

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	
後期高齢者医療関連情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	・被保険者(※):75歳以上の者(年齢到達予定者を含む。)、又は65歳以上75歳未満で一定の障害がある者(本人申請に基づき認定した者) ・世帯構成員:被保険者と同一の世帯に属する者 ・過去に被保険者であった者及びその者と同一の世帯に属していた者 ※高齢者の医療の確保に関する法律第50条から第55条の2に基づく被保険者
その必要性	被保険者資格の管理(高齢者の医療の確保に関する法律第50条等)、一部負担割合の判定(高齢者の医療の確保に関する法律第67条等)や保険料の賦課(高齢者の医療の確保に関する法律第104条等)等の事務を行う上で、被保険者(被保険者資格の取得予定者を含む。)とその被保険者が属する世帯構成員の所得等の情報を管理するため。
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 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 4情報(氏名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	・個人番号:対象者を正確に特定するために記録するもので、番号法第9条及び別表第一第59号により利用可。 ・その他識別情報(内部番号): (宛名番号・世帯番号)住民基本台帳や資格に関する情報を管理するために記録するもの。 (被保険者番号)資格や保険料の賦課・徴収、給付に関する情報を管理するために記録するもの。 ・基本4情報、連絡先:被保険者について、通知及び照会を行うために記録するもの。 ・その他住民票関係情報:資格管理に関する事務を行うために記録するもの。 ・地方税関係情報:保険料賦課・徴収に関する事務を行うために記録するもの。 ・健康・医療関係情報:給付に関する事務を行うために記録するもの。 ・医療保険関係情報:資格管理に関する事務を行うために記録するもの。 ・障害者福祉関係情報:障害認定に関する事務を行うために記録するもの。 ・生活保護・社会福祉関係情報:適用除外に関する事務を行うために記録するもの。 ・介護・高齢者福祉関係情報:高額医療・高額介護合算療養費に関する事務を行うために記録するもの。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月5日
⑥事務担当部署	事業課、給付課

3. 特定個人情報の入手・使用	
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 () <input type="checkbox"/> 行政機関・独立行政法人等 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 () <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 (「医療保険者又は広域連合」、「高齢者の医療の確保に関する法律第57条第1項に規定する他の法令による給付の支給を行うこととされている者」、「共済組合」)
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [<input checked="" type="checkbox"/>] 専用線 [] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 (住民基本台帳ネットワークシステム)
③入手の時期・頻度	<p>1. 広域連合は市区町村から以下の特定個人情報を入手する。</p> <ul style="list-style-type: none"> ・資格管理業務 <ul style="list-style-type: none"> ・被保険者資格に関する届出：転入時等に市区町村窓口において、被保険者となる住民より入手した届出情報 番号利用開始日(平成28年1月1日)以後に、届出のある都度で入手。 ・住民基本台帳情報：年齢到達により被保険者となる住民及び世帯構成員、障害認定により被保険者となる可能性のある住民及び世帯構成員、並びに既に被保険者となっている住民及び世帯構成員の住基情報(世帯単位)。 個人番号の付番・通知日(平成27年10月5日)以後に準備行為として一括で入手。 番号利用開始日(平成28年1月1日)以後は、日次の頻度。 ・住登外登録情報：年齢到達により被保険者となる住民及び世帯構成員、障害認定により被保険者となる可能性のある住民及び世帯構成員、並びに既に被保険者となっている住民及び世帯構成員の住登外登録情報(世帯単位)。 個人番号の付番・通知日(平成27年10月5日)以後に準備行為として一括で入手。 番号利用開始日(平成28年1月1日)以後は、日次の頻度。 ・賦課・収納業務 <ul style="list-style-type: none"> ・所得・課税情報：後期高齢者医療の被保険者の保険料及び一部負担割合算定に必要な情報。 頻度は月次。 ・期割情報：市区町村が実施した期割保険料の情報。 頻度は日次。 ・収納情報：市区町村が収納及び還付充当した保険料の情報。 頻度は日次。 ・滞納者情報：市区町村が管理している保険料滞納者の情報。 頻度は日次。 ・給付業務 <ul style="list-style-type: none"> ・療養費関連情報等：市区町村等で申請書等を基に作成した療養費情報等。 頻度は月次。 <p>2. 地方公共団体情報システム機構からの個人番号情報の入手 統合専用端末で中間サーバーを介して地方公共団体情報システム機構に即時照会して入手する。 頻度は随時。</p> <p>3. 情報提供ネットワークシステムからの特定個人情報の入手 医療保険者等以外の情報保有機関へ支払基金を介して情報照会を依頼する。 頻度は随時。</p>

④入手に係る妥当性

1. 入手する根拠
 - 当広域連合が構成市区町村の窓口業務担当部署から情報を入手する根拠
 - 【住民基本台帳情報】
 - ・高齢者の医療の確保に関する法律第48条、地方自治法第292条
 - 【住民基本台帳情報以外の情報】
 - ・高齢者の医療の確保に関する法律第48条、第138条、地方自治法第292条
 - 構成市区町村の窓口業務担当部署が市区町村内の他の部署から情報を入手する根拠
 - 【住民基本台帳情報】
 - ・住民基本台帳法第1条
 - 【住民基本台帳情報以外の情報】
 - ・番号法第9条第2項に基づく条例
 - 地方公共団体情報システム機構から個人番号を入手する根拠
 - ・住民基本台帳法第30条の9
 - 情報提供ネットワークシステムから特定個人情報を入手する根拠
 - ・番号法第19条8号及び同法別表第二項番80

広域連合と市区町村は別の機関であるが、「一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について(通知)」(平成27年2月13日府審第27号、総行住第14号、総税市第12号)の記の2により、窓口業務を構成市区町村に残しその他の審査・認定業務等を広域連合が処理する場合等については、同一部署内での内部利用となると整理されている。このため、当広域連合が構成市区町村の窓口業務担当部署から情報を入手することは、同一部署内での内部利用となる。なお、窓口業務担当部署から入手する情報は、法令に基づき窓口業務担当部署が市区町村内の他の部署から適切に入手した情報となっている。
2. 入手の時期・頻度の妥当性
 - ・資格管理業務
 - ・被保険者資格に関する届出：転入時等に市区町村窓口において申請者に被保険者証を即時交付する必要があるため届出のある都度。
 - ・住民基本台帳情報：住民異動が日々発生し、被保険者資格に反映する必要があるため日次。
 - ・住登外登録情報：被保険者に関する住民異動が日々発生し、最新の住所等を被保険者資格に反映する必要があるため日次。
 - ・賦課・収納業務
 - ・所得・課税情報：個人住民税の異動に関する賦課が月次で行われ、最新の所得等を保険料に反映させる必要があるため月次。
 - ・期割情報：被保険者資格に関する異動が日々発生し、被保険者資格を喪失した者について、未到来納期分の保険料を速やかに精算する必要があるため日次。
 - ・収納状況：保険料に関する納付等の収納事務が日々発生するため日次。
 - ・滞納者情報：保険料に関する納付等の収納事務が日々発生し、保険料の納付によって滞納者でなくなったことを滞納者情報に反映する必要があるため日次。
 - ・給付業務
 - ・療養費関連情報等：療養費の申請は日々発生するが、療養費は月ごとにまとめて支給決定するため月次。
3. 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併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常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。
4. 情報提供ネットワークシステムからの特定個人情報入手に係る妥当性
 - ・当広域連合は番号法別表第二項番80、81の規定に基づき、統合専用端末連携またはサーバー間連携を利用し、中間サーバーを介して医療保険者等以外の情報保有機関に情報照会の依頼を行うことにより、特定個人情報を入手する。
 - ・特定個人情報の入手の時期や頻度は、医療保険者等以外の情報保有機関に対し、情報照会依頼を行う都度、随時入手する。
5. 地方公共団体情報システム機構から個人番号の入手に係る妥当性
 - ・当広域連合が構成市区町村の窓口業務担当部署から入手ができない個人番号は、住民基本台帳法第30条の9の規定に基づき、支払基金を介して、地方公共団体情報システム機構から入手する。
 - ・統合専用端末で中間サーバー等を介して即時照会し、随時入手する。

<p>⑧使用方法 ※</p>	<p>1. 資格管理業務</p> <ul style="list-style-type: none"> ・被保険者証の即時交付申請 市区町村の後期高齢者医療窓口において、住民から被保険者資格に関する届出を受け付け、個人番号等の確認を行った後に市区町村の窓口端末に入力する。市区町村の窓口端末への入力後は、広域連合の標準システムにおいて即時に受付・審査・決定が行われるので、市区町村の窓口端末から被保険者証等を発行し交付する。 ・住民基本台帳等の取得 市区町村の住基システムから抽出された被保険者や被保険者の世帯員及び年齢到達予定者等の住民票の異動に関する情報を、市区町村の窓口端末のオンラインファイル連携機能を用いて広域連合の標準システムへ送信し、広域連合の標準システム内でも同情報を管理する。 ・被保険者資格の異動 広域連合の標準システム内に蓄積されている住民に関する情報から、年齢到達者等を抽出し、被保険者資格に関する審査・決定を行う。また、広域連合の標準システムより被保険者情報等を市区町村の窓口端末へ配信し、市区町村の窓口端末から同データを移出して、市区町村システム内に移入することで、市区町村システムにおいても同情報を管理する。 <p>2. 賦課・収納業務</p> <ul style="list-style-type: none"> ・保険料賦課 個人住民税に関するデータを、市区町村の地方税システムから移出し、市区町村の窓口端末のオンラインファイル連携機能を用いて広域連合の標準システムへ送信し、広域連合の標準システム内でも同情報を管理する。広域連合の標準システムで賦課計算を行い、保険料賦課額を決定し、保険料情報データを市区町村の窓口端末に配信し、市区町村の窓口端末から同データを移出して、市区町村システム内に移入し、市区町村では当該住民に賦課決定通知書等で通知する。 ・保険料収納 市区町村システムでは、保険料に関する徴収方法と納期を決定し、特別徴収の場合は年金保険者に徴収依頼を実施するとともに当該住民には特別徴収額通知書等で通知、普通徴収の場合は当該住民に納付書を送付し、特別徴収や普通徴収に関する収納管理を行う。また、保険料収納に関する情報等に関するデータを移出し、市区町村の窓口端末のオンラインファイル連携機能を用いて広域連合の標準システムへ送信し、広域連合の標準システム内でも同情報を管理する。 <p>3. 給付業務</p> <ul style="list-style-type: none"> 市区町村の後期高齢者医療窓口において、住民からの療養費支給申請書に関する届出を受け付け、その届出内容を市区町村の窓口端末に入力する。広域連合の標準システム内では、当該情報の他にレセプト情報等を管理しており、それらを用いて療養費支給の認定処理を行い、療養費支給決定情報等を市区町村の窓口端末に送信し、当該住民に対して広域連合から療養費支給決定通知書等を交付する。 <p>4. 情報提供ネットワークシステムからの特定個人情報入手</p> <ul style="list-style-type: none"> ・個人番号を標準システムの識別番号(宛名番号、被保険者番号)と紐付けて必要な情報の検索・参照を行うことに使用する。 ・資格認定や給付決定等の審査事務に他の情報保有機関の情報が必要なとき、中間サーバーを通じて情報提供ネットワークシステムで情報照会を行い、取得した情報を被保険者枝番と紐付けた標準システムの識別番号(宛名番号、被保険者番号)で当該被保険者の申請情報と照合・確認することに使用する。
<p>情報の突合 ※</p>	<ul style="list-style-type: none"> ・被保険者からの申請等を受け付ける場面において、申請書に記載された情報と広域連合で管理する被保険者資格等の情報を突合することにより、個人番号を用いて個人と業務データの正確な紐付けを個人番号で行う。 ・同一広域連合内である市区町村から他の市区町村に転居した場合に、転居先の市区町村から入手した住民基本台帳等の情報と広域連合で管理する被保険者資格等の情報を突合することにより、個人番号を用いて同一人の名寄せを行う。 ・資格認定や給付決定の審査事務で必要な情報を、中間サーバーを通じて情報提供ネットワークシステムで他の情報保有機関に情報照会を行い、取得した情報は、被保険者枝番と紐付けた標準システムの識別番号(宛名番号、被保険者番号)で該当被保険者の申請情報と突合する。
<p>情報の統計分析 ※</p>	<ul style="list-style-type: none"> ・個人に着目した分析・統計は行わず、資格取得、喪失等の集計や統計のみを行う。
<p>権利利益に影響を与え得る決定 ※</p>	<p>被保険者資格決定、保険料賦課額決定、給付金決定</p>
<p>⑨使用開始日</p>	<p>平成27年10月5日</p>

委託事項2	中間サーバーにおける資格履歴管理事務	
①委託内容	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	
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 ※	・被保険者(※):75歳以上の者(年齢到達予定者を含む。)又は65歳以上75歳未満で一定の障害がある者(本人申請に基づき認定した者)のうち、個人番号を有する者 ・世帯構成員:被保険者と同一の世帯に属する者のうち、個人番号を有する者 ・過去に被保険者であった者及びその者と同一の世帯に属していた者のうち、個人番号を有する者 ※高齢者の医療の確保に関する法律第50条から第55条の2に基づく被保険者 注)なお、世帯構成員に関しては、被保険者資格の履歴管理は行わない。
	その妥当性	・当広域連合における資格履歴を管理するため。 ・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。
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	[<input type="checkbox"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()	
⑤委託先名の確認方法	当広域連合のWebサイトにて公開する。	
⑥委託先名	熊本県国民健康保険団体連合会(熊本県国民健康保険団体連合会は、国民健康保険中央会に再委託する)	
再委託	⑦再委託の有無 ※	[再委託する]
	⑧再委託の許諾方法	<選択肢> 1) 再委託する 2) 再委託しない 委託先の熊本県国民健康保険団体連合会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、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に係る業務の履行能力、再委託先への立ち入り調査に係る要件、その他当広域連合が求め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係る履行体制図(委託先による再委託先に対する監督体制を含む。)の提出を受け、熊本県国民健康保険団体連合会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等、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、再委託を許諾する(再委託先が更に再委託する場合も同様とする。) 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	中間サーバーにおける資格履歴管理事務の全て

委託事項4		中間サーバーにおける本人確認事務
①委託内容		地方公共団体情報システム機構から住民基本台帳ネットワークシステムを使用した個人番号取得及び本人確認情報の取得
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]
	対象となる本人の範囲 ※	<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 ・被保険者(※):75歳以上の者(年齢到達予定者を含む。)又は65歳以上75歳未満で一定の障害がある者(本人申請に基づき認定した者)のうち、個人番号を有する者 ・世帯構成員:被保険者と同一の世帯に属する者のうち、個人番号を有する者 ・過去に被保険者であった者及びその者と同一の世帯に属していた者のうち、個人番号を有する者 ※高齢者の医療の確保に関する法律第50条から第55条の2に基づく被保険者
	その妥当性	当広域連合と地方公共団体情報システム機構との対応窓口を、支払基金に一本化するため。
③委託先における取扱者数		[10人以上50人未満]
④委託先への特定個人情報ファイルの提供方法		<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 [<input type="radio"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()
⑤委託先名の確認方法		当広域連合のWebサイトにて公開する。
⑥委託先名		社会保険診療報酬支払基金
再委託	⑦再委託の有無 ※	[再委託する]
	⑧再委託の許諾方法	<選択肢> 1) 再委託する 2) 再委託しない 委託先の支払基金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、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に係る業務の履行能力、再委託先への立ち入り調査に係る要件、その他当広域連合が求め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係る履行体制図(委託先による再委託先に対する監督体制を含む。)の提出を受け、支払基金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等、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、再委託を許諾する(再委託先が更に再委託する場合も同様とする。)
	⑨再委託事項	中間サーバーの運用・保守業務

委託事項5		標準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		標準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、パッチ検証等)及びシステム運用事務(バックアップ取得、システム障害等のインフラ復旧等)
②取扱いを委託する特定個人情報ファイルの範囲		<input type="checkbox"/> 特定個人情報ファイルの全体 <input type="checkbox"/> 特定個人情報ファイルの一部
	対象となる本人の数	<input type="checkbox"/> 10万人以上100万人未満 <input type="checkbox"/> 100万人以上1,000万人未満
	対象となる本人の範囲 ※	・被保険者(※):75歳以上の者(年齢到達予定者を含む。)又は65歳以上75歳未満で一定の障害がある者(本人申請に基づき認定した者)のうち、個人番号を有する者 ・世帯構成員:被保険者と同一の世帯に属する者のうち、個人番号を有する者 ・過去に被保険者であった者及びその者と同一の世帯に属していた者のうち、個人番号を有する者 ※高齢者の医療の確保に関する法律第50条から第55条の2に基づく被保険者
	その妥当性	システム全体に係る運用・保守等を適正に実施するためには、専門的かつ高度な知識・技術を有する者にファイル全体の取扱いを委託する必要がある。 クラウド環境の場合、受託者は、クラウド事業者が提示する責任共有モデルを理解した上で、システム運用・保守を適切に行う必要がある。
③委託先における取扱者数		<input type="checkbox"/> 10人以上50人未満 <input type="checkbox"/> 50人以上100人未満 <input type="checkbox"/> 100人以上500人未満 <input type="checkbox"/> 500人以上1,000人未満
④委託先への特定個人情報ファイルの提供方法		<input type="checkbox"/> 専用線 <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> 紙 <input type="checkbox"/> その他 (システム直接操作)
⑤委託先名の確認方法		当広域連合のWebサイトにて公開する。
⑥委託先名		国民健康保険中央会
再委託	⑦再委託の有無 ※	<input type="checkbox"/> 再委託する <input type="checkbox"/> 再委託しない
	⑧再委託の許諾方法	委託先の国民健康保険中央会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、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に関する業務の履行能力、再委託先への立ち入り調査に係る要件、その他当広域連合が求め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((委託先による再委託先に対する監督体制を含む。))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、再委託を許諾する。(再委託先が更に再委託する場合も同様とする。) 標準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。 標準システムを、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	標準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	[<input type="radio"/>] 提供を行っている (24) 件 [<input type="radio"/>] 移転を行っている (1) 件 [<input type="checkbox"/>] 行っていない
提供先1	番号法第19条第8号 別表第二に定める各情報照会者(別紙1「特定個人情報の提供先一覧」を参照)
①法令上の根拠	番号法第19条第8号 別表第二の各項(別紙1「特定個人情報の提供先一覧」を参照)
②提供先における用途	番号法第19条第8号 別表第二に定める各事務(別紙1「特定個人情報の提供先一覧」を参照)
③提供する情報	番号法第19条第8号 別表第二に定める各特定個人情報(別紙1「特定個人情報の提供先一覧」を参照)
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	・被保険者(※): 75歳以上の者(年齢到達予定者を含む。)又は65歳以上75歳未満で一定の障害がある者(本人申請に基づき認定した者)のうち、個人番号を有する者 ・過去に被保険者であった者及びその者と同一の世帯に属していた者のうち、個人番号を有する者 ※高齢者の医療の確保に関する法律第50条から第55条の2に基づく被保険者
⑥提供方法	[<input type="radio"/>] 情報提供ネットワークシステム [<input type="checkbox"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()
⑦時期・頻度	情報提供ネットワークシステムを通じて他の情報保有機関からの情報提供の求めを受け付けた都度
移転先1	市区町村
①法令上の根拠	「一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について(通知)」(平成27年2月13日付け 府番第27号・総行住第14号・総税市第12号 内閣府大臣官房番号制度担当参事官・総務省自治行政局住民制度課長・自治税務局市町村税課長通知)の「2 構成地方公共団体の事務の一部を共同処理する場合について」において、広域連合と市区町村のやり取りは内部利用に当たるとされているが便宜上「移転」の欄に記載している。
②移転先における用途	・市区町村において、後期高齢者医療制度に関する保険料に関して、徴収方法を決定し、特別徴収の場合は年金保険者に徴収を依頼し、普通徴収の場合は納期限を定め普通徴収を実施する。また、住民へは保険料決定通知書や納付書等により賦課・徴収に関する通知を行う。
③移転する情報	・資格管理業務 ・被保険者情報 : 後期高齢者医療の被保険者情報等 ・被保険者証発行用情報 : 被保険者証、短期被保険者証、資格証明書発行用の情報等(被保険者証に関する情報) ・住所地特例者情報 : 住所地特例者の情報等 ・賦課業務 ・保険料情報 : 保険料算定結果の情報及び賦課計算の基となる情報等 ・給付業務 ・療養費支給決定通知情報 : 療養費支給決定通知に関する窓口対応に必要な情報等
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

	期間	<p style="text-align: center;">＜選択肢＞</p> <p style="text-align: center;">1) 1年未満 2) 1年 3) 2年</p> <p style="text-align: center;">4) 3年 5) 4年 6) 5年</p> <p style="text-align: center;">7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上</p> <p style="text-align: center;">10) 定められていない</p>
②保管期間	その妥当性	<p>＜標準システムにおける保管期間＞ 高齢者の医療の確保に関する法律により、平成26年度までに賦課された保険料に関しては期間の制限なく保険料賦課額を減額更正できるとされているため、事務に必要な期間、保管することとしている。</p> <p>＜中間サーバーにおける保管期間＞</p> <ul style="list-style-type: none"> ・中間サーバー内の委託区画ファイル及び副本区画ファイルに保存される情報については、被保険者が当広域連合で資格を喪失した時点から、照会条件として指定される範囲及び情報連携で副本を提供する可能性のある年(最長5年間)まで保管する。 ・情報提供等記録項目については、7年間保管する。 ・本人確認項目については、個人番号を利用するために一時的に格納されるものであるためその保管期間は1年を超えることはない。
③消去方法		<p>＜標準システムにおける措置＞</p> <ul style="list-style-type: none"> ・保管期間経過後は、システムから適切に消去等を行い、消去等に係る記録を作成し、管理する。 ・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ISO/IEC27001に準拠した廃棄プロセスを確保していること。 ・廃棄プロセスの適切な実施について、第三者の監査機関による監査を受け、その内容を確認できること。 <p>＜取りまとめ機関が定める当広域連合の運用における措置＞</p> <ul style="list-style-type: none"> ・保管期間経過後は、中間サーバーから適切に廃棄等を行う。 ・使用済みの電子記録媒体を廃棄する場合には、シュレッダー等で粉砕する。
7. 備考		
-		

(別添2) 特定個人情報ファイル記録項目

特定個人情報ファイル記録項目

個人番号管理情報

- ・宛名番号
- ・被保険者枝番
- ・被保険者番号
- ・個人番号

宛名番号

被保険者枝番

<資格関連情報>

住民基本台帳情報
 外国人登録情報
 住登外登録情報
 混合世帯情報
 障害認定申請情報
 負担区分判定対象情報
 個人異動情報
 適用除外者情報
 被保険者
 被保険者世代管理
 被保険者履歴
 老人保健情報
 負担区分根拠情報
 基準収入額申請世帯情報
 負担区分一時記憶WK
 個人情報変更履歴情報
 負担区分判定登録抑止対象情報
 扶養控除候補者情報
 マイナンバー設定候補者WK
 国保住所特例者情報
 住民基本台帳情報(清音化)
 外国人登録情報(清音化)
 住登外登録情報(清音化)
 個人番号管理情報(個人情報)

<賦課・収納関連情報>

賦課世帯管理
 所得情報
 資格異動ログ
 減額対象所得判定情報管理
 所得情報照会結果管理
 所得情報照会結果管理明細

<給付関連情報>

給付記録管理
 葬祭費(その他)
 高額療養費支給管理
 特別療養費支給
 給付制限個人管理
 高額療養費精算管理
 エラーレセプト
 再審査レセプト
 当月レセプト
 療養費支給
 被保険者月別資格日数
 高額介護合算療養費等支給申請書情報
 外来年間合算支給申請書情報
 高額療養費計算WK

<共通情報>

稼働ログ管理
 選択履歴
 メモ管理

<情報連携関連項目>

加入者情報管理(判定対象情報)
 加入者情報管理(個人情報)

<情報連携関連情報>

加入者情報管理(個人情報)
 加入者情報管理(システム基本情報)
 情報照会要求管理
 情報照会状況管理
 加入者情報管理(判定対象情報)

<共通情報>

稼働ログ管理

副本管理(判定対象情報)

副本管理(資格情報)

副本管理(高額介護合算療養費情報)

副本管理(葬祭費)

副本管理(自己負担額証明書(外来年間合算)情報)

副本管理(自己負担額証明書(高額介護合算療養費)情報)

副本管理(メッセージ情報)

被保険者番号

<資格関連情報>

障害認定申請情報
個人異動情報
適用除外者情報
被保険者
被保険者世代管理
被保険者履歴
証発行管理
送付先情報
負担区分世帯番号情報
負担区分根拠情報
一部負担金減免申請情報
標準負担額減額認定情報
標準負担額減額入院情報
特定疾病認定申請情報
負担区分一時記憶WK
過去被保険者番号情報
加入保険者情報
被扶養者障害特定疾病証明書情報
個人情報変更履歴情報
短期証資格証候補者情報
追加情報該当者
参照用負担区分情報
扶養控除候補者情報
限度額適用申請情報
被保険者(清音化)
被保険者履歴(清音化)
基準収入額申請世帯情報
個人番号管理情報(被保険者情報)
個別事情管理(加入者基本情報)
個別事情管理(加入者制御情報)
証交付不要申請管理

<賦課・収納関連情報>

賦課情報
賦課世帯管理
市町村別賦課情報
所得情報
保険料減免管理情報
賦課対象情報
資格異動ログ
実態調査用被保険者番号管理
期割収納情報
収納履歴
滞納情報
徴収猶予
徴収猶予内訳
期割収納削除情報
収納削除履歴
滞納削除情報
徴収猶予削除
徴収猶予内訳削除
減額対象所得判定情報管理

<情報連携管理情報>

加入者情報管理(資格情報)
加入者情報管理(判定対象情報)
情報照会要求管理
副本管理(判定対象情報)
副本管理(資格情報)
副本管理(高額介護合算療養費情報)
副本管理(葬祭費)
副本管理(自己負担額証明書(外来年間合算)情報)
副本管理(自己負担額証明書(高額介護合算療養費)情報)
加入者情報管理(加入者制御情報)
加入者情報管理(加入者資格情報)
加入者情報管理(被保険者証等情報)
加入者情報管理(限度額適用認定証関連情報)
加入者情報管理(特定疾病療養受給者証情報)

<給付関連情報>

給付記録管理
高額療養費支給
葬祭費(その他)
高額療養費支給管理
特別療養費支給
口座
給付制限個人管理
給付制限レセプト管理
高額療養費精算管理
エラーレセプト
支給管理
高額該当管理
再審査レセプト
当月レセプト
療養費支給
被保険者月別資格日数
レセプト負担区分管理
高額介護合算療養費等支給申請書情報
自己負担額証明情報
高額療養費特別支給金支給管理
特定医療費等連絡対象者管理
突合レセプト増減情報
突合査定結果情報
後発医薬品差額通知送付情報
給付制限追加情報
一定点数超過管理セットアップ
一定点数超過管理
第三者行為求償連携管理
外来年間合算支給申請書情報
外来年間合算自己負担額情報
外来年間合算計算結果情報
外来年間合算計算結果内訳情報
高額介護合算計算結果情報
高額介護合算計算結果内訳情報
高額療養費計算WK
高額該当負担区分WK
他県公費累積WK

<情報提供等記録項目>

処理番号
処理番号の枝番
事務名称
事務手続名称
情報照会者部署名称
情報提供者部署名称
提供の求めの日時
提供の日時
特定個人情報名称
不開示コード
過誤事由コード
被保険者枝番

<本人確認項目>

その他条件 履歴情報
その他条件 消除者
その他条件 異動事由
主たる照会条件
事務区分(住基法)
事務区分(番号法)
住所
住所(大字以降)
住民区分
個人番号
利用事由
変更状況
市町村コード
市町村名
性別
情報表示
氏名
氏名かな
券面記載の氏名
券面記載の氏名かな
券面記載氏名が通称名の場合の本名等
券面記載氏名が通称名の場合の本名かな
照会対象期間終了 年月日
照会対象期間開始 年月日
照会対象期間(照会基準日)
生存状況
生年月日
異動事由
異動年月日
異動有無
要求レコード番号

<共通情報>

稼働ログ管理
選択履歴
メモ管理

※中間サーバーに保存される「委託区画ファイル」、「副本区画ファイル」は、基幹システムで扱う特定個人情報ファイル(後期高齢者医療関連情報ファイル)の副本であることから、一体のものとして評価を行っている。

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.リスク1⑨除く。)

1. 特定個人情報ファイル名

後期高齢者医療関連情報ファイル

2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)

リスク1: 目的外の入手が行われるリスク

<p>対象者以外の情報の入手を防止するための措置の内容</p>	<p>【市区町村(本人)から個人番号を入手する場合の措置】 入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村で本人確認を行った上で、市区町村の基幹系システムから取り込んでいるものである。 また、市区町村からのデータ送信によって入手した情報を広域連合の標準システムのデータベースに更新する際には、項目間の関連性や整合性のチェック(※1)を行っており、確認リスト(※2)が出力されたら、広域連合及び市区町村の事務取扱担当者がそれぞれ確認リストの内容をよく確認し、必要に応じて、入手情報の修正、再作成を行う。</p> <p>※1: ここでいう関連性・整合性チェックとは、既に個人番号が紐付いている(宛名番号が同じ)人に、以前と違う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などの機能のことを指す。 ※2: 確認リストとは既に個人番号が紐付いている(宛名番号が同じ)人に、以前と違う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、その旨がわかるようなリスト(一覧表)を指す。 ※3: 事務取扱担当者とは、特定個人情報の事務取扱担当者(※3)がそれぞれ確認リストの内容をよく確認し、実際に広域連合の標準システムを操作し運用する職員等を指す。</p> <p>(注)市区町村の窓口端末からのデータ送信については、内部利用と整理されているが、便宜上「入手」の欄に記載している。</p> <p>【地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報を入手する場合の措置】 <取りまとめ機関が定める当広域連合の運用における措置> ・あいまい検索により複数の対象者の結果が得られた場合、不要な検索結果については速やかに削除する。 ・当広域連合の照会要求に該当した機構保存本人確認情報のみ入手するため、対象者以外の情報入手が行われることはない。 <中間サーバーにおける措置> ・当広域連合以外の照会要求が参照できないよう、中間サーバーが照会要求や結果送信を制御している。</p>
<p>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</p>	<p>【市区町村(本人)から個人番号を入手する場合の措置】 入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村で本人確認を行った上で、市区町村の基幹系システムから取り込んでいるものである。 なお、市区町村の窓口端末の入力画面では、必要な情報のみが入力項目として表示されるので、必要以上の情報が市区町村から入力されることのリスクを軽減している。 また、市区町村からのデータ送信によって入手した情報を広域連合の標準システムのデータベースに更新する際には、項目間の関連性や整合性のチェックを行っており、確認リストが出力されたら、広域連合及び市区町村の事務取扱担当者がそれぞれ確認リストの内容をよく確認し、必要に応じて入手情報の修正、再作成を行う。</p> <p>【地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報を入手する場合の措置】 <中間サーバーにおける措置> ・統合専用端末における支払基金との通信は、厚生労働省が定めたインターフェース仕様に沿って行われることにより、必要以外の機構保存本人確認情報の入手を防止している。</p>
<p>その他の措置の内容</p>	<p>—</p>
<p>リスクへの対策は十分か</p>	<p>[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</p>

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	<p>【市区町村(本人)から個人番号を入手する場合の措置】 入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村が適切な方法で入手している。</p> <p>【地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報を入手する場合の措置】 <中間サーバーにおける措置> ・個人番号の入手は統合専用端末を経由した方法でのみ行われるため、不適切な方法で入手が行われることはない。</p>
リスクへの対策は十分か	<p>[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</p>
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村において本人確認措置を行った上で、市区町村の基幹システムから取り込んでいるものである。
個人番号の真正性確認の措置の内容	入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村で本人確認措置を行った上で、市区町村の基幹システムから取り込んでいるものである。 また、市区町村からのデータ送信によって入手した情報を広域連合の標準システムのデータベースに更新する際には、項目間の関連性や整合性のチェックを行っており、確認リストが出力されたら、広域連合及び市区町村の事務取扱担当者がそれぞれ確認リストの内容をよく確認し、必要に応じて入手情報の修正、再作成を行う。
特定個人情報の正確性確保の措置の内容	入手元は、市区町村の窓口端末に限定されており、送信されるデータは市区町村で本人確認措置を行った上で、市区町村の基幹システムから取り込んでいるものである。 なお、被保険者に関する住民票の異動に関する情報については、市区町村が市区町村の窓口端末の画面入力にてデータベースに登録した情報と、市区町村の住基システムから入手した情報を突合し整合性チェックを行う。不整合がある場合には、確認リストを出力し、広域連合及び市区町村の事務取扱担当者がそれぞれ確認リストの内容をよく確認し、必要に応じて入手情報の修正、再作成を行う。 また、広域連合の標準システムにおいて対象者の検索結果を表示する画面には、個人識別情報と個人番号を同一画面上に表示することによって、個人識別事項の確認を促し個人番号のみによる対象者の特定を行うことを抑止することで、不正確な特定個人情報で事務を行うことのリスクを軽減している。
その他の措置の内容	—
リスクへの対策は十分か	<p>[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</p>
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	<p>【市区町村(本人)から個人番号を入手する場合の措置】</p> <ul style="list-style-type: none"> ・広域連合の標準システムは市区町村の窓口端末とのみ接続され、接続には専用線を用いる。 ・広域連合の標準システムと市区町村の窓口端末との通信には、認証・通信内容の暗号化を実施している。 ・広域連合の標準システムのサーバー及び端末が接続するローカルエリアネットワーク及び市区町村の窓口端末との専用ネットワークは、ウイ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。 ・ウイ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、ファイアウォール等の設定変更が必要となった際は迅速に実施する。 ・広域連合の標準システム端末には、事務に関係のないアプリケーションはインストールしない。 <p>【地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報を入手する場合の措置】 <中間サーバーにおける措置> ・中間サーバーと当広域連合の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、IPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。</p>
リスクへの対策は十分か	<p>[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</p>
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	当広域連合では市区町村の宛名システムに相当するシステムは存在しない。
事務で使用するその他のシステムにおける措置の内容	当広域連合では広域連合の標準システム以外のシステムは存在しない。
その他の措置の内容	広域連合の標準システムは独立したシステムとなっており、市区町村の窓口端末以外のネットワークシステムからアクセスできないようにすることで、目的を超えた紐付けや、必要のない情報と紐付けさ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2: 権限の無い者(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

ユーザー認証の管理	[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	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・広域連合の標準システム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。 ・広域連合の標準システムへのログイン時の認証において、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号の表示、検索、更新ができない機能により、不適切な操作等が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、パスワードの使いまわしをしないことを徹底している。 <p><取りまとめ機関が定める当広域連合の運用における措置></p> <ul style="list-style-type: none"> ・中間サーバーを利用する職員等を限定し、取り扱うことができる事務の範囲及び個人番号取扱い権限(アクセス権限)の有無を決定して、ユーザIDを管理簿に記載、管理する。 ・共用のユーザIDの使用を禁止する。 ・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。 ・退職や異動でシステム利用者でなくなった者のユーザIDは利用できないよう登録を抹消する。 <p><中間サーバーにおける措置></p> <ul style="list-style-type: none"> ・統合専用端末及びサーバー間連携を利用したシステム操作や特定個人情報等へのアクセスを行う前にログイン操作を行い、統合専用端末の操作者を認証するよう中間サーバーで制御している。 <p><クラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・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には、特定個人情報ファイルの取扱権限を持つIDを発行する。 ・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ないよう系統的に制御する。 ・広域連合ごとに適切なアクセス権をロール設定を割り当てることで、他の自身の広域連合以外の情報にアクセスできないように系統的に制御している。
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない

	<p>具体的な管理方法</p>	<p><標準システムにおける措置> 当広域連合の情報セキュリティ対策基準等に基づき、以下の管理を行う。 (1)ID/パスワードの発効管理 ・広域連合の標準システムへのアクセス権限と事務の対応表を作成する。 ・広域連合の標準システムへのアクセス権限が必要となった場合、事務取扱担当者が担当事務ごとに更新権限の必要があるか、照会権限のみでよいかの種別を確認し、事務に必要なアクセス権限(※1)のみを申請する。 ・情報システム管理者(※2)は、申請に基づき対応表を確認の上、承認(アクセス権限の付与)を行う。 (2)失効管理 ・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、情報システム管理者は、権限を有していた事務取扱担当者の異動/退職情報を確認し、当該事由が生じた際には迅速にアクセス権限を更新し、当該IDを失効させる。</p> <p>※1: 広域連合の標準システムでは、ID、パスワード、操作可能とする機能を組み合わせて、操作(アクセス)権限を管理している。 ※2: 当広域連合の情報セキュリティ対策基準では、各情報システムを所管する担当課長を「情報システム管理者」と定義しており、情報システム管理者は所管する情報システムの設定変更等を行う権限を有するとともに、同システムの情報セキュリティに関する責任を有する。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> アクセス権限は、情報システム管理者(※3)が各職員等の担当事務分野とアクセス権限を決定し、標準システムにおけるユーザ認証の管理やアクセス権限の発効・失効と同様に管理する。 (1)発効管理 ・採用や異動などで中間サーバーを利用する事務を担当する職員等には、担当となる日から有効なアクセス権限を、管理者の指示により登録し、管理簿に記載する。 (2)失効管理 ・異動や退職などで担当から外れる職員等には、異動日や退職日をもって現在のアクセス権限が失効するよう、情報システム管理者の指示により登録を変更し、管理簿に記載する。</p> <p><中間サーバーにおける措置> 当広域連合の情報システム管理者が統合専用端末において以下の管理を行う。 ・IDは、ID付与権限をもった情報システム管理者用IDと一般的なユーザIDがある。 ・支払基金が各医療保険者等の情報システム管理者用IDに対して一般的なIDの付与権限を与えることにより、各医療保険者等において情報システム管理者が職員に対して一般的なユーザIDを付与することが可能となる。 ・指定日から職員IDを有効にしたり、指定日から職員IDを無効とするよう中間サーバー側で制御している。 ・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。</p> <p>※3:「医療保険者向け中間サーバーとの接続運用に係る運用管理規程(医療保険者向け)」には、「情報システム責任者」とされているが、当広域連合の情報セキュリティ対策基準では「情報システム管理者」が行うこととしている。</p> <p><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等には、情報システム管理者が、特定個人情報ファイルの取扱権限を持つIDを発効する。 ・移行作業終了後は際には、情報システム管理者が迅速にアクセス権限を更新し、当該IDを失効させる。</p>
<p>アクセス権限の管理</p>	<p>[行っている]</p>	<p><選択肢> 1)行っている 2)行っていない</p>

	<p>具体的な管理方法</p>	<p><標準システムにおける措置> ・当広域連合の情報セキュリティ対策基準等に基づき、情報システム管理者は、以下のようなアクセス権限の管理を実施する。 ・情報システム管理者権限については、毎月証跡(ログ)と使用記録の目視確認を行う。 ・一般ユーザ権限については、定期的及び必要に応じてユーザー一覧を広域連合の標準システムより画面出力し、ユーザ管理台帳と目視による突合を行ってアクセス権限の確認及び不正利用の確認を行う。 ・広域連合の標準システムにログイン・ログアウトを実施した職員等(ログインID含む)、時刻、操作内容(照会内容)の記録を定期的及び必要に応じて確認し、不正な運用が行われていないかを点検する。 ・職員等向けに、情報セキュリティ教育を実施し情報セキュリティ対策の重要性及び意識向上を行うとともに、情報システム運用教育を実施し情報システムの適正な運用を行うことの啓発に努めている。 ・広域連合の標準システムでは、共用IDは使用しないこととしている。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> ・ユーザID、アクセス権限の登録や変更は、情報システム管理者以外には行えないものとする。 ・情報システム管理者は、ユーザIDやアクセス権限の登録や変更を行う都度、管理者の確認を得て管理簿に記載し保管する。 ・情報システム管理者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与など管理簿の点検・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。</p> <p><中間サーバーにおける措置> ・該当する当広域連合の職員等に許可された業務メニューのみ表示するよう中間サーバーで制御している。</p> <p><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、情報システム管理者が、特定個人情報ファイルの取扱権限を持つIDを発効する。 ・移行作業終了後は、情報システム管理者が迅速にアクセス権限を更新し、当該IDを失効させる。</p>
<p>特定個人情報の使用の記録</p>	<p>[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</p>	
	<p>具体的な方法</p>	<p><標準システムにおける措置> ・広域連合の標準システム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・アクセス失敗の履歴を記録している。 ・情報システム管理者は定期的及び必要に応じて、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点検する。 ・当該記録については、一定期間保存することとしている。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> ・中間サーバーの使用について、情報システム管理者は、定期的に又はセキュリティ上の問題が発生した際に操作ログに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点検する。</p> <p><中間サーバーにおける措置> ・特定個人情報ファイルを扱う統合専用端末の操作履歴(操作ログ)を中間サーバーで記録している。</p>
<p>その他の措置の内容</p>	<p>—</p>	
<p>リスクへの対策は十分か</p>	<p>[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</p>	

リスク3: 従業員が事務外で使用するリスク

<p>リスクに対する措置の内容</p>	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・広域連合の標準システムへのログイン時の認証において、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号の表示、検索、更新ができない機能を設けている。 ・また、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号を電子記録媒体等へ書込むこと等もできない。 ・広域連合の標準システム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及び必要に応じて、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を点検する。 ・職員等向けに、情報セキュリティ教育を実施し情報セキュリティ対策の重要性及び意識向上を行うとともに、情報システム運用教育を実施し情報システムの適正な運用を行うことの啓発に努めている。 ・中間サーバーとのサーバー間連携機能の開始・停止等の操作は、情報システム管理者によって統合専用端末の操作を許可された者のみしか行うことができない。 <p><中間サーバーにおける措置></p> <ul style="list-style-type: none"> ・統合専用端末連携及びサーバー間連携を利用した情報照会依頼時等において、当広域連合の職員に許可された事務／事務手続のみ取り扱うことができるよう中間サーバーで制御している。 <p><クラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・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。 ・移行作業にあたって、作業員以外は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。 ・移行以外の目的・用途でファイルを作成しないよう、作業員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。 ・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。 ・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。
<p>リスクへの対策は十分か</p>	<p>[十分である]</p> <p><選択肢></p> <p>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</p>

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

<p>リスクに対する措置の内容</p>	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・GUIによるデータ抽出機能(※1)は広域連合の標準システム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及び複製されることはない。 ・また、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号を電子記録媒体等へ書込むこと等もできない。 ・ファイルのバックアップ及び統合専用端末との情報授受については、操作権限によるアクセス制御以外に、操作を行う広域連合の標準システム端末を限定して運用することとする。 ・広域連合の標準システム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、情報システム管理者が定期的及び必要に応じて記録の内容を確認し、不正な運用が行われていないかを点検する。 ・職員等向けに、情報セキュリティ教育を実施し情報セキュリティ対策の重要性及び意識向上を行うとともに、情報システム運用教育を実施し情報システムの適正な運用を行うことの啓発に努めている。 ・バックアップファイルは暗号化し、保管室に施錠保管する。 ・電子記録媒体は媒体管理簿に記載し、施錠保管する。 <p>※1:ここでいうGUIによるデータ抽出機能とは、後期高齢者医療関係情報ファイルのデータベースからデータを抽出に当たっての抽出条件等を、端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で端末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。</p> <p><取りまとめ機関が定める当広域連合の運用における措置></p> <p>委託区画ファイル、副本区画ファイル及び本人確認ファイルについては、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・中間サーバーを利用して複製等のファイル操作が可能な職員等を最小限に限定する。 ・電子記録媒体やフラッシュメモリへの複製を行う場合、不必要な複製を制限するため事前に情報システム管理者の承認を得る。 ・被保険者の登録情報を確認する以外にファイルを複製しないよう、職員等に対し周知徹底する。 ・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視する。 <p><中間サーバーにおける措置></p> <ul style="list-style-type: none"> ・情報提供等記録ファイルについては、統合専用端末やサーバー間連携を利用して当広域連合の職員が情報提供等記録をファイル出力(ダウンロード)(※2)する際は、情報提供等記録ファイルから機関別符号等を除いた範囲の項目にしかアクセスできず、当該アクセス可能な項目のみしか複製できないよう制限している。 ・委託区画ファイル及び副本区画ファイルについては、統合専用端末やサーバー間連携を利用して当広域連合の職員がファイル出力(ダウンロード)(※2)する際に特定の項目にしかアクセスできず、当該アクセス可能な項目のみしか複製できないよう制限している。 <p>※2:ファイル出力(ダウンロード)する機能は、住民基本台帳ネットワークシステム及び情報提供ネットワークシステムから取得した特定個人情報を標準システムに取り込むために必要となる。</p> <p><クラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・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には、特定個人情報ファイルの取扱権限を持つIDを発効する。 ・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。 ・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。 ・移行以外の目的・用途でファイルを作成しないよう、作業者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。 ・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。 ・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。
<p>リスクへの対策は十分か</p>	<p>[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</p>
<p>特定個人情報の使用におけるその他リスク及びそのリスクに対する措置</p>	
<p>—</p>	

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

<p>情報保護管理体制の確認</p>	<p>当広域連合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。</p> <ul style="list-style-type: none"> ・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、施設及び設備の整備、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 ・情報セキュリティマネジメントシステムの国際規格の認証取得情報
<p>特定個人情報ファイルの閲覧者・更新者の制限</p>	<p>[制限している] (選択肢) 1) 制限している 2) 制限していない</p> <p>具体的な制限方法</p> <p><当広域連合で行う委託業務における措置> ・委託契約仕様書に「当広域連合セキュリティポリシーに従い作業を行うこと」と定め、受託条件明細において「委託先の責任者、委託内容、作業者、作業場所」を明記している。 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、定期会議にて委託業務の報告を受けるとともに、事故発生時には委託業者は直ちに通知を行うよう、委託契約書に明記している。</p> <p><取りまとめ機関で行う委託業務における措置> ・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中間サーバーで制御している。 ・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。また、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。</p>
<p>特定個人情報の使用の記録</p>	<p>[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</p> <p>具体的な方法</p> <p><当広域連合で行う委託業務における措置> ・委託先の従業員等が広域連合の標準システムへログインした際に、ログインを実施した従業員等・時刻・操作内容が広域連合の標準システムに記録されるので、情報システム管理者が広域連合の標準システムの記録を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、当広域連合の文書に関する訓令第23条に従い、一定期間保存する。</p> <p><取りまとめ機関で行う委託業務における措置> ・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。</p>
<p>特定個人情報の提供ルール</p>	<p>[定めている] (選択肢) 1) 定めている 2) 定めていない</p> <p>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</p> <p><当広域連合で行う委託業務における措置> ・当広域連合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及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、又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こととしている。 ・さらに、当広域連合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、操作ログを確認し、詳細な調査・確認が必要と判断したときは調査を行い、又は報告を求める。</p> <p><取りまとめ機関で行う委託業務における措置> ・契約書において当広域連合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視する。</p>

	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	<p><当広域連合で行う委託業務における措置></p> <ul style="list-style-type: none"> ・定期会議にて委託業務の報告を受けるとともに、事故発生時には委託業者は直ちに通知を行うよう、委託契約書に明記している。 ・委託元と委託先間の特定個人情報のやり取りに関しては、広域連合の標準システム上で操作内容を記録している。 ・記録の保存期間については、当広域連合の文書に関する訓令第23条に従い、一定期間保存する。 ・さらに当広域連合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、操作ログを確認し、詳細な調査・確認が必要と判断したときは調査を行い、又は報告を求める。 <p><取りまとめ機関で行う委託業務における措置></p> <ul style="list-style-type: none"> ・提供情報は、業務委託完了時に全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視する。
特定個人情報の提供ルール		<p>[定めている] <選択肢></p> <p>1) 定めている 2) 定めていない</p>
	ルール内容及びルール遵守の確認方法	<p><当広域連合で行う委託業務における措置></p> <ul style="list-style-type: none"> ・特定個人情報等は、業務完了後は速やかに返還し、又は漏えいを起こさない方法によって確実に消去、もしくは処分することを、当広域連合の情報セキュリティ対策基準に基づき、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、情報システム管理者が消去及び廃棄状況の調査、確認を行う。 <p><取りまとめ機関で行う委託業務における措置></p> <ul style="list-style-type: none"> ・情報提供等記録については、番号法第23条第3項に基づく施行令第29条の規定において、保存期間は7年間とされており、保存期間経過後は、当広域連合が適切に廃棄等を行う。
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		<p>[定めている] <選択肢></p> <p>1) 定めている 2) 定めていない</p>
	規定の内容	<ul style="list-style-type: none"> ・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。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・特定個人情報の目的外利用の禁止、複写・複製の禁止。 ・再委託の禁止(再委託するケースでは、その条件)。 ・漏えい、滅失、棄損、改ざん等の防止策の義務付け。 ・漏えい事案等が発生した場合の委託先の責任の明確化。 ・委託契約終了後の特定個人情報の返却又は廃棄。 ・特定個人情報を取り扱う従業者の限定と明確化。 ・従業者に対する監督・教育。 ・委託先への監査、立入調査。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報の消去・返却・保管ルールに関する規定。 ・契約内容の遵守状況について報告の義務付け。 <p>等を定めるとともに委託先が当広域連合と同等の安全管理措置を講じていることを確認する。</p>
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		<p><選択肢></p> <p>[十分に行っている]</p> <p>1) 特に力を入れて行っている 2) 十分行っている 3) 十分に行っていない 4) 再委託していない</p>

	<p>原則として再委託は行わないこととする。ただし広域連合と委託先の協議により再委託を行うことが適当であると合意した場合は、再委託を行うことができる。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。</p> <ul style="list-style-type: none"> ・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。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・特定個人情報の目的外利用の禁止、複写・複製の禁止。 ・再委託の禁止(再委託するケースでは、その条件)。 ・漏えい、滅失、棄損、改ざん等の防止策の義務付け。 ・漏えい事案等が発生した場合の委託先の責任の明確化。 ・委託契約終了後の特定個人情報の返却又は廃棄。 ・特定個人情報を取り扱う従業者の限定と明確化。 ・従業者に対する監督・教育。 ・委託先への監査、立入調査。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報の消去・返却・保管ルールに関する規定。 ・契約内容の遵守状況について報告の義務付け等。 <p>また再委託先が当広域連合と同等の安全管理措置を講じていることを確認する。</p>
<p>具体的な方法</p>	<ul style="list-style-type: none"> ・標準システムを、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OS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。 ・標準システムを、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示した上で、許諾を得ること。
<p>その他の措置の内容</p>	<p>—</p>
<p>リスクへの対策は十分か</p>	<p>[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</p>
<p>特定個人情報ファイルの取扱いの委託におけるその他リスク及びそのリスクに対する措置</p> <p>—</p>	

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	<p>広域連合の標準システムから市区町村の窓口端末へのデータ配信の実施においては、広域連合の標準システムへのログインを実施した職員等・時刻・操作内容及びデータ配信されたデータが広域連合の標準システムに記録されるため、情報システム管理者が広域連合の標準システムの記録を調査することで操作者個人を特定する。</p> <p>記録の保存期間については、当広域連合の文書に関する訓令第23条に従い、一定期間保存する。</p> <p>(注) 市区町村の窓口端末へのデータ配信については、内部利用と整理されているが、便宜上「移転」の欄に記載している。</p>
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	<ul style="list-style-type: none"> ・広域連合の標準システムから市区町村の窓口端末へのデータ配信については、「府番第27号 一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について(通知) 平成27年2月13日」において、同一部署内での内部利用の取扱いとするとされている。 ・市区町村の窓口端末以外への特定個人情報のデータ配信は行っていない。 ・情報システム管理者は広域連合の標準システムから市区町村へのデータ配信に関する記録と関連する書面の記録を照合して確認し、不正なデータ配信が行われていないかを監査する。
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: 不正な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・広域連合の標準システムからのデータ配信は、市区町村の窓口端末以外には行えない仕組みとなっており、配信処理が可能な職員等については、広域連合の標準システムへのログインIDによる認可により事務取扱担当者に限定している。 ・広域連合の標準システムへのログインを実施した職員等・時刻・操作内容及びデータ配信されたデータが広域連合の標準システムに記録されるため、情報システム管理者が広域連合の標準システムの記録を調査することで、操作者個人を特定する。 ・広域連合の標準システムのサーバー及び端末が接続するローカルエリアネットワーク及び市区町村に設置する窓口端末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している。 ・広域連合の標準システム端末には、事務に関係のないアプリケーションはインストールしない。 ・データ配信先の市区町村は、高齢者の医療の確保に関する法律第107条及び第108条(法令上の根拠)に基づき、保険料徴収等を行うためにデータを取り扱うため、データの使途は明確である。
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	<ul style="list-style-type: none"> ・広域連合の標準システムからのデータ配信は、市区町村の窓口端末以外には行えない仕組みとなっている。 ・配信データと配信先については、必ず二人以上の担当者によって、広域連合の標準システムへの入力(実行指示)内容の確認を行う。 ・広域連合の標準システムのサーバー及び端末が接続するローカルエリアネットワーク及び市区町村に設置する窓口端末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している。 ・広域連合の標準システム端末には、事務に関係のないアプリケーションはインストールしない。
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	<p><標準システムにおける措置> 情報照会結果の入手元は、統合専用端末及びサーバー間連携を行う端末に限定されており、入手データは情報提供ネットワークシステム及び中間サーバーにおいて厳格な審査が行われている。 なお、情報照会の要求を行う際、広域連合の標準システム又は市町村の窓口端末の入力画面では、必要な情報のみが入力項目及び選択肢として表示されるので、必要以上の情報が端末から入力されて目的外の情報照会がされることのリスクを軽減している。</p> <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバーにおける措置> ①統合専用端末やサーバー間連携を利用して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(※)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支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバーで記録しているため、不適切な統合専用端末の操作や、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。</p> <p>(※)番号法別表第二に基づき、事務手続ごとに情報照会者、情報提供者、照会・提供可能な特定個人情報リスト化したもの。</p>		
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	<p><標準システムにおける措置> 中間サーバーを介することなく、情報提供ネットワークシステムシステムに接続して情報照会を行うことはできないしくみとなっている。 情報照会に用いるインターフェースについては、中間サーバーによって厳格にそのファイル仕様が規定されており、標準システムにおいてもその仕様を準拠してインターフェースファイルを作成することとしているため、指定された規格に即した情報のみを取り扱うことになる。</p> <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバーにおける措置> 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。 ②中間サーバーと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厚生労働省統合ネットワークを利用することにより、安全性を確保している。 ③中間サーバーと医療保険者等の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、又は公衆回線を使用する場合はIPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。</p>		
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	<p><標準システムにおける措置> 情報照会によって入手した情報を広域連合の標準システムのデータベースに更新する際には、照会要求との関連性や項目間の整合性のチェックを行っており、確認リストが出力されたら、事務取扱担当者が確認リストの内容をよく確認し、必要に応じて入手元の情報保有機関に確認し、必要に応じて再度、情報照会を行うなどの措置を行う。</p> <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバーにおける措置> ・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、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。</p>		
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	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・広域連合の標準システムは市区町村の窓口端末とのみ接続され、接続には専用線を用いる。 ・広域連合の標準システムと市区町村の窓口端末との通信には、認証・通信内容の暗号化を実施している。 ・中間サーバーとサーバー間連携を行う場合、中間サーバーとサーバー間連携を行う端末は1台に限定し、中間サーバーとの接続には専用線を用い通信には認証・通信内容の暗号化を実施している。 ・広域連合の標準システムのサーバー及び端末が接続するローカルエリアネットワーク及び市区町村の窓口端末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、ファイアウォール等の設定変更が必要となった際は迅速に実施する。 ・広域連合の標準システム端末には、事務に関係のないアプリケーションはインストールしない。 <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。</p> <p><中間サーバーにおける措置></p> <ol style="list-style-type: none"> 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中間サーバーは、外部システムからの接続に対し認証を行い、許可されていない外部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。また、標準システムと中間サーバーとはオンライン接続しないこととしている。 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支払基金の職員が情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバーで記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑制する仕組みになっている。 ⑤中間サーバーと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厚生労働省統合ネットワーク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。 ⑥中間サーバーと医療保険者等の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、又は公衆回線を使用する場合はIPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。 <p>※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。</p>
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	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・広域連合の標準システムにおいて副本データを作成する際には、広域連合の標準システムへのログインを実施した職員等・時刻・操作内容及びデータ配信されたデータが広域連合の標準システムに記録されるため、情報システム管理者が広域連合の標準システムの記録を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、当広域連合の文書に関する訓令第23条に従い、一定期間保存する。 ・情報システム管理者は広域連合の標準システムから統合専用端末への副本データ登録に関する記録を確認し、不正なデータ登録が行われていないかを点検する。 <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。</p> <p><中間サーバーにおける措置></p> <ol style="list-style-type: none"> ①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、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支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバーで記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑制する仕組みになっている。
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6: 不適切な方法で提供されるリスク

<p>リスクに対する措置の内容</p>	<p><標準システムにおける措置> ・広域連合の標準システムにおいて副本データを作成する際には、広域連合の標準システムへのログインを実施した職員等・時刻・操作内容及びデータ配信されたデータが広域連合の標準システムに記録されるため、情報システム管理者が広域連合の標準システムの記録を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、当広域連合の文書に関する訓令第23条に従い、一定期間保存する。 ・情報システム管理者は広域連合の標準システムから統合専用端末への副本データ登録に関する記録を確認し、不正なデータ登録が行われていないかを監査する。 ・なお、中間サーバーを介することなく、情報提供ネットワークシステムに接続して情報提供を行うことはできないしくみになっている。</p> <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバーにおける措置> ①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支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバーで記録しているため、不適切な統合専用端末の操作や、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。 ③中間サーバーと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厚生労働省統合ネットワーク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。 ④中間サーバーと医療保険者等の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、又は公衆回線を使用する場合はIPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。</p>
<p>リスクへの対策は十分か</p>	<p>[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</p>

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

<p>リスクに対する措置の内容</p>	<p><標準システムにおける措置> 中間サーバーを介することなく、情報提供ネットワークシステムシステムに接続して情報提供を行うことはできないしくみとなっている。 副本登録に用いるインターフェースについては、中間サーバーによって厳格にそのファイル仕様が規定されており、標準システムにおいてもその仕様を準拠してインターフェースファイルを作成することとしているため、指定された規格に即した情報のみを取り扱うことになる。</p> <p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバーにおける措置> ①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データの形式チェックと、統合専用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統合専用端末において、情報提供データベースの副本データを標準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は、該当する医療保険者等のみが利用できるよう制限している。</p>
<p>リスクへの対策は十分か</p>	<p>[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</p>

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

<統合専用端末と標準システムとの間の情報授受に係るリスク対策>

- ・統合専用端末と標準システムとの間の情報授受に係る業務を行う職員等を必要最小限に限定し、そのユーザIDとアクセス権限が付与された者以外が情報授受に係る業務ができないよう系統的に制御する。
- ・情報授受で電子記録媒体やフラッシュメモリへの複製を行う場合、不必要な複製を制限するため事前に情報システム管理者の承認を得る。
- ・情報授受に用いる電子記録媒体やフラッシュメモリが使用できる標準システムの端末を限定し、それ以外の端末では使用しない運用をする。
- ・フラッシュメモリを使用する場合はパスワード認証機能付きで、書き込まれるデータは全て自動暗号化される媒体とし、情報システム管理者がパスワード設定した媒体以外は統合専用端末で使用できないよう系統的に制御する。
- ・標準システムの端末及び統合専用端末の操作ログを記録し、情報システム管理者が定期的に又はセキュリティ上の問題が発生した際に、電子記録媒体やフラッシュメモリへの不必要な複製をチェックする。
- ・統合専用端末は中間サーバ以外とは接続せず、他の業務に兼用できないよう他のネットワークやシステムと分離する。
- ・統合専用端末の使用後、ハードディスク等内の特定個人情報データはすべて削除する。
- ・リライトできる電子記録媒体又はフラッシュメモリではデータを保存せず、使用した都度、データをすべて削除する。

<中間サーバーと標準システムとの間の情報授受に係るリスク対策>

- ・中間サーバーとサーバー間連携を行う端末は1台とする。
- ・中間サーバーとサーバー間連携を行う端末は、標準システムのローカルネットワークと中間サーバー以外とは接続せず、他の業務に兼用できないよう他のネットワークやシステムと分離する。
- ・不正アクセス防止策として、標準システムのネットワークと中間サーバーとの間にファイアウォールを導入する。
- ・中間サーバーとのサーバー間連携機能の開始・停止等の操作は、情報システム管理者によって統合専用端末の操作を許可された者のみしか行うことができない。

情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。

<中間サーバーにおける措置>

- ①支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバーで記録しているため、不適切な統合専用端末の操作や、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中間サーバーにて担保されており、不正な名寄せが行われるリスクに対応している。
- ③中間サーバーと情報提供ネットワークシステムの間は、高度なセキュリティを維持した厚生労働省統合ネットワークを利用することにより、安全性を確保している。
- ④中間サーバーと医療保険者等の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、又は公衆回線を使用する場合はIPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。
- ⑤中間サーバーでは、特定個人情報を管理するデータベースを医療保険者等ごとに区分管理(アクセス制御)しており、中間サーバーを利用する医療保険者等であっても他の医療保険者等が管理する情報には一切アクセスできない。

7. 特定個人情報の保管・消去

リスク1: 特定個人情報の漏えい・滅失・毀損リスク

①NISC政府機関統一基準群	[政府機関ではない]	〈選択肢〉 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	〈選択肢〉 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規定	[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・規定の職員への周知	[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

〈標準システムにおける措置〉
 ・標準システムは、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。
 ・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。
 ・クラウド環境にアクセスできる運用・保守拠点では、電子錠等による入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにする。また、管理簿等による入退室情報の収集ができ、入退室の記録を取得可能とする。
 ・電子記録媒体は、適切に管理された鍵にて施錠可能な場所に保管し、利用の際には都度、媒体管理簿に記入する。
 ・使用済み電子記録媒体を廃棄する場合は物理的破壊等によりデータを復元できないように完全に消去する。

〈中間サーバーにおける措置〉
 ・中間サーバーを取りまとめ機関のデータセンターに設置し、設置場所への入退室記録管理、監視カメラによる監視及び施錠管理をすることでリスクを回避する。

〈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。

<p>⑥技術的対策</p> <p>具体的な対策の内容</p>	<p>[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</p> <p><標準システムにおける措置> ・標準システムにおいて保有する特定個人情報、端末等を通じてインターネットに流出することを防止するため、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。 ・標準システムでは、セキュリティ対策を実施するクラウドマネージドサービス(クラウド事業者により運用管理まで含めた形で提供されるサービス)等を活用し、アクセス制御、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。 ・クラウドマネージドサービスの利用にあたっては、クラウド事業者は個人番号を含む電子データを取り扱わない契約とし、クラウド事業者が個人番号等にアクセスできないように、アクセス制御を行う。 ・標準システムには、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。 ・広域連合の標準システムのウイルス管理マネージャ(※1)を用いて、ウイルスパターンファイルの適用が漏れている機器を把握し、情報システム管理者等が迅速に適用を行う。 ・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。 ・国の定めた基準に基づき、安全なセキュリティ環境を構築している。 ※1: ウイルス管理マネージャとは、広域連合の標準システムの各サーバー、各端末のウイルス対策状況を集中管理する機能。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> ・統合専用端末及びサーバー間連携を行う端末はインターネットに接続できないよう分離する。 ・統合専用端末は中間サーバー以外の情報系端末等に兼用できないよう分離などにより、リスクを回避する。 ・サーバー間連携を行う端末は中間サーバーと標準システム以外の情報系端末等に兼用できないよう分離などにより、リスクを回避する。</p> <p><中間サーバーにおける措置> ①中間サーバー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、中間サーバー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。 ②中間サーバーでは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。 ③中間サーバーでは、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。 ④導入しているOS及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。 ⑤中間サーバーと当広域連合の通信は、VPN等の技術を用いた専用線、IP-VPNによる閉域サービス、又は公衆回線を使用する場合はIPSecによる暗号化された通信経路を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。</p> <p><クラウド移行作業時に関する措置> ・移行作業時に用いる電子記録媒体に格納したファイルは暗号化し、追記はできない状態とし、作業終了後は、不正利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。</p>
<p>⑦バックアップ</p>	<p>[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</p>
<p>⑧事故発生時手順の策定・周知</p>	<p>[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</p>
<p>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</p> <p>その内容</p> <p>再発防止策の内容</p>	<p>[発生なし] <選択肢> 1) 発生あり 2) 発生なし</p> <p>—</p> <p>—</p>
<p>⑩死者の個人番号</p> <p>具体的な保管方法</p>	<p>[保管している] <選択肢> 1) 保管している 2) 保管していない</p> <p>生存者の個人番号と同様の方法にて安全管理措置を実施する。</p>
<p>その他の措置の内容</p>	<p>—</p>
<p>リスク対策は十分か</p>	<p>[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</p>

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	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・システム上、市区町村からの日次での送信データによって、住民基本台帳情報及び住登外登録情報等を入手し、広域連合の標準システムのデータベースを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ことはない。 また、その他の情報についても、市区町村から定期的にデータ連携による入手を行うことで、広域連合の標準システムのデータベースを更新しているため、特定個人情報が古い情報のまま保管され続けることはない。 <p><取りまとめ機関が定める当広域連合の運用における措置></p> <ul style="list-style-type: none"> ・被保険者の資格情報等の新規登録又は情報の更新があった際は、速やかに中間サーバーの委託区画又は副本区画の情報を登録・更新する。
リスク対策は十分か	[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	<p><標準システムにおける措置></p> <ul style="list-style-type: none"> ・高齢者の医療の確保に関する法律により平成26年度までに賦課された保険料に関しては期間の制限なく保険料賦課額を減額更正できるとされているため、事務に必要な期間が経過した時点で消去することとしている。 ・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ISO/IEC27001に準拠した廃棄プロセスを確保していること。 ・廃棄プロセスの適切な実施について、第三者の監査機関による監査を受け、その内容を確認できること。 <p><取りまとめ機関が定める当広域連合の運用における措置></p> <ul style="list-style-type: none"> ・資格審査時に中間サーバーの運用支援環境(委託区画)に特定個人情報を登録する。資格審査の結果、資格を得られない場合には、運用支援環境(委託区画)に登録した特定個人情報を消去する。 ・特定個人情報の保管期間を超えた被保険者について、中間サーバー委託区画に登録されている資格情報を削除する。 ・また、バッチ処理を起動することで副本区画に登録されている副本情報を削除する。 <p><クラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・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。 ・データ消去を他者に委託する場合は、特定個人情報が記録された機器を廃棄する際は、消去証明書等により消去されたことを確認する。
その他の措置の内容	—
リスク対策は十分か	[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	
<p>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</p> <p>【運用上のルールによる措置】</p> <ul style="list-style-type: none"> ・プリンタ、FAX等の出力用紙の放置禁止の徹底 ・不要となった特定個人情報記載の用紙のシュレッダーの実施 ・溶解処分業者の委託契約による保存満了分文書廃棄の実施 ・書類又はメディアの搬送時の所在追跡可能な手段の実施 ・執務用デスク周辺の整理整頓及び退社時の施錠の実施 ・離席時のスクリーンセーバー又はシャットダウン ・リース機器返却時、HDD内の特定個人情報が復元不可能な形態での消去の実施 ・機器の廃棄時、HDDやメモリーの破壊の実施 ・電子記録媒体からデータを読み込む前に必ずウイルスチェックを行う <p>【特定個人情報の漏えい事案等が発生した場合の対応】</p> <p>平成27年9月28日特定個人情報保護委員会告示(平成27年12月25日改正)の「特定個人情報の漏えい事案等が発生した場合の対応について」に基づき、次の対応を行う。</p> <ol style="list-style-type: none"> (1) 事業者内の責任ある立場の者に直ちに報告するとともに、被害の拡大を防止する。 (2) 事実関係を調査、監査し、番号法違反又は番号法違反のおそれが把握できた場合には、その原因究明を行う。 (3) 上記(2)で把握した事実関係による影響の範囲を特定する。 (4) 上記(2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。 (5) 事案の内容に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに本人に連絡又は本人が容易に知り得る状態に置く。また、事実関係及び再発防止策等について、速やかに公表する。 (6) 厚生労働大臣が定めるガイドライン等の規定による報告先に速やかに報告する。また、重大事案など指定のある事案については個人情報保護委員会に報告する。 	

IV その他のリスク対策※

1. 監査	
①自己点検	<p>[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分やっている 3) 十分にやっていない</p>
具体的なチェック方法	<p>当広域連合の情報システム管理者は、広域連合の標準システム及び所管するネットワークにおける情報セキュリティポリシーに沿った情報セキュリティ対策状況について点検を行うために、自己点検項目のチェックリストを作成し、当該チェックリストを用いて必要に応じて(年に1度実施)点検を実施し、その点検結果を最高情報セキュリティ責任者(※1)に報告している。</p> <p>※1: 当広域連合の情報セキュリティ対策基準により、広域連合事務局長を最高情報セキュリティ責任者とし、最高情報セキュリティ責任者は、当広域連合における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。</p>
②監査	<p>[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分やっている 3) 十分にやっていない</p>
具体的な内容	<p>・当広域連合の最高情報セキュリティ責任者は、熊本県後期高齢者医療広域連合個人情報保護審査会条例(令和5年3月31日までは、熊本県後期高齢者医療広域連合個人情報保護条例)に基づき、必要に応じて当広域連合の個人情報保護審査会に対し、自己点検結果を諮問する。</p> <p>・個人情報保護審査会による答申で指摘された事項についての改善状況及び広域連合の事務全般の執行状況については、定期的(年に1度実施)に監査委員(※1)の監査(定期監査)を受け、その監査結果を広域連合議会に提出する。</p> <p>・個人情報保護審査会による答申及び監査委員による監査結果によって指摘された事項は改善状況を確認し、PDCAサイクルによる課題又は問題点の把握、改善に努めている。</p> <p>※1: 監査委員は、広域連合の財務に関する事務の執行、経営に関する事業の管理及び広域連合の事務事業の執行について監査等を実施する独任制の機関であり、広域連合規約に基づき広域連合長が議会の同意を得て選任する。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> 当広域連合は、運用管理規程に基づき、標準システム及び当広域連合の運用における安全管理措置について、定期的に監査を行うこととしている。</p>
2. 従業員に対する教育・啓発	
従業員に対する教育・啓発	<p>[特に力を入れてやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分やっている 3) 十分にやっていない</p>
具体的な方法	<p>・職員及び会計年度任用職員の就任時には、情報セキュリティ管理者が、広域連合及び市区町村職員を対象とした新任担当者研修会の中で個人情報保護を含む情報セキュリティについての研修を実施している。</p> <p>・また、就任時以外にも、広域連合の全職員を対象とした個人情報保護を含む情報セキュリティについての研修を、必要に応じて(年に1度実施)実施している。</p> <p>・委託者に対しては、委託契約書において個人情報保護に関する秘密保持契約を締結するとともに、情報セキュリティ管理者が委託者に対して情報セキュリティポリシー等のうち委託者が守るべき内容の遵守及びその機密事項を説明している。</p> <p>・セキュリティ研修等の未受講者に対しては、再受講の機会を付与している。</p> <p>・違反行為を行ったものに対しては、都度指導の上、違反行為の重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。</p> <p><取りまとめ機関が定める当広域連合の運用における措置> ・中間サーバーの統合専用端末における操作について、厚生労働省が当広域連合の職員に対して、統合専用端末導入前に研修を行う。</p>
3. その他のリスク対策	
-	

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	〒862-0911 熊本市東区健軍2丁目4番10号(熊本市町村自治会館2階) 熊本県後期高齢者医療広域連合 総務課 ※郵送の場合の宛先についても同上
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	請求方法、指定様式等について当広域連合のWebサイト上に表示済。
③手数料等	[無料] <選択肢> 1)有料 2)無料 (手数料額、納付方法:手数料は無料であるが、写しの作成及び送付に要する費用は請求者負担。納付方法は納付書による口座振込。)
④個人情報ファイル簿の公表	[行っていない] <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	—
公表場所	—
⑤法令による特別手続	—
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	〒862-0911 熊本市東区健軍2丁目4番10号(熊本市町村自治会館2階) 熊本県後期高齢者医療広域連合 事業課
②対応方法	<ul style="list-style-type: none"> ・問い合わせの受付時に受付票を起票し、対応について記録を残す。 ・情報漏えい等の重大な事案に関する問い合わせであれば、関係先等にその事実確認を行うための標準的な処理期間を有する。

VI 評価実施手続

1. 基準日評価	
①実施日	令和4年12月28日
②しきい値判断結果	<p>[基礎項目評価及び全項目評価の実施が義務付けられる]</p> <p>〈選択肢〉</p> <p>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</p> <p>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)</p> <p>3)基礎項目評価の実施が義務づけられる(任意に全項目評価を実施)</p> <p>4)特定個人情報保護評価の実施が義務づけられない(任意に全項目評価を実施)</p>
2. 国民・住民等からの意見の聴取	
①方法	熊本県後期高齢者医療広域連合のホームページにて意見を募集。 熊本県後期高齢者医療広域連合事務局に特定個人情報保護評価書を設置し、意見を募集。
②実施日・期間	
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	
②方法	当広域連合における個人情報保護審査会による点検。
③結果	
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	