

新旧対照表

○特定個人情報保護評価書(国民年金に関する事務 重点項目評価書)

新	旧
<p>特定個人情報保護評価書(重点項目評価書)</p>	<p>特定個人情報保護評価書(重点項目評価書)</p>
<p>表紙 項目一覧</p>	<p>表紙 項目一覧</p>
<p>I 基本情報</p>	<p>I 基本情報</p>
<p>1. 特定個人情報ファイルを取り扱う事務～7. 他の評価実施機関</p> <p>※本項目は変更がないため記載を省略する。(以下「略」の表示がある場合は全て同じ。)</p>	<p>1. 特定個人情報ファイルを取り扱う事務～7. 他の評価実施機関</p> <p>略</p>
<p>II 特定個人情報ファイルの概要</p>	<p>II 特定個人情報ファイルの概要</p>
<p>1. 特定個人情報ファイル名</p> <p>(1)国民年金ファイル</p>	<p>1. 特定個人情報ファイル名</p> <p>(1)国民年金ファイル</p>
<p>2. 基本情報</p>	<p>2. 基本情報</p>
<p>3. 特定個人情報の入手・使用</p>	<p>3. 特定個人情報の入手・使用</p>
<p>①入手元</p>	<p>①入手元</p>
<p>[○]本人又は本人の代理人、[○]評価実施機関内の他部署(区民生活部区民課、区民生活部課税課、保健福祉部福祉事務所、<u>総務部情報政策課</u>)、[○]行政機関・独立行政法人等(日本年金機構)、[○]地方公共団体・地方独立行政法人(他自治体)</p>	<p>[○]本人又は本人の代理人、[○]評価実施機関内の他部署(区民生活部区民課、区民生活部課税課、保健福祉部福祉事務所、政策経営部情報政策課)、[○]行政機関・独立行政法人等(日本年金機構)、[○]地方公共団体・地方独立行政法人(他自治体)</p>
<p>②入手方法～ ⑥使用開始日</p>	<p>②入手方法～ ⑥使用開始日</p>
<p>略</p>	<p>略</p>
<p>4. 特定個人情報ファイルの取扱いの委託</p>	<p>4. 特定個人情報ファイルの取扱いの委託</p>
<p>委託の有無</p>	<p>委託の有無</p>
<p>[委託する] (6)件</p>	<p>[委託する] (5)件</p>
<p>委託事項1～5</p>	<p>委託事項1～5</p>
<p>略</p>	<p>略</p>
<p>委託事項6</p>	<p>委託事項6</p>
<p>国民年金業務設計及び運営業務</p>	
<p>①委託内容</p>	<p>①委託内容</p>
<p>(設計) ・国民年金に係る業務の分析及び業務マニュアル並びに 運営管理マニュアル等の作成 (運営業務) ・国保年金課における国民年金に係る書類の受付及び電</p>	

新		旧	
	話対応(書類の決裁等の公権力行使にあたる業務は除く)		
②委託先における取扱者数	10人以上50人未満	②委託先における取扱者数	
③委託先名	株式会社DACS、株式会社ベルシステム24、株式会社エヌ・ティ・ティデータ共同事業体	③委託先名	
④再委託の有無	[再委託する]	④再委託の有無	
⑤再委託の許諾方法	・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承諾した業者のみ再委託を許諾する。	⑤再委託の許諾方法	
⑥再委託事項	国民年金業務設計及び運営業務	⑥再委託事項	
5. 特定個人情報の提供・移転(委託に伴うものを除く。)		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		6. 特定個人情報の保管・消去	
7. 備考		7. 備考	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(3) 中間サーバコネクタDBファイル	
2. 基本情報	
3. 特定個人情報の入手・使用	
①入手元	[○]本人又は本人の代理人、[○]評価実施機関内の他部署(区民生活部区民課、総務部情報政策課、保健福祉部福祉事務所)、[○]行政機関・独立行政法人等(日本年金機構)、[○]地方公共団体・地方独立行政法人(他自治体)
②入手方法～ ⑥使用開始日	略
4. 特定個人情報ファイルの取扱いの委託～7. 備考	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(5)障害基礎年金受給確認ファイル	
2. 基本情報	
3. 特定個人情報の入手・使用	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(3) 中間サーバコネクタDBファイル	
2. 基本情報	
3. 特定個人情報の入手・使用	
①入手元	[○]本人又は本人の代理人、[○]評価実施機関内の他部署(区民生活部区民課、政策経営部情報政策課、保健福祉部福祉事務所)、[○]行政機関・独立行政法人等(日本年金機構)、[○]地方公共団体・地方独立行政法人(他自治体)
②入手方法～ ⑥使用開始日	略
4. 特定個人情報ファイルの取扱いの委託～7. 備考	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(5)障害基礎年金受給確認ファイル	
2. 基本情報	
3. 特定個人情報の入手・使用	

新		旧	
①～⑥	略	①～⑥	略
4. 特定個人情報ファイルの取扱いの委託		4. 特定個人情報ファイルの取扱いの委託	
委託の有無	[委託する] (3)件	委託の有無	[委託する] (2)件
委託事項1～2	略	委託事項1～2	略
委託事項3	国民年金業務設計及び運營業務	委託事項3	
①委託内容	(設計) ・国民年金に係る業務の分析及び業務マニュアル並びに 運営管理マニュアル等の作成 (運營業務) ・国保年金課における国民年金に係る書類の受付及び電 話対応(書類の決裁等の公権力行使にあたる業務は除く)	①委託内容	
②委託先における取扱者数	10人以上50人未満	②委託先における取扱者数	
③委託先名	株式会社DACS、株式会社バルシステム24、株式会社エヌ・ ティ・ティデータ共同事業体	③委託先名	
④再委託の有無	[再委託する]	④再委託の有無	
⑤再委託の許諾方法	・原則として再委託は行わないが、再委託に関する承認申 請書により、再委託理由等を明確にし、区が承諾した業者 のみ再委託を許諾する。	⑤再委託の許諾方法	
⑥再委託事項	国民年金業務設計及び運營業務	⑥再委託事項	
5. 特定個人情報の提供・移転(委託に伴うものを除く。)		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		6. 特定個人情報の保管・消去	
7. 備考		7. 備考	
Ⅲリスク対策		Ⅲリスク対策	
1. 特定個人情報ファイル名		1. 特定個人情報ファイル名	
(1)国民年金ファイル		(1)国民年金ファイル	
(2)福祉住民登録外者等記録ファイル		(2)福祉住民登録外者等記録ファイル	
2. 特定個人情報の入手(情報提供ネットワークを通じた入手を除く。)		2. 特定個人情報の入手(情報提供ネットワーク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:目的外の入手が行われるリスク	
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		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	

新	旧
<p>(不適切な方法で入手が行われるリスク対策)</p> <ul style="list-style-type: none"> ・国民年金に関する事務を取り扱うにあたり、根拠法令である国民年金法及び国民年金市町村事務処理基準等に規定された内容を遵守することで、不適切な方法による情報の入手を防止する。 ・番号法及び杉並区個人情報保護条例における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・情報セキュリティマネジメント実施基準による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・システムの操作に当たり、操作履歴を採取し保管することで、対象者以外の情報の入手を抑止する。また、入力する情報は、法令で定められ、杉並区情報公開・個人情報保護審議会への必要な手続きを行ったものに限定する。 ・本人から情報を取得する場合は、国民年金の第1号被保険者等に係る事務に用いる旨を説明した上で取得する。 ・他自治体、日本年金機構等、本人以外からの情報をシステムを通して取得する場合は、アクセス権が与えられた者のみが取得できるようにシステム的に制限する。 ・日付の範囲指定で操作ログを採取し、入手時期や数量等が不自然なものがないかを確認する。 <p>(入手した特定個人情報 that 不正確であるリスク対策)</p> <ul style="list-style-type: none"> ・窓口での聴聞や添付書類との整合性から正確性を担保する。 ・本人から個人番号の提供を受ける場合には、個人番号カードや通知カードの提示を受ける。また、本人確認を行う際は、番号法第16条及び施行令第12条に基づき、本人確認書類の提示等を受ける。また、受けた申請書等については、4情報を確認することで入手する情報の正確性を担保する。 ・他区市町村等、本人以外から個人番号の提供を受ける際は、情報提供元が本人に対して個人番号及び4情報が正しいことを確認する。 ・個人番号カードの提示が無い場合には、運転免許証の提示等により得られた本人確認情報とシステムによって確認する本人確認情報との対応付けを行い、個人番号が本人のものであることを担保する。 ・国等から示される事務処理要領等を参考に事務処理対象者の個人番号カード等の提示を受け、本人確認及び個人番号の確認を行う。 ・入手した特定個人情報について、保持している特定個人情報と突合を行い、真正性及び正確性確認を行う。 ・杉並区に住民登録をしている者の4情報及び個人番号については、住民基本台帳に関 	<p>(不適切な方法で入手が行われるリスク対策)</p> <ul style="list-style-type: none"> ・国民年金に関する事務を取り扱うにあたり、根拠法令である国民年金法及び国民年金市町村事務処理基準等に規定された内容を遵守することで、不適切な方法による情報の入手を防止する。 ・番号法及び杉並区個人情報保護条例における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・情報セキュリティマネジメント実施基準による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・システムの操作に当たり、操作履歴を採取し保管することで、対象者以外の情報の入手を抑止する。また、入力する情報は、法令で定められ、杉並区情報公開・個人情報保護審議会への必要な手続きを行ったものに限定する。 ・本人から情報を取得する場合は、国民年金の第1号被保険者等に係る事務に用いる旨を説明した上で取得する。 ・他自治体、日本年金機構等、本人以外からの情報をシステムを通して取得する場合は、アクセス権が与えられた者のみが取得できるようにシステム的に制限する。 ・日付の範囲指定で操作ログを採取し、入手時期や数量等が不自然なものがないかを確認する。 <p>(入手した特定個人情報 that 不正確であるリスク対策)</p> <ul style="list-style-type: none"> ・窓口での聴聞や添付書類との整合性から正確性を担保する。 ・本人から個人番号の提供を受ける場合には、個人番号カードや通知カードの提示を受ける。また、本人確認を行う際は、番号法第16条及び施行令第12条に基づき、本人確認書類の提示等を受ける。また、受けた申請書等については、4情報を確認することで入手する情報の正確性を担保する。 ・他区市町村等、本人以外から個人番号の提供を受ける際は、情報提供元が本人に対して個人番号及び4情報が正しいことを確認する。 ・個人番号カードの提示が無い場合には、運転免許証の提示等により得られた本人確認情報とシステムによって確認する本人確認情報との対応付けを行い、個人番号が本人のものであることを担保する。 ・国等から示される事務処理要領等を参考に事務処理対象者の個人番号カード等の提示を受け、本人確認及び個人番号の確認を行う。 ・入手した特定個人情報について、保持している特定個人情報と突合を行い、真正性及び正確性確認を行う。 ・杉並区に住民登録をしている者の4情報及び個人番号については、住民基本台帳に関

新	旧
<p>する事務で取得したものを国民年金システムから利用するため、当該データの正確性については担保されたものとして利用する。</p> <ul style="list-style-type: none"> ・住民登録外者の場合は、住民基本台帳ネットワークを通して住民登録地である自治体へ個人番号を照会し、本人確認情報との対応付けを行う。 ・情報の入力、削除、訂正を行う場合には処理者と点検者を別にし、二重チェックを行うことで正確性を担保する。 <p>(入手した際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・窓口で本人又は本人の代理人が来庁する場合は、<u>個人番号利用事務実施者</u>が直接申請書等を収受する。また、受付事務が完了次第、直ちに書類を定められた保管箱へ格納する。 ・郵送で情報を入手する場合は、送付先誤り等による情報漏えい・紛失等を防止するため、事前に担当所属名及び所在地を広く周知する。また、返信用封筒等はあらかじめ担当所属名及び所在地を印刷等したものを使用する。 ・端末には、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。 ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・システム操作に必要なソフトウェアについては情報政策課への申請に基づいて必要数のみを付与するので入力を行える端末機は限定される。また操作に必要なID、パスワードは、各所属長から情報システム担当課長への申請に基づいて付与することで操作権限のない者による不正な操作を防止する。 	<p>する事務で取得したものを国民年金システムから利用するため、当該データの正確性については担保されたものとして利用する。</p> <ul style="list-style-type: none"> ・住民登録外者の場合は、住民基本台帳ネットワークを通して住民登録地である自治体へ個人番号を照会し、本人確認情報との対応付けを行う。 ・情報の入力、削除、訂正を行う場合には処理者と点検者を別にし、二重チェックを行うことで正確性を担保する。 <p>(入手した際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・窓口で本人又は本人の代理人が来庁する場合は、職員が直接申請書等を収受する。また、受付事務が完了次第、直ちに書類を定められた保管箱へ格納する。 ・郵送で情報を入手する場合は、送付先誤り等による情報漏えい・紛失等を防止するため、事前に担当所属名及び所在地を広く周知する。また、返信用封筒等はあらかじめ担当所属名及び所在地を印刷等したものを使用する。 ・端末には、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。 ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・システム操作に必要なソフトウェアについては情報政策課への申請に基づいて必要数のみを付与するので入力を行える端末機は限定される。また操作に必要なID、パスワードは、各所属長から情報システム担当課長への申請に基づいて付与することで操作権限のない者による不正な操作を防止する。
<p>3. 特定個人情報の使用</p>	<p>3. 特定個人情報の使用</p>
<p>リスク1: 目的を超えた紐付け、事務に必要な情報と紐付けが行われるリスク</p>	<p>リスク1: 目的を超えた紐付け、事務に必要な情報と紐付けが行われるリスク</p>
<p>リスクに対する措置の内容</p> <ul style="list-style-type: none"> ・宛名システム機能は中間サーバコネクタが実施する仕組みであり、個人番号利用事務以外では個人番号の検索ができないよう、システム上で制御する。 ・中間サーバコネクタには個人番号、4情報等の情報連携に必要な情報のみ記録し、不必要な情報との紐付けができないよう、システム上で制御する。 ・本特定個人情報ファイルに入力する端末機は物理的に区 	<p>リスクに対する措置の内容</p> <ul style="list-style-type: none"> ・宛名システム機能は中間サーバコネクタが実施する仕組みであり、個人番号利用事務以外では個人番号の検索ができないよう、システム上で制御する。 ・中間サーバコネクタには個人番号、4情報等の情報連携に必要な情報のみ記録し、不必要な情報との紐付けができないよう、システム上で制御する。 ・本特定個人情報ファイルに入力する端末機は物理的に区

新		旧	
	<p>画された執務室でのみ操作可能であり、<u>個人番号利用事務実施者</u>ごとに配付されたユーザID及びパスワードで認証を行うことで不要なアクセスを防いでいる。</p> <ul style="list-style-type: none"> 個人番号利用事務のみ個人番号検索を可能とする仕組みとするため、他システムにおける個人番号利用事務以外の情報の紐付けは行えないよう、システム上で制御する。 システム間の接続制御のため、ファイアウォールを設置することで登録外のシステムからの接続が行われないようシステム上で制御する。 ファイアウォールで制御したシステム間の通信は、ログとして記録し、ログの確認により適正な通信が行われているか監視する。 		<p>画された執務室でのみ操作可能であり、職員ごとに配付されたユーザID及びパスワードで認証を行うことで不要なアクセスを防いでいる。</p> <ul style="list-style-type: none"> 個人番号利用事務のみ個人番号検索を可能とする仕組みとするため、他システムにおける個人番号利用事務以外の情報の紐付けは行えないよう、システム上で制御する。 システム間の接続制御のため、ファイアウォールを設置することで登録外のシステムからの接続が行われないようシステム上で制御する。 ファイアウォールで制御したシステム間の通信は、ログとして記録し、ログの確認により適正な通信が行われているか監視する。
リスクへの対策は十分か	略	リスクへの対策は十分か	略
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		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	略	ユーザ認証の管理	略
具体的な管理方法	略	具体的な管理方法	略
その他の措置の内容	<p>(アクセス権限の発行・失効の管理)</p> <ul style="list-style-type: none"> アクセス権限の発行は、業務主管課からの発行申請により情報システム担当課長の承認後、当該課長から管理権限を付与された職員が行う。失効は、業務主管課からの解除申請により、管理権限を付与された職員が行う。その他、申請漏れ等への対応として、人事異動情報その他の権限失効に関わる情報を管理権限を付与された職員が得た段階で、随時その権限の失効を行う。 <p>(アクセス権限の管理)</p> <ul style="list-style-type: none"> セキュリティ責任者(業務主管課長)はアクセス権限と事務の対応表(事務担当者に対する権限付与の範囲を規定したもの)を作成し、定期的に付与されている権限と対応表が一致しているか点検を行い、違いが発見された場合には、ただちに適正な状態に修正する。 ユーザーアカウントおよびアクセス権について不要・不適 	<p>(アクセス権限の発行・失効の管理)</p> <ul style="list-style-type: none"> アクセス権限の発行は、業務主管課からの発行申請により情報システム担当課長の承認後、当該課長から管理権限を付与された職員が行う。失効は、業務主管課からの解除申請により、管理権限を付与された職員が行う。この他、申請漏れ等への対応として、人事異動情報その他の権限失効に関わる情報の管理権限を付与された職員が得た段階で、随時その権限の失効を行う。 <p>(アクセス権限の管理)</p> <ul style="list-style-type: none"> セキュリティ責任者(業務主管課長)はアクセス権限と事務の対応表(事務担当者に対する権限付与の範囲を規定したもの)を作成し、定期的に付与されている権限と対応表が一致しているか点検を行い、違いが発見された場合には、ただちに適正な状態に修正する。 ユーザーアカウントおよびアクセス権について不要・不適 	

新	旧
<p>切なものがないか定期的に確認する手順が「情報セキュリティマネジメント実施基準」に定められおり、当該規定に基づき確認を行う。</p> <p>(特定個人情報の使用の記録)</p> <ul style="list-style-type: none"> ・システムの操作ログを保管する。ログは個人番号を参照・入力した際に個人単位で記録することとし、操作者を識別可能な一意の番号_、操作時間、トランザクション(処理データ)名、操作端末名、操作を行っていたデータ名等を記録する。 ・保管するログは、物理的に区画・施錠された保管棚で、「杉並区文書等保存年限基準」及び「情報セキュリティマネジメント実施基準」に基づき管理する。 ・災害時データ復旧用を実施するデータの遠隔地保管のために可搬媒体の受け渡しを行う場合には「荷物搬入出記録簿」に記録する。 <p>(入退室管理)</p> <ul style="list-style-type: none"> ・不正な第三者からのアクセスを制御するため、特定個人情報を取り扱う執務室内への入退室管理について「情報セキュリティマネジメント実施基準」に規定し、規定された内容を遵守することで、権限のない者が特定個人情報を使用するリスクに対応する。 <p>(災害時データ復旧用媒体管理)</p> <ul style="list-style-type: none"> ・災害時データ復旧用を実施するデータの遠隔地保管のために可搬媒体に保存されたデータの持ち出しは、区及び委託業者共に予め相互に名簿を交換した者のみが作業を実施し、持ち出し時に施錠(鍵は区が管理し、受託業者は解錠出来ない。)を行うことで、入退室管理装置及び監視カメラを設置し、かつ、使用目的別に区画、施錠した専用の室の外において上記以外の者が当該可搬媒体を取り扱うリスクを防止する。 	<p>切なものがないか定期的に確認する手順が「情報セキュリティマネジメント実施基準」に定められおり、当該規定に基づき確認を行う。</p> <p>(特定個人情報の使用の記録)</p> <ul style="list-style-type: none"> ・システムの操作ログを保管する。ログは個人番号を参照・入力した際に個人単位で記録することとし、操作者を識別可能な一意の番号(職員番号)、操作時間、トランザクション(処理データ)名、操作端末名、操作を行っていたデータ名等を記録する。 ・保管するログは、物理的に区画・施錠された保管棚で、「杉並区文書等保存年限基準」及び「情報セキュリティマネジメント実施基準」に基づき管理する。 ・災害時データ復旧用を実施するデータの遠隔地保管のために可搬媒体の受け渡しを行う場合には「荷物搬入出記録簿」に記録する。 <p>(入退室管理)</p> <ul style="list-style-type: none"> ・不正な第三者からのアクセスを制御するため、特定個人情報を取り扱う執務室内への入退室管理について「情報セキュリティマネジメント実施基準」に規定し、規定された内容を遵守することで、権限のない者が特定個人情報を使用するリスクに対応する。 <p>(災害時データ復旧用媒体管理)</p> <ul style="list-style-type: none"> ・災害時データ復旧用を実施するデータの遠隔地保管のために可搬媒体に保存されたデータの持ち出しは、区及び委託業者共に予め相互に名簿を交換した者のみが作業を実施し、持ち出し時に施錠(鍵は区が管理し、受託業者は解錠出来ない。)を行うことで、入退室管理装置及び監視カメラを設置し、かつ、使用目的別に区画、施錠した専用の室の外において上記以外の者が当該可搬媒体を取り扱うリスクを防止する。

新		旧	
リスクへの対策は十分か	略	リスクへの対策は十分か	略
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		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	
<p>(従業者が事務外で使用するリスク対策)</p> <ul style="list-style-type: none"> ・国民年金に関する事務を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での情報収集の禁止等の指導を徹底することで、事務外の使用を防止する。 ・委託業務については、契約に基づき、委託業者が従事者に対して杉並区が定めた個人情報保護に関する教育を行い、業務外での情報収集の禁止を徹底する。区は当該教育の実施について履行確認を行う。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。 <p>(特定個人情報ファイルが不正に複製されるリスク対策)</p> <ul style="list-style-type: none"> ・情報の持ち出しについて「資源管理基準」、「庁内ネットワーク及びネットワークパソコン等利用基準」及び「情報セキュリティマネジメント実施基準」の中で規定し、職員に周知・徹底する。 ・住民情報端末においては、大量複製につながるフラッシュメモリ等の使用について、持ち出しを制限・管理するソフトウェアを導入し、USBポートからのデータ出力を不可としている。また、管理権限を付与された職員以外はOSの設定変更、ソフトウェアの変更等を行えないよう、システム上で制御する。 ・データ持ち出し時に使用する電子媒体(USBメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・バックアップ以外にファイルを複製しないよう、職員・委託先に対し指導している。 ・災害時データ復旧用に実施するデータの遠隔地保管のための可搬媒体の持ち出しについては、施錠(鍵は区が管理し、受託者は解錠出来ない)により輸送時又は保管時に開封が行われないようにすることで、外部保管時に情報が複製されるリスクを防止する。 		<p>(従業者が事務外で使用するリスク対策)</p> <ul style="list-style-type: none"> ・国民年金に関する事務を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での情報収集の禁止等の指導を徹底することで、事務外の使用を防止する。 <p>・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。</p> <p>(特定個人情報ファイルが不正に複製されるリスク対策)</p> <ul style="list-style-type: none"> ・情報の持ち出しについて「資源管理基準」、「庁内ネットワーク及びネットワークパソコン等利用基準」及び「情報セキュリティマネジメント実施基準」の中で規定し、職員に周知・徹底する。 ・住民情報端末においては、大量複製につながるフラッシュメモリ等の使用について、持ち出しを制限・管理するソフトウェアを導入し、USBポートからのデータ出力を不可としている。また、管理権限を付与された職員以外はOSの設定変更、ソフトウェアの変更等を行えないよう、システム上で制御する。 ・データ持ち出し時に使用する電子媒体(USBメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・バックアップ以外にファイルを複製しないよう、職員・委託先に対し指導している。 ・災害時データ復旧用に実施するデータの遠隔地保管のための可搬媒体の持ち出しについては、施錠(鍵は区が管理し、受託者は解錠出来ない)により輸送時又は保管時に開封が行われないようにすることで、外部保管時に情報が複製されるリスクを防止する。 	
4. 特定個人情報ファイルの取扱いの委託 []委託しない		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		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 ～	略	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 ～	略

新		旧	
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		再委託先による特定個人情報ファイルの適切な取扱いの担保	
具体的な方法	<ul style="list-style-type: none"> ・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承認した業者については再委託を許諾するとともにセキュリティ事項については委託と同様の措置を義務付けている。 ・委託先において、再委託先の特定個人情報の取扱いの監督を行っているかどうかを区で監督することにより、再委託先の特定個人情報の取扱いについても間接的に監督する。 	具体的な方法	<ul style="list-style-type: none"> ・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承認した業者については再委託を許諾するとともにセキュリティ事項については委託と同様の措置を義務付けている。
その他の措置の内容	<p>(情報保護管理体制の確認)</p> <ul style="list-style-type: none"> ・委託する際は、ISMS、プライバシーマーク等の認証取得を求めるなど、委託先の社会的信用と能力を確認する。 <p>(特定個人情報ファイルの閲覧者・更新者の制限)</p> <ul style="list-style-type: none"> ・委託先で特定個人情報ファイルの処理等に係る者を明確化するため、契約後速やかに所属・氏名等を明記した実施体制の提出を義務付けている。また、体制に変更があった場合にも、変更後の体制を速やかに提出することを義務付ける。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させるとともに、セキュリティ研修の実施を義務付ける。 ・誓約書の提出があった要員に対してのみシステムの利用者権限を与える。 ・操作権限によって画面に表示される項目及び発行する帳票は必要なもののみとする。 <p>(特定個人情報ファイルの取扱いの記録)</p> <ul style="list-style-type: none"> ・システムの操作ログを記録する。 <p>(委託元と委託先間の特定個人情報の提供)</p> <p>【システム運用業務】</p> <ul style="list-style-type: none"> ・委託先へ特定個人情報を提供した場合、その記録を行った上、受領者の確認印等により受け渡し者を明確にするための手順を定める。 ・契約で委託業務実施場所を区が管理する施設に限定し、外部への持ち出しを禁止する。但し、免除申請の継続処理に関する電磁記録媒体の交換業務に限っては、委託業務実施場所を日本年金機構が管理する施設内に限定する。 <p>【設計・運用業務】</p>	その他の措置の内容	<ul style="list-style-type: none"> ・委託する際は、ISMS、プライバシーマーク等の認証取得を求めるなど、委託先の社会的信用と能力を確認する。 ・委託先で特定個人情報ファイルの処理等に係る者を明確化するため、契約後速やかに所属・氏名等を明記した実施体制の提出を義務付けている。また、体制に変更があった場合にも、変更後の体制を速やかに提出することを義務付ける。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させるとともに、セキュリティ研修の実施を義務付ける。 ・誓約書の提出があった要員に対してのみシステムの利用者権限を与える。 ・操作権限によって画面に表示される項目及び発行する帳票は必要なもののみとする。 <ul style="list-style-type: none"> ・システムの操作ログを記録している。 <ul style="list-style-type: none"> ・契約で個人情報の持ち出し、提供の禁止を明記し、委託業務の実施場所については、区が管理する施設に限定している。但し、免除申請の継続処理に関する電磁記録媒体の交換業務に限っては日本年金機構が管理する施設内に限定している。

新		旧	
	<p>運営管理マニュアルの一つとして、情報管理ルールを定めた情報セキュリティマニュアルを策定し、その中で参照できる範囲を限定する。また、契約で外部への持ち出しを禁止する。</p> <p>(委託元と委託先間の提供された特定個人情報の消去)</p> <p>【システム運用業務】 ・業務を処理するために委託元から引き渡され、または委託先が収集し、若しくは作成した個人情報が記録されている資料等は、業務完了後、直ちに返還するものとする。ただし、委託元が特定個人情報の消去について別に指示した場合には、委託先事業者から任意の様式による消去結果に係る報告書の提出を義務付ける。</p> <p>・特定個人情報を含むデータを災害時データ復旧用として遠隔地保管を行う場合は、契約書に指定するセキュリティ要件を明確にした施設に限定する。なお、データは施錠された状況による受け渡し(鍵は区が管理し、受託業者は解錠出来ないためリスクはない。)に限定し、データ消去の委託は行わない。</p> <p>【設計・運営業務】 特定個人情報を含むデータの受け渡しは発生しないため、消去の委託は発生しない。</p> <p>(携帯電話、カメラ等の管理基準)</p> <p>【システム運用業務】 ・システム運用を行う専用の部屋では、管理基準で携帯電話、カメラ等の使用を禁止する。</p> <p>【設計・運営業務】 ・運営業務を行う執務室内では、管理基準及び情報管理ルールを定めた情報セキュリティマニュアルにより携帯電話、カメラ等の使用を禁止する。また、メモ用紙類の取扱いその他運営業務における情報管理ルールについて、情報セキュリティマニュアルに定める。</p>		<p>・特定個人情報を含むデータを災害時データ復旧用として遠隔地保管を行う場合は、契約書に指定するセキュリティ要件を明確にした施設に限定する。なお、データは施錠された状況による受け渡し(鍵は区が管理し、受託業者は解錠出来ないためリスクはない。)に限定し、データ消去の委託は行わない。</p> <p>・システム運用を行う専用の室では、管理基準で携帯電話、カメラ等の使用を禁止している。</p>
リスクへの対策は十分か	略	リスクへの対策は十分か	略
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		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	
【特記事項】 設計・運営業務の業務全般については、日報及び月報並びに履行評価により適宜、委託業務がきちんと行われているかを確認する。		—	
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。)	<input type="checkbox"/> 提供・移転しない	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。)	<input type="checkbox"/> 提供・移転しない

新	旧
<p>リスク:不正な提供・移転が行われるリスク</p> <p>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対策における措置</p> <p>(不適切な方法で、提供・移転が行われるリスク)及び(誤った相手に提供・移転してしまうリスク)</p> <ul style="list-style-type: none"> ・「介護保険伝送端末」による提供にあたっては、国保連合会所管の専用回線及びその終端である専用端末を通して提供するため、誤った相手に提供するリスクは存在しない。 ・媒体(電磁記録媒体・紙)による提供にあたっては、職員が直接、公用車により年金事務所へ搬入することで搬送事故を予防し、送付書(記録)も保管する。 <p>(誤った情報を提供・移転してしまうリスク)</p> <ul style="list-style-type: none"> ・国民年金に関する事務では、処理を行った者と点検する者を別にし、二重チェックを行うことで誤った情報・相手に情報を提供することを防止する。 ・端末は事前に登録を行っており、登録外の端末からの通信を行えない設定としている。 <p>(提供する際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 <p>6. 情報提供ネットワークシステムとの接続 <input type="checkbox"/>接続しない(入手) <input checked="" type="checkbox"/>接続しない(提供)</p> <p>7. 特定個人情報の保管・消去</p> <p>8. 監査</p> <p>9. 従業者に対する教育・啓発</p> <p>10. その他のリスク対策</p>	<p>リスク:不正な提供・移転が行われるリスク</p> <p>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対策における措置</p> <p>(不適切な方法で、提供・移転が行われるリスク)及び(誤った相手に提供・移転してしまうリスク)</p> <ul style="list-style-type: none"> ・「介護保険伝送端末」による提供にあたっては、国保連合会所管の専用回線及びその終端である専用端末を通して提供するため、誤った相手に提供するリスクは存在しない。 ・媒体(電磁記録媒体・紙)による提供にあたっては、職員が直接、公用車により年金事務所へ搬入することで搬送事故を予防し、送付書(記録)も保管する。 <p>(誤った情報を提供・移転してしまうリスク)</p> <ul style="list-style-type: none"> ・国民年金に関する事務では、処理を行った職員と点検する職員を別にし、二重チェックを行うことで誤った情報・相手に情報を提供することを防止する。 ・端末は事前に登録を行っており、登録外の端末からの通信を行えない設定としている。 <p>(提供する際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 <p>6. 情報提供ネットワークシステムとの接続 <input type="checkbox"/>接続しない(入手) <input checked="" type="checkbox"/>接続しない(提供)</p> <p>7. 特定個人情報の保管・消去</p> <p>8. 監査</p> <p>9. 従業者に対する教育・啓発</p> <p>10. その他のリスク対策</p>
<p>Ⅲリスク対策</p> <p>1. 特定個人情報ファイル名</p> <p>(5)障害基礎年金受給確認ファイル</p> <p>2. 特定個人情報の入手(情報提供ネットワークを通じた入手を除く。)</p> <p>リスク:目的外の入手が行われるリスク</p> <p>リスクに対する措置の内容</p> <ul style="list-style-type: none"> ・情報セキュリティマネジメント実施基準に基づき、情報セキュリティ教育を実施する際、対象者と無関係な情報へのアクセス、及び対象者情報であっても業務に不必要な情報へのアクセスは不正アクセスに該当し、番号法及び杉並区個人 	<p>Ⅲリスク対策</p> <p>1. 特定個人情報ファイル名</p> <p>(5)障害基礎年金受給確認ファイル</p> <p>2. 特定個人情報の入手(情報提供ネットワークを通じた入手を除く。)</p> <p>リスク:目的外の入手が行われるリスク</p> <p>リスクに対する措置の内容</p> <ul style="list-style-type: none"> ・情報セキュリティマネジメント実施基準に基づき、情報セキュリティ教育を実施する際、対象者と無関係な情報へのアクセス、及び対象者情報であっても業務に不必要な情報へのアクセスは不正アクセスに該当し、番号法及び杉並区個人

新		旧	
	<p>情報保護条例における罰則規定があること、並びに操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することでコンプライアンスの意識を高め、対象者以外の情報入手、及び必要以外の情報入手を防止している。</p> <ul style="list-style-type: none"> ・本特定個人情報ファイルのアクセスについては監査ログとして記録し、ログの確認により適正にアクセスがされているかを監視する。 ・本特定個人情報ファイルが情報を入手するにあたり、予めシステムパラメータとして「定時届事務の対象である受給コードを有する者」という抽出条件を設定した上で汎用機から出力されたものに限定することで、対象者以外の情報を入手することを防止する。 ・対象者の情報であっても入手する情報は「小型電子計算組織システム登録書」によって情報政策課に登録した記録項目に限定する。 ・ファイアウォールを設置し、システム間の接続を制御することにより、予め許可をしたシステムを除く外部のシステムからの接続が行われないよう制御する。 ・本特定個人情報ファイルを保管するフォルダは、操作を要す<u>個人番号利用事務実施者及び情報システム担当課長から権限を付与された職員のみアクセス権を設定する。</u> 		<p>情報保護条例における罰則規定があること、並びに操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することでコンプライアンスの意識を高め、対象者以外の情報入手、及び必要以外の情報入手を防止している。</p> <ul style="list-style-type: none"> ・本特定個人情報ファイルのアクセスについては監査ログとして記録し、ログの確認により適正にアクセスがされているかを監視する。 ・本特定個人情報ファイルが情報を入手するにあたり、予めシステムパラメータとして「定時届事務の対象である受給コードを有する者」という抽出条件を設定した上で汎用機から出力されたものに限定することで、対象者以外の情報を入手することを防止する。 ・対象者の情報であっても入手する情報は「小型電子計算組織システム登録書」によって情報政策課に登録した記録項目に限定する。 ・ファイアウォールを設置し、システム間の接続を制御することにより、予め許可をしたシステムを除く外部のシステムからの接続が行われないよう制御する。 ・本特定個人情報ファイルを保管するフォルダは、操作を要す職員のみアクセス権を設定する。
リスクへの対策は十分か	略	リスクへの対策は十分か	
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		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>(不適切な方法で入手が行われるリスク対策)</p> <ul style="list-style-type: none"> ・番号法及び杉並区個人情報保護条例における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・本特定個人情報ファイルを保管するフォルダは、操作を要す<u>個人番号利用事務実施者及び情報システム担当課長から権限を付与された職員のみアクセス権を設定する。</u> ・情報セキュリティマネジメント実施基準による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は、法令で定められ、杉並区情報公開・個人情報保護審議会への必要な手続きを行ったものに限定する。 ・システムの操作に当たり、操作履歴を採取し、保管することで、必要以外の情報の入手を 		<p>(不適切な方法で入手が行われるリスク対策)</p> <ul style="list-style-type: none"> ・番号法及び杉並区個人情報保護条例における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・本特定個人情報ファイルを保管するフォルダは、操作を要す職員のみアクセス権を設定する。 ・情報セキュリティマネジメント実施基準による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は、法令で定められ、杉並区情報公開・個人情報保護審議会への必要な手続きを行ったものに限定する。 ・システムの操作に当たり、操作履歴を採取し、保管することで、必要以外の情報の入手を 	

新		旧	
<p>抑止する。</p> <p>(入手した特定個人情報 that 不正確であるリスク対策)</p> <ul style="list-style-type: none"> ・杉並区に住民登録をしている者の4情報及び個人番号については、住民基本台帳に関する事務で取得したものを国民年金システムから利用するため、当該データの正確性については担保されたものとして利用する。 ・本特定個人情報ファイルが入手する情報の正確性は次のとおり確保する。 <p>国民年金ファイル(汎用機)から入手する情報・・・汎用機内のデータをシステムのバッチ処理により抽出して取り込むため、入手した情報が不正確であるリスクへの措置は(1)国民年金ファイルと同一となる。</p> <p>障害基礎年金受給確認ファイルに直接入力する情報・・・日本年金機構から提供される対象者名簿情報については、区が保有する障害基礎年金受給情報と突合して確認する。なお入力に際しては誤入力防止のために入力者と点検者を分けた2重チェックを行う。</p> <p>(入手の際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・日本年金機構から提供される対象者名簿は、職員が直接公用車で年金事務所に行き、受領することで搬送事故を予防する。 ・汎用機から特定個人情報を入手する際の手動のファイル転送は、区画された専用の室内のファイアウォールによって保護された通信経路を用いて行う。 ・端末には、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・ファイアウォールを設置し、システム間の接続を制御することにより、予め許可をしたシステムを除く外部のシステムからの接続が行われないよう制御する。 		<p>抑止する。</p> <p>(入手した特定個人情報 that 不正確であるリスク対策)</p> <ul style="list-style-type: none"> ・杉並区に住民登録をしている者の4情報及び個人番号については、住民基本台帳に関する事務で取得したものを国民年金システムから利用するため、当該データの正確性については担保されたものとして利用する。 ・本特定個人情報ファイルが入手する情報の正確性は次のとおり確保する。 <p>国民年金ファイル(汎用機)から入手する情報・・・汎用機内のデータをシステムのバッチ処理により抽出して取り込むため、入手した情報が不正確であるリスクへの措置は(1)国民年金ファイルと同一となる。</p> <p>障害基礎年金受給確認ファイルに直接入力する情報・・・日本年金機構から提供される対象者名簿情報については、区が保有する障害基礎年金受給情報と突合して確認する。なお入力に際しては誤入力防止のために入力者と点検者を分けた2重チェックを行う。</p> <p>(入手の際に特定個人情報が漏えい・紛失するリスク対策)</p> <ul style="list-style-type: none"> ・日本年金機構から提供される対象者名簿は、職員が直接公用車で年金事務所に行き、受領することで搬送事故を予防する。 ・汎用機から特定個人情報を入手する際の手動のファイル転送は、区画された専用の室内のファイアウォールによって保護された通信経路を用いて行う。 ・端末には、外部媒体へのデータ出力を制御するためのソフトウェアを導入し、データの外部媒体出力は、予め所属内で定めている管理者が当該ソフトウェアによって承認処理を行った場合にのみ可能とする。データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 ・ファイアウォールを設置し、システム間の接続を制御することにより、予め許可をしたシステムを除く外部のシステムからの接続が行われないよう制御する。 	
3. 特定個人情報の使用		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紐付けが行われるリスク		リスク1: 目的を超えた紐付け、事務に必要な情報と紐付けが行われるリスク	
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		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	略	ユーザ認証の管理	略
具体的な管理方法	略	具体的な管理方法	略

	新		
<p style="text-align: center;">その他の措置の内容</p>	<p>(機器の管理)</p> <ul style="list-style-type: none"> 退庁する際は事務処理用端末を定められたキャビネット内に施錠保管する。 情報持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。 <p>(アクセス権限の発効・失効管理)</p> <ul style="list-style-type: none"> 本特定個人情報ファイルのアクセス権限の管理は、その事務担当職員内で統括者となっている者が設定し、管理する。 <p>(特定個人情報の使用の記録)</p> <ul style="list-style-type: none"> 本特定個人情報ファイルのアクセスについては監査ログとして記録し、ログの確認により適正にアクセスがされているかを監視する。 保管するログは、物理的に区画・施錠された保管棚で、「杉並区文書等保存年限基準」及び「情報セキュリティマネジメント実施基準」に基づき管理する。 災害時データ復旧用に実施するデータの遠隔地保管のために可搬媒体の受け渡しを行う場合には「荷物搬入出記録簿」に記録する。 <p>(入退室管理)</p> <ul style="list-style-type: none"> 本特定個人情報ファイルを保存するファイルサーバは、入退室管理装置及び監視カメラが設置され、かつ、使用目的別に物理的に区画、施錠された専用の室に設置する。 <p>(災害時データ復旧用媒体管理)</p> <ul style="list-style-type: none"> 災害時データ復旧用に実施するデータの遠隔地保管のために可搬媒体に保存されたデータの持ち出しは、区及び委託業者共に予め相互に名簿を交換した者のみが作業を実施し、持ち出し時に施錠(鍵は区が管理し、受託業者は 	<p style="text-align: center;">その他の措置の内容</p>	<p style="text-align: center;">旧</p>

新		旧	
	<p>解錠出来ない。)を行う。また入退室管理装置及び監視カメラを設置することで上記以外の者が当該可搬媒体を取り扱うリスクを防止する。</p> <p>(情報の持ち出し及び外部媒体の管理)</p> <p>・事務処理用端末ではフラッシュメモリその他の外部媒体への情報の出力を制御するソフトウェアを導入することにより、外部媒体を用いて情報の持ち出しを行う際には、情報持ち出しにかかる管理者の承認を必要とする。</p>		<p>解錠出来ない。)を行う。また入退室管理装置及び監視カメラを設置することで上記以外の者が当該可搬媒体を取り扱うリスクを防止する。</p> <p>(情報の持ち出し及び外部媒体の管理)</p> <p>・事務処理用端末ではフラッシュメモリその他の外部媒体への情報の出力を制御するソフトウェアを導入することにより、外部媒体を用いて情報の持ち出しを行う際には、情報持ち出しにかかる管理者の承認を必要とする。</p>
リスクへの対策は十分か	略	リスクへの対策は十分か	略
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		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	
略		略	
4. 特定個人情報ファイルの取扱いの委託 []委託しない		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		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 ～ 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	略	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 ～ 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	略
具体的な方法	<p>・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承認した業者については再委託を許諾するとともにセキュリティ事項については委託と同様の措置を義務付けている。</p> <p>・委託先において、再委託先の特定個人情報の取扱いの監督を行っているかどうかを区で監督することにより、再委託先の特定個人情報の取扱いについても間接的に監督する。</p>	具体的な方法	<p>・原則として再委託は行わないが、再委託に関する承認申請書により、再委託理由等を明確にし、区が承認した業者については再委託を許諾するとともにセキュリティ事項については委託と同様の措置を義務付けている。</p>
その他の措置の内容	<p>(情報管理体制の確認)</p> <p>・委託する際は、ISMS、プライバシーマーク等の認証取得を求めるなど、委託先の社会的信用と能力を確認する。</p> <p>(ユーザ認証の管理)</p> <p>【システム運用業務】</p>	その他の措置の内容	<p>(情報管理体制の確認)</p> <p>・委託する際は、ISMS、プライバシーマーク等の認証取得を求めるなど、委託先の社会的信用と能力を確認する。</p> <p>(ユーザ認証の管理)</p> <p>・運用保守業務でサーバの操作が必要な場合は、業務の</p>

新	旧
<p>・運用保守業務でサーバの操作が必要な場合は、業務の都度、情報政策課からユーザ ID とパスワードの払出を委託先へ行い、運用保守業務の作業以外はサーバの操作ができない運用とする。</p> <p>【設計運用業務】</p> <p>・<u>端末機の事前登録(端末認証)を行い、ユーザID・パスワードによる認証を行う。また、パスワードは「資源管理基準」、「庁内ネットワーク及びネットワークパソコン等利用基準」に定められた期間内に変更する。</u></p> <p>・<u>登録されているユーザ情報については、管理権限を付与された職員が定期的に確認し、記録に残す。</u></p> <p>・<u>各システム共にユーザIDの共有を禁止している。</u></p> <p>(委託元と委託先間の特定個人情報の提供)</p> <p>【システム運用業務】</p> <p>・<u>委託先へ特定個人情報を提供した場合、その記録を行った上、受領者の確認印等により受け渡し者を明確にするための手順を定める。</u></p> <p>・<u>契約で委託業務実施場所を区が管理する施設に限定し、外部への持ち出しを禁止する。</u></p> <p>【設計運用業務】</p> <p>・<u>運営管理マニュアルの一つとして、情報管理ルールを定めた情報セキュリティマニュアルを策定し、その中で参照できる範囲を限定する。また、契約で外部への持ち出しを禁止する。</u></p> <p>(ログによる監視)</p> <p>【システム運用業務】</p> <p>・<u>運用保守業務以外でのアクセス等の不正アクセスが行われていないかを操作ログの確認により監視する。</u></p> <p>【設計運用業務】</p> <p>・<u>システムの操作ログを保管する。ログは個人番号を参照・入力した際に個人単位で記録することとし、操作者を識別可能な一意の番号、操作時間、トランザクション(処理データ)名、操作端末名、操作を行っていたデータ名等を記録する。</u></p> <p>・<u>保管するログは、物理的に区画・施錠された保管棚で、「杉並区文書等保存年限基準」及び「情報セキュリティマネジメント実施基準」に基づき管理する。</u></p> <p>(携帯電話、カメラ等の管理基準)</p>	<p>都度、情報政策課からユーザ ID とパスワードの払出を委託先へ行い、運用保守業務の作業以外はサーバの操作ができない運用とする。</p> <p>(情報の持ち出し)</p> <p>・<u>契約で個人情報の持ち出しを認めない。</u></p> <p>(ログによる監視)</p> <p>・<u>運用保守業務以外でのアクセス等の不正アクセスが行われていないかを操作ログの確認により監視する。</u></p>

新		旧	
	<p>【システム運用業務】 システム運用を行う専用の部屋では、管理基準で携帯電話、カメラ等の使用を禁止する。</p> <p>【設計運営業務】 ・運営業務を行う執務室内では、管理基準及び情報管理ルールを定めた情報セキュリティマニュアルにより携帯電話、カメラ等の使用を禁止する。また、メモ用紙類の取扱いその他運営業務における情報管理ルールについて、情報セキュリティマニュアルに定める。</p> <p>(委託元と委託先間の提供された特定個人情報の消去)</p> <p>【システム運用業務】 ・業務を処理するために委託元から引き渡され、または委託先が収集し、若しくは作成した個人情報が記録されている資料等は、業務完了後、直ちに返還するものとする。ただし、委託元が特定個人情報の消去について別に指示した場合には、委託先事業者から任意の様式による消去結果に係る報告書の提出を義務付けている。</p> <p>・特定個人情報を含むデータを災害時データ復旧用として遠隔地保管を行う場合は、契約書に指定するセキュリティ要件を明確にした施設に限定する。なお、データは施錠された状況による受け渡し(鍵は区が管理し、受託業者は解錠出来ないためリスクはない。)に限定し、データ消去の委託は行わない。</p> <p>【設計・運営業務】 ・特定個人情報を含むデータの受け渡しは発生しないため、消去の委託は発生しない。</p>		<p>(災害用データの保管)</p> <p>・特定個人情報を含むデータを災害時データ復旧用として遠隔地保管を行う場合は、契約書に指定するセキュリティ要件を明確にした施設に限定する。なお、データは施錠された状況による受け渡し(鍵は区が管理し、受託業者は解錠出来ないためリスクはない。)に限定し、データ消去の委託は行わない。</p>
リスクへの対策は十分か	略	リスクへの対策は十分か	略
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		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	
【特記事項】 設計・運営業務の業務全般については、日報及び月報並びに履行評価により適宜、委託業務がきちんと行われているかを確認する。		—	
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。)	<input type="checkbox"/> 提供・移転しない	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。)	<input type="checkbox"/> 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		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(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。)		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		におけるその他のリスク及びそのリスクに対する措置	
(不適切な方法で提供・移転が行われるリスク対策)		(不適切な方法で提供・移転が行われるリスク対策)	
・媒体(紙)による提供にあたっては、職員が直接、公用車により年金事務所に搬入することで搬送事故を予防しており、送付書(記録)も保管している。		・媒体(紙)による提供にあたっては、職員が直接、公用車により年金事務所に搬入することで搬送事故を予防しており、送付書(記録)も保管している。	

新	旧																				
<p>(提供する際に特定個人情報が漏えい・紛失するリスク対策) ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。</p> <p>(誤った情報を提供・移転してしまうリスク対策) ・日本年金機構への提供にあたっては、事前に日本年金機構から送付される対象者名簿と提供を行う情報について個人番号利用事務実施者による2重チェックで照合する。</p> <p>6. 情報提供ネットワークシステムとの接続 <input type="radio"/>接続しない(入手) <input type="radio"/>接続しない(提供)</p> <p>7. 特定個人情報の保管・消去</p> <p>8. 監査</p> <p>9. 従業者に対する教育・啓発</p> <p>10. その他のリスク対策</p>	<p>(提供する際に特定個人情報が漏えい・紛失するリスク対策) ・データ持ち出し時に使用する電子媒体(フラッシュメモリ)は、施錠管理する保管場所に保管し、持出管理を行い、記録データについては、処理後直ちに消去し、消去したことを複数名で確認する。</p> <p>(誤った情報を提供・移転してしまうリスク対策) ・日本年金機構への提供にあたっては、事前に日本年金機構から送付される対象者名簿と提供を行う情報について職員による2重チェックで照合する。</p> <p>6. 情報提供ネットワークシステムとの接続 <input type="radio"/>接続しない(入手) <input type="radio"/>接続しない(提供)</p> <p>7. 特定個人情報の保管・消去</p> <p>8. 監査</p> <p>9. 従業者に対する教育・啓発</p> <p>10. その他のリスク対策</p>																				
<p>IV 開示請求、問合せ</p>	<p>IV 開示請求、問合せ</p>																				
<table border="1"> <tr> <td colspan="2" data-bbox="190 754 1108 794">1. 特定個人情報の開示・訂正・利用停止請求</td> </tr> <tr> <td data-bbox="190 798 492 911">① 請求先</td> <td data-bbox="497 798 1108 911">郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区総務部情報政策課情報公開係</td> </tr> <tr> <td data-bbox="190 914 492 1027">② 請求方法～ ④ 個人情報ファイル簿への不記載等</td> <td data-bbox="497 914 1108 1027">略</td> </tr> <tr> <td colspan="2" data-bbox="190 1031 1108 1070">2. 特定個人情報ファイルの取扱いに関する問合せ</td> </tr> <tr> <td colspan="2" data-bbox="190 1074 1108 1106">略</td> </tr> </table>	1. 特定個人情報の開示・訂正・利用停止請求		① 請求先	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区総務部情報政策課情報公開係	② 請求方法～ ④ 個人情報ファイル簿への不記載等	略	2. 特定個人情報ファイルの取扱いに関する問合せ		略		<table border="1"> <tr> <td colspan="2" data-bbox="1180 754 2087 794">1. 特定個人情報の開示・訂正・利用停止請求</td> </tr> <tr> <td data-bbox="1180 798 1482 911">① 請求先</td> <td data-bbox="1487 798 2087 911">郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報政策課情報公開係</td> </tr> <tr> <td data-bbox="1180 914 1482 1027">② 請求方法～ ④ 個人情報ファイル簿への不記載等</td> <td data-bbox="1487 914 2087 1027">略</td> </tr> <tr> <td colspan="2" data-bbox="1180 1031 2087 1070">2. 特定個人情報ファイルの取扱いに関する問合せ</td> </tr> <tr> <td colspan="2" data-bbox="1180 1074 2087 1106">略</td> </tr> </table>	1. 特定個人情報の開示・訂正・利用停止請求		① 請求先	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報政策課情報公開係	② 請求方法～ ④ 個人情報ファイル簿への不記載等	略	2. 特定個人情報ファイルの取扱いに関する問合せ		略	
1. 特定個人情報の開示・訂正・利用停止請求																					
① 請求先	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区総務部情報政策課情報公開係																				
② 請求方法～ ④ 個人情報ファイル簿への不記載等	略																				
2. 特定個人情報ファイルの取扱いに関する問合せ																					
略																					
1. 特定個人情報の開示・訂正・利用停止請求																					
① 請求先	郵便番号166-8570 東京都杉並区阿佐谷南1-15-1 杉並区政策経営部情報政策課情報公開係																				
② 請求方法～ ④ 個人情報ファイル簿への不記載等	略																				
2. 特定個人情報ファイルの取扱いに関する問合せ																					
略																					
<p>V 評価実施手続 略</p>	<p>V 評価実施手続 略</p>																				