

「住民基本台帳に関する事務に関する特定個人情報保護評価書記載要領(案)」 に関する内容の適合性・妥当性

市町村(特別区を含む。以下同じ。)の「住民基本台帳に関する事務」に係る特定個人情報保護評価書の作成を支援することを目的として、地方公共団体情報システム機構(J-LIS)が、特定個人情報保護委員会の了承を得た上で、住民基本台帳ネットワークシステムに関連する項目の記載要領を示すもの。

■ 白地項目(赤字記載)

市町村CSの仕様等に係るもので、本記載要領の回答を各市町村がそのまま評価書へ転記できる項目。

■ 橙色で網掛けした項目(記載あり)

(赤字記載) 市町村CSの仕様等に係るもので、本記載要領の回答を各市町村がそのまま評価書へ転記できる項目。

(赤字記載以外)市町村CS、既存住民基本台帳システム等について、記載例や参考情報を示している項目であり、本記載要領の内容を各市町村の実情に合わせて適宜修正・追加の上、評価書に記載すべき項目。

■ 橙色で網掛けした項目(記載なし)

各市町村が実情に合わせて回答を作成し、評価書に記載すべき項目。

※委員会です承するのは赤字部分(全項目評価書の赤字部分は、基礎項目評価書、重点項目評価書の赤字部分の内容を含んだ記載となっているため、下記には全項目評価書の記載内容を示している。)

※送付先情報ファイルのリスク対策については、記載例を示さない設問は本人確認情報ファイルにおける設問への回答と同様の対策内容を選択・記載するようにされている。

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
○適切な時期に実施しているか。	—	—	問題は認められない	・多くの市町村における既存住基システムの改修が行われる前に、市町村CSの仕様等に係る記載要領を示すことが可能な時期である。
○適切な実施主体が実施しているか。	○特定個人情報ファイルを保有する者以外に特定個人情報ファイルに関わる者が特定個人情報保護評価が適切に実施されるよう協力する内容となっているか。	—	問題は認められない	・住民基本台帳に関する事務において、本人確認情報ファイル、送付先情報ファイルといった特定個人情報ファイルを保有するのは市町村長であるので、市町村長が評価実施主体となることは指針に適合している。 ・市町村CSのリスク対策等、住民基本台帳に関する事務の評価をする上で記載が必要になるものの、開発者であるJ-LISにしか知り得ない情報について情報提供していることは、指針第3の2「特定個人情報ファイルを保有しようとする者又は保有する者以外に特定個人情報ファイルに関わる者が存在する場合は、その者は、特定個人情報保護評価が適切に実施されるよう協力するものとする。」に適合している。

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
<p>○特定個人情報保護評価の対象となる事務の実態に基づき、特定個人情報保護評価書様式で求められる全ての項目について検討し、記載しているか。</p>	<p>○特定個人情報保護評価が適切に実施されるよう評価実施機関に協力する者として、特定個人情報保護評価の対象となる事務の実態に基づき、情報提供すべき内容について検討し、記載しているか。</p>	—	問題は認められない	<p>・地方公共団体情報システム機構が開発する市町村CSの仕様等に係る内容について、市町村が転記しやすいよう赤字で明記しており、市町村の住民基本台帳に関する事務に係る特定個人情報保護評価の実施への協力として十分なものである。</p>
<p>○特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。</p>	<p>○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の実現する機能の内容は具体的か。当該システムにおける接続について適切に記載しているか。</p>	(P4) 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	問題は認められない	<p>・住民基本台帳ネットワークシステムのうち、市町村CS部分の実現すべき機能について具体的に列挙し、検索機能や情報連携機能等それぞれの機能や処理の概要を分かりやすく記載している。</p> <p>・当該システムと情報をやりとりするシステムは、既存住民基本台帳システムと個人番号カード管理システムのみであることを適切に記載している。</p>
	<p>○特定個人情報ファイルの単位は適切か。また、特定個人情報ファイルを取り扱う理由は妥当であるか。</p>	(P5) I 基本情報 4. 特定個人情報ファイルを取り扱う理由	問題は認められない	<p>・事務の内容に即して、既存住基システムで取り扱う特定個人情報ファイルの単位を(1)住民基本台帳ファイルとし、市町村CSで取り扱う特定個人情報ファイルの単位を(2)本人確認情報ファイル、(3)送付先情報ファイルとして整理しておりファイルの分け方は妥当である。</p> <p>・住民基本台帳に関する事務を実施する上で、当該特定個人情報ファイルを取り扱う必要があることを、具体的な事務の流れに即して記載している。</p>
	<p>○特定個人情報ファイルの使用方法や情報の突合に関して具体的な記載内容になっているか。</p>	(P10) II 特定個人情報ファイルの概要 <本人確認情報ファイル> 3. 特定個人情報の入手・使用 (P15) II 特定個人情報ファイルの概要 <送付先情報ファイル> 3. 特定個人情報の入手・使用	問題は認められない	<p>・本人確認情報ファイル及び送付先情報ファイルが具体的にどのような流れで、どのようなことに使用されるかについて、事務の流れ及びシステム上の情報の流れの双方の観点から分かりやすく記載している。</p> <p>・本人確認情報ファイル及び送付先情報ファイルに記録される情報を他から入手する際にどのような突合を行うか、当該ファイルに記録された情報と他の情報をどのように突合するか、また、これらの突合を何のために行うか具体的に記載している。</p>

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
<p>○特定個人情報ファイルを取り扱うプロセスにおいて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、特定個人情報保護評価の対象となる事務の実態に基づき、特定しているか。</p>	—	<p>(p18) Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策</p>	問題は認められない	<p>・市町村CSの仕様に係るリスク対策は赤字で記載されており、特定個人情報保護評価書の様式に例示されている各リスクに具体的にどのように対応しているかについて記載している。</p>
<p>○特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。</p> <p>○記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。</p>	○特定個人情報の入手	<p>(P18) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 ＜本人確認情報ファイル＞ 2. 特定個人情報の入手</p>	問題は認められない	<p>・目的外の入手が行われるリスク対策として、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の情報が入手されないようシステム上の措置を講じている。また、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情報以上の指定を必須とすることなどの対策について明記している。</p> <p>・不適切な方法で入手が行われるリスク対策として、本人確認情報の入手元を既存住基システムに限定する措置を講じることについて記載している。</p> <p>・入手した特定個人情報が不正確であるリスク対策として、入手した個人番号が本人の個人番号として間違いのないよう市町村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ことにより、個人番号の真正性確認の措置を講じることについて記載している。</p> <p>・入手の際に特定個人情報が漏えい・紛失するリスク対策として、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ついて記載している。</p>
		<p>(P26) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 ＜送付先情報ファイル＞ 2. 特定個人情報の入手</p>	問題は認められない	<p>・入手した特定個人情報が不正確であるリスク対策として、個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応付く個人番号を取得することをシステム上担保することについて記載している。</p> <p>・入手した特定個人情報が不正確であるリスク対策として、既存住基システムにおいて正確性が確保された送付先情報を適切に受信することをシステムにより担保することについて記載している。</p>

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
	○特定個人情報の使用	(P19) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 ＜本人確認情報ファイル＞ 2. 特定個人情報の使用	問題は認められない	<ul style="list-style-type: none"> ・事務に必要なない情報との紐付けが行われるリスク対策として、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こと、また、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ないこと等の対策を講じることについて記載している。 ・権限のない者によって不正に使用されるリスク対策として、特定個人情報にアクセスする際に生体認証等を行うことについて記載している。 ・権限のない者によって不正に使用されるリスク対策として、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・保管し、アクセス権限についてチェックを行うことについて記載している。 ・権限のない者によって不正に使用されるリスク対策や従業者が事務外で使用するリスク対策として、特定個人情報の使用の記録について、アクセスログ・操作ログにより本人確認情報を扱うシステムの操作履歴を記録することについて記載している。 ・特定個人情報ファイルが不正に複製されるリスク対策として、システム上、管理権限を与えられた者以外の者が、情報の複製を行うことができない仕組みについて記載している。
	○特定個人情報の使用	(P26) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 ＜送付先情報ファイル＞ 2. 特定個人情報の使用	問題は認められない	<ul style="list-style-type: none"> ・権限のない者によって不正に使用されるリスク対策として、アクセスログ・操作ログにより本人確認情報を扱うシステムの操作履歴を記録することについて記載している。

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
	○特定個人情報の提供・移転	(P22) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 <本人確認情報ファイル> 2. 特定個人情報の提供・移転	問題は認められない	<ul style="list-style-type: none"> ・不正な提供・移転が行われるリスク対策として、特定個人情報の提供を行う際に、提供日時や操作者等の提供記録をシステム上で管理するなど特定個人情報の提供・移転の記録を行うことについて記載している。 ・誤った特定個人情報を提供・移転するリスク対策として、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すること、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ことについて記載している。 ・誤った相手に特定個人情報を提供・移転するリスク対策として、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移転はなされないことなどをシステム上で担保することについて記載している。
		(P28) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 <送付先情報ファイル> 2. 特定個人情報の提供・移転	問題は認められない	<ul style="list-style-type: none"> ・誤った特定個人情報を提供・移転するリスク対策として、既存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システム上担保することについて記載している。 ・誤った相手に特定個人情報を提供・移転するリスク対策として、個人番号カード管理システムと市町村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移転はなされないことをシステム上担保することについて記載している。
	○特定個人情報の保管・消去	(P24) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 <本人確認情報ファイル> 2. 特定個人情報の保管・消去	問題は認められない	<ul style="list-style-type: none"> ・特定個人情報の漏えい・滅失・毀損に対するリスク対策として、番号法では死者の個人番号についても生存者のそれと同様、安全管理措置義務が課されており、生存者の個人番号と同様の保管方法で保管していることについて記載している。 ・特定個人情報が古い情報のまま保管され続けるリスク対策として、既存住基システムとの整合処理を定期的実施し、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ついて記載している。 ・特定個人情報が消去されずいつまでも存在するリスク対策として、システム上保存期間を経過した本人確認情報を消去する仕組みとしており、保管期間を経過した特定個人情報を消去する手順が定められていることについて記載している。

審査の観点(指針第10(2))	今回特に着目した事項	記載要領の該当箇所	所見	コメント
		(P29) Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 ＜送付先情報ファイル＞ 2. 特定個人情報の保管・消去	問題は認められない	<p>・特定個人情報が古い情報のまま保管され続けるリスク対策として、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、連携後速やか(1営業日後)に削除する仕組みとされているとともに媒体を用いて連携する場合も当該媒体は連携後、連携先である機構において適切に管理され市町村では保管されないことについて記載している。</p> <p>・特定個人情報が消去されずいつまでも存在するリスク対策として、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など保管期間を経過した特定個人情報を消去する手順を定めていることについて記載している。</p>

【総評】

本人確認情報ファイル及び送付先情報ファイルともに、特定個人情報ファイルの内容及び特定個人情報の流れが明確に記載されており、また、市町村CSの仕様等に係る記載項目やリスクの特定及びリスク対策が具体的かつ分かりやすく記載されており、特段の問題は認められないものと考えられる。