

特定個人情報保護評価書(基礎項目評価書)

評価書番号	評価書名
4	軽自動車税(種別割)に関する事務 基礎項目評価書

個人のプライバシー等の権利利益の保護の宣言

周防大島町は、軽自動車税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ることにより、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

周防大島町長

公表日

令和7年7月1日

I 関連情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	軽自動車税(種別割)に関する事務
②事務の概要	地方税法に基づき、軽自動車課税台帳の管理、賦課、証明書発行等の事務を行う。 特定個人情報ファイルは、以下の場合に使用する。 ①軽自動車税課税台帳の管理、異動、調査等 ②軽自動車税の賦課、更正、通知等 ③減免申請関係事務 ④軽自動車税関係証明書の発行 ⑤納付情報を軽自動車税納付確認システム(軽JNKS)に登録
③システムの名称	・軽自動車税システム(基本セット内) ・宛名管理システム(基本セット内) ・団体内統合宛名システム(基本セット内) ・EUCシステム(基本セット内) ・統合収納管理システム(基本セット内) ・統合滞納管理システム(基本セット内) ・地方公共団体情報連携中間サーバーシステム ・コンビニ交付システム ・軽自動車税納付確認システム(軽JNKS) ・軽自動車検査情報市区町村提供システム ・軽自動車保有関係手続のワンストップサービス(軽OSS) ・統合宛名管理システム(基本セット内) ・課税資料イメージファイリングシステム

2. 特定個人情報ファイル名

- ・軽自動車税関係ファイル
- ・統合収納関係ファイル
- ・統合滞納関係ファイル
- ・住登外者宛名番号管理関係ファイル
- ・団体内統合宛名関係ファイル

3. 個人番号の利用

法令上の根拠	①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(番号法)(平成25年5月31日法律第27号)及び別表(第九条関係) ・第9条(利用範囲) ＜別表(第九条関係)における利用範囲の根拠＞ 上欄(個人番号利用事務実施者)が「市町村長」の項のうち、下欄(法定事務)に「地方税」が含まれる項
--------	--

4. 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	＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定 [実施する]
②法令上の根拠	・番号法第19条第8号(特定個人情報の提供の制限)及び「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第十九条第八号に基づく利用特定個人情報の提供に関する命令」(利用特定個人情報省令)第2条の表 ＜利用特定個人情報省令第2条の表における情報提供の根拠＞ ・軽自動車税(種別割)事務では、情報提供は実施していない。 ＜利用特定個人情報省令第2条の表における情報照会の根拠＞ ・第一欄(情報照会者)が「市町村長」の項のうち、第二欄(事務)に「地方税法」が含まれる項 ・公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律による特定公的給付の支給の実施(160の項)

5. 評価実施機関における担当部署

①部署	周防大島町 総務部 税務課
-----	---------------

②所属長の役職名	税務課長		
6. 他の評価実施機関			
7. 特定個人情報の開示・訂正・利用停止請求			
請求先	政策企画課 〒742-2192 山口県大島郡周防大島町大字小松126番地2 電話 0820-74-1007		
8. 特定個人情報ファイルの取扱いに関する問合せ			
連絡先	税務課 〒742-2192 山口県大島郡周防大島町大字小松126番地2 電話 0820-74-1008		
9. 規則第9条第2項の適用			[]適用した
適用した理由			

Ⅱ しきい値判断項目

1. 対象人数		
評価対象の事務の対象人数は何人か	[1万人以上10万人未満]	<選択肢> 1) 1,000人未満(任意実施) 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
いつ時点の計数か	令和7年7月1日 時点	
2. 取扱者数		
特定個人情報ファイル取扱者数は500人以上か	[500人未満]	<選択肢> 1) 500人以上 2) 500人未満
いつ時点の計数か	令和7年7月1日 時点	
3. 重大事故		
過去1年以内に、評価実施機関において特定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

Ⅲ しきい値判断結果

しきい値判断結果	
基礎項目評価の実施が義務付けられる	

IV リスク対策

1. 提出する特定個人情報保護評価書の種類		
[基礎項目評価書]		<選択肢> 1) 基礎項目評価書 2) 基礎項目評価書及び重点項目評価書 3) 基礎項目評価書及び全項目評価書 2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。
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。）		
目的外の入手が行われ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
3. 特定個人情報の使用		
目的を超えた紐付け、事務に必要なの情報との紐付けが行われ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
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
4. 特定個人情報ファイルの取扱いの委託 []委託しない		
委託先における不正な使用等の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
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		
不正な提供・移転が行われる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
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)		
目的外の入手が行われ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
不正な提供が行われ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

7. 特定個人情報の保管・消去		
特定個人情報の漏えい・滅失・毀損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
8. 人手を介在させる作業		
	[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
人為的ミスが発生するリスクへの対策は十分か		■ 経常作業時におけるリスクに対する措置としては、以下を講じている。 ① 特定個人情報の入手に関する対策 ・ 目的外の入手防止: 軽自動車等の主たる定置場を有するかを判断し、課税対象でない申告は差し戻している。 ・ 地方税法等により記載項目・様式が定められており、不必要な情報の入手を防止している。 ・ 必要最低限のデータベースを使用し、不必要な特定個人情報を持たないことにしている。 ② 必要な情報以外の入手防止 ・ 課税対象者情報のみをシステム上で保有し、不必要な情報の入手を防止している。 ・ 認証・監査・証跡機能により、特定の権限者以外の操作を防止し、情報照会・提供の記録を保持している。 ③ 特定個人情報の使用に関する対策 ・ 目的を超えた紐付け防止: 個人番号利用業務以外では個人番号が含まれない画面表示としている。 ・ 他業務からは、アクセス制御によって、個人番号にアクセスできないように系統的に制御している。 ・ ユーザ認証の管理: 二要素認証によるユーザIDの認証を実施している。 ・ アクセス権限による機能の制限を実施している。 ・ 不正な端末からの利用を防止する制御を実施している。 ・ 人事異動等によりアクセス権限がなくなる場合、速やかにユーザIDの失効させている。 ④ 特定個人情報の提供・移転に関する対策 ・ 不正な提供・移転防止: アプリケーションの内部処理から個人番号を参照する際にも、アクセス制御が必ず反映される仕組みとしている。 ・ 提供・移転先の端末では、権限を持った職員の許可がなければ特定個人情報の閲覧や抽出ができない仕組みとしている。 ・ eLTAXを介して電子的に提供する場合は、適切に管理されたLGWAN回線を利用している。 ⑤ その他のリスク対策 ・ 監査と教育: 定期的な監査を実施している。 ・ 職員に対するセキュリティ研修を実施している。
	判断の根拠	

9. 監査		
実施の有無	☐ 〇 自己点検 ☐ 内部監査 ☐ 外部監査	
10. 従業員に対する教育・啓発		
従業員に対する教育・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
11. 最も優先度が高いと考えられる対策 [] 全項目評価又は重点項目評価を実施する		
最も優先度が高いと考えられる対策	☐ 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 ☐	
	<選択肢> 1) 目的外の入手が行われるリスクへの対策 2) 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への対策 3) 権限のない者によって不正に使用されるリスクへの対策 4) 委託先における不正な使用等のリスクへの対策 5) 不正な提供・移転が行われるリスクへの対策(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。) 6) 情報提供ネットワークシステムを通じて目的外の入手が行われるリスクへの対策 7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 9) 従業員に対する教育・啓発	
当該対策は十分か【再掲】	☐ 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
判断の根拠	■周防大島町における措置 ・人事異動の際には必ず住民情報システムの権限異動を実施し、不正なログイン等がないよう徹底している。また、共有フォルダ等へのアクセス権限も整理し、適切な運用を行っている。 ・サーバーのある電算室は電子施錠されており、許可された者のみ入室できるようになっており、物理的に特定個人情報へのアクセスができないよう運営している。 ■ガバメントクラウドにおける措置 ①物理的安全管理措置 ・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。 ・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。 ②技術的安全管理措置 ・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。 ・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ついて【第2.1版】」(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。 ・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。 ・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。 ・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。 ・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。 ・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。 ・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。	

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1年6月1日	4. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	番号法第19条第7号(特定個人情報の提供の制限)及び別表第二 (別表第二における情報提供の根拠) 別表第2の第3欄(情報提供者)が「市町村長」の項のうち、第4欄(特定個人情報)に「地方税関係情報」が含まれる項 (1.2,3,4,6,8,9,11,16,18,23,26,27,28,29,31,34,35,37,39,40,42,48,54,57,58,59,61,62,63,64,65,66,67,70,71,74,80,84,87,91,92,94,97,101,102,103,106,107,108,113,114,115,116,117及び120の項) (別表第2における情報照会の根拠) 別表第2の27の項	番号法第19条第7号(特定個人情報の提供の制限)及び別表第二 (別表第二における情報提供の根拠) 別表第2の第3欄(情報提供者)が「市町村長」の項のうち、第4欄(特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (別表第二における情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれら法律に基づく条例による地方税の賦課徴収又は地方税に関する調査(犯則事例の調査を含む。)」に関する事務であって主務省令で定めるもの」が含まれる項(27の項)及び番号法別表第二の主務省令で定める事務及び情報を定める命令第20条	事後	
令和3年5月19日	I 関連情報 4. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	番号法第19条第7号(特定個人情報の提供の制限)及び別表第二 (別表第二における情報提供の根拠) 別表第2の第3欄(情報提供者)が「市町村長」の項のうち、第4欄(特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (別表第二における情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれら法律に基づく条例による地方税の賦課徴収又は地方税に関する調査(犯則事例の調査を含む。)」に関する事務であって主務省令で定めるもの」が含まれる項(27の項)及び番号法別表第二の主務省令で定める事務及び情報を定める命令第20条	番号法第19条第8号(特定個人情報の提供の制限)及び別表第二 (別表第二における情報提供の根拠) 別表第2の第3欄(情報提供者)が「市町村長」の項のうち、第4欄(特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (別表第二における情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれら法律に基づく条例による地方税の賦課徴収又は地方税に関する調査(犯則事例の調査を含む。)」に関する事務であって主務省令で定めるもの」が含まれる項(27の項)及び番号法別表第二の主務省令で定める事務及び情報を定める命令第20条	事後	番号法の改正に伴う変更
令和6年10月1日	I 関連情報 3. 個人番号の利用 法令上の根拠	1、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(番号法)第9条第1項 別表第一 第16の項 2、番号法別表第一の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号) 第16条	番号法第9条第1項、別表の24の項	事後	番号法の改正(令和5年法律第48号、令和6年5月27日施行)による
令和6年10月1日	I 関連情報 4. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	番号法第19条第8号(特定個人情報の提供の制限)及び別表第二 (別表第二における情報提供の根拠) 別表第2の第3欄(情報提供者)が「市町村長」の項のうち、第4欄(特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (別表第二における情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれら法律に基づく条例による地方税の賦課徴収又は地方税に関する調査(犯則事例の調査を含む。)」に関する事務であって主務省令で定めるもの」が含まれる項(27の項)及び番号法別表第二の主務省令で定める事務及び情報を定める命令第20条	番号法第19条第8号に基づく主務省令第2条の表 (情報提供の根拠) 第3欄(情報提供者)が「市町村長」の項のうち、第4欄(利用特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれら法律に基づく条例又は森林環境税及び森林環境譲与税に関する法律(平成三十一年法律第三号による地方税又は森林環境税の賦課徴収に関する事務であって第五十条で定めるもの)」が含まれる項(48の項)	事後	番号法の改正(令和5年法律第48号、令和6年5月27日施行)による
令和6年10月1日	II しきい値判断項目 1. いつ時点の計数か		令和6年10月1日 時点	事後	記載内容の変更による
令和6年10月1日	II しきい値判断項目 2. いつ時点の計数か		令和6年10月1日 時点	事後	記載内容の変更による
令和6年10月1日	IV リスク対策 8. 人手を介在させる作業 人為的ミスが発生するリスクへの対策は十分か		十分である	事後	様式の変更による
令和6年10月1日	IV リスク対策 8. 人手を介在させる作業 人為的ミスが発生するリスクへの対策は十分か 【判断の根拠】		マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録等の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には4情報による照会を行うことを厳守している。また、上記のほか、下記の局面で特定個人情報の取扱いに関して手作業が介在するが、いずれの局面においても複数人での確認を行うようにしており、人為的ミスが発生するリスクへの対策は十分であると考えられる。 ・申請書に記載された個人番号及び本人情報のデータベースへの入力 ・特定個人情報の記載がある申請書等(USBメモリを含む。)の保管 ・個人番号及び本人情報が記載された申請書の廃棄	事後	様式の変更による

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6年10月1日	IV リスク対策 10. 従業者に対する教育・啓発	特に力を入れて行っている	十分に行っている	事後	様式の変更による
令和6年10月1日	IV リスク対策 11. 最も優先度が高いと考えらる対策		3) 権限のない者によって不正に使用されるリスクへの対策	事後	様式の変更による
令和6年10月1日	IV リスク対策 11. 最も優先度が高いと考えらる対策 当該対策は十分か【再掲】		十分である	事後	様式の変更による
令和6年10月1日	IV リスク対策 11. 最も優先度が高いと考えらる対策 当該対策は十分か【再掲】 【判断の根拠】		・人事異動の際には必ず住民情報システムの権限異動を実施し、不正なログイン等がないよう徹底している。また、共有フォルダ等へのアクセス権限も整理し、適切な運用を行っている。 ・サーバーのある電算室は電子施錠されており、許可された者のみ入室できるようになっており、物理的に特定個人情報へのアクセスができないよう運営している。	事後	様式の変更による
令和7年7月1日	I 関連情報 1. 特定個人情報ファイルを取り扱う事務 ③システムの名称	軽自動車税システム、収納管理システム、団体内統合宛名システム、中間サーバー	・軽自動車税システム(基本セット内) ・宛名管理システム(基本セット内) ・団体内統合宛名システム(基本セット内) ・EUCシステム(基本セット内) ・統合収納管理システム(基本セット内) ・統合滞納管理システム(基本セット内) ・地方公共団体情報連携中間サーバーシステム ・コンビニ交付システム ・軽自動車税納付確認システム(軽JNKS) ・軽自動車検査情報市区町村提供システム ・軽自動車保有関係手続のワンストップサービス(軽OSS) ・統合宛名管理システム(基本セット内) ・課税資料イメージファイリングシステム	事前	地方公共団体情報システム標準化・共通化移行による
令和7年7月1日	I 関連情報 2. 特定個人情報ファイル名	軽自動車税情報ファイル、収納情報ファイル、宛名情報ファイル	・軽自動車税関係ファイル ・統合収納関係ファイル ・統合滞納関係ファイル ・住登外者宛名番号管理関係ファイル ・団体内統合宛名関係ファイル	事前	地方公共団体情報システム標準化・共通化 移行による
令和7年7月1日	I 関連情報 4. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表 (情報提供の根拠) 第3欄(情報提供者)が「市町村長」の項のうち、第4欄(利用特定個人情報)に「地方税関係情報」が含まれる項並びに関係する主務省令で定める事務及び情報を定める命令 (情報照会の根拠) 第1欄(情報照会者)が「市町村長」のうち、第2欄(事務)に「地方税法その他の地方税法に関する法律及びこれらの法律に基づく条例又は森林環境税及び森林環境譲与税に関する法律(平成三十一年法律第三号による地方税又は森林環境税の賦課徴収に関する事務であって第五十条で定めるもの)」が含まれる項(48の項)	・番号法第19条第8号(特定個人情報の提供の制限)及び「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第十九条第八号に基づく利用特定個人情報の提供に関する命令」(利用特定個人情報省令)第2条の表 <利用特定個人情報省令第2条の表における情報提供の根拠> ・軽自動車税(種別割)事務では、情報提供は実施していない。 <利用特定個人情報省令第2条の表における情報照会の根拠> ・第一欄(情報照会者)が「市町村長」の項のうち、第二欄(事務)に「地方税法」が含まれる項 ・公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律による特定公的給付の支給の実施(160の項)	事前	地方公共団体情報システム標準化・共通化 移行による
令和7年7月1日	IV リスク対策 4. 特定個人情報ファイルの取扱いの委託	委託しない	十分である	事前	地方公共団体情報システム標準化・共通化 移行による

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7年7月1日	IV リスク対策 8. 人手を介在させる作業判断の根拠	マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドラインに従い、マイナンバー登録等の際には、本人からのマイナンバー取得の徹底や、住基ネット照会を行う際には4情報による照会を行うことを厳守している。また、上記のほか、下記の局面で特定個人情報の取扱いに関して手作業が介在するが、いずれの局面においても複数人での確認を行うようにしており、人為的ミスが発生するリスクへの対策は十分であると考えられる。 ・申請書に記載された個人番号及び本人情報のデータベースへの入力 ・特定個人情報の記載がある申請書等(USBメモリを含む。)の保管 ・個人番号及び本人情報が記載された申請書の廃棄	■経常作業時におけるリスクに対する措置としては、以下を講じている。 ①特定個人情報の入手に関する対策 ・目的外の入手防止:軽自動車等の主たる定置場を有するかを判断し、課税対象でない申告は差し戻している。 ・地方税法等により記載項目・様式が定められており、不必要な情報の入手を防止している。 ・必要最低限のデータベースを使用し、不必要な特定個人情報を持たないことにしている。 ②必要な情報以外の入手防止 ・課税対象者情報のみをシステム上で保有し、不必要な情報の入手を防止している。 ・認証・監査・証跡機能により、特定の権限者以外の操作を防止し、情報照会・提供の記録を保持している。 ③特定個人情報の使用に関する対策 ・目的を超えた紐付け防止:個人番号利用業務以外では個人番号が含まれない画面表示としている。 ・他業務からは、アクセス制御によって、個人番号にアクセスできないようにシステムの制御している。 ・ユーザ認証の管理:二要素認証によるユーザIDの認証を実施している。 ・アクセス権限による機能の制限を実施している。 ・不正な端末からの利用を防止する制御を実施している。 ・人事異動等によりアクセス権限がなくなる場合、速やかにユーザIDの失効させている。 ④特定個人情報の提供・移転に関する対策 ・不正な提供・移転防止:アプリケーションの内部処理から個人番号を参照する際にも、アクセス制御が必ず反映される仕組みとしている。 ・提供・移転先の端末では、権限を持った職員のみ許可がなければ特定個人情報の閲覧や抽出	事前	地方公共団体情報システム標準化・共通化 移行による
令和7年7月1日	IV リスク対策 11. 最も優先度が高いと考えられる対策 最も優先度が高いと考えられる対策	3) 権限のない者によって不正に使用されるリスクへの対策	8) 特定個人情報の漏えい・滅失・毀損リスクへの対策	事前	地方公共団体情報システム標準化・共通化 移行による
令和7年7月1日	IV リスク対策 11. 最も優先度が高いと考えられる対策 判断の根拠	・人事異動の際には必ず住民情報システムの権限異動を実施し、不正なログイン等がないよう徹底している。また、共有フォルダ等へのアクセス権限も整理し、適切な運用を行っている。 ・サーバーのある電算室は電子施錠されており、許可された者のみ入室できるようになっており、物理的に特定個人情報へのアクセスができないよう運営している。	■周知入局時における措置 ・人事異動の際には必ず住民情報システムの権限異動を実施し、不正なログイン等がないよう徹底している。また、共有フォルダ等へのアクセス権限も整理し、適切な運用を行っている。 ・サーバーのある電算室は電子施錠されており、許可された者のみ入室できるようになっており、物理的に特定個人情報へのアクセスができないよう運営している。 ■ガバメントクラウドにおける措置 ①物理的安全管理措置 ・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。 ・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。 ②技術的安全管理措置 ・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。 ・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ついて【第2.1版】」(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。 ・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日継続する	事前	地方公共団体情報システム標準化・共通化 移行による