

### Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名	
児童手当等支給台帳ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク： 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	<p>【申請時における措置】</p> <p>①個人番号の記載を要する届出書、申請書及び申告書等は、法令及び条例等において規定されるため、受給者等が個人番号の記載が必要であることを確認することができる。</p> <p>②認定請求書等受領時に保管する場所を統一し、他の職員や外部からの覗き見等ができないよう対応する。</p> <p>③マニュアルやWEB上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報入所を防止する。</p> <p>④住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索、申請フォームを選択して必要な情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。</p> <p>⑤個人番号カード等の身分証明書の提示による本人確認を厳守することで、対象者以外の情報入手を防止する。郵送での受付時も、身分証明書の写しの添付を求める。</p> <p>【システムにおける措置】</p> <p>①児童手当等支給事務等に関係のない情報を入手する事がないよう情報システム責任者が監視を行うとともに、職員に対する教育を徹底する。</p> <p>②職員の職責に基づきシステム上の権限を設定し不適切な操作ができないようになっており、すべての操作についてログを取得し保管している。なお、一定期間保管し、必要に応じて確認が行える仕組みとする。</p>
リスクへの対策は十分か	<p>[ 十分である ] &lt;選択肢&gt;</p> <p>1) 特に力を入れている                      2) 十分である</p> <p>3) 課題が残されている</p>
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
<p>&lt;不適切な方法で入手が行われるリスクに対する措置&gt;</p> <p>①調査・照会等により情報を入手する場合、照会先に調査目的、根拠法令等を示したうえ回答を求める。</p> <p>②システムを操作する職員に個別のユーザーIDとパスワードによる認証及び生体認証を行っており、不適切な方法で特定個人情報の入手ができない仕組みとしている。</p> <p>③住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、本人からの情報のみが送信される。</p> <p>④サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。</p> <p>&lt;入手した特定個人情報が不正確であるリスクに対する措置&gt;</p> <p>①入力、削除または訂正作業に用いた帳票等は、規定に基づいて管理し、保管する。</p> <p>②入手した情報に疑義がある場合は調査を行い、情報を修正する。</p> <p>③住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した委託機関は署名検証（有効性確認、改ざん検知等）を実施することとなる。これにより、本人確認を実施する。</p> <p>④サービス検索・電子申請機能への個人番号の入力時には、チェックデジット等の機能により、不正確な個人番号が入力されないようにしている。また、個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。</p> <p>&lt;入手の際に特定個人情報が漏えい・紛失するリスクに対する措置&gt;</p> <p>①申請書等の帳票を施錠できる保管庫にて保管する。</p> <p>②申請書等の受領後、当該文書の保存については執務場所以外への持ち出しを禁止する。</p> <p>③郵送での受付の際は担当課の住所・部署名を明確化して誤送付によるリスクを軽減する。</p> <p>④サービス検索・電子申請機能と地方公共団体との間は、委託事業者が委託契約にもとづき、申請情報を封緘し、書留等の記録が残る追跡可能な手段で地方公共団体に郵送することにより、安全を確保している。</p>	

3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
リスクに対する措置の内容	業務共通システムとの連携においては、利用者が適切なアクセス権限を保持している場合のみ特定個人情報の連携を許可する仕様となっており、目的を超えた紐付けや事務に必要な情報との紐付けが行われないようにシステム上でアクセス制御を行う。 また、児童手当支給事務における特定個人情報は、職務上必要と認められる権限が与えられた者しかアクセスできないようにしている。
リスクへの対策は十分か	[ 十分である ] <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: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク	
ユーザ認証の管理	[ 行っている ] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	システムを利用する必要がある職員を特定し、個人ごとにユーザIDを割り当てるとともに、ユーザIDと生体認証及びパスワードによる個人認証を行う。
その他の措置の内容	端末PCについて、画面の盗み見・不正利用対策として、一定時間操作が行われなかった場合にスクリーンセーバを起動し、元の画面に復帰する際には再度生体認証を行う仕組みとする。さらに一定時間経過後に自動的にログオフする制御を行う。
リスクへの対策は十分か	[ 十分である ] <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
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
4. 特定個人情報ファイルの取扱いの委託 [ ] 委託しない	
リスク: 委託先における不正な使用等のリスク	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[ 定めている ] <選択肢> 1) 定めている 2) 定めていない
規定の内容	契約書において、秘密保持、個人情報の使用、複製等、管理、個人情報の取得、個人情報の返還及び事故発生時の対応等について規定しており、必要に応じて、職員がその内容を確認する。
再委託先による特定個人情報ファイルの適切な取扱いの担保	[ 再委託していない ] <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 4) 再委託していない
具体的な方法	
その他の措置の内容	
リスクへの対策は十分か	[ 十分である ] <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
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[ ] 提供・移転しない
リスク： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[ 定めている ]	<選択肢> 1) 定めている                      2) 定めていない
ルールの内容及びルール遵守の確認方法	番号法及び条例の規定により、認められている範囲内でのみ情報の提供・移転を行う。	
その他の措置の内容		
リスクへの対策は十分か	[ 十分である ]	<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
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

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	<p>【中間サーバー・ソフトウェアにおける措置】</p> <p>①情報照会機能(注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照会リスト(注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。</p> <p>②中間サーバーの職員認証・権限管理機能(注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>(注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。  (注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。  (注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	[ 十分である ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 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	<p>【業務共通システムにおける措置】</p> <p>番号法により認められている機関、事務をシステム的かつ職員による審査にて判断し、提供できる仕組みを構築している。</p> <p>【中間サーバー・ソフトウェアにおける措置】</p> <p>①情報提供機能(注)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照会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、照会許可照会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を要求であることをチェックを実施している。</p> <p>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を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。</p> <p>③特に慎重な対応を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。</p> <p>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。</p> <p>(注)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。</p>		
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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			
<p>【中間サーバー・ソフトウェアにおける措置】</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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>(注)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。</p> <p>【中間サーバー・プラットフォームにおける措置】</p> <p>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には高度なセキュリティを維持した行政専用ネットワーク(総合行政ネットワークなど)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。</p> <p>②中間サーバーと団体についてはVPNなどの技術を利用し、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。</p> <p>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・障害対応などであり、業務上特定個</p>			

7. 特定個人情報の保管・消去		
リスク: 特定個人情報の漏えい・滅失・毀損リスク		
①事故発生時手順の策定・周知	[ 十分に行っている ]	<選択肢> 1) 特に力を入れている 2) 十分に行っている 3) 十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[ 発生あり ]	<選択肢> 1) 発生あり 2) 発生なし
その内容	<p><b>【事例1】</b></p> <p>①事案／当該事案に関する個人情報の件数 市内事業者あてメールの誤送信(各受信者が他者のメールアドレスを閲覧できる状態となったもの)／250件</p> <p>②発生時期 平成28年6月</p> <p>③原因 職員の誤操作(「TO」欄に全送信先のメールアドレスを入力し送信)</p> <p>④発生時の対応 全送信先へ事件の発生を周知・謝罪するとともに、誤送信したメールの削除を依頼</p> <p><b>【事例2】</b></p> <p>①事案／当該事案に関する個人情報の件数 「不審者情報」メールを希望する市民あてメールの誤送信(各受信者が他者のメールアドレスを閲覧できる状態となったもの)／127件</p> <p>②発生時期 平成30年6月</p> <p>③原因 職員の誤操作(「CC」欄に全送信先のメールアドレスを入力し送信)</p> <p>④発生時の対応 全送信先へ事件の発生を周知・謝罪するとともに、誤送信したメールの削除を依頼</p>	
再発防止策の内容	<p><b>【事例1】について</b></p> <ul style="list-style-type: none"> <li>メールの一斉送信時には、複数職員で確認を行うこととした。</li> <li>宛先入力欄に「BCC」欄が常に表示されるよう設定し、必ず「BCC」で送信することとした。</li> <li>メール送信操作実行後、ただちに送信されず、一定時間送信トレイに保管されるよう設定した。</li> </ul> <p><b>【事例2】について</b></p> <ul style="list-style-type: none"> <li>庁内システムで使用する共通メールソフトの設定を変更し、庁外メールアドレス宛に送信するメールは全て強制的にBCCで送信されるようにした。</li> </ul>	
その他の措置の内容		
リスクへの対策は十分か	[ 十分である ]	<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
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

8. 監査	
実施の有無	[ <input type="radio"/> ] 自己点検                      [ <input type="radio"/> ] 内部監査                      [ <input type="checkbox"/> ] 外部監査
9. 従業者に対する教育・啓発	
従業者に対する教育・啓発	[ <input type="checkbox"/> 十分に行っている ]                      <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	<p>&lt;福祉システムにおける措置&gt; 「千葉県情報セキュリティ対策基準」に基づき、 ・情報セキュリティ責任者等に対しては、年1回以上、情報セキュリティの確保に関する、①セキュリティ事故の検出、報告、復旧及び対応手法、②リスク分析手法、③セキュリティ対策の導入及び運用手法、④セキュリティ事故の事例、⑤セキュリティ教育手法の内容を基本とした研修を実施している。 ・職員等に対しては、情報セキュリティの確保に関する、①情報セキュリティの重要性、②情報システム利用者の責任、③セキュリティ事故の事例、④モラルの啓発、⑤禁止行為及びそれらに対する罰則の内容を基本とした研修を年に1回、個人情報保護に関する研修と併せて実施している。</p> <p>【中間サーバー・プラットフォームにおける措置】 ①運用規則などに基づき、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、セキュリティ研修などを実施することとしている。</p>
10. その他のリスク対策	
<p>【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(入退室管理など)、ITリテラシー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。</p>	