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
41	健康増進事業の実施に関する事務　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

杉並区は健康増進事業の実施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

杉並区長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和8年3月31日

［令和7年5月　様式4］

項目一覧

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	健康増進事業の実施に関する事務
②事務の内容　※	健康増進法（平成14年法律第103号）（「以下、「健康増進法」という。）による健康増進事業の実施に関する事務であって主務省令で定めるもの Ⅰ　がん検診及び歯科健康診査、肝炎ウイルス検査（以下、「健診（検診）」という。）の概要と対象者 1　がん検診 （1）概要 東京都がん検診の精度管理のための技術的指針及び杉並区がん検診実施要綱に基づき、がんの早期発見・早期治療により区民の健康増進を図るために、がん検診を実施する。 （2）対象者 ①胃がん検診（胃内視鏡検査）：50歳以上の者で前年度胃がん検診（胃内視鏡検査）を受診していない者 ②胃がん検診（胃部エックス線検査）：50歳以上の者で前年度胃がん検診（胃内視鏡検査）を受診していない者 ③肺がん検診　40歳以上の者 ④子宮頸がん検診　20歳以上の女性で前年度子宮頸がん検診を受診していない者 ⑤乳がん検診　40歳以上の女性で前年度乳がん検診を受診していない者 ⑥大腸がん検診　40歳以上の者 上記①～⑥のがん検診を勤務先等で受診できる者は除く。 2　歯科健康診査 （1）概要 杉並区成人歯科健康診査実施要綱及び杉並区後期高齢者歯科健康診査実施要綱に基づき、歯科疾患予防・口腔の健康の保持増進・口腔機能の維持向上を図るため、歯科健康診査を実施する。 （2）対象者 ①成人歯科健康診査：20・25・30・35・40・45・50・60・70歳の者 ②後期高齢者歯科健康診査：76歳の者 3　肝炎ウイルス検査 （1）概要 杉並区区民健康診査等実施要綱に基づき、肝炎ウイルス感染の早期発見・早期治療・発病の予防・まん延の防止及び正しい知識を図るため、区民健診診査と同時に肝炎ウイルス検査を実施する。 （2）対象者 以下に規定する区民健康診査受診者のうち、過去に肝炎ウイルスの受診歴がない者 ①成人等健康診査 1）30歳以上39歳未満の者（ただし、本健康診査と同様の健診を勤務先等で受診できる者は除く） 2）40歳以上で生活保護法による被保護世帯に属する者 3）中国残留邦人等の円滑な帰国の促進並びに永住帰国した中国残留邦人等及び特別配偶者の自立を支援に関する法律による支援給付を受給している者 ②国保特定健康診査：40歳から74歳までの杉並区国民健康保険に加入している者 ③後期高齢者健康診査：後期高齢者医療制度に加入している者 Ⅱ　事務の内容 1　受診券の発行 住民基本台帳(以下、「住基」という。)の情報を基に、上記健診（検診）の各項番「（2）対象者」に対し、それぞれの健診（検診）受診券を作成・発行する。 ただし、区が実施するがん検診及び30歳から39歳までの成人等健診は、勤務先等で受診できる者を除いており、以下の条件を満たす対象者に受診券を送付する。 （1）窓口・郵送・電子申請のいずれかで区にがん検診及び30歳から39歳までの成人等健診の申し込みを行った者 （2）国保特定健康診査対象者 （3）【肺がん検診のみ】後期高齢者健康診査対象者及び40歳以上の成人等健康診査対象者、75歳以上の者 （4）毎年受診可能ながん検診は、前年度受診履歴がある者 （5）隔年実施のがん検診は、前々年度受診履歴がある者 （6）30歳から39歳までの成人等健診は、過去3年間に受診歴のある者 2　受診券の再発行 住基の情報を基に、受診券を紛失等した者に対して、受診券の再発行を行う。 3　健診（検診）受診結果の管理 健診（検診）実施機関で健診（検診）を受けた区民の受診票について、当該健診（検診）実施機関からの提出を受理し、受診結果を入力・管理する。 4　精密検査受診調査・勧奨通知の送付 がん検診の精密検査未把握者に対して、健診（検診）実施機関あるいは受診者に対し、精密検査受診の有無の調査と精密検査受診勧奨の通知を行う。 5　東京都及び国への報告 統計法に基づき、地域保健・健康増進事業報告として健診（検診）を受けた者の数等を東京都を経由し、国に報告する。 ※　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(平成25年法律第27号)(以下、「番号法」という。)の別表第二に基づき、区は健診（検診）に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報照会を行う。また、他機関からの情報照会に対応する為に、健康増進事業に係る特定個人情報を中間サーバーに登録する。情報提供ネットワークによる情報照会・提供を行う事務は、上記3。

③対象人数	[30万人以上] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

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	健診(検診)等データ管理システム
②システムの機能	1　受診券の交付 ・住基情報及び過去の受診履歴に応じて受診券の作成・発行処理を行う機能。 2　健診(検診)受診結果の管理 ・健診(検診)受診結果の登録処理を行う機能。 3　がん検診精密検査受診勧奨 ・がん検診精密検査未把握者に対して、精密検査受診調査を行うための宛名ラベル等を出力する機能。 4　住基等異動情報の連携 ・住基情報、国民健康保険情報、後期高齢者医療情報、生活保護情報の各異動データの連携処理を行い、健診(検診)対象者の情報の正確性を保つ機能。
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　（国民健康保険システム、後期高齢者医療システム、生活保護情報提供システム）

システム2～5

システム2

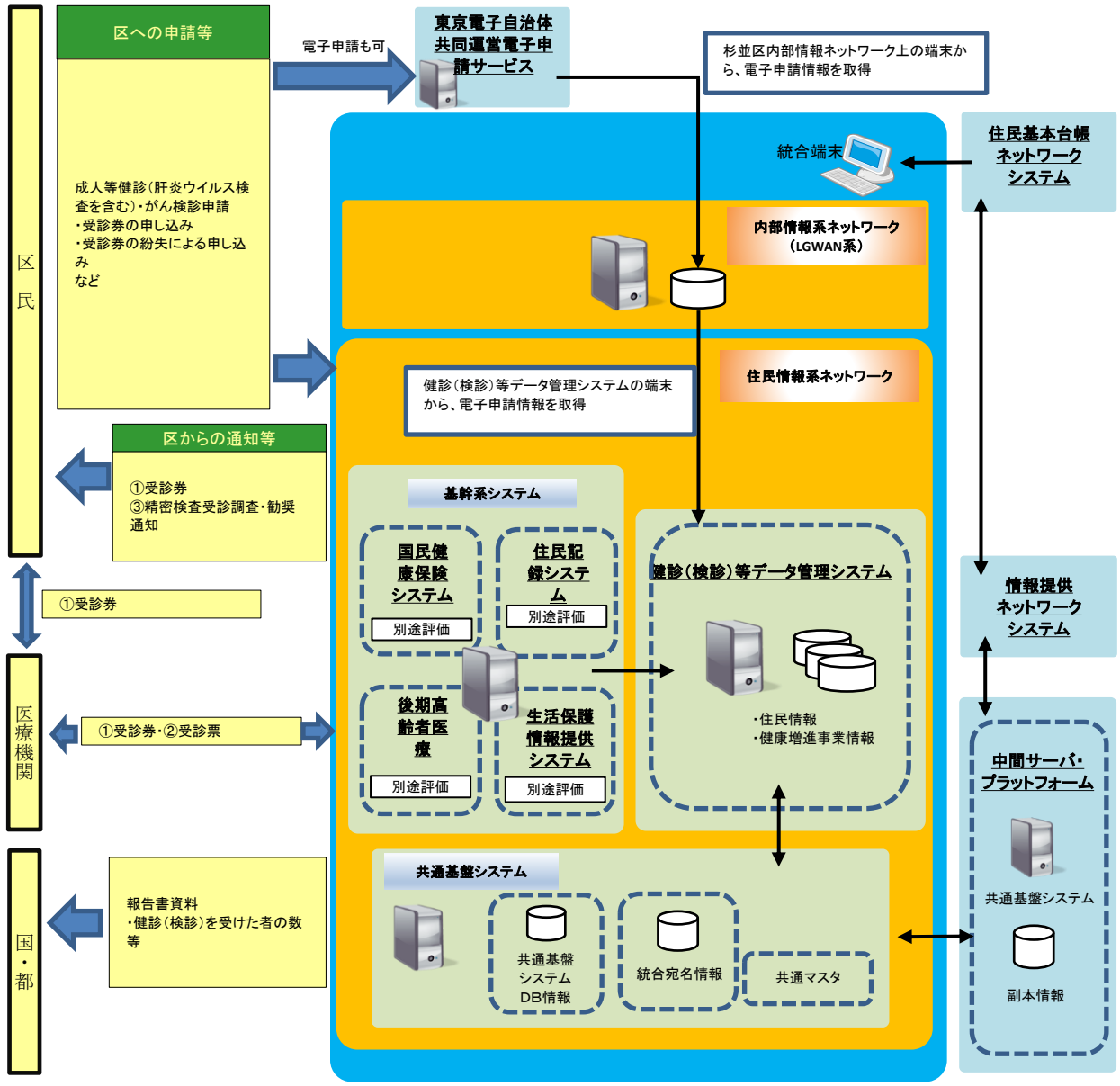
①システムの名称	共通基盤システム
②システムの機能	1　団体内統合宛名番号の付番と管理 　当該システムで、同一個人番号で一意となる団体内統合宛名番号の付番、及び宛名番号と個人番号との紐付け管理機能を実現する。 2　符号取得のためのシステム連携 　当該システムで団体内統合宛名番号を新たに付番した時、中間サーバへの符号取得要求、及び符号取得依頼の受付を行う。 3　文字コードの変換機能 　業務システムの文字コードと中間サーバ用の文字コードを変換する。 4　団体内統合宛名番号への変換・提供機能 　業務システムと中間サーバの連携時に宛名番号(または個人番号)を団体内統合宛名番号に変換する。業務システムからの問合せに対して、団体内統合宛名番号を提供する。 5　システム間通信プロトコル対応 　FTP連携時の通信プロトコル。 6　中間サーバからの要求による情報提供機能 　中間サーバからの要求による中間サーバへの4情報(住所、氏名、生年月日、性別。以下「4情報」の表示がある場合は全て同じ)提供。中間サーバへ提供するための4情報管理(登録・更新)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　（健診(検診)等データ管理システム、中間サーバ・プラットフォーム）

システム3	
①システムの名称	中間サーバ・プラットフォーム
②システムの機能	1　符号管理 　情報照会・情報提供に用いる個人の識別子である「情報提供用個人識別符号（以下「符号」という。）」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」を紐付け、その情報を保管・管理する。 2　情報照会 　情報照会機能は、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）の情報照会・情報提供受領（照会した情報の受領）を行う。 3　情報提供 　情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報連携対象）の提供を行う。 4　既存システム接続 　共通基盤システムと既存システム、共通基盤システム、基幹系システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報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、保管・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、保有・管理する。 7　データ送受信 　共通基盤システム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）との間で情報照会・情報提供、符号取得のための情報等を連携する。 8　操作者認証・権限管理 　共通基盤システムを利用する操作者のアクセス権限・操作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。 9　システム管理 　バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の消去を行う。
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　（ 共通基盤システム　　）
3. 特定個人情報ファイル名	
健康増進事業情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	健診（検診）の対象者及び受診結果を正確に把握し、適正な管理を行うため。
②実現が期待されるメリット	・個人番号を利用して他自治体等と情報連携することにより、転出入に関係なく健診（検診）情報を把握して、活用することにより、健康増進事業に活かすことができる。
5. 個人番号の利用　※	
法令上の根拠	・番号法 　第9条第1項　別表の111の項
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	［　　実施する　　］　　＜選択肢＞ 1）実施する 2）実施しない 3）未定
②法令上の根拠	・番号法第19条第8号及び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 （命令における情報提供の根拠） 139の項 （命令における情報照会の根拠） 139の項

7. 評価実施機関における担当部署	
①部署	杉並保健所健康推進課
②所属長の役職名	健診担当課長
8. 他の評価実施機関	
―	

（別添1）事務の内容
（備考）

（別添1）事務の内容



健康増進事業の実施に関する事務では、各健診（検診）の要件に該当する者に対し、受診券等を発行し、窓口渡し又は郵送する。ただし、成人等健診（肝炎ウイルス検査を含む）・がん検診については、窓口・郵送・電子申請で申し込みを行った者にも受診券を発行する。

●住基情報を基に、各健診（検診）の要件に該当する者に対し、①受診券を作成・発行する。
●住基情報を基に、受診券を紛失等した者に対し①受診券の再発行を行う。
●健診（検診）実施機関で健診（検診）を受診した区民の①受診券・②受診票について当該医療機関からの提出を受理し、受診結果を入力・管理する。
●精密検査未把握者の受診情報を把握するため、健診（検診）実施機関・区民に対し、③精密検査受診調査・勧奨通知を送付する。
●統計法に基づき、地域保健・健康増進事業報告として健診（検診）を受けた者の数等を東京都を経由し、国に報告する。

（備考）

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	
健康増進事業情報ファイル	
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　※	杉並区に住民登録がある健康増進事業の対象者及び利用者
その必要性	区民の健康増進に関する記録の適正な管理を図り、健康増進事業に関する記録を正確かつ統一的に行い、区民の健康を増進する必要があるため。
④記録される項目	[　10項目以上50項目未満　]　＜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 [○] 5情報（氏名、氏名の振り仮名、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	○識別情報 ・個人番号・・・手続時点において同一人の確認・特定をより的確に行うために必要である。 ・その他識別情報（内部番号）・・・既存住民基本台帳システム及び庁内連携システムで利用する識別情報（世帯番号・宛名番号）についても本人特定の他、庁内他事務のシステムと必要な情報を連携するために必要である。 ○連絡先等情報 ・4情報、連絡先（電話番号等）・・・申請者に対する申請内容の確認、問合せのために必要である。 ○業務関係情報 ・健康・医療関係情報・・・健診(検診)の適切な実施及び健診(検診)結果の管理をするために必要である。 ・生活保護・社会福祉関係情報・・・健診(検診)の自己負担金が免除対象となるので、生活保護の受給状況に関する情報が必要である。
全ての記録項目	別添2を参照。
⑤保有開始日	令和4年6月1日
⑥事務担当部署	杉並保健所健康推進課　保健福祉部国保年金課

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　（ 区民生活部区民課　保健福祉部国保年金課　保健福祉部福祉事務所 ） [　] 行政機関・独立行政法人等　（ ） [○] 地方公共団体・地方独立行政法人　（ 他自治体 ） [○] 民間事業者　（ 健診（検診）実施機関 ） [○] その他　（ 自部署 ）
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　（ 既存住民基本台帳システム ）
③入手の時期・頻度	住民基本情報： （入手元）区民生活部区民課 （入手頻度・時期）バッチ処理による日時連携 （入手方法）既存住民基本台帳システム 国民健康保険情報： （入手元）保健福祉部国保年金課 （入手頻度・時期）バッチ処理による日時連携 （入手方法）庁内連携システム 後期高齢者医療情報： （入手元）保健福祉部国保年金課 （入手頻度・時期）バッチ処理による日時連携 （入手方法）庁内連携システム 生活保護情報： （入手元）保健福祉部福祉事務所 （入手頻度・時期）バッチ処理による月次連携 （入手方法）庁内連携システム 健診(検診)結果情報： （入手元）健(検)診実施機関 （入手頻度・時期）月1回 （入手方法）紙、電子記録媒体
④入手に係る妥当性	・住民基本情報：既存住民基本台帳システムを使用して入手する住民基本情報については、本人等からの申請を受けた都度追加・更新する必要があり、法令等に基づく健診(検診)対象者であることの確認をおこなうものである。 ・国民健康保険情報：庁内連携システムを使用して入手する国民健康保険情報については、本人等からの申請を受けた都度更新する必要があり、法令等に基づく健診(検診)対象者であることの確認をおこなうものである。 ・後期高齢者医療情報：庁内連携システムを使用して入手する後期高齢者医療情報については、資格要件に該当した都度更新する必要があり、法令等に基づく健診(検診)対象者であることの確認をおこなうものである。 ・生活保護情報：庁内連携システムを使用して入手する生活保護情報については、自己負担金の徴収の有無について確認をおこなうものである。 ・健診(検診)結果情報：健診(検診)実施機関から入手する健診(検診)結果情報については、健康増進法第19条の2により規定されている健康増進事業実施要領に基づき、健診(検診)情報が健診(検診)実施機関から区に報告されるものである。
⑤本人への明示	・健康増進事業の実施に関する必要な各種情報については、番号法第19条8号及び別表第2の102の2項に基づき、収集していることを、広く区民に周知している。 ・健診(検診)実施機関又は本人から入手する場合は、本人等が記入する受診票にも、区が健診(検診)結果の統計や精度管理に活用することを明記している。
⑥使用目的 ※	・健康増進事業における適正な健診（検診）対象者の把握、案内、実施結果管理、要精密検査者の受診勧奨等を行うため。
変更の妥当性	―

⑦使用の主体	使用部署 ※	杉並保健所健康推進課、保健福祉部国保年金課
	使用者数	[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
⑧使用方法 ※		・健診（検診）の実施に関する対象者の把握 ・本人からの問い合わせに対応 ・健診（検診）の実施結果の管理 ・がん検診に係る精密検査受診の有無の調査、要精密検査者の受診勧奨 ・東京都及び国へ報告 ・健診(検診)情報を情報連携により照会・提供
	情報の突合 ※	・上記「⑧使用方法」欄に示す事務を正確かつ効率的に行うために、内部の宛名番号を突合キーとして、既存住民基本台帳システムから転送される4情報及び庁内連携システムから転送される国民健康保険情報・後期高齢者医療情報・生活保護受給情報、と本特定個人情報ファイル内の健診（検診）対象者に関する情報とを突合して個人特定を行う。
	情報の統計分析 ※	・東京都及び国へ健診（検診）受診者状況報告を行うが、特定の個人を判別するような情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	－
⑨使用開始日		令和4年6月1日

4. 特定個人情報ファイルの取扱いの委託

委託の有無 ※		[委託する]　＜選択肢＞ 1）委託する　2）委託しない （ 2 ） 件
委託事項1		健診(検診)等データ管理システム運営業務
①委託内容		健診(検診)等データ管理システム等の問合せ対応、バージョンアップ対応、障害対応等の保守業務、共通基盤システムの運用保守業務
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 ※	健康増進法等関連法令に定められる健診(検診)対象者
	その妥当性	システムの運用保守全般を委託しているため、そのシステムが取扱う特定個人情報ファイルについても取扱う必要がある。
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

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　（ 地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、IP-VPN等の閉域網の利用も可能。 ）
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載により確認できる。また、「Ⅴ. 開示請求、問合せ　1. ①請求先」への当区の情報公開請求による開示請求を行うことでも確認可能。
⑥委託先名		・日本コンピューター株式会社 ・日本電気株式会社
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	・再委託するかしないかについては、委託契約によるが、再委託の必要がある場合は、事前に委託先と書面による協議を行い、再委託の必要性や業務内容、再委託先のセキュリティ管理体制を確認した上で許諾する。
	⑨再委託事項	システム保守の一部
委託事項2～5		
委託事項2		ガバメントクラウドへのデータ移行作業
①委託内容		ガバメントクラウドへのデータ移行作業
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　※	健康増進法等関連法令に定められる健診(検診)対象者
	その妥当性	既存システムからデータ移行するために、特定個人情報ファイル全体を委託の対象にする必要がある。
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
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　（ 地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、IP-VPN等の閉域網の利用も可能。 ）
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載により確認できる。また、「Ⅴ. 開示請求、問合せ　1. ①請求先」への当区の情報公開請求による開示請求を行うことでも確認可能。
⑥委託先名		・日本コンピューター株式会社 ・日本電気株式会社
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	・再委託するかしないかについては、委託契約によるが、再委託の必要がある場合は、事前に委託先と書面による協議を行い、再委託の必要性や業務内容、再委託先のセキュリティ管理体制を確認した上で許諾する。
	⑨再委託事項	ガバメントクラウドへのデータ移行作業の一部

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　（　　1 ）件　［　　］移転を行っている　（　　）件 ［　　］行っていない
提供先1		市町村長
①法令上の根拠		番号法第19条第8号及び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表の第139の項
②提供先における用途		健康増進法による健康増進事業の実施に関する事務
③提供する情報		健康増進事業情報
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		「2.基本情報③対象者となる本人の範囲」と同じ
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		照会を受けた都度
6. 特定個人情報の保管・消去		
①保管場所　※		＜杉並区における措置＞ 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　健診(検診)結果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中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。 ＜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の規格に基づく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	［　　20年以上　　］ ＜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	がん検診については、健康増進法第19条の2に基づく「がん予防重点健康教育及びがん検診実施のための指針」に、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いる。また、肝炎ウイルス検査や歯科健康診査について明確な規定はないが、がん検診に準じている。ただし、区民からの健診（検診）結果確認の問い合わせ等に対応するため、長期保管する必要がある。

③消去方法	＜健診(検診)等データ管理システムにおける措置＞ ・各健診(検診)に応じて、受診回数及び受診間隔が定まっており、かつ受診対象年齢が幅広いため、区民からの問い合わせに対応する必要があることから、受診歴は削除しない。 ＜紙媒体における措置＞ ・保管期間を過ぎた紙媒体（健診(検診)結果等）は、年１回庁内で行う機密文書の一斉廃棄により溶解処理をしている。 ＜中間サーバー・プラットフォームにおける措置＞ 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事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。 さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。

7．備考

－

（別添2）特定個人情報ファイル記録項目

別紙【記録項目】のとおり

別紙【記録項目】

●健康増進事業情報ファイル　①住民基本台帳情報

1	市区町村番号	2	整理番号	3	カナ氏名	4	漢字氏名
5	本名カナ氏名	6	本名漢字氏名	7	通称カナ氏名	8	通称漢字氏名
9	アルファベット氏名	10	漢字併記カナ氏名	11	漢字併記氏名	12	生年月日
13	性別	14	町番号	15	行政区番号	16	番地
17	枝番	18	小枝	19	郵便番号	20	住所
21	方書	22	続柄1	23	続柄2	24	続柄3
25	続柄4	26	世帯番号	27	世帯主カナ氏名	28	世帯主漢字氏名
29	住登外区分	30	外国人フラグ	31	外国人国籍	32	住民となった日
33	住民でなくなった日	34	最新異動区分	35	最新異動日	36	最新異動届出日
37	住民異動区分	38	住民異動日	39	取消区分	40	転入前住所
41	転入前方書	42	転出後住所	43	転出後方書	44	補記論理和
45	連携番号	46	連携処理日	47	転入前住所コード	48	DV区分

●健康増進事業情報ファイル　②国保資格情報

1	市区町村番号	2	整理番号	3	履歴番号	4	保険者番号
5	被保険者証記号	6	被保険者証番号	7	国保加入日	8	国保脱退日
9	異動区分	10	異動日	11	異動処理日	12	最新フラグ

●健康増進事業情報ファイル　③後期資格情報

1	市区町村番号	2	整理番号	3	履歴番号	4	保険者番号
5	被保険者番号	6	後期高齢者加入日	7	後期高齢者脱退日	8	異動区分
9	異動日	10	異動処理日	11	最新フラグ		

●健康増進事業情報ファイル　④生保資格情報

1	市区町村番号	2	サブシステム	3	整理番号	4	受給者種別
5	受給開始日	6	受給終了日	7	受給有無	8	異動処理日
9	停止日	10	停止解除日				

●健康増進事業情報ファイル　⑤送付先情報

1	整理番号	2	送付先区分	3	送付先氏名	4	送付先カナ氏名
5	送付先郵便番号	6	送付先住所	7	送付先方書	8	送付先集配局
9	国保後期区分						

●健康増進事業情報ファイル　⑥肺がん検診一次検査結果情報

1	肺がん検診の受診年度	2	肺がん検診の受診日	3	肺がん検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	肺がん検診の受診医療機関
9	肺がん検診の受診方法	10	肺がん検診の過去の受診歴	11	肺がん検診時の肺がんに係る症状	12	肺がん検診時の喫煙指数
13	肺がん検診の胸部エックス線検査判定	14	肺がん検診の胸部エックス線検査所見	15	肺がん検診の喀痰検査受診日	16	肺がん検診の喀痰検査判定
17	肺がん検診の喀痰検査所見	18	肺がん検診の精密検査対象の有無	19	肺がん検診のその他所見	20	

●健康増進事業情報ファイル　⑦肺がん検診精密検査結果情報

1	肺がん検診の受診年度	2	肺がん検診の精密検査受診日	3	肺がん検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	肺がん検診の精密検査受診医療機関
9	肺がん検診の精密検査結果	10	肺がん検診の精密検査所見	11	精密検査時の偶発症の有無	12	精密検査担当医師名

●健康増進事業情報ファイル　⑧乳がん検診一次検査結果情報

1	乳がん検診の受診年度	2	乳がん検診の受診日	3	乳がん検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	乳がん検診の受診医療機関
9	乳がん検診の受診方法	10	乳がん検診の過去の受診歴	11	乳がん検診時の乳がんに係る症状	12	乳がん検診のマンモグラフィー検査判定
13	乳がん検診のマンモグラフィー検査所見	14	乳がん検診の精密検査対象の有無	15	乳がん検診のその他所見		

●健康増進事業情報ファイル　⑨乳がん検診精密検査結果情報

1	乳がん検診の受診年度	2	乳がん検診の精密検査受診日	3	乳がん検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	乳がん検診の精密検査受診医療機関
9	乳がん検診の精密検査結果	10	乳がん検診の精密検査所見	11	精密検査時の偶発症の有無	12	精密検査担当医師名

●健康増進事業情報ファイル　⑩胃がん検診一次検査結果情報

1	胃がん検診の受診年度	2	胃がん検診の受診日	3	胃がん検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	胃がん検診の受診医療機関
9	胃がん検診の受診方法	10	胃がん検診の過去の受診歴	11	胃がん検診時の胃がんに係る症状	12	胃がん検診の胃部エックス線検査判定
13	胃がん検診の胃部エックス線検査所見	14	胃がん検診の胃内視鏡検査判定	15	胃がん検診の胃内視鏡検査所見	16	胃がん検診の精密検査対象の有無
17	胃がん検診のその他所見						

●健康増進事業情報ファイル　⑪胃がん検診精密検査結果情報

1	胃がん検診の受診年度	2	胃がん検診の精密検査受診日	3	胃がん検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	胃がん検診の精密検査受診医療機関
9	胃がん検診の精密検査結果	10	胃がん検診の精密検査所見	11	精密検査時の偶発症の有無	12	精密検査担当医師名

●健康増進事業情報ファイル　⑫子宮頸がん検診一次検査結果情報

1	子宮頸がん検診の受診年度	2	子宮頸がん検診の受診日	3	子宮頸がん検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	子宮頸がん検診の受診医療機関
9	子宮頸がん検診の受診方法	10	子宮頸がん検診の過去の受診歴	11	子宮頸がん検診時の子宮頸がんに係る症状	12	子宮頸がん検診の視診所見有無
13	子宮頸がん検診の視診所見内容	14	子宮頸がん検診の内診所見有無	15	子宮頸がん検診の内診所見内容	16	子宮頸がんの頸部細胞診検査判定
17	子宮頸がんの頸部細胞診検査所見	18	子宮頸がん検診の精密検査対象の有無	19	子宮頸がん検診のその他所見		

●健康増進事業情報ファイル　⑬子宮頸がん検診精密検査結果情報

1	子宮頸がん検診の受診年度	2	子宮頸がん検診の精密検査受診日	3	子宮頸がん検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	子宮頸がん検診の精密検査受診医療機関
9	子宮頸がん検診の精密検査結果	10	子宮頸がん検診の精密検査所見	11	精密検査時の偶発症の有無	12	精密検査担当医師名

●健康増進事業情報ファイル　⑭大腸がん検診一次検査結果情報

1	大腸がん検診の受診年度	2	大腸がん検診の受診日	3	大腸がん検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	大腸がん検診の受診医療機関
9	大腸がん検診の受診方法	10	大腸がん検診の過去の受診歴	11	大腸がん検診時の大腸がんに係る症状	12	大腸がん検診の便潜血検査判定
13	大腸がん検診の便潜血検査所見	14	大腸がん検診の精密検査対象の有無	15	大腸がん検診のその他所見		

●健康増進事業情報ファイル　⑮大腸がん検診精密検査結果情報

1	大腸がん検診の受診年度	2	大腸がん検診の精密検査受診日	3	大腸がん検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	大腸がん検診の精密検査受診医療機関
9	大腸がん検診の精密検査結果	10	大腸がん検診の精密検査所見	11	精密検査時の偶発症の有無	12	精密検査担当医師名

●健康増進事業情報ファイル　⑯肝炎ウイルス一次検査結果情報

1	肝炎ウイルス検診の受診年度	2	肝炎ウイルス検診の受診日	3	肝炎ウイルス検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	肝炎ウイルス検診の受診医療機関
9	肝炎ウイルス検診の受診方法	10	肝炎ウイルス検診時の問診:肝臓病歴、肝機能が悪いと言われた経験	11	肝炎ウイルス検診時の問診:肝臓病歴、肝機能が悪いと言われた時期	12	肝炎ウイルス検診時の問診:広範な外科的処置歴の有無
13	肝炎ウイルス検診時の問診:広範な外科的処置時期	14	肝炎ウイルス検診時の問診:妊娠・分娩時の多量出血歴の有無	15	肝炎ウイルス検診時の問診:妊娠・分娩時の多量出血経験	16	肝炎ウイルス検診時の問診:定期的な肝機能検査受診歴の有無
17	肝炎ウイルス検診時の問診:B型肝炎ウイルス検査の受診歴の有無	18	肝炎ウイルス検診時の問診:B型肝炎ウイルス検査の受診時期	19	肝炎ウイルス検診時の問診:B型肝炎治療歴の有無	20	肝炎ウイルス検診時の問診:B型肝炎治療時期
21	肝炎ウイルス検診時の問診:C型肝炎ウイルス検査の受診歴の有無	22	肝炎ウイルス検診時の問診:C型肝炎ウイルス検査の受診時期	23	肝炎ウイルス検診時の問診:C型肝炎治療歴の有無	24	肝炎ウイルス検診時の問診:C型肝炎治療時期
25	肝炎ウイルス検診のB型肝炎ウイルス検査判定	26	肝炎ウイルス検診のC型肝炎ウイルス検査判定				

●健康増進事業情報ファイル　⑰肝炎ウイルス精密検査結果情報

1	肝炎ウイルス検診の受診年度	2	肝炎ウイルス検診の精密検査受診日	3	肝炎ウイルス検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	肝炎ウイルス検診の精密検査受診医療機関
9	肝炎ウイルス検診の精密検査結果	10	肝炎ウイルス検診の精密検査所見				

●健康増進事業情報ファイル　⑱歯周疾患一次検査結果情報

1	歯周疾患検診の受診年度	2	歯周疾患検診の受診日	3	歯周疾患検診の受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	歯周疾患検診の受診医療機関
9	歯周疾患検診の受診方法	10	歯周疾患検診の問診:1日で歯をみがく頻度	11	歯周疾患検診の問診:歯間ブラシやフロスの使用頻度	12	歯周疾患検診の問診:過去1年間の歯科検診の受診の有無
13	歯周疾患検診の問診:喫煙歴	14	歯周疾患検診の問診:喫煙を始めた年齢	15	歯周疾患検診の問診:喫煙を止めた年齢	16	歯周疾患検診の問診:1日の平均喫煙本数
17	歯周疾患検診の問診:糖尿病罹患の有無	18	歯周疾患検診の問診:関節リウマチ罹患の有無	19	歯周疾患検診の問診:狭心症・心筋梗塞・脳梗塞罹患の有無	20	歯周疾患検診の問診:内臓脂肪型肥満の有無
21	歯周疾患検診の問診:妊娠の有無	22	歯周疾患検診の問診:その他全身の状態	23	歯周疾患検診の健全歯数	24	歯周疾患検診の未処置歯数
25	歯周疾患検診の処理歯数	26	歯周疾患検診の喪失歯数	27	歯周疾患検診の要補綴歯数	28	歯周疾患検診の欠損補綴歯数
29	歯周疾患検診の現在歯数	30	歯周疾患検診の歯肉出血BOP(17または16)	31	歯周疾患検診の歯肉出血BOP(11)	32	歯周疾患検診の歯肉出血BOP(26または27)
33	歯周疾患検診の歯肉出血BOP(47または46)	34	歯周疾患検診の歯肉出血BOP(31)	35	歯周疾患検診の歯肉出血BOP(36または37)	36	歯周疾患検診の歯肉出血BOP(最大値)
37	歯周疾患検診の歯周ポケットPD(17または16)	38	歯周疾患検診の歯周ポケットPD(11)	39	歯周疾患検診の歯周ポケットPD(26または27)	40	歯周疾患検診の歯周ポケットPD(47または46)
41	歯周疾患検診の歯周ポケットPD(31)	42	歯周疾患検診の歯周ポケットPD(36または37)	43	歯周疾患検診の歯周ポケットPD(最大値)	44	歯周疾患検診の歯石の付着
45	歯周疾患検診の口腔清掃状態	46	歯周疾患検診の歯列咬合所見	47	歯周疾患検診の顎関節	48	歯周疾患検診の粘膜所見
49	歯周疾患検診のその他所見	50	歯周疾患検診の判定区分				

●健康増進事業情報ファイル　⑦歯周疾患精密検査結果情報

1	歯周疾患検診の受診年度	2	歯周疾患検診の精密検査受診日	3	歯周疾患検診の精密検査受診時年齢	4	保険者番号
5	被保険者記号	6	被保険者番号	7	枝番	8	歯周疾患検診の精密検査受診医療機関
9	歯周疾患検診の精密検査結果	10	歯周疾患検診の精密検査所見				

○共通基盤システムDB

1	氏名	2	住所	3	生年月日	4	性別
5	通称	6	個人番号	7	団体内統合宛名番号	8	個人コード

○情報連携

1	胃がん検診	2	肺がん検診	3	子宮頸がん検診	4	乳がん検診
5	大腸がん検診	6	成人歯科健診	7	後期高齢者歯科健診	8	肝炎ウイルス検査

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	
健康増進事業情報ファイル	
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	・「健康推進課情報セキュリティ実施手順」に基づき、情報セキュリティ教育を実施する際、対象者と無関係な情報へのアクセスは不正アクセスに該当し、番号法及び個人情報の保護に関する法律（以下、「個人情報保護法」という）における罰則規定があること、操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、対象者以外の情報入手を防止している。 ・窓口で情報を入手する場合は、番号法16条及び同施行令第12条に基づき、本人確認書類の提示等を受けることで、対象者以外の情報入手を防止している。
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	・「健康推進課情報セキュリティ実施手順」に基づき、情報セキュリティ教育を実施する際、対象者情報であっても、業務に不必要な情報へのアクセスは不正アクセスに該当し、番号法及び個人情報保護法における罰則規定があること、操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、必要以外の情報入手を防止している。 ・申請用紙等について、あらかじめ法令等により定められた様式で提出されることから、必要以外の情報が記載できない書式となっている。
その他の措置の内容	・健診(検診)等データ管理システムは住基情報及び国民健康保険情報、後期高齢者医療情報、生活保護情報との連携処理にて取得する方法のみであるため、対象者以外の情報は入手されない。 ・健診（検診）実施機関から提出された受診票をシステムへ取り込む際、受診票に記載された4情報とマッチングを行い、適切な情報のみをシステムに取り込む。
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	・番号法及び個人情報保護法における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・委託業務については委託先との契約により、委託業者が従事者に対して情報セキュリティ教育を行い、根拠法令等の規定に基づく正当な情報入手を指導する。 ・健康増進事業の実施に関する事務を取り扱うにあたり、根拠法令である健康増進法及び同施行令等に規定された内容を遵守することで、不適切な方法による情報の入手を防止する。 ・「健康推進課情報セキュリティ実施手順」による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は、法令で定められ、杉並区情報公開・個人情報保護審議会への必要な手続きを行なったものに限定する。 ・システムの操作に当たり、情報セキュリティ実施手順に則って、操作履歴の採取、保管、及び定期的な確認を行うことで、必要以外の情報の入手を抑止する。 ・本人から情報を取得する場合は、健診（検診）に係る事務に用いる旨を説明した上で取得する。
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：　入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・本人から個人番号の提供を受ける場合には、個人番号カードや通知カードの提示を受ける。また、本人確認を行う際は、番号法16条及び同施行令第12条に基づき、本人確認書類の提示等を受ける。また、受けた申請書等については、4情報を確認することで入手する情報の正確性を担保する。 ・他区市町村等、本人以外から個人番号の提供を受ける際は、情報提供元が本人に対して個人番号及び4情報が正しいことを確認する。
個人番号の真正性確認の措置の内容	・国等から示される事務処理要領等を参考に事務処理対象者の個人番号カード等の提示を受け、本人確認及び個人番号の確認を行う。 ・入手した特定個人情報について、保持している特定個人情報と突合を行い、真正性及び正確性確認を行う。 ・個人番号カードの提示が無い場合には、運転免許証の提示等により得られた本人確認情報とシステムによって確認する本人確認情報との対応付けを行い、個人番号が本人のものであることを担保する。 ・住民登録外者の場合は、住民基本台帳ネットワークを通して住民登録地である自治体へ個人番号を照会し、本人確認情報との対応付けを行う。

特定個人情報の正確性確保の措置の内容	・窓口での聴聞や添付書類との整合性から正確性を担保する。 ・情報の入力、削除、訂正を行う場合には処理者と点検者を別にし、二重チェックを行うことで正確性を担保する。 ・正確性に疑義が生じた場合は、健康増進法及び同施行令等に基づき、適宜調査を行い、必要に応じてデータを修正することで正確性を担保する。 ・入手した特定個人情報について、保持している特定個人情報と突合を行い、正確性を担保する。
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が漏えい・紛失するリスク	
リスクに対する措置の内容	・窓口で本人又は本人の代理人が来庁する場合は、個人番号利用事務実施者が直接申請書等を収受する。また、受付事務等が完了次第、直ちに書類を定められた場所へ格納する。 ・郵送で情報を入手する場合は、送付先誤り等による情報漏えい・紛失等を防止するため、事前に担当所属名及び所在地を広く周知する。また、返信用封筒等はあらかじめ担当所属名及び所在地が印字されているものを利用する。 ・電子申請にて情報を入手する場合は、東京電子自治体共同運営電子申請サービスと杉並区の内部情報系システムとの間は、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・紛失するリスクに対応している。 ・端末には、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。データ持ち出し時に使用する電子媒体（USBメモリ等）は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・システム起動に必要なソフトウェアは、情報管理課への申請による必要個数のみが貸与されるため入力が行える端末を限定し、操作に必要なID、パスワードは、各所属長から情報システム担当課長への申請により付与する運用とすることで、操作権限のない者による不正な操作を防止している。
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
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、事務に必要の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	・宛名システム機能は共通基盤システムが実施する仕組みであり、個人番号利用事務以外では個人番号の検索ができないよう、システム上で制御する。 ・共通基盤システムには個人番号、4情報等の情報連携に必要となる情報のみ記録し、不必要な情報との紐付けができないよう、システム上で制御する。 ・入力する端末機は、入退室管理をする執務室でのみ操作可能であり、システムを利用する者ごとに配布されたユーザID・パスワードによる認証及び生体認証を行うことで不要なアクセスを防いでいる。
事務で使用するその他のシステムにおける措置の内容	・個人番号利用事務のみ個人番号検索を可能とする仕組みとするため、他システムにおける個人番号利用事務以外からの情報の紐付けは行えないよう、システム上で制御している。 ・ファイアウォールを設置し、システム間の接続を制御することにより、予め許可したシステムを除く外部のシステムからの接続が行われないよう制御する。 ・ファイアウォールで制御したシステム間の通信は、ログとして記録し、ログの確認により適正な通信が行われているか監視する。
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： 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	・端末の事前登録（端末認証）を行い、ユーザID・パスワードによる認証を行う。また、パスワードは「資源管理基準」、「庁内ネットワーク等利用要領」により定められた期間内に変更する。 ・登録されているユーザ情報については管理権限を付与された職員が定期的に確認し、記録に残す。 ・システムを利用する者１人に付与されるIDは１つのみで、IDの共有を禁止する。
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	・アクセス権限の発行は、健康推進課からの発行申請により情報システム担当課長の承認後、当該課長から管理権限を付与された職員が行う。失効は、健康推進課からの解除申請により、管理権限を付与された職員が行う。この他、申請漏れ等への対応として、人事異動情報その他の権限失効に関わる情報を管理権限を付与された職員が得た段階で、随時その権限を失効している。
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	・情報セキュリティ管理者（所属長）は、アクセス権限と事務の対応表（事務担当者に対する権限付与の範囲を規定したもの）を作成し、定期的に付与されている権限と対応表が一致しているか点検を行い、違いが発見された場合には、ただちに適正な状態に修正する。 ・ユーザーアカウントおよびアクセス権について不要・不適切なものがないか定期的に確認する手順が「健康推進課情報セキュリティ実施手順」に定められており、当該規定に基づき確認を行っている。 ・各システム共にユーザーIDの共有を禁止している。
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	・システムの操作ログを保管する。ログは個人番号を参照・入力した際に個人単位で記録する。 ・保管するログは、物理的に区画・施錠された保管棚で、「杉並区文書等保存年限基準」及び「健康推進課情報セキュリティ実施手順」に基づき管理する。
その他の措置の内容	・不正な第三者からのアクセスを制御するため、特定個人情報を取り扱う執務室内への入退室管理について「健康推進課情報セキュリティ実施手順書」に規定し、規定された内容を遵守することで、権限のない者が特定個人情報を使用するリスクに対応する。
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： 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	・健診（検診）に関する事務を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での情報収集の禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での情報収集の禁止を徹底する。区は当該教育の実施について履行確認を行う。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。
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	・情報の持ち出しについて「資源管理基準」、「庁内ネットワーク等利用要領」及び「健康推進課情報セキュリティ実施手順」の中で規定し、職員に周知・徹底を行っている。 ・端末には、大量複製につながるUSBメモリ等の使用について、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。 ・データ持ち出し時に使用する電子媒体（USBメモリ）は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。その他の端末はUSBポートからのデータ出力を不可としている。また、管理権限を付与された職員以外はOSの設定変更、ソフトウェアの変更等を行えないよう、システム上で制御している。 ・バックアップ以外にファイルを複製しないよう、職員・委託先に対し指導している。
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

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	
―	

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		・委託する際は、ISMS、プライバシーマーク等の認証取得を求めるなど、委託先の社会的信用と能力を確認する。 ・「個人情報に係る外部委託契約仕様書の特記ガイドライン」に基づき、区が個人情報を保護するために必要があると認めるときは、受託者が業務を行う事務所、作業所等の立入り、個人情報の管理状況等について調査・立入調査を実施する。また、受託者が再委託を行っている場合は、再委託先に対しても区は受託者に対する調査と同様の調査を実施する。
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	・委託先において特定個人情報ファイルの処理等に係る者を明確化するため、契約後速やかに所属・氏名等を明記した実施体制の提出を義務付けている。また、体制に変更があった場合にも、変更後の体制を速やかに提出することを義務付ける。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させるとともに、セキュリティ研修の実施を義務付けている。 ・誓約書の提出があった要員に対してのみシステム操作の権限を与えている。 ・操作権限によって画面に表示される項目及び発行する帳票は必要なもののみとする。
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	・システムの操作ログを記録している。
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	・契約で個人情報の持ち出しは認めていない。 ・提供の禁止を契約書に明記している。
	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	・リモート保守を実施する場合やデータ移行作業をする場合は専用区画で実施することとし、入退室の記録を残している。 ・保守等に用いる端末へのログインには多要素認証を用いることとし、許可された者以外の作業を禁止している。 ・業務データを取り扱う端末のインターネットへの接続を禁止している。 ・次のような場合を除き、区はガバメントクラウドから保守事業者の環境へのデータの持ち出しを許可していない。 ①ガバメントクラウドへのサイバー攻撃等により、ガバメントクラウド上からデータを退避する必要が生じた場合 ②ガバメントクラウド上のシステムで障害が発生し、クラウド環境では原因が特定できない場合 ③業務データを保管するために利用しているクラウド事業者を変更する場合 ④このほか、ガバメントクラウドからデータを持ち出すことに緊急または相当の必要性があると区が認める場合 ・保守事業者は、ガバメントクラウドからのデータの持ち出しを行った場合、保守事業者の環境に持ち出したデータを保管する必要がなくなった段階で、速やかに返還又は廃棄し、区に報告することとしている。 ・業務データの保守環境からの持ち出しは許可していない。
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	契約で、以下の措置をとる旨を規定している。 ・業務を処理するために委託元から引き渡され、または委託先が収集し、若しくは作成した個人情報が記録されている資料等は、業務完了後直ちに返還するものとする。ただし委託元が特定個人情報の消去について別に指示した場合には、委託先事業者から任意の様式による消去結果に係る報告書の提出を義務付けている。

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	以下について、個人情報特記仕様書にて個人情報の取り扱いについて明記している。 ・個人情報の適切な管理 ・秘密の保持 ・再委託の制限 ・目的外の使用の禁止 ・第三者への提供の制限 ・複写及び複製の制限 ・個人情報の返還・廃棄 ・個人情報の取扱いに関する実地検査 ・事故発生時の報告 ・関係法令の遵守
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	・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承認した業者については、再委託を許諾するとともにセキュリティ事項について委託と同様の措置を義務付ける。 ・「個人情報に係る特記仕様書」において、再委託を行う場合の措置や実地検査に係る規定を設けている。これにより、委託先において、再委託先の特定個人情報の取扱いの監督を行っているかどうかを区が間接的に監督する。
その他の措置の内容		・委託事業者の業務実施場所において、携帯電話やカメラ等の通信機器や録画機器の使用を、契約で制限している。
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
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	＜中間サーバ・ソフトウェアにおける措置＞ ・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用照合リスト（※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する。 ・中間サーバの職員認証・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となる。 （※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）番号法別表第2及び第19条第9号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバ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	＜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を入手するため、正確な照会対象者に係る特定個人情報を入手することを担保する。
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： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜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を入手するため、正確な照会対象者に係る特定個人情報を入手することを担保する。
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： 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	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、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、一定期間経過後に結果情報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。 （※）中間サーバーは、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ー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、漏えい・紛失のリスクに対応している。 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漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。
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	＜中間サーバ・ソフトウェアにおける措置＞ ・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用照合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、照会許可用照合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。 ・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信し、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。 ・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。 ・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信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	＜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用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リスクに対応している。 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漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、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	＜中間サーバ・ソフトウェアにおける措置＞ ・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信した上で、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。 ・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。 ・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。 （※）特定個人情報を副本として保存・管理する機能。
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
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	
＜中間サーバー・ソフトウェアにおける措置＞ ①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。 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。 ③中間サーバー・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、中間サーバー・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。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	

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	・区に設置する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、かつ、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。 ・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。 ・健康増進事業情報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、杉並区文書等管理規定に従い、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＞ ①中間サーバー･プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ＜ガバメントクラウドにおける措置①＞ 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クラウド事業者は、その従業員に対して、適正な許可のない装置等の外部への持出は認めていない。 また、クラウド事業者は、区のデータにアクセスできない措置を講じている。 ＜ガバメントクラウドにおける措置②＞ ガバメントクラウド内の特定個人情報を記録するサーバについては、次の対策を行っている。 ・サーバ設置エリアへの入退室管理 ・監視カメラ及び侵入検知防止システムによる常時監視 ・事前申請による入館管理 ・入館時における二要素認証の実施及び入退室状況の監査	

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	＜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＞ ・区のLAN及びWAN（インターネット網）からの通信はファイアウォールにより遮断している。 ＜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杉並区が委託したアプリケーション開発事業者等は、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杉並区が委託したアプリケーション開発事業者等は、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の環境は、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杉並区やアプリケーション開発事業者等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杉並区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。 ＜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。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥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。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	
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		[　発生あり　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	令和4年11月5日、区職員が住民基本台帳ネットを不正に検索して得た個人情報を漏えいしたとして、住民基本台帳法違反容疑により逮捕される事案が発生した。 ※本事案は、当該職員が区民生活部区民課に在籍していた令和3年度に発生した。
	再発防止策の内容	「杉並区職員の逮捕に伴う再発防止対策検討委員会報告書」に基づき、再発防止対策を実施する。 再発防止策は以下（1）～（3）のとおりである。 （1）操作ログ点検の充実・強化 ・氏名等による検索は、事前に検索内容を記録票へ記入して、他の職員の確認を受けた上で行う。 ・操作ログの点検は各課で毎月実施することとし、その操作ログと記録票を突合する。 （2）職員に対する教育・研修の充実・強化 ・初任者研修等に加え、新たに毎年、全職員に対して職場ごとに公務員倫理・情報セキュリティの研修を実施する。 ・住基ネット操作権限を持つ職員に対しては、権限付与時の教育・研修に加え、新たに毎年、動画視聴方式等による教育・研修を実施する。 ・区民課の住基ネット業務管理補助者に対する教育・研修（区民課住基ネット業務管理補助者研修）については、初任時に加え、新たに毎年、教育・研修を実施する。 ・住基ネットに関する職員自己点検の内容について、設問を見直す。 （3）職場環境の見直し ・各職場において、セキュリティ対策について、話し合いを行い、必要に応じて、住基ネット端末の設置場所などのレイアウト変更を行う等、職場環境の必要な見直し・改善を図り、より一層風通しのよい職場づくりを進め、職場全体で不正行為を防止する。 ・情報の持出しを防ぐために、区民課の住基ネット端末設置エリアへの電子機器持込みは原則禁止とする。 ・住基ネット端末設置エリアには、このことを張り紙等で明示する。
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		ー
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		・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	・保管年限を経過した文書は廃棄を行うことについて決裁の上、総務課が全庁取りまとめて廃棄する。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、廃棄し、その事について記録簿に記録する。 ・保管年限を経過した特定個人情報は、定期的に業務主管課からの依頼により、情報管理課職員による消去処理を実施し、その記録を残す。 ＜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等の規格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	ー
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
ー

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。 ・杉並区情報セキュリティ対策基準に基づく各課におけるセキュリティ点検を年に1度実施の上、政策経営部情報政策課に報告している。 ＜中間サーバ・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・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	＜本区における措置＞ ・杉並区情報セキュリティ対策基準及び杉並区特定個人情報取扱規程に基づき定期的に行う。監査結果を踏まえて安全管理措置（体制、規定を含む。）を改善する。 ＜中間サーバ・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。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録された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。 ＜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	・人事異動等により、新規に事務を取り扱う場合における、個人情報の取り扱いに係る研修の実施について「健康推進課情報セキュリティ実施手順」で規定し、研修を実施する。また、異動者に限らず、職員については定期的に個人情報保護に係るセキュリティ等研修を実施する。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させるとともに、セキュリティ研修の実施を義務付ける。 ＜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。 ・中間サーバ・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・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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者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杉並区及びその業務データの取扱いについて委託を受けるアプリケーション開発事業者等が責任を有する。
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、杉並区に業務アプリケーションサービスを提供するアプリケーション開発事業者等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、杉並区とデジタル庁及び関係者で協議を行う。

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	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報管理課情報公開係
②請求方法	・指定の様式を定め、書面により、窓口で受け付けている。（詳細は、下記URLもしくは、”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”への問合せにより確認できる。） ・書面の様式・受付手続きの詳細のリンク先 杉並区公式ホームページ－申請書サービス-行政関連-情報公開等－自己情報開示・訂正・消去・利用中止請求書（URL:https://www.city.suginami.tokyo.jp/shinseisho/gyosei/johokoukai/1006209.html）
特記事項	任意の様式においても記載事項を網羅していれば、開示・訂正・利用停止請求を受け付ける
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	・健康増進事業情報ファイル
公表場所	「1. ①請求先」と同じ
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	郵便番号167-0051 東京都杉並区荻窪5-20-1 杉並区保健福祉部杉並保健所健康推進課健診係
②対応方法	・問い合わせの受付時に受付票を起票し、対応について記録に残す。 ・情報漏えい等の重大な事案に関する問い合わせについて、関係先に事実確認を行う為の標準的な処理期間を設ける。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年2月14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	健康増進事業の実施に関する事務全項目評価書（案）を区公式ホームページ、閲覧場所にて公示。 意見ははがき、封書、ファックス、Eメール、閲覧場所にある意見用紙による受付。
②実施日・期間	令和6年8月1日から令和6年8月31日
③期間を短縮する特段の理由	
④主な意見の内容	1件　システム構築の技術的な面での信頼性に疑問がある。政府に対する信頼度も低い中での、情報の一本化は避けるべき。
⑤評価書への反映	評価書の記載に関する意見ではなかったため反映なし。
3. 第三者点検	
①実施日	令和6年9月26日
②方法	杉並区情報公開・個人情報審議会による第三者点検を実施した。
③結果	杉並区情報公開・個人情報審議会において、介護保険に関する事務の特定個人情報保護評価書の適合性・妥当性の審査の結果、本特定個人情報保護評価においては、それらのリスク対策が適切に講じられていることを確認するとともに、特定個人情報ファイルの取扱いに伴い個人のプライバシーへの影響を及ぼす可能性がある事項や問題について適切に評価、確認及び取組が実施されていることを確認した。
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	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年4月17日	Ⅲ2リスク4	情報政策課	情報管理課	事後	重要な変更に当たらない（組織改正による課の名称変更）
令和5年4月17日	Ⅲ7リスク3	情報政策課	情報管理課	事後	重要な変更に当たらない（組織改正による課の名称変更）
令和5年4月17日	V1①	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報政策課情報公開係	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報管理課情報公開係	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和5年4月17日	Ⅲ7リスク1 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］	［発生あり］	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和5年4月17日	Ⅲ7リスク1 ⑨その内容	（追加）	令和4年11月5日、区職員が住民基本台帳ネットを不正に検索して得た個人情報を漏えいしたとして、住民基本台帳法違反容疑により逮捕される事案が発生した。 ※本事案は、当該職員が区民生活部区民課に在籍していた令和3年度に発生した。	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和5年4月17日	Ⅲ7リスク1 ⑨再発防止策の内容	（追加）	「杉並区職員の逮捕に伴う再発防止対策検討委員会報告書」に基づき、再発防止対策を実施する。 再発防止策は以下（1）～（3）のとおりである。 （1）操作ログ点検の充実・強化 ・氏名等による検索は、事前に検索内容を記録票へ記入して、他の職員の確認を受けた上で行う。 ・操作ログの点検は各課で毎月実施することとし、その操作ログと記録票を突合する。 （2）職員に対する教育・研修の充実・強化 ・初任者研修等に加え、新たに毎年、全職員に対して職場ごとに公務員倫理・情報セキュリティの研修を実施する。 ・住基ネット操作権限を持つ職員に対しては、権限付与時の教育・研修に加え、新たに毎年、動画視聴方式等による教育・研修を実施する。 ・区民課の住基ネット業務管理補助者に対する教育・研修（区民課住基ネット業務管理補助者研修）については、初任時に加え、新たに毎年、教育・研修を実施する。 ・住基ネットに関する職員自己点検の内容について、設問を見直す。 （3）職場環境の見直し ・各職場において、セキュリティ対策について、話し合いを行い、必要に応じて、住基ネット端末の設置場所などのレイアウト変更を行う等、職場環境の必要な見直し・改善を図り、より一層風通しのよい職場づくりを進め、職場全体で不正行為を防止する。 ・情報の持出しを防ぐために、区民課の住基ネット端末設置エリアへの電子機器持込みは原則禁止とする。 ・住基ネット端末設置エリアには、このことを張り紙等で明示する。	事後	その他の項目の変更であり事前の提出・公表が義務付けられない

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年2月7日	Ⅰ基本情報 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 ③他のシステムとの接続	（追加）	・「宛名システム等」に「〇」をつける。 ・「その他」から「中間サーバコネクタ」の名称を削除。	事後	機器更改のため
令和6年2月7日	Ⅰ基本情報 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2 ①システムの名称 ③他のシステムとの接続	（追加）	①システムの名称 「中間サーバコネクタ」の記載を「共通基盤システム」に変更。 ③他システムとの接続 「宛名システム等」に「〇」をつける。	事後	機器更改のため
令和6年2月7日	Ⅰ基本情報 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3 ②システムの機能 ③他のシステムとの接続	（追加）	②システムの機能 「中間サーバコネクタ」の記載を「共通基盤システム」に変更。 ③他のシステムとの接続 「宛名システム等」に「〇」をつける。 その他の「中間サーバコネクタ」の記載を「共通基盤システム」に変更。	事後	機器更改のため
令和6年2月7日	Ⅱ　ファイルの概要 委託事項2	中間サーバコネクタの運用保守業務	共通基盤システムの運用保守業務	事後	機器更改のため
令和6年2月7日	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 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要ない情報との紐づ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	・宛名システム機能は中間サーバコネクタが実施する仕組みであり、個人番号利用事務以外では個人番号の検索ができないよう、システム上で制御する。 ・中間サーバコネクタには個人番号、基本4情報等の情報連携に必要となる情報のみ記録し、不必要な情報との紐付けができないよう、システム上で制御する。	・宛名システム機能は共通基盤システムが実施する仕組みであり、個人番号利用事務以外では個人番号の検索ができないよう、システム上で制御する。 ・共通基盤システムには個人番号、基本4情報等の情報連携に必要となる情報のみ記録し、不必要な情報との紐付けができないよう、システム上で制御する。	事後	機器更改のため
令和6年2月7日	（別添1）事務内容	（追加）	「中間サーバコネクタ」の記載を「共通基盤システム」に変更。	事後	機器更改のため
令和6年2月7日	（別添2）ファイル記録項目	（追加）	「中間サーバコネクタ」の記載を「共通基盤システム」に変更。	事後	機器更改のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年2月7日	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 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	（略）番号法及び杉並区個人情報保護条例における罰則規定があること、（略）	（略）番号法及び個人情報の保護に関する法律（以下、「個人情報保護法」という）における罰則規定があること、（略）	事後	条例改正のため
令和6年2月7日	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 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	（略）番号法及び杉並区個人情報保護条例における罰則規定があること、（略）	（略）番号法及び個人情報保護法における罰則規定があること、（略）	事後	条例改正のため
令和6年2月7日	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 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	・番号法及び杉並区個人情報保護条例における罰則規定を広く個人番号利用事務実施者に周知することで（略）	・番号法及び個人情報保護法における罰則規定を広く個人番号利用事務実施者に周知することで（略）	事後	条例改正のため
令和6年2月7日	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 4. 特定個人情報ファイルの取扱いの委託 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 規定の内容	以下について、個人情報特記仕様書にて個人情報の取り扱いについて明記している。 ・個人情報の適切な管理 ・秘密の保持 ・再委託の禁止 ・目的外の使用の禁止 ・第三者への提供の禁止 ・複写及び複製の禁止 ・個人情報の返還・廃棄 ・個人情報の取扱いに関する立入調査 ・事故発生時の報告 ・法令及び杉並区の条例遵守	以下について、個人情報特記仕様書にて個人情報の取り扱いについて明記している。 ・個人情報の適切な管理 ・秘密の保持 ・再委託の制限 ・目的外の使用の禁止 ・第三者への提供の制限 ・複写及び複製の制限 ・個人情報の返還・廃棄 ・個人情報の取扱いに関する実地検査 ・事故発生時の報告 ・関係法令の遵守	事後	特記仕様書の改正のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年2月7日	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 4. 特定個人情報ファイルの取扱いの委託 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 具体的な方法	・「個人情報に係る特記仕様書」において、「再委託等を行う場合、受託者は、再委託等において実施される業務についての本特記事項遵守について監督及び区への必要な報告を行わなければならない」としている。この報告により、（略）	・「個人情報に係る特記仕様書」において、再委託を行う場合の措置や実地検査に係る規定を設けている。これにより、（略）	事後	特記仕様書の改正のため
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1　健診（検診）等データ管理システム運営業務 ①委託内容	健診(検診)等データ管理システム等の問合せ対応、バージョンアップ対応、障害対応等の保守業務	健診(検診)等データ管理システム等の問合せ対応、バージョンアップ対応、障害対応等の保守業務、共通基盤システムの運用保守業務	事前	委託事項2の記載内容を委託事項1へ統合したため
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1　健診（検診）等データ管理システム運営業務 ③委託先における取扱者数	10人未満	50人以上100人未満	事前	従事人数の変更による修正
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1　健診（検診）等データ管理システム運営業務 ④委託先への特定個人情報ファイルの提供方法	その他 ・運用管理、障害対応作業における、当システム端末機からの閲覧及び必要に応じた修正を行う。委託先はデータの取り出し、庁舎外への持ち出しを行わない。	専用線 地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、IP-VPN等の閉域網の利用も可能。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1　健診（検診）等データ管理システム運営業務 ⑥委託先名	日本コンピューター株式会社	・日本コンピューター株式会社 ・日本電気株式会社	事前	委託事項2の記載内容を委託事項1へ統合したため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項1　健診（検診）等データ管理システム運営業務 ⑦再委託の有無 ⑧再委託の許諾方法 ⑨再委託事項	⑦再委託しない	⑦再委託する ⑧再委託するかしないかについては、委託契約によるが、再委託の必要がある場合は、事前に委託先と書面による協議を行い、再委託の必要性や業務内容、再委託先のセキュリティ管理体制を確認した上で許諾する。 ⑨システム保守の一部	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項2　共通基盤システムの運用保守業務①～⑨	共通基盤システムの運用保守業務	委託事項2に関する記載は全て削除	事前	委託事項2の記載内容を委託事項1へ統合したため
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項2	記載なし	ガバメントクラウドへのデータ移行作業	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項2 ①委託内容	記載なし	ガバメントクラウドへのデータ移行作業	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項2 ②取扱いを委託する特定個人情報ファイルの範囲	記載なし	特定個人情報ファイルの全体	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 ４．特定個人情報ファイルの取扱いの委託 委託事項2 ②取扱いを委託する特定個人情報ファイルの範囲 ・対象となる本人の数 ・対象となる本人の範囲 ・その妥当性	記載なし	10万人以上100万人未満 ・健康増進法等関連法令に定められる健診（検診）対象者 ・既存システムからデータ移行するために、特定個人情報ファイル全体を委託の対象にする必要がある。	事前	ガバメントクラウドへの移行に伴う記載の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ③委託先における取扱者数	記載なし	10人以上50人未満	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ④委託先への特定個人情報ファイルの提供方法	記載なし	専用線 その他（地方公共団体における情報セキュリティポリシーに関するガイドラインに基づき、IP-VPN等の閉域網の利用も可能。）	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑤委託先名の確認方法	記載なし	下記、「⑥委託者名」の項の記載により確認できる。また、「Ⅴ. 開示請求、問合せ　1. ①請求先」への当区の情報公開請求による開示請求を行うことでも確認可能。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑥委託先名	記載なし	・日本コンピューター株式会社 ・日本電気株式会社	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑦再委託の有無 ⑧再委託の許諾方法 ⑨再委託事項	記載なし	⑦再委託する ⑧再委託するかしないかについては、委託契約によるが、再委託の必要がある場合は、事前に委託先と書面による協議を行い、再委託の必要性や業務内容、再委託先のセキュリティ管理体制を確認した上で許諾する。 ⑨ガバメントクラウドへのデータ移行作業の一部	事前	ガバメントクラウドへの移行に伴う記載の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	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 ①保管場所	ガバメントクラウドに関する記載なし	＜ガバメントクラウドにおける措置①＞ 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の規格に基づく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。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	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 ③消去方法	ガバメントクラウドに関する記載なし	＜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杉並区からの操作によって実施される。杉並区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等の規格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、杉並区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。	事前	ガバメントクラウドへの移行に伴う記載の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	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 ４．特定個人情報ファイルの取扱いの委託 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	ガバメントクラウドへの移行に伴うリスク対策に関する記載なし	・リモート保守を実施する場合やデータ移行作業をする場合は専用区画で実施することとし、入退室の記録を残している。 ・保守等に用いる端末へのログインには多要素認証を用いることとし、許可された者以外の作業を禁止している。 ・業務データを取り扱う端末のインターネットへの接続を禁止している。 ・次のような場合を除き、区はガバメントクラウドから保守事業者の環境へのデータの持ち出しを許可していない。 ①ガバメントクラウドへのサイバー攻撃等により、ガバメントクラウド上からデータを退避する必要が生じた場合 ②ガバメントクラウド上のシステムで障害が発生し、クラウド環境では原因が特定できない場合 ③業務データを保管するために利用しているクラウド事業者を変更する場合 ④このほか、ガバメントクラウドからデータを持ち出すことに緊急または相当の必要性があると区が認める場合 ・保守事業者は、ガバメントクラウドからのデータの持ち出しを行った場合、保守事業者の環境に持ち出したデータを保管する必要がなくなった段階で、速やかに返還又は廃棄し、区に報告することとしている。 ・業務データの保守環境からの持ち出しは許可していない。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	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 ４．特定個人情報ファイルの取扱いの委託 その他の措置の内容	・システム運用を行う専用の室では、「コンピュータ室管理基準」で携帯電話、カメラ等の使用を制限している。	・委託事業者の業務実施場所において、携帯電話やカメラ等の通信機器や録画機器の使用を、契約で制限している。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	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．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 ⑤物理的対策　具体的な対策の内容	ガバメントクラウドに関する記載なし	＜ガバメントクラウドにおける措置①＞ 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クラウド事業者は、その従業員に対して、適正な許可のない装置等の外部への持出は認めていない。また、クラウド事業者は、区のデータにアクセスできない措置を講じている。	事前	ガバメントクラウドへの移行に伴う記載の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	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. 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 ⑤物理的対策　具体的な対策の内容	・データセンターに構築し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。	＜ガバメントクラウドにおける措置②＞ ガバメントクラウド内の特定個人情報を記録するサーバについては、次の対策を行っている。 ・サーバ設置エリアへの入退室管理 ・監視カメラ及び侵入検知防止システムによる常時監視 ・事前申請による入館管理 ・入館時における二要素認証の実施及び入退室状況の監査	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	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. 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 ⑥技術的対策　具体的な対策の内容	ガバメントクラウドに関する記載なし	＜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杉並区が委託したアプリケーション開発事業者等は、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杉並区が委託したアプリケーション開発事業者等は、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の環境は、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杉並区やアプリケーション開発事業者等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杉並区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。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	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. 特定個人情報の保管・消去 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　手順の内容	ガバメントクラウドに関する記載なし	＜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等の規格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。	事前	ガバメントクラウドへの移行に伴う記載の変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月1日	Ⅳ　その他のリスク対策 1．監査 ②監査	ガバメントクラウドに関する記載なし	＜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。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和6年11月1日	Ⅳ　その他のリスク対策 3．その他のリスク対策	ガバメントクラウドに関する記載なし	＜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杉並区及びその業務データの取扱いについて委託を受けるアプリケーション開発事業者等が責任を有する。 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、杉並区に業務アプリケーションサービスを提供するアプリケーション開発事業者等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、杉並区とデジタル庁及び関係者で協議を行う。	事前	ガバメントクラウドへの移行に伴う記載の変更
令和7年2月14日	Ⅰ　基本情報 5．個人番号の利用 法令上の根拠	・番号法 第9条第1項　別表第1の76の項	・番号法 第9条第1項　別表の111の項	事後	番号法改正
令和7年2月14日	Ⅰ　基本情報 6　情報提供ネットワークシステムによる情報連携　法令上の根拠	・番号法第19条第8号及び別表第2 （別表第2における情報提供の根拠） 102の2の項 （別表第2における情報照会の根拠） 102の2の項	・番号法第19条第8号及び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 （命令における情報提供の根拠） 139の項 （命令における情報照会の根拠） 139の項	事後	番号法改正
令和7年2月14日	Ⅱファイルの概要 5．特定個人情報ファイルの提供・移転 提供先1　①法令上の根拠	番号法第19条第8号及び別表第2の102の2	番号法第19条第8号及び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表の第139の項	事後	番号法改正

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年7月9日	Ⅱ　ファイルの概要 6．特定個人情報の保管・消去 ①保管場所	＜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。	＜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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	Ⅱ　ファイルの概要 6．特定個人情報の保管・消去 ③消去方	＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は、当区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。 ・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。	＜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事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制 度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。 さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事前	自治体中間サーバー・プラットフォーム更改のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年7月9日	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 6. 情報提供ネットワークシステムとの接続 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	＜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・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。	＜中間サーバー・プラットフォームにおける措置＞ ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	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 6. 情報提供ネットワークシステムとの接続 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	＜中間サーバー・プラットフォームにおける措置＞ ③中間サーバ・プラットフォームの保守・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。	③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、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。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	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 6. 情報提供ネットワークシステムとの接続 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	＜中間サーバー・プラットフォームにおける措置＞ ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	＜中間サーバー・プラットフォームにおける措置＞ ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	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. 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 ⑤物理的対策 具体的な対策の内容	＜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。	＜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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。	事前	自治体中間サーバー・プラットフォーム更改のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年7月9日	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．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 ⑥技術的対策 具体的な対策の内容	中間サーバー･プラットフォームにおける措置を追加	＜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。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥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。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	Ⅳ　その他のリスク対策 1．監査 ②監査 具体的な内容	＜中間サーバ・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・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。	＜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。 ②政府情報システムのためのセキュリティ評価制度（ISMAP）に登録された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。	事前	自治体中間サーバー・プラットフォーム更改のため
令和7年7月9日	Ⅳ　その他のリスク対策 3．その他のリスク対策	＜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。	＜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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者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。	事前	自治体中間サーバー・プラットフォーム更改のため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年3月10日	Ⅲリスク対策（プロセス） 7．特定個人情報の保管・消去 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	発生あり	発生なし	事後	3年以上経過のため
令和8年3月10日	その内容	令和4年11月5日、区職員が住民基本台帳ネットを不正に検索して得た個人情報を漏えいしたとして、住民基本台帳法違反容疑により逮捕される事案が発生した。 ※本事案は、当該職員が区民生活部区民課に在籍していた令和3年度に発生した。	削除	事後	3年以上経過のため
令和8年3月10日	再発防止策	「杉並区職員の逮捕に伴う再発防止対策検討委員会報告書」に基づき、再発防止対策を実施する。 再発防止策は以下（1）～（3）のとおりである。 （1）操作ログ点検の充実・強化 ・氏名等による検索は、事前に検索内容を記録票へ記入して、他の職員の確認を受けた上で行う。 ・操作ログの点検は各課で毎月実施することとし、その操作ログと記録票を突合する。 （2）職員に対する教育・研修の充実・強化 ・初任者研修等に加え、新たに毎年、全職員に対して職場ごとに公務員倫理・情報セキュリティの研修を実施する。 ・住基ネット操作権限を持つ職員に対しては、権限付与時の教育・研修に加え、新たに毎年、動画視聴方式等による教育・研修を実施する。 ・区民課の住基ネット業務管理補助者に対する教育・研修（区民課住基ネット業務管理補助者研修）については、初任時に加え、新たに毎年、教育・研修を実施する。 ・住基ネットに関する職員自己点検の内容について、設問を見直す。 （3）職場環境の見直し ・各職場において、セキュリティ対策について、話し合いを行い、必要に応じて、住基ネット端末の設置場所などのレイアウト変更を行う等、職場環境の必要な見直し・改善を図り、より一層風通しのよい職場づくりを進め、職場全体で不正行為を防止する。 ・情報の持出しを防ぐために、区民課の住基ネット端末設置エリアへの電子機器持込みは原則禁止とする。 ・住基ネット端末設置エリアには、このことを張り紙等で明示する。	削除	事後	3年以上経過のため