資料1－1

令和6年1月31日
第270回個人情報保護委員会資料

特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
1	関東ITソフトウェア健康保険組合における 適用、給付及び徴収関係事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

関東ITソフトウェア健康保険組合（以下「当組合」という。）は、適用、保険給付及び保険料等徴収関係事務において特定個人情報ファイルを取り扱うに当たり、その取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えい、その他の事態が発生す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	・当組合は一般財団法人日本情報経済社会推進協会（JIPDEC)から、日本工業規格JISQ15001：2017に適合して個人情報について適切な保護措置を講ずる体制を整備・運用している事業者等に認定される「プライバシーマーク」を取得しています。 ・特定個人情報を取り扱うことができる職員を限定し、他の職員や外部から特定個人情報にアクセスできないようシステム的に制御します。 ・特定個人情報にアクセスしたとき、いつ・だれが・どこからアクセスをしたか、システムで操作記録を自動的に残します。 ・基幹システムと中間サーバー等をサーバー間接続することにより、電子記録媒体等で統合専用端末とのデータ授受業務を減らし、電子記録媒体等への不正な複製や媒体の持出し、紛失等が生じるリスクを軽減します。

評価実施機関名

関東ITソフトウェア健康保険組合

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

［平成30年5月　様式4］

項目一覧

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	適用、給付及び徴収関係事務
②事務の内容　※	＜制度内容＞ 　当組合は、健康保険法（大正11年法律第70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。）等に基づき、医療保険の運営の効率化、給付の内容及び費用の負担の適正化並びに加入者の健康の維持・増進、加入者が受ける医療の質の向上を図ることを目的としている。その目的を達成するため当組合では、事業主と被保険者の代表による事業・運営計画の策定、保険料の徴収、保険給付、診療報酬明細書の内容審査、健康診査や体力づくり等の保健事業、加入者への広報活動、直営健診センターや保養施設の運営等を行っている。 　また、他の医療保険者等と共同して「被保険者等に係る情報の収集又は整理に関する事務」及び「被保険者等に係る情報の利用又は提供に関する事務」を社会保険診療報酬支払基金（以下「支払基金」という。）に委託することができる旨の規定が健康保険法に盛り込まれ、加入者の資格履歴情報と被保険者枝番の採番管理、地方公共団体等と情報提供ネットワークシステムを通じた情報照会・提供、加入者の本人確認に係る事務、その事務処理に必要な情報提供ネットワークシステムに接続する医療保険者等向け中間サーバー等（以下「中間サーバー等」という。）及び住民基本台帳ネットワークシステムに接続するためのサーバの運用・管理を支払基金に一元的に委託することが可能になった。 　当組合の加入者は、関東甲信越地方の情報通信業の①事業所の従業者である被保険者及びその被扶養者（一般加入者）、②事業所を退職するまで2ヶ月以上被保険者であった期間があり任意に継続加入を申し出た者及びその被扶養者（任意継続加入者）で、いずれも後期高齢者医療保険制度の適用年齢75歳に到達すると加入者の資格を喪失する。 ＜事務内容＞ 　当組合が行う事務のうち、番号法別表第1の項番2「健康保険法による保険給付の支給、保健事業若しくは福祉事業の実施又は保険料等の徴収に関する事務であって主務省令で定める」事務について、加入者の個人番号等の特定個人情報を以下の範囲で利用する。 なお、健康保険事務に必要な事業所からの届出書の一部について、令和2年11月から事業所が電子データにしてオンラインでマイナポータル（社会保険・税手続オンライン・ワンストップサービス）経由で申請 し、それをオンラインで当組合が受け付けすることが可能になる（※1）。 1．適用事務（加入者への保険給付や保険料徴収に当たって適用する資格関係情報等を取り扱う事務） (1)被保険者資格取得、資格喪失、被扶養者の異動等による資格の認定、資格関係情報変更の事務処理に係る個人番号の確認及び資格関係情報等の参照 (2)事業所又は加入者から個人番号が入手できない場合や個人番号又は基本4情報を確認する必要がある場合、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個人番号や基本4情報を入手（※2） (3)平成29年5月以降、情報連携のために加入者の個人番号及び資格関係情報を中間サーバー等に登録して、被保険者枝番を取得し、資格喪失や異動等の資格関係情報に変更があった場合、中間サーバー等の登録情報を更新 (4)他の医療保険者等から異動してきた被保険者や被扶養者の資格認定に当たり確認情報が必要な場合は、中間サーバー等内で従前に加入していた医療保険者等に情報照会し、資格喪失していることを確認、また、被扶養者の資格認定に必要な課税証明書や住民票等情報、給付金・還付金等の支給に利用する公的給付支給等口座情報（以下「公金受取口座情報」という。）（被保険者が希望する場合に限る。）は、情報提供ネットワークシステムを利用して当該情報保有機関に情報照会し確認（※3） (5)健康保険被保険者証の再発行や高齢受給者証等の発行・管理事務に係る対象者の確認及び資格関係情報等の参照 (6)月額変更、算定、賞与等の標準報酬に係る届出書について資格関係情報等の参照 （※1）マイナポータルは政府が運営するオンラインサービスで、マイナポータルに接続する当組合のオンラインネットワークは、従来から支払基金に接続して使用していたオンライン請求ネットワーク（以下「オンライン請求NW」という。）を利用する。なお、マイナポータルの運営主体は、申請データの中身を閲覧等できないようにシステム上制御されている。 （※2）地方公共団体情報システム機構からの個人番号入手や基本4情報入手は、支払基金経由で中間サーバー等を介して即時照会又はファイル一括照会する。 （※3）従前に加入していた医療保険者等への情報照会は被保険者枝番を用いて支払基金の中間サーバー等内で行い、情報提供ネットワークシステムを通じた当該情報保有機関への情報照会は、被保険者枝番を用いた照会データを支払基金の中間サーバー等で機関別符号を用いた照会データに変換して行う。

	2．給付事務（加入者への給付決定に係る資格関係情報等を取り扱う事務） ⑴傷病手当金、出産育児一時金、埋葬料等の給付に係る届出書に個人番号が記載されている場合の個人番号の確認及び資格関係情報等の参照 ⑵給付金の計算に係る計算条件等の情報索引 ⑶給付の決定に当たり給付要件の確認が必要な場合、情報提供ネットワークシステムを利用して他の情報保有機関に照会し確認（※4） ⑷情報連携のために、加入者の給付関係情報を中間サーバー等に登録 ⑸限度額適用認定証等の給付関係証書類や医療費のお知らせ等の発行・管理事務に係る対象者の確認及び資格関係情報等の参照 （※4）情報提供ネットワークシステムを通じた情報照会は、被保険者枝番を用いた照会データを支払基金の中間サーバー等で機関別符号を用いた照会データに変換して行う。 3．徴収事務（保険料等の徴収に係る資格関係情報等を取り扱う事務） ⑴任意継続被保険者の保険料等の計算に係る計算条件等の情報索引 ⑵任意継続被保険者の保険料徴収や未納管理、資格喪失時還付金等の保険料徴収に係る事務について資格関係情報等の参照 （付）給付金・還付金等の支給に際して、「公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律」が令和4年1月に施行され、被保険者が公金受取口座情報の利用を希望した場合に限り、情報提供ネットワークシステムを通じて情報照会を行い、口座情報登録システム（デジタル庁）から当該被保険者の公金受取口座情報を入手して振込等の事務処理に利用することが可能になった。

③対象人数	[30万人以上] <選択肢> 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	健康保険組合事務基幹システム（以下「基幹システム」という。）
②システムの機能	基幹システムは、既存の(1)適用関係機能、(2)給付関係機能、(3)徴収関係機能と新規の(4)個人番号管理機能の4つのシステム機能で構成される。 (1)適用関係機能（以下「適用システム」という。） ・加入者の資格取得、喪失、異動、個人番号その他加入者情報の審査、登録、変更、削除 ・加入者及び加入者情報の検索、参照 ・その他、健康保険被保険者証、高齢受給者証、資格喪失証明書等の資格関係証書の発行、管理 (2)給付関係機能（以下「給付システム」という。） ・給付申請の審査、登録、変更、削除 ・給付金計算 ・その他、限度額適用認定証等の給付関係証書の発行、管理、医療費のお知らせ等の作成 (3)徴収関係機能（以下「徴収システム」という。） ・月額、算定、賞与等、標準報酬に係る届の審査、登録、変更 ・保険料計算 ・保険料の徴収、収納管理 (4)個人番号管理機能（以下「個人番号管理システム」という。） ・個人番号及び被保険者枝番と既存システムで用いている識別番号（※）との紐付けテーブルの作成、変更、削除 ・個人番号の重複登録の審査 （※）「識別番号」は、既存システムで被保険者及び被扶養者を特定するために当組合で発番した一意の番号で、事業所コード、証記号番号＋枝番及び続柄コード、続柄枝番である。 （「証記号番号＋枝番」は、オンライン資格確認等の実施に対応して従来からの「証記号番号」に個人を識別する2桁の番号（枝番）を、令和2年度から付加するものである。 以下、「証記号番号＋枝番」について同じ。）
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 （ 中間サーバー等、レセプトシステム、レセプト情報管理システム、レセプト分析システム、保健システム、調査報告システム、月報システム、マイナポータル ）
システム2～5	
システム2	

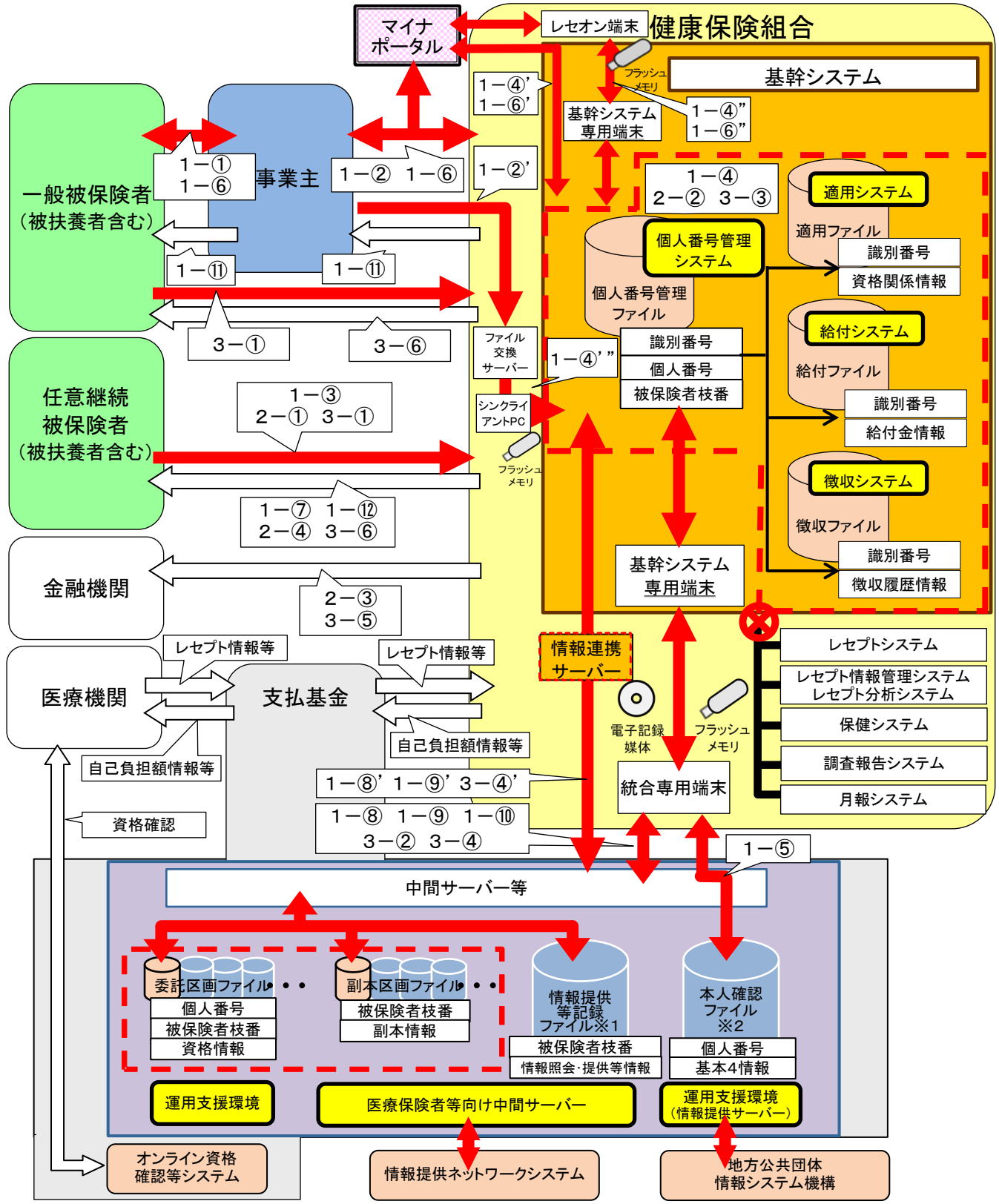
①システムの名称	中間サーバー等
②システムの機能	中間サーバー等は、医療保険者等全体又は医療保険制度横断で資格管理等を行う際に必要となるシステムであり、(1)資格履歴管理事務に係る機能、(2)情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能、(3)地方公共団体情報システム機構に対して住民基本台帳ネットワークシステムを通じて機構保存本人確認情報の提供を求める機能を有する。中間サーバー等は、医療保険情報提供等実施機関である支払基金及び国民健康保険中央会が取りまとめて運営する(以下「取りまとめ機関」という。)。 (1)資格履歴管理事務に係る機能 (ⅰ)資格履歴管理 新規加入者の基本4情報(又はその一部)、資格情報(個人番号を含む。)及び各種証情報を中間サーバー等に登録する。 (ⅱ)オンライン資格確認等システムへの資格情報の提供 個人番号を除いた資格履歴ファイルをオンライン資格確認等システムに提供する。 (2)情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能 (ⅰ)機関別符号取得 他の情報保有機関へ情報照会・提供を行う際、個人を特定するために必要となる機関別符号を取得する。 (ⅱ)情報照会 情報提供ネットワークシステムを通じて、特定個人情報の情報照会及び照会した情報の受領を行う。 (ⅲ)情報提供 情報提供ネットワークシステムを通じて、情報照会要求の受領及び当該特定個人情報の提供を行う。 (ⅳ)情報提供等記録生成 情報提供ネットワークシステムを通じて、他の情報保有機関へ情報照会・提供を行った記録を生成する。 (3)本人確認事務に係る機能 (ⅰ)個人番号取得 基本4情報(又はその一部)を基に、地方公共団体情報システム機構から本人確認情報(個人番号)を取得する。 (ⅱ)基本4情報取得 個人番号を基に、地方公共団体情報システム機構から本人確認情報(基本4情報等)を取得する。
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　(オンライン資格確認等システム、基幹システム　)
システム3	
①システムの名称	電子申請受付クライアントソフト
②システムの機能	事業所がマイナポータル経由で提出した健康保険事務に係る届出書の電子申請データを、オンライン請求NWを通じて電子申請用端末(以下「レセオン端末」という。)で受け付けし、基幹システムで審査した結果をレセオン端末からオンライン請求NWを通じてマイナポータル経由で事業所に通知するパッケージシステムで、レセオン端末上で稼動する。 (1)オンライン接続機能 オンライン請求NWを通じてマイナポータルにログイン/ログアウトする。 (2)電子申請データのダウンロード機能 マイナポータル経由で提出された事業所の電子申請データを一覧表示して確認し、基幹システムで受付・審査処理をするためにフラッシュメモリにダウンロードする。 (3)電子申請データの受付・審査結果送信機能 電子申請データの受付・審査結果を事業所に通知するため、基幹システムからフラッシュメモリに記録した情報をマイナポータル経由で送信する。 (4)申請履歴等の保存機能 電子申請データの受付及び審査結果等の履歴情報を保存、閲覧する。 ※この電子申請受付クライアントソフトは、国が開発し健保組合に提供されるものを使用する。

③他のシステムとの接続	[　] 情報提供ネットワークシステム	[　] 庁内連携システム
	[　] 住民基本台帳ネットワークシステム	[　] 既存住民基本台帳システム
	[　] 宛名システム等	[　] 税務システム
	[○] その他　（ マイナポータル	）

3. 特定個人情報ファイル名	
健康保険基幹情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	「特定個人情報ファイルを取り扱う事務」に示した事務で、基幹システムにおける加入者の資格関係情報や給付関係情報、徴収関係情報の検索・照会、情報提供ネットワークシステムを通じた情報照会・提供を正確かつ効率的に実施するため、個人番号及び被保険者枝番と既存システムで用いている識別番号を紐付けて管理する必要があることから、健康保険基幹情報ファイルを特定個人情報ファイルとして保有する。
②実現が期待されるメリット	(1)個人番号を利用することにより、加入者の資格関係情報、給付関係情報及び徴収関係情報のより正確かつ効率的な更新、検索・照会をすることが可能になり、誤った相手に対する資格関係の変更・異動や給付、保険料の賦課・徴収等を行うリスクが軽減できる。 (2)被保険者の事業所異動により既存システムで用いている識別番号の変更が行われた後も、個人番号を利用することにより異動前後の給付関係情報、徴収関係情報をより正確かつ効率的に名寄せして検索・照会することができ、情報の連続性が損なわれるリスクが軽減できる。 (3)加入者が当組合に申請届出をする際に添付することが定められている他の情報保有機関発行の書類について、中間サーバー等を通じて情報提供ネットワークシステムで情報照会することにより、書類の添付を省略することができる。
5. 個人番号の利用 ※	
法令上の根拠	・番号法　第9条第1項（利用範囲）　別表第1　項番2 　番号法別表第1の主務省令で定める事務を定める命令　第2条 ・住民基本台帳法　第30条の9（国の機関等への本人確認情報の提供）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法　第19条第8号（特定個人情報の提供の制限） （照会）別表第2　項番3 　　番号法別表第2の主務省令で定める事務及び情報を定める命令　第3条 （提供）別表第2　項番1、2、3、4、5、9、12、15、17、22、26、27、33、39、42、43、58、62、78、80、87、93、97、106、109、120 　　番号法別表第2の主務省令で定める事務及び情報を定める命令　第1条、第2条、第3条、第4条、第5条、第8条、第10条の2、第11条の2、第12条の3、第15条、第19条、第20条、第22条の2、第24条の2、第25条、第25条の2、第31条の2の2、第33条、第41条の2、第43条、第44条、第46条、第49条、第53条、第55条の2、第59条の3 （委託の根拠）健康保険法　第205条の4　第1項及び第2項 当組合は、健康保険法の規定に基づき、支払基金に情報提供ネットワークシステムを通じた情報照会・提供事務を委託する。情報提供ネットワークシステムを通じて取得した情報を保険給付の支給等の事務に活用するのは当組合であるが、情報提供ネットワークシステムに接続する主体は支払基金である。
7. 評価実施機関における担当部署	
①部署	企画部
②所属長の役職名	総務事務局長
8. 他の評価実施機関	
なし	

（別添1）事務の内容

事務全体図 （当組合は、基幹システムと中間サーバー等をサーバー間接続します。）



※1 情報提供等記録ファイルについては、当組合が基幹システム専用端末画面で参照することが可能であるが、参照できる範囲は、当組合からの委託により、支払基金が情報照会及び情報提供したものに限られる。

※2 本人確認ファイルについては、当組合が統合専用端末画面で参照することが可能であるが、参照できる範囲は、当組合からの委託により、支払基金が情報照会したものに限られる。

（備考）

※図中の「識別番号」は、既存システム内で被保険者及び被扶養者を特定するために当組合で発番した一意の番号で、
証記号番号＋枝番及び続柄コード、続柄枝番である。
※個人番号を格納する「個人番号管理ファイル」と、識別番号や被保険者枝番を連携キーとして「適用ファイル」、「給付ファイル」、
「徴収ファイル」、「委託区画ファイル」、「副本区画ファイル」が紐付くため、これらのファイルを一つの特定個人情報ファイル
（健康保険基幹情報ファイル）としている。ただし、「委託区画ファイル」及び「副本区画ファイル」においては、医療保険者等ごとに
論理的に区分された区画に情報が保存されることとなっており、各医療保険者等は自らの区画に保存された情報のみ保有する。
※図中の「個人番号管理システム」は番号制度導入に伴い開発したシステムであり、「適用システム」「給付システム」「徴収システム」
は、
個人番号管理機能開発及び情報連携に伴い改修を行ったシステムである。
※「基幹システムへの登録」とは、基幹システム専用端末を用いて各種情報を登録する行為である。また、基幹システム専用端末
は、基幹システムに情報を登録するための、インターネット閲覧やメールの送受信等ができないように制御された端末である。
※図中の「統合専用端末」とは、中間サーバー等と地方公共団体情報システム機構に接続可能な端末を統合し、どちらにも
情報照会を行うことができる端末である。
※図中の「情報連携サーバー」とは、委託区画ファイルへの資格情報の登録や更新及び副本区画ファイルへの副本情報の登録や
更新を行う際に統合専用端末を用いず中間サーバー等と基幹システムをサーバー間接続をして行うための送受信用サーバーで、
ウィルス対策ソフト及びファイアウォールでセキュリティ保護し、他の外部ネットワークシステムとは分離している。
なお、地方公共団体情報システム機構や他の情報保有機関への情報照会は統合専用端末で行い、情報連携サーバーを介した
サーバー間接続では行わない。
※図中の「レセオン端末」とは、マイナポータルにオンライン請求NWを通じて接続し、端末に搭載したダウンロードAPにより事業主
がマイナポータル経由で提出した電子申請データのダウンロード及び電子申請データの受付・審査結果を事業主宛にマイナポー
タル経由で通知する専用端末で、他のネットワークや基幹システムとは接続しない。

〈個人番号を取り扱う事務の流れ〉
1．適用事務
1－① 一般被保険者は事業主に対し、被保険者資格取得等の異動認定に関する申請を行う。
新規資格取得又は被保険者の個人番号変更届をする場合は、事業主が被保険者の個人番号及び本人確認を行う。
新規被扶養者認定又は被扶養者の個人番号変更届をする場合は、被保険者が被扶養者の個人番号及び本人確認を行い
事業主に申請する。
1－② 事業主は、個人番号を記載した被保険者資格取得や異動、月額賞与関連等の各種届出書を作成し、当組合へ紙、電子
記録媒体にて提出する。
事業主が各種届出書を電子申請データで作成した場合は、オンラインでマイナポータル経由で当組合に提出する。
1－②’事業主は、ファイル交換サービス上に各種届出等をアップロードして提出する。
1－③ 任意継続被保険者は、各種届出書を当組合へ直接提出する。
被保険者が個人番号変更届をする場合は、当組合が被保険者の個人番号及び本人確認を行う。
新規被扶養者認定又は被扶養者の個人番号変更届をする場合は、被保険者が被扶養者の個人番号及び本人確認を
行って当組合に提出する。
1－④ 当組合は、紙、電子記録媒体又はフラッシュメモリによる届出書を確認し基幹システム専用端末で基幹システムに登録す
る。
1－④’マイナポータル経由で提出された電子申請データは、オンライン請求NWを通じて基幹システム専用端末で確認し、基幹
システム専用端末で基幹システムに登録する。
1－④”レセオン端末で受け付ける場合は、オンライン請求NWを通じてレセオン端末で確認し、電子申請データをフラッシュメモ
リに一時記録して、フラッシュメモリから基幹システム専用端末で基幹システムに登録する。
1－④’”当組合は、シンクライアントPCでファイル交換サービス上の届出書をダウンロードし、ダウンロードした届出書をフラッシ
ュメモリに一時記録して、フラッシュメモリから基幹システム専用端末で基幹システムに登録する。
1－⑤ 個人番号の記載が必要な届出書に個人番号の記載がない場合や、記載された個人番号の確認又は基本4情報を確認する
必要がある場合、当組合が地方公共団体情報システム機構に照会する。
照会は、統合専用端末でオンラインにより支払基金に情報照会依頼を行い、支払基金が地方公共団体情報システム機構に
情報照会を行った結果をオンラインにより統合専用端末で確認の上、フラッシュメモリに一時保存して、基幹システム専用
端末で基幹システムに登録する。
1－⑥ 基幹システム登録の際に疑義や登録エラーが生じた事業主からの届出は、当組合から事業主に報告又は返却して訂正
を求める。訂正に当たり被保険者に確認する事項がある場合は、事業主が被保険者に確認する。
1－⑥’電子申請データが基幹システム登録の際に疑義や登録エラーが生じた場合は、当組合からオンライン請求NWを通じて
マイナポータル経由で事業主に通知する。なお、正常に登録処理が完了した電子申請データについても結果通知を
マイナポータル経由で事業主に通知する。
1－⑥”レセオン端末で行う場合は、通知を基幹システム専用端末からフラッシュメモリに一時記録してレセオン端末に読み込み
し、オンライン請求NWを通じてマイナポータル経由で事業主に通知する。
1－⑦ 基幹システム登録の際に疑義や登録エラーが生じた任意継続被保険者からの届出書は、当組合から被保険者に報告又は
返却して訂正を求める。
1－⑧ 新規資格取得や新規被扶養者認定の場合、基幹システムに登録した個人番号、基本4情報（又はその一部）及び資格情報
を基幹システム専用端末からフラッシュメモリに一時保存して、統合専用端末でオンラインにより委託区画ファイルに
登録し、被保険者枝番を取得する。取得した被保険者枝番は、統合専用端末で確認の上、フラッシュメモリに一時保存
して、基幹システム専用端末で基幹システムに登録する。
1－⑧’サーバー間接続によりこれを行う場合は、基幹システム専用端末から情報連携サーバーを介してオンラインにより
資格情報を委託区画ファイルに登録して被保険者枝番を取得し、基幹システム専用端末で基幹システムへの登録、
確認をする。
1－⑨ 新規資格取得や異動を認定した後、情報連携のために資格関係情報を基幹システム専用端末からフラッシュメモリに一時
保存して、統合専用端末でオンラインにより副本区画ファイルに登録する。
1－⑨’サーバー間接続によりこれを行う場合は、基幹システム専用端末から情報連携サーバーを介してオンラインにより

副本区画ファイルに登録する。

1－⑩ 他の医療保険者等や情報保有機関に情報照会するときは、被保険者枝番を用いた照会データを基幹システム専用端末フラッシュメモリに一時保存して、統合専用端末からオンラインで中間サーバー等に送る。他の医療保険者等から異動してきた被保険者や被扶養者の資格認定では、中間サーバー等内で従前に加入していた医療保険者等に資格喪失を照会して、結果を統合専用端末で確認する。また、被扶養者の資格認定に必要な課税証明書や住民票等情報は、中間サーバー等で被保険者枝番を機関別符号に変換した照会データを情報提供ネットワークシステムで当該情報保有機関に情報照会して、結果を統合専用端末で確認する。
1－⑪ 必要に応じて発行した健康保険被保険者証は、事業主を経由して一般被保険者に交付する。
1－⑫ 任意継続被保険者の場合は、当組合が直接被保険者に対して、健康保険被保険者証を交付する。

2. 徴収事務
2－① 任意継続被保険者の資格喪失時において、被保険者は証記号番号+枝番又は個人番号を記載した納付済保険料の還付請求書の作成を行い、当組合へ提出する。
2－② 当組合は、還付請求書に記載された証記号番号+枝番又は個人番号を確認し、基幹システムの専用端末で還付金計算を行い、基幹システムに保険料還付情報を登録する。
2－③ 当組合は金融機関に対し、被保険者への保険料還付金の振込処理を行う。（＃1）
2－④ 当組合は被保険者に対し、紙による還付保険料振込の通知を行う。

3. 給付事務
3－① 被保険者は証記号番号+枝番又は個人番号を記載した紙の給付金支給申請書の作成を行い、当組合へ提出する。なお傷病手当金又は出産手当金の場合、被保険者は事業主へ紙の給付金支給申請書を送付して出勤状況等事業主証明欄の記載を受け、事業主から被保険者に返送し、被保険者が給付金支給申請書を当組合へ提出する。
3－② 当組合は、他の情報保有機関に給付決定に必要な情報照会を行う場合、被保険者枝番を用いた照会データを基幹システム専用端末からフラッシュメモリに一時保存して統合専用端末からオンラインで中間サーバー等に送り、中間サーバー等で被保険者枝番を機関別符号に変換した照会データを情報提供ネットワークシステムで当該情報保有機関に情報照会して、結果を統合専用端末で確認する。
3－③ 当組合は、給付金支給申請書に記載された証記号番号+枝番又は個人番号を確認し、基幹システム専用端末で基幹システムに申請書情報の登録を行う。
3－④ 登録後、情報連携のために給付関係情報を基幹システム専用端末からフラッシュメモリに一時保存して、統合専用端末でオンラインにより副本区画ファイルに登録する。
3－④’サーバー間接続によりこれを行う場合は、基幹システム専用端末から情報連携サーバーを介してオンラインにより給付関係情報を副本区画ファイルに登録する。
3－⑤ 当組合は金融機関に対し、被保険者への給付金振込処理を行う。（＃1）
3－⑥ 当組合は被保険者に対し、紙による給付金支給決定通知書を送付し、給付金振込内容の通知を行う。

＃1＜給付金･還付金等の振込事務について＞
一般被保険者への給付金等は、被保険者が所属する事業所又は被保険者が届け出た金融機関等口座に振込処理を行う。
任意継続被保険者又は資格喪失者への給付金･還付金等は、被保険者が届け出た金融機関等口座に振込処理を行う。
なお、「公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律」が令和4年1月に施行され、令和4年10月以降、被保険者が公金受取口座情報の利用を希望した場合に限り、照会データをオンラインで中間サーバー等に送り情報提供ネットワークシステムで口座情報登録システム（デジタル庁）に照会して取得した当該被保険者の公金受取口座に振込処理を行う。

＜基幹システムと接続している他のシステムについて＞
※マイナポータルと基幹システムはオンライン請求NWで直接API接続し、他のネットワークとの接続はできないようシステム的に制御する。
※基幹システムと接続しているレセプトシステム、レセプト情報管理システム、レセプト分析システム、保健システム、調査報告システム、月報システム（以下「レセプトシステム等」という。）は、インターネットに接続する情報系システムから分離している。
※レセプトシステム等は識別番号を利用して適用ファイルから証記号番号+枝番等を利用するが、個人番号管理ファイルは利用しない。
※レセプトシステム等から個人番号管理ファイルは参照できないようシステム的に制御する。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
健康保険基幹情報ファイル		
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 ※		当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
	その必要性	当組合の事務を行う上で、加入者の資格や保険料の賦課・徴収、給付に関する情報を記録・管理する必要があるため。
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 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [○] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　公金受取口座情報　）
	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。 ・その他識別情報（内部番号）：既存システムの識別番号を個人番号と紐付け、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。 ・医療保険関係情報：保険料の賦課・徴収、給付に関する事務処理を行い、通知及び照会を行うために記録するもの。 ・公金受取口座情報：被保険者が希望した場合に限り情報保有機関に照会して取得し、給付金等の支給事務に用いる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28年10月3日
⑥事務担当部署		適用一課、適用二課、給付課、徴収課、審査課

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 （ ） [○] 行政機関・独立行政法人等 （ 日本年金機構、日本私立学校振興・共済事業団、デジタル庁 ） [○] 地方公共団体・地方独立行政法人 （ 市町村、後期高齢者医療広域連合 ） [○] 民間事業者 （ 加入事業所 ） [○] その他 （ 地方公共団体情報システム機構、国家公務員共済組合、国家公務員共済組合連合会、地方公務員共済組合、地方公務員災害補償基金、全国健康保険協会、国民健康保険組合、当組合以外の健康保険組合 ）
②入手方法	[○] 紙 [○] 電子記録媒体（フラッシュメモリを除く。） [○] フラッシュメモリ [ ] 電子メール [○] 専用線 [ ] 庁内連携システム [○] 情報提供ネットワークシステム [○] その他 （ 住民基本台帳ネットワークシステム、マイナポータル、ファイル交換サービス ）
③入手の時期・頻度	(1)個人番号の新規加入入手（電子申請による入手を含む。） ・資格取得する一般被保険者や資格認定するその被扶養者の個人番号は事業所からの届出書で入手する：随時 ・任意継続被保険者の資格認定する被扶養者の個人番号は被保険者からの届出書で入手する：随時 ・個人番号の記載が必要な届出書に個人番号が記載されていない場合又は記載された個人番号の確認が必要 な場合は、統合専用端末で中間サーバー等を介して支払基金経由で地方公共団体情報システム機構に即時照会又はファイル一括照会して入手する：随時 (2)個人番号変更入手（電子申請による入手を含む。） ・個人番号に誤りや番号変更が生じたとき、一般被保険者又はその被扶養者の新個人番号は事業所からの届出書で任意継続被保険者又はその被扶養者の新個人番号は被保険者からの届出書で入手する：随時 (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：随時

④入手に係る妥当性		＜個人番号の入手方法の妥当性＞ 個人番号取得の法令上の根拠は番号法第14条第1項で、次のように入手する。 【本人又は本人の代理人から個人番号の入手】 　任意継続被保険者の資格認定時の被扶養者の個人番号や、個人番号の変更が生じた任意継続被保険者又はその被扶養者の新個人番号については、被保険者本人又は本人の代理人が定められた届出書に個人番号を記載し、それを郵送又は直接当組合に届け出ることにより、当組合が入手する。 【加入事業所から個人番号の入手】 　資格取得時の一般被保険者の個人番号及び資格認定時のその被扶養者の個人番号や、個人番号の変更が生じた一般被保険者又はその被扶養者の新個人番号については、事業所が被保険者本人又は本人の代理人から提出を受けて届出書に個人番号を記載し、その書類を郵送又は当組合が指定したファイル交換サービス又は電子申請データ にしてマイナポータル経由で（※1）当組合に届け出ることにより、当組合が入手する。 　当組合が事業所から届出書を受け付けるに当たっては、定められた紙の届出書又は暗号規約等の仕様が定められた電子記録媒体及びフラッシュメモリ又は当組合が指定したファイル交換サービス又はマイナポータル経由で申請された電子申請データのいずれかで行う。 【地方公共団体情報システム機構から個人番号の入手】 　個人番号の記載が必要な届出書に個人番号が記載されていない場合又は記載された個人番号の確認が必要な場合は、統合専用端末で中間サーバー等を介して支払基金経由で地方公共団体情報システム機構に即時照会又はファイルー括照会し入手する。 （※1）厚労省の「行政手続きコスト削減のための基本計画（令和元年6月改定）において、マイナポータル等を利用した電子申請環境の構築によって電子申請環境が整っていない健保組合への電子申請 の導入を図る方針が示され、さらに、政府による社会保険・税手続きのオンライン・ワンストップ化の 推進の取り組みも踏まえ、2020年11月から開始する電子申請サービスにより事業所からマイナポータル経由で申請されたデータで当組合が入手する。 ＜個人番号の入手の時期・頻度の妥当性＞（※2） (1)新規加入入手 ・資格取得する被保険者や資格認定する被扶養者の個人番号は、その届け出があった都度、随時入手する。 ・個人番号の記載が必要な届出書に個人番号が記載されていない場合又は記載された個人番号の確認が必要な場合は、その届け出があった都度、統合専用端末で中間サーバー等を介して支払基金経由で地方公共団体情報システム機構に即時照会又はファイルー括照会により随時入手する。 (2)個人番号変更入手 ・届け出た番号の誤りの発覚や変更があった場合、新番号の届け出があった都度、随時入手する。 （※2）電子申請による入手の場合も同様に、事業所からマイナポータル経由で届け出（申請）があった都度、随時入手する。 ＜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＞ ・当組合は番号法別表第2項番3の規定に基づき、基幹システム専用端末を利用し、中間サーバー等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本人への明示		リーフレットや当組合機関誌・Web等において、個人番号の入手・利用を行う趣旨や個人番号の記載が必要な帳票の記載要領をあらかじめ明示する。 ※なお、個人番号入手の法令上の根拠は、番号法第14条第1項である。 加入者に対し、個人番号の利用について以下の内容を示している。 ・資格履歴管理事務において、支払基金に個人番号を提供し、支払基金が個人番号を管理すること。 ・情報提供ネットワークシステムを通じた情報照会・提供事務において、支払基金が機関別符号を入手、管理すること、及び支払基金が情報提供等記録を生成、管理すること。 ・本人確認事務において、支払基金に個人番号を提供すること。
⑥使用目的　※		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」に記載した、 1．加入者資格情報の更新管理、健康保険被保険者証等の発行・管理、異動・標準報酬関係届出書の資格情報確認 2．給付申請帳票の資格情報確認・審査、給付金計算及び限度額適用認定証等の発行・管理 3．保険料徴収や未納管理 の事務処理で、個人番号を既存システムの識別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。 また、資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは従前の医療保険者等に情報照会を行い、被扶養者の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は当該情報保有機関に情報照会を行い、取得した情報を被保険者枝番と紐付けた既存システムの識別番号で当該加入者の申請情報と照合・確認することに使用する。
	変更の妥当性	使用目的の変更なし

⑦使用の主体	使用部署 ※	適用一課、適用二課、給付課、徴収課、審査課
	使用者数	[　　50人以上100人未満　　]　＜選択肢＞ 1）10人未満　　2）10人以上50人未満 3）50人以上100人未満　　4）100人以上500人未満 5）500人以上1,000人未満　　6）1,000人以上
⑧使用方法 ※		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」に記載した事務処理の、 1．加入者資格情報の更新管理、健康保険被保険者証等の発行・管理、異動・標準報酬関係届出書の資格情報確認 2．給付申請帳票の資格情報確認・審査、給付金計算及び限度額適用認定証等の発行・管理の資格情報確認 3．保険料徴収の資格情報確認、保険料収納情報確認による未納管理 で、個人番号を既存システムの識別番号と紐付け、必要な情報を健康保険基幹情報ファイルから検索・参照する。 また、資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは被保険者枝番を用いた照会データで中間サーバー等内で情報照会を行い、被扶養者の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は被保険者枝番を用いた照会データを中間サーバー等で機関別符号を用いた照会データに変換し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既存システムの識別番号で当該加入者の申請情報と照合・確認する。
	情報の突合 ※	・個人番号が記載された届出書の受付・登録処理を行う際に、個人番号に紐付けされた既存システムの識別番号により基幹システムで管理している資格等の情報と突合することにより、正確な加入者の確認や業務データの審査・内容確認を行う。 ・異動により既存システムの識別番号が変更されているとき、異動前の資格情報項目と突合して同一人を名寄せし、必要な情報の履歴の参照を行う。 ・任意継続被保険者の加入処理を行う際に、それまで被保険者であった期間の資格情報項目と突合して同一人の名寄せをし、正確な審査を行うために加入期間や被扶養者などを参照・確認する。 ・資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは被保険者枝番を用いた照会データで中間サーバー等内で情報照会を行い、被扶養者の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は被保険者枝番を用いた照会データを中間サーバー等で機関別符号を用いた照会データに変換し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既存システムの識別番号で当該加入者の申請情報と照合・確認する。
	情報の統計分析 ※	特定個人情報を用いた統計分析は行わない
	権利利益に影響を与え得る決定 ※	加入者の資格決定、保険料賦課額決定、給付金決定
⑨使用開始日		平成28年10月3日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 4 ） 件
委託事項1		基幹システム導入、保守・点検、障害調査等
①委託内容		基幹システムの導入・設定作業、定期保守・点検、障害調査や復旧等の作業
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
	その妥当性	基幹システムの導入、保守、改修、障害調査等の適切な実施に当たり、専門的かつ高度な知識・技術を要するために、特定個人情報の取扱いを委託することが必要である。
③委託先における取扱者数		[10人以上50人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 当組合のサーバー内の特定個人情報ファイルを使用して基幹システムの動作・稼動確認テストを行う。 ）
⑤委託先名の確認方法		当組合への問合せ又は開示請求
⑥委託先名		公益財団法人日本生産性本部 ICT・ヘルスケア推進部
再委託	⑦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
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項2～5		
委託事項2		中間サーバー等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加入者資格の履歴管理、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、及び資格履歴情報をオンライン資格確認等システムに登録
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　※	当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
	その妥当性	当組合における資格履歴を管理するため。
③委託先における取扱者数		[　50人以上100人未満　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑤委託先名の確認方法		当組合への問合せ又は開示請求
⑥委託先名		支払基金
再委託	⑦再委託の有無　※	[　再委託する　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	委託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、再委託先への立入調査に係る要件、その他当組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	中間サーバー等の運用・保守業務
委託事項3		中間サーバー等における情報提供ネットワークシステムを通じた情報照会・提供事務
①委託内容		情報提供ネットワークシステムを使用した情報照会・情報提供、情報照会・情報提供を行うために必要となる機関別符号の取得及び管理
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　※	当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
	その妥当性	当組合と情報提供ネットワークシステムとの対応窓口を、支払基金に一本化するため。 また、当組合の機関別符号を、支払基金が一元的に取得するため。

③委託先における取扱者数		[　　50人以上100人未満　　] <選択肢> 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑤委託先名の確認方法		当組合への問合せ又は開示請求
⑥委託先名		支払基金
再委託	⑦再委託の有無　※	[　　再委託する　　] <選択肢> 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	委託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、再委託先への立入調査に係る要件、その他当組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	中間サーバー等の運用・保守業務
委託事項4		中間サーバー等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　] <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　※	当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
	その妥当性	当組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		[　　50人以上100人未満　　] <選択肢> 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [　]その他　（　）
⑤委託先名の確認方法		当組合への問合せ又は開示請求
⑥委託先名		支払基金

再委託	⑦再委託の有無 ※	＜選択肢＞ [　　再委託する　　]　　1）再委託する　2）再委託しない
	⑧再委託の許諾方法	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、再委託先への立入調査に係る要件、その他当組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	中間サーバー等の運用・保守業務
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 26 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	番号法第19条第8号 別表第2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2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2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2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	当組合の加入者である一般被保険者及び任意継続被保険者とその被扶養者で、個人番号を有する者。
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	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
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　] 庁内連携システム　　[　] 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	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	
6．特定個人情報の保管・消去	
①保管場所　※	○当組合のセキュリティ管理区域は「特定個人情報を取り扱う事務を実施する区画」である。 ○特定個人情報ファイルは外部のデータセンター内のサーバに保管し、個人番号が記載された届出書等の帳票類、電子記録媒体及びフラッシュメモリもセキュリティ管理区域内に設置した保管庫に保管する。 なお、基幹システム専用端末や基幹システムに接続していない事務用PC、個人ロッカー・事務デスク内には一切保管・留置しないよう規制している。 組合事務所及びデータセンターの建物　：警備員による立入りの監視 組合事務室及びデータセンター　：　IDカードによるセキュリティドア、職員及び常駐の委託先従業者（以下「職員等」という。）の入退室・訪問者の記録管理 組合事務所のセキュリティ管理区域　：パーティションで囲い、特定個人情報を取り扱う職員以外の者が立ち入るときは個人情報保護管理者の許可を必要とする データセンターのサーバ室　：　第三者の立入りを制限、当組合の職員の入館については事前申請とする 組合事務所の保管庫　：　IDカードによるセキュリティドア、職員等の入退室の記録管理、個人情報保護管理者による施錠管理及び入出庫の立会い・記録管理 ※電子申請された届出書データは決済処理が終了するまでの間、基幹システムに保管・管理する。 決済処理をした届出書データは基幹システム保管・管理するか、電子記録媒体に記録して媒体を上記の保管庫に保管・管理する。 ※ファイル交換サービスで届け出のあった届出書は、ダウンロードするまでファイル交換サービス内のストレージに保管される。 ＜中間サーバー等における措置＞ ①中間サーバー等の運用支援環境の設置場所は、取りまとめ機関が所有のサーバー環境（オンプレミス環境）の場合、セキュリティを確保したサーバー室に設置し、許可された者のみが入退室できる管理対象区域にて設置する。また、クラウド環境の場合、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。 ②特定個人情報は、運用支援環境（情報提供サーバー）のデータベース内に保存され、バックアップもデータベース上に保存される。

②保管期間	期間	[　　20年以上　　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	基幹システムに保存する個人番号については、当組合の「システム等運用管理規程」に規定された保存期間に基づき、資格喪失後10年間保管する。 ・電子申請された届出書データは決済処理が終了するまでの間、基幹システム又は電子記録媒体で保管･管理する。 ・ファイル交換サービスに係るファイルは、シンクライアントPC上にデータが保存されることはないが、フラッシュメモリへダウンロードするまでの期間は、ファイル交換サービス上には保存する。 ・決済処理をした届出書データ等は、当組合の「文書保存規程」及び「システム等運用管理規程」に定められた期間、基幹システム又は電子記録媒体で保管する。 ・中間サーバー等内の委託区画ファイルに保存される情報については、オンライン資格確認等システムで資格履歴を必要とする期間（10年間）、また、副本区画ファイルに保存される情報については、加入者が当組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		＜基幹システムにおける措置＞ ・基幹システム内の特定個人情報は、基幹システムの検索機能を使って資格喪失日から保管期間が経過した特定個人情報を確認し、基幹システムの消去機能を使って個人番号を完全消去する。 ・その他、基幹システム内に保管したデータファイル等は、保管期間が終了したものを定期的に基幹システムで検出し、消去機能を使って完全に消去する。 ・電子記録媒体及びフラッシュメモリにデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄する。 ※上記の消去又は廃棄を行った場合、管理簿にその記録を記載する。 ・フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去する。 ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去又は物理的に破壊した証明書類の提出で確認する。 条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を媒体管理簿に記載する。 ＜ファイル交換サービスサーバーにおける措置＞ ・ファイル交換サービス上に保存されるファイルはフラッシュメモリにダウンロード後、速やか（ダウンロード当日）に消去する。なお、消去漏れ防止のため自動削除機能を設定（10日間）し、設定期間経過後に自動消去する。 ・ファイル交換サービスからフラッシュメモリにダウンロードしたファイルは、基幹システムへの移行後、速やか（ダウンロード当日）に消去する。 ・フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去する。 ＜電子申請された届出書の措置＞ ・電子申請データをレセオン端末に取得後、レセオン端末内の電子申請データは速やかに削除する。 ・フラッシュメモリでレセオン端末と基幹システム間の電子データの授受を行ったときは、処理に使用後速やかに媒体からデータを消去する。 ・基幹システム内や電子記録媒体に保管した電子申請データは、上記＜基幹システムにおける措置＞の通り保管期間の終了後に消去又は廃棄をする。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・保管期間経過後は、中間サーバー等から適切に廃棄等を行う。 ・廃棄する電子記録媒体は、メディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。 ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去又は物理的に破壊した証明書類の提出で確認する。 条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を媒体管理簿に記載する。

7. 備考

なし

（別添2）特定個人情報ファイル記録項目

健康保険基幹情報ファイル

【適用ファイル】

＜加入者情報項目＞
証記号番号+枝番
扶養番号
識別番号
氏名
カナ氏名
性別
生年月日
加入区分（強制・任継・特退）
本支部コード
事業所コード
続柄コード
資格取得年月日
取得理由
取得受付年月日
資格喪失年月日
喪失理由
喪失受付年月日
証交付年月日−回収年月日
証有効開始年月日−終了年月日
証券面記載氏名、カナ氏名
証回収理由
所属コード
従業員番号
郵便番号
住所
電話番号
喪失予定年月日
前納区分
改定年月
改定区分
標準報酬月額
報酬月額
賞与支払額
賞与支払年月日
＜届出記録項目＞
氏名変更受付日
氏名変更年月日
氏名変更理由
産休開始受付日
産休開始年月日
産休満了予定日
産休終了受付日
産休終了年月日
育児休業開始受付年月日
育児休業開始年月日
育児休業満了予定年月日
育児休業終了受付日
育児休業終了年月日
銀行コード
支店コード
口座種別
口座番号
名義人名
＜公費項目＞
公費負担者番号
受給開始年月日−終了年月日

【徴収ファイル】

＜任意継続・特例退職保険料項目＞
識別番号
前納区分
保険料収納記録
改定年月
改定区分
標準報酬月額

【給付ファイル】

＜適用情報＞
識別番号
一部負担金割合
＜高額介護合算療養費項目＞
給付年度
自己負担額計算対象年月日(自−至)
被用者保険加入年月(自−至)
自己負担額合計
自己負担額高齢者分再掲
所得区分
＜傷病手当金支給項目＞
療養のため休んだ年月日(自−至)
療養のため休んだ日数
支給開始年月日−終了年月日
支給期間
支給額
＜埋葬料支給項目＞
死亡年月日
埋葬年月日
支給額
支給年月日
＜出産育児一時金項目＞
出産年月日
生産児数
死産児数
支給額
支給年月日
＜出産手当金支給項目＞
出産年月日
出産のため休んだ期間(自−至)
出産のため休んだ日数
支給額
支給年月日
＜家族埋葬料支給項目＞
被保険者との続柄
死亡年月日
埋葬年月日
支給額
支給年月日
＜家族出産育児一時金支給項目＞
出産年月日
生産児数
死産児数
支給額
支給年月日
＜高齢受給者証情報＞
証交付年月日−回収年月日
有効開始年月日−終了年月日
一部負担金割合
＜限度額適用認定証関連情報＞
証交付年月日−回収年月日
有効開始年月日−終了年月日
適用区分
長期入院該当年月日
＜特定疾病療養受療証情報＞
証交付年月日−回収年月日
有効開始年月日−終了年月日
認定疾病区分
自己負担限度額

【個人番号管理ファイル】

＜個人番号管理テーブル＞
個人番号
被保険者枝番
識別番号
性別
生年月日
続柄コード
＜個人番号記録＞
登録年月日
変更年月日−変更理由
変更前個人番号
削除年月日
未登録理由
＜「被保険者枝番」記録＞
登録年月日
変更年月日−変更理由
変更前「被保険者枝番」
削除年月日

【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
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

※個人番号と紐付ける
既存システムの「識別番号」
事業所コード、証記号番号+枝番、
続柄コード、従業員番号、扶養番号

※中間サーバー等に保存される「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（健康保険基幹情報ファイル）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を除く。）

1．特定個人情報ファイル名	
健康保険基幹情報ファイル	
2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・機関誌や当組合Web等で、個人番号の記載が必要な届出書の種類、様式、記載説明を明示して周知する。 ・郵送又は対面により個人番号を入手する場合は、番号法第16条（本人確認の措置）に則り本人確認書類を提出させて本人確認を行い、併せて資格情報を参照して加入者であることを確認する。 【加入事業所から個人番号を入手する場合の措置】※ ・機関誌や当組合Web等で、事業所に個人番号の記載が必要な届出書の種類、様式、記載説明を明示して周知する。 ・事業所が被保険者から個人番号の提出を受ける際、番号法第16条（本人確認の措置）に則り本人確認を実施するよう通知し、これを求める。 ・事業所から届出書を受け付けたとき、当組合で資格情報を参照して加入者であることを確認する。 ※電子申請された届出書の受け付け（入手）も上記と同様の措置をとる。また、電子申請データは、電子証明書又は法人認証基盤によって申請者（加入事業所等）の身元確認がされたデータをマイナポータルからオンライン請求NWを通じてのみ受け付ける。 【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（オンラインによる入手）】 ＜取りまとめ機関が定める当組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基幹システムに情報登録を行わず、速やかに削除する。 ・当組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。 ＜中間サーバー等における措置＞ ・当組合以外の照会要求が参照できないよう、中間サーバー等が照会要求や結果送信を制御している。
必要な情報以外を入手することを防止するための措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・機関誌や当組合Web等で、個人番号の記載が必要な届出書の種類、様式、記載説明を明示、周知し、被保険者に不必要な個人番号を記載させないようにする。 ・当組合で定めた様式以外の届出書又は必要外の記載がされている届出書は受け付けない。 ・個人番号の記載が必要ない届出書に誤って個人番号が記載されている届出書は受け付けない。 【加入事業所から個人番号を入手する場合の措置】※ ・事業所に個人番号の記載が必要な届出書の種類、様式、記載説明を通知し、被保険者に当該事務に不必要な個人番号を記載させないようにする。 ・当組合で定めた様式以外の届出書又は必要外の記載がされている届出書は受け付けない。 ・個人番号の記載が必要ない届出書に誤って個人番号が記載されている届出書は受け付けない。 ※電子申請された届出書の受け付け（入手）も上記と同様の措置をとり、届出書のデータ作成仕様に定められた以外の情報が記録されている場合はシステム的に受け付けない。なお、事業所が日本年金機構に届出作成プログラムにより作成した場合は、データに必要な情報以外が記録されることはない。 【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（オンラインによる入手）】 ＜中間サーバー等における措置＞ ・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イ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。
その他の措置の内容	なし
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・機関誌や当組合Web等に、届出書の提出は郵送又は対面により当組合に提出することを明示して周知を図り、それ以外の方法では入手を行わない。 ・郵送又は対面により個人番号を記載した届出書の受付をする際、番号法第16条（本人確認の措置）に則り本人確認書類を提出させて本人確認を行い、本人確認ができない場合は受け付けない。 【加入事業所から個人番号を入手する場合の措置】※ ・事業所が被保険者から個人番号の提出を受ける際、番号法第16条（本人確認の措置）に則り本人確認を実施するよう通知し、これを求める。 ・届出書に事業所名、届出書作成者氏名の記載を求めて、真正性を確認する。 ・事業所が電子記録媒体及びフラッシュメモリで届出書を届け出る場合、取り決めたパスワード、暗号化処置をした媒体以外は受け付けない。 ・事業所がファイル交換サービスで届出書を届け出る場合、ファイル交換サービス上に事業所がアップロードした届出書のみ受け付ける。 ※電子申請された届出書の受け付け（入手）も上記と同様の措置をとる。また、電子申請データは、電子証明書又は法人認証基盤によって申請者（加入事業所等）の身元確認がされたデータをマイナポータルからオンライン請求NWを通じてのみ受け付ける。 【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（オンラインによる入手）】 ＜中間サーバー等における措置＞ ・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。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・郵送又は対面により個人番号を記載した届出書の受付をする際、番号法第16条（本人確認の措置）に則り本人確認書類を提出させて本人確認を行う。 ・被扶養者の個人番号を届出書に記載するとき、その本人確認は被保険者が行う。 【加入事業所から個人番号を入手する場合の措置】 ・事業所が被保険者から個人番号の提出を受ける際、番号法第16条（本人確認の措置）に則り本人確認を実施するよう通知し、これを求める。
個人番号の真正性確認の措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・個人番号通知カード又は個人番号カードにより、届出書に記載された個人番号の真正性を確認する。 ・提出された届出書から個人番号を入力して、チェックデジットや既に登録されている別人の個人番号と同番号でないことを基幹システムでチェックする。 ・個人番号の真正性に疑義が生じたときは、本人に連絡をして確認するか、支払基金を介して地方公共団体情報システム機構から個人番号や本人確認情報を取得して確認する。 【加入事業所から個人番号を入手する場合の措置】※ ・事業所で個人番号を収集する際、個人番号通知カード又は個人番号カードにより真正性を確認することを通知し、これを求める。 ・事業所から届け出された届出書から個人番号を入力して、チェックデジットや既に登録されている別人の個人番号と同番号でないことを基幹システムでチェックする。 ・個人番号の真正性に疑義が生じたときは、事業所に連絡をして確認するか、支払基金を介して地方公共団体情報システム機構から個人番号や本人確認情報を取得して確認する。 ※電子申請された届出書の受け付け（入手）も上記と同様の措置をとる。

特定個人情報の正確性確保の措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・個人番号通知カード又は個人番号カードにより、届出書に記載された個人番号の正確性を確認する。 ・提出された届出書から個人番号を入力する際に、届出書と読み合わせを行い正確性を期する。 また、ダブルチェックを行って正確性を期する。 ・個人番号を入力して、チェックデジットや既に登録されている別人の個人番号と同番号でないことを基幹システムでチェックする。 ・個人番号の正確性に疑義が生じたときは、本人に連絡をして確認するか、支払基金を介して地方公共団体情報システム機構から個人番号や本人確認情報を取得して確認する。 【加入事業所から個人番号を入手する場合の措置】※ ・事業所で個人番号を届出書に記載した際、提出された個人番号と読み合わせて正確性を期することを通知し、これを求める。 ・事業所から届け出された届出書から個人番号を入力する際に、届出書と読み合わせを行い正確性を期する。 また、ダブルチェックを行って正確性を期する。 ・個人番号を入力して、チェックデジットや既に登録されている別人の個人番号と同番号でないことを基幹システムでチェックする。 ・個人番号の正確性に疑義が生じたときは、事業所に連絡をして確認するか、支払基金を介して地方公共団体情報システム機構から個人番号や本人確認情報を取得して確認する。 ※電子申請された届出書の受け付け（入手）も上記と同様の措置をとる（ただし、個人番号を手入力することはないので、上記の「届出書と読み合わせ、ダブルチェック」は除く。）。
その他の措置の内容	なし
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	【本人から個人番号を入手する場合の措置（郵送又は対面による入手）】 ・郵送による入手には書留等を用い、誤送付がないよう送付先を印字した様式を利用する。 ・特定個人情報が記載された届出書は管理簿に記載して速やかに保管庫に施錠保管する。また、届出書を使用後は文書管理規程に従って保管及び廃棄措置する。 【加入事業所から個人番号を入手する場合の措置】※ ・郵送による入手には書留等を用い、誤送付がないよう送付先を印字した様式を利用する。 ・ファイル交換サービスを利用する場合、事前に組合と共有したパスワードを使用し、ファイル交換サービス上にファイルをアップロードする。組合は共有したパスワードにて届出書をダウンロードして入手する。 ・ファイル交換サービスの通信経路は、HTTPS通信（TLS1.2）により暗号化を施しており、送受信の際、最新のパターンファイルで自動的にウイルスチェックを実施する。 ・事業所から届けられた届出書及び電子記録媒体及びフラッシュメモリは送付伝票と内容・数量を照合確認した上で、受領管理簿を起票する。 ・特定個人情報が記載された届出書は管理簿に記載して速やかに保管庫に施錠保管する。また、届出書を使用後は文書管理規程に従って保管及び廃棄措置をする。 ・電子記録媒体及びフラッシュメモリによる入手は、暗号規約や標準フォーマット等が定められた仕様に基づきパスワード設定、暗号化を行い、書留等を用いて搬送する。 ・事業所から入手した電子記録媒体及びフラッシュメモリは媒体管理簿に記載し、速やかに保管庫に施錠保管する。 ・電子記録媒体及びフラッシュメモリに記録されたデータは、事前にウイルスチェックを行い、読み込んだ件数を事業所に書類で知らせて相違ないか確認する。 ・保管する必要がない使用済の電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を管理簿に記載する。 ※電子申請された届出書の受け付け（入手） 事業所は、TSL/SSLによる暗号化でセキュリティを確保した届出データをマイナポータル経由で申請 することとする。 当組合が、マイナポータル経由でオンライン請求NWにより届出データを受け付けし基幹システムに登録する処理等は、権限を付与された必要最小限の職員等だけが行えるようシステム的に制御する。 なお、オンライン請求NWはIP-VPNによる閉鎖された通信回線で、通信内容の秘匿や盗聴防止の対応がされている。 【入手した情報の登録･確認をする基幹システム専用端末】 ・基幹システムの専用端末にはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく。 ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについて、操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・基幹システムの専用端末はインターネット等外部ネットワークと隔離する。 ・特定個人情報にアクセスする権限が与えられていない職員等が基幹システムの専用端末を使用する場合、特定個人情報へのアクセスができないようシステム的に制御する。 【電子申請された届出書を受け付けるマイナポータル連携サーバー及びレセオン端末】 ・マイナポータル連携サーバー及びレセオン端末にはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく。 ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークやシステムとは分離する。 ・マイナポータル連携サーバー及びレセオン端末は、使用権限を付与された必要最小限の職員等だけが操作できるようシステム的に制御する。 【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（オンラインによる入手）】 ＜中間サーバー等における措置＞ ・中間サーバー等と当組合の通信は、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。 【ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置】 ・シンクライアントPC端末にはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく。 ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについて、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・特定個人情報にアクセスする権限が与えられていない職員等がシンクライアントPC端末を使用する場合、特定個人情報へのアクセスができないようシステム的に制御する。

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

特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置
特定個人情報の入手における帳票の取扱いや確認・判断の誤り、基幹システム及び中間サーバー等、電子申請データ受付処理の利用・操作の誤り等によるリスクを防ぐため、必要な法令・省令、業務フロー、基幹システム及び中間サーバー等、電子申請データ受付処理の利用・操作等の教育・訓練を適宜実施する。 電子申請された届出書の受け付け（入手）においては、健保連が管理する当組合に付与されたアカウントでマイナポータルにログインすることで、当組合宛に申請されたデータのみマイナポータルから入手できるよう制御されている。

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・基幹システムは、識別番号と個人番号を紐付けて管理し参照が可能であるが、個人番号を用いない事務処理においては、個人番号にアクセスできないようシステム的に制御する。 ・特定個人情報ファイルを取り扱う事務に記載した事務においても、ログイン時には個人番号のアクセスや個人番号の入力、参照、表示などの紐付け機能を遮断した状態に設定されていて、必要がある場合のみアクセス権限がある職員等に限って設定を切り替え紐付けできるようシステム的に制御する。 ・特定個人情報にアクセス権限のない職員等がシステム操作をする場合、いかなる方法によっても個人番号にアクセスできず、個人番号の参照、表示など紐付けができないようシステム的に制御する。
事務で使用するその他のシステムにおける措置の内容	・特定個人情報ファイルを取り扱う事務に記載した事務以外は、いかなる方法によっても個人番号のアクセスや個人番号の入力、参照、表示などができないようシステム的に制御する。 ・特定個人情報にアクセス権限のない職員等がシステム操作する場合、全ての事務処理において個人番号にアクセスできず、個人番号の参照、表示等ができないようシステム的に制御する。
その他の措置の内容	なし
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	＜基幹システムにおける措置＞※ ・全てのシステム利用者に発効するユーザID及び登録されたパスワードでログイン認証を行う。 ・共有のユーザIDは使用しないこととする。 ・全てのシステム利用者に、各人が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、ユーザIDと合わせてユーザ管理簿に記載、管理する。 ・アクセス権限が付与されたシステム利用者以外は個人番号を取り扱えないようシステム管理・制御機能に設定して、システム的に制御する。 ・アクセス権限を付与するシステム利用者は最小限に限定する。 ・ユニークなパスワードの設定を徹底する。 ・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システム管理・制御機能から速やかに抹消する。 ※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のユーザー認証管理も、上記＜基幹システムにおける措置＞と同様に行う。 なお、マイナポータルにログインする当組合のユーザーIDの管理は、健保連により行われる。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・中間サーバー等を利用する職員を限定し、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と合わせてユーザ管理簿に記載、管理する。 ・共用のユーザIDの使用を禁止する。 ・パスワードに設けられた有効期間に沿って、定期的に変更を行う。 ・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。 ＜ファイル交換サービスサーバーにおける措置＞ ・ファイル交換サービスの運用担当者がサーバーへアクセスする際は、事前レビュー・承認を必要とする他、専用のGWサーバー（SecureCube/AccessCheck）上で認証し、接続制限とログの取得を実施する。 ・IPアドレス制限機能を利用して、許可された環境外からのログインを禁止する。 ※ファイル交換サービスにおいても上記＜基幹システムにおける措置＞と同様に行う。 ＜中間サーバー等における措置＞ ・統合専用端末又はサーバー間接続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等で制御している。

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
	具体的な管理方法	＜基幹システムにおける措置＞ 【アクセス権限の発効】 ・採用や異動等で適用、給付、徴収担当となる職員等には、担当となる日から有効なアクセス権限を、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能に設定し、ユーザ管理簿に記載する。 【アクセス権限の失効】 ・異動や退職等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、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能の設定を変更し、ユーザ管理簿に記載する。 ※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のアクセス権限の発効・失効管理も、上記＜基幹システムにおける措置＞と同様に行う。 なお、マイナポータルにログインする当組合のアクセス権限の発効・失効は、健保連に申請して行う。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・アクセス権限は、データ保護担当者が各職員の担当事務分野とアクセス権限を決定し、基幹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 ・採用や異動等で中間サーバー等を利用する事務を担当する職員には、担当となる日から有効なアクセス権限を、データ保護担当者の指示によりシステム担当課（IT推進課）が登録し、ユーザ管理簿に記載する。 （2)失効管理 ・異動や退職等で担当から外れる職員には、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、データ保護担当者の指示によりシステム担当課（IT推進課）が登録を変更し、ユーザ管理簿に記載する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ 【アクセス権限の発効】 ・採用や異動等で適用、給付、徴収担当となる職員等には、担当となる日から有効なアクセス権限を、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能に設定し、ユーザ管理簿に記載する。 【アクセス権限の失効】 ・異動や退職等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、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能の設定を変更し、ユーザ管理簿に記載する。 ・ファイル交換サービスにおいて自動ロック機能を利用して、使わなくなったアカウントを失効する。 ＜中間サーバー等における措置＞ 当組合のデータ保護担当者が統合専用端末において以下の管理を行う。 ・IDは、ID付与権限をもったデータ保護担当者用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データ保護担当者用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データ保護担当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。 ・指定日からユーザIDを有効にしたり、指定日からユーザIDを無効とするよう中間サーバー側で制御している。 ・パスワードを定期的に更新するよう中間サーバー側で制御している。 ・パスワードの最長有効期限を定めている。
アクセス権限の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
		＜基幹システムにおける措置＞※ ・ユーザID、アクセス権限の発効や更新は、システム担当課（IT推進課）以外は行えないものとする。 ・システム担当課（IT推進課）はユーザIDやアクセス権限の発効や更新を行う都度、データ保護担当者の確認を得てユーザ管理簿に更新記録を記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、ユーザ管理簿の点検・見直しを行う。

	具体的な管理方法	・ユニークなパスワードの設定を徹底する。 ※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のアクセス権限の管理も、上記＜基幹システムにおける措置＞と同様に行う。 なお、マイナポータルにログインする当組合のパスワードは、設けられた有効期間に沿って定期的に変更を行う。 ・事務の目的を超えて公金受取口座情報等が利用できないように、公金受取口座情報等に不必要な情報が紐付かないようにシステムで制御されている。 ＜取りまとめ機関が定める当組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、システム担当課（IT推進課）以外は行えないものとする。 ・システム担当課（IT推進課）は、ユーザIDやアクセス権限の登録や変更を行う都度、データ保護担当者の確認を得てユーザ管理簿に記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、ユーザ管理簿の点検・見直しを行う。 ・パスワードに設けられた有効期間に沿って、定期的に変更を行う。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ユーザID、アクセス権限の発効や更新は、システム担当課（IT推進課）以外は行えないものとする。 ・システム担当課（IT推進課）はユーザIDやアクセス権限の発効や更新を行う都度、データ保護担当者の確認を得てユーザ管理簿に更新記録を記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、ユーザ管理簿の点検・見直しを行う。 ・ユニークなパスワードの設定を徹底する。 ＜中間サーバー等における措置＞ ・該当する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等で制御している。

特定個人情報の使用の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	＜基幹システムにおける措置＞※ ・個人番号の登録や更新、情報検索、個人番号を含むデータ表示機能等の使用及び特定個人情報ファイルへのアクセス等について、操作ログを自動的に記録する。 ・操作ログには、処理年月日、時間、操作者等を記録する。 ・操作ログは一定期間保管し、不正アクセスや事故が疑われるときに点検し追跡できるようにする。 ・データ保護担当者は、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を確認し、不正な運用が行われていないかを点検する。 ※電子申請された届出書を受け付けし基幹システムに登録処理等を行う操作ログの記録も、上記＜基幹システムにおける措置＞と同様に行う。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・中間サーバー等の使用について、データ保護担当者は、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を確認し、不正な運用が行われていないかを点検する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・操作ログを確認し、不正操作の痕跡を1ヶ月ごとに確認する。 ・特定個人情報ファイルへのアクセス等について、操作ログを自動的に記録する。 ・操作ログには、処理年月日、時間、操作者等を記録する。 ・操作ログは一定期間保管し、不正アクセスや事故が疑われるときに点検し追跡できるようにする。 ・データ保護担当者は、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を確認し、不正な運用が行われていないかを点検する。 ＜中間サーバー等における措置＞ ・特定個人情報ファイルを扱う統合専用端末又はサーバー間接続の操作履歴（操作ログ）を中間サーバー等で記録している。
その他の措置の内容		なし
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク3： 従業者が事務外で使用するリスク		
リスクに対する措置の内容		＜基幹システムにおける措置＞ ・アクセス権限がある職員等でも、Ｉ基本情報「1．特定個人情報ファイルを取り扱う事務」に記載した事務以外では個人番号や特定個人情報ファイルにアクセスできないようシステム的に制御する。 ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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。 ・職員等に対して、特定個人情報の適切な取扱いを理解させることを目的として定期的に教育、研修を行う。 ＜電子申請された届出書の受け付けにおける措置＞ ・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与された必要最小限の職員等に限定し、アクセス権限が付与された職員等でも限定された端末以外からは電子申請データにアクセスできないようシステム的に制御する。 ・電子申請データをフラッシュメモリに一時的に複写するときは、アクセス権限を付与された職員等が事前に管理者の承認を得て、システム管理責任者がパスワード設定した媒体の使用を管理簿に記載して行い、処理に使用後速やかに媒体からデータを完全に消去して返却し、責任者はそれを確認する。 ・電子申請データをレセオン端末に取得後、レセオン端末内の電子データは速やかに削除する。 ・管理簿とログの突合等、定期的な操作ログのチェックや、職員等に対する教育、研修は上記＜基幹システムにおける措置＞と同様に行う。

	＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・アクセス権限がある職員等でも、Ⅰ基本情報「1．特定個人情報ファイルを取り扱う事務」に記載した事務以外では個人番号や特定個人情報ファイルにアクセスできないようシステム的に制御する。 ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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。 ・職員等に対して、特定個人情報の適切な取扱いを理解させることを目的として定期的に教育、研修を行う。 ＜中間サーバー等における措置＞ ・統合専用端末又はサーバー間接続を利用した情報照会依頼時等において、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等で制御している。
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4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	＜基幹システムにおける措置＞※ ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体又はフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・バックアップファイルは暗号化し、データセンター内のサーバにて管理する。 ・電子記録媒体又はフラッシュメモリに複製を行う場合は、不必要な複製を制限するため事前に管理者の承認を得て、利用記録等を媒体管理簿に記載する。処理に使用後フラッシュメモリからは速やかにデータを完全消去し、返却された電子記録媒体又はフラッシュメモリを管理者が確認して、保管庫に施錠保管する。 ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去した又は物理的に破壊した証明書類の提出で処置を確認する。 条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を管理簿に記載する。 ・廃棄する電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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出しが行われていないか監視する。 ※ファイル交換サービスにおいても上記＜基幹システムにおける措置＞と同様に行う。 ＜電子申請された届出書の受け付けにおける措置＞ ・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与された必要最小限の職員等に限定し、アクセス権限が付与された職員等でも限定された端末以外からは電子申請データにアクセスできないようシステム的に制御する。 ・電子申請データをフラッシュメモリに複写するときは、アクセス権限を付与された職員等が事前に管理者の承認を得て、システム管理責任者がパスワード設定した媒体の使用を管理簿に記載して行い、処理に使用後速やかに媒体からデータを完全に消去して返却し、責任者はそれを確認する。 ・電子申請データをレセオン端末に取得後、レセオン端末内の電子データは速やかに削除する。 ・管理簿とログの突合等、定期的な操作ログのチェックや、職員等に対する教育、研修は上記＜基幹システムにおける措置＞と同様に行う。 ＜取りまとめ機関が定める当組合の運用における措置＞ 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。 ・中間サーバー等を利用して複製等のファイル操作が可能な職員を最小限に限定する。 ・電子記録媒体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データ保護担当者の承認を得る。 ・加入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出しが行われていないか監視する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。 ・電子記録媒体又はフラッシュメモリに複製を行う場合は、不必要な複製を制限するため事前に管理者の承認を得て、利用記録等を媒体管理簿に記載する。処理に使用後フラッシュメモリからは速やかにデータを完全消去し、返却された電子記録媒体又はフラッシュメモリを管理者が確認して、保管庫に施錠保管する。 ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去した又は物理的に破壊した証明書類の提出で処置を確認する。

	条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を管理簿に記載する。 ・廃棄する電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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出しが行われていないか監視する。 ＜中間サーバー等における措置＞ ・情報提供等記録ファイルについては、統合専用端末を利用して職員が情報提供等記録をファイル出力（ダウンロード）※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。 なお、基幹システム専用端末を利用して当組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）することはできない。 ・委託区画ファイル及び副本区画ファイルについては、統合専用端末を利用して職員がファイル出力（ダウンロード）※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。 なお、基幹システム専用端末を利用して当組合の職員が副本区画のファイル出力（ダウンロード）することはできない。また、基幹システム専用端末を利用して当組合の職員が委託区画のファイル出力 （ダウンロード）をする際は、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。 ※統合専用端末にファイル出力（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基幹システムに取り込むために必要となる。
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	
なし	

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		・プライバシーマーク、ISMS、ISO9000等の認証取得をしている等、情報保護管理について十分な体制である委託先を選定する。 ・委託を行う前に委託先を訪問し、セキュリティ設備、作業環境等を確認する。 ・委託先の管理体制、担当者名簿とセキュリティ教育・研修受講歴等の提示を求める。
特定個人情報ファイルの閲覧者・更新者の制限		[　　制限している　　]　＜選択肢＞ 1）制限している　　2）制限していない
	具体的な制限方法	＜当組合事務所に来て行う委託業務における措置＞ ・基幹システムの保守・点検等の作業で稼動確認テストを行う場合は、あらかじめ作業内容と使用する特定個人情報ファイルの連絡を受け、必要に応じて当組合職員を立ち会わせる。 ＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ ・担当する従業者を必要最小限に限定し、取扱い範囲やアクセス権限等を明確にした担当者名簿の提出を受けて確認し、必要に応じて変更指示をして制限する。 ・隔離された作業場所、保管場所の限定を求める。 ・業務委託契約で、特定個人情報ファイルの閲覧・更新の範囲制限を明記する。 ＜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等で制御している。 ・運用管理要領等にアクセス権限と事務の対応表を規定し、職員と臨時職員、取りまとめ機関と委託事業者の所属の別等により、実施できる事務の範囲を限定している。また、対応表は随時見直しを行う。 ・パスワードの最長有効期間を定め、定期的に更新を実施する。
特定個人情報ファイルの取扱いの記録		[　　記録を残している　　]　＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	＜当組合事務所に来て行う委託業務における措置＞ ・基幹システムの保守・点検等の作業で稼動確認テストを行う場合は、当組合に事前に連絡し、作業内容の記録、報告を行わせ一定期間保管する。 ＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ 次の記録を一定期間保管することを義務付け、不正な取扱いがされていないことを定期又は不定期に調査すること、また必要によって記録の提出や当組合が立入調査することを契約条件とする。 ・提供した書類や電子記録媒体及びフラッシュメモリの授受及び保管記録。 ・操作ログ及び作業内容記録。 ・消去又は廃棄の記録とその証明書類。 ＜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等で記録している。 ・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。
特定個人情報の提供ルール		[　　定めている　　]　＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ 契約書や誓約書で、委託先から再委託や他者への提供は行わないルールにしている。 ルールの遵守については、次の方法で確認を行う。 ・業務担当者ごとの業務実施量等の記録を定期的に提出させ、他者や外部に提供・委託していないことを確認する。 ・委託契約に定める調査権に基づき、立入調査や報告を求める。 ＜取りまとめ機関で行う委託業務における措置＞ ・契約書において当組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。

	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ ・基幹システムの保守・点検等作業に係る業務契約書に、特定個人情報ファイルの提供・使用について、安全管理や使用の記録作成等の義務を定め、当組合に随時報告又は必要に応じて当組合が立入調査する。 ＜取りまとめ機関で行う委託業務における措置＞ ・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。
特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ ・基幹システムの保守・点検等作業の稼動確認テストでは特定個人情報ファイルを使用するだけで、原則として特定個人情報の消去を委託先では行なわせない。 ・特別に当組合の職員が文章等で指示又は依頼して消去する場合は、職員が消去の結果を確認する。 ＜取りまとめ機関で行う委託業務における措置＞ ・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、当組合が適切に廃棄等を行う。 ・機構保存本人確認情報については、当組合から取りまとめ機関に電子記録媒体を渡した場合は、取りまとめ機関が当組合に機構保存本人確認情報を提供する際に電子記録媒体を返却する。当組合に返却できない場合は、一定期間保管した上で、取りまとめ機関が物理的破壊を行う。
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		[　　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	・秘密保持義務。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・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、複写・複製の禁止。 ・再委託の禁止。 ・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元への速やかな報告と委託先の責任。 ・委託契約終了後の特定個人情報の返却又は消去。 ・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。 ・契約内容の遵守状況について報告の義務付け　　等。
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　　4）再委託していない
	具体的な方法	再委託契約に次の事項を盛り込むこととし、委託先による再委託先に対する必要かつ適切な監督のもと再委託先において安全管理措置が講じられていることを確認する。再委託先が更に委託する場合においても同様に取り扱うものとする。 ・秘密保持義務。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・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、複写・複製の禁止。 ・再委託の禁止。 ・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元への速やかな報告と委託先の責任。 ・委託契約終了後の特定個人情報の返却又は消去。 ・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。 ・契約内容の遵守状況について報告の義務付け　　等。
その他の措置の内容		なし
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
＜ファイル交換サービスにおける措置＞ ファイル交換サービスサーバー上のファイルは暗号化されて保存されるため、ファイル交換サービスを提供する事業者は、ファイル交換サービスサーバー上の情報を取り扱わず、閲覧することができない仕様になっている

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[○] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[ ] ＜選択肢＞ 1）記録を残している 2）記録を残していない
具体的な方法	
特定個人情報の提供・移転に関するルール	[ ] ＜選択肢＞ 1）定めている 2）定めていない
ルールの内容及びルール遵守の確認方法	
その他の措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	

6. 情報提供ネットワークシステムとの接続	[　] 接続しない（入手）　[　] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	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。 ＜中間サーバー等における措置＞ ①統合専用端末又は基幹システム専用端末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用照合リスト（※）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②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）を中間サーバー等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。 （※）番号法別表第2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をリスト化したもの。 ＜公金受取口座情報の入手に関する基幹システムにおける措置＞ ①本人が給付金の請求をする申請書の受取口座情報を記載する欄に、登録されている公金受取口座情報の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みとすることにより、目的外の公金受取口座情報の入手を防止する。 ②チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みについては、書類の記載内容を健保業務システムに登録した際の職員のチェック並びに事務所管課の上長の決裁時のチェックを行うと共に、健保業務四システムに、口座の利用希望があった加入者のみの情報照会を行う仕組みを構築する。 ③加入者が誤った認識で申請し、本意ではない情報連携を行うことを防ぐため、公金受取口座制度の趣旨や事務での利用方法を当組合ホームページ並びに申請書様式へ記載する。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	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。 ＜中間サーバー等における措置＞ ①中間サーバー等は、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中間サーバー等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中間サーバー等と医療保険者等の通信は、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。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	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。 ＜中間サーバー等における措置＞ ・中間サーバー等は、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。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	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。 ＜中間サーバー等における措置＞ ①中間サーバー等は、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医療保険者等の基幹システムからの接続に対し認証を行い、許可されていない基幹システムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④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）を中間サーバー等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。 ⑤中間サーバー等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中間サーバー等と医療保険者等の通信は、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。 ※中間サーバー等は、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。
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	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。 ＜中間サーバー等における措置＞ ①情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバー等にも格納して、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④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）を中間サーバー等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。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	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。 ＜中間サーバー等における措置＞ 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）を中間サーバー等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中間サーバー等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中間サーバー等と医療保険者等の通信は、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。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	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。 ＜中間サーバー等における措置＞ 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基幹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。
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

＜統合専用端末と基幹システムとの間の情報授受に係るリスク対策＞
・統合専用端末と基幹システムとの間の情報授受に係る業務を行う職員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システム的に制御する。
・情報授受で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データ保護担当者の承認を得る。
・情報授受に用いるフラッシュメモリが使用できる基幹システムの専用端末を限定し、それ以外の基幹システムの専用端末では使用できないようシステム的に制御する。
・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の媒体とし、データ保護担当者がパスワード設定した媒体以外は基幹システム専用端末及び統合専用端末で使用できないようシステム的に制御する。
・基幹システム専用端末及び統合専用端末の操作ログを記録し、データ保護担当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、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等以外とは接続せず、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全て削除する。
・フラッシュメモリに一時的に保存した個人情報は使用の都度、速やかにデータを消去し、責任者はそれを確認する。
・フラッシュメモリの利用記録等は管理簿に記載し、保管庫に施錠保管する。

＜サーバー間接続に係る情報連携サーバーと基幹システムとの情報授受に係るリスク対策＞
・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システム的に制御する。
・情報授受の操作を行う基幹システム専用端末を限定し、それ以外の専用端末は使用できないようシステム的に制御する。
・情報連携サーバーは中間サーバー等及び基幹システム以外とは接続せず、他のネットワークやシステムと分離する。
・情報連携サーバーにファイアウォールを設置して不正アクセスを防止し、ウイルス対策ソフトの導入及びパターンファイルの随時更新を行ってデータを保護する。
・情報連携サーバーを使用した操作ログを記録し、システム管理責任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、チェックする。
・情報連携サーバーには一時的に情報を格納するだけで、情報授受が終了した時点でシステムで自動的に消去する。
・情報連携サーバーの運用・保守事業者は個人番号を内容に含む電子申請データを取り扱わない契約とし、情報連携サーバーの運用・保守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。
・データセンターに設置された基幹システム（サーバ）と基幹システム専用端末間の通信は、IP－VPNによる閉域サービスを使用することで、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。
・基幹システム（サーバ）と情報連携サーバー間の通信は、IP－VPNによる閉域サービスを使用することで、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。
・情報連携サーバーと中間サーバー間の通信は、IP－VPNによる閉域サービスを使用することで、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。

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。
＜中間サーバー等における措置＞
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）を中間サーバー等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等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中間サーバー等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。
④中間サーバー等と医療保険者等の通信は、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中間サーバー等では、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、中間サーバー等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安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜セキュリティ管理区域（特定個人情報を取り扱う事務を実施する区画）における措置＞ ・IDカードによる立入の制限、入退室記録管理 ・カメラ、携帯電話等の記録媒体の持ち込みの禁止 ・消火設備、煙感知器等の設置 ・基幹システムの専用端末をインターネット等外部ネットワークと隔離等 ・基幹システムが特定個人情報を取り扱うサーバは日本国内に設置等により、リスクを回避する。 ＜データセンターのサーバ室における措置＞ ・IDカードによる立入の制限、入退室記録管理 ・無停電電源装置（UPS）の付設等により、リスクを回避する。 ＜組合事務所の保管庫における措置＞ ・IDカードによる立入の制限、入退室記録管理等により、リスクを回避する。 ＜ファイル交換サービスサーバーの措置の内容＞ ・ファイル交換サービスサーバ上の特定個人情報は、AESで暗号化して保存される。 ・利用するファイル交換サービスは、クラウドサービスプロバイダとしてのクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」及びクラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」、政府情報システムのためのセキュリティ評価制度（ISMAP）の認証を取得している。 ・敷地内には赤外線監視カメラを設置し、24時間有人監視を実施し、不正入館を防ぐ ・入館時には顔写真付身分証明書による本人確認に加え、マントラップゲートを設置し、共連れを防ぐ ・各エリア毎に設けられた生体認証装置により、アクセス範囲を制御している ・本番データが入った媒体のデータセンターからの持ち出しは原則禁止しており、必要がある場合には事前許可・確認が必須となる ・出口ではX線検査装置に加え、3Dホログラフィックボディスキャナーを設けており、機器・媒体の持ち出しを監視している。 ＜中間サーバー等における措置＞ ・運用支援環境は、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。 ・クラウド環境にアクセスできる運用・保守拠点では、電子錠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、監視カメラ等による入退室及び室内映像の収集ができ、入退室の記録を取得可能とする。 ＜サーバー間接続に係る情報連携サーバーと基幹システムとの情報授受に係るリスク対策＞ ・データセンターに設置された基幹システム（サーバー）と基幹システム専用端末間の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗難防止の対応をしている。 ・基幹システム（サーバー）と情報連携サーバー間の通信は、IP-VPNによる閉域サービスを使用することで、データ転送時の通信内容秘匿、盗難防止の対応をしている。 ・情報連携サーバーと中間サーバー間の通信は、IP-VPNによる閉域サービスを使用することで、データ転送時の通信内容秘匿、盗難防止の対応をしている。	
⑥技術的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない

	具体的な対策の内容	＜基幹システムにおける措置＞ ・不正アクセス防止のため、ファイアウォールの設置 ・ウイルス対策ソフトの導入、パターンファイルの随時更新 ・オペレーティングシステム等のパッチの随時適用 ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・フラッシュメモリは暗号化機能付きフラッシュメモリを使用。 ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御 ・情報連携サーバーには一時的に情報を格納し、情報授受が終了した時点でシステムで自動的に消去 ・基幹システム専用端末は、他の情報系端末等に兼用しない ・サーバ及び基幹システム専用端末をインターネット等外部ネットワークに接続できないよう分離等 ・基幹システムで保管している「個人番号管理ファイル」は、暗号化処理を行い、情報漏えい等の防止の措置を講じる ・データセンターとの情報授受において、通信内容の秘匿、盗聴防止の措置を講じた回線を利用等により、リスクを回避する。 ＜電子申請された届出書の受け付けにおける措置＞ ・マイナポータルに接続するオンライン請求NWは、通信内容の秘匿や盗聴防止がされたIP-VPNによる閉鎖された通信回線を使用する。 ・マイナポータル内部において、オンライン請求NWの接続先と事業主の接続先は論理的に分離されている。 ・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与 された必要最小限の職員等だけに限定したアクセス制御をし、アクセス権限が付与された職員等 でも限定された端末以外からは電子申請データにアクセスできないようシステム的に制御する。 ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークとは接続できないよう分離する。 ・マイナポータル連携サーバー及びレセオン端末にはファイアウォールの設定やウイルス対策ソフト を導入しパターンファイルを随時更新する。 等により、リスクを回避する。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・統合専用端末及び情報連携サーバーはインターネットに接続できないよう分離 ・統合専用端末及び情報連携サーバーは中間サーバー等以外の情報系端末等に兼用できないよう分離等により、リスクを回避する。 ＜ファイル交換サービスサーバーの措置の内容＞ ・ファイル交換サービスサーバ上の特定個人情報は、AESで暗号化して保存される。 ・利用するファイル交換サービスは、クラウドサービスプロバイダとしてのクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」及びクラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」、政府情報システムのためのセキュリティ評価制度（ISMAP）の認証を取得している。

		＜ファイル交換サービスの措置の内容＞ ・多段にファイアウォールを設置し、必要な通信以外を遮断する。 ・不正アクセスの検知時は、必要に応じた被害の拡大防止、調査、対策を実施する。 ・WAF（Web Application Firewall）を設置し、不正な攻撃パターンを検知する。検知後は必要に応じた対策を実施する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・フラッシュメモリは暗号化機能付きフラッシュメモリを使用 ＜中間サーバー等における措置＞ ①運用支援環境において保有する特定個人情報がインターネットに流出することを防止するため、中間サーバー等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運用支援環境では、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内容に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。 ④運用支援環境では、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。 ⑤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。 ⑥中間サーバー等と当組合の通信は、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。 ⑦運用支援環境とオンライン資格確認等システムとの通信は、個人番号が送信されることがないように、厚生労働省が定め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提供するようシステム的に制御されている。 ⑧オンライン資格確認等システム側から運用支援環境へはアクセスしないよう制御（情報を提供した際の処理結果電文は除く。）する。

⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容		
再発防止策の内容		
⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	死亡喪失後、保管期間内の加入者情報は、生存する加入者と同様の安全管理措置を講じて保管する。	
その他の措置の内容	なし	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	＜基幹システムにおける措置＞ ・被扶養者については年1回、現況確認により情報の更新を実施する。 ・当組合の機関誌、Webページ等で加入者や事業所に異動・変更の届出の周知を図る。 ・口座情報登録システムから入手する公金受取口座情報は次の方法で適宜更新する。なお、公金受取口座情報は、常に最新の情報連携で取得した情報のみ保管する（過去の情報連携で取得した公金受取口座情報を保管し続けることはない。）。 ＊給付金申請の際に公金受取口座情報の利用希望があった場合は、その都度情報照会をして更新する。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・加入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等の委託区画又は副本区画の情報を登録・更新する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1）定めている 2）定めていない

	手順の内容	＜基幹システムにおける措置＞ ・喪失日から保管期間が経過した加入者を定期的に基幹システムで検出し、消去機能を使って個人番号を完全消去する。 ・その他、基幹システム内に保管したデータファイル等は、保管期間が終了したものを定期的に基幹システムで検出し、消去機能を使って完全に消去する。 ・電子記録媒体及びフラッシュメモリにデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダー、フラッシュメモリを溶解廃棄にて物理的に破壊して廃棄する。 ※上記の消去又は廃棄を行った場合、管理簿にその記録を記載する。 ＜電子申請された届出書における措置＞ ・電子申請データをレセオン端末に取得後、レセオン端末内の電子申請データは速やかに削除する。 ・フラッシュメモリでレセオン端末と基幹システム間の電子データの授受を行ったときは、処理に使用後、速やかに媒体からデータを消去する。 ・基幹システム内や電子記録媒体に保管した電子申請データは、上記＜基幹システムにおける措置＞の通り保管期間の終了後に消去又は廃棄をする。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ファイル交換サービスに係るファイルは、フラッシュメモリへダウンロードするため、シンクライアントPC上にデータが保存されず、特定個人情報が消去されずいつまでも存在することはない。 ・ファイル交換サービス上に保存されるファイルは、速やかに消去する。 ・消去漏れ防止のため自動削除機能を設定する。期間は10日間設定とし、設定期間経過後に自動削除する。 ・フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去する。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・資格審査時に中間サーバー等の運用支援環境(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加入者について、中間サーバー等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。
その他の措置の内容		なし
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

【運用上のルールによる措置】
・プリンタ、FAX等の出力用紙の放置禁止の徹底
・保存期間が過ぎた特定個人情報の記載された用紙（届出書や帳票類）はシュレッダーで粉砕して廃棄
・溶解処分業者による保存満了分文書廃棄の実施（処分方法や廃棄証明書発行等の契約条件の見直しによる確実な廃棄の実施）
・書類又は電子記録媒体及びフラッシュメモリ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
・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去又は物理的に破壊した証明書類の提出で処置を確認
条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を管理簿に記載する。
・廃棄する電子記録媒体及びフラッシュメモリについて、電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載
・電子記録媒体及びフラッシュメモリ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

【ファイル交換サービスにおける措置】
・ファイル交換サービスサーバー上のファイルは暗号化されて保存されるため、ファイル交換サービスを提供する事業者は、ファイル交換サービスサーバー上の情報を取り扱わず、閲覧することができない仕様になっている。

【ファイル交換サービスサーバーの措置の内容】
・障害対策として、機器の冗長化、ネットワークの冗長化、電源の冗長化を実施している
・障害検知・復旧の措置として、24時間365日、サービスの監視、サイバー攻撃のモニタリングを実施している。
・定期的に、プラットフォーム診断（月１回）、webアプリケーション診断（年１回以上）、ペネトレーションテスト（年１回以上）を実施している。

【特定個人情報の漏えい等事案が発生した場合の対応】
「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則（平成27年特定個人情報保護委員会規則第５号）」及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（平成26年12月11日個人情報保護委員会）の（別添２）特定個人情報の漏えい等に関する報告等（事業者編）」に基づき、次の対応を行う。

(1)事業所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)事案の内容等に応じて、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。
(6)事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策について、速やかに公表する。
(7)番号法違反の事案又は番号法違反のおそれのある事案を把握した場合には、事実関係及び再発防止策等について、速やかに本告示等に基づく報告先に報告する。
ただし、重大事態に該当する事案又はそのおそれのある事案が発覚した時点で、直ちにその旨を個人情報保護委員会に報告し、その後、重大事態に該当する事案は、本規則の規定に従って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		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	・定期的に、評価書記載事項や個人情報保護管理規程に基づいて特定個人情報の取扱い及び業務運用が行われているか、チェックリストを作って各担当部署内で点検し報告する。 ・点検の結果、問題や不備が明らかになったときは、速やかに究明に当たり、是正措置をする。 ＜取りまとめ機関が定める当組合の運用における措置＞ ・当組合は、取りまとめ機関から実施要領を契機に自己点検を実施（年1回）し、実施結果を取りまとめ機関へ報告（年1回）することとしている。 ・自己点検の対象システムは、中間サーバー等、既存システム及び統合専用端末であり、医療保険者等向け中間サーバー等との接続運用に係る運用管理規程（以下「運用管理規程（医療保険者向け）」という。）の別紙「安全管理措置一覧」を使用して行う。
②監査		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な内容	＜内部監査＞ 情報セキュリティ基本方針に基づき、定期的に監査責任者が特定個人情報の取扱いや運用実態を次の観点から監査する。 ・評価書記載事項及び個人情報保護管理規程の遵守 ・特定個人情報保護に関する体制、人的安全管理措置の実施内容 ・特定個人情報保護、安全管理措置の周知、教育の実施内容 ・特定個人情報保護に関する物理的、技術的安全管理措置の実施内容 ・インシデントの発生状況、再発防止策の実施内容 ※当該点検結果に基づき、必要に応じて是正指示をする。 ＜外部監査＞ 当組合とは独立した外部法人（プライバシーマーク指定審査機関）によって特定個人情報の取扱いや運用実態の監査を受ける。 ＜取りまとめ機関が定める当組合の運用における措置＞ 当組合は、運用管理規程（医療保険者等向け）に基づき、基幹システム及び当組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。 ＜ファイル交換サービス運用事業者における措置の内容＞ ISMS及びセキュリティ格付けによる外部監査、さらに内部監査に基づき、担当者が適正に処理を行っているか確認している。 ＜監査結果の反映＞ 監査の結果、問題や不備が明らかになったときは、速やかに問題究明に当たり、是正措置をする。 また、これを次回の特定個人情報保護評価におけるリスク評価の参考とする。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜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	【当組合における教育・啓発】 ・職員等の採用・就任時に、個人情報保護管理規程及び取扱要領等の教育を行う。 ・最低毎年2回、役職員全員に特定個人情報取扱いの教育を行う。 ・教育実施後、理解度の把握や啓発を図るため、テストやレポート提出を行う。 ・事故が発生した場合、その原因、影響、再発防止策などを役職員全員に周知する。 ・QC活動などを通じて、リスク回避の方策や改善案等を職員に考えさせ提案させる。 ・適当な外部機関の教育、研修プログラムに交代で参加させる。 ・他の組合等のリスク対策やルールについて意見交換等ができる交流の機会を設ける。 ・派遣職員については、契約時の派遣先による当組合の契約における特定個人情報の取扱いの周知徹底を行い、当組合に在職中は職員と同等に上記のような教育・啓発に参加させて教育する。 【取りまとめ機関が定める当組合の教育における措置】 ・情報提供ネットワークシステム運用主体や厚生労働省、取りまとめ機関等が医療保険者等向けに実施する教育・研修・訓練等に当組合の職員を参加させる。 ・運用管理規程（医療保険者等向け）の「5.1教育」に則り、情報提供ネットワークシステム運用主体が提供する教育計画及び取りまとめ機関が提供する教育・研修資料を基に毎年教育計画を作成して実施す

		る。 ・教育実施後、受講者のQ＆A対応や理解度向上を目的としたフォローアップ対応を適宜行う。 ・受講者の意見等を踏まえた上で教育内容の改善を検討すると共に、収集した意見等の集計結果をレポートにまとめ、取りまとめ機関に提供する。 【ファイル交換サービス運用事業者における措置の内容】 研修やOJTで、機密情報の取扱やセキュリティに関する教育を行っている。 【違反行為の措置】 ・違反行為が組合内外に与える影響の重大性に応じて、戒告、減給、停職、解雇等の処分を行う。 ・違反行為による損害賠償を請求することがある。 ・これらの措置、処分について就業規則に定め、周知する。

3. その他のリスク対策

＜ファイル交換サービス運用事業者における措置の内容＞
不測事態対策委員会が常設機関として存在し、事案が発覚した際には、被害や損失を最小限にとどめ、かつ一刻も早い定常状態への復旧・回復を行うために、迅速かつ適切な対応行動がとれるようになっている。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	関東ITソフトウェア健康保険組合　企画部企画課　東京都新宿区百人町2-27-6　tel:03-5925-5307
②請求方法	当組合所定の様式による書面で、特定個人情報の開示・訂正・利用停止請求を受け付ける。 ・様式1　個人情報開示等請求書
特記事項	当組合の機関誌、Webページ等に、請求先等について掲載する。
③手数料等	[　　無料　　]　　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　行っていない　]　　＜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法令による特別の手続	なし
⑥個人情報ファイル簿への不記載等	なし

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	関東ITソフトウェア健康保険組合　企画部企画課　東京都新宿区百人町2-27-6　tel:03-5925-5307
②対応方法	・問合せ受付時に受付票を起票し、問合せ内容及び対応方法、経過等について記録を残す。 ・重要度や緊急度のランク付けを行い、対応する担当者や回答期限を設定する。 ・情報漏えい等の重大な事案に関する問い合わせは、理事長へ報告の上、対応を決定する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和6年1月29日
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	当組合Webページに掲載し、パブリックコメントによる意見聴取を実施した。
②実施日・期間	令和5年12月15日～令和6年1月14日（計31日間）
③期間を短縮する特段の理由	期間短縮はなし。
④主な意見の内容	意見なし。
⑤評価書への反映	意見なし。
3. 第三者点検	
①実施日	―
②方法	―
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	令和6年1月29日
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年6月3日	評価書全般	帳票、書類、届出書	「届出書」に用語を統一	事後	重要な変更に当たらない形式的な変更
令和1年6月3日	Ⅰ1．特定個人情報ファイルを取り扱う事務 ②事務の概要	1．適用事務 (1)平成28年9月から、資格を有する加入者の個人番号を事業所又は加入者から収集し登録する事務 (2)～(7) (※1)、(※2) 2．給付事務 3．徴収事務	初期収集に関する項番(1)を全文削除し、以下の項番を(1)～(6)に振り直した。 その他、初期収集に関連した表記の削除・修正や、事務運用の実態に合わせた文章表記の修正をした。	事後	初期収集は過去に一時的に行い既に平成28年度で終了していたものが残っていたため記述を削除し、その他の文章表記の修正
令和1年6月3日	Ⅰ6．情報提供ネットワークシステムによる情報連携 ②法令上の根拠	・番号法　第19条第7号（特定個人情報の提供の制限） （提供）別表第2　項番1、2・・・・120	・番号法　第19条第7号（特定個人情報の提供の制限） （提供）別表第2　項番1、2・・・・119	事後	番号法改正で項番が変更されただけの軽微な変更
令和1年6月3日	Ⅰ7．評価実施機関における担当部署 ②所属長	②所属長	②所属長の役職名	事後	基礎項目評価書様式の変更に伴なう項目の変更
令和1年6月3日	Ⅰ（別添1）事務の内容	（備考） 1．現存被保険者・被扶養者の個人番号の初期収集の流れ 1－①　～　1－⑨	1．及び1－①～1－⑨を全文削除し、以降の項番を1から振直し。	事後	初期収集は過去に一時的に行い既に平成28年度で終了したものが残っていたため記述を削除し、その他文章表記の修正
令和1年6月3日	Ⅱ 3．特定個人情報の入手・使用 ③入手の時期・頻度	(1)個人番号の初期収集入手 ・機関別符号一斉取得・・・・。 ・事業所又は任意継続・・・・。 (2)個人番号の新規加入入手 ・初期収集後の新規加入者・・・・。 ・初期収集後の個人番号が・・・・。	(1)の全項及び(2)のうち「初期収集」が記載されている2項目を削除し、(2)以降の項番を(1)から振直し。	事後	初期収集は過去に一時的に行い既に平成28年度で終了したものが残っていたため記述を削除し、その他文章表記の修正
令和1年6月3日	Ⅱ 3．特定個人情報の入手・使用 ④入手に係る妥当性	(1)個人番号の初期収集入手 ・現存加入者の個人番号・・・・。 ・入手できない現存加入者の・・・・。	(1)の全項目を削除し、(2)以降の項番を(1)から振直し。	事後	初期収集は過去に一時的に行い既に平成28年度で終了したものが残っていたため記述を削除し、その他文章表記の修正
令和1年6月3日	Ⅱ 4．特定個人情報ファイルの取扱いの委託 [委託事項4] ④委託先への特定個人情報ファイルの提供方法	[○]電子記録媒体（フラッシュメモリーを除く）	[　]電子記録媒体（フラッシュメモリーを除く）	事後	電子記録媒体での提供は、過去に一時的に行い既に平成28年度で終了したものが残っていたため記述を削除
令和1年6月3日	Ⅲ 2．特定個人情報の入手 リスク1，リスク2，リスク4	【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（電子記録媒体による入手）】	この項目を全文削除。	事後	電子記録媒体での提供は、過去に一時的に行い既に平成28年度で終了したものが残っていたため記述を削除
令和1年6月3日	Ⅳ 2．従業者に対する教育・啓発	【取りまとめ機関が定める当組合の運用における措置】 ・中間サーバー等の・・・・統合専用端末導入前に研修を行う。	【措置】を次の内容に変更。 ・厚労省、取りまとめ機関等が実施する教育・研修への参加 ・取りまとめ機関が提供する資料により毎年教育計画を作成、実施 ・教育実施後のフォローアップ ・受講者の意見等をまとめ、取りまとめ機関に提供	事後	統合専用端末の導入前に一時的に行った研修の記載が残っていたため削除し、取りまとめ機関が新たに定めた運用管理規程の「教育」の内容に書換え
令和2年6月23日	(全項目評価書)全般	事務内容の一部修正等	事務内容の一部修正等	事後	運用実態に合わせた修正
令和2年6月23日	Ⅰ 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] ②システムの機能	(※)「識別番号」は、既存システムで被保険者及び被扶養者を特定するために当組合で発番した一意の番号で、事業所コード、証記号番号及び続柄コード、従業員番号及び扶養番号である。	(※)「識別番号」は、既存システムで被保険者及び被扶養者を特定するために当組合で発番した一意の番号で、事業所コード、証記号番号＋枝番及び続柄コード、従業員番号及び扶養番号である。 (「証記号番号＋枝番」は、オンライン資格確認等の実施に対応して従来からの「証記号番号」に個人を識別する2桁の番号（枝番）を、令和2年度から付加するものである。以下、「証記号番号＋枝番」について同じ。）	事後	「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正のため、事後に提出

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2年6月23日	Ⅰ 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)資格履歴管理事務に係る機能 新規加入者の基本4情報（又はその一部）、資格情報（個人番号含む。）を中間サーバー等に登録する。	(1)資格履歴管理事務に係る機能 （ｉ）資格履歴管理 新規加入者の基本4情報（又はその一部）、資格情報（個人番号を含む。）及び各種証情報を中間サ ーバー等に登録する。 （ⅱ）オンライン資格確認等システムへの資格情報の提供 個人番号を除いた資格履歴ファイルをオンライン資格確認等システムに提供する。	事後	同　上
令和2年6月23日	同 ［システム2］ ③他のシステムとの接続	その他 （　　）	その他 （オンライン資格確認等システム）	事後	同　上
令和2年6月23日	Ⅰ6. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	・番号法　第19条第7号（特定個人情報の提供の制限） （提供）別表第2　項番1、2・・・・119	・番号法　第19条第7号（特定個人情報の提供の制限） （提供）別表第2　項番1、2・・・・120	事後	番号法改正で項番号が変更されただけの軽微な変更で、事後（改正後）に提出
令和2年6月23日	Ⅰ（別添1）事務の内容 個人番号を取り扱う事務の流れ図、及び （備考）事務の流れの説明		流れ図に、 医療機関と中間サーバー等の間にオンライン資格確認等システムのフローを追加 （備考）欄の、「証記号番号」を「証記号番号＋枝番」に変更	事後	「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正のため、事後に提出
令和2年6月23日	Ⅱ 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ①委託内容	個人番号を利用した加入者資格の履歴管理、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	個人番号を利用した加入者資格の履歴管理、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、及び資格履歴情報をオンライン資格確認等システムに登録	事後	同　上
令和2年6月23日	Ⅱ 6. 特定個人情報の保管・消去 ①保管場所	＜中間サーバー等における措置＞ ・中間サーバー等は、支払基金のデータセンターに設置しており、許可された者のみが入退室できる管理対象区域に設置する。	＜中間サーバー等における措置＞ ①中間サーバー等の運用支援環境の設置場所は、取りまとめ機関が所有のサーバー環境（オンプレミス環境）の場合、セキュリティを確保したサーバー室に設置し、許可された者のみが入退室できる管理対象区域にて設置する。また、クラウド環境の場合、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。 ②特定個人情報は、運用支援環境（情報提供サーバー）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。	事後	同　上
令和2年6月23日	Ⅱ（別添2）特定個人情報ファイル記録項目	＜加入者情報項目＞　証記号、証番号	＜加入者情報項目＞　証記号番号+枝番 ＜被保険者証項目＞＜高齢受給者証項目＞＜限度額適用認定証項目＞＜特定疾病療養受療証項目＞等に項目名の追加、修正	事後	同　上
令和2年6月23日	Ⅲ 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策	＜中間サーバー等における措置＞ ・中間サーバー等を支払基金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。	＜中間サーバー等における措置＞ ・運用支援環境は、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。 ・クラウド環境にアクセスできる運用・保守拠点では、電子錠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、監視カメラ等による入退室及び室内映像の収集ができ、入退室の記録を取得可能とする。	事後	同　上

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2年6月23日	Ⅲ 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策	＜中間サーバー等における措置＞ ①中間サーバー等において保有する特定個人情報がインターネットに流出することを防止するため、中間サーバー等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中間サーバー等では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中間サーバー等では、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。 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中間サーバー等と当組合の通信は、IPSec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。	＜中間サーバー等における措置＞ ①運用支援環境において保有する特定個人情報がインターネットに流出することを防止するため、中間サーバー等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運用支援環境では、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内容に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。 ④運用支援環境では、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。 ⑤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。 ⑥中間サーバー等と当組合の通信は、IPSec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。 ⑦運用支援環境とオンライン資格確認等システムとの通信は、個人番号が送信されることがないように、厚生労働省が定め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提供するようシステム的に制御されている。 ⑧オンライン資格確認等システム側から運用支援環境へはアクセスしないよう制御（情報を提供した際の処理結果電文は除く。）する。	事後	同　上
令和2年9月18日	評価書全般 （Ⅲ2.特定個人情報の入手、Ⅲ7.特定個人情報の保管・消去等）		電子申請による届出書の入手経路の追加に伴う追記等 （特定個人情報の入手やレセオン端末に関するリスク対策の追記等）	事前	重要な変更
令和3年2月3日	Ⅰ 2. 特定個人情報ファイルを取り扱う事務において使用するシステム ［システム1］ ③他のシステムとの接続	その他（ レセプトシステム、レセプト情報管理・分析システム、保健システム、調査報告システム、月報システム ）	その他（ 中間サーバー等、レセプトシステム、レセプト情報管理・分析システム、保健システム、調査報告システム、月報システム、マイナポータル ）	事前	重要な変更の対象項目ではないが、サーバー間接続開始に係る事項のため事前に変更
令和3年2月3日	Ⅰ（別添1）事務の内容 事務内容図 及び内容説明		図に、基幹システムと中間サーバー等を接続する「情報連携サーバー」を追加 （備考）欄 「情報連携サーバー」の説明を追加 適用事務、徴収事務にサーバー間接続の事務の流れを追加	事前	重要な変更の対象項目ではないが、サーバー間接続開始に係る事項のため事前に変更
令和3年2月3日	Ⅲ 2. 特定個人情報の入手 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		【入手した情報の登録･確認をする基幹システム専用端末】 に追加 『・サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。』	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	同	【電子申請された届出書を受け付けるレセオン端末】 ・レセオン端末にはファイアウォール、ウイルス対策ソフトを導入して パターンファイルを随時更新しておく。 ・レセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークやシステムとは分離する。 ・レセオン端末は、使用権限を付与された必要最小限の職員等だけが操作できるようシステム的に制御する。	【電子申請された届出書を受け付けるマイナポータル連携サーバー及びレセオン端末】 ・マイナポータル連携サーバー及びレセオン端末にはファイアウォール、ウイルス対策ソフトを導入して パターンファイルを随時更新しておく。 ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークやシステムとは分離する。 ・マイナポータル連携サーバー及びレセオン端末は、使用権限を付与された必要最小限の職員等だけが操作できるようシステム的に制御する。	事前	サーバー間接続開始のため重要な変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年2月3日	Ⅲ 3. 特定個人情報の使用 リスク2：権限のない者によって不正に使用されるリスク ユーザー認証の管理	＜中間サーバー等における措置＞ ・統合専用端末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、操作者を認証するよう中間サーバー等で制御している。	＜中間サーバー等における措置＞ ・統合専用端末又はサーバー間接続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、操作者を認証するよう中間サーバー等で制御している。	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 3. 特定個人情報の使用 リスク2：権限のない者によって不正に使用されるリスク 特定個人情報の使用の記録	＜中間サーバー等における措置＞ ・特定個人情報ファイルを扱う統合専用端末による操作履歴（操作ログ）を中間サーバー等で記録している。	＜中間サーバー等における措置＞ ・特定個人情報ファイルを扱う統合専用端末又はサーバー間接続による操作履歴（操作ログ）を中間サーバー等で記録している。	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 3. 特定個人情報の使用 リスク3：従業者が事務外で使用するリスク		＜基幹システムにおける措置＞　に追加 『・サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。』	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 3. 特定個人情報の使用 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		＜基幹システムにおける措置＞　に追加 『・サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。』	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	同	＜中間サーバー等における措置＞ ・情報提供等記録ファイルについては、統合専用端末を利用して当組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）※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、統合専用端末を利用して当組合の職員がファイル出力（ダウンロード）※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。	＜中間サーバー等における措置＞ ・情報提供等記録ファイルについては、統合専用端末を利用して当組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）※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。 　なお、基幹システム専用端末を利用して当組合の職員が情報提供等記録をファイル出力（ダウンロー）することはできない。 ・委託区画ファイル及び副本区画ファイルについては、統合専用端末を利用して当組合の職員がファイル出力（ダウンロード）※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。 　なお、基幹システム専用端末を利用して当組合の職員が副本区画のファイル出力（ダウンロード）することはできない。また、基幹システム専用端末を利用して当組合の職員が委託区画のファイル出力（ダウンロード）をする際は、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。	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		＜サーバー間接続に係る情報連携サーバーと基幹システムとの情報授受に係るリスク対策＞を追加	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策		＜サーバー間接続に係る情報連携サーバーと基幹システムとの情報授受に係るリスク対策＞を追加	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	Ⅲ 7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策		＜基幹システムにおける措置＞　に追加 『・サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御 ・情報連携サーバーには一時的に情報を格納し、情報授受が終了した時点でシステムで自動的に消去』	事前	サーバー間接続開始のため重要な変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年2月3日	同	＜電子申請された届出書の受け付けにおける措置＞ ・レセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークとは接続できないよう分離する。 ・レセオン端末にはファイアウォールの設定やウイルス対策ソフト を導入しパターンファイルを随時更新する。	＜電子申請された届出書の受け付けにおける措置＞ ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークとは接続できないよう分離する。 ・マイナポータル連携サーバー及びレセオン端末にはファイアウォールの設定やウイルス対策ソフト を導入しパターンファイルを随時更新する。	事前	サーバー間接続開始のため重要な変更
令和3年2月3日	同	＜取りまとめ機関が定める当組合の運用における措置＞ ・統合専用端末はインターネットに接続できないよう分離 ・統合専用端末は中間サーバー等以外のシステムに兼用できないよう分離 等により、リスクを回避する。	＜取りまとめ機関が定める当組合の運用における措置＞ ・統合専用端末及び情報連携サーバーはインターネットに接続できないよう分離 ・統合専用端末及び情報連携サーバーは中間サーバー等以外のシステムに兼用できないよう分離 等により、リスクを回避する。	事前	サーバー間接続開始のため重要な変更
令和4年11月1日	Ⅰ－1．特定個人情報ファイルを取り扱う事務 ②事務の内容		給付金・還付金等の支給に利用する公的給付支給等口座情報（以下「公金受取口座情報」という。）（被保険者が希望する場合に限る。）は、情報提供ネットワークシステムを利用して当該情報保有機関に情報照会し確認 （付）給付金・還付金等の支給に際して、「公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律」が令和4年1月に施行され、被保険者が公金受取口座情報の利用を希望した場合に限り、情報提供ネットワークシステムを通じて情報照会を行い、口座情報登録システム（デジタル庁）から当該被保険者の公金受取口座情報を入手して振込等の事務処理に利用することが可能になった。	事前	公金受取口座情報取得のための重要な変更
令和4年11月1日	Ⅰ－6．情報提供ネットワークシステムによる情報連携 ②法令上の根拠	（提供）番号法別表第2の主務省令で定める事務及び情報を定める命令　第31条の2	（提供）番号法別表第2の主務省令で定める事務及び情報を定める命令　第31条の2の2	事後	公金受取口座情報取得のための重要な変更
令和4年11月1日	（別添1）事務の内容		＃1＜給付金･還付金等の振込事務について＞ 一般被保険者への給付金等は、被保険者が所属する事業所又は被保険者が届け出た金融機関等口座に振込処理を行う。 任意継続又は資格喪失者への給付金･還付金等は、被保険者が届け出た金融機関等口座に振込処理を行う。 なお、「公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律」が令和4年1月に施行され、令和4年10月以降、被保険者が公金受取口座情報の利用を希望した場合に限り、照会データをオンラインで中間サーバー等に送り情報提供ネットワークシステムで口座情報登録システム（デジタル庁）に照会して取得した当該被保険者の公金受取口座に振込処理を行う。	事前	公金受取口座情報取得のための重要な変更
令和4年11月1日	Ⅱ－2．基本情報 ④記録される項目		主な記録項目｜その他（　公金受取口座情報　） その妥当性｜・公金受取口座情報：被保険者が希望した場合に限り情報保有機関に照会して取得し、給付金等の支給事務に用いるために記録するもの。	事前	同上
令和4年11月1日	Ⅱ－3．特定個人情報の入手・使用 ①入手元	行政機関・独立行政法人等（日本年金機構、日本私立学校振興・共済事業団）	行政機関・独立行政法人等（日本年金機構、日本私立学校振興・共済事業団、デジタル庁）	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年11月1日	Ⅲ−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 　アクセス権限の管理		＜基幹システムにおける措置＞※ ・事務の目的を超えて公金受取口座情報等が利用できないように、公金受取口座情報等に不必要な情報が紐付かないようにシステムで制御されている。	事前	同上
令和4年11月1日	Ⅲ−6. 情報提供ネットワークシステムとの接続 リスク1：目的以外の入手が行われるリスク		＜公金受取口座情報の入手に関する基幹システムにおける措置＞ ①本人が給付金の請求をする申請書の受取口座情報を記載する欄に、登録されている公金受取口座情報の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みとすることにより、目的外の公金受取口座情報の入手を防止する。 ②チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みについては、書類の記載内容を健保業務システムに登録した際の職員のチェック並びに事務所管課の上長の決裁時のチェックを行うと共に、健保業務四システムに、口座の利用希望があった加入者のみの情報照会を行う仕組みを構築する。 ③加入者が誤った認識で申請し、本意ではない情報連携を行うことを防ぐため、公金受取口座制度の趣旨や事務での利用方法を当組合ホームページ並びに申請書様式へ記載する。	事前	同上
令和4年11月1日	Ⅲ−7. 特定個人情報の保管・消去 リスク1：特定個人情報の漏えい・滅失・毀損リスク 　⑥技術的対策		＜基幹システムにおける措置＞ ・基幹システムで保管している「個人番号管理ファイル」は、暗号化処理を行い、情報漏えい等の防止の措置を講じる	事後	当初より暗号化処理を行っていたが、技術的対策に記載していなかったため、事後追加
令和4年11月1日	Ⅲ−7. 特定個人情報の保管・消去 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		・口座情報登録システムから入手する公金受取口座情報は次の方法で適宜更新する。なお、公金受取口座情報は、常に最新の情報連携で取得した情報のみ保管する（過去の情報連携で取得した公金受取口座情報を保管し続けることはない。）。 　＊給付金申請の際に公金受取口座情報の利用希望があった場合は、その都度情報照会をして更新する。	事前	
令和4年11月1日	Ⅰ−6. 情報提供ネットワークシステムによる情報連携 　②法令上の根拠	・番号法　第19条第7号（特定個人情報の提供の制限）	・番号法　第19条第8号（特定個人情報の提供の制限）	事後	番号法改正（令和3年9月1日施行）により号番号を事後に変更
令和4年11月1日	Ⅱ−5. 特定個人情報の提供・移転（委託に伴うものを除く。） 　提供先1 　①法令上の根拠 　②提供先における用途 　③提供する情報	番号法第19条第7号	番号法第19条第8号	事後	番号法改正（令和3年9月1日施行）により号番号を事後に変更
令和4年11月1日	Ⅲ−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	【特定個人情報の漏えい事案等が発生した場合の対応】 「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則（平成27年特定個人情報保護委員会規則第5号）」及び「事業者における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（平成27年特定個人情報保護委員会告示第2号）」に基づき、次の対応を行う。	【特定個人情報の漏えい等事案が発生した場合の対応】 「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則（平成27年特定個人情報保護委員会規則第5号）」及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（平成26年12月11日個人情報保護委員会）の（別添2）特定個人情報の漏えい等に関する報告等（事業者編）」に基づき、次の対応を行う。	事後	「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の改正（令和4年4月1日施行）により、資料名等を変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年11月1日	Ⅲ−3. 特定個人情報の使用 リスク4	・電子記録媒体及びフラッシュメモリの利用記録等は媒体管理簿に記載し、保管庫に施錠保管する。	・電子記録媒体又はフラッシュメモリに複製を行う場合は、不必要な複製を制限するため事前に管理者の承認を得て、利用記録等を媒体管理簿に記載する。処理に使用後フラッシュメモリからは速やかにデータを完全消去し、返却された電子記録媒体又はフラッシュメモリを管理者が確認して、保管庫に施錠保管する。	事後	
令和4年11月1日	Ⅲ−2. 特定個人情報の入手 リスク4	・特定個人情報が記載された届出書は速やかに保管庫に施錠保管する。	・特定個人情報が記載された届出書は管理簿に記載して速やかに保管庫に施錠保管する。	事後	
令和4年11月1日	Ⅲ−7. 特定個人情報の保管・消去 リスク1ー⑤		・基幹システムが特定個人情報を取り扱うサーバは日本国内に設置	事後	
令和4年11月1日	Ⅲ−7. 特定個人情報の保管・消去 リスク1ー⑥		・基幹システムで保管している「個人番号管理ファイル」は、暗号化処理を行い、情報漏えい等の防止の措置を講じる	事後	
令和4年11月1日	(別添2)特定個人情報ファイル記録項目 ＜届出記録項目＞		銀行コード 支店コード 口座種別 口座番号 名義人名	事前	
令和6年3月1日	Ⅰ (別添1)事務の内容 事務の流れ図		事業主と健康保険組合の間にファイル交換サーバーとシンクライアントPCのフローを追加	事前	マイナンバーの収集方法を新たに追加
令和6年3月1日	(別添1)事務の内容 ＜個人番号を取り扱う事務の流れ＞ 1. 適用事務 1ー②´		事業主は、ファイル交換サービス上に各種届出等をアップロードして提出する。	事前	同上
令和6年3月1日	(別添1)事務内容 ＜個人番号を取り扱う事務の流れ＞ 1. 適用事務 1ー④	当組合は、紙、電子記録媒体による届出書を確認し基幹システム専用端末で基幹システムに登録する。	当組合は、紙、電子記録媒体又はフラッシュメモリによる届出書を確認し基幹システム専用端末で基幹システムに登録する。	事前	同上
令和6年3月1日	(別添1)事務内容 ＜個人番号を取り扱う事務の流れ＞ 1. 適用事務 1ー④’”		当組合は、シンクライアントPCでファイル交換サービス上の届出書をダウンロードし、ダウンロードした届出書をフラッシュメモリに一時記録して、フラッシュメモリから基幹システム専用端末で基幹システムに登録する。	事前	同上
令和6年3月1日	Ⅱ3. 特定個人情報の入手・使用 ②入手方法	[○]その他(住民基本台帳ネットワークシステム、マイナポータル)	[○]フラッシュメモリ [○]その他(住民基本台帳ネットワークシステム、マイナポータル、ファイル交換サービス)	事前	同上
令和6年3月1日	Ⅱ3. 特定個人情報の入手・使用 ④入手に係る妥当性 【加入事業所から個人番号の入手】	資格取得時の一般被保険者の個人番号及び資格認定時のその被扶養者の個人番号や、個人番号の変更が生じた一般被保険者又はその被扶養者の新個人番号については、事業所が被保険者本人又は本人の代理人から提出を受けて届出書に個人番号を記載し、その書類を郵送又は電子申請データ にしてマイナポータル経由で(※1)当組合に届け出ることにより、当組合が入手する。 　当組合が事業所から届出書を受け付けるに当たっては、定められた紙の届出書又は暗号規約等の仕様が定められた電子記録媒体又はマイナポータル経由で申請された電子申請データのいずれかで行う。	資格取得時の一般被保険者の個人番号及び資格認定時のその被扶養者の個人番号や、個人番号の変更が生じた一般被保険者又はその被扶養者の新個人番号については、事業所が被保険者本人又は本人の代理人から提出を受けて届出書に個人番号を記載し、その書類を郵送又は当組合が指定したファイル交換サービス又は電子申請データ にしてマイナポータル経由で(※1)当組合に届け出ることにより、当組合が入手する。 　当組合が事業所から届出書を受け付けるに当たっては、定められた紙の届出書又は暗号規約等の仕様が定められた電子記録媒体及びフラッシュメモリ又は当組合が指定したファイル交換サービス又はマイナポータル経由で申請された電子申請データのいずれかで行う。	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月1日	Ⅱ6. 特定個人情報の保管・消去 ①保管場所		※ファイル交換サービスで届け出のあった届出書は、ダウンロードするまでファイル交換サービス内のストレージに保管される。	事前	同上
令和6年3月1日	Ⅱ6. 特定個人情報の保管・消去 ②保管期間 その妥当性		・ファイル交換サービスに係るファイルは、シンクライアントPC上にデータが保存されることはないが、フラッシュメモリへダウンロードするまでの期間は、ファイル交換サービス上には保存する。	事前	同上
令和6年3月1日	Ⅱ6. 特定個人情報の保管・消去 ③消去方法	＜基幹システムにおける措置＞ ・電子記録媒体にデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダーで物理的に破壊して廃棄する。	＜基幹システムにおける措置＞ ・電子記録媒体及びフラッシュメモリにデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄する。 ＜ファイル交換サービスサーバーにおける措置＞ ・ファイル交換サービス上に保存されるファイルはフラッシュメモリにダウンロード後、速やか（ダウンロード当日）に消去する。なお、消去漏れ防止のため自動削除機能を設定（10日間）し、設定期間経過後に自動消去する。 ・ファイル交換サービスからフラッシュメモリにダウンロードしたファイルは、基幹システムへの移行後、速やか（ダウンロード当日）に消去する。 ・フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去する。	事前	同上
令和6年3月1日	Ⅲ2. 個人情報の入手 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	【加入事業所から個人番号を入手する場合の措置】※ ・事業所が電子記録媒体で届出書を届け出る場合、取り決めたパスワード、暗号化処置をした媒体以外は受け付けない。	【加入事業所から個人番号を入手する場合の措置】※ ・事業所が電子記録媒体及びフラッシュメモリで届出書を届け出る場合、取り決めたパスワード、暗号化処置をした媒体以外は受け付けない。 ・事業所がファイル交換サービスで届出書を届け出る場合、ファイル交換サービス上に事業所がアップロードした届出書のみ受け付ける。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 2. 個人情報の入手 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 【加入事業所から個人番号を入手する場合の措置】	【加入事業所から個人番号を入手する場合の措置】※ ・事業所から届けられた届出書及び電子記録媒体は送付伝票と内容・数量を照合確認した上で、受領管理簿を起票する。 ・特定個人情報が記載された届出書は管理簿に記載して速やかに保管庫に施錠保管する。また、届出書を使用後は文書管理規程に従って保管及び廃棄措置をする。 ・電子記録媒体による入手は、暗号規約や標準フォーマット等が定められた仕様に基づきパスワード設定、暗号化を行い、書留等を用いて搬送する。 ・事業所から入手した電子記録媒体は媒体管理簿に記載し、速やかに保管庫に施錠保管する。 ・電子記録媒体に記録されたデータは、事前にウイルスチェックを行い、読み込んだ件数を事業所に書類で知らせて相違ないか確認する。 ・保管する必要がない使用済の電子記録媒体は、メディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を管理簿に記載する。	【加入事業所から個人番号を入手する場合の措置】※ ・ファイル交換サービスを利用する場合、事前に組合と共有したパスワードを使用し、ファイル交換サービス上にファイルをアップロードする。組合は共有したパスワードにて届出書をダウンロードして入手する。 ・ファイル交換サービスの通信経路は、HTTPS通信（TLS1.2）により暗号化を施しており、送受信の際、最新のパターンファイルで自動的にウイルスチェックを実施する。 ・事業所から届けられた届出書及び電子記録媒体及びフラッシュメモリは送付伝票と内容・数量を照合確認した上で、受領管理簿を起票する。 ・特定個人情報が記載された届出書は管理簿に記載して速やかに保管庫に施錠保管する。また、届出書を使用後は文書管理規程に従って保管及び廃棄措置をする。 ・電子記録媒体及びフラッシュメモリによる入手は、暗号規約や標準フォーマット等が定められた仕様に基づきパスワード設定、暗号化を行い、書留等を用いて搬送する。 ・事業所から入手した電子記録媒体及びフラッシュメモリは媒体管理簿に記載し、速やかに保管庫に施錠保管する。 ・電子記録媒体及びフラッシュメモリに記録されたデータは、事前にウイルスチェックを行い、読み込んだ件数を事業所に書類で知らせて相違ないか確認する。 ・保管する必要がない使用済の電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を管理簿に記載する。	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月1日	同		【ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置】 ・シンクライアントPC端末にはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく。 ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについて、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・特定個人情報にアクセスする権限が与えられていない職員等がシンクライアントPC端末を使用する場合、特定個人情報へのアクセスができないようシステム的に制御する。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 リスク2：ユーザー認証の管理		＜ファイル交換サービスサーバーにおける措置＞ ・ファイル交換サービスの運用担当者がサーバーへアクセスする際は、事前レビュー・承認を必要とする他、専用のGWサーバー（SecureCube/AccessCheck）上で認証し、接続制限とログの取得を実施する。 ・IPアドレス制限機能を利用して、許可された環境外からのログインを禁止する。 ※ファイル交換サービスにおいても上記＜基幹システムにおける措置＞と同様に行う。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 リスク2：アクセス権限の発効・失効の管理		＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ 【アクセス権限の発効】 ・採用や異動等で適用、給付、徴収担当となる職員等には、担当となる日から有効なアクセス権限を、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能に設定し、ユーザ管理簿に記載する。 【アクセス権限の失効】 ・異動や退職等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、データ保護担当者の指示によりシステム担当課（IT推進課）がシステム管理・制御機能の設定を変更し、ユーザ管理簿に記載する。 ・ファイル交換サービスにおいて自動ロック機能を利用して、使わなくなったアカウントを失効する。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 リスク2：アクセス権限の管理		＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ユーザID、アクセス権限の発効や更新は、システム担当課（IT推進課）以外は行えないものとする。 ・システム担当課（IT推進課）はユーザIDやアクセス権限の発効や更新を行う都度、データ保護担当者の確認を得てユーザ管理簿に更新記録を記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、ユーザ管理簿の点検・見直しを行う。 ・ユニークなパスワードの設定を徹底する。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 リスク2： 特定個人情報の使用の記録		＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・操作ログを確認し、不正操作の痕跡を1ヶ月ごとに確認する。 ・特定個人情報ファイルへのアクセス等について、操作ログを自動的に記録する。 ・操作ログには、処理年月日、時間、操作者等を記録する。 ・操作ログは一定期間保管し、不正アクセスや事故が疑われるときに点検し追跡できるようにする。 ・データ保護担当者は、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を確認し、不正な運用が行われていないかを点検する。	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 リスク3：従業員が事務外で使用するリスク	＜基幹システムにおける措置＞ ・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、電子記録媒体による届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。	＜基幹システムにおける措置＞ ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・アクセス権限がある職員等でも、Ⅰ基本情報「1．特定個人情報ファイルを取り扱う事務」に記載した事務以外では個人番号や特定個人情報ファイルにアクセスできないようシステム的に制御する。 ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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。 ・職員等に対して、特定個人情報の適切な取扱いを理解させることを目的として定期的に教育、研修を行う。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 3．特定個人情報の使用 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	＜基幹システムにおける措置＞ ・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、電子記録媒体による届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体又はフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・廃棄する電子記録媒体は、メディアシュレッダーで物理的に破壊して廃棄して廃棄し、廃棄記録を媒体管理簿に記載する。	＜基幹システムにおける措置＞※ ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システムの専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体又はフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・廃棄する電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。	事前	同上
令和6年3月1日	同		＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ファイルのバックアップ、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員だけが当該端末を操作できるようアクセス制御する。 ・電子記録媒体又はフラッシュメモリに複製を行う場合は、不必要な複製を制限するため事前に管理者の承認を得て、利用記録等を媒体管理簿に記載する。処理に使用後フラッシュメモリからは速やかにデータを完全消去し、返却された電子記録媒体又はフラッシュメモリを管理者が確認して、保管庫に施錠保管する。 ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去した又は物理的に破壊した証明書類の提出で処置を確認する。 条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を管理簿に記載する。 ・廃棄する電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。 ・定期的に操作ログをチェックし、必要のないアクセスが行われていないか監視する。 ・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出しが行われていないか監視する。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 4．特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録	＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ ・提供した書類や電子記録媒体の授受及び保管記録。	＜委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）＞ ・提供した書類や電子記録媒体及びフラッシュメモリの授受及び保管記録。	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月1日	Ⅲリスク対策（プロセス） 4．特定個人情報ファイルの取扱いの委託 委託におけるその他のリスク対策		＜ファイル交換サービスにおける措置＞ ファイル交換サービスサーバー上のファイルは暗号化されて保存されるため、ファイル交換サービスを提供する事業者は、ファイル交換サービスサーバー上の情報を取り扱わず、閲覧することができない仕様になっている	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 7．特定個人情報の保管・消去 リスク1．特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策		＜ファイル交換サービスサーバーの措置の内容＞ ・ファイル交換サービスサーバ上の特定個人情報は、AESで暗号化して保存される。 利用するファイル交換サービスは、クラウドサービスプロバイダとしてのクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」及びクラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証を取得している。 ・敷地内には赤外線監視カメラを設置し、24時間有人監視を実施し、不正入館を防ぐ ・入館時には顔写真付身分証明書による本人確認に加え、マントラップゲートを設置し、共連れを防ぐ ・各エリア毎に設けられた生体認証装置により、アクセス範囲を制御している ・本番データが入った媒体のデータセンターからの持ち出しは原則禁止しており、必要がある場合には事前許可・確認が必須となる ・出口ではX線検査装置に加え、3Dホログラフィックボディスキャナーを設けており、機器・媒体の持ち出しを監視している。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 7．特定個人情報の保管・消去 リスク1．特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策	＜基幹システムにおける措置＞ ・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、電子記録媒体による届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。	＜基幹システムにおける措置＞ ・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、電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、操作を行う基幹システムの専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステム的に制御する。 ・フラッシュメモリは暗号化機能付きフラッシュメモリを使用。	事前	同上
令和6年3月1日	同		＜ファイル交換サービスサーバーの措置の内容＞ ファイル交換サービスサーバ上の特定個人情報は、AESで暗号化して保存される。 利用するファイル交換サービスは、クラウドサービスプロバイダとしてのクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」及びクラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証を取得している。 ＜ファイル交換サービスの措置の内容＞ 多段にファイアウォールを設置し、必要な通信以外を遮断する。 不正アクセスの検知時は、必要に応じた被害の拡大防止、調査、対策を実施する。 WAF（Web Application Firewall）を設置し、不正な攻撃パターンを検知する。検知後は必要に応じた対策を実施する。 ＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・電子記録媒体及びフラッシュメモリによる届出書等データの読出しについては、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。 ・フラッシュメモリは暗号化機能付きフラッシュメモリを使用	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 7．特定個人情報の保管・消去 リスク3．特定個人情報が消去されずいつまでも存在するリスク	＜基幹システムにおける措置＞ ・電子記録媒体にデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダーで物理的に破壊して廃棄する。	＜基幹システムにおける措置＞ ・電子記録媒体及びフラッシュメモリにデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダー、フラッシュメモリを溶解廃棄にて物理的に破壊して廃棄する。	事前	同上

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月1日	同		＜ファイル交換サービスから届出書をダウンロードするシンクライアントPCにおける措置＞ ・ファイル交換サービスに係るファイルは、フラッシュメモリへダウンロードするため、シンクライアントPC上にデータが保存されず、特定個人情報が消去されずいつまでも存在することはない。 ・ファイル交換サービス上に保存されるファイルは、速やかに消去する。 ・消去漏れ防止のため自動削除機能を設定する。期間は10日間設定とし、設定期間経過後に自動削除する。 ・フラッシュメモリに一時的に記録した特定個人情報は、使用の都度速やかに完全消去する。	事前	同上
令和6年3月1日	Ⅲリスク対策（プロセス） 7. 特定個人情報の保管・消去 保管・消去におけるその他のリスク対策	【運用上のルールによる措置】 ・書類又は電子記録媒体の搬送時の所在追跡可能な手段の実施 ・廃棄する電子記録媒体は、メディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載 ・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	【運用上のルールによる措置】 ・書類又は電子記録媒体及びフラッシュメモリの搬送時の所在追跡可能な手段の実施 ・廃棄する電子記録媒体及びフラッシュメモリについて、電子記録媒体はメディアシュレッダー、フラッシュメモリは溶解廃棄にて物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載 ・電子記録媒体及びフラッシュメモリ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	事前	同上
令和6年3月1日	同		【ファイル交換サービスにおける措置】 ・ファイル交換サービスサーバー上のファイルは暗号化されて保存されるため、ファイル交換サービスを提供する事業者は、ファイル交換サービスサーバー上の情報を取り扱わず、閲覧することができない仕様になっている。 【ファイル交換サービスサーバーの措置の内容】 ・障害対策として、機器の冗長化、ネットワークの冗長化、電源の冗長化を実施している ・障害検知・復旧の措置として、24時間365日、サービスの監視、サイバー攻撃のモニタリングを実施している。 ・定期的に、プラットフォーム診断（月１回）、webアプリケーション診断（年１回以上）、ペネトレーションテスト（年１回以上）を実施している。	事前	同上
令和6年3月1日	Ⅳその他のリスク対策 1. 監査 ②監査		＜ファイル交換サービス運用事業者における措置の内容＞ ISMS及びセキュリティ格付けによる外部監査、さらに内部監査に基づき、担当者が適正に処理を行っているか確認している。	事前	同上
令和6年3月1日	Ⅳその他のリスク対策 2. 従業者に対する教育・啓発		【ファイル交換サービス運用事業者における措置の内容】 研修やOJTで、機密情報の取扱やセキュリティに関する教育を行っている。	事前	同上
令和6年3月1日	Ⅳその他のリスク対策 3. その他のリスク対策		＜ファイル交換サービス運用事業者における措置の内容＞ 不測事態対策委員会が常設機関として存在し、事案が発覚した際には、被害や損失を最小限にとどめ、かつ一刻も早い定常状態への復旧・回復を行うために、迅速かつ適切な対応行動がとれるようになっている。	事前	同上

別紙1 「特定個人情報の提供先一覧」 （1/2）

提供先※		①法令上の根拠	②提供先における用途	③提供する情報
1	厚生労働大臣	番号法第19条第8号 別表第2 第1項	健康保険法第5条第2項の規定により厚生労働大臣が行うこととされた健康保険に関する事務であって主務省令で定めるもの	医療保険各法又は高齢者の医療の確保に関する法律による医療に関する給付の支給又は保険料の徴収に関する情報（以下「医療保険給付関係情報」という。）であって主務省令で定めるもの
2	全国健康保険協会	番号法第19条第8号 別表第2 第2項	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
3	健康保険組合	番号法第19条第8号 別表第2 第3項	健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
4	厚生労働大臣	番号法第19条第8号 別表第2 第4項	船員保険法第4条第2項の規定により厚生労働大臣が行うこととされた船員保険に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
5	全国健康保険協会	番号法第19条第8号 別表第2 第5項	船員保険法による保険給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
6	都道府県知事	番号法第19条第8号 別表第2 第9項	児童福祉法による小児慢性特定疾病医療費の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
7	市町村長	番号法第19条第8号 別表第2 第12項	児童福祉法による肢体不自由児通所医療費の支給に関する事務であって主務省令で定めるもの	児童福祉法第21条の5の31に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
8	都道府県知事	番号法第19条第8号 別表第2 第15項	児童福祉法による障害児入所医療費の支給に関する事務であって主務省令で定めるもの	児童福祉法第24条の22に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの
9	市町村長	番号法第19条第8号 別表第2 第17項	予防接種法による給付（同法第15条第1項の疾病に係るものに限る。）の支給に関する事務であって主務省令で定めるもの	医療保険各法その他の法令による医療に関する給付の支給に関する情報であって主務省令で定めるもの
10	都道府県知事	番号法第19条第8号 別表第2 第22項	精神保健及び精神障害者福祉に関する法律による入院措置に関する事務であって主務省令で定めるもの	精神保健及び精神障害者福祉に関する法律第30条の2に規定する他の法律による医療に関する給付の支給に関する情報であって主務省令で定めるもの
11	都道府県知事等	番号法第19条第8号 別表第2 第26項	生活保護法による保護の決定及び実施又は徴収金の徴収に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
12	市町村長	番号法第19条第8号 別表第2 第27項	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
13	日本私立学校振興・共済事業団	番号法第19条第8号 別表第2 第33項	私立学校教職員共済法による短期給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
14	国家公務員共済組合	番号法第19条第8号 別表第2 第39項	国家公務員共済組合法による短期給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
15	市町村長又は国民健康保険組合	番号法第19条第8号 別表第2 第42項	国民健康保険法による保険給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
16	市町村長又は国民健康保険組合	番号法第19条第8号 別表第2 第43項	国民健康保険法による保険給付の支給に関する事務であって主務省令で定めるもの	国民健康保険法第56条第1項に規定する他の法令による保険の支給に関する情報であって主務省令で定めるもの
17	地方公務員共済組合	番号法第19条第8号 別表第2 第58項	地方公務員等共済組合法による短期給付の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
18	市町村長	番号法第19条第8号 別表第2 第62項	老人福祉法による費用の徴収に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
19	厚生労働大臣	番号法第19条第8号 別表第2 第78項	雇用保険法による傷病手当の支給に関する事務であって主務省令で定めるもの	雇用保険法第37条第8項に規定する他の法令による給付の支給に関する情報であって主務省令で定めるもの

別紙1「特定個人情報の提供先一覧」 (2/2)

提供先※		①法令上の根拠	②提供先における用途	③提供する情報
20	後期高齢者医療広域連合	番号法第19条第8号 別表第2 第80項	高齢者の医療の確保に関する法律による後期高齢者医療給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
21	都道府県知事等	番号法第19条第8号 別表第2 第87項	中国残留邦人等支援給付等の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
22	市町村長	番号法第19条第8号 別表第2 第93項	介護保険法による保険給付の支給又は地域支援事業の実施に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの
23	都道府県知事又は保健所を設置する市の長	番号法第19条第8号 別表第2 第97項	感染症の予防及び感染症の患者に対する医療に関する法律による費用の負担又は療養費の支給に関する事務であって主務省令で定めるもの	感染症の予防及び感染症の患者に対する医療に関する法律第39条第1項に規定する他の法律による医療に関する給付の支給に関する情報であって主務省令で定めるもの
24	独立行政法人日本学生支援機構	番号法第19条第8号 別表第2 第106項	独立行政法人日本学生支援機構法による学資の貸与及び支給に関する事務であって主務省令で定めるもの	医療保険各法その他の法令による医療に関する給付の支給に関する情報であって主務省令で定めるもの
25	都道府県知事又は市町村長	番号法第19条第8号 別表第2 第109項	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による自立支援給付の支給に関する事務であって主務省令で定めるもの	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7条に規定する他の法令により行われる給付の支給に関する情報であって主務省令で定めるもの
26	都道府県知事	番号法第19条第8号 別表第2 第120項	難病の患者に対する医療等に関する法律による特定医療費の支給に関する事務であって主務省令で定めるもの	医療保険給付関係情報であって主務省令で定めるもの

※当組合は、健康保険法の規定に基づき、支払基金に情報提供ネットワークシステムを通じた情報照会・提供事務を委託する。
情報提供ネットワークシステムを通じて取得した情報を保険給付の支給等の事務に活用するのは当組合であるが、情報提供ネットワークシステムに接続する主体は支払基金である。
ここでは、支払基金が情報提供ネットワークシステムに接続して特定個人情報を提供する提供先を記載している。