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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）		システム名称	区民情報系基盤システム	

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	—		十分である	目的外の入手に関しては、区民情報系基盤システムの自動処理以外での入手はなく、システムにおいても必要なデータ項目以外の連携を制御しており、対象者以外の特定個人情報を保有しない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	データ連携において、必要なデータ項目以外の連携を制限し対象者以外の特定個人情報を保有しないようにしている。			
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	—			
				システム	データ連携において、必要なデータ項目以外の連携を制限し不要な情報を保有しないようにしている。			
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	—		十分である	不適切な方法での入手に関しては、区民情報系基盤システムの自動処理以外での入手はなく、他のネットワークやサーバーから容易にアクセスできない仕組みとなっている。また端末からのアクセスに関しても機器により通信を制御し暗号化している。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。 端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御し暗号化している。			
－	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	本人からの特定個人情報の入手が無いため対象外とした。		十分である	当該システムにおいては、本人からの特定個人情報の入手はない。また、正確性の担保についても適切なルールが規定されていることに加えて、不正データ発生時の処置やシステム停止に伴う誤ったファイル更新を防止する仕組となっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「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	本人からの特定個人情報の入手が無いため対象外とした。			
				システム	本人からの特定個人情報の入手が無いため対象外とした。			
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職員等が業務上必要のない情報の作成をすることを禁止している。 ②情報を作成する者は、情報の作成時に大田区で定められている、情報資産レベル・機密性・完全性・可用性による情報資産の分類に基づき、実施手順に当該情報の分類と取扱制限を定めている。			
				システム	③区民情報系基盤システムのユーザは、区民情報系基盤システムに連携されたデータやファイルに直接アクセス権を持たせない仕様としている。 ④不正なデータを連携したことによって区民情報系基盤システムが停止した場合、システム管理者が不正データを除去又は修正する機能を設けている。 ⑤特定個人情報の区民情報系基盤システム内でのデータは、連携の連番チェックを行い常に最新を担保している。			
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							
		入手の際に特定個人情報が漏えい・紛失する		システム以外	①情報を作成する者は、紛失や流出等の防止や情報の作成途中で不要になった場合の当該情報の消去を義務付けている。 ②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、情報資産の分類に応じた常時の適切な取扱を定めている。			入手の際の漏えい・紛失に関しては、適切にルールが規定されていることに加えて、システムにおいても、他のネットワークやサーバーから容易にアクセスできない仕組みであり、端末

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム

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
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	③庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。 端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御し暗号化している。 ④区民情報系基盤システムのユーザは、区民情報系基盤システムに連携されたデータやファイルに直接アクセス権を持たせない仕様としている。		十分である	からのアクセスも機器により制御し暗号化されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
－	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	①人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除し、利用されていないIDが放置されないよう、定期的に点検している。		十分である	目的を超えた紐付け、事務に必要のない情報都の紐付けに関しては、ユーザIDやパスワードの管理について適切なルールが規定されていることに加えて、システムにおいても、データ連携機能要件により目的を超えたアクセスが防止されており、さらに他のネットワークやサーバーから容易にアクセスできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。また、データ連携機能要件を定め目的を超えたアクセスを防止している。			
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	対象とするシステムは事務で使用するその他システムに該当しないため対象外とした。			
				システム	対象とするシステムは事務で使用するその他システムに該当しないため対象外とした。			
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ユーザ認証は、生体登録等によって行い、ユーザー認証情報の管理について、以下のルールを設けて適正に管理している。 ＜生体認証＞ ・生体認証でログインした際、操作者が離席した時に自動で端末画面がロックされ操作できなくなる機能等を設ける。 ＜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、他人に利用させてはならない。また、他人のIDを利用してはならない。 ＜パスワード＞ ・パスワードは、他者に知られないように管理しなければならない。 ・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しなければならない。 等	行っている		権限のない者による不正使用に関しては、ユーザIDパスワードの管理についてのルールが定められていることに加えて、
				システム	②システムにユーザ管理機能を設けている。 ③生体登録情報の認証結果を利用してシステム認証を行う機能（シングルサインオン連携）を設けている。			
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アクセス権限の発効・失効の管理として、ユーザ登録及び抹消等の手続を定めており、人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、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	②随時のアクセス権設定リクエストに対し、権限の付与・削除を行う機能を設けている。			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム

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
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人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除し、利用されていないIDが放置されないよう、定期的に点検するルールを定めている。 ②システム担当課職員への特権IDの付与状況を一元管理し、定期的にその状況をするルールを定めている。 ③管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理するルールを定めている。	行っている	十分である	システムにおいても、生体認証によるユーザ認証機能シングルサインオン連携、アクセス権限の管理機能等で制御されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	④外部からの不正アクセス、成り済ましや庁内からの不正アクセスを考慮し、アクセス権限の一覧を作成し、一覧に基づきアクセス制御等の対策を行っている。 ⑤システムへのログインを含めアクセスログを取得する機能を設けている。（取得したアクセスログは証跡が追える形式で保存する。）			
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アクセス記録及び情報セキュリティの確保に必要な記録を取得し、保管することを定めている。また、取得したアクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じている。	記録を残している		
				システム	②サーバー側のシステム管理者を含めアクセスログを出力する機能を設けている。			
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業務上予め定められた目的以外の情報資産を使用することを禁止とするルールを定めている。 ②利用を許可されていない情報の使用を禁止とするルールを定めている。 ③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、常に適切な取扱を行うこととするルールを定めている。		十分である	従業者の事務外での使用については、情報資産の利用についての適切なルールが定められていることに加えて、システム内でのみ処理を行い、他のネットワークやサーバーから容易にアクセスできない仕組みになっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。また、データ連携機能要件を定め目的を超えたアクセスを防止している。 ③サーバー側のシステム管理者を含めアクセスログを出力する機能を設けている。			
－	**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業務上必要の無い情報の作成を禁止するルールを定めている。 ②外部記憶媒体にコピーする必要がある場合、外部記憶媒体利用管理簿で管理するルールを定めている。		十分である	不正な複製に関しては、データ作成及び複製時の適切なルールが定められていることに加えて、システム内のみの処理であり他のネットワーク及びサーバーから容易にアクセスできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	③庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。また、データ連携機能要件を定め目的を超えたアクセスを防止している。 ④サーバー側のシステム管理者を含めアクセスログを出力する機能を設けている。			
－	**特定個人情報の使用におけるその他のリスク**							
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**							

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム	

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
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外部委託先において必要なセキュリティ対策が確保されていることを定期的に確認するルールを設けている。 ②システム運用・保守の外部委託先に、情報セキュリティ対策に関する管理状況を定期的に報告させるルールを設けている。 等の内容を、保守委託契約書に明記している。 ③委託先事業者全般について、定期会議等で履行状況を確認している。 ④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。 ⑤委託先事業者全般について、インシデント発生時やその予兆があった場合、速やかに報告することを義務付けている。		十分である	委託先における個人情報の管理については、「大田区個人情報保護条例」及び各種設計書、保守委託契約書、各セキュリティポリシーの規定等により、取扱ルールや管理体制・取扱権限を制限している。これらのことが実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
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委託先に対するアクセス権限の発効・失効のルールや手順を設けている。	制限している		
				システム	②委託先のユーザIDに対するアクセス権限の付与・削除・期限管理機能を設けている。			
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	①各システム及び各ネットワークの運用・システム設定変更・保守等のために実施した作業は、システム設定変更等の記録簿による管理やシステムログ等により、作業内容、作業者名等を記録するルールを定めている。	記録を残している		
				システム	②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。また、データ連携機能要件を定め目的を超えたアクセスを防止している。 ③サーバー側のシステム管理者を含めアクセスログを出力する機能を設けている。			
25	特定個人情報ファイルの提供ルール（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委託契約書により、知りえた情報の秘密の保持、第三者への提供を禁止している。	定めている		
26	特定個人情報ファイルの提供ルール（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委託契約書による外部への持出しの禁止を定めている他、保護ケース等による運搬や、暗号化、記録簿による管理などを定めている。			
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委託契約書により提供資料の返還の義務付けや、契約終了後の情報の消去等を定めている。	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	①委託契約書により、受託業務以外の目的外利用、複写複製等の禁止や、施設設備の適正な管理などを定めている。	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	委託契約書により、以下の様な適切な取扱いを担保している ①再委託先の履行について委託元の責務 ②再委託前の事前承認の義務 ③再委託先との同一管理要件による契約締結義務 など。	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**							
				システム以外	—			

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム

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
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	対象ファイル：「3.情報提供ファイル」、「4.統合宛名番号ファイル」「7.庁内連携ファイル」 ①統合宛名管理機能の管理端末を使用する際には、操作ログを残すようにしている。 連携部分については、記録を行っていないが以下の機能により、情報の完全性を担保している。 ②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。また、データ連携機能要件を定め目的を超えたアクセスを防止している。 ③特定個人情報の区民情報系基盤システム内のデータは、連携の連番チェックを行い常に最新を担保している。	記録を残していない	十分である	特定個人情報の提供・移転の記録については、システム間の連携処理を自動実行するシステムであるため、連携処理実行に関する記録は保持しているが個々の情報項目の記録は残していない。個々の情報項目の提供・移転の記録は、提供元（移転元）及び提供先（移転先）で記録されるものである。 しかしながら、対象システムにおいても、システムの自動処理以外での移転・提供がないことに加えて、設計書に記載のあるシステム以外への移転・提供は行えないこと、さらにほかのネットワークやサーバーからのアクセスが容易にできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、不正な提供・移転への対策に関しては「十分である」と評価した。
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	①区民情報系基盤システムによるデータ連携は、設計書に記載のあるシステム以外への提供は行わないルールを定めている。 ②業務で個人情報を扱う際には、個人情報保護審議会による承認が必要である。	定めている		
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	①人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除し、利用権限の無い、または利用権限の異なる操作がされないよう、定期的に点検するルールを定めている。 ②管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理するルールを定めている。 ③特権を付与されたID及びパスワードの設定・変更について、外部委託事業者へ行わせる場合の監視や作業ログの確認等を行うルールを定めている。		十分である	不適切な方法での提供・移転に関しては、ユーザID・パスワード等の管理について適正にルール化されていることに加えて、システムにおいても他のネットワークやサーバーから容易にアクセスできない仕組みとなっており、適切なユーザによる処理のみ実施できることが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	対象ファイル：「3.情報提供ファイル（情報照会結果ファイル）」、「4.統合宛名番号ファイル」「7.庁内連携ファイル」 ④庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。 端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御しロードバランサーにて暗号化している。			
－	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連携データに誤りがあるか、定期的に提供元データと突合チェックを実施する手順を設けている。		十分である	誤った情報、誤った相手への提供・移転については、連携データの整合性チェックの機能及び提供元との定期的な突合チェックを実施していることをドキュメントにより確認できたため、「十分である」と評価した。
				システム	対象ファイル：「3.情報提供ファイル（情報照会結果ファイル）」「4.統合宛名番号ファイル」「7.庁内連携ファイル」 ②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。 端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御しロードバランサーにて暗号化している。また、整合性を図る観点から各連携システムが管理する範囲にあわせて保持する仕組みとし、整合性チェックを行える仕組みを構築している。 ③区民情報系基盤システムによるデータ連携は、設計書に記載のあるシステム以外への提供を行っていない。			
－	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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）		システム名称	区民情報系基盤システム	

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
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	①情報セキュリティ管理体制は各責任者に役割を持たせ安全管理体制を構築している。	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	①情報セキュリティポリシーの各規程において、次の事項を規定している。 ・情報資産の分類に応じた管理 ・情報資産台帳とリスク分析 ・人的な情報セキュリティ対策 ・物理的な情報セキュリティ対策 ・技術的な情報セキュリティ対策 ・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	①職員全員がアクセス可能な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		

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム	

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
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	政府情報システムのセキュリティ制度（ISMAP）のリストに登録されているクラウド（以降、ガバメントクラウドを含む）事業者、またはISMAPのリストに登録予定のクラウド事業者から調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築する前提として、評価対象事務に係るシステムの設置場所において、次の物理的対策を設けている。 ・地震等の振動対策のための、床への固定等 ・盗難対策のための、固定や施錠等 ・停電時における安全な停止対策のための、無停電電源装置の設置 ・ディスク障害等のシステム障害時に備えるための、ディスクの２重化などのデータ冗長化 ・事前に許可されていない装置等を外部に持出できない ・「生体認証」による入退出の管理 などを定め、実施している。	十分に行っている	十分である	特定個人情報の漏えい・滅失・毀損については、安全管理体制・規定、職員への周知、物理的対策等が適切なルールに定められていることに加えて、不正プログラム対策や不正アクセス対策、発生時のバックアップ等の措置についても各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
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評価対象事務に係るシステムにおいて、次の様なルールを設けている。 ＜サーバー等情報システムの対策＞ ・一般ユーザのパスワードの定期的な変更 ・システム運用保守における作業の記録及び記録の適切な管理 ・ネットワーク構成図、情報システム仕様書の適切な管理　等 ＜端末機器の管理＞ ・接続する端末機器の適切な設置・変更・廃止 ・接続する端末機器の状況の定期的な確認　等 ＜ネットワークの対策＞ ・ネットワーク機器の適切な設定およびアクセス制御 ・接続するネットワーク機器の状況の定期的な確認　等 ＜ソフトウェアの管理＞ ・ソフトウェアの無断インストール禁止 ・ソフトウェアの適切な管理 ・定期的なソフトウェア導入状況の点検、およびパッチの適用　等	十分に行っている		
				システム	②庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。 端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御しロードバランサーにて暗号化している。また、整合性を図る観点から各連携システムが管理する範囲にあわせて保持する仕組みとし、整合性チェックを行える仕組みを構築している。 ③評価対象事務に係るシステムにおいて、次の技術的対策を講じている。 ＜不正プログラム対策＞ ・不正プログラム対策ソフトウェアのパターンファイルの最新化 ・不正プログラム対策のソフトウェアの更新 ＜不正アクセス対策＞ ・攻撃の記録の保存 ・庁内のサーバー等に対する攻撃や外部のサイトに対する攻撃の監視 ＜データ暗号化＞ ・データを保管するストレージ筐体全体のデータ暗号化 ④クラウド事業者は利用者のデータにアクセスしない契約等となっている。 ⑤区民情報系基盤システムの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑥クラウド事業者の運用保守地点からクラウドサービスへの接続については、閉域ネットワークで構成する。	十分に行っている		
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外部委託先におけるバックアップデータを記録した媒体の保管のルールや手順を定めている。 ②情報システムのバックアップで取得した完全性又は可用性の高いデータは、災害等の被害を受けにくい遠隔地に保管している。 ③原則として端末に情報資産を保存してはならず、また、指定端末以外の情報機器内に情報資産を保存する場合は、定期的なバックアップの取得等の必要な対策をとることを定めている。	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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム

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
				システム	④漏洩・滅失・毀損リスクに対策として、庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御しロードバランサーにて暗号化している。 ⑤滅失・毀損から確実かつ迅速にリカバリが行えるよう世代管理を行いバックアップを実施している。			
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	①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設けている。 ・情報セキュリティ事故を発見した場合の、事故・障害のあった対象、事故・障害の状況、業務への影響等を連絡・報告する。 ・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。 ・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・保管する。 ②職員への当該手順の周知を行っている。	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を確認すること	【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	生存者と同様に管理しているため、以下の規定等を定めている。 ①情報システムのバックアップで取得した完全性又は可用性の高いデータは、災害等の被害を受けにくい遠隔地に保管する。 ②指定端末以外の情報機器内に情報資産を保存する場合は、定期的なバックアップの取得等の必要な対策を義務付けている。	保管していない		
				システム	③漏洩・滅失・毀損リスクに対策として、庁内で稼働するシステムのネットワークを「区民情報系事務」「内部情報系事務」「インターネット接続環境」と各々分離させ、他の領域と通信をできないようにしている。端末からのアクセスは、区民情報系基盤システム内にある通信機器やファイアウォールにて通信を制御しロードバランサーにて暗号化している。 また、滅失・毀損から確実かつ迅速にリカバリが行えるよう世代管理を行いバックアップを実施している。			
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	―		十分である	情報の完全性について、完全性・可用性の担保のための適切なルールが定められていることに加えて、システムにおいても同実施手順をうけて、データ連携時の連番チェックやバックアップなどの仕組みにより、古い情報のまま保管されない措置が行われている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	①特定個人情報の区民情報系基盤システム内のデータは、連携の連番チェックを行い常に最新を担保している。 また、滅失・毀損から確実かつ迅速にリカバリが行えるよう世代管理を行いバックアップを実施している。 ②区民情報系基盤システムへデータが格納される項目ごとに、中間サーバーへ当該データを連携する間隔を定義し、データ連携を実施するよう設計されている。 ③バックアップデータはストレージで記録する際に世代管理を行い、最新のデータを担保し古い世代のバックアップデータを保持し続けない設計になっている。			
－	**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**							
				システム以外	①サーバー等の廃棄に伴うデータ消去については、廃棄サーバーに記録されたデータやファイルを、消磁機や消去ソフトを使用して、又は破砕するなど完全に復元できないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去するする手順を設けている。			特定個人情報の消去については、情報資産の廃棄について

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.情報参照ファイル（情報照会依頼ファイル） 3.情報提供ファイル（情報照会結果ファイル）	システム名称	区民情報系基盤システム	

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
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	②区民情報系サーバ機器群上に構築されているシステムで利用しているサーバー等の廃棄に伴うデータ消去については、廃棄サーバーやディスクに記録されたデータやファイルを、消磁機や消去ソフトを使用して、又は破砕するなど完全に復元できない状態とし、HDD消去記録票にて管理している。	定めている	十分である	の適切なルールが定められていることに加えて、システムにおける消去手順も整備されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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	—		十分である	目的外の入手に関しては、区民情報系基盤システムの自動処理以外での入手はなく、システムにおいても必要なデータ項目以外の連携を制御しており、対象者以外の特定個人情報を保有しない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	①中間サーバー機器と区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている			
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	—			
				システム	①中間サーバー機器と区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている			
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	—		十分である	不適切な方法での入手に関しては、区民情報系基盤システムの自動処理以外での入手はなく、他のネットワークやサーバーから容易にアクセスできない仕組みとなっている。また端末からのアクセスに関しても機器により通信を制御し暗号化している。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	①中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている			
－	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	本人からの特定個人情報の入手が無いため対象外とした。		十分である	当該システムにおいては、本人からの特定個人情報の入手はない。また、正確性の担保についても適切なルールが規定されていることに加えて、不正データ発生時の処置やシステム停止に伴う誤ったファイル更新を防止する仕組となっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「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	本人からの特定個人情報の入手が無いため対象外とした。			
				システム	本人からの特定個人情報の入手が無いため対象外とした。			
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	—			
				システム	① 中間サーバー機器と区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている ③区民情報系基盤システムから連携された特定個人情報を副本として情報提供データベースへ反映させる機能を持っている ④区民情報系基盤システムの持つ正本と中間サーバーが持つ副本の整合性を確認できるよう、副本をファイルとして出力する機能を持っている			
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	—		十分である	入手の際の漏えい・紛失に関しては、適切にルールが規定されていることに加えて、システムにおいても、他のネットワークやサーバーから容易にアクセスできない仕組みであり、端末からのアクセスも機器により制御し暗号化されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	①中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている			
－	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】	－	—			
－	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							

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	権限の無い者がシステムを操作し、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ないように、以下の対策を行なっている。 ①人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除し、利用されていないIDが放置されないよう、定期的に点検している。		十分である	目的を超えた紐付け、事務に必要のない情報都の紐付けに関しては、ユーザIDやパスワードの管理について適切なルールが規定されていることに加えて、システムにおいても、データ連携機能要件により目的を超えたアクセスが防止されており、さらに他のネットワークやサーバーから容易にアクセスできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたたため、「十分である」と評価した。
				システム	②中間サーバー機器と区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ③特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている			
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	対象とするシステムは事務で使用するその他システムに該当しないため対象外とした。			
				システム	対象とするシステムは事務で使用するその他システムに該当しないため対象外とした。			
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ユーザ認証情報の管理について、以下のルールを設けて適正に管理している。 ＜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、他人に利用させてはならない。また、他人のIDを利用してはならない。 ＜パスワード＞ ・パスワードは、他者に知られないように管理しなければならない。 ・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しなければならない。 等		十分である	権限のない者による不正使用に関しては、ユーザIDパスワードの管理についてのルールが定められていることに加えて、システムにおいても、生体認証によるユーザ認証機能シングルサインオン連携、アクセス権限の管理機能等で制御されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたたため、「十分である」と評価した。
				システム	②中間サーバーの認証・権限管理機能により、中間サーバーへログインする利用者のアクセス権限の登録、更新、削除等を行っている			
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アクセス権限の発効・失効の管理として、ユーザ登録及び抹消等の手続を定めており、人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除する手順を設けている。			
				システム	②中間サーバーの認証・権限管理機能により、中間サーバーへログインする利用者のアクセス権限の登録、更新、削除等を行っている			
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	アクセス権限の管理について、以下のルールを設けて適正に管理している。 ①人事異動の発令や担当する職務の変更等があるときは、その都度ユーザ登録の状況を点検し、異動、退職等で不要になったユーザIDは、速やかに削除し、利用されていないIDが放置されないよう、定期的に点検している。 ②システム担当課職員への特権IDの付与状況を一元管理し、定期的にその状況を点検している。 ③管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理する。 などの対策を行なっている。			
				システム	④中間サーバーの認証・権限管理機能により、中間サーバーへログインする利用者のアクセス権限の登録、更新、削除等を行っている			

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー	

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
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アクセス記録及び情報セキュリティの確保に必要な記録を取得し、保管することを定めている。また、取得したアクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じている。			
				システム	②中間サーバーを利用して情報照会及び提供を行った際のアクセス記録を保持し、アクセス記録の検索、抽出、出力等の機能を持っている			
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	従業者が不正に使用しないように、 ①（1）情報資産を利用する者の業務上予め定められた目的以外の情報資産使用禁止。利用を許可されていない情報の使用禁止。 （2）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、常に適切な取扱を行うこと。 などを定めている。		十分である	従業者の事務外での使用については、情報資産の利用についての適切なルールが定められていることに加えて、システム内でのみ処理を行い、他のネットワークやサーバーから容易にアクセスできない仕組みになっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたたため、「十分である」と評価した。
				システム	②中間サーバーを利用して情報照会及び提供を行った際のアクセス記録を保持し、アクセス記録の検索、抽出、出力等の機能を持っている			
－	**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	不正に複製されることが無い様に ①業務上必要の無い情報の作成を禁止するルールを定めている。 ②外部記憶媒体にコピーする必要がある場合、外部記憶媒体利用管理簿で管理するルールを定めている。		十分である	不正な複製に関しては、データ作成及び複製時の適切なルールが定められていることに加えて、システム内のみの処理であり他のネットワーク及びサーバーから容易にアクセスできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたたため、「十分である」と評価した。
				システム	③中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている ④中間サーバーを利用して情報照会及び提供を行った際のアクセス記録を保持し、アクセス記録の検索、抽出、出力等の機能を持っている			
－	**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外部委託先において必要なセキュリティ対策が確保されていることを定期的に確認するルールを設けている。 ②システム運用・保守の外部委託先に、情報セキュリティ対策に関する管理状況を定期的に報告させるルールを設けている。 等の内容を、保守委託契約書に明記している。 ③委託先事業者全般について、定期会議等で履行状況を確認している。 ④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。 ⑤委託先事業者全般について、インシデント発生時やその予兆があった場合、速やかに報告することを義務付けている。			
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委託先に対するアクセス権限の発効・失効のルールや手順を設けている。			
				システム	②中間サーバーの認証・権限管理機能により、中間サーバーへログインする利用者のアクセス権限の登録、更新、削除等を行っている			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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各システム及び各ネットワークの運用・システム設定変更・保守等のために実施した作業は、システム設定変更等の記録簿による管理やシステムログ等により、作業内容、作業者名等を記録するルールを定めている。 ②作業などで必要となるハードディスク等の媒体は区が用意したものを使い、外部へ持ち出せないように管理している。		十分である	委託先における個人情報の管理については、「大田区個人情報保護条例」及び各種設計書、保守委託契約書、各セキュリティポリシーの規定等により、取扱ルールや管理体制・取扱権限を制限している。これらのことが実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	③中間サーバーを利用して情報照会及び提供を行った際のアクセス記録を保持し、アクセス記録の検索、抽出、出力等の機能を持っている			
25	特定個人情報ファイルの提供ルール（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委託契約書により、知りえた情報の秘密の保持、第三者への提供を禁止している。			
26	特定個人情報ファイルの提供ルール（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委託契約書による外部への持出しの禁止を定めている他、保護ケース等による運搬や、暗号化、記録簿による管理などを定めている。			
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委託契約書により提供資料の返還の義務付けや、契約終了後の情報の消去等を定めている。			
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	①委託契約書により、受託業務以外の目的外利用、複写複製等の禁止や、施設設備の適正な管理などを定めている。			
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	委託契約書により、以下の様な適切な取扱いを担保している ①再委託先の履行について委託元の責務 ②再委託前の事前承認の義務 ③再委託先との同一管理要件による契約締結義務 など。			
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	―		十分である	特定個人情報の提供・移転の記録については、システム間の連携処理を自動実行するシステムであるため、連携処理実行に関する記録は保持しているが個々の情報項目の記録は残していない。個々の情報項目の提供・移転の記録は、提供元（移転元）及び提供先（移転先）で記録されるものである。 しかしながら、対象システムにおいても、システムの自動処理以外での移転・提供がないことに加えて、設計書に記載のあるシステム以外への移転・提供は行えないこと、さらにほかのネットワークやサーバーからのアクセスが容易にできない仕組みとなっている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、不正な提供・移転への対策に関しては「十分である」と評価した。
				システム	対象ファイル：「1.提供情報ファイル」 ①中間サーバーを利用して情報照会及び提供を行った際のアクセス記録を保持し、アクセス記録の検索、抽出、出力等の機能を持っている ②区民情報系基盤システムから連携された特定個人情報を副本として情報提供データベースへ反映させる機能を持っている			
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区民情報系基盤システムとのデータ連携は、区民情報系基盤システム設計書に記載のあるシステム以外への提供は行わないルールを定めている。 ②業務で個人情報を扱う際には、個人情報保護審議会による承認が必要である。			
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**							
				システム以外	―			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	対象ファイル：「1.提供情報ファイル」 ①中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている。 ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている。 ③中間サーバーの認証・権限管理機能により、中間サーバーへログインする利用者のアクセス権限の登録、更新、削除等を行っている。		十分である	不適切な方法での提供・移転に関しては、ユーザID・パスワード等の管理について適正にルール化されていることに加えて、システムにおいても他のネットワークやサーバーから容易にアクセスできない仕組みとなっており、適切なユーザによる処理のみ実施できることが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
－	**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	—		十分である	誤った情報、誤った相手への提供・移転については、連携データの整合性チェックの機能及び提供元との定期的な突合チェックを実施していることをドキュメントにより確認できたため、「十分である」と評価した。
				システム	対象ファイル：「1.提供情報ファイル」 ①中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている。 ②特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている。 ③中間サーバーと区民情報系基盤システムのデータ連携は、区民情報系基盤システム設計書に記載のあるシステム以外への提供を行っていない。			
－	**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。		十分である	目的外の入手に関しての適切なルールが規定されていることに加えて、システムにおいても、職員の権限管理、マスター管理、照合リストによりアクセスを管理する仕組みとなっている。これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
				システム	対象ファイル：「2.符号管理ファイル」 中間サーバー・ソフトウェアにおける措置 ②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、情報提供許可証の発行と照会内容の照会許可用照合リストとの照合を情報提供ネットワークシステムに求め、情報提供許可証を受領してから情報照会を実施する仕組みになっている。 　これにより番号法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。 ③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。 ④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可能としている。			
－	**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**							
				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 ①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。 等			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	対象ファイル：「2.符号管理ファイル」 中間サーバーは個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されている。 ②中間サーバーと情報提供ネットワークシステムとの間は、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。 　また中間サーバー・ソフトウェアが動作するサーバー、運用端末、管理端末及び中間サーバー接続端末は、原則他の業務システムとは物理的に独立した専用機器を用いる。 ③中間サーバー・ソフトウェアが動作するサーバー、運用端末及び管理端末は、専用の安全な区画に設置し、サーバーに専用回線を用い、接続できるクライアントを制限する。 ④中間サーバー接続端末は、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。 ⑤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。 ⑥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		十分である	入手の安全性に関しては、ICカード、ユーザID、パスワードの管理について適切なルールが規定されていることに加えて、システムにおいても独立した物理構成・ネットワークとなっており、さらに不正アクセス等を検知する仕組みとなっている。これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
－	リスク3：囚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	—		十分である	入手時の正確性については、中間サーバーの処理以外で特定個人情報の入手ができないことに加えて、国より提供される仕組みにより担保されている。 これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
				システム	対象ファイル：「2.符号管理ファイル」 ①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。 ②提供先においても、誤った情報を提供した場合の措置が担保されている。 中間サーバー・ソフトウェアにおける措置 ③中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・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：囚手の際に特定個人情報が漏えい・紛失するリスク							
				システム以外	入手の際に情報漏えい・紛失しないように ①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。 ②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。 ことなどを定める。			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	中間サーバー・ソフトウェアにおける措置 ③特定個人情報を送信する際は暗号化を行っており、受信する際には復号を行っている。 　また、情報照会が完了または中断した情報照会結果については、一定期間経過後に自動削除する。 ④情報提供ネットワークを介して特定個人情報を送信する際、暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。 ⑤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。 ⑥ログの取得を行い、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。 ⑦中間サーバーと情報提供ネットワークシステムとの間は、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。		十分である	入手時の漏えい・紛失については、情報資産の利用時・情報の作成時の管理ルールが適切に規定されていることに加えて、システムにおいても権限管理及びアクセス管理、暗号化の措置が取られている仕組みになっている。 これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
－	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	①機密性の高い情報資産を他部署等に提供する者は、事前にセキュリティ管理者に許可を得るよう規定が定められている。		十分である	不正な提供に関しては、機密性の高い情報資産の取り扱いについて適切にルールが規定されていることに加えて、システムにおいても権限情報管理や職員認証機能、アクセス制御等の仕組みにより措置されている。 これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
				システム	対象ファイル：「1.提供情報ファイル」 中間サーバー・ソフトウェアにおける措置 ②情報提供ネットワークシステムから配信されるマスター（照合許可用照合リスト情報、この情報を構成する機関コード、事務コード、特定個人情報種別コード等のマスター情報）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。 　特に慎重な対応を求められる情報については、自動応答を行わないように自動応答不可フラグを設定し、送信内容を改めて確認したうえで提供を行う。 ③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。 ④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可能とする。			
－	リスク6：不適切な方法で提供されるリスク							
				システム以外	①情報資産を利用する者は、業務の予め定められた目的以外に情報資産を利用することを禁止されている。			

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	対象ファイル：「1.提供情報ファイル」 中間サーバー・ソフトウェアにおける措置 ②情報提供ネットワークシステムから配信されるマスター（照合許可用照合リスト情報、この情報を構成する機関コード、事務コード、特定個人情報種別コード等のマスター情報）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。 　情報提供の際には、情報提供ネットワークシステムから情報提供許可証とともに情報照会者までの経路情報を受領し提供する情報を生成する。 ③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。 ④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可能とする。 ⑤中間サーバーと情報提供ネットワークシステムとの間は、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。		十分である	不適切な提供については、情報資産の利用についての適切なルールが定められていることに加えて、システムにおいても職員権限情報、権限管理機能、アクセス制御等の仕組みにより措置されている。これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
－	**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	①機密性の高い情報資産の完全性を確保するため、処理・入力時の複数確認を行うよう規定が定められている。 ②機密性の高い情報資産を他部署等に提供する者は、事前にセキュリティ管理者に許可を得るよう規定が定められている。		十分である	誤った情報、誤った相手への提供については、機密性の高い情報資産の完全性確保のための適切なルールが定められていることに加えて、システムにおいてもアクセス記録やマスタ照合、定期的なデータ突合等の仕組みにより措置されている。 これらのことが国により策定された中間サーバーの各種ドキュメントに記載されており、かつ実際に利用する国のASPサービスに適用されることが確認できたため、「十分である」と評価した。
				システム	対象ファイル：「1.提供情報ファイル」 中間サーバー・ソフトウェアにおける措置 ③情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、照会内容に対応した情報提供を行う。また、保管されたアクセス記録より提供先情報を抽出する機能を有している ④「情報提供データベースへのインポートデータ」の形式チェック及び中間サーバー接続端末の画面表示により情報提供データベースの内容を確認することができる。 ⑤正本・副本に差異が無いかを確認するために定期的に突合用ファイルを出力するための突合用ファイル出力機能を有している ⑥情報提供ネットワークシステムから配信されるマスター（照合許可用照合リスト情報、この情報を構成する機関コード、事務コード、特定個人情報種別コード等のマスター情報）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	①情報セキュリティ管理体制は各責任者に役割を持たせ安全管理体制を構築している。			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	①情報セキュリティポリシーの各規程において、次の事項を規定している。 ・情報資産の分類に応じた管理 ・情報資産台帳とリスク分析 ・人的な情報セキュリティ対策 ・物理的な情報セキュリティ対策 ・技術的な情報セキュリティ対策 ・運用におけるセキュリティ対策		十分である	特定個人情報の漏えい・滅失・毀損については、安全管理体制・規定、職員への周知、物理的対策等が適切なルールに定められていることに加えて、不正プログラム対策や不正アクセス対策、発生時のバックアップ等の措置についても各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
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職員全員がアクセス可能なグループウェアに掲示し周知している。			
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	<中間サーバーにおける対策> 　中間サーバーをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理を実施している。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避している。 <大田区における対策> ①評価対象事務に係るシステムの設置場所において、次の物理的対策を設けている。 ・地震等の振動対策のための、床への固定等 ・盗難対策のための、固定や施錠等 ・停電時における安全な停止対策のための、無停電電源装置の設置 ・ディスク障害等のシステム障害時に備えるための、ディスクの2重化などのデータ冗長化 ・「生体認証」による入退室の管理			
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評価対象事務に係るシステムにおいて、次の様なルールを設けている。 ＜サーバー等情報システムの対策＞ ・一般ユーザのパスワードの定期的な変更 ・システム運用保守における作業の記録及び記録の適切な管理 ・ネットワーク構成図、情報システム仕様書の適切な管理等 ＜端末機器の管理＞ ・接続する端末機器の適切な設置・変更・廃止 ・接続する端末機器の状況の定期的な確認　等 ＜ネットワークの対策＞ ・ネットワーク機器の適切な設定およびアクセス制御 ・接続するネットワーク機器の状況の定期的な確認　等 ＜ソフトウェアの管理＞ ・ソフトウェアの無断インストール禁止 ・ソフトウェアの適切な管理 ・定期的なソフトウェア導入状況の点検　等			
				システム	②中間サーバーでは、UTM（コンピューターウィルスやハッキングなどの脅威からネットワークを包括的に保護する装置）の導入により、アクセス制限、侵入検知、侵入防止対策を行っている。 　また、機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化をおこなっている。また、中間サーバー機器はマシンルーム等の安全な区画に設定している。 ③特定個人情報を取り扱う利用事務ごとにアクセス制御を行う ④中間サーバーにはウィルス対策ソフトを導入し、パターンファイルの更新を行う。また、OS及びミドルウェアに対しても、必要に応じてセキュリティパッチの適用を行う。			

【全項目評価書版】

評価書番号及び評価書名	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル	システム名称	中間サーバー

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
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	適切なバックアップを行うために ①外部委託先におけるバックアップを記録した媒体の保管のルールや手順を定めている。 ②情報システムのバックアップで取得した完全性又は可用性の高いデータを記録する外部記録媒体は、災害等の被害を受けにくい遠隔地に保管している。 ③原則として端末に、情報資産を保存してはならず、また、指定端末以外の情報機器内に情報資産を保存する場合は、定期的なバックアップの取得等の必要な対策をとることを定めている。			
				システム	④中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている。また、中間サーバー機器はマシンルーム等の安全な区画に設定している。 ⑤特定個人情報を取り扱う利用事務ごとにアクセス制御を行っている。 ⑥中間サーバーのバックアップ要件を以下と定めている。 利用範囲　ユーザエラーによるデータ損失からの回復を目標とする 取得間隔　日次バックアップを取得する 保存期間　1年未満とする			
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	①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設けている。 ・情報セキュリティ事故を発見した場合の、事故・障害のあった対象、事故・障害の状況、業務への影響等を連絡・報告する手順。 ・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手順。 ・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保管ルール。 ②職員への当該手順の周知を行っている。			
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	－			
			【再発防止策の内容】	システム以外	－			
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	生存者と同様に管理しているため、以下の規定等を定めている。 ①情報システムのバックアップで取得した完全性又は可用性の高いデータを記録する外部記録媒体は、災害等の被害を受けにくい遠隔地に保管する。 ②指定端末以外の情報機器内に情報資産を保存する場合は、定期的なバックアップの取得等の必要な対策を義務付け。			
				システム	③中間サーバー機器は、他のシステムとは物理的に独立した機器構成をしており、区民情報系基盤システムとの通信は、ファイアウォールによる通信制御及びLGWANサーバー証明書を用いたSSL通信による暗号化を行っている。また、中間サーバー機器はマシンルーム等の安全な区画に設定している。 ④特定個人情報を取り扱う利用事務ごとにアクセス制御を行う。 ⑤中間サーバーのバックアップ要件を以下と定めている。 利用範囲　ユーザエラーによるデータ損失からの回復を目標とする 取得間隔　日次バックアップを取得する 保存期間　1年未満とする			
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**							
				システム以外	―			情報の完全性について、完全性・可用性の担保のための適

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	（評価書番号）	特定個人情報保護評価書共通別添資料（番号法実施に伴う情報連携機能　全項目評価書）	特定個人情報ファイル名称	1.提供情報ファイル 2.符号管理ファイル		システム名称	中間サーバー	
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
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	①区民情報系基盤システムから連携された特定個人情報を副本として情報提供データベースへ反映させる機能を持っている ②区民情報系基盤システムの持つ正本と中間サーバーが持つ副本の整合性を確認できるよう、副本をファイルとして出力する機能を持っている		十分である	切なルールが定められていることに加えて、システムにおいても同実施手順をうけて、データ連携時の連番チェックやバックアップなどの仕組みにより、古い情報のまま保管されない措置が行われている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
－	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サーバー等の廃棄に伴うデータ消去については、廃棄サーバーに記録されたデータやファイルを、消磁機や消去ソフトを使用して、又は破砕するなど完全に復元できない状態として廃棄する手順を設けている。		十分である	特定個人情報の消去については、情報資産の廃棄についての適切なルールが定められていることに加えて、システムにおける消去手順も整備されている。 これらのことが各種ドキュメントに記載されており、かつ実際の運用においても実行されていることが確認できたため、「十分である」と評価した。
				システム	②情報提供データベースの削除予定日を迎えると削除する機能を持っている			
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】	－	―			