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	
(2)本人確認情報ファイル	
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	本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に、届出、申請等の窓口において、その内容及び身分証明書等による本人確認を厳格に行い、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	・平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上(氏名と住所の組合わせ、氏名と生年月日の組合わせ)の指定を必須とする。
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　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	本人確認情報の入手元を既存住基システムに限定する。
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	窓口において、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。
個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、本人確認を行う。 ・出生等により新たに個人番号が指定される場合や、転入の際に個人番号カード（若しくは通知カードと法令により定められた身分証明書の組み合わせ）の提示がない場合には、市町村CSにおいて本人確認情報と個人番号の対応付けの確認を行う。
特定個人情報の正確性確保の措置の内容	・本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、必ず入力、削除及び訂正した内容を確認する。 ・入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理し、保管する。 ・本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。
その他の措置の内容	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、住基ネット情報資産管理規程に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。
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	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、市町村CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
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、事務に必要のない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	市町村CSと宛名管理システム間の接続は行わない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。 なお、市町村CSのサーバ上には住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（物理的なアクセス制限、MACアドレスによるフィルタリング等）を講じる。	
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：　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	生体認証による操作者認証を行う。	
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	・拠点管理権限操作者（各区市民課長等）が操作者に対し、操作権限と事務の一覧表に基づき、事務に必要な権限（操作者ID）のみを付与している。 ・権限を有していた職員の異動や退職の際は、対象職員を各課の拠点管理権限操作者（各区市民課長等）が確認の上でシステムの利用権限を失効させる。	
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	・アクセス権限の管理については、操作者IDの管理簿を作成し管理するとともに、適宜、システムの照会機能を使用して、操作権限の履歴及び状況により確認している。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーションの操作履歴の記録を取得し、保管する。	
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	・本人確認情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・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。	
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	・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。	
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	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。 また、バックアップ以外にファイルを複製しないよう、職員・委託先等に対し指導する。
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
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	
その他、特定個人情報の使用にあたり、以下の措置を講じる。 ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない ・統合端末のディスプレイを、来庁者から見えない位置に置く ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめる ・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。	
４．特定個人情報ファイルの取扱いの委託　[　]委託しない	
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク	
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、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。
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法	・作業者を限定するために、委託作業者の名簿を提出させている。 ・委託業務の範囲を明確にした上で閲覧及び更新の権限を持つ者を必要最小限とし、アカウント管理を行っている。 ・閲覧及び更新の履歴（ログ）を取得し、不正な使用がないことを確認している。
特定個人情報ファイルの取扱いの記録	[　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	契約書に基づき、委託業務の実施状況を適時確認するとともに、その記録を残す。 また、委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。
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	・契約書において、個人情報の取扱いを第三者に行わせる場合は、本市の承諾を必要としており、委託先の申請に基づき、再委託の必要性、再委託先の情報管理体制を確認した上で、再委託を承諾している。 ・個人情報を取扱う作業場所は、市が指定する場所のみとしている。 ・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。
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、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。
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	1．ルールの内容 ：委託契約書別記「個人情報取扱特記事項」において、委託先は、個人情報が記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。 ：ハードディスク等の記録装置に保存された特定個人情報については、記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。 ：廃棄を行う場合には、日時、担当者及び処理内容を記録し、保管する。 2．ルール遵守の確認方法 ：委託契約書別記「個人情報取扱特記事項」の定めにより、本市は委託先に対し、立入検査の実施を求めることができる。 ：記録装置に保存された特定個人情報の消去については、本市に対し、作業完了報告を実施させることとしている。
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	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。

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		[再委託していない] ＜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	－
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	特定個人情報（個人番号、4情報等）の提供・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、7年分保存する。 なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。
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	・番号利用法第19条第6号及び住基法第30条の6第1項の規定に該当するか確認のうえ提供する。 ・提供された情報を記録し、定期的にその情報や操作履歴を確認することで、特定個人情報の不正な提供を防止する。
その他の措置の内容		「サーバー室等への入室権限」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。
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		相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。
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： 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		・誤った情報を提供・移転してしまうリスクへの措置 システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。 また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施するため、認証できない相手先への情報の提供なされないことがシステム上担保される。
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

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		
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
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		
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
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		
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
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		
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
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		
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
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		
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
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		
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
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		

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	・サーバー室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・サーバー室は常時施錠し、入退室を行う場合には、入退室管理者から事前に許可を受けたうえで鍵を貸与された者のみが入退室を行うことができる。 ・入退室管理を徹底するため出入口の場所を限定する。	
⑥技術的対策	[　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	・不正プログラム対策 コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度）に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールを導入する。	
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	生存する個人の個人番号とともに、死亡による消除後、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）保管する。	
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　2）十分である 3）課題が残されている

リスク２：　特定個人情報が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	既存住基システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。
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	・システム上、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）を経過した住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報を消去する仕組みとする。 ・磁気ディスクの廃棄時は、情報資産管理手順に基づき、内容の消去、破壊等を行うとともに、情報資産管理台帳にその記録を残す。 また、専用ソフトによるフォーマット、物理的粉砕等を行うことにより、内容を読み出すことができないようにする。 ・情報資産管理手順に基づき、帳票資産取扱記録簿を作成し、受渡し、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。 ・帳票の廃棄時は、裁断、溶解等を行うとともに、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	
－	