

諮問第1011号

特定個人情報保護評価における第三者点検について
(国民健康保険事務)

令和8年8月7日
地域行政部マイナンバー担当課
保健福祉政策部国保・年金課

1 諮問の趣旨

(1) 特定個人情報保護評価について

特定個人情報保護評価は、「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。)に基づく番号制度の枠組みの下での制度上の保護措置の一つであり、特定個人情報ファイルを保有しようとする又は保有する場合は、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分析し、そのようなリスクを軽減するための措置を講ずること、さらにこのような措置が個人のプライバシー等の権利利益の保護措置として十分であると認められることを宣言するものである。

具体的には、行政機関の長等が評価の実施主体となり、評価対象が特定個人情報を取り扱う事務ごとに定められている。また、特定個人情報の対象人数等のしきい値によって、特定個人情報保護評価の種類が基礎項目評価・重点項目評価・全項目評価の三類型に区分され、併せて区民意見募集や第三者点検、国民への公表などの実施手続が定められている。

なお、「国民健康保険事務」は、しきい値判断の結果、対象者が10万人以上30万人未満かつ特定個人情報ファイルの取扱者が500人以上となることから、全項目評価の実施が義務付けられることとなる。

(2) 諮問の理由

番号法第28条の規定において、行政機関の長等は特定個人情報ファイルを保有しようとするとき又は重要な変更を加えようとするときは、特定個人情報保護評価を実施することとされている。

この度、「国民健康保険事務」に係る特定個人情報ファイルについて、重要な変更を加える必要が生じたため、「特定個人情報保護評価に関する規則」(以下「規則」という。)第7条第4項に基づく「特定個人情報保護評価書」(以下「評価書」という。)の第三者点検について、「世田谷区情報公開・個人情報保護審議会条例」第2条第1項第2号の規定により諮問するものである。

※審議資料No. 1-2「特定個人情報評価書作成の判断基準」及び審議資料No. 1-3「番号法における特定個人情報保護評価「全項目評価」の流れ」参照

2 諮問の内容

(1) ガバメントクラウドの利用について

審議資料No. 1-4～No. 1-6のとおり。

(2) 国民健康保険事務における評価書の変更の内容

特定個人情報ファイルを取り扱う現行システム(SKY2国民健康保険システム)のガバメントクラウドへの移行に伴い、評価書(全項目評価書)の記載項目のうち、「特定個人情報ファイルの取扱いの委託の有無」、「特定個人情報の保管場所」、「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」及び「その他のリスク対策」に変更が生じる。これは、規則第11条に規定される重要な変更該当するため、特定個人情報保護評価を再実施する。

3 区民意見募集

規則第7条第1項に基づき区民意見募集を実施した。結果は以下のとおり。

(1) 対象事務及び概要

国民健康保険事務について全項目評価書の改定案を作成し、区民意見募集を実施

(2) 期間

令和8年6月1日～同月30日の30日間実施

(3) 結果

期間中に区民意見が以下1件あった。

ご意見	区の考え方
「特定個人情報ファイルの取り扱いに重要な変更を加える」とは具体的に何を指すのか。	本件は、国民健康保険事務において、ガバメントクラウドの利用により、個人情報の保管場所や取扱い方法が変更されるため、その影響を踏まえて改めて評価を実施するものです。 変更点の詳細は、「国民健康保険事務に関する全項目評価書案」の「(別添3)変更箇所」にてご確認ください。

4 区のマイナンバー制度セキュリティ会議

本件について、令和8年7月29日開催の令和8年度第1回マイナンバー制度セキュリティ会議にて審議し、了承された。

5 第三者点検の対象

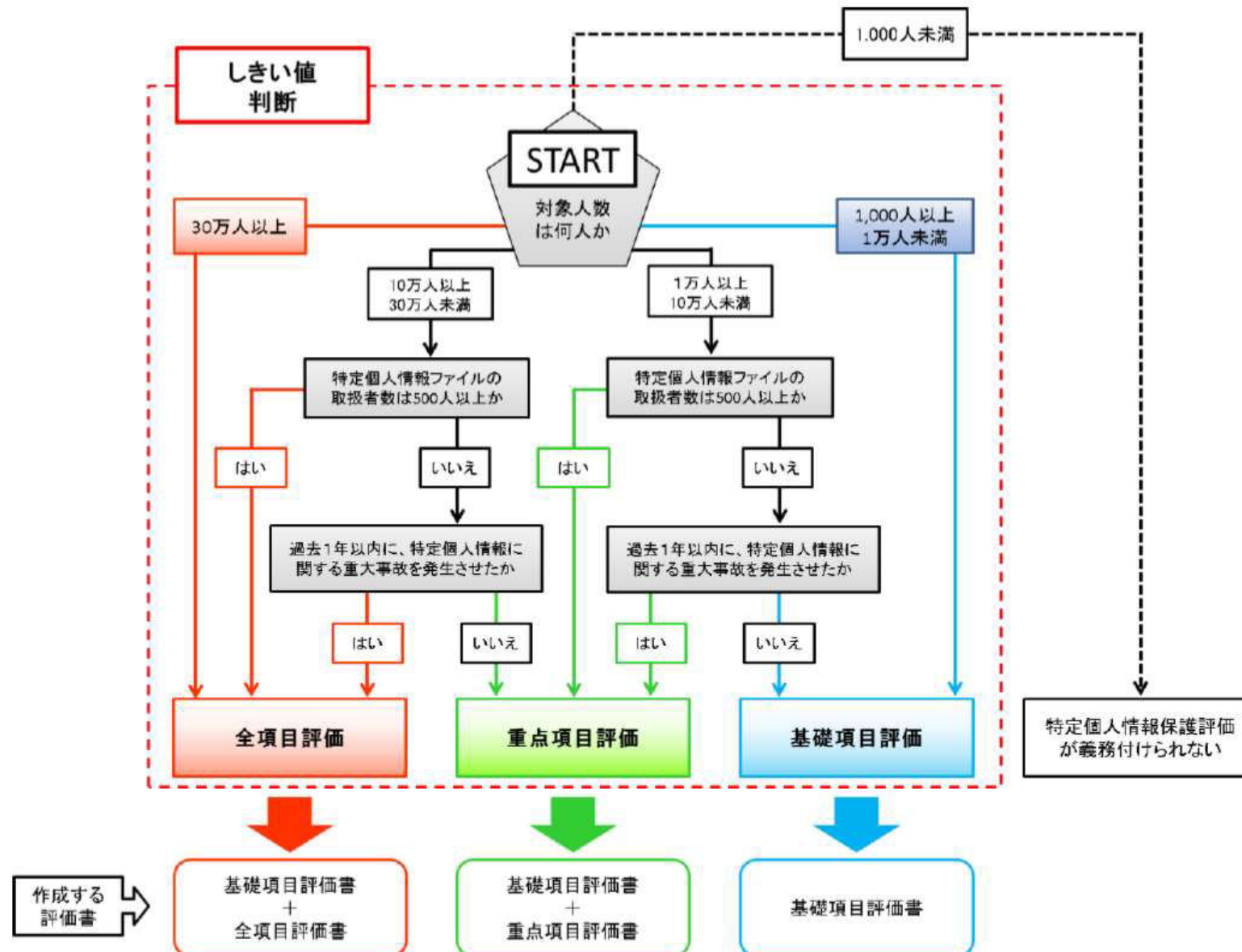
審議資料No. 1－7「特定個人情報保護評価書（全項目評価書）」のとおり。

※改定前の評価書との相違点及び審査の観点については、審議資料No. 1－8のとおり。

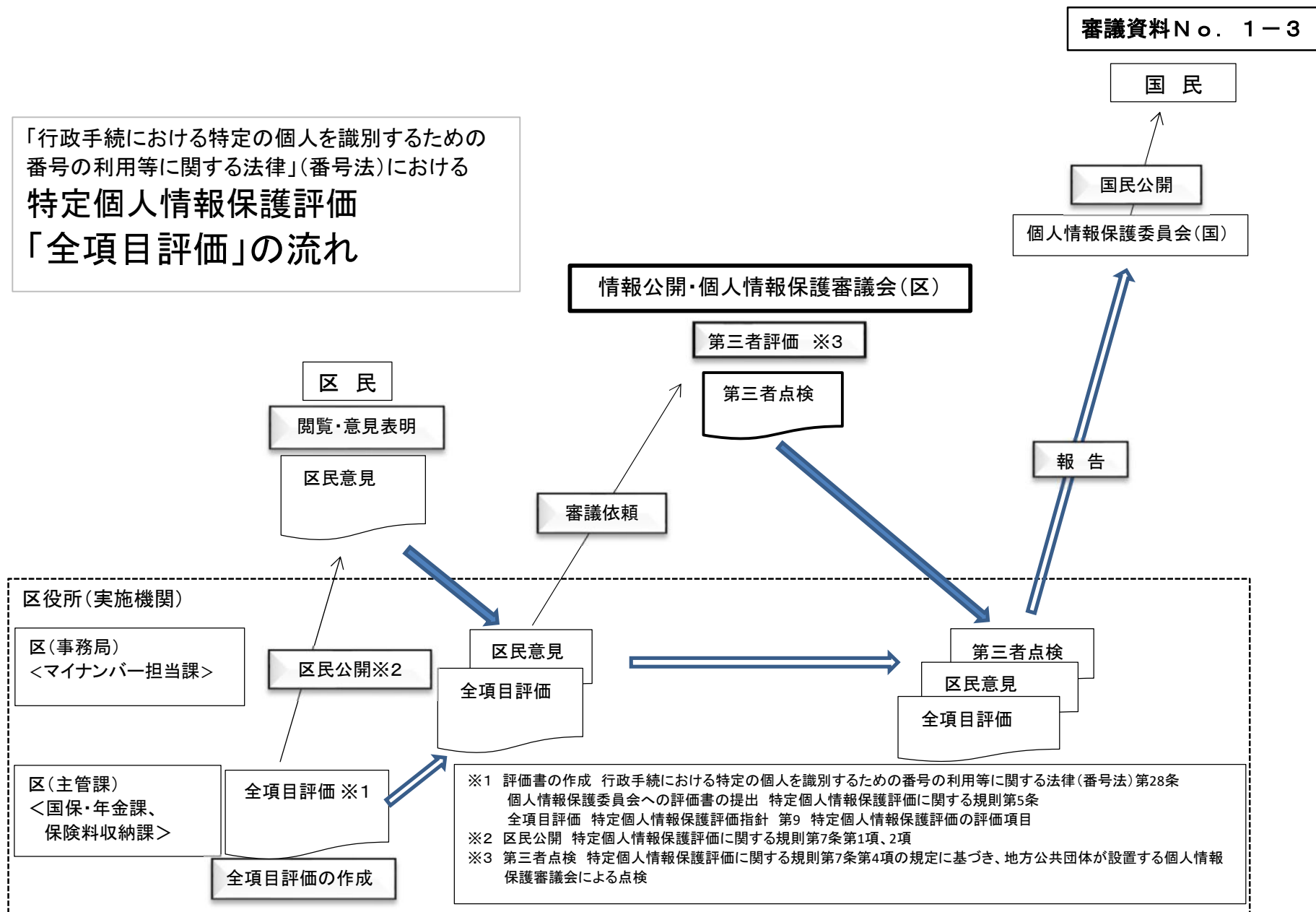
6 今後のスケジュール（予定）

令和8年12月 国の個人情報保護委員会へ評価書の提出
評価書の公表

特定個人情報評価書作成の判断基準



「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」(番号法)における
特定個人情報保護評価
「全項目評価」の流れ



ガバメントクラウド利用に伴う特定個人情報保護評価の再実施について

1 データセンターサービスの終了に伴うガバメントクラウドへの移行

「国民健康保険事務」及び「国民健康保険 保険料収納事務」に係る特定個人情報ファイルを取り扱う現行システム（以下「SKY2 国民健康保険システム」という。）は、当該システムを開発し、運用・保守業務を受託しているシステムベンダが提供するデータセンターサービス上で稼働している。当該データセンターサービスについては、令和9年3月をもってサービスの提供が終了する予定となっており、同時期以降の継続利用は困難である。

一方、当該システムベンダは、自社で開発及び運用しているシステムについて、その基盤となるシステムリソースをガバメントクラウド上に集約しているため、SKY2 国民健康保険システムについても、ガバメントクラウドへ移行することにより、既に区の他業務システムで利用しているインフラ運用保守等の共通的なサービスの利用が可能となる。また、ガバメントクラウドは、政府が定める情報セキュリティ基準に基づき整備・運用されており、セキュリティ対策や運用面において、他の利用環境と比較して一定の優位性を有している。このため、特定個人情報を取り扱うシステムの基盤として、適切な環境であると認められる。さらに、区においては、既にガバメントクラウド利用を前提としたネットワーク環境の整備を完了しており、新たな基盤整備に係る負担は限定的である。

以上の状況を踏まえ、SKY2 国民健康保険システムについては、現行のデータセンター環境からガバメントクラウドへ移行することとし、令和9年1月に移行を実施する方針とする。

※ガバメントクラウドについて

デジタル社会形成基本法（令和3年法律第35号）第29条の規定に基づき、デジタル庁が調達するものであって、地方公共団体が業務システム等を効率的に利用できるよう提供されるクラウドサービス等である。

詳細は、審議資料No. 1-5に記載のとおり。

2 評価書の改定

評価書の改定内容のうち、ガバメントクラウドのクラウド事業者が提供するクラウド上の基盤及び接続に関する部分については、令和4年10月にデジタル庁より提供された「ガバメントクラウドにおける特定個人情報保護評価について」（審議資料No. 1-6）における全項目評価書の記載例を基に作成した。

この他、事務個別に変更が生じる箇所については、評価書ごとに修正を実施した。

3 ガバメントクラウドにおけるリスク対応策の概要

システムの移行先となるガバメントクラウドについては、デジタル庁が政府情報システムのためのセキュリティ評価制度（ISMAP）のリストに登録されたクラウドサービスから調達して、区に対して個別領域の利用権を付与し、運用管理を委託する。

「国民健康保険事務」及び「国民健康保険 保険料収納事務」においては、ガバメントクラウド共同利用方式により、区は、システムのアプリケーション等を提供するASPとの間で、「アプリケーション等提供・保守契約」及び「ガバメントクラウド運用管理補助委託契約」を締結する。

特定個人情報を保有するシステムを構築するガバメントクラウドの環境は、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され、区やASP・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も、閉域ネットワークで構成し、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。

その他、継続的なモニタリング・ログ管理や脅威検出・DDoS 対策の常時実施、ウイルス対策パターンファイルの更新、OS・ミドルウェアへのセキュリティパッチ適用などの技術的対策のほか、物理的対策として、クラウド事業者のシステムのサーバー等の構築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うなど、これまでと同等のセキュリティ対策を実施する。

ガバメントクラウドに関する要件

- デジタル庁が、「政府情報システムのためのセキュリティ評価制度」(ISMAP)のリストに登録されたクラウドサービスから、要件を満たすクラウドサービスを調達。
- 地方公共団体が活用するクラウド環境については、「データを団体ごとに論理的に分離するとともに、厳格なアクセス制御を行う等、高い機密性を確保」「他システムとの接続は専用線により行う」など、セキュリティ対策を適切に講じる。

【主な要件】

- ①不正アクセス防止やデータ暗号化などにおいて、最新かつ最高レベルの情報セキュリティが確保できること。
- ②クラウド事業者間でシステム移設を可能とするための技術仕様等が公開され、客観的に評価可能であること。
- ③システム開発フェーズから、運用、廃棄に至るまでシステムライフサイクルを通じた費用が低廉であること。
- ④契約から開発、運用、廃棄に至るまで国によって統制ができること。
- ⑤データセンタの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外へ持出を行わないこと。
- ⑥一切の紛争は、日本の裁判所が管轄するとともに、契約の解釈が日本法に基づくものであること。

出典:「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)

ガバメントクラウド対象クラウドサービス一覧

クラウドサービス名

Amazon Web Services

Google Cloud

Microsoft Azure

Oracle Cloud Infrastructure

さくらのクラウド

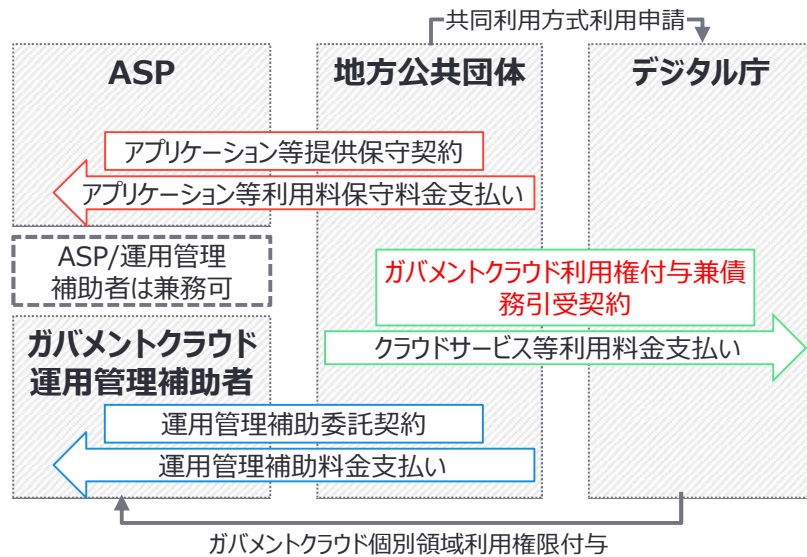
出典:ガバメントクラウド整備のためのクラウドサービスの提供
ー令和8年度募集ーにおける審査結果
(令和8年3月27日・デジタル庁)

共同利用方式(アカウント分離)による利用

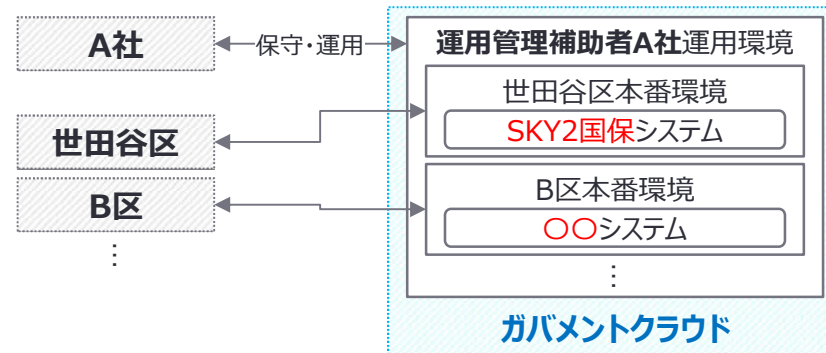
- 各業務システムのガバメントクラウド利用方式は、「世田谷区標準化事業_全体計画書_2.0版」にて、原則国の推奨する「共同利用方式」(受託者が複数自治体の運用管理補助を行う方式)を利用する方針としている。
- 団体間のシステム分離方法は「アカウント分離」を採用し、他団体の環境の影響を受けにくい構成とした。

共同利用方式

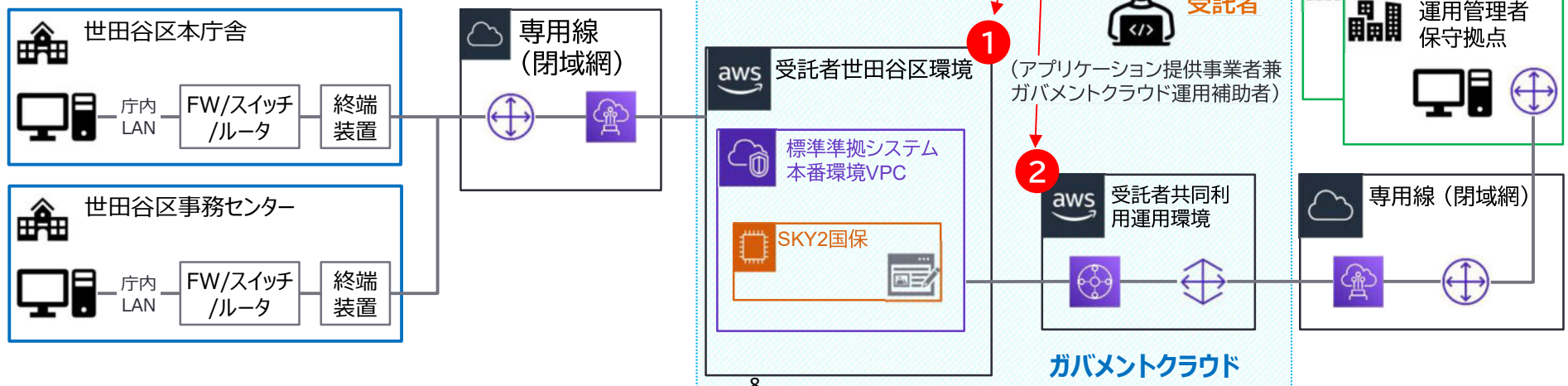
契約関係



利用方式



利用イメージ (評価対象システム全体)



ガバメントクラウドにおける特定個人情報保護評価について

令和4年10月 デジタル庁

1. 「重要な変更」について

行政機関の長等は、特定個人情報ファイルを保有しようとする場合には、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（平成二十五年法律第二十七号）（以下「番号法」という。）第二十八条の規定に基づき、特定個人情報保護評価を実施する必要があります。

(1) 「重要な変更」の該当性の判断

貴市町村においては、既存のシステムについてはすでに同条に基づき特定個人情報ファイルを取り扱う事務ごとに特定個人情報保護評価を実施されているところであると認識しております。

他方、同条後段において、特定個人情報ファイルを取り扱う事務について、重要な変更が発生する場合には、重要な変更を加える前に特定個人情報保護評価を再実施することとされています。

「重要な変更」とは、特定個人情報保護評価に関する規則（平成二十六年特定個人情報保護委員会規則第一号）（以下「規則」という。）第十一条に基づき、特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号）（以下「指針」という。）第6の2（2）において、当該指針の別表に定める重点項目評価書及び全項目評価書の以下の項目が変更されることをいうものとされています。

基礎項目評価書については、「重要な変更」が規定されていないため、評価の再実施は不要です。

なお、上記に関わらず、重点項目事項評価書・全項目評価書に重要な変更に当たらない変更が生じる場合又は基礎項目評価書にしきい値判断の結果の変更に該当しない変更が生じた場合には、規則第十四条及び指針第7の規定に基づいて、必要な修正を行う必要がありますので、そのような変更が生じないかについて検討・確認をお願いします。

【参考】特定個人情報保護評価指針 別表

別表（第6の2（2）関係）	
特定個人情報保護評価書の名称	重要な変更の対象である記載項目
1 重点項目評価書	1 個人番号の利用 2 情報提供ネットワークシステムによる情報連携 3 特定個人情報ファイルの種類 4 特定個人情報ファイルの対象となる本人の範囲 5 特定個人情報ファイルに記録される主な項目 6 特定個人情報の入手元 7 特定個人情報の使用目的 8 特定個人情報ファイルの取扱いの委託の有無 9 特定個人情報ファイルの取扱いの再委託の有無 10 特定個人情報の保管場所 11 リスク対策（重大事故の発生を除く。）
2 全項目評価書	1 特定個人情報ファイルを取り扱う事務の内容 2 個人番号の利用 3 情報提供ネットワークシステムによる情報連携 4 特定個人情報ファイルの種類 5 特定個人情報ファイルの対象となる本人の範囲 6 特定個人情報ファイルに記録される主な項目 7 特定個人情報の入手元 8 特定個人情報の使用目的 9 特定個人情報の使用部署 10 特定個人情報の使用方法 11 特定個人情報の突合 12 特定個人情報の統計分析 13 特定個人情報の使用による個人の権利利益に影響を与え得る決定 14 特定個人情報ファイルの取扱いの委託の有無 15 取扱いを委託する特定個人情報ファイルの対象となる本人の範囲 16 特定個人情報ファイルの取扱いの再委託の有無 17 特定個人情報の保管場所 18 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（重大事故の発生を除く。） 19 その他のリスク対策

(2) 特定個人情報保護評価の再実施の時期

「重要な変更」に該当する場合には、特定個人情報保護評価の再実施の時期については、ガバメントクラウド上に副本データを移行するまでに評価を実施する必要があります。

2. 記載例について

指針第3の2においては、「特定個人情報ファイルを保有しようとする者又は保有する者以外に特定個人情報ファイルに関わる者が存在する場合は、その者は、特定個人情報保護評価が適切に実施されるよう協力するものとする。」とされております。

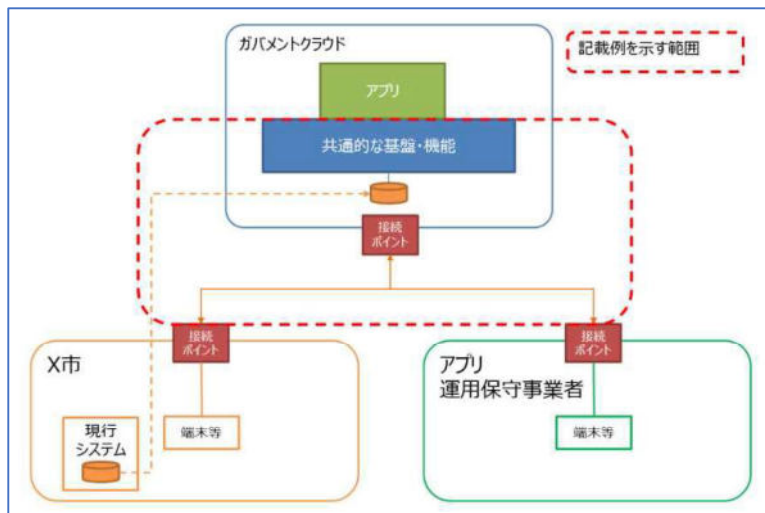
今般、ガバメントクラウドはデジタル庁が調達したことから、次の(1)及び(2)の考えに基づいて記載例を策定し、別紙のとおり提供するものです。

各市町村におかれては、番号法をはじめとする個人情報保護に関する法令の趣旨を踏まえ、記載例を含む今回の情報提供を参考に適切に評価を実施してください。

なお、内容については、令和4年8月30日時点の情報に基づき、個人情報保護委員会事務局と調整済みのものです。

(1) 記載例の射程

今回提供する記載例については、評価書に記載する内容のうち、ガバメントクラウドのクラウド事業者が提供するクラウド上の基盤及び接続に関する部分になります。



記載例を示していない箇所であっても、特定個人情報保護評価の趣旨に鑑み、上記の射程以外に関する部分について、別途記載が必要となりますので、ご留意下さい。

具体的には、委託に関する項目について、ガバメントクラウドへ移行する際のデータ抽出、移行、破棄においては委託先が特定個人情報を扱うことが想定されますので、各団体において追記する必要があります。

(2) 記載例において「重要な変更」に該当する項目

ガバメントクラウド上にシステムを構築するにあたり、上記 2 (1) の範囲において、変更が想定されるのは、次に掲げる項目です。

記載例においては、これらの項目において必要な情報を記載しています。

<重点項目評価書>

- 10 特定個人情報の保管場所
- 11 リスク対策

<全項目評価書>

- 17 特定個人情報の保管場所
- 18 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
- 19 その他のリスク対策

なお、デジタル庁及びクラウドサービス事業者は特定個人情報にはアクセスしないため、クラウドサービス事業者は番号法上の「委託」先には当たらないと解されますので、委託に関する別表の以下の項目に関しては変更を想定しておりません。

<重点項目評価書>

- 8 特定個人情報ファイルの取扱いの委託の有無
- 9 特定個人情報ファイルの取扱いの再委託の有無

<全項目評価書>

- 14 特定個人情報ファイルの取扱いの委託の有無
- 15 取扱いを委託する特定個人情報保護ファイルの対象となる本人の範囲
- 16 特定個人情報ファイルの取扱いの再委託の有無

以上

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
17	国民健康保険事務 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

世田谷区は、国民健康保険事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために十分な措置を行い、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

国民健康保険事務では、事務の一部を外部業者に委託しているが、委託先による不正入手、不正な使用等への対策として、特に業者選定の際に業者の情報保護管理体制を契約条件として設定している。

評価実施機関名

東京都世田谷区長

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5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	国民健康保険 資格認定及び保険料賦課並びに保険給付事務
②事務の内容 ※	国民健康保険法に基づき以下の事務を行う。 ①社会保険離脱や転出入、または、出生死亡等様々な資格異動に伴う被保険者資格の取得喪失の認定 ②所得を元に軽減等の要件を適用した上での保険料計算及び賦課 ③医療機関等からのレセプトの審査および医療機関等への保険者負担分の支払い業務 ④出産育児一時金および葬祭費の支給ならびに第三者行為による損害賠償金の請求 ⑤国民健康保険加入者を対象とした特定健康診査及びその結果に基づく指導 ⑥国民健康保険制度の趣旨普及 ⑦サービス検索・電子申請機能での受領 ⑧オンライン資格確認等システムに係る資格履歴管理事務 ⑨オンライン資格確認等システムに係る機関別符号の取得等事務 ※詳細は別添1「事務内容」を参照 ※以下、①～⑦の事務を「被保険者資格管理等に係る事務」、⑧・⑨の事務を「オンライン資格確認等システムに係る事務」という。 ※オンライン資格確認等システム…「医療保険制度の適正かつ効率的な運営を図るための健康保険法等の一部を改正する法律」によりオンライン資格確認のしくみの導入を行うこととされたことと、当該しくみのような、他の医療保険者等と共同して「被保険者等に係る情報の収集または整理に関する事務」及び「被保険者等に係る情報の利用または提供に関する事務」を国民健康保険団体連合会（以下「国保連合会」という。）または社会保険診療報酬支払基金（以下「支払基金」という。）に委託することができる旨の規定が国民健康保険法に盛り込まれていることを踏まえ、オンライン資格確認等システムへの資格情報の提供に係る加入者等の資格履歴情報の管理、機関別符号の取得、及び一部の情報提供について共同して支払基金等に委託することとし、国保連合会から再委託を受けた国民健康保険中央会（以下「国保中央会」という。）及び支払基金（以下「取りまとめ機関」という。）が、医療保険者等向け中間サーバー等の運営を共同して行う。
③対象人数	＜選択肢＞ [10万人以上30万人未満] 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	SKY2国民健康保険システム	
②システムの機能	①資格得喪に関わる情報を記録する機能 ②資格確認書等・医療証等の発行、発行履歴を記録する機能 ③保険料の賦課計算を行う機能及び賦課情報を記録する機能 ④給付情報の記録または高額療養費支給ならびに出産葬祭費支給を行う機能 ⑤各情報を照会に応じて表示する機能	
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 [] 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 (	[○] 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	番号連携サーバー
②システムの機能	1. 宛名管理機能 ①サーバ内の宛名データベースのセットアップ ②宛名の異動データを取り込み、宛名データベースへ反映 ③個人番号にて同一人判定を行い、団体内統合宛名番号を採番し管理 ④宛名データベースの検索、参照、更新 ⑤オンラインで入力したデータを業務システムに連携 ⑥団体内統合宛名番号を業務システムに連携 2. 情報提供機能 ①中間サーバに連携する各業務情報をデータベースへセットアップ ②各業務の異動データを取り込み、データベースに反映 ③各業務情報の参照、入力、変更、削除を行う。 ④各業務情報を一括で中間サーバに連携 ⑤各業務の異動情報を中間サーバに連携 3. 情報照会機能（他機関への情報照会） ①各業務の宛名番号で対象者を検索し、他自治体への情報提供を依頼し、オンラインにて表示する。 ②情報照会の対象者情報を元に、中間サーバに情報を要求し、一括ファイルを作成する。 4. 符号要求 ①処理通番を要求・受信し、符号要求データを既存住基または住基GWに送信する。
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 [○] 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3	
①システムの名称	中間サーバー
②システムの機能	中間サーバーは、情報提供システムネットワークシステム（インターフェイスシステム）、番号連携サーバーとのデータ受け渡しを行うことで、符号の取得（※1）や各情報保有機関で保有する特定個人情報の照会と提供等の業務を実現する。 1. 符号管理機能：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」と、情報照会、情報提供に用いる個人の識別子である「符号」とを紐付け、その情報を保管・管理する機能。 2. 情報照会機能：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）の情報照会及び情報提供受領（照会した情報の受領）を行う機能。 3. 情報提供機能：情報提供ネットワークを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う機能。 4. 既存システム接続機能：中間サーバーと既存システム、番号連携サーバー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ための機能。 5. 情報提供等記録管理機能：特定個人情報（連携対象）の照会、または提供があった旨の情報提供等記録を生成し、管理する機能。 6. 情報提供データベース管理機能：特定個人情報（連携対象）を副本として、保持・管理する機能。 7. データ送受信機能：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）との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 8. セキュリティ管理機能：セキュリティを管理する機能。 9. 職員認証・権限管理機能：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（連携対象）へのアクセス制御を行う機能。 10. システム管理機能：バッチの状況管理、業務統計情報の集計、稼働状況の通知、保管期限切れ情報の削除を行う機能。 （※1）セキュリティの観点により、特定個人情報の照会と提供の際は、「個人番号」を直接利用せず「符号」を取得して利用する。

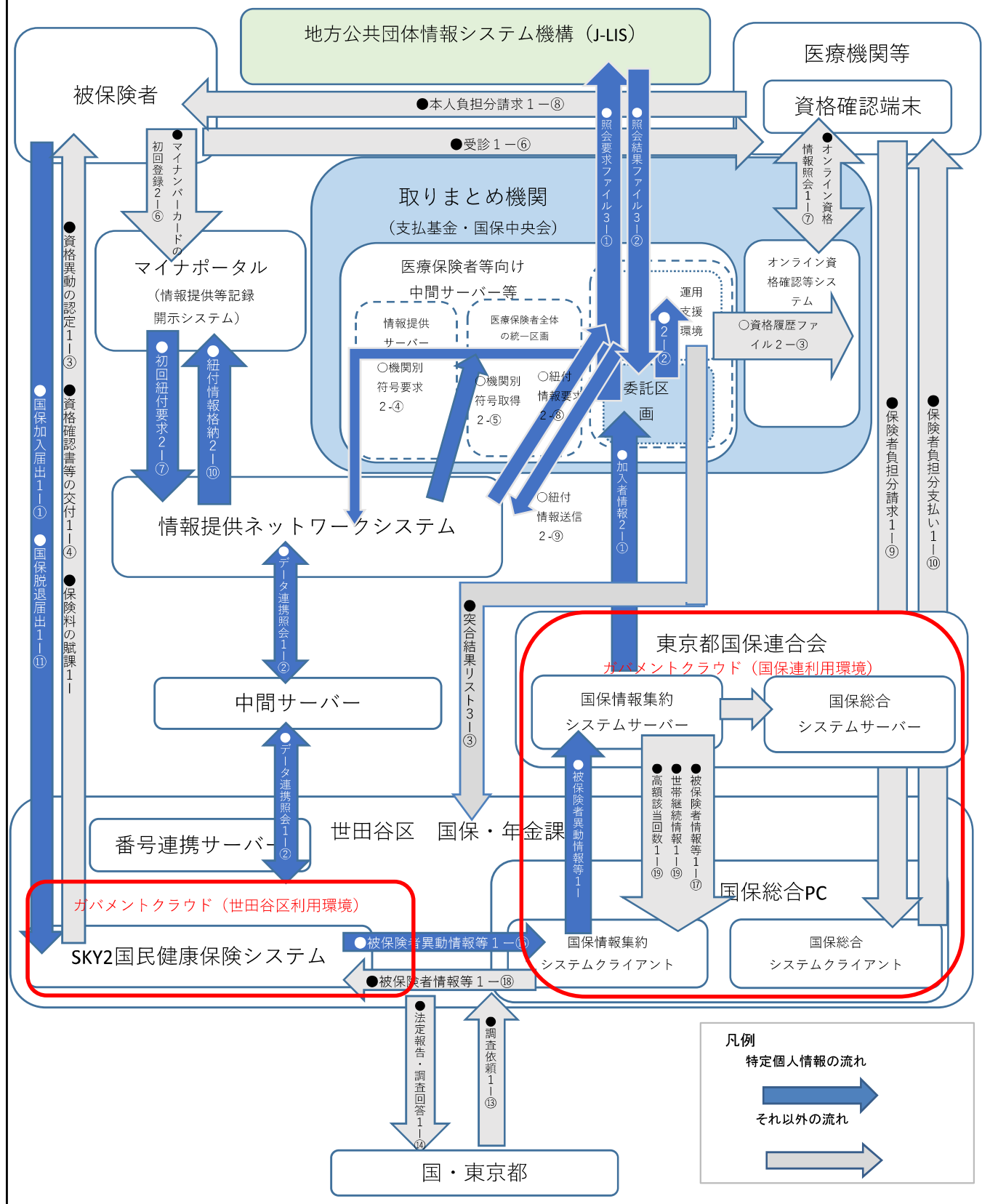
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 市内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他 ()
システム4	
①システムの名称	国保総合システムおよび国保情報集約システム(以下「国保総合(国保集約)システム(*)」という。) * 国保総合(国保集約)システムは、国保連合会に設置される国保総合(国保集約)システムサーバ群と、市区町村に設置される国保総合PCで構成される。
②システムの機能	1. 資格継続業務(詳細は別添1を参照) (1)被保険者異動情報(資格情報(世帯)ファイル、資格情報(個人)ファイル)の送信 市区町村の国保総合PCのファイル転送機能(*)を用いて、被保険者資格異動に関するデータを市区町村から国保連合会へ送信する。 (2)被保険者異動情報の受信(国保資格取得喪失年月日連携ファイル、市区町村被保険者ID連携ファイル) 都道府県内の市区町村間を転居した場合、転出市区町村と転入市区町村の適用終了日(転出)と適用開始日(転入)の重複・空白期間をチェックする。 また、資格取得年月日や資格喪失年月日の引き継ぎを行い、該当市区町村の国保総合PCへ被保険者異動情報を配信する。 2. 高額該当回数の引き継ぎ業務(詳細は別添1を参照) (1)継続候補世帯の抽出(継続候補世帯リスト) 市区町村の国保総合PCのオンライン処理機能を用いて、世帯継続性の容認に関するデータを転入地市区町村から国保連合会へ送信する。 (2)継続世帯の確定(継続世帯確定リスト) 転入地市区町村が世帯継続性を認めた場合には、転出地市区町村から転入地市区町村へ高額該当情報を引き継ぐためのデータ(転出地市区町村高額該当情報データ)を作成し、転入地市区町村の国保総合PCへ当該データを配信する。 3. オンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者異動情報の提供 (詳細は別添1を参照) (1)被保険者異動情報(資格情報(世帯)ファイル、資格情報(個人)ファイル)の送信 市区町村の国保総合PCのファイル転送機能(*)を用いて、被保険者資格異動に関するデータを市区町村から国保連合会へ送信する。 (2)医療保険者等向け中間サーバー等への被保険者異動情報の送信 オンライン資格確認等システムで被保険者等の資格情報を利用するため、国保連合会は、市区町村より受領した被保険者異動情報に関するデータを医療保険者等向け中間サーバー等へ被保険者異動情報を送信する。 * ファイル転送機能とは、市区町村の国保総合PCのWebブラウザーを用いて、各種ファイルを国保連合会の国保総合(国保集約)システムへ送信する機能と、国保連合会の国保総合(国保集約)システムサーバ内に格納されている各種ファイルや帳票などを、市区町村の国保総合PCに配信する機能のことをいう。
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 ☐ 市内連携システム ☐ 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 (SKY2国民健康保険システム)

システム5	
①システムの名称	医療保険者等向け中間サーバー等
②システムの機能	医療保険者等向け中間サーバー等は、医療保険者等全体または医療保険制度横断で資格管理等を行う際に必要となるシステムであり、取りまとめ機関が運営する。 なお、市区町村国保に関しては、情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能のうち情報照会及び情報提供、本人確認事務に係る機能については、「地方公共団体における情報連携プラットフォームに係る中間サーバー(自治体中間サーバー)」を利用するため、「医療保険者等向け中間サーバー等」では、情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能のうち情報照会及び情報提供、本人確認事務に係る機能は行わないが、被保険者の基本情報(氏名、生年月日、性別、住所)と個人番号の紐づけが正しいか否かを検査する用途に限って、医療保険者等向け中間サーバー等によるJ-LISへの照会を行う。 1. 資格履歴管理事務に係る機能 (1)資格履歴管理(評価対象) ・医療保険者等から送信された被保険者異動情報を、委託区画に登録する。 ・運用支援環境において、委託区画から取得した被保険者異動情報を基に、資格履歴ファイルに格納する。(当該機能については支払基金が特定個人情報保護評価を実施するため当評価の対象外。) (2)被保険者の基本情報(氏名、生年月日、性別、住所)と個人番号の紐づけが正しいか否かを検査する用途に限って、医療保険者等向け中間サーバー等によるJ-LISへの照会を行う。 (3)オンライン資格確認等システムへの資格情報の提供(個人番号を用いないため評価対象外) ・資格履歴ファイルをオンライン資格確認等システムに提供する。 2. 情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能 (1)機関別符号取得(評価対象外)※ ・医療保険者等からの符号取得要求を受領後、システムの自動処理により、符号取得要求ファイルを生成し、情報提供サーバーに転送する。 ・支払基金職員が情報提供サーバーアプリケーションを操作することで、情報提供ネットワークシステムから機関別符号を取得し、機関別符号ファイルに格納する。 (2)情報提供(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)(評価対象外)※ ・マイナポータルからの自己情報開示の求めを受け付け、システムの自動処理により、運用支援環境において被保険者等を特定し、資格履歴ファイルからオンライン資格確認等システムで管理している情報と紐付けるために使用する情報を提供する。 ※当該機能については支払基金が特定個人情報保護評価を実施するため当評価の対象外。
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 ☐ 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 (オンライン資格確認等システム、国保情報集約システム)

システム6～10	
システム6	
①システムの名称	サービス検索・電子申請機能
②システムの機能	国民健康保険の加入手続き 【住民向け機能】 自らが受けることができるサービスをオンラインで検索及び申請ができる機能 【地方公共団体向け機能】 住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能
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（申請管理システム）
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
国民健康保険ファイル	
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	<被保険者資格管理等に係る事務> ・個人の所得を正しく把握し、正確な保険料賦課または自己負担限度額認定を行うため。 ・必要な情報を正確かつ迅速に取得し処理するには、電算システムの利用が不可欠であるため。 <オンライン資格確認等システムに係る事務> ・オンライン資格確認で被保険者等の資格情報を利用するためには、医療保険者等向け中間サーバー等において、医療保険者等の加入者等の履歴情報を正確に管理する必要があるため。また、その履歴情報の生成の際には、同一人であることを正確に把握するために個人番号を用いる必要があるため。
②実現が期待されるメリット	<被保険者資格管理等に係る事務> ・これまで文書に依存していた所得情報の他庁照会が、特定個人番号を活用しデータでのやりとりとなることで、事務処理における精度・速度ともに向上が可能となり、もって被保険者の利便に資することが可能となる。 <オンライン資格確認等システムに係る事務> ・オンライン資格確認等システムを通して、資格喪失後の受診に伴う事務コスト等の削減、限度額適用認定証等の発行業務等の削減、記号番号等の入力自動化による返戻レセプトの削減、後続開発システムとの連携による保健医療データ活用のしくみを実現する。
5. 個人番号の利用 ※	
法令上の根拠	<被保険者資格管理等に係る事務> 番号法第9条第1項 別表の44の項 <オンライン資格確認等システムに係る事務> ・番号法第9条第1項 別表の44の項 ・番号法別表第1の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項 ・住民基本台帳法第30条の9 別表第1項番73の2(J-LIS照会による本人確認)
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	<被保険者資格管理等に係る事務> 番号法第19条第8号に基づく主務省令第2条の表の以下の項 1、2、3、5、6、13、16、19、27、38、42、48、56、65、67、69、70、71、83、87、111、115、125、131、137、141、145、158 <オンライン資格確認等システムに係る事務> ・番号法 附則第6条第4項(利用目的:情報連携のためではなくオンライン資格確認等システムに係る事務として機関別符号を取得する等) ・国民健康保険法 第113条の3 第1項及び第2項
7. 評価実施機関における担当部署	
①部署	世田谷区保健福祉政策部国保・年金課
②所属長の役職名	保健福祉政策部 国保・年金課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容



(備考)

1 被保険者資格管理等に係る事務

- 1-①転入や社会保険喪失などによる国民健康保険加入の届出を受ける。
- 1-②保険料計算に必要な所得情報などを、庁内連携、または情報提供ネットワークにて中間サーバより取得する。
- 1-③加入条件を確認した上で加入者に対する資格の認定を行う。
- 1-④資格確認書等を交付する。
- 1-⑤所得情報を基に保険料を計算し納付書を送付する。
- 1-⑥マイナンバーカードもしくは資格確認書等を医療機関等に提示して、受診する。
- 1-⑦医療機関等に設置されている資格確認端末にて、資格を確認する。
- 1-⑧かかった医療費の3割を自己負担分として患者に請求する。
- 1-⑨残りの7割(保険者負担分)を国保連を経由してレセプトにより請求する。
- 1-⑩正当な請求に関しては国保連経由で医療機関へ支払いを行う。
- 1-⑪国保加入者の転出・死亡等により、国保脱退届を受ける。

(以下は随時)

- 1-⑫国保の資格異動ほかの情報を、中間サーバに転送する。
- 1-⑬⑭国・都からの依頼により調査事務を行い、回答する。
- 1-⑮異動があった被保険者に関する被保険者異動情報を作成し、データを移入する。
- 1-⑯被保険者異動情報のデータを送信する。
- 1-⑰被保険者の取得・喪失・継続に関する処理を行なう。被保険者情報を作成し、データを配信する。
- 1-⑱SKY2国民健康保険システムにデータを移入する。
- 1-⑲⑳の被保険者異動情報に基づき、世帯継続情報・高額該当回数を送信する。

2 オンライン資格確認等システムに係る事務

(資格履歴管理事務)

- 2-①加入者情報を、医療保険者等向け中間サーバー等システムの委託区画へ送信する。
- 2-②運用支援環境において、委託区画から取得した加入者情報を基に、資格履歴ファイルに格納する。
- 2-③資格履歴ファイルをオンライン資格確認等システムに提供する。
(機関別符号の取得等事務)
- 2-④符号取得要求ファイルを生成後、情報提供サーバーを経由して、情報提供ネットワークシステムへ機関別符号を要求する。
- 2-⑤情報提供ネットワークシステムから機関別符号を取得し、統一区画内の機関別符号ファイルに格納する。
(情報提供(マイナンバーカードを資格確認書等として利用するために必要な初回登録等))
- 2-⑥被保険者がマイナポータルの自己情報取得機能を利用して、初回登録(もしくは自己情報開示要求)を行う。
- 2-⑦マイナポータルから情報提供ネットワークへ、初回紐付け(もしくは自己情報開示)要求を行う。
- 2-⑧情報提供ネットワークシステムから運用支援環境へ、⑦で要求のあった被保険者等の紐付け情報(保険者番号・資格確認書等記号番号等)を要求する。
- 2-⑨運用支援環境にて被保険者等を特定し、紐付け情報を送信する。
- 2-⑩紐付け情報をマイナポータルに格納する。

3 オンライン資格確認の準備のための医療保険者等向け中間サーバー等上の被保険者異動情報の基本4情報照会(本人確認)

- ・市町村から国民健康保険に関する「医療保険者等向け中間サーバー等における資格履歴管理事務」の再委託を受けたとりまとめ機関が、医療保険者等向け中間サーバー等システムの委託区画に登録されている被保険者資格情報の正確性を担保するために、同区画の同情報から「基本4情報照会要求ファイル(個人番号)」を抽出する。
- 3-①取りまとめ機関は、住民基本台帳ネットワークシステムに「基本4情報照会要求ファイル(個人番号)」を送信する。
- 3-②取りまとめ機関は、住民基本台帳ネットワークシステムから、照会結果ファイル(照会対象者の基本4情報(本人確認情報)+個人番号)を取得(受信)する。
- ・取りまとめ機関は、照会結果ファイルと委託区画に登録されている被保険者資格情報の基本4情報が同じかどうかのチェックを個人番号で突合を行い、突合結果を市町村へ通知するために突合結果リストデータ(Excel)を作成する。突合結果リストには個人番号は記録しない。
- 3-③取りまとめ機関は、上述「3-4」の突合結果リストデータ(EXCEL)を市町村へ通知する。(通知された突合結果をもとに、市町村が自庁の住民基本台帳や住基ネット端末を用いて最新情報を調査し、必要に応じて特定個人情報の訂正を行い、既設ルートで被保険者情報の異動を行う)

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	
国民健康保険ファイル	
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 ※	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
その必要性	個人を正確に特定し、公平・公正な国民健康保険事務を行うため（保険料収納事務を除く）
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 [○] 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	①その他識別情報:個人を正確に特定するため ②5情報:保険料賦課及び保険給付を的確に行うため ③地方税関係情報:保険料計算や限度額認定を的確に行うため ④医療保険関係情報:保険料計算を的確に行うため
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年6月
⑥事務担当部署	世田谷区保健福祉政策部国保・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 （ 財務部課税課、地域行政部住民記録・戸籍課 ） [☐] 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 （ 他区市町村 ） [☐] 民間事業者 （ ） [☐] その他 （ 東京都国民健康保険団体連合会 ）
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 （ サービス検索・電子申請機能 ）
③入手の時期・頻度	<国保連合会以外からの入手> 随時 <国保連合会からの入手> 当区は国保連合会より、以下の時期・頻度で特定個人情報を入手する。 ・資格継続業務 ・被保険者情報(国保資格取得喪失年月日連携ファイル、市町村被保険者ID連携ファイル等) : 国民健康保険に関する都道府県単位の被保険者資格情報。 平成30年4月1日以後に、日次の頻度。 ・高額該当の引き継ぎ業務 ・引き継ぎ情報(継続候補世帯リスト、継続世帯確定リスト等) : 転出地市区町村から転入地市区町村へ高額該当情報を引き継ぐための情報。 平成30年4月1日以後に、月次の頻度
④入手に係る妥当性	<国保連合会以外からの入手> ・新規の申請については、原則として本人からの紙ベースによる提供となっており、これにより保険料賦課及び保険給付に必要な情報を入手する。 ・必要に応じて、申請等の情報の正確性確認を行うため、庁内連携または情報提供ネットワークシステムを通じて被保険者の所得情報の特定等に必要な情報を随時入手する。 <国保連合会からの入手> 国民健康保険に関して、被保険者資格等の管理を都道府県単位で実施する必要があるため、個人番号利用事務の一部を国保連合会に委託しているため、当区が保険給付の支給、保険料の徴収または保健事業等を実施するためには、国保連合会から当該情報を入手する必要がある。 なお、入手する情報は、当区分の被保険者、擬制世帯主、過去に被保険者であった者、過去に擬制世帯主であった者のみであり、当該事務において必要な範囲内の情報である。 1. 入手の時期・頻度の妥当性 ・資格継続業務 ・被保険者情報 : 国保総合(国保集約)システム上で管理している被保険者資格を、住民基本台帳に記載する必要があるため、日次で連携を行うことで住民票の記載事項の正確性を確保する。 ・高額該当の引き継ぎ業務 ・引き継ぎ情報 : 高額療養費制度は、医療機関等での支払額が、暦月で一定額を超えた場合に、その超過額を支給する制度のため月次計算を行うが、その計算前に月次で連携を行うことで、支給の正確性を確保する。 2. 入手方法の妥当性 ・入手は専用線を用いて行うが、信頼性、安定性の高い通信環境が実現でき、さらに通信内容の暗号化とあわせて通信内容の漏えいや盗聴に対するリスクが低く、頻繁に通信が必要な場合には通所の通信回線である公衆網を使うよりも低コストとなることが期待できる。
⑤本人への明示	・本人から入手する情報については、本人を通じて入手することとし、また利用目的を本人に明示する。ただし国民健康保険法等、他の法令で定めがある場合は、その限りではない。 ・庁内連携又は情報提供ネットワークシステムを通じた入手を行うことは番号法に明示されているが、窓口対応する場合は、口頭にて本人に説明を行う。

⑥使用目的 ※		個人の情報を的確に把握し、迅速かつ正確な保険料賦課及び保険給付業務を行うため。
	変更の妥当性	—
⑦使用の主体	使用部署 ※	国保・年金課、世田谷総合支所区民課(区民係、太子堂出張所、経堂出張所)、北沢総合支所区民課(区民係)、玉川総合支所区民課(区民係、用賀出張所、二子玉川出張所)、砧総合支所区民課(区民係)、烏山総合支所区民課(区民・戸籍係、烏山出張所)、各総合支所地域振興課まちづくりセンター(池尻、若林、上町、下馬、上馬、梅丘、代沢、新代田、松原、松沢、奥沢、九品仏、上野毛、深沢、祖師谷、船橋、喜多見、砧、上北沢、上祖師谷)
	使用者数	[500人以上1,000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 ※		①社会保険離脱や転出入、または、出生死亡等様々な資格異動に伴う被保険者資格の取得喪失の認定 ②所得を元に軽減等の要件を適用した上での保険料計算及び賦課 ③被保険者への療養費支給業務 ④国民健康保険加入者を対象とした特定健康診査及びその結果に基づく指導
	情報の突合 ※	必要に応じ、国民健康保険事務にて保有する情報と、SKY2住民記録システム、SKY2住民税システム等と情報の突合を行う。
	情報の統計分析 ※	国・都への報告資料等のため統計・分析を行うが、特定個人情報を用いて特定の個人を判別しうる統計・分析は行わない。
	権利利益に影響を与え得る決定 ※	①資格異動に伴う得喪の認定 ②療養費の給付決定
⑨使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託

[illegible]

委託事項2～5		
委託事項2		資格継続業務、高額該当回数の引き継ぎ業務に関する保険者事務共同処理業務
①委託内容		・療養給付の審査・支払に付随する業務として、都道府県単位で管理することとなる資格取得年月日や喪失年月日の管理(資格継続業務)と、同一都道府県内で転居があった場合における高額療養費の該当回数を通算するための同一世帯判定に必要な情報等の管理(高額該当の引き継ぎ業務)を委託する(国保情報集約システムを使用する)。 ・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。 ・オンライン資格確認等システムで被保険者等の資格情報を利用するため、国保連合会は、市区町村より受領した被保険者資格異動に関するデータを編集し、「医療保険者等向け中間サーバー等」へ送信、登録を行う。
②取扱いを委託する特定個人情報ファイルの範囲		＜選択肢＞ [特定個人情報ファイルの一部] 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	＜選択肢＞ [10万人以上100万人未満] 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 ※	・被保険者(*): 都道府県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、当区に住所を有する者 ・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者(例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。) ・過去に被保険者であった者および過去に擬制世帯主であった者 * 国民健康保険法第5条から第6条に基づく被保険者のうち、当区に加入資格が適用される者をいう。
	その妥当性	・被保険者の情報は、国民健康保険に関する事務の基礎情報であるため管理する必要がある。 ・医療費の自己負担限度額が非課税区分に該当するかどうかを判定する際には、擬制世帯主の住民税課税状況を含んで判定をするため、被保険者のみでなく、擬制世帯主の情報も必要である。 ・療養給付の審査・支払に関する業務等を行う上で、被保険者とその被保険者が属する世帯の世帯主(擬制世帯主)に関する所得等の情報を管理する必要がある。 ・「国民健康保険法(昭和33年法律第192号)」第110条によって保険給付を受ける権利は、2年間有効、「地方自治法(昭和22年法律第67号)第236条1項」によって不当利得の返還を受ける。権利は5年間有効とされているため、過去の特定個人情報についても管理する必要がある。 ・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務およびオンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者資格情報の提供(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。
③委託先における取扱者数		＜選択肢＞ [10人以上50人未満] 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		契約した委託先は、区ホームページにて公表している。
⑥委託先名		東京都国民健康保険団体連合会
再委託	⑦再委託の有無 ※	＜選択肢＞ [再委託する] 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	再委託を行う場合には、委託先から再委託先の商号または名称、住所、再委託する理由、再委託する業務の範囲、再委託先に関する業務の履行能力、再委託予定金額等およびその他当区のセキュリティポリシー等で委託先に求めるべきとされている情報について記載した書面による再委託申請および再委託に関する履行体制図の提出を受け、委託先と再委託先が秘密保持に関する契約を締結していることなど、再委託先における安全管理措置を確認し、決裁等必要な手続を経た上で再委託を承認する。
	⑨再委託事項	資格継続業務、高額該当回数の引き継ぎ業務で使用する国保総合(国保集約)システムに関する運用業務の一部(バッチ処理/パラメータの入力/バッチ処置の実行/バックアップデータの取得と保管/システム障害発生時の復旧支援作業/各種マスターメンテナンス/外字作成・登録)など。

委託事項3	医療保険者等向け中間サーバー等における資格履歴管理事務
①委託内容	オンライン資格確認のための準備として、医療保険者等向け中間サーバー等において、個人番号を利用した被保険者資格の履歴管理、被保険者枝番の採番管理、被保険者枝番と個人番号との紐付管理および個人番号の紐づけが正しいか否かを検査するためのJ-LIS照会などを行う。
②取扱いを委託する特定個人情報ファイルの範囲	＜選択肢＞ [特定個人情報ファイルの一部] 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	＜選択肢＞ [10万人以上100万人未満] 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 ※	・被保険者(＊): 都道府県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、当区に住所を有する者 ・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者(例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。) ・過去に被保険者であった者および過去に擬制世帯主であった者 ＊ 国民健康保険法第5条から第6条に基づく被保険者のうち、当区に加入資格が適用される者をいう。
その妥当性	・オンライン資格確認等システムで被保険者等の資格情報を利用するために、加入者の資格履歴情報の管理を行う。
③委託先における取扱者数	＜選択肢＞ [10人以上50人未満] 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	契約した委託先は、区ホームページにて公表している。
⑥委託先名	東京都国民健康保険団体連合会 (東京都国民健康保険団体連合会は、国保中央会に再委託する。)

再委託	⑦再委託の有無 ※	＜選択肢＞ 1) 再委託する 2) 再委託しない [再委託する]
	⑧再委託の許諾方法	当区は、再委託は原則禁止であり、やむを得ず再委託する必要がある場合に限り、委託先からの事前の申請に基づき、再委託を承諾するものである。委託先とは「電算処理の業務委託契約の特記事項」（以下、特記事項）を取り交わし、再委託の承認にあたっては、以下の事項を遵守することを必須条件とする。 ・委託先の東京都国民健康保険連合会は、再委託先に委託契約及び特記事項を遵守させる。 ・委託先は、再委託申請を行う際、再委託先にかかる再委託の内容及び特記事項第3項に規定する事項を書面にて提出する。 ・委託先が再委託先を選定する際、区の求めに応じて、再委託先の委託業務状況等の報告資料を提出させること、及び再委託先への実地調査を行うことができることを必須条件とする。 ・委託先と再委託先の間で秘密保持に関する契約等を締結する。また、再委託先が更に再委託することも原則禁止であり、やむを得ず更に再委託する必要がある場合には、再委託と同様の条件（ただし、再委託先よりもより厳しい条件とする）と手続きにより、事前に当区の承認を得なければならないものとする。更に再委託が繰り返される場合も同様とする。 当区は委託先に対して直接的な監督義務を負い、再委託先に対しては間接的な監督義務を負う。委託先は再委託先に対して直接的な監督義務を負うものとする。委託先及び再委託先（再委託先以降を含む）は、監督義務のほか、特記事項第6項のとおり罰則規定が及ぶことを認識して業務を行うものとする。 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理対策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上及び運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化等)をどのように確保したかを書面にて示した上で、許諾を得ること。
	⑨再委託事項	医療保険者等向け中間サーバー等における資格履歴管理事務 （医療保険者等向け中間サーバー等の運用・保守業務を含む）

再委託	⑦再委託の有無 ※	＜選択肢＞ 1) 再委託する 2) 再委託しない [再委託する]
	⑧再委託の許諾方法	当区は、再委託は原則禁止であり、やむを得ず再委託する必要がある場合に限り、委託先からの事前の申請に基づき、再委託を承諾するものである。委託先とは「電算処理の業務委託契約の特記事項」（以下、特記事項）を取り交わし、再委託の承認にあたっては、以下の事項を遵守することを必須条件とする。 ・委託先の東京都国民健康保険連合会は、再委託先に委託契約及び特記事項を遵守させる。 ・委託先は、再委託申請を行う際、再委託先にかかる再委託の内容及び特記事項第3項に規定する事項を書面にて提出する。 ・委託先が再委託先を選定する際、区の求めに応じて、再委託先の委託業務状況等の報告資料を提出させること、及び再委託先への実地調査を行うことができることを必須条件とする。 ・委託先と再委託先の間で秘密保持に関する契約等を締結する。また、再委託先が更に再委託することも原則禁止であり、やむを得ず更に再委託する必要がある場合には、再委託と同様の条件（ただし、再委託先よりもより厳しい条件とする）と手続きにより、事前に当区の承認を得なければならないものとする。更に再委託が繰り返される場合も同様とする。 当区は委託先に対して直接的な監督義務を負い、再委託先に対しては間接的な監督義務を負う。委託先は再委託先に対して直接的な監督義務を負うものとする。委託先及び再委託先（再委託先以降を含む）は、監督義務のほか、特記事項第6項のとおり罰則規定が及ぶことを認識して業務を行うものとする。 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理対策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上及び運用上のセキュリティ（OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化等）をどのように確保したかを書面にて示した上で、許諾を得ること。
	⑨再委託事項	医療保険者等向け中間サーバー等の運用・保守業務

委託事項5	国保総合(国保集約)システムに係るアプリケーション保守業務及びシステム運用事務		
①委託内容	国保総合(国保集約)システムに係るアプリケーション保守業務(アプリケーション改修、データパッチ実施等)及びシステム運用事務(バックアップ取得、システム障害等発生時のデータ復旧等)		
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一部]	<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	<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 ※	・被保険者(*): 都道府県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、当区に住所を有する者 ・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者(例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。) ・過去に被保険者であった者および過去に擬制世帯主であった者 * 国民健康保険法第5条から第6条に基づく被保険者のうち、当区に加入資格が適用される者をいう	
	その妥当性	・被保険者の情報は、国民健康保険に関する事務の基礎情報であるため管理する必要がある。 ・医療費の自己負担限度額が非課税区分に該当するかどうかを判定する際には、擬制世帯主の住民税課税状況を含んで判定をするため、被保険者のみでなく、擬制世帯主の情報も必要である。 ・療養給付の審査・支払に関する業務等を行う上で、被保険者とその被保険者が属する世帯の世帯主(擬制世帯主)に関する所得等の情報を管理する必要がある。 ・「国民健康保険法(昭和33年法律第192号)」第110条によって保険給付を受ける権利は、2年間有効、「地方自治法(昭和22年法律第67号)第236条1項」によって不当利得の返還を受ける権利は5年間有効とされているため、過去の特定個人情報についても管理する必要がある。 ・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務およびオンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者資格情報の提供(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。	
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	契約した委託先は、区ホームページにて公表している。		
⑥委託先名	東京都国民健康保険団体連合会 (東京都国民健康保険団体連合会は、国保中央会に再委託する)		

再委託	⑦再委託の有無 ※	＜選択肢＞ [再委託する] 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	当区は、再委託は原則禁止であり、やむを得ず再委託する必要がある場合に限り、委託先からの事前の申請に基づき、再委託を承諾するものである。委託先とは「電算処理の業務委託契約の特記事項」（以下、特記事項）を取り交わし、再委託の承認にあたっては、以下の事項を遵守することを必須条件とする。 ・委託先の東京都国民健康保険連合会は、再委託先に委託契約及び特記事項を遵守させる。 ・委託先は、再委託申請を行う際、再委託先にかかる再委託の内容及び特記事項第3項に規定する事項を書面にて提出する。 ・委託先が再委託先を選定する際、区の求めに応じて、再委託先の委託業務状況等の報告資料を提出させること、及び再委託先への実地調査を行うことができることを必須条件とする。 ・委託先と再委託先の間で秘密保持に関する契約等を締結する。 また、再委託先が更に再委託することも原則禁止であり、やむを得ず更に再委託する必要がある場合には、再委託と同様の条件（ただし、再委託先よりもより厳しい条件とする）と手続きにより、事前に当区の承認を得なければならないものとする。更に再委託が繰り返される場合も同様とする。 当区は委託先に対して直接的な監督義務を負い、再委託先に対しては間接的な監督義務を負う。委託先は再委託先に対して直接的な監督義務を負うものとする。委託先及び再委託先（再委託先以降を含む）は、監督義務のほか、特記事項第6項のとおり罰則規定が及ぶことを認識して業務を行うものとする。 国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 ・クラウド事業者が提供するクラウドサービスは、政府情報システムのためのセキュリティ評価制度（ISMAP）に基づくクラウドサービスリストに掲載されているものとする。 国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc)をどのように確保したかを書面にて示した上で、許諾を得ること。
	⑨再委託事項	国保総合(国保集約)システムに係るアプリケーション保守業務及びシステム運用事務の全て

委託事項6～10	
委託事項6	
SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等	
①委託内容	
郵送や電子で届いた加入・脱退の申請、及び非自発的失業者の保険料軽減に伴う入力作業等	
②取扱いを委託する特定個人情報ファイルの範囲	＜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 ＜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 ※ SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
	その妥当性 郵送や電子で申請される国保の加入・脱退、減免について、適切にSKY2国民健康保険システムに入力することで、保険料の公平・公正な賦課、徴収に繋げることができる。
③委託先における取扱者数	
＜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	
契約した委託先は、区ホームページにて公表している。	
⑥委託先名	
TOPPAN株式会社	
再委託	⑦再委託の有無 ※
	＜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
委託業務の附属業務についてやむを得ず再委託する必要があるときは、再受託者に、当該委託契約書に記載された情報セキュリティに関する特記事項を遵守させるとともに、再受託者の氏名、再委託の内容及び業務執行場所を、区に事前に通知し、その承認を得ることを委託契約上の条件としている。	
⑨再委託事項	
①加入・脱退申請書等の内容確認、②非自発的失業者の保険料軽減申請書等の内容確認、③基幹システム入力	
委託事項11～15	
委託事項16～20	

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 (27) 件 [☐] 移転を行っている (2) 件 [☐] 行っていない
提供先1	厚生労働大臣
①法令上の根拠	番号法第19条第8号 別表第2の1
②提供先における用途	健康保険法第5条第2項の規定により厚生労働大臣が行うこととされた健康保険に関する事務であって主務省令で定めるもの
③提供する情報	医療保険各法または高齢者の医療の確保に関する法律による医療に関する給付の支給又は保険料の徴収に関する情報(以下、「医療保険給付関係情報」という。)であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
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	随時

提供先2～5	
提供先2	全国健康保険協会
①法令上の根拠	番号法第19条第8号 別表第2の2
②提供先における用途	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☒ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時
提供先3	健康保険組合
①法令上の根拠	番号法第19条第8号 別表第2の3
②提供先における用途	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☒ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時

提供先4	厚生労働大臣
①法令上の根拠	番号法第19条第8号 別表第2の4
②提供先における用途	船員保険法第4条第2項の規定により厚生労働大臣が行うこととされた船員保険に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	[☒] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 ([] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙)
⑦時期・頻度	随時
提供先5	全国健康保険協会
①法令上の根拠	番号法第19条第8号 別表第2の5
②提供先における用途	船員保険法による保険給付の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	[☒] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 ([] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙)
⑦時期・頻度	随時

提供先6～10	
提供先6	都道府県知事
①法令上の根拠	番号法第19条第8号 別表第2の9
②提供先における用途	児童福祉法による小児慢性特定疾病医療費の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時
提供先7	市町村長
①法令上の根拠	番号法第19条第8号 別表第2の12
②提供先における用途	児童福祉法による肢体不自由児通所医療費の支給に関する事務であって主務省令で定めるもの
③提供する情報	児童福祉法第21条の5の31に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時

提供先8	都道府県知事
①法令上の根拠	番号法第19条第8号 別表第2の15
②提供先における用途	児童福祉法による障害児入所医療費の支給に関する事務であって主務省令で定めるもの
③提供する情報	児童福祉法第24条の22に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時
提供先9	市町村長
①法令上の根拠	番号法第19条第8号 別表第2の17
②提供先における用途	予防接種法による給付(同法第15条第1項の疾病に係るものに限る。)の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険各法その他の法令による医療に関する給付の支給に関する情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時

提供先10	都道府県知事等
①法令上の根拠	番号法第19条第8号 別表第2の22
②提供先における用途	精神保健及び精神障害者福祉に関する法律による入院措置に関する事務であって主務省令で定めるもの
③提供する情報	精神保健及び精神障害者福祉に関する法律第30条の2に規定する他の法律による医療に関する給付の支給に関する情報であって主務省令で定めるもの
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] <u>＜選択肢＞</u> 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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時
提供先11～15	
提供先11	都道府県知事等
①法令上の根拠	番号法第19条第8号 別表第2の26
②提供先における用途	生活保護法による保護の決定及び実施又は徴収金の徴収に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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] <u>＜選択肢＞</u> 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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時

提供先12	市町村長
①法令上の根拠	番号法第19条第8号 別表第2の27
②提供先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時
提供先13	社会福祉協議会
①法令上の根拠	番号法第19条第8号 別表第2の30
②提供先における用途	社会福祉法による生計困難者に対し無利子または低利で資金を融通する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
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時

提供先16～20	
提供先16	市町村長または国民健康保険組合
①法令上の根拠	番号法第19条第8号 別表第2の42
②提供先における用途	国民健康保険法による保険給付の支給または保険料の徴収に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時
提供先17	地方公務員共済組合
①法令上の根拠	番号法第19条第8号 別表第2の58
②提供先における用途	地方公務員等共済組合法による短期給付の支給に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	随時

提供先18	市町村長
①法令上の根拠	番号法第19条第8号 別表第2の62
②提供先における用途	老人福祉法による費用の徴収に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
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	随時
提供先19	厚生労働大臣
①法令上の根拠	番号法第19条第8号 別表第2の78
②提供先における用途	雇用保険法による傷病手当の支給に関する事務であって主務省令で定めるもの
③提供する情報	雇用保険法第37条第8項に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
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	随時

提供先20	後期高齢者医療広域連合
①法令上の根拠	番号法第19条第8号 別表第2の80
②提供先における用途	高齢者の医療の確保に関する法律による後期高齢者医療給付の支給または保険料の徴収に関する事務であって主務省令で定めるもの
③提供する情報	医療保険給付関係情報であって主務省令で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☒ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時

提供先21	都道府県知事等
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表125の項
②提供先における用途	中国残留邦人等支援給付等の支給に関する事務であって第127条で定めるもの
③提供する情報	医療保険給付関係情報であって第127条で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	[☒] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 ([] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙)
⑦時期・頻度	随時

提供先22	市町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表131の項
②提供先における用途	介護保険法による保険給付の支給又は地域支援事業の実施に関する事務であって第133条で定めるもの
③提供する情報	医療保険給付関係情報であって第133条で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時
提供先23	都道府県知事または保健所を設置する市の長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表137の項
②提供先における用途	感染症の予防及び感染症の患者に対する医療に関する法律による費用の負担または療養費の支給に関する事務であって第139条で定めるもの
③提供する情報	感染症の予防及び感染症の患者に対する医療に関する法律第39条第1項に規程する他の法律による医療に関する給付の支給に関する情報であって第139条で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時

提供先26	都道府県知事
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表158の項
②提供先における用途	難病の患者に対する医療等に関する法律による特定医療費の支給に関する事務であって第160条で定めるもの
③提供する情報	難病の患者に対する医療等に関する法律第12条に規定する他の法令による給付の支給に関する情報であって第160条で定めるもの
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時
提供先27	世田谷区教育委員会
①法令上の根拠	番号法第19条第11号 (条例による利用)
②提供先における用途	医療保険に関する事務 (SKY2住民票内容表示)
③提供する情報	保険証番号、資格取得情報、資格喪失情報
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	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	随時

移転先1	各総合支所(地域振興課、区民課、街づくり課)、 各総合支所地域振興課まちづくりセンター(太子堂、経堂、北沢、等々力、用賀、二子玉川、成城、烏山)、各保健福祉センター(生活支援課、保健福祉課、健康づくり課、子ども家庭支援課)、政策企画課、政策研究・調査課、広報広聴課、DX推進担当課、総務課、人事課、用地課、市民活動・生涯現役推進課、地域行政課、住民記録・戸籍課、マイナンバーカード担当課、環境保全課、商業課、都市農業課、障害施策推進課、障害者地域生活課、障害保健福祉課、高齢福祉課、子ども育成推進課、児童課、児童相談支援課、児童相談所、一時保護課、保育認定・調整課、世田谷保健所(健康企画課、健康推進課、感染症対策課、地域保健課、生活保健課)、市街地整備課、建築審査課、住宅管理課、防災街づくり課、建築安全課、道路管理課、道路事業推進課、交通安全自転車課
①法令上の根拠	番号法第9条第2項 (条例による利用)
②移転先における用途	世田谷区の基幹システムであるSKY2にて、住民票関連情報として使用
③移転する情報	医療保険関係情報
④移転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移転する情報の対象となる本人の範囲	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥移転方法	[☐] 庁内連携システム [☐] 電子メール [☐] フラッシュメモリ [☐] その他 () [☐] 専用線 [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] 紙
⑦時期・頻度	随時
移転先2～5	
移転先2	各保健福祉センター(生活支援課、保健福祉課、健康づくり課、子ども家庭支援課)、DX推進担当課、課税課、市民活動・生涯現役推進課、保健福祉政策課、保健医療福祉推進課、生活福祉課、障害施策推進課、障害者地域生活課、障害保健福祉課、高齢福祉課、介護予防・地域支援課、子ども育成推進課、子ども家庭課、児童相談支援課、児童相談所、保育課、保育認定・調整課、保育計画・整備支援担当課、世田谷保健所(感染症対策課)、住宅管理課、あんしんすこやかセンター(池尻、太子堂、若林、上町、経堂、下馬、上馬、梅丘、代沢、新代田、北沢、松原、松沢、奥沢、九品仏、等々力、上野毛、用賀、深沢、二子玉川、祖師谷、成城、船橋、喜多見、砧、上北沢、上祖師谷、烏山)
①法令上の根拠	番号法第9条第2項 (条例による利用)
②移転先における用途	保健福祉総合情報システムにて、医療保険情報として使用
③移転する情報	医療保険関係情報
④移転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移転する情報の対象となる本人の範囲	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者
⑥移転方法	[☐] 庁内連携システム [☐] 電子メール [☐] フラッシュメモリ [☐] その他 () [☐] 専用線 [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] 紙
⑦時期・頻度	随時

6. 特定個人情報の保管・消去														
①保管場所 ※		＜世田谷区における措置＞ 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理：ICカード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 申請書及び届出書等の紙媒体、及び外部記録媒体は、鍵のかかるロッカーや保管庫に保管している。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜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。												
②保管期間	期間	＜選択肢＞ <table border="0"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td colspan="3">10) 定められていない</td> </tr> </table> [定められていない]	1) 1年未満	2) 1年	3) 2年	4) 3年	5) 4年	6) 5年	7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上	10) 定められていない		
	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	国民健康保険法ほか法令では、データ保管期間の定めはない。												
③消去方法		＜世田谷区における措置＞ ①データベースに登録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。 ③外部記憶媒体に一時的に登録した特定個人情報等の申請データは、使用の都度速やかに完全消去する。 ＜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 SP800-88、ISO/IEC27001等に当た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。 ＜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世田谷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

国民健康保険ファイル

<宛名情報>

宛名番号 個人番号 法人番号 世帯番号 氏名情報 生年月日 性別 続柄 住民となった年月日 住民となった届出年月日 住民となった事由

住民区分(日本人・外国人) 世帯主情報 現住所情報 住所を定めた年月日 住所を定めた届出年月日 前住所情報 転入元住所情報 転出先住所情報 本籍・筆頭者情報 消除情報 国籍 在留カード等の番号 在留資格情報 通称 処理停止情報 送付先情報 送付先履歴情報 相続人情報 相続人続柄情報 相続人履歴情報 納税管理人情報 納税管理人履歴情報 記事情報 連絡先情報 破産管財人情報 破産管財人履歴情報

口座情報

<資格情報>

宛名番号 記号番号 記号番号ごとの枝番(個人を識別する2桁の番号)

保険証番号 記号番号開始日 記号番号終了日

資格取得情報(取得日、届出日、取得事由) 資格喪失情報(喪失日、届出日、喪失事由)

市町村被保険者ID情報

適用開始情報(開始日、届出日、開始事由) 適用終了情報(終了日、届出日、終了事由)

適用変更情報(異動日、届出日、異動事由)

退職者受給情報(退職資格該当日、退職資格非該当日、退職裁定日、退職受給発生年月)

世帯情報 世帯主情報 世帯被保情報 世帯メモ情報

退職該当情報 学遠該当情報 老健該当情報 施設入所情報

個人証情報 高齢受給者証情報

券面記載情報 資格確認書等裏面への性別記載の有無情報 自己情報不開示の申し出の有無情報

社保情報 介護適用除外情報 世帯負担割合情報 個人負担割合情報

滞納証情報 世帯被保年齢判定情報

旧国保被保険者情報 特定同一世帯所属者異動連絡票情報 旧被扶養者情報 旧被扶養者異動連絡票情報

非自発的失業者情報

<資格履歴情報>

世帯履歴情報 世帯主履歴情報 世帯被保履歴情報

退職該当履歴情報 学遠該当履歴情報 老健該当履歴情報 施設入所履歴情報

介護適用除外履歴情報 世帯負担割合履歴情報 滞納証履歴情報

特定健診被保険者マスタ情報 被保険者マスタ情報

<賦課情報>

宛名番号 記号番号 記号番号ごとの枝番(個人を識別する2桁の番号)

課税年度(相当年度)

調定年度(賦課年度)

基礎所得割額、基礎均等割額、基礎年税額、基礎減免額、基礎納付額

基礎退職所得割額、基礎退職均等割額、基礎退職年税額、基礎退職減免額、基礎退職納付額

支援所得割額、支援均等割額、支援年税額、支援減免額、支援納付額

支援退職所得割額、支援退職均等割額、支援退職年税額、支援退職減免額、支援退職納付額

介護所得割額、介護均等割額、介護年税額、介護減免額、介護納付額

介護退職所得割額、介護退職均等割額、介護退職年税額、介護退職減免額、介護退職納付額

期別賦課情報(月期別の賦課情報)

賦課被保情報(賦課時点の月別資格情報)

国保所得情報

減免情報 軽減情報

年金受給者情報 年金連携情報 年金連携履歴情報 仮徴収情報

<給付記録情報>

宛名番号 記号番号 記号番号ごとの枝番(個人を識別する2桁の番号)

給付記録番号 給付種別 審査年月 診療年月

支給区分 支給決定日 支給処理日 支給決定額

貸付額 充当額 調整額

給付記録情報 療養費支給情報

高額明細情報 若年高額支給情報 高齢高額外来支給情報 高齢高額支給情報 高額支給情報

高額療養費償還払い情報 高額該当情報 転居特例情報 世帯所得区分情報

出産育児葬祭費情報

減額認定証情報 結核精神証情報 特定疾病証情報

不当利得情報 第三者行為情報

差額支給情報 貸付情報 償還払い情報

高額介護合算情報

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		
国民健康保険ファイル		
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	＜国保連合会以外からの入手＞ ・対象者以外の情報を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他市町村から情報を入手する際は対象者以外の情報を入手してしまうことがないよう、事務マニュアルを整備して処理の標準化を図る。 ・マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。 ＜国保連合会からの入手＞ ・国保総合PCにおける措置 ・入手元は、国保連合会の国保総合(国保集約)システムに限定されており、配信されるデータは国保連合会において、関連性や妥当性および整合性のチェック(*)が行われていることが前提となるため、対象者以外の情報を入手することはない。 ・国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことにより、誤った対象者に関する特定個人情報の入手を防止している。 *：ここでいう関連性・整合性チェックとは、すでに個人番号が紐付いている(宛名番号が同じ)人に、以前と異なる個人番号を紐付けようとした場合、あるいは個人番号が空白の場合に、確認リストを出力する等の機能のことを指す。	
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	＜国保連合会以外からの入手＞ ・必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他の市町村から情報を入手する際は必要な情報以外を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。 ・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。 ＜国保連合会からの入手＞ ・国保総合PCにおける措置 ・入手元は、国保連合会の国保総合(国保集約)システムに限定されており、配信されるデータは国保連合会においてあらかじめ指定されたインタフェース(*)によって配信されることが前提となるため、必要な情報以外を入手することはない。 *：ここでいう指定されたインタフェースとは、国保総合(国保集約)システムの外部インタフェース仕様書に記載されている国保連合会の国保総合(国保集約)システムと市区町村に設置する国保総合PCとの間でやりとりされるデータ定義のことをいい、その定義に従った項目(法令等で定められた範囲)でないと、国保連合会の国保総合(国保集約)システムからデータ配信ができないしくみになっている。	
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	＜国保連合会以外からの入手＞ ・申請者より情報を入手する際はその相手方へ、収集する情報の使用目的及び用途について説明書類を用い十分説明する。庁内連携により入手する場合は庁内連携システムを通じて行うが、権限を持った者しか情報照会を行えず、また、その照会履歴は記録として保存される仕組みとなっている。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、後に署名検証も行われるため、本人からの情報のみが送信される。 ・サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。 ＜国保連合会からの入手＞ ・国保総合PCにおける措置 特定個人情報の入手元は、国保連合会の国保総合(国保集約)システムに限定されており、専用線を用いるとともに、指定されたインタフェース(法令で定められる範囲)でしか入手できないようシステムで制御しており国保総合(国保集約)システムの外部インタフェース仕様書に記載されている対象、周期およびデータ定義等によって、当区と国保連合会の双方に共通の認識があり、その定義に従った内容でないとデータの送受信ができないことで、不適切な方法で入手が行われるリスクを軽減している。	
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	<国保連合会以外からの入手> ・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、本人確認を行う。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。 <国保連合会からの入手> ・国保総合PCにおける措置 ・特定個人情報の入手元は、国保連合会の国保総合(国保集約)システムに限定されているとともに、国保総合PCにおいて国保連合会から入手する情報は、当区において本人確認を行った上で国保連合会に送信した被保険者情報に、国保連合会が事務処理等を行った結果を付加して配信された情報であるため、本人確認は当区において国保連合会に送付する前に実施済みである。 ・さらに、国保連合会においても当区のシステムと同様の宛名番号をキーとして個人識別事項を管理しており、宛名番号をキーとして必要なデータが配信されることをシステム上で担保することで正確性を確保している。		
個人番号の真正性確認の措置の内容	<国保連合会以外からの入手> 個人番号カードの提示、もしくは通知カードと身分証明書の提示に加え、以前に提示された個人番号との照合により、真正性確認を行う。 <国保連合会からの入手> ・国保総合PCにおける措置 ・国保連合会から入手する特定個人情報ファイルには、個人番号は記録されていない。		
特定個人情報の正確性確保の措置の内容	<国保連合会以外からの入手> ・届出書等から特定個人情報を入力する際は、入力後に別の担当者による二重チェックを実施する。 ・個人番号だけでなく、氏名・住所・生年月日等を複合的にチェックする。 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。 <国保連合会からの入手> ・国保総合PCにおける措置 ・国保連合会から配信される被保険者情報については、当区および他市から送信された被保険者異動情報等をもとに、国保総合(国保集約)システムにおいて処理を行い、その処理結果は当区および他市の双方に配信され、当区および他市の職員が確認している。 ・国保連合会から配信される継続世帯確定結果については、当区から送信した被保険者異動情報等をもとに、国保総合(国保集約)システムにおいて処理を行い、その処理結果を当区の職員が確認している。		
その他の措置の内容	—		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク4： 入手の際に特定個人情報that漏えい・紛失するリスク		
リスクに対する措置の内容	<国保連合会以外からの入手> ・窓口では本人から直接書面を受け取ることを原則とする。 ・郵送の場合は、担当部署の所在地及び宛先を印字した専用封筒を使用するよう促す。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <国保連合会からの入手> ・当区の国保総合PCは、国保連合会のみと接続され、接続には専用線を用いる。 ・当区の国保総合PCと国保連合会の国保総合(国保集約)システムとの通信には、認証・通信内容の暗号化を実施している。 ・当区の国保総合PCと国保連合会の国保総合(国保集約)システムとの専用ネットワークは、ウィルス対策ソフトウェア、ファイアウォール等によってセキュアなシステム稼働環境を確保することにより、不適切な方法によってデータが漏えい・紛失することのリスクを軽減している。 ・ウィルス対策ソフトウェアは自動でアップデートを行うこととしており、接続拠点の追加、削除等を含め、ファイアール等の設定変更が必要となった際は、国保連合会により迅速に実施される。 ・国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことにより、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 ・国保総合PCへのログイン時の職員認証の他に、ログインを実施した職員・時刻・操作内容の記録が実施されるため、その抑止効果として、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 ・国保総合PCと既存の自庁システムとの間の情報の授受において使用する電子記録媒体については、次の措置を講じる。 ・電子記録媒体は、権限を付与された最小限の職員だけが、限られた作業場所において取扱う。 ・電子記録媒体は、媒体管理簿で管理し、保管庫に施錠保管する。 ・電子記録媒体に保存する情報は、作業が終わる都度、速やかに情報を消去する。 ・電子記録媒体を廃棄する場合は、全ての情報を消去の上、物理破壊によりデータを復元不可能な状態にする。	
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	個人番号利用業務以外から、または個人番号を必要としない業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている	
事務で使用するその他のシステムにおける措置の内容	- 事務に必要な情報はシステム内に保持しない。 - データで提出されるなどによりシステム内に保持せざるを得ない場合は、データベース上には保持するが、画面には表示しないよう制限を行う。	
その他の措置の内容	<国保総合PCにおける措置> - 市区町村の職員等が不正にデータ抽出等できないように、GUIによるデータ抽出機能(*)は国保総合PCに搭載しないことにより、個人番号利用業務以外でデータが抽出等されることはなく、事務に必要な情報との紐付けが行われるリスクを軽減している。 *:ここでいうGUIによるデータ抽出機能とは、国民健康保険関係情報ファイルのデータベースからデータを抽出するにあたって、抽出条件等を端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で国保総合PC上のハードディスク等にファイルを出力する機能のことを指す。	
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	<国保総合PC以外のPCにおける措置> - 職員証(ICカード)とパスワードの二要素によりユーザIDの認証を行う。 - ユーザIDに付与されるアクセス権限によって、業務従事者が業務に必要な範囲の特定個人情報ファイルだけにアクセスすることができるよう制御する。 - 人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。 - サービス検索・電子申請機能を LGWAN 接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 - なりすましによる不正を防止する観点から共用IDの利用を禁止する。 <国保総合PCにおける措置> - 国保総合PCを利用する必要がある事務取扱担当者を特定し、個人ごとにユーザIDを割り当てるとともに、パスワードによるユーザ認証を実施する。 - なりすましによる不正を防止する観点から、共用IDの発行は禁止している。 - 国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことにより、特定個人情報が不正に使用されることリスクを軽減している。 - ログインしたまま端末を放置せず、離席時にはログアウトすることやログインID、パスワードの使い回しをしないことを徹底している。 - パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。
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	- 発効管理: 人事異動があった場合等には、速やかに発効処理を行う。 - 失効管理: 人事異動があった場合等には、速やかに失効処理を行う。 ※発効、失効いずれの場合も、発効・失効作業を行った者以外の他の者が二重チェックを行い、正しく登録・削除されているかを確認する。 - サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ① 発効の管理 ・アクセス権限が必要となった場合、ユーザID管理者が事務に必要な情報にアクセスできるユーザIDを発効する。 ・ユーザID管理者が各事務に必要なアクセス権限の管理表を作成する。 ・アクセス権限の付与を必要最低限とする。 ② 失効の管理 ・定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。
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	不特定多数が利用できるようなIDは発行せず、業務上の必要な範囲に対してユーザIDを発行する。 定期的にユーザID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザID管理者が確認を行う。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。

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	<国保総合PC以外のPCにおける措置> ・誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。 ・特定個人情報のアクセスログについて、年1回以上随時分析し、業務時間帯以外のアクセス、業務上想定されない頻度のアクセスの有無がないか確認する。分析の結果は、情報システム管理者に報告する。 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。 <国保総合PCにおける措置> ・国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容を記録している。 ・情報システム管理者は定期的又はセキュリティ上の問題が発生した際に、記録の内容と関連する書面の記録を照合して確認し、不正な運用が行われていないかを監査する。 ・当該記録については、一定期間保存することとしている。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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		定期的実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。	
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		<国保総合PC以外のPCにおける措置> ・通常ユーザ用と管理者用とにアクセス権限を分け、システムのバックアップデータ等の重要データには管理者権限のみがアクセスできるようにする。 ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ・アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、LGWAN 接続端末への保存や外部記憶媒体への書き出し等ができるよう系統的に制御する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。 <国保総合PCにおける措置> ・市区町村の職員等が不正にデータ抽出等できないように、GUIによるデータ抽出機能は国保総合PCに搭載しないことにより、個人番号利用事務以外でデータが抽出等されることはない。 ・国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容が記録され、国保連合会においても定期的又はセキュリティ上の問題が発生した際に、記録の内容を確認し、不正な運用が行われていないかが監査される。 ・国保総合PCと既存の自庁システムとの間の情報の授受において使用する電子記録媒体については、次の措置を講じる。 ・電子記録媒体は、権限を付与された最小限の職員だけが、限られた作業場所において取扱う。 ・電子記録媒体は、媒体管理簿で管理し、保管庫に施錠保管する。 ・電子記録媒体に保存する情報は、作業が終わる都度、速やかに情報を消去する。 ・電子記録媒体を廃棄する場合は、全ての情報を消去の上、物理破壊によりデータを復元不可能な状態にする。	
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			
—			

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	<SKY2国民健康保険システムの保守・運用委託> <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> 委託契約書において、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ている。 (1) 情報セキュリティ及び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 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所 ② 委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所 ③ 委託業務に関する緊急時連絡先一覧 (3) 委託業務に係る実施スケジュールを明記した文書 <上記以外の委託> 当区の情報セキュリティ対策基準に基づき、委託先において個人情報が適正に管理されているかどうかを以下の観点で確認する。 ・個人情報の管理的な保護措置(個人情報取扱規定、体制の整備等) ・個人情報の物理的保護措置(人的安全管理、施設および設備の整備、データ管理、バックアップ等) ・個人情報の技術的保護措置(アクセス制御、アクセス監視やアクセス記録等) ・委託内容に応じた情報セキュリティ対策が確保されること ・プライバシーマーク、情報セキュリティマネジメントシステム(ISO27001)の国際規格の認証取得情報	
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	<SKY2国民健康保険システムの保守・運用委託> ・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。 <市区町村保険者事務共同処理業務> ・当区の情報セキュリティ対策基準に基づき、委託契約書には「委託先の責任者、委託内容、作業場所、作業場所の特定」を明記することとしている。 ・また、アクセス権限を付与する従業員数を必要最小限に制限し、付与するアクセス権限も必要最小限とすることを委託事業者に遵守させることとしている。 ・さらに、委託事務の定期報告および緊急時報告義務を委託契約書に明記し、アクセス権限の管理状況を定期的に報告させることとしている。 <医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> ・取りまとめ機関の職員に許可された業務メニューのみ表示するよう医療保険者等向け中間サーバー等で制御している。 ・運用管理要領等にアクセス権限と事務の対応表を規定し、職員と臨時職員、取りまとめ機関と委託事業者の所属の別等により、実施できる事務の範囲を限定している。 ・アクセス権限と事務の対応表は随時見直しを行う。 ・パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。 <国保総合(国保集約)システムのクラウド移行作業時に関する措置> ・データ抽出・テストデータ生成及びデータ投入に関する作業時には、委託先の責任者が特定個人情報ファイルの取扱権限を持つIDを発効するが、当該IDの権限及び数は必要最小限とし、作業者は範囲を超えた操作が行えないようシステムの制御することを委託先に遵守させることとしている。 ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている。 <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・委託先に従事者名簿を提出させ、閲覧・更新権限のIDを付与する者を必要最小限とする。 ・自己が利用しているIDは、他人に利用させない(IDの共用を指定されている場合は除く。) ・共用IDを利用する場合は、共用IDの利用者以外の者に利用させない。 ・パスワードを秘密にし、パスワードの照会等には一切応じない(パスワード発行業務を除く。) ・パスワードのメモの不用意な作成等により、パスワード流出の機会を作らない。 ・パスワードは、十分な長さとし、想像し難い文字列とする。 ・複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しない。 ・パソコン等のパスワードの記憶機能を利用しない。 ・社員間でパスワードを共有しない(IDの共用を指定されている場合を除く。)。	

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	<SKY2国民健康保険システムの保守・運用委託> ・通常業務における端末からの情報照会・更新については、作業端末へのログイン記録を残している。 ・システム保守作業については、作業内容の記録を提出させている。 ・電子記録媒体等については、管理簿を作成し、引渡し及び返却を管理する。 <市区町村保険者事務共同処理業務> ・委託先の従業員等が当区の国民健康保険に関する被保険者等の個人番号を閲覧等した場合には、国保連合会の国保総合(国保集約)システムにおいて、特定個人情報にアクセスした従業員等・時刻・操作内容を記録することとしている。 ・国保連合会の特定個人情報保護責任者は、定期的にまたはセキュリティ上の問題が発生した際に当該記録の内容と関連する書面の記録を照合して確認し、不正な運用が行われていないかを監査する。 ・当区の情報セキュリティ管理者は、委託契約に基づき、委託先に当該記録の開示を請求し、調査することで操作者個人を特定する。 ・記録の保存期間については、当区の公文書管理規則第12条に従って、一定期間保存する。 <医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> ・操作ログを中間サーバーで記録している。 ・操作ログは、セキュリティ上の問題が発生した際、又は必要なタイミングでチェックを行う。 <国保総合(国保集約)システムのクラウド移行作業時に関する措置> ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 ・移行作業にあたって、作業員以外を対象ファイルにアクセスできないようにし、リスク範囲を限定することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとしている。 ・特定個人情報ファイルにアクセスする移行作業は二人で行う相互牽制の体制で実施することを委託先に遵守させることとしている。 ・移行作業に関しては定期的にログをチェックし、データ抽出等の不正な持ち出しが行われていないか監視することを委託先に遵守させることとしている。 <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> 事務用パソコン及び業務パソコンの利用作業について、それぞれログイン状況(アクセスログ)を記録して残している。
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	<SKY2国民健康保険システムの保守・運用委託> <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・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、情報セキュリティに関する教育の実施等を義務づけている。 <資格継続業務、高額該当回数を引き継ぎ業務に関する保険者事務共同処理業務> ・当区の情報セキュリティ対策基準に基づき、委託先は、特定個人情報の目的外利用および第三者に提供してはならないこと、特定個人情報の複写、複製、またはこれらに類する行為をすることはできないことなどについて委託契約書に明記する。 ・また、委託先においても個人情報の漏えい、滅失または毀損の防止を義務付けするとともに、当区の情報セキュリティ管理者が委託契約に基づき、必要があるときは委託先に対して調査を行い、または報告を求める。 <医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> ・契約書において当区が保有する個人情報を第三者に漏らしてはならない旨を定めており、委託先から他者への特定個人情報の提供を認めていない。 ・定期的に操作ログをチェックし、データ抽出等の不正な持ち出しが行われていないか監査する。

	委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	<SKY2国民健康保険システムの保守・運用委託> <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・委託契約書において、以下の事項を義務づけている。 (1)区より特定個人情報を含む情報資産を受領した場合、区に対して受領証を提出すること。 (2)区より受領した情報資産を適切に管理するため、情報資産の受領記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を提示すること。 (3)委託業務が完了したときは、区より受領した情報資産を速やかに区に返却すること。返却が不可能な情報資産は区の下承のもと、バックアップデータを含め、情報及び情報資産を復元できないように処置した上で廃棄すること。 ・区は、委託先へ特定個人情報を含む情報資産を提供(引渡し)した場合は、所定の記録簿に記載するとともに、事後、所属長が確認することとしている。 <市区町村保険者事務共同処理業務> ・当区の情報セキュリティ対策基準に基づき、委託契約書において、委託業務の定期報告および緊急時報告を義務付けし、特定個人情報の取扱いに関して定期的に委託先から書面にて報告を受けることとしている。 ・当区から国保連合会への特定個人情報の送付に関しては、国保総合PCで送付を行った際に送付記録を帳簿に記入している。 ・記録の保存期間については、当区の公文書管理規則第12条に従い、一定期間保存する。 ・特定個人情報等の貸与に関しては、外部提供する場合に必要な応じてパスワードの設定を行うこと、および管理者の許可を得ることを遵守するとともに、委託終了時の返還・廃棄について委託契約書に明記することとしている。 ・さらに、当区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは調査を行い、または報告を求める。 <医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> ・提供情報は、業務委託完了時にすべて返却又は消去する。 ・定期的に操作ログをチェックし、データ抽出等の不正な持ち出しが行われていないか監査する。
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
	ルール内容及びルール遵守の確認方法	<SKY2国民健康保険システムの保守・運用委託> ・業務完了後にデータ削除を行い、削除証明書を提出させる。 ・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、情報セキュリティに関する教育の実施等を義務づけている。 <資格継続業務、高額該当回数等の引継ぎ業務に関する保険者事務共同処理業務> ・特定個人情報等は、業務完了後は速やかに返還し、または漏えいを起こさない方法によって確実に消去、または処分することを、委託契約書に明記することとしている。 ・委託契約終了後は、委託先から特定個人情報等の消去・廃棄等に関する報告書を提出させ、当区の情報システム管理者が消去および廃棄状況を確認する。 <クラウド移行作業時に関する措置> ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 <SKY2国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・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、情報セキュリティに関する教育の実施等を義務づけている。 ・加入・脱退等の申請データをダウンロードしたのち、入力処理や点検作業終了後、問題がなければ適切なタイミングでデータの削除を行う。 ・ダウンロードデータや入力情報を紙に出力した場合は、必要な点検作業の終了後、区に引き渡し、区が廃棄することとしている。

		・運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、開発者及び運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化等)をどのように確保したかを書面にて示した上で、許諾を得ること。 <国保総合(国保集約)システムのクラウド移行作業時に関する措置> ・データ抽出・テストデータ生成及びデータ投入に関する作業者には、委託先の責任者が特定個人情報ファイルの取扱権限を持つIDを発効するが、当該IDの権限及び数は必要最小限とし、作業者は範囲を超えた操作が行えないようシステム的に制御することを委託先に遵守させることとしている。 ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとしている。 ・特定個人情報ファイルにアクセスする移行作業は二人で行う相互牽制の体制で実施することを委託先に遵守させることとしている。 ・移行作業に関しては定期的にログをチェックし、データ抽出等の不正な持ち出しが行われていないか監視することを委託先に遵守させることとしている。
--	--	---

その他の措置の内容	—		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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			
<国保連合会における措置> ・国保総合(国保集約)システムにおいて保有する特定個人情報、インターネットに流出することを防止するため、国保総合(国保集約)システムはインターネットには接続できないようシステム面の措置を講じている。 ・国保総合(国保集約)システムではUTM(コンピュータウイルスやハッキング等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、侵入検知および侵入防止を行うとともに、ログの解析を行う。 ・国保総合(国保集約)システムでは、ウイルス対策ソフトウェアを導入し、パターンファイルの更新を行う。 ・導入しているOSおよびミドルウェアについて、必要なセキュリティパッチの適用を行う。 ・国保総合(国保集約)システムのデータベースに直接アクセスできる端末を連合会の管理区域に設置し、設置場所への入退室記録管理、監視カメラによる監視および施錠管理を行う。 ・特定個人情報等を取扱う機器、電子媒体および書類等の盗難または紛失等を防止するために、物理的な安全管理措置を講ずる。 ・国保総合(国保集約)システムを使用して特定個人情報ファイルの複製等の操作が可能な職員を最小限に限定する。 ・特定個人情報ファイルを電子記録媒体に複製する際には、不必要な複製を制限するため、事前に特定個人情報保護責任者(連合会)の承認を得る。 ・許可された電子記録媒体または機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。 ・電子記録媒体は、媒体管理簿で管理し、保管庫に施錠保管する。電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。保管する必要がない使用済の電子記録媒体はシュレッダーで粉砕し破棄する。 <取りまとめ機関における措置> ・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護保護評価書を実施している。			

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	[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	移転は庁内ネットワークや庁内システム間連携のみであり、連携時のログ、アクセスログ等により記録する。		
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない	
ルール内容及びルール遵守の確認方法	番号法および条例の規定により、認められる範囲の特定個人情報の移転について、規定の範囲内において特定個人情報の提供を行う。		
その他の措置の内容	設置された端末では、権限を持った職員の許可がなければ情報の取り出しができないようにしている。		
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	・情報の移転については、移転の記録が残る庁内連携システムを通して行うことで、不適切な移転を防止する。 ・他市区町村への情報提供については、情報提供ネットワーク接続用の端末でしか操作できず、また権限を持った職員しか操作できない仕組みとしている。		
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： 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	・庁内連携では、番号法及び条例にて規定された部署のみ照会可能となっている。 ・庁内連携では、本業務で保有する情報をすべて連携することは行わず、限定された情報のみ照会対象としている。		
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	<世田谷区における措置> ・番号法の規定に基づき、認められている範囲内において特定個人情報の照会を行う。 <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会リスト(※2)との照会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ほかに、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 3) 課題が残されている	2) 十分である
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、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。 <中間サーバーの運用における措置> ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法及び条例上認められる提供以外は受け付けないようにしており、システム上提供が認められなかった場合においても記録を残し、提供記録は7年分保管する。		
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 3) 課題が残されている	2) 十分である
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	<世田谷区における措置> ・入手した特定個人情報について、SKY2国民健康保険システム内の情報と突合を行い、真正性及び正確性確認を行う。また、別途、届出または申告時には、その都度、届出などの内容と突合を行い、特定個人情報の正確性確認を行う。 <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、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 3) 課題が残されている	2) 十分である

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できない。 ＜中間サーバーの運用における措置＞ ・情報照会、情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報が漏えい・紛失することを防止する。	
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、中間サーバーにも格納して、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。 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。 (※)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。 ＜中間サーバーの運用における措置＞ ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法及び条例上認められる提供以外は受け付けないようにしており、システム上提供が認められなかった場合においても記録を残し、提供記録は7年分保管する。	
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

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保守・運用を行う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。 ＜中間サーバーの運用における措置＞ ・情報照会、情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報がやりとりされることを防止する。	
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	＜世田谷区における措置＞ ・庁内連携システムでは本業務で保有する情報をすべて連携することは行わず、番号法の規定及び条例に基づき認められる情報のみを提供する仕組みとしている。 ＜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。 (※)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保守・運用を行う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	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退館管理：ICカード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 ④LGWAN 接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ⑤外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 <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。	

⑥技術的対策	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 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	<世田谷区における措置> ・SKY2国民健康保険システムへのアクセス時におけるICカード＋パスワード認証 ・ウィルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・LGWAN 接続端末へのウィルス検出ソフトウェア等の導入により、ウィルス定義ファイルの定期的な更新及びウィルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <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、ウィ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情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <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、ウィ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。 <国保総合(国保集約)システムにおける措置> ・区市町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。 ・国保総合PCで利用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。 ・国保総合PCには、ウィルス対策ソフトウェアを導入し、ウィルスパターンファイルは適時更新する。 ・不正アクセス防止策として、ファイアウォールを導入している。 ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。
⑦バックアップ	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている] <選択肢> 1) 特に力を入れて行っている 2) 十分にやっている 3) 十分にやっていない

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	住民記録システムの宛名と連動しており、生存者と同様の管理がなされている	
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: 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	<世田谷区における措置> 被保険者情報については、随時、本人確認を行い、変更があればその都度データを修正する。 ・LGWAN 接続端末は、基本的には、個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。 <国保総合(国保集約)システムにおける措置> ・国保総合PCに登録した情報はサーバにのみ保存され、国保総合PCの端末に保存されることはなく国保総合PCの端末から国保総合(国保集約)システムの個人番号(特定個人情報ファイル)を操作することはできない仕組みとしている。 国保総合PCに登録した情報については被保険者の住所異動等が発生する都度更新しているため、特定個人情報が古い情報のまま保管され続けるリスクはない。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めていない]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	<世田谷区における措置> データ保管期間の定めはないため、消去は行っていない。上で述べたリスク対策のもと、データを保管する。 ・LGWAN 接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。 ・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。 <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 SP800-88、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。 <国保総合(国保集約)システムの保管・消去> ・国保総合PCにおける措置 ・登録された情報は国保総合PCに保管されるデータはなく、国保総合PCからは、国保総合(国保集約)システムの個人番号(特定個人情報ファイル)を操作することはできないため、特定個人情報が消去されずいつまでも存在するリスクはない。	

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			
＜世田谷区における措置＞ サーバ、端末（パソコン）、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。機器リース終了による返却の場合も、同様とする。 ・紙文書は、溶解またはシュレッダー処分を行う。 ・電磁的な記録媒体は、破碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行った上で廃棄する。 ・サーバ、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによるデータ消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。			
＜取りまとめ機関における措置＞ ・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務（オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供）」の特定個人情報保護評価を実施している。			

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分にを行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にを行っている 3) 十分に行っていない
	具体的なチェック方法	<世田谷区における措置> ・実際の運用が評価書記載の内容と合致しているかについて、定期的にチェックを行う。 <中間サーバー・プラットフォームにおける措置> ・運用規則に基づき、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	[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) 十分に行っている 3) 十分に行っていない
	具体的な内容	<世田谷区における措置> 適正な個人情報の保護やリスク対策を図るため、監査計画を策定し、定期的及び必要に応じて随時、内部監査を実施し、監査の結果を踏まえて必要な改善を行う。監査に当たっては、以下の観点から実施する。 ・ 評価書記載事項と運用実態のチェック ・ 個人情報保護に関する規程・体制整備 ・ 個人情報保護に関する人的安全管理措置 ・ 安全管理措置の周知・教育 ・ 個人情報保護に関する技術的安全管理措置 <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。 <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、定期的に監査を実施することとしている。 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。 <国保総合(国保集約)システム> ・「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)」第29条の3第2項による個人情報保護委員会への特定個人情報ファイルの取扱いの状況に関する報告(それに伴い、国保連合会にも同様の報告を求めることにする)。

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) 十分に行っていない
具体的な方法	<世田谷区における措置> ①職員が番号制度に関する基礎的事項を常時確認できるよう、研修資料を庁内公開している。また、研修資料は毎年度見直しを実施している。 ②研修終了後に受講者アンケートを実施し、説明内容の理解度を測るほか、次回以降の研修資料等の見直しに活用する。 ③委託先事業者の従業者については、契約時の仕様書に個人情報保護遵守を明記し、委託先事業者の責任者の責において、研修・指導を行わせる。必要に応じて、研修資料等を提供させ、実効性を担保する。 ④違反行為を行った者に対しては、指導を行う。違反行為の程度によっては、懲戒の対象となりうる。また、全従業者に対して、違反事項発生を周知し、再発防止を徹底する。 <中間サーバー・プラットフォームにおける措置> ①IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、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、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。 <国保総合(国保集約)システムに関する教育・啓発> ・教育事項: 国保総合(国保集約)システムの操作・運用ならびに個人情報保護に関する教育および研修 ・教育頻度: 年間1回程度 ・教育方法: 集合教育 ・教育対象: 職員および嘱託員 <サイバーセキュリティに関する国保連合会での教育・啓発> ・教育事項: 特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威および当該脅威による被害の発生または拡大を防止するため必要な措置に関するものを含むもの ・教育頻度: おおむね一年ごと ・教育方法: 未定 ・教育対象: 特定個人情報ファイルを取り扱う事務に従事する者 ・違反行為に対する措置: 違反行為を行ったものに対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。 ・委託先である国保連合会に対しては、契約内容において、個人情報保護に関する秘密保持契約を締結している。 ・教育の未受講者に対しては、再受講の機会を付与している。 *「個人情報の保護に関する法律およ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の一部を改正する法律の一部の施行に伴う関係政令の整備に関する政令(平成27年政令第427号)」によるもの。	

3. その他のリスク対策

＜世田谷区における措置＞

・世田谷区行政手続における特定個人を識別するための番号の利用等に関する条例第7条及び同条例施行規則第6条の規定に基づき、マイナンバー制度セキュリティ会議を設置し、特定個人情報ファイルの取扱いに関する企画及び運用計画、セキュリティ対策等を審議する。

＜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。

＜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。

②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。

＜取りまとめ機関における措置＞

・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。

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	郵便番号154-8504 東京都世田谷区世田谷4-21-27 世田谷区総務部区政情報課区政情報係
②請求方法	指定様式による書面の提出により、開示・訂正・利用停止請求を受け付ける。
特記事項	区ホームページ上に、請求先、請求方法、諸費用等について掲載する。
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	国民健康保険ファイル
公表場所	区政情報センター、区ホームページ
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	世田谷区保健福祉政策部国保・年金課 電話03-5432-2330
②対応方法	電話による対応を受付ける

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和8年8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	以下のとおり、区民意見募集を行う。 ・区ホームページに掲載する。 ・国民健康保険窓口にて、「特定個人情報保護評価書」全文を閲覧できるようにする。
②実施日・期間	令和8年 月 日(火)～令和8年 月 日(水)(30日間)
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28日
②方法	世田谷区情報公開・個人情報保護審議会による点検
③結果	異議なし
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7年3月15日	Ⅰ 基本情報－1 特定個人情報 ファイルを取り扱う事務－② 事務の内容	国民健康保険法に基づき以下の事務を行う。 ①社会保険離脱や転出入、または、出生死亡等様々な資格異動に伴う被 保険者資格の取得喪失の認定 ②所得を元に軽減等の要件を適用した上での保険料計算及び賦課 ③医療機関等からのレセプトの審査および医療機関等への保険者負担分 の支払い業務 ④出産育児一時金および葬祭費の支給ならびに第三者行為による損害賠 償金の請求 ⑤国民健康保険加入者を対象とした特定健康診査及びその結果に基づく 指導 ⑥国民健康保険制度の趣旨普及 ⑦オンライン資格確認等システムに係る資格履歴管理事務 ⑧オンライン資格確認等システムに係る機関別符号の取得等事務	国民健康保険法に基づき以下の事務を行う。 ①社会保険離脱や転出入、または、出生死亡等様々な資格異動に伴う被保険者 資格の取得喪失の認定 ②所得を元に軽減等の要件を適用した上での保険料計算及び賦課 ③医療機関等からのレセプトの審査および医療機関等への保険者負担分の支払 い業務 ④出産育児一時金および葬祭費の支給ならびに第三者行為による損害賠償金の 請求 ⑤国民健康保険加入者を対象とした特定健康診査及びその結果に基づく指導 ⑥国民健康保険制度の趣旨普及 ⑦サービス検索・電子申請機能での受領 ⑧オンライン資格確認等システムに係る資格履歴管理事務 ⑨オンライン資格確認等システムに係る機関別符号の取得等事務	事後	
令和7年3月15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	①資格得喪に関わる情報を記録する機能 ②医療証等の発行、発行履歴を記録する機能 ③保険料の賦課計算を行う機能及び賦課情報を記録する機能 ④給付情報の記録または高額療養費支給ならびに出産葬祭費支給を行う 機能 ⑤各情報を照会に応じて表示する機能	①資格得喪に関わる情報を記録する機能 ②資格確認書等・医療証等の発行、発行履歴を記録する機能 ③保険料の賦課計算を行う機能及び賦課情報を記録する機能 ④給付情報の記録または高額療養費支給ならびに出産葬祭費支給を行う機能 ⑤各情報を照会に応じて表示する機能	事後	
令和7年3月15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 6	—	「サービス検索・電子申請機能」を追加	事後	
令和7年3月15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－②法令上の根拠 ※法令上の根拠に関する各項 目含む	—	番号法の改正に伴う修正	事後	
令和7年3月15日	(別添 1) 事務の内容	—	図に紙申請又は電子申請（びったりサービス）を追記 図に資格確認書等を追記	事後	

令和7年3月15日	(別添1) 事務の内容 ※他シート各項目含む	—	資格確認書等を追記	事後	
令和7年3月15日	II 特定個人情報ファイルの概要－3 特定個人情報の入手・仕様－②入手方法	紙・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	紙・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 (サービス検索・電子申請機能)	事後	
令和7年3月15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－委託の有無	5件	6件	事前	
令和7年3月15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6	—	「S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等」を追加	事前	
令和7年3月15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	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理：I C カード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、D R タグによる媒体管理 申請書及び届出書等の紙媒体は、鍵のかかるロッカーや保管庫に保管している。	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理：I C カード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、D R タグによる媒体管理 申請書及び届出書等の紙媒体、及び外部記録媒体は、鍵のかかるロッカーや保管庫に保管している。	事後	
令和7年3月15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	<世田谷区における措置> ①データベースに記録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。	<世田谷区における措置> ①データベースに記録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。 ③外部記憶媒体に一時的に記録した特定個人情報等の申請データは、使用の都度速やかに完全消去する。	事後	

令和7年3月15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－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	<国保連合会以外からの入手> ・対象者以外の情報を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他市町村から情報を入手する際は対象者以外の情報を入手してしまうことがないよう、事務マニュアルを整備して処理の標準化を図る。	<国保連合会以外からの入手> ・対象者以外の情報を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他市町村から情報を入手する際は対象者以外の情報を入手してしまうことがないよう、事務マニュアルを整備して処理の標準化を図る。 ・マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。	事後	
令和7年3月15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－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	<国保連合会以外からの入手> ・必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他の市町村から情報を入手する際は必要な情報以外を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。	<国保連合会以外からの入手> ・必要な情報以外を誤って記載することがないよう、記入例等の案内書類を工夫する。また、他の市町村から情報を入手する際は必要な情報以外を入手してしまうことがないよう、事務マニュアルを整備し処理の標準化を図る。 ・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。	事後	
令和7年3月15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－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	<国保連合会以外からの入手> ・申請者より情報を入手する際はその相手方へ、収集する情報の使用目的及び用途について説明書類を用い十分説明する。庁内連携により入手する場合は庁内連携システムを通じて行うが、権限を持った者しか情報照会を行えず、また、その照会履歴は記録として保存される仕組みとなっている。	<国保連合会以外からの入手> ・申請者より情報を入手する際はその相手方へ、収集する情報の使用目的及び用途について説明書類を用い十分説明する。庁内連携により入手する場合は庁内連携システムを通じて行うが、権限を持った者しか情報照会を行えず、また、その照会履歴は記録として保存される仕組みとなっている。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、後に署名検証も行われるため、本人からの情報のみが送信される。 ・サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。	事後	

令和7年3月15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不適切な方法で入手が行われるリスク－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	<国保連合会以外からの入手> ・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、本人確認を行う。	<国保連合会以外からの入手> ・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、本人確認を行う。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証（有効性確認、改ざん検知等）を実施することとなる。これにより、本人確認を実施する。	事後	
令和7年3月15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不適切な方法で入手が行われるリスク－３入手した特定個人情報が不正確であるリスク－特定個人情報の正確性確保の措置の内容	<国保連合会以外からの入手> ・届出書等から特定個人情報を入力する際は、入力後に別の担当者による二重チェックを実施する。 ・個人番号だけでなく、氏名・住所・生年月日等を複合的にチェックする。	<国保連合会以外からの入手> ・届出書等から特定個人情報を入力する際は、入力後に別の担当者による二重チェックを実施する。 ・個人番号だけでなく、氏名・住所・生年月日等を複合的にチェックする。 ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	事後	
令和7年3月15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不適切な方法で入手が行われるリスク－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	<国保連合会以外からの入手> ・窓口では本人から直接書面を受け取ることを原則とする。 ・郵送の場合は、担当部署の所在地及び宛先を印字した専用封筒を使用するよう促す。	<国保連合会以外からの入手> ・窓口では本人から直接書面を受け取ることを原則とする。 ・郵送の場合は、担当部署の所在地及び宛先を印字した専用封筒を使用するよう促す。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事後	
令和7年3月15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－２権限のない（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－具体的な管理方法	<国保総合PC以外のPCにおける措置> ・職員証（ＩＣカード）とパスワードの二要素によりユーザＩＤの認証を行う。 ・ユーザＩＤに付与されるアクセス権限によって、業務従事者が業務に必要な範囲の特定個人情報ファイルだけにアクセスすることができるように制御する。 ・人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。	<国保総合PC以外のPCにおける措置> ・職員証（ＩＣカード）とパスワードの二要素によりユーザＩＤの認証を行う。 ・ユーザＩＤに付与されるアクセス権限によって、業務従事者が業務に必要な範囲の特定個人情報ファイルだけにアクセスすることができるように制御する。 ・人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。 ・サービス検索・電子申請機能を LGWAN 接続端末上で利用する必要がある場合は職員を特定できるような形でIDを付与し、IDとパスワードによる認証を行う。 ・なりすましによる不正を防止する観点から同一日の ID使い回し利用を禁止する。	事後	

令和7年3月15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－２権限のない（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－アクセス権限の発効・失効の管理－具体的な管理方法	－	・サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ① 発効の管理 ・アクセス権限が必要となった場合、ユーザID管理者が事務に必要な情報にアクセスできるユーザIDを発効する。 ・ユーザID管理者が各事務に必要なアクセス権限の管理表を作成する。 ・アクセス権限の付与を必要最低限とする。 ② 失効の管理 ・定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。	事後	
令和7年3月15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－２権限のない（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－アクセス権限の管理－具体的な管理方法	共用IDは発行せず、個人に対してユーザIDを発行する。	不特定多数が利用できるようなIDは発行せず、業務上の必要な範囲に対してユーザIDを発行する。 ・定期的なユーザID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザID管理者が確認を行う。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。	事後	
令和7年3月15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－２権限のない（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－特定個人情報の使用の記録－具体的な方法	<国保総合PC以外のPCにおける措置> ・誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。 ・特定個人情報のアクセスログについて、年1回以上随時分析し、業務時間帯以外のアクセス、業務上想定されない頻度のアクセスの有無がないか確認する。分析の結果は、情報システム管理者に報告する。	<国保総合PC以外のPCにおける措置> ・誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。 ・特定個人情報のアクセスログについて、年1回以上随時分析し、業務時間帯以外のアクセス、業務上想定されない頻度のアクセスの有無がないか確認する。分析の結果は、情報システム管理者に報告する。 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、またID権限の紐づけは名簿等でも管理を行うことで、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。	事後	

令和7年3月15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－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	定期的を実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	定期的を実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。 ・サービス検索・電子申請機能へアクセスできる端末を制限する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。	事後	
令和7年3月15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－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	<国保総合PC以外のPCにおける措置> ・通常ユーザ用と管理者用とにアクセス権限を分け、システムのバックアップデータ等の重要データには管理者権限のみがアクセスできるようにする。	<国保総合PC以外のPCにおける措置> ・通常ユーザ用と管理者用とにアクセス権限を分け、システムのバックアップデータ等の重要データには管理者権限のみがアクセスできるようにする。 ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ・アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、LGWAN 接続端末への保存や外部記憶媒体への書き出し等ができるようシステム的に制御する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定された USB メモリ等のみを使用する。 ・外部記憶媒体内のデータは暗号化する。	事後	
令和7年3月15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－情報保護管理体制の確認	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> 委託契約書において、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ている。 (1) 情報セキュリティ及び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 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所 ② 委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所 ③ 委託業務に関する緊急時連絡先一覧 (3) 委託業務に係る実施スケジュールを明記した文書	事前	

令和7年3月15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－特定個人情報ファイルの閲覧者・更新者の制限－具体的な制限方法	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・委託先に従事者名簿を提出させ、閲覧・更新権限の I D を付与する者を必要最小限とする。 ・自己が利用しているIDは、他人に利用させない（IDの共用を指定されている場合は除く。）。 ・共用IDを利用する場合は、共用IDの利用者以外の者に利用させない。 ・パスワードを秘密にし、パスワードの照会等には一切応じない（パスワード発行業務を除く。）。 ・パスワードのメモの不用意な作成等により、パスワード流出の機会を作らない。 ・パスワードは、十分な長さとし、想像し難い文字列とする。 ・複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しない。 ・パソコン等のパスワードの記憶機能を利用しない。 ・社員間でパスワードを共有しない（IDの共用を指定されている場合を除く。）。	事前	
令和7年3月15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－特定個人情報ファイルの取扱いの記録－具体的な方法	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> 事務用パソコン及び業務パソコンの利用作業について、それぞれログイン状況（アクセスログ）を記録して残している。	事前	
令和7年3月15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－特定個人情報の提供ルール－委託先から他者への提供に関するルール内容及びルール遵守の確認方法	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・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、情報セキュリティに関する教育の実施等を義務づけている。	事前	

令和7年3月15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－特定個人情報の提供ルール－委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等 > ・委託契約書において、以下の事項を義務づけている。 (1)区より特定個人情報を含む情報資産を受領した場合、区に対して受領証を提出すること。 (2)区より受領した情報資産を適切に管理するため、情報資産の受領記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を提示すること。 (3)委託業務が完了したときは、区より受領した情報資産を速やかに区に返却すること。返却が不可能な情報資産は区の下承のもと、バックアップデータを含め、情報及び情報資産を復元できないように処置した上で廃棄すること。 ・区は、委託先へ特定個人情報を含む情報資産を提供（引渡し）した場合は、所定の記録簿に記載するとともに、事後、所属長が確認することとしている。	事前	
令和7年3月15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－特定個人情報の消去ルール－ルールの内容及びルール遵守の確認方法	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等 > ・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、情報セキュリティに関する教育の実施等を義務づけている。 ・加入・脱退等の申請データをダウンロードしたのち、入力処理や点検作業終了後、問題がなければ適切なタイミングでデータの削除を行う。 ・ダウンロードデータや入力情報を紙に出力した場合は、必要な点検作業の終了後、区に引き渡し、区が廃棄することとしている。	事前	
令和7年3月15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	—	< S K Y 2 国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等 > ・秘密保持義務・管理体制等の通知・目的外使用等及び複写等の禁止・物的セキュリティ対策・人的セキュリティ対策・技術的及び運用におけるセキュリティ対策・監査・施設への立入検査の受入れ	事前	

令和7年3月15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	—	<ＳＫＹ２国民健康保険システムへの国保の加入・脱退や非自発的失業者の保険料軽減の入力処理等> ・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るとともに、再委託先に同様の事項を遵守させることを義務づけている。	事前	
令和7年3月15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 特定個人情報ファイルの保管・消去－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	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、２４時間有人監視、監視カメラ ②入退館管理：ＩＣカード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、ＤＲタグによる媒体管理	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、２４時間有人監視、監視カメラ ②入退館管理：ＩＣカード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、ＤＲタグによる媒体管理 ④LGWAN 接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ⑤外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。	事後	
令和7年3月15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 特定個人情報ファイルの保管・消去－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	<世田谷区における措置> ・ＳＫＹ２国民健康保険システムへのアクセス時におけるＩＣカード＋パスワード認証 ・ウィルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・ウィルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク	<世田谷区における措置> ・ＳＫＹ２国民健康保険システムへのアクセス時におけるＩＣカード＋パスワード認証 ・ウィルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・LGWAN 接続端末へのウィルス検出ソフトウェア等の導入により、ウィルス定義ファイルの定期的な更新及びウィルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線である LGWAN 回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起らないようにしており、さらに通信自体も暗号化している。	事後	

令和7年3月15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 特定個人情報ファイルの保管・消去－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ーリスクに対する措置の内容	<世田谷区における措置> 被保険者情報については、随時、本人確認を行い、変更があればその都度データを修正する。	<世田谷区における措置> 被保険者情報については、随時、本人確認を行い、変更があればその都度データを修正する。 ・LGWAN 接続端末は、基本的には、個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。	事後	
令和7年3月15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 特定個人情報ファイルの保管・消去－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ー消去手順ー手順の内容	<世田谷区における措置> データ保管期間の定めはないため、消去は行っていない。上で述べたリスク対策のもと、データを保管する。	<世田谷区における措置> データ保管期間の定めはないため、消去は行っていない。上で述べたリスク対策のもと、データを保管する。 ・LGWAN 接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。 ・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。	事後	
令和7年3月15日	V 開示請求、問合せ	国民健康保険 国保資格・賦課、給付記録、高額療養費保険料充当、短期証・資格証	国民健康保険ファイル	事後	
令和7年3月15日	VI評価実施手続 1. 基礎項目評価 ①実施日	令和5年8月1日	令和6年12月1日	事後	
令和7年3月15日	VI評価実施手続 3. 第三者点検 ①実施日	令和5年10月27日、11月7日、12月15日	令和7年2月28日	事前	
令和7年8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	<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ー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された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。	<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	

令和7年8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	<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世田谷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。 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、物理的破壊により完全に消去する。	<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世田谷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	
令和7年8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 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> 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できない。	事前	
令和7年8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 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中間サーバー・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。	<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・プラットフォームの保守・運用を行う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	

令和7年8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 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 バー・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 ラットフォームの保守・運用を行う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	
令和7年8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 ⑤物理的対策 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＞ ①中間サーバー・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ー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された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。	＜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	
令和7年8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 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＞ 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。	＜中間サーバー・プラットフォームにおける措置＞ ①②③省略 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	

令和7年8月1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、定期的に監査を実施することとしている。	<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、定期的に監査を実施することとしている。 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	
令和7年8月1日	IV その他のリスク対策 3. その他のリスク対策	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。 ②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。	<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、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	

令和8年8月1日	I (別添1 事務内容)	ガバメントクラウドの範囲の記載なし	ガバメントクラウドの範囲の記載あり	事前	
令和8年8月1日	II 特定個人情報ファイルの概要 3. 特定個人情報ファイルの取扱いの委託 ①委託内容	S K Y 1 国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等	S K Y 1 国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出、ガバメントクラウドへのシステム構築・データ移行等	事前	
令和8年8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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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: 特定個人情報の漏洩・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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	

令和8年8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 洩・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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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 ⑥消去手順	<ガバメントクラウドにおける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8月1日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	<ガバメントクラウドにおける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	

改定前の特定個人情報保護評価書との相違点及び審査の観点(国民健康保険事務)

I 基本情報					
(別添1)事務の内容					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
1	21	(別添1)事務の内容	ガバメントクラウドの 範囲を明記	ガバメントクラウドの範囲を記載	ガバメントクラウドの範囲の記載なし
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					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
2	26	委託事項1 ①委託内容	ガバメントクラウド(デジタル庁調達)移行に伴い、追加する委託内容は妥当か	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出、 <u>ガバメントクラウドへのシステム構築・データ移行等</u>	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等
6. 特定個人情報の保管・消去					
3	53	①保管場所	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止:外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理:ICカード+手のひら静脈認証、要員所在管理システム ③持込・持出防止:金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 申請書及び届出書等の紙媒体、及び外部記録媒体は、鍵のかかるロッカーや保管庫に保管している。 <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。
4	53	③消去方法	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <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 SP800-88、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壊等を実施する。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> ①データベースに登録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。 ③外部記憶媒体に一時的に記録した特定個人情報等の申請データは、使用の都度速やかに完全消去する。 <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世田谷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。

Ⅷ 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					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
5	70	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(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <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。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止: 外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退館管理: ICカード+手のひら静脈認証、要員所在管理システム ③持込・持出防止: 金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 ④LGWAN 接続端末については、業務時間内のセキュリティファイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ⑤外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 <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。
6	71	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(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。))に規定する「ASP」をいう。以下同じ。又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。))は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <中間サーバー・プラットフォームにおける措置> (同右) <国保総合(国保集約)システムの保管・消去> (同右)	<世田谷区における措置> ・SKY2国民健康保険システムへのアクセス時におけるICカード+パスワード認証 ・ウイルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・LGWAN 接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起らないようにしており、さらに通信自体も暗号化している。 <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。 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、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。 <国保総合(国保集約)システムにおける措置> ・区市町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。 ・国保総合PCで使用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。 ・国保総合PCには、ウイルス対策ソフトウェアを導入し、ウイルスパターンファイルは適時更新する。 ・不正アクセス防止策として、ファイアウォールを導入している。 ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。

7	72	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(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <u><ガバメントクラウドにおける措置></u> <u>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 SP800-88、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。</u> <国保総合(国保集約)システムの保管・消去> (同右)	<世田谷区における措置> データ保管期間の定めはないため、消去は行っていない。上で述べたリスク対策のもと、データを保管する。 ・LGWAN 接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。 ・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。 <国保総合(国保集約)システムの保管・消去> ・国保総合PCにおける措置 ・登録された情報は国保総合PCに保管されるデータはなく、国保総合PCからは、国保総合(国保集約)システムの個人番号(特定個人情報ファイル)を操作することはできないため、特定個人情報が消去されずいつまでも存在するリスクはない。
---	----	---	------------------------------	--	---

IV その他のリスク対策

1. 監査					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
8	74	②監査 具体的な内容	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <u><ガバメントクラウドにおける措置></u> <u>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。</u> <中間サーバー・プラットフォームにおける措置> (同右) <国保総合(国保集約)システム> (同右)	<世田谷区における措置> 適正な個人情報の保護やリスク対策を図るため、監査計画を策定し、定期的及び必要に応じて随時、内部監査を実施し、監査の結果を踏まえて必要な改善を行う。監査に当たっては、以下の観点から実施する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規程・体制整備 ・個人情報保護に関する人的安全管理措置 ・安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 <中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を実施することとしている。 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。 <国保総合(国保集約)システム> ・「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)」第29条の3第2項による個人情報保護委員会への特定個人情報ファイルの取扱いの状況に関する報告(それに伴い、国保連合会にも同様の報告を求めることにする)。
3. その他のリスク対策					
9	76	その他のリスク対策	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <u><ガバメントクラウドにおける措置></u> <u>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。</u> <u>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。</u> <u>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。</u> <中間サーバー・プラットフォームにおける措置> (同右) <取りまとめ機関における措置> (同右)	<世田谷区における措置> ・世田谷区行政手続における特定個人を識別するための番号の利用等に関する条例第7条及び同条例施行規則第6条の規定に基づき、マイナンバー制度セキュリティ会議を設置し、特定個人情報ファイルの取扱いに関する企画及び運用計画、セキュリティ対策等を審議する。 <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リテラシー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。 ②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。 <取りまとめ機関における措置> ・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「情報提供ネットワークシステムを通じた情報照会・提供事務」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。

諮問第1012号

特定個人情報保護評価における第三者点検について
(国民健康保険 保険料収納事務)

令和8年8月7日
地域行政部マイナンバー担当課
保健福祉政策部保険料収納課

1 諮問の趣旨

(1) 特定個人情報保護評価について

特定個人情報保護評価は、「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。)に基づく番号制度の枠組みの下での制度上の保護措置の一つであり、特定個人情報ファイルを保有しようとする又は保有する場合は、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分析し、そのようなリスクを軽減するための措置を講ずること、さらにこのような措置が個人のプライバシー等の権利利益の保護措置として十分であると認められることを宣言するものである。

具体的には、行政機関の長等が評価の実施主体となり、評価対象が特定個人情報を取り扱う事務ごとに定められている。また、特定個人情報の対象人数等のしきい値によって、特定個人情報保護評価の種類が基礎項目評価・重点項目評価・全項目評価の三類型に区分され、併せて区民意見募集や第三者点検、国民への公表などの実施手続が定められている。

なお、「国民健康保険 保険料収納事務」は、しきい値判断の結果、対象者が10万人以上30万人未満かつ特定個人情報ファイルの取扱者が500人以上となることから、全項目評価の実施が義務付けられることとなる。

(2) 諮問の理由

番号法第28条の規定において、行政機関の長等は特定個人情報ファイルを保有しようとするとき又は重要な変更を加えようとするときは、特定個人情報保護評価を実施することとされている。

この度、「国民健康保険 保険料収納事務」に係る特定個人情報ファイルについて、重要な変更を加える必要が生じたため、「特定個人情報保護評価に関する規則」(以下「規則」という。)第7条第4項に基づく「特定個人情報保護評価書」(以下「評価書」という。)の第三者点検について、「世田谷区情報公開・個人情報保護審議会条例」第2条第1項第2号の規定により諮問するものである。

※審議資料No. 2-2「特定個人情報評価書作成の判断基準」及び審議資料No. 2-3「番号法における特定個人情報保護評価「全項目評価」の流れ」参照

2 諮問の内容

(1) ガバメントクラウドの利用について

審議資料No. 2-4～No. 2-6のとおり。

(2) 国民健康保険 保険料収納事務における評価書の変更の内容

特定個人情報ファイルを取り扱う現行システム(SKY2国民健康保険システム)のガバメントクラウドへの移行に伴い、評価書(全項目評価書)の記載項目のうち、「特定個人情報ファイルの取扱いの委託の有無」、「特定個人情報の保管場所」、「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」及び「その他のリスク対策」に変更が生じる。これは、規則第11条に規定される重要な変更該当するため、特定個人情報保護評価を再実施する。

3 区民意見募集

規則第7条第1項に基づき区民意見募集を実施した。結果は以下のとおり。

(1) 対象事務及び概要

国民健康保険 保険料収納事務について全項目評価書の改定案を作成し、区民意見募集を実施

(2) 期間

令和8年6月1日～同月30日の30日間実施

(3) 結果

意見0件

4 区のマイナンバー制度セキュリティ会議

本件について、令和8年7月29日開催の令和8年度第1回マイナンバー制度セキュリティ会議にて審議し、了承された。

5 第三者点検の対象

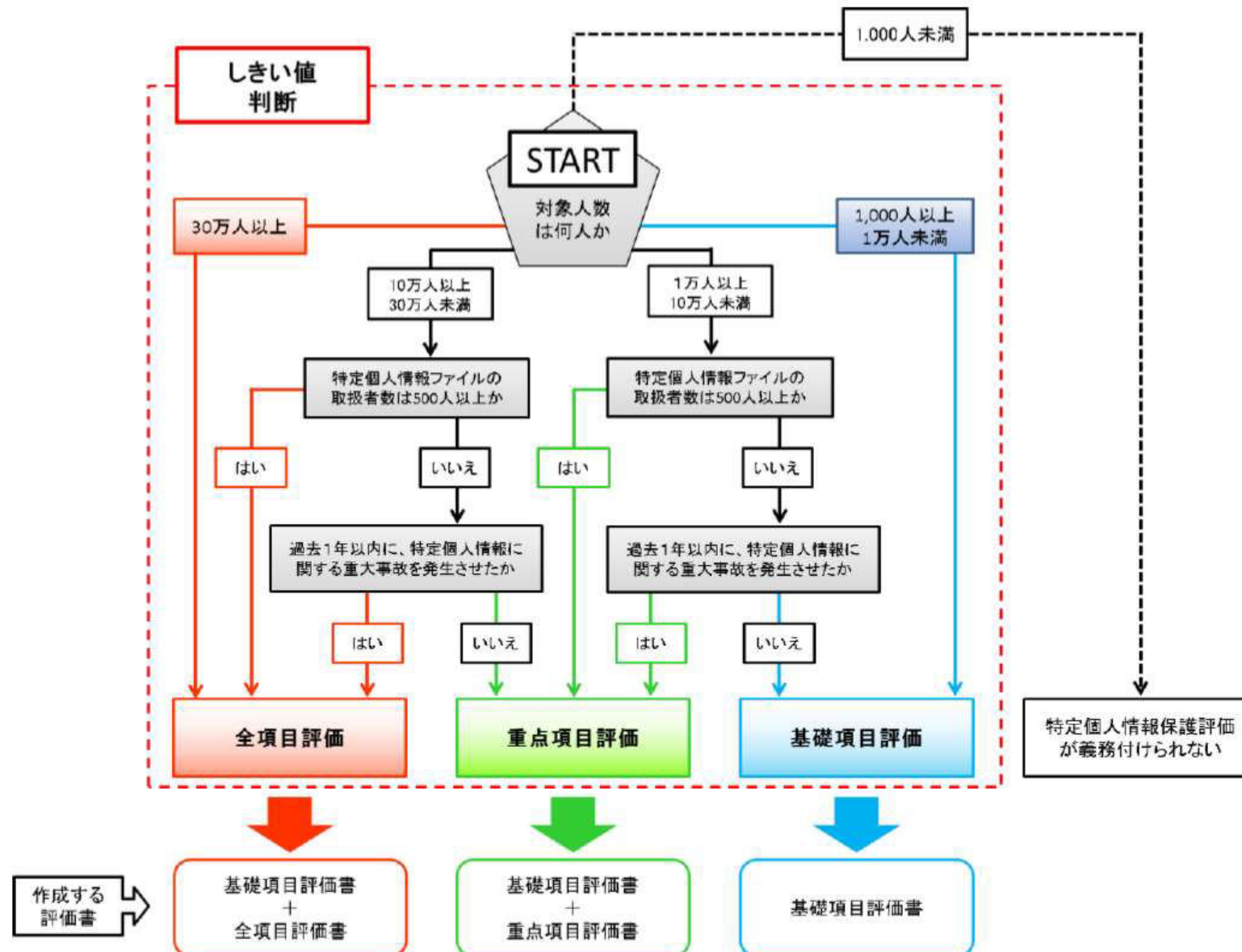
審議資料No. 2-7「特定個人情報保護評価書（全項目評価書）」のとおり。

※改定前の評価書との相違点及び審査の観点については、審議資料No. 2-8のとおり。

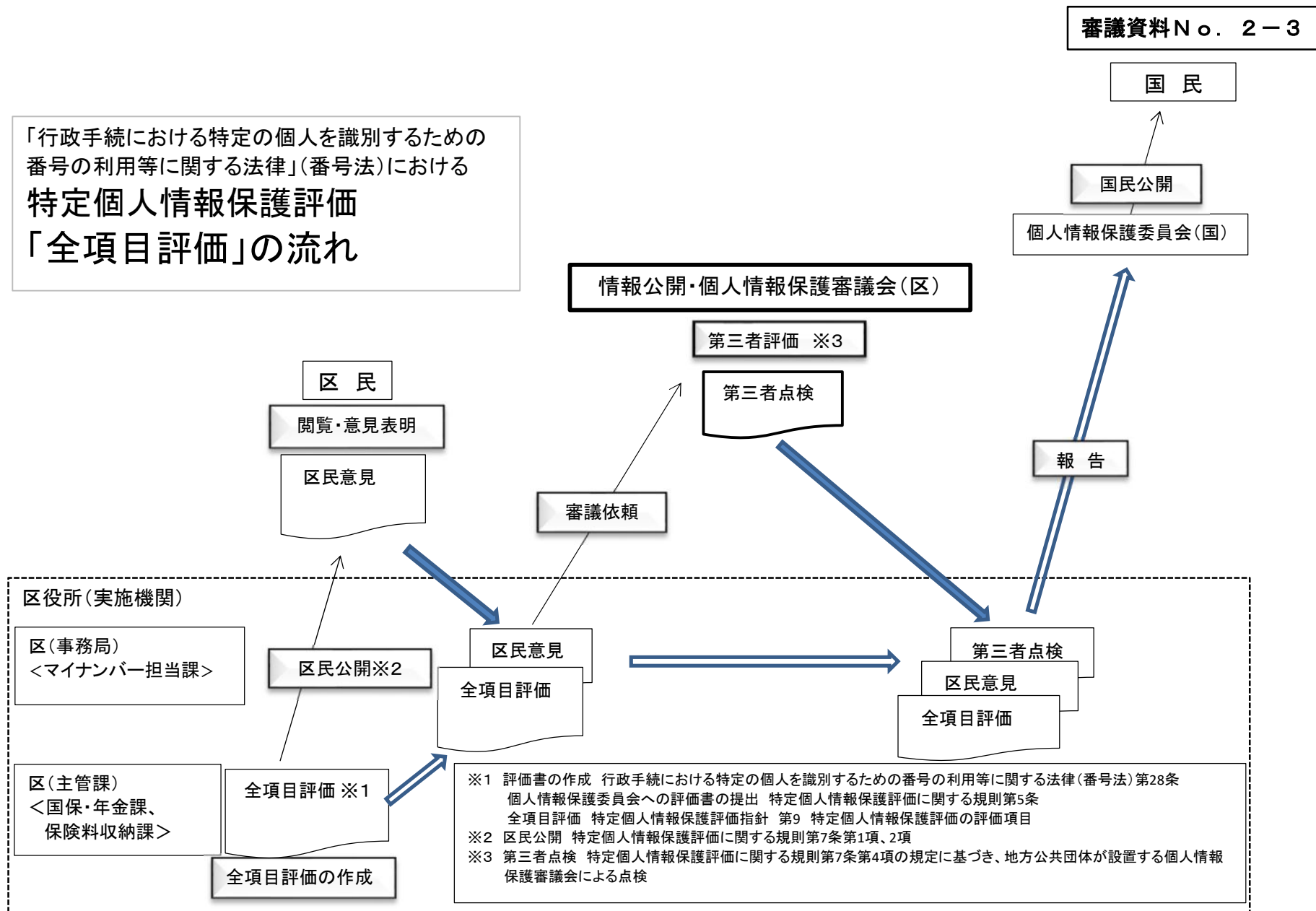
6 今後のスケジュール（予定）

令和8年12月 国の個人情報保護委員会へ評価書の提出
評価書の公表

特定個人情報評価書作成の判断基準



「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」(番号法)における
特定個人情報保護評価
「全項目評価」の流れ



ガバメントクラウド利用に伴う特定個人情報保護評価の再実施について

1 データセンターサービスの終了に伴うガバメントクラウドへの移行

「国民健康保険事務」及び「国民健康保険 保険料収納事務」に係る特定個人情報ファイルを取り扱う現行システム（以下「SKY2 国民健康保険システム」という。）は、当該システムを開発し、運用・保守業務を受託しているシステムベンダが提供するデータセンターサービス上で稼働している。当該データセンターサービスについては、令和9年3月をもってサービスの提供が終了する予定となっており、同時期以降の継続利用は困難である。

一方、当該システムベンダは、自社で開発及び運用しているシステムについて、その基盤となるシステムリソースをガバメントクラウド上に集約しているため、SKY2 国民健康保険システムについても、ガバメントクラウドへ移行することにより、既に区の他業務システムで利用しているインフラ運用保守等の共通的なサービスの利用が可能となる。また、ガバメントクラウドは、政府が定める情報セキュリティ基準に基づき整備・運用されており、セキュリティ対策や運用面において、他の利用環境と比較して一定の優位性を有している。このため、特定個人情報を取り扱うシステムの基盤として、適切な環境であると認められる。さらに、区においては、既にガバメントクラウド利用を前提としたネットワーク環境の整備を完了しており、新たな基盤整備に係る負担は限定的である。

以上の状況を踏まえ、SKY2 国民健康保険システムについては、現行のデータセンター環境からガバメントクラウドへ移行することとし、令和9年1月に移行を実施する方針とする。

※ガバメントクラウドについて

デジタル社会形成基本法（令和3年法律第35号）第29条の規定に基づき、デジタル庁が調達するものであって、地方公共団体が業務システム等を効率的に利用できるよう提供されるクラウドサービス等である。

詳細は、審議資料No. 2-5に記載のとおり。

2 評価書の改定

評価書の改定内容のうち、ガバメントクラウドのクラウド事業者が提供するクラウド上の基盤及び接続に関する部分については、令和4年10月にデジタル庁より提供された「ガバメントクラウドにおける特定個人情報保護評価について」（審議資料No. 2-6）における全項目評価書の記載例を基に作成した。

この他、事務個別に変更が生じる箇所については、評価書ごとに修正を実施した。

3 ガバメントクラウドにおけるリスク対応策の概要

システムの移行先となるガバメントクラウドについては、デジタル庁が政府情報システムのためのセキュリティ評価制度（ISMAP）のリストに登録されたクラウドサービスから調達して、区に対して個別領域の利用権を付与し、運用管理を委託する。

「国民健康保険事務」及び「国民健康保険 保険料収納事務」においては、ガバメントクラウド共同利用方式により、区は、システムのアプリケーション等を提供するASPとの間で、「アプリケーション等提供・保守契約」及び「ガバメントクラウド運用管理補助委託契約」を締結する。

特定個人情報を保有するシステムを構築するガバメントクラウドの環境は、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され、区やASP・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も、閉域ネットワークで構成し、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。

その他、継続的なモニタリング・ログ管理や脅威検出・DDoS 対策の常時実施、ウイルス対策パターンファイルの更新、OS・ミドルウェアへのセキュリティパッチ適用などの技術的対策のほか、物理的対策として、クラウド事業者のシステムのサーバー等の構築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うなど、これまでと同等のセキュリティ対策を実施する。

ガバメントクラウドに関する要件

- デジタル庁が、「政府情報システムのためのセキュリティ評価制度」(ISMAP)のリストに登録されたクラウドサービスから、要件を満たすクラウドサービスを調達。
- 地方公共団体が活用するクラウド環境については、「データを団体ごとに論理的に分離するとともに、厳格なアクセス制御を行う等、高い機密性を確保」「他システムとの接続は専用線により行う」など、セキュリティ対策を適切に講じる。

【主な要件】

- ①不正アクセス防止やデータ暗号化などにおいて、最新かつ最高レベルの情報セキュリティが確保できること。
- ②クラウド事業者間でシステム移設を可能とするための技術仕様等が公開され、客観的に評価可能であること。
- ③システム開発フェーズから、運用、廃棄に至るまでシステムライフサイクルを通じた費用が低廉であること。
- ④契約から開発、運用、廃棄に至るまで国によって統制ができること。
- ⑤データセンタの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外へ持出を行わないこと。
- ⑥一切の紛争は、日本の裁判所が管轄するとともに、契約の解釈が日本法に基づくものであること。

出典:「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)

ガバメントクラウド対象クラウドサービス一覧

クラウドサービス名

Amazon Web Services

Google Cloud

Microsoft Azure

Oracle Cloud Infrastructure

さくらのクラウド

出典:ガバメントクラウド整備のためのクラウドサービスの提供
ー令和8年度募集ーにおける審査結果
(令和8年3月27日・デジタル庁)

ガバメントクラウドにおける特定個人情報保護評価について

令和4年10月 デジタル庁

1. 「重要な変更」について

行政機関の長等は、特定個人情報ファイルを保有しようとする場合には、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（平成二十五年法律第二十七号）（以下「番号法」という。）第二十八条の規定に基づき、特定個人情報保護評価を実施する必要があります。

(1) 「重要な変更」の該当性の判断

貴市町村においては、既存のシステムについてはすでに同条に基づき特定個人情報ファイルを取り扱う事務ごとに特定個人情報保護評価を実施されているところであると認識しております。

他方、同条後段において、特定個人情報ファイルを取り扱う事務について、重要な変更が発生する場合には、重要な変更を加える前に特定個人情報保護評価を再実施することとされています。

「重要な変更」とは、特定個人情報保護評価に関する規則（平成二十六年特定個人情報保護委員会規則第一号）（以下「規則」という。）第十一条に基づき、特定個人情報保護評価指針（平成二十六年特定個人情報保護委員会告示第四号）（以下「指針」という。）第6の2（2）において、当該指針の別表に定める重点項目評価書及び全項目評価書の以下の項目が変更されることをいうものとされています。

基礎項目評価書については、「重要な変更」が規定されていないため、評価の再実施は不要です。

なお、上記に関わらず、重点項目事項評価書・全項目評価書に重要な変更に当たらない変更が生じる場合又は基礎項目評価書にしきい値判断の結果の変更に該当しない変更が生じた場合には、規則第十四条及び指針第7の規定に基づいて、必要な修正を行う必要がありますので、そのような変更が生じないかについて検討・確認をお願いします。

【参考】特定個人情報保護評価指針 別表

別表（第6の2（2）関係）	
特定個人情報保護評価書の名称	重要な変更の対象である記載項目
1 重点項目評価書	1 個人番号の利用 2 情報提供ネットワークシステムによる情報連携 3 特定個人情報ファイルの種類 4 特定個人情報ファイルの対象となる本人の範囲 5 特定個人情報ファイルに記録される主な項目 6 特定個人情報の入手元 7 特定個人情報の使用目的 8 特定個人情報ファイルの取扱いの委託の有無 9 特定個人情報ファイルの取扱いの再委託の有無 10 特定個人情報の保管場所 11 リスク対策（重大事故の発生を除く。）
2 全項目評価書	1 特定個人情報ファイルを取り扱う事務の内容 2 個人番号の利用 3 情報提供ネットワークシステムによる情報連携 4 特定個人情報ファイルの種類 5 特定個人情報ファイルの対象となる本人の範囲 6 特定個人情報ファイルに記録される主な項目 7 特定個人情報の入手元 8 特定個人情報の使用目的 9 特定個人情報の使用部署 10 特定個人情報の使用方法 11 特定個人情報の突合 12 特定個人情報の統計分析 13 特定個人情報の使用による個人の権利利益に影響を与え得る決定 14 特定個人情報ファイルの取扱いの委託の有無 15 取扱いを委託する特定個人情報ファイルの対象となる本人の範囲 16 特定個人情報ファイルの取扱いの再委託の有無 17 特定個人情報の保管場所 18 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（重大事故の発生を除く。） 19 その他のリスク対策

(2) 特定個人情報保護評価の再実施の時期

「重要な変更」に該当する場合には、特定個人情報保護評価の再実施の時期については、ガバメントクラウド上に副本データを移行するまでに評価を実施する必要があります。

2. 記載例について

指針第3の2においては、「特定個人情報ファイルを保有しようとする者又は保有する者以外に特定個人情報ファイルに関わる者が存在する場合は、その者は、特定個人情報保護評価が適切に実施されるよう協力するものとする。」とされております。

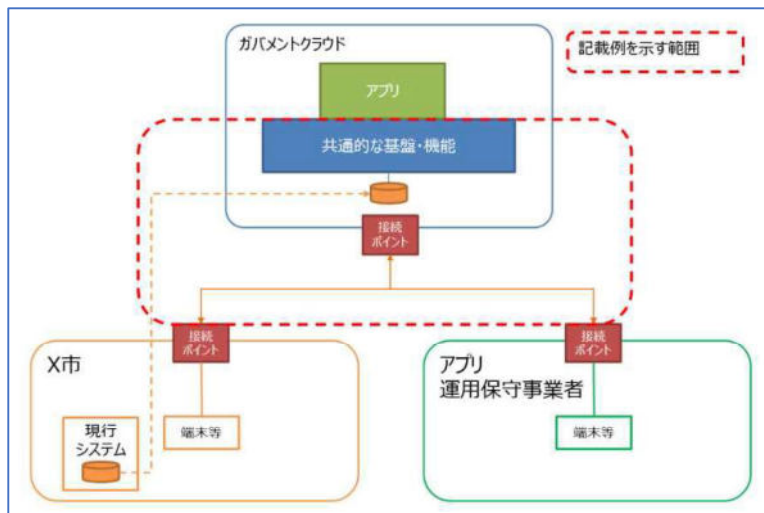
今般、ガバメントクラウドはデジタル庁が調達したことから、次の(1)及び(2)の考えに基づいて記載例を策定し、別紙のとおり提供するものです。

各市町村におかれては、番号法をはじめとする個人情報保護に関する法令の趣旨を踏まえ、記載例を含む今回の情報提供を参考に適切に評価を実施してください。

なお、内容については、令和4年8月30日時点の情報に基づき、個人情報保護委員会事務局と調整済みのものです。

(1) 記載例の射程

今回提供する記載例については、評価書に記載する内容のうち、ガバメントクラウドのクラウド事業者が提供するクラウド上の基盤及び接続に関する部分になります。



記載例を示していない箇所であっても、特定個人情報保護評価の趣旨に鑑み、上記の射程以外に関する部分について、別途記載が必要となりますので、ご留意下さい。

具体的には、委託に関する項目について、ガバメントクラウドへ移行する際のデータ抽出、移行、破棄においては委託先が特定個人情報を扱うことが想定されますので、各団体において追記する必要があります。

(2) 記載例において「重要な変更」に該当する項目

ガバメントクラウド上にシステムを構築するにあたり、上記 2 (1) の範囲において、変更が想定されるのは、次に掲げる項目です。

記載例においては、これらの項目において必要な情報を記載しています。

<重点項目評価書>

- 10 特定個人情報の保管場所
- 11 リスク対策

<全項目評価書>

- 17 特定個人情報の保管場所
- 18 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
- 19 その他のリスク対策

なお、デジタル庁及びクラウドサービス事業者は特定個人情報にはアクセスしないため、クラウドサービス事業者は番号法上の「委託」先には当たらないと解されますので、委託に関する別表の以下の項目に関しては変更を想定しておりません。

<重点項目評価書>

- 8 特定個人情報ファイルの取扱いの委託の有無
- 9 特定個人情報ファイルの取扱いの再委託の有無

<全項目評価書>

- 14 特定個人情報ファイルの取扱いの委託の有無
- 15 取扱いを委託する特定個人情報保護ファイルの対象となる本人の範囲
- 16 特定個人情報ファイルの取扱いの再委託の有無

以上

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
18	国民健康保険 保険料収納事務 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

世田谷区は、国民健康保険収納事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために十分な措置を行い、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

国民健康保険収納事務では、事務の一部を外部業者に委託しているが、委託先による不正入手、不正な使用等への対策として、特に業者選定の際に業者の情報保護管理体制を契約条件として設定している。

評価実施機関名

東京都世田谷区長

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5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	国民健康保険 保険料収納事務
②事務の内容 ※	世田谷区では、SKY2国民健康保険システムにより保険料収納、滞納整理事務を行っている。 ①国民健康保険料収納事務 ・国民健康保険料徴収金の消込み、及び口座振替不能者への督促を行う。 ・国民健康保険料過誤納金の還付充当を行う。 ・国民健康保険料の口座振替手続きを行う。 ・国民健康保険料徴収金の収納管理(納付委託)を行う。 ・納付者が納付書により納付したことについて、金融機関からの納入済通知書等により確認する。 ②国民健康保険料納付相談及び徴収整理事務 ・国民健康保険料の収納及び納付相談を行う。 ・国民健康保険料徴収金の徴収整理を行う。 ・国民健康保険料徴収金の徴収猶予を行う。 ・国民健康保険料未納者への督促及び催告を行う。 ③国民健康保険料、介護保険滞納処分事務 ・国民健康保険料未納者に対する納付交渉や財産調査、財産の差押え等滞納処分、その他交付要求、繰上徴収を行う。 ・国民健康保険料未納者に対する捜索を行う。 ・差押え財産の公売、配当事務を行う。 ・介護保険被第一号被保険者の保険料の普通徴収に係る未納者に対する財産調査や差押え等滞納処分、交付要求、繰上徴収を行う。 ④電話催告センター運行事務 ・業務委託により、現年度のみの未納者を対象に、オペレーターの電話による催告を行う。架電週の1回は夜間催告を実施する。 ⑤他区市町村への情報照会・提供事務 ・他区市町村への住民票・戸籍・賦課状況・課税状況等の照会、及び他区市町村からの照会への回答を行う。 (※)「(別添1)事務内容」を参照
③対象人数	[10万人以上30万人未満] ＜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

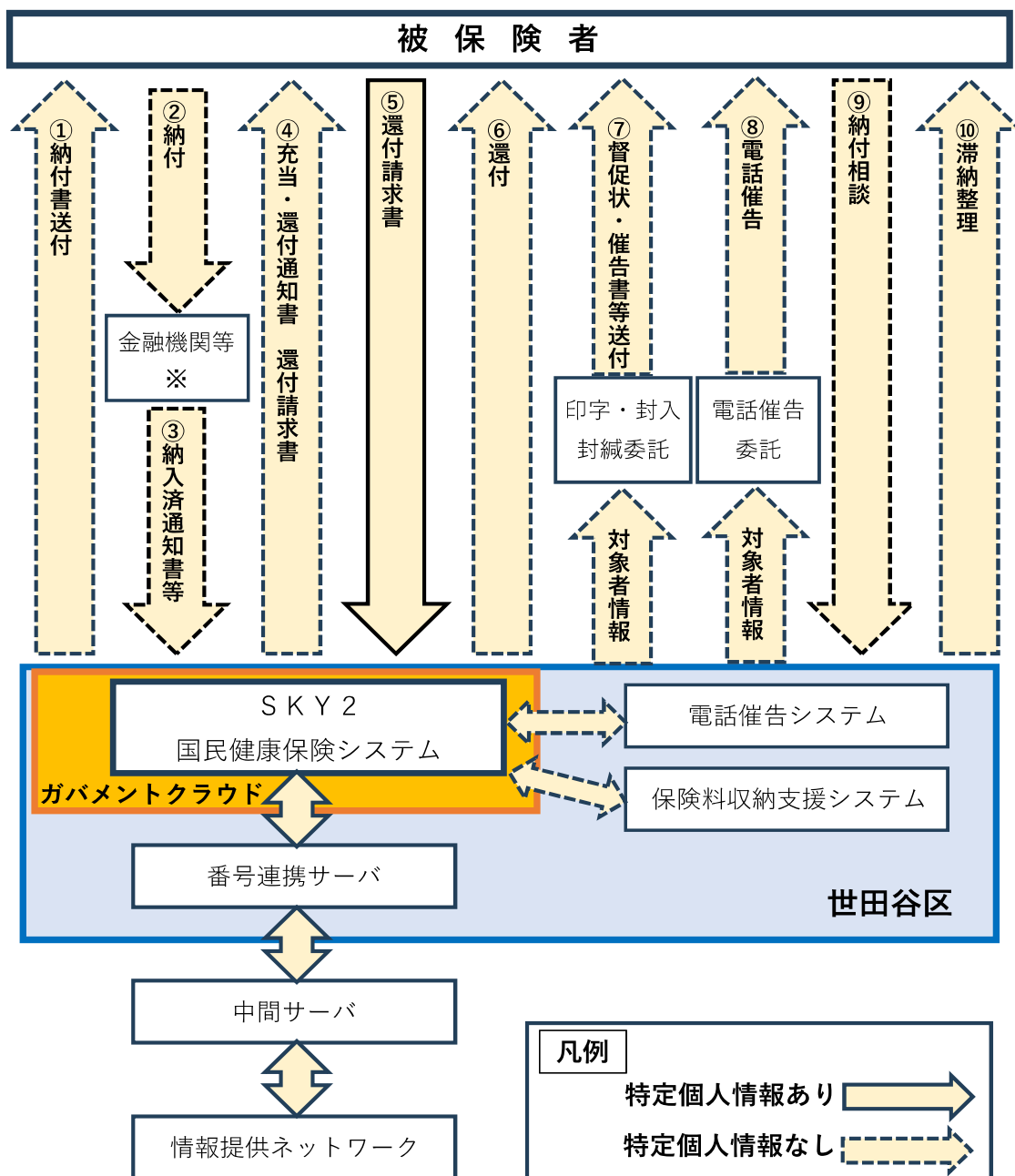
2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1	
①システムの名称	SKY2国民健康保険システム
②システムの機能	1. 収納機能(窓口業務メニュー、督促、還付・充当、返戻・公示、収納情報修正、口座振替停止) 2. 滞納機能(国保滞納システムを利用し、滞納者の状況を確認する。納付交渉の経過記録記載。財産調査や差押え等の記録を記載。) 3. 口座機能(口座振替による国保料の支払いに対して口座管理を行う。) 4. 資格得喪情報記録機能 5. 保険証・医療証等の発行、発行履歴の記録機能 6. 保険料賦課計算機能及び賦課情報の記録機能 7. 給付情報の記録、高額療養費支給、出産葬祭費支給機能 8. 各情報の照会・表示機能
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 (電話催告システム、保険料収納支援システム)

システム2～5	
システム2	
①システムの名称	番号連携サーバー
②システムの機能	1. 宛名管理機能 ①サーバー内の宛名データベースのセットアップ ②宛名の異動データを取り込み、宛名データベースへ反映 ③個人番号にて同一人判定を行い、団体内統合宛名番号を採番し管理 ④宛名データベースの検索、参照、更新 ⑤オンラインで入力したデータを業務システムに連携 ⑥団体内統合宛名番号を業務システムに連携 2. 情報提供機能 ①中間サーバーに連携する各業務情報をデータベースへセットアップ ②各業務の異動データを取り込み、データベースに反映 ③各業務情報の参照、入力、変更、削除を行う。 ④各業務情報を一括で中間サーバーに連携 ⑤各業務の異動情報を中間サーバーに連携 3. 情報照会機能(他機関への情報照会) ①各業務の宛名番号で対象者を検索し、他自治体への情報提供を依頼し、オンラインにて表示する。 ②情報照会の対象者情報を元に、中間サーバーに情報を要求し、一括ファイルを作成する。 4. 符号要求 ①処理通番を要求・受信し、符号要求データを既存住基または住基GWに送信する。
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 [] 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 (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	中間サーバーは、情報提供システムネットワークシステム(インターフェイスシステム)、番号連携サーバーとのデータ受け渡しを行うことで、符号の取得(※1)や各情報保有機関で保有する特定個人情報の照会と提供等の業務を実現する。 1. 符号管理機能: 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」と、情報照会、情報提供に用いる個人の識別子である「符号」とを紐付け、その情報を保管・管理する機能。 2. 情報照会機能: 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)の情報照会及び情報提供受領(照会した情報の受領)を行う機能。 3. 情報提供機能: 情報提供ネットワークを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能。 4. 既存システム接続機能: 中間サーバーと既存システム、番号連携サーバー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ための機能。 5. 情報提供等記録管理機能: 特定個人情報(連携対象)の照会、または提供があった旨の情報提供等記録を生成し、管理する機能。 6. 情報提供データベース管理機能: 特定個人情報(連携対象)を副本として、保持・管理する機能。 7. データ送受信機能: 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)との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 8. セキュリティ管理機能: セキュリティを管理する機能。 9. 職員認証・権限管理機能: 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(連携対象)へのアクセス制御を行う機能。 10. システム管理機能: バッチの状況管理、業務統計情報の集計、稼働状況の通知、保管期限切れ情報の削除を行う機能。 (※1)セキュリティの観点により、特定個人情報の照会と提供の際は、「個人番号」を直接利用せず「符号」を取得して利用する。
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 [] 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	電話催告システム
②システムの機能	・国民健康保険料の滞納情報をもとに、電話催告対象者リストを作成し、架電する。 ・催告対象者との折衝状況を管理する。
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 ☒ 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5	
①システムの名称	保険料収納支援システム
②システムの機能	金融機関から受領する納付済通知書や還付請求書をスキャナによりOCR処理し、収納データや還付請求データを作成する。
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 ☒ 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6～10	
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
収納管理台帳ファイル、滞納整理台帳ファイル	
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	・個人を正しく把握し、正確な保険料収納事務を行うため。 ・多くの対象者を正確かつ迅速に処理するには、電算システムの利用が必要不可欠であるため。
②実現が期待されるメリット	個人の特定の正確性が向上することにより、国民健康保険料収納事務の公平・公正・効率化が図られ、よって被保険者の利便に資することとなる。
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44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 ☐ 実施しない ☒ 未定
②法令上の根拠	【情報提供】なし 【情報照会】番号法第19条第8号に基づく主務省令第2条の表69の項
7. 評価実施機関における担当部署	
①部署	保険料収納課
②所属長の役職名	保険料収納課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容



(備考)

- ①被保険者へ、納付書を送付する。
- ②金融機関等で納付する。
- ③納付された収納金の送付及び納入済通知書・納入データの受領
- ④支払い期別において、保険料を上回る納付があった際は、充当・還付を行い、被保険者へ通知する。
なお、国民健康保険料の振替口座を還付金の振込口座としていない被保険者に対しては還付請求書を同封する。
- ⑤還付請求書の送付により、還付請求と還付金の振込口座を指定する。
なお公金受取口座を振込口座に指定する場合はマイナンバーを記入する。
- ⑥被保険者の口座に還付金を振り込む。
- ⑦納付がない場合や納付額が不足する場合は、督促状、催告書を送付する。
- ⑧納付がない場合や納付額が不足する場合は、委託事業者による電話催告を行う。
- ⑨被保険者からの納付相談
- ⑩督促・催告等を行っても納付がない場合は、滞納整理を行う。

※口座振替、区の窓口の他、金融機関窓口、決済アプリ、インターネットによるクレジット払いによる納付

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		
収納管理台帳ファイル、滞納整理台帳ファイル		
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 ※	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者	
その必要性	個人又は口座情報を正確に特定し、公平・公正な保険料徴収又は正確・迅速な還付事務を行うため。	
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 [☐] 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	1. その他識別情報:対象者を正確に特定するために保有 2. 5情報、連絡先、その他住民票関係情報:①還付通知書、督促状、催告書等の発付に当たっての送付先確認、②本人への連絡等のため、③滞納整理を進める上での確認のため。 3. 医療保険関係情報:医療保険関係情報により国民健康被保険者の特定、加入・脱退の確認を行う。
	全ての記録項目	別添2を参照。
⑤保有開始日	平成27年6月	
⑥事務担当部署	保険料収納課	

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 （ 住民記録・戸籍課、課税課、納税課、国保・年金課 ） ☐ 行政機関・独立行政法人等 （ 内閣（デジタル庁） ） ☐ 地方公共団体・地方独立行政法人 （ 他区市町村 ） ☐ 民間事業者 （ ） ☐ その他 （ ）	
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 （ ）	
③入手の時期・頻度	随時	
④入手に係る妥当性	収納・滞納整理・滞納処分事務を行う上で、必要に応じて情報の正確性の確認を行うため、庁内連携システムや情報提供ネットワークシステムを通じて納付者・滞納者の特定等に必要な情報を随時入手する。	
⑤本人への明示	・本人から入手する情報については、本人を通じて入手することとし、また利用目的を本人に明示する。ただし、国民健康保険法等や、他の法令で定めがある場合は、その限りではない。 ・庁内連携又は情報提供ネットワークシステムを通じた入手を行うことは番号法に明示されているが、窓口対応する場合は、口頭にて本人に説明を行う。	
⑥使用目的 ※	国民健康保険料の公平・公正な保険料徴収又は正確・迅速な還付事務を行うため。	
	変更の妥当性	—
⑦使用の主体	使用部署 ※	保険料収納課、各総合支所区民課（世田谷総合支所区民係、太子堂出張所、経堂出張所、北沢総合支所区民係、玉川総合支所区民係、用賀出張所、二子玉川出張所、砧総合支所区民係、烏山出張所、烏山総合支所区民・戸籍係）、各総合支所地域振興課まちづくりセンター（池尻、太子堂、若林、上町、経堂、下馬、上馬、梅丘、代沢、新代田、北沢、松原、松沢、奥沢、九品仏、等々力、上野毛、用賀、深沢、二子玉川、祖師谷、成城、船橋、喜多見、砧、上北沢、上祖師谷、烏山）
	使用者数	[500人以上1,000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 ※	1. 収納事務 国民健康保険の資格、賦課情報から、保険料徴収対象者を把握し、収納事務を行う。 情報提供ネットワークシステムから公金受取口座情報を取得し、対象者の口座情報を特定し、還付事務を行う。 2. 滞納整理事務 保険料滞納者との交渉により、納付交渉者を特定し、滞納整理事務を行う。 3. 滞納処分事務 住民税情報から滞納者の財産調査を行い、滞納処分事務を進める。また、場合によっては他区市町村に対し、滞納者の照会を行い、財産調査の根拠とする。	
	情報の突合 ※	1. 収納事務 保険料の収納事務に係るデータについて、国民健康保険の資格・賦課情報、公金受取口座情報との突合を行う。 2. 滞納整理事務 保険料滞納整理にあたり、特定した納付交渉者の情報について、国民健康保険の資格・賦課情報との突合を行う。 3. 滞納処分事務 税情報等を基にした財産調査の結果について、対象者の収納（滞納）情報との突合を行う。また、他区市町村から入手した情報は、世田谷区の滞納者と相違ないかどうか、資格・賦課情報との突合を行った上で、滞納処分事務を進める。
	情報の統計分析 ※	都や各部署等への報告資料等のため統計・分析を行うが、特定個人情報を用いて特定の個人を判別しうる統計分析は行わない。
	権利利益に影響を与え得る決定 ※	差押え等の滞納処分（不利益処分）決定
⑨使用開始日	平成28年1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 (1) 件	
委託事項1	SKY2国民健康保険システムの保守・運用	
①委託内容	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出、ガバメントクラウドへのシステム構築・データ移行等	
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 ※	SKY2国民健康保険システムに情報が記録されている者のうち、個人番号を有する者	
その妥当性	保険料収納事務の遂行にあたっては、国民健康保険料のより正確な保険料徴収及び還付事務に必要な範囲の特定個人情報を保有しているSKY2国民健康保険システムの安定的な運営が不可欠であり、当該システムの円滑な保守運用業務を行う上で、国民健康保険料に係る納付者・滞納者のデータベース等を含むシステム上のあらゆる情報を取り扱う必要がある。	
③委託先における取扱者数	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	
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	契約した委託先は、区ホームページにて公表している。	
⑥委託先名	富士通Japan株式会社、世田谷サービス公社	
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	委託業務の附属業務についてやむを得ず再委託する必要があるときは、再受託者に、当該委託契約書に記載された情報セキュリティに関する特記事項を遵守させるとともに、再受託者の氏名、再委託の内容及び業務執行場所を、区に事前に通知し、その承諾を得ることを委託契約上の条件としている。
	⑨再委託事項	システム運用状況の管理、パッチジョブ運用、リハーサル支援、障害発生時の対応支援等
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

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 () 件 [] 移転を行っている () 件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[] <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	
⑥提供方法	[] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 () [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] <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移転する情報の対象となる本人の範囲	
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [] その他 () [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		＜世田谷区における措置＞ 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止：外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理：ICカード＋手のひら静脈認証、要員所在管理システム ③持込・持出防止：金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 申請書及び届出書等の紙媒体、及び外部記録媒体は、鍵のかかるロッカーや保管庫に保管している。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜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。
	②保管期間 期間 その妥当性	＜選択肢＞ [定められていない] 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない 国民健康保険法等において、データ保管期間の定めはなく、還付を含む収納事務や滞納処分が終了するまで、情報が必要となるため保管する。 収納事務又は滞納処分が終了した後は、適宜消去する。
③消去方法		＜世田谷区における措置＞ ①データベースに登録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。 ③外部記憶媒体に一時的に登録した特定個人情報等の申請データは、使用の都度速やかに完全消去する。 ＜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 SP800-88、ISO/IEC27001等に当た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。 ＜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世田谷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		
特になし		

(別添2) 特定個人情報ファイル記録項目

(1) 収納管理台帳ファイル

<宛名情報>

宛名番号 個人番号 法人番号 世帯番号

氏名情報 生年月日 性別 続柄

住民となった年月日 住民となった届出年月日 住民となった事由

住民区分(日本人・外国人) 世帯主情報

現住所情報 住所を定めた年月日 住所を定めた届出年月日

前住所情報 転入元住所情報 転出先住所情報

本籍・筆頭者情報 消除情報

国籍 在留カード等の番号 在留資格情報 通称

処理停止情報 送付先情報 送付先履歴情報

相続人情報 相続人続柄情報 相続人履歴情報

納税管理人情報 納税管理人履歴情報

記事情報 連絡先情報

破産管財人情報 破産管財人履歴情報

口座情報(公金受取口座情報を含む。)

<年調定情報>

税目 賦課年度 相当年度

納付義務者番号 賦課異動理由 更正事由 更正日 通知書番号 年調定額

記号番号

<月期別調定情報>

税目 賦課年度 相当年度

納付義務者番号 期別 月別 納期限

個人基本種別 賦課異動理由 更正事由 完納日 最終納付日 最終収入日 保険料調定額

保険料収入額 保険料仮消込額 保険料被充当予定額 保険料未納額 保険料過誤納額

延滞金調定額 延滞金収入額 延滞金仮消込額 延滞金被充当予定額 延滞金未納額 延滞金過誤納額 退職納入申告日

納期特例区分 時効予定日 不納欠損処理日 不納欠損処理日 不納欠損区分

延滞金減免区分 延滞金確定日 延滞金執行日

口座振替区分 振替金額 口座振替理由 口座振替日

変更納期限 催告書発付日 授命年月日 催告納期

記号番号

<消込情報>

税目 賦課年度 相当年度 納付義務者番号 分納回数 期月 子番

通知書番号 領収日 収入日 納付区分 収納種別

消込金額 消込本税額 消込延滞金 確定延滞金 未確定延滞金

消込処理情報 仮消込情報 仮消込エラー情報

<履歴情報>

調定履歴情報 消込履歴情報 仮消込履歴情報

証明書発行履歴

充当履歴情報 還付履歴情報 控除不足充当履歴

<その他収納管理情報>

口座振替情報 返戻情報 返戻住所情報

過誤納情報 還付通知書情報 納付書情報

滞繰調定情報 滞繰異動情報

控除不足情報 処分情報

(別添2) 特定個人情報ファイル記録項目

(2) 滞納整理台帳ファイル

<宛名情報>

宛名番号 個人番号 法人番号 世帯番号

氏名情報 生年月日 性別 続柄

住民となった年月日 住民となった届出年月日 住民となった事由

住民区分(日本人・外国人) 世帯主情報

現住所情報 住所を定めた年月日 住所を定めた届出年月日

前住所情報 転入元住所情報 転出先住所情報

本籍・筆頭者情報 消除情報

国籍 在留カード等の番号 在留資格情報 通称

処理停止情報 送付先情報 送付先履歴情報

相続人情報 相続人続柄情報 相続人履歴情報

納税管理人情報 納税管理人履歴情報

記事情報 連絡先情報

破産管財人情報 破産管財人履歴情報

口座情報

<記事情報>

宛名番号 記事連番 記事年月日 記事時刻 記事コード 記事内容

折衝情報 交渉情報 予定情報

処分コード 調書番号

<滞納個人情報>

宛名番号 担当区分 地区コード 受入年月日

現年滞納額 滞納繰越額

滞納区分 最終折衝日 職業 滞納理由 滞納理由補足 特記事項 納付方法

訪問予定年月日 訪問予定日 訪問予定時刻

最終納付年月日 最終納付金額 最終催告種別 最終催告年月日 最終催告期限

催告停止日 催告停止期限 催告停止事由

返戻情報 実態調査情報 生活保護情報

差押情報(電話・不動産・給与・預金・郵貯・生保・債権)

繰上徴収件数 納付委託件数 分割納付件数 徴収猶予件数 延滞金減免件数

差押件数 参加差押件数 交付要求件数 換価猶予件数 処分停止件数 時効中断件数

時効予定日 臨戸分納区分 徴収区分

戸籍情報

連絡先情報

<分納情報>

処分コード 調書番号 処分連番 回数 指定期日 調定年度 課税年度 税目

通知書番号 事業年度開始日 申告区分 申告連番 期別 期別順番

保険料分納額 督促分納額 延滞金分納額 加算金分納額 受付番号

<滞納整理情報>

滞納履歴

処分情報 処分調定情報

公売管理情報 財産情報 証券管理情報

納付指導計画

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		
収納管理台帳ファイル、滞納整理台帳ファイル		
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	・対象者以外の情報を誤って記載することがないように、記入例等の案内書類を工夫する。 ・他市区町村から情報を入手する際は、対象者以外の情報入手をしないよう、事務マニュアル等を整備し、処理を統一化する。	
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	・必要な情報以外を誤って記載することがないように、記入例等の案内書類を工夫する。 ・他市区町村から情報を入手する際は、必要以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。	
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： 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	・情報提出を依頼する際は、その目的及び提出された情報の使用用途について、説明書等を用いて説明する。 ・庁内連携にて入手する場合は、庁内連携システムを使用するが、権限を持った者しか情報照会ができず、また情報照会の記録が保存される仕組みとなっている。	
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	・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、本人確認を行う。	
個人番号の真正性確認の措置の内容	・個人番号カードの提示、もしくは通知カードと身分証明書の提示に加え、以前に提出された保険料収納課資料等に記載された個人番号との照合により、真正性確認を行う。	
特定個人情報の正確性確保の措置の内容	・国保・年金課と連携して所得情報、住所情報の正確性を確認する。必要に応じて住民基本台帳ネットワークシステムを利用して、本人確認を行う。また、本人にも確認する。 ・個人番号だけでなく、氏名・住所・生年月日等を複合的にチェックする。	
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	・窓口では本人から直接書面を受け取ることを原則とする。 ・郵送の場合は、担当部署の所在地及びあて先を印字した専用封筒を使用するよう促す。	
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	個人番号利用業務以外から、または個人番号を必要としない業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。		
事務で使用するその他のシステムにおける措置の内容	- 事務に必要な情報はシステム内に保持しない。 - データで提出されるなどによりシステム内に保持せざるを得ない場合は、データベース上には保持するが、画面には表示しないよう制限を行う。		
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	- 職員証(ICカード)とパスワードの二要素によりユーザIDの認証を行う。 - ユーザIDに付与されるアクセス権限によって、業務従事者が業務に必要な範囲の特定個人情報ファイルだけにアクセスすることができるように制御する。 - 人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。		
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	- 発効管理: 人事異動があった場合等には、速やかに発効処理を行う。 - 失効管理: 人事異動があった場合等には、速やかに失効処理を行う。 ※発効、失効いずれの場合も、発効・失効作業を行った者以外の他の者が二重チェックを行い、正しく登録・削除されているかを確認する。		
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	共用IDは発行せず、個人に対してユーザIDを発行する。		
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	- 誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。 - 特定個人情報のアクセスログについて、年一回以上随時分析し、業務時間帯以外のアクセス、業務上想定されない頻度のアクセスの有無がないか確認する。分析の結果は、情報システム管理者に報告する。		
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	定期的実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏洩時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。		
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	通常ユーザ用と管理者用とにアクセス権限を分け、システムのバックアップデータ等の重要データには管理者権限のみがアクセスできるようにする。		
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			
—			

☐ 委託しない

情報保護管理体制の確認	・委託契約書において、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ている。 (1) 情報セキュリティ及び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) 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所 2) 委託業務において個人情報を取り扱う者及び個人情報に係る記録媒体の授受に携わる者の氏名並びに業務執行場所 3) 委託業務に関する緊急時連絡先一覧
--------------------	--

具体的な制限方法 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。

具体的な方法

- ・システム保守作業については、作業内容の記録を提出させている。
- ・電子記録媒体については、管理簿を作成し、引渡し及び返却を管理する。

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	・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、情報セキュリティに関する教育の実施等を義務づけている。
------------------------------	---

- 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
 - ・委託契約書において、以下の事項を義務づけている。
 - (1)区より特定個人情報を含む情報資産を受領した場合、区に対して受領証を提出すること。
 - (2)区より受領した情報資産を適切に管理するため、情報資産の受領記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を提示すること。
 - (3)委託業務が完了したときは、区より受領した情報資産を速やかに区に返却すること。返却が不可能な情報資産は、区の下承のもと、バックアップデータを含め、情報及び情報資産を復元できないように処置した上で廃棄すること。
 - ・区は、委託先へ特定個人情報を含む情報資産を提供(引渡し)した場合は、所定の記録簿に記載するとともに、事後、所属長が確認することとしている。

ルール内容及び ルール遵守の確認方法	・業務完了後にデータ削除を行い、削除証明書を提出させる。 ・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、情報セキュリティに関する教育の実施等を義務づけている。
-------------------------------	---

規定の内容	・秘密保持義務 ・管理体制等の通知 ・目的外使用等及び複写等の禁止 ・物的セキュリティ対策 ・人的セキュリティ対策 ・技術的及び運用におけるセキュリティ対策 ・監査・施設への立入検査の受入れ
-------	---

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	・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るとともに、再委託先に同様の事項を遵守させることを義務づけている。	
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
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	<世田谷区における措置> ・番号法の規定に基づき、認められている範囲内において特定個人情報の照会を行う。 <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会リスト(※2)との照会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ほかに、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	<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。 <中間サーバーの運用における措置> ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法及び条例上認められる提供以外は受け付けないようにしており、システム上提供が認められなかった場合においても記録を残し、提供記録は7年分保管する。		
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	
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク			
リスクに対する措置の内容	<世田谷区における措置> ・入手した特定個人情報について、SKY2国民健康保険システム内の情報と突合を行い、真正性及び正確性確認を行う。また、別途、届出または申告時には、その都度、届出などの内容と突合を行い、特定個人情報の正確性確認を行う。 <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できない。 ＜中間サーバーの運用における措置＞ ・情報照会、情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報漏えい・紛失することを防止する。	
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、中間サーバーにも格納して、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不正に提供されるリスクに対応している。 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。 (※) 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。 ＜中間サーバーの運用における措置＞ ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ何のために利用したかがすべて記録される。番号法及び条例上認められる提供以外は受け付けず、システム上提供が認められなかった場合においても記録を残し、提供記録は7年分保管する。	
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

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会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。 ＜中間サーバーの運用における措置＞ ・情報照会、情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報がやりとりされることを防止する。	
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	＜世田谷区における措置＞ ・庁内連携システムでは本業務で保有する情報をすべて連携することは行わず、番号法の規定及び条例に基づき認められる情報のみを提供する仕組みとしている。 ＜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。 (※)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	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止: 外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退館管理: ICカード+手のひら静脈認証、要員所在管理システム ③持込・持出防止: 金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 ④LGWAN 接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ⑤外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、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。 <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。

⑥技術的対策	十分にしている ＜選択肢＞ 1) 特に力を入れてしている 2) 十分にしている 3) 十分にいない
具体的な対策の内容	＜世田谷区における措置＞ ・SKY2国民健康保険システムへのアクセス時におけるICカード＋パスワード認証 ・ウイルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・LGWAN 接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ＜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地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。)に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ＜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。 ＜国保総合(国保集約)システムにおける措置＞ ・区市町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。 ・国保総合PCで利用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。 ・国保総合PCには、ウイルス対策ソフトウェアを導入し、ウイルスパターンファイルは適時更新する。 ・不正アクセス防止策として、ファイアウォールを導入している。 ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。
⑦バックアップ	十分にしている ＜選択肢＞ 1) 特に力を入れてしている 2) 十分にしている 3) 十分にいない
⑧事故発生時手順の策定・周知	十分にしている ＜選択肢＞ 1) 特に力を入れてしている 2) 十分にしている 3) 十分にいない

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	生存者と死者を区別することなく、同様の基準で管理する。	
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	被保険者情報については、随時、本人確認を行い、変更があればその都度データを修正している。	
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： 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	・収納事務又は滞納処分が終了した後、情報を適宜消去する。正しく消去されていることを職員が確認する。 ・紙媒体については、保管期間ごとに分けて保管し、保管期限の過ぎたものは外部業者による溶解処理を行う。 ＜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 SP800-88、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		
サーバ、端末(パソコン)、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。機器リース終了による返却の場合も、同様とする。 ・紙文書は、溶解またはシュレッダー処分を行う。 ・電磁的な記録媒体は、破碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行った上で廃棄する。 ・サーバ、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによるデータ消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。		

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	<世田谷区における措置> ・実際の運用が評価書記載の内容と合致しているかについて、定期的にチェックを行う。 <中間サーバー・プラットフォームにおける措置> ・運用規則に基づき、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	[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) 十分に行っている 3) 十分に行っていない
具体的な内容	<世田谷区における措置> 適正な個人情報の保護やリスク対策を図るため、監査計画を策定し、定期的及び必要に応じて随時、より客観的な評価ができる監査を実施し、監査の結果を踏まえて必要な改善を行う。監査に当たっては、以下の観点から実施する。 ・ 評価書記載事項と運用実態のチェック ・ 個人情報保護に関する規程・体制整備 ・ 個人情報保護に関する人的安全管理措置 ・ 安全管理措置の周知・教育 ・ 個人情報保護に関する技術的安全管理措置 <中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 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	<世田谷区における措置> ①職員が番号制度に関する基礎的事項を常時確認できるよう、研修資料を庁内公開している。また、研修資料は毎年度見直しを実施している。 ②委託先事業者の従業者については、契約時の仕様書に個人情報保護遵守を明記し、委託先事業者の責任者の責において、研修・指導を行わせる。必要に応じて、研修資料等を提供させ、実効性を担保する。 ③違反行為を行った者に対しては、指導を行う。違反行為の程度によっては、懲戒の対象となりうる。また、全従業者に対して、違反事項発生を周知し、再発防止を徹底する。 <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

＜世田谷区における措置＞

・世田谷区行政手続における特定個人を識別するための番号の利用等に関する条例第7条及び同条例施行規則第6条の規定に基づき、マイナンバー制度セキュリティ会議を設置し、特定個人情報ファイルの取扱いに関する企画及び運用計画、セキュリティ対策等を審議する。

＜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。

＜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リテラン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。

②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。

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154-8504 東京都世田谷区世田谷4-21-27 世田谷区総務部区政情報課区政情報係
②請求方法	指定様式による書面の提出により、開示・訂正・利用停止請求を受け付ける。
特記事項	区ホームページ上に、請求先、請求方法、諸費用等について掲載する。
③手数料等	[無 料] <選択肢> (手数料額、納付方法: 1) 有料 2) 無料)
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	収納管理台帳ファイル、滞納整理台帳ファイル
公表場所	区政情報センター、世田谷区総務部区政情報課、世田谷区ホームページ
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	東京都世田谷区 保険料収納課 電話:03-5432-2342
②対応方法	電話による対応を受け付ける。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和7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	パブリックコメントによる区民意見募集を行う。 ・区のお知らせ「せたがや」にて周知する。 ・番号制度・マイナンバーカード交付推進担当課、区政情報センター、総合支所区政情報コーナー、総合支所くみん窓口・出張所・まちづくりセンター、図書館、区のホームページにて、「特定個人情報保護評価」全文を閲覧できるようにする。
②実施日・期間	令和4年7月1日(金)～令和4年7月30日(土)(30日間)
③期間を短縮する特段の理由	—
④主な意見の内容	—
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和4年8月26日(金)
②方法	世田谷区情報公開・個人情報保護審議会による点検
③結果	異議なし
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
平成27年4月1日	I-1-②事務の内容	⑤徴収嘱託員の事務 ・徴収嘱託員を活用して、未納者宅への納付勧奨訪問や口座振替勧奨を行う。	削除	事後	
平成28年4月1日	I-7-②所属長	保険料収納課長 畑中 健	保険料収納課長 太田 一郎	事後	
平成28年4月1日	II-3-①入手先	[○]評価実施機関内の他部署（国保・年金課、地域窓口調整課、課税課、納税課）	[○]評価実施機関内の他部署（国保・年金課、住民記録・戸籍課、課税課、納税課）	事後	
平成28年7月1日	II-3-⑦使用部署	保険料収納課、太子堂出張所、経堂出張所、北沢出張所、等々力出張所、用賀出張所、用賀出張所二子玉川分室、成城出張所、烏山出張所、烏山総合支所区民・戸籍係	保険料収納課、各総合支所区民課（太子堂出張所、経堂出張所、北沢出張所、等々力出張所、用賀出張所、用賀出張所二子玉川分室、成城出張所、烏山出張所、烏山総合支所区民・戸籍係）	事後	
平成29年7月1日	II-3-⑦使用部署	保険料収納課、各総合支所区民課（太子堂出張所、経堂出張所、北沢出張所、等々力出張所、用賀出張所、用賀出張所二子玉川分室、成城出張所、烏山出張所、烏山総合支所区民・戸籍係）	保険料収納課、各総合支所区民課（世田谷総合支所区民係、太子堂出張所、経堂出張所、北沢総合支所区民係、玉川総合支所区民係、用賀出張所、用賀出張所二子玉川分室、砧総合支所区民係、烏山出張所、烏山総合支所区民・戸籍係）	事後	
平成30年4月1日	I-7-②所属長	保険料収納課長 太田 一郎	保険料収納課長 尾野 聰始	事後	
平成31年4月1日	I-7-②所属長の役職名 (旧:所属長)	保険料収納課長 尾野 聰始(所属長の氏名)	保険料収納課長	事後	

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4年10月1日	I-2-システム5	—	①システムの名称 電話催告システム ②システムの機能 ・国民健康保険料の滞納情報をもとに、電話催告対象者リストを作成し、架電する。 ・催告対象者との折衝状況を管理する。 ③他のシステムとの接続 [○] 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	事前	
令和4年10月1日	I-2-システム6	—	①システムの名称 保険料収納支援システム ②システムの機能 金融機関から受領する納付済通知書や還付請求書をスキャナによりOCR処理し、収納データや還付請求データを作成する。 ③他のシステムとの接続 [○] 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	事前	
令和4年10月1日	I-4-①事務実施上の必要性	納付処理	保険料収納事務	事前	
令和4年10月1日	I-6-②法令上の根拠	番号法第19条第7号 別表第2の以下の項 1、2、3、4、5、9、26、27、30、33、39、42、44、58、62、80、87、93、119	番号法第19条第8号 別表第2の以下の項 1、2、3、4、5、9、26、27、30、33、39、42、44、58、62、80、87、93、120	事前	
令和4年10月1日	(別添1)事務の内容(図表)	—	図表の差し替え 還付請求書、電話催告システム、保険料収納支援システムの追加など	事前	

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4年10月1日	(別添1)事務の内容(備考)	①被保険者へ、納付書を送付する。 ②納付書により納付したことについて、金融機関や出張所等からの領収済通知書にて確認し、記録する。 ③納付額が多い場合は、超過額について、充当・還付を行い、納付者へ通知する。 ④必要に応じて、滞納者に生活状況や収入状況等の調査を行う。 ⑤上記④について、納付者からの回答を得る。 ⑥口座振替や、督促・催告の実施にあたり、対象者情報を業者に提供する。 ⑦委託業者から、データ等の返却・納品。 ⑧納付がない場合や納付額が少ない場合は、督促状、催告書を送付する。 ⑨滞納整理による納付。 ⑩電話催告を行う。 ⑪督促・催告等を行っても納付がない場合は、滞納整理を行う。	①被保険者へ、納付書を送付する。 ②金融機関等で納付する。 ③納付された収納金の送付及び納入済通知書・納入データの受領 ④支払い期別において、保険料を上回る納付があった際は、充当・還付を行い、被保険者へ通知する。 なお、国民健康保険料の振替口座を還付金の振込口座としていない被保険者に対しては還付請求書を同封する。 ⑤還付請求書の送付により、還付請求と還付金の振込口座を指定する。 なお公金受取口座を振込口座に指定する場合はマイナンバーを記入する。 ⑥被保険者の口座に還付金を振り込む。 ⑦納付がない場合や納付額が不足する場合は、督促状、催告書を送付する。 ⑧納付がない場合や納付額が不足する場合は、委託事業者による電話催告を行う。 ⑨被保険者からの納付相談 ⑩督促・催告等を行っても納付がない場合は、滞納整理を行う。 ※口座振替、区の窓口の他、金融機関窓口、決済アプリ、インターネットによるクレジット払いによる納付	事前	
令和4年10月1日	Ⅱ-2-③対象となる本人の範囲その必要性	個人を正確に特定し、公平・公正な保険料徴収を行うため。	個人又は口座情報を正確に特定し、公平・公正な保険料徴収又は正確・迅速な還付事務を行うため。	事前	
令和4年10月1日	Ⅱ-2-④記録される項目その妥当性	2. 4情報、連絡先、その他住民票関係情報:①督促状、催告書等の発付に当たっての送付先確認、②本人への連絡等のため、③滞納整理を進める上での確認のため。	2. 4情報、連絡先、その他住民票関係情報:①還付通知書、督促状、催告書等の発付に当たっての送付先確認、②本人への連絡等のため、③滞納整理を進める上での確認のため。	事前	
令和4年10月1日	Ⅱ-3-①入手元	[○] 評価実施機関内の他部署() [] 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()	[○] 評価実施機関内の他部署(住民記録・戸籍課、課税課、納税課、国保・年金課) [○] 行政機関・独立行政法人等(内閣府) [○] 地方公共団体・地方独立行政法人(他区市町村)	事前	
令和4年10月1日	Ⅱ-3-④入手に係る妥当性	滞納整理を行う上で、必要に応じて情報の正確性の確認を行うため、庁内連携システムや情報提供ネットワークシステムを通じて滞納者の特定等に必要な情報を随時入手する。	収納・滞納整理・滞納処分事務を行う上で、必要に応じて情報の正確性の確認を行うため、庁内連携システムや情報提供ネットワークシステムを通じて納付者・滞納者の特定等に必要な情報を随時入手する。	事前	

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4年10月1日	Ⅱ-3-⑥使用目的	国民健康保険料の公平・公正・効率的な保険料徴収のため。	国民健康保険料の公平・公正な保険料徴収又は正確・迅速な還付事務を行うため。	事前	
令和4年10月1日	Ⅱ-3-⑦使用部署	保険料収納課、各総合支所区民課(世田谷総合支所区民係、太子堂出張所、経堂出張所、北沢総合支所区民係、玉川総合支所区民係、用賀出張所、用賀出張所二子玉川分室、砧総合支所区民係、烏山出張所、烏山総合支所区民・戸籍係)	保険料収納課、各総合支所区民課(世田谷総合支所区民係、太子堂出張所、経堂出張所、北沢総合支所区民係、玉川総合支所区民係、用賀出張所、二子玉川出張所、砧総合支所区民係、烏山出張所、烏山総合支所区民・戸籍係)、各総合支所地域振興課まちづくりセンター(池尻、太子堂、若林、上町、経堂、下馬、上馬、梅丘、代沢、新代田、北沢、松原、松沢、奥沢、九品仏、等々力、上野毛、用賀、深沢、二子玉川、祖師谷、成城、船橋、喜多見、砧、上北沢、上祖師谷、烏山)	事前	
令和4年10月1日	Ⅱ-3-⑧使用方法	1. 収納事務 国民健康保険の資格、賦課情報から、保険料徴収対象者を把握し、収納事務を行う。	1. 収納事務 国民健康保険の資格、賦課情報から、保険料徴収対象者を把握し、収納事務を行う。 情報提供ネットワークシステムから公金受取口座情報を取得し、対象者の口座情報を特定し、還付事務を行う。	事前	
令和4年10月1日	Ⅱ-3-⑧情報の突合	1. 収納事務 保険料の納付データについて、国民健康保険の資格・賦課情報との突合を行う。	1. 収納事務 保険料の収納事務に係るデータについて、国民健康保険の資格・賦課情報、公金受取口座情報との突合を行う。	事前	
令和4年10月1日	Ⅱ-4-②取扱いを委託する特定個人情報ファイルの範囲その妥当性	保険料収納事務の遂行にあたっては、国民健康保険料のより正確な保険料徴収に必要な範囲の特定個人情報保有しているSKY2保険料収納システムの安定的な運営が不可欠であり、当該システムの円滑な保守運用業務を行う上で、国民健康保険料に係る滞納者のデータベース等を含むシステム上のあらゆる情報を取り扱う必要がある。	保険料収納事務の遂行にあたっては、国民健康保険料のより正確な保険料徴収及び還付事務に必要な範囲の特定個人情報保有しているSKY2保険料収納システムの安定的な運営が不可欠であり、当該システムの円滑な保守運用業務を行う上で、国民健康保険料に係る納付者・滞納者のデータベース等を含むシステム上のあらゆる情報を取り扱う必要がある。	事前	
令和4年10月1日	Ⅱ-4-③委託先における取扱者数 ⑥委託先名	10人以上50人未満 富士通株式会社	50人以上100人未満 富士通Japan株式会社	事前	
令和4年10月1日	Ⅱ-5-提供先1から17①法令上の根拠	番号法第19条第7号	番号法第19条第8号	事前	
令和4年10月1日	Ⅱ-5-提供先18①法令上の根拠	番号法第19条第7号 別表第2の119	番号法第19条第8号 別表第2の120	事前	
令和4年10月1日	Ⅱ-6-②保管期間その妥当性	納付が終了するまで、または滞納処分が終了するまで情報が必要となるため、保管する。 納付または滞納処分が終了した後は、適宜消去する。	国民健康保険法等において、データ保管期間の定めはなく、還付を含む収納事務や滞納処分が終了するまで、情報が必要となるため保管する。 収納事務又は滞納処分が終了した後は、適宜消去する。	事前	

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4年10月1日	Ⅱ-6-③消去方法	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、保守された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去する。	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、保守された情報が読み出しできないよう、物理的破壊により完全に消去する。	事前	
令和4年10月1日	(別添2)特定個人情報ファイル記録項目	口座情報	口座情報(公金受取口座情報を含む。)	事前	
令和4年10月1日	Ⅲ-3-リスク2 ユーザ認証の具体的な管理方法	・ユーザIDとパスワードによる認証を行う。 ・人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。	・職員証(ICカード)とパスワードの二要素によりユーザIDの認証を行う。 ・ユーザIDに付与されるアクセス権限によって、業務従事者が業務に必要な範囲の特定個人情報ファイルだけにアクセスすることができるように制御する。 ・人事異動等によりアクセス権限がなくなる場合は、速やかに失効処理を行う。	事前	
令和4年10月1日	Ⅲ-3-リスク2 特定個人情報の使用の記録の具体的な方法	・誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。	・誰が、いつ、どの情報にアクセスしたかについて、アクセスログを残して管理する。 ・特定個人情報のアクセスログについて、年一回以上随時分析し、業務時間帯以外のアクセス、業務上想定されない頻度のアクセスの有無がないか確認する。分析の結果は、情報システム管理者に報告する。	事前	
令和4年10月1日	Ⅲ-6-リスク1 リスクに対する措置の内容	(※2)番号法別表第2及び第19条第14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。	(※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。	事前	
令和4年10月1日	Ⅲ-6-リスク2 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＞ ・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、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・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。	事前	
令和4年10月1日	Ⅲ-6-リスク3 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＞ ・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、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が担保されている。	＜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が担保されている。	事前	

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4年10月1日	Ⅲ-7-リスク3 消去手順の内容	・納付が終了した後、または滞納処分が終了した後、情報を消去する。正しく消去されていることを職員が確認する。 ・紙媒体については、保管期間ごとに分けて保管し、保管期限の過ぎたものは外部業者による溶解処理を行う。	・収納事務又は滞納処分が終了した後、情報を適宜消去する。正しく消去されていることを職員が確認する。 ・紙媒体については、保管期間ごとに分けて保管し、保管期限の過ぎたものは外部業者による溶解処理を行う。	事前	
令和4年10月1日	Ⅳ-2 従業者に対する教育・啓発の具体的な方法	<世田谷区における措置> ①職員に対して、年一回、セキュリティ研修を行う際に、評価書を配布し、内容理解及びその遵守を徹底する。 ②委託先事業者の従業者については、契約時の仕様書に個人情報保護遵守を明記し、委託先事業者の責任者の責において、研修・指導を行わせる。必要に応じて、研修資料等を提供させ、実効性を担保する。 ③違反行為を行った者に対しては、指導を行う。違反行為の程度によっては、懲戒の対象となりうる。また、全従業者に対して、違反事項発生を周知し、再発防止を徹底する。	<世田谷区における措置> ①職員が番号制度に関する基礎的事項を常時確認できるよう、研修資料を庁内公開している。また、研修資料は毎年度見直しを実施している。 ②委託先事業者の従業者については、契約時の仕様書に個人情報保護遵守を明記し、委託先事業者の責任者の責において、研修・指導を行わせる。必要に応じて、研修資料等を提供させ、実効性を担保する。 ③違反行為を行った者に対しては、指導を行う。違反行為の程度によっては、懲戒の対象となりうる。また、全従業者に対して、違反事項発生を周知し、再発防止を徹底する。	事前	
令和4年10月1日	Ⅳ-3 その他のリスク対策	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。 ②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。	<世田谷区における措置> ・世田谷区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条例第7条及び同条例施行規則第6条の規定に基づき、マイナンバー制度セキュリティ会議を設置し、特定個人情報ファイルの取扱いに関する企画及び運用計画、セキュリティ対策等を審議する。 <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、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。 ②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。	事前	
令和4年10月1日	V-④個人情報ファイル名	—	追加 国民健康保険料過誤納金還付請求書	事前	
令和5年11月1日	Ⅵ評価実施手続 1. 基礎項目評価 ①実施日	令和4年5月1日時点	令和5年11月1日時点	事後	
令和6年12月1日	Ⅰ-2-システム1③他システムとの接続	既存住民基本台帳システム 税務システム	削除	事後	
令和6年12月1日	Ⅱ-5 特定個人情報の提供の有無	提供を行っている	提供を行っていない	事後	

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12月1日	Ⅱ-5 特定個人情報の提供の有無	提供先1～18	削除	事後	
令和6年12月1日	Ⅱ 特定個人情報ファイルの概要 ー別添2ファイルの記録項目 ー収納管理台帳ファイル	納税義務者番号、本税調定額 本税収入額 本税仮消込額 本税被充当予定額 本税未納額 本税過誤納額	納付義務者番号、保険料調定額 保険料収入額 保険料仮消込額 保険料被充当予定額 保険料未納額 保険料過誤納額	事後	
令和6年12月1日	Ⅱ 特定個人情報ファイルの概要 ー別添2ファイルの記録項目 ー滞納管理台帳ファイル	本税分納額	保険料分納額	事後	
令和6年12月1日	Ⅵ評価実施手続 1. 基礎項目評価 ①実施日	令和5年11月1日時点	令和6年12月1日時点	事後	
令和7年8月6日	Ⅱ-6-①保管場所	①中間サーバー・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ー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された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。	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	

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8月6日	Ⅱ-6-③消去方法	①特定個人情報の消去は世田谷区から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、保守された情報が読み出できないよう、物理的破壊により完全に消去する。	①特定個人情報の消去は世田谷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	
令和7年8月6日	Ⅲ-6-リスク4 リスクに対する措置の内容	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。	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できない。	事前	
令和7年8月6日	Ⅲ-6-リスク6 リスクに対する措置の内容	③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	
令和7年8月6日	Ⅲ-6-リスク7 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	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。	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	

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8月6日	Ⅲ-7-⑤物理的対策 具体的な対策の内容	①中間サーバー・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ー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された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。	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	
令和7年8月6日	Ⅲ-7-⑥技術的対策 具体的な対策の内容	—	追加 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	
令和7年8月6日	Ⅳ-1-②監査 具体的な内容	・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、定期的に監査を実施することとしている。	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	

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8月6日	IV-3. その他のリスク対策	①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	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	
令和7年9月1日	I-5法令上の根拠	番号法第9条第1項 別表の30の項	番号法第9条第1項 別表の44の項	事後	
令和7年9月1日	I-6-②法令上の根拠	【情報照会】番号法第19条第8号に基づく主務省令第2条の表160の項	【情報照会】番号法第19条第8号に基づく主務省令第2条の表69の項	事後	
令和7年9月1日	VI評価実施手続 1. 基礎項目評価 ①実施日	令和6年12月1日時点	令和7年9月1日時点	事後	
令和8年8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 ①委託内容	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出、ガバメントクラウドへのシステム構築・データ移行等	事前	
令和8年8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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	
令和8年8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: 特定個人情報の漏洩・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おける措置>について記載なし	<ガバメントクラウドにおける措置>について記載追加	事前	

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8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 洩・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おける措置＞について記 載なし	＜ガバメントクラウドにおける措置＞について記 載追加	事前	
令和8年8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おける措置＞について記 載なし	＜ガバメントクラウドにおける措置＞について記 載追加	事前	
令和8年8月1日	Ⅳ その他のリスク対策 1. 監査 ②監査 具体的な内容	＜ガバメントクラウドにおける措置＞について記 載なし	＜ガバメントクラウドにおける措置＞について記 載追加	事前	
令和8年8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おける措置＞について記 載なし	＜ガバメントクラウドにおける措置＞について記 載追加	事前	

改定前の特定個人情報保護評価書との相違点及び審査の観点(国民健康保険 保険料収納事務)

I 基本情報					
(別添1)事務の内容					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
1	114	(別添1)事務の内容	ガバメントクラウドの 範囲を明記	ガバメントクラウドの範囲を記載	ガバメントクラウドの範囲の記載なし
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					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
2	117	委託事項1 ①委託内容	ガバメントクラウド(デジタル庁調達)移行に伴い、追加する委託内容は妥当か	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出、 <u>ガバメントクラウドへのシステム構築・データ移行等</u>	SKY2国民健康保険システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等
6. 特定個人情報の保管・消去					
3	119	①保管場所	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止:外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退室管理:ICカード+手のひら静脈認証、要員所在管理システム ③持込・持出防止:金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 申請書及び届出書等の紙媒体、及び外部記録媒体は、鍵のかかるロッカーや保管庫に保管している。 <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。
4	119	③消去方法	ガバメントクラウド(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <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 SP800-88、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壊等を実施する。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> ①データベースに登録されたデータは、システム機能にて完全に消去する。 ②申請書及び届出書等の紙媒体については、外部業者による溶解処理を行う。 ③外部記憶媒体に一時的に登録した特定個人情報等の申請データは、使用の都度速やかに完全消去する。 <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世田谷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。

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					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
5	129	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(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <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。 <中間サーバー・プラットフォームにおける措置> (同右)	<世田谷区における措置> 世田谷区事務センター、システム運用委託先業者のデータセンター等において、以下の対策を実施している。 ①外部進入防止: 外周赤外線センサー監視、24時間有人監視、監視カメラ ②入退館管理: ICカード+手のひら静脈認証、要員所在管理システム ③持込・持出防止: 金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理 ④LGWAN 接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ⑤外部記憶媒体については、限定された USB メモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 <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。
6	130	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(デジタル庁調達)における措置が適切か	<世田谷区における措置> (同右) <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、ネットワークアクセシビリティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDoS対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <中間サーバー・プラットフォームにおける措置> (同右) <国保総合(国保集約)システムにおける措置> (同右)	<世田谷区における措置> ・SKY2国民健康保険システムへのアクセス時におけるICカード+パスワード認証 ・ウイルス対策ソフトウェアの導入 ・外部ネットワークと遮断された庁内ネットワーク ・LGWAN 接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 <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。 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。 <国保総合(国保集約)システムにおける措置> ・区市町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。 ・国保総合PCで使用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。 ・国保総合PCIには、ウイルス対策ソフトウェアを導入し、ウイルスパターンファイルは適時更新する。 ・不正アクセス防止策として、ファイアウォールを導入している。 ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。

7	131	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(デジタル庁調達)における措置が適切か	(同右) ＜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 SP800-88、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。	・収納事務又は滞納処分が終了した後、情報を適宜消去する。正しく消去されていることを職員が確認する。 ・紙媒体については、保管期間ごとに分けて保管し、保管期限の過ぎたものは外部業者による溶解処理を行う。
---	-----	---	------------------------------	--	---

Ⅳ その他のリスク対策

1. 監査					
通番	ページ	項目	審査の観点 主な相違点	改定後(下線部が修正・追記箇所)	改定前(下線部が修正・削除箇所)
8	132	②監査 具体的な内容	ガバメントクラウド(デジタル庁調達)における措置が適切か	＜世田谷区における措置＞ (同右) ＜中間サーバー・プラットフォームにおける措置＞ (同右) ＜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。	＜世田谷区における措置＞ 適正な個人情報の保護やリスク対策を図るため、監査計画を策定し、定期的及び必要に応じて随時、より客観的な評価ができる監査を実施し、監査の結果を踏まえて必要な改善を行う。監査に当たっては、以下の観点から実施する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規程・体制整備 ・個人情報保護に関する人的安全管理措置 ・安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 ＜中間サーバー・プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 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。
3. その他のリスク対策					
9	133	その他のリスク対策	ガバメントクラウド(デジタル庁調達)における措置が適切か	＜世田谷区における措置＞ (同右) ＜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。 ＜中間サーバー・プラットフォームにおける措置＞ (同右)	＜世田谷区における措置＞ ・世田谷区行政手続における特定個人を識別するための番号の利用等に関する条例第7条及び同条例施行規則第6条の規定に基づき、マイナンバー制度セキュリティ会議を設置し、特定個人情報ファイルの取扱いに関する企画及び運用計画、セキュリティ対策等を審議する。 ＜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。 ②中間サーバーについて、地方公共団体にとって必要な意見を国やJ-LISに上げていく。