

2020年（令和2年）5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

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）

2020年（令和2年）5月11日付けで諮問（第1008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

新型コロナウイルス感染症の拡大が市民生活に大きな影響を与える中、2020年（令和2年）4月30日に創設された新型コロナウイルス感染症等に係る徴収猶予の特例に基づき、納税の猶予制度の特例措置が講じられることとなった。その中で、収入に相当の減少があった納税者の国税・地方税及び社会保険料について、無担保かつ延滞金なしで1年間、納付を猶予する特例を設けること、とされている。

今回の特例猶予制度については、法律の改正後、できるだけ速やかに申請や猶予の決定が行われるようにするとともに、課税団体窓口への来庁が不要な申請について、新たにeLTAX（地方税ポータルシステムの呼称で、地方税における手続をインターネットを利用して電

子的に行うシステム。以下「e L T A X」という。)による電子申請を対象に加えることとした、と国から示されている。

このことから、従前から面談、書面等にて相談や申請を受けていた新型コロナウイルス感染症等に係る徴収猶予の特例申請について、内閣総理大臣から緊急事態宣言及び外出自粛要請がなされている状況や新型コロナウイルス感染症リスクの低減を図ること並びに市民負担の軽減及び利便性向上の観点から、e L T A X並びに神奈川県及び県内市町村で利用する電子自治体共同運営システム（以下「共同運営システム」という。）による電子申請の受付を行うこととした。

以上のことから、この電子申請による受付について、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) 対象手続

新型コロナウイルス感染症等に係る徴収猶予の特例申請

(3) 電子申請・届出システムの利用

ア コンピュータ処理を行う必要性について

できるだけ速やかに申請や猶予の決定を行う必要があること、新型コロナウイルス感染症リスクの低減を図ること並びに市民の負担軽減及び利便性向上の観点からコンピュータ処理を行う必要がある。

イ 電子申請・届出システムで取り扱う個人情報について

氏名、生年月日、住所、電話番号等、徴収猶予申請書に関すること（住所、氏名、生年月日、収入、支出等）、収支の明細書に関すること（住所、氏名、収入、支出、家族の状況等）、財産収支状況書に関すること（住所、氏名、収入、支出、財産等の状況等）、財産目録に関すること（住所、氏名、財産の状況等）等

(4) e L T A Xについて

ア e L T A Xの安全対策

緊急の時的な対策であり、e L T A Xの既存機能（税務代理権限証書）を流用するものである。なお、2013年（平成25年）9月12日付け藤沢市個人情報保護制度運営審議会答申第591号及び第592号で答申されたシステムである。

(ア) 申請者がe L T A Xへのアクセスを行う際は、利用者ID及び暗証番号の入力を行うことで不正なアクセスを防止している。

(イ) 申請者が申請等データをe L T A Xへ送信する際は、電子証明書によって電子署名を行い、第三者によるなりすましやデータ改ざんを防止している。

(ウ) 必要な場面でSSL方式の暗号化を行い、個人情報の盗難防止

をしている。また、個人情報記録するデータベースやサーバはファイアウォールとアクセス監視システムなどによりセキュリティが確保されている。

イ 契約方法

本市では、e L T A Xサービスの利用については、国税連携及び公的年金に係る特別徴収事務において、A S P事業者に委託して行う共同利用型を採用しており、今回の電子申請についてもA S P共同利用型で行う。

ウ 本市の安全対策

(ア) 端末利用者の制限

e L T A X送受信端末の審査システムを使用する際には、担当者を限定し、端末起動時及びスクリーンセイバー解除時に生体認証を行うことで、端末利用を制限する。また、ログイン時のI D及びパスワードについても担当者を限定し、付与することにより、不正アクセスを防止している。

(イ) 受信したデータの管理

e L T A X送受信端末にて受信したデータは、申請書形式の紙媒体に印刷し、藤沢市行政文書取扱規程に従い保存している。

(5) 共同運営システムについて

2015年（平成27年）3月12日付け藤沢市個人情報保護制度運営審議会答申第718号で答申されたシステムである。

ア 共同運営システムの安全対策

(ア) ネットワーク

利用者側が通信するインターネットからのセキュリティがファイアウォール等により十分に確保されている。また、インターネット通信はS S Lを利用した暗号化により情報の外部漏えいを防いでいる。

職員は専用回線の総合行政ネットワーク（L G W A N）を利用している。システムのログインにはファイアウォールによるセキュリティが確保され、L G W A Nについてもファイアウォールによるセキュリティ管理が行われている。

(イ) 施設要件

当該システムのインターネットデータセンター施設は、情報システム安全対策基準への適合及びL G W A N－A S Pの必要条件を満たしている。

(ウ) 管理基準

サービス提供事業者のセキュリティポリシーが管理基準となっており、運用・保守業務については、国際標準規格のI T I L

に基づき構築し、SLM（サービスレベルマネジメント）を行っている。

SLMについては、ISO9001に適合するよう管理策を講じ、運用・保守業務に係る個人情報保護対策及び情報セキュリティ対策については、ISO15001及びISO/IEC27001（ISMS）に基づく体系的な管理策を講じている。また、プライバシーマーク制度の使用許諾事業者認定も取得している。

イ 契約方法

システムを運営するNTTデータ関西支社と神奈川県が提供委託業務契約を締結して運用し、本市は神奈川県と協定を締結し、システムを利用している。また、本市はシステムを運営する同社と神奈川電子自治体共同運営サービス電子申請システム提供委託業務における個人情報の取扱いに関する協定を締結することにより、個人情報を適切に管理するよう指導監督を行っている。

ウ 本市の安全対策

(ア) 端末利用者の制限

共同運営システムを使用する際には、担当者を限定し、端末起動時及びスクリーンセイバー解除時に生体認証を行うことで、端末利用を制限する。また、ログイン時のID及びパスワードについても担当者ごとに付与することにより、不正アクセスを防止している。

(イ) 受信したデータの管理

共同運営システムで受信したデータは、申請書形式の紙媒体に印刷し、藤沢市行政文書取扱規程に従い保存している。

(6) 実施時期

2020年（令和2年）4月30日

(7) 添付資料

ア 令和2年4月30日総務省自治税務局企画課長通知「新型コロナウイルス感染症等に係る徴収猶予の特例の取扱いについて」

イ 令和2年4月27日総務省自治税務局電子化推進室事務連絡「新型コロナウイルス感染症緊急経済対策における徴収猶予の特例（案）における電子申請について」

ウ 徴収猶予申請書

エ 収支の明細書

オ 財産収支状況書

カ 財産目録

キ 国税連携システム機能イメージ

ク 国税連携概要イメージ図

ケ 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。

できるだけ速やかに申請や猶予の決定を行う必要があること、新型
コロナウイルス感染症リスクの低減を図ること並びに市民の負担軽
減及び利便性向上の観点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

実施機関が「2 実施機関の説明要旨」(4)ア及びウ並びに(5)ア及
びウに示す安全対策は、次のとおりである。

ア e L T A Xの安全対策

- (ア) ネットワークへの不正アクセスを防止するための措置
(4)ア(ア)
- (イ) 情報の改ざんを防止するための措置
(4)ア(イ)
- (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
(4)ア(ウ)
- (エ) データの安全性を高めるための措置
(4)ア(ウ)
- (オ) 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
(4)ウ(ア)
- (カ) 日常的な安全対策
(4)ウ(イ)

イ 共同運営システムの安全対策

- (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
(5)ア(ア)
- (イ) データの安全性を高めるための措置
(5)ア(ア)
- (ウ) 安全対策を確認できるようにするための措置
(5)ア(イ), (5)ア(ウ)
- (エ) 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

(5)ウ(ア)

(オ) 日常的な安全対策

(5)ウ(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