

# 特定個人情報保護評価書(全項目評価書)

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

個人情報保護委員会 承認日【行政機関等のみ】
公表日



# 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. リスク1 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)
<b>リスク1: 目的外の入手が行われるリスク</b>			
リスクに対する措置の内容	<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;                      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、提供許可証の発行と照会内容の照会許可用照会リスト( 2)との照会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。</p> <p>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。</p> <p>( 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) <b>番号法の規定によ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に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。</b>                      ( 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。</p>		
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	
<b>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</b>			
リスクに対する措置の内容	<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;                      中間サーバーは、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。</p> <p>&lt; 中間サーバー・プラットフォームにおける措置 &gt;                      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。                      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。</p>		
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	
<b>リスク3: 入手した特定個人情報ที่ไม่正確であるリスク</b>			
リスクに対する措置の内容	<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;                      中間サーバーは、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。</p>		
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	<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;  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っている。  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照合リストを管理する機能。</p> <p>&lt; 中間サーバー・プラットフォームにおける措置 &gt;  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。  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。  中間サーバー・プラットフォームの事業者においては、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。</p>
リスクへの対策は十分か	<p>[ ] &lt; 選択肢 &gt;  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</p>
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	<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;  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、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。  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。  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。</p>
リスクへの対策は十分か	<p>[ ] &lt; 選択肢 &gt;  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</p>
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	
<p>&lt; 中間サーバー・ソフトウェアにおける措置 &gt;  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。</p> <p>&lt; 中間サーバー・プラットフォームにおける措置 &gt;  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。  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。  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。  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事業者における情報漏えい等のリスクを極小化する。</p>	

**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

NISC政府機関統一基準群	[ ]	<p>&lt;選択肢&gt;                      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</p>
安全管理体制	[ ]	<p>&lt;選択肢&gt;                      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</p>
安全管理規程	[ ]	<p>&lt;選択肢&gt;                      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</p>
安全管理体制・規程の職員への周知	[ ]	<p>&lt;選択肢&gt;                      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</p>
物理的対策	[ ]	<p>&lt;選択肢&gt;                      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</p>
具体的な対策の内容		<p>&lt;中間サーバー・プラットフォームにおける措置&gt;                      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。  <b>事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。</b></p>
技術的対策	[ ]	<p>&lt;選択肢&gt;                      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</p>
具体的な対策の内容		<p>&lt;中間サーバー・プラットフォームにおける措置&gt;                      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。                      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。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。</p>

## その他のリスク対策

1. 監査	
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> 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。
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> 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. 従業者に対する教育・啓発	
従業者に対する教育・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> IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、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、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。
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> 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。	