【Ⅴ.3.③別紙】

第三者点検委員会からの意見と結果について
【第1回　平成27年8月19日実施分】

No	評価書該当箇所	意見内容	意見提出者	評価書修正箇所	主管課意見
1	全体	適切な時期における評価の実施がされていますか。	委員会	―	評価・開発のスケジュールとしては、27年9月以降にシステム改修（パッケージ）を開始する予定です。
2	Ⅲ　リスク対策 3. 特定個人情報の使用 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	アクセス権限の手続きの確認、点検の確認の体制を推進していただきたい。	委員会	―	アクセス権限の付与及び削除、権限の定期的な確認等今後の体制について、点検委員会にて説明しました。
3	Ⅲ　リスク対策 4. 特定個人情報ファイルの取扱いの委託 リスク　委託先における不正な使用等のリスク	委託業者用のシステム利用ID管理及び委託先点検による運用確認を継続的に実施していただきたい。	委員会	-	利用IDの管理や委託作業の運用等について、点検委員会にて説明しました。
4	Ⅲ　リスク対策 9. 従業者に対する教育・啓発 従業者に対する教育・啓発	研修については受講者の理解度を確認することが望ましい。	委員会	-	セキュリティテストの実施や大田区情報セキュリティ対策標準実施手順の所在を常に明らかにし理解度の確保に努めます。
5	Ⅱ　特定個人情報ファイルの概要 6.特定個人情報の保管・消去 保管場所	サーバー室への入室について、事前申請さえすればある程度の職員が出入りできる状態に見える。重要な情報を扱う場所でセキュリティが甘いように思える。	委員会		情報システム課職員より、サーバー室への入退室許可について、入室制限を厳密に行っていることを点検委員会にて説明しました。
6	評価補足シート 9教育・啓発 9.1.1従業員に対する教育・啓発の具体的な方法 評価結果に至った理由	②研修等の実施方法が確立されている。とあるが、確立されているだけでなく、「実際に行っている」ので十分に評価できるという表現にする。	委員会	②研修等の実施方法が確立しており、実際に行っている	下線部のとおり修正しました。

【Ⅴ.3.③別紙】

第三者点検委員会からの意見と結果について
【第2回　令和元年10月17日実施分】

No	評価書該当箇所	意見内容	意見提出者	評価書修正箇所	主管課意見
1	全体	再評価の概要にある委託の変更が再評価の対象となるのであれば、H29年にも機会があったのではないか。	委員会	(別添2)変更箇所中、当該行の提出時期にかかる説明欄 (都広域連合による評価事項のため削除)	従前の評価書には、広域連合の委託分まで記載していたため、平成29年に見直して、重要な変更ではなく軽微な修正という扱いで修正したものであると説明。評価書については下線部のとおり追記。
2	全体	H28に、氏名情報に個人番号が追加されているが誤記の訂正か。 この時点で別の個人番号に関わる点検作業により点検が行われた旨を追記すべきと思われるが。	委員会	ー	H28より個人番号の取扱いを開始した。その後、毎年実施している自己点検の際、追記した。なお、個人番号を追記した項目の変更は、重要な変更箇所と定められている個所ではないため、再実施のための第三者点検委員会は行っていないと説明。
3	全体	「システムサーバー」は固有名詞なのか。入室は生体認証のみか。生体認証だけで精度の問題は無いのか。入退室制限を行っていないとの回答もあったが、どの程度の目的で監視しているのか。また、総称であれば「サーバー」が適切と思われる。	委員会	ー	評価書中の「サーバー」の記載は、固有名詞ではなく総称。また、入室は、生体認証のみであるが、その他複数のセキュリティ対策を実施している。外部記録媒体については、データセンターとは別の事務室内で、鍵のかかる保管庫を保管場所と指定している。また、利用については、管理簿で管理していると説明。
4	【後期高齢者医療システム関連情報ファイル分】Ⅲリスク対策 2. 特定個人情報の入手　リスクに対する措置の内容	ログの管理について、頻度の記載が求められる。	委員会	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、おおむね3か月に1回程度確認し不正なアクセスを監視している。	下線部のとおり追記
5	【後期高齢者医療システム関連情報ファイル】Ⅲ　リスク対策 3. 特定個人情報の使用　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　ユーザ認証の管理(具体的な管理方法)	「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」の部分のみ箇条書きのため違和感がある。 また特権アクセスに関する記載が必要である。	委員会	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。 ④管理者権限はシステムベンダ-がメンテナンス時のみ利用可となっている。	下線部のとおり追記
6	【両ファイルとも】Ⅲ　リスク対策 4. 特定個人情報ファイルの取扱いの委託　リスク:　委託先における不正な使用等のリスク　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(規定の内容)	機密情報の指定・必要な保護措置等が具体的に示されてない。秘密の保持についても同様である。	委員会	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)	下線部のとおり追記

【Ⅴ.3.③別紙】

第三者点検委員会からの意見と結果について
【第2回　令和元年10月17日実施分】

No	評価書該当箇所	意見内容	意見提出者	評価書修正箇所	主管課意見
7	【後期高齢者医療システム関連情報ファイル】Ⅲ　リスク対策 4．特定個人情報ファイルの取扱いの委託　リスク：　委託先における不正な使用等のリスク	評価補足シートの評価結果に至った理由③システムベンダなどから確認できることは意味がないと思われるが。	委員会	（評価補足シート） 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	下線部のとおり追記
8	【後期高齢者医療システム関連情報ファイル】Ⅲ　リスク対策 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　リスク1： 特定個人情報の漏えい・滅失・毀損リスク	アクセスの記録・確認・管理に関する記述が求められる。	委員会	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。	左記のとおり追記
9	【後期高齢者医療システム関連情報ファイル】Ⅲ　リスク対策 9．従業員に対する教育・啓発 従業者に対する教育・啓発（具体的な方法）	具体的な方法欄に各出張所でのセキュリティ研修の実施内容を追記されたい。	委員会	出張所の従事者に対する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。	左記のとおり追記
10	【後期高齢者医療関連情報ファイル】Ⅲ　リスク対策　　3．特定個人情報の使用　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　ユーザ認証の管理 （具体的な管理方法）	生体認証は行っていないのか。 アカウントロック、自動ログアウトは「システム」ではないか。 離席時のログアウトは、「システム以外」ではないか。	委員会	【システム以外】 ・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 【標準システム】 ・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。 ・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	生体認証も行っていると説明し、下線部のとおり追記。システム以外とシステムで記載を誤っていた箇所は移記。
11	【後期高齢者医療関連情報ファイル】Ⅲ　リスク対策　　4．特定個人情報ファイルの取扱いの委託 リスク：　委託先における不正な使用等のリスク	評価結果の理由としては、システムは連合の評価を使用してもよいが、システム以外は大田区の措置内容に基づいて大田区が評価すべきである。	委員会	（評価補足シート） 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 以上より、「十分である」と評価した	左記のとおり修正

【Ⅴ.3.③別紙】

第三者点検委員会からの意見と結果について
【第2回　令和元年10月17日実施分】

No	評価書該当箇所	意見内容	意見提出者	評価書修正箇所	主管課意見
12	【後期高齢者医療関連情報ファイル】 Ⅲ リスク対策　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: 不正な提供・移転が行われるリスク 特定個人情報の提供・移転に関するルール（ルールの内容及びルール遵守の確認方法）	提供・移転の事実の記録・確認・管理の記述が求められる。	委員会	データ連携の記録はログにより確認している。	左記のとおり追記
13	【後期高齢者医療関連情報ファイル】Ⅲ リスク対策　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 リスク1: 特定個人情報の漏えい・滅失・毀損リスク	アクセスの記録・確認・管理に関する記述が求められる。	委員会	・システムへのアクセス記録はログにより確認している	左記のとおり追記
14	【後期高齢者医療関連情報ファイル】Ⅲ リスク対策　9. 従業員に対する教育・啓発 従業者に対する教育・啓発（具体的な方法）	従業者に対する教育は大田区の実施事項であり、評価理由は大田区の措置の内容に対して実施されるものである。修正の検討を要す。	委員会	（補足シート） 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	左記のとおり修正

【Ⅴ.3.③別紙】

第三者点検委員会からの意見と結果について
【第3回　令和4年6月8日実施分】

No	評価書該当箇所	意見内容	意見提出者	評価書修正箇所	主管課意見
1	全体	監査の記述が評価補足シートと基礎項目評価書、および重点項目評価書で異なっており、実態が分からない。	委員会	基礎項目評価書 Ⅳ 6. 監査 実施の有無 [〇]自己点検 [〇]内部監査 [〇]外部監査 重点項目評価書 Ⅲ1. 後期高齢者医療システム関連情報ファイル 8. 監査 実施の有無 [〇]自己点検 [ ]内部監査 [〇]外部監査 Ⅲ1. 後期高齢者医療関連情報ファイル 8. 監査 実施の有無 [〇]自己点検 [〇]内部監査 [〇]外部監査	大田区の責任範囲における運用監査については、平成29年度及び令和4年度に外部監査を実施。また、標準システムについて、広域連合は毎年内部監査を実施している。 評価書の記載誤りのため、左記のとおり修正する。
2	全体	「後期高齢者医療システム関連情報ファイル」と「後期高齢者医療関連情報ファイル」の違いが分かりづらい。	委員会	－	「後期高齢者医療システム関連情報ファイル」は、大田区の後期高齢者医療システムで取り扱うファイル、「後期高齢者医療関連情報ファイル」は、広域連合の標準システムで取り扱うファイルである。今後記載方法を検討する。
3	Ⅰ　基本情報　2. 特定個人情報ファイルを取り扱う事務において使用するシステム　システム1　後期高齢者医療システム　③他のシステムとの接続	システム1　情報提供ネットワークシステムへの接続とすべきではないのか。	委員会	－	情報提供ネットワークシステムとは、情報連携機能（区民情報系基盤）を介して接続しており、直接連携していない。 情報提供ネットワークシステムへの接続は、情報連携機能（共通別添資料）で記載。
4	Ⅱ特定個人情報ファイルの概要 後期高齢者医療システム関連情報ファイル 2. 基本情報　④記録される項目 全ての記録項目	連携後の公金受取口座情報はNo29（口座情報）に含まれると考えてでよいか。	委員会	－	No.29（口座情報）に該当する。
5	Ⅲリスク対策 後期高齢者医療システム関連情報ファイル 後期高齢者医療関連情報ファイル 3. 特定個人情報の使用 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	パスワードの定期的変更について、最近は定期変更を定めず、パスワードの複雑性を重視する場合が多いが、定期変更しているとの理解でよいか。	委員会	－	ログインパスワードについては、180日ごとに強制的に変更を要求される仕組みとなっている。
6	Ⅲリスク対策 後期高齢者医療システム関連情報ファイル 6. 情報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　リスクに対する措置の内容	【システム外】 公金受取口座利用意志は窓口での申請時等に関わるのか。関わるならば本人の確認が行われる。	委員会	－	還付等の申請書で利用の意思を記載していただくことを想定。 申請書に印字された被保険者番号により、本人確認及び情報連携を実施する。 （申請書にマイナンバーは記載されない）