別記様式第4号（第4条関係） 評価補足シート

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			
項番	評価基準		措置				評価	
	【重点項目評価書】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：目的外の入手が行われるリスク							
1	リスクに対する措置の内容	事務を遂行する上で必要な者以外の特定個人情報を入手しないこと 事務を遂行する上で必要な者の特定個人情報のうち、必要なもの以外を入手しないこと	【措置の内容】	システム以外	【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いる。 ②窓口において、申請書･届出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。 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設けている。 ④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、課内でセキュリティ研修を実施している。 ⑤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。 ⑥申請書･届出書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。		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。
				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おり、誰が･いつ･どのような操作(どのような情報を参照したか等)を実施したかを確認し不正なアクセスを監視している。 ③区民情報系基盤システムとの連携においては、宛名コードをキーとして連携することにより、確実に対象を特定した連携を行うことにより、対象者以外の個人情報の入手を禁止する。			
－	特定個人情報の入手におけるその他のリスク							
2	リスクに対する措置	－	【措置の内容】	－	区は窓口等で区民より受領する届書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し、全ての媒体は鍵のかかる書庫で適切に保管する。			
－	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							
		特定個人情報の使用目的を超えて取扱わないこと		システム以外	①大田区情報セキュリティ部会または大田区情報公開･個人情報保護審議会において承認を得られた情報項目以外はシステム及び電子記録媒体に保持することが禁止されている。 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いる。 ④毎年、セキュリティ研修を行い、セキュリティ意識を高め、必要のない情報にアクセスしないように教育を行っている。			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

別記様式第４号（第４条関係） 評価補足シート

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	

項番	評価基準		措置				評価	
	【重点項目評価書】 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	リスクに対する措置の内容	特定個人情報の使用目的を超えて取扱わないこと 特定個人情報を事務に必要のない情報と併せて取扱わないこと	【措置の内容】	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仕様とする。 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(データテーブル)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(データテーブル)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、誰が･いつ･どのような操作(どのような情報を参照したか等)を実施したかのログを取得し、かつ、不正なアクセスがないか定期的に監視している。		十分である	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							
4	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	生体情報の登録･ユーザID･パスワード等の適切な管理について以下の運用ルールが定められている。 ①IDは職員番号、生体情報は職員が専用機器で登録を行う。 ②パスワードは6か月ごとに変更を強制され、前回と同じパスワードは設定できない。 ③アカウントロックを解除するためには所定の手続きを行わなければならない。		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）による認証となっている。 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。			
5	その他措置の内容	－	【措置の内容】	－	①国民年金システムの利用権限の付与･変更･失効は、システム管理者以外は実施できない。 ②他部署職員が国民年金システムを利用する場合、又は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･承認を経て利用権限を付与･変更するルールを定めている。 ③権限の変更やユーザIDの失効などは、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を変更･削除する手順を設けている。			
－	特定個人情報の使用におけるその他のリスク							
6	リスクに対する措置の内容	－	【措置の内容】	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入力(登録･変更)または、操作できないよう制御している。 ②システムを利用できる端末は限定されている（サーバ側でシステムにアクセスできる端末を管理しており、それ以外の端末からはシステム利用ができない仕様となっている） ③個人･操作端末単位で操作ログを取得しており、誰が･いつ･どのような操作(どのような情報を参照したか等)を実施したかを確認し不正なアクセスを監視している。			
－	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な使用等のリスク							

別記様式第4号（第4条関係） 評価補足シート

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	

項番	評価基準		措置				評価	
	【重点項目評価書】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	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	委託先事業者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切に返却・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個人情報及び機密情報の保護、秘密の保持 ⑥責任者等の特定、教育の実施 ⑦定期及び事故発生時の報告、立入検査		十分である	①委託先における特定個人情報ファイルの適切な取扱いを確保するために、委託契約書において、委託先の義務や禁止事項を定めている。 ②業務従事者へのアクセス権限付与に関するルール・手続を定めており、かつ、業務がそれにしたがって運用されている。 以上より、「十分である」と評価した。
8	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再委託先は委託先と同様の義務・責任を負うこと			
9	その他の措置の内容	-	【措置の内容】	-	①委託先事業者専用のユーザIDを払い出し、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。 ②委託先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。 ③不正な操作が無いことについて、操作履歴により適時確認するルールを定めている。 ④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。			
-	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							
10	リスクに対する措置の内容	-	【措置の内容】	-	個人・操作端末単位で操作ログを取得しており、誰が・いつ・どのような操作(どのような情報を参照したか等)を実施したかを確認し不正なアクセスを監視している。また、SE作業時には事前承認と事前報告を実施している。			
-	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。）							
-	リスク1：不正な提供・移転が行われるリスク							
11	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は大田区情報セキュリティ部会または大田区情報公開・個人情報審議会の承認手続が必要であり、承認されないと他システムとの接続ができない。 ②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。 ③特定個人情報の移転は、番号法第9条で定められた事務で必要な場合のみ行うこととなっている。（大田区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条例　平成27年9月30日制定） ④他機関への特定個人情報の提供はない（又は発生しない）。		十分である	番号法第9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。 以上より、「十分である」と評価した。
12	その他の措置の内容	-	【措置の内容】	-				
-	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							

別記様式第4号（第4条関係） 評価補足シート

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	

項番	評価基準		措置				評価	
	【重点項目評価書】 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
13	リスクに対する措置の内容	－	【措置の内容】	－	①区が日本年金機構に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化鍵の管理を適正に行う。 ②区が日本年金機構に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。 ③区が日本年金機構に提供する紙媒体は、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。 ④区が日本年金機構に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。 ⑤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、都度、ログファイル(いつ、どのデータ･ファイルが、どのシステムからどのシステムに提供されたか等のログ)が自動生成され、区民情報系基盤システム内に保持される。 ⑥国民年金システムと区民情報系基盤システムとの間で連携するデータ(ファイル)にデータ内容の誤りがあった場合、連携を中止する仕様となっている。			
－	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							
14	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：不正な提供が行われるリスク							
15	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				
－	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							
16	リスクに対する措置の内容	－	【措置の内容】	－				
－	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							
17	①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 ⇒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 ⇒ 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	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。 以上より、「十分である」と評価した。
18	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	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				

別記様式第4号（第4条関係） 評価補足シート

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	

項番	評価基準		措置				評価	
	【重点項目評価書】 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
19	その他の措置の内容	－	【措置の内容】	－	①システムサーバーは大田区役所が管理する特定の場所に設置され、入館・入室は生体認証による制限等を実施している。 ②外部記録媒体や個人情報が記録されている文書を保管する場合は施錠可能な場所に保管するルールが定められ、実施している。 ③外部記録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。 ④磁気ディスクの廃棄時は、内容の復元及び判読が不可能になるような方法により完全消去する。 ⑤帳票等の文書廃棄は、事務処理等で不要となった都度、シュレッダーで裁断している。 ⑥国民年金システムでは、保存年限を経過したデータは、SE作業にて適時削除することができる。 ⑦バックアップは日次で実施し、毎月2回外部記憶媒体への書き出しを行っている。 ⑧機器の廃棄は現地立会及び廃棄報告書を提出させている。			
－	**特定個人情報の保管・消去におけるその他のリスク**							
20	リスクに対する措置の内容	－	【措置の内容】	－				
－	**8. 監査**							
－	**監査**							
21	実施の有無	－	【実施の有無】	システム以外	大田区では第三者（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、総務部長、大田区情報セキュリティ委員会に報告を行っている。			
－	**9. 教育・啓発**							
－	**従業者に対する教育・啓発**							
22	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、情報政策課と協議の上立案し、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】 従業者に対して、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	大田区情報セキュリティ対策基準に従業員に対する教育や監査手順が定められており、手順に従って運用されている。
－	**10. その他のリスク対策**							
23	リスクに対する措置の内容	－	【措置の内容】	－				