Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名

⑵　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:　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	1　対象者以外の情報の入手を防止するための措置(データ入力時) ・　本人確認情報の入手(新規・更新データ)は既存住基システムに限定しているため、既存住基システムへの本人確認情報の登録・更新の際に、窓口において届出・申請の内容及び届出・申請人の本人確認(身分証明書等)を厳格に行い、対象者以外の情報の入手の防止に努めている。 2　必要な情報以外を入手することを防止するための措置(データ検索時) ・　平成14年6月10日総務省告示第334号等により、市町村CSから入手できる本人確認情報を転入通知・確定情報、住民票の写しの交付の特例に関する情報、転入・転出の特例に関する情報、住民基本台帳カードの運用状況、戸籍の附表記載事項通知情報等に限定して入手することをシステム上で担保している。 ・　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、性別を除く2情報以上(氏名と住所、氏名と生年月日との組合せ)の指定を必須としている。
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

1　手順書に定めるリスク対策
・　座間市情報セキュリティポリシーに基づき、住民基本台帳ネットワークの「情報セキュリティ実施手順書」を定めている。「人的セキュリティ」として、情報資産の目的外使用の禁止、CS等関連機器の情報システム管理者が指名した者以外の操作を禁止している。
　また、「技術的セキュリティ」としては、CSへのアクセスログを取得すること、アクセスが許可された職員へ操作権限と利用者IDを付与する。
2　住民基本台帳ネットワークシステムのセキュリティに関する要綱(以下「セキュリティ要綱」という。)に定めるリスク対策
・　アクセス管理者を定め不正アクセス防止のためにユーザID、パスワードの登録・管理、生体認証の登録及びアクセスログの管理等を行っている。

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

リスクに対する措置の内容	1　他のシステムとの接続に係るリスク対策 ・　CSは既存住基システム、住基ネット以外のシステムとは接続していない。したがって、他の庁内システムからCSへのアクセスはできないこととなる。また、既存住基システムとCS間では、法令に基づく事務で使用する以外の情報とのひも付けは行わない。 2　システム運用・管理に係るリスク対策 ・　CSのサーバ上には住基ネッの管理及び運用に必要なソフトウエア以外作動せず、また、CSが設置されたセグメントにあるハブ等の周辺機器は盗難、破壊等から保護すること、権限のない者が機器を接続できないように、重要機械室等の鍵等で入退室管理された部屋に設置する。 3　セキュリティ要綱に定めるリスク対策 ・　アクセス管理者はパソコン等管理台帳を作成し、搭載が許可されたソフトウエア以外のものが搭載されていないこと、また、アクセス対象機器その他のネットワークに接続されている機器について、ネットワーク構成図と一致していることを適時確認する。
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。
		1　手順書に定めるリスク対策

その他の措置の内容	・ 重要な入出力帳票は盗難、漏えい、き損及び滅失防止のため、入退出管理がされ防火設備が設置された部屋に保管する。 ・ 入出力帳票及び特定個人情報を含む記録媒体は、物理的破壊等の記載・記録内容の漏えいを防止する措置を講じた上で廃棄する。 ・ 情報システム管理者の許可なく、パソコン等の端末のセキュリティ機能の変更、ソフトウエアのインストール又は機器の増設、変更をしてはならない。 ・ 担当職員の技能の向上とセキュリティポリシーの遵守を図るための研修を年1回以上行う。 また、システムの変更等により必要と認められる時に、担当職員に対して随時に研修を行う。 ・ 異動又は退職した担当職員のパスワードは速やかに消除し、システムを利用できないようにする。 2 セキュリティ要綱に定めるリスク対策 ・ 事務室、耐火書庫への入退出は、入退出管理者の許可を受ける。また、重要機械室への入退出は、指紋認証による登録を受ける。
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当たり、以下の措置を講じる。
・ スクリーンセーバーを利用して、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とともに、覗き見を防止するプライバシーフィルターを付ける。
・ 本人確認情報が表示された画面のハードコピーをするときは、帳票類等管理簿に記録するとともに情報資産管理者の承認を得る。
・ 大量データの出力に際しては、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

リスク: 委託先における不正な使用等のリスク

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	・ 法令等の遵守 ・ 秘密等の保持 ・ 個人情報の取扱い ・ 再委託の禁止(委託者が承諾した場合を除く) ・ 目的外使用、第三者への提供の禁止 ・ 複写、複製の禁止(委託者の承諾した場合を除く) ・ 個人情報の安全な保管 ・ 委託者から引き渡された原票の返還義務 ・ 事故報告義務 ・ 委託者の勧告、調査権限
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担保		[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 4）再委託していない
	具体的な方法	委託業務の全部又は一部を他に委託し又は請け負わせる場合は、書面により委託者の承諾を受ける。
その他の措置の内容		「住民基本台帳ネットワークシステムの受託者の調査に関する要領」を策定し、受託しようとする事業者のセキュリティ等に関する調査を行っている。
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

1 情報保護管理体制の確認
・ セキュリティ管理者は、外部委託をしようとする場合は、委託業者のセキュリティポリシーに関する管理体制を調査するとともに、委託業務の内容、委託の理由及び委託予定業者のセキュリティポリシーに関する事項(個人情報保護に関する関連法令の遵守状況、セキュリティに関する認識及び体制、情報資産の安全性及び機密性に対する認識及び体制、不足の事態の発生に対する対応)等について、セキュリティ会議の審議を経てセキュリティ統括責任者の承認を得なければならない。
2 特定個人情報ファイルの閲覧者・更新者の制限
・ 委託業者は、委託業務現場主任者等届出書を提出する。
・ 開発・保守等委託業者の使用するユーザID及びパスワードは、構築(開発)、保守終了後に不要となった時点で速やかに削除する。
・ 記録媒体が含まれる機器の修理等は原則庁舎内で行う。
・ 委託業者が作業などを行う場合は、担当職員が立ち合う。
3 特定個人情報ファイルの取扱いの記録
・ 委託業者は、委託業務に着手したときは委託業務着手届を、業務が完了したときは委託業務完了届を提出する。
・ 委託業者は、作業報告書を提出する。

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
リスク：　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	個人情報を取り扱う部署は、保護条例第8条の規定により、個人情報を取り扱う目的、収集の方法、記録の内容、利用提供の範囲等を定めた登録簿を備えることとし、新たに個人情報を取り扱う場合又は登録内容を変更する場合は、個人情報保護審査会へ報告することとなる。この登録簿は、一般の閲覧に供されている。 また、保護条例には、個人情報の不正取得・提供等に対して罰則規定が設けられている。
その他の措置の内容	・「重要機械室への入室権限」（入退出管理）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」（アクセス制御）を有する者を厳格に管理する。 ・ 本人確認情報が記録・記載された記録媒体又は帳票類を重要機械室又は事務室以外への持ち出すときは、帳票類等管理簿に記録するとともに情報資産管理者の承諾を得る。 ・ 外部記録媒体の利用に関しては、システム上個人情報を媒体渡しとなっている業務に限り許可する。
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	
1　不適切な方法及び誤った相手に提供が行われるリスク対策 ・ 特定個人情報の提供において、相手方(県サーバ)と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されないことがシステム上担保される。 ・ 特定個人情報は、電子メール等で送信してはならない。 2　誤った情報を提供・移転することへのリスク措置 ・ システム上、紹介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。 ・ 本人確認情報に変更が生じた際には、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。 3　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(個人番号カード管理システム)とCSの間の通信では相互認証を実施するため、認証できない相手方への情報の提供はされないこと がシステム上担保される。	

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）
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：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	
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：　特定個人情報の漏えい・滅失・毀損リスク	
①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

周知	3）十分に行っていない
②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	
その他の措置の内容	データバックアップを毎日実施し、バックアップデータは外部に保管・施錠している。
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

情報システムに障害又は侵害、情報資産の漏えい等(以下「不正行為」という。)が発生した場合における連絡、証拠保全、被害拡大の防止等に必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるための緊急時対応計画書等を定め、実行する。

1　情報セキュリティ緊急時対応計画書によるリスク対策
- システム、セキュリティ等に関する管理者を定める管理体制の整備
- 不正行為の分類と脅威度の判定及び脅威度に基づく対応を規定
- 緊急連絡網の整備

2　情報セキュリティ障害対応手順書によるリスク対策
- システム障害、不正アクセス、情報漏えいへの対応手順としてインシデントの分類、事象確認、初期対応、復旧作業、復旧後の措置を規定
- 障害時の緊急連絡網を整備

8. 監査

実施の有無	[○] 自己点検　[　] 内部監査　[○] 外部監査

9. 従業者に対する教育・啓発

従業者に対する教育・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
具体的な方法	1　定期研修 ・　新しく配属になった職員の技能の取得及び担当職員（フルタイム・パートタイム会計年度任用職員を含む。）の技能向上とセキュリティポリシーの遵守を図るために、定期研修を行う。 2　随時研修 ・　システムの変更、法改正等により必要と認められる時に、随時研修を行う。 3　緊急時対応訓練 ・「緊急時対応訓練実施要項」を定め、不正アクセス情報漏えい等について障害が発生した場合を想定し、連絡体制及び復旧手続に基づき、緊急時の対応訓練を実施する。

10. その他のリスク対策

1　物理的セキュリティ対策
- サーバ等の重要機器は、重要機械室に設置する。
- システムで使用する電源は無停電電源装置とし、サーバ等の機器は予備電源を備える。
- システムで使用する配線は床下又は天井での配線とする。
- サーバはRAID構成とし、現用機(メインサーバ)に障害が発生した場合は速やかに交替機(セカンダリーサーバ)に移行できる機器構成とする。

2　技術的セキュリティ対策及び運用管理
- データファイルは日々異動情報のバックアップを取得し、月1回フルバックアップを取得する。
- システム改修等において必要と認められる時は、データ及びシステムのバックアップデータを作成する。

3　コンピュータウイルス対策
- 機構が配信するウイルス対策ソフトを適用する。
- 端末がウイルスに感染したと思われる現象を発見したときは、ネットワークから速やかに切り離す等適切な措置を講じる。

Ⅲ　リスク対策　※（7. ②を除く。）

1. 特定個人情報ファイル名

⑶　送付先情報ファイル

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:　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	1　対象者以外の情報の入手を防止するための措置(データ入力時) ・　本人確認情報の入手(新規・更新データ)は既存住基システムに限定しているため、既存住基システムへの本人確認情報の登録・更新の際に、窓口において届出・申請の内容及び届出・申請人の本人確認(身分証明書等)を厳格に行い、対象者以外の情報の入手の防止に努めている。 2　必要な情報以外を入手することを防止するための措置(データ検索時) ・　務省告示第334号等により、市町村CSから入手できる本人確認情報を転入通知・確定情報、住民票の写しの交付の特例に関する情報、転入・転出の特例に関する情報、住民基本台帳カードの運用状況、戸籍の附表記載事項通知情報等に限定して入手することをシステム上で担保している。 ・　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、本人確認情報際の検索条件として、性別を除く2情報以上(氏名と住所、氏名と生年月日との組合せ)の指定を必須としている。
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

1　手順書に定めるリスク対策
・　座間市情報セキュリティポリシーに基づき、住民基本台帳ネットワークの手順書を定めている。「人的セキュリティ」として、情報資産
　の目的外使用の禁止、CS等関連機器の情報システム管理者が指名した者以外の操作を禁止している。また、「技術的セキュリティ」
　としては、CSへのアクセスログを取得すること、アクセスが許可された職員へ操作権限と利用者IDを付与する。
2　住民基本台帳ネットワークシステムのセキュリティ要綱に定めるリスク対策
・　アクセス管理者を定め不正アクセス防止のためにユーザID、パスワードの登録・管理、生体認証の登録及びアクセスログの管理

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

リスクに対する措置の内容	1　他のシステムとの接続に係るリスク対策 ・　CSは既存住基システム、住民基本台帳ネットワークシステム以外のシステムとは接続していない。したがって、他の庁内システムからCSへのアクセスはできないこととなる。また、既存住基システムとCS間では、法令に基づく事務で使用する以外の情報とのひも付けは行わない。 2　システム運用・管理に係るリスク対策 ・　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エア以外作動せず、また、CSが設置されたセグメントにあるハブ等の周辺機器は盗難、破壊等から保護すること、権限のない者が機器を接続できないように、重要機械室等の鍵等で入退室管理された部屋に設置する。 3　セキュリティ要綱に定めるリスク対策 ・　アクセス管理者はパソコン等管理台帳を作成し、搭載が許可されたソフトウエア以外のものが搭載されていないこと、また、アクセス対象機器その他のネットワークに接続されている機器について、ネットワーク構成図と一致していることを適時確認する。
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。
		1　手順書に定めるリスク対策

その他の措置の内容	・ 重要な入出力帳票は盗難、漏えい、き損及び滅失防止のため、入退出管理がされ防火設備が 設置された部屋に保管する。 ・ 入出力帳票及び特定個人情報を含む記録媒体は、物理的破壊等の記載・記録内容の漏えいを防止する措置を講じた上で廃棄する。 ・ 情報システム管理者の許可なく、パソコン等の端末のセキュリティ機能の変更、ソフトウエアのインストール又は機器の増設、変更をしてはならない。 ・ 担当職員の技能の向上とセキュリティポリシーの遵守を図るための研修を年1回以上行う。また、システムの変更等により必要と認められる時に、担当職員に対して随時に研修を行う。 ・ 異動又は退職した担当職員のパスワードは速やかに消除し、システムを利用できないようにする。 2 セキュリティ要綱に定めるリスク対策 ・ 事務室、耐火書庫への入退出は、入退出管理者の許可を受ける。また、重要機械室への入退出は、指紋認証による登録を受ける。
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当たり、以下の措置を講じる。
・ スクリーンセーバーを利用して、長時間にわたり本人確認情報を表示させない。
・ CS端末のディスプレイを、来庁者から見えない位置に置くとともに、覗き見を防止するプライバシーフィルターを付ける。
・ 本人確認情報が表示された画面のハードコピーをするときは、帳票類等管理簿に記録するとともに情報資産管理者の承認を得る。
・ 大量データの出力に際しては、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

リスク: 委託先における不正な使用等のリスク

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	・ 法令等の遵守 ・ 秘密等の保持 ・ 個人情報の取扱い ・ 再委託の禁止(委託者が承諾した場合を除く) ・ 目的外使用、第三者への提供の禁止 ・ 複写、複製の禁止(委託者の承諾した場合を除く) ・ 個人情報の安全な保管 ・ 委託者から引き渡された原票の返還義務 ・ 事故報告義務 ・ 委託者の勧告、調査権限
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担保		[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 4）再委託していない
	具体的な方法	委託業務の全部又は一部を他に委託し又は請け負わせる場合は、書面により委託者の承諾を受ける。
その他の措置の内容		「住民基本台帳ネットワークシステムの受託者の調査に関する要領」を策定し、受託しようとする事業者のセキュリティ等に関する調査を行っている。
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

1 情報保護管理体制の確認
・ セキュリティ管理者は、外部委託をしようとする場合は、委託業者のセキュリティポリシーに関する管理体制を調査するとともに、委
託業務の内容、委託の理由及び委託予定業者のセキュリティポリシーに関する事項(個人情報保護に関する関連法令の遵守状況、セキュリティに関する認識及び体制、情報資産の安全性及び機密性に対する認識及び体制、不足の事態の発生に対する対応)等について、セキュリティ会議の審議を経てセキュリティ統括責任者の承認を得なければならない。
2 特定個人情報ファイルの閲覧者・更新者の制限
・ 委託業者は、委託業務現場主任者等届出書を提出する。
・ 開発・保守等委託業者の使用するユーザID及びパスワードは、構築(開発)、保守終了後に不要となった時点で速やかに削除する。
・ 記録媒体が含まれる機器の修理等は原則庁舎内で行う。
・ 委託事業者が作業などを行う場合は、担当職員が立ち合う。
3 特定個人情報ファイルの取扱いの記録
・ 委託業者は、委託業務に着手したときは委託業務着手届を、業務が完了したときは委託業務完了届を提出する。
・ 委託事業者は、作業報告書を提出する。

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

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： 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	個人情報を取り扱う部署は、保護条例第8条の規定により、個人情報を取り扱う目的、収集の方法、記録の内容、利用提供の範囲等を定めた登録簿を備えることとし、新たに個人情報を取り扱う場合又は登録内容を変更する場合は、個人情報保護審査会へ報告することとなる。この登録簿は、一般の閲覧に供されている。 また、保護条例には、個人情報の不正取得・提供等に対して罰則規定が設けられている。	
その他の措置の内容	・「重要機械室への入室権限」(入退出管理)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」(アクセス制御)を有する者を厳格に管理する。 ・ 本人確認情報が記録・記載された記録媒体又は帳票類を重要機械室又は事務室以外への持ち出すときは、帳票類等管理簿に記録するとともに情報資産管理者の承諾を得る。 ・ 外部記録媒体の利用に関しては、システム上個人情報を媒体渡しとなっている業務に限り許可する。	
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		
1 不適切な方法で提供・移転が行われるリスクへの措置 ・ 相手方(個人番号カード管理システム)と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。 2 誤った情報を提供・移転してしまうリスクへの対応 ・ システム上、住基システムから入手した情報の内容に編集を加えず、適切に個人番号カード管理システムに提供することを担保する。 3 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(個人番号カード管理システム)と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移転はなされないことがシステム上担保される。		
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）	
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： 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
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： 特定個人情報の漏えい・滅失・毀損リスク		
①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
②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	[発生なし]	＜選択肢＞ 1）発生あり 2）発生なし

に関する重大事故が発生したか		
	その内容	
	再発防止策の内容	
その他の措置の内容		データバックアップを毎日実施し、バックアップデータは外部に保管・施錠している。
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

1 特定個人情報が古い情報のまま保管されるリスクへの措置
・ 本特定個人情報ファイル(送付先情報ファイル)は、送付先情報の連携を行う必要が生じた都度作成・連携することとしており、システム上で連携後速やかに(1営業日後)に削除する仕組みとする。
また、媒体を用いて連携する場合、当該媒体は連携後に連携先である機構において適正に管理され、市では保管しない。
2 特定個人情報が消去されずいつまでも存在するリスクへの対応
・ システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。

8. 監査

実施の有無	[○] 自己点検 [○] 内部監査 [○] 外部監査

9. 従業者に対する教育・啓発

従業者に対する教育・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
	具体的な方法	1 定期研修 ・ 新しく配属になった職員の技能の取得及び担当職員(フルタイム・パートタイム会計年度任用職員を含む。)の技能向上とセキュリティポリシーの遵守を図るために、定期研修を行う。 2 随時研修 ・ システムの変更、法改正等により必要と認められる時に、随時研修を行う。 3 緊急時対応訓練 ・「緊急時対応訓練実施要項」を定め、不正アクセス情報漏えい等について障害が発生した場合を想定し、連絡体制及び復旧手続に基づき、緊急時の対応訓練を原則年1回実施する。

10. その他のリスク対策

1 物理的セキュリティ対策
・ サーバ等の重要機器は、重要機械室に設置する。
・ システムで使用する電源は無停電電源装置とし、サーバ等の機器は予備電源を備える。
・ システムで使用する配線は床下又は天井での配線とする。
・ サーバはRAID構成とし、現用機(メインサーバ)に障害が発生した場合は速やかに交替機(セカンダリーサーバ)に移行できる機器構成とする。
2 技術的セキュリティ対策及び運用管理
・ データファイルは日々異動情報のバックアップを取得し、月1回フルバックアップを取得する。
・ システム改修等において必要と認められる時は、データ及びシステムのバックアップデータを作成する。
3 コンピュータウイルス対策
・ 機構が配信するウイルス対策ソフトを適用する。
・ 端末がウイルスに感染したと思われる現象を発見したときは、ネットワークから速やかに切り離す等適切な措置を講じる。