資料４

「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等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

都道府県の「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」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）　都道府県サーバの仕様等に係るもので、本記載要領の回答を各都道府県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）　都道府県サーバの仕様等に係るもので、本記載要領の回答を各都道府県がそのまま評価書へ転記できる項目。

（赤字記載以外）都道府県サーバ等について、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都道府県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）　各都道府県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。

※委員会で了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。）

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	・都道府県サーバの改修はＪ－LISが行っており、指針第６の１ウの経過措置の適用により特定個人情報保護評価指針の適用の日から６月を超えない範囲でシステムの開発におけるプログラミングを開始する場合は、プログラミング開始後、特定個人情報ファイルを保有する前に特定個人情報保護評価を実施することができるとされており、都道府県が都道府県サーバにおける特定個人情報保護評価を実施する上で、そ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	・住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務において都道府県知事保存本人確認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都道府県知事であるので、都道府県知事が評価実施主体となることは指針に適合している。 ・都道府県サーバのリスク対策等、住民基本台帳ネットワークに係る本人確認情報の管理及び提供等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
○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。	○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。	―	問題は認められない	・地方公共団体情報システム機構が開発する都道府県サーバの仕様等に係る内容について、都道府県が転記しやすいよう赤字で明記しており、都道府県の「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」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。
○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。	○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。	（P3） 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	・住民基本台帳ネットワークシステムの内の都道府県サーバ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。
	○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。	（P4） 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	・事務の内容に即して、特定個人情報ファイルの単位を都道府県知事保存本人確認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。 ・住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等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。
	○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。	（P7） Ⅱ特定個人情報ファイルの概要 3．特定個人情報の入手・使用	問題は認められない	・都道府県知事保存本人確認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。 ・都道府県知事保存本人確認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、都道府県知事保存本人確認情報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。
○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。	―	（p11） Ⅲ　特定個人情報の取扱いプロセスにおけるリスク対策	問題は認められない	・都道府県サーバの仕様に係るリスク対策に関する記載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。 ○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。	○特定個人情報の入手	（P11） Ⅲ特定個人情報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	問題は認められない	・目的外の入手が行われるリスク対策として、市町村から通知を受けることとされている情報のみを入手することについてシステム上の措置を講じることを明記している。 ・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市町村CSに限定する措置を講じることについて記載している。 ・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ないよう市町村において真正性が確認された情報を市町村CSを通じて入手できることを、システムで担保することにより、個人番号の真正性確認の措置を講じる、また、特定個人情報を入手した後、その情報の正確性を保つためにシステム上、本人確認情報更新の際に、論理チェックを行う仕組みとするとともに入手元である市町村CSにおいて、項目（フォーマット、コード）のチェックを実施することについて記載している。 ・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。
	○特定個人情報の使用	（P12） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 2．特定個人情報の使用	問題は認められない	・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は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検索サブシステム及び業務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、本人確認情報を扱うシステムのアクセスログや操作ログにより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。

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	（P14） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 2．特定個人情報の提供・移転	問題は認められない	・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・移転してしまうリスク対策として、全国サーバと都道府県サーバ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移転はなされないことをシステム上担保していることを記載している。
	○特定個人情報の保管・消去	（P15） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 2．特定個人情報の保管・消去	問題は認められない	・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、都道府県サーバの集約センターにおいて、監視カメラを設置してサーバ設置場所への入退室者を特定し管理する、都道府県サーバの集約センターにおいては、サーバ設置場所、記録媒体の保管場所を施錠管理するなどの物理的対策や都道府県サーバの集約センターにおいて、ファイアウォールを導入し、ログの解析を行うなどの技術的対策を行うことについて記載している。 ・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す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、市町村CS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、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は法令（住基法施行令第30条の6）に定める保存期間を経過した後にシステム的に消去することにより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ることについて記載している。

【総評】

都道府県知事保存本人確認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、都道府県サーバ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と考えられる。