【Ⅴ3.③別紙】　第三者点検及び第三者点検委員会事務局からの意見と結果について

第三者点検委員会（平成27年度対応分）

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	Ⅱ特定個人情報ファイルの概要 2.基本情報 ④記録される項目 主な記録項目	医療保険関係情報を利用する記載となっているが、別添資料「業務フロー図」には当該情報を利用している記載となっていない。	委員会	**必要に応じて、国保システムを閲覧し、国民健康保険の資格状況を確認**	別添資料「業務フロー図.」の資格業務で当該情報を利用する旨の文言を特記事項欄に追記しました。
2	Ⅱ特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 委託事項4　①委託内容 委託事項5　①委託内容	何のデータを取扱うかを具体的に記載するのが望ましい。	委員会	委託事項4 障害基礎年金所得状況届受付データ(受付日、届出内容等)を国民年金システムに入力・登録する業務委託 委託事項5 障害基礎年金等の受給に関する所得状況調査用のデータ(証書番号、障害の等級等)を電子ファイル化する業務委託	下線部のとおり修正しました。
3	Ⅲ3.特定個人情報の使用 リスク1 リスクに対する措置の内容	国民年金のサーバに対し、システム管理者権限で直接コンソールに接続し操作を行った場合について、そのログが取得できているか、また、他のログと同様に確認、監視出来ているかを確認し、できているようであればその旨を追記した方が望ましい。	委員会	**③システム管理者権限で直接コンソールに接続しシステムの操作を行った場合においても、誰が・いつ・どのような操作(どのような情報を参照したか等)を実施したかのログを取得し、かつ、不正なアクセスがないか定期的に監視している。**	下線部のとおり追記しました。
4	Ⅲ3.特定個人情報の使用 リスク1 リスクに対する措置の内容	国民年金システムの管理者ユーザ数を教えていただきたい。	委員会		本番環境(実際に業務で利用するシステムの環境)、検証環境(システム改修等の検証時に利用するシステムの環境)等、複数のシステム環境を保有している。管理者ユーザは1つの環境につき1ユーザ存在することなどを委員会にて説明しました。
5	Ⅲ3.特定個人情報の使用 リスク2 具体的な管理方法	アカウントロックの権能が付与されているか確認し、付与されていれば追記した方が望ましい。	委員会	**④認証を複数回失敗すると、自動でアカウントロック機能が作動する。また、アカウントロックを解除するためには所定の手続きを行わなければならないルールが定められている。**	下線部のとおり追記しました。

【Ⅴ3.③別紙】　第三者点検及び第三者点検委員会事務局からの意見と結果について

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
6	Ⅲ3.特定個人情報の使用 リスク2 具体的な管理方法	カード認証時のパスワード強度を教えていただきたい。	委員会		数字やアルファベットのみの単一文字ではなく複数の文字を組み合わせた一定以上の文字数から構成されるパスワードとなっていることなどを委員会にて説明しました。
7	Ⅲ3.特定個人情報の使用 リスク2 その他の措置の内容 ①国民年金システムの利用権限の付与・変更・失効は、システム管理者以外は**実施しない運用としている。**	その他の措置の内容 ①に「システム管理者以外は実施しない運用としている。」という記載があるが、機械的な制御が出来ているのであれば、「システム管理者以外は実施できない運用となっている」等に修正した方が望ましい。	委員会	①国民年金システムの利用権限の付与・変更・失効は、システム管理者以外は**実施できない。**	下線部のとおり修正しました。

【Ⅴ3.③別紙】　第三者点検及び第三者点検委員会事務局からの意見と結果について

第三者点検委員会（平成30年度対応分）

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	Ⅲリスク対策 2.特定個人情報の入手 その他のリスク及びそのリスクに対する措置	年金データの入手方法や提供方法の時系列について、評価書の記載では分かりにくい。記載箇所を変更するなどして分かりやすくできないか。	委員会	2. その他のリスク及びそのリスクに対する措置 区は窓口等で区民より受領する届書情報の他に日本年金機構から還元される処理結果情報を電子記録媒体及び紙媒体により入手する。これらを入手する際は、週1回程度担当職員が公用車で日本年金機構に出向き施錠可能なトランクに格納して区に持ち帰るか、もしくは日本年金機構が簡易書留等で区に郵送する。なお、入手した情報は指定の回付票等で管理し、全ての媒体は鍵のかかる書庫で適切に保管する。	下線部のとおり修正しました。
2	Ⅲリスク対策 5.特定個人情報の提供・移転 その他のリスク及びそのリスクに対する措置	年金データの入手方法や提供方法の時系列について、評価書の記載では分かりにくい。記載箇所を変更するなどして分かりやすくできないか。	委員会	5. その他のリスク及びそのリスクに対する措置 ①区が日本年金機構に提供する電子データファイルは、日本年金機構の作成仕様に基づく電子政府推奨暗号化形式で暗号化を施し、所定のルールに基づいたパスワードを付したZIP形式ファイルとする。なお、区及び日本年金機構の双方において暗号化鍵の管理を適正に行う。 ②区が日本年金機構に提供する電子データファイルは、電子記録媒体（CDまたはDVD）に保存し、それを施錠可能なトランクに格納して担当職員が公用車で週1回程度運搬を行う。 ③区が日本年金機構に提供する紙媒体は、施錠可能なトランクに格納して担当職員が公用車で週1回程度運搬を行うか、もしくは、簡易書留による郵送により行う。 ④区が日本年金機構に提供する電子記録媒体及び紙媒体は、指定の回付票等で管理する。なお、電子記録媒体及び紙媒体は鍵のかかる書庫で適切に保管管理を行う。 以下省略	下線部のとおり修正しました。

【Ｖ3.③別紙】　第三者点検及び第三者点検委員会事務局からの意見と結果について

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
3	Ⅲリスク対策 7.特定個人情報の保管・消去 その他の措置の内容	入退室の認証システムが正しく機能することを定期的に確認する必要がある。例えばシステムサーバーを設置している特定の場所について、入館・入室の生体認証を登録していない人を正しく除外するかどうかの確認も実施してはどうか。	委員会		これまで正しく除外することの確認は特に実施していなかったため、情報システム課に意見を伝え、今後は確認を行うようにします。
4	Ⅲリスク対策 7.特定個人情報の保管・消去 その他の措置の内容	文書等の保管については廃棄のルールを定め明記した方がよい。	委員会	③外部記録媒体及び文書等の廃棄を行う場合は、「データ消去・媒体廃棄申請書」によりセキュリティ管理者の承認を得て行う手順を定めている。 ④磁気ディスクの廃棄時は、内容の復元及び判読が不可能になるような方法により完全消去する。 ⑤帳票等の文書廃棄は、事務処理等で不要となった都度、シュレッダーで裁断している。 ⑥国民年金システムでは、保存年限を経過したデータは、システムの設定により自動処理でデータを削除することができる。	下線部のとおり追記しました。
5	Ⅲリスク対策 9.従業者に対する教育・啓発	具体的な方法の「従事者」の記載を評価書の記載と同様「従業者」に統一したほうがよい。	委員会	【国保年金課の対応】 従業者に対して、年1回以上、以下に関する研修を実施している。	下線部のとおり追記しました。

【Ⅴ3.③別紙】　第三者点検及び第三者点検委員会事務局からの意見と結果について

第三者点検委員会（令和5年度対応分）

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	Ⅲリスク対策 7.特定個人情報の保管・消去 その他の措置の内容	特定個人情報の保管・消去について、バックアップのタイミング（周期等）や廃棄時に関する対策を記載してはどうか。	委員会	⑦バックアップは日次で実施し、毎月2回外部記憶媒体への書き出しを行っている。 ⑧機器の廃棄は現地立会及び廃棄報告書を提出させている。	下線部のとおり修正しました。
2	Ⅲ3.特定個人情報の使用 リスク2 具体的な管理方法	【システム以外】の「適切な管理」について具体的に記載したほうがいいのではないか。	委員会	生体情報の登録・ユーザID・パスワード等の適切な管理について以下の運用ルールが定められている。 ①IDは職員番号、生体情報は職員が専用機器で登録を行う。 ②パスワードは6か月ごとに変更を強制され、前回と同じパスワードは設定できない。 ③アカウントロックを解除するためには所定の手続きを行わなければならない。	下線部のとおり修正しました。
3	Ⅲ3.特定個人情報の使用 リスク2 具体的な管理方法	【システム】の②について、「Windows認証」はわかりづらいので変えたほうがよい。また、生体認証のあとに「等」とあるが、明確に記載したほうがよい。	委員会	②端末の認証は、二要素認証（ID・パスワード、生体情報）による認証となっている。	下線部のとおり修正しました。