

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
2	税務総合システム 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

奈良県は、税務総合システム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の保護に取り組んでいることを宣言する。

特記事項

- ・奈良県は「地方税に関する事務」を行うために「税務総合システム」を使用している。
- ・税務総合システムに係る運用管理業務を外部業者に委託しているが、不正入手・不正使用対策として「個人情報取扱特記事項」に基づく守秘義務を課し、情報セキュリティ遵守状況を確認している。
- ・内部による不正利用防止のため、システム操作者に守秘義務を課し、ID及びパスワードにより操作者、照会範囲を限定、追跡調査のためシステムのアクセスログを保存するなど対策を講じている。

評価実施機関名

奈良県知事

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和7年10月29日

項目一覧

I 基本情報
（別添1）事務の内容
II 特定個人情報ファイルの概要
（別添2）特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
（別添3）変更箇所

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	地方税に関する事務
②事務の内容 ※	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税のうち県税の賦課徴収又は地方税のうち県税に関する調査(犯罪事件の調査を含む。)に関する事務であって主務省令で定めるもの 1 納税者からの申告及び届出等による課税管理業務 (法人県民税、法人事業税、個人事業税、不動産取得税、軽油引取税、自動車税種別割等) 2 収納及び課税の情報による収納、還付、充当等を行う収納管理業務 3 滞納者情報による催告書等送付や滞納整理を行う滞納管理業務 4 納税者のあて名情報(基本あて名、税目別あて名、課税別あて名)の管理を行うあて名管理業務 ※納税者からの申告・届出又は調査により課税し、納税通知書等を送付するとともに、納税者が納付した税金を県の歳入として受け入れ、納付額が課税額より多い場合は超過額を還付、納税者からの納付がない場合や納付額が課税額より少ない場合は督促を行った後、滞納整理を行う。 ① 納税者から提出される申告書等を受け付け、確認を行う。 ② 関係機関等からの情報により、申請書等の確認を行う。 ③ 必要に応じて納税者や申告書等の内容について、調査を行う。 ④ ①～③により課税した内容について、納税者に納税通知書を送付する。 ⑤ ①～③により決定した減免決定について、納税者に減免決定通知書等を送付する。 ⑥ 納税者が納付書により納付したことについて、金融機関からの領収済通知書により確認する。 ⑦ 納付額が課税額より多い場合は超過額を還付のうえ、納税者に還付通知書を送付する。 ⑧ 納税者からの納税証明書交付申請書を受け付け、確認を行う。 ⑨ ⑧に係る納税証明書を納税者に交付する。 ⑩ 納税者からの納付がない場合や納付額が課税額より少ない場合は、納税者に督促状を送付する。 ⑪ 督促した納税者から納付がない場合や納付額が課税額より少ない場合は、催告書の送付や滞納整理を行う。 (※詳細は、「(別添1)事務の内容」を参照)
③対象人数	[30万人以上] <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 5) 30万人以上
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	税務総合システム
②システムの機能	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税のうち県税の賦課徴収又は地方税のうち県税に関する調査(犯罪事件の調査を含む。)に関する事務であって主務省令で定めるものに関する電算処理 1 課税管理サブシステム 課税、減免等の課税管理業務を行う。 2 収納管理サブシステム 収納、還付、充当、納税証明書、督促状送付等の収納管理業務を行う。 3 滞納管理サブシステム 催告書送付や納税者単位の滞納状況及び財産、折衝記録等の滞納管理業務を行う。 4 あて名管理サブシステム 納税者のあて名情報の管理業務を行う。
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 (国税連携システム、税務総合クラウドサービス)

システム2～5

システム2

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 符号管理対応機能 中間サーバーの符号管理機能に対応するための機能 2 情報照会支援機能 中間サーバーの情報照会機能に対応する機能 3 情報提供支援機能 中間サーバーの情報提供機能に対応し、既存システムが行うべき情報提供等を支援する機能 4 基本4情報等の出力機能 中間サーバーからの情報提供要求に対応し、個人番号および基本4情報のデータを中間サーバーに通知する機能 5 団体内統合宛名番号付番機能 団体内統合宛名システム端末及び既存システムからの要求に対し、団体内統合宛名番号の割り当てを行い、業務利用番号や基本4情報と紐付ける機能 6 宛名情報等管理機能 団体内統合宛名番号を主キーとして、各情報を適切に管理する機能 7 未電算業務等対応機能 団体内統合宛名システム運用端末を用いて未電算業務等に対応するための機能 8 共通変換機能 既存システムの中間サーバー連携を支援するため、既存システムからの入出力データについて共通的に変換する機能 9 職員認証・権限管理機能 システムへログインするための認証機能およびログイン後の権限管理の機能 10 システム管理機能 システムの安定運用のために必要な機能 11 住民基本台帳ネットワークシステムとの回線連携機能
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 ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☒ その他 （ 中間サーバー、税務総合クラウドサービス ） ☐ 庁内連携システム ☐ 既存住民基本台帳システム ☐ 税務システム

システム3

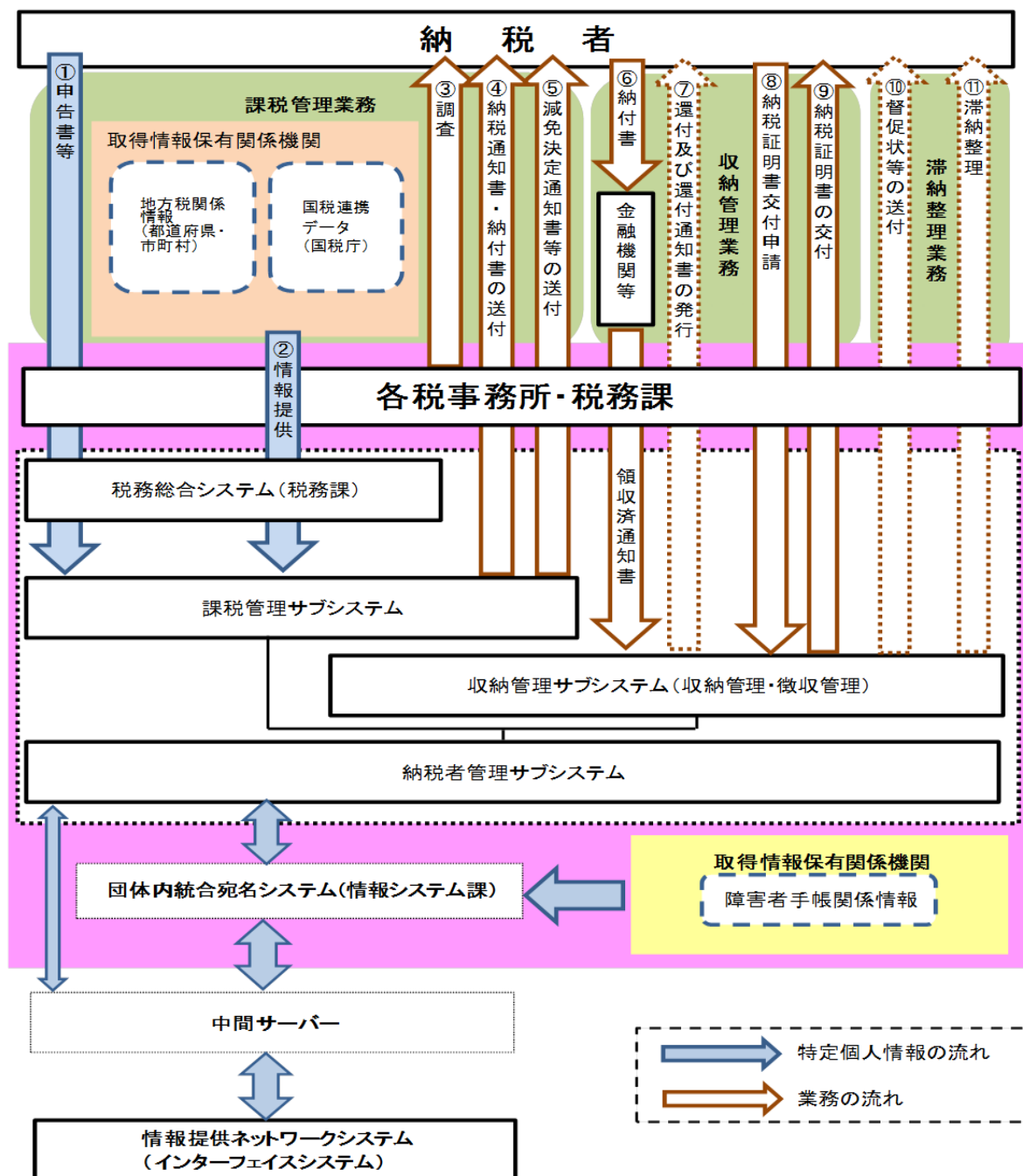
①システムの名称	中間サーバー
②システムの機能	中間サーバーは、情報提供ネットワークシステム(インターフェイスシステム)、税務総合システムなど既存システム、団体内統合宛名システム等の各システムとデータの受け渡しを行うことで、符号の取得(※1)や各機関で保有する特定個人情報の照会と提供等の業務を実現する。 (※1)セキュリティの観点により、特定個人情報の照会と提供の際は、「個人番号」を直接利用せず「符号」を取得して利用する。 1 符号管理機能: 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 2 情報照会機能: 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う機能。 3 情報提供機能: 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報
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	国税連携システム	
②システムの機能	所得税確定申告書等に係るデータ(国税連携データ)を、国税庁からeLTAXを通じて各地方公共団体へ送信する。各地方公共団体では、受信サーバのオプション機能を利用して、受信データの管理、検索、帳票表示、印刷、ダウンロード、団体間回送などを行うことができる。 1 確定申告データダウンロード機能 2 確定申告イメージデータダウンロード機能 3 確定申告データの検索、印刷、XMLファイルのCSV変換機能 4 団体間回送機能 (※詳細は、「(別添1)事務の内容2」を参照)	
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 ☐ 住民基本台帳ネットワークシステム ☐ 宛名システム等 ☒ その他 (税務総合クラウドサービス)	☐ 庁内連携システム ☐ 既存住民基本台帳システム ☒ 税務システム

システム5	
①システムの名称	税務総合クラウドサービス
②システムの機能	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税のうち県税の賦課徴収又は地方税のうち県税に関する調査(犯罪事件の調査を含む。)に関する事務であって主務省令で定めるものに関する電算処理 1 課税管理サブシステム 課税、減免等の課税管理業務を行う。 2 収納管理サブシステム 収納、還付、充当、納税証明書、督促状送付等の収納管理業務を行う。 3 滞納管理サブシステム 催告書送付や納税者単位の滞納状況及び財産、折衝記録等の滞納管理業務を行う。 4 あて名管理サブシステム
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 （国税連携システム)
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	
税務総合システムデータベースファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	県税の公平・公正な課税、徴収事務の効率化 ・個人の特定、個人の宛名の突合を効率化 ・障害者関係情報による自動車税種別割等の減免事務を効率化
②実現が期待されるメリット	県税の公平・公正な課税、納税者の利便性向上 ・個人の特定、個人の宛名の突合の正確性の向上により公平・公正な課税が実現 ・障害者関係情報により、自動車税種別割等の減免を受ける際の事務手続の効率化が図られることによる利便性向上
5. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項 別表24の項 ・自動車税環境性能割の減免申請(地方税法第167条、奈良県税条例第56条の13) ・自動車税種別割の減免申請(地方税法第177条の17、奈良県税条例第63条)
6. 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	[提供側] 提供は行わない [照会側] 番号法第19条第8号に基づく主務省令第2条の表 49の項 ・自動車税環境性能割の減免のため身体障害者手帳情報を照会(地方税法第167条、奈良県税条例第56条の13) ・自動車税種別割の減免申請のため身体障害者情報を照会(地方税法第177条の17、奈良県税条例第63条)
7. 評価実施機関における担当部署	
①部署	総務部税務課
②所属長の役職名	税務課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容



(備考)

納税者からの申告・届出又は調査により課税し、納税通知書を送付するとともに、納税者が納付した税金を県の歳入として受け入れ、納付額が課税額より多い場合は超過額を還付、納税者からの納付がない場合や納付額が課税額より少ない場合は督促を行った後、滞納整理を行う。

- ① 納税者から提出される申告書等を受け付け、確認を行う。
- ② 関係機関等からの情報により、申請書等の確認を行う。
- ③ 必要に応じて、納税者や申告書等の内容について、調査を行う。
- ④ ①～③により課税した内容について、納税者に納税通知書を送付する。
- ⑤ ①～③により決定した減免決定について、納税者に減免決定通知書等を送付する。
- ⑥ 納税者が納付書により納付したことについて、金融機関からの領収済通知書により確認する。
- ⑦ 納付額が課税額より多い場合は超過額を還付のうえ、納税者に還付通知書を送付する。
- ⑧ 納税者からの納税証明書交付申請書を受け付け、確認を行う。
- ⑨ ⑧に係る納税証明書を納税者に交付する。
- ⑩ 納税者からの納付がない場合や納付額が課税額より少ない場合は、納税者に督促状を送付する。
- ⑪ 督促した納税者から納付がない場合や納付額が課税額より少ない場合は、滞納整理を行う。

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

税務総合システムデータベースファイル

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	＜選択肢＞ 1) 1万人未満 [10万人以上100万人未満]	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 ※	納税者及び課税調査対象者	
その必要性	公平・公正な賦課徴収のため、必要な範囲の特定個人情報情報を保有	
④記録される項目	[100項目以上]	＜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	1 個人番号及びその他識別情報:対象者を正確に特定するために保有 2 4情報及び連絡先:賦課決定に際し課税要件を確認するため、納税通知書等の送付先を確認するため、本人への連絡のため 3 国税関係情報:課税調査対象者に関する情報を確認し、課税事務を行うため 4 障害者福祉関係情報:障害者に対する税の減免決定を行うため 5 地方税関係情報:車両番号、車種等を記録することにより、自動車税種別割の公平かつ適正な課税を行うため	
全ての記録項目	別添2を参照。	
⑤保有開始日	平成28年3月	
⑥事務担当部署	奈良県総務部税務課	

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 (税務署(国税庁)) ☐ 地方公共団体・地方独立行政法人 (他の都道府県、市町村) ☐ 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 ()	
③入手の時期・頻度	☐ 定期的に入手する事務(毎年) ・個人事業税の定期課税に関する事務「毎週、3～8月」 ☐ 個別に対応する事務(随時) ・申告及び届出時「申請等を受け付けた都度」 ・納税者の特定時「事務上、納税者の特定が必要な都度」	
④入手に係る妥当性	☐ 定期的に行う事務 ・個人事業税の定期課税を行うため、税務署(国税庁)から国税連携システムを経由して、電子記録媒体により税務システムへ前年分所得税確定申告書の情報を毎年3～8月に毎週入手している。 ☐ 個別に対応する事務 ・自動車税種別割の納税義務者は、奈良県税条例の定めるところにより、地方税法施行規則で定める様式によって、自動車税種別割の賦課徴収に関し必要な事項を記載した申告書又は報告書を提出しなければならない。(地方税法第177条の13、奈良県税条例第59条) ・上の様式に記載された個人番号について、番号法施行規則に基づき、個人番号カード、住民基本台帳ネットワーク端末その他の方法により、真正性の確認と本人確認を行う。	
⑤本人への明示	本人から入手する情報については、本人に対して、入手すること及びその利用目的を明示する。ただし、地方税法等で定める情報については、その限りではない。また、他の機関及び庁内連携又は情報提供ネットワークシステムを通じた入手を行うことは番号法に明示されているとともに、窓口対応する場合は本人に口頭で説明を行う。	
⑥使用目的 ※	公平・公正な賦課、徴収事務の効率化	
	変更の妥当性	—
⑦使用の主体	使用部署 ※	奈良県総務部税務課、奈良県税事務所、中南和県税事務所(2窓口センター含む)、自動車税事務所
	使用者数	[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

⑧使用方法 ※		1 課税管理に関する事務 ・申告及び届出等による情報から課税管理業務を行う。 2 収納管理に関する事務 ・収納及び課税等の情報から収納、還付、充当などの収納管理業務を行う。 3 滞納管理に関する事務 ・滞納者情報等から滞納管理業務を行う。 4 共通宛名管理に関する事務 ・納税者の宛名情報の特定や突合を行い、宛名管理業務を行う。
	情報の突合 ※	1 課税管理に関する事務 ・自動車税種別割の減免決定を行うため、本人から提出された減免に係る申告書等の内容と情報提供ネットワークシステムから入手した障害者関係情報との突合を行う。 上記1～3に係る4 共通宛名管理に関する事務 ・納税者の特定を行うため、税務総合システムが持つ宛名情報と情報提供ネットワークシステムから入手した特定個人情報とを団体内統合宛名システムを介して直近の4情報(氏名、性別、生年月日、住所)を付加した納税者関係情報とを突合する。
	情報の統計分析 ※	納税者の地方税情報、障害者情報について、税の賦課徴収に関する統計や分析は行うが、特定個人情報を用いて特定の個人を判別しようとする情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	障害者に対する自動車税種別割等の減免決定を行う。
⑨使用開始日		平成28年3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 1) 委託する 委託しない 2) 委託しない (4) 件)	
委託事項1		税務総合システム管理運用業務	
①委託内容		税務総合システムの運用管理、バッチ処理、障害対応及び軽微な仕様変更等	
②取扱いを委託する特定個人情報ファイルの範囲		特定個人情報ファイルの全体 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部 2) 特定個人情報ファイルの一部	
	対象となる本人の数	10万人以上100万人未満 1) 1万人未満 2) 1万人以上10万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上 5) 1,000万人以上	
	対象となる本人の範囲 ※	県税に係る納税者及び課税調査対象者	
	その妥当性	県税の公平・公正な賦課、徴収を目的として必要な範囲の特定個人情報を保有している税務総合システムの運用管理を行うため、県税に係る納税者及び課税調査対象者の情報を取り扱う必要がある。この取扱いには高度なITシステムの操作技術が必要であることから、最新のIT技術に精通し、運用業務に実績がある業者に運用を委託し、特定個人情報を取り扱わせる必要がある。	
③委託先における取扱者数		10人未満 1) 10人未満 2) 10人以上50人未満 2) 10人以上50人未満 3) 50人以上100人未満 3) 50人以上100人未満 4) 100人以上500人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 5) 500人以上1,000人未満 6) 1,000人以上 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法		専用線 1) 専用線 電子メール 2) 電子メール 電子記録媒体(フラッシュメモリを除く。) 2) 電子メール フラッシュメモリ 3) フラッシュメモリ 紙 3) フラッシュメモリ その他 3) フラッシュメモリ (3) フラッシュメモリ)	
⑤委託先名の確認方法		県ホームページに掲載する。	
⑥委託先名		アイスター株式会社	
再委託	⑦再委託の有無 ※	再委託しない 1) 再委託する 2) 再委託しない 2) 再委託しない	
	⑧再委託の許諾方法		
	⑨再委託事項		

委託事項2～5		
委託事項2		県税窓口受付等業務
①委託内容		自動車税環境性能割・自動車税種別割申告書受付や記載内容の定型的な審査、納税証明書の発行等の自動車税事務所及び県税事務所(窓口センター)の窓口業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	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
	対象となる本人の範囲 ※	納税者
	その妥当性	自動車税種別割等の公平・公正な賦課、徴収を目的として、窓口業務において必要な範囲の特定個人情報を取り扱う必要がある。この業務においては、個人情報を安全にかつ適正に取扱い、正確に遂行する必要があることから、窓口業務に精通し、業務実績がある業者に委託し、特定個人情報を取り扱う必要がある。
③委託先における取扱者数		[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
④委託先への特定個人情報ファイルの提供方法		[☐] 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 ()
⑤委託先名の確認方法		県ホームページに掲載する。
⑥委託先名		日本郵政スタッフ株式会社 大阪支社
再委託	⑦再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項3		税務総合システム改修業務	
①委託内容		税制改正等により発生する税務総合システムの改修	
②取扱いを委託する特定個人情報ファイルの範囲		〔 特定個人情報ファイルの一部 〕 ＜選択肢＞ 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	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	
	対象となる本人の範囲 ※	県税に係る納税者及び課税調査対象者	
	その妥当性	県税の公平・公正な賦課、徴収を目的として必要な範囲の特定個人情報を保有している税務総合システムの改修を行うため、県税に係る納税者及び課税調査対象者の情報を取り扱う必要がある。この取扱いには高度なITシステムの操作技術が必要であることから、最新のIT技術に精通し、改修業務に実績がある業者に委託し、特定個人情報を取り扱わせる必要がある。	
③委託先における取扱者数		〔 10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	
④委託先への特定個人情報ファイルの提供方法		〔 ○ 〕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 ()	
⑤委託先名の確認方法		県ホームページに掲載する。	
⑥委託先名		日本電気株式会社 関西支社	
再委託	⑦再委託の有無 ※	〔 再委託しない 〕 ＜選択肢＞ 1) 再委託する 2) 再委託しない	
	⑧再委託の許諾方法		
	⑨再委託事項		

[illegible]

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 (1) 件 ☐ 移転を行っている () 件 ☐ 行っていない
提供先1	都道府県知事
①法令上の根拠	番号法第19条第10号
②提供先における用途	個人事業税の賦課及び徴収
③提供する情報	本県で賦課しない者に係る所得税の申告書情報
④提供する情報の対象となる本人の数	☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
⑤提供する情報の対象となる本人の範囲	国税連携システム(eLTAX)で入手した所得税の申告書情報のうち、本県で賦課しない所得税申告者等
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 (国税連携システム(eLTAX))
⑦時期・頻度	他都道府県が賦課する者であったことが判明した場合に送付する。(随時)
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	
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	
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

①保管場所 ※

<税務総合システムにおける措置>

- ・入退室管理システムを行っているサーバー室で管理すると共に、監視カメラによる入退室者及びシステム操作者の監視を行う。
- ・県庁の入退室管理(IDカード)が行われている部屋に設置したサーバー内に保管する。
- ・サーバーの運用管理を行う外部委託業者には出勤簿記入を義務づけ、管理職など責任のある者による出勤簿確認を毎日実施している。また、サーバー管理に使用する端末は他の業務に使用せずセキュリティに気を付けている。なお、週1回外部委託業者から税務総合システムの稼働状況の報告を受けるとともに、月1回定例会議を開催しシステム稼働状況の情報共有を図っている。

<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政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。
- ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。
- ・日本国内でデータを保管している。
- ・特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。

<団体内統合宛名システムにおける措置>

- ・入退室管理システムを行っているサーバー室で管理すると共に、監視カメラによる入退室者及びシステム操作者の監視を行う。
- ・特定個人情報は、サーバー室内に設置された団体内統合宛名システムのデータベース内に保存し、バックアップも同室内の機器に保存することとしている。

<国税連携システム(eLTAX)における措置>

国税連携システムの国税連携データ受信サーバーは、地方税共同機構が認定している事業者に委託し、管理している。

<税務総合クラウドサービスにおける措置>

- ①県外の入退室管理(※)が行われているデータセンターに設置したサーバ内に保管している。
※建屋及び室内への入退室権限を持つ者を限定し、身分証による本人確認により入退室する者の管理を行う。
 - ②サーバの運用管理は、外部委託業者が行っているが、ID及びパスワードによる認証が必要であり、サーバ管理に使用する端末は他の業務に使用しておらず、信頼性の高いウイルス対策ソフトを導入し、パターンファイルは常に最新の状態にして、セキュリティ対策を行っている。
- なお、総括管理者は、月1回外部委託業者からシステムの稼働状況の報告を受けている。

②保管期間	期間	＜選択肢＞ 1) 1年未満2) 1年3) 2年 4) 3年5) 4年6) 5年 7) 6年以上10年未満8) 10年以上20年未満9) 20年以上 10) 定められていない
	その妥当性	県税の賦課、徴収権限が切れるまで、及び訴訟への対応や、課税誤りへ対応するため。
③消去方法	＜税務事務の運用における措置＞ ・データについては、システムにて消去する。 ・紙媒体については、外部業者による裁断溶解処理を行う。 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ・クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度 (ISMAP) に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ・中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 ＜団体内統合宛名システムにおける措置＞ ・ディスク交換やハード更改等の際は、団体内統合宛名システムの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・住民基本台帳ネットワークシステムの最新4情報で洗い替えをするため、住民基本台帳法施行令の本人確認情報の保存期間に従う。H27年10月1日までは、除票（死亡を除く）となってから5年、以降は、150年保存する。 ＜国税連携システム (eLTAX) における措置＞ ・国税連携システムの国税連携データ受信サーバー内のデータは、国税連携クライアントから操作手引書により本県の権限ある職員が定められた手順により消去する。	
7. 備考		
税務総合クラウドサービスはパッケージシステムであり、個別カスタマイズ開発は令和7年度より開始予定。令和8年9月に本番運用開始予定。		

(別添2) 特定個人情報ファイル記録項目

■税務総合システムデータベース

《番号管理テーブル》

納税者管理番号,個人・法人区分,個人・法人番号,氏名・名称,住所,性別,生年月日・設立年月日,補記コード,利用制限区分,変更理由,真正確認区分,真正確認年月日,宛名連携区分,宛名連携年月日,更新種別,宛名連携結果,法人種別,予備,新規年月日,更新年月日,更新時間,更新県税,更新端末,更新ユーザ

《納税者マスタ》

納税者番号,履歴連番,個人法人区分,個人法人番号,氏名漢字,氏名カナ,郵便番号,住所コード,番地方書,生年月日,性別,状態区分コード,状態区分コード設定日,注意コード,左詰氏名漢字,左詰住所,全住所名称,突合用住所,回答氏名漢字,回答氏名カナ,回答性別,回答生年月日,回答住所,処理結果コード,照会一致項目,法人種別,公表同意,突合状況,突合年月日,ホスト回答日,真正性確認区分,真正性確認送信日,真正性確認確定日,作成日,更新日

(別添2) 特定個人情報ファイル記録項目

■税務総合クラウドサービスデータベース

【マイナンバー(記録項目35項目)】

マイナンバーレコード

名寄番号,マイナンバー,最新枝番,マイナンバー区分,更新区分,通知日,更新情報

マイナンバー基本情報レコード

マイナンバー,マイナンバー最新枝番,マイナンバー区分,氏名(法人名),住所,性別

マイナンバー履歴レコード

名寄番号,枝番,マイナンバー,マイナンバー区分,更新区分,通知日,更新情報

マイナンバー基本情報履歴レコード

マイナンバー,マイナンバー枝番,マイナンバー区分,氏名(法人名),住所,性別,生年月日,同期日,更新情報

マイナンバーログレコード

アクセス情報,ユーザID,利用区分,アクセス区分,画面／帳票ID,個人番号

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名		
税務総合システムデータベースファイル		
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1： 目的外の入手が行われるリスク		
対象者以外の情報の入手を防止するための措置の内容	＜税務事務の運用における措置＞ ・本人が書面を提出する際に、本人が本人以外の情報を誤って記載することがないようにチェックを行う。 ・情報提供ネットワークシステム等を通じて入手する際も、対象者以外の情報を入手しないこととする。 ・奈良県税条例第56条の13及び第63条で定める自動車税環境性能割・自動車税種別割減免申請書において減免対象者となる障害者の個人番号を記載していただき、真正性の確認を行う。 ＜団体内統合宛名システムにおける措置＞ ・業務所管課において届出内容や本人確認書類（身分証明等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。	
必要な情報以外を入手することを防止するための措置の内容	＜税務事務の運用における措置＞ ・必要最小限の情報のみ記載する書面様式になるようにする。 ・個人情報利用の際に税システム内に使用結果log（利用者・時間・利用内容等）を保存して、不適正な利用を抑制する。また、logを定期的にチェックする。 ＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムは、番号制度利用対象システムのみ接続し、対象外のシステムは接続しない。 ・団体内統合宛名システムは、主に業務システムから統合宛名管理上で必要な項目のみ連携することを想定しており、業務データは保有しない。	
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	
リスク2： 不適切な方法で入手が行われるリスク		
リスクに対する措置の内容	＜税務事務の運用における措置＞ ・書面を本人に提示する際に、何のための書類か、どのように利用するかを説明した上で、書面を提出していただく。 ・情報提供ネットワークシステム等を通じて入手する際も、特定の権限者以外は情報照会できず、また、情報照会・提供の履歴が税務総合システムに保存される。 ＜団体内統合宛名システムにおける措置＞ 特定個人情報を入手する際、以下の対策を講じる。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ・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適切な方法で入手できない対策を実施する。	
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3: 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	<税務事務の運用における措置> ・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、本人確認を行う。 ・代理人から個人番号の提供を受ける場合は、代理権の確認・代理人の身元(実存)の確認を行った上で、本人の番号確認を行う。 <団体内統合宛名システムにおける措置> ・特定個人情報の入手の際には、業務所管課の事務で確立された手順に従って本人であることが担保されたデータのみを連携する。
個人番号の真正性確認の措置の内容	<税務事務の運用における措置> ・個人番号カードの提示、もしくは通知カードと身分証明書の提示を受けて、個人番号の真正性確認を行う。以前に取得した個人番号が変更されていないか、申告書及び届出書提出の際にチェックを行い、変更があれば修正を行う。また、必要に応じて団体内統合宛名システムまたは住民基本台帳ネットワークシステムを利用して、個人番号の確認を行う。 <団体内統合宛名システムにおける措置> ・上記のとおり、業務所管課の事務で個人番号の真正性が確認されたデータを連携する。
特定個人情報の正確性確保の措置の内容	<税務事務の運用における措置> ・必要に応じて住民基本台帳ネットワークシステムを利用して、本人確認を行う。また、本人にも確認していただく。 <団体内統合宛名システムにおける措置> ・団体内統合宛名システムの登録者情報は、正確な情報となるよう定期的に住民基本台帳ネットワークシステムの情報と照合して情報の維持管理を行う。
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

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	<税務総合システムにおける措置> ・情報提供ネットワークシステムは暗号化を実施する。 ・書面の場合は、本人から直接書面を受け取ることを原則とし、郵送などの場合は担当所属名及び所在地を明記して、当該所在地あてに返送していただく。 ・端末PCをユーザID、パスワード及び顔認証による認証を行い、利用者を限定している。 ・端末PCのパスワードについては、8桁以上、英字大文字、英字小文字、数字を最低1文字ずつ組み合わせたもので、堅牢なパスワードとしている。 <団体内統合宛名システムにおける措置> ・特定個人情報を取り扱うシステムに対して、アクセス制御の措置を講じる。 ・ウイルス対策ソフトウェアを導入し、常に最新のパターンファイルを適用することで、セキュリティ上の有効性を確認する。 ・OSや導入するソフトウェアに対するセキュリティパッチはその有効性や必要性等を検証した上で適用し、その動作の安定性も確認する。 ・特定個人情報にアクセスする端末はインストールする標準ソフトウェアを定めており、システム管理者の許可なくソフトウェアをインストールすることを禁止する。 <税務総合クラウドサービスにおける措置> ・情報提供ネットワークシステムは暗号化を実施する。 ・書面の場合は、本人から直接書面を受け取ることを原則とし、郵送などの場合は担当所属名及び所在地を明記して、当該所在地あてに返送していただく。 ・端末PCをユーザID、パスワード及び顔認証による認証を行い、利用者を限定している。 ・端末PCのパスワードについては、8桁以上、英字大文字、英字小文字、数字、記号を最低1文字ずつ組み合わせたもので、堅牢なパスワードとしている。
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、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	<団体内統合宛名システムにおける措置> ・団体内統合宛名システムは、番号法第9条第1項別表及び関係主務省令に定められた業務に従事する職員以外からの特定個人情報へのアクセスが行えないような仕組みであり、団体内統合宛名システムへは個人番号、氏名や生年月日等の基本的な情報のみ保持しており、当該事務に必要な情報との紐付けは物理的に不可能である。	
事務で使用するその他のシステムにおける措置の内容	・税務総合システムには、税務に関係のない情報を保有しない。 ・税務総合システムは、庁内において、団体内統合宛名システムと接続するが、特定個人情報の連携については、情報提供ネットワークシステムへ関係情報を照会する場合の処理に限られるよう制限する。また、税務システムから他のシステムへの特定個人情報の連携は、情報照会に必要な情報（個人番号及び宛名情報等）以外の情報連携は行わないよう制限する。 ・税務総合クラウドサービスには、税務に関係のない情報を保有しない。 ・税務総合クラウドサービスは、庁内において、団体内統合宛名システムと接続するが、特定個人情報の連携については、情報提供ネットワークシステムへ関係情報を照会する場合の処理に限られるよう制限する。また、税務総合クラウドサービスから他のシステムへの特定個人情報の連携は、情報照会に必要な情報（個人番号及び宛名情報等）以外の情報連携は行わないよう制限する。	
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 3) 課題が残されている 2) 十分である	
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	<税務事務の運用における措置> ・端末をID、パスワード及び顔認証による認証を行い、利用者を限定している。 ・利用する端末において、一定時間の操作がない場合にはロックを実施している。 <団体内統合宛名システムにおける措置> ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止し、個人ごとにユーザIDを付与する。 ・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する。	
アクセス権限の発効・失効の管理	[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	<税務事務の運用における措置> ・部署及び業務別にアクセス権限を管理している。 ・業務ごとに更新権限の必要があるか、照会権限のみでよいかを確認し、業務に必要なアクセス権限のみを付与している。 ・権限を有していた職員の異動退職情報をセキュリティ責任者が確認し、異動退職があった際はアクセス権限を更新し、当該IDを失効させる。 <団体内統合宛名システムにおける措置> ①ユーザID及びパスワードの発行管理 ・アクセス権限と業務の対応表を作成する。 ②失効管理 ・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を更新し、当該IDを失効させる。	

アクセス権限の管理		☐ 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	<税務総合システムにおける措置> ・システムパスワードは、IDカード発行時に付与している。 ・異動退職時に業務上アクセス不要となったIDやアクセス権を変更又は削除している。 <団体内統合宛名システムにおける措置> ・ユーザIDやアクセス制御を定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。 <税務総合クラウドサービスにおける措置> ・システムパスワードは、ID発行時に付与している。 ・異動退職時に業務上アクセス不要となったIDやアクセス権を変更又は削除している。			
特定個人情報の使用の記録		☐ 記録を残している		<選択肢> 1) 記録を残している 2) 記録を残していない	
	具体的な方法	・特定個人情報等システムデータの更新記録は7年間保管する。 ・システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、ログ記録は7年間保管する。 ・また記録は月1回セキュリティ責任者が検査・分析を行い、不正アクセスがないことを確認する。			
その他の措置の内容		税務事務に利用する端末において、離席時は顔認証システムによる離席時ロックを実施している。			
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3: 従業者が事務外で使用するリスク					
	リスクに対する措置の内容	<税務事務の運用における措置> ・毎年、全庁的に全職員を対象に、必要最低限の情報セキュリティ知識の取得とセキュリティ意識の向上のため、セルフチェックを実施している。 ・各所属において、年1回の情報セキュリティ研修(講師は各所属のセキュリティ主任)を実施している。 ・各所属において、毎年、情報セキュリティ対策を具体的に実施するための「情報セキュリティ実施手順書」、事故発生時の対応手順を定めた「情報セキュリティ事故対応手順書」の見直しを実施している。 ・業務外利用の禁止や業務情報漏えい注意について、各種研修、担当者会議等の場で啓発している。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 <団体内統合宛名システムにおける措置> ・システムの操作履歴(操作ログ)を記録する。 ・職員に対しては、特定個人情報保護委員会が作成した「特定個人情報の適正な取扱いに関するガイドライン」を参考にしてデータ保護に関する研修を行う。 ・委託先に対しては業務外で使わないよう上記と同様にガイドラインを参考にして仕様書に定め、個人情報保護にかかる誓約書を提出させる。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。			
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4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	<税務総合システムにおける措置> ・システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、ログ記録は7年間保管する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 <団体内統合宛名システムにおける措置> ・委託先に対しては、仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。 ・職員に対しては、データ保護に関する研修を行う。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 <税務総合クラウドサービスにおける措置> ・システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、ログ記録は7年間保管する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。	
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		
<団体内統合宛名システムにおける措置> ・スクリーンセーバ等を利用して、長時間にわたり特定個人情報を表示させない。 ・端末機のディスプレイを来庁者から見えない位置に置く。		

☐ 委託しない

情報保護管理体制の確認	＜税務事務の運用における措置＞ 外部委託業者を選定する際、先方の個人情報適正管理体制等を確認する。 ・個人情報の管理的保護措置（個人情報取扱規程、体制等の整備等） ・個人情報の物理的保護措置（人的安全管理、施設及び設備の整備、データ管理、バックアップ等） ・個人情報の技術的保護措置（アクセス制限、アクセス監視や記録等） ＜団体内統合宛名システムにおける措置＞ ・システムの運用等を委託するときは、あらかじめ管理者と協議を行い、特定個人情報の保護を適切に行える委託先であることを確認する。
--------------------	---

[制限している] <選択肢>
1) 制限している 2) 制限していない

＜税務事務の運用における措置＞

- ・委託契約書において、個人情報取扱特記事項を明記している。（秘密の保持、収集の制限、目的外利用及び提供の禁止、適正管理、複写又は複製の禁止等）

＜団体内統合宛名システムにおける措置＞

- ・委託にかかる実施体制の提出を義務づける。
- ・委託事業者に対し、個人情報保護にかかる誓約書を提出させる。
- ・誓約書の提出があった要員に対してのみ、システム操作の権限を与える。

[記録を残している] <選択肢>
1) 記録を残している 2) 記録を残していない

＜税務総合システムにおける措置＞

- ・委託先における特定個人情報についてのシステム利用履歴について、利用者ID、操作日時などデータベースへのアクセスログを7年間保管する。

＜団体内統合宛名システムにおける措置＞

- ・委託先における特定個人情報についてのシステム利用履歴について、利用者ID、操作日時などデータベースへのアクセスログを7年間保管する。

＜税務総合クラウドサービスにおける措置＞

- ・委託先における特定個人情報についてのシステム利用履歴について、利用者ID、操作日時などデータベースへのアクセスログを7年間保管する。

特定個人情報の提供ルール		[定めている]	<選択肢> 1) 定めている 2) 定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<税務事務の運用における措置> ・委託契約書に基づき、委託先は奈良県の指示がある場合を除き、特定個人情報の目的外利用及び第三者への提供をしてはならない。また、委託先は奈良県の承認があるときを除き、特定個人情報の複写・複製、又はこれらに類する行為をすることができない。 ・委託契約書に基づき、必要があると認めるときは調査を行い、または報告を求める。 <団体内統合宛名システムにおける措置> ・委託契約書に基づき、委託先は奈良県の指示がある場合を除き、特定個人情報の目的外利用及び第三者への提供をしてはならない。 ・委託先は奈良県の承認があるときを除き、特定個人情報の複写・複製、又はこれらに類する行為をすることができない。 ・委託契約書に基づき、必要があると認めるときは調査を行い、または報告を求める。	
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<税務事務の運用における措置> ・委託契約書に基づき、委託先は奈良県から提供を受けた特定個人情報が記録された資料は事務処理後直ちに奈良県に返却する。 ・委託先に特定個人情報等を提供する際は所定の授受簿に記録し、委託元と委託先双方でこれを確認のうえ特定個人情報等の授受を行う。 ・委託契約書に基づき、必要があると認めるときは調査を行い、または報告を求める。 <団体内統合宛名システムにおける措置> ・運用保守委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を奈良県庁舎内に限定し、外部への持ち出しを禁止する。 ・委託契約書に基づき、必要があると認めるときは調査を行い、または報告を求める。	
特定個人情報の消去ルール		[定めている]	<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	<税務事務の運用における措置> ・委託契約書に基づき、委託先は奈良県から提供を受けた特定個人情報が記録された資料は事務処理後直ちに奈良県に返却する。 ・消去時には職員が立ち会うとともに、消去した情報項目・消去方法・消去日等を明記した文書を提出させる。	
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	<税務事務の運用における措置> 委託契約書において個人情報取扱特記事項を明記している。 ・秘密の保持 ・収集の制限 ・目的外利用・提供の禁止 ・漏えい、滅失及びき損の防止 ・従事者の監督 ・複写又は複製の禁止 ・再委託の禁止（承諾を受けたものは除く） ・資料等の返還等 ・取扱状況についての指示等 ・事故発生時における報告 <団体内統合宛名システムにおける措置> 委託契約書において個人情報取扱特記事項を明記している。 ・秘密の保持 ・収集の制限 ・目的外利用・提供の禁止 ・漏えい、滅失及びき損の防止 ・複写又は複製の禁止 ・再委託の禁止（承諾を受けたものは除く） ・資料等の返還等 ・取扱状況についての指示等 ・事故発生時における報告	

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確保	[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	再委託を行う場合には、上記と同様の秘密保持の遵守することや奈良県情報セキュリティポリシーを遵守することを規定している。	
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1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	＜選択肢＞ 1) 記録を残している 2) 記録を残していない
具体的な方法	＜eLTAXによる提供＞ ・国税連携システム（eLTAX）を利用して他都道府県へ提供する特定個人情報については、データ登録を行った職員や送信日時、送信状況等の当該提供記録をシステム上で記録をしている。（記録の保存期間は7年）	
特定個人情報の提供・移転に関するルール	[定めている]	＜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	＜eLTAXによる提供＞ ・国税連携システム（eLTAX）を利用した特定個人情報の提供について、提供するデータの作成やシステムへの情報の格納、地方税ポータルセンタ（eLTAX）への送信方法が操作手引書等に記載されており、それに基づき提供処理を行っている。 ・国税連携システム（eLTAX）では、特定個人情報の提供は、番号法施行規則第20条第3号の規定に基づき、安全性及び信頼性を確保するために必要な基準として、内閣総理大臣が定める基準に従って行っている。	
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
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	＜eLTAXによる提供＞ ・国税連携システム（eLTAX）において特定個人情報の提供処理を行う場合、システムでは決められた機能以外での提供は行うことができず、提供先として都道府県以外を設定することはできない仕様になっている。 また、地方税ポータルセンタ（eLTAX）と都道府県間は閉域網であるLGWAN、地方税ポータルセンタ（eLTAX）と国税庁間は専用回線を用いており、データも暗号化をしているため情報漏えいや紛失のリスクが軽減されている。 ・国税連携システム（eLTAX）では、特定個人情報の提供は、番号法施行規則第20条第3号の規定に基づき、安全性及び信頼性を確保するために必要な基準として、内閣総理大臣が定める基準に従って行っている。	
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
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	＜eLTAXによる提供＞ 国税連携システム（eLTAX）で提供する電子データについては、番号法施行規則第20条第3号の規定に基づく、安全性及び信頼性を確保するために必要な基準として、内閣総理大臣が定める基準に従って行うこととする。 国税連携システムの回送機能は、提供先として都道府県以外を設定することはできない仕様になっている。本県から地方税ポータルセンタ（eLTAX）までは閉域網であるLGWANが利用され、暗号化通信がされている。地方税ポータルセンタ（eLTAX）から国税庁までは、専用回線が利用され、暗号化通信がされており、決められた情報のみを提供するように系統的に担保している。 なお、他都道府県との間の情報連携については、地方税ポータルセンタ（eLTAX）から他都道府県までは、閉域網であるLGWANが利用されているほかは、同様である。	
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	<税務事務の運用における措置> ・番号法の規定に基づき、認められる範囲内において特定個人情報の照会を行う。また、理解度を高めるため、規定内容の周知を行い、業務以外に利用することを禁止する。 ・個人情報利用の際に税システム内に使用結果log(利用者・時間・利用内容等)を保存して、不適正な利用を抑制する。また、logを定期的にチェックする。 <中間サーバー・ソフトウェアにおける措置> ・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、情報提供許可証の発行と照会内容の照会許可照会リスト(※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情報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している。 ・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仕組みになっている。 (※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) 番号法の規定に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報リスト化したもの (※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 <団体内統合宛名システムにおける措置> ・番号法の規定に基づき、各業務と団体内統合宛名番号の紐付けを行い、認められる範囲内において特定個人情報の照会を行う。また、法規定に従い、業務以外に利用することを禁止する。 ・特定個人情報にアクセスできる職員は必要最小限とし、かつ団体内統合宛名システムにおいて業務上必要なデータのみにアクセスできるよう制御する。また、操作ログを記録することで、不適切な利用を抑制する。 ・ファイアーウォール、ルーター等のシステム防護措置により、団体内統合宛名システムを無権限のアクセスから保護する措置を講ずる。 ・ネットワーク上の利用制限により、庁外から団体内統合宛名システムへ接続することを制限する。		
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: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	<中間サーバー・ソフトウェアにおける措置> ・中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理す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入手のみ実施できるよう設計されるため、安全性が担保されている。 <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、安全性を確保している。 ・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3： 入手した特定個人情報 が不正確であるリスク		
リスクに対する措置の内容	＜税務総合システムにおける措置＞ ・入手した特定個人情報について、税務総合システム内の情報と突合を行い、真正性及び正確性の確認を行う。また、別途、届出又は申告時には、その都度、届出などの内容と突合を行い、特定個人情報の正確性の確認を行う。 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ＜税務総合クラウドサービスにおける措置＞ ・入手した特定個人情報について、税務総合クラウドサービス内の情報と突合を行い、真正性及び正確性の確認を行う。また、別途、届出又は申告時には、その都度、届出などの内容と突合を行い、特定個人情報の正確性の確認を行う。	
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4： 入手の際に特定個人情報 が漏えい・紛失するリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、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入手のみを実施するため、漏えい・紛失のリスクに対応している(※)。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報 が漏えい・紛失するリスクを軽減している。 ・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仕組みになっている。 (※) 中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜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、漏えい・紛失のリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。	
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5: 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	＜中間サーバー・ソフトウェアにおける措置＞ ・情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ・特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ・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仕組みになっている。 (※) 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の要求の受領及び情報提供を行う機能	
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6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・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仕組みになっている。 (※) 暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能 ＜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、不適切な方法で提供されるリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	
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7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容	<中間サーバー・ソフトウェアにおける措置> ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報提供されるリスクに対応している。 ・情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ・情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 (※)特定個人情報を副本として保存・管理する機能	
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
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仕組みになっている。 ・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、安全性を確保している。 ・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している。 ・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・運用を行う事業者及びクラウドサービス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1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[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
	具体的な対策の内容	<税務総合システムにおける措置> ・サーバー及び周辺機器の設置場所は、防火設備が整い、IDカードとパスワードで入退室者を制限し、監視カメラで入退室者を監視している。 ・サーバー機器等ラックは耐震措置が行われており、施錠管理を行っている。 ・サーバー機器等に係る電源についても、予備電源を設置しており、非常用発電機も備え付けがある。 <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、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 <団体内統合宛名システムにおける措置> ・団体内統合宛名システムをデータセンターに設置し、入館管理及び監視カメラによる監視を行う。 ・データセンター内のサーバー、サーバーの管理機能にアクセス可能な端末、特定個人情報の保存媒体等を設置するサーバー室への入退室管理、監視及び施錠管理する。 <税務総合クラウドサービスにおける措置> データセンター内で運用されている。データセンターには監視カメラを設置しており、入室する場合はシステム管理者の事前承認が必要となる。 ・入室時には静脈認証装置をはじめ、体重や外形を計測して共連れを防ぐセキュリティポータルなど生体認証を利用している。 ・24時間常駐の警備員が、データセンターへの接近者の監視、セキュリティ監視と、さまざまな事故管理を行っている。 ・UPS(無停電電源装置)やGTG(自家発電設備)により、万一の商用電力停電時にも電力供給が可能な設備であり、設備の定期的な試運転点検も行っている。

⑥技術的対策	[十分にを行っている] ＜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
具体的な対策の内容	＜税務総合システムにおける措置＞ ・システムを利用するにはログインパスワードを設定するほかIDカード及び顔認証による認証を必要としている。 ・ウィルス対策ソフト等のパターンファイルは、毎日、手動更新を行っている。 ＜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、ウィ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。 ・中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ・中間サーバーのデータベースに保存される特定個人情報、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ・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している。 ・中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ＜団体内統合宛名システムにおける措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置する。 ・コンピュータウイルス対策ソフトウェアを導入する。 ・OSには随時パッチ適用を実施する。 ＜税務総合クラウドサービスにおける措置＞ ○不正プログラム対策 ・ウィルス対策ソフトを使用して、サーバで定期的なウィルスチェックを実施している。 ・また、定期的に検証済みのパターンファイルに更新している。 ・なお、サーバへのソフトウェア導入及びバージョン更新時は、セキュリティ管理者の許可を得るとともに、体系的な検証等を実施した上で、システム管理者が実施することとしており、不正なプログラムの導入を防止している。 ・また、サーバについては、オペレーティングシステム、ミドルウェア及びドライバのセキュリティ情報等を収集し、必要に応じて、修正プログラムを導入している。 ○不正アクセス防止策 ・ユーザーID及びログインパスワードを設定している。また、許可された外部入出力装置以外への出力を無効化している。 ・ウィルス対策ソフトを使用して、サーバを定期的にウィルスチェックをしている。また、定期的に、検証済みのパターンファイルに更新している。 ・外部からのアクセスに対しては、ネットワークを分離することでアクセスそのものを遮断している。 ・データベースへのアクセスに対しては、ファイアウォールで不正アクセスを遮断するとともに、システム管理者から許可を得た者以外は、データベースを参照・更新・消去することができない仕組みとしている。

⑦バックアップ	[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
⑧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
⑨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	—	
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	死者の個人番号と生存する個人の個人番号とを分けて管理しないため、「Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策」において示す生存する個人の個人番号と同様の管理を行う。	
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

リスク2: 特定個人情報古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	<税務事務の運用における措置> ・納税者情報は、随時、必要に応じて本人確認を行う。 <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提供される団体内統合宛名システムの登録者については、住民基本台帳ネットワークシステムから定期的に基本4情報(住所、氏名、性別、生年月日)を受領して最新の情報に更新する。
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3: 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[定めている] <選択肢> 1) 定めている 2) 定めていない
手順の内容	<税務事務の運用における措置> ・保管期間の過ぎた特定個人情報をシステムからデータ消去する。 ・保管期間の過ぎたバックアップも消去する。 ・紙媒体は保管期間が過ぎると外部業者により裁断溶解処理を行う。 <団体内統合宛名システムにおける措置> ・システム上で、保管期間の経過した特定個人情報は削除する。 ・磁気ディスクの廃棄時は、帳票等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。
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	
・サーバー、端末機器(パソコン)、記憶媒体等の廃棄、保管転換又はリース返却等、行政情報を消去する際は、復元不可能な状態にすることとしている。 ・廃棄、保管転換又はリース返却時対応を実施した場合は、セキュリティ管理者の承認を得たうえ、実施内容を記録に残している。 ・コンピュータ、外部記憶媒体(バックアップ媒体も含む)及び記憶装置を有するプリンター等の周辺機器の廃棄、保管転換又はリース返却時は、次のとおり対応する。 (1) 記憶装置又は記憶媒体を廃棄する場合は、消磁、破碎、溶解、その他の当該記憶装置又は記憶媒体に記録されていたファイル及びドキュメントの復元が不可能となるよう措置する。 (2) 業者委託する場合は、記憶装置(媒体)の物理的破壊を行い、廃棄証明書を提出させる。	

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的なチェック方法	<税務事務の運用における措置> ・評価書の記載内容どおりの運用ができているか、年1回担当部署内でチェックを実施する。 <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、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、定期的に自己点検を実施することとしている。 <団体内統合宛名システムにおける措置> ・内部手順書等に基づき、運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な内容	<税務事務の運用における措置> 税務担当以外の県職員による自己監査を以下の観点から定期的の実施するとともに、監査の結果を踏まえ、体制や規程を改善していく。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規程、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知、教育 ・個人情報保護に関する技術的安全管理措置 <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ・政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 <団体内統合宛名システムにおける措置> ・内部手順書等に基づき、定期的に監査を行うこととしている。	
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[十分にやっている]	<選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な方法	<税務事務の運用における措置> ・職員に対して、個人情報保護に関する研修の受講を推奨している。 ・eラーニング研修の推奨とともに、各所属で毎年セキュリティ管理者による職員対象のセキュリティ研修を実施する。税務初任者研修時にもセキュリティについての内容も実施する。 ・委託業者に対して、契約内容に個人情報保護に関する特記事項を明記し、秘密保持契約を締結している。 ・違反行為を行った者に対しては、その都度指導する。違反行為の程度によっては懲罰の対象となる。 <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こととしている。 ・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こととしている。 <団体内統合宛名システムにおける措置> ・職員に対しては、特定個人情報を扱う業務に携わる前に個人情報保護に関する研修を行う。 1) 新規採用職員(毎年) 2) 会計年度任用職員(採用の都度 年20回程度) 3) 文書主任・セキュリティ主任研修(毎年) 4) 職場内研修(毎年) セキュリティ主任が所属職員(管理職、会計年度任用職員を含む)を対象に実施。 実施後は、研修実施報告書で情報セキュリティ委員会への受講者の報告を義務づけている。 5) eラーニング研修 セキュリティ主任及び情報システム担当者は受講を義務づけている。 平成27年度からは特定個人情報を扱う所属については、管理職を含め関係職員に対してeラーニングの受講を義務づける。 ・委託業者に対して、契約内容に個人情報保護に関する特記事項を明記し、秘密保持契約を締結している。 ・委託業者に対しては、契約内容に個人情報保護に関する研修の実施を義務付けている。 ・違反行為を行った者に対しては、その都度指導する。違反行為の程度によっては懲戒の対象となる。	
3. その他のリスク対策		
<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活用することにより、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者による高レベルのセキュリティ管理(入退室管理等)、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。		

V 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	総務部法務文書課 県政情報公関係 〒630-8501 奈良市登大路町30番地 TEL:0742-27-8348 FAX:0742-27-1323
②請求方法	指定様式より開示・訂正・利用停止請求を受け付ける。
特記事項	県ホームページ上に、請求先、請求方法などについて掲載する。
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 手数料額: ○開示請求手数料300円/件 (奈良スーパーアプリによる請求の場合200円/件) ○開示実施手数料 白黒10円/枚、カラー50円/枚 (※開示請求手数料額に達するまでは無料) (奈良スーパーアプリによる請求に対する開示はアプリ) (手数料額、納付方法: 上で 実施(手数料は無料)) 納付方法: 窓口(現金)、納入通知書、奈良スーパーアプリ
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	個人事業税の賦課徴収、不動産取得税の賦課徴収、鉱区税の賦課徴収、特別地方消費税の賦課徴収、軽油引取税賦課徴収、狩猟税の賦課徴収、自動車税環境性能割の賦課徴収、自動車税種別割の賦課徴収、県税滞納整理事務、収納管理事務、口座振替収納事務、納税証明事務、産業廃棄物税の賦課徴収、たばこ税の賦課徴収
公表場所	奈良県庁東棟1階県政情報センター
⑤法令による特別の手続	—
⑥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	総務部税務課税制企画管理係 〒630-8501 奈良市登大路町30番地 TEL:0742-27-8364 FAX:0742-26-3674
②対応方法	問い合わせ時に、問い合わせ内容と対応内容を記録しておく。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和6年9月19日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	奈良県パブリックコメント手続要綱に基づき実施
②実施日・期間	令和6年9月30日(月)～令和6年11月1日(金)
③期間を短縮する特段の理由	
④主な意見の内容	意見なし
⑤評価書への反映	
3. 第三者点検	
①実施日	令和6年11月26日(火)
②方法	奈良県個人情報保護審議会において第三者点検を受けた。
③結果	特定個人情報保護評価書の再実施(全項目評価書)については、特定個人情報保護指針(平成26年4月18日特定個人情報保護委員会公示第4号)第10の1(2)に定める適合性及び妥当性を有していると認めます。なお、実施機関においては、広く住民から当該評価書の意見をもとめられるよう意見聴衆の方法を工夫するとともに、当該評価書の趣旨や内容をわかりやすく公示するように努めてください。
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)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
	Ⅱ－6.特定個人情報の保管・消去①保管場所	＜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おり、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ・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。	＜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政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ・特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する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。	事前	自治体中間サーバー・プラットフォーム更改に伴う変更 (令和7年5月2日地情機第4951号地方公共団体情報システム機構及び総合行政ネットワーク全国センター長通知)によるもの
	Ⅱ－6.特定個人情報の保管・消去③消去方法	＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ・ディスク交換やハード更改等の際は、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いて、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。	＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ・クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度(ISMAP)に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ・中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事前	同上
	Ⅲ－6.情報ネットワークとの接続 リスク4:入手の際に特定個人情報が漏えい・紛失するリスク	＜中間サーバー・ソフトウェアにおける措置＞ 省略	＜中間サーバー・ソフトウェアにおける措置＞ 省略 ＜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、漏えい・紛失のリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。	事前	同上
	Ⅲ－6.情報ネットワークとの接続 リスク6:不適切な方法で提供されるリスク	＜中間サーバー・ソフトウェアにおける措置＞ ・セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・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仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能 ＜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、不適切な方法で提供されるリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・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いては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	＜中間サーバー・ソフトウェアにおける措置＞ ・セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・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仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能 ＜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、不適切な方法で提供されるリスクに対応している。 ・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漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの保守・運用を行う事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	事前	同上

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
	Ⅲー6.情報ネットワーク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仕組みになっている。 ・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、安全性を確保している。 ・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している。 ・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。	<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仕組みになっている。 ・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、安全性を確保している。 ・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している。 ・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・運用を行う事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事前	同上
	Ⅲー7.特定個人情報の保管・消去 リスク1:特定個人情報の漏えい・滅失・毀損リスク⑤ L物理的対策	<税務総合システムにおける措置> ・省略 <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。 <団体内統合宛名システムにおける措置> ・省略 <税務総合クラウドサービスにおける措置> ・省略	<税務総合システムにおける措置> ・省略 <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、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 <団体内統合宛名システムにおける措置> ・省略 <税務総合クラウドサービスにおける措置> ・省略	事前	同上
	Ⅲー7.特定個人情報の保管・消去 リスク1:特定個人情報の漏えい・滅失・毀損リスク⑥ 技術的対策	<税務総合システムにおける措置> ・省略 <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。 <団体内統合宛名システムにおける措置> ・省略 <税務総合クラウドサービスにおける措置> ・省略	<税務総合システムにおける措置> ・省略 <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。 ・中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ・中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ・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している。 ・中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 <団体内統合宛名システムにおける措置> ・省略	事前	同上

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
	IV その他のリスク対策 1. 監査②監査 具体的な内容	＜税務事務の運用における措置＞ ・省略 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ＜団体内統合宛名システムにおける措置＞ ・省略	＜税務事務の運用における措置＞ ・省略 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ・政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 ＜団体内統合宛名システムにおける措置＞ ・省略	事前	同上
	IV その他のリスク対策 3その他のリスク対策	＜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活用することにより、統一した設備環境による高レベルのセキュリティ管理(入退室管理等)、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	＜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活用することにより、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者による高レベルのセキュリティ管理(入退室管理等)、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。	事前	同上