

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期にかかる説明
令和6年3月18日	【賦課情報ファイル】 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－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。)ーリスク2:不適切な方法で提供・移転が行われるリスクーリスクに対する措置の内容	番号法第19条第9号	番号法第19条第10号	事後	法改正によるもの
令和6年3月18日	【滞納情報ファイル】 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－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。)ーリスク2:不適切な方法で入手が行われるリスクーリスクに対する措置の内容	個人情報保護条例	個人情報の保護に関する法律(平成15年法律第57号)	事後	加古川市個人情報保護条例の廃止に伴うもの
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供ネットワークシステムとの接続ーリスク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ーリスクに対する措置の内容	総務大臣	内閣総理大臣	事後	法改正によるもの
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供ネットワークシステムとの接続ーリスク3. 入手した特定個人情報が不正確であるリスクーリスクに対する措置の内容	総務大臣	内閣総理大臣	事後	法改正によるもの
令和6年3月18日	V 開示請求、問合せー1.特定個人情報の開示・訂正・利用停止請求ー②請求方法	加古川市個人情報保護条例第20条	個人情報の保護に関する法律第77条	事後	加古川市個人情報保護条例の廃止に伴うもの
令和6年3月18日	I 基本情報ー5. 個人番号の利用ー法令上の根拠	(追加)	2. 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(令和3年法律第38号)第9条	事前	ー

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期にかかる説明
令和6年3月18日	【賦課情報ファイル】 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-6. 情報提供ネットワークとの接続-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	(追加)	<団体内統合宛名システムにおける措置> 番号法上認められた職務権限を有する職員しか特定個人情報にアクセスが行えないよう制御されている。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため
令和6年3月18日	【賦課情報ファイル】 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-6. 情報提供ネットワークとの接続-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	(追加)	<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中間サーバーとLGWANで接続される等、外部を排除した限られたネットワーク内での連携となるので安全は確保される。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため
令和6年3月18日	【賦課情報ファイル】 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-6. 情報提供ネットワークとの接続-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	(追加)	<団体内統合宛名システムにおける措置> 中間サーバーとの連携は団体内宛名番号で紐づく仕組みのため、入手した特定個人情報は正確性が保たれる。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期にかかる説明
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供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－リスクに対する措置の内容	(追加)	<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中間サーバーとLGWANで接続される等、外部を排除した限られたネットワーク内での入手であるため、漏洩・紛失のリスクはない。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供ネットワークとの接続－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	(追加)	<団体内統合宛名システムにおける措置> 番号法上認められた職務権限を有する職員しか特定個人情報にアクセスが行えないよう制御されているため、安全は確保される。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供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－リスクに対する措置の内容	(追加)	<団体内統合宛名システムにおける措置> 提供の記録が逐一保存される仕組みが整備された情報提供ネットワークシステムを用いて連携することで、不適切な方法で特定個人情報が提供されることを防止する。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期にかかる説明
令和6年3月18日	【賦課情報ファイル】 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－6. 情報提供ネットワークとの接続－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	(追加)	<団体内統合宛名システムにおける措置> 中間サーバーへの連携は適切な頻度で行い、その正確性を担保する。また、情報提供の際は相手先とその妥当性について検証し、誤った相手に提供してしまうことを防止することが担保されたシステムを国が構築している。	事後	従来から対策を行っていたが、リスク対策に関する責任範囲を明確にするため
令和6年3月18日	【収納情報ファイル】 Ⅱ 特定個人情報ファイルの概要－6. 特定個人情報の保管・消去－①保管場所	(追加)	<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。	事前	-
令和6年3月18日	【収納情報ファイル】 Ⅱ 特定個人情報ファイルの概要－6. 特定個人情報の保管・消去－③消去方法	・保管期間を終了したデータは適宜システムから削除を行う。	<当市の保有システムにおける措置> ・保管期間が終了したものはシステムで一括消去する。 ・保管期間を過ぎた申告書等紙媒体の特定個人情報については、文書取扱規程に基づき外部事業者にて溶解処理を行っている。 <中間サーバー・プラットフォームにおける措置> ・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。	事前	-
令和6年3月18日	【収納情報ファイル】 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－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(入手) 【 】接続しない(提供)	事前	-

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期にかかる説明
令和6年3月18日	【収納情報ファイル】 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－6. 情報提供ネットワークシステムとの接続	(項目全て空白)	(項目全て追加)	事前	-
令和6年3月18日	【収納情報ファイル】 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. 特定個人情報の保管・消去－⑤物理的対策－具体的な対策の内容	(追加)	<p><中間サーバー・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・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いない物品、記録媒体、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。 	事前	-
令和6年3月18日	【収納情報ファイル】 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. 特定個人情報の保管・消去－⑥技術的対策－具体的な対策の内容	(追加)	<p><中間サーバー・プラットフォームにおける措置></p> <ul style="list-style-type: none"> ・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。 	事前	-