藤沢市個人情報保護制度運営審議会答申第１１２４号

２０２２年（令和４年）３月１０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　鬨之

市税及び県民税（特別徴収に係る現年度分の個人の市民税及び県民税を除く。）の徴収及び収納並びに滞納処分に係るコンピュータ処理について（答申）

２０２２年（令和４年）２月２４日付けで諮問（第１１２４号）された市税及び県民税（特別徴収に係る現年度分の個人の市民税及び県民税を除く。）の徴収及び収納並びに滞納処分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

各種法令に基づき，行政機関は，人手作業により作成した照会文書をシステムから出力し複数の金融機関に郵送し，財産調査を行っている。また，金融機関から回答された文書も人手作業によりシステムに入力し業務に活用している。こうした一連の業務は，現在，書面を前提として行われており，照会文書の作成，回答文書のデータ化などに伴う作業が負担となっている。本市納税課において地方税法第２０条の１１及び国税徴収法第１４１条の規定に基づき行っている滞納整理に係る財産調査についても，同様に人手作業かつ書面により行われており，事務量が過分に必要であり，事務処理の効率性が著しく損なわれている。

一方，回答する金融機関側においても業務負担は大きく，行政機関からの調査量は年間約６，０００万件と膨大で，受け取った照会文書を人手作業により顧客情報と照合し，書面の仕分け・保管作業等を行った上，該当者がいた場合に回答を書面として作成し郵送を行っている。

行政機関，金融機関ともに人手作業となるため，行政機関が照会文書を作成し金融機関に発送するまでに期間を要した場合や，金融機関が行政機関に対し回答を行うまでに期間を要した場合，調査対象者の預貯金等の情報把握が遅れ，早期の滞納解消が困難になる等，行政機関側の業務において支障・停滞が発生するおそれがある。

このような状況から，各金融機関に対して行っている財産調査について，２０２１年（令和３年）６月３０日内閣官房情報通信技術（ＩＴ）総合戦略室及び金融庁から総務省に向けて預貯金等照会・回答業務のデジタル化の推進について要請がなされ，総務省自治税務局電子化推進室長から各都道府県に，神奈川県政策局自治振興部市町村課長から県内の市町村に向けて，預貯金等の照会・回答業務のデジタル化の推進について積極的に検討するよう通知が発出されており，本市納税課としても,預貯金等の照会･回答業務のデジタル化の推進により，財産調査を電子化することで，作業の省力化・迅速化が図られ，人手による作業負担，人件費の削減や金融機関から回答を得るまでの期間短縮等，書面により実施されていた課題の多くを解決することが見込まれることから，株式会社ＮＴＴデータ・アイが提供する預貯金等照会電子化サービスであるＮＤＩ ｐｉｐｉｔＬＩＮＱ（以下「ｐｉｐｉｔＬＩＮＱ」という。）を導入することとした。

以上のことから，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) コンピュータ処理について

ア　コンピュータ処理の概要

(ｱ) 基幹系システム（日本電気株式会社製。以下「ＣＯＫＡＳ－ｉ」という。）により抽出した照会データを株式会社ＮＴＴデータ・アイの提供するツールを用いて変換しＬＧＷＡＮ回線でｐｉｐｉｔＬＩＮＱに送信する。

(ｲ) ｐｉｐｉｔＬＩＮＱは照会データを各金融機関に振り分け，ｅＢ-ＮＷ（ＩＰ－ＮＷ）回線閉域網を用いてデータの送受信を行う。

(ｳ) ｐｉｐｉｔＬＩＮＱが金融機関からの回答データを行政機関単位に振り分け，ＬＧＷＡＮ回線により送信する。

(ｴ) ｐｉｐｉｔＬＩＮＱから送信された回答データはＬＧＷＡＮ

回線を用いてＣＯＫＡＳ‐ｉにダウンロードする。

イ　コンピュータ処理の必要性

預貯金等照会・回答業務のデジタル化の推進は，人手による作業負担の軽減，人件費の削減や金融機関から回答を得るまでの期間短縮等，作業の省力化・迅速化が図られる。また，調査対象者の預貯金等の情報把握の遅れによる早期の滞納解消が困難になる等，当該業務において支障・停滞が発生するおそれを予防するものであり，多くの情報を迅速かつ正確に処理するため，コンピュータ処理を行う必要がある。

ウ　コンピュータ処理を行う個人情報について

氏名，生年月日，住所（居所含む。），電話番号，金融機関取引に関すること（預金，融資，為替，保険等）

エ　取扱金融機関

ｐｉｐｉｔＬＩＮＱ参加金融機関

(3) 契約について

システムを運営する株式会社ＮＴＴデータ・アイとの業務委託契約

(4) 安全対策について

ア　本市の安全対策

(ｱ) 執務室内にワイヤーロックで施錠された端末を利用する。

(ｲ) 許可された者のみが生体認証システムを利用し端末にログインする。

(ｳ) ｐｉｐｉｔＬＩＮＱとの接続はＬＧＷＡＮ回線を使用する。

(ｴ) ｐｉｐｉｔＬＩＮＱログイン時のＩＤ及びパスワードは担当者を限定して付与することで不正アクセスを防止する。

(ｵ) ｐｉｐｉｔＬＩＮＱ送受信端末にて受信したデータは，ＬＧＷＡＮ回線を用い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。）に保管し，日常的な安全対策として，藤沢市情報セキュリティポリシー及び藤沢市情報システム管理運営規程を遵守する。

(ｶ) データの保存先であるＧドライブについては，ログインにＩＤとパスワードが必要となり，そのパスワードは定期的に変更する。

(ｷ) Ｇドライブに保存されたデータは照会対象者の滞納が解消されたら速やかに消去する。

イ　受託者の安全対策

(ｱ) 本市と受託者との間のデータの送受信については，ＬＧＷＡＮ回線を用いて行う。

(ｲ) 金融機関との間のデータの送受信についてはｅＢ-ＮＷ/ＩＰ-ＮＷ（閉塞網かつ通信経路を暗号化）を用いて行う。

(ｳ) ｐｉｐｉｔＬＩＮＱは，日本国内にデータセンタを有するセキュアなクラウドであるＯｐｅｎＣａｎｖａｓ上に構築されており，そのデータの置き場所は国内のみで国外にデータを置くことはない。また，ＦＷによる不正アクセス制御（不正アクセスの遮断），ウイルス対策，データ暗号化，操作ログの取得，ユーザーＩＤ，ＰＷによるログイン認証を実施している。

(ｴ) ＯｐｅｎＣａｎｖａｓはクラウドサービスに関する情報セキュリティ管理策の国際標準「ＩＳＯ２７０１７」，及び，情報セキュリティマネジメントシステム「ＩＳＯ／ＩＥＣ２７００１」認証を取得している。また，政府情報システムのためのセキュリティ評価制度（以下「ＩＳＭＡＰ」という。）において，政府が求めるセキュリティ要求を満たしているサービスであると認定され，ＩＳＭＡＰクラウドサービスリストに登録されている。

(ｵ) 個人情報保護ガイドライン（通則編）に定められた事業者が実施する安全管理措置を実施している。

ウ　金融機関の安全対策

(ｱ) 受託者との通信にはｅＢ－ＮＷ／ＩＰ－ＮＷを利用（閉塞網かつ通信経路を暗号化）

(ｲ) 各金融機関が定める情報セキュリティポリシーの遵守

(ｳ) ｐｉｐｉｔＬＩＮＱサービス利用規約の遵守

(5) 実施時期（予定）

２０２２年（令和４年）６月１日

(6) 添付資料

ア　令和３年６月３０日付け内閣官房情報通信技術（ＩＴ）総合戦略室・金融庁「預貯金等照会・回答業務のデジタル化の推進について（要請）」

イ　令和３年７月１日付け総務省自治税務局電子化推進室長「預貯金等の照会・回答業務のデジタル化の推進について」

ウ　令和３年７月５日付け神奈川県政策局自治振興部市町村課長「預貯金等の照会・回答業務のデジタル化の推進について」

エ　ｐｉｐｉｔＬＩＮＱセキュリティ対策について

オ　ｐｉｐｉｔＬＩＮＱ概要

カ　ｐｉｐｉｔＬＩＮＱ運用フロー

キ　ｐｉｐｉｔＬＩＮＱ導入効果（行政機関）

ク　ｐｉｐｉｔＬＩＮＱ導入効果（金融機関）

ケ　ｐｉｐｉｔＬＩＮＱ利用状況

コ　預貯金等照会電子化サービス業務委託契約書（案）

サ　個人情報取扱事務届出書

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。

預貯金等照会・回答業務のデジタル化の推進は，人手による作業負担の軽減,人件費の削減や金融機関から回答を得るまでの期間短縮等,作業の省力化・迅速化が図られる。また，調査対象者の預貯金等の情報把握の遅れによる早期の滞納解消が困難になる等，当該業務において支障・停滞が発生するおそれを予防するものであり，多くの情報を迅速かつ正確に処理するため，コンピュータ処理を行う必要がある。

以上のことから判断すると，コンピュータ処理を行う必要性が認められる。

(2) 安全対策について

実施機関が「２　実施機関の説明要旨」(4)のアからウまでにおいて示す安全対策は，次のとおりである。

ア　本市の安全対策

(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(ｲ)，ア(ｴ)

(ｲ) システムの不正アクセスを防止するための措置

ア(ｲ)，ア(ｴ)，ア(ｶ)

(ｳ) 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

ア(ｳ)，ア(ｵ)

(ｴ) 利用後にデータを確実に消去するための措置

ア(ｷ)

(ｵ) 日常的な安全対策

ア(ｱ)，ア(ｵ)，ア(ｶ)

イ　受託者の安全対策

(ｱ) 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(ｱ)，イ(ｲ)，イ(ｳ)

(ｲ) 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(ｴ)

(ｳ) 日常的な安全対策

イ(ｵ)

ウ　金融機関の安全対策

(ｱ) 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

ウ(ｱ)

(ｲ) 日常的な安全対策

ウ(ｲ)，ウ(ｳ)

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。

なお，受託者の安全対策の万全性について，本市において確認する方法を検討することを要望する。

以　上