

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	簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務

個人のプライバシー等の権利利益の保護の宣言

独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構は、簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務における特定個人情報ファイルの取扱いに当たり、同ファイルの取扱いがお客さまの財産、個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために十分な措置を講じることをもって、お客さまの財産、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

簡易生命保険契約に係る管理業務については、独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構が監督・指導等の責任を負いつつ、郵政民営化法等の定めにより株式会社かんぽ生命保険が当機構の委託を受けて行うこととされており、簡易生命保険契約の管理業務に関するシステムや特定個人情報ファイルを取り扱う全ての事務を行う同社も同様の措置を講じることとする。

評価実施機関名

独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構

個人情報保護委員会 承認日【行政機関等のみ】

公表日

項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務
②事務の内容 ※	簡易生命保険は、「国民に、簡易に利用できる生命保険を、確実な経営により、なるべく安い保険料で提供し、もって国民の経済生活の安定を図り、その福祉を増進すること」を目的として(簡易生命保険法[昭和24年法律第68号]第1条)、国が、憲法第25条第2項の規定に鑑み、社会福祉の向上及び増進の方策として事業を行うものとして制度化されたものである。 簡易生命保険契約については、日本郵政公社(以下「公社」という。)の解散に際し、郵政民営化法(平成17年法律第97号)第163条第3項の認可を受けた実施計画の定めにより簡易生命保険契約に係る公社の権利及び義務を独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構(以下「機構」という。)が承継し(同実施計画2(2)③ロ(イ))、株式会社かんぽ生命保険(以下「かんぽ生命」という。)は、機構の委託を受けて簡易生命保険管理業務を行うこととなったため(同実施計画1(1)②)、かんぽ生命は、公社から承継した簡易生命保険契約に係るシステムを活用して、特定個人情報ファイルを取り扱う全ての事務を行っている。 そのため、特定個人情報ファイルの取扱いの実態やリスク対策の具体的な内容については、かんぽ生命が把握しており、Ⅱ特定個人情報ファイルの概要や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等については、かんぽ生命におけるものを記載している(Ⅱ4.、Ⅲ4.、Ⅲ7. ⑨、Ⅳ及びⅤを除く。) なお、簡易生命保険契約においては、社会保障・税番号制度の導入に伴い、平成28年1月以降支払事由が発生する「生命保険契約の一時金の支払調書」及び「生命保険契約の年金の支払調書」において、保険契約者及び保険金等受取人の個人番号を記載する必要があるため、個人番号を取得するもの。 【Ⅰ. 個人番号を特定個人情報ファイルに登録する事務】 1. かんぽ生命支店等及び郵便局 ・かんぽ生命支店及び本社法人営業開発部(以下「支店等」という。)並びに郵便局において保険金等の支払請求等をされたお客さまから個人番号の提示を受け、郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 2. かんぽ生命支店等渉外社員及び郵便局社員 ・お客さま宅等において保険金等の支払請求等をされたお客さまから個人番号の提示を受け、かんぽ生命支店等渉外社員等が携帯端末機(インターネット閲覧機能や社外とのメール機能がない専用端末機(PT5))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 3. お客さまによる個人番号のオンライン申告 ・お客さま自身が、かんぽ生命が業務委託した公的個人認証サービスを提供するプラットフォーム事業者(以下、「委託PF事業者」という。)が開発した認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCを用いて、かんぽ生命から送付した各種通知物等に記載されている二次元バーコードを読み取り、スマートフォン又はポスタルタブレットPCにマイナンバーカードをかざすことで、委託PF事業者のシステムを経由して個人番号を収集し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 4. かんぽ生命契約サービス部 ・年金支払中のお客さまから個人番号が記載された書類等のコピーを専用封筒により郵送回答を受け、端末機(インターネット機能やメール機能がない専用端末機)に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 なお、かんぽ生命支店等及び郵便局、かんぽ生命支店等渉外社員及び郵便局社員においては、端末機から登録された個人番号を照会できず、個人番号の取得状況のみ照会可能となっている。 【Ⅱ. 特定個人情報ファイルを使用する事務】 1. かんぽ生命情報管理センター ・上記Ⅰにより登録された個人番号を支払調書データに付加して、CD等の記録媒体を用いてかんぽ生命契約サービス部へ提出する。 2. かんぽ生命契約サービス部 ・支払調書については、以下の方法で税務署へ提出する ①「法定調書提出クラウドサービス」※を利用した提出 国税庁が定めるクラウド提出に必要な要件を満たした支払調書データ(当年分を含む過去4年分) ② 電子媒体による郵送での提出 上記①以外の支払調書データ ※「法定調書提出クラウドサービス」は国税庁長官の認定を受けたクラウドサービスであり、提供事業者が国税庁長官の認定を受けるためには、認定の対象となるクラウドサービス又はオンプレミスが、政府情報システムのためのセキュリティ評価制度(ISMAP)のクラウドサービスリストに掲載されていること、提供事業者及び利用者各々の立場から安全管理措置を講じられていること、サーバが日本国内に所在していることなど、国税庁告示で定める要件に適合することが必要となる。
③対象人数	＜選択肢＞ [30万人以上] 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

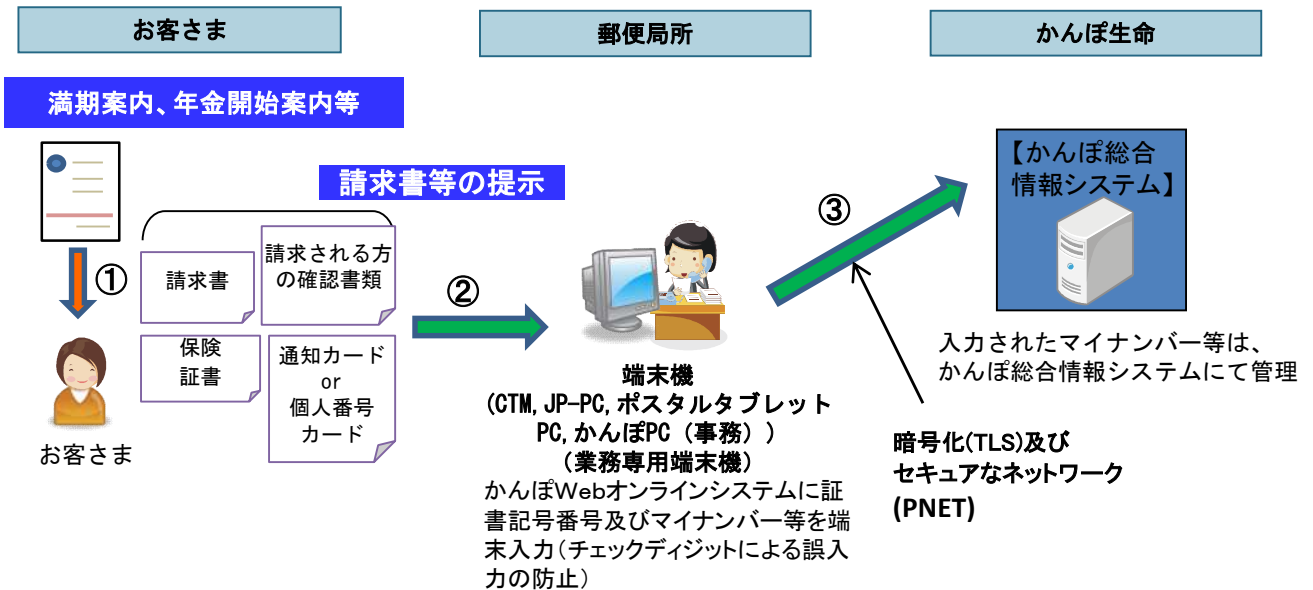
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	かんぽ総合情報システム
②システムの機能	かんぽ総合情報システムは、かんぽ生命が管理している簡易生命保険契約に関する保険契約情報を管理しており、個人番号については、かんぽ総合情報システム内の個人番号等管理マスタにおいて個人番号の登録、修正、削除及び管理の機能を有している。 管理している個人番号については、税務署に提出する支払調書データ作成時に保険金等の支払データの証書記号番号等と紐付け、反映する。
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☐ その他（他のシステムとの接続はない） ☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム
システム2～5	
システム2	
①システムの名称	e-私書箱
②システムの機能	野村総合研究所で開発した企業の電子的なお知らせを個人に届けるクラウドサービスである。デジタル庁のマイナポータルや国税庁のe-Tax等の行政手続システムと連携することで、行政手続の電子化を実現するもの。支払調書における「法定調書提出クラウドサービス」は2022年1月に国税庁長官の認定を受けている。
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☐ その他（他のシステムとの接続はない） ☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム
システム6～10	
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
特定個人情報ファイル(支払調書)	
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	- 番号制度に関する税制上の措置として、生命保険会社が法定調書として税務署に提出する支払調書に個人番号の記載を求める措置が講じられたところである。 - 既存のかんぽ総合情報システムにおける支払調書データに必要な簡易生命保険契約の情報に加え、個人番号を紐付けて付定する必要があるため、特定個人情報ファイルを保有する。
②実現が期待されるメリット	- 特定個人情報ファイルを利用して、大量の簡易保険契約に係る支払調書データを作成するに当たり、個人番号を紐付けて記載することが可能となる。 - 法定調書提出クラウドサービスを利用することで専用回線（閉域網）での連携が可能になる。 - マイナポータル連携サービスを利用することで、お客さまへの確定申告書情報の連携が可能となり、お客さまがe-TAXでの確定申告時に確定申告書情報が自動で連携される機能を用いることによってお客さまの負担が軽減する。
5. 個人番号の利用 ※	
法令上の根拠	1.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。）第9条 2.所得税法（昭和44年法律第33号）第225条

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	[実施しない]	<選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠		
7. 評価実施機関における担当部署		
①部署	保険部業務課	
②所属長の役職名	保険部業務課長	
8. 他の評価実施機関		
—		

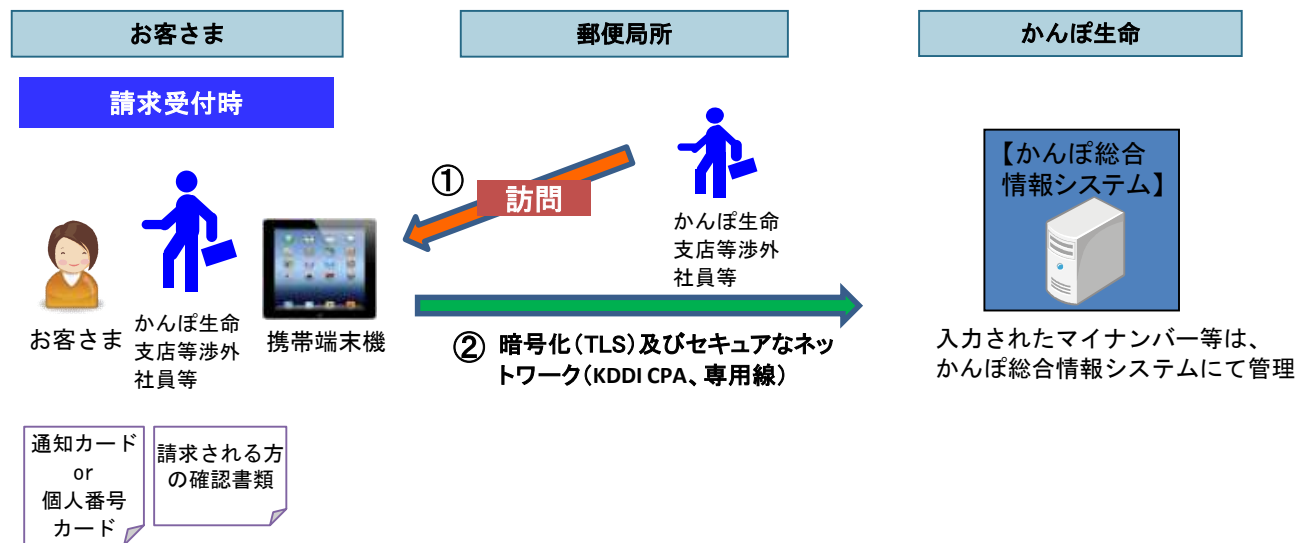
(別添1) 事務の内容

【Ⅰ. 個人番号を特定個人情報ファイルに登録する事務】

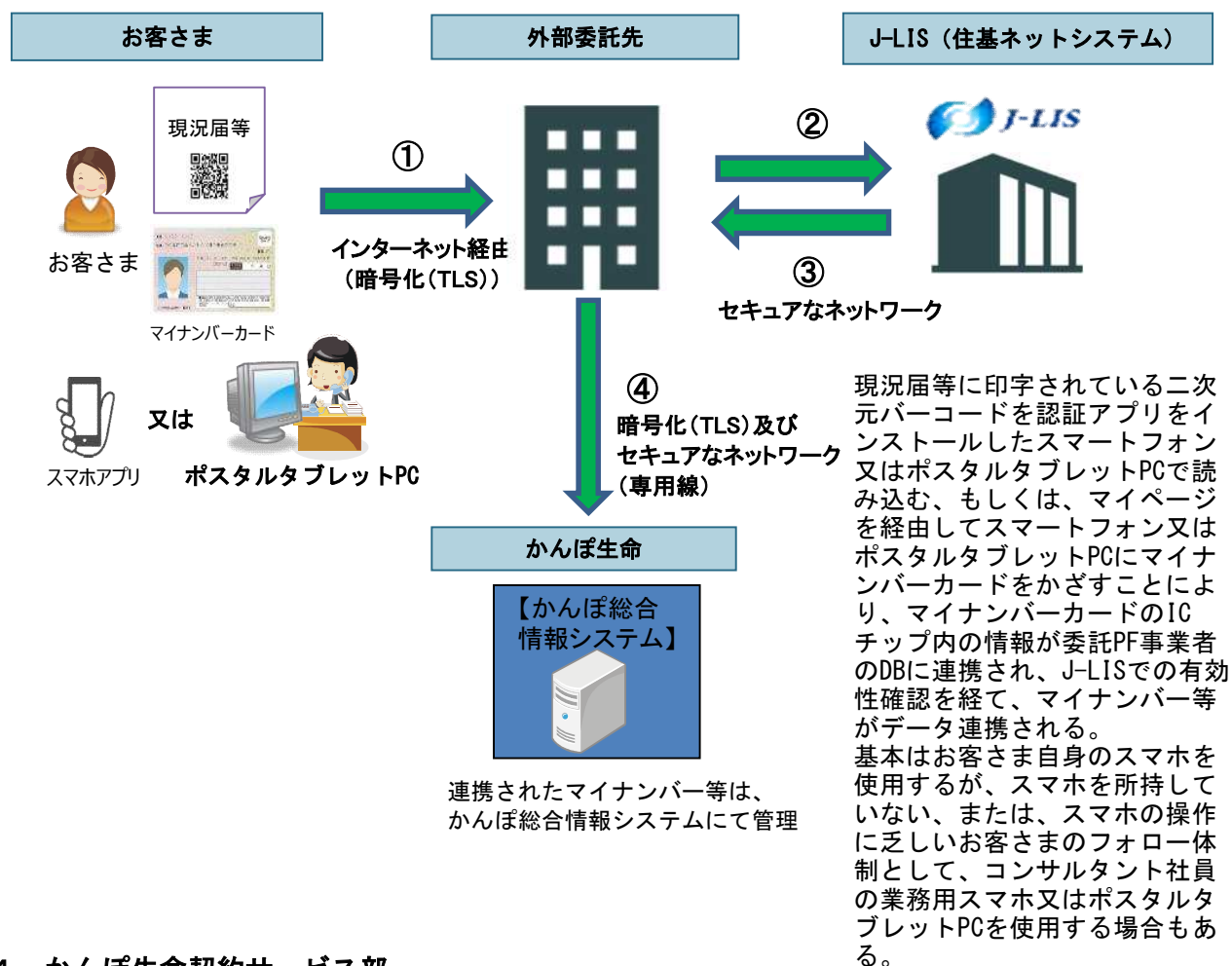
1. かんぽ生命支店等及び郵便局



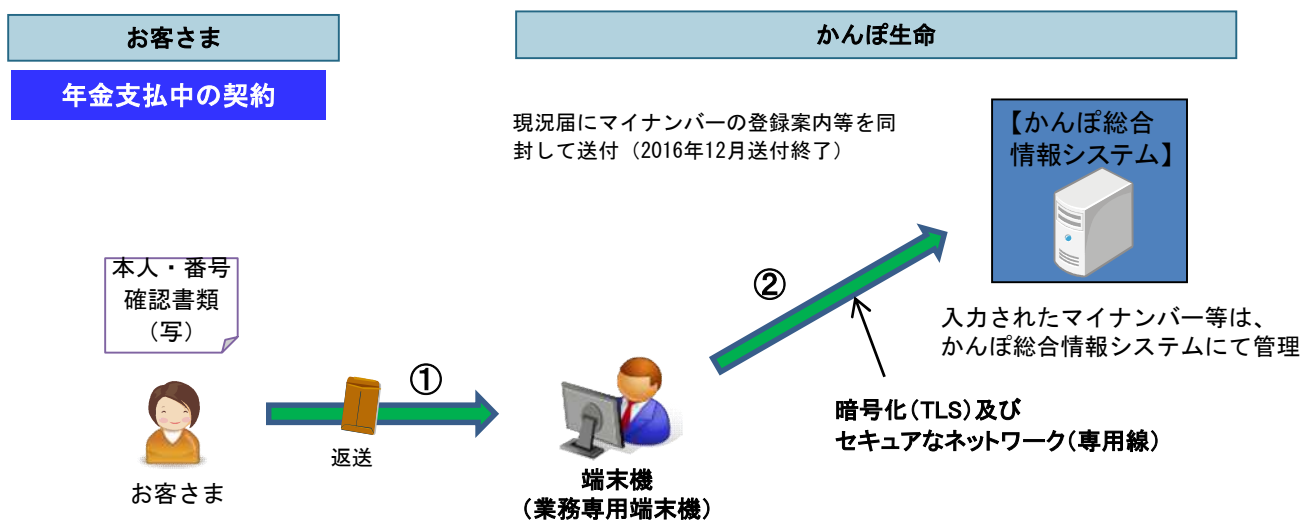
2. かんぽ生命支店等渉外社員及び郵便局社員



3. お客さまによる個人番号のオンライン申告 公的個人認証サービス（JPKI）



4. かんぽ生命契約サービス部



(備考)

1. かんぽ生命支店等及び郵便局

- ①かんぽ生命から満期案内、年金支払開始等のご案内を送付する。
- ②保険金等の支払請求等のために窓口に来られたお客さまから個人番号の提示を受ける。
- ③郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。
端末機とかんぽ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。

2. かんぽ生命支店等渉外社員及び郵便局社員

- ①保険金等の支払請求等の手続きのためにお客さま宅を訪問し、個人番号の提示を受け、携帯端末機(インターネット機能やメール機能がない専用端末(PT5))に個人番号を登録する。
- ②携帯端末機(PT5)は取扱いの都度、データ送信により個人番号等管理マスタへ個人番号を登録する。
携帯端末機(PT5)とかんぽ総合情報システム間は携帯電話網を使用した暗号化及びセキュアな通信を行っており、安全性が確保されている。
また、端末認証サービスで端末を限定しており、セキュアな通信を行っている。

3. お客さまによる個人番号のオンライン申告

公的個人認証サービス(JPKI)

- ①現況届等に印字されている二次元バーコードを認証アプリをインストールしたスマートフォン又はポスタルタブレットPCで読み込む、もしくは、マイページを経由してスマートフォン又はポスタルタブレットPCにマイナンバーカードをかざすことにより、マイナンバーカードのICチップ内の情報が委託PF事業者のDBに連携される。
- ②委託PF事業者のDBからJ-LISへ電子証明書の有効性確認を行う。
- ③有効性確認の結果が連携される。
- ④委託PF事業者のDBから個人番号データがかんぽ生命に連携され、個人番号等管理マスタへ個人番号を登録する。
委託PF事業者のDBとかんぽ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。

4. かんぽ生命契約サービス部

- ①かんぽ生命契約サービス部がお客さまから個人番号等届出書等の郵送回答を受ける。
- ②かんぽ生命契約サービス部が端末機(インターネット機能やメール機能がない専用端末機)から個人番号等管理マスタへ個人番号を登録する。
端末機とかんぽ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。

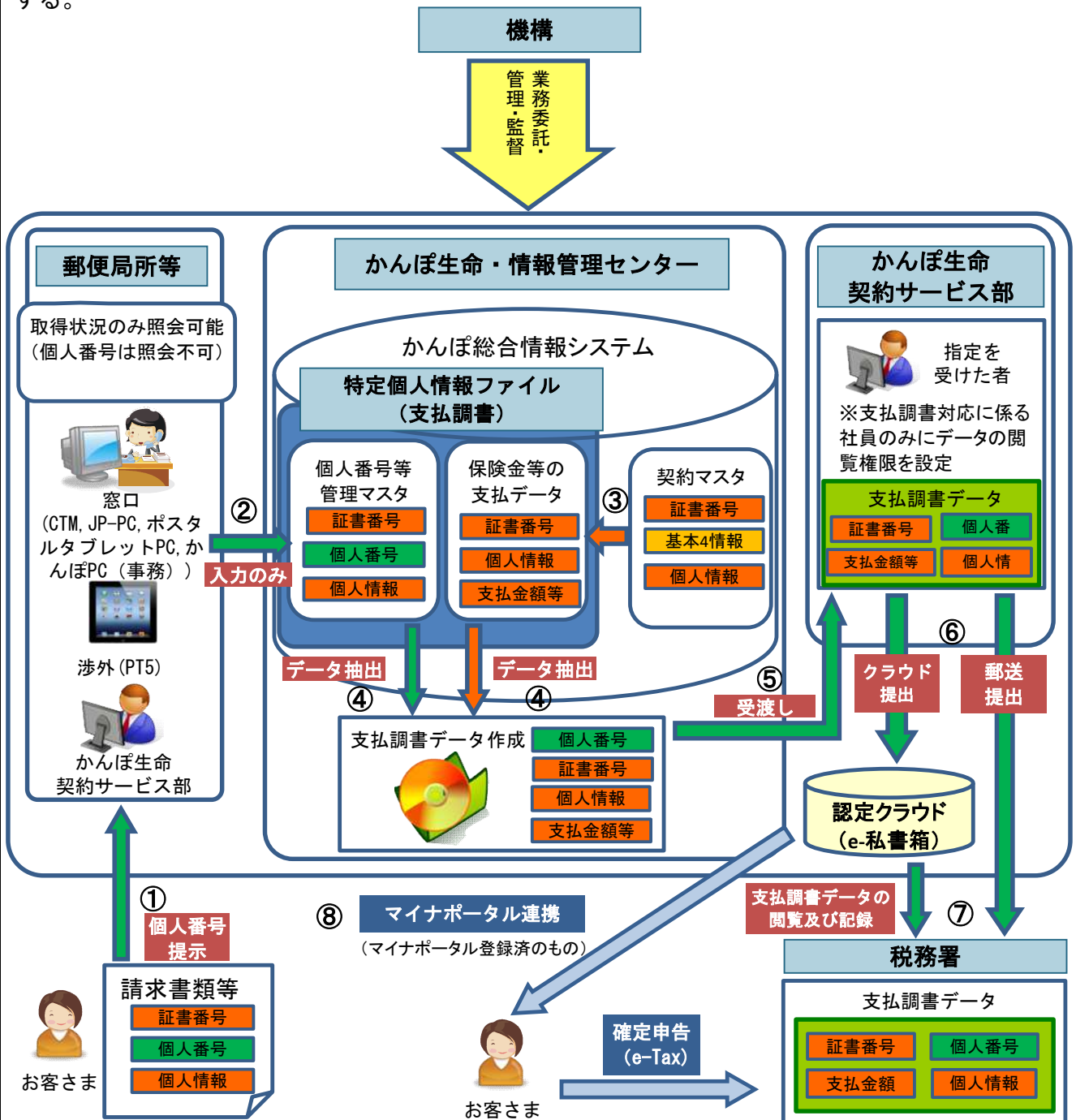
【Ⅱ. 特定個人情報ファイルを使用する事務】

1. かんぽ生命情報管理センター

・登録された個人番号を支払調書データに付加して、CD等の記録媒体を用いてかんぽ生命契約サービス部へ提出する。

2. かんぽ生命契約サービス部

・支払調書データを電子媒体により郵送する方法及び認定クラウドを利用する方法で税務署へ提出する。



(備考)

(事務の流れ)

- ① 郵便局等来局又は渉外社員の訪問により、保険金等支払請求時等にお客さま(保険契約者及び保険金等受取人)から、個人番号カード等の提示をうけ、個人番号を取得する。(かんぽ生命契約サービス部の場合は個人番号が記載された専用紙の返送を受ける。)
- ② 「個人番号等登録請求画面」に証書番号・受取人種別・カナ氏名・個人番号を入力する。
- ③ 契約マスタから、保険金等支払に関するデータを抽出。
- ④ ③で抽出したデータと個人番号等管理マスタのデータを「特定個人情報ファイル(支払調書)」とし、保険証書記号番号等で突合して支払調書データを作成する。
- ⑤ かんぽ生命情報管理センターからかんぽ生命契約サービス部へ支払調書データの受け渡しを行う。
- ⑥ かんぽ生命契約サービス部から以下の方法で支払調書データを税務署へ提出する。
 - ・電子媒体による郵送での提出
 - ・認定クラウドを利用した提出
- ⑦ 税務署は上記の方法で提出された支払調書データの閲覧および記録を行い、郵送でも受領する。
- ⑧ お客さまがマイナポータル上で確定申告書情報の連携を選択すると、支払調書データが連携され(※)、お客さまが確定申告(e-Tax)を行う際に、確定申告書に必要な情報が自動で連携される。
 - ※ かんぽ生命が認定クラウドでの提出を行った契約のうちマイナンバーをご登録いただいているお客さまのみが対象。

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		
特定個人情報ファイル(支払調書)		
2. 基本情報		
①ファイルの種類 ※	システム用ファイル ☐ システム用ファイル ☐ 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	1,000万人以上 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上	
③対象となる本人の範囲 ※	簡易生命保険契約に係る保険金等の受取人及び保険契約者等	
その必要性	支払調書データに個人番号を付加して、税務署に提出するため	
④記録される項目	50項目以上100項目未満 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 100項目以上	
主な記録項目 ※	・識別情報 ☐ 個人番号 ☐ 個人番号対応符号 ☐ その他識別情報(内部番号) ・連絡先等情報 ☐ 5情報(氏名、氏名の振り仮名、性別、生年月日、住所) ☐ 連絡先(電話番号等) ☐ その他住民票関係情報 ・業務関係情報 ☐ 国税関係情報 ☐ 地方税関係情報 ☐ 健康・医療関係情報 ☐ 医療保険関係情報 ☐ 児童福祉・子育て関係情報 ☐ 障害者福祉関係情報 ☐ 生活保護・社会福祉関係情報 ☐ 介護・高齢者福祉関係情報 ☐ 雇用・労働関係情報 ☐ 年金関係情報 ☐ 学校・教育関係情報 ☐ 災害関係情報 ☐ その他 (カナ氏名及び保険金等の支払データ)	
	その妥当性	対象者を特定するために個人番号、その他識別情報(内部番号)(保険証書記号番号、個人番号等対象者コード及び受取人登録関係者コード)並びにカナ氏名を保有 その他、支払調書作成のために必要な保険金等の支払データを保有
	全ての記録項目	別添2を参照。
⑤保有開始日	2016/01/01	
⑥事務担当部署	保険部業務課(委託先: かんぽ生命事務サービス推進部、契約サービス部)	

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 () ☐ 地方公共団体・地方独立行政法人 () ☐ 民間事業者 () ☐ その他 ()
②入手方法	☐ 紙 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 電子メール ☐ 専用線 ☐ 庁内連携システム ☐ 情報提供ネットワークシステム 本人等から個人番号カード等の提示を受け、(携帯)端末機に入力 ☐ その他 (認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCにマイナンバーカードをかざす)
③入手の時期・頻度	【かんぽ生命支店等及び郵便局】、【かんぽ生命支店等渉外社員及び郵便局社員】 ・本人等から簡易生命保険契約に係る保険金等の支払請求等を受けた都度、個人番号、簡易生命保険契約に係る保険証書記号番号等、必要な個人情報を入手する。 【お客さまによる個人番号のオンライン申告】 ①簡易生命保険契約に係る年金受取人が、「もっと かんぽらくらくサービス」の利用申込みのため、現況届等に印字された二次元バーコードを認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCで読み取り、スマートフォン又はポスタルタブレットPCにマイナンバーカードをかざしたタイミングにより、個人番号を入手する。 ②簡易生命保険契約に係る契約者がマイページを介して、認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCにマイナンバーカードをかざしたタイミングにより、個人番号を入手する。 【かんぽ生命契約サービス部】 ・簡易生命保険契約に係る年金受取人から個人番号等届出書の提出(郵送)を受けた都度、個人番号、簡易生命保険契約に係る保険証書記号番号等、必要な個人情報を入手する。
④入手に係る妥当性	・郵政民営化法の規定により機構に承継された簡易生命保険契約については、その管理に関する業務をかんぽ生命に委託しており、更にかんぽ生命から日本郵便株式会社(以下「日本郵便」という。)に一部業務を再委託している。そのため、利用者である本人等が、かんぽ生命の支店等や日本郵便の郵便局に請求された際に、その都度、必要な個人番号を入手する。 【かんぽ生命支店等及び郵便局】 ・入手方法は、本人等からの個人番号カード等の提示を受け、社員が個人番号を端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))に入力する。 ・入手の時期・頻度は、各契約における保険金等の支払事由等が発生した都度、年間通じて常時、請求を受け付ける。 【かんぽ生命支店等渉外社員及び郵便局社員】 ・入手方法は、本人等からの個人番号カード等の提示を受け、社員が個人番号を携帯端末機(PT5)に入力する。 ・入手の時期・頻度は、各契約における保険金等の支払事由等が発生した都度、年間通じて常時、請求を受け付ける。 【お客さまによる個人番号のオンライン申告】 ・入手方法は、お客さま自身が、委託PF事業者が開発した認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCを用いて、かんぽ生命から送付した各種通知物等に記載されている二次元バーコードを読み取り、スマートフォン又はポスタルタブレットPCにマイナンバーカードをかざすことで個人番号を入手する。 ・入手の時期・頻度は、①「もっと かんぽらくらくサービス」の利用申込みの際または②年間通じて常時受け付ける。 【かんぽ生命契約サービス部】 ・入手方法は、年金受取人から個人番号カード等の写しの送付を受けて、社員が個人番号を端末機に入力する。 ・入手の時期・頻度は、過去に送付した個人番号等届出書について年金受取人から随時提出(郵送)を受け付ける。

⑤本人への明示		・番号法第14条(提供の要求)において、本人等に対して個人番号の提供を求めることができる旨が規定されている。 ・本人等から簡易生命保険契約に係る保険金等の支払請求等を受ける都度、個人番号の利用目的等を記載した「個人情報の利用について」を交付する。 ・委託PF事業者が開発した認証アプリをダウンロードしたスマートフォン又はポスタルタブレットPCにマイナンバーカードをかざす際に、スマートフォン又はポスタルタブレットPCの画面上に個人番号の利用目的を表示する。
⑥使用目的 ※		簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)を作成するため
	変更の妥当性	—
⑦使用の主体	使用部署 ※	かんぽ生命契約サービス部
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※		・個人番号等管理マスタに登録された個人番号を保険金等の支払データに付加した支払調書データを暗号化し、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、専用回線(閉塞網)を介して認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携する(暗号化を行う通信方式を用いてデータ連携を行う)ことで税務署に提出する。
	情報の突合 ※	行わない
	情報の統計分析 ※	—
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	委託する <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	簡易生命保険契約に係る保険金等の支払に関する支払調書データ(税務署提出用)作成事務	
①委託内容	簡易生命保険契約の管理に関する業務	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	1,000万人以上 <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 ※	特定個人情報ファイルの対象者の範囲と同様	
その妥当性	機構は簡易生命保険契約に係るシステムを保有しておらず、特定個人情報ファイルを取り扱う事務はかんぽ生命に委託しているため、特定個人情報ファイルの取扱いに係るリスク対策等に関しては、かんぽ生命において安全管理措置を実施。	
③委託先における取扱者数	1,000人以上 <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 (システムが設置されているかんぽ生命にて取扱いを行う。)	
⑤委託先名の確認方法	機構ホームページにより、確認可能。	
⑥委託先名	かんぽ生命	
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	【日本郵便】 ・郵政民営化法等の定めにより、かんぽ生命は機構の委託を受けて簡易生命保険管理業務を行うこととなり、その一部を日本郵便に再委託することが義務付けられており、法令等に基づき再委託を実施。 なお、機構とかんぽ生命における委託契約書の中で、日本郵便との再委託について、かんぽ生命はあらかじめ機構の同意を得て行うものと約定し、かんぽ生命と日本郵便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が講じられていることを確認している。 【その他】 ・委託先のかんぽ生命から再委託の許諾申請があった場合は、再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他機構が求める情報を記載した書面の提供を受け、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等、再委託先における安全管理措置を確認した上で、再委託の承認を行う。
	⑨再委託事項	上記委託事項と同じ
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）

[illegible]

6. 特定個人情報の保管・消去

①保管場所 ※

【かんぽ総合情報システム(個人番号等管理マスタ)】、【かんぽ総合情報システム(保険金等の支払データ)】

セキュリティゲートを設けて入退室を行っている建物(かんぽ生命情報管理センター)にあって、入退室管理を行っている部屋に設置したメインフレームに個別のマスタファイルとして保管し、暗号化とアクセス制限を施す。

【入手経路による保管状況】

1. かんぽ生命支店等及び郵便局

端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))には個人情報を保管しない。

2. かんぽ生命支店等渉外社員及び郵便局社員

携帯端末機(PT5)には個人情報を保管しない。

3. お客さまによる個人番号のオンライン申告

① 委託PF事業者を介して入手する個人番号は一時的に委託PF事業者で保管し、かんぽ生命で個人番号の取得処理が正常に終了した後、委託PF事業者で消去する。

② 業務用携帯電話(スマートフォン)又はポスタルタブレットPCを使用してお客さまが「もっとかんぽらくらくサービス」の利用申込みを行う場合に備え、業務用携帯電話にはキャッシュの自動削除、スクリーンショット不可の制限をかける。

4. かんぽ生命契約サービス部

専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。

・専用端末(スタンドアロン)

専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともに、ログについても管理者による定期的なチェックを行っている。

・専用端末(閉域網通信用)

端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)としないことを確認する。

5. 認定クラウド(法定調書提出クラウドサービス)

国税庁告示で定める要件に適合することにつき、クラウドサービス事業者等が国税庁長官の認定を受けているクラウドサービス

【支払調書データ(副本)(電子媒体)】

支払調書データについては、電子記録媒体管理簿に登記し、施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。

②保管期間	期間	＜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	【かんぽ総合情報システム(個人番号等管理マスタ)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管することとする。 【かんぽ総合情報システム(保険金等の支払データ)】 支払調書データへ出力すると自動的に消去される。 【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))には個人情報を保管しない。 2. かんぽ生命支店等渉外社員及び郵便局社員 携帯端末機(PT5)には個人情報を保管しない。 3. お客さまによる個人番号のオンライン申告 ① 委託PF事業者を介して入手する個人番号は一時的に委託PF事業者で保管し、かんぽ生命で個人番号の取得処理が正常に終了した後、委託PF事業者で消去する。 ② 業務用携帯電話(スマートフォン)又はポスタルタブレットPCを使用してお客さまが「もっと かんぽらしくサービス」の利用申込みを行う場合に備え、キャッシュの自動削除、スクリーンショット不可の制限をかける。 4. かんぽ生命契約サービス部 ・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともに、ログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。 【支払調書データ(副本)(電子媒体)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管することとする。 ・支払調書データについては、電子記録媒体管理簿に登録し、施錠できるキャビネットに保管する。
	③消去方法	保存期間経過後システムの的に削除
7. 備考		

(別添2) 特定個人情報ファイル記録項目

(個人番号等管理マスタ項目)

保険証書記号番号、個人番号等対象者コード、個人番号等登録通番、マイナンバー、法人番号、個人番号等取得状態コード、個人番号等未取得理由コード、個人番号等登録年月日、受取人登録通番、受取人登録関係者コード、番号登録者カナ氏名、受付局所番号

--

(保険金等の支払データ項目)

法定資料の種類、整理番号1、本支店当区分番号、提出義務者(住所(居所)又は所在地)、提出義務者(氏名又は名称)、提出義務者(電話番号)、整理番号2、提出者(住所(居所)又は所在地)、提出者(氏名又は名称)、訂正表示、年分、受取人(住所(居所)又は所在地)、受取人(国外住所表示)、受取人(氏名又は名称)、契約者(住所(居所)又は所在地)、契約者(国外住所表示)、契約者(氏名又は名称)、被保険者(住所(居所)又は所在地)、被保険者(国外住所表示)、被保険者(氏名又は名称)、保険金額等、増加又は割増保険金額等、未払利益配当金等、貸付金額・同未収利息、未払込保険料額等、前納保険料等払戻金、差引支払保険金額等、既払込保険料等、保険事故等、保険事故等の発生年月日(年)、保険事故等の発生年月日(月)、保険事故等の発生年月日(日)、保険等の種類、保険金等の支払年月日(年)、保険金等の支払年月日(月)、保険金等の支払年月日(日)、摘要、保険会社等法人番号、受取人(個人・法人区分)、契約者(個人・法人区分)、個人・法人区分、既払込保険料等の剰余金又は割戻金、提出年月日(年)、提出年月日(月)、提出年月日(日)、本支店等区分番号、年金の種類、年金の支払金額、未払金額、剰余金又は割戻金、年金の支払金額に対する掛金額、差引金額、源泉徴収税額、相続等生命保険年金に該当(年金の支払開始日(年))、相続等生命保険年金に該当(年金の支払開始日(月))、相続等生命保険年金に該当(年金の支払開始日(日))、相続等生命保険年金に該当(残存期間年数)、相続等生命保険年金に該当(支払開始日年齢)、相続等生命保険年金に該当(支払期間年数)、相続等生命保険年金に該当(保証期間年数)、相続等生命保険年金に該当(支払総額又は支払総額見込額)、相続等生命保険年金に該当(支払総額等のうちに保険料又は掛金額の占める割合・整数部)、相続等生命保険年金に該当(支払総額等のうちに保険料又は掛金額の占める割合・小数部)、相続等生命保険年金に該当(年金に係る権利について相続税法第24条の規定により評価された額)

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	
特定個人情報ファイル(支払調書)	
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	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 保険契約の取扱いにおいて、保険金等支払請求等の際、請求人が正当な権利を有している者であることの確認を行うことが前提であることから、対象者以外の情報を入手しないよう措置している。 2. かんぽ生命支店等渉外社員及び郵便局社員 1と同様。 3. お客さまによる個人番号のオンライン申告 認証アプリの処理において契約内容として登録されている対象者の生年月日及び性別とスマートフォン又はポスタルタブレットPCにかざされたマイナンバーカードの生年月日及び性別を照合し、両者が一致しなければ個人番号の入手ができないよう措置している。 4. かんぽ生命契約サービス部 年金の受取人に対し、現況届の案内を送付した際、個人番号等届出書及び返信用封筒を同送していることが前提であることから、対象者以外の情報を入手しないよう措置している。
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	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 保険証書記号番号を入力し、保険契約の契約者又は保険金等受取人であることを確認の上個人番号を入力することから、必要最小限の情報のみ入力することとして措置している。 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 情報の入手元はマイナンバーカードとなるため、個人番号及び実存(本人)確認として必要な最低限の情報のみ入手することとして措置している。 4. かんぽ生命契約サービス部 年金の受取人に対し現況届の案内を送付した際、個人番号等届出書及び返信用封筒を同封しており、年金受取人から個人番号等確認書類の写し及び実存(本人)確認資料の写しの返送を受け、必要最小限の情報のみ入手することとして措置している。
その他の措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の取得時に個人番号の記載のある証明書類の写しを作成することや個人番号のメモを取ることは禁止している。 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 業務用携帯電話(スマートフォン)又はポスタルタブレットPCを使用してお客さまが「もっと かんぽらくらくサービス」の利用申込みを行う場合に備え、キャッシュの自動削除、スクリーンショット不可の制限をかけている。また、認証アプリは、マイナンバーカード又はポスタルタブレットPCから読み取った情報をサーバへデータ連携する仕組みであり、マイナンバーカードから読み取った情報をスマートフォン内又はポスタルタブレットPC内に保管することはない。 4. かんぽ生命契約サービス部 1、2と同様。
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	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の取得に際しては、個人番号カードの提示に基づき端末機（インターネット機能やメール機能がない端末機（CTM）、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機（JP-PC(3001)、ポスタルタブレットPC又はかんぽPC（事務）））に入力を行うこととして手続に定め、特定個人情報の写しを作成することはない。 2. かんぽ生命支店等渉外社員及び郵便局社員 個人番号の取得に際しては、個人番号カードの提示に基づき携帯端末機（インターネット機能や外部メール機能がない専用端末機（PT5））に入力を行うこととして手続に定めており、特定個人情報の写しを作成することはない。 3. お客さまによる個人番号のオンライン申告 個人番号取得の委託に際して、公的個人認証サービスを提供するプラットフォーム事業者を選定しているほか、業務用携帯電話（スマートフォン）又はポスタルタブレットPCを使用する場合に備え、業務用携帯電話にはキャッシュの自動削除、スクリーンショット不可の制限をかけており、特定個人情報を保存することはない。また、認証アプリは、マイナンバーカードから読み取った情報をサーバへデータ連携する仕組みであり、マイナンバーカードから読み取った情報をスマートフォン又はポスタルタブレットPC内に保管することはない。 4. かんぽ生命契約サービス部 個人番号の入力に際しては、個人番号カード等の写しに基づき端末機（インターネット機能やメール機能がない専用端末機）に入力を行うこととし、入力後の個人番号等の確認書類の写しについては廃棄をする。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 入手した特定個人情報 that 不正確であるリスク		
入手の際の本人確認の措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の記載のある通知カード、個人番号カード又は住民票の写しの提示を受け、個人番号を確認するほか、実存(本人)確認を行う。 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 公的個人認証サービスを利用した実存(本人)確認を行う。 4. かんぽ生命契約サービス部 個人番号の記載のある通知カードの写し、個人番号カードの写し又は住民票の写しにより、個人番号を確認するほか、実存(本人)確認を行う。	
個人番号の真正性確認の措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の記載のある通知カード、個人番号カード又は住民票の写しの提示を受け、提示を行っている方が本人であることを確認する。 また、入力時にはチェックディジット(※)による誤入力の防止の措置を取っている。 ※…末尾以外の数字を基にある数式で算出した値と末尾の数字を比較し、番号の入力誤りを検出する方式 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 公的個人認証サービスを利用した実存(本人)確認を行うことから、特定個人情報の正確性について確保されている。特定個人情報の取得はマイナンバーカードのICチップを読み取る方法で行うため、誤入力は発生しない。また、認証アプリは委託先PF事業者サーバにかんぽ生命サーバからの電文を正しく受領し、復号できたことをもって起動する仕様であるため、偽造された二次元コードがかんぽ生命以外のサーバからの電文である場合は、委託先PF事業者側で不正電文と検知している。 4. かんぽ生命契約サービス部 個人番号の記載のある通知カードの写し、個人番号カードの写し又は住民票の写しにより、個人番号を確認するほか、実存(本人)確認を行う。	
特定個人情報の正確性確保の措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 保険契約の取扱いにおいて、保険金等支払請求等の際、請求人が正当な権利を有している者であることの確認を行うことが前提であることから、特定個人情報の正確性について確保されている。 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 公的個人認証サービスを利用した実存(本人)確認を行うことから、特定個人情報の正確性について確保されている。特定個人情報の取得はマイナンバーカードのICチップを読み取る方法で行うため、誤入力は発生しない。 4. かんぽ生命契約サービス部 1、2と同様。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク		
リスクに対する措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 ・特定個人情報について控え及び写しを作成しないこととしているほか、端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))は紙媒体への出力機能を有しているが、個人番号が記録されたデータについては紙媒体で出力できないようシステムで制御している。おって、マイナンバーの取扱いに関して、各種法令等に従いマイナンバーの保護に十分な注意を払うこと及び各種法令などに違反している事実又はその兆候を把握した場合には、速やかに報告することを社内規定に定めている。 なお、携帯端末機(PT5)は紙媒体を出力する機能を有していない。 ・かんぽ総合情報システム(個人番号等管理マスタ)からのデータのダウンロードや電子記録媒体への出力もできないように措置している。 2. かんぽ生命支店等渉外社員及び郵便局社員 同上。 3. お客さまによる個人番号のオンライン申告 ・業務用携帯電話(スマートフォン)又はポスタルタブレットPCを使用する場合に備え、業務用携帯電話にはキャッシュの自動削除、スクリーンショット不可の制限をかけており、特定個人情報を保存することはない。また、認証アプリは、マイナンバーカードから読み取った情報をサーバへデータ連携する仕組みであり、マイナンバーカードから読み取った情報をスマートフォン又はポスタルタブレットPC内に保管することはない。 4. かんぽ生命契約サービス部 1、2と同様。	
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		
端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))又は携帯端末機(PT5)とかんぽ総合情報システム間においては特定個人情報に暗号化を施すとともに、日本郵便及びかんぽ生命でセキュリティ基盤(Prisma Access)を構築の上、PNETの既存設備を有効活用することで、セキュアなネットワークを使用している。 特に、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)は、外部サービスのクラウド上でWEBサイトにアクセスするため、万が一マルウェアが仕掛けられたWEBサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。また、許可されたWEBサイト以外からのファイルのダウンロード・アップロードの制限を行うことで、マルウェアに感染し情報が漏えいするリスクを低減している。さらに、即時の検知や防御、ネットワーク遮断等の対応を行うEDR(エンドポイントディテクション&レスポンス)の導入と、EDRで検知したインシデント発生時の初動対応、影響調査、結果報告までをサポートするMDR(マネージド・ディテクション&レスポンス)サービスの運用により、標的型攻撃やランサムウェアの脅威に対応している。 また、外部メールの送信は、必ず管理者をCCに入れなければ送信できない仕組みや、送信時の添付ファイルは自動的に暗号化され、外部メールからの受信時には添付ファイルの検疫・無害化が行われている。 公的個人認証サービスを提供するプラットフォーム事業者を委託PF事業者として選定しているほか、委託PF事業者とかんぽ生命間においては、特定個人情報に暗号化を施すとともに、通信については専用線を敷設し、セキュアな環境でデータを入手している。 ポスタルタブレットPC及びかんぽPC(事務)については、ログオン時またはシャットダウン時に端末機内のローカルデータが自動削除される。加えて、かんぽPC(事務)については、シャットダウン未実施によるローカルデータ残留対策として、一定期間端末機を操作しなかった場合には、自動でシャットダウンされる仕組みとしている。		

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号等管理マスタについては、個人番号を取り扱う支払調書データ作成事務において辞令簿等により指定を受けた者のみがアクセス権を有しており、地方公共団体の宛名システムに相当するような複数の事務で個人番号を共通して参照するシステムは存在しない。 そのため、個人番号等管理マスタを閲覧することができない社員による、生命保険業務の他の情報との個人番号を介した紐付けは発生しない。	
事務で使用するその他のシステムにおける措置の内容	同上	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・ユーザIDに必要最低限の権限を付与し、事務処理上必要のないデータへのアクセスを制限している。 ・職員が離席する際には、パスワード設定された画面ロックを利用するなど、情報漏えい、なりすまし等の不正行為を防止する措置を講じている。	
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	異動等の事由が生じたことにより、不要となったユーザIDについては、ユーザID管理者が失効等の処理を行っている。	
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない	
具体的な管理方法	・ユーザごとにIDを発行している。 ・パスワードは、定期的に更新を実施するようシステムで制御している。 ・異動等の事由が生じたことにより、不要となったユーザIDについては、ユーザID管理者が失効等の処理を行っている。 ・委託PF事業者が個人番号をその内容に含む電子データを取り扱うことはできないように、管理業務に必要なデータベースのアクセス権限は付与していない。 ・認定クラウド事業者及び認定クラウドの運用管理者において、Firewall によるアクセス制限、WEBアプリケーションの脆弱性攻撃遮断、侵入検知システムによる運用監視・アクセス記録といった仕組みにより、権限の無い者の不正利用・アクセスを防止を行っている。 ・認定クラウドの運用管理者がゲートウェイ経由で本番環境にアクセスした場合には、ゲートウェイにおいてアクセス履歴(ログオン情報)が記録されることにより、不正ユーザによる情報閲覧などのアクセスを追跡している。	
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	個人番号等管理マスタにアクセスした記録については、ジャーナルに出力されることから、ジャーナル監査により不正なアクセス等がないか確認するとともに、必要に応じてジャーナルを分析する。	
その他の措置の内容	かんぽ総合情報システムの個人番号等管理マスタに個人番号を登録するための端末機は、かんぽ総合情報システム上で「特定個人ファイル(支払調書)」に含まれる個人番号を検索・閲覧・取得する機能を有していない。	
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: 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	機構とかんぽ生命における委託契約書の中で、顧客の保険契約に係る情報については契約の遂行以外の目的に使用しない旨を約定しており、かんぽ生命の関連マニュアル等においても同様の明記を行って、社員への研修・指導の措置を講じている。 また、かんぽ生命及び日本郵便への番号法施行に伴う対応に係る研修資料において、個人番号の目的外の利用禁止、複写及びメモの禁止等を明記して社員への周知・指導を徹底する。 年金受取人から提出(郵送)された個人番号等届出書に基づき個人番号を入力する場合は、管理者等から許可を取った上で入退室管理を行っているセキュリティを設けた部屋で行う。 支払調書データの複製を行う場合は、管理者等から許可を取った上で入退室管理を行っているセキュリティを設けた部屋で行う。なお、複製を行えるパソコンのIDは担当者1名にのみ付与し、限定している。また、複製を行う際には立会者を設けて行っている。	
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	・個人番号等管理マスタに関するアクセス権については、ユーザIDが払い出され、辞令簿により指定を受けた者のみ有しており、特定個人情報等の取扱いに関する留意事項等について、定期的な研修等を行う。 ・開発担当者のファイルアクセスは不可としているため複製は不可能。 ・かんぽ総合情報システムはインターネットと分離されており、不正アクセスやウイルスによって情報を抜き取られることはない。また、電子媒体作成時においても暗号化を施しており、使用部署に限り郵送している。 ・端末機(CTM)はインターネット機能やメール機能がなく、端末上に特定個人番号を保管していないため、盗難、紛失、詐取された場合でも不正に複製されることはない。 ・端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))は、インターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じており、また、端末上に特定個人番号を保管していないため、盗難、紛失、詐取された場合でも不正に複製されることはない。 ・携帯端末機(PT5)については、USBポートがあるが、電子記録媒体への書き込みができないようシステムで制限をかけている。 ・携帯端末機(PT5)については、複数の要素(IDとPW、IDと生体認証(顔認証))によるログイン承認を行っており、ログインできなければ、かんぽ総合情報システムへ接続できない。また、携帯端末機の通信不可とすることも可能で、通信を不可とすればかんぽ総合情報システムへ接続できない。 ・端末機のうち、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)では、ローカルディスクにデータを保存することが可能であるが、『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』に記載されている措置をとっている。 ・端末機のうち、かんぽPC(事務)では、光学式ドライブからのデータ書き込みは、申請により許可された社員のみ制限されており、マイナンバーカード登録業務を行う拠点に設置するかんぽPC(事務)では、光学式ドライブを配備しない。また、USBドライブからのデータ書き込みは、申請により許可された社員、端末、およびUSB機器のみに制限されている。 ・端末機のうち、JP-PC(3001)又はポスタルタブレットPCでは、光学式ドライブからのデータ書き込み及び、USBドライブからのデータ書き込みは行えないように制限されている。 ・業務用携帯電話(スマートフォン)を使用する場合に備え、業務用携帯電話にはキャッシュの自動削除、スクリーンショット不可の制限をかけている。 ・専用端末(スタンドアロン、閉域網通信用)は、管理者の許可を得た者のみしか入退室出来ないようICカードによる入退室チェック機能による施錠管理(入退室時にICカードをかざし、暗証番号を入力しないと入退室出来ない仕組み)が措置されたセキュリティルームに設置されており、専用端末を利用するためのアカウントは特定の担当者のみに限定して付与されている。複製を行う際には必ず立会者を設けて実施するようにするとともに、専用端末の使用履歴のログは管理者により定期的(3か月毎)に監査を行うこととしている。また、セキュリティを設けた部屋には監視カメラを設置しており、専用端末の使用履歴に不正使用の疑いがある場合は、監視カメラの映像をチェックするようにしている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
—		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	機構とかんぽ生命における委託契約書の中で、「守秘義務」及び「顧客情報の管理」等に関する事項を約定し、機構はかんぽ生命に対して、簡易生命保険管理業務の実施を適正かつ円滑に行うことを目的として、「個人情報保護管理体制」を確認できるよう関連規程類等の提出を求め、必要な措置が講じられていることを確認している。 また、これらの状況について、委託先であるかんぽ生命及び再委託先である日本郵便を対象として、特定個人情報の取扱いを含めた委託業務の実施状況を監査するとともに、必要な場合にはかんぽ生命の外部委託先に対しても機構が直接実地での監査を行うことができるように措置している。 かんぽ生命は、個人データの安全管理を図るための内部管理体制として、会社全体の個人情報の保護に関する事務を統括する個人情報保護統括責任者のほか、各部署に個人情報の保護に関する事務を管理する者を配置し、個人情報の適切な保護と取り扱いを行っている。	
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	かんぽ生命契約サービス部の一部の社員のみ閲覧権限を与える。	
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	特定個人情報の取扱いの記録について、プログラム処理にて毎日自動で抽出し、確認する運用としている。	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルール内容及びルール遵守の確認方法	・特定個人情報が含まれている支払調書データの電子媒体においては媒体管理簿へ「データ内容」、「利用目的」、「作成年月日」、「移送日」、「移送先」、「担当者名」等を記載している。 ・送付を行う際は、「送付先」、「関係書類」等を複数人で点検・確認し、封入・封緘を行っている。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	
委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	支払調書データの作成事務に関して、委託元と委託先間の提供は行わない。	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルール内容及びルール遵守の確認方法	【かんぽ総合情報システム(個人番号等管理マスタ)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管し、保管期間経過後システムの的に削除する。 【かんぽ総合情報システム(保険金等の支払データ)】 次回の保険金等の支払データ作成時に自動的に消去される。(最大1か月間保持) 【支払調書データ(副本)(電子媒体)】 ・媒体管理簿に記載された「保存期間」が経過したものについて、速やかに廃棄を行う。 ・電子記録媒体の廃棄方法は、管理者等が当該データが不用となった情報であること、媒体数等を確認し、物理的に復元不能な状態にして廃棄する。廃棄にあたっては事前に情報セキュリティ統括室に廃棄申請を行い、許可を受けた上で実施。廃棄後は電子記録媒体管理簿に廃棄の旨を記録している。	

委託契約書中の特定個人情報ファイルの取扱いに関する規定		[定めている] <選択肢> 1) 定めている 2) 定めていない	
	規定の内容	かんぽ生命との業務委託契約書等において、次の事項を規定する。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告を求める ・委託先に対しての実地の調査 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ない 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	【日本郵便】 かんぽ生命と日本郵便との間において、特定個人情報ファイルの適切な取扱いについて、以下の事項を確保する。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・再委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告を求める ・委託先に対しての実地の調査 【その他】 かんぽ生命と外部委託先との間において、再委託を行う場合には特定個人情報ファイルの適切な取扱いについて、以下の事項を確保する。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・再委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告を求める ・委託先に対しての実地の調査 その他、「特定個人情報の適正な取扱いに関するガイドライン」等で求められている必要かつ適切な安全管理措置を講ずることを義務付けている。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置			
—			

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[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	・特定個人情報が含まれている支払調書データの電子媒体においては媒体管理簿へ「データ内容」、「利用目的」、「作成年月日」、「移送日」、「移送先」、「担当者名」等を記載している。 ・媒体管理簿においては、管理者が月に1回以上点検・確認を行っている。 ・媒体管理簿の保存期間は翌年度始から1年間保存としている。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	税務署への電子媒体での搬送に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末（スタンドアロン）にて管理し、セキュリティ確保のため、暗号化した上で専用回線（閉塞網）を用いて、認定クラウド（e-私書箱（法定調書提出クラウドサービス））へデータ連携（ファイル連携）する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末（スタンドアロン）にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	税務署への電子媒体での搬送に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末（スタンドアロン）にて管理し、セキュリティ確保のため、暗号化した上で専用回線（閉塞網）を用いて、認定クラウド（e-私書箱（法定調書提出クラウドサービス））へデータ連携（ファイル連携）する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末（スタンドアロン）にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	
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: 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	支払調書のデータの搬送に当たっては、かんぽ生命契約サービス部において「送付先」、「関係書類」等を複数人で確認し、送付している。 また、データにおいては暗号化及び搬送容器の施錠を行い、開錠及び復号化するパスワードは別途通知する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、セキュリティ確保のため、暗号化した上で専用回線(閉塞網)を用いて、認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携(ファイル連携)する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。
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			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク4: 入手の際に特定個人情報漏えい・紛失するリスク			
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 3) 課題が残されている	2) 十分である
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			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク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			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク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			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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			

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
		【かんぽ総合情報システム(個人番号等管理マスタ)】、【かんぽ総合情報システム(保険金等の支払データ)】 ・かんぽ生命情報管理センターでは、あらかじめ設置されている端末機又は持ち込みを許可された電子記録媒体を除き、機器等の持ち込みを禁止している。また、電子記録媒体については、電子記録媒体授受簿により管理を行っている。 ・個人番号等管理マスタはセキュリティゲートを設けて入退室を行っている建物(かんぽ生命情報管理センター)で管理している。また、入退室管理を行っている部屋に設置したメインフレームに個別のマスタファイルとして保管している。 ・インターネットと分離されており、不正アクセスやウイルスによって情報を抜き取られることはない。 ・支払調書データを作成しCD等の電子記録媒体に出力する際には情報管理センターにおいて暗号化を施しており、電子媒体とパスワードについては、別々にかんぽ生命情報管理センターからかんぽ生命契約サービス部へ送付される。 ・年金受取人から提出(郵送)された個人番号等届出書に基づき個人番号を入力する場合は、管理者等から許可を取った上で入退室管理を行っているセキュリティを設けた部屋で行う。 ・支払調書データの複製を行う場合は、管理者等から許可を取った上で入退室管理を行っているセキュリティを設けた部屋で行う。なお、複製を行えるパソコンのIDは担当者1名にのみ付与し、限定している。また、複製を行う際には立会者を設けて行っている。 【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 ・個人番号は紙媒体で取得・保管を行わない。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))は施錠された執務室内に設置されている。 ・端末機(JP-PC(3001))は、ワイヤーチェーンによる施錠を施す。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))に特定個人情報は保管しないよう社内規定に定め運用する措置を取っている。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))は、社員証または社員番号および社員個人が設定したパスワードを入力しなければ、ログインができない。 ・お客さまから提示を受けた個人番号が記載された証明書類は、登録が完了次第速やかにお客さまへ返却する。 ・端末機(ポスタルタブレットPC又はかんぽPC(事務))を使用した在宅勤務時に、個人番号の取扱いが必要となる業務は行わない。 2. かんぽ生命支店等渉外社員及び郵便局社員 ・個人番号は紙媒体で取得・保管を行わない。

	具体的な対策の内容	・お客さまから提示を受けた個人番号が記載された証明書類は、登録が完了次第速やかにお客さまへ返却する。 ・携帯端末機(PT5)は端末に特定個人情報情報は保管しない。 3. お客さまによる個人番号のオンライン申告 ・業務用携帯電話及びポスタルタブレットPCに特定個人情報情報は保管しない。 ・委託PF事業者のサーバに一時保管される個人番号のうちかんぽ総合情報システムへの登録が完了したものは、かんぽ生命から送信する「削除対象番号を示すキー情報と削除指示」のファイルに基づき、一時保管された日付の翌営業日中に消去する。 4. かんぽ生命契約サービス部 ・お客さまから返信を受けた個人番号等確認書類の写し及び実存(本人)確認書類の写しについては、個人番号の入力確認後速やかに廃棄する。 ・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともにログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。 【支払調書データ(副本)(電子媒体)】 ・支払調書データについて電子記録媒体管理簿に登録し、施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。 ・支払調書データは管理者が当該データが不要となった情報であること、媒体数等を確認・点検し、物理的に復元不能な状態にして廃棄する。 ・廃棄に当たっては事前にかんぽ生命情報セキュリティ統括室に廃棄申請を行い、許可を受けた上で実施する。廃棄後は電子記録媒体管理簿に廃棄の旨を記録する。 【管理区域への持込機器の制限】 かんぽ生命契約サービス部のセキュリティルームには、あらかじめ設置されている端末機又は持ち込みを許可された電子記録媒体を除き、機器等の持込みを禁止している。また、電子記録媒体については、電子記録媒体授受簿により管理を行っている。 【端末機及び記憶媒体の廃棄と記録の保管】 不要となった端末機及び記憶媒体を廃棄する場合、データの読み出しができないように物理的に破壊し、その記録を保管している。廃棄を委託する場合、データの読み出しができないように物理的に破壊する場に職員は立ち合い、委託先からは廃棄証明書を提出させ、記録を保管している。
--	------------------	---

⑥技術的対策	十分にしている <選択肢> 1) 特に力を入れてしている 2) 十分にしている 3) 十分にしていない
具体的な対策の内容	【かんぽ総合情報システム(個人番号等管理マスタ)】 ・個人番号等管理マスタは個別のマスタファイルとして暗号化とアクセス制限を施している。 【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC)は、社員証の利用および社員個人が設定したパスワードの入力または社員番号および社員個人が設定したパスワードの入力がログインのために必要。かんぽPC(事務)は、社員証の利用および社員個人が設定したパスワードの入力、社員番号および社員個人が設定したパスワードの入力、または生体認証がログインのために必要。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))に特定個人情報を入力した場合は暗号化を即時に行った上でセンター側に送信し、端末内部には情報を残さないようにしている。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))とかんぽ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。 ・端末機(CTM)はインターネット機能やメール機能がない業務専用の端末機である。 ・端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))はインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機である。 ・JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)は、外部サービスのクラウド上でWebサイトにアクセスするため、万が一マルウェアが仕掛けられたWebサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。また、許可されたWebサイト以外からのファイルのダウンロード・アップロードの制限を行うことで、マルウェアに感染し情報が漏えいするリスクを低減している。さらに、即時の検知や防御、ネットワーク遮断等の対応を行うEDR(エンドポイントディテクション&レスポンス)の導入と、EDRで検知したインシデント発生時の初動対応、影響調査、結果報告までをサポートするMDR(マネージド・ディテクション&レスポンス)サービスの運用により、標的型攻撃やランサムウェアの脅威に対応している。また、外部メールの送信は、必ず管理者をCCに入れなければ送信できない仕組みや、送信時の添付ファイルは自動的に暗号化され、外部メールからの受信時には添付ファイルの検疫・無害化が行われている。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))は、かんぽ総合情報システムでマイナンバーを参照・検索できない。 ・端末機(ポスタルタブレットPC又はかんぽPC(事務))を使用した在宅勤務時に、個人番号の取扱いが必要となる業務は行わない。 ・ポスタルタブレットPC及びかんぽPC(事務)については、ログオン時またはシャットダウン時に端末機内のローカルデータが自動削除される。加えて、かんぽPC(事務)については、シャットダウン未実施によるローカルデータ残留対策として、一定期間端末機を操作しなかった場合には、自動でシャットダウンされる仕組みとしているほか、ポスタルタブレットPCにはリモートワイプ(遠隔消去)機能を搭載している。 ・かんぽPC(事務)、ポスタルタブレットPCは在宅環境からの接続を考慮し、セキュリティフレームワークとして「SASE」を導入し、セキュリティ機能の強化を図っている。 2. かんぽ生命支店等渉外社員及び郵便局社員 ・携帯端末機(PT5)については、複数の要素(IDとPW、IDと生体認証(顔認証))によるログイン承認を行っており、ログインできなければ、かんぽ総合情報システムへ接続できない。 ・携帯端末機(PT5)に特定個人情報を入力した場合は即時に暗号化を行っている。 ・携帯端末機(PT5)とかんぽ総合情報システム間は携帯電話網を使用した暗号化及びセキュアな通信を行っており、安全性が確保されている。 ・携帯端末機はインターネット機能や外部メール機能がない業務専用の端末機である。 ・携帯端末機(PT5)は、特定個人情報を保管しない。 ・携帯端末機(PT5)は、シャットダウン時に携帯端末機(PT5)内のローカルデータを自動削除する仕様としている。業務終了時には携帯端末機(PT5)をシャットダウンする運用としており、万が一シャットダウンしなかった場合でも、携帯端末機(PT5)が無操作状態で8時間経過した場合は自動でシャットダウンする仕組みとしている。 3. お客さまによる個人番号のオンライン申告 業務用携帯電話(スマートフォン)を使用する場合に備え、業務用携帯電話にはキャッシュの自動削

		除、スクリーンショット不可の制限をかけている。また、リモートロック、リモートワイプ(遠隔消去)、回線停止が可能。 なお、ポスタルタブレットPCについては、前1と同様。 4. かんぽ生命契約サービス部 ・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともにログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。 【税務署に関する対応】 1. 税務署への支払調書データ作成 媒体変換装置に連携された媒体作成の基データは、媒体出力後、翌日のシステム(媒体変換装置)立ち上げ時に消去。 2. 税務署からの支払調書データに関する照会への対応 かんぽ生命の契約サービス部等のうち、支払調書の照会対応等の業務に携わる一部の社員にのみ、個人番号の照会閲覧の権限を付与しており、端末機へのログイン時には正当なIDとPWが必要。
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	死者の個人番号は、生存する個人の個人番号と分けて管理しないため、「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」における生存する個人の個人番号と同様の管理を行う。
その他の措置の内容		セキュリティ対策に関する政府の方針である「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」の内容を踏まえて、情報セキュリティ管理規程等の見直しを実施し、機構における情報セキュリティ対策の強化を行っている。 また、機構は、かんぽ生命が調達した仕様書において、 ・総務大臣が認定する「署名検証者プラットフォーム事業者」であることが入札参加要件とされていること、 ・委託事業者の選定の際には、各認定で求められる情報の保管・消去の要件を委託業務全体に適用して満たすことを要求されていること、 ・委託事業者よりサービス水準定義書を取得し内容を確認していること、 を確認し、物理的対策及び技術的対策を図っている。 なお、各種認定名は以下のとおり。 ・情報セキュリティのマネジメントに関する国際認証ISO27001,ISO27017 ・米国公認会計士(AICPA)が定める内部統制の有効性に関する保証報告書SOC2(Service Organization Controls 2) ・FISC による『金融機関等コンピューターシステムの安全対策基準』と日本データセンター協会(JDCC)の定める「データセンターファシリティスタンダード」におけるもっとも厳しい基準であるTier4に準拠したデータセンターにて運用(東京第一データセンタ) ・ISAE3000(非財務情報を保証対象とする国際監査基準)に則った監査統制
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	【かんぽ総合情報システム(個人番号等管理マスタ)】 (別添1)の4つの入手経路により、個人番号の変更があった場合は、変更後の個人番号を登録する。 【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 保険金等の支払請求等のために窓口に来られたお客さまに、個人番号の変更がないか確認を行い、変更があった場合は、変更後の個人番号の提示を受け、端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 2. かんぽ生命支店等渉外社員及び郵便局社員 保険金等の支払請求等の手続きのためにお客さま宅を訪問し、個人番号の変更がないか確認を行い、変更があった場合は、変更後の個人番号の提示を受け、携帯端末機(PT5)に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。 3. お客さまによる個人番号のオンライン申告 1、2と同じ。 また、簡易生命保険契約に係る契約者がマイページを介して、随時、登録時と同様の手法で変更後の個人番号の申告が可能。 4. かんぽ生命契約サービス部 お客さまから個人番号等届出書の郵送回答を受けた個人番号を最新のものとして、端末機に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。	
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	【かんぽ総合情報システム(個人番号等管理マスタ)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管し、保管期間経過後系統的に削除する。 【かんぽ総合情報システム(保険金等の支払データ)】 次の保険金等の支払データ作成時に自動的に消去される。(最大1か月間保持) 【支払調書データ(副本)(電子媒体)】 ・支払調書の控えについては、媒体管理簿に記載された「保存期間」が経過したものについて、速やかに廃棄を行う。 ・電子記録媒体の廃棄方法は、管理者等が当該データが不用となった情報であること、媒体数等を確認し、物理的に復元不能な状態にして廃棄する。廃棄にあたっては事前に情報セキュリティ統括室に廃棄申請を行い、許可を受けた上で実施。廃棄後は電子記録媒体管理簿に廃棄の旨を記録している。 【委託PF事業者のサーバに一時保管される個人番号】 ・かんぽ総合情報システムへの登録が完了した個人番号データは、かんぽ生命から送信する「削除対象番号を示すキー情報と削除指示」のファイルに基づき、一時保管された日付の翌営業日中に消去する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置

個人情報等が漏えいした場合の対策として、機構は、独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針（平成16年9月14日付け総管情第85号）等に基づき策定した機構個人情報管理規程等を遵守して対応することとしている。

- ① 総括保護管理者及び保護管理者への報告
- ② 総務省等への報告
- ③ 報告書の作成
- ④ 再発防止策の策定

また、かんぽ生命において個人情報等が漏えいした場合には、機構はかんぽ生命からの報告に基づき上記対応を行うこととしている。

かんぽ生命において特定個人情報等が漏えいした場合は、以下の対応を行うこととしている。

- ① コンプライアンス統括部長及び情報セキュリティ統括室長への報告
- ② 事実関係の調査及び原因の究明
- ③ 影響を受ける可能性のある本人への連絡
- ④ 事実関係及び再発防止策等の公表の判断
- ⑤ 社内関係者への報告
- ⑥ 監督官庁等への報告
- ⑦ 再発防止策の策定及び有効性の検証

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	機構は、特定個人情報を取得すること及び提供を受けることはなく、また、特定個人情報ファイルも保有していないことから、自己点検は行えないため、かんぽ生命における自己点検の状況を以下に記述する。 かんぽ生命支店等において、四半期ごとに、個人情報保護に係る項目（社外への情報漏えいの防止状況、個人情報の残留点検簿の実施状況等）について、自己点検を実施している。 かんぽ生命本社各部署には、コンプライアンス統括部（情報セキュリティ統括室）が年に1度、個人情報保護・情報セキュリティに係る項目（電子記録媒体管理簿及び授受簿による媒体の管理状況、残留点検の実施状況等）について、モニタリングを実施している。点検の結果、発見された事項は、当該発生拠点から発生原因、改善状況、再発防止策の報告を求め、情報セキュリティ統括室等でその内容の確認及びフォローアップモニタリングを行っている。	
②監査	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な内容	年度当初に機構からかんぽ生命あて監督方針を通知し、委託先であるかんぽ生命及び再委託先である日本郵便を対象として、特定個人情報の取扱いを含めた委託業務の実施状況を監査するとともに、不適正事例が発生した場合には、その発生原因等を分析し、必要に応じて一層の再発防止策を講じるよう指導するなど、改善に向けた取組強化及び改善状況の検証を行う。 また、必要な場合にはかんぽ生命の外部委託先に対しても機構が直接実地での監査を行うことができるように措置している。 かんぽ生命支店等及び郵便局に対して年度を通じて監査を行い、その監査結果を用いて、かんぽ生命本社及び日本郵便本社への監査を行う。 なお、監督方針には、重点確認項目として顧客情報の管理を設定している。 かんぽ生命においては、内部監査部が、本社各部、エリア本部及び支店並びに、日本郵便の本社、支社及び郵便局を対象として、個人情報の管理方法等について定めた規程の遵守状況等について、定期的に監査を実施する。監査における指摘事項については、是正及び改善措置状況の定期的なフォローアップ時又は次回の監査時に改善状況を確認している。	
2. 従業員に対する教育・啓発		
従業員に対する教育・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	【かんぽ生命】 委託先であるかんぽ生命では、個人情報の適正な管理を行うため、個人情報保護・情報セキュリティマニュアル等を策定しており、そのマニュアル等に基づく年度計画により定期的に研修・点検等を実施している。また、全社員に周知しているコンプライアンス・ハンドブックにも顧客情報保護の項目を掲げ、日頃の研修・指導時に活用している。なお、情報漏えい等を行った場合、懲戒処分及び刑事罰の対象となることをマニュアル等に明記している。 特定個人情報の取扱い、漏えい等発生時の対応等については、個人情報保護等に関する取扱規程及び各取扱手続等に定め、研修等において教育・訓練を行っている。 かんぽ生命においては、全社員を対象に実施している個人情報保護等を含むコンプライアンスに関するeラーニング研修で、実施期間中に数回実施状況を管理者に連携し、管理者等から受講を促すよう指導・周知を行い、受講率が100%になる取り組みを行っている。 【日本郵便】 再委託先である日本郵便では、個人情報の適正な管理を行うため、採用時の教育及び定期的な教育・訓練、個人データ管理責任者等への教育・訓練、個人データの安全管理に関する取扱規程に違反した場合の懲戒処分の周知など社員に対し安全管理措置の周知徹底、教育及び訓練を行っている。 特定個人情報の取扱い、漏えい等発生時の対応等については、個人情報保護等に関する取扱規程及び各取扱手続等に定め、研修等において教育・訓練を行っている。 日本郵便においては、個人情報保護等を含むコンプライアンスに関する研修の欠席者に対して、別途、同様の研修を実施することとし、欠席者へのフォローアップを行っている。	
3. その他のリスク対策		
機構においては、特定個人情報の取扱いを含めた委託業務の実施状況を監査するとともに、不適正事例が発生した場合には、その発生原因等を分析し、必要に応じて一層の再発防止策を講じるよう指導するなど、改善に向けた取組強化及び改善状況の検証を行っている。その結果は担当の理事を議長、担当の部長を構成員とする管理業務推進会議において各種の課題・問題を分析、把握し、理事長に報告することとしている。		

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒105-0001 東京都港区虎ノ門5-13-1 虎ノ門40MTビル3階 独立行政法人郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構 総務部総務課 情報公開窓口 電話 03(5472)7101 ※郵送の場合の宛先についても同上
②請求方法	指定様式(下記URLを参照)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。 (https://www.yuchokampo.go.jp/disclosure/index.html)
特記事項	機構ホームページ上に、請求先、請求方法、諸費用等について掲載する。
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 開示請求手数料は法人文書(1契約ごと)ごとに300円。納付方法は「情 (手数料額、納付方法: 報公開窓口)で直接、現金で納付するか、郵送にて普通為替証書又は) 定額小為替証書で納付
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	簡易保険契約原簿ファイル、債権差押命令ファイル、不祥事故関連ファイル
公表場所	機構ホームページ(下記URLを参照) (https://www.yuchokampo.go.jp/disclosure/file.html)
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	〒105-0001 東京都港区虎ノ門5-13-1 虎ノ門40MTビル3階 独立行政法人郵便貯金簡易生命管理・郵便局ネットワーク支援機構 総務部総務課 情報公開窓口 電話 03(5472)7101
②対応方法	・開示請求に対する決定は、原則として30日以内に行われる。 ・開示は、文書等の閲覧、写しの交付により実施される。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和7年9月26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	評価実施機関ホームページ
②実施日・期間	令和7年9月26日から令和7年10月27日までの32日間
③期間を短縮する特段の理由	期間短縮なし
④主な意見の内容	なし
⑤評価書への反映	—
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7年11月5日
②個人情報保護委員会による審査	

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	I基本情報 ②事務の内容	2.かんぽ生命契約サービス部 ・支払調書データ(電子媒体)を税務署へ提出する。	2.かんぽ生命契約サービス部 ・支払調書については、以下の方法で税務署へ提出する ①「法定調書提出クラウドサービス」※を利用した提出 国税庁が定めるクラウド提出に必要な要件を満たした支払調書データ(当年分を含む過去4年分) ② 電子媒体による郵送での提出 上記①以外の支払調書データ ※「法定調書提出クラウドサービス」は国税庁長官の認定を受けたクラウドサービスであり、提供事業者が国税庁長官の認定を受けるためには、認定の対象となるクラウドサービス又はオンプレミスが、政府情報システムのためのセキュリティ評価制度(ISMAP)のクラウドサービスリストに掲載されていること、提供事業者及び利用者各々の立場から安全管理措置を講じられていること、サーバが日本国内に所在していることなど、国税庁告示で定める要件に適合することが必要となる。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	I基本情報 システム2 ①システムの名称 ②システムの機能 ③他のシステムとの接続	記載なし(追加)	①e-私書箱 ②野村総合研究所で開発した企業の電子的なお知らせを個人に届けるクラウドサービスである。デジタル庁のマイナポータルや国税庁のe-Tax等の行政手続システムと連携することで、行政手続の電子化を実現するもの。支払調書における「法定調書提出クラウドサービス」は2022年1月に国税庁長官の認定を受けている。 ③その他[○](他のシステムとの接続はない)	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	I基本情報 4. 特定個人情報ファイルを取り扱う理由 ②実現が期待されるメリット	記載なし(追加)	・法定調書提出クラウドサービスを利用することで専用回線(閉域網)での連携が可能になる。 ・マイナポータル連携サービスを利用することで、お客さまへの確定申告書情報の連携が可能となり、お客さまがe-TAXでの確定申告時に確定申告書情報が自動で連携される機能を用いることによってお客さまの負担が軽減する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	(別添1)事務の内容 【Ⅱ.特定個人情報ファイルを使用する事務】 2.かんぽ生命契約サービス部	・支払調書データ(電子媒体)を税務署へ提出する。 ※フロー図についても支払調書データ(電子媒体)を税務署へ提出するように記載している。	・支払調書データを電子媒体により郵送する方法及び認定クラウドを利用する方法で税務署へ提出する。 ※フロー図を認定クラウドを使用して提出するフローも追加して変更しています。	事前	法定調書のクラウド提出に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	(別添1) 事務の内容 【Ⅱ. 特定個人情報ファイルを使用する事務】 2. かんぽ生命契約サービス部(事務の流れ)	⑥ かんぽ生命契約サービス部から税務署へ支払調書データを提出する。	⑥ かんぽ生命契約サービス部から以下の方法で税務署へ支払調書データを税務署へ提出する。 ・電子媒体による郵送での提出 ・認定クラウドを利用した提出 ⑦ 税務署は上記の方法で提出された支払調書データの閲覧および記録を行い、郵送でも受領する。 ⑧ お客さまがマイナポータル上で確定申告書情報の連携を選択すると、支払調書データが連携され(※)、お客さまが確定申告(e-Tax)を行う際に、確定申告書に必要な情報が自動で連携される。 ※ かんぽ生命が認定クラウドでの提出を行った契約のうちマイナンバーをご登録いただいているお客さまのみが対象。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 3. 特定個人情報の入手・使用 ⑧ 使用方法	・個人番号等管理マスタに登録された個人番号を保険金等の支払データに付加して、CD等の記録媒体を用いて税務署に提出する。	・個人番号等管理マスタに登録された個人番号を保険金等の支払データに付加した支払調書データを暗号化し、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、専用回線(閉塞網)を介して認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携する(暗号化を行う通信方式を用いてデータ連携を行う)ことで税務署に提出する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) ⑧ 提供方法	記載なし(追加)	[○] 専用線	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ① 保管場所	1と同様。	・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともに、ログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。 5. 認定クラウド(法定調書提出クラウドサービス) 国税庁告示で定める要件に適合することにつき、クラウドサービス事業者等が国税庁長官の認定を受けているクラウドサービス	事前	法定調書のクラウド提出に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ① 保管場所	【支払調書データ(副本)(電子媒体)】 ・施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。	【支払調書データ(副本)(電子媒体)】 ・支払調書データについては、電子記録媒体管理簿に登記し、施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ② 保管期間	1と同様。	・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともに、ログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ② 保管期間	【支払調書データ(副本)(電子媒体)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管することとする。	【支払調書データ(副本)(電子媒体)】 税務における更正決定等の期間制限に鑑みて、支払調書データを税務署に提出した翌年度始から7年間保管することとする。 ・支払調書データについては、電子記録媒体管理簿に登記し、施錠できるキャビネットに保管する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4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: 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 具体的な管理方法	記載なし(追加)	・認定クラウド事業者及び認定クラウドの運用管理業者において、Firewall によるアクセス制限、WEB アプリケーションの脆弱性攻撃遮断、侵入検知システムによる運用監視・アクセス記録といった仕組みにより、権限の無い者の不正利用・アクセスを防止を行っている。 ・認定クラウド事の運用管理業者がゲートウェイ経由で本番環境にアクセスした場合には、ゲートウェイにおいてアクセス履歴(ログオン情報)が記録されることにより、不正ユーザによる情報閲覧などのアクセスを追跡している。	事前	法定調書のクラウド提出に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4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 リスクに対する措置の内容	記載なし(追加)	・専用端末(スタンドアロン、閉域網通信用)は、管理者の許可を得た者のみしか入退室出来ないようICカードによる入退室チェック機能による施錠管理(入退室時にICカードをかざし、暗証番号を入力しないと入退室出来ない仕組み)が措置されたセキュリティルームに設置されており、専用端末を利用するためのアカウントは特定の担当者のみに限定して付与されている。複製を行う際には必ず立会者を設けて実施するようにするとともに、専用端末の使用履歴のログは管理者により定期的(3か月毎)に監査を行うこととしている。また、セキュリティを設けた部屋には監視カメラを設置しており、専用端末の使用履歴に不正使用の疑いがある場合は、監視カメラの映像をチェックするようにしている。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4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 特定個人情報の提供ルール 委託先から他者への提供に関するルール内容及びルール遵守の確認方法	記載なし(追加)	・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅲリスク対策(プロセス) 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を通じた提供を除く。) 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・移転に関するルール ルール内容及びルール遵守の確認方法	税務署への電子媒体での提出に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。	税務署への電子媒体での搬送に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、セキュリティ確保のため、暗号化した上で専用回線(閉塞網)を用いて、認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携(ファイル連携)する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4日	Ⅲリスク対策(プロセス) 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を通じた提供を除く。) 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	税務署への電子媒体での提出に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。	税務署への電子媒体での搬送に当たっては、セキュリティ確保のため、データの暗号化及び搬送容器の施錠を行い、郵便物の追跡が行える方法により郵送する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、セキュリティ確保のため、暗号化した上で専用回線(閉塞網)を用いて、認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携(ファイル連携)する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	事前	法定調書のクラウド提出に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	Ⅲリスク対策(プロセス) 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を通じた提供を除く。) 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	税務署への提出に当たっては、かんぽ生命契約サービス部において「送付先」、「関係書類」等を複数人で確認し、送付している。 また、データにおいては暗号化及び搬送容器の施錠を行い、開錠及び復号化するパスワードは別途通知する。	支払調書のデータの搬送に当たっては、かんぽ生命契約サービス部において「送付先」、「関係書類」等を複数人で確認し、送付している。 また、データにおいては暗号化及び搬送容器の施錠を行い、開錠及び復号化するパスワードは別途通知する。 ・特定個人情報が含まれる電子媒体の支払調書データをネットワークに一切接続されていない専用端末(スタンドアロン)にて管理し、セキュリティ確保のため、暗号化した上で専用回線(閉塞網)を用いて、認定クラウド(e-私書箱(法定調書提出クラウドサービス))へデータ連携(ファイル連携)する。 ・クラウド提出を行う際は、ネットワークに一切接続されていない専用端末(スタンドアロン)にて管理されている支払調書データからクラウド提出する支払調書データを抽出し、その内容を複数人で点検・確認するとともに、認定クラウドへのデータ連携においても、データ送信先に誤りがないか、連携データの重複・漏れがないか等について、操作ログを複数人で点検・確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4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: 特定個人情報の漏洩・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	・端末機は社員証で入退室管理を行っている執務室内に設置し、ワイヤーチェーンによる施錠を施す。 ・端末機に特定個人情報は保管しない。	・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともにログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4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: 特定個人情報の漏洩・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	【支払調書データ(副本)(電子媒体)】 施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。	【支払調書データ(副本)(電子媒体)】 ・支払調書データについて電子記録媒体管理簿に登録し、施錠できるキャビネットに保管している。また、キャビネットの鍵は電子式のキーボックスにより、特定の者のみ取り出せるよう管理を行っている。 ・支払調書データは管理者が当該データが不要となった情報であること、媒体数等を確認・点検し、物理的に復元不能な状態にして廃棄する。 ・廃棄に当たっては事前にかんぽ生命情報セキュリティ統括室に廃棄申請を行い、許可を受けた上で実施する。廃棄後は電子記録媒体管理簿に廃棄の旨を記録する。	事前	法定調書のクラウド提出に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4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: 特定個人情報の漏洩・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	・端末機へのログイン時には、正当なIDとPWが必要。 ・端末機に特定個人情報を入力した場合は即時に暗号化を行っている。 ・端末機からかんぽ総合情報システム間の通信については、暗号化及びセキュアな通信を行っており、安全性が確保されている。 ・端末機はインターネット機能やメール機能がない業務専用の端末機である。	・専用端末(スタンドアロン)と専用端末(閉域網通信用)をICカードによる入退室管理を行っているセキュリティルームに設置し、ワイヤーチェーンによる施錠を施して、防犯カメラによる監視を行っている。 ・専用端末(スタンドアロン) 専用端末(スタンドアロン)は個人情報を保持しているが、スタンドアロン端末であるため外界との通信を遮断しており、媒体でのデータのやり取りについても暗号化された媒体(USBの場合は端末認証機能付き)で行うとともに、端末に保管された個人情報についても暗号化や持ち出し制限のプロテクトを行っている。また、複製媒体作成時は管理者が必ず立ち会う運用を行うとともにログについても管理者による定期的なチェックを行っている。 ・専用端末(閉域網通信用) 端末に個人情報を保持せず、通信時はインターネットではなく、専用線(閉域網)を使用して暗号化通信を行う。なお、送信作業のログは送信の都度、管理者がチェックし、誤送信(宛先誤り、重複、送信漏れ等)とならないことを確認する。	事前	法定調書のクラウド提出に伴う修正です。
令和7年11月4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: 特定個人情報の漏洩・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	・かんぽPC(標準)、ポスタルタブレットPCは在宅環境からの接続を考慮し、セキュリティフレームワークとして「SASE」を導入し、セキュリティ機能の強化を図っている。	・かんぽPC(事務)、ポスタルタブレットPCは在宅環境からの接続を考慮し、セキュリティフレームワークとして「SASE」を導入し、セキュリティ機能の強化を図っている。	事後	誤字の修正です。
令和7年11月4日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容	【I. 個人番号を特定個人情報ファイルに登録する事務】 1. かんぽ生命支店等及び郵便局 ・かんぽ生命支店及び本社法人営業開発部(以下「支店等」という。)並びに郵便局において保険金等の支払請求等をされたお客さまから個人番号の提示を受け、郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001、5001)、ポスタルタブレットPC又はかんぽPC(事務)))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。	【I. 個人番号を特定個人情報ファイルに登録する事務】 1. かんぽ生命支店等及び郵便局 ・かんぽ生命支店及び本社法人営業開発部(以下「支店等」という。)並びに郵便局において保険金等の支払請求等をされたお客さまから個人番号の提示を受け、郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4日	(別添1) 事務内容 【I. 個人番号を特定個人情報ファイルに登録する事務】 (備考) 1	③郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001、5001)、ポスタルタブレットPC又はかんぽPC(事務)))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。	③郵便局員等が端末機(インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)))に個人番号を入力し、かんぽ総合情報システムの個人番号等管理マスタに登録する。	事後	JP-PC(5001)利用終了に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	Ⅱ ファイルの概要 3.特定個人情報の入手・使用 ④入手に係る妥当性	【かんぽ生命支店等及び郵便局】 ・入手方法は、本人等からの個人番号カード等の提示を受け、社員が個人番号を端末機（インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機（JP-PC(3001)、5001）、ポスタルタブレットPC又はかんぽPC(事務)）に入力する。	【かんぽ生命支店等及び郵便局】 ・入手方法は、本人等からの個人番号カード等の提示を受け、社員が個人番号を端末機（インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機（JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)）に入力する。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 6.特定個人情報の保管・消去 ①保管場所	【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 端末機(CTM、JP-PC(3001)、5001)、ポスタルタブレットPC又はかんぽPC(事務)には個人情報を保管しない。	【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)には個人情報を保管しない。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4日	Ⅱ ファイルの概要 6.特定個人情報の保管・消去 ②保管期間 その妥当性	【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 端末機(CTM、JP-PC(3001)、5001)、ポスタルタブレットPC又はかんぽPC(事務)には個人情報を保管しない。	【入手経路による保管状況】 1. かんぽ生命支店等及び郵便局 端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)には個人情報を保管しない。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4日	Ⅲリスク対策(プロセス) 2. 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) リスク2: 不適切な方法で入手が行われるリスク リスクに対する措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の取得に際しては、個人番号カードの提示に基づき端末機（インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機（JP-PC(3001)、5001）、ポスタルタブレットPC又はかんぽPC(事務)）に入力を行うこととして手続に定め、特定個人情報の写しを作成することはしない。	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 個人番号の取得に際しては、個人番号カードの提示に基づき端末機（インターネット機能やメール機能がない端末機(CTM)、またはインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機（JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)）に入力を行うこととして手続に定め、特定個人情報の写しを作成することはしない。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4日	Ⅲリスク対策(プロセス) 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4: 入手の際に特定個人情報情報が漏えい・紛失するリスク リスクに対する措置の内容	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 ・特定個人情報について控え及び写しを作成しないこととしているほか、端末機（CTM、JPPC(3001,5001)、ポスタルタブレットPC又はかんぽPC(事務)）は紙媒体への出力機能を有しているが、個人番号が記録されたデータについては紙媒体で出力できないようシステムで制御している。	【入手経路による措置状況】 1. かんぽ生命支店等及び郵便局 ・特定個人情報について控え及び写しを作成しないこととしているほか、端末機（CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぽPC(事務)）は紙媒体への出力機能を有しているが、個人番号が記録されたデータについては紙媒体で出力できないようシステムで制御している。	事後	JP-PC(5001)利用終了に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4日	Ⅲリスク対策(プロセス) 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4: 入手の際に特定個人情報 情報が漏えい・紛失するリスク 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	端末機(CTM、JP-PC(3001,5001)、ポスタルタブレットPC又はかんぼPC(事務))又は携帯端末機(PT5)とかんぼ総合情報システム間においては特定個人情報に暗号化を施すとともに、日本郵便及びかんぼ生命でセキュリティ基盤(Prisma Access)を構築の上、PNETの既存設備を有効活用することで、セキュアなネットワークを使用している。 特に、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務)は、外部サービスのクラウド上でWEBサイトにアクセスするため、万が一マルウェアが仕掛けられたWebサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。	端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))又は携帯端末機(PT5)とかんぼ総合情報システム間においては特定個人情報に暗号化を施すとともに、日本郵便及びかんぼ生命でセキュリティ基盤(Prisma Access)を構築の上、PNETの既存設備を有効活用することで、セキュアなネットワークを使用している。 特に、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務)は、外部サービスのクラウド上でWEBサイトにアクセスするため、万が一マルウェアが仕掛けられたWebサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4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 リスクに対する措置の内容	・端末機(JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))は、インターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じており、また、端末上に特定個人番号を保管していないため、盗難、紛失、詐取された場合でも不正に複製されることはない。 (略) ・端末機のうち、JP-PC(3001,5001)、ポスタルタブレットPC又はかんぼPC(事務)では、ローカルディスクにデータを保存することが可能であるが、『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』に記載されている措置をとっている。 ・端末機のうち、JP-PC(5001)では、光学式ドライブからのデータ書き込みは、申請により許可された社員のみに制限されている。また、USBドライブからのデータ書き込みも、申請により許可された社員、端末、およびUSB機器のみに制限されている。	・端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))は、インターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じており、また、端末上に特定個人番号を保管していないため、盗難、紛失、詐取された場合でも不正に複製されることはない。 (略) ・端末機のうち、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務)では、ローカルディスクにデータを保存することが可能であるが、『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』に記載されている措置をとっている。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4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 具体的な対策の内容	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 ・個人番号は紙媒体で取得・保管を行わない。 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))は施錠された執務室内に設置されている。 ・端末機(JP-PC(3001,5001))は、ワイヤーチェーンによる施錠を施す。 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))に特定個人情報は保管しないよう社内規定に定め運用する措置を取っている。 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))は、社員証または社員番号および社員個人が設定したパスワードを入力しなければ、ログインができない。	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 ・個人番号は紙媒体で取得・保管を行わない。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))は施錠された執務室内に設置されている。 ・端末機(JP-PC(3001))は、ワイヤーチェーンによる施錠を施す。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))に特定個人情報は保管しないよう社内規定に定め運用する措置を取っている。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))は、社員証または社員番号および社員個人が設定したパスワードを入力しなければ、ログインができない。	事後	JP-PC(5001)利用終了に伴う修正です。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年11月4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 具体的な対策の内容	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC)は、社員証の利用および社員個人が設定したパスワードの入力または社員番号および社員個人が設定したパスワードの入力がログインのために必要。かんぼPC(事務)は、社員証の利用および社員個人が設定したパスワードの入力、社員番号および社員個人が設定したパスワードの入力、または生体認証がログインのために必要。 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))に特定個人情報を入力した場合は暗号化を即時に行った上でセンター側に送信し、端末内部には情報を残さないようにしている。 ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))とかんぼ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。 ・端末機(CTM)はインターネット機能やメール機能がない業務専用の端末機である。 ・端末機(JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))はインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機である。 ・JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務)は、外部サービスのクラウド上でWEBサイトにアクセスするため、万が一マルウェアが仕掛けられたWebサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。(略) ・端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))は、かんぼ総合情報システムでマイナンバーを参照・検索できない。	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC)は、社員証の利用および社員個人が設定したパスワードの入力または社員番号および社員個人が設定したパスワードの入力がログインのために必要。かんぼPC(事務)は、社員証の利用および社員個人が設定したパスワードの入力、社員番号および社員個人が設定したパスワードの入力、または生体認証がログインのために必要。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))に特定個人情報を入力した場合は暗号化を即時に行った上でセンター側に送信し、端末内部には情報を残さないようにしている。 ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))とかんぼ総合情報システム間の通信については暗号化及びセキュアな通信を行っており、安全性が確保されている。 ・端末機(CTM)はインターネット機能やメール機能がない業務専用の端末機である。 ・端末機(JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))はインターネット機能やメール機能はあるものの、ホワイトリストによる制限、社外あてメールのパスワード付与やあて先に上長を含めない場合にメールの送信を不可とする等の対策を講じた端末機である。 ・JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務)は、外部サービスのクラウド上でWEBサイトにアクセスするため、万が一マルウェアが仕掛けられたWebサイトにアクセスした場合でも、感染するのは分離されている外部サービスのクラウド上の環境であり、実際に利用している当該端末には影響を及ぼさないインターネット分離の仕組みによりマルウェア感染による情報漏えいリスクを低減している。(略) ・端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))は、かんぼ総合情報システムでマイナンバーを参照・検索できない。	事後	JP-PC(5001)利用終了に伴う修正です。
令和7年11月4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	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 保険金等の支払請求等のために窓口に来られたお客さまに、個人番号の変更がないか確認を行い、変更があった場合は、変更後の個人番号の提示を受け、端末機(CTM、JP-PC(3001、5001)、ポスタルタブレットPC又はかんぼPC(事務))に個人番号を入力し、かんぼ総合情報システムの個人番号等管理マスタに登録する。	【入手経路による保管状況】 1. かんぼ生命支店等及び郵便局 保険金等の支払請求等のために窓口に来られたお客さまに、個人番号の変更がないか確認を行い、変更があった場合は、変更後の個人番号の提示を受け、端末機(CTM、JP-PC(3001)、ポスタルタブレットPC又はかんぼPC(事務))に個人番号を入力し、かんぼ総合情報システムの個人番号等管理マスタに登録する。	事後	JP-PC(5001)利用終了に伴う修正です。