特定個人情報保護評価書（重点項目評価書）

評価書番号	評価書名
49	地方税の収滞納に関する事務　重点項目評価書

個人のプライバシー等の権利利益の保護の宣言	
藤沢市は、地方税の収滞納に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。	
特記事項	

評価実施機関名
藤沢市長

公表日
令和7年2月26日

［令和6年10月　様式3］

項目一覧

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	地方税の収滞納に関する事務
②事務の内容	地方税法及び藤沢市市税条例に基づき、地方税の収滞納に関する事務として、次の手続きを行っている。 (1) 市税について公正・公平な徴収事務を行う。また、市税に関する徴収に必要な情報の把握に努め、 法令に基づき適正な滞納整理事務を行う。 (2) 金融機関等からの納付書兼納入済通知書等により収納状況を確認する。 (3) 過誤納付により納付額が課税額を超過している場合は、過誤納還付通知書を送付し、超過額を還付する。 (4) 補助金等給付事務に係る納税確認を行う。 (5) 納税者からの納付がない、又は納付額が課税額に満たない場合、納税者に対し督促状を送付する。 (6) 市外等へ転出した滞納者の居住先での滞納情報等（犯則事件の調査を含む。）の実態調査を行う。 (7) 督促状発送後、納税者からの納付がない場合は、滞納処分を行う。 藤沢市は、行政手続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（以下「番号法」という。）の規定に従い、特定個人情報を次の事務で取り扱う。 (1) 賦課及び収納情報に基づく市税の収納、還付、充当を行う収納管理業務 (2) 滞納情報による督促状の送付、滞納者の調査（犯則事件の調査を含む。）、滞納処分を行う滞納管 理業務 (3) 収納管理システムにおける滞納者情報に係る宛名の名寄せ等宛名管理業務
③対象人数	[　10万人以上30万人未満　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	収納管理システム
②システムの機能	賦課情報取込 ・賦課情報登録機能 個人住民税業務より、賦課情報を受け取り、収納情報に登録する。 更正が行われた場合は、更正処理後の賦課情報も受け取る。 収納 ・消込機能 納税義務者または各機関より各種納付情報を受け取り、収納情報の消込処理を行う。 ・還付、充当機能 還付、充当の対象者を抽出し、充当先がある場合は、充当処理を行い、納税義務者へ充当通知書を通知する。 督促を実施しても納付が行われない納税者を抽出し、段階的に催告書を出力する。 口座振替管理機能 納税者より口座振替に関する申込、変更、取消等を受け付け、金融機関へ照会等を行い、納付方法を登録、 変更、取消を行う。 滞納繰越: ・滞納繰越機能 前年度の滞納分について、滞納繰越処理を行う。 発行: ・ 各種証明書発行機能 納税(付)証明書、完納証明書等を作成、交付する。 ・ 納付書再発行機能 照会: ・ 収納情報照会機能 該当の者に対する、課税・収納情報等を照会する。 会計資料作成: 収入日計表、収納月計表等の各種会計資料が作成できる。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [○] その他　（個人住民税システム、固定資産税システム、軽自動車税システム、滞納管理システム）
システム2～5	

システム2	
①システムの名称	滞納管理システム
②システムの機能	滞納整理 ・滞納者登録機能 収納情報より、滞納者を抽出し、滞納情報に登録する。 ・催告機能 督促を促しても納付しない納税者に対して、催告書を出力する。 ・相談対応機能 納税者より徴収猶予の申請を受付け、審査結果を登録する。 納税義務者の納税計画に対する納税誓約書を受け取り、情報を管理する。 納税義務者より、延滞金減免の申請を受付け、審査結果を登録する。 ・処分機能 財産調査 収滞納情報に基づき、各外部機関に財産に関する調査を行い、財産情報を登録する。 交付要求 裁判所、破産管財人、行政機関等からの債務者情報に対し、交付要求を行う。 交付要求を行った旨を登録し、滞納者に通知する。 差し押さえ 財産情報及び滞納情報に基づき、差押書を作成し、滞納者へ通知する。 財産を差し押さえ、差押情報を登録する。 公売（換価） 差し押さえた財産に基づき、滞納者に換価通知書を送付して、公売を行い、換価情報を登録する。 執行停止 所在不明、財産なし、資力なし等の徴収不能者に対して、滞納処分の執行を停止し、執行停止情報を登録する。 決算： ・不納欠損 執行停止及び時効により納税義務が消滅した時、滞納情報から該当データを抹消する。 ・滞納繰越 前年度の滞納分について、滞納繰越処理を行う。 発行： ・ 各種証明書発行機能 各種証明書等を作成、交付する。 ・ 納付書再発行機能 照会： ・滞納納情報照会機能 該当の者に対する、滞納情報等を照会する。 統計資料作成： 必要な統計資料を作成し、該当期間に報告する。
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [○] 宛名システム等　　[　　] 税務システム [○] その他　（ 収納管理システム　　）

システム3	
①システムの名称	宛名管理システム
②システムの機能	(1) 宛名情報管理機能 ・既存住民基本台帳システムに登録された情報を取得する。 ・藤沢市固有の識別番号(以下「宛名番号」という。)の付番を行い、個人番号にひも付けて管理する。 (2) 住民登録外者登録機能 ・住民登録登録外者の氏名・住所などの4情報等を登録し、宛名番号を付番する。 (3) 法人登録機能 ・特別徴収義務者の会社名・住所等を登録し、宛名番号を付番する。 (4) 送付先情報登録機能 ・申請書に基づき、送付先情報の登録・管理する。 (5) 相続人・納税管理人登録機能 ・申請書に基づき、相続人・納税管理人の登録・管理する。 (6) 口座情報管理機能 ・申請書に基づき、口座情報の登録・管理する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[○] 税務システム [　] その他　(　)
システム4	
①システムの名称	中間サーバ
②システムの機能	1. 各種設定機能 利用する職員のアカウント登録、権限管理等の設定 等。 2. 符号取得機能 団体内統合宛名システムにて保持している団体内統合宛名番号を利用し、符号を取得する。 3. 情報提供用のデータ登録機能 特定個人情報(連携対象)の登録を行う。 4. 情報照会機能 情報提供の求めを行い、特定個人情報(連携対象)を取得する。 5. 情報提供機能 情報提供の求めに対して、特定個人情報(連携対象)の提供を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [　] その他　(　)

システム5	
①システムの名称	団体内統合宛名システム
②システムの機能	1　団体内統合宛名番号管理 ・団体内統合宛名番号管理機能 団体内統合宛名番号の付番を行う。 団体内統合宛名番号と既存住基システムの宛名番号をひも付けて管理する。 ・宛名情報管理機能 氏名・住所などの4情報を団体内統合宛名番号にひも付けて管理する。 ・中間サーバー連携機能 中間サーバーとのオンラインデータ連携、オフラインデータ連携用の媒体作成を行う。
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [○] 宛名システム等　　[○] 税務システム [○] その他　（ 中間サーバ　　）
システム6～10	
システム11～15	
システム16～20	

3. 特定個人情報ファイル名
1. 収納情報ファイル 2. 滞納情報ファイル

4. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項及び別表24の項

5. 情報提供ネットワークシステムによる情報連携 ※		
①実施の有無	[　　実施する　　]	＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	利用特定個人情報提供主務省令第2条の表48の項	

6. 評価実施機関における担当部署	
①部署	財務部　納税課
②所属長の役職名	納税課長

7. 他の評価実施機関

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
収納情報ファイル		
2. 基本情報		
①ファイルの種類　※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		賦課期日（1月1日）時点で当市に住所を有する個人、または当市内に事業所または家屋敷を有する個人で当市に住所を有しない者で、所得にかかる各種申告（給与支払報告書、公的年金支払報告書、確定申告書等）があった者
	その必要性	地方税法第34条および第45条の2～第45条の3の3、地方税法294条および317条の2に基づいて課税された賦課情報を使用するため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目　※	・識別情報 [○]個人番号　[　]個人番号対応符号　[○]その他識別情報（内部番号） ・連絡先等情報 [　]4情報（氏名、性別、生年月日、住所）　[　]連絡先（電話番号等） [　]その他住民票関係情報 ・業務関係情報 [　]国税関係情報　[○]地方税関係情報　[　]健康・医療関係情報 [　]医療保険関係情報　[　]児童福祉・子育て関係情報　[　]障害者福祉関係情報 [　]生活保護・社会福祉関係情報　[　]介護・高齢者福祉関係情報 [　]雇用・労働関係情報　[　]年金関係情報　[　]学校・教育関係情報 [　]災害関係情報 [　]その他　（　　）
	その妥当性	個人番号：滞納情報の個人を正確に特定するために保有（参照）する。 その他識別情報（内部番号）：当市において、個人を一意に識別するためにシステム独自の識別番号（宛名番号）を保有する。 地方税関係情報：納付の元となる課税（調定）情報を保有する。
	全ての記録項目	別添1を参照。
⑤保有開始日		平成28年1月1日
⑥事務担当部署		財務部　納税課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ ） [○] 行政機関・独立行政法人等 （ ） [○] 地方公共団体・地方独立行政法人 （ ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [○] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ 収納管理システム ）
③使用目的 ※		納税義務者の個人番号を利用し、より正確且つ効率的な徴収事務を行うため。
④使用の主体	使用部署	財務部 納税課
	使用者数	[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑤使用方法		Ⅰ．徴収事務 同一納税義務者にも関わらず、複数の収納情報が発生していた場合の名寄せを行うために個人番号を利用する。
	情報の突合	Ⅰ．徴収事務 ・収納情報を照合するにあたり、個人番号を利用して名寄せを実施する。
⑥使用開始日		平成28年1月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ）件
委託事項1		住民情報システムCokas-iの構築及び運用保守等
①委託内容		住民情報システムCokas-iの構築及び運用保守等
②委託先における取扱者数		[100人以上500人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		日本電気株式会社 神奈川支社
再委託	④再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	委託先より再委託承諾願いを収受し、再委託承諾書を通知する。なお、委託先との契約に含まれている「機密の保持」について、再委託先にも遵守を義務付けている。
	⑥再委託事項	上記委託内容と同様。

委託事項2～5	
委託事項6～10	
委託事項11～15	
委託事項16～20	
5．特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[　] 提供を行っている　（　　）件　[　] 移転を行っている　（　　）件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[　] 情報提供ネットワークシステム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　] 庁内連携システム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	

移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	
6. 特定個人情報の保管・消去	
保管場所　※	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証（ログイン）、認可（処理権限の付与）、監査（ログ運用）を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー･プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事 業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セ キュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアッ プも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存され る。
7. 備考	

（別添１）特定個人情報ファイル記録項目

収納情報ファイル

	項目名
１	賦課年度（賦課決定された年度）
２	課税年度（本来課税すべき年度）
３	科目
４	期別
５	宛名番号
６	個人番号（※）
７	調定情報
８	調定額
９	納期限
１０	納付情報
１１	納付額
１２	納付年月日
１３	更新年月日
１４	更新職員ID

※　個人番号は、宛名番号と紐づけて宛名管理システムの情報から参照する。

Ⅲ　リスク対策　※(7. ②を除く。)

1. 特定個人情報ファイル名	
収納情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク:　目的外の入手が行われるリスク	
リスクに対する措置の内容	＜運用における措置＞ 収納情報ファイルについては、課税台帳情報ファイルに登録されている課税情報から作成されるものであり、課税情報については、当市課税課で取り扱う特定個人情報ファイル（課税対象者情報ファイル、課税資料ファイル、課税台帳情報ファイル、資産情報ファイル、軽自動車税情報ファイル）から入手した情報を元に作成されている。収納情報ファイルについては、次のとおり措置が講じられた情報を使用している。 【課税対象者情報ファイル】 ・賦課期日（1月1日）時点で当市に住所を有していたかどうかについては、最新の住民情報を管理している既存住民基本台帳システムより情報の移転を受けており、対象外の住民に対する課税が発生しないよう、賦課期日近辺の異動者については、特に注意をして確認を行っている。 ・その他、特定個人情報の取り扱いに関しては、当市セキュリティポリシーに準ずる。 【課税資料ファイル】 ・賦課期日（1月1日）時点での課税対象者情報に記録のない申告情報については、当該市町村で課税するかどうかを判断した上で、課税する場合は、住民票上の住所地市町村に対して通知する等を行っており、目的の範囲を超えた入手が行われない対策をとっている。（地方税法第294条） ・課税対象でない場合は、当該市町村を調査した上で、郵送等により当該市町村へ情報を伝達している。 【課税台帳情報ファイル】 課税対象者情報ファイル、課税資料ファイル、資産情報ファイルと同等の措置を講じている。 【資産情報ファイル】 ・提出された申告情報については、当該市町村で所有されている資産であるかを判断した上で、その所有者の確認を行っており、目的の範囲を超えた入手が行われない対策をとっている。 ・課税対象でない申告を受理した場合は、当人へ連絡等を行うことで対象者以外の情報を入手しない等の措置を講じている。 【軽自動車税情報ファイル】 ・賦課期日時点で当市に住所を有していたかどうかについては、最新の住民情報を管理している既存住民基本台帳システムより情報の移転を受けており、対象外の住民に対する課税が発生しないよう、賦課期日近辺の異動者については、特に注意をして確認を行っている。 ・その他、特定個人情報の取り扱いに関しては、当市セキュリティポリシーに準ずる。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
リスクに対する措置の内容	＜収納管理システム（宛名管理機能）における措置＞ 宛名管理システムにおいては、個人番号関連業務以外は個人番号にアクセスできないよう、個人番号を宛名情報（4情報）とは物理的に分けて管理しており、番号利用事務（システム）以外では、アクセスできないようにしている。 ＜収納管理システムにおける措置＞ ・番号利用業務以外の部門（条例に規定されていない業務も含む）における照会では、操作権限により、個人番号が参照できないような仕組みが構築されている。（個人番号を物理的に表示しない）また、収納管理システムに対して、不要なアクセスができないよう、適切なアクセス制御対策を実施している。 ・収納管理システムにおいては、システム操作に関する操作履歴の記録を適切な方法で実施している。 ＜収納管理システムの運用における措置＞ ・収納管理システムの稼働するLANでは、外部からの侵入ができないようファイアウォールによる適切なアクセス制御を実施している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	・端末のログイン時は生体認証、業務システムへのログイン時は生体認証による識別とパスワードによる認証を実施しており、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施している。 ・システムの利用できる端末を管理することにより、不要な端末からの利用ができないような制限を実施している。 ・認証パスワードについては、現在有効であるか、適切なパスワード値であるか否かをシステムでチェックしている。有効期限までに変更を行わない場合は、対応するユーザIDが失効される。
その他の措置の内容	システムは画一的に管理されており、利用可能時間外には業務端末にアクセスすることができないようになっている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
・端末から離れる時は初期画面に戻す。 ・端末のディスプレイは来庁者から見えない位置に置く。 ・個人情報の画面のハードコピー及び打ち出した本人確認情報は、事務処理に必要最低限の範囲で行うものとし、確実に機密文書として破棄する	

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
リスク: 委託先における不正な使用等のリスク		
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　　定めている　　]	＜選択肢＞ 1）定めている　　2）定めていない
規定の内容	データの保護及び秘密の保持等に関する仕様書にて、以下の内容を明記 ・藤沢市個人情報の保護に関する条例の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複写及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の破棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務	
再委託先による特定個人情報ファイルの適切な取扱いの担保	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　　4）再委託していない
具体的な方法	・再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・再委託契約終了後の特定個人情報の返却または廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定等 ・また、再委託先が当市と同等の安全管理措置を講じていることを確認する。	
その他の措置の内容	＜運用における措置＞ 特定個人情報ファイルの取扱いの記録を残しており、委託側において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク: 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[ ]	<選択肢> 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続	[　] 接続しない（入手）　[○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	＜団体内統合宛名システムにおける措置＞ ・各業務システムから中間サーバーあての情報照会要求の中継においては、照会元・照会先・照会内容等の改変は行わないことで、中間サーバーにおける目的外入手の抑制の措置に従うことを担保する。 ・接続システムの認証及び団体内統合宛名システム接続端末での職員認証等の機能を備えており、あらかじめ承認されたシステム・職員以外の情報入手を抑止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応する。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログ アウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切 なオンライン連携を抑止する。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。 ＜中間サーバーの運用における措置＞ 中間サーバーに対する職員認証・利用権限の設定にあたっては、中間サーバを利用する最低限の職員のみユーザー登録を行い、必要最低限の利用権限を付与することで目的外の入手が行われるリスクに対応。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保する。 ・中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保する。 ・中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	

7. 特定個人情報の保管・消去		
リスク: 特定個人情報の漏えい・滅失・毀損リスク		
①事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容		
再発防止策の内容		
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

＜特定個人情報が消去されずいつまでも存在するリスク＞
保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。
（ガバメントクラウドにおける措置）
データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。
＜物理的な対策＞
・サーバー室とデータ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする
・出入り口には機械による入退室を管理する設備を設置する。
・入退室管理を徹底するため出入口の場所を限定する。
・監視設備として監視カメラ等を設置する。
・業務用端末は、盗難防止用ワイヤーを設置する。
＜中間サーバー・プラットフォームにおける措置＞
・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。
・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。
（ガバメントクラウドにおける措置）
①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。
②事前に許可されていない装置等に関しては、外部に持出できないこととしている。

＜技術的な対策＞
・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。
・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。
・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。
（中間サーバー・プラットフォームにおける措置）
・中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。
・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。
・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。
（ガバメントクラウドにおける措置）
①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。
②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。
③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。
④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。
⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。
⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。
⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。
⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。

8. 監査			
実施の有無	[○] 自己点検	[○] 内部監査	[　] 外部監査

9. 従業者に対する教育・啓発			
従業者に対する教育・啓発		[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
	具体的な方法	・「マイナンバー制度に係る職員等の教育研修計画」に基づき、個人番号利用事務実施課を対象にした集合研修を実施するとともに、受講者が課内へ研修内容の周知を行っている。また、職員全員を対象に、毎年電子上での机上研修（eラーニング）による個人情報保護及び情報セキュリティに関する研修を実施している。 ・中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施する。 ・中間サーバー・プラットフォームの業務に就く場合は、運用規則等について研修を行う。	

10. その他のリスク対策

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
滞納情報ファイル		
2. 基本情報		
①ファイルの種類　※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		賦課期日（1月1日）時点で当市に住所を有する個人、または当市内に事業所または家屋敷を有する個人で当市に住所を有しない者で、所得にかかる各種申告（給与支払報告書、公的年金支払報告書、確定申告書等）により課税された者で、かつ指定された納期限までに徴収金を完納できなかった者
	その必要性	地方税法第331条、第334条に基づき、滞納された個人住民税の徴収を適正に行うため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目　※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [　] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[○] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	個人番号：滞納情報の個人を正確に特定するために保有（参照）する。 その他識別情報（内部番号）：当市において、個人を一意に識別するためにシステム独自の識別番号（宛名番号）を保有する。 地方税関係情報：納付の元となる課税（調定）情報を保有する。
	全ての記録項目	別添1を参照。
⑤保有開始日		平成28年1月1日
⑥事務担当部署		財務部　納税課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ ） [○] 行政機関・独立行政法人等 （ ） [○] 地方公共団体・地方独立行政法人 （ ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [○] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ 収納管理システム ）
③使用目的 ※		納税義務者の個人番号を利用し、より正確且つ効率的な滞納整理事務を行うため。
④使用の主体	使用部署	財務部 納税課
	使用者数	[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑤使用方法		Ⅰ. 滞納整理事務 同一納税義務者にも関わらず、複数の滞納情報が発生していた場合の名寄せを行い、滞納情報を一元管理する。
	情報の突合	Ⅰ. 滞納整理事務 ・滞納情報を照合するにあたり、個人番号を使用して名寄せを実施する。
⑥使用開始日		平成28年1月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ）件
委託事項1		住民情報システムCokas-iの構築及び運用保守等
①委託内容		住民情報システムCokas-iの構築及び運用保守等
②委託先における取扱者数		[100人以上500人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		日本電気株式会社 神奈川支社
再委託	④再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	委託先より再委託承諾願いを収受し、再委託承諾書を通知する。なお、委託先との契約に含まれている「機密の保持」について、再委託先にも遵守を義務付けている。
	⑥再委託事項	上記委託内容と同様。

委託事項2～5	
委託事項6～10	
委託事項11～15	
委託事項16～20	
5．特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[　] 提供を行っている　（　　）件　[　] 移転を行っている　（　　）件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[　] 情報提供ネットワークシステム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　] 庁内連携システム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	

移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	
6．特定個人情報の保管・消去	
保管場所　※	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証（ログイン）、認可（処理権限の付与）、監査（ログ運用）を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。 （ガバメントクラウドにおける措置） ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事 業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セ キュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアッ プも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存され る。
7．備考	

（別添1）特定個人情報ファイル記録項目

滞納情報ファイル

	項目名
1	宛名番号
2	個人番号（※）
3	財産情報
4	財産区分
5	処分情報
6	処分年月日
7	処分解除年月日
8	処分完了年月日
9	賦課年度
10	課税年度
11	科目
12	期別
13	分納情報
14	誓約年月日
15	誓約解除年月日
16	賦課年度
17	課税年度
18	科目
19	期別
20	執行停止情報
21	停止年月日
22	取消年月日
23	賦課年度
24	課税年度
25	科目
26	期別
27	更新年月日
28	更新職員ID

※　個人番号は、宛名番号と紐づけて宛名管理システムの情報から参照する。

Ⅲ　リスク対策　※(7. ②を除く。)

1. 特定個人情報ファイル名	
滞納情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク:　目的外の入手が行われるリスク	
リスクに対する措置の内容	＜運用における措置＞ 滞納情報ファイルについては、課税台帳情報ファイルに登録されている課税情報及び収納情報ファイルから作成されるものであり、本項は「Ⅲ　リスク対策（収納情報ファイル）」-「2.特定個人情報の入手」-「リスクに対する措置の内容」に記載されている措置が講じられた情報を使用している。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
3. 特定個人情報の使用	
リスク1:　目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
リスクに対する措置の内容	＜滞納管理システム（宛名管理機能）における措置＞ 宛名管理システムにおいては、番号利用事務以外で個人番号が取得されることのないように、番号利用事務（システム）以外で個人番号での検索を行うことはできない。また、番号利用事務（システム）以外では個人番号は画面表示されない。 ＜滞納管理システムにおける措置＞ ・番号利用業務以外の部門（条例に規定されていない業務も含む）における照会では、操作権限により、個人番号が参照できないような仕組みが構築されている。（個人番号を物理的に表示しない）また、滞納管理システムに対して、不要なアクセスができないよう、適切なアクセス制御対策を実施している。 ・滞納管理システムにおいては、システム操作に関する操作履歴の記録を適切な方法で実施している。 ＜滞納管理システムの運用における措置＞ ・滞納管理システムの稼働するLANでは、外部からの侵入ができないようファイアウォールによる適切なアクセス制御を実施している。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	・端末のログイン時は生体認証、業務システムへのログイン時は生体認証による識別とパスワードによる認証を実施しており、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施している。 ・システムの利用できる端末を管理することにより、不要な端末からの利用ができないような制限を実施している。 ・認証パスワードについては、現在有効であるか、適切なパスワード値であるか否かをシステムでチェックしている。有効期限までに変更を行わない場合は、対応するユーザIDが失効される。	
その他の措置の内容	システムは画一的に管理されており、利用可能時間外には業務端末にアクセスすることができないようになっている。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
・端末から離れる時は初期画面に戻す。 ・端末のディスプレイは来庁者から見えない位置に置く。 ・個人情報の画面のハードコピー及び打ち出した本人確認情報は、事務処理に必要最低限の範囲で行うものとし、確実に機密文書として破棄する		
4. 特定個人情報ファイルの取扱いの委託		**[ ] 委託しない**
リスク： 委託先における不正な使用等のリスク		
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	＜選択肢＞ 1）定めている　2）定めていない
規定の内容	データの保護及び秘密の保持等に関する仕様書にて、以下の内容を明記 ・藤沢市個人情報の保護に関する条例の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複写及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の破棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務	

再委託先による特定個人情報ファイルの適切な取扱いの担保	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　　4）再委託していない
具体的な方法	・再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・再委託契約終了後の特定個人情報の返却または廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定等 ・また、再委託先が当市と同等の安全管理措置を講じていることを確認する。	
その他の措置の内容	＜運用における措置＞ 特定個人情報ファイルの取扱いの記録を残しており、委託側において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）　［ ○ ］提供・移転しない		
リスク:　不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[　　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[　　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置

6. 情報提供ネットワークシステムとの接続	[○] 接続しない（入手）	[○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2：不正な提供が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		

7. 特定個人情報の保管・消去		
リスク： 特定個人情報の漏えい・滅失・毀損リスク		
①事故発生時手順の策定・周知	[十分に行っている]	＜選択肢＞ 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	＜選択肢＞ 1）発生あり 2）発生なし
その内容		
再発防止策の内容		
その他の措置の内容		

リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置

＜特定個人情報が消去されずいつまでも存在するリスク＞
保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。
（ガバメントクラウドにおける措置）
データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。
＜物理的な対策＞
・サーバー室とデータ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする
・出入り口には機械による入退室を管理する設備を設置する。
・入退室管理を徹底するため出入口の場所を限定する。
・監視設備として監視カメラ等を設置する。
・業務用端末は、盗難防止用ワイヤーを設置する。
（ガバメントクラウドにおける措置）
①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。
②事前に許可されていない装置等に関しては、外部に持出できないこととしている。

＜技術的な対策＞
・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。
・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。
・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。
（ガバメントクラウドにおける措置）
①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。
②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。
③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。
④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。
⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。
⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。
⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。
⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。

8. 監査

実施の有無	[○] 自己点検	[○] 内部監査	[　] 外部監査

9. 従業者に対する教育・啓発			
従業者に対する教育・啓発		[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
	具体的な方法	・「マイナンバー制度に係る職員等の教育研修計画」に基づき、個人番号利用事務実施課を対象にした集合研修を実施するとともに、受講者が課内へ研修内容の周知を行っている。また、職員全員を対象に、毎年電子上での机上研修（eラーニング）による個人情報保護及び情報セキュリティに関する研修を実施している。 ・中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施する。 ・中間サーバー・プラットフォームの業務に就く場合は、運用規則等について研修を行う。	

10. その他のリスク対策

Ⅳ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	藤沢市　市民自治部　市民相談情報課　情報公開センター 〒251－8601　神奈川県藤沢市朝日町1－1 0466－50－3567
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
③法令による特別の手続	
④個人情報ファイル簿への不記載等	
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	藤沢市　財務部　納税課 〒251－8601　神奈川県藤沢市朝日町1－1 0466－50－3509
②対応方法	・問合せを受け付けた場合、問合せ内容及びこれに係る対応について、記録を作成し残す。 ・情報の漏えい等の重大な事案に関する問合せについて、関係先等に事実確認を行うため、処理期間を設ける。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年1月16日
②しきい値判断結果	[　　基礎項目評価及び重点項目評価の実施が義務付けられる　　] ＜選択肢＞ 1）基礎項目評価及び重点項目評価の実施が義務付けられる 2）基礎項目評価の実施が義務付けられる（任意に重点項目評価を実施） 3）特定個人情報保護評価の実施が義務付けられない（任意に重点項目評価を実施）
2. 国民・住民等からの意見の聴取 【任意】	
①方法	
②実施日・期間	
③主な意見の内容	
3. 第三者点検 【任意】	
①実施日	
②方法	
③結果	

（別添2）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年3月12日	表紙 個人のプライバシー等の権利利益の保護の宣言 特記事項	本評価書による事務の開始は，システム再構築後の運用開始を予定している令和3年1月からとなるため，新規に評価書を作成しています。このため，令和2年12月末までは，現行評価書による運用となります。	（削除）	事後	運用を開始したことによる記載内容の削除のため、重要な変更に当たらない。
令和3年3月12日	Ⅰ基本情報　5．情報提供ネットワークシステムによる情報連携②法律上の根拠	番号法第9条第7号及び別表第二 （別表第二における情報提供の根拠） なし（提供を行わない）	（削除）	事後	記載の見直しのため、重要な事項に該当しない。
令和3年3月12日	Ⅲリスク対策（収納情報F） 6．情報提供ネットワークシステムとの接続	接続しない（提供）	接続しない（入手）　接続しない（提供）	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和3年3月12日	Ⅲリスク対策（滞納情報F） 6．情報提供ネットワークシステムとの接続	接続しない（提供）	接続しない（入手）　接続しない（提供）	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和6年12月18日	Ⅰ 基本情報　4．個人番号の利用	番号法第9条第1項及び別表第一　16の項	番号法第9条第1項及び別表　24の項	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和6年12月18日	Ⅲリスク対策（滞納情報F） 6．情報提供ネットワークシステムとの接続	接続しない（入手）　接続しない（提供）	接続する（入手）　接続しない（提供） 根拠法令　利用特定個人情報提供主務省令第2条の表48の項	事前	
令和6年12月18日	Ⅴ評価実施手続	令和2年3月9日	令和6年11月15日	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和7年2月26日	Ⅱ 特定個人情報ファイルの概要（収納情報F） 4．特定個人情報ファイルの取扱いの委託	委託の有無　委託しない	委託の有無　委託する 委託事項1　住民情報システムCokas-iの構築及び運用保守等 ①委託内容　住民情報システムCokas-iの構築及び運用保守等 ②委託先における取扱者数　100人以上500人未満 ③委託先名　日本電気株式会社　神奈川支社 ④再委託の有無　再委託する ⑤委託先の許諾方法　委託先より再委託承諾願いを収受し、再委託承諾書を通知する。なお、委託先との契約に含まれている「機密の保持」について、再委託先にも遵守を義務付けている。 ⑥再委託事項　上記委託内容と同様。	事前	
令和7年2月26日	Ⅱ 特定個人情報ファイルの概要（滞納情報F） 4．特定個人情報ファイルの取扱いの委託	委託の有無　委託しない	委託の有無　委託する 委託事項1　住民情報システムCokas-iの構築及び運用保守等 ①委託内容　住民情報システムCokas-iの構築及び運用保守等 ②委託先における取扱者数　100人以上500人未満 ③委託先名　日本電気株式会社　神奈川支社 ④再委託の有無　再委託する ⑤委託先の許諾方法　委託先より再委託承諾願いを収受し、再委託承諾書を通知する。なお、委託先との契約に含まれている「機密の保持」について、再委託先にも遵守を義務付けている。 ⑥再委託事項　上記委託内容と同様。	事前	

令和7年2月26日	Ⅱ 特定個人情報ファイルの概要(収納情報F) 6. 特定個人情報の保管・消去	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	
令和7年2月26日	Ⅱ 特定個人情報ファイルの概要(滞納情報F) 6. 特定個人情報の保管・消去	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。	当市では収納管理に係る情報を電磁的記録媒体で調製しており、以下に示した条件を満たしているサーバ内にデータとして保管している。 ・権限のない者が入室できないよう入退室管理システムによる入退室の制御がなされ、監視カメラにより監視されているサーバ室にサーバを設置している。 ・サーバ室はICカード、生体認証等により、許可された者のみが入室できることとしている。 ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザID・生体認証による識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。 ・届出書等の関係帳票類は、入退室管理をする執務室内において、鍵付きキャビネット等で保管している。 (ガバメントクラウドにおける措置) ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事 業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セ キュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアッ プも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内	事前	

令和7年2月26日	Ⅲ リスク対策(収納情報F) 4. 特定個人情報ファイルの取扱いの委託	委託しない	委託契約書中の特定個人情報ファイルの取扱いに関する規定:定めている 既定の内容:データの保護及び秘密の保持等に関する仕様書にて、以下の内容を明記 ・藤沢市個人情報の保護に関する条例の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複写及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の破棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務 再委託先による定個人情報ファイルの取扱いに関する担保:十分に行っている 具体的な方法: ・再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責　任の明確化 ・再委託契約終了後の特定個人情報の返却または廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定等 ・また、再委託先が当市と同等の安全管理措置を講じていることを確認する。 その他の措置の内容: ＜運用における措置＞ 特定個人情報ファイルの取扱いの記録を残しており、委託側において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。 リスクへの対策は十分か:十分である	事前	
令和7年2月26日	Ⅲ リスク対策(滞納情報F) 4. 特定個人情報ファイルの取扱いの委託	委託しない	委託契約書中の特定個人情報ファイルの取扱いに関する規定:定めている 既定の内容:データの保護及び秘密の保持等に関する仕様書にて、以下の内容を明記 ・藤沢市個人情報の保護に関する条例の遵守 ・秘密の保持 ・指示目的以外使用及び第三者への提供の禁止 ・データの受領 ・データの持出し ・データの複写及び複製の禁止 ・安全管理義務 ・データの返却・消去 ・記録媒体の破棄 ・監督及び監査 ・従業員に対する教育の実施 ・事故発生の報告義務 再委託先による定個人情報ファイルの取扱いに関する担保:十分に行っている 具体的な方法: ・再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責　任の明確化 ・再委託契約終了後の特定個人情報の返却または廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定等 ・また、再委託先が当市と同等の安全管理措置を講じていることを確認する。 その他の措置の内容: ＜運用における措置＞ 特定個人情報ファイルの取扱いの記録を残しており、委託側において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。 リスクへの対策は十分か:十分である	事前	
令和7年2月26日	Ⅲ リスク対策(収納情報F) 6. 情報提供ネットワークシステムとの接続	接続しない(入手)　接続しない(提供)	接続しない(提供)		

令和7年2月26日	Ⅲ リスク対策(収納情報F) 6. 情報提供ネットワークシステムとの接続] リスク1目的外の入手が行われるリスク		リスクに対する措置の内容 ＜団体内統合宛名システムにおける措置＞ ・各業務システムから中間サーバーあての情報照会要求の中継においては、照会元・照会先・照会内容等の改変は行わないことで、中間サーバーにおける目的外入手の抑制の措置に従うことを担保する。 ・接続システムの認証及び団体内統合宛名システム接続端末での職員認証等の機能を備えており、あらかじめ承認されたシステム・職員以外の情報入手を抑止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可用照合リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応する。 ②中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログ アウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切 なオンライン連携を抑止する。 (※1)情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 (※2)番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 (※3)中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。 ＜中間サーバーの運用における措置＞ 中間サーバーに対する職員認証・利用権限の設定にあたっては、中間サーバを利用する最低限の職員のみユーザー登録を行い、必要最低限の利用権限を付与することで目的外の入手が行われるリスクに対応。 リスクへの対策は十分か：十分である	事前	
令和7年2月26日	Ⅲ リスク対策(収納情報F) 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保する。 ・中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保する。 ・中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの	事前	

令和7年2月26日	Ⅲ リスク対策(収納情報F) 7．特定個人情報の保管・消去 特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	＜特定個人情報が消去されずいつまでも存在するリスク＞ 保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。 ＜物理的な対策＞ ・サーバー室とデータ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする ・出入り口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。 ・業務用端末は、盗難防止用ワイヤーを設置する。 ＜技術的な対策＞ ・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。 ・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。	＜特定個人情報が消去されずいつまでも存在するリスク＞ 保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。 （ガバメントクラウドにおける措置） データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ＜物理的な対策＞ ・サーバー室とデータ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする ・出入り口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。 ・業務用端末は、盗難防止用ワイヤーを設置する。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ・事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 （ガバメントクラウドにおける措置） ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ＜技術的な対策＞ ・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。 ・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。 （中間サーバー・プラットフォームにおける措置） ・中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 （ガバメントクラウドにおける措置） ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	事前	
令和7年2月26日	Ⅲ リスク対策(滞納情報F) 7．特定個人情報の保管・消去 特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	＜特定個人情報が消去されずいつまでも存在するリスク＞ 保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。 ＜物理的な対策＞ ・サーバー室とデータ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする ・出入り口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。 ・業務用端末は、盗難防止用ワイヤーを設置する。 ＜技術的な対策＞ ・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。 ・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。	＜特定個人情報が消去されずいつまでも存在するリスク＞ 保管する情報の種類によりデータ保持年限のある情報については、保存年限を超えれば消去される。 （ガバメントクラウドにおける措置） データの復元がなされないよう、クラウド事業者において、NIST 800-88、 ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ＜物理的な対策＞ ・業務用端末は、盗難防止用ワイヤーを設置する。 （ガバメントクラウドにおける措置） ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラ ウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ＜技術的な対策＞ ・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウィルスチェックを実施する。また、新種の不正プログラムに対応するために、ウィルスパターンファイルは定期的に更新し、最新のものを使用する。 ・情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス防止策として、インターネット及び内部情報系とネットワークを分離することで、セキュリティを担保している。 （ガバメントクラウドにおける措置） ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	事前	
令和7年2月26日	Ⅴ 評価実施手続	令和6年11月15日	令和7年1月16日	事後	その他の項目の変更であり事前の提出・公表が義務付けられない