別記第4号様式の2（第4条関係） 評価補足シート

【全項目評価書版】							
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム	

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類	措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
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							
－	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1：目的外の入手が行われるリスク						
1	対象者以外の情報の入手を防止するための措置の内容	対象者以外の特定個人情報の入手を防止するための措置を講じること	【措置の内容】	システム以外：窓口において、届書・申請書等の内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報が入手されない（本人及び世帯員以外の情報が含まれていないかを確認する）ように業務ルールを定めており、ルールに従って業務を行っている。 システム：区民情報系基盤システムとの連携においては、宛名番号をキーとして連携することで確実に対象を特定した連携を行い、対象者以外の個人情報の入手を禁止する。		十分である	①特定個人情報を目的外で入手することが大田区個人情報保護条例で禁じられている。 ②ルール・手続き等が定められており、かつ、業務がそれにしたがって運用されている。 ③システムで実装している機能等が仕様設計書等で確認することができる。 以上より、「十分である」と評価した。
2	必要な情報以外を入手することを防止するための措置の内容	特定個人情報のうち、必要な情報以外を入手することを防止するための措置を講じること	【措置の内容】	システム以外：①個人情報を収集するときは、個人情報を取り扱う事務の目的を明確にし、当該事務の目的を達成するために必要かつ最小限の範囲内で、適法かつ公正な手段によって収集しなければならない旨のルールを定めており、ルールに従って業務を行っている。 ②業務上必要のない情報や保持を許可されていない情報を収集・記録してはならない旨のルールを設けており、ルールに従って業務を行っている。 ③本人が必要な情報以外を誤って記載することがないような様式（書面）を使用している。また、記載要領・記載例の提示等により、不要な情報の記載を排除している。 システム：①国民年金システムにおいて必要な情報項目のみで構成したデータ様式とし、区民情報系基盤システムから必要な情報項目以外を入手できない設計としている。 ②個人・所属グループ（課・係等）単位で利用できるシステムメニューを設定しており、業務で必要としない情報を利用できないよう制御している。			
3	その他の措置の内容	－	【措置の内容】	－	個人情報の取扱に対する意識強化のために、年に1回以上、区全体及び課内でセキュリティ研修を実施している。		
－	リスク2：不適切な方法で入手が行われるリスク						
4	リスクに対する措置の内容	不適切な方法で特定個人情報の入手が行われるリスクに対する措置を講じること	【措置の内容】	システム以外：①書面による届書・申請書等受領の際には必ず本人又は代理人の本人確認を行ったうえで受領するルールを定めている。 ②業務上必要のない情報を収集してはならない旨のルールが定められており、これを厳守し業務上必要な場合に限り特定個人情報を入手している。 ③不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。 システム：①個人・所属グループ（課・係等）単位で利用できるシステムメニューを設定しており、業務で必要としない情報を利用できないよう制御している。 ②個人・操作端末単位で操作ログを取得している。		十分である	①特定個人情報の入手は適切な方法で必要最小限度で行う旨のルール・手続き等が定められており、かつ、業務がそれにしたがって運用されている。 ②システム管理者が運用状況を監視することで、不正アクセスを防止している。 以上より、「十分である」と評価した。

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】							
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム	

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	リスク3：入手した特定個人情報が不正確であるリスク							
5	入手の際の本人確認の措置の内容	特定個人情報を入手する際の本人確認措置を講じること	【措置の内容】	システム以外	届書・申請書等の受付の際、個人番号カード、運転免許証または旅券等の身元確認書類の提示を求め確実な本人確認を行っている。		十分である	①本人確認方法は、あらかじめ定められた方法で行うルールを定めている。 ②ルール・手続き等が定められており、かつ、業務がそれにしたがって運用されている。 ③システム上も特定個人情報の不正取得・改竄を防止する機能が備わっている。 以上より、「十分である」と評価した。
6	個人番号の真正性確認の措置の内容	入手した個人番号が本人の個人番号で間違いないことを確認する措置を講じること	【措置の内容】	システム以外	届書・申請書等に添えて、個人番号カード又は個人番号が記載された住民票の写し等の番号確認書類及び運転免許証又は旅券等の身元（実存）確認書類が提出されたときは、届書・申請書等にその旨を記入する。			
				システム	「システム以外」で記載した措置により個人番号の真正性を確認する。			
7	特定個人情報の正確性確保の措置の内容	特定個人情報の正確性確保の措置を講じること	【措置の内容】	システム以外	①届書・申請書等の受理において必要な情報が記載されているか等を確認するルールを設けている。 ②情報が不正に改ざんされないよう、申請書・届出書・電子媒体等は施錠できる保管庫に格納している。 ③不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。			
				システム	①特定個人情報はシステム内のデータベースに格納され、当該データベースへのアクセス方法はシステム管理者以外は知り得ない。 ②個人・操作端末単位で操作ログを取得している。			
8	・その他の措置の内容	－	【措置の内容】	－	－			
－	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							
9	リスクに対する措置の内容	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を講じること	【措置の内容】	システム以外	①届書・申請書・電子媒体等を机上に放置しない等適切な管理を行い、開庁時以外は施錠できる保管庫に格納している。 ②事務処理の中で発生する個人情報を含む帳票類については、担当者が内容を確認しながら他の帳票類と区分し、不要になったタイミングで速やかにシュレッダーで裁断している。 ③区は窓口等で区民より受領する届書・申請書等情報の他に日本年金機構から還元される処理結果情報を電子記録媒体及び紙媒体により入手する。これらを入手する際は、週１回程度担当職員が公用車で日本年金機構に出向き施錠可能なトランクに格納して区に持ち帰るか、もしくは日本年金機構が簡易書留等で区に郵送する。なお、入手した情報は指定の回付票等で管理する。 ④不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。		十分である	①漏えい・紛失ををを防止するための手順が情報セキュリティ実施手順に定められている。 ②業務が上記手順に基づき実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	①システムユーザは限定されており、システム利用までに端末のWindows認証、システムのユーザ認証が必要となっている。 ②システムを利用できる端末は限定されている。 ③個人・操作端末単位で操作ログを取得している。 ④特定個人情報はシステム内のデータベースに格納され、当該データベースへの接続方法はシステム管理者以外は知り得ない。このため当該情報をデータベースから入手することはシステム管理者以外は不可能となっている。 ⑤システムと操作端末間の通信は暗号化されている。			
－	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							
10	リスクに対する措置の内容	－	【措置の内容】	－	－			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】						
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	3．特定個人情報の使用							
－	リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク							
11	宛名システム等における措置の内容	宛名システム等における、目的を超えた紐付け、事務に必要ない情報との紐付けが行われるリスクに対する措置を講じること	【措置の内容】	システム以外	①システム及び電子記録媒体に保持する情報項目は大田区情報公開・個人情報保護審議会に意見聴取を行い決定している。 ②個人情報を収集するときは、個人情報を取り扱う事務の目的を明確にし、当該事務の目的を達成するために必要かつ最小限の範囲内で、適法かつ公正な手段によって収集しなければならない旨のルールを定めており、ルールに従って業務を行っている。 ③業務上必要のない情報や、保持を許可されていない情報を収集、記録してはならない旨のルールを定めており、ルールに従って業務を行っている。 ④不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。		十分である	①大田区情報公開・個人情報保護審議会での承認を得ないと情報の紐付けを実施することはできない。 ②大田区個人情報保護条例により業務外の利用が禁じられている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	①区民情報系基盤システムより入手している情報項目は必要最小限の項目に限定されており、連携ファイルレイアウトにない項目は連携されない(システムに提供されない)。規定された項目以外を連携しようとした場合も、システムは必要な項目のみ取り込みを行い、それ以外を取り込まない。 ②新たな項目を紐付しようとした場合でも、国民年金システムのデータベース領域を拡張することはシステム管理者でなければ実施できないため、業務で必要としない情報項目をデータベースに追加することはできない。 ③システム管理者権限で直接コンソールに接続しシステムの操作を行った場合においても、個人･操作端末単位で操作ログを取得している。			
12	事務で使用するその他のシステムにおける措置の内容	事務で使用するその他のシステムにおける、目的を超えた紐付け、事務に必要ない情報との紐付けが行われるリスクに対する措置を講じること	【措置の内容】	システム以外	①他部署にて管理しているシステムの利用において、業務に関係のない情報の検索、閲覧、利用を禁止するルールを定めており、ルールに従って業務を行っている。 ②他部署にて管理しているシステム内で保持している情報を新たに業務で利用する場合、大田区情報公開・個人情報保護審議会に意見聴取を行う。 ③他部署にて管理しているシステムを利用する職員は、必要最小限の人数としている。また利用にあたっては、他部署へ法律に基づいた申請を行うことが条件となっており、これに基づいて許可・不許可のシステム設定がなされる運用となっている。			
				システム	参照できる情報項目は他部署でシステム的に制限されており、法律に基づき業務上必要最小限の情報のみ参照できるよう閲覧制限を課せられている。			
13	その他の措置の内容	－	【措置の内容】	－	－			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】								
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル		システム名称	国民年金システム	

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	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							
14	ユーザ認証の管理	ユーザ認証の管理を実施すること	【具体的な管理方法】	システム以外	①生体情報の登録、ユーザID・パスワードの適切な管理について、パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する等の運用ルールが定められており、ルールに従って業務を行っている。 ②なりすましによる不正を防止する観点から、共用IDの発行は禁止している。 ③ログインしたまま端末を放置せず、離席時には画面ロックまたはログアウトすることやパスワードの使いまわしをしないことを徹底している。	行っている	十分である	①権限のない者の不正利用防止のための手順が情報セキュリティ対策基準に定められている。 ②業務が上記手順に基づき実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	①システム認証は、庁内認証基盤とのシングルサインオン認証となっている。 ②端末の認証は、二要素認証（ID・パスワード、生体情報）による。 ③国民年金システム上でユーザIDの利用権限等を管理する機能を有している。 ④認証を複数回失敗すると、自動でアカウントロック機能が作動する。			
15	アクセス権限の発効・失効の管理	アクセス権限の発効・失効の管理を実施すること	【具体的な管理方法】	システム以外	①システムへのアクセス権限の発効・変更・失効は、システム管理者以外は実施しない運用としている。 ②利用する職員に変更が発生した場合、申請書により所定の審査・承認を経てアクセス権限を発効・変更するルールを定めており、ルールに従って業務を行っている。 ③アクセス権限の失効は、システム管理者にて人事異動時及び定期的に確認を行い、必要の無いIDを速やかに削除する手順を設けている。	行っている		
				システム	個人・所属グループ(課・係等)単位でアクセス権限を発効・失効する機能を設けており、アクセス権限の発効・失効を行う職員(システム管理者)を限定している。			
16	アクセス権限の管理	アクセス権限の管理を実施すること	【具体的な管理方法】	システム以外	①システム管理者が人事異動時及び定期的に確認を行い、必要の無いIDを削除する手順を定めている。 ②アクセス権限は業務上必要な最小限の範囲で、設定するルールを定めており、ルールに従って業務を行っている。 ③不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。	行っている		
				システム	①個人・操作端末単位で操作ログを取得している。 ②システム管理者は、システムのオンライン画面上でどのユーザにどの権限が付与されているかを確認及び変更することができる。			
17	特定個人情報の使用の記録	特定個人情報の使用の記録を実施すること	【具体的な方法】	システム以外	不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。	記録を残している		
				システム	①個人・操作端末単位で操作ログを取得している。 ②当該記録については、長期間保存することとしている。			
18	その他措置の内容	－	【措置の内容】	－	－			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】							
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム	

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類	措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	**リスク3：従業者が事務外で使用するリスク**						
19	リスクに対する措置の内容	従業者が事務外で特定個人情報を使用するリスクに対する措置を講じること	【措置の内容】	システム以外：①条例で事務の目的以外で特定個人情報を利用してはならないことを定めている。 ②不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。 システム：個人･操作端末単位で操作ログを取得している。		十分である	①特定個人情報を目的外で利用することが大田区個人情報の保護に関する法律施行条例施行規則で禁じられている。 ②ルール・手続き等が定められており、かつ、操作履歴確認作業等の業務がそれにしたがって実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
－	**リスク4：特定個人情報ファイルが不正に複製されるリスク**						
20	リスクに対する措置の内容	特定個人情報ファイルが不正に複製されるリスクに対する措置を講じること	【措置の内容】	システム以外：①システムに記録されている個人情報等のデータについて、改ざんや業務目的以外のコピーを禁止するルールを定めており、ルールに従って業務を行っている。 ②委託先事業者が個人情報及び機密情報を適正に取り扱うために、委託契約仕様書に当該情報の取扱いに係る条項(個人情報の複製の禁止、委託業務終了時の個人情報の消去･返還等)を別途定めている。 ③外部記憶媒体にデータをコピーする場合、管理者の許可を得るルール及び手順を定めており、ルールに従って業務を行っている。 ④不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。 システム：①端末からデータ(ファイル等)の外部記憶媒体等への書き出しは、使用を許可された外部記憶媒体にのみ行うことができる。 ②個人･操作端末単位で操作ログを取得している。		十分である	①特定個人情報を不正に複製することが大田区が取り扱う個人情報、個人番号及び特定個人情報の管理に関する規程で禁じられている。 ②ルール・手続き等が定められており、かつ、操作履歴確認作業等の業務がそれにしたがって実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
－	**特定個人情報の使用におけるその他のリスク**						
21	リスクに対する措置の内容	－	【措置の内容】	システム：－			

別記第4号様式の2（第4条関係） 評価補足シート

【全項目評価書版】							
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム	

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	4．特定個人情報ファイルの取扱いの委託							
－	委託先による特定個人情報の不正入手・不正な使用に関するリスク委託先による特定個人情報の不正な提供に関するリスク委託先による特定個人情報の保管・消去に関するリスク委託契約終了後の不正な使用等のリスク再委託に関するリスク							
22	情報保護管理体制の確認	委託先における情報保護管理体制の確認を行うこと	【確認方法】	システム以外	①個人情報の取扱いに関与する委託先にはプライバシーマークの取得、ISMS認証取得の要件を満たすか確認している。 ②個人情報の取扱いに関与する委託契約時には、「個人情報及び機密情報の取扱いに関する付帯条項」を添付し、「情報セキュリティ体制の報告、責任者等の特定、定期及び事故発生時の報告」について明記した契約を締結している。 ③委託契約中は、定期及び事故発生時の報告を受け、情報保護管理体制を確認している。 ④委託先事業者との定例会を1か月に1回開催しており、その中で問題と改善案を検討し、決定した改善方法により業務を運用している。		十分である	①個人情報を取り扱う委託契約締結時に必ず「個人情報及び機密情報の取扱いに関する付帯条項」を契約仕様書に付すことが義務付けられている。 ②ルール・手続き等が定められており、かつ、操作履歴確認作業等の業務がそれにしたがって実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。
23	特定個人情報ファイルの閲覧者・更新者の制限	委託先における特定個人情報ファイルの閲覧者・更新者の制限を行うこと	【具体的な制限方法】	システム以外	①委託契約書において、委託先の要員名簿の提出と変更時における報告・更新を義務付けている。 ②システムへのアクセス権限の追加及び変更は、申請書により所定の審査・承認を経てユーザIDを付与している。 ③システムへのアクセス権限の追加及び変更は、システム管理者以外は設定することができない。 ④システムの利用には生体認証を用いたうえで要員ごとにユーザIDと紐付を行い、利用状況を確認し不正なID利用が無いように監視している。 ⑤委託事業者に付与する権限は業務上必要最小限の権限を割り当てている。 ⑥不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。	制限している		
				システム	個人・所属グループ(課・係等)単位でアクセス権限を発効・失効する機能を設けており、アクセス権限の発効・失効を行う職員を限定している。			
24	特定個人情報ファイルの取扱いの記録	委託先における特定個人情報ファイルの取扱いの記録を行うこと	【具体的な方法】	システム以外	不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。	記録を残している		
				システム	個人・操作端末単位で操作ログを取得している。 操作ログは長期間保存される。			
25	特定個人情報の提供ルール（委託先から他者への提供に関するルールの内容及びルール遵守の確認方法）	特定個人情報ファイルの提供ルールを設けること（委託先から他者への提供に関するルールの内容及びルール遵守の確認方法）	【確認方法】	システム以外	①委託先から外部委託先を除く他社への提供の禁止を契約書に明記している。 ②委託先は定期的に個人情報及び機密情報の管理状況について報告すること及び委託者の監査・調査に応じることが義務図けられている。			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】						
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
26	特定個人情報の提供ルール（委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法）	特定個人情報ファイルの提供ルールを設けること（委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法）を設けること	【確認方法】	システム以外	委託先に以下を義務付けている。 ①大田区から提供を受けた特定個人情報データの外部持ち出しの禁止 ②作業終了後に大田区から提供を受けた特定個人情報データを適正に返却・消去すること ③大田区から提供を受けた特定個人情報データの目的外利用の禁止 ④大田区から提供を受けた特定個人情報データの複写及び複製の禁止 大田区で以下の運用ルールを定めている。 ⑤システム保守事業者等が個人情報データを庁内から外部に持ち出す場合は、「外部持ち出し申請書」によりセキュリティ管理者の承認を得なければならない。 ⑥外部記憶媒体を用いて大田区と委託先事業者との間で個人情報の受け渡しを行う場合、「メディア受け渡し票」により外部記憶媒体の受け渡し履歴を記録する。 以下の方法で確認を行っている ⑦委託先による定期的に個人情報及び機密情報の管理状況についての定期報告及び監査・調査の実施 ⑧②⑤⑥については、委託先より提出された各種申請書等及び廃棄証明書の点検	定めている		以上より、「十分である」と評価した。

【全項目評価書版】								
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル		システム名称	国民年金システム	
項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
27	特定個人情報の消去ルールの内容及びルール遵守の確認方法	委託先における特定個人情報の消去ルールの内容及びルール遵守の確認方法を定めること	【確認方法】	システム以外	委託先に以下を義務付けている。 ①作業終了後に大田区から提供を受けた特定個人情報データを適正に返却・消去すること ②データ消去をした場合は、データ消去報告書を提出すること	定めている		
28	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	委託契約書において特定個人情報ファイルの取扱いに関する規定を定めること	【規定の内容】	システム以外	委託先に以下を義務付けている。 ①大田区から提供を受けた特定個人情報データの外部持ち出しの禁止 ②作業終了後に大田区から提供を受けた特定個人情報データを適正に返却・消去すること ③大田区から提供を受けた特定個人情報データの目的外利用・第三者への提供の禁止 ④大田区から提供を受けた特定個人情報データの複写及び複製の禁止 ⑤個人情報を取り扱う従業者を特定し、報告すること	定めている		
29	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確保	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確保を実施すること	【具体的な方法】	システム以外	委託先事業者に以下を義務付けている。 ①再委託の原則禁止 ②やむを得ず再委託を実施する場合の手続き ③再委託先は受託者と同様の義務・責任を負うこと ④受託者は再委託先の履行について自ら業務を遂行した場合と 同様の責任を負い、必要かつ適切な監督を行うこと	十分に行っている		
30	その他の措置の内容	－	【措置の内容】	－	－			
－	**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**							
31	リスクに対する措置の内容	－	【措置の内容】	－	－			
－	**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。）**							
－	**リスク1：不正な提供・移転が行われるリスク**							
32	特定個人情報の提供・移転の記録	特定個人情報の提供・移転の記録を行うこと	【具体的な方法】	システム以外	①他部署からデータ抽出などの電算処理の依頼がある場合、所定の様式による申請受理後、内容を精査し承認するルールが定められている。 ②日本年金機構へ電子記録媒体及び紙媒体により特定個人情報を提供する際は、指定の回付票で管理する。	記録を残している	十分である	①番号法第19条・条例(移転)・大田区電子計算組織管理運営規則により、特定個人情報の提供・移転の記録及びその確認方法(手続き)が明文化されている。 ②システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	「システム以外」で記載した措置により記録を行っている。			
33	特定個人情報の提供・移転に関するルールの内容及びルール遵守の確認方法	特定個人情報の提供・移転に関するルールの内容及びルール遵守の確認方法を定めること	【確認方法】	システム以外	①他システムとの接続及び特定個人情報の提供・移転をする場合は大田区情報公開・個人情報保護審議会へ事前に報告し、意見聴取するルールが定められており、ルールに従って業務を行っている。 ②他部署からデータ抽出等の電算処理の依頼があった場合、所定の様式による申請・承認手続を経なければならないルールを定めており、ルールに従って業務を行っている。 ③上記②は、番号法第9条又は第19条に基づいて、承認手続きが行われる。 ④ルールの遵守状況は定期的な自己点検により確認する。	定めている		
34	その他の措置の内容	－	【措置の内容】	－	－			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】							
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム	

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	リスク2：不適切な方法で提供・移転が行われるリスク							
35	リスクに対する措置の内容	不適切な方法で特定個人情報の提供・移転が行われるリスクに対する措置を講じること	【措置の内容】	システム以外	①他部署からデータ抽出などの電算処理の依頼がある場合、所定の様式による申請受理後、内容を精査し承認するルールが定められている。 ②日本年金機構への特定個人情報の提供は下記の方法による。 提供する電子データファイルは、日本年金機構の作成仕様に基づく電子政府推奨暗号化形式で暗号化を施し、所定のルールに基づいたパスワードを付したZIP形式ファイルとする。なお、区及び日本年金機構の双方において暗号鍵の管理を適正に行う。 提供する電子データファイルは、電子記録媒体（CDまたはDVD）に保存し、それを施錠可能なトランクに格納して担当職員が公用車で週1回程度運搬を行う。 提供する紙媒体は、施錠可能なトランクに格納して担当職員が公用車で週1回程度運搬を行うか、もしくは、簡易書留による郵送により行う。 提供する電子記録媒体及び紙媒体は、指定の回付票等で管理する。なお、電子記録媒体及び紙媒体は鍵のかかる書庫で適切に保管管理を行う。		十分である	①情報セキュリティ実施手順により、特定個人情報の提供・移転時の確認方法（手続き）が明文化されている。 ②システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	「システム以外」で記載した方法により措置を行っている。			
－	リスク3：誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク							
36	リスクに対する措置の内容	誤った特定個人情報を提供・移転してしまうリスクおよび誤った相手に特定個人情報を提供・移転するリスクに対する措置を講じること	【措置の内容】	システム以外	①他システムと接続する場合、大田区情報公開・個人情報保護審議会へ事前に意見聴取を行っている。 ②届書・申請書等受付時及び国民年金システムに登録時にダブルチェックを実施した情報を日本年金機構へ提供している。		十分である	①大田区情報公開・個人情報保護審議会条例第2条（2）及び国民年金係資格事務マニュアルにより、特定個人情報の提供・移転先及び提供する情報の内容の確認方法（手続き）が明文化されている。 ②システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	国民年金システムと区民情報系基盤システムとのデータ連携は、地方公共団体情報システムデータ要件・連携要件標準仕様書に定められた項目により行う。			
－	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							
37	リスクに対する措置の内容	－	【措置の内容】	－	－			

【全項目評価書版】						
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類	措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	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						
38	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、目的外の特定個人情報の入手が行われるリスクに対する措置を講じること	【措置の内容】	システム以外 システム			
－	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						
39	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、安全が保たれない方法によって特定個人情報の入手が行われるリスクに対する措置を講じること	【措置の内容】	システム以外 システム			
－	リスク3：入手した特定個人情報が不正確であるリスク						
40	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、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を講じること	【措置の内容】	システム以外 システム			
－	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						
41	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、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を講じること	【措置の内容】	システム以外 システム			
－	リスク5：不正な提供が行われるリスク						
42	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、特定個人情報の不正な提供が行われるリスクに対する措置を講じること	【措置の内容】	システム以外 システム			
－	リスク6：不適切な方法で提供されるリスク						
43	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、不適切な方法で特定個人情報が提供されるリスクに対する措置を講じること	【措置の内容】	システム以外 システム			
－	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						
44	リスクに対する措置の内容	情報提供ネットワークシステムとの接続において、誤った特定個人情報を提供してしまうリスク、誤った相手に特定個人情報を提供してしまうリスクに対する措置を講じること	【措置の内容】	システム以外 システム			
－	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						
45	リスクに対する措置の内容	－	【措置の内容】	－			

別記第4号様式の2（第4条関係） 評価補足シート

【全項目評価書版】								
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル		システム名称	国民年金システム	
項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
－	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							
46	①NISC政府機関統一基準群	N/A				政府機関ではない		
47	②安全管理体制	特定個人情報の漏えい・滅失・毀損リスクに対する安全管理体制を構築すること	【整備状況】	システム以外	情報セキュリティ管理体制について各責任者および担当者を定めている。	十分に整備している	十分である	①特定個人情報の漏えい・滅失・毀損防止のための手順が情報セキュリティ対策基準に定められている。 ②業務が上記手順に基づき実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
48	③安全管理規程	特定個人情報の漏えい・滅失・毀損リスクに対する安全管理規程を整備すること	【整備状況】	システム以外	情報セキュリティの手順文書において、次の事項を規定している。 ①情報資産の分類と管理 ②人的な情報セキュリティ対策 ③物理的な情報セキュリティ対策 ④技術的な情報セキュリティ対策 ⑤運用におけるセキュリティ対策	十分に整備している		
49	④安全管理体制・規程の職員への周知	特定個人情報の漏えい・滅失・毀損リスクに対する安全管理体制・規程を職員へ周知すること	【周知状況】	システム以外	職員全員が利用しているグループウェアに掲示し周知している。	十分に周知している		
50	⑤物理的対策	特定個人情報の漏えい・滅失・毀損リスクに対する物理的対策を講じること	【具体的な対策の内容】	システム以外	①外部記憶媒体について、次のルール等を設けており安全管理措置を講じている。 ・私物等の使用禁止 ・持ち帰り禁止 ・鍵のついた書庫等での保管 ・使用管理簿による管理 ②帳票類・電子データ・職員証の管理について、放置の禁止や施錠保管等の安全管理措置を講じている。 ③サーバや端末等について、以下の物理的対策を講じている。 ・ラックの施錠管理 ・ワイヤーロックによる固定 ・入退室管理など ④端末の廃棄を行う際は、データ消去証明書の提出を義務付けている。	十分に行っている		
51	⑥技術的対策	特定個人情報の漏えい・滅失・毀損リスクに対する技術的対策を講じること	【具体的な対策の内容】	システム以外	①ネットワーク構成図の整備、システム機器やソフトウェアのシステム機器管理台帳への記録、システム管理者以外のソフトウェアのインストールや設定変更の禁止、不正なソフトウェアコピーの禁止等のルールを定めており、ルールに従って業務を行っている。 ②不正な操作が無いことについて、操作ログにより適時確認するルールを定めており、定期的に操作ログを確認し不正な書き出しがないか点検を行っている。	十分に行っている		
				システム	①個人・操作端末単位で操作ログを取得している。 ②外部及び内部からの不正アクセスに対する措置を講じることを義務付けている。 ③特定個人情報を閲覧できる端末へのログインには、ID・パスワードと生体認証による二要素認証を義務付けている。 ④③のパスワードを定期的に変更している。			
52	⑦バックアップ	特定個人情報の漏えい・滅失・毀損リスクに対するバックアップを実施すること	【措置の内容】	システム以外	①定期的に業務システムのデータベース等のバックアップを取得することが義務付けられている。 ②バックアップされたデータ毎に保存期間を定めており、期間を過ぎたデータは削除している。	十分に行っている		
				システム	①日次でクラウドへのバックアップを設定をしている。 ②遠隔地バックアップを実施している。			

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】						
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム

項番	評価基準		措置			評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
53	⑧事故発生時手順の策定・周知	特定個人情報に関する事故発生時の対応手順を策定し、職員に周知すること	【措置の内容】	システム以外	情報セキュリティ事故及びシステム障害を発見した場合の手順を以下のように定めている。 ①情報セキュリティ事故を発見した場合は、発生日時、事故・障害のあった対象、事故・障害の状況、業務への影響等を以下のルートで連絡・報告し、必要な措置を講じる。 第一発見者 ⇒ 当該係長 ⇒ システム担当係長⇒セキュリティ対策担当（管理係長）⇒ 国保年金課長 ⇒ 区民部長及び情報政策課長 ②業務への影響を最小限にとどめるための代替手段を講じ、その旨を関係各機関に周知する。 ③事故・障害の情報を情報セキュリティ事故・システム障害報告書に記録し、発生後一定期間保管する。	十分に行っている		

別記第４号様式の２（第４条関係） 評価補足シート

【全項目評価書版】

評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務	特定個人情報ファイル名称	国民年金情報ファイル	システム名称	国民年金システム

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
54	⑨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	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確認すること	【重大事故の内容】	システム以外	－	発生なし		
			【再発防止策の内容】	システム以外	－	発生なし		
55	⑩死者の個人番号	死者の個人番号の保管有無および保管がある場合は、保管方法を確認すること	【具体的な管理方法】	システム以外	生存者と死者を区別することなく、同じセキュリティ対策を施している。	保管している		
				システム	生存者と死者を区別することなく、同じセキュリティ対策を施している。			
56	その他の措置の内容	－	【措置の内容】	－	－			
－	**リスク2：特定個人情報が古い情報のまま保管され続けるリスク**							
57	リスクに対する措置の内容	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対する措置を講じること	【具体的な対策の内容】	システム以外	住民からの届書・申請書等を元にシステム入力を行っており、入力内容は複数人で確認を行うことで入力漏れや誤りを防止している。		十分である	①個人情報が古い情報のまま保管され続けることを防止する手順が、業務マニュアル及び仕様書に定められている。 ②業務が上記手順に基づき実施されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	①保管している特定個人情報が更新された場合、都度区民情報系基盤システムを介して最新情報を反映（上書き）している。 ②バックアップデータは日次で自動取得される。（システムトラブル等によりデータリストアの必要性が生じても、１営業日前の情報に戻すことが可能である）			
－	**リスク3：特定個人情報が消去されずいつまでも存在するリスク**							
58	消去手順	特定個人情報の消去手順を整備すること	【手順の内容】	システム以外	①外部記憶媒体及び文書等の廃棄を行う場合は、「データ消去・媒体廃棄申請書」によりセキュリティ管理者の承認を得て行う手順を定めている。 ②情報毎に保存期限が決められており、保存期限を経過した紙文書は定期的に溶解処分している。 ③USBメモリを使用する場合は原則データの移動用途とし、使用後すみやかにデータ消去を実施している。また、消去したことの記録と確認を実施している。	定めている	十分である	①データ消去に関わる運用ルール・手順等が情報セキュリティ対策基準に定められている。 ②業務の実施方法が確立されている。 ③システムで実装している機能等が仕様設計書等で確認でき設計書通り運用されている。 以上より、「十分である」と評価した。
				システム	データの保存期限を経過したデータは、国民年金システム保守事業者により適時でデータを消去することができる。			
59	その他の措置の内容	－	【措置の内容】	－	－			
－	**特定個人情報の保管・消去におけるその他のリスク**							
60	リスクに対する措置の内容	－	【措置の内容】	－	－			

【全項目評価書版】		
評価書番号及び評価書名	9	国民年金事務及び特別障害給付金に関する事務

項番	評価基準		措置				評価	
	【全項目評価書】リスク対策項目	リスク評価基準	分類		措置の内容（評価書に記載すべき内容）	確認結果（評価書に記載されている選択肢）	評価結果（評価書に記載されている選択肢）	評価結果に至った理由
Ⅳ　その他のリスク対策								
－	1．監査							
－	監査							
1	自己点検の具体的なチェック方法	評価書に記載したとおりに運用がなされているか、およびその他特定個人情報ファイルの取扱いが適正かを評価担当部署において自己点検すること	【具体的なチェック方法】	システム以外	①年金業務で取扱う情報資産における情報セキュリティ対策状況の毎年度の自己点検実施について、以下の内容を定めている。 ・実施計画の立案 ・点検項目による自己点検の実施 ・自己点検結果と改善策の報告 ・自己点検結果に基づく改善 ②所管における自己点検について、以下の内容を定めている。 ・課長は、課内の情報セキュリティの確保及び実施手順の実施状況と有効性の評価のため、自己点検を実施する。 ・課長は、自己点検の結果や評価の内容を踏まえ、実施手順の見直しを行う。実施手順の見直しに際しては、その結果等を課内及び関係者に十分に周知する。		十分に行っている	①自己点検の実施についての運用ルール・手順等が情報セキュリティ標準実施手順に定められている。 ②自己点検の実施方法が確立されており、実際に行っている。 以上より、「十分に行っている」と評価した。
2	監査の具体的な内容	評価書に記載したとおりに運用がなされているか、およびその他特定個人情報ファイルの取扱いが適正かを監査すること	【具体的な内容】	システム以外	①年金業務で取扱う情報資産における情報セキュリティ対策状況について、定期的（必要があれば随時）に監査を実施することが義務付けられている。 ②毎年度、監査計画を大田区情報セキュリティ委員会に提出し、審議承認を得て実行している。 ③監査は第三者（業務委託者）による助言型監査を行い、監査結果は指摘内容への回答を含めて、大田区情報セキュリティ委員会に報告を行っている。 ④重点項目評価や全項目評価対象事務については、総務課において評価5年経過到達以前の定期再評価までに外部専門事業者による外部監査（事業名：特定個人情報保護評価書適正性確認事業）を周期的に実施し、評価書記入内容の適正な運用状況を確認する。この確認結果は、大田区特定個人情報保護評価第三者点検委員会に概要報告と意見聴取を行ない、他の特定個人情報保護評価書の点検や特定個人情報の取扱いなどに役立てることとしている。		十分に行っている	①監査の実施についての運用ルール・手順等が情報セキュリティ標準実施手順に定められている。 ②監査の実施方法が確立されており、実際に行っている。 以上より、「十分に行っている」と評価した。
－	従業者に対する教育・啓発							
3	従業者に対する教育・啓発の具体的な方法	特定個人情報を取扱う従業者等に対して、特定個人情報の安全管理を図るために教育・啓発を行い、違反行為を行った従業者等に対して措置を講じること	【具体的な方法】	システム以外	【大田区全体の対応】 ①研修については、毎年度、研修計画を人事研修部門、情報セキュリティ対策担当等と協議の上立案し、情報セキュリティ委員会での審議承認を得て実行している。 ②毎年度、新規採用者、転入者、主任主事、新任係長などの職層研修や、全課の担当職員に対して情報セキュリティ研修を実施している。 ③研修後は、受講者アンケートを実施してフィードバックを行っている。 ④研修実施状況は、情報セキュリティ委員会に報告を行っている。 【国保年金課の対応】 従事者に対して、年１回以上、以下に関する研修を実施している。 ・セキュリティ基本方針・対策基準・実施手順の理解 ・個人情報の取扱い ・外部記憶媒体の適切な利用と管理 ・パスワード管理について　等		十分に行っている	①教育についての運用ルール・手順等が情報セキュリティ標準実施手順に定められている。 ②研修等の実施方法が確立されており、実際に行っている。 以上より、「十分に行っている」と評価した。
－	その他のリスク対策							
4	リスクに対する措置の内容	－	【措置の内容】	－	－			