

仕様書

1 件名

組合員等のマイナンバー収集等業務

2 目的

発注者である公立学校共済組合愛知支部（以下「愛知支部」という。）が「行政手続き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「マイナンバー法」という。）」に基づき、愛知支部の組合員及びその被扶養者のマイナンバー（マイナンバー法第 2 条第 5 項に規定する個人番号）を取り扱うにあたり、外部専門組織のサービスを活用することにより、安全性を確保した業務の遂行を実現することを目的とする。

3 委託業務の概要

愛知支部において新たに組合員資格を取得する者及び新たに組合員の被扶養者として認定される者（以下「組合員等」という。）における資格取得届書又は被扶養者申告書提出手続き（以下「資格関係手続き」という。）におけるマイナンバー情報提出について、組合員等のマイナンバー情報をインターネット上で提出を可能とするシステムの提供及び組合員等から提出された画像データの精査・納品データ作成等を業務委託するものである。

また、マイナンバーの収集業務を円滑に遂行するにあたり、以下の基本方針に従うものとする。

- （１）「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」「個人情報の保護に関する法律」（平成 15 年法律第 57 号）及び「政府機関等のサイバーセキュリティ対策のための統一基準群」等に従い、適切にマイナンバーを取り扱うものとする。
- （２）マイナンバー収集業務により収集されるマイナンバー及び個人情報（以下「マイナンバー等」という。）については、原則として収集の都度速やかに発注者に渡すこととするとともに、受注者の環境（ただし、日本国内に限る。）において管理（保管・廃棄）する。

4 委託業務の内容

（１）申込受付フォームの提供

組合員等が下記の情報をインターネット上で入力できる受付フォームを提供する。

- ①共済組合員番号
- ②組合員漢字氏名
- ③組合員カナ氏名
- ④収集対象者続柄
- ⑤収集対象者漢字氏名
- ⑥収集対象者カナ氏名
- ⑦収集対象者生年月日
- ⑧収集対象者性別

⑨電話番号

⑩メールアドレス

※「⑤収集対象者漢字氏名」「⑥収集対象者カナ氏名」については、「④収集対象者続柄」が組合員本人であった場合は、「②組合員漢字氏名」「③組合員カナ氏名」を引用する仕組みとする。

(2) マイナンバー情報の提出フォームの提供

組合員等のマイナンバーを確認するための情報（以下「マイナンバー情報」という。）と本人であることを確認するための書類（以下「本人確認情報」という。）をインターネット上でアップロードできる提出フォームを提供する。なお、対象となる組合員等のマイナンバー情報及び本人確認情報は以下のとおりとする。

ア マイナンバー情報

- ・マイナンバーカード（マイナンバーが記載されている面）
- ・住民票の写し（マイナンバーの記載のあるもの）
- ・マイナンバー通知カードの写し（住所及び氏名に変更がない場合に限る）
- ・マイナンバー通知書の写し（住所及び氏名に変更がない場合に限る）

イ 本人確認書類

- ・免許証等顔写真付きの身分証明書
- ・対象となる組合員等のマイナンバーカード（顔写真が掲載されている面）

(3) 提出画像の精査業務

ア 書類精査業務

(ア) 受託者は、組合員等が上記4（2）でアップロードしたマイナンバー情報及び本人確認情報に不足がないこと若しくは画像において記載内容が読み取りできることを確認する。

(イ) 受託者は、組合員等が上記4（1）で入力した情報と（2）でアップロードしたマイナンバー情報及び本人確認情報が一致していることを確認する。

イ 不備対応

上記(ア)で情報に不足がある場合、画像において記載内容が読み取れない場合、又は上記(イ)において記載内容の情報が一致していない場合には、対象の組合員等に対して再アップロードを依頼するメールを配信する。

ウ 督促対応

上記イにおいて再アップロード依頼メールを配信後、一定期間を経過してもアップロードしない組合員等に対してアップロードを催促するメールを配信する。

エ 手続き完了メールの配信

情報の一致を確認後、対象の組合員等に対して手続き完了をメールにより通知する。

(4) 管理サイトの提供

愛知支部の当該事務担当者が組合員毎の提出状況、審査結果の確認及び提出画像データ並びに結果データのダウンロードが可能な管理サイトを提供する。

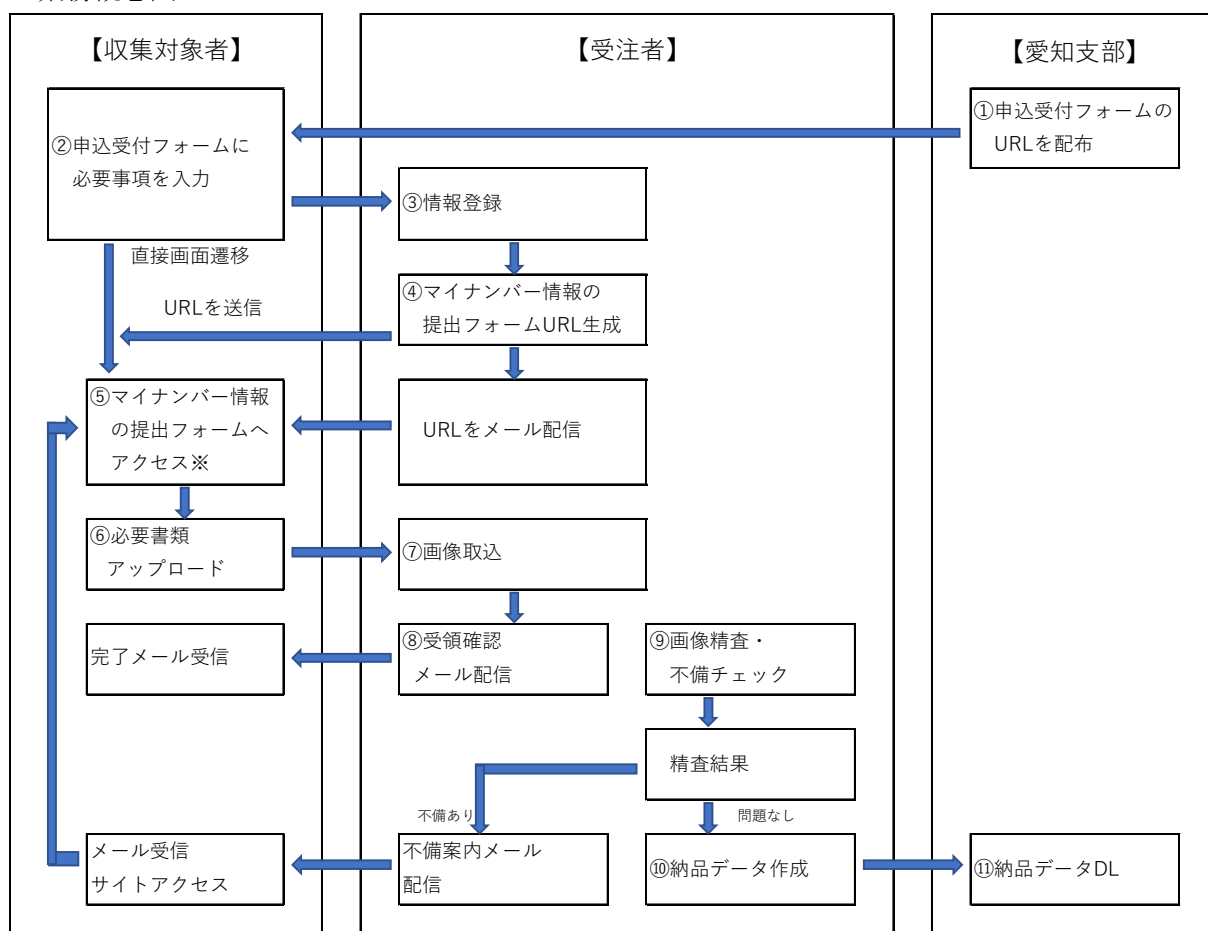
結果データは、収集対象者の入力の翌営業日にダウンロード可能となるようにする。

結果データは、情報入力等を行った組合員等（以下「申込者」という。）における登録情報

の一覧表（上記４（１）で入力した全ての情報を含むCSVファイル）と画像データ（PDF形式）が含まれているものとする。

なお、結果データは、提出した申込者の情報及び画像データの情報については、「６ セキュリティ要件」に定める要件を満たす安全性の高いセキュリティ基準に準拠した環境で最低２か月程度保管できることとする。

<業務概念図>



（５）監視・運用業務

受注者は、以下の項目に留意し、愛知支部が業務遂行できるための適切な運用を行うこと。

- ア 本業務に関する愛知支部からの問合せ窓口を設置すること。
- イ 本業務への問合せ対応は、「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）に定める休日を除く月曜日から金曜日までの 9 時から 17 時までを必須とすること。
- ウ 当月分の以下の作業実績を取りまとめた「実績報告書」を作成し、翌月 10 日（10 日が休日の場合はその前営業日、ただし、3 月分のみ 3 月 31 日）までに愛知支部に提出すること。
なお、報告書形式等の詳細については、契約締結後発注者と協議し取り決めるものとする。
- （ア） マイナンバー収集件数
- （イ） その他（協議して取り決める事項）
- エ 愛知支部は受注者が月次業務の実績及び適正な請求書を受理したときは、収集及び運用に係る費用を受注者に対して支払うものとする。

オ 各フォーム・サイトの正常稼働を定期的に確認する。異常が発生した場合は、愛知支部担当者に速やかに連絡し、異常解消に向けた対応を行う。

(6) その他

(1) から (5) に付随する業務を行うこと。

5 本件業務の委託条件

(1) 委託期間

令和8年4月1日から令和9年3月31日まで（令和9年3月31日受付分まで）

(2) 想定件数（見込み）

対象期間	見込件数
令和8年4月1日から令和9年3月31日までの受付分	9,200 件

(3) 各システムの提供条件

対象システム	対応チャンネル	利用者	提供条件	その他条件
入力フォーム	パソコン、スマートフォン	新たに資格取得した組合員	24 時間 365 日 (メンテナンス等の実施による休止は可とする。)	組合員及び被扶養者のデータがそれぞれ入力できるものとする。
提出フォーム	パソコン、スマートフォン	新たに資格取得した組合員		
管理サイト	パソコン	愛知支部		

※パソコン、スマートフォン等の利用条件は以下のとおりとする。

パソコン：Microsoft Edge 最新版、Google Chrome 最新版

スマートフォン：iPhone Safari 最新版、Android Google Chrome 最新版

※従来型携帯電話（フィーチャーフォン、ガラケー）は対応しない。

(4) 対象業務の提供条件

対象システム	対応者	提供条件	備考
精査業務	受託者	平日 9 時から 17 時	
監視運用業務	受託者	24 時間 365 日（メンテナンス等の実施による休止は可とする。）	

(5) 障害対応

サーバ等重要な機器は、大規模災害に備えて冗長化（二重化）等の対策が取られており、障害発生時でも早急な復旧が可能なこと。

6 セキュリティ要件

受託者は、マイナンバー等が漏えい、滅失又は毀損することなく、適切な管理を行うために

組織的・人的・物理的・技術的等の安全管理措置を講じるとともに、「政府機関等のサイバーセキュリティ対策のための統一基準群」等を参照し、必要な安全管理措置を講じること。

なお、本業務の再委託先がある場合は、受注者の責任においてその組織における安全管理措置を徹底することが求められるものとする。

また、収集した特定個人情報を含む組合員情報等の目的外利用を禁ずる。

(1) 情報セキュリティ対策

ア 受託者は、情報セキュリティ管理について情報セキュリティマネジメントシステム（ISO/IEC 27001）、クラウドサービスセキュリティ管理策（ISO/IEC 27017）、個人情報マネジメントシステム（ISO/JIS Q 15001）、プライバシーマーク、オフィスセキュリティマークのうちいずれかの公的資格を有していること。又は、資格同等の情報セキュリティ対策を実施していることを証明できること。

イ 受託者は、サービスの機密性、完全性、可用性を確保するため、以下のセキュリティ対策を実施すること。

(ア) 通信経路上での暗号化（SSL等）

(イ) ウイルス対策ソフトの導入及びパターンファイルの定期的な更新並びにセキュリティパッチの定期的な運用等による不正プログラム対策

(ウ) ID、パスワード等によるユーザー認証、侵入防止システムの導入等による24時間監視、サーバ等重要な機器の設置場所への立ち入り制限による不正アクセス対策

(エ) その他必要なセキュリティ対策（「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠していること。）

ウ 本業務に関する機器を設置するデータセンターは、日本国内に設置されたものであり、耐震設備、電源設備、空調設備、セキュリティ設備、耐火設備、保管設備、ネットワーク設備、監視設備等を有する堅牢な施設に設置されており、不正侵入及びデータの改ざん等の不正アクセス防止に対する万全のセキュリティ対策が講じられていること。

(2) 情報セキュリティインシデントへの対処

ア 受託者は、情報セキュリティインシデントへの対処においての準備から事後処理に至る全般的なインシデント対処プロセスを確立していること。

イ 当事者及び関係者の役割を含む体制をあらかじめ定めていること。（連絡先窓口及び対応可能時間帯含む）

ウ インシデント対処体制、責任者、担当者から当該体制への報告フロー等の概要について、対処能力の証明として契約締結までに説明ができること。

エ 委託期間中に情報セキュリティ対策の実施状況及び情報セキュリティインシデント等の検知有無等について定期的な報告を行うこと。

オ 情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、委託先が受託事業を一時中断するなどの必要な措置を講じた上で、報告手順に従い遅滞なく愛知支部に報告を行うとともに対処を行うこと。