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 【第1回目】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 リスク1:目的外の入手が行われるリスク 対象者以外の情報の入手を防止するための措置の内容 【システム以外】 ①窓口において、申請書･届出書等の内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報が入手されない(本人及び世帯員以外の情報が含まれていないかを確認する)ように業務を行っている。 【国保システム】 【収納支援システム】 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)を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ①窓口において、申請書･届出書等の内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報が入手されない(本人及び世帯員以外の情報が含まれていないかを確認する)ように業務ルールを定めており、ルールに従って業務を行っている。 【国保システム】 【収納支援システム】 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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
2	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 リスク1:目的外の入手が行われるリスク 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 【システム以外】 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。 【国保システム】 【収納支援システム】 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）を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 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おり、ルールに従って業務を行っている。 【国保システム】 【収納支援システム】 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）を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
3	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 リスク2:不適切な方法で入手が行われるリスク リスクに対する措置の内容 【国保システム】 【収納支援システム】 ④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）を実施したかを管理している。	「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【国保システム】 【収納支援システム】 ④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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
4	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 リスク3:入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容 【システム以外】 ②申請書・届出書の記載情報が適正かを審査する手続き（他課への確認等）を実施している。 【国保システム】 【収納支援システム】 ③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）を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ②申請書･届出書の記載情報が適正かを審査する手続き(他課への確認等)を実施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。 【国保システム】 【収納支援システム】 ③個人･操作端末単位で操作ログを取得しており、誰が･いつ･どのような操作を実施したか確認し不正なアクセスを監視している。	対応の内容を追記しました。
5	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 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 リスクに対する措置の内容 【国保システム】 【収納支援システム】 ③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）を実施したかを管理している。	「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【国保システム】 【収納支援システム】 ③個人･操作端末単位で操作ログを取得しており、誰が･いつ･どのような操作を実施したか確認し不正なアクセスを監視している。	対応の内容を追記しました。

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 【第1回目】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
6	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 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 宛名システム等における措置の内容 【国保システム】 ①区民情報系基盤システム・収納支援システムにより入手している情報項目は必要最小限の項目に限定されており、連携ファイルレイアウトにない項目は連携されない（システムに提供されない）。 ②システムのデータベース（データテーブル）領域を拡張することはシステム管理者でなければ実施できないため、業務で必要としない情報項目をデータベース（データテーブル）に追加することはできない。 【収納支援システム】 ①国保システムにより入手している情報項目は必要最小限の項目に限定されており、連携ファイルレイアウトにない項目は連携されない（システムに提供されない）。 ②システムのデータベース（データテーブル）領域を拡張することはシステム管理者でなければ実施できないため、業務で必要としない情報項目をデータベース（データテーブル）に追加することはできない。	本件はアクセス制御とシステム処理要件に関係する。アクセス制御などは明記している。ただし、セキュリティは運用や新たな脅威に対し柔軟な対応が出来ることが重要であり、この意味で十分なセキュリティ対策か否かは判断つきかねる。システム要件に関してのリスク分析が弱い。従って、充分に妥当とは言えない。運用はともかく、システムに対し十分なリスク分析が実施されていない。	委員会	【国保システム】 ①区民情報系基盤システム・収納支援システムにより入手している情報項目は必要最小限の項目に限定されており、連携ファイルレイアウトにない項目は連携されない（システムに提供されない）。 規定された項目以外を連携しようとした場合も、システムは必要な項目のみ取り込みを行い、それ以外を取り込まない仕様とする。 ②新たな項目を紐付しようとした場合でも、システムのデータベース（データテーブル）領域を拡張することはシステム管理者でなければ実施できないため、業務で必要としない情報項目をデータベース（データテーブル）に追加することはできない。 【収納支援システム】 ①国保システムにより入手している情報項目は必要最小限の項目に限定されており、連携ファイルレイアウトにない項目は連携されない（システムに提供されない）。 規定された項目以外を連携しようとした場合も、システムは必要な項目のみ取り込みを行い、それ以外を取り込まない仕様とする。 ②新たな項目を紐付しようとした場合でも、システムのデータベース（データテーブル）領域を拡張することはシステム管理者でなければ実施できないため、業務で必要としない情報項目をデータベース（データテーブル）に追加することはできない。	対応の内容を追記しました。
7	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 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 事務で使用するその他のシステムにおける措置の内容 【国保システム】 【収納支援システム】 ①他部署にて管理しているシステムを利用する国保年金課職員は、参照権限しか付与されない。また、参照できる情報項目が必要最小限に制限されている。 ②他部署にて管理しているシステムを利用する国保年金課職員は、必要最小限の人数としている。	本件はアクセス制御とシステム処理要件に関係する。アクセス制御などは明記している。ただし、セキュリティは運用や新たな脅威に対し柔軟な対応が出来ることが重要であり、この意味で十分なセキュリティ対策か否かは判断つきかねる。システム要件に関してのリスク分析が弱い。従って、充分に妥当とは言えない。運用はともかく、システムに対し十分なリスク分析が実施されていない。	委員会	【国保システム】 【収納支援システム】 ①他部署にて管理しているシステムを利用する国保年金課職員は、参照権限しか付与されない。また、参照できる情報項目が必要最小限に制限されている。 参照できる情報項目は他部署でシステム的に制限されており、法律に基づいた閲覧制限を課せられている。 ②他部署にて管理しているシステムを利用する国保年金課職員は、必要最小限の人数としている。また、利用にあたっては、他部署へ法律に基づいた申請を行うことが条件となっており、これに基づいて許可・不許可のシステム設定がなされる仕様となっている。	対応の内容を追記しました。
8	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 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 具体的な管理方法 【システム以外】 ②アクセス権限は割振られたIDの一覧と業務の対応表を作成し管理している。 【国保システム】 【収納支援システム】 ①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）を実施したかを管理している。	「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ②アクセス権限は割り振られたIDの一覧と業務の対応表を作成し不正なアクセスを監視している。 【国保システム】 【収納支援システム】 ①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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
9	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 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 特定個人情報の使用の記録 具体的な方法 【国保システム】 【収納支援システム】 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）を実施したかを管理している。	「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【国保システム】 【収納支援システム】 個人・操作端末単位で操作ログを取得しており、誰が・いつ・どのような操作を実施したか確認し不正なアクセスを監視している。	対応の内容を追記しました。

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 【第1回目】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
10	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 3特定個人情報の使用 リスク3:従業員が事務外で使用するリスク リスクに対する措置の内容 【システム以外】 ②不正な操作が無いことについて、操作履歴により適時確認する。 【国保システム】 【収納支援システム】 ③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)を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ②不正な操作が無いことについて、操作履歴により適時確認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。 【国保システム】 【収納支援システム】 ③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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
11	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 3特定個人情報の使用 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 リスクに対する措置の内容 【システム以外】 ①システムに記録されている個人情報等のデータについて、改ざんや業務目的以外のコピーを禁止するルールを定めている。 【国保システム】 【収納支援システム】 ③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)を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ①システムに記録されている個人情報等のデータについて、改ざんや業務目的以外のコピー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。 【国保システム】 【収納支援システム】 ③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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。
12	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 4.特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認 ①委託契約締結時、委託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。 ②委託契約中は、定期報告・事故発生時の報告を受けるだけではなく立入検査を行い、情報保護管理体制を確認している。	不十分である。契約や報告、記録だけでなく、一歩踏み込み実地監督が必要である。	委員会	④委託契約中は、定期報告・事故発生時の報告を受けるだけではなく不定期に立入検査を行い、情報保護管理体制を確認している。 ⑤上記について問題を認識した場合は、即座に委託先委託先統括リーダーに業務改善の指示を行っている。 改善支持を受けた委託事業者は、業務改善計画を立て、定期研修のほかスポット研修を実施して再発防止に取り組むことを契約仕様書に記載しており、かつ運用されている。	対応の内容を追記しました。
13	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 4.特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法 【システム以外】 ①委託事業者専用のIDカードを払い出しし、IDカード利用簿により利用状況を管理している。 ③不正な操作が無いことについて、操作履歴により適時確認する。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【システム以外】 ④委託事業者専用のIDカードを払い出しし、IDカード利用簿により利用状況を確認し不正なID利用が無いように監視している。 ⑥不正な操作が無いことについて、操作履歴により適時確認するルールを定めており、定期的に操作履歴のログを確認し不正な書き出しがないか点検を行っている。	対応の内容を追記しました。
14	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 4.特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な制限方法 【国保システム】 【収納支援システム】 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)を実施したかを管理している。	「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	【国保システム】 【収納支援システム】 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)を実施したかを確認し不正なアクセスを監視している。	対応の内容を追記しました。

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 【第1回目】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
15	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 6.情報提供ネットワークシステムとの接続 記載なし	間接的に情報提供ネットワークシステムに接続しているのであれば、記載は必要である。	委員会	評価書へ必要事項を追記しました。	必要事項を追記しました。
16	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 7.特定個人情報の保管・消去 具体的な対策の内容 ⑥技術的対策 【システム以外】 ネットワーク構成図の整備、システム機器やソフトウェアの危機管理台帳への記録、システム管理者以外のソフトウェアのインストールや設定変更の禁止、不正なソフトウェアのコピーの禁止等のルールを定めている。 【国保システム】 【収納支援システム】 ③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）を実施したかを管理している。	＊＊を実施していることを記述すのではなく、＊＊を実施する規則やルールがあるか？システム設計がされているか？が重要である。 「管理している」とは具体的にどのようなことなのかの記載がない。	委員会	⑥技術的対策 【システム以外】 ネットワーク構成図の整備、システム機器やソフトウェアのシステム機器管理台帳への記録、システム管理者以外のソフトウェアのインストールや設定変更の禁止、不正なソフトウェアコピーの禁止等のルールを定めており、ルールに従って業務を行っている。 【国保システム】 【収納支援システム】 ③個人･操作端末単位で操作ログを取得しており、誰が･いつ･どのような操作を実施したか確認し不正なアクセスを監視している。	対応の内容を追記しました。
17	Ⅳその他のリスク対策 1.監査 ①自己点検 具体的な内容 情報資産における情報セキュリティ対策状況の毎年度の自己点検実施について、以下の内容を定めている。 ・実施計画の立案 ・点検項目による自己点検の実施 ・自己点検結果と改善策の報告 ・自己点検結果に基づく改善	妥当と言えるが、手順は評価書に記載あり。ただし、そのような手順書が組織に存在するのか、教育として徹底されているのか、未確認である。	委員会	情報資産における情報セキュリティ対策状況の毎年度の自己点検実施について、以下の内容を定めている。 ・実施計画の立案 ・点検項目による自己点検の実施 ・自己点検結果と改善策の報告 ・自己点検結果に基づく改善 なお、今年度は平成26年12月から平成27年2月にかけて実施した。	対応の内容を追記しました。
18	Ⅳその他のリスク対策 1.監査 ②監査 具体的な内容 情報資産における情報セキュリティ対策状況の毎年度の自己点検実施について、以下の内容を定めている。 ・監査実施計画の立案 ・委託先に係る監査 ・監査結果の保管 ・監査結果への対応	妥当と言えるが、実施手順書が存在するのか。監査結果の扱い、保証監査か助言監査か、自己検査か第三者検査かの位置付けが不明である。	委員会	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。 今年度は、平成26年5月～10月にかけて実施した。	実施した内容を具体的に追記しました。
19	Ⅳその他のリスク対策 2.従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	教育には一般職員、幹部、事務、システム担当者など、対象によってカリキュラムが異なる。また、実施したエビデンスが（試験の実施による理解度）などの説明がないため、妥当とは言い切れない。	委員会	【大田区全体の対応】 研修については、毎年度、研修計画を人材育成担当、情報システム課と協議の上立案し、情報セキュリティ委員会での審議承認を得て実行している。 平成26年度では、新規採用者、転入管理職、管理職候補者を含む新任係長、主任主事10年目に研修を実施し、さらに全課の担当職員に対して研修を実施している。研修後は、受講者アンケートを実施してフィードバックを行っている。（平成25年度には、全管理職向けの情報セキュリティ研修を実施。） 研修結果は、情報セキュリティ委員会に報告を行っている。 【国民健康課の対応】 従事者に対して、年1回以上、以下に関する研修を実施している。 ・セキュリティ基本方針・対策基準・実施手順の理解 ・個人情報の取扱い ・外部記憶媒体の適切な利用と管理 ・パスワード管理について　等 今年度は上記について3月に実施した。 また、4月に、新たに国保年金課に配属された職員に対しセキュリティ研修(個人情報の取扱いに係る留意事項、情報システム機器の取扱い、情報セキュリティポリシー等の規程の理解)、を実施した。	対応の内容を追記しました。

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 【第1回目】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
20	評価補足シート 2.1 リスク1 目的外の入手が行われるリスク 2.1.1 対象者以外の情報の入手を防止するための措置の内容 評価に至った理由 ②業務の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、業務がそれにしたがって運用されている。	対応の内容を追記しました。
21	評価補足シート 2.2 リスク2 不適切な方法で入手が行われるリスク 2.2.1 リスクに対する措置の内容 評価に至った理由 ②業務の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、業務がそれにしたがって運用されている。	対応の内容を追記しました。
22	評価補足シート 2.3 2.3.3 特定個人情報の正確性確保の措置の内容 評価に至った理由 ②業務の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、業務がそれにしたがって運用されている。	対応の内容を追記しました。
23	評価補足シート 3.3 リスク3 従業者が事務外で使用するリスク 3.3.1 リスクに対する措置の内容 評価に至った理由 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。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、操作履歴確認作業等の業務がそれにしたがって運用されている。	対応の内容を追記しました。
24	評価補足シート 3.4 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 3.4.1 リスクに対する措置の内容 評価に至った理由 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。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、操作履歴確認作業等の業務がそれにしたがって運用されている。	対応の内容を追記しました。
25	評価補足シート 4.特定個人情報ファイルの取扱いの委託（全体） 評価に至った理由 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。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②ルール・手続きが定められており、かつ、操作履歴確認作業等の業務がそれにしたがって運用されている。	対応の内容を追記しました。
26	評価補足シート 自己点検の具体的なチェック方法 Ⅳ-１－１－① 評価に至った理由 ②自己点検の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②自己点検の実施方法が確立されており、実際に行っている。	対応の内容を追記しました。
27	評価補足シート 自己点検の具体的なチェック方法 Ⅳ-１－１－② 評価に至った理由 ②監査の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②監査の実施方法が確立されており、実際に行っている。	対応の内容を追記しました。
28	評価補足シート 自己点検の具体的なチェック方法 Ⅳ-1-2 評価に至った理由 ②研修の実施方法が確立されている。	評価結果に至った理由は、「実際に業務が定められたルールどおりに実施されていること」が重要である。	委員会	②研修の実施方法が確立されており、実際に行っている。	対応の内容を追記しました。

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 【第1回目】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
29	2.特定個人情報の入手 リスク1: 目的外の入手 対象者以外の情報の入手を防止するための措置の内容 【システム以外】 ①窓口において、申請書･届出書等の内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報が入手されない(本人及び世帯員以外の情報が含まれていないかを確認する)ように業務ルールを定めており、ルールに従って業務を行っている。 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、課内でセキュリティ研修を実施している。 【国保システム】 【収納支援システム】 ①個人･所属グループ(課･係等)単位で利用できるシステムメニューを設定しており、業務で必要としない情報を利用できないよう制御している。 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)を実施したかを確認し不正なアクセスを監視している。	マイナンバーでは、本人の確認の上での入手が重要である。	委員会	【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。 ②窓口において、申請書･届出書等の内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報が入手されない(本人及び世帯員以外の情報が含まれていないかを確認する)ように業務ルールを定めており、ルールに従って業務を行っている。 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、課内でセキュリティ研修を実施している。 【国保システム】 【収納支援システム】 ①個人･所属グループ(課･係等)単位で利用できるシステムメニューを設定しており、業務で必要としない情報を利用できないよう制御している。 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)を実施したかを確認し不正なアクセスを監視している。 ③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することにより、確実に対象を特定した連携を行うことにより、対象者以外の個人情報の入手を禁止する。	【システム以外】 個人情報の収集について追記した。 【国保システム】 【収納支援システム】 システム連携について追記した。
30	リスク2: 不適切な方法で入手が行われるリスク 2.2 【システム以外】 本人確認を行った上で所定の手続き(どの申請にはどの様式により、どの書類が必要となっているか等)により本人情報を入手している。それ以外の方法による入手を一切認めていない。	より詳細なリスク分析資料が必要である。	委員会	【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本人確認を行った上で所定の手続き(どの申請にはどの様式により、どの書類が必要となっているか等)により本人情報を入手している。それ以外の方法による入手を一切認めていない。	窓口における本人確認について追記した。
31	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が行われるリスク 宛名システム等における措置の内容 【システム以外】 大田区個人情報保護審議会において承認を得られた情報項目以外はシステム及び電子記録媒体に保持することが禁止されている。	セキュリティは運用や新たな脅威に対し柔軟な対応ができることが重要 より一層踏み込んだ分析が望まれる。	委員会	【システム以外】 ①大田区個人情報保護審議会において承認を得られた情報項目以外はシステム及び電子記録媒体に保持することが禁止されている。 ②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。 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定めている。 ④毎年、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を行っている。	個人情報の利用について追記した。

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 【第1回目】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
32	4.特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認 ①委託契約締結時、委託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。 ②委託契約中は、定期報告・事故発生時の報告を受けるだけでなく不定期に立入検査を行い、情報保護管理体制を確認している。 ③上記について問題を認識した場合は、即座に委託先統括リーダーに業務改善の指示を行っている。改善指示を受けた委託事業者は、業務改善計画を立て、定期研修のほかスポット研修を実施して再発防止に取り組むことを契約仕様書に記載しており、かつ運用されている。 ④委託事業者との定例会を1ヶ月に1回開催しており、その中で問題と改善案を検討し、決定した改善方法により業務を運用している。	他者へ提供されていないことの確認方法を記載する必要がある。	委員会	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、「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、「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。 ④委託契約中は、定期報告・事故発生時の報告を受けるだけでなく不定期に立入検査を行い、情報保護管理体制を確認している。 ⑤上記について問題を認識した場合は、即座に委託先統括リーダーに業務改善の指示を行っている。改善指示を受けた委託事業者は、業務改善計画を立て、定期研修のほかスポット研修を実施して再発防止に取り組むことを契約仕様書に記載しており、かつ運用されている。 ⑥委託事業者との定例会を1ヶ月に1回開催しており、その中で問題と改善案を検討し、決定した改善方法により業務を運用している。	個人情報の取扱い、委託契約について追記した。
33	4.特定個人情報ファイルの取扱いの委託 具体的な制限方法 【システム以外】 ①委託事業者専用のIDカードを払い出しし、IDカード利用簿により利用状況を確認し不正なID利用が無いように監視している。 ②上記①のIDに付与する権限は業務上必要最小限の権限を割り当てている。 ③不正な操作が無いことについて、操作履歴により適時確認するルールを定めており、定期的に操作履歴のログを確認し不正な書き出しがないか点検を行っている。	新制度では、委託管理は従来以上に要求されている。十分な対応を実施することがわかるような記述が必要である。	委員会	①委託契約書において、委託先の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システムの利用権限の追加及び変更は、申請書により所定の審査・承認を経てIDを付与している。 ③システムの利用権限の追加及び変更は、システム管理者でしか設定することはできない。 ④委託事業者専用のIDカードを払い出しし、IDカード利用簿により利用状況を確認し不正なID利用が無いように監視している。 ⑤上記④のIDに付与する権限は業務上必要最小限の権限を割り当てている。 ⑥不正な操作が無いことについて、操作履歴により適時確認するルールを定めており、定期的に操作履歴のログを確認し不正な書き出しがないか点検を行っている。	委託契約、システムの利用手続きについて追記した。
34	Ⅱファイルの概要 3.特定個人情報の入手・使用 ③入手時期・頻度 ・被保険者もしくはその世帯構成員の生保等に関わる異動発生時（随時）	－	事務局	③入手時期・頻度 ・被保険者もしくはその世帯構成員の生活保護等に関わる異動発生時（随時）	「生保」を「生活保護」に文言修正しました。
35	Ⅱ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 委託件数12件 【内訳（委託内容：委託事業者）】 ①国保システム保守：株式会社NTTデータ ②収納支援システムの保守：株式会社シンク ③窓口サービス委託：テンプスタッフ株式会社 ④保険証等の印刷発送：光ビジネスサービス株式会社、凸版印刷株式会社、株式会社イムラ ⑤データ入力作業：株式会社日比野情報サービス、株式会社イマージュ ⑥特定保健指導業務：株式会社ベネフィットワン・ヘルスケア ⑦国保システムの運用作業：日本電気株式会社 ⑧サーバ等機器保守：日本電気株式会社 ⑨レセプト点検作業：株式会社ニチイ学館	－	事務局	委託件数11件 【内訳（委託内容：委託事業者）】 ①国保システム保守：株式会社NTTデータ ②収納支援システムの保守：株式会社シンク ③窓口サービス委託：テンプスタッフ株式会社 ④データ入力作業：株式会社イマージュ ⑤データ入力作業：株式会社日比野情報サービス ⑥納付案内センター業務：株式会社ベルシステム24 ⑦国保システムの運用作業：日本電気株式会社 ⑧サーバ等機器保守：日本電気株式会社 ⑨保険証の印刷発送：凸版印刷株式会社 ⑩通知書等の印刷発送：光ビジネスサービス株式会社 ⑪レセプト点検業務：株式会社ニチイ学館	事務局の指示により、委託業務単位から委託事業者単位の記載に変更しました。 納付案内センターを追加しました。 特定健診及び特定保健指導関連業務の委託においては、今後、医師会との調整が必要となるため、削除しました。 ※特定個人情報を取扱う者の人数に変更が生じるが、しきい値判断に影響はありません。

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 【第1回目】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
36	Ⅱファイルの概要 5.特定個人情報の提供・移転 提供先期間単位で記載 提供先1:厚生労働大臣 法令上の根拠:番号法第19条第7号 別表第二　第1項　第4項 提供する情報:〇〇情報、△△情報	－	事務局	提供先期間単位で記載 提供先1:厚生労働大臣 法令上の根拠:番号法第19条第7号 別表第二　第4項 提供する情報:〇〇情報	事務局の指示により、提供先単位から法令上の根拠単位の記載に変更しました。
37	Ⅱファイルの概要 5.特定個人情報の提供・移転 移転先 ②移転先における用途　未記入	－	事務局	移転先 ②移転先における用途　必要事項を記入	未記入箇所に必要事項を記入しました。
38	（別添2） 特定個人情報ファイル記録項目 1850項目の詳細な情報項目一覧表	－	事務局	1850項目の詳細な情報項目についてグルーピングした一覧表を作成	情報項目が詳細に記載されていたため、記載方法を変更しました。

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 【第2回目】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	全体	評価書に「国保連」や「国保連合会」と記載があるが、「東京都国民健康保険団体連合会」が正式名称ではないか。	委員会	「**東京都国民健康保険団体連合会**」に統一修正	意見内容を考慮し、修正しました。
2	全項目評価書 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3 ③他のシステムとの接続 [ ]その他（国保システム）	「その他」欄に「○」に記載がない。	委員会	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3 ③他のシステムとの接続 **[○]**その他（国保システム）	誤記であるため、修正しました。
3	全項目評価書 （別添1）事務の内容	収納支援システムの機能に「欠損機能」と記載があるが、正しくは「不納欠損機能」ではないか。	委員会	「欠損機能」の表記を「**不納欠損機能**」に修正	誤記であるため、修正しました。
4	全項目評価書 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 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性	委託先がどの特定個人情報ファイルを取り扱うか不明確なので、具体的な情報項目等を明示すると良い。	委員会	委託事項1～12について、以下の項目を追記しました。 **※取り扱う特定個人情報ファイル：「（別添2）特定個人情報ファイル記録項目」のNO**	意見内容を考慮し、修正しました。
5	全項目評価書 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12 ⑨再委託事項 資格継続業務、高額該当回数の引き継ぎ業務で使用する国保総合(国保集約)システムに関する運用業務の一部（バッチ処理パラメータの入力／バッチ処置の実行／バックアップデータの取得と保管／システム障害発生時の復旧支援作業／各種マスターメンテナンス／外字作成・登録）など。	東京都国民健康保険団体連合会は国保総合（国保集約）システムの保守業務も再委託していると思われる。事実確認を行ってください。	委員会	資格継続業務、高額該当回数の引き継ぎ業務で使用する国保総合(国保集約)システムに関する運用業務の一部（バッチ処理パラメータの入力／バッチ処置の実行／バックアップデータの取得と保管／システム障害発生時の復旧支援作業／各種マスターメンテナンス／外字作成・登録）、**及び国保総合(国保集約)システムの保守業務**など。	確認を行った結果に基づき修正しました。
6	全項目評価書 （別添2）特定個人情報ファイル記録項目 4賦課情報：医療・介護・支援金及び合計分の**保険料**賦課等の情報 他複数個所	評価書に「保険料」と記載があるが、介護保険等の他保険と混同し分かりにくい。	委員会	（別添2）特定個人情報ファイル記録項目 賦課情報：医療・介護・支援金及び合計分の**国民健康保険料**賦課等の情報 他複数個所においても同様の修正	意見内容を考慮し、修正しました。
7	全項目評価書 （別添2）特定個人情報ファイル記録項目 21税情報：**国保年金システム**の税情報で確認不可の税情報 22住記情報：**国保年金システム**の住民情報で確認不可の税情報	評価書に「国保システム」と記載があるが、当該箇所だけ「国保年金システム」と記載されている。 誤記であれば修正いただきたい。	委員会	（別添2）特定個人情報ファイル記録項目 21税情報：**国保システム**の税情報で確認不可の税情報 22住記情報：**国保システム**の住民情報で確認不可の税情報	誤記であるため、修正しました。
8	全項目評価書 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 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 ＊：ここでいう指定されたインタフェースとは、国保総合(国保集約)システムの外部インタフェース仕様書に記載されている東京都国民健康保険団体連合会の国保総合(国保集約)システムと市区町村に設置する国保総合PCとの間でやりとりされるデータ 定義のことをいい、その定義に従った項目(法令等で定められた範囲)でないと、東京都国民健康保険団体連合会の**保総合(国保集約)システム**からデータ配信ができないしくみになっている。	「保総合(国保集約)システム」と記載があるが誤記ではないか。	委員会	＊：ここでいう指定されたインタフェースとは、国保総合(国保集約)システムの外部インタフェース仕様書に記載されている東京都国民健康保険団体連合会の国保総合(国保集約)システムと市区町村に設置する国保総合PCとの間でやりとりされるデータ 定義のことをいい、その定義に従った項目(法令等で定められた範囲)でないと、東京都国民健康保険団体連合会の**国保総合(国保集約)システム**からデータ配信ができないしくみになっている。	誤記であるため、修正しました。

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 【第2回目】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
9	全項目評価書 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 3.特定個人情報の使用 ユーザ認証の管理 具体的な管理方法 【システム以外】 ICカード・ユーザID・パスワードの適切な管理について運用ルールが定められている。 (例)離席時にICカードをリーダライターから取り外す、ICカード紛失時の手続き、ユーザIDの払い出しの手続き、パスワード強度、パスワードを定期的に変更する等	「共用IDの利用」について分かりにくい。説明を補足すると良い。	委員会	【システム以外】 ICカード・ユーザID・パスワードの適切な管理について運用ルールが定められている。 (例)離席時にICカードをリーダライターから取り外す、ICカード紛失時の手続き、ユーザIDの払い出しの手続き、パスワード強度、パスワードを定期的に変更する等 **委託事業者等が作業を行うために共用IDを発行している場合がある。当該IDはWindows認証時に利用するIDであり、誰が何のためにいつ利用したか等を管理簿やシステムのログ情報で適正に管理している（各システム要件については、下記のとおり）。**	意見内容を考慮し、修正しました。
10	全項目評価書 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 3.特定個人情報の使用 アクセス権限の発効・失効の管理 具体的な管理方法 【システム以外】 ②他部署職員が国保システム･収納支援システムを利用する場合、又は利用する職員に**変更がは**発生した場合、申請書により所定の審査・承認を経て利用権限を付与・変更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。	「変更がは」と記載があるが誤記ではないか。	委員会	②他部署職員が国保システム･収納支援システムを利用する場合、又は利用する職員に**変更が**発生した場合、申請書により所定の審査・承認を経て利用権限を付与・変更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。	誤記であるため、修正しました。
11	全項目評価書 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 6.情報提供ネットワークシステムとの接続 リスクに対する措置の内容 【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。 ・共用IDを利用する場合は、共用IDの利用者以外の者に知られないように管理し、共用IDの利用者以外に利用させない。 ＜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。	「共用IDの利用」について分かりにくい。説明を補足すると良い。	委員会	【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。 **・委託事業者等がWindows認証の共用IDを利用する場合は、共用IDの利用者以外の者に知られないように管理し、共用IDの利用者以外に利用させない。** ＜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。	意見内容を考慮し、修正しました。
11	全項目評価書 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 7.特定個人情報の保管・消去 消去手順 手順の内容 【システム以外】 ①外部記憶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。 ②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。当該消去作業を委託により実施する場合は、データを完全に消去した旨の報告書を納品物に指定している。 ③帳票等の文書廃棄は、事務処理等で不要となった都度、**裁断機**により破砕している。	「裁断機」より「シュレッダー」の方が適切な表記ではないか。	委員会	【システム以外】 ①外部記憶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。 ②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。当該消去作業を委託により実施する場合は、データを完全に消去した旨の報告書を納品物に指定している。 ③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。	意見内容を考慮し、修正しました。

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 【第3回目】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	全項目評価書 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 ③他システムとの接続 [○]その他 （収納支援システム）	国保総合（集約）システムの抜けか。	委員会	全項目評価書 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 ③他システムとの接続 [○]その他 （収納支援システム**、国保総合（集約）システム**）	記載漏れのため、修正しました。
2	全項目評価書 Ⅰ基本情報 4. 特定個人情報ファイルを取り扱う理由 ①事務実施上の必要性 ・オンライン資格確認で被保険者等の資格情報を利用するためには、医療保険者等向け中間サーバー等において、医療保険者等の加入者等の履歴情報を正確に管理する必要があり、その履歴情報の生成の際には、同一人であることを正確に把握するために個人番号を用いることから、特定個人情報として**国民健康保険関連情報ファイ**ルを提供する。	・「国民健康保険関連情報ファイル」は「国民健康保険情報ファイル」ではないか。	委員会	・オンライン資格確認で被保険者等の資格情報を利用するためには、医療保険者等向け中間サーバー等において、医療保険者等の加入者等の履歴情報を正確に管理する必要があり、その履歴情報の生成の際には、同一人であることを正確に把握するために個人番号を用いることから、特定個人情報として**国民健康保険情報ファイル**を提供する。	誤記であるため、修正しました。
3	全項目評価書 （別添1）事務の内容	図中、「国保 情報集約システム」は記述誤りか。	委員会	「**国保総合（集約）システ**ム」に修正	誤記であるため、修正しました。
4	全項目評価書 （別添1）事務の内容	図の上部に記載の「（別添）1-2事務内容」」に該当する資料が不明である。	委員会	**「（別添）1-2事務内容」」を削除**	表は存在しないため、削除しました。
5	全項目評価書 （別添1）事務の内容及び（備考）	・「医療保険者等向け中間サーバー等」「医療保険者等向け中間サーバー等システム」の用語を統一したほうがよい。	委員会	**「医療保険者等向け中間サーバー等」**に統一修正	意見を反映し、文言を統一しました。
6	全項目評価書 Ⅱ ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く） 移転先7 ⑥移転方法 [○]その他	移転方法その他に記載がない。	委員会	**「[○]庁内連携システム」**へ修正	誤記であるため、修正しました。
7	（別添2）ファイル記録項目	オンライン資格確認で使用する項目に特定個人情報ファイル記録項目の番号を附番して関連付けたほうが良い。	委員会	・被保険者証記号及び被保険者証番号ごとに付番した枝番（個人を識別する2桁の番号）**【№2】** ・券面記載の被保険者証記**号**）**【№2】** ・券面記載の被保険者証番号）**【№2】** ・券面記載の氏名（漢字）**【№18】** ・券面記載の氏名（漢字）の読み仮名**【№18】** ・券面記載氏名が通称名の場合の本名等（漢字）**【№18】** ・券面記載氏名が通称名の場合の本名等（漢字）の読み仮名**【№18】** ・被保険者証裏面への性別記載の有無**【№18】** ・DV被害者等に関する自己情報不開示の申し出の有無**【№18】** ・自己負担限度額が変更となった場合、又は治癒により証を回収した場合の回収の理由が発生した日**【№2】**	意見を反映し、修正しました。
8	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2：不適切な方法で入手が行われるリスク リスクに対するの措置の内容 【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。**	措置の内容のシステム以外で、本人確認に運転免許証がないが、リスク3の本人確認と同じ措置ではないのか。	委員会	**①申請書等の受理はあらかじめ決められた窓口又は郵送によるものとし、本人又は代理人の本人確認を必ず行うものとする。**	記載内容を修正しました。
9	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3：入手した特定個人情報が不正確であるリスク 入手の際の本人確認の措置の内容	欄を区切る線がないので曖昧な記述である。	委員会	区切り線を追加しました。	

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 【第3回目】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
10	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3：入手した特定個人情報が不正確であるリスク 個人番号の真正性確認の措置の内容 【国保システム】 大田区に住民登録されていない対象者(遠隔地被保険者等)である者以外は、区民情報系基盤システムより個人番号情報を入手する(**システム**から個人番号を入力･登録しない)。	(システムから個人番号を入力・登録しない)となっているが、システム名を表記して区別すべき。	委員会	【国保システム】 大田区に住民登録されていない対象者(遠隔地被保険者等)である者以外は、区民情報系基盤システムより個人番号情報を入手する(**国保システム**から個人番号を入力･登録しない)。	意見を反映し、システム名を追加しました。
11	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3：入手した特定個人情報が不正確であるリスク 個人番号の真正性確認の措置の内容 【収納支援システム】 国保システムより個人番号情報を入手する(**システム**から個人番号を入力･登録しない)。	(システムから個人番号を入力・登録しない)となっているが、システム名を表記して区別すべき。		【収納支援システム】 国保システムより個人番号情報を入手する(収納支援システムから個人番号を入力･登録しない)。	意見を反映し、システム名を追加しました。
12	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3：入手した特定個人情報が不正確であるリスク 特定個人情報の正確性確保の措置の内容 【システム以外】 ③窓口で受領した申請書・届出書等の内容をシステムに**入力（登録）する前に**、入力内容を確認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。	登録前に確認する画面はあるのか。システム以外でクロスチェックはしないのか。	委員会	③窓口で受領した申請書・届出書等の内容をシステムに**入力前後に**入力内容を確認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。	措置内容を追加しました。
13	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 3. 特定個人情報の使用 リスク2：権限のないもの（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	共用IDの発行やパスワード使い回しの禁止、離席時の画面ロックはシステム以外のセキュリティ教育ではないのか?	委員会	①生体情報の登録、ユーザID・パスワードの適切な管理について運用ルールが定められている。 **②なりすましによる不正を防止する観点から、共用IDの発行は禁止している。** **③ログインしたまま端末を放置せず、離席時には画面ロックまたはログアウトすることやパスワードの使いまわしをしないことを徹底している。** ④パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。	【国保システム】【収納支援システム】【国保総合（国保集約）システム】から【システム以外】へ記載箇所を変更しました。
14	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 3. 特定個人情報の使用 リスク2：権限のないもの（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 アクセス権の発効・失効の管理 具体的な管理方法 【システム以外】 ③権限の失効は、システム管理者にて人事異動時及び定期的に確認を行い、必要の無いIDを削除する手順を設けている。	・システム以外の措置でシステム管理者が人事異動時および定期的に確認するとあるが、異動時おおび確認地に必要の無いIDを発見した場合に「すみやかに」削除される必要があるが、削除のタイミングの記述が必要。	委員会	③権限の失効は、システム管理者にて人事異動時及び定期的に確認を行い、必要の無いIDを**速やか**に削除する手順を設けている。	措置内容を追加しました。
15	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルール ルールの内容及びルール遵守の確認方法	納品時のデータ消去報告書の提出等、ルール遵守の確認方法が必要ではないか。	委員会	②データ消去をした場合は、データ消去報告書を提出すること	確認方法を追加しました。
16	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 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知た提供を除く。） 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 【国保システム】 【収納支援システム】 ②特定個人情報ファイルの**情報項目**に誤り等がないかチェックする機能をシステムに設ける。	情報項目に誤りがないかは試験で判明する。値ではないか。	委員会	【国保システム】 【収納支援システム】 ②特定個人情報の**値に**誤り等がないかチェックする機能をシステムに設ける。	意見を反映し、文言を修正しました。

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 【第3回目】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
17	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 6. 情報提供ネットワークシステムとの接続 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 リスクに対する措置の内容 【国保システム】 ③庁内のネットワークを「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」と各々分離し、**インターネット網**からの通信をできないようにしている。	インターネット網ではなく、インターネット接続環境ではないか。	委員会	③庁内のネットワークを「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」と各々分離し、**インターネット接続環境**からの通信をできないようにしている。	誤記であるため、修正しました。
18	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 6. 情報提供ネットワークシステムとの接続 リスク3：入手した特定個人情報が不正確であるリスク リスクに対する措置の内容 【国保システム】 ①情報提供ネットワークシステムにデータを提供する際、及び情報提供ネットワークシステムからデータを取得しシステムに取り込む際は、バリデーションチェック等により不正確なデータの提供・取り込みを抑止している。	バリデーションチェックをするとあるが、どのようなバリデーションを行うのか、具体性に欠ける。	委員会	①情報提供ネットワークシステムにデータを提供する際、及び情報提供ネットワークシステムからデータを取得しシステムに取り込む際は**、データ入力値に矛盾がないかなど**バリデーションチェック等により不正確なデータの提供・取り込みを抑止している。	意見を反映し、文言を追加しました。
19	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 6. 情報提供ネットワークシステムとの接続 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 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及びそのリスクに対する措置	項目欄が存在しない。	委員会	該当欄を表示	
20	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 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 ⑤物理的対策 具体的な対策の内容	バックアップの世代管理や遠隔保管などは実施していないのか。	委員会	**④バックアップデータは世代管理を行うとともに、遠隔地保管を行っている。**	対策内容を追加しました。
21	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 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 ⑤物理的対策 具体的な対策の内容	端末などの交換、廃棄時のデータ保護の記述がない。	委員会	**⑤端末の廃棄を行う際は、データ消去証明書の提出を義務付けている。**	対策内容を追加しました。
22	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 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 ⑥技術的対策 具体的な対策の内容 **①端末とサーバ間の通信を暗号化している。**	通信上の対策なので、保管時、暗号化しているのであればそのように記載したほうがよい。	委員会	**該当の記述を削除**	
23	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 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 ⑥技術的対策 具体的な対策の内容 【国保】システム】 ②特定個人情報はシステム内のデータベースに格納され、当該データベースへの接続方法はシステム管理者以外は知り得ない。**このため当該情報の改ざんは不可能となっている。**	DBへの接続方法は管理者しか知らないことで改ざんが不可能」は無理がある。管理者IDの使用許可と記録などが必要。	委員会	**①特定個人情報はシステム内のデータベースに格納され、当該データベースへの接続はシステム管理者権限を付与された限られた人のみが行うことができ、操作ログを記録・保管している。**	意見を反映し、対策内容を修正しました。
24	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 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 ⑥技術的対策 具体的な対策の内容 【国保】システム】 **生体情報**のパスワードを定期的に変更している。	「生体情報のパスワード」の意味が不明。	委員会	**⑤ユーザーID**のパスワードを定期的に変更している。	意見を反映し、文言を修正しました。
25	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 7.特定個人情報の保管・消去 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】	外部に保存されたものについての使用期限や条件を明記しているか。	委員会	**③USBメモリを使用する場合は原則データの移動用途とし、使用後すみやかにデータ削除を実施している。また、削除したことの確認を実施している。**	措置内容を追加しました。

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 【第3回目】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
26	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 7.特定個人情報の保管・消去 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】	保存情報については台帳等に整理され、それぞれの情報毎に保管期限が規定されており、それに沿って保管期限の見直し、廃棄・消去等がなされていると思うが、その記述が無く、措置の具体性に欠くところがある。	委員会	**④情報毎に保存期限が決められており、保存期限を経過したものは定期的に溶解処分している。**	措置内容を追加しました。
27	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 7.特定個人情報の保管・消去 リスク2：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】	外部に保存されたものについての使用期限や条件を明記しているか。	委員会	**⑤USBメモリを使用する場合は原則データの移動用途とし、使用後すみやかにデータ削除を実施している。また、削除したことの確認を実施している。**	措置内容を追加しました。
28	Ⅳ その他リスク対策 1. 監査 ①自己点検 具体的なチェック方法 ②所管における自主点検について、以下の内容を定めている。 ・課長は、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、**自主点検**を実施する。また、必要に応じて、自主点検の結果について部長の評価を受ける。 ・課長は、**自主点検**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。	自己点検と自主点検が混在しており、意味の相違が不明である。	委員会	②所管における自己点検について、以下の内容を定めている。 ・課長は、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部長の評価を受ける。 ・課長は、**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。	誤記のため、修正しました。

住民等からの意見聴取の結果について

No	評価書該当箇所	意見内容	評価書 修正箇所	主管課意見
1	意見なし			