

藤沢市個人情報保護制度運営審議会答申第1143号

2022年（令和4年）7月14日

藤沢市長 鈴木 恒夫 様

藤沢市個人情報保護制度
運営審議会会長 畠山 関之

資金調達に関することに係るコンピュータ処理について（答申）

2022年（令和4年）7月4日付けで諮問（第1143号）された資金調達に関することに係るコンピュータ処理について、次のとおり答申します。

1 審議会の結論

藤沢市個人情報の保護に関する条例（平成15年藤沢市条例第7号。以下「条例」という。）第18条の規定によるコンピュータ処理を行うことについては、適当であると認められる。

2 実施機関の説明要旨

実施機関の説明を総合すると、本事務の実施に当たりコンピュータ処理を行う必要性は、次のとおりである。

(1) 諮問に至った経過

本市では、平成29年度から、ふるさと納税ポータルサイトを活用した寄附金の受け入れを開始している。

ふるさと納税は、寄附金額に応じて所得税や住民税から控除が受けられる制度であり、控除のための手続きの一つとして「寄附金税額控除に係る申告特例申請（いわゆる、ワンストップ特例申請）」がある。

この手続きでは、寄附者がふるさと納税をした自治体に対してワンストップ特例申請書を提出することにより寄附金税額控除を受けられるものであり、令和3年度に本市がワンストップ特例申請書を受け付けた件数は1,256件となっている。

現状、ワンストップ特例申請書及び本人確認書類について、本市では原則、郵送での提出を求めており、他の自治体の多くも同様の運用を行っている。しかし、郵送による申請については、寄附者に申請書類の準備や切手代金の負担がかかること、また、自治体においても年々増加する申請件数に対し、申請内容のチェック、データ入力作業及び

入力データの入力誤り等の確認作業の負担が増えていることが課題となっていた。

そのような中、本市がふるさと納税関係業務委託を締結している「株式会社さとふる」が、寄附者がオンライン上でワンストップ特例申請をすることができる仕組み「ワンストップ特例オンライン申請サービス（以下、「本サービス」という。）」の提供を2022年秋頃から開始することになったことから、寄附者の利便性向上や職員の業務効率向上が図られる本サービスについて、導入することとした。

以上により、本サービスを導入することで、寄附者情報のやりとりにおいて新たにコンピュータ処理を行うことから、藤沢市個人情報の保護に関する条例第18条の規定に基づき、藤沢市個人情報保護制度運営審議会に諮問するものである。

(2) 本サービスの概要

本サービスでは、寄附者がふるさと納税ポータルサイト「さとふる」で行った寄附について、スマートフォン上で専用アプリケーション「さとふるアプリ」を起動し、マイナンバーカードの情報を読み取ることにより、寄附者はこれまで郵送で行っていたワンストップ特例申請をオンラインで完結でき、また、本市も寄附者申請データを LGWAN 環境でダウンロードできるというもの。

(3) 本サービスの提供主体

本サービスは、株式会社さとふるがスマートフォンアプリとして提供するものである。また、株式会社さとふるは、本サービスのうち、公的個人認証及びマイナンバーを含む寄附者情報の管理・保管について、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年12月13日法律第153号。以下、「公的個人認証法」という。）第17条第1項第6号の規定により総務大臣から認定を受けている「株式会社野村総合研究所」に再委託するもの。

(4) 本サービスが活用するサービス・アプリケーション等

ア さとふるアプリ

株式会社さとふるが寄附者に対して提供する、ふるさと納税の寄附、寄附履歴の確認及びオンラインワンストップ特例申請等が行えるアプリケーション。

イ e-NINHO

再委託先の株式会社野村総合研究所が提供する、マイナンバーカードの IC チップに格納された「署名用電子証明書」、「利用者証明用電子証明書」並びに「電子署名」を活用して、オンライン上で本人確認（署名検証）及びマイナンバー収集・管理を行うサービス。

(5) 本サービスの流れ

ア マイナンバーカードの読み取り

寄附者は、スマートフォンでさとふるアプリを起動し、マイナンバーカードを読み取る。

イ 基本4情報の取得

さとふるアプリ上で呼び出された e-NINHO の機能により、基本4情報（氏名・性別・住所・生年月日）の取得を行う。

ウ 本人確認

e-NINSHO により、地方公共団体システム機構（J-LIS）に対し、マイナンバーカードの IC チップに格納されている署名用電子証明書の有効性について照会する。

エ マイナンバー等の寄附者情報の収集

「ウ」で署名用電子証明書が有効と判断された場合に限り、マイナンバー等の券面情報や株式会社さとふるが管理する寄附者情報が暗号化され、e-NINSHO サーバでデータが収集される。

オ 寄附者情報のオンライン申請管理システムへの連携

e-NINSHO サーバに収集されたデータは、同じく株式会社野村総合研究所のデータセンターで管理されているオンライン申請管理システム（LGWAN-ASP サービス）のサーバとの間でデータ連携（データ生成）を行う。

カ 自治体によるデータ取得

自治体は、LGWAN 接続ができる基幹系端末から、株式会社野村総合研究所が提供する LGWAN -ASP サービスであるオンライン申請管理システムに LGWAN 環境にてアクセスし、蓄積された寄附者データを CSV 形式にて非公開系ネットワークドライブ（以下、「Gドライブ」という。）にダウンロードを行う。

なお、自治体が LGWAN -ASP サービスにオンライン接続する際、アクセス ID 及び LGWAN 接続ルータのグローバル IP アドレスによる制御が行われる。

(6) 新たにコンピュータ処理を行う個人情報

ア 株式会社野村総合研究所が管理、保管するマイナンバー情報等

(ア) マイナンバー

(イ) 氏名

(ウ) 性別

(エ) 住所

(オ) 生年月日

イ 株式会社野村総合研究所が管理、保管する寄附に関する情報

- (ア) 寄附番号
 - (イ) 氏名（姓）
 - (ウ) 氏名（名）
 - (エ) 氏名（フリガナ）（姓）
 - (オ) 氏名（フリガナ）（名）
 - (カ) 住所
 - (キ) 生年月日
 - (ク) 電話番号
 - (ケ) 寄附年月日
 - (コ) 寄附金額
- (7) 安全対策等について
- ア 本市における安全対策
 - (ア) 職員は、e-NINSHO で収集された情報を LGWAN 経由で CSV ファイルにてダウンロードする際、交付された I D、パスワードを用いて本サービスにログインするものとする。
 - (イ) 交付された I D 及びパスワードの利用は、所属長に使用を許可された職員に限定する。
 - (ウ) 人事異動の都度、利用者登録する職員情報を見直すとともに、I D 及びパスワード管理の徹底と定期更新を行う。
 - (エ) 取り扱うすべての情報に対し、不正な持ち出し、改ざん、破壊、紛失及び漏えい等が行われないよう管理をする。
 - (オ) G ドライブに保存されたデータは、寄附金税額控除にかかる申告特例通知書支援ツールに取り込み後、速やかに削除する。
 - イ 事業者の安全対策
 - (ア) 個人情報を含む情報の管理、保管については、公的個人認証法第 17 条第 1 項第 6 号の規定により総務大臣から認定を受け、署名検証または利用者証明検証を行うことができる株式会社野村総合研究所が行う。
 - (イ) 自治体が LGWAN-ASP サービスにオンライン接続する際の通信許可として、アクセス ID 及び自治体毎の LGWAN 接続ルータのグローバル IP アドレスによる制御を行っており、外部への情報流出対策がなされている。
- (8) 実施時期
2022 年（令和 4 年）10 月（予定）
- (9) 添付資料
- ア ワンストップ特例オンライン申請サービスの利用にかかる申込書（案）
 - イ e-NINSHO サービス水準定義書

- ウ ワンストップオンライン申請サービスご提案資料
- エ ワンストップオンライン申請サービスご提案資料（補足）

3 審議会の判断理由

当審議会は、次に述べる理由により、「1 審議会の結論」のとおり
の判断をするものである。

(1) コンピュータ処理を行う必要性について

実施機関では、コンピュータ処理を行う必要性について、次のよう
に述べている。

現状、ワンストップ特例申請書及び本人確認書類について、本市で
は原則、郵送での提出を求めており、他の自治体の多くも同様の運用
を行っている。しかし、郵送による申請については、寄附者に申請書
類の準備や切手代金の負担がかかること、また、自治体においても年々
増加する申請件数に対し、申請内容のチェック、データ入力作業及び
入力データの入力誤り等の確認作業の負担が増えていることが課題と
なっていた。

そのような中、本市がふるさと納税関係業務委託を締結している「株
式会社さとふる」が、寄附者がオンライン上でワンストップ特例申請
をすることができる仕組み「ワンストップ特例オンライン申請サービ
ス（以下、「本サービス」という。）」の提供を2022年秋頃から開始
することになったことから、寄附者の利便性向上や職員の業務効率向
上が図られる本サービスについて、導入することとした。

(2) 安全対策について

実施機関が「2 実施機関の説明要旨」(7)のア及びイにおいて示す
安全対策は、次のとおりである。

ア 本市における安全対策

(ア) 必要最小限の担当者以外の者がデータにアクセスできないよ
うにするための措置

ア(ア)、ア(イ)、ア(ウ)

(イ) 利用後にデータを確実に消去するための措置措置

ア(オ)

(ウ) 日常的な安全対策

ア(エ)

イ 事業者の安全対策

(ア) 実施機関が受託者の安全対策を確認できるようにするための
措置

イ(ア)

(イ) ネットワークを通じた情報漏えいを防止するための措置

イ(イ)

以上のことから判断すると、安全対策上の措置が講じられていると認められる。

以上に述べたところにより、コンピュータ処理を行うことは、適当であると認められる。

以 上