

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
5	収滞納管理 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

明和町は、収納・滞納等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

なし

評価実施機関名

明和町長

公表日

令和6年12月26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	取滞納管理事務
②事務の概要	取滞納管理事務処理にあたり、より効率的・効果的な業務を推進し、収納率の向上はもとより、厳正・適正な滞納整理を実施し、税負担の公平と納税秩序の確立を図る
③システムの名称	1. 取滞納管理システム(e-ADWORLD2, ライフパートナー) 2. 団体内統合宛名システム 3. 中間サーバー
2. 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、3. 口座振替ファイル	
3. 個人番号の利用	
法令上の根拠	番号法第9条第1項 別表第一の16の項
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> [実施する] 1) 実施する 2) 実施しない 3) 未定
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) なし(取滞納管理に関する事務において情報提供ネットワークシステムによる情報提供は行わない) (別表第二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賦課徴収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)
5. 評価実施機関における担当部署	
①部署	税務課
②所属長の役職名	税務課長
6. 他の評価実施機関	
なし	
7. 特定個人情報の開示・訂正・利用停止請求	
請求先	総務課 三重県多気郡明和町大字馬之上945番地 0596-52-7111
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 三重県多気郡明和町大字馬之上945番地 0596-52-7143
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	<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	[1万人以上10万人未満] 令和6年12月24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	<選択肢> 1) 500人以上 2) 500人未満
いつ時点の計数か	[500人未満] 令和6年12月24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	<選択肢> 1) 発生あり 2) 発生なし
[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	[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
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	<div style="display: flex; justify-content: space-between; align-items: center;"> [十分である] <div style="text-align: right;"> <p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p> </div> </div>
8. 人手を介在させる作業	
[] 人手を介在させる作業はない	
人為的ミスが発生するリスクへの対策は十分か	<div style="display: flex; justify-content: space-between; align-items: center;"> [十分である] <div style="text-align: right;"> <p><選択肢></p> <p>1) 特に力を入れている</p> <p>2) 十分である</p> <p>3) 課題が残されている</p> </div> </div>
判断の根拠	<p>特定個人情報を受け渡す際は、事前に、暗号化、パスワードによる保護、確実なマスキング処理等を行うとともに、これらの対策を確実に実施したことの確認を複数人で行うなどの対策を講じていることから、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。</p>

9. 監査	
実施の有無	<input type="checkbox"/> 自己点検 <input type="checkbox"/> 内部監査 <input type="checkbox"/> 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	<input type="checkbox"/> 十分に行っている <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <選択肢> <ol style="list-style-type: none"> 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 <input type="checkbox"/> 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	<input type="checkbox"/> 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 <input type="checkbox"/> <選択肢> <ol style="list-style-type: none"> 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】	<input type="checkbox"/> 十分である <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <選択肢> <ol style="list-style-type: none"> 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	システムにアクセス可能な職員はIDと静脈認証によって限定しており、アクセス可能な職員の名簿は年度ごとに管理することで、アクセス権限の適切な管理を行っている。またアクセスログを記録し不正なアクセスがないことを定期的に確認している。これらの対策を講じていることから権限のないものによって不正に使用されるリスクへの対策は「十分である」と考えられる。

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
平成29年6月15日	I - 5. - ②	税務課長 北岡 和成	税務課長 松井 友吾	事後	
平成29年6月15日	II - 1. - 時点日欄	平成26年10月31日 時点	平成29年5月31日 時点	事後	
平成29年6月15日	II - 2. - 時点日欄	平成26年10月31日 時点	平成29年5月31日 時点	事後	
平成30年8月31日	I - 5. - ②	税務課長 松井 友吾	税務課長	事後	
平成30年8月31日	II - 1. - 時点日欄	平成29年5月31日 時点	平成30年8月31日 時点	事後	
平成30年8月31日	II - 2. - 時点日欄	平成29年5月31日 時点	平成30年8月31日 時点	事後	
令和1年5月31日	II - 1. - 時点日欄	平成30年8月31日 時点	令和1年5月31日 時点	事後	
令和1年5月31日	II - 2. - 時点日欄	平成30年8月31日 時点	令和1年5月31日 時点	事後	
令和1年5月31日	IV. リスク対策	(様式変更に伴う記載内容追加)	IV全体を新たに記載	事後	
令和2年9月29日	I - 7. - 請求先	総務課長	総務防災課	事後	
令和2年9月29日	II - 1. - 時点日欄	令和1年5月31日 時点	令和2年9月29日 時点	事後	
令和2年9月29日	II - 2. - 時点日欄	令和1年5月31日 時点	令和2年9月29日 時点	事後	
令和3年8月20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項 別表第二の27の項	<p>・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</p> <p>(別表第二における情報提供の根拠) なし (収滞納管理に関する事務において情報提供ネットワークシステムによる情報提供は行わない)</p> <p>(別表第二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賦課徴収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)</p>	事前	番号法第19条に係る改正の施行日に先立ち、事前に公表
令和3年8月20日	II - 1. - 時点日欄	令和2年9月29日 時点	令和3年8月20日 時点	事後	
令和3年8月20日	II - 2. - 時点日欄	令和2年9月29日 時点	令和3年8月20日 時点	事後	

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4年6月2日	Ⅱ - 1. - 時点日欄	令和3年8月20日 時点	令和4年6月2日 時点	事後	
令和4年6月2日	Ⅱ - 2. - 時点日欄	令和3年8月20日 時点	令和4年6月2日 時点	事後	
令和5年6月23日	Ⅱ - 1. - 時点日欄	令和4年6月2日 時点	令和5年6月23日 時点	事後	
令和5年6月23日	Ⅱ - 2. - 時点日欄	令和4年6月2日 時点	令和5年6月23日 時点	事後	
令和6年12月24日	Ⅱ - 1. - 時点日欄	令和5年6月23日 時点	令和6年12月24日 時点	事後	
令和6年12月24日	Ⅱ - 2. - 時点日欄	令和5年6月23日 時点	令和6年12月24日 時点	事後	
令和6年12月24日	I - 7. - 請求先	総務防災課	総務課	事後	
令和6年12月24日	Ⅳ. 8 人手を介在させる作業	-	十分である	事後	
令和6年12月24日	Ⅳ. 8 判断の根拠	-	特定個人情報を受け渡す際(USB メモリを使用する場合を含む。)は、事前に、暗号化、パスワードによる保護、確実なマスキング処理等を行うとともに、これらの対策を確実に実施したことの確認を複数人で行うなどの対策を講じていることから、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。	事後	
令和6年12月24日	Ⅳ. 11 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	事後	
令和6年12月24日	Ⅳ. 11 当該対策は十分か	-	十分である	事後	
令和6年12月24日	Ⅳ. 11 判断の根拠	-	システムにアクセス可能な職員はIDと静脈認証によって限定しており、アクセス可能な職員の名簿は年度ごとに管理することで、アクセス権限の適切な管理を行っている。 またアクセスログを記録し不正なアクセスがないことを定期的に確認している。これらの対策を講じていることから権限のないものによって不正に使用されるリスクへの対策は「十分である」と考えられる。	事後	