実施した。

イ 指針第6の2（2）に、保有する特定個人情報ファイルに重要な変更を加えようとするときは、当該変更を加える前に、特定個人情報保護評価を再実施するものとする、と規定されていることから、全項目評価を再実施するため、本評価書を作成した。

（ア）本評価の対象となる事務の実態に基づき、特定個人情報保護評価書様式で求められるすべての項目について検討し、記載した。

（イ）しきい値判断については、特定個人情報の保有数は住民登録を有する者の約44万人分であるため、当該事務の特定個人情報保護評価は全項目評価に該当する。なお、特定個人情報ファイルの取扱者数は、健康づくり課健診・予防接種担当の職員約10人である。

（ウ）過去に特定個人情報に関する重大事故の発生は起きていない。

ウ 指針第5の3（3）イに、全項目評価書を作成した後、規則第7条第1項の規定に基づき、全項目評価書を公示して広く住民等の意見を求め、これにより得られた意見を十分考慮した上で全項目評価書に必要な見直しを行うものとする、と規定されていることから、2024年（令和6年）12月25日から2025年1月23日までの間に住民に対する意見聴取を実施した。意見は1件あったが、ワクチン接種事業自体に対する反対意見であり、評価書への反映はしていない。

エ 指針第5の3（3）イに、公示し住民等の意見を求め、必要な見直しを行った全項目評価書について、規則第7条第4項の規定に基づき、第三者点検を受けるものとする、と規定されていることから、今回、藤沢市個人情報保護制度運営審議会に諮問し、第三者点検を受けるものである。

以上のことから判断すると、本評価の実実施手続等は、指針に定める実施手続等に適合していると認められる。

(2) 妥当性について

実施機関では、本評価の変更点について、次のように述べている。

ア 「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
住民基本台帳ファイル6.特定個人情報の保管・消去」に次の項目を追加します。

①保管場所

<ガバメントクラウドにおける措置>

・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/IEC 27017、ISO/IEC 27018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。
- ・特定個人情報、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 消去方法

＜ガバメントクラウドにおける措置＞

- ・特定個人情報の消去は地方自治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。
- ・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/IEC 27001等にしながら確実にデータを消去する。
- ・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に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。

イ 「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 1. 特定個人情報ファイル名 住民基本情報ファイル 7. 特定個人情報の保管・消去」に次の項目を追加します。

リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策

＜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。
- ・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。

リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥ 技術的対策

＜ガバメントクラウドにおける措置＞

- ・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。
- ・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15「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営管理補助者（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。
- ・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。
- ・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。
- ・地方公共団体が委託したASP又はガバメント運用管理補助者は、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。
- ・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。
- ・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。
- ・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。

リスク3：特定個人情報が消去されずにいつまでも存在するリスク 消去手順 手順の内容

＜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。

ウ 「IVその他のリスク対策1. 監査②監査」に次の項目を追加します。

<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

エ 「IVその他のリスク対策3. その他のリスク対策」に次の項目を追加します。

<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なる。具体的な取扱いについて、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。

以上のことから判断すると、本評価の内容は、指針に定める特定個人情報保護評価の目的等に照らし妥当であると認められる。

以上に述べたところにより、特定個人情報保護評価書（新型コロナウイルス感染症対策に係る予防接種に関する事務）については、適当であると認められる。

以 上