特定個人情報保護評価書（重点項目評価書）

評価書番号	評価書名
22	岐阜市　介護保険事務　重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

岐阜市は、介護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理解し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	岐阜市では「岐阜市特定個人情報ファイル安全管理規程」を定めており、特定個人情報保護評価については本規程を活用したリスク評価を実施している。 介護保険事務では、事務の一部を外部業者に委託しているため、業者選定の際に業者の情報保護管理体制を確認し、併せて秘密保持に関しても契約に含めることで万全を期している。

評価実施機関名

岐阜市長

公表日

［令和7年5月　様式3］

項目一覧

Ⅰ　基本情報

1．特定個人情報ファイルを取り扱う事務	
①事務の名称	介護保険事務
②事務の内容	岐阜市は、介護保険法（平成９年法律第１２３号）及び行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）の規定に従い、特定個人情報を以下の事務で取り扱う。 ・第1号被保険者の資格取得、資格喪失、変更等の届出 ・第1号、第2号被保険者の被保険者証交付、再交付申請等の申請 ・保険料賦課、特別徴収額の通知 ・保険料の収納、還付 ・保険料の減免、徴収猶予等の申請 ・保険料滞納者に係る支払い方法の変更 ・要支援認定、要介護更新認定等の申請 ・居宅介護福祉用具購入費、介護予防福祉用具購入費、居宅介護住宅改修費等の支給 ・居宅サービス、介護予防サービス等の計画作成依頼 ・負担限度額認定や各種減免認定の申請 ・高額介護サービス費、高額介護予防サービス費、高額医療合算介護サービス費等の支給申請 ・保険者事務共同処理業務 　高額医療合算介護（予防）サービス費の事務に個人番号を利用し、当市の介護保険と国民健康保険の給付情報に関する名寄せを行う。 　また高額障害福祉サービス等給付費支給の事務に個人番号を利用し、当市の介護保険と障害者総合支援の給付情報に関する名寄せを行う。 ※当市では、「保険者事務共同処理業務」について、国民健康保険団体連合会（国保連合会）に委託をして事務を実施しており、国保連合会が当該事務を実施するにあたって、個人番号が記載された「受給者異動連絡票（訂正時には訂正連絡票）」を提供している。 　番号法に基づいて、岐阜市は、介護保険に関する事務において、情報提供ネットワークシステムに接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。情報提供に必要な情報を「副本」として中間サーバーへ登録する。 〇地域支援事業に関する事務 ・被保険者の保健医療の向上及び福祉の増進を図るため、被保険者、介護サービス事業者その他の関係者が被保険者に係る情報を共有し、及び活用することを促進する事業として、介護情報基盤を活用した情報連携を実施する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務＞ ・市区町村は、介護情報基盤へ本事務に係る対象者の個人番号を含む対象者情報、介護保険関係情報、介護保険認定情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の紐付け及び登録を行う。 ・介護サービス事業所は、介護保険資格確認等WEBサービス経由で、事業所の利用者に関して市区町村が登録した情報の確認等を行う。 ・住民は、マイナポータル経由で、本事務に係る自身の介護保険資格情報、介護保険認定審査進捗情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の情報の確認等を行う。
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

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	介護保険システム
②システムの機能	1. 資格管理機能 住民基本台帳などの情報をもとに被保険者台帳を作成し、被保険者の資格取得や資格喪失の管理及び住所地特例者や適用除外者の管理を行う。 2. 納付機能 第一号被保険者の保険料の賦課、徴収方法(特別徴収又は普通徴収)の決定、収納実績、滞納、過誤納の管理を行う。 3. 認定機能 要介護・要支援認定申請の受付から認定結果登録までの管理を行う。 4. 受給機能 要介護・要支援と認定された被保険者の居宅サービス計画作成依頼情報や介護保険施設の入退所者情報を管理する。 利用者負担減免や負担限度額認定を管理する。 国民健康保険団体連合会に受給者台帳を送付する。 5. 給付機能 国民健康保険団体連合会からの現物給付実績を受け取り、給付実績を管理する。また、償還払い支給の実績管理を行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [○] その他　(認定審査会支援システム　伝送通信ソフト　)

システム2	
①システムの名称	共通基盤連携システム（庁内連携システム、宛名システム（以下「統合宛名システム」という。）等を含む。）
②システムの機能	1．統合宛名機能 （1）団体内統合宛名番号採番機能 業務システムからの要求に応じて、団体内統合宛名番号を採番し、業務システム及び中間サーバに返却する。 （2）番号管理情報更新機能 住民基本台帳情報（現存者）、宛名（住登外）情報の更新データが送付されてきた場合に、団体内統合宛名番号、個人番号、宛名番号（業務）の紐付け情報を更新する。 （3）業務システム連携機能 業務システムからの要求に応じて、個人番号、又は団体内統合宛名番号に紐付く宛名情報を返却する。 （4）業務システム連携機能（番号情報） 業務システムからの要求があったとき又は番号管理情報の変更の際に、宛名番号（業務）に紐付く個人番号及び団体内統合宛名番号を返却する。 （5）団体内統合宛名番号表示機能 業務システムで団体内統合宛名番号を保持しない、またはシステム化されていない業務向けに、番号の紐付け情報を検索・表示する。 （6）中間サーバ連携機能（5情報提供） 中間サーバ又は中間サーバ接続端末からの要求に応じて、団体内統合宛名番号に紐付く宛名情報を返却する。 2．中間サーバ連携機能 （1）情報提供機能 統合DBから特定個人情報を抽出し、中間サーバに連携（提供）する。 3．情報照会機能 （1）情報照会機能 業務システムから「他団体への情報照会依頼」を受信する。 （2）情報照会連携機能 業務システムから受信した「他団体への情報照会依頼」を中間サーバに連携する。 （3）照会結果取得機能 中間サーバから「他団体からの情報提供内容」を受信する。 （4）照会結果回答機能 中間サーバから受信した「他団体からの情報提供内容」を業務システムに連携する。 （5）番号変換機能 宛名番号（業務）⇔団体内統合宛名番号の変換を行う。 （6）文字コード変換機能 業務システムにて使用しているデータの文字コードを変換する。
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	1．符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「統合宛名番号」とを紐付け、その情報を保管・管理する。 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。 3．情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。 4．各事務システム接続機能 中間サーバと各事務システム、統合宛名システム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。 5．情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 6．情報提供データベース管理機能 特定個人情報（連携対象）を副本として，保持・管理する。 7．データ送受信機能 中間サーバ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。 8．セキュリティ管理機能 セキュリティを管理する。 9．職員認証・権限管理機能 中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う。 10．システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼動状態の通知、保管切れ情報の削除を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [○] その他　（ 共通基盤連携システム　　）
システム4	
①システムの名称	認定審査会支援システム
②システムの機能	1．認定機能 要介護・要支援認定申請の受付から認定結果登録までの管理を行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（ 介護保険システム　　）

システム5	
①システムの名称	伝送通信ソフト
②システムの機能	1．受給者情報異動連絡票データの送信 受給者情報異動連絡票データを暗号化し、国民健康保険団体連合会へ送信する。 2．受給者情報訂正連絡票データの送信 受給者情報訂正連絡票データを暗号化し、国民健康保険団体連合会へ送信する。 ※伝送通信ソフトとは、国保連合会が介護保険審査支払等システムにて使用するデータについて、電子メール方式で保険者（市区町村）と国民健康保険団体連合会との間で、データの送受信を行うシステムのことをいう。なお、保険者と国民健康保険団体連合会との通信環境は専用回線を使用している。
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　（ 介護保険システム　）

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	【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　（ e-Gov電子申請サービス　）

システム7	
①システムの名称	介護情報基盤
②システムの機能	＜介護情報基盤を活用した情報連携に係る介護保険事務＞ 介護情報基盤が介護保険に係る各種データを扱う際には、個人を特定するキーとして、介護保険被保険者番号又はPublic Medical Hub（以下「PMH」という。）固有の識別子（PMHキー）にて制御する仕様としている（PMHキーは、特定個人情報と紐づけることで個人を特定するキーである）。詳細な機能は以下のとおり。 ①特定個人情報の登録・管理 ・情報連携のため、本市区町村は、介護情報基盤（PMH介護領域）へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。（LGWAN回線等経由） ・介護情報基盤に登録された特定個人情報は、自治体からのアクセスのみに制御される。また特定個人情報を出力する機能はない。 ②PMHキー採番 ・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。 （連携後、マイナポータル上からPMHキーは削除される。）以降、マイナポータルからの介護情報参照等が可能となる。 ③介護保険資格確認等WEBサービスからの参照 ・介護事業所が介護保険資格確認等WEBサービス経由で、事業所にて管理している被保険者の介護情報を確認する。 ・介護保険資格確認等WEBサービスは、被保険者番号をキーに介護情報基盤に対して介護情報（証等の情報、認定情報等）を照会する。 ・介護情報基盤は被保険者番号をキーに介護情報基盤の介護情報を取得し返却する。 ④マイナポータルからの参照 ・住民がマイナポータル経由で、自身の介護保険情報を確認する。 ・マイナポータルは、PMH仮名識別子をキーに介護情報基盤に被保険者情報を照会する。 ・介護情報基盤はPMH共通にPMH仮名識別子を連携しPMHキーを取得し、PMHキーをキーに介護情報基盤の介護情報を取得し返却する。
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　（ 介護保険システム　　）

システム8	
①システムの名称	
②システムの機能	
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　（　）
システム9	
①システムの名称	
②システムの機能	
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　（　）
システム10	
①システムの名称	
②システムの機能	
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　（　）
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
介護保険システムファイル	
4. 個人番号の利用 ※	
法令上の根拠	1. 番号法 ・番号法第9条第1項　別表の100の項 2. 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別表の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号。以下「番号法別表主務省令」という。） ・番号法別表主務省令第50条
5. 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	1　情報提供の根拠 ・番号法第19条第8号 ・番号法第19条第8号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁・総務省令第9号。「番号法第19条第8号主務省令」という。）第2条の表において、介護保険給付等関係情報及び介護保険法による給付の支給に関する情報を提供することとされているもの 2　情報照会の根拠 ・番号法第19条第8号 ・番号法第19条第8号主務省令第2条の表の131の項 ・番号法第19条第8号主務省令第2条の表の132の項
6. 評価実施機関における担当部署	
①部署	岐阜市役所　福祉部　介護保険課
②所属長の役職名	介護保険課長
7. 他の評価実施機関	

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	
介護保険システムファイル	
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 ※	介護保険法第9条（被保険者）に基づき、岐阜市が保険者となる第1号被保険者及び第2号被保険者のうち要介護（要支援）認定申請を行った者並びにその世帯員等（資格喪失者を含む。）
その必要性	介護保険の公平かつ適正な申請・届出業務を行うため、本人を正確に確認し、介護保険の被保険者に関する情報を適切に取得・管理する必要がある。
④記録される項目	[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 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　（　公的給付支給等口座情報　）
その妥当性	・個人番号、その他識別情報（内部番号） ：本人確認等、対象者を正確に特定するために保有 ・5情報、連絡先等情報、その他住民票関係情報 ：対象者の申請・届出時点の居住地、世帯情報を把握するために保有 ・介護・高齢者福祉関係情報 ：介護保険の被保険者の管理を行うために保有 ・地方税関係情報・医療保険関係情報・生活保護・社会福祉関係情報・年金関係情報 ：介護保険料の賦課処理を行うために保有 ・その他（公金給付支給等口座情報） ：給付支給等口座情報に保険料の還付及び申請のあった各種給付金等を振り込むため ＜介護情報基盤を活用した情報連携に係る介護保険事務＞ ・識別情報 介護被保険者番号、個人番号（マイナンバー）、PMHキー…介護情報基盤が外部と情報連携するために必要となる。 ・業務関係情報 介護・高齢者福祉関係情報…（介護保険事務の適切な実施にあたり必要となる情報を管理し、）介護情報基盤が、外部と情報連携するために必要となる。
全ての記録項目	別添1を参照。
⑤保有開始日	平成27年10月1日
⑥事務担当部署	福祉部介護保険課

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 （ 市民課/市民税課/生活福祉一課・生活福祉二課・生活福祉三課/国保・年金課/福祉医療課 ） [○] 行政機関・独立行政法人等 （ デジタル庁 ） [○] 地方公共団体・地方独立行政法人 （ 他市町村 ） [ ] 民間事業者 （ ） [○] その他 （ 社会保険診療報酬支払基金 ）
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、LGWAN回線を用いた介護保険システムからのデータ連携、医療保険者等向け中間サーバー ）
③使用目的 ※		介護保険料の賦課、被保険者の資格管理、保険給付の支給、要介護認定等の業務をより適正に実施するため。
④使用の主体	使用部署	介護保険課、高齢福祉課、西部事務所、東部事務所、北部事務所、南部東事務所、南部西事務所、日光事務所、柳津地域事務所、市民課
	使用者数	[100人以上500人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑤使用方法		・被保険者の認定に関する業務の管理に使用 ・被保険者の資格に関する業務の管理に使用 ・被保険者の給付に関する業務の管理に使用 ・被保険者の受給に関する業務の管理に使用 ・被保険者の賦課に関する業務の管理に使用 ・被保険者の収滞納に関する業務の管理に使用 ＜介護情報基盤を活用した情報連携に係る介護保険事務＞ ・情報連携のため、本市区町村は、介護情報基盤（PMH介護領域）へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。（LGWAN回線等経由） ・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 ・医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。（連携後、マイナポータル上からPMHキーは削除される。）以降、マイナポータルからの介護情報参照等が可能となる。
	情報の突合	・被保険者の管理・処理を行うため、介護保険システムに保有する情報と突合を行う
⑥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] (5) 件	<選択肢> 1) 委託する 2) 委託しない
委託事項1		介護システム等運用業務委託	
①委託内容		介護システム等の始業点検、ヘルプデスク、不具合切り分け、定例処理等の運用業務	
②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
③委託先名		タック株式会社	
再委託	④再委託の有無 ※	[再委託しない]	<選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法		
	⑥再委託事項		
委託事項2～5			
委託事項2		介護システム等パッケージソフトウェア保守業務委託	
①委託内容		介護システム等の問合せ対応、バージョンアップ対応、障害対応等の保守業務	
②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
③委託先名		株式会社 日立システムズ 中部支社	
再委託	④再委託の有無 ※	[再委託しない]	<選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法		
	⑥再委託事項		
委託事項3		申請受付、データ入力及び帳票出力業務	
①委託内容		申請受付、データ入力及び帳票出力	
②委託先における取扱者数		[10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
③委託先名		株式会社 アシスト	
再委託	④再委託の有無 ※	[再委託しない]	<選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法		
	⑥再委託事項		

委託事項4		保険者事務共同処理業務（高額医療合算介護（予防）サービス費算定業務）
①委託内容		介護保険法第51条の2及び第61条の2に基づき支給する高額医療合算介護（予防）サービス費について、当市は国保連合会に対して、個人番号を利用した被保険者向け勧奨通知作成の事務を委託する。 また、障害者の日常生活及び社会生活を総合的に支援するための法律第76条の2に基づき支給する高額障害福祉サービス等給付費について、当市は、国保連合会に対して、個人番号を利用した同法に基づくサービス受給者に係る介護保険利用者負担額の情報提供事務を委託する。 なお、当該委託業務において個人番号を利用することは、番号法別表主務省令第50条第3号において、介護給付、予防給付又は市町村特別給付の支給に関する事務と整理され、同令第60条第7号において自立支援給付の支給に関する事務と整理されているため妥当である。
②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
③委託先名		岐阜県国民健康保険団体連合会
再委託	④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
	⑤再委託の許諾方法	原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、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、再委託予定金額等及びその他当市のセキュリティー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及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、必要な手続を経た上で、再委託を承認する。
	⑥再委託事項	国保連合会の保険者事務共同処理業務で使用する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5		総合窓口受付業務委託
①委託内容		総合窓口で実施する介護保険窓口業務
②委託先における取扱者数		[　100人以上500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
③委託先名		パーソルビジネスプロセスデザイン株式会社
再委託	④再委託の有無 ※	[　再委託しない　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項6		介護情報基盤を活用した情報連携に係る介護保険事務における特定個人情報ファイルの一部の取扱
①委託内容		介護情報基盤の利用・情報連携業務及び運用保守業務
②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
③委託先名		岐阜県国民健康保険団体連合会（岐阜県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	④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
	⑤再委託の許諾方法	書面又は電磁的方法による承諾
	⑥再委託事項	介護情報基盤におけるPMHキーを用いた情報連携 介護情報基盤の運用保守

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 （ 20 ）件 [○] 移転を行っている （ 8 ）件 [ ] 行っていない
提供先1	別紙1のとおり
①法令上の根拠	別紙1のとおり
②提供先における用途	別紙1のとおり
③提供する情報	別紙1のとおり
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	別紙1のとおり
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	別紙1のとおり
提供先2～5	
提供先2	
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	別紙2のとおり
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	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	別紙2のとおり
①法令上の根拠	別紙2のとおり
②移転先における用途	別紙2のとおり
③移転する情報	別紙2のとおり
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	別紙2のとおり
⑥移転方法	[○] 庁内連携システム　　[　] 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　（介護保険システムから抽出した特定個人情報ファイルを、住民情報系ネットワーク内の共有フォルダを介して移転する）
⑦時期・頻度	照会を受けたら都度
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

保管場所 ※	＜岐阜市における措置＞ ・介護保険システムのサーバは、外部データセンター内のサーバ室に設定しており、サーバ室への入退室は、職員、保守事業者等のうち入室を許可された者のみに制限し管理しており、入室の事前申請の承認、入退室管理簿の記録をしている。 ・データセンター内のサーバ室への入退室は、ICカード（許可された者のみ所有）、静脈認証等の生体認証、パスワード（許可された者ごとに設定）による認証を必要とし、また監視カメラによる監視をしている。 ・サーバ室へのパソコン、外部記憶媒体、通信機器等の無断持ち込みを禁止している。 ・データの滅失、毀損を防止するため、サーバ室は火災、水害、埃、振動、温度等の対策がされ、非常用電源及び無停電電源装置を備えている。 ＜本庁マシン室における措置＞ ・入室は入口ドアのパスワード認証、入退室管理簿の記録で管理している。 ・監視カメラにより、入退室や作業状況を監視している。 ・停電(落雷等)によるデータの消失を防ぐために、無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・端末はセキュリティワイヤーで固定する。 ＜各課事務室における措置＞ ・各課事務室の全端末はセキュリティワイヤー等で固定されている。 ・各課事務室の全端末の配線については、整理・集約し、引っかけ・抜け防止策を実施している。 ・申請書等は鍵付きキャビネットに保管している。 ・総合窓口事務室への入室はICカードにより厳重に管理されている。 ・業務時間外の総合窓口事務室はシャッターで閉鎖される。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ガバメントクラウドにおける措置＞ ・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。 ・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。 ・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。 ・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、NIST800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ・既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データの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。 ＜介護情報基盤を活用した情報連携に係る介護保険事務＞ ・特定個人情報の格納領域を分けて、ユーザアカウント権限の制御を行い、さらにアクセス者の識別を行う。 ・外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離する。 ・不正侵入を検知・防御するシステムを導入することで、ネットワーク、Webアプリケーションへの不正アクセスを防止する。 ・ログ監査により、不正アクセスを検知する。 ・データ暗号化、通信暗号化を行う。

7. 備考

（別添１）特定個人情報ファイル記録項目

介護保険者番号, 被保険者番号, 履歴通番, 介護異動事由コード, 異動年月日, 資格異動届出者氏名（漢字）,
資格異動届出者関係コード, 資格異動届出者電話番号, 資格異動届出年月日, 資格取得事由コード, 資格取得年月日,
資格取得届出者氏名（漢字）, 資格取得届出者関係コード, 資格取得届出者電話番号, 資格取得届出年月日, 資格喪失事由コード,
資格喪失年月日, 資格喪失届出者氏名（漢字）, 資格喪失届出者関係コード, 資格喪失届出者電話番号, 資格喪失届出年月日,
個人番号, 個人区分コード, 住基ネット個人番号, 都道府県コード, 市町村コード, 町名コード, キー氏名（カナ）,
あいまい検索キー氏名（カナ）, 氏名（カナ）, 通称名（カナ）, キー氏名（漢字）, 氏名（漢字）, 通称名（漢字）,本名通称名区分コード,
氏名（英字）, 併記用氏名（漢字）, 氏名分類コード, 生年月日年号コード, 生年月日, 性別コード,都道府県名（漢字）,
市町村名（漢字）,住所（漢字）,番地（漢字）,方書（漢字）,住所（漢字）連結,親郵便番号,子郵便番号電話番号,
転入元市町村名（漢字）,住所地特例者区分コード,住所地特例者適用開始年月日,住所地特例者適用変更年月日,
住所地特例者適用終了年月日,適用除外事由コード,適用除外開始年月日,適用除外終了年月日,賦課対象コード,
記載１備考（漢字）,記載２備考（漢字）記載３備考（漢字）,番地区分コード,番地,号番号枝番号,行政区コード,方書（カナ）,
市内外区分コード,政令広域コード,地方公共団体コード,外国人在留資格期間コード,外国人在留開始年月日,
外国人在留終了年月日,外国人在留資格コード,世代通番,抑止コード,日常生活圏域コード,受給者履歴通番,
受給者要介護状態区分コード,受給者認定年月日,受給者結果変更事由コード,受給者認定結果通知書発行年月日,
受給者認定有効期間開始年月日,受給者認定有効期間終了年月日,受給者支給限度管理期間終了年月日,受給者再審査フラグ,
受給者申請取消事由コード,受給者申請取消年月日,受給者認定中断事由コード,受給者認定中断年月日,
受給者認定取消事由コード,受給者認定取消年月日,受給者申請事由コード,受給者申請年月日,受給者申請かかりつけ医コード,
受給者申請者関係コード,受給者訪問対象地区コード,受給者識別コード,
受給者同意書有無コード,受給者前保険者名（漢字）,受給者申請者名（漢字）,受給者申請者電話番号,受給者申請書備考（漢字）,
受給者居宅住所都道府県コード,受給者居宅住所市町村コード,受給者居宅住所町名コード,受給者居宅都道府県名（漢字）,
受給者居宅市町村名（漢字）,受給者居宅住所（漢字）,受給者居宅番地（漢字）,受給者居宅方書（漢字）,受給者居宅親郵便番号,
受給者居宅子郵便番号,受給者居宅電話番号,受給者居宅市内外区分コード,受給者特定疾病コード,受給者政令広域コード,
受給者介護要状態コード,受給者労災等番号,処理年月日,受給者みなし認定区分コード,
受給者介護保険審査会結果前要介護状態区分コード,区分変更用前回受給者履歴通番,経過措置前情報（結果、有効期間、希望）,
通知書理由,賦課年度,納付原簿履歴通番,納付原簿入力所得区分コード,納付原簿所得区分コード,徴収方法区分コード,
納付原簿調定額,納付原簿年額,納付原簿月割額,納付原簿確定保険料額,納付原簿賦課年月日,納付原簿賦課期日年月日,
納付原簿通知書通知理由コード,納付原簿賦課結果コード,納付原簿前回徴収方法区分コード,納付原簿納入通知書発行年月日,
納付原簿特別徴収義務者コード,納付原簿年金コード,納付原簿基礎年金番号,納付原簿回付情報各種年月日,
納付原簿特別徴収依頼作成年月日,納付原簿特別徴収中止区分コード,納付原簿特別徴収中止事由コード,
納付原簿特別徴収中止依頼作成年月日,納付原簿特別徴収中止通知書発行年月日,納付原簿仮徴収額変更年月日,
納付原簿仮徴収額変更依頼作成年月日,納付原簿仮徴収額変更通知書発行年月日,納付原簿減免区分コード,
納付原簿徴収猶予区分コード,納付原簿全期前納報奨金額,納付原簿調定取消事由コード,納付原簿調定取消年月日,
納付原簿行政区コード,納付原簿政令広域コード,納付原簿更正操作者コード,納付原簿激変緩和措置フラグ,
納付原簿特例標準割合適用フラグ,納付原簿３段階特例標準割合適用フラグ,納付原簿更新画面の備考,
仮徴収額変更の変更後所得段階X,仮徴収額変更の変更後特例（標準）割合,適用フラグ,
仮徴収額変更の変更後３段階特例（標準）,割合適用フラグ,更新通番,
更新操作者コード,更新年月日,更新時刻,作成操作者コード,作成年月日,作成時刻

Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名	
介護保険システムファイル	
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:　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	・本人等からの申告・申請情報の入手については、届出の窓口において対象者以外の情報を入手しないよう、本人確認書類（身分証明書等）の確認を厳格に行う。 ・届出書の様式は必要な対象者以外の情報及び不必要な情報が記載されないよう定められている。 ・届出及び申請内容を複数人で審査・確認し、対象者以外の情報及び不必要な情報の入手の防止に努める。 ・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、対象以外の情報の入手を防止する。 ・申請時に個人番号付電子申請データに電子証明書を付与することで、本人以外のなりすましを防止する。 ・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。 ・庁内他部署からの入手は庁内連携システムを利用し、対象者以外の情報及び不必要な情報の入手ができないよう制限している。 ・職権を濫用し、利用目的以外の目的で特定個人情報を収集してはならないことについて、情報セキュリティー教育で規定や罰則について周知する。 ・入手する特定個人情報の利用目的を変更する場合には、岐阜市個人情報保護審議会の意見を聴き、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲内で行う。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・定められたインターフェース仕様に沿って決められたデータ項目のみが返却されるようシステム的に制御している。自治体ごとのアクセス制御も実施する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）からPublic MedicalHub（PMH）に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

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
・不適切な方法で入手が行われるリスクに対する措置 ：届出・申請においては書面にて本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を行うこととする。 ：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、のち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誘導において住民に何の手続き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もらい、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な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できるよう措置を講じている。 ：システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ：認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を実施する。 ：システムの操作履歴（アクセスログ・操作ログ）を記録し、不正行為を行っていないことを確認する。 ・入手した特定個人情報が不正確であるリスクに対する措置 ：入手した情報については、窓口での聞き取りや本人確認書類との照合等を通じて確認することで正確性を確保している。 ：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。 ：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。 ：職員にて収集した情報に基づいて入力、削除及び訂正を行う際は、正確性を確保するために、入力、削除及び訂正を行なった者以外の者が確認する等、必ず入力、削除及び訂正した内容を確認する。 ・入手の際に特定個人情報が漏えい・紛失するリスクに対する措置 ：書面は直接手渡しで、受領することを原則とする。 ：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。 ：サービス検索・電子申請機能と e-Gov電子申請サービスは、専用線であるGSS G-Net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。 ：端末から一時的に離席する際は端末にロックをかけ、作業後はログオフを行う。 ：システムへの入力は、岐阜市の施設以外及び岐阜市の保有する端末以外で実施できない。

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
リスクに対する措置の内容	・統合宛名システムは、特定個人情報を取り扱う事務ごとに、特定個人情報の使用目的で認められる範囲の対象者及び情報以外が参照できないようアクセス制御を行っている。 ・特定個人情報ファイルには、適切な権限がある担当者のみがアクセスできるよう設計されている。適切な権限がある担当者からのアクセスであっても個人番号を表示する必要ない業務（機能）からのアクセスについては、個人番号を画面表示しない設計としている。 ・情報セキュリティ管理者は、職員が管理する課共有フォルダ内において、業務に必要のない特定個人情報が収集・保管されていないことを定期的に確認する。 〈介護情報基盤を活用した情報連携に係る介護保険事務における追加措置〉 ・個人情報を格納する領域については、外部連携先システムが直接アクセスが行えないようネットワークを分離をするとともにシステム自動処理により、介護情報基盤システム内に格納される運用になっている。 ・外部連携先システムとの通信はVPN等の技術を用いた暗号化を行うことで通信内容秘匿、盗聴対策の対応をしている。
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： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている]　＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・システムへのアクセスにおいて、システムを利用する必要がある職員を特定し、ユーザID/パスワードによる認証を実施している。 ・認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不正利用が行えない対策を実施する。 ・パスワードには、有効期限の設定、同一又は類似パスワード再利用制限、最低文字数の設定等を行っている。 ・識別情報（ユーザID/パスワード）を複数人で共有することを禁止している。 ・端末のパスワードの記録機能を使用しない。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・介護情報基盤へのログインはユーザID、パスワードで行う。 ・ログイン用のユーザIDは、管理者がユーザ登録を行った者に限定して発行される。
その他の措置の内容	・アクセス権限の管理 ：アクセス権限と業務（担当職員）の対応表を作成し、ID/パスワードの発行管理を行う。 ：業務に対応したアクセス権限を確認し、業務に必要なアクセス権限のみを申請する。 ：権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を更新し、当該IDを失効させる。 ：権限の申請・変更・失効については申請書を使用し、記録を残す。 ：パスワードに有効期限を設け、定期的にパスワードの変更を行わないと、システムが利用できないよう設定する。 ：システム保守運用等のために管理者権限等の特権を付与されたID（以下「特権ID」という。）の利用については、パスワードの定期的な変更、特権IDによるアクセス環境（作業場所、接続端末等）の特定、利用の事前承認等の厳重な管理を行う。 ・特定個人情報の使用の記録 ：システムのログイン、操作履歴を記録し、不正・異常なアクセスがないことを定期的に点検している。 ：ログイン、操作履歴を記録し点検していることを、職員等に周知している。

リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置

・従業者が事務外で使用するリスクに対する措置
：利用時間外においては、介護保険システムを停止している。
：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。
：外部媒体へのデータのコピーや印刷を制御することで、許可なく持ち出せないようにしている。
：全職員が、年に1回、個人情報保護に関して自己点検を行い、事務外での利用をしないよう周知している。（新規採用者については都度実施している）
：各種ログを取得しているため、業務外利用をした場合には特定可能であることを職員に周知し、事務外の利用を抑止している。

・特定個人情報ファイルが不正に複製されるリスクに対する措置
：バックアップファイルの取得は入退室管理をしているデータセンタでの作業に限定され、また、バックアップファイルの持ち出しはセキュリティ責任者による承認を必須としている。
：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接続端末への保存ができるようシステム的に制御する。

4. 特定個人情報ファイルの取扱いの委託　　[　]委託しない

リスク:　委託先における不正な使用等のリスク

委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　　定めている　　]	＜選択肢＞ 1）定めている　　2）定めていない
規定の内容	以下の規定を委託契約書及び個人情報取扱特記仕様書に定めている。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務（委託業務終了後を含む） ・改竄、漏えい、滅失及び毀損の防止 ・再委託先に関する制限事項の遵守 ・提供した情報資産の複写又は複製の禁止 ・委託業務終了時の情報資産の返還、廃業等 ・「情報セキュリティ対策チェックシート」による自己点検の実施 ・委託業務の定期報告及び緊急時報告義務 ・市による監査及び検査 ・市による事故時等の公表 ・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等） ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・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 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項	

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担保		[　　十分に行っている　　]　＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	・再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・再委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する教育の確認 ・契約内容の遵守状況について報告を求める規定 等 〈介護情報基盤を活用した情報連携に係る介護保険事務における追加措置〉 ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先である公益社団法人国民健康保険中央会が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年1回公益社団法人国民健康保険中央会から報告を受ける。
その他の措置の内容		・情報保護管理体制の確認 ：委託先に「情報セキュリティ対策チェックシート」を提出させ、そのチェック項目の中で、委託先の情報保護管理体制として個人情報保護責任者と個人情報保護担当者が任命され、その役割や権限が明確になっていることを確認している。 ・特定個人情報ファイルの閲覧者・更新者の制限 ：委託先に「情報セキュリティ対策チェックシート」を提出させ、そのチェック項目の中で、委託先においてアクセス権限を付与する従業員数及びアクセス権限の範囲を必要最小限とすることを遵守させている。 ：契約書に、アクセス権限の管理状況等、情報セキュリティ対策の実施状況を定期的に報告することを記載している。 ・特定個人情報ファイルの取扱いの記録 ：委託先に「情報セキュリティ対策チェックシート」を提出させ、そのチェック項目の中で、特定個人情報ファイルを含む重要データについてアクセス権限の設定を行い、そのアクセス記録を保管することを遵守させている。 ・特定個人情報の提供ルール ：契約書において、特定個人情報を含む情報資産の第三者への提供禁止を定めている。 ：委託先に「情報セキュリティ対策チェックシート」を提出させ、そのチェック項目の中で、委託先において情報資産の第三者への提供の禁止を従業者に対して遵守させていることを確認している。 ：保守運用委託及びオペレーション業務委託に関しては、仕様書にて委託業務実施場所を岐阜市庁舎内に限定し、外部への持ち出しを禁止している。 ：委託先に情報提供する際には、日付、枚数、媒体等を記載した管理簿を作成し、情報セキュリティ管理者の承認を得たうえで受け渡ししている。 ：委託先に「情報セキュリティ対策チェックシート」を提出させ、そのチェック項目の中で、情報の受け渡しの際に管理簿等で記録を取って実施することを確認している。 ・特定個人情報の消去ルール ：保守運用委託及びオペレーション業務委託等に関しては、仕様書にて委託業務実施場所を岐阜市庁舎内に限定し、かつ直接のシステム操作であるため、特定個人情報を含むデータの受け渡しは発生しないため、消去の委託はしない。
リスクへの対策は十分か		[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
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		
・委託先において契約書等に示す情報セキュリティの遵守が疎かになるリスクに対し、業務着手時及び年度当初に「情報セキュリティ対策チェックシート」により、遵守状況の自己点検を徹底させている。		

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:　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
ルールの内容及びルール遵守の確認方法	・岐阜市個人情報等取扱規程（令和5年岐阜市訓令乙第5号）に従い、データ移転先からの利用申請を求め、データ移転元がその法的根拠等を判断し、承認を得たもののみ、データの移転を行っている。 ・特定個人情報ファイルを扱う業務システムから移転は、庁内連携システムによるデータ連携、または、住民情報系ネットワーク（インターネットに接続されない）内に作成された、アクセス可能な者が制限される共有フォルダを用いたデータの受け渡しのみとしている。 ・庁内連携システムにおいて、情報システム管理者が特定個人情報ファイルの連携毎に移転の目的や法的根拠を確認した上で、移転先の業務遂行に必要な情報項目と移転タイミングをシステムの設計書として定めている。
その他の措置の内容	・庁内連携システムを利用した情報の移転は全て実行結果の記録を残している。 ・共有ディレクトリを利用した情報の移転は、データ授受管理簿で記録を残している。
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	
・不適切な方法で提供・移転が行われるリスクに対する措置 ：庁内連携システムによる移転の実行は自動化されており、特定の権限を持つ者以外実行できないよう、アクセス制限されている。 ・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に対する措置 ：庁内連携システムは、仕組みとして移転元と移転先の関連付け及び移転する情報が定義されており、人的に誤った情報の移転及び誤った相手への移転を防止する。 ：庁内連携システムの設計書等に記載される、移転元と移転先の関連付け、移転する情報については、情報システム管理者、情報セキュリティ管理者が点検、承認し記録する。	

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	・目的外の入手が行われるリスクに対する措置 ：情報提供ネットワークシステムを利用する者を限定し、利用者の管理を徹底することで、情報提供ネットワーク接続による目的外の入手のリスクに対応している。 ：情報セキュリティ管理者及び情報システム管理者は、中間サーバの利用者IDを定期的に棚卸し、不用な利用者IDを消去する。 ：職員等の中間サーバのログイン認証は、中間サーバを利用可能な職員毎のユーザIDにより行い、その操作内容の記録を実施することから、職員等は中間サーバの利用者IDを他の職員と共有しない。 ＜中間サーバ・ソフトウェアにおける措置＞ ：情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ：中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。 ・安全が保たれない方法によって入手が行われるリスクに対する措置 ：中間サーバとの接続において、不適切な端末等が接続できないよう対策を講じることで、リスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ：中間サーバは、国が設置・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・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・入手した特定個人情報が不正確であるリスクに対する措置 ：他団体への特定個人情報の照会に際し、情報提供ネットワーク以外の手段を用いないことで、中間サーバ・ソフトウェアにおいて講じられた措置によってリスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ：中間サーバは、情報提供ネットワークシステムを使用して、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。 ・入手の際に特定個人情報が漏えい・紛失するリスクに対する措置 ：他団体への特定個人情報の照会に際し、情報提供ネットワーク以外の手段を用いないことで、中間サーバ・ソフトウェア、中間サーバ・プラットフォームにおいて講じられた措置によってリスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ：中間サーバは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ：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。 ：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。 ：中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・入手の際に特定個人情報が漏えい・紛失するリスク ＜中間サーバ・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ：中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害の対応等、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。

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：不正な提供が行われるリスク	
リスクに対する措置の内容	・不正な提供が行われるリスクに対する措置 ：情報提供ネットワークシステムによる情報提供については、必ず共通基盤連携システムの中間サーバ連携機能を経由することとし、許可されたシステム以外からの情報提供を禁止している。 ：特に慎重な対応が求められる情報については、自動応答を行わないように自動応答不可フラグを設定している。 ：中間サーバとの接続において、不適切な端末等が接続できないよう対策を講じている。 ：中間サーバに保存する特定個人情報ファイルの更新を職員等が誤って実施できないよう、システムを利用する必要がある職員を特定し、権限管理、利用者IDを定期的な棚卸し、不要なIDの消去等を行う。 ＜中間サーバ・ソフトウェアにおける措置＞ ：情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ：情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、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。 ：機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ：中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 ・不適切な方法で提供されるリスクに対する措置 ：他団体への特定個人情報の提供に際し、情報提供ネットワーク以外の手段を用いないことで、中間サーバ・ソフトウェア、中間サーバ・プラットフォームにおいて講じられた措置によってリスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ：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。 ：中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバ･プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ：中間サーバ・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。 ・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に対する措置 ：他団体への特定個人情報の提供に際し、情報提供ネットワーク以外の手段を用いないことで、中間サーバ・ソフトウェアにおいて講じられた措置によってリスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ：情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、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。 ：情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ：情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。

リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置

＜中間サーバ・ソフトウェアにおける措置＞
・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。
・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。
＜中間サーバ･プラットフォームにおける措置＞
・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。
・中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
・中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。
・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォーム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: 特定個人情報の漏えい・滅失・毀損リスク		
①事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
②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	—	
	物理的対策 ＜外部データセンターにおける措置＞ ・データセンター内のサーバ室への入退室は、職員、保守事業者等のうち入室を許可された者のみに制限し管理しており、入室の事前申請の承認、入退室管理簿の記録をしている。 ・データセンター内のサーバ室への入退室は、ICカード（許可された者のみ所有）、静脈認証等の生体認証、パスワード（許可された者ごとに設定）による認証を必要とし、また監視カメラによる監視をしている。 ・サーバ室へのパソコン、外部記憶媒体、通信機器等の無断持ち込みを禁止している。 ・データの滅失、毀損を防止するため、サーバ室は火災、水害、埃、振動、温度等の対策がされ、非常用電源及び無停電電源装置を備えている。 ＜本庁マシン室における措置＞ ・入室は入口ドアのパスワード認証、入退室管理簿の記録で管理している。 ・監視カメラにより、入退室や作業状況を監視している。 ・停電(落雷等)によるデータの消失を防ぐために、無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・端末はセキュリティワイヤーで固定する。 ＜各課事務室における措置＞ ・各課事務室の全端末はセキュリティワイヤー等で固定されている。 ・各課事務室の全端末の配線については、整理・集約し、引っかけ・抜け防止策を実施している。 ・総合窓口事務室への入室はICカードにより厳重に管理されている。 ・業務時間外の総合窓口事務室はシャッターで閉鎖される。 ＜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。	

その他の措置の内容	＜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。 技術的対策 ・システムの操作履歴を記録する。 ・サーバ、パソコンにウイルス対策ソフトを常駐しリアルタイムチェックを実施し、新種の不正プログラムに対応するために、ウイルスパターンファイルは自動化により最新のものを適用している。 ・ネットワークを通じての不正アクセス対策として、ファイアウォールやIPSにより不正、不要な通信の検知や遮断をしている。 ・OSやアプリケーション等に対するセキュリティ対策パッチ適用は、必要性、動作の安全性等を確認した上で実施することとしている。 ・パソコンは許可なくソフトウェアを導入できないよう管理者権限を制限しており、また、パソコンを許可なくネットワークに接続できないよう、端末の認証等の制限をしている。 ＜中間サーバー・プラットフォームにおける措置＞ 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。 ＜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築する。 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。 ＜サービス検索・電子申請機能における措置＞ ・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。
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
・特定個人情報が古い情報のまま保管され続けるリスク ：庁内の他システムとの整合処理を定期的に実施し、保存中の情報が最新であるかどうかを確認する。 ・事実関係、再発防止策等の公表 　＜サービス検索・電子申請機能における措置＞ ・住民情報系端末は、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。 ・特定個人情報が消去されずいつまでも存在するリスク ：磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ：廃棄時には、規定に基づき、廃棄を行うとともに、廃棄日時、担当者及び処理内容を記録する。 ＜サービス検索・電子申請機能における措置＞ ・住民情報系端末については、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、必要に応じて情報セキュリティ管理者が確認する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ①クラウド事業者が保有・管理する環境（日本国内）に設置し、クラウド事業者による設置場所への入退室記録管理及び施錠管理をすることでリスクを回避する。クラウド事業者は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、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ものを選定し、「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ものとする。 ②クラウド環境にアクセスできる運用・保守拠点では、以下の対策方針に則り運用保守事業者が保守拠点への対策を講じている。 ＜通信のなりすまし防止＞ ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 ・情報システムの機器番号等による接続機器の識別を行う。 ＜不正プログラムの感染防止＞ ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラムを検出する。 ＜不正プログラム対策の管理＞ ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラム対応状況を一元管理する。 ＜構築時の脆弱性対策＞ ・最新のセキュリティパッチを適用する。 ＜運用時の脆弱性対策＞ ・最新のセキュリティパッチを自動適用する。 ＜ログの蓄積・管理＞ ・運用保守端末の操作ログを収集する。 ＜時刻の正確性確保＞ ・クラウドサービスが提供している時刻同期のサービスを時刻同期元とする。 ＜情報の物理的保護＞ ・運用保守端末への対策として下記を実施する。 端末の離席対策（自動スクリーンロック） 端末のワイヤーロック 記録装置のパスワードロック、暗号化 データ消去ソフトや物理的破壊による情報の完全廃棄 ・セキュリティ区画への対策として下記を実施する。 携帯電話、メモリデバイス等の持ち込みの監視及び制限 物品持ち出し管理 ＜侵入の物理的対策＞ ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 ＜外部記録媒体を利用する場合の保管・消去に係るリスク対策＞ ・作業に用いる外部記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる外部記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ③特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っている。

＜技術的安全管理措置＞
・アクセス制御
ユーザアカウント権限の制御を行っている。
外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離している。
一情報の種別に応じた格納領域の分割を行っている。
・アクセス者の識別と認証
クラウドサービスのリソースへのアクセス権を一時的に付与するサービスやクラウドサービスのリソースへの操作を許可または拒否する権限を定義するサービスを活用した認可、OS等による認可でアクセス者の識別を行っている。
・外部からの不正アクセス等の防止
ウイルス/マルウェア対策・標的型攻撃対策・IDS/IPS・改ざん検知を行い、ネットワークへの不正なアクセスの防止、不正プログラムへの対策を行う。
Webアプリケーションへの不正アクセスを防止する。
セキュリティ設計やセキュアコーディング等のセキュリティ対策を実施した上で、本システムの稼働前にセキュリティの専門家によるセキュリティ診断（ペネトレーションテスト等）を実施し、セキュリティ対策が十分行われていることを確認している。
ログ監査を行い不正アクセスを検知する。
・漏えい等の防止
業務データの暗号化については、キーポリシーによる柔軟なアクセス制御、およびクラウドサービス利用終了時に暗号化消去によるデータの完全廃棄を行うことを目的として、原則ユーザーが独自に作成、管理、制御する暗号化キーを使用し、データの暗号化を行っている。
通信経路の暗号化を行っている。
情報の種別に応じた格納領域の分割を行っている。
・データの遠隔地保管
大阪リージョンにバックアップファイルを保管する。

④個人情報等が漏えいした場合の対策として、セキュリティポリシーを遵守し、必要な措置を講ずることとしており、緊急時には、緊急連絡先等により対応する。
・情報システム担当者にて事案を確認
・情報セキュリティ管理者（又は情報セキュリティ責任者）に連絡・報告、応急処置等の指示
・最高情報セキュリティ責任者（又は情報セキュリティ統括責任者）・情報セキュリティ委員会に報告
・事実関係の調査、原因の究明及び影響範囲の特定を行う
・影響を受ける可能性のある本人への連絡及び関係する機関等へ連絡・対応指示
・個人情報等を漏えいさせた医療保険者等の制度所管省庁（厚生労働省、財務省、総務省、文部科学省）及び個人情報保護委員会への報告

8. 監査

実施の有無	［ ○ ］自己点検　［ ○ ］内部監査　［ ○ ］外部監査

9. 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	・職員に対しては、定期的に個人情報保護に関する研修を行っている。 ・委託業者に対しては、契約内容に個人情報保護に関する研修の実施を義務付け、秘密保持契約を締結している。 ・違反行為を行った者に対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。 ＜中間サーバー・プラットフォームにおける措置＞ IPA（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材を作成し、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。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 　情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。	

10. その他のリスク対策

＜中間サーバー・プラットフォームにおける措置＞
中間サーバー・プラットフォームを活用することにより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・監視を実施する。

＜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およ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。

＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞
　情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。

Ⅳ　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	〒500－8701 岐阜県岐阜市司町40番地1　岐阜市役所　福祉部　介護保険課
②請求方法	個人情報の保護に関する法律（平成15年法律第57号）に基づき、所定の請求書に必要事項を記載し、提出する。
③法令による特別の手続	―
④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	岐阜市役所　福祉部　介護保険課 （058）214－2091
②対応方法	問合せの受付時に起票し、対応について記録を残す。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年3月24日
②しきい値判断結果	[　　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　　] ＜選択肢＞ 1）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 2）基礎項目評価の実施が義務付けられる（任意に重点項目評価を実施） 3）特定個人情報保護評価の実施が義務付けられない（任意に重点項目評価を実施）
2. 国民・住民等からの意見の聴取 【任意】	
①方法	岐阜市市民意見聴取プロセス実施要綱に基づきパブリックコメントによる意見聴取を実施する。パブリックコメントの実施に際しては、市報に公表している旨の記事を掲載し、市ホームページ及び市内公共施設にて全文を閲覧できるようにする。
②実施日・期間	令和6年12月2日から令和6年12月27日まで
③主な意見の内容	意見提出：0件
3. 第三者点検 【任意】	
①実施日	2025/02/27
②方法	岐阜市個人情報保護審議会による第三者点検の実施
③結果	原案通り認める旨の答申を得た。

（別添2）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　特定個人情報の入手・使用	生活福祉一課・生活福祉二課	生活福祉一課・生活福祉二課・生活福祉三課	事後	重要な変更に当たらないため事後に提出（組織改編）
令和7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	パーソルテンプスタッフ株式会社　岐阜オフィス	パーソルビジネスプロセスデザイン株式会社	事後	重要な変更に当たらないため事後に提出（委託先名の変更）
令和7年8月1日	Ⅱ　特定個人情報ファイルの概要 5　特定個人情報の提供・移転　別紙2	福祉事務所 生活福祉一課 生活福祉二課	福祉事務所 生活福祉一課 生活福祉二課 生活福祉三課	事後	重要な変更に当たらないため事後に提出（組織改編）
令和7年8月1日	Ⅱ　特定個人情報ファイルの概要 5　特定個人情報の提供・移転　別紙2	市民生活部 国保・年金課	市民協働生活部 国保・年金課	事後	重要な変更に当たらないため事後に提出（組織改編）
令和7年8月1日	Ⅱ　特定個人情報ファイルの概要 5　特定個人情報の提供・移転　別紙2	市民生活部 市民課	市民協働生活部 市民課	事後	重要な変更に当たらないため事後に提出（組織改編）
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	＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバー・プラットホームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・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	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年8月1日	Ⅲ　リスク対策 5　情報ネットワークシステムとの接続 リスク1：目的外の提供が行われるリスク リスクに対する措置の内容	・入手の際に特定個人情報が漏えい・紛失するリスク ＜中間サーバ・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ：中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害の対応等であり、業務上、特定個人情報へはアクセスすることはできない。	・入手の際に特定個人情報が漏えい・紛失するリスク ＜中間サーバ・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ：中間サーバ・プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害の対応等、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	自治体中間サーバー・プラットフォーム更改に伴う変更

令和7年8月1日	Ⅲ　リスク対策 5　情報ネットワークシステムとの接続 リスク2：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	・不適切な方法で提供されるリスクに対する措置 ＜中間サーバ・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ：中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	・不適切な方法で提供されるリスクに対する措置 ＜中間サーバ・プラットフォームにおける措置＞ ：中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ：中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ：中間サーバ・プラットフォームの事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年8月1日	Ⅲ　リスク対策 5　情報ネットワークシステムとの接続 情報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・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォーム事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年8月1日	Ⅲ　リスク対策 7　特定個人情報の保管・消去 その他の措置の内容	物理的対策 ＜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データセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	物理的対策 ＜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・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更

令和7年8月1日	Ⅲ　リスク対策 7　特定個人情報の保管・消去 その他の措置の内容	技術的対策 ＜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事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	技術的対策 ＜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・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
令和7年8月1日	Ⅲ　リスク対策 10　その他のリスク対策	＜中間サーバー・プラットフォームにおける措置＞ 中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実施する。	＜中間サーバー・プラットフォームにおける措置＞ 中間サーバー・プラットフォームを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・監視を実施する。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更
	Ⅰ 基本情報 2　特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ②システムの機能	1. 統合宛名機能 （6）中間サーバ連携機能（4情報提供）	1. 統合宛名機能 （6）中間サーバ連携機能（5情報提供）	事後	住民基本台帳法の改正に伴う変更
	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 ①システムの名称	―	サービス検索・電子申請機能	事前	次期オンラインサービスへの移行に向けた追記
	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 ②システムの機能	―	【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	事前	次期オンラインサービスへの移行に向けた追記
	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 ③他のシステムとの接続	―	[○]その他　（e-Gov電子申請サービス）	事前	次期オンラインサービスへの移行に向けた追記
	Ⅱ 特定個人情報ファイルの概要 2　基本情報 ④記録される項目 その妥当性	・4情報、連絡先等情報、その他住民票関係情報	・5情報、連絡先等情報、その他住民票関係情報	事後	住民基本台帳法の改正に伴う変更 重要な変更にあたらない
	Ⅱ 特定個人情報ファイルの概要 3　特定個人情報の入手・使用 ②入手方法	[○]その他（LGWAN回線を用いた介護保険システムからのデータ連携、医療保険者等向け中間サーバー）	[○]その他（サービス検索・電子申請機能、LGWAN回線を用いた介護保険システムからのデータ連携、医療保険者等向け中間サーバー）	事前	次期オンラインサービスへの移行に向けた追記

	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	＜各課事務における措置＞ ・申請書は鍵付きキャビネットに保管している。	＜各課事務における措置＞ ・申請書等は鍵付きキャビネットに保管している。	事前	次期オンラインサービスへの移行に伴う追記
	Ⅲ リスク対策 2 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスク：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	―	・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、対象以外の情報の入手を防止する。 ・申請時に個人番号付電子申請データに電子証明書を付与することで、本人以外のなりすましを防止する。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 2 特定個人情報の入手 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。） 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	―	：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、のち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誘導において住民に何の手続き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もらい、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な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できるよう措置を講じている。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 2 特定個人情報の入手 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。） 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	―	：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。 ：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。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 2 特定個人情報の入手 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。） 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	―	：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。 ：サービス検索・電子申請機能と e-Gov電子申請サービスは、専用線であるGSS G-Net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。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 3 特定個人情報の使用 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 具体的な管理方法	・介護保険システムへのアクセスにおいて、システムを利用する必要がある職員を特定し、ユーザID/パスワードによる認証を実施している。	・システムへのアクセスにおいて、システムを利用する必要がある職員を特定し、ユーザID/パスワードによる認証を実施している。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 3 特定個人情報の使用 特定個人情報の利用におけるその他リスク及びそのリスクに対する措置	―	・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。 ：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接続端末への保存ができるようシステム的に制御する。	事前	次期オンラインサービスへの移行に向けた追記

	Ⅲ リスク対策 7 特定個人情報ファイルの保管・消去 その他の措置の内容	―	＜サービス検索・電子申請機能における措置＞ ・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。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 7 特定個人情報ファイルの保管・消去 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 特定個人情報が古い情報のまま保管され続けるリスク	―	＜サービス検索・電子申請機能における措置＞ ・住民情報系端末は、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。	事前	次期オンラインサービスへの移行に向けた追記
	Ⅲ リスク対策 7 特定個人情報ファイルの保管・消去 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 特定個人情報が消去されずいつまでも存在するリスク	―	＜マイナポータル（サービス検索・電子申請機能）における措置＞ ・住民情報系端末については、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、必要に応じて情報セキュリティ管理者が確認する。	事前	次期オンラインサービスへの移行に向けた追記
	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	―	○地域支援事業に関する事務 ・被保険者の保健医療の向上及び福祉の増進を図るため、被保険者、介護サービス事業者その他の関係者が被保険者に係る情報を共有し、及び活用することを促進する事業として、介護情報基盤を活用した情報連携を実施する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・市区町村は、介護情報基盤へ本事務に係る対象者の個人番号を含む対象者情報、介護保険関係情報、介護保険認定情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の紐付け及び登録を行う。 ・介護サービス事業所は、介護保険資格確認等WEBサービス経由で、事業所の利用者に関して市区町村が登録した情報の確認等を行う。 ・住民は、マイナポータル経由で、本事務に係る自身の介護保険資格情報、介護保険認定審査進捗情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の情報の確認等を行う。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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7 ①システムの名称	―	介護情報基盤	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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7 ②システムの機能	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 介護情報基盤が介護保険に係る各種データを扱う際には、個人を特定するキーとして、介護保険被保険者番号又はPublic Medical Hub（以下「PMH」という。）固有の識別子（PMHキー）にて制御する仕様としている（PMHキーは、特定個人情報と紐づけることで個人を特定するキーである）。詳細な機能は以下のとおり。 ①特定個人情報の登録・管理 ・情報連携のため、本市区町村は、介護情報基盤（PMH介護領域）へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。 （LGWAN回線等経由） ・介護情報基盤に登録された特定個人情報は、自治体からのアクセスのみに制御される。また特定個人情報を出力する機能はない。 ②PMHキー採番 ・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記

			・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。 （連携後、マイナポータル上からPMHキーは削除される。）以降、マイナポータルからの介護情報参照等が可能となる。 ③介護保険資格確認等WEBサービスからの参照 ・介護事業所が介護保険資格確認等WEBサービス経由で、事業所にて管理している被保険者の介護情報を確認する。 ・介護保険資格確認等WEBサービスは、被保険者番号をキーに介護情報基盤に対して介護情報（証等の情報、認定情報等）を照会する。 ・介護情報基盤は被保険者番号をキーに介護情報基盤の介護情報を取得し返却する。 ④マイナポータルからの参照 ・住民がマイナポータル経由で、自身の介護保険情報を確認する。 ・マイナポータルは、PMH仮名識別子をキーに介護情報基盤に被保険者情報を照会する。 ・介護情報基盤はPMH共通にPMH仮名識別子を連携しPMHキーを取得し、PMHキーをキーに介護情報基盤の介護情報を取得し返却する。		
	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7 ③他のシステムとの接続	―	[○] その他 （介護保険システム）	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅱ 特定個人情報ファイルの概要 2. 基本情報 ④記録される項目 その妥当性	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・識別情報 介護被保険者番号、個人番号（マイナンバー）、PMHキー…介護情報基盤が外部と情報連携するために必要となる。 ・業務関係情報 介護・高齢者福祉関係情報…（介護保険事務の適切な実施にあたり必要となる情報を管理し、）介護情報基盤が、外部と情報連携するために必要となる。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ①入手元	―	[○] その他 （社会保険診療報酬支払基金）	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ②入手方法	[○] その他 （サービス検索・電子申請機能）	[○] その他 （サービス検索・電子申請機能、LGWAN回線を用いた介護保険システムからのデータ連携、医療保険者等向け中間サーバー）	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤使用方法	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・情報連携のため、本市区町村は、介護情報基盤（PMH介護領域）へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。（LGWAN回線等経由） ・介護情報基盤は、医療保険者等向け中間サーバーーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 ・医療保険者等向け中間サーバーーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。（連携後、マイナポータル上からPMHキーは削除される。）以降、マイナポータルからの介護情報参照等が可能となる。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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	―	介護情報基盤を活用した情報連携に係る介護保険事務における特定個人情報ファイルの一部の取扱	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記

	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	―	介護情報基盤の利用・情報連携業務及び運用保守業務	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 ②委託先における取扱者数	―	10人以上50人未満	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 ③委託先名	―	岐阜県国民健康保険団体連合会（岐阜県国民健康保険団体連合会は、国保中央会に再委託する）	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 ⑤再委託の許諾方法	―	再委託する	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 ③委託先名	―	書面又は電磁的方法による承諾	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 ⑥再委託事項	―	介護情報基盤におけるPMHキーを用いた情報連携 介護情報基盤の運用保守	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	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 保管場所	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・特定個人情報の格納領域を分けて、ユーザアカウント権限の制御を行い、さらにアクセス者の識別を行う。 ・外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離する。 ・不正侵入を検知・防御するシステムを導入することで、ネットワーク、Webアプリケーションへの不正アクセスを防止する。 ・ログ監査により、不正アクセスを検知する。 ・データ暗号化、通信暗号化を行う。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅲ　リスク対策 2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスクに対する措置の内容	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・定められたインターフェース仕様に沿って決められたデータ項目のみが返却されるようシステム的に制御している。自治体ごとのアクセス制御も実施する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）からPublic MedicalHub（PMH）に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅲ　リスク対策 3．特定個人情報の使用 リスクに対する措置の内容	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・個人情報を格納する領域については、外部連携先システムが直接アクセスが行えないようネットワークを分離をするとともにシステム自動処理により、介護情報基盤システム内に格納される運用になっている。 ・外部連携先システムとの通信はVPN等の技術を用いた暗号化を行うことで通信内容秘匿、盗聴対策の対応をしている。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅲ　リスク対策 3　特定個人情報の使用 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 具体的な管理方法	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・介護情報基盤へのログインはユーザID、パスワードで行う。 ・ログイン用のユーザIDは、管理者がユーザ登録を行った者に限定して発行される。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記

	Ⅲ 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	—	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の 規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・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 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅲ 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担保 具体的な方法	—	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先である公益社団法人国民健康保険中央会が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年1回公益社団法人国民健康保険中央会から報告を受ける。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記
	Ⅲ リスク対策 7. 特定個人情報の保管・消去 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	—	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ①クラウド事業者が保有・管理する環境（日本国内）に設置し、クラウド事業者による設置場所への入退室記録管理及び施錠管理をすることでリスクを回避する。クラウド事業者は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、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ものを選定し、「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ものとする。 ②クラウド環境にアクセスできる運用・保守拠点では、以下の対策方針に則り運用保守事業者が保守拠点への対策を講じている。 ＜通信のなりすまし防止＞ ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 ・情報システムの機器番号等による接続機器の識別を行う。 ＜不正プログラムの感染防止＞ ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラムを検出する。 ＜不正プログラム対策の管理＞ ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラム対応状況を一元管理する。 ＜構築時の脆弱性対策＞ ・最新のセキュリティパッチを適用する。 ＜運用時の脆弱性対策＞ ・最新のセキュリティパッチを自動適用する。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記

			＜ログの蓄積・管理＞ ・運用保守端末の操作ログを収集する。 ＜時刻の正確性確保＞ ・クラウドサービスが提供している時刻同期のサービスを時刻同期元とする。 ＜情報の物理的保護＞ ・運用保守端末への対策として下記を実施する。 端末の離席対策（自動スクリーンロック） 端末のワイヤーロック 記録装置のパスワードロック、暗号化 データ消去ソフトや物理的破壊による情報の完全廃棄 ・セキュリティ区画への対策として下記を実施する。 携帯電話、メモリデバイス等の持ち込みの監視及び制限 物品持ち出し管理 ＜侵入の物理的対策＞ ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 ＜外部記録媒体を利用する場合の保管・消去に係るリスク対策＞ ・作業に用いる外部記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。 また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる外部記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ③特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っている ＜技術的安全管理措置＞ ・アクセス制御 ユーザアカウント権限の制御を行っている。 外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離している。 一情報の種別に応じた格納領域の分割を行っている。 ・アクセス者の識別と認証 クラウドサービスのリソースへのアクセス権を一時的に付与するサービスやクラウドサービスのリソースへの操作を許可または拒否する権限を定義するサービスを活用した認可、OS等による認可でアクセス者の識別を行っている。 ・外部からの不正アクセス等の防止 ウイルス/マルウェア対策・標的型攻撃対策・IDS/IPS・改ざん検知を行い、ネットワークへの不正なアクセスの防止、不正プログラムへの対策を行う。 Webアプリケーションへの不正アクセスを防止する。 セキュリティ設計やセキュアコーディング等のセキュリティ対策を実施した上で、本システムの稼働前にセキュリティの専門家によるセキュリティ診断（ペネトレーションテスト等）を実施し、セキュリティ対策が十分行われていることを確認している。 ログ監査を行い不正アクセスを検知する。 ・漏えい等の防止 業務データの暗号化については、キーポリシーによる柔軟なアクセス制御、およびクラウドサービス利用終了時に暗号化消去によるデータの完全廃棄を行うことを目的として、原則ユーザーが独自に作成、管理、制御する暗号化キーを使用し、データの暗号化を行っている。 通信経路の暗号化を行っている。 情報の種別に応じた格納領域の分割を行っている。 ・データの遠隔地保管 大阪リージョンにバックアップファイルを保管する。 ④個人情報等が漏えいした場合の対策として、セキュリティポリシーを遵守し、必要な措置を講ずることとしており、緊急時には、緊急連絡先等により対応する。 ・情報システム担当者にて事案を確認 ・情報セキュリティ管理者（又は情報セキュリティ責任者）に連絡・報告、応急処置等の指示 ・最高情報セキュリティ責任者（又は情報セキュリティ統括責任者）・情報セキュリティ委員会に報告 ・事実関係の調査、原因の究明及び影響範囲の特定を行う ・影響を受ける可能性のある本人への連絡及び関係する機関等へ連絡・対応指示 ・個人情報等を漏えいさせた医療保険者等の制度所管省庁（厚生労働省、財務省、総務省、文部科学省）及び個人情報保護委員会への報告 ・事実関係、再発防止策等の公表		

	Ⅲ リスク対策 10. その他のリスク対策	―	＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 　情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。	事前	介護情報基盤を活用した情報連携による介護保険事務の開始に伴う追記