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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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個人情報保護条例									
－	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	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。			十分である	・個人情報の保護については法令等で定めており、セキュリティ研修を実施し、職員に対する教育を行っている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照・更新範囲を設定している。 ②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し、確実に対象を特定した連携を行うこととする。これにより、対象者以外の個人情報の入手を禁止する。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
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毎年、区の情報セキュリティポリシーに基づいた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している。				
				システム	①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照範囲を設定している。 ②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し、確実に対象を特定した連携を行うこととする。これにより、対象者以外の個人情報の入手を禁止する。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
3	その他の措置の内容	－	【措置の内容】	－					
－	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窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第960 号）」に基づき確認を行うものとする。 ③セキュリティ研修または新人・異動者向けの研修において、窓口・郵送等の届出の受け取りまたは基盤システム以外の方法を用いて特定個人情報を入手してはならないことを教育を行う。			十分である	対象となる入手のケースは「窓口や郵送等における届書による入手」及び「区民情報系基盤システムから連携で送付されてくる入手」がある。 ・「窓口における対面での入手」においては、本人確認方法を「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について」に基づき実施する。 ・「区民情報系基盤システムから連携で送付されてくる入手」に関しては、情報は区民情報系基盤システムを経由して住民基本台帳や税情報が送付されてくるが、基本的にデータの真正性は各提供元で担保されているもので、介護保険システムにおいてデータを改変することがない。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ②組織ごとに業務権限を割り振り、事務実施者以外の者がアクセスし、データの盗取等が行われないよう、権限ごとにデータの参照・更新範囲を設定している。 ③介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系基盤システムに限定する。 ④介護保険システムと介護認定審査会システムの連携はネットワークアクセス制御された共有ファイルサーバーを経由して行い、暗号化されたファイルにより連携するように設計されている。 ⑤介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ⑥記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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	①窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第960 号）」に基づき確認を行うものとする。 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毎年、区の情報セキュリティポリシーに基づいた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している。	・制定予定の要綱は住民票の写し等の交付申請等に係る本人確認に関する取扱い要綱に準じた内容とする予定。		十分である	・対象となる入手のケースは「窓口や郵送等における届書による入手」及び「基盤システムから連携で送付されてくる入手」がある。 ・「窓口における対面での入手」においては、本人確認方法を「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について」に基づき実施する。 ・「区民情報系基盤システムから連携で送付されてくる入手」に関しては、情報は区民情報系基盤システムを経由して住民基本台帳や税情報が送付されてくるが、基本的にデータの真正性は各提供元で担保されているもので、介護保険システムにおいてデータを改変することがない。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
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	①窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第960 号）」に基づき確認を行うものとする。 ③住民基本台帳から連携される個人番号は、担当部署にて真正性が確認された番号のみが介護保険システムへデータ連携される。 ④すでにデータ連携により個人番号を入手している事が介護保険システムで確認できる場合は、介護保険システムの画面上に表示される入手済みの個人番号と申請書に書かれた個人番号の照合を行い、真正性を確認する。				
				システム	①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し、確実に対象を特定した連携を行うこととする。				
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個人番号以外の個人情報についても、複数の担当によるダブルチェックやクロスチェックなどの複合的な確認を行う。 ②申請書等は施錠できる保管庫に格納する。また保管庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。				
				システム	①個人情報を入力する画面には複数の論理チェックが設けられており、矛盾した内容のデータを入力すると、エラーが表示されて入力ができなくなる仕組みとなっている。 ②介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。				
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区の情報セキュリティポリシーに基づき、申請書は鍵付の保管庫に保管し、許可された人以外の使用および参照を禁ずる。また、保管庫の鍵については担当係長が施錠管理の上、保管している。 ②申請書や出力帳票等は、机上に放置しない。離籍時などは、画面をロックし、ディスプレイに情報を表示させた状態にしないなどの作業時間中の情報漏えい対策を実施している。			十分である	・入手の際に特定個人情報が漏えい・紛失することを防止する措置として、申請書等の滅失の防止に関する規定及びシステム機能における保護措置が文書の記載によって確認でき、また実際の運用も記載と同様であるため「十分である」としている。
				システム	①介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ②介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系基盤システムに限定する。 ③介護保険システムと介護認定審査会システムの連携はネットワークアクセス制御された共有ファイルサーバーを経由して行い、暗号化されたファイルにより連携するように設計されている。				
－	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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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
－	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設けている。 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定めている。 ③毎年、区の情報セキュリティポリシーに基づいた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している。			十分である	目的を超えた紐付けや事務に必要ない情報との紐付けを防止するための条例や基準が規定されていること、システムの設計上、必要な情報以外を参照できないよう制限しているため、「十分である」と評価する。
				システム	①技術的な対策としては、共通別添資料「番号法実施に伴う情報連携機能　全項目評価書」参照のこと。				
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設けており、定期的に研修等を通じ周知すると共に運用が正しく行われているか確認している。 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、定期的に研修等を通じ周知すると共に運用が正しく行われているか確認している。 ③毎年、区の情報セキュリティポリシーに基づいた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している。						
				システム	①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照・更新範囲を設定している。 ②データ連携の設計において、あらかじめ連携の対象データ項目を限定している。				
13	その他の措置の内容	－	【措置の内容】	－					
－	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正規職員の介護保険システムに関するアクセス権限付与・失効及び変更は人事異動時にシステム管理者により付与される。 ②非常勤・委託先従業員の介護保険システムに関するアクセス権限付与及び変更は、申請書により所定の審査・承認を経てIDを付与し、交付することとしている。 ③介護保険システムのアクセス権限は、システム管理者により人事異動時及び定期的に確認を行い、必要の無いIDを無効にしている。 ④離席時や業務上必要のないときは、パソコン等の画面をロックするかパソコン等からログオフしなければならない		行っている	十分である	権限の無い者による不正利用防止のための措置について、認証のための手順、IDの管理、パスワードの管理が整備されていることを文書の記載により確認でき、実際の運用ともあっているため「十分である」と評価する。
				システム	①介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ②介護保険システムの管理機能によって利用可能なIDの一覧及びIDごとのログを記録している。				
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正規職員の介護保険システムに関するアクセス権限付与・失効及び変更は人事異動時にシステム管理者により付与される。 ②非常勤・委託先従業員の介護保険システムに関するアクセス権限付与及び変更は、申請書により所定の審査・承認を経てIDを付与し、交付することとしている。 ③介護保険システムのアクセス権限は、システム管理者により人事異動時及び定期的に確認を行い、必要の無いIDを無効にしている。		行っている		
				システム	①介護保険システムのアクセス権限の変更及び失効機能はシステム管理者のみ可能。 ②介護保険システムの利用には生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムの管理機能によってアクセス権限の付与、変更、終了等の履歴を記録している。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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
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介護保険システムのアクセス権限は、システム管理者により人事異動時及び定期的に確認を行い、必要の無いIDを無効にしている。		行っている		
				システム	①介護保険システムのアクセス権限は割り振られたIDの一覧と事務の対応表を作成し管理している。 ②介護保険システムの管理機能によってアクセス権限の付与、変更、終了等の履歴を記録している。				
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	①申請書は受領時に日付入りの収受印を押印のうえ、日付ごとに綴り、施錠できる保管庫に格納している。また、保管庫の鍵については担当係長が施錠管理の上、保管している。		記録を残している		
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月2回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
18	その他措置の内容	-	【措置の内容】	-					
-	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毎年、区の情報セキュリティポリシーに基づいた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している。 ②申請書等の個人情報が記載された資料は鍵付の書庫に保管し、許可された人以外の使用および参照を禁じている。また、書庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。			十分である	事務以外の目的での個人情報等の利用禁止ルールが定められていることが文書で確認でき、また実際の運用も同様であるため「十分である」と評価する。
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月2回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル		システム名称	介護保険システム	

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）	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毎年、区の情報セキュリティポリシーに基づいた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している。 ②申請書等の個人情報が記載された資料は鍵付の書庫に保管し、許可された人以外の使用および参照を禁じている。また書庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。 ③原則データ移動のみ許可された外部記録媒体を使用し、使用管理簿に使用者・使用時間等を記載し、システム管理者及び担当係長の確認を得る。			十分である	個人情報が不正に複製されることを防止するためのルールが明文化されており、情報資産管理システムにより外部接続媒体への書き出し制限、書き出した場合のログの記録と上司への通知等の措置が取られている。そのため「十分である」と評価する。
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。 ③情報資産管理システムにより、許可された外部記録媒体以外の媒体は端末等の機器に使用できない設定となっている。 ④情報資産管理システムにより、許可された外部記録媒体に、何のファイルをいつ、誰が書き出したのかが記録されると同時に、直属の上司に書き出した情報が通知される設定となっている。				
－	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					
－	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個人情報の取扱に関与する委託契約時には、「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、立入検査等」について明記した契約を締結している。 ③システム保守事業者が作業で使用する機器など事前に申請を受け、その通りのものを持ち込んでいるか確認している。サーバ室等への入退室管理を行っている。作業で使用した資料の返却など確認している。 ④介護保険課において窓口受付、事務処理等を委託している業者に対しては、作業で使用した資料の返却など確認している。				
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、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非常勤・委託先従業員の介護保険システムに関するアクセス権限付与及び変更は、申請書により所定の審査・承認を経てIDを付与し、交付することとしている。 ③委託先のIDに付与する権限は業務上必要最小限のアクセス権限を割り当てている。 ④介護保険システムのアクセス権限の変更及び失効機能はシステム管理者のみ可能。		制限している	十分である	委託先による個人情報の不正な取扱いを防止するための措置として、情報セキュリティ及び個人情報の取扱いに関するルールが文書で確認でき、また実際の運用も同様であるため「十分である」と評価する。
				システム	①委託先の介護保険システムに係るID及びアクセス権限一覧表を作成し保管する。 ②介護保険システムの管理機能によって委託先に付与されたIDの権限は閲覧又は更新可能なデータの範囲を制限している。				
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			記録を残している		
				システム	①介護保険システムについては操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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
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委託先から第三者へ個人情報を提供することは認めていない。		定めている		
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	以下の点について、委託契約書に明記することとしている。 ①委託先は、特定個人情報の目的外利用及び第三者に提供してはならないこと、特定個人情報の複写、複製、又はこれらに類する行為をすることはできない。 ②委託先においても個人情報の漏えい、滅失又は毀損の防止等に関する安全確保の措置の義務付け。 ③当区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは委託先に対して調査を行い、又は報告を求める。 ④委託期間中に6か月に1回以上、個人情報の管理状況について「個人情報及び機密情報の管理に関する報告書」を委託先から提出する。				
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	個人情報の取扱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、「提供資料の返還、情報の消去、立入検査等」を明記した契約を締結している。また、委託期間中に6か月に1回以上、個人情報の管理状況について「個人情報及び機密情報の管理に関する報告書」を委託先から提出することとし、そちらの報告書にて確認している。		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	個人情報の取扱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、「個人情報及び機密情報の保護」「受託業務以外の利用禁止」「複写及び複製の禁止」等のセキュリティ要件を明記した契約を締結している。		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	個人情報の取扱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、「再委託」に関するセキュリティ要件を明記した契約を締結している。また、委託期間中に6か月に1回以上、個人情報の管理状況について「個人情報及び機密情報の管理に関する報告書」を委託先から提出することとしている。		再委託していない		
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特定個人情報を提供・移転する際は、番号法第19条の規定や条例に基づいたものであることを条件とし、申請書等の保存により記録を保持する。		記録を残している	十分である	・提供・移転に関しては番号法9条2項に定めがあるとおりに運用を行うこと、情報提供のたびに適用依頼書をシステム管理者に提出させて記録を行っていること、システムではすべての操作ログをとっていることにより「十分である」と評価する。
				システム	①区民情報系基盤システムとのデータ連携は、その都度、ログファイルを作成し、いつ、どのデータ・ファイルが連携されたか等のログを保持している。				
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特定個人情報を提供・移転する際は、番号法第19条の規定や条例に基づいたものであることを条件とすることを、職員研修等をとおして理解を深め、周知徹底する。		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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル			システム名称	介護保険システム	
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）	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突発的かつデータ連携で設計されていないデータの抽出・集計については、公文書による依頼にて行うこととする。 ②受領した作業依頼文書については、番号法で許可されているか、あるいは条例で定めがあるか確認した後に、提供・または移転を行う。			十分である	・提供・移転に関しては番号法9条2項に定めがあるとおりに運用を行うこと、情報提供のたびに適用依頼書をシステム管理者に提出させて記録を行っていること、システムではすべての操作ログをとっており、アクセス権による制限も行っていることにより「十分である」と評価する。
				システム	①通常のデータの提供・移転は区民情報系ネットワークで行う。 ②介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系システムに限定する。 ④介護保険システムと介護認定審査会システムの連携はネットワークアクセス制御された共有ファイルサーバーを経由して行い、暗号化されたファイルにより連携するように設計されている。 ⑤介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ⑥記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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突発的かつデータ連携で設計されていないデータの抽出・集計については、公文書による依頼にて行うこととする。 ②受領した作業依頼文書については、番号法で許可されているか、あるいは条例で定めがあるか確認した後に、提供・または移転を行う。			十分である	・提供・移転に関しては番号法9条2項に定めがあるとおりに運用を行うこと、情報提供のたびに適用依頼書をシステム管理者に提出させて記録を行っていること、システムではすべての操作ログをとっており、アクセス権による制限も行っていることにより「十分である」と評価する。
				システム	①通常のデータの提供・移転は区民情報系ネットワークで行う。 ②介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系基盤システムに限定する。 ④データ連携の設計において、あらかじめ連携の対象データ項目を限定している。 ⑤介護保険システムと介護認定審査会システムの連携はネットワークアクセス制御された共有ファイルサーバーを経由して行い、暗号化されたファイルにより連携するように設計されている。 ⑥介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ⑦記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
－	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】	－					
－	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	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、事務の目的を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、大田区介護保険条例施行規則に記載の様式を基に届出者・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。			十分である	・個人情報を取得するときは、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取得しなければならない旨のルールを定めている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①介護保険システムに介護保険業務に必要な情報以外は登録できないよう対策している。 ②庁内からの住民記録・税情報等の入手にあたっては、庁内連携機能の制御機能にて、予め許可された情報のみ入手可能。 ③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、情報提供許可情報と照会内容の照会許可情報との照合が必要な仕組みになっている。 これにより番号法に定められた情報連携以外の照会は拒否されるため、目的外の特定個人情報の入手を制御している。 ④職員認証、権限管理機能で、権限のない職員のアクセスを防ぎ、目的外の特定個人情報の入手が行われることを制御している。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。 ⑤どのユーザ又は既存システム、どの事務に対して情報照会や情報提供可能かを、情報照会許可用照合リスト及び権限グループ等を用いて、アクセス制御を行う。なお、このアクセス制御は、職員認証・権限管理機能を用いて設定している。				
－	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	適切な認証を受けたもの以外からのアクセスが生じないようにユーザ認証情報の管理について、以下のルールを設けている。 <ID> ・自己が利用しているIDは、他者に知られないように管理し、他人に利用させない。また、他人のIDを利用させない。 <パスワード> ・パスワードは、他者に知られないように管理する。 ・パスワードは十分な長さとし、文字列は第三者が類推することが困難なものにする。			十分である	・IDやパスワードの運用に関して、情報セキュリティ及び個人情報の取扱いに関するルールが文書で確認でき、実際にその通りに運用している。 ・システム設計時に、十分なセキュリティが確保できるように様々な措置を行っている。 ・すべての操作のログを保存している。 以上のことから総合的に十分であると評価する。
				システム	①情報提供ネットワークにおいては、高度なセキュリティを維持した行政専用のネットワークを利用することにより、安全性を確保している。ネットワークはVPN（仮想プライベートネットワーク）等の技術を利用し、団体ごとに通信回線を分離し暗号化を行っている。 ②サーバー、運用端末及び管理端末は、専用の安全な区画に設置し、接続できる端末は必要最小限に制御され、セキュリティを十分に担保したうえで、専用環境又は共用環境に設置する。 ③パーソナルファイアウォール及びウィルス検出ソフトウェア、ファイアウォール、IDS（侵入検知システム）、WAF（Webアプリケーションファイアウォール）、サンドボックスの導入により、不正アクセス及びマルウェアを検知する。 ④正常・異常に関わらず、ログの取得・保管を行う。 ・情報提供等記録／アクセス記録、アクセスログ、DBログなど				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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	①窓口における対面での申請書受領の際には必ず本人または代理人の本人確認を行ったうえで受領する。 ②上記①以外の場合については、平成28年1月1日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第960 号）」に基づき確認を行うものとする。 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毎年、区の情報セキュリティポリシーに基づいた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している。			十分である	・「窓口における対面での入手」においては、本人確認方法を「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について」に基づき実施する。 ・個人情報を取得するときは、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取得しなければならない旨のルールを定めている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①入力については操作記録（ログ）を取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。証跡については完全性を担保し、容易に改ざんできない対策を施している。 ②区民情報系基盤システムとのデータ連携は、その都度、ログファイルを作成し、いつ、どのデータ・ファイルが連携されたか等のログを保持している。 ③情報提供ネットワークシステム配信マスター情報を取得し、番号法別表第二に規定される情報照会者、事務、情報提供者、特定個人情報の項目等が定められている情報のみ入手している。 ④入手元においても、誤った情報を提供された場合を想定した措置が担保されている。 ⑤特に、中間サーバーでは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。				
－	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	①業務で使用する個人情報を含むデータ等が記録された電子媒体及び入出力帳票並びに文書等は放置せず、閉庁時には施錠できる場所で保管している。 ②事務処理段階で発生する個人情報を含む帳票類で不要となるものは、担当者が必ず内容を確認しながら他の帳票類と区分し、再度内容確認の上シュレッダーにより裁断をしている。 ③情報を作成する者は、作成途上の情報についても、紛失や流出等を防止を義務付ける。また、情報の作成途上で不要になった情報は消去する。 ④情報資産を利用する者は、業務で使用するデータを記録した外部記録媒体、入出力帳票及び文書等を机上に放置しない等、常時に適切な取扱を義務付けることなどを定め実施している。 ⑤操作端末の画面は来庁者から見えない位置に配置している。			十分である	・個人情報の保護については条例で定めており、セキュリティ研修を実施し、職員に対する教育を行っている。 ・入手した個人情報の保管や消去について取り扱いのルールを定めており、セキュリティ教育を行い、取り扱いルールの徹底を行っている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①アクセスできる端末をシステム設定により限定している。 ②システム管理者によるアクセス権限の設定により利用を制限している。 ③個人単位の操作ログを取得し追跡可能な形式で管理しており、対象者以外の情報の入手の抑止を図っている。証跡については完全性を担保し、容易に改ざんできない対策を施している。 ④システムのネットワークは庁内の専用線で接続され、外部インターネット環境とは隔離された環境にある。 ⑤回線は、特定個人情報を送信する際に暗号化を行い、取得したログについては適切な頻度で不正検知の目的で確認を行っている。 ⑥職員認証・権限管理機能によりアクセス権限を管理している。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。				
－	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	①大田区情報公開・個人情報保護審議会へ諮問・報告する内容に連携するデータ項目も明示し、承認等を得た後にシステム改修・データ連携を開始している。			十分である	・個人情報の保護については条例で定めており、セキュリティ研修を実施し、職員に対する教育を行っている。 ・個人情報を新規で利用する場合、その利用目的が正当か審査する機関や事務手続きが定められており、実際に運用されている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①特定個人情報は人手を介さないファイル転送方式とし、提供する先は区民情報系基盤システムに限定することで誤った相手に提供・移転することを防いでいる。 ②職員認証、権限管理機能で、権限のない職員のアクセスを防ぎ、不正な特定個人情報の提供が行われることを制御している。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。 ③どのユーザ又は既存システム、どの事務に対して情報照会や情報提供可能かを、情報照会許可用照合リスト及び権限グループ等を用いて、アクセス制御を行う。なお、このアクセス制御は、職員認証・権限管理機能を用いて設定している。 ④特に、中間サーバーにおいては、情報提供ネットワークシステムから配信される情報（照合許可用照合リスト情報、この情報を構成する機関、事務、特定個人情報種別等の情報）に基づき不正な特定個人情報の提供が行われることを制御している。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル		システム名称	介護保険システム		
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）	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	①大田区情報公開・個人情報保護審議会へ諮問・報告する内容に連携するデータ項目等を明示し、承認等を得た後にシステム改修・データ連携を開始している。			十分である	・個人情報を新規で利用する場合、その利用目的が正当か審査する機関や事務手続きが定められており、実際に運用されている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①特定個人情報は人手を介さないファイル転送方式とし、提供する先は区民情報系基盤システムに限定することで誤った相手に提供・移転することを防いでいる。 ②職員認証、権限管理機能で、権限のない職員のアクセスを防ぎ、不適切な特定個人情報の提供が行われることを制御している。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。 ③どのユーザ又は既存システム、どの事務に対して情報照会や情報提供可能かを、情報照会許可用照合リスト及び権限グループ等を用いて、アクセス制御を行う。なお、このアクセス制御は職員認証・権限管理機能を用いて設定している。 ④情報提供ネットワークシステムから配信される情報（照合許可用照合リスト情報、この情報を構成する機関、事務、特定個人情報種別等の情報）に基づき不適切な特定個人情報の提供が行われることを制御している。			
－	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	①大田区情報公開・個人情報保護審議会へ諮問・報告する内容に連携するデータ項目も明示し、承認等を得た後にシステム改修・データ連携を開始している。			十分である	・個人情報を新規で利用する場合、その利用目的が正当か審査する機関や事務手続きが定められており、実際に運用されている。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
				システム	①特定個人情報は人手を介さないファイル転送方式とし、提供する先は区民情報系基盤システムに限定することで誤った相手に提供・移転することを防いでいる。 ②中間サーバーにおいては、情報提供ネットワークシステムに情報連携を行う際には、アクセス記録を生成し、保管する。また、保管されたアクセス記録より提供先記録等を抽出する機能を有している ③正本・副本の整合性を確認するために、副本データをファイルとして出力する機能を有している。 ④情報提供ネットワークシステムから配信される情報（照合許可用照合リスト情報、この情報を構成する機関、事務、特定個人情報種別等の情報）に基づき不適切な特定個人情報の提供が行われることを制御している。			
－	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								
45	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	介護保険課のセキュリティ対策で安全管理体制を、次のように定めている。 ①セキュリティ管理者…介護保険課長をあてる。介護保険課が保有し、又は使用する情報資産に対する管理責任を負う ②セキュリティ対策担当…課長から委任を受け、情報セキュリティ対策の運用を実施する。		十分に整備している		
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	大田区のセキュリティ対策において、次の措置を行っている。 ①情報セキュリティ管理体制 ②情報資産の分類及び管理 ③人的な情報セキュリティ対策 ④物理的な情報セキュリティ対策 ⑤技術的な情報セキュリティ対策 ⑥運用における情報セキュリティ対策 ⑦評価・見直し		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	①毎年、セキュリティ研修を行っている。 ②職員が常にセキュリティの基準を確認できるように職員向け掲示板に掲示している。		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介護保険システムのサーバーは庁舎外のデータセンターに設置されており、災害による被害を最小限にとどめる対策をとっている。 ②データセンターでは、入退室管理、各種物理サーバーの盗難防止対策等を厳格に実施している。 ③介護保険システムに登録されているデータについては日次でバックアップ処理を実施している。		十分に行っている		

【全項目評価書版】

評価書番号及び評価書名	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	介護保険情報ファイル	システム名称	介護保険システム

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）	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
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			十分に行っている	十分である	個人情報の漏えい、滅失、毀損を防止するための十分な措置が取られいて、それぞれの措置の根拠が文書でも確認できるため「十分である」と評価する。
				システム	①介護保険システムのアクセス権限の変更及び失効機能はシステム管理者のみ可能。 ②介護保険システムの利用には生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月2回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。 ⑤介護保険システムとシステム利用端末間の通信はすべて暗号化されている。				
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	大田区のセキュリティ対策として、次の事項で定期バックアップとる事を規定している。 ①物理的な情報セキュリティ対策 ②技術的な情報セキュリティ対策		十分に行っている		
				システム	①介護保険システムのバックアップは日次で実施されている				
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	大田区のセキュリティ対策として、次の事項を規定している。 1.庁内からの事故・欠陥等の報告手順 2.区民等からの通報による事故・欠陥等の報告手順 3.侵害時の対応		十分に行っている		
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で管理している。		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で管理している。				
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				十分である	基盤システムにより、住民基本台帳システム・税システム等と連携しており、情報に異動があった場合は連携により、随時情報が更新される。
				システム	介護保険システムにおいて、情報に異動があれば、その都度データを修正している				
－	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届書等は申請年及び保管期限ごとに分けて保存し、保管期間を過ぎたものは定期的に溶解処分している。 ②外部記録媒体やサーバ等の廃棄に伴うデータ消去については、記録媒体の完全初期化等情報を復元できないように処置する手順を設けている。 ③外部記録媒体やサーバ等の廃棄を行う際には作業完了後、速やかに作業完了証明書を提出させている。証明書には抹消年月日、抹消方法、作業者所属・氏名等を記載させている。		定めている	十分である	特定個人情報が記録された文書や手順が確認できたため、「十分である」と評価する。
				システム	①保管期間が過ぎた情報は、随時に消去する。消去後、確かに消去されているか職員が確認する。				
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】	－					

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル	システム名称	介護保険システム	

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）	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：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。 システム：①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照・更新範囲を設定している。 ②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し、確実に対象を特定した連携を行うこととする。これにより、対象者以外の個人情報の入手を禁止する。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。			十分である	・対象となる入手のケースは「窓口や郵送等における届書による入手」及び「区民情報系基盤システムから連携で送付されてくる入手」がある。 ・「窓口における対面での入手」においては、本人確認方法を「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について」に基づき実施する。 ・「区民情報系基盤システムから連携で送付されてくる入手」に関しては、情報は基盤システムを経由して住民基本台帳や税情報が送付されてくるが、基本的にデータの真正性は各提供元で担保されているもので、介護保険システムにおいてデータを改変することがない。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
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毎年、区の情報セキュリティポリシーに基づいた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している。 システム：①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照範囲を設定している。 ②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し、確実に対象を特定した連携を行うこととする。これにより、対象者以外の個人情報の入手を禁止する。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。					
3	その他の措置の内容	－	【措置の内容】	－					
－	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窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第 960 号）」に基づき確認を行うものとする。 ③セキュリティ研修または新人・異動者向けの研修において、窓口・郵送等の届出の受け取りまたは基盤システム以外の方法を用いて特定個人情報を入手してはならないことを教育を行う。 システム：①介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ②組織ごとに業務権限を割り振り、事務実施者以外の者がアクセスし、データの盗取等が行われないよう、権限ごとにデータの参照・更新範囲を設定している。 ③介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系基盤システムに限定する。 ④介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ⑤記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。			十分である	個人情報が不適切な方法で入手されるのを防止するためのルールが明文化されており、情報資産管理システムにより外部接続媒体への書き出し制限、書き出した場合のログの記録と上司への通知等の措置が取られている。そのため「十分である」と評価する。

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル	システム名称	介護保険システム

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）	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	①窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第 960 号）」に基づき確認を行うものとする。 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毎年、区の情報セキュリティポリシーに基づいた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している。	・制定予定の要綱は住民票の写し等の交付申請等に係る本人確認に関する取扱い要綱に準じた内容とする予定。		十分である	・対象となる入手のケースは「窓口や郵送等における届書による入手」及び「区民情報系基盤システムから連携で送付されてくる入手」がある。 ・「窓口における対面での入手」においては、本人確認方法を「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について」に基づき実施する。 ・「区民情報系基盤システムから連携で送付されてくる入手」に関しては、情報は基盤システムを経由して住民基本台帳や税情報が送付されてくるが、基本的にデータの真正性は各提供元で担保されているもので、介護保険システムにおいてデータを改変することがない。 ・システム面の対策としては組織ごとに業務権限を割り振り、必要な情報以外を参照または更新できないように画面コントロールを行っていること、すべての操作においてIDごとに操作ログを記録していること、連携設計時に確実に対象を特定した連携を行っている。 以上のことから総合的に判断して「十分である」と評価する。
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	①窓口における対面での申請書受領の際には個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。代理人による申請の際は、委任状のほかに代理人の個人番号カード又は通知カードの提示を求め、本人確認を行うものとする。 ②上記①以外の場合については、平成28年１月１日施行の「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法律施行規則の規定に基づく個人番号利用事務実施者が適当と認める書類等について（大田区告示第 960 号）」に基づき確認を行うものとする。 ③住民基本台帳から連携される個人番号は、担当部署にて真正性が確認された番号のみが介護保険システムへデータ連携される。 ④すでにデータ連携により個人番号を入手している事が介護保険システムで確認できる場合は、介護保険システムの画面上に表示される入手済みの個人番号と申請書に書かれた個人番号の照合を行い、真正性を確認する。				
				システム	①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し、確実に対象を特定した連携を行うこととする。				
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個人番号以外の個人情報についても、複数の担当によるダブルチェックやクロスチェックなどの複合的な確認を行う。 ②申請書等は施錠できる保管庫に格納する。また保管庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。				
				システム	①個人情報を入力する画面には複数の論理チェックが設けられており、矛盾した内容のデータを入力すると、エラーが表示されて入力ができなくなる仕組みとなっている。 ②介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ③記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
8	・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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル	システム名称	介護保険システム	

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）	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データ移動時は許可された外部記録媒体を使用し、使用管理簿に使用者・使用時間等を記載し、システム管理者等の確認を得る。 ②区の情報セキュリティポリシーに基づき、申請書は鍵付の保管庫に保管し、許可された人以外の使用および参照を禁ずる。また、保管庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。 ③申請書や出力帳票等は、机上に放置しない。離籍時などは、画面をロックし、ディスプレイに情報を表示させた状態にしないなどの作業時間中の情報漏えい対策を実施している。 システム：①伝送通信ソフトは、専用回線を使用し、伝送ソフト通信ソフト利用端末から東京都国民健康保険団体連合会まで通信の暗号化を行っている。 ②介護保険システムの利用には、生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムが他のシステム（介護保険認定審査会システムを除く）との連携により個人情報を入手する際には、情報の入手元をネットワークアクセス制御及びシステム間認証により、区民情報系基盤システムに限定する。 ④介護保険システムと介護認定審査会システムの連携はネットワークアクセス制御された共有ファイルサーバーを経由して行い、暗号化されたファイルにより連携するように設計されている。			十分である	・入手の際に特定個人情報が漏えい・紛失することを防止するルールが文書で確認でき、実際の運用も同様であるため「十分である」と評価する。
－	**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】	－				
－	**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： システム：統合宛名管理機能への接続は行わない。			十分である	目的を超えた紐付けや事務に必要ない情報との紐付けができないよう設計されているため、「十分である」と評価する。
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設けている。 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いる。 ③毎年、区の情報セキュリティポリシーに基づいた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している。 システム：①組織及び職員ごとに業務権限を割り振り、必要な情報以外を参照または更新できないよう、権限ごとにデータの参照・更新範囲を設定している。 ②データ連携の設計において、あらかじめ連携の対象データ項目を限定している。				
13	その他の措置の内容	－	【措置の内容】	－				
－	**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伝送通信用端末は専用端末であり、IDの利用についてID利用管理簿で管理している。 システム：		行っている	十分である	権限の無い者による不正利用防止のための措置について、認証のための手順、IDの管理、パスワードの管理が整備されていることを文書の記載により確認でき、実際の運用ともあっているため「十分である」と評価する。
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端末ログイン用パスワードの発効・失効権限は、東京都国民健康保険団体連合会のみとなっている。 ②パスワードの変更は年１回行っている。 システム：		行っている		
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伝送通信ソフト利用のためのIDの管理は東京都国民健康保険団体連合が行っている。 システム：		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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル			システム名称	介護保険システム	
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）	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
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			記録を残している		
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。				
18	その他措置の内容	－	【措置の内容】	－					
－	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毎年、区の情報セキュリティポリシーに基づいた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している。 ②申請書等の個人情報が記載された資料は鍵付の書庫に保管し、許可された人以外の使用および参照を禁じている。また、書庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。			十分である	事務以外の目的での個人情報等の利用禁止ルールが定められていることが文書で確認でき、また実際の運用も同様であるため「十分である」と評価する。
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。 ③情報資産管理システムにより、許可された外部記録媒体以外の媒体は端末等の機器に使用できない設定となっている。 ④情報資産管理システムにより、許可された外部記録媒体に、何のファイルをいつ、誰が書き出したのかが記録されると同時に、直属の上司に書き出した情報が通知される設定となっている。				
－	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毎年、区の情報セキュリティポリシーに基づいた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している。 ②申請書等の個人情報が記載された資料は鍵付の書庫に保管し、許可された人以外の使用および参照を禁じている。また書庫の鍵については担当係長のデスクの引き出しにて施錠管理の上、保管している。 ③原則データ移動のみ許可された外部記録媒体を使用し、使用管理簿に使用者・使用時間等を記載し、システム管理者等の確認を得る。			十分である	個人情報が不正に複製されることを防止するためのルールが明文化されており、情報資産管理システムにより外部接続媒体への書き出し制限、書き出した場合のログの記録と上司への通知等の措置が取られている。そのため「十分である」と評価する。
				システム	①介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ②記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。 ③情報資産管理システムにより、許可された外部記録媒体以外の媒体は端末等の機器に使用できない設定となっている。 ④情報資産管理システムにより、許可された外部記録媒体に、何のファイルをいつ、誰が書き出したのかが記録されると同時に、直属の上司に書き出した情報が通知される設定となっている。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル			システム名称	介護保険システム		
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）	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						
－	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などの認証取得状況や、情報管理体制の確認している。 ②個人情報の取扱に関与する委託契約時には、「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、立入検査等」について明記した契約を締結している。 ③委託契約締結時、委託先事業者に情報セキュリティ体制の報告・責任者等の特定を義務付けている。					
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大田区の情報セキュリティ対策基準に基づき、委託契約書には「委託先の責任者、委託内容」を明記することとしている。 ②委託事務の定期報告及び緊急時報告義務を委託契約書に明記し、アクセス権限の管理状況を定期的に報告させることとしている。 ③IDを付与する従業員数を必要最小限に制限し、付与するアクセス権限も必要最小限とする。		制限している			
				システム	①特定個人情報ファイル取扱いのユーザIDを作成し、このIDでのみへアクセスできることとする。					
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	①委託先の従業員等が大田区の介護保険に関する受給権者の個人番号を閲覧等した場合には、東京都国民健康保険団体連合会のシステム等において、特定個人情報にアクセスした従業員等・時刻・操作内容を記録することにしているので、大田区の情報セキュリティ管理者が委託契約に基づき、委託先に当該記録の開示を請求し、調査することで操作者個人を特定する。		記録を残している			
				システム	①委託先は東京都国民健康保険団体連合会に限定されており、そこでの記録については、東京都国民健康保険団体連合会が行う。また、それを確認する方法は上記の通り。					
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	【システム以外】 ①大田区の情報セキュリティ対策基準に基づき、委託先は、特定個人情報の目的外利用及び第三者に提供してはならないこと、特定個人情報の複写、複製、又はこれらに類する行為をすることはできないことなどについて委託契約書に明記することとしている。 ②個人情報の保護に関する法律第23条により、委託先においても個人情報の漏えい、滅失又は毀損の防止等に関する安全確保の措置を義務付けしている。 ③大田区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは委託先に対して調査を行い、又は報告を求める。		定めている			
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	①大田区の情報セキュリティ対策基準に基づき、委託契約書において、委託業務の定期報告及び緊急時報告を義務付けし、特定個人情報の取扱いに関して定期的に委託先から報告を受けることとしている。 ②大田区から東京都国民健康保険団体連合会への特定個人情報の送付に関しては、伝送通信ソフトで送付を行った際に送付記録を帳簿に記入している。また、記録の保存期間については、大田区の文書管理規程第38条に従い、一定期間保存する。 ③委託先に特定個人情報を提供する場合にはパスワードの設定を行うこと、及び管理者の許可を得ることを遵守するとともに、委託終了時の返還・廃棄について委託契約書に明記することとしている。さらに、大田区の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは調査を行い、又は報告を求める。					
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	①特定個人情報等は、業務完了後は速やかに返還し、又は漏えいを起こさない方法によって確実に消去、もしくは処分することを、大田区の情報セキュリティ対策基準に基づき、委託契約書に明記することとしている。 ②委託契約終了後は、委託先から特定個人情報等の消去・廃棄等に関する報告書を提出させ、情報システム管理者が消去及び廃棄状況の確認を行う。		定めている			

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル			システム名称	介護保険システム	
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）	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
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	①秘密保持義務 ②事業所内からの特定個人情報の持出しの禁止 ③特定個人情報の目的外利用の禁止 ④漏えい事案等が発生した場合の再委託先の責任の明確化 ⑤委託契約終了後の特定個人情報の返却又は廃棄 ⑥従業者に対する監督・教育 ⑦契約内容の遵守状況について報告を求める規定 等を定めるとともに委託先が大田区と同等の安全管理措置を講じていることを確認する。		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	原則として再委託は行わないこととするが、再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。 ①秘密保持義務 ②事業所内からの特定個人情報の持出しの禁止 ③特定個人情報の目的外利用の禁止 ④漏えい事案等が発生した場合の再委託先の責任の明確化 ⑤再委託契約終了後の特定個人情報の返却又は廃棄 ⑥従業者に対する監督・教育 ⑦契約内容の遵守状況について報告を求める規定 等 また再委託先が大田区と同等の安全管理措置を講じていることを確認する。		再委託していない		
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	特定個人情報の提供・移転を行わないため対象外とした。				
				システム	特定個人情報の提供・移転を行わないため対象外とした。				
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	特定個人情報の提供・移転を行わないため対象外とした。				
34	その他の措置の内容	－	【措置の内容】	－					
－	**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	特定個人情報の提供・移転を行わないため対象外とした。				
				システム	特定個人情報の提供・移転を行わないため対象外とした。				

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル			システム名称	介護保険システム	
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）	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	特定個人情報の提供・移転を行わないため対象外とした。				
				システム	特定個人情報の提供・移転を行わないため対象外とした。				
－	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】	－					
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	情報提供ネットワークシステムとの接続がないため対象外とした				
				システム	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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】	－	情報提供ネットワークシステムとの接続がないため対象外とした				
－	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	介護保険課のセキュリティ対策で安全管理体制を、次のように定めている。 ①セキュリティ管理者…介護保険課長をあてる。介護保険課が保有し、又は使用する情報資産に対する管理責任を負う ②セキュリティ対策担当…課長から委任を受け、情報セキュリティ対策の運用を実施する。		十分に整備している		
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	大田区のセキュリティ対策において、次の措置を行っている。 ①情報セキュリティ管理体制 ②情報資産の分類及び管理 ③人的な情報セキュリティ対策 ④物理的な情報セキュリティ対策 ⑤技術的な情報セキュリティ対策 ⑥運用における情報セキュリティ対策 ⑦評価・見直し		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	①毎年、セキュリティ研修を行っている。 ②職員が常にセキュリティの基準を確認できるように職員向け掲示板に掲示している。		十分に周知している		

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	2	介護保険事務　全項目評価書	特定個人情報ファイル名称	受給者台帳ファイル	システム名称	介護保険システム

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）	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
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	【大田区】 ①外部記録媒体については、大田区の情報セキュリティ対策基準に基づいた対策を行う。 ②介護保険システムのサーバーは庁舎外のデータセンターに設置されており、災害による被害を最小限にとどめる対策をとっている。 ③データセンターでは、入退室管理、各種物理サーバーの盗難防止対策等を厳格に実施している。 【東京都国民健康保険団体連合会】 ①ファイルの送受信はセキュリティの担保された専用回線で行う。 ②個人番号を管理するサーバは、既存業務処理サーバと分離する。 ③認証管理サーバを設置する。		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			十分に行っている		
				システム	【大田区】 ①介護保険システムのアクセス権限の変更及び失効機能はシステム管理者のみ可能。 ②介護保険システムの利用には生体認証システムに登録されたIDとパスワードの組み合わせによる認証が必要。 ③介護保険システムに操作ログが記録され、いつ、誰が、誰の情報にアクセスし、どのような操作をしたのかが記録される仕組みとなっている。 ④記録された操作ログについては月２回程度職員が確認を行う。その際に通常考えうるアクセス数を超える極端なアクセスのあったログが見つかった場合には該当職員に聞き取りを行う。 ⑤介護保険システムとシステム利用端末間の通信はすべて暗号化されている。 ⑥介護保険システムに登録されているデータについては日次でバックアップ処理を実施している 【東京都国民健康保険団体連合会】 ①送受信するファイルは暗号化を行う。 ②既存ファイアウォールに不正アクセス等に対するセキュリティを強化する。 ③すべてのサーバ及び端末へ外部記録媒体の管理機能及び操作ログ・収集・監査機能を設ける。 ④伝送端末向けにWindowsセキュリティパッチを配布し、定期的に更新する。 ⑤ログの収集および分析を行う。			
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			十分に行っている		
				システム	業務データのバックアップを実施する。				
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	大田区のセキュリティ対策として、次の事項を規定している。 1.庁内からの事故・欠陥等の報告手順 2.区民等からの通報による事故・欠陥等の報告手順 3.侵害時の対応		十分に行っている		
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	ー		発生なし		
			【再発防止策の内容】	システム以外	ー		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で管理している。		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で管理している。				
56	その他の措置の内容	ー	【措置の内容】	ー					
ー	**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				十分である	介護保険システムで情報を作成しており、介護保険システムで更新されたデータを連携している。
				システム	受給者台帳ファイルは更新された介護保険情報、住民記録情報をもとに作成されるため、古い情報のまま保管されることはない。				
ー	**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外部記録媒体を使用後は必ずデータを削除することとし、使用管理簿へ記載する手順を定めている。		定めている	十分である	特定個人情報が記録された文書や手順が確認できたため、「十分である」と評価する。
				システム					
59	その他の措置の内容	ー	【措置の内容】	ー					
ー	**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	ー	【措置の内容】	ー					

様式4　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	2	介護保険事務　全項目評価書

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）	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
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大田区のセキュリティ対策において毎年度の自己点検を定めている。 1.実施計画の立案 2自己点検の実施 3.点検結果の報告 4.結果に基づく改善 ②介護保険課における自己点検について、以下の内容を定めている。 ・組織長は、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。また、必要に応じて、自己点検の結果についてセキュリティ部局管理者（福祉部長）の評価を受ける。 ・組織長は、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。 介護保険課の実施手順については、必要に応じて随時改訂している。			十分に行っている	監査方法について定めた文書や手順が確認できたため、「十分である」と評価する。
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。 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。 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、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。 ②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、評価書記載内容の適正な運用状況を確認する。 この確認結果は、大田区特定個人保護評価第三者点検委員会に概要報告と意見聴取を行い、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	監査方法について定めた文書や手順が確認できたため、「十分である」と評価する。
－	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	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。 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。 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、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。 ②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、評価書記載内容の適正な運用状況を確認する。 この確認結果は、大田区特定個人保護評価第三者点検委員会に概要報告と意見聴取を行い、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	介護保険課・地域福祉課介護保険担当に対しては定期的に全職員に対してセキュリティ教育を行っており、大田区全体としてもセキュリティ研修は実施されている。そのため「十分である」と評価する。
－	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】	－					