資料２

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）

平成 26 年　月　日

総務省大臣官房企画課個人番号企画室

１．はじめに

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）第 27 条では、行政機関の長等は、特定個人情報ファイルを保有しようとするときは、特定個人情報保護評価を実施することとされている。

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た情報連携を行うため、既存システムが持つ個人情報の副本等を保有することとなる。このため、特定個人情報保護評価の実施が義務付けられる事務において、情報提供ネットワークシステムを使用した情報連携を行う場合は、中間サーバーについても、地方公共団体の機関において、特定個人情報保護評価を実施することが必要となる。

一方、「特定個人情報保護評価指針」（平成 26 年４月 18 日特定個人情報保護委員会告示第４号）第３の２において、「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」とされており、それを受け、「特定個人情報保護評価指針の解説」（平成 26 年４月 20 日特定個人情報保護委員会）において、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、システムやアプリケーションの設計・開発等の調達を実施する者が存在するなど、特定個人情報ファイルに関わる者が存在する場合については、特定個人情報ファイルの保有者では変更することのできないシステムやアプリケーションの仕様などに関わる部分について、システムやアプリケーションの設計・開発等を行った者が、特定個人情報保護評価が適切に実施されるよう情報提供に協力することとされている。

そのため、地方公共団体における中間サーバーについては、地方公共団体の機関において、特定個人情報保護評価が適切に実施されるよう、当該ソフトウェアを一括開発する総務省及び中間サーバー・プラットフォームを整備する地方公共団体情報システム機構から必要な情報を提供するものである。

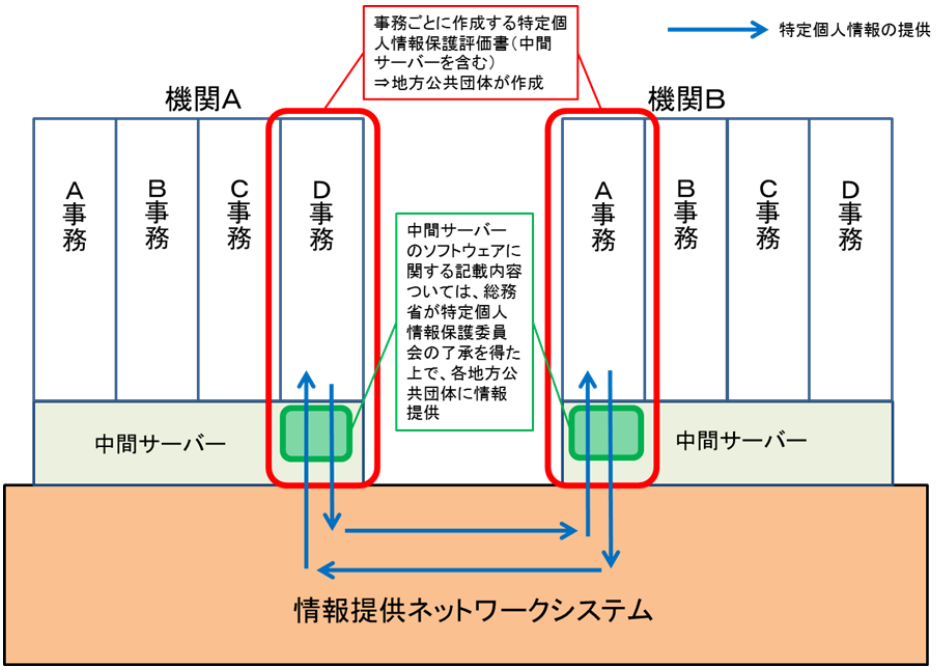
２．中間サーバーに係る特定個人情報保護評価の前提

(1) 特定個人情報保護評価に係る事務の考え方

特定個人情報ファイルを取り扱う事務には、番号法第９条第１項及び別表第一に掲げる事務、番号法第９条第２項の規定に基づき地方公共団体が条例で定める事務、番号法第９条第３項から第５項までの規定に基づき特定個人情報ファイルを取り扱う事務、住民基本台帳法に基づく住民票に関する事務等が存在する。

特定個人情報保護評価は、システムやサーバー単独で行うのではなく、特定個人情報ファイルを取り扱う事務ごとに実施するものである。

中間サーバーは、上記の特定個人情報ファイルを取り扱う事務について、情報提供や情報照会に係る機能を担うものであり、中間サーバーに係る評価は、当該事務に係る基礎項目評価書、重点項目評価書又は全項目評価書（以下「特定個人情報保護評価書」と総称する。以下同じ。）の中で記載することとなり、本書も同想定で記載している。



※　「特定個人情報保護評価指針の解説」（平成 26 年 4 月 20 日特定個人情報保護委員会）P. 22 から転載

※　なお、各地方公共団体において特定個人情報の照会又は提供を行う際は、情報提供ネットワークシステムを使用するものであるが、情報提供ネットワークシステムは、特定個人情報保護委員会と協議して、総務大臣が設置・管理するものであり（番号法第 21 条第 1 項）、情報提供ネットワークシステムにおいて保有する特定個人情報ファイルに関する特定個人情報保護評価は、関係行政機関の長の協力を得て、総務大臣が実施することから、各地方公共団体が実施する特定個人情報保護評価において、情報提供ネットワークシステムに係る特定個人情報保護評価を記載する必要はない。

(2) 特定個人情報ファイルの考え方

特定個人情報ファイルの単位は、評価実施機関の合理的裁量に委ねられている。本書では、中間サーバーにおいて保有する特定個人情報が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り、中間サーバーにおいて保有す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ものであることから、１つの特定個人情報ファイルとする想定で作成している。

また、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、同様に当該事務に係る特定個人情報ファイルと一体のものと想定している。

このため、全項目評価書については、中間サーバーにおいて保有する特定個人情報単独で記載するのではなく、特定個人情報保護評価を実施する事務に係る特定個人情報ファイルの中で、中間サーバーに係る部分についても記載することとしている。

なお、特定個人情報ファイルの単位は、評価実施機関の合理的裁量に委ねられていることから、評価実施機関の判断で、本書とは異なる特定個人情報ファイルの単位を採用することも、可能である。

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

(1) 記載が必要と考えられる箇所

中間サーバーに係る特定個人情報保護計画管理書及び特定個人情報保護評価書において、記載が必要と考えられる箇所は以下のとおりである。

【特定個人情報保護評価計画管理書】

記載が必要と考えられる項目	左のうち、記載例を別紙で示しているもの	
	SW	PF
（別添1）システム概要図		
（別添2）各システムの個人番号へのアクセス　1．個人番号にアクセスできるシステム		
個人番号を直接保有するシステム		

【特定個人情報保護評価書のうち全項目評価書】

記載が必要と考えられる項目	左のうち、記載例を別紙で示しているもの	
	SW	PF
Ⅰ　基本情報		
1．特定個人情報ファイルを取り扱う事務		
②事務の内容		
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		
①システムの名称		
②システムの機能		
③他のシステムとの接続		
（別添1）事務の内容		
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		
4．特定個人情報ファイルの取扱いの委託		
5．特定個人情報の提供・移転（委託に伴うものを除く。）		
6．特定個人情報の保管・消去		
①保管場所		○
③消去方法		○
（別添2）特定個人情報ファイル記録事項		
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		
4．特定個人情報ファイルの取扱いの委託		
6．情報提供ネットワークシステムとの接続		
リスク1：目的外の入手が行われるリスク	○	
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3：入手した特定個人情報が不正確であるリスク	○	
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5：不正な提供が行われるリスク	○	
リスク6：不適切な方法で提供されるリスク	○	○
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	○	
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	○	○

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. 特定個人情報の保管・消去		
	⑤物理的対策		○
	⑥技術的対策		○
Ⅳ　その他のリスク対策			
	1. 監査		
	①自己点検		○
	②監査		○
	2. 職員に対する教育・啓発		○
	3. その他のリスク対策		○
SW：中間サーバー・ソフトウェア　PF：中間サーバー・プラットフォーム			

※　基礎項目評価書及び重点項目評価書については、全項目評価書における該当項目を参考にされたい。

(2) 個別留意事項

上記のうち、特定個人情報保護評価計画管理書及び全項目評価書における留意事項は、以下のとおりである。

全項目評価書記載事項のうち、「中間サーバー・ソフトウェア」（※１）及び「中間サーバー・プラットフォーム」（※２）において対策を行っている事項については、記載例を示しているので、参考とされたい（別紙参照）。

なお、記載例を示している箇所であっても、特定個人情報保護評価の趣旨に鑑み、各地方公共団体での運用における対策は別途記載が必要となる。

※１　中間サーバー・ソフトウェア

番号法令に基づく、情報提供ネットワークシステムを使用した情報連携等を実施するため、地方公共団体（情報照会機関）からの特定個人情報の照会、及び地方公共団体（情報提供機関）による特定個人情報の提供それに付随する業務を行うアプリケーション（プログラム）群を指す（ハードウェアを含まない。）。

※２　中間サーバー・プラットフォーム

各地方公共団体の経費節減、セキュリティ、運用の安定性の確保の観点から、クラウドの積極的な活用により共同化・集約化を図るため、地方公共団体情報システム機構により整備・運用される中間サーバーの拠点。

（ア）「特定個人情報保護評価計画管理書」における留意事項

○　特定個人情報ファイルを取り扱う社会保障・税・災害対策分野等の個別事務ごとに記載するため、中間サーバーを事務として独立させて記載する必要はない。個別事務において中間サーバーを使用する場合は、「システムの名称」欄に、業務システム等とともに中間サーバーを記載すること。

○　「（別添１）システム概要図」箇所における留意事項

・　中間サーバーについては、情報提供用個人識別符号を保有するため、システム概要図には個人番号を直接保有するシステム（オレンジ色の網掛けなし）として記載すること（※）。なお、特定個人情報保護評価の実施義務の対象外の事務のみの地方公共団体であれば、オレンジ色の網掛けにすること。
・　中間サーバーと既存システムとのネットワーク構成については、「システム方式設計書　2.1 ネットワーク構成」の章を参照して、各地方公共団体の導入の形態等の事情を考慮して記載を行うこと。

※　地方公共団体における中間サーバーについては、個人番号を直接保有するシステム構成にはなっていないところであるが、「特定個人情報の提供を管理するために個人番号に代わって用いられる特定の個人を識別する符号」である情報提供用個人識別符号（番号法施行令第 20 条第１項）を保有することとしており、当該符号は番号法第２条第８項の規定により、番号法上の個人番号として取り扱われることから、この特定個人情報保護評価書の作成に当たっては、個人番号を直接保有するシステムとして位置付けているもの。

（イ）「特定個人情報保護評価書（全項目評価書）」における留意事項

評価対象の事務における特定個人情報の入手・委託・提供・保管・消去に当たって、中間サーバーを使用する場合には、中間サーバーに関する記載を行うこと。以下、特に留意すべき点について述べるが、以下の項目以外についても、各地方公共団体において必要な項目の記載を行うこと。

①　「Ⅰ　基本情報　１．特定個人情報ファイルを取り扱う事務」箇所について

・　関連箇所：「②事務の内容」
・　中間サーバーの「事務の内容」に関しては、「システム方式設計書　1.2 中間サーバーの概要」の章を参照し、各地方公共団体の事情を考慮して記載すること。

②　「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」箇所について

・　関連箇所：「①システムの名称」、「②システムの機能」、「③他のシステムとの接続」
・　中間サーバーのシステムの機能に関しては、「システム方式設計書　6.1 機能要件の概要」等の章を参照して記載すること。

③　「Ⅰ　基本情報　（別添１）事務の内容」箇所について

・　中間サーバーの「事務の内容」の図に関しては、「システム方式設計書　6.2.1 符号管理機能(図 6.2.1-2)」及び「システム方式設計書　6.2.3 情報提供機能(図 6.2.3-1)」等を参照し、各地方公共団体の事情を考慮して記載すること。

・　なお、その際は、中間サーバーで保有する副本等が、業務システムで保有する特定個人情報ファイルと一体のものであることが分かるように記載すること。

④　「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」箇所について

・　評価対象の事務において、中間サーバーを使用して情報の入手を行う場合においては、その旨の記載を行うこと。

※　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又は提供以外に、中間サーバーを使用することはないため、⑥使用目的から⑨使用開始日までは中間サーバーに係る記載を行うことは想定していない。

⑤　「Ⅱ　特定個人情報ファイルの概要　４．特定個人情報ファイルの取扱いの委託」箇所について

・　評価対象の事務において、中間サーバーに保存される特定個人情報ファイルの取扱いを委託する場合においては、その旨の記載を行うこと。

※　本書では、中間サーバー・プラットフォームにおいても、特定個人情報ファイルは、各地方公共団体が自ら管理することとしていることから、特定個人情報ファイルの取扱いの委託と扱っていない。

⑥　「Ⅱ　特定個人情報ファイルの概要　５．特定個人情報の提供・移転（委託に伴うものを除く。）」箇所について

・　評価対象の事務において、中間サーバーを使用して他団体への情報提供を行う場合においては、本項目における「提供先」の記載事項について記載を行うこと。

⑦　「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」箇所について

・　関連箇所：「①保管場所」、「③消去方法」

例）

①保管場所	＜○○市における措置＞ ・…… ・……　**各地方公共団体で記載する** ＜中間サーバー・プラットフォームにおける措置＞ ・…… ・……　**記載例を参考に記載する**

・　各地方公共団体における業務システムに関しては、＜○○市における措置＞のように、＜中間サーバー・プラットフォームにおける措置＞と分けて、各地方公共団体において記載すること。
・　地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して記載すること。
・　地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用しない地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞は記載せずに、＜○○市における措置＞の中に、各地方公共団体で中間サーバーについても考慮した内容を記載すること。

⑧　「Ⅱ　特定個人情報ファイルの概要　２．基本情報（別添２）特定個人情報ファイル記録項目」箇所について

・　中間サーバーで保有される特定個人情報のうち、業務システムで保有される特定個人情報と重複しない情報提供用個人識別符号、団体内統合宛名番号（又は団体内統合利用番号）、情報提供等の記録等についても、記載すること。
・　中間サーバーで保有される特定個人情報のうち、業務システムで保有される特定個人情報と重複する項目については、記録項目を二重に記載する必要はない。

⑨　「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　４．特定個人情報ファイルの取扱いの委託」箇所について

・　評価対象の事務において、中間サーバーに保存される特定個人情報ファイルの取扱いを委託する場合においては、そのリスク対策について記載を行うこと。

※　本書では、中間サーバー・プラットフォームにおいても、特定個人情報ファイルは、各地方公共団体が自ら管理することとしていることから、特定個人情報ファイルの取扱いの委託と扱っていない。

⑩　「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　６．情報提供ネットワークシステムとの接続」箇所について

・　関連箇所：「リスク１：目的外の入手が行われるリスク」から「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」、「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」まで

例）

リスクに対する措置の内容	＜○○業務システムのソフトウェアにおける措置＞ ・…… ・……　各地方公共団体で記載する ＜○○業務システムの運用における措置＞ ・…… ・……　各地方公共団体で記載する ＜中間サーバー・ソフトウェアにおける措置＞ ・…… ・……　記載例を参考に記載する ＜中間サーバー・プラットフォームにおける措置＞ ・…… ・……　記載例を参考に記載する ＜中間サーバーの運用における措置＞ ・…… ・……　各地方公共団体で記載する

- 各地方公共団体における業務システムに関しては、＜ソフトウェアにおける措置＞、＜運用における措置＞について、各地方公共団体において記載すること。＜中間サーバーのソフトウェア機能における措置＞については、記載例を参考に、各地方公共団体の事情を考慮して記載すること。
- ＜中間サーバーの運用における措置＞については、各地方公共団体において記載すること。
- 地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して記載すること。

⑪　**「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．特定個人情報の保管・消去」箇所について**

- 関連箇所：「⑤物理的対策」、「⑥技術的対策」

例）

⑤物理的対策		
	具体的な対策の内容	＜○○市における措置＞ ・…… ・……　各地方公共団体で記載する ＜中間サーバー・プラットフォームにおける措置＞ ・…… ・……　記載例を参考に記載する

・　各地方公共団体における業務システムに関しては、＜○○市における措置＞のように、＜中間サーバー・プラットフォームにおける措置＞と分けて、各地方公共団体において記載すること。
・　地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して記載すること。
・　地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用しない地方公共団体においては、＜○○市における措置＞の中に、各地方公共団体で中間サーバーについても考慮した内容を記載すること。

⑫　「Ⅳ　その他のリスク対策　１．監査」箇所について

・　評価対象の事務において中間サーバー・プラットフォームを活用する場合は、中間サーバー・プラットフォームに関する記載が必要になる。
・　関連箇所：「①自己点検」、「②監査」
・　「①自己点検　具体的なチェック方法」及び「②監査　具体的な方法」欄は、地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して、記載すること。

⑬　「Ⅳ　その他のリスク対策　２．職員に対する教育・啓発」箇所について

・　評価対象の事務において中間サーバー・プラットフォームを活用する場合は、中間サーバー・プラットフォームに関する記載が必要になる。
・　「具体的方法」欄は、地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して、記載すること。

⑭　「Ⅳ　その他のリスク対策　３．その他のリスク対策」箇所について

・　評価対象の事務において中間サーバー・プラットフォームを活用する場合は、中間サーバー・プラットフォームに関する記載が必要になる。
・　地方公共団体情報システム機構が用意する中間サーバー・プラットフォームを活用する地方公共団体においては、＜中間サーバー・プラットフォームにおける措置＞について、記載例を参考に、各地方公共団体の事情を考慮して、記載すること。

(3) その他の留意事項

特定個人情報保護評価書の公表に際しては、当該評価書を公表することによりセキュリティ上のリスクがあると認められる記載内容は非公表とすることができる。中間サーバーの設計書等や各地方公共団体のネットワーク構成図等に関して、期間、回数等の具体的な数値や技術的細目に及ぶ具体的な方法を記載する場合には、セキュリティ上のリスクの観点から公表しないことを検討すべき場合があることに留意されたい。

なお、特定個人情報保護評価書に非公表とする部分があっても、第三者点検においては、非公表部分を含めて第三者点検を行うことが想定されている。総務省では、住民等の意見聴取及び第三者点検においても、必要に応じて地方公共団体に協力することとしている。

本書については、地方公共団体以外の機関が閲覧できる「デジタルＰMO」のサイトに掲載することとしている。

資料２
（別紙）

特定個人情報保護評価書（全項目評価書）（案）

評価書番号	評価書名

個人のプライバシー等の権利利益の保護の宣言	
特記事項	

評価実施機関名

特定個人情報保護委員会　承認日 【行政機関等のみ】
公表日
平成　年　月　日

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		
①保管場所※		＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。
②保管期間	期間	[ ] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	
③消去方法		＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、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、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。

7. 備考

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．リスク1⑨を除く）

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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、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用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、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備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）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照会及び照会した情報の受領を行う機能。 （※2）番号法別表第2及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①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るため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ①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（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①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て、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①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た特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）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特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①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（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき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チェックを実施している。 ②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、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）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提供の要求の受領及び情報提供を行う機能。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①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（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③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業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
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	＜中間サーバー・ソフトウェアにおける措置＞ ①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することで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
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
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①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（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理する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）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、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ける情報漏えい等のリスクを極小化する。

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	[ ]	＜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	[ ]	＜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	[ ]	＜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	[ ]	＜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	[ ]	＜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	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
⑥技術的対策	[ ]	＜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	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	

Ⅳ　その他のリスク対策　※

1. 監査		
①自己点検		[ ]　＜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 チェック方法	＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
②監査		[ ]　＜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
	具体的な内容	＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー･プラットフォームについて、定期的に監査を行うこととしている。
2. 職員に対する教育･啓発		
職員に対する教育･啓発		[ ]　＜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	＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ②中間サーバー･プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。
3. その他のリスク対策		
＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用･監視を実現する。		