

【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	<u>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</u>	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	<u>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。</u>	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ください。	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	<u>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。</u>	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ください。	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 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「従業者」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。

【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7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	I 基本情報 1.特定個人情報ファイルを取り扱う事務 ②事務の内容 (別添1)事務の内容	同一パッケージシステムの記載は必要か(意味があるか)。	委員会		国民年金システムと住民記録システム及び国保システムは同一パッケージシステムであるため、他システムとの連携と異なり共通基盤システムを介さないことを示す意図で記載を行ったことを委員会にて説明しました。
2	II ファイルの概要 6.特定個人情報の保管・消去 ③消去方法	個人単位の通常業務としての消去を指しているのか、ファイル全体の消去を指しているのかあいまいである。	委員会	①特定個人情報ファイルの消去は大田区からの操作によって実施される。	下線部のとおり修正しました。
3	III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 その他措置の内容	課内研修だけでなく、区全体でも研修を実施していることを記載してはどうか。	委員会	個人情報の取扱に対する意識強化のために、年に1回以上、区全体及び課内でセキュリティ研修を実施している。	下線部のとおり修正しました。
4	IIIリスク対策 3.特定個人情報の使用 リスク1:目的を超えた紐付け、事務に必要なない情報との紐付けが行われるリスク 事務で使用するその他システムにおける措置の内容	参照権限のみ付与されているとの記述があるが、それを使い他のデータとの紐付けができるため不十分。	委員会	他部署にて管理しているシステムの利用において、業務に關係のない情報の検索、閲覧、利用を禁止する。	下線部のとおり修正しました。
5	IIIリスク対策 3.特定個人情報の使用 リスク1:目的を超えた紐付け、事務に必要なない情報との紐付けが行われるリスク 事務で使用するその他システムにおける措置の内容	業務と無関係の情報の検索、閲覧、利用を禁止する旨の記載があるが、どのように禁止されているかの記載が求められる。	委員会	他部署にて管理しているシステムの利用において、業務に關係のない情報の検索、閲覧、利用を禁止するルールを定めており、ルールに従って業務を行っている。	下線部のとおり修正しました。
6	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 アクセス権限の管理	システム管理者はユーザに付与された権限を確認できるとの記載があるが、変更もできるのであれば記載してはどうか。	委員会	②システム管理者は、システムのオンライン画面上でどのユーザにどの権限が付与されているかを確認及び変更することができる。	下線部のとおり修正しました。
7	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	書類の他にデータファイルのチェック方法を追加する必要があるのではないか。	委員会	届書・申請書等受付時及び国民年金システムに登録時にダブルチェックを実施した情報を日本年金機構へ提供している。	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
8	Ⅲリスク対策 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・毀損のリスク ⑤物理的対策(具体的な対策の 内容)	具体的な対策として複数 人で行う措置はあるか。	委員会		外部記録媒体の使用管理 等は管理者が使用の都度 確認を行うことで相互チェ ックの役割を果たしている ことを委員会にて説明しま した。
9	Ⅲリスク対策 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・毀損のリスク ⑤物理的対策(具体的な対策の 内容)	無停電電源システムな どはサーバやネット ワークに対して設置さ れているか。	委員会		サーバに対して無停電電源 装置が設置されていること 及びネットワーク機器に対 しては無停電電源が設置さ れていないが庁舎自体に停 電時の一時電源が備わって いることを委員会で説明し ました。