別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】										
評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療システム関連情報ファイル			システム名称	後期高齢者医療システム		
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）	備考（補足確認内容）	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	①個人情報を収集する時は、個人情報を取り扱う事務の目的を明確にし、当該事務を行うために必要かつ最小限の範囲で、適法且つ公正な手段によって収集する旨のルールを定めている。 ②個人情報を収集する時は、所定の様式を利用するため様式で定めた項目は事務に必要な情報項目のみであり、それ以外の入手を防止している。 ③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。 ④業務上必要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。 ⑤個人情報の取扱いに対する意識強化のために、年1回以上、課内でセキュリティ研修を実施している。 ⑥電子記録媒体による入手の場合、電子記録媒体の利用時に申請、承認するルール、様式を定めている。			十分である	①特定個人情報を目的外で入手することが個人情報保護法ガイドライン（行政機関等編）5-1保有に関する制限で禁じられている。 ②ルール、手続きなどが定められており、それに従って業務が運用されている。 ③システムで実装している機能等が設計書等や機能検証により確認することができる。 以上により、「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住民記録情報や税情報に関する連携においては、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。 ④ログの確認結果を所属長に報告し、必要に応じて改善を行うこととしている。					
－	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】	－						
－	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									
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】	システム以外	①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時は、個人情報を取扱う事務の目的を明確にし、当該事務を行うために必要且つ最小限の範囲で、適法且つ公正な方法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業務上必要ない情報の保持、許可されていない情報の収集や記録を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実施し、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教育を行っている。	①大田区情報公開・個人情報審議会条例2条（2） ②個人情報保護法ガイドライン（行政機関等編）5-1保有に関する制限 ③大田区情報セキュリティ対策基準　2.2.4　情報資産の入手 ④国保年金・後期高齢者医療担当事務説明会　情報セキュリティ		十分である	①大田区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個人情報保護法ガイドライン（行政機関等編）5-1保有に関する制限により業務外で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設計書等や機能検証により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住民記録情報や税情報をシステム連携により入手する情報項目は必要最小限の項目に限定しており、連携ファイルレイアウトにない項目は連携されない。 規定された項目以外を連携しようとした場合でもシステムは規定された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、業務上必要としない情報項目を追加することはできない					
－	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	生体認証・ユーザID・パスワードの適切な管理について運用ルールが定められている。 アクセス権限の発効、失効のルールが定められている。 離席時のログオフ、ユーザIDの払い出しの手続き、パスワードの定期的変更が定められている。		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実施手順で定められている ②業務が情報セキュリティ実施手順に基づいて実施されている ③システムで実装している機能等が設計書等や機能検証により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システム認証は、ユーザIDと暗証番号によるユーザ認証となっている。 ②端末認証は、ユーザID、生体認証、パスワードによる認証となっている。 ③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管理者権限はシステムベンダーがメンテナンス時のみ利用可となっている。					
5	その他措置の内容	－	【措置の内容】	－						
－	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						

別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】										
評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療システム関連情報ファイル			システム名称	後期高齢者医療システム		
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）	備考（補足確認内容）	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な使用等のリスク									
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	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（契約書附帯条項の遵守） 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		定めている	十分である	①個人情報を取扱う委託契約締結時に必ず「個人情報及び機密の情報」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操作履歴確認作業等の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設計書等や機能検証により確認することができる 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	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		十分に行っている			
9	その他の措置の内容	－	【措置の内容】	－	①委託契約書等に基づき委託内容が適切に実施されていることを月１回確認すると共にその記録を保管している ②委託先事業者から適宜セキュリティ対策の実施状況の報告を受けるとともにその記録を保管している ③委託契約書において、委託先における特定個人情報の取扱状況に関して、定期的な報告を義務付ける規程及び実地の監査・調査等を行うことができることについて定めている					
－	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】	－						
－	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個人情報保護審議会の承認手続きが必要であり、承認されないと他システムとの接続ができず、特定個人情報の提供・移転は行えないルールが定められている。 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後、内容を精査し承認手続きを経て処理を行うルールが定められている。 ③上記①②は、いずれも番号法第9条又は第19条に規定されていることを前提とし、条例及び規則に基づいて、承認手続きが行われる。		定めている	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設計書等や機能検証により確認することができる 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】	－	移転する情報は必要最小限の項目のみに限定しており、ファイルレイアウトに定義していない項目は連携されない。 データ連携の記録はログにより確認している。					
－	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									
13	リスクに対する措置の内容	－	【措置の内容】	－						
－	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	①職員等が、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、記録することは禁止されている。 ②個人情報の収集については、条例にて取り扱う事務の目的を明確にし、事務の目的の達成するために必要な最小限の範囲内で、適法かつ公正な手段によって収集しなければならないと定めている。 ③届出・申請等の様式　について、住民基本台帳事務処理要領に記載の参考様式を基に届出者・申請者が記載する箇所を事務処理に必要な項目に限定している。 ④窓口において、記載例を提示して必要な情報以外を記載しないように対策している。			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設計書等や機能検証により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により入手する情報項目は必要最小限の項目に限定しており、連携ファイルレイアウトにない項目は連携されない（後期高齢者医療システムに連携されない）。					
－	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					本事業では、情報提供ネットワークシステムによる情報提供は行われない。	
				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】	－	※区民情報系基盤システムの特定個人情報ファイルのシステム機能については、共通別添資料「番号法実施に伴う情報連携に関する事務　全項目評価書」を参照ください。					
－	7．特定個人情報の保管・消去									

別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】

評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療システム関連情報ファイル		システム名称	後期高齢者医療システム	

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）	備考（補足確認内容）	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：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は以下のように定め職員に周知している 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・障害があった対象、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			十分である	①物理的な情報セキュリティ対策がルール化されており実施されている。 ②情報資産の管理や保管方法が定められており実施されている。 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					
			【再発防止策の内容】	システム以外					
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、大田区が管理するデータセンターに設置され、データセンター及びサーバールームへの入館・入室は生体認証による入退室制限を実施している。 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、事務室内の施錠可能な場所に保管するルールが定められ、職員により管理を実施している。 ③システムへのアクセス記録はログによりおおむね3か月に1回程度確認している。				

別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】									
評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療システム関連情報ファイル			システム名称	後期高齢者医療システム	
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）	備考（補足確認内容）	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
－	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】	－					
21	実施の有無	－	【実施の有無】	システム以外	自己点検 ①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、自主点検を実施する。また、必要に応じて、自主点検の結果について部長の評価を受ける。 ・課長は、自主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。 ③区民部国保年金課　情報セキュリティ実施手順の最終改定日は以下のとおり。 平成30年9月26日 外部監査 ①監査については、大田区情報セキュリティ対策基準、セキュリティ監査事務概要に記載がある。 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。		自己点検及び外部監査		
－	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 出張所の従事者に対しての事務手続きに関する研修は、国保年金課と同様に実施している。なおセキュリティ研修は各出張所で行っている。			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 以上により「十分に行っている」と評価した
－	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】	－					

別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】										
評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療関連情報ファイル			システム名称	標準システム（東京都後期高齢者医療広域連合電算処理システム）		
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）	備考（補足確認内容）	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	①個人情報を収集する時は、個人情報を取り扱う事務の目的を明確にし、当該事務を行うために必要かつ最小限の範囲で、適法且つ公正な手段によって収集する旨のルールを定めている。 ②個人情報を収集する時は、所定の様式を利用するため様式で定めた項目は事務に必要な情報項目のみであり、それ以外の入手を防止している。 ③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。 ④業務上必要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。 ⑤個人情報の取扱いに対する意識強化のために、年1回以上、課内でセキュリティ研修を実施している。 ⑥電子記録媒体による入手の場合、電子記録媒体の利用時に申請、承認するルール、様式を定めている。			十分である	①特定個人情報を目的外で入手することが個人情報保護法ガイドライン（行政機関等編）5-1保有に関する制限で禁じられている。 ②ルール、手続きなどが定められており、それに従って業務が運用されている。 ③システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「十分である」と評価した。
				システム	大田区からのデータ送信によって入手した情報を標準システムのデータベースに更新する際には、項目間の関連性や整合性のチェックを行っており、確認リストが出力された場合は、入手元へ確認リストを送信した後、入手元にて確認リストのエラー内容等を確認した上で入手情報の再作成や修正等を行う。					
－	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】	－						
－	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									
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】	システム以外	①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時は、個人情報を取扱う事務の目的を明確にし、当該事務を行うために必要且つ最小限の範囲で、適法且つ公正な方法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業務上必要ない情報の保持、許可されていない情報の収集や記録を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実施し、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教育を行っている。			十分である	①大田区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個人情報保護法ガイドライン（行政機関等編）5-1保有に関する制限により業務外での利用が禁じられている ③システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「十分である」と評価した。
				システム	標準システムは独立したシステムとなっており、標準システムの窓口端末のデータ送受信機器以外のネットワークシステムからアクセスできないようにすることで、目的を超えた紐付けや、必要のない情報と紐付けされるリスクを軽減している。					
－	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									
				システム以外	ユーザID、パスワードの管理や運用のルールを以下のように定めている ・パスワードは十分な強度を設ける ・パスワードの定期的な更新を実施する ・ログインしたまま端末を放置せず、離席時にはログアウトする					

別記様式第４号（第４条関係） 評価補足シート

【重点項目評価書版】

評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療関連情報ファイル		システム名称	標準システム（東京都後期高齢者医療広域連合電算処理システム）	

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）	備考（補足確認内容）	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	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	・標準システムを利用する必要がある事務取扱担当者を特定し、一人ひとりに割り当てられた職員IDとそれに対応するパスワードの入力及び生体認証によってユーザ認証を行う。 ・標準システムへのログイン時の認証において、個人番号利用事務の操作権限が付与されていない職員等がログインした場合には、個人番号の表示、検索、更新ができない機能により、不適切な操作等がされることのリスクを軽減している。 ・一定回数のログイン失敗によるアカウントロックを実施する ・一定時間操作がない場合自動ログアウトを実施する		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実施手順で定められている ②業務が情報セキュリティ実施手順に基づいて実施されている ③システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「十分である」と評価した。
5	その他措置の内容	－	【措置の内容】	－					
－	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					
－	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								
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	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（契約書付帯条項の遵守） 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		定めている	十分である	①個人情報を取扱う委託契約締結時に必ず「個人情報及び機密の情報」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操作履歴確認作業等の業務の実施方法が確立されている ③システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「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	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		十分に行っている		
9	その他の措置の内容	－	【措置の内容】	－	①委託契約書等に基づき委託内容が適切に実施されていることを月１回確認すると共にその記録を保管している ②委託先事業者から適宜セキュリティ対策の実施状況の報告を受けるとともにその記録を保管している ③委託契約書において、委託先における特定個人情報の取扱状況に関して、定期的な報告を義務付ける規程及び実地の監査・調査等を行うことができることについて定めている				
－	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】	－					
－	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	・広域連合の標準システムから市区町村の窓口端末のデータ送受信機器へのデータ配信は、「府番第27号 一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について（通知） 平成27年2月13日」において、同一部署内での内部利用の取扱いとするとされている。 ・情報セキュリティ運用ガイドラインに、提供された情報の目的外利用及び第三者への提供の禁止について、委託契約書に明記することを規定している。 ・東京都広域連合における個人情報保護条例第15条に、目的外利用及び外部提供の制限について定めており、市区町村の窓口端末のデータ送受信機器以外への特定個人情報のデータ配信は行っていない。		定めている	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が明文化されている ②システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「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】	－	データ連携の記録はログにより確認している。				
－	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								
13	リスクに対する措置の内容	－	【措置の内容】	－					
－	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								

【重点項目評価書版】

評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療関連情報ファイル		システム名称	標準システム（東京都後期高齢者医療広域連合電算処理システム）	

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）	備考（補足確認内容）	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
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の対応は緊急を要するため広域連合、委託者、各市区町村システム関係者にて連絡ルート、各拠点の連絡先、対応者を明確にし迅速に対処できるよう緊急連絡体制を整えている。 報告ルート 発見者 ⇒ 所属上長 ⇒ システム関係者 ⇒ 情報セキュリティ統括責任者		十分に行っている	十分である	①物理的な情報セキュリティ対策がルール化されており実施されている。 ②情報資産の管理や保管方法が定められており実施されている。 ③システムについては東京都後期高齢者医療広域連合が公表している評価書において評価された内容を確認し、大田区においてもその内容で十分であると評価する。 以上により、「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					
19	その他の措置の内容	－	【措置の内容】	－	・広域連合の標準システムのサーバーはデータセンターの施錠されたラック内に設置している。 ・データセンターへの入館及びサーバー室への入退出は厳重に管理されており、サーバーの操作を許可された者だけが入場できる場所にサーバーを設置している。 ・データセンターはバイオ(生体)認証を用いた入退出管理を実施しており、入退出を行った個人を特定する。 ・職員等は、サーバー室に入室する場合、身分証明書等を携帯し、管理課職員の求めにより提示する。 ・(不正アクセス行為の禁止等に関する法律にいう)アクセス制御機能としては、ユーザIDによるユーザの識別、パスワードによる認証、認証したユーザに対する認可の各機能により、そのユーザがサーバー及びシステムで操作できる事項を制限し、認証(ログイン)、認可（処理権限の付与)を行っている。 ・システムへのアクセス記録はログにより確認している				

別記様式第4号（第4条関係） 評価補足シート

【重点項目評価書版】									
評価書番号及び評価書名	（評価書番号）	（評価書名）	特定個人情報ファイル名称	後期高齢者医療関連情報ファイル		システム名称	標準システム（東京都後期高齢者医療広域連合電算処理システム）		
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）	備考（補足確認内容）	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
－	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	自己点検 ・情報管理責任者は、特定個人情報ファイルの適正な取扱いについてすべての職員に理解され、管理策が適切に実施されているかを点検するため、自己点検を次の手順で実施する。 （1）自己点検の実施方法 1）自己点検は、ISMS実施計画に定めた時期及び必要に応じて実施する。 2）職員等は、「自己点検票」に基づき自己点検し、結果はISMS事務局が取りまとめて情報セキュリティ委員会に報告する。 （2）自己点検結果の活用 1）職員等は、自己点検の結果に基づき、自己の職務の範囲内で改善を図る。 2）情報セキュリティ委員会は、自己点検結果に基づき組織としての改善を図る。 監査 ・広域連合では、「情報セキュリティマネジメントシステム基本方針」を情報セキュリティに関する最上位の規範として位置づけ、情報セキュリティ対策に関する日常的な監視活動や、概ね年1回以上監査及び自己点検を通して、継続的に情報セキュリティの維持・改善を行っている。 ・情報セキュリティに関する監査については、情報セキュリティ監査責任者及び情報セキュリティ監査副責任者を置くとともに、内部監査計画の立案、監査対象、監査リーダー及びメンバーの選定を行い、特定個人情報ファイルの取扱いを監査対象とした監査を行っている。 ・定期的に各種サーバ・端末のログを収集、ログ監査レポートを作成し、データ抽出等の不正な持ち出しが行われていないか監査を行っている。		自己点検、内部監査及び外部監査		
－	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。 以上により「十分に行っている」と評価した。
－	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】	－					