資料3

「中間サーバーに関する特定個人情報保護評価の実施に当たって（案）」に関する内容の適合性・妥当性

中間サーバーのソフトウェアの一括開発を行う総務省が、「中間サーバーに関する特定個人情報保護評価の実施に当たって（案）（以下「記載要領本体」という。）」、「（別紙）特定個人情報保護評価（全項目評価書）（案）（以下「評価書記載例」という。）」及び「システム方式設計書」により、中間サーバーに係る事務の特定個人情報保護評価書を作成する地方公共団体に対し、必要となる情報の提供・支援を行うことを目的として、記載要領本体及び評価書記載例について特定個人情報保護委員会の了承を得た上で、中間サーバーに関連する項目の記載要領を示すもの。

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	・地方公共団体が特定個人情報保護評価を行う際、中間サーバーに関する記載が必要となるが、中間サーバーの仕様等については、当該ソフトウェアを一括開発する総務省が地方公共団体へ必要な情報を提供することとされている。 　各地方公共団体における評価実施時期は、各地方公共団体の各事務において主として使用するシステムの改修時期により判断するため、各地方公共団体の事務ごとに異なるが、今年度中にシステム改修を行う地方公共団体も想定される。今回の情報提供によって、地方公共団体は、中間サーバーの仕様等に係る記載例等を事前に把握し、中間サーバーに関する記載も含め、各事務における評価書を作成することができる。
○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。	（記載要領本体P1） 1．はじめに 2．中間サーバーに係る特定個人情報保護評価の前提 （記載要領本体P4） 3．特定個人情報保護評価計画管理書及び特定個人情報保護評価書に関して （2）個別留意事項	問題は認められない	・中間サーバーにおいて保有される特定個人情報ファイルを保有するのは地方公共団体であるため、地方公共団体が評価実施主体となることは指針に適合している。 ・中間サーバーのリスク対策等、地方公共団体が各事務の評価をする上で記載が必要となるものの、中間サーバーのソフトウェアを一括開発している総務省しか知り得ない情報について情報提供していること、地方公共団体情報システム機構が整備・運用する中間サーバー・プラットフォームを活用する地方公共団体向けに中間サーバー・プラットフォームの仕様等に関する記載例を示していることは、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。	○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	・記載要領本体において、地方公共団体が特定個人情報保護評価書の記載がしやすいよう、評価項目ごとに考え方を示しており、かつ、システム方式設計書の参照すべき部分についても示している。また、リスク対策等については、評価書記載例において、全項目評価書における記載例を示している。 【記載要領本体】 評価書において、中間サーバー・ソフトウェア及び中間サーバー・プラットフォームに係る仕様に関する記載を行う必要がある箇所を示すほか、当該部分について評価書を作成するに当たっての留意事項等を示したもの。各地方公共団体は、「別紙」の記載例と「システム方式設計書」を参照することとなる。 【評価書記載例】 中間サーバーのソフトウェア機能及び中間サーバー・プラットフォームにおける措置について、記載例を示している。各地方公共団体は、記載例を参考に各団体の事情を考慮して記載することとされている。 【システム方式設計書】（中間サーバーの基本要件及びシステム化方式を記載したもの） 設計書中、「ネットワーク構成」「中間サーバーの概要」「機能要件の概要」「符号管理機能」「情報提供機能」等を参照するよう、上記の記載要領本体において指示されている。
	○記載例等を示していない項目について、記載例等を示していないことは評価の趣旨に照らし妥当か。	（評価書記載例） Ⅰ1．3．4．5．6．7．8． Ⅱ1．2．3．4．5．6． Ⅲ1．2．3．4．5．7．	問題は認められない	記載例等を示していない項目とその妥当性については次のとおり。 ・特定個人情報ファイルを取り扱う事務の名称、対象人数、特定個人情報ファイルを取り扱う理由、担当部署等の基本情報の記載例等がないが、これらは各機関における事務の実態に応じて記載すべきであることから、記載例等を示していなくても問題は認められないと考えられる。 ・特定個人情報ファイルの取扱いの委託についての記載例等がないが、中間サーバー・プラットフォームの保守・運用業者は特定個人情報ファイルにアクセスできず、特定個人情報ファイルを取り扱うことはないため、記載例等を示していなくても問題は認められないと考えられる。 ・情報提供ネットワークシステムを通じた入手又は提供を除いた特定個人情報の入手・使用・提供・移転についての記載例等がないが、中間サーバーで情報提供ネットワークシステムを通じた入手又は提供を除いた特定個人情報の入手・使用・提供・移転を行うことはないため、記載例等を示していなくても問題は認められないと考えられる。 ・特定個人情報の保管期間や、特定個人情報が古い情報のまま保管され続けるリスクについての記載例等がないが、中間サーバーは自動削除等の機能はなく、保管期間等は各機関で適切に記載すべき事項であることから、記載例等を示していなくても問題は認められないと考えられる。

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。	（記載要領本体P2） 2．中間サーバーに係る特定個人情報保護評価の前提 （2） 特定個人情報ファイルの考え方	問題は認められない	次の理由から、中間サーバーにおいて保有される副本や情報提供等記録は、業務システムにおいて保有する特定個人情報ファイルと一体のものと整理しているが、これらの理由は妥当なものと認められる。 ・中間サーバーにおいて保有される特定個人情報は単独で入手等されるものではなく、特定個人情報保護評価に係る事務を処理する既存システムにおける個人情報の副本となるものであることから、中間サーバーにおいて保有される特定個人情報のうち、業務システムで保有する業務情報の副本に係る特定個人情報については、業務情報と一体的に扱われる特定個人情報ファイルと整理している。 ・中間サーバーで保存する情報提供等の記録についても、特定個人情報保護評価に係る事務を処理する中で自動的に生成されるものであることから、同様に事務に係る特定個人情報ファイルと一体のものと整理している。
	○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中間サーバーの内容の機能に関する記載は妥当かつ具体的か。	（記載要領本体P4） 3．特定個人情報保護評価計画管理書及び特定個人情報保護評価書に関して （2）個別留意事項	問題は認められない	・中間サーバーの機能として、ハードウェアを含まないアプリケーション群である「中間サーバー・ソフトウェア」と、中間サーバーの拠点となる「中間サーバー・プラットフォーム」がある。中間サーバー・ソフトウェアは、地方公共団体において共通的に整備することが必要となるものであるため、全ての地方公共団体は総務省が一括開発したソフトウェアを使用するが、中間サーバーを自庁に設置する場合、中間サーバー・プラットフォームを活用せず各地方公共団体でハードウェアを整備・運用するため、中間サーバー・プラットフォームに係る記載をしない団体も想定される。 この点、本体及び記載例は「中間サーバー・ソフトウェア」と「中間サーバー・プラットフォーム」を明確に分けて記載しており、かつ、内容も具体的であるため、妥当である。 また、中間サーバーにおいて副本を保有することを明示するよう指示していることも、中間サーバーの機能の具体化に資するものであり、妥当である。

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	（評価書記載例P3） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続	問題は認められない	＜中間サーバー・ソフトウェアにおけるリスク対策＞ ・目的外の入手が行われるリスク対策として、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可照合リストとの照合を情報提供ネットワークシステムに求め、番号法上認められた情報連携以外の照会を拒否する機能をシステム上備えることなどが具体的に記載されている。 ・安全が保たれない方法によって入手が行われるリスク対策として、中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理す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入手のみ実施できるよう設計されていることについて記載されている。 ・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、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、情報提供用個人識別符号により紐付られた照会対象者に係る特定個人情報のみを入手することについて記載されている。 ・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、中間サーバーは、特定個人情報を暗号化して情報提供ネットワークシステムを使用して送信し、照会者の中間サーバーでしか復号できない仕組みとなっていることについて記載されている。 ＜中間サーバー・プラットフォームにおけるリスク対策＞ ・安全が保たれない方法によって入手が行われるリスク対策として、中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワークを利用していること、通信を暗号化することで安全性が確保されている旨具体的に記載されている。 ・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、中間サーバーと団体においては通信を暗号化していることや、事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等に限定されており、特定個人情報へはアクセスすることができないことが具体的に記載されている。

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
	○特定個人情報の提供	（評価書記載例P4） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続	問題は認められない	＜中間サーバー・ソフトウェアにおける措置＞ ・不正な提供が行われるリスク対策として、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（情報提供機能）を利用して、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をチェックできるということが明確に記載されている。 ・不適切な方法で提供されるリスク対策として、情報提供ネットワークシステムに送信する情報については暗号化して情報提供を行うこととされていること、ログイン時の職員認証等不適切なオンライン連携の防止措置が講じられていることについて記載されている。 ・誤った情報又は誤った相手に提供してしまうリスク対策として、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、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供を行うこと等について具体的に記載されている。 ＜中間サーバー・プラットフォームにおける措置＞ ・不適切な方法で提供されるリスク対策として、中間サーバーと関係するシステム間において、高度なセキュリティを維持した行政専用のネットワークを使用していること、通信を暗号化していること、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は、特定個人情報に係るアクセスができないよう管理されていることについて分かりやすく記載されている。
	○特定個人情報の保管・消去	（評価書記載例P2、P5） ・Ⅱ特定個人情報ファイルの概要 6．特定個人情報の保管・消去 ・Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 7．特定個人情報の漏えい・滅失・毀損リスク	問題は認められない	＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の保管・消去、特定個人情報の漏えい・滅失・毀損リスクに係る措置として、データセンターに構築する中間サーバー・プラットフォームについて、設置場所への入退室者管理、有人監視及び施錠管理などの物理的対策や、ウイルス対策ソフトの導入、パターンファイルの更新、必要に応じたセキュリティパッチの更新などの技術的対策を行うことについて、具体的に記載されている。

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
	○分散管理の徹底	（評価書記載例P4） Ⅲ特定個人情報の取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 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6：不適切な方法で提供されるリスク 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 Ⅳその他のリスク対策	問題は認められない	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバー・ソフトウェアについては、情報連携にのみ情報提供用個人識別符号を用いること、許可されていないシステムからのアクセス禁止等の措置について記載されている。 ＜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・プラットフォームでは、データベースを地方公共団体ごとに区分管理（アクセス制御）するほか、中間サーバー・プラットフォームの保守・運用を行う事業者は特定個人情報にはアクセスできないようにすることで、中間サーバーにおいて保有される特定個人情報の保有者である地方公共団体以外の者は、当該特定個人情報には一切アクセスできないこととしており、分散管理の徹底が図られていると考えられる。

【総評】

記載要領本体において、地方公共団体が中間サーバーに関して特定個人情報保護評価書を作成する場合の考え方や、参照すべきシステム方式設計書の該当箇所が適切に示されている。また、評価書記載例において、中間サーバーにおける特定個人情報の取扱いについて、リスク対策が具体的かつ分かりやすく示されており、国民の懸念（情報の一元管理等）にも対応していると考えられることから、特段の問題は認められないと考えられる。