

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
11	予防接種に関する事務 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

目黒区は、予防接種に関する事務において、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

目黒区長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和7年3月19日

[令和6年10月 様式4]

項目一覧

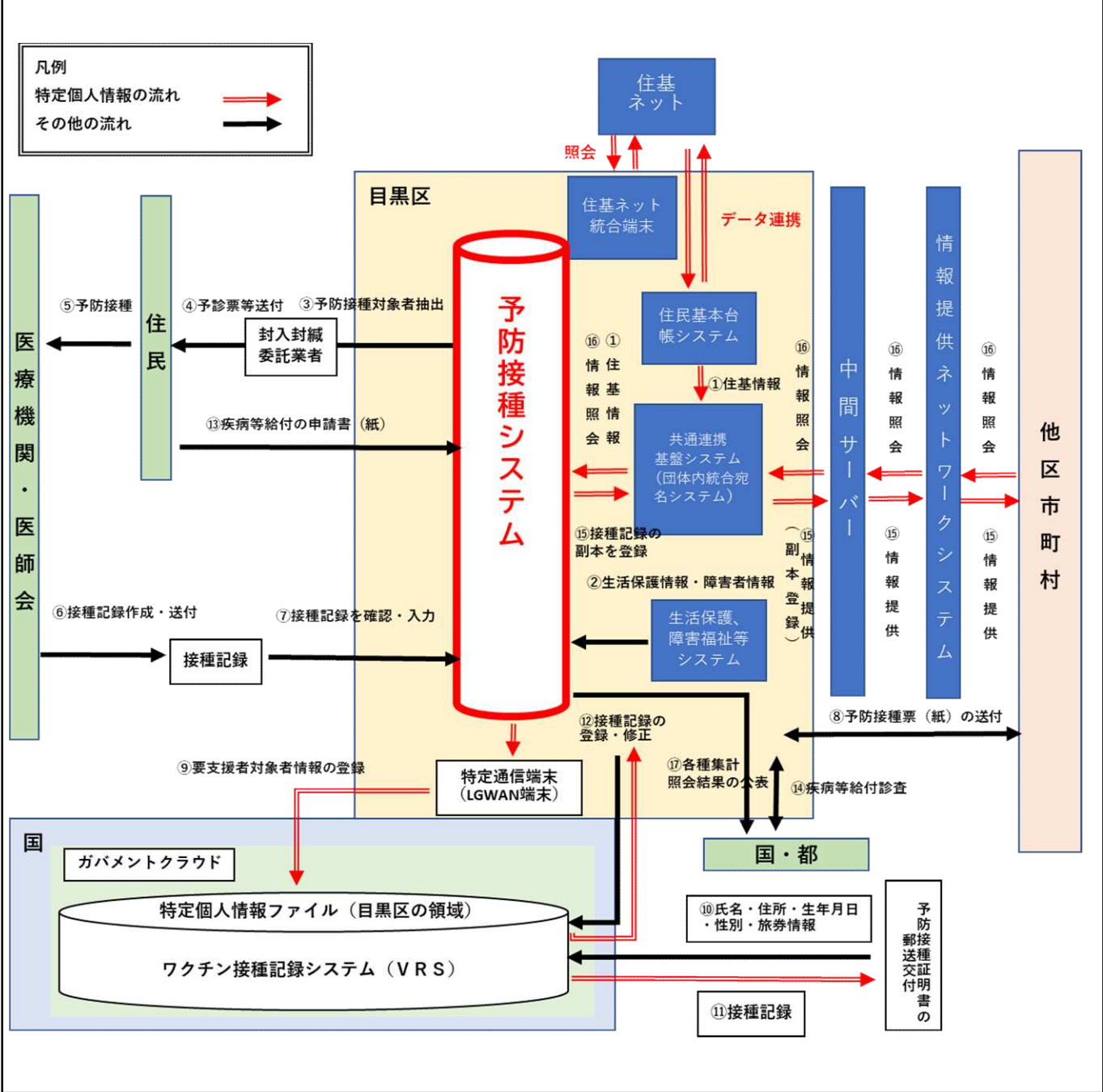
I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

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	予防接種に関する事務
②事務の内容 ※	予防接種に関する事務は、予防接種法(昭和23年法律第68号)及び新型インフルエンザ等対策特別措置法(平成24年法律第31号)に基づく予防接種の実施、接種記録の管理・保管に関するものであり、対象者への接種勧奨、予防接種の実費徴収、医療機関での予防接種の実施、医療機関への接種委託料の支払い、接種記録の管理・保管を行う。 これらの業務を行うに当たり、次の事務において特定個人情報を取り扱う。 1 各種予防接種の案内 2 予防接種履歴の管理・接種証明書の交付 3 予防接種による健康被害救済給付
③対象人数	[30万人以上] <選択肢> 1) 1,000人未満 3) 1万人以上10万人未満 5) 30万人以上 2) 1,000人以上1万人未満 4) 10万人以上30万人未満
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	予防接種システム
②システムの機能	1 対象者管理機能 業務固有番号を含む、住所、氏名等の情報を管理する機能。接種勧奨を行うための対象者を抽出する。 2 接種履歴管理機能 対象者の接種した予防接種情報を管理・保管する。 3 接種歴照会機能 過去の接種歴照会や、予診票の再発行を行う。 4 集計・統計機能 予防接種情報を集計し、国や県への事業報告書を作成する。 5 副本作成機能 中間サーバーに登録する副本を作成する。
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 [] 住民基本台帳ネットワークシステム [○] 宛名システム等 [○] その他 (生活保護等の他の業務システム) [○] 庁内連携システム [○] 既存住民基本台帳システム [○] 税務システム
システム2～5	
システム2	
①システムの名称	共通連携基盤システム
②システムの機能	1 申請管理機能 申請者が地方公共団体に対し申請手続等を行うマイナポータルと標準準拠システムの間を連携する機能 2 庁内データ連携機能 標準準拠システムが、他の標準準拠システムにデータを送信又は他の標準準拠システムからデータを受信することを効率的かつ円滑に行う機能 3 住登外者宛名番号管理機能 庁内で管理する住登外者(既存住民基本台帳システム以外の標準準拠システムにおいて住民とは別に管理しておく必要がある者をいう。)を一意に特定するための住登外者宛名番号を付番・管理する機能 4 団体内統合宛名機能 団体内統合宛名番号を付番し、中間サーバーと連携する機能 5 EUC機能 職員自身が表計算ソフト等を用いて情報を活用するために基幹業務システムのデータを抽出、分析、加工、出力する機能

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 （ 予防接種システム、他の業務システム、中間サーバー ）
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 情報の照会及び提供に用いる個人の識別子である「符号」と統一識別番号とを紐付け、その情報を保管・管理する。 2 情報照会 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)の照会をするとともに、照会した情報の受領を行う。 3 情報提供 情報提供ネットワークシステムを介して、特定個人情報の照会があった旨を受領するとともに、当該特定個人情報(連携対象)の提供を行う。 4 団体内統合宛名システム接続 中間サーバーと団体内統合宛名システムとの間で照会内容、提供内容、特定個人情報(連携対象)等について連携する。 5 情報提供等記録管理 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 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 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、照会、提供情報等について連携する。 8 セキュリティ管理 暗号化／復号機能と、鍵情報及び照会許可照会リスト情報を管理する。 9 職員認証・権限管理 中間サーバーを利用する職員の認証を行うとともに、当該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 バッチの状況管理、業務統計情報の集計、稼動状態の通知及び保管期限切れ情報の削除を行う。 11 自己情報提供 情報提供ネットワークシステムを介して自己情報に対する提供の求めを受領し、当該の特定個人情報(連携情報)及び自己情報提供用添付ファイルの提供を行う。 12 お知らせ お知らせ情報提供対象者へのお知らせ情報の送信依頼に対し、情報提供ネットワークシステムを介して、お知らせ情報の提供と、その状況確認依頼に対し回答結果の受領を行う。
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	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	1 本人確認情報検索 統合端末により、4情報(氏名・住所・性別・生年月日)の組み合わせをもとに本人確認情報の検索を行い、一覧を画面上に表示する。 2 地方公共団体情報システム機構への情報照会 全国サーバーに対して、個人番号又は4情報の組み合わせによる本人確認情報の照会要求を行い、該当する個人の本人確認情報を受領する。

(別添1) 事務の内容



(備考)

(1)住民情報の登録

- ①住民情報を住民基本台帳システムから取得
- ②予防接種対象に関する生活保護、障害者福祉等に関する住民情報を紙媒体による取得

(2)予防接種の実施

- ③予防接種情報を予防接種システムより抽出
- ④区民等に勧奨通知等および予防接種票を送付
- ⑤接種対象者が予防接種協力医療機関へ受診
- ⑥医療機関等において接種記録を予診票に記載し、区へ送付
- ⑦予診票に記載されている接種記録を医療機関等から取得し、接種歴を予防接種システムに入力
- ⑧他区市町村で予防接種をする場合は、区市町村相互間で依頼書、報告書および予防接種票を相互に送付

(3)新型コロナワクチンの予防接種事務

- ⑨住民基本台帳システムの情報のうち要支援対象者の宛名番号および要支援対象者フラグを特定通信端末(LGWAN端末)にダウンロードしたうえで、同端末からワクチン接種記録システム(VRS)に接続し、アップロード
 - ⑩窓口または郵送により予防接種証明書(紙)の交付申請があった場合、ワクチン接種記録システム(VRS)で接種記録を照会する。
 - ⑪接種記録の情報を、個人番号・氏名・住所・生年月日・性別・旅券情報(ローマ字氏名・国籍と地域・旅券番号)の情報と照合して本人を特定し、接種証明書として出力し郵送する。
 - ⑫個別接種記録のワクチン接種記録管理システム(VRS)への登録・修正・照会
- ※令和6年3月31日までは、特定通信端末から特定個人情報ファイル(CSVファイル)の登録を行っていた
登録済みの情報はVRS上に保存されており、個人の接種記録の登録・修正・照会・予防接種証明書発送時に画面表示される。
令和6年10月1日以降、VRSにアクセス不可

(4)健康被害救済の給付

- ⑬区民等からの予防接種による疾病等給付の申請の受付
- ⑭疾病等給付の審査結果を国に報告、国から給付の審査結果の確認

(5)予防接種記録情報の提供および取得

- ⑮予防接種歴を中間サーバーへ副本登録・情報提供
- ⑯他市町村が保有する予防接種歴情報を中間サーバーへ照会

(6)集計情報の報告

- ⑰各種集計情報を国または東京都へ報告

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	
予防接種台帳記録ファイル	
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 ※	予防接種法等関連法令に定められる予防接種の対象者
その必要性	区で実施する予防接種に関する情報を適正に管理する必要がある。
④記録される項目	[100項目以上] <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	1 識別情報 ・対象者を正確に特定するため 2 連絡先等情報 ・接種券を発送する際、正確な住所・連絡先を把握するため ・年齢や性別により、対象者・接種時期等を判断するため 3 業務関係情報 ・接種情報管理及び接種要件・自己負担免除要件確認のため
全ての記録項目	別添2を参照。
⑤保有開始日	2016/01/01
⑥事務担当部署	健康推進部 感染症対策課
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 (戸籍住民課 税務課 国保年金課 障害者支援課 生活福祉課) [☐] 行政機関・独立行政法人等 (地方公共団体情報システム機構) [☐] 地方公共団体・地方独立行政法人 (他地方公共団体) [☐] 民間事業者 () [☐] その他 (目黒区医師会 実施医療機関)

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 (住民基本台帳ネットワークシステム、ワクチン接種記録システム(VRS))
③入手の時期・頻度	【識別情報及び連絡先情報等】 ・住民記録システムからの連携により自動的に入手する。 【業務関係情報】 ☒ 予防接種情報 ・接種を行った医療機関から月次単位で予診票を受領し入手する。 ・転入時に転出元市区町村への接種記録の照会が必要になる都度入手する。 ・転出先市区町村から接種記録の照会を受ける都度入手する。 ☒ 生活保護情報・障害者情報 ・必要に応じて関係所管から入手する。 ☒ 予防接種による健康被害救済制度に係る情報 ・随時
④入手に係る妥当性	・識別情報については、番号法第14条において個人番号利用事務実施者は他の個人番号利用事務等実施者に対して個人番号の提供を求めることができるとされているため、予防接種事業に係る事務において必要な時期に情報を入手する必要がある。 ・連絡先等情報については、正確な本人特定のため、予診票に記載された情報と突合するため、また、接種勧奨に使用するために取得する必要がある。 ・業務関係情報である医療機関や本人等から入手する接種記録については、予防接種法施行令第6条の2及び予防接種法施行規則第2条の7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。生活保護情報・障害者情報は、B類疾病における自己負担の免除等を行うために入手する必要がある。 ・予防接種による健康被害救済制度に係る情報については、予防接種法施行規則(昭和23年厚生省令第36号)第10条及び同第11条に基づいて入手している。
⑤本人への明示	・識別情報については、番号法第14条において本人又は他の個人番号利用事務実施者に対し個人番号の提供を求めることができるとされている。 ・連絡先等情報については、医療機関で接種を受ける前に、住民票住所の印字がある本人確認証を提示、またその住所を予診票に記載するよう、お知らせ等に示している。 ・予防接種情報については、予診票に、同票の提出の本人又は保護者による同意欄を設けている。 ・健康被害救済制度に係る情報については、予防接種法施行規則第10条及び同第11条に明記している。また、請求書に同意欄を設けている。
⑥使用目的 ※	予防接種事務に関する対象者の特定及び予防接種履歴の管理、勧奨、または健康被害者に対する給付金支給
変更の妥当性	—
⑦使用の主体	使用部署 ※ 健康推進課感染症対策課、保健予防課、碑文谷保健センター、健康推進課(※) ※健康推進課はシステムの運用管理部署
	使用者数 [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

委託事項2～5		
委託事項2		共通連携基盤システム運用・保守業務
①委託内容		カハメントクラウドでの申請管理機能・団体内統合宛名機能を含む予防接種システム等の事務処理システムの基盤環境の構築、運用、システム移行業務、システムデータの滅失に備えたバックアップデータの保管等
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 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	
③委託先における取扱者数		[10人以上50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		問い合わせがあった場合は随時回答する。
⑥委託先名		株式会社日立システムズ
再委託	⑦再委託の有無 ※	[再委託する] <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	事前に書面による申請を受け、再委託内容・再委託先・理由等により、許諾を判断する。許諾する場合には、再委託先事業者は、委託業者が果たすべき安全管理措置と同等の措置を講ずる能力のあることが確認された事業者に限定することとし、委託業者は再委託先と締結する再委託契約において、委託業者と同等の安全管理義務を課すものとする。
	⑨再委託事項	上記①の委託内容のうち、必要最小限の範囲内で区が認める事項
委託事項3		磁気媒体等外部保管
①委託内容		システムのデータの滅失等に備えたバックアップデータの遠隔地保管及び集配
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 ※	予防接種法等関連法令に定められる予防接種の対象者
	その妥当性	全ての接種対象者の情報を管理しているため、上記の範囲を取り扱う必要がある。
③委託先における取扱者数		[10人以上50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

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 (2) 件 [] 移転を行っている () 件 [] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	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第2条の表25の項、26の項、27の項、28の項、29の項
②提供先における用途	予防接種法による予防接種の実施及び給付の支給等に関する事務であって上記主務省令で定めるもの
③提供する情報	予防接種に関する記録及び給付の支給に関する情報
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	予防接種法等関連法令に定められる予防接種の対象者
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	情報提供ネットワークシステムを通じて依頼のあった都度
提供先2～5	
提供先2	厚生労働大臣、都道府県知事又は市町村長
①法令上の根拠	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第2条の25の項、26の項、153の項、154の項
②提供先における用途	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であって上記主務省令で定めるもの
③提供する情報	予防接種に関する記録
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	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対象者
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	情報提供ネットワークシステムを通じて依頼のあった都度
提供先6～10	
提供先11～15	
提供先16～20	

②保管期間	期間	＜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 [20年以上]
	その妥当性	予防接種法施行規則第3条及び厚生労働省通知「予防接種法第5条第1項の規定による予防接種の実施について」の別添「定期予防接種実施要領」の1において、少なくとも5年管理・保管すると定められており、接種記録の確認や証明書の発行事務において長期保管する必要がある。
③消去方法		＜目黒区における特定個人情報の消去＞ 保管期間が経過したデータは、システムにてデータベースから削除する。 ＜中間サーバー・プラットフォームにおける特定個人情報の消去＞ 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。 ＜ワクチン接種記録システム（VRS）における特定個人情報の消去＞ 1 システム利用市区町村は、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を用いて消去することができる。 2 ワクチン接種記録システム上の各市区町村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ため、消去することができない。
7. 備考		
—		

(別添2) 特定個人情報ファイル記録項目

<予防接種台帳記録ファイル>

1 識別情報

個人番号、情報提供用個人識別符号、整理番号(宛名番号)

2 連絡先等情報

氏名(漢字)、カナ氏名、性別、生年月日、年齢、月齢、住所、方書、送付用方書、町丁目コード、町丁目、番地、枝番、小枝番、郵便番号、行政区番号、行政区名称、地区番号、地区名称、規制区分、住民区分、住登外区分、続柄、世帯番号、世帯主漢字氏名、世帯主カナ氏名、住民となった日、住民でなくなった日、異動区分、異動年月日、住民異動区分、住民異動年月日、転入前住所、転入前方書、転出後住所、転出後方書、宛名種別、外国人、外国人本名カナ、外国人本名漢字、外国人本名使用フラグ、生保区分、後期高齢区分、送付用郵便番号、送付用住所、送付用方書、送付先集配局、送付先使用、集配局、補記区分、連携番号、事業予定連番、送付先除外区分、取消コード、他区名その他、区外者カナ氏名、連絡先

3 業務関係情報

接種番号、接種名称、期・回数区分、接種種別、予防枝番、年度、接種日(各予防接種)、接種日年齢(各予防接種)、接種区分(各予防接種)、接種量(各予防接種)、Lot番号(各予防接種)、ワクチンメーカー(各予防接種)、ワクチン区分(各予防接種)、簿冊番号(各予防接種)、シーケンシャル番号(各予防接種)、登録日(各予防接種)、登録区(各予防接種)、登録区分(各予防接種)、印刷日(各予防接種)、印刷区分(各予防接種)、予診票送付区分(各予防接種)、再交付日(各予防接種)、再発行窓口(各予防接種)、郵送戻り、郵送戻り日、担当者、予診票年度、予診理由、予診番号、接種医療機関(その他)、会場コード、会場(医療機関)、医療機関コード、小学校区分、中学校区分、依頼書の有無、対象年月日、受付方法、受付年月日、保護者氏名、申請者電話番号、申請理由、申請理由その他、発行月日、発行方法、滞在先住所、滞在先電話番号、依頼書送付先、依頼書送付先電話番号、依頼書宛名、依頼書備考、証明書印刷日、文書年度、文書決裁番号、文書番号、区外者フラグ、受付連番、抽出キー、抽出時集配局、抽出時地区、登録者、登録者ID、負担金区分、任意負担区分、免除区分、支払対象外、母子手帳を元に修正、予備コード、申請年月日、申請種別/申請理由、手帳番号、総合等級、種別、交付年月日、再交付年月日、返還年月日、障害認定日、障害部位、等級、障害名、個人課税区分、世帯課税区分、被災者区分、障害手帳区分

4 団体内統合宛名システム記録項目(※1)

宛名番号、個人番号、団体内統合宛名番号、符号取得状況、不開示・自動応答不可フラグ設定情報

5 中間サーバー記録項目(※2)

団体内統合宛名番号、情報提供用個人識別符号、副本情報、情報提供等の記録等、不開示・自動応答不可フラグ

6 ワクチン接種記録システム(VRS)記録項目

個人番号、宛名番号、自治体コード、接種券番号、属性情報(氏名、生年月日、性別)、接種状況(実施/未実施)、接種回、接種日、接種会場、接種医師名、ワクチンメーカー、ロット番号、要支援対象者フラグ、ワクチン種類(※3)、製品名(※3)、旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※3)、証明書ID(※3)、証明書発行年月日(※3)

(※1) 情報提供ネットワークシステムを通じた情報提供を行うため、団体内統合宛名システムにおいて別途保有される情報

(※2) 情報提供ネットワークシステムを通じた情報提供を行うため、中間サーバーにおいて別途保有される情報

(※3) 新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ

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		
予防接種台帳記録ファイル		
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	1 既に予防接種システムに登録のある対象者について、新たな情報の入手につき、記録の修正等を行うときは、対象を取り違えないよう、システムで検索を行い、対象者を特定する。 2 届出・申請等の手続で情報を入手するときは、届出者・申請者等の確認を行うとともに、記入方法を窓口で説明する等、案内を充実させることにより、対象者のみの情報の記入となるようにする。 3 住民情報については、登録の際に厳重な本人確認を行っている住民基本台帳を管理する住民記録システムから入手する。 4 他の業務システムから情報を入手するときは、宛名番号により、正確に対象者本人とひも付く情報のみを連携するようにする。 5 住民基本台帳ネットワークシステムから目黒区の住民基本台帳に登録のない対象者情報を入手する際は、4情報（氏名・住所・性別・生年月日）の組み合わせによる照会を対象者を特定する。	
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	1 住民記録システムから入手する情報は、あらかじめ設定した項目のみとする。 2 健康被害救済給付認定申請手続においては、所定の様式を使用し、必要のない情報の入手の防止する。 3 他の業務システムから入手する情報は、あらかじめ設定した項目のみとする。 4 住民基本台帳ネットワークシステムから入手する情報は、必要な項目以外は入手できないようにシステム上制約されている。	
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	1 システムを利用する必要がある職員を特定し、生体（静脈）情報とパスワードによる二要素認証を行うとともに、操作ログによる証跡を記録する。 2 住民からの届出・申請等の受付は、本事務に従事する職員以外には行わせないことで、入手権限を有しない者による詐取・奪取が行われないようにする。 <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）のデータベースは、区市町村ごとに論理的に区分されており、他の区市町村、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されている。	
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3： 入手した特定個人情報ที่ไม่正確であるリスク		
入手の際の本人確認の措置の内容	1 届出・申請等の受付の際は、本人確認書類（官公署が発行する写真付きの身分証明書等）の提示を受け、本人確認を行うとともに、個人番号カード等により、個人番号の確認を行う。 2 目黒区の住民基本台帳に登録がない者の場合は、必要に応じ、住民基本台帳ネットワークシステムにより本人確認情報と個人番号の対応付けを確認する。 3 情報の入力、削除及び修正を行う場合は、正確性を確保するため、入力、削除及び訂正を行った者以外の者が確認する。 4 接種記録については、システムへの登録内容と予診票・接種票等の内容とを照合する。	
個人番号の真正性確認の措置の内容	届出・申請等の受付の際については、本人の個人番号カード又は通知カード、本人確認書類の提示や窓口での聞き取りにより本人確認を行い、個人番号を確認する。	
特定個人情報の正確性確保の措置の内容	1 入手した情報については、窓口での聞き取りや添付書類との照合等を通じて確認することで正確性を確保している。 2 職員にて収集した情報に基づいて、間違いがあれば職権で適宜修正することで正確性を確保している。 3 入力作業員、審査作業員、決裁作業員を分担して入力ミスを軽減する。	
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漏えい・紛失するリスク		
リスクに対する措置の内容	1 予防接種システムの端末は、来庁者から見えない位置に配置するとともに、のぞき見防止フィルターを使用する。 2 プリンタは、部外者が出力された帳票を見たり、持ち去ったりすることができない場所に設置する。 3 個人番号が記載された帳票の執務室外への持ち出しは行わない。 4 執務室への入退室は、責任者が許可した者に制限する。 5 住民からの届出書・申請書等は、入力、削除及び訂正作業に用いた帳票等とともに、鍵付の書庫に保管する。	
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
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、事務に必要な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	システムの権限管理機能により制御を行い、個人番号利用事務実施者のみ個人番号を参照できるよう制御を行う。	
事務で使用するその他のシステムにおける措置の内容	個人番号利用事務以外の事務従事者が参照する場合には、権限管理機能により制御を行う。	
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: 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	システム利用は、所属長が認めた職員等のIDについて操作権限を割り当て、二要素によるユーザ認証を行っている。	
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	1 各所属長をセキュリティ責任者とし、職員の所属や担当に応じて必要な情報のみアクセスできるよう、権限の付与を行う。 2 異動等により所属が変わる際には、速やかにユーザー情報の更新を行い、適切な権限設定を維持するとともに、定期的な点検を行う。 3 臨時的に職員へ権限を付与する場合は、必要なアクセスの詳細を判断し、所属長の承認を得て発行・登録する。	
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	1 所管するシステムで使用するID及びパスワードは、個人単位で付与している。 2 システム管理者は、ユーザIDやアクセス権を定期的に確認し、不要なIDや過大なアクセス権を変更または削除する。この処理は、システム管理者の指示により、システム担当者が行う。	
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	予防接種システムへのログイン記録とともに、システムの操作ログ(画面遷移、帳票発行等)の記録を行う。	

その他の措置の内容	1 端末の利用にあたり、ログインユーザ以外の職員に端末を操作させない。また、他職員がログインしている状態で端末を操作しない運用を行っている。 2 自分のID・パスワードで他人が操作できないよう対策を講じている。(ID・パスワードを他人に教えない、ID・パスワードを付箋紙等に記載して貼らない、他の職員に自分のID・パスワードでログインさせない)	
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: 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	定期的なセキュリティ研修を行い、個人情報の業務外利用の禁止や漏えい防止策について、職員に周知徹底する。	
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: 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	1 予防接種システムの端末は特定個人情報ファイルの複製ができない仕組みとする。 2 各端末での外部記憶媒体用のインターフェイスを封じ、USBメモリ等への複写ができない仕組みとする。	
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
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		
<その他のリスク> 使用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> 1 事務処理後や離席時は画面ロック(初期画面に戻すこと)を徹底し、一定時間操作がない場合は、スクリーンセーバーにより画面ロックがかかる設定とする。 2 端末のディスプレイは、来庁者から見えない位置に配置するとともに、のぞき見防止フィルターを使用する。 3 データ出力に際しては、事前に管理責任者の承認を得る。		
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	委託契約書及び特定個人情報に係る覚書にて、特定個人情報保護管理体制に関する以下の文書の提出を義務づける。 1 情報セキュリティ及び特定個人情報保護に関する社内規程又は基準 2 以下の内容を含む従事者名簿 ① 特定個人情報保護の責任者の氏名及び連絡先 ② 委託業務において特定個人情報を取り扱う者の氏名及び業務執行場所 ③ 事故発生時の連絡先 3 個人情報保護に関する従事者教育の実施 <ワクチン接種記録システム(VRS)における措置> 目黒区、国、当該システムの運用保守事業者の三者の関係を規定した「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(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。	
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	委託契約書において、委託業務で取り扱う情報の目的外使用や複写等の禁止、委託業務の終了後の情報の消去及び消去内容の報告、委託業務で使用するパソコン等の盗難防止対策の実施、システム用IDの適切な管理等の対策の実施、情報セキュリティに関する教育の実施等、情報セキュリティの確保に必要な人的・物的・技術的対策の実施を義務づけている。	
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	委託先へ提供した資料を電子データ化する際に扱った従業員、日時、処理内容等を管理し、定期的に報告することを契約内容に含めている。	

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		委託先は目黒区に対してのみ特定個人情報の提供ができる。それ以外に対しては一切認められず、その旨を委託契約書に明記する。また、委託契約の報告条項に基づき、契約満了時に特定個人情報の取扱いについて書面にて報告させる。必要であれば、当区職員が現地調査することも可能とする。	
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		委託先に提供する際、日付、枚数を記録した受渡しの確認印を押印してもらい、区がそれを確認する。委託先から特定個人情報を受領する場合も同様とする。	
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		委託先に特定個人情報の消去を行わせるときは、物理的な破壊・専用ソフトウェアによるフォーマット等により、内容を読み出すことができないようにさせ、消去を証する書面の提出を求めることとし、必要に応じ、実地の検査等により確認することとする。	
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		目的外利用の禁止、特定個人情報の閲覧者・更新者の制限、特定個人情報の提供先の限定、情報漏洩を防ぐための保管管理に責任を負うべき旨、情報が不要となったとき又は要請があったときは情報の返還、消去等必要な措置を講じるべき旨、個人情報の取扱いについてチェックを行った上で契約満了時に報告すべき旨及び必要に応じて区が委託先の視察・監査を行うことができる旨を定める。	
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		目黒区が承諾した場合に限り、再委託を認めており、再委託先は特定個人情報ファイルの取扱い等について、委託先と同様の措置を行うことを契約書に明記する。	
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		＜予防接種システム及び共通連携基盤システムにおける措置＞ 特定個人情報の照会時には、どの端末・職員が、どの住民の情報についていつ参照を行ったかの記録をデータベースに逐一保存することで、不正な入手を防止する。 ＜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(※1)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照合リスト(※2)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(※3)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。 (※1)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照会及び照会した情報の受領を行う機能 (※2)番号法の規定によ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提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの (※3)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へのアクセス制御を行う機能			
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		＜予防接種システム及び共通連携基盤システムにおける措置＞ 情報提供ネットワークシステムとの全ての連携(接続)は、共通連携基盤システムの団体内統合宛名機能を介して中間サーバーが行う構成となっており、情報提供ネットワークシステム側から、本区の業務システムへのアクセスはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ 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、内閣総理大臣が設置・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設計されるため、安全性が担保されている。 ＜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、安全性を確保している。 2 中間サーバーと団体については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安全性を確保している。			
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3: 入手した特定個人情報 that 不正確であるリスク		
リスクに対する措置の内容	＜予防接種システム及び共通連携基盤システムにおける措置＞ 中間サーバへの連携にあたっては事前に十分なテスト及び検証を行い、不正確な入手を防止する。 ＜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。	
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	＜予防接種システム及び共通連携基盤システムにおける措置＞ 中間サーバと共通連携基盤システムの連携は、LGWAN、庁内ネットワーク及びサーバ間のみの通信とすることで、漏えい・紛失を防止する。 ＜中間サーバ・ソフトウェアにおける措置＞ 1 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(※)。 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。 (※) 中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜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。 2 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。 3 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	＜予防接種システム及び共通連携基盤システムにおける措置＞ 特定個人情報の提供時には、情報提供の記録(端末、職員、対象住民、照会日時)をデータベースに逐一保存することで、不正な提供を防止する。 ＜中間サーバ・ソフトウェアにおける措置＞ 1 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照会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、照会許可照会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。 2 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領し、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。 3 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。 4 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。 (※) 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提供の要求の受領及び情報提供を行う機能	

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	<予防接種システム及び共通連携基盤システムにおける措置> 特定の権限者以外は情報の照会及び提供ができず、さらに、情報照会・情報提供記録をデータベースに逐一保存することで、不適切な方法で特定個人情報が行りとりされることを防止する。 <中間サーバー・ソフトウェアにおける措置> 1 セキュリティ管理機能(※)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、情報照会者から受領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。 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になっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能。 <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ことを防止する。 2 中間サーバーと団体については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・紛失を防止する。 3 中間サーバーの保守・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	<予防接種システム及び共通連携基盤システムにおける措置> 1 誤った情報を提供してしまうリスクへの措置 提供・移転する情報の体系的な論理チェックを行い、誤った情報が作成されることを防止する。 2 誤った相手に提供してしまうリスクへの措置 番号法に基づき認められる情報に限り、認められた相手へのみ提供できる仕組みになっている。 <中間サーバー・ソフトウェアにおける措置> 1 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領した上で、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。 2 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。 3 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		
<その他のリスク> 接続の際に特定個人情報情報が漏えい・紛失するリスク <リスクに対する措置の内容> ○予防接種システム及び共通連携基盤システムにおける措置 情報提供ネットワークシステムとの全ての連携(接続)は、団体内統合宛名システムを介して中間サーバーが行う構成となっており、情報提供ネットワークシステム側から、区の業務システムへのアクセスはできない。 ○中間サーバ・ソフトウェアにおける措置 1 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。 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上担保されており、不正な名寄せが行われるリスクに対応している。 ○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、安全性を確保している。 2 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安全性を確保している。 3 中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。		
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
具体的な対策の内容	<目黒区における措置> 1 区施設内のサーバ設置場所の管理 ①区施設内の他の部屋とは区別し、専用の部屋とする。 ②出入口には、電子錠等による入退室を管理する設備を設ける。 ③監視カメラによる24時間監視を行う。 ④許可されたもの以外の機器持込み・使用を禁止する。 2 データセンターにおける管理 ①特定非営利活動法人日本データセンター協会が定める安全管理基準により高い安全性を確保する。 ②データセンターの入館・サーバ室の入退室を管理する設備を設ける。 ③地震や火災など災害に対して、データ保全の安全性・可用性を確保できる施設・設備とする。 ④機器の故障や保守など一部設備の停止時において、コンピューティングサービスを継続して提供できる冗長構成の設備を設ける。 ⑤バックアップデータは、データセンター内で管理する。 3 本特定個人情報を取り扱う部屋の管理 ①特定個人情報ファイル内のデータの参照・更新をすることができる業務端末は、セキュリティワイヤーで固定する。 ②特定個人情報が記載された書類は、鍵付きの書庫に保管する。 ③部外者の立入りを禁止する。 ④許可されたもの以外の機器持込み・使用を禁止する。 <中間サーバー・プラットフォームにおける措置> 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。 <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。 なお、主に以下の物理的対策を講じている。 1 サーバ設置場所等への入退室記録管理、施錠管理 2 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。

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		<目黒区における措置> 1 予防接種システムは、不正な侵入への対策が施された固有のネットワークにより構成され、インターネットとの接続は行っていない。 2 予防接種システムの端末は、外部記憶媒体の接続ができないよう設定されている。 3 システム操作者の権限設定は、担当する業務の内容に応じて詳細に設定し、アクセスログを記録している。 <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。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。 <ワクチン接種記録システムにおける措置> ワクチン接種記録システムは、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。 1 論理的に区分された当該市区町村の領域にデータを保管する。 2 当該領域のデータは、暗号化処理をする。 3 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。 4 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。 5 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。
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	生存者の特定個人情報と同様の方法にて安全管理措置を実施する。	
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	1 住民登録のある対象者に係る情報については、住民記録システムとの間におけるデータ連携により、定期的に自動更新する。 2 住民登録のない対象者に係る情報については、必要に応じ、住民基本台帳ネットワークシステムにより確認し、データを更新する。 3 非課税世帯等の要件確認に必要な情報については、他の業務システムとのデータ連携等により、最新の情報に更新する。 4 接種履歴については、接種情報入手の都度、データを更新する。 5 支払口座に係る情報等については、対象者からの依頼書等により確認する。 6 削除後一定期間経過したデータは、システム機能により消去する。	
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: 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	<目黒区における措置> 1 保管期間の満了した本特定個人情報ファイル内のデータは、システム上、一括して削除する仕組みとする。 2 磁気ディスクの廃棄時・リース機器の返還時には、内部のデータを削除し、物理的な破壊・専用ソフトウェアによるフォーマット等により、内容を読み出すことができないようにする。消去を証する書面の提出を求めることとし、必要に応じ、実地の検査等により確認することとする。 3 特定個人情報ファイルの消去については、その記録を残す。 4 本特定個人情報ファイルに関係する特定個人情報が記載された届出書・申出書・帳票等を廃棄するときは、溶解・細断等の措置により行い、区の決裁文書等を管理するシステムに廃棄処理日を記録する。 <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
具体的なチェック方法	<目黒区における措置> 年に1回、担当課内において、次の観点による自己点検を実施し、評価書の記載内容どおりの運用がなされていることを確認する。 1 評価書記載事項と運用実態のチェック 2 特定個人情報を含む個人情報の保護に関する規定及び体制の整備 3 特定個人情報を含む個人情報の保護に関する人的安全管理措置 4 職員の役割責任の明確化及び安全管理措置の周知・教育 5 特定個人情報を含む個人情報の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> 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) 十分にっていない
具体的な内容	<目黒区における措置> 1 年に1回、情報システムの管理及び運用が適正かつ円滑に行われていることの確認を目的とし、部局相互で行う内部監査を実施する。 2 情報セキュリティポリシーが遵守されていることを客観的に検証するため、適宜、第三者の監査人による外部監査を実施する。 <中間サーバー・プラットフォームにおける措置> 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	[特に力を入れて行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な方法	<目黒区における措置> 1 関係職員(会計年度任用職員等を含む。)に対して、初任時及び一定期間毎に、必要な知識の習得のための研修を実施し、その記録を残している。 2 各責任者に対して、その管理に関する必要な知識や技術を習得させるための研修を毎年実施し、その記録を残すとともに、関係職員に対して、一定期間毎に必要な知識の習得のための研修を実施し、その記録を残している。 3 受託業者に対し、契約において個人情報に関する研修の実施を義務付けている。 <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＞

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。

＜ワクチン接種記録システム(VRS)利用における措置＞

万が一、障害や情報漏えいが生じた場合に備え、デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出の「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」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)に基づき、適切な対応をとることができる体制を構築する。

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	目黒区健康推進部感染症対策課 郵便番号:153-8573 東京都目黒区上目黒二丁目19番15号 電話:03-5722-7047
②請求方法	書面で提出することにより受け付ける。
特記事項	目黒区公式ウェブサイトにおいて請求に必要な様式及び請求方法を公表する。
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	[行っている] <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	個人情報ファイル簿に記載の名称
公表場所	目黒区公式ウェブサイト
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	目黒区健康推進部感染症対策課 郵便番号:153-8573 東京都目黒区上目黒二丁目19番15号 電話:03-5722-7047
②対応方法	1 問合わせがあった場合は、問い合わせの内容と対応の経過について記録を残す。情報漏えい等に関する問合わせがあった場合は、実施機関において必要な対応を行い、情報政策推進部行政情報マネジメント課に報告する。 2 情報漏えい等に関する問合わせがあった場合は、実施機関において必要な対応を行い、企画経営部行政情報マネジメント課に報告する。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和6年9月1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	区報に実施についての記事を掲載するとともに、区公式ウェブサイト及び総合庁舎その他区有施設において評価書を公開し、意見を受け付ける。
②実施日・期間	令和6年12月1日から令和7年1月6日まで
③期間を短縮する特段の理由	—
④主な意見の内容	意見なし
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和7年2月3日
②方法	目黒区情報公開・個人情報保護審議会において点検を行う。
③結果	特定個人情報の取扱いやセキュリティ対策について質疑があった。
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	