

藤沢市個人情報保護制度運営審議会答申第1035号

2020年（令和2年）9月10日

藤沢市長 鈴木 恒夫 様

藤沢市教育委員会
教育長 岩本 将宏 様

藤沢市個人情報保護制度
運営審議会会長 畠山 関之

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，介護保険料の賦課，徴収及び滞納処分，国民健康保険料の賦課，徴収及び滞納処分，高齢者の医療の確保に関する法律（昭和57年法律第80号）の規定等による事務並びに学校給食の企画，運営及び指導に関することに係るコンピュータ処理について（答申）

2020年（令和2年）8月21日付けで諮問（第1035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，介護保険料の賦課，徴収及び滞納処分，国民健康保険料の賦課，徴収及び滞納処分，高齢者の医療の確保に関する法律（昭和57年法律第80号）の規定等による事務並びに学校給食の企画，運営及び指導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) 諮問に至る経過

本市では、税料等の多様な納付環境の導入と収納情報のデータ化を進めることで、納付者の利便性の向上とともに、事務の効率化に取り組んでおり、現行の納付環境としては、取扱金融機関やコンビニエンスストア等の窓口納付、口座振替などがある。

本年5月の新型コロナウイルス感染症拡大による緊急事態宣言下以降、不要不急の外出自粛と第二波、第三波への警戒が必要とされる中、納付者の外出を避けたい、混雑している金融機関等の窓口を利用したくない、といった理由から、新しい生活様式の実践として、自宅や職場などからインターネットバンキングを活用し、24時間支払い可能な決済手段のニーズが顕在化している。

このことから、本市では、納付者の利便性の向上と事務の効率化を図るため、日本マルチペイメントネットワーク運営機構（以下「機構」という。）が構築・運営するマルチペイメントネットワーク（以下「MPN」という。）を活用したMPN収納を導入する。

なお、MPN収納は、納付者がスマートフォン、パソコン、ATM等の様々な金融機関チャネルを利用し、いつでもどこでも簡単に公金を支払うことができる電子決済サービスであり、地方公共団体等の収納機関に収納情報を即時に又は一括して通知することで、収納事務の効率化を実現する仕組みである。

このMPN収納の仕組みは、機構が定めた規程や仕様に沿って構築・運営されており、膨大な収納情報を効率的かつ安全に処理するため、コンピュータ処理が前提とされていることから、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) コンピュータ処理を行う必要性

本市の税料等の収納事務においては、基幹業務システムを導入し、収納情報をコンピュータ処理している。本市が、MPNを活用し、銀行等の収納金融機関やMPNに接続するためには、通信サーバを構築・維持し、複数の地方公共団体等とMPNの中継接続を行う収納機関共同利用センター（以下「センター」という。）とデータ送受信を行うことから、コンピュータ処理を行う必要がある。

(3) コンピュータ処理の概要

MPNは、民間企業、官公庁又は地方公共団体がセンターを介して金融機関と接続する閉域ネットワーク（IP-VPNによる仮想閉域網を利用）であり、機構により運営されている。提供されるサービスのうち、本市はオンライン方式と一括伝送方式を利用する。

ア オンライン方式

納付者が金融機関チャネルを介して納付情報のキー情報を入力し、センターに照会処理を行い、納付後、収納情報を通知する方式

イ 一括伝送方式

納付者が金融機関の窓口で納付した後、金融機関が納付書をデータ化して収納情報を作成し、MPN経由で本市に収納情報を通知する方式

(4) コンピュータ処理を行う対象種目及び個人情報項目

ア 対象種目

市県民税（特別徴収）、市県民税（普通徴収）、法人市民税、固定資産税・都市計画税（土地・家屋）、固定資産税（償却資産）、軽自動車税（種別割）、市たばこ税、入湯税、事業所税、介護保険料、国民健康保険料、後期高齢者医療保険料、学校給食費

イ 個人情報項目

税（料）目、通知書番号、車両番号（軽自動車税のみ）、納付期限、税額（料）、延滞金、取引金融機関コード

(5) 本市と関係機関の間の契約等

ア センター運営事業者 株式会社エヌ・ティ・ティ・データ
業務委託契約

イ 金融機関

MPN関連事項の覚書
従来の指定金融機関契約及び収納代理金融機関契約等の基本契約に係る覚書として締結予定

ウ 機構

MPN関連事項の覚書
収納機関登録（各種規約・仕様書等を承諾の上申請）

(6) 安全対策等について

ア 本市の安全対策

(ア) 各所管課執務室内に静脈認証によるユーザ認証が行われ、ワイヤロックで施錠された基幹系端末（各課1台）に限定し、L G W A N回線を使用し、センターと接続する。

(イ) 本業務の管理責任者を定め、管理画面にアクセスすることができる者を限定する。なお、パスワードは定期的に変更する。

(ウ) 納付情報及び収納情報の保管については、必要最小限とし、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コンピュータシステム管理運営規程を遵守する。

(エ) 業務遂行上又は管理上、紙に出力したデータは、施錠したキャビネットに保管する。電子データについては、保管期間終了後、速やかにネットワークドライブから消去する。

イ MPN収納全体の安全対策

機構及びMPN参加機関は、MPN収納全体のセキュリティを確立するため、マルチペイメントネットワーク情報セキュリティ基本方針に基づき、次の項目について、各機関のセキュリティ確保規程に規定し、又は留意することで安全性の確保を行っている。

また、各機関において、セキュリティ対策の実効性が確保されているか機構が指定する外部機関による監査が実施されている。

(ア) システム的なセキュリティ対策

- a 不正アクセス防止
- b 接続先の特定
- c 暗号化
- d 外部ソフトウェアパッケージ導入時の評価・管理
- e オペレーション面の安全管理
- f サイバーセキュリティ管理
- g クラウドサービス管理

(イ) 論理的なセキュリティ対策

- a 標準アクセスに関するルール
- b 開発・運用の各組織間・組織内の相互牽制体制
- c 開発管理体制
- d 障害発生時の対応策
- e プログラムの管理

(ウ) 物理的なセキュリティ対策

- a 侵入防止策
- b 防犯設備
- c 入退室管理
- d 磁気媒体の運搬時や保管に際しての施錠管理
- e コンピュータ働環境の整備
- f 機器の保守・点検体制

(エ) コンティンジェンシープラン

- a 策定・整備に関する経営層の承認
- b 被害想定における複数原因（自然災害以外）の設定
- c 訓練の実施

(オ) 各種記録・セキュリティ規程類の管理運営

- a 各種記録の一定期間の保管
- b セキュリティ規程類の定期的な変更管理

ウ センターの安全対策

(ア) 条例、ウェブアプリケーションのセキュリティ対策に関する仕様書並びにデータの保護及び秘密の保持等に関する仕様書を遵守する。

(イ) 金融機関等コンピュータシステム(FISC)安全対策基準(公益財団法人金融情報システムセンター策定)に則り、立ち入り制限するなどの対策を施すとともに、侵入防止システムを導入し、外部からの不正なアクセスを24時間監視するなど強固なセキュリティを保つ。

(ウ) 本市とセンターの納付情報や収納情報の電送においては、L G W A N回線を使用する。

(エ) 機構が定める基本方針に基づき、セキュリティ基本方針及び規程を整備し、遵守する。また、機構の要求する水準のセキュリティレベルを充足しているか、定期的に監査を受ける。

エ 金融機関の安全対策

機構が定める基本方針に基づき、セキュリティ基本方針及び規程を整備し、遵守する。また、機構の要求する水準のセキュリティレベルを充足しているか、定期的に監査を受ける。

(7) 広報等周知

M P N収納の開始については、2020年(令和2年)10月以降、広報ふじさわ、市ホームページ、庁内デジタルサイネージ等に記事を掲載し、市民に周知をする予定である。

(8) 実施時期

2021年(令和3年)1月1日(予定)

(9) 添付書類

ア コンピュータ処理の概要図

イ マルチペイメントネットワーク情報セキュリティ基本方針

ウ マルチペイメントネットワーク収納に係る収納機関共同利用センター業務委託契約書

エ マルチペイメントネットワーク収納に係る収納機関共同利用センター業務委託仕様書

オ F I S C (金融機関等コンピュータシステム) 安全対策基準

カ 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。

本市の税料等の収納事務においては、基幹業務システムを導入し、収納情報をコンピュータ処理している。本市が、MPNを活用し、銀行等の収納金融機関やMPNに接続するためには、通信サーバを構築・維持し、複数の地方公共団体等とMPNの中継接続を行うセンターとデータ送受信を行うことから、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

ア 実施機関が「2 実施機関の説明要旨」(6)のア及びウからエまでに示す安全対策は、次のとおりである。

(ア) 本市の安全対策

- a システムの不正アクセスを防止するための措置
ア(ア)
- b 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(ア)
- c 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)
- d 利用後にデータを確実に消去するための措置
ア(エ)
- e 日常的な安全対策
ア(ア), ア(ウ), ア(エ)

(イ) 受託者の安全対策

- a システムの不正アクセスを防止するための措置
ウ(イ)
- b 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
ウ(イ)
- c 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(ウ)
- d 日常的な安全対策
ウ(ア), ウ(エ)

(ウ) 金融機関の安全対策

- a 実施機関が金融機関の安全対策を確認できるようにするた

めの措置

エ

イ MPN収納全体の安全対策について、実施機関では、次のような安全対策を講じるとしている。

機構及びMPN参加機関は、MPN収納全体のセキュリティを確立するため、マルチペイメントネットワーク情報セキュリティ基本方針に基づき、次の項目について、各機関のセキュリティ確保規程に規定し、又は留意することで安全性の確保を行っている。

また、各機関において、セキュリティ対策の実効性が確保されているか機構が指定する外部機関による監査が実施されている。

(ア) システム的なセキュリティ対策

- a 不正アクセス防止
- b 接続先の特定
- c 暗号化
- d 外部ソフトウェアパッケージ導入時の評価・管理
- e オペレーション面の安全管理
- f サイバーセキュリティ管理
- g クラウドサービス管理

(イ) 論理的なセキュリティ対策

- a 標準アクセスに関するルール
- b 開発・運用の各組織間・組織内の相互牽制体制
- c 開発管理体制
- d 障害発生時の対応策
- e プログラムの管理

(ウ) 物理的なセキュリティ対策

- a 侵入防止策
- b 防犯設備
- c 入退室管理
- d 磁気媒体の運搬時や保管に際しての施錠管理
- e コンピュータ働環境の整備
- f 機器の保守・点検体制

(エ) コンティンジェンシープラン

- a 策定・整備に関する経営層の承認
- b 被害想定における複数原因（自然災害以外）の設定
- c 訓練の実施

(オ) 各種記録・セキュリティ規程類の管理運営

- a 各種記録の一定期間の保管
- b セキュリティ規程類の定期的な変更管理

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