（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
令和4年8月10日	Ⅱ ファイルの概要_本人確認 2. 基本情報 ⑥事務担当部署	企画総務局総務課、各区市民部市民課及び出張所	企画総務局区政課、各区市民部市民課及び出張所	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_本人確認 3. 特定個人情報の入手・使用 ⑦使用の主体 使用部署	企画総務局総務課、各区市民部市民課及び出張所	企画総務局区政課、各区市民部市民課及び出張所	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_送付先 2. 基本情報 ⑥事務担当部署	企画総務局総務課、各区市民部市民課及び出張所	企画総務局区政課、各区市民部市民課及び出張所	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_送付先 3. 特定個人情報の入手・使用 ⑦使用の主体 使用部署	企画総務局総務課、各区市民部市民課及び出張所	企画総務局区政課、各区市民部市民課及び出張所	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_住基台帳 6. 特定個人情報の保管・消去 ③消去方法	・委託業者により特定個人情報が保存された記録媒体に対して一定回数以上の無作為な書き込み等を行った上で、媒体そのものを物理的に破壊する。なお、廃棄については、住民記録システム情報セキュリティ実施手順に基づき、情報システム業務管理者(システムを所管する課（総務課）長)の承認を得るとともに、管理台帳に廃棄日・処理内容を記録する。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。	・委託業者により特定個人情報が保存された記録媒体に対して一定回数以上の無作為な書き込み等を行った上で、媒体そのものを物理的に破壊する。なお、廃棄については、住民記録システム情報セキュリティ実施手順に基づき、情報システム業務管理者(システムを所管する課（区政課）長)の承認を得るとともに、管理台帳に廃棄日・処理内容を記録する。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 3. 特定個人情報の使用 リスク2 アクセス権限の発効・失効の管理 具体的な管理方法	1. 発効管理 ・人事異動等により、ユーザIDの登録が必要な場合、情報システム利用管理者（業務担当課（各区市民課等）所属長）は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(総務課)長）に提出し、承認を得る。 ・情報システム業務管理者は、職員のアクセス権を職務内容に沿ったものであるか確認した上で登録する。 2. 失効管理 ・人事異動等により、ユーザーIDの削除が必要な場合、情報システム利用管理者は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(総務課)長）に提出し、承認を得る。 ・情報システム業務管理者は、ユーザID申請書に基づき、ユーザIDの削除を行う。	1. 発効管理 ・人事異動等により、ユーザIDの登録が必要な場合、情報システム利用管理者（業務担当課（各区市民課等）所属長）は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、職員のアクセス権を職務内容に沿ったものであるか確認した上で登録する。 2. 失効管理 ・人事異動等により、ユーザーIDの削除が必要な場合、情報システム利用管理者は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、ユーザID申請書に基づき、ユーザIDの削除を行う。	事後	組織名の変更によるもので、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ていない。
令和4年8月10日	Ⅴ開示請求、問合せ 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	広島市企画総務局総務課 〒730－8586 広島市中区国泰寺町一丁目6番34号 電話番号：082－504－2112（直通）	広島市企画総務局区政課 〒730－8586 広島市中区国泰寺町一丁目6番34号 電話番号：082－504－2112（直通）	事後	組織名の変更によるもので、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ていない。

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8月10日	Ⅱ ファイルの概要_住基台帳 6. 特定個人情報の保管・消去 ①保管場所	・データセンターでは、以下の3か所の入口において入退管理を行う。それぞれの入口を通過するためには、事前に入室申請がなされた個人ごとのICカードが必要となる。また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 なお、上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。	・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_住基台帳 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＞ ①中間サーバー･プラットフォームは中間サーバー用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。	＜中間サーバー・プラットフォームにおける措置＞ ①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。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_住基台帳 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＞ ②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＞ ②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、物理的破壊により完全に消去する。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅱ ファイルの概要_本人確認 6. 特定個人情報の保管・消去 ①保管場所	・データセンターでは、以下の3か所の入口において入退管理を行う。それぞれの入口を通過するためには、事前に入室申請がなされた個人ごとのICカードが必要となる。また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 なお、上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。	・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。	事後	現状の運用を明文化したことによるもので、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ていない。

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8月10日	Ⅱ ファイルの概要_送付先 6. 特定個人情報の保管・消去 ①保管場所	・データセンターでは、以下の3か所の入口において入退管理を行う。それぞれの入口を通過するためには、事前に入室申請がなされた個人ごとのICカードが必要となる。また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 なお、上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。	・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策(プロセス)_ 住基台帳 3. 特定個人情報の使用 リスク2 アクセス権限の発効・失効の管理 具体的な管理方法	＜共通基盤における措置＞ 1. 発効管理 ・人事異動等により、ユーザIDの登録が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書を共通基盤管理者に提出し、承認を得る。 ・共通基盤管理者はユーザID申請書に基づき、ユーザIDの割り当て及びICカードの発行を行う。	＜共通基盤における措置＞ 1. 発効管理 (1)人事異動等により、ユーザIDの登録が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書を共通基盤管理者に提出し、承認を得る。 (2)共通基盤管理者はユーザID申請書に基づき、ユーザIDの割り当て及びICカードの発行を行う。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策(プロセス)_ 住基台帳 3. 特定個人情報の使用 リスク2 特定個人情報の使用の記録 具体的な方法	＜共通基盤における措置＞ ・共通基盤の利用に係る稼働記録(ログ)では、利用者、日時、利用端末等を記録している。 ・稼働記録(ログ)は、10年間保存することとしている。	＜共通基盤における措置＞ ・共通基盤の利用に係る操作記録(ログ)では、利用者、日時、利用端末等を記録している。 ・操作記録(ログ)は、10年間保存することとしている。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策(プロセス)_ 住基台帳 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	＜共通基盤における措置＞ 共通基盤の利用に係る稼働記録(ログ)を取得・保存しており、事務外で利用した場合には、その職員を特定可能であることを職員に周知し、事務外での使用の抑止を図っている。	＜共通基盤における措置＞ 共通基盤の利用に係る操作記録(ログ)を取得・保存しており、事務外で利用した場合には、その職員を特定可能であることを職員に周知し、事務外での使用の抑止を図っている。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策(プロセス)_ 住基台帳 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	契約時に受託者の情報資産の管理体制(ISO27001認証、プライバシーマーク認定)を確認するとともに、情報資産の取扱いを徹底するため、業務に従事する要員の誓約書を提出させている。	契約時に受託者の情報資産の管理体制(ISO27001認証、プライバシーマーク認定)を確認するとともに、情報資産の取扱いを徹底するため、誓約書を提出させている。	事後	現状の運用を明文化したことによるもので、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ていない。

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8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な方法	＜共通基盤における措置＞ ・共通基盤に係る稼働記録（ログ）を取得・保存している（委託先及び再委託先の従業員がシステムを操作する場合を含む。）。 ・稼働記録（ログ）には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・稼働記録（ログ）はそれぞれ、10年間保存することとしている。	＜共通基盤における措置＞ ・委託先及び再委託先の従業員の共通基盤に係る操作記録（ログ）を取得し、保存している。 ・操作記録（ログ）には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録（ログ）はそれぞれ、10年間保存することとしている。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの提供ルール 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	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、誓約書を提出させている。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 5. 特定個人情報の提供・移転リスク1 特定個人情報の提供・移転の記録 具体的な方法	＜共通基盤における措置＞ ・共通基盤に係る稼働記録（ログ）については、日時、連携ID、移転・提供元システム名、移転・提供先システム名等を記録している。 ・稼働記録（ログ）はそれぞれ、10年間保存することとしている。	＜共通基盤における措置＞ ・共通基盤に係る操作記録（ログ）については、日時、連携ID、移転・提供元システム名、移転・提供先システム名等を記録している。 ・操作記録（ログ）はそれぞれ、10年間保存することとしている。	事後	現状の運用を明文化したことによるもので、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ていない。
	Ⅲ リスク対策（プロセス）_ 住基台帳 6. 情報提供ネットワークシステムとの接続 リスク5 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＞ ①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（※）。 ②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。 ③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。 ④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・ソフトウェアにおける措置＞ ①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用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、照会許可用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。 ②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。 ③機微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。 ④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。	事後	現状の運用を明文化したことによるもので、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ていない。

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8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 7. 特定個人情報の消去 リスク1 ⑤物理的対策 具体的な対策の内容	・データセンターでは、以下の3か所の入口において入退管理を行う。それぞれの入口を通過するためには、事前に入室申請がなされた個人ごとのICカードが必要となる。また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートは有人監視を実施しており、それぞれの入口には監視カメラを設置している。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 なお、上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。	・データセンターでは、以下の3か所の入口において入退管理を行う。 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証（指紋）の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること（共連れ）を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 7. 特定個人情報の消去 リスク1 ⑤物理的対策 具体的な対策の内容	＜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。	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを中間サーバー用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。 ②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。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅳ リスク対策（その他） 2. 従業員に対する教育・啓発 従業員に対する教育・啓発 具体的な方法	＜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、毎年1回、自己点検を実施することとしている。	＜中間サーバー・プラットフォームにおける措置＞ IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、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、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 本人確認 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	契約書に定める情報保護管理に関する事項を遵守させ、契約締結時には、業務に従事する要員全員の誓約書を提出させている。 また、月1回は委託業務の履行状況を書面により報告させ、情報保護管理を適正に実施していることを確認している。	契約書に定める情報保護管理に関する事項を遵守させ、契約締結時には、誓約書を提出させている。 また、月1回は委託業務の履行状況を書面により報告させ、情報保護管理を適正に実施していることを確認している。	事後	現状の運用を明文化したことによるもので、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ていない。

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8月10日	Ⅲ リスク対策（プロセス）_ 本人確認 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの提供ルール 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	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書において、本市は委託先に対し、報告及び立入検査の実施を求めることができる。	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、誓約書を提出させている。 ・契約書において、本市は委託先に対し、報告及び立入検査の実施を求めることができる。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 本人確認 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・個人情報の適正な管理について契約書に規定し、委託先等職員以外の従業者には、適正な個人情報の取扱いに係る誓約書を提出させる。	・システムの操作履歴(操作ログ)を記録する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・個人情報の適正な管理について契約書に規定し、適正な個人情報の取扱いに係る誓約書を委託先から提出させる。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 送付先 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・個人情報の適正な管理について契約書に規定し、委託先等職員以外の従業者には、適正な個人情報の取扱いに係る誓約書を提出させる。	・システムの操作履歴(操作ログ)を記録する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・個人情報の適正な管理について契約書に規定し、適正な個人情報の取扱いに係る誓約書を委託先から提出させる。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 送付先 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	契約書に定める情報保護管理に関する事項を遵守させ、契約締結時には、業務に従事する要員全員の誓約書を提出させている。 また、月１回は委託業務の履行状況を書面により報告させ、情報保護管理を適正に実施していることを確認している。	契約書に定める情報保護管理に関する事項を遵守させ、契約締結時には、誓約書を提出させている。 また、月１回は委託業務の履行状況を書面により報告させ、情報保護管理を適正に実施していることを確認している。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_送付先 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの提供ルール 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	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書において、本市は委託先に対し、報告及び立入検査の実施を求めることができる。	・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項により個人情報の適正な取扱いを義務づけるとともに、誓約書を提出させている。 ・契約書において、本市は委託先に対し、報告及び立入検査の実施を求めることができる。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 2. 特定個人情報の入手 リスク3 入手の際の本人確認の措置の内容	＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の情報と紐付けられたり、全く別の情報に書き換えられたりすることはない。	＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の情報と紐付けられたり、別の情報に書き換えられたりすることはない。	事後	現状の運用を明文化したことによるもので、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ていない。

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8月10日	Ⅲ リスク対策（プロセス）_ 住基台帳 2. 特定個人情報の入手 リスク3 特定個人情報の正確性確保の措置の内容	＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の個人番号と紐付けられたり、全く別の番号に書き換えられたりすることはない。	＜共通基盤における措置＞ ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の個人番号と紐付けられたり、別の番号に書き換えられたりすることはない。	事後	現状の運用を明文化したことによるもので、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ていない。
令和4年8月10日	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 ②請求方法 特記事項	広島市ホームページに請求方法や手数料等について掲載している。 http://www.city.hiroshima.lg.jp/www/contents/0000000000000/1118363629312/index.html	広島市ホームページに請求方法や手数料等について掲載している。 https://www.city.hiroshima.lg.jp/soshiki/5/5470.html	事後	現状の運用を明文化したことによるもので、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ていない。
令和6年12月25日	Ⅰ　基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	（右記を追加）	届出は窓口や郵送での書類の受入、サービス検索・電子申請機能での受領により行う。 サービス検索・電子申請機能により申請された電子申請データを申請管理システムにより受領又は基幹システムに取り込むことにより行う。	事前	
令和6年12月25日	Ⅰ　基本情報 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6を追加	事前	
令和6年12月25日	Ⅰ　基本情報 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3①システムの名称	共通基盤（庁内連携システム及び宛名システムに相当）	共通基盤（庁内連携システム、宛名システム及び申請管理システムに相当）	事前	
令和6年12月25日	Ⅰ　基本情報 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 ③他のシステムとの接続	証明書発行システム	証明書発行システム、申請管理システム	事前	
令和6年12月25日	Ⅰ　基本情報 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2 ②システムの機能	3. 個人番号カードを利用した転入（特例転入） ：転入の届出を受け付けた際に、あわせて個人番号カードが提示された場合、当該個人番号カードを用いて転入処理を行う。 4. 本人確認情報検索 ：統合端末において入力された4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。	3. 個人番号カードを利用した転入（特例転入） ：個人番号カードの交付を受けている者等の転入が予定される場合に、転出証明書情報をCSを通じて受け取り、その者に係る転入の届出を受け付けた際に、個人番号カードを用いて転入処理を行う（一定期間経過後も転入の届出が行われない場合は、受け取った転出証明書情報を消去する。）。 4. 本人確認情報検索 ：統合端末において入力された住民票コード、個人番号又は4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月25日	Ⅰ　基本情報 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3 ②システムの機能	（右記を追加）	（略） サービス検索・電子申請機能と共通基盤間のデータ連携を行い、サービス検索・電子申請機能への申請データ取得要求及び返信のあった申請データの取得並びに申請データ処理状況の登録を行う。取得した申請データは、「2. システム間連携制御機能」により住民記録システムからマイナンバーカードに搭載されている利用者証明用電子証明書のシリアル番号と住記宛名番号が紐づいた情報を取得し、申請データに含まれるシリアル番号を住記宛名番号へ変換し、住記宛名番号及び団体内統合宛名番号を申請データに紐づけてデータベースに保管するとともに、申請データを業務システムに連携する機能。	事前	
令和6年12月25日	Ⅰ　基本情報 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3 ③他のシステムとの接続	（右記を追加）	（略）サービス検索・電子申請機能	事前	
令和6年12月25日	Ⅰ　基本情報 6. 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	:番号利用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1、2、3、4、6、7、8、10、12、13、14、16、20、22、22の3、22の4、23、24、24の2、24の3、25、26の3、27、28、31、31の2、31の3、32、33、37、38、39、40、41、43、43の3、43の4、44の2、45、47、48、49の2、50、51、53、55、56、57、58、59、59の2、59の3条 ※番号利用法別表第二の21、30、89、105、117の項に係る主務省令は未制定。	（右記を削除）	事前	
令和6年12月25日	（別添1）住民基本台帳 事務の内容	資料の差し替え	資料の差し替え	事前	
令和6年12月25日	（別添1）住民基本台帳 事務の内容 備考	1. 住民基本台帳の記載に関する事務 1-①. 住民から異動届等の届出を受け付ける。 1-②. 既存住基システムに異動情報を入力し、住民基本台帳を更新する。 （中略） 9. 既存住基システムと証明書発行システムとの連携 9-①. 住民票の写し等を発行するために必要となる証明書データの異動情報を、証明書発行システムに送信する。 9-②. 市町村CSから住民票コード及び電子証明書シリアル番号情報を受領し、証明書発行システムに送信する。	1. 住民基本台帳の記載に関する事務 1-①. 住民から異動届等の届出を受け付ける。 1-②. 既存住基システムに異動情報を入力し、住民基本台帳を更新する。 1-③. 住民から転出届、転入予定連絡を受け付ける。 1-④. マイナポータルから転出届、転入予定連絡をダウンロードする。 1-⑤. 共通基盤の申請管理システムから転出届、転入予定連絡を受信し、住民基本台帳を更新する。 （中略） 9. 既存住基システムと証明書発行システムとの連携 9-①. 市町村CSから住民票コード及び電子証明書シリアル番号を受信する。 9-②. 住民票の写し等を発行するために必要となる証明書データの異動情報とシリアル番号を、証明書発行システムに送信する。 9-③. 宛名番号を紐づけたシリアル番号を共通基盤の申請管理システムに送信する。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月25日	（別添1）本人確認・送付先情報 事務の内容 備考	3. 個人番号カードを利用した転入（特例転入） 3-①.転入手続を行う住民から提示された個人番号カードを利用して本人確認(「2. 本人確認」を参照)を行う。 3-②.統合端末から、市町村CSを経由して転出地市町村に対し転出証明書情報の送信依頼を行う（※特定個人情報を含まない）。 3-③.市町村CSにおいて転出地市町村より転出証明書情報を受信する。 3-④.既存住基システムにおいて、市町村CSから転出証明書情報を受信し、転入処理を行う。 （中略） 4. 本人確認情報検索に関する事務 4-①.基本4情報の組み合わせをキーワードとして、市町村CSの本人確認情報を検索する。	3. 個人番号カードを利用した転入（特例転入） 3-①.市町村CSにおいて転出地市町村より転出証明書情報を受信する。 3-②.既存住基システムにおいて、市町村CSから転出証明書情報を受信する。 3-③.転入手続を行う住民から提示された個人番号カードを利用して本人確認(「2. 本人確認」を参照)を行う。 ※転出証明書情報に記載の転出の予定年月日から30日後までに転入手続が行われない場合には、当該転出証明書情報を消去する。 ※3-③の転入手続時に転出証明書情報を受信していない場合又は消去している場合には、統合端末から、市町村CSを経由して 転出地市町村に対し転出証明書情報の送信依頼を行い(※特定個人情報を含まない)、その後、3-①・②を行う。 3-④.既存住基システムにおいて、転入処理を行う。 （中略） 4. 本人確認情報検索に関する事務 4-①.住民票コード、個人番号又は4情報の組み合わせをキーワードとして、市町村CSの本人確認情報を検索する。	事前	
令和6年12月25日	Ⅱ ファイルの概要_住基台帳 3. 特定個人情報の入手・使用 ①入手元	（右記を追加）	情報システム課	事前	
令和6年12月25日	Ⅱ ファイルの概要_住基台帳 3. 特定個人情報の入手・使用 ②入手方法 その他	（右記を追加）	サービス検索・電子申請機能、申請管理システム	事前	
令和6年12月25日	Ⅱ ファイルの概要_住基台帳6. 特定個人情報の保管・消去③消去方法	（右記を追加）	・マイナンバー利用事務系端末に一時的に記録した個人番号付電子申請データは、紙に打ち出し後、速やかに完全消去する。 ・電子記憶媒体に一時的に記録した個人番号付電子申請データは、使用の都度速やかに完全消去する。	事前	
令和6年12月25日	Ⅱ ファイルの概要_本人確認 3. 特定個人情報の入手・使用 ②入手方法	〔〇〕電子記録媒体（フラッシュメモリを除く。）	〔　〕電子記録媒体（フラッシュメモリを除く。）	事前	
令和6年12月25日	Ⅱ ファイルの概要_本人確認 3. 特定個人情報の入手・使用 ⑧使用方法	・住民票の記載事項の変更又は新規作成が生じた場合、既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→市町村CS)、受領した情報を元に本人確認情報ファイルを更新し、当該本人確認情報の更新情報を都道府県知事に通知する（市町村CS→県サーバ）。 （中略） ・4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報ファイルの検索を行う。	・住民票の記載事項の変更又は新規作成が生じた場合、既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→市町村CS)、受領した情報を元に本人確認情報ファイルを更新し、当該本人確認情報の更新情報を都道府県知事に通知する（市町村CS→都道府県サーバ）。 （中略） ・住民票コード、個人番号又は4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報ファイルの検索を行う。	事前	
令和6年12月25日	Ⅱ ファイルの概要_送付先 2. 基本情報 ④記録される項目 主な記録項目 その他	交付申請書等の送付先の情報	個人番号通知書及び交付申請書の送付先の情報	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月25日	Ⅱ ファイルの概要_送付先 2. 基本情報 ④記録される項目 主な記録項目 その妥当性	・その他（交付申請書等の送付先の情報	・その他（個人番号通知書及び交付申請書の送付先の情報）	事前	
令和6年12月25日	（別添2）ファイル記録項目_住基台帳	資料の差し替え	資料の差し替え	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 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 対象者以外の情報の入手を防止するための措置	既存住基システムへの情報の登録の際に、入力した者とは別の者が入力内容を確認し、対象者以外の情報登録を防止する。	既存住基システムへの情報の登録の際に、仮登録と決裁を異なる者で実施することで、対象者以外の情報登録を防止する。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 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 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	システムへの登録時は、入力者以外の者が入力状況を確認し、必要な情報以外の登録を防止する。	システムへの登録時は、仮登録と決裁を異なる者で実施することで、必要な情報以外の登録を防止する。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 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3 特定個人情報の正確性確保の措置の内容	既存住基システムへの情報の登録の際に、入力した者とは別の者が入力内容を確認する。	既存住基システムへの情報の登録の際に、仮登録と決裁を異なる者で実施することで、入力内容を確認する。 ＜サービス検索・電子申請機能における措置＞ ・個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。	事前	
令和6年12月25日	Ⅲ−リスク対策（プロセス）_ 住基台帳 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4−リスクに対する措置の内容	（右記を追加）	・LGWANと本市のネットワークの間に DMZ を設け、共通基盤から外部への直接通信を遮断することにより、安全を確保している。また、FW や連携サーバで外部接続先との通信を制限している。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 3. 特定個人情報の使用 リスク2 アクセス権限の発効・執行の管理 __具体的な管理方法	1. 発効管理 ・人事異動等により、ユーザIDの登録が必要な場合、情報システム利用管理者（業務担当課（各区市民課等）所属長）は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、職員のアクセス権を職務内容に沿ったものであるか確認した上で登録する。 2. 失効管理 ・人事異動等により、ユーザーIDの削除が必要な場合、情報システム利用管理者は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、ユーザID申請書に基づき、ユーザIDの削除を行う。	1. 発効管理 ・人事異動等により、ユーザIDの登録が必要な場合、情報システム利用管理者（業務担当課（各区市民課等）所属長）は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、職員のアクセス権を職務内容に沿ったものであるか確認した上で既存住基システム運用保守委託事業者に登録を依頼する。 2. 失効管理 ・人事異動等により、ユーザーIDの削除が必要な場合、情報システム利用管理者は、速やかに当該職員について、ユーザID申請書を情報システム業務管理者（システム管理主管課(区政課)長）に提出し、承認を得る。 ・情報システム業務管理者は、既存住基システム運用保守委託事業者にユーザIDの削除を依頼する。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月25日	Ⅲ-リスク対策（プロセス）_ 住基台帳 3. 特定個人情報の使用-リスク3 -リスクに対する措置の内容	（右記を追加）	・機能ごとにアクセスできる端末の制限を行っている。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 4. 特定個人情報ファイルの取り扱いの委託 委託契約書中の特定個人情報ファイルの取り扱いに関する規定 規定の内容	秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。	秘密保持、収集の制限、従事者の監督、目的外の利用及び提供の制限、再委託の禁止、適正管理、作業場所以外での業務の禁止等、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 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。） リスク1 特定個人情報の提供・移転に関するルール ルールの内容及びルール遵守の確認方法	＜共通基盤における措置＞ 1. ルールの内容 ：特定個人情報を提供・移転する場合には、情報を保有している事務と情報を必要としている事務との間で事前に協議を行った上で、共通基盤担当に申請書を提出する手順となっている。申請書が提出されない場合、共通基盤を利用した提供・移転はできない。 ：磁気ディスク、USBメモリ等の可搬記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤の運用管理機能で制御されている。可搬記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、共通基盤担当へ申請する手順としている。また、利用できる可搬記録媒体は、本市情報政策部が調達したもので、記録された情報を暗号化する機能を有するものに限定している。 2. ルール遵守の確認方法 ：申請書及び共通基盤の設定の突き合わせを行い、申請書に記載された連携仕様通りの庁内連携が行われているかどうか、申請書に記載された通りの可搬記録媒体使用許可の制御が行われているかどうか確認する。 ：共通基盤により、業務システム端末の運用状況を監視しており、許可されていない可搬記録媒体が接続された場合には、監視画面に警告が表示されるとともに、当該端末、ユーザ等を記録した稼働記録（ログ）が取得・保存される。	＜共通基盤における措置＞ ・ルールの内容 ・共通基盤を利用して別の事務で使用しているシステムに特定個人情報を提供・移転する場合には、情報を保有している事務と情報を必要としている事務との間で事前に協議を行った上で、共通基盤担当に申請書を提出する手順となっている。申請書が提出されない場合、共通基盤を利用した提供・移転はできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤の運用管理機能で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、共通基盤担当へ申請する手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ・ルール遵守の確認方法 ・申請書及び共通基盤の設定の突き合わせを行い、申請書に記載された連携仕様どおりの庁内連携が行われているかどうか、申請書に記載されたとおりの電子記録媒体使用許可の制御が行われているかどうか確認する。 ・共通基盤により、業務システム端末の運用状況を監視しており、許可されていない電子記録媒体が接続された場合には、監視場面に警告が表示されるとともに、当該端末、ユーザ等を記録した操作記録（ログ）が取得・保存される。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	（右記を追加）	・特定個人情報を取り扱う事務室等については、部外者の進入を禁止している。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを中間サーバー用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。 ②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＞ ①中間サーバー・プラットフォームを中間サーバー用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。 ②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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 住基台帳 7. 特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な対策の内容	（右記を追加）	・LGWANと本市のネットワークの間に DMZ を設け、共通基盤から外部への直接通信を遮断することにより、安全を確保している。また、境界 FW や連携サーバで外部接続先との通信を制限している。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_本人確認 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・個人情報の適正な管理について契約書に規定し、適正な個人情報の取扱いに係る誓約書を委託先から提出させる。	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・職員以外の従業者（委託先等）には、当該事項についての誓約書の提出を求める。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_本人確認 3. 特定個人情報の使用 リスク4 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	（右記を追加）	・大量のデータ出力に際しては、事前に管理責任者の承認を得る。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_ 本人確認 4. 特定個人情報ファイルの取り扱いの委託 委託契約書中の特定個人情報ファイルの取り扱いに関する規定 規定の内容	秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。	秘密保持、収集の制限、従事者の監督、目的外の利用及び提供の制限、再委託の禁止、適正管理、作業場所以外での業務の禁止等、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_本人確認 3. 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。） リスク1 その他の措置の内容	・特定個人情報は本市のデータセンター内に設置したサーバーのデータベース内に保管されており、許可を得た者のみが入退室を認められている。 ・本特定個人情報ファイルを扱うシステムへのアクセス権限を有する者を厳格に管理し、情報の持ち出しを制限する。 ・媒体を用いて情報を連携する場合には、原則として媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 媒体を用いて情報を連携する場合には、原則として媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_本人確認 3. 特定個人情報の使用 リスク2 リスクに対する措置の内容 特定個人情報の使用の記録 具体的な方法	バックアップされた操作履歴について、保管庫に施錠保管する。	バックアップされた操作履歴（の記録）を保管庫に施錠保管する。	事前	
令和6年12月25日	Ⅲ リスク対策（プロセス）_送付先情報 3. 特定個人情報の使用 リスク2 リスクに対する措置の内容 特定個人情報の使用の記録 具体的な方法	バックアップされた操作履歴について、保管庫に施錠保管する。	バックアップされた操作履歴（の記録）を保管庫に施錠保管する。	事前	