平成２２年度

目黒区包括外部監査報告書

【公表版】

平成２３年１月

目黒区包括外部監査人　池　　永　　朝　　昭

同補助者　　戎　　井　　重　　樹

同補助者　　丹　生　谷　　美　　穂

同補助者　　金　　子　　憲　　康

同補助者　　矢　　上　　浄　　子

本報告書（公表版）は、目黒区に対して提出された監査報告書（別紙含む）（以下、「報告書」という）の一部内容について、目黒区の要請を受けて削除、変更等の改変を加え、対外的に公表されることを前提に編集を行ったものである。外部監査人が報告書に改変を加えざるを得なかったのは、同報告書において言及される文書等の一部に目黒区が指定する「情報セキュリティ関連文書」（情報セキュリティに関連する規程や報告）が含まれており、また、本件監査の際に包括外部監査人が締結を求められた目黒区との「情報セキュリティ関連文書取扱いに関する覚書」に、外部監査人には「情報セキュリティ関連文書で包括外部監査人が知り得た目黒区の人事、技術、事務手続き等の情報（以下、「機密情報」という）を第三者に開示または提供してはならない」との規定があり、機密情報に含まれる情報を含む報告書をそのまま公開することが困難であったためである。さらに、改変の対象となった部分の中には、報告書の公開それ自体が情報の脆弱性に対するリスクになりうるという目黒区の懸念から、目黒区の追加的な要請を受けて適宜削除、変更等の改変を行った部分がある。本報告書（公表版）参照の際には、以上の点に留意されたい。

第１　包括外部監査の概要

１　外部監査の種類

目黒区条例第５３号（目黒区外部監査契約に基づく監査に関する条例）第２条に定める地方自治法第２５２条の２７第２項に規定する目黒区との包括外部監査契約に基づく監査。

２　特定した事件、監査対象部及び監査対象年度

（１）特定した事件

目黒区における個人情報を取り扱う情報システムの管理体制、運用及び検証体制について。

（２）監査対象年度

平成２１年度執行分を中心にし、必要に応じて過年度分についても監査した。

（３）監査対象部署

情報課、国保年金課、戸籍住民課、健康福祉計画課、地域ケア推進課、介護保険課、選挙管理委員会事務局、生活福祉課及び子育て支援課。

（４）監査対象となる個別の情報システム

以下の表記載の情報システム。

システム	担当部署	システムの概要
国保収納推進員	国保年金課	保険料未納者情報による訪問事務
戸籍事務	戸籍住民課	戸籍事務
保健福祉情報	健康福祉計画課	福祉事務処理
包括支援業務支援	地域ケア推進課	地域包括支援センターへの行政情報の提供及び書面伝送
介護保険	介護保険課	介護保険被保険者資格管理、保険料納付管理、受給者管理、給付実績管理
選挙人名簿、期日前投票	選挙管理委員会事務局	選挙人名簿調製、期日前投票管理事務
生活保護	生活福祉課	生活保護法施行に要する一般事務、生活保護法外の援護事務全般
児童扶養手当管理	子育て支援課	児童扶養手当事務

３　監査対象事件の選定の理由

平成１２年に政府による「ＩＴ基本戦略」が打ち出されてから、国と地方公共団体において電子政府・電子自治体の実現に向けた数多くの情報化施策が講じられ、現在、コンピュータ及びネットワークを中核とする情報システムは、国と地方公共団体の行政事務において不可欠な要素となっている。平成１９年には、総務省より「新電子自治体推進指針」が公表され、以降、電子自治体の実現のための新たな取組みが総務省のイニシアチブにより推し進められている。各自治体においても、これらの取組みに対応した新たな情報化施策が策定され、実行に移されている段階にある。

目黒区においても、情報化に対応した取組みが早くから進められている。例えば、平成７年度から平成１１年度にかけて実行された「目黒区地域情報化推進計画」では、税務事務、国保事務等の住民サービス系システムが再構築され、災害情報システム、保健福祉情報システム等の個別システムが導入された。平成１４年度には、区の情報化施策の方向性を示す「目黒区情報化ビジョン」が策定され、同ビジョンに沿って庁内ＬＡＮ及びグループウェアの整備並びに電子調達システム、施設予約システム等の個別システムの導入が行われた。また、平成１８年度から平成２０年度にかけて、全庁共通の内部管理事務を対象とした文書管理システム、庶務事務システム、人事給与システム、財務情報システム及びシステム共通基盤からなる「内部情報システム」が、総額約９億９６００万円の費用を投じて開発され、稼動するに至っている。さらに平成２１年３月、目黒区は、総務省の「新電子自治体推進指針」及び区の情報化を取り巻く環境の変化に対応するために、新たに「目黒区情報化推進計画」を策定し、実施中である。

以上のように、目黒区における情報化施策は年々深化と広がりを見せており、これに伴い、情報システムに対する区の依存度も格段に高まっている。このようなシステム依存度の高まりは、他方で、事故や災害により情報システムの機能に障害が生じた場合の行政事務や区民生活への影響リスクを増大させるものである。また、区のシステム上取り扱われる情報は日々増加し、複雑化しているところ、情報漏えいや情報の不適切な使用といったリスクへの対処の重要性も増してきている。特に、区の取り扱う個人情報に関しては、個人情報保護法その他関連する法律・条例を踏まえた適正な取扱いの確保が強く要請されている。

このような状況においては、総務省の「新電子自治体推進指針」でも提唱されているように、自治体レベルでの情報セキュリティ対策をさらに強化し、これを徹底していくことが不可欠である。総務省によれば平成１８年４月時点で全ての都道府県及び市区町村において個人情報保護条例が制定され、またほとんどの自治体で情報セキュリティポリシーが策定されるなど、制度的な整備は進んでいるとのことであるが、他方において、自治体職員や業務委託先の従業員のパソコン等の盗難やウィルス感染、情報共有ソフトの使用、資料の紛失等による情報漏え

い等の事案は各地で後を断たない。

目黒区では、昭和６３年に個人情報保護条例を定めており、また情報セキュリティリスクに対処するため、平成１４年に「情報セキュリティ基本方針」及びこれに基づく「情報セキュリティ対策基準」を、平成１６年には「目黒区電子情報処理規則」を策定し、全庁で遵守すべき情報処理に関する基準設定を行ったほか、各個別システムについて、それぞれ個別システム管理運用基準及びセキュリティ実施基準を策定している。また、平成１６年には、外部委託による情報セキュリティ監査が実施され、平成１７年度以後は各課の自主点検が、平成１９年度以降は毎年１回、「目黒区情報セキュリティ監査実施要綱」に従った内部監査が、それぞれ行われている。これらの自主点検や監査結果においても、各課における情報システム管理上の問題点や要改善点が指摘されている。

また、目黒区の内部情報システムを対象として二つの外部委託業者により実施された平成２０年度のシステム評価及び平成２１年度のシステム監査においては、内部情報システムの目的である事務の効率化や情報セキュリティ対策に関連する問題点が指摘されている。

他方、昨年（平成２１年度）の補助金交付団体や指定管理者を監査対象とする包括外部監査の実施過程においては、個人情報の不適切な取扱いが指摘されており、個人情報管理の徹底が求められているこれらの団体の現状は、区における個人情報管理についても検証する必要性を示唆するものであった。

以上の状況に鑑みれば、区民の個人情報を保有し、取り扱う個別の情報システムにおける管理の具体的な運用及び体制について、その適切性を検証する必要性があることが認められる。検証には、情報システムについて全面的な情報セキュリティ監査を行うことが有効であると考えられる。すなわち、情報セキュリティ対策に関しては、制度面の整備のみにとどまらず、日々変化する自治体の情報化を取り巻く環境、情報セキュリティに係る脅威・脆弱性や対策技術に対応するために、情報セキュリティ対策全般の実効性の評価・見直しを定期的に行うことが有効であり、そのためには、第三者による情報セキュリティ監査が最も効果的である。

監査人団では区の使用するある一定範囲の情報システムを対象とした情報セキュリティ監査の実施を視野に入れ、総務省の「地方公共団体における情報セキュリティ監査に関するガイドライン」[1]（平成１５年１２月２５日策定、平成１９年７月６日全部改定）（以下、「総務省ガイドライン」という）を含め検討した。残念ながら、総務省ガイドラインの付録にある「情報セキュリティ監査業務委託仕様書（例）」では、「監査人要件」として、監査チームにシステム監査技術者等の情報セキュリティ監査に必要な資格を有する者を１人以上含むことを挙げており、また、この点に関する総務省の口頭による回答も、情報セキュリティ監査

[1] http://www.soumu.go.jp/menu_news/s-news/2007/070706_3.html

は有資格者１人以上の関与を当然予定しているとのことであった。このことからすると、有資格者のいない監査人団の監査には、技術的セキュリティの評価の側面において限界があると言わざるを得ない。また、目黒区の包括外部監査向けの予算は限定されており、情報セキュリティ監査に必要な資格及び経験を有する人員を補充して充実した監査をおこなうことは予算的に不可能である[2]。

しかし、監査の対象を個人情報の適切な管理という点にしぼり、総務省ガイドライン等を参照して個人情報を保存し、あるいは受け付ける情報システムの管理体制とその運用や検証体制を監査することは、情報セキュリティ監査そのものではないが十分実施可能であり、また、有用な監査となると考えられる。

そこで、目黒区の保有する個人情報を取り扱うものであり、取り扱う個人情報が区の給付・支援業務や債権回収など金銭の出入りに直接結びつくものであるかどうか、また区が保有する個人情報そのもの（いわゆる「四情報」（氏名、生年月日、性別及び住所）を含むもの）を一度に大量に取り扱うものであるかどうかといった点を選定基準として、監査対象部課及びシステムを上記２（３）及び（４）のとおり特定し、目黒区における個人情報を取り扱う情報システムの管理体制、運用及び検証体制について、監査を実施することとした。

４　包括外部監査の方法

（１）監査の要点

総務省ガイドラインのうち、はじめて情報セキュリティ監査を行う場合等の初期段階における必須の監査項目として掲げられている１１０項目（別紙１参照）に依拠しつつ、主に以下のような要点に着眼して監査を行った。

①　組織体制

情報セキュリティの組織体制、権限、責任は明確であるか。情報化推進委員会は情報セキュリティの重要事項について適切な報告を受け、また決定や組織に対する指示を行っているか。

②　物理的セキュリティ

サーバ等の管理について、災害対策や損傷等防止を考慮した対策が適切に実施されているか。管理区域の指定やアクセス制限がなされているか。

---

[2] 情報セキュリティ監査の内容を含む地方公共団体の情報システムに対する監査を包括外部監査人が行った例（横須賀市（平成１７年度）、船橋市（平成１８年度）、広島市（平成１９年度）、さいたま市（平成１９年度）の監査報告書等）を調査すると、包括外部監査人団の人数は、横須賀市で１０名、監査費用１８００万円、船橋市で８名、監査費用１７００万円（ただし監査テーマはもう一つ有り）、広島市で６名、監査費用１８９９万円（ただし監査テーマはもう一つ有り）、さいたま市で１０名、監査費用１９００万円（ただし監査テーマはもう一つ有り）となっている。目黒区の監査費用の上限は６００万円であり、包括外部監査人補助者としてさらにシステム監査人有資格者を加えることは監査のコスト上到底無理である。

③　人的セキュリティ

情報資産等の外部持出制限についてのルールが遵守されているか。記録媒体に関する管理が適切になされているか。情報セキュリティ研修が実施されているか。ＩＤ及びパスワード管理が適切になされているか。

④　技術的セキュリティ

ＩＤ及びパスワードの管理が情報システム管理者によって適切になされているか。パスワードファイルの管理が適切になされているか。外部からのアクセス制限が適切になされているか。

⑤　運用

情報セキュリティ関連規程遵守上の問題に対して、情報化推進委員会は適切かつ速やかな対処を行っているか。情報システム統括責任者、情報システム管理者、セキュリティ統括責任者及びセキュリティ責任者によって、情報セキュリティ関連規程の遵守状況について定期的な確認が行われているか。問題が発生したときには報告がなされているか。

⑥　評価・見直し

情報セキュリティ関連規程は総務省ガイドラインの改定等をも考慮しながら適切に見直されているか。情報セキュリティについて各部局において定期又は必要に応じた自己点検は行われているか。内部監査は適切に実施されているか。

⑦　その他

個人情報の保護の観点から、個人情報を含む情報を情報システムから出力した紙媒体が不要な場合に廃棄に至るまで適切な手段がとられているか等、情報セキュリティに関連する事項について適切に対処がなされているか。

（２）包括外部監査の主な監査手続

監査に当たっては、監査対象部課に対するアンケート調査を行ったうえ、監査対象部課より情報セキュリティ関連の規程類や関連資料の提出及び情報セキュリティ関連規程にのっとった運用の実態の説明を求めた。また、監査対象部課へ往査し、現場でのヒアリングを実施するほか、サーバの設置状況等現場の把握に努めた。

５　包括外部監査の実施期間

平成２２年９月１３日から平成２２年１２月３０日まで

６　包括外部監査の経過及び実動時間

包括外部監査も貴重な税金から費用を支弁しているものであり、監査の効率性

及び有効性が当然問われるものである。そこで、昨年度の包括外部監査報告書でも説明したが、本件包括外部監査の経過について包括外部監査人及び補助者（以下、「監査チーム」という）が特に留意した点と経過を以下に簡単に説明する。

監査結果が、その対象部局・対象団体にとって有益であり、かつ、その対象部課が内部統制におけるＰＤＣＡサイクルを回して改善を行うためには、表面的ではない深度ある監査が必要である。監査チームはこの点を考慮し、指摘にあたって特に真の問題はどこにあるのかを特定することに留意した。

また、監査対象部課は、資料作成、ヒアリングへの出席等その対応に時間を割かなければならいことを十分考慮し、報告書添付の資料作成を区に依頼して被監査対象部課に過重な負担や、監査期間中に日常業務に支障をきたすことがないよう、効率的な監査を行うことを念頭に置いた。

監査報告書作成にあたっては、一般区民にとって長すぎる報告書が決して読みやすいものではないことを考慮しつつ、かつ監査人としての説明として必要にして十分と思われるレベルになるように、簡潔かつ要点を抑えた記載につとめた。

監査の経過については、概略、以下のとおりである。なお、監査チームのメンバー間のメールによる意見交換や打ち合わせ、通知書、質問書又は報告書案の起案及びそれに対するメールによる意見交換、資料検討、目黒区との連絡等に要した時間は多数日にわたるため、記載を省略し、主に会議とヒアリング実施日のみを記載している。

平成２２年

４月　１日　平成２２年度包括外部監査契約の締結に係る告示
５月２５日　補助者の公示（補助者の始期：６月１日）
６月　１日　監査チームの第１回会議を開催
６月　２日　目黒区総務課へ予備調査の日程及び資料提出要請の連絡
６月２２日　目黒区と監査チームとの会議（予備調査の開始）
７月　６日　目黒区と監査チームとの会議（予備調査）
７月１５日　目黒区と監査チームとの会議（予備調査）
７月２２日　目黒区と監査チームとの会議（予備調査）
８月　２日　監査チーム会議（監査テーマ選定及び提出依頼資料に関する検討）、監査委員との意見交換
８月１１日　目黒区と監査チームとの会議（予備調査）、監査チーム会議（監査テーマ選定及び提出依頼資料に関する検討）
８月３１日　監査チーム会議（監査テーマ選定及び監査通知書の確定）、目黒区へ監査通知書送付
９月１０日　目黒区に質問票の送付

９月１７日～　質問票の回収、集計作業
　　２２日
９月２９日　介護保険課、地域ケア推進課、選管事務局及び生活福祉課のヒアリング
９月３０日　戸籍住民課のヒアリング
１０月１日　子育て支援課、国保年金課のヒアリング
１０月６日　健康福祉計画課、地域ケア推進課、高齢福祉課、障害福祉課、生活福祉課及び子ども政策課のヒアリング
１０月１５日　監査チーム会議（ヒアリングの結果報告、意見交換）
１０月２５日　国保年金課のヒアリング
１０月２７日　選管事務局及び生活福祉課のヒアリング
１０月２９日　監査チーム会議（ヒアリングの結果報告、意見交換）
１０月２９日　戸籍住民課及び子育て支援課のヒアリング
１１月１日　介護保険課、北部地区サービス事務所及び健康福祉計画課のヒアリング
１１月４日　地域ケア推進課及び東部包括支援センターのヒアリング
１１月１１日　監査チーム会議（ヒアリングの結果報告、意見交換）
１１月２４日　国保年金課のヒアリング
１１月２５日　情報課のヒアリング
１１月２６日　地域ケア推進課、北部包括支援センター、南部包括支援センター、健康福祉計画課及び障害福祉課のヒアリング
１１月２９日　監査チーム会議（ヒアリングの結果報告、意見交換）
１１月３０日　戸籍住民課及び子育て支援課のヒアリング
１２月１日　選管事務局、健康福祉計画課、高齢福祉課、生活福祉課及び子ども政策課のヒアリング
１２月７日　中央包括支援センター、西部包括支援センター、地域ケア推進課、介護保険課、高齢福祉課及び生活福祉課のヒアリング
１２月９日　国保年金課のヒアリング
１２月１３日　監査チーム会議（報告書ドラフト、意見交換）
１２月１７日　国保年金課、健康福祉計画課、高齢福祉課及び障害福祉課のヒアリング
１２月２０日　監査チーム会議（報告書ドラフト、意見交換）
１２月２８日　監査チーム会議（報告書ドラフト、意見交換）
１月１３日　監査チーム会議（報告書ドラフト、意見交換）

監査に要した時間（監査報告書作成のための時間も含む）は、監査チーム合計で６５６時間である。

7　外部監査の体制

目黒区包括外部監査人	弁護士	池　永　朝　昭
同	補助者	公認会計士	戎　井　重　樹
同	補助者	弁護士	丹生谷　美　穂
同	補助者	弁護士	金　子　憲　康
同	補助者	弁護士	矢　上　浄　子

8　利害関係

包括外部監査の対象とした事件につき、地方自治法第２５２条の２９の規定により記載すべき利害関係はない。

9　本報告書の構成と留意点

本報告書は、報告書、資料及び報告書公表版からなる。このうち、公表版と資料の一部のみが目黒区によって公開されると思われる。これは目黒区が指定する情報セキュリティに関連する規程や報告を「情報セキュリティ関連文書」と呼び、これを非公開としており（ただしその根拠については明文規定を欠いているが、運用上そのようにしているとの説明を受けている）、また、本件監査の際に包括外部監査人が締結を求められた目黒区との「情報セキュリティ関連文書取扱いに関する覚書」（以下、「覚書」という）により、外部監査人には「情報セキュリティ関連文書で包括外部監査人が知り得た目黒区の人事、技術、事務手続き等の情報（以下、「機密情報」という）を第三者に開示または提供してはならない」と規定されているため、機密情報に含まれる情報を含む監査報告書（それは監査委員が地方自治法上、公開する義務を負っている）をそのまま公開することは困難である。また監査報告書がそのまま公開されると、それ自体がヒントを与えてしまうリスクになるという目黒区の懸念から、監査人は公表版作成の要請を受けたものである。

もとより、本監査報告書の全面的公開がそのようなリスクを発生させることは、包括外部監査人として望むものではないし、区の懸念も理解できるが、他方、区民の知る権利や区民に対する説明責任の重要性にも思いをいたすとき、適切な範

囲の監査報告書の公開はやはり必要である。監査人としては、このような知る権利と説明責任を念頭におきつつ、監査対象のシステムがいずれも外部システムにつながっておらず外部アクセスは不可能であり、リスクがあるとすれば内部の者に対するヒントを与えるというリスクが残るのみであることを考慮した上で、公表版を準備した。

第２　目黒区の個人情報保護及び情報セキュリティの概要

１　歴史

（１）目黒区個人情報保護条例（昭和６３年１０月制定）[3]

目黒区の個人情報保護及び情報セキュリティに関する歴史は、昭和６３年１０月に制定され、平成元年６月から施行された目黒区個人情報保護条例（以下、「個人情報保護条例」という）に始まる。　個人情報の保護に関する法律（以下、「個人情報保護法」という）が制定されたのが平成１５年４月、施行されたのが平成１７年４月であるから、目黒区は相当先進的に取組みを開始していたといえる。

個人情報保護条例は平成１２年、平成１７年及び平成１９年に改正されているが、国の個人情報保護法制確立にあわせた平成１７年改正にあたっては、「個人情報保護条例見直し検討委員会」が組織され、個人情報保護法への対応、目黒区情報公開・個人情報保護審議会における見直しの議論等の視点を踏まえた改正の検討を行い、その報告を受けたうえで改正がなされている。

本件監査に関連する個人情報保護条例の条文は、適正管理の原則（第１０条）、個人情報保護責任者の設置（第１１条）、受託者に対する措置（第１２条）、適正利用の原則（第１３条）、目的外利用の制限（第１４条）、電子計算組織への記録禁止事項（第１６条）、外部の電子計算組織と区の電子計算組織との結合の原則的禁止（第１７条）、運用状況の保護及び公表（第３０条）などがある。

（２）情報セキュリティ基本方針及び情報セキュリティ対策基準（平成１４年８月）

平成１４年５月に幅広い情報化政策の立案やその推進体制も視野にいれた機関として「目黒区情報化推進委員会」（以下、「情報化推進委員会」という）が設置された。

情報化推進委員会では、急速な情報環境の変化へ対処するとともに、ＩＴを活用した区民サービスの充実と一層の業務の効率化を進めるために、今後の区の情報化の指針となる「情報化ビジョン」を策定することとし、検討を開始した。当時の事情はつまびらかでないが、この流れの中で経営企画部情報課は、同年８月に、目黒区における最初の情報セキュリティ関連規程となる「情報セキュリティ基本方針」（平成１４年８月１日付け目企情第１６１号決定）及びこれに基づく「情報セキュリティ対策基準」（平成１４年８月１日付け目企情第１６１号決定）を策定した。

なお、総務省は、平成１３年３月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」[4]（以下、「総務省セキュリティポリシーガイド

---

[3] http://www.city.meguro.tokyo.jp/gyosei/hirakareta/kojinjoho/hogo/jorei/index.html

[4] 平成１３年３月３０日策定、その後平成１８年９月２９日に全部改定。

ライン」という）を策定し、また、前述のとおり平成１５年１２月に総務省ガイドラインを策定している。総務省セキュリティポリシーガイドラインは平成１８年９月に、また総務省ガイドラインは平成１９年７月にそれぞれ改定されたが、目黒区ではこれらの改正に呼応した情報セキュリティ基本方針及び情報セキュリティ対策基準の改定はなされなかった。平成２２年にいたり、ようやく情報セキュリティ基本方針、情報セキュリティ対策基準も改定された。この改定は、目黒区政策決定会議に付議されたうえ決定されている。[5]

目黒区政策決定会議は、「目黒区政策決定会議等の設置及び運営に関する規則」（平成１６年８月目黒区規則第８０号）に基づいて、区の行財政運営の最高方針及び基本施策を審議決定する機関として設置されており、区長、副区長及び教育長並びに部長をもって構成される会議体である。

（３）目黒区情報化ビジョン（平成１４年１１月）[6]

目黒区は、平成１２年度に目黒区基本構想（以下、「基本構想」という）及び目黒区基本計画（以下、「基本計画」という）を策定し、基本構想で提示された３つの基本理念（①人権と平和の尊重、②環境との共生、③住民自治の確立）を定め、また、それらを実現するため目黒区が目指すまちづくりの４つの基本目標（①豊かな人間性をはぐくむ文化の香り高いまち、②ふれあいと活力のあるまち、③ともに支え合い健やかに安心して暮らせるまち、④環境に配慮した安全で快適に暮らせるまち）とその実現に関わる３つの基本方針（①区民と行政の協働によるまちづくりの推進、②男女が平等に参画する社会づくりの推進、③基礎的自治体としての行政能力の充実）を定めていた。基本方針の③についてはさらに１０項目の施策が定められており、その７項目目として「行政情報システムの整備として情報通信基盤の活用やプライバシー保護体制の確立を掲げていた[7]。この基本計画の補助計画と位置づけられる「目黒区情報化ビジョン」（以下、「情報化ビジョン」という）が、平成１４年１１月に定められている。

情報化推進委員会は平成１４年５月から検討を行い、平成１４年１０月に情報

---

http://www.soumu.go.jp/denshijiti/jyouhou_policy/pdf/100712_1.pdf

[5] 第１の９で述べたとおり、目黒区は情報セキュリティ対策基準は、「情報セキュリティ関連文書」として公開をしないという運用を行っており、また、今回の包括外部監査を行う上で包括外部監査人が目黒区から締結することを要求されたために締結した「覚書」により、情報セキュリティ関連文書で包括外部監査人が職務上知り得た目黒区の人事、技術、事務手続き等の情報は「機密情報」とされ、第三者への開示又は提供、複製等が禁止され、また情報セキュリティ関連文書を利用する場合は、事前に区と協議し承認を得なければならないとされている。そして、情報セキュリティ関連文書として、情報セキュリティ基本方針及び情報セキュリティ対策基準等、本件監査報告書で名称や内容を記載している多数の文書が指定されている。この管理のあり方に関わる問題については、第３の包括的指摘事項で取り上げ検討する。

[6] http://www.city.meguro.tokyo.jp/gyosei/keikaku/torikumi/johoka/vision/index.htm

[7] http://www.city.meguro.tokyo.jp/gyosei/keikaku/keikaku/koso/kihonkeikaku/kihon/index.html

化ビジョンを策定して、政策会議に提出した。政策会議は情報化ビジョンを同年１１月に決定し、議会への説明をへて同年１２月に公開した。情報化ビジョンは、個人情報保護と情報セキュリティに関して以下のように述べている。

> **１　個人情報保護**
>
> **ＩＴの一段の進歩により、情報処理の形態が多様化しつつあるため、個人情報の取り扱いやプライバシー保護については、法令や目黒区個人情報保護条例などにしたがい、慎重に対応します。特に、外部コンピュータとの接続や、持ち運び可能な記録媒体の管理については、細心の注意を払う必要があります。**
>
> **また、職員に対しては、研修の充実などにより個人情報の保護を徹底するとともに、データ保護に関する技術の習得と習熟に努めてまいります。**
>
> **２　セキュリティ対策**
>
> **不正アクセス、ハッカーによるサイト攻撃や情報の流出、改ざん、コンピュータウイルス感染などの犯罪行為、もしくは人為的ミスによって引き起こされる混乱は、ネットワーク社会に深刻な事態を招くこととなります。災害や障害等を含めた、このような脅威から情報資産を守るために、情報化の推進にあたっては、情報セキュリティ基本方針に基づいてセキュリティ対策に万全を期すよう努めます。**

また、システムの監査については以下のように述べている。

> **８　費用対効果の評価**
>
> **業務をシステム化する際には、事前評価とシステム稼働後の事後評価を、事務処理時間の削減効果、経費削減効果、行政対応能力の向上効果などの観点から評価する仕組みを検討していきます。**
>
> **さらに、個々の業務システムだけでなく、全庁的な視点からその有効性、情報化の効率性、安全性を客観的に判断する仕組みを検討するとともに、専門的知識を有する第三者機関によるシステムの評価・監査も検討していきます。**

（４）目黒区電子情報処理規則（平成１５年８月）[8]

情報化ビジョンを公表後、目黒区は電子情報処理組織の管理規程の整備に着手し、まず「目黒区電子情報処理規則」（以下、「電子情報処理規則」という）を策定し、全庁で遵守すべき情報処理に関する基準設定を行った。電子情報処理規則では、電子情報組織の管理のための体制が定められた。電子情報処理規則は、その後、平成１６年、平成１７年、平成１９年、平成２０年と改正されているが、現在の規程は概ね以下のように定めている。

[8] http://www.city.meguro.tokyo.jp/gyosei/keikaku/torikumi/johoka/kitei/kisoku/index.html

① 「区の総合的かつ計画的な情報化施策の推進及び適正かつ安全で効率的な電子情報処理の実現を図るため、目黒区情報化推進委員会を設置する。」とされ、情報化推進委員会の法令上の位置づけが明確化され、情報化推進委員会の所掌事項、組織及び運営に関し必要な事項は、区長が別に定めるとされた（第９条）。

② 情報システム統括責任者を設置し、企画経営部長がその任にあたることとされた（第５条第１項）。

③ 情報システム統括責任者を補佐する情報システム管理者を設置し、企画経営部情報課長がその任にあたるとされた（第５条第２項）。

④ 部が所管する電子情報処理の管理運用については、当該部の長がその責任を負うとされた（第５条第３項）（情報セキュリティ対策基準では「セキュリティ統括責任者」と呼んでいる）。

⑤ 電子情報処理に従事する職員は、電子情報を災害、障害、過失及び不正の脅威から保護し、電子情報処理の高度な安全性の確保に努めなければならないという目的規定が設けられた（第１１条第１項）。

⑥ ⑤の目的を達するために、区長は、電子情報のセキュリティ対策に係る基本方針の制定及び改定を行うものとし（第１１条第２項）、情報システム統括責任者は、係る基本方針に基づき、電子情報のセキュリティ対策に係る基準の制定及び改定を行うものとする（第１１条第３項）。これにより、「情報セキュリティ基本方針」の法令上の位置づけは区長による基本方針であることが明確化された。また、「情報セキュリティ対策基準」は「情報セキュリティ基本方針」に基づく情報システム統括責任者が制定する電子情報のセキュリティ対策に係る基準であることも明確化された。

⑦ 情報システム管理者はホストシステムについて、課長はその所管する個別システムについて、電子情報のセキュリティ対策の実際の手順等を定めた実施基準を定め、これを電子情報処理に従事する職員に遵守させなければならない（第１２条）。

⑧ 情報システム統括責任者は、ホストシステムにおける適正かつ安全で効率的な電子情報処理を実施するため、ホストシステムの管理運用に係る基準を定めなければならない（第１５条第１項）。

⑨ 部に置かれる個別システムについては、情報システム統括責任者は、個別システムの管理運用に係る共通基準を定めなければならない（第１６条第２項）。部長は、かかる共通基準に基づき、当該部が所管する個別システムごとにその管理運用に係る基準を定めなければならない（第１６条第３項）。

（５）個別システムのセキュリティ対策に係る基準の制定（平成１５年８月～平成２２年６月）

電子情報処理規則の前記（４）⑨指摘の条項にもとづき、個別システムについ

ては情報システム統括責任者である企画経営部長によって管理運用にかかる共通基準が、個別システムについてはセキュリティ責任者である各課の課長によって電子情報のセキュリティ対策の実際の手順等を定めた実施基準が、それぞれ定められていった。監査対象となっているシステムを中心に、管理運用基準及びセキュリティ実施基準を掲げると、次の一覧表のとおりである[9]。

基準等の名称	制定年月（改正）	対象システム	監査対象	担当部課
目黒区全庁ネットワークセキュリティ実施基準	平成１５年８月	全庁ネットワーク	×	情報課
全庁イントラネット・システム（meg-net）管理運用基準及びセキュリティ実施基準	平成１５年８月	全庁イントラネット・システム	×	情報課
内部情報システム管理運用基準及びセキュリティ実施基準	平成１９年１０月	内部情報システム	×	情報課
標準個別システム管理運用基準及びセキュリティ実施基準	平成１８年４月（平成２２年４月）	国保収納推進員システム	○	国保年金課
戸籍情報システムに係る管理運用基準	平成１８年１２月	戸籍事務（戸籍情報システム）	○	戸籍住民課
戸籍情報システムに係るセキュリティ実施基準	平成１８年４月	戸籍事務（戸籍情報システム）	○	戸籍住民課
保健福祉情報システム障害時対応マニュアル	平成１８年９月	保健福祉情報システム	○	健康福祉計画課
保健福祉情報システム管理運用基準及びセキュリティ実施基準	平成１６年３月（平成２１年３月）	保健福祉情報システム	○	健康福祉計画課
包括支援センターシステム管理運用基準及びセキュリティ実施基準	平成２１年４月	包括支援業務支援システム	○	地域ケア推進課
介護保険システム管理運用基準及びセキュリティ実施基準	平成１６年１月（平成２１年４月）	介護保険システム	○	介護保険課
IC カード取扱基準	平成１８年８月	介護保険システム	○	介護保険課
介護保険システム障害時対	平成１８年８月	介護保険システム	○	介護保険課

[9] ここに掲げられているすべての基準等は「情報セキュリティ関連文書」として非公開とされている。

応マニュアル				
選挙人名簿・期日前投票システム管理運用基準及びセキュリティ実施基準	平成２２年６月	選挙人名簿・期日前投票システム	○	選挙管理委員会事務局
生活保護システム管理運用基準及びセキュリティ実施基準	平成１８年３月	生活保護	○	生活福祉課
児童扶養手当個別システムセキュリティ管理規程	平成１６年１１月	児童扶養手当管理	○	子育て支援課

（６）内部監査と目黒区情報セキュリティ監査実施要綱（平成１９年１０月）

目黒区情報化ビジョン制定後（平成１４年１１月)、目黒区では、ある課所轄の個別のシステムについて、一定のセキュリティ項目基準が遵守されているかどうかを他の課長が監査するという方式の内部監査を行っていたが、その実施については根拠規程や基準がとくに定められてはいなかった。平成１９年１０月に至り、「目黒区情報セキュリティ監査実施要綱」（以下、「情報セキュリティ監査実施要綱」という）を情報課が制定し、内部監査において実施されている項目をルール化した。

情報セキュリティ監査実施要綱では、情報セキュリティ対策基準において情報システム統括管理者が監査体制を確立してセキュリティ対策の徹底及び改善を図るとのみ規定されている情報セキュリティ監査の監査対象、監査人、監査人の権限・責務、監査計画、監査補結果報告等、内部監査の大枠を規定している。すなわち、

① 情報セキュリティの内部監査は、情報システム統括責任者が指名する職員が監査人となり実施すること（監査に関する庶務は企画経営部情報課の責任とされている)。

② 監査計画及び監査実施計画（監査テーマ、監査範囲、監査方法、監査実施日程などを含む）は情報システム統括責任者（企画経営部長）がこれを策定し、情報化推進委員会に報告すること。

③ 情報システム統括責任者は監査実施計画に基づく実施通知を被監査部門に通知すること。

④ 監査人は監査実施計画に基づき監査を実施すること。

⑤ 情報システム統括責任者は監査結果を被監査部門に通知し、監査結果をとりまとめて情報化推進委員会に報告すること。

⑥ 被監査部門のセキュリティ統括責任者は、指摘事項等に対する改善策、改善実施時期などについて情報システム統括責任者に回答すること。

などが定められている。

これらを見れば明らかなとおり、実効性のある内部監査の実現は、情報システ

ム統括責任者である企画経営部長（より具体的には企画経営部情報課）がどのような監査計画、監査実施計画、報告等を行うかにかかっている体制となっているといえる。

（７）目黒区危機管理指針（平成１９年１１月）

目黒区は平成１９年１１月に「目黒区危機管理指針」を制定している。これは目黒区危機管理対策本部等設置要項（平成１９年１１月）に基づいて定められた危機管理の共通事項を定めるとともに各部署が作成する危機管理マニュアル等のガイドラインを示した基本文書であるが、その中で想定される危機の大分類として情報セキュリティが掲げられている。そして、情報セキュリティが問題となる例として「個人情報の漏洩、公文書の紛失・データ消失、情報システム障害・停止、コンピュータウィルス、サイバーテロ、不正アクセス・改ざん」が指摘されている。また、危機に対処するための個別マニュアルの作成が定められており、マニュアル整理状況の一覧表には（５）で一覧表において掲げた規程のうち、まだ存在していなかった「選挙人名簿・期日前投票システム管理運用基準及びセキュリティ実施基準」及び「包括支援センターシステム管理運用基準及びセキュリティ実施基準」を除く全ての規程、情報セキュリティ基本方針、情報セキュリティ対策基準が記載されている。

したがって、目黒区危機管理方針の個別マニュアルの整備に関する基準は、情報セキュリティ関連規程に取り込まれるべきものとして認識されていたといえる。

（８）目黒区情報化推進計画（平成２１年３月）

情報化ビジョン（平成１４年１１月）策定後、庁内ＬＡＮの構築やグループウェアの導入など庁内の情報処理体制の整備等が進んだため、目黒区では情報化ビジョンを見直し、目黒区情報化推進計画（以下、「情報化推進計画」という）を平成２１年３月に策定した。情報化推進計画は、情報化ビジョンと同様、基本計画の補助計画として位置づけられるものである。計画期間は平成２１年度から平成２５年度までとされている。その内容は、４つの基本理念（①ＩＣＴを利用した区民サービスの向上、②ＩＣＴを利用した業務の効率化、③情報セキュリティ対策の強化、④グリーンＩＣＴの実現）を掲げ、それぞれの理念ごとに目標を立て、取組方針とそれを実現する施策を掲げるというものである。情報化推進計画は多岐にわたるが、本件監査に関連すると思われる内容のみを摘示すると、次の一覧表のとおりである。

基本理念	目　標	取組方針	施　　策
ＩＣＴを活用した区民サービスの向上	区民が安全に安心して暮らせるまちにする	《取組方針２－１》災害に迅速に対応する	（施策２－１－２）災害時の業務継続 ①業務継続計画策定（必要事項や留意事項を定めたガイドラインの策定）
	区民との協働を進める	《取組方針３－２》区政の透明性を高める	（施策３－２－１）区政に関する情報の提供 ①行政情報ポータルサイトの構築 ②行政情報目録の区ホームページでの公開・充実
ＩＣＴを活用した業務の効率化	電子情報自治体推進体制を整備する	《取組方針５－１》ＩＣＴの統括管理を確立する	（施策５－１－１）情報化推進体制の見直し ①庁内情報推進組織の必要に応じた見直し ②情報システム評価体制の整備
	情報システムを最適化する	《取組方針６－１》最適化の枠組みを整備する	（施策６－１－１）情報システム管理のガイドラインの策定 ①情報システム関係の導入、調達、開発・構築、運用、評価・改善、アクセシビリティ、セキュリテイに関するガイドラインの整備と運用実態の評価
		《取組方針６－２》情報システムを適正に評価する	（施策６－２－１）情報システムの評価・監査の実施 ①情報システムの目的、運用状況や投資効果等について区職員が評価する手法を確立し、情報システムの定期的な評価と改善を行う ②経済産業省の「システム監査基準（平成１６年１０月改定）」に従い、一定の資格（システム監査技術者等）をもった第三者の監査人による信頼性、安全性及び効率性の観点から専門的監査を実施する。
情報セキュリティ対策の強化	情報セキュリティ対策を強化する	《取組方針８－１》情報セキュリティ対策を強化する	（施策８－１－１）情報セキュリティ対策の改善 ①情報セキュリティポリシーの見直し ②情報セキュリティのための人材育成 ③情報セキュリティ基準の作成・実行及び適時の見直し・改善 ④情報セキュリティ監査の実施方法の検討と実施
			（施策８－１－２）物理的・技術的な情報セキュリティ対策の向上 ①区の情報システムが扱うデータの重要度や業務の種類を考慮した外部データセンターの活用 ②外部搬出データの抑制、外部記憶媒体の暗号化の仕組みの導入等、情報漏えい防止策の強化 ③ネットワークセキュリティシステムの充実

（９）目黒区基本計画（平成２１年１０月）[10]

先にのべたとおり、目黒区は平成１２年度に基本構想及び基本計画を策定していたが、区政を取り巻く環境の大きな変化と区政の諸課題に対応するために平成２１年１０月に基本計画を改定した（以下、「基本計画」とは、別段の断りがない限り、改定後のものを指すことにする）。基本計画では、１０年を計画期間とし、四つの基本目標（①豊かな人間性をはぐくむ文化の香り高いまち、②ふれあいと活力のあるまち、③ともに支え合い健やかに安心して暮らせるまち、④環境に配慮した安全で快適なまち）とそれを具体化させる施策について三つの基本方針（①区民と行政の協働によるまちづくりの推進、②男女が平等に共同参画する社会作りの推進、③基礎自治体としての行財政能力の充実）を維持している。その上で、基本計画を推進するうえで、特に保つことが必要な区の姿勢に関する事項が必要との考えから、「計画推進姿勢の取組方向」の一つとして「身近な政府としての自治体運営の確立」という項目を掲げ、①地方政府としての自治・財政権の拡充、②透明で開かれた区政の推進、③住民参加の仕組みの拡充、④行財政改革の推進、⑤電子自治体の推進、⑥公共施設の計画的配置・整備の６施策の実行を約束している。６施策のうち、本件監査について関係すると思われるものを以下に掲げる。

施策２　透明で開かれた区政の推進

- **○　積極的な情報公開・提供により、区民との情報の共有化を図るとともに区民への説明責任を果たします。**
- **○　情報開示制度を充実させるとともに、情報の公開や提供を拡充し、区が保有する情報の公開を総合的に進めます。**
- **○　個人情報保護制度の的確な運用により、区民のプライバシーの権利を尊重し、個人情報の適切な保護をはかります。**

施策５　電子自治体の推進

- **○　長期的な視野で電子自治体を推進する体制を整備し、有効に活用できる人材を確保・育成します。**
- **○　パソコンや携帯電話などから、いつでもどこからでも手続きや支払いができる電子申請や電子マネーなど支払い方法の拡充を図ります。**
- **○　情報システムを職員自身が評価できる仕組みをつくり、定期的に評価・改善することにより、費用対効果を高めます。**
- **○　情報システムの信頼性、安全性及び効率性を高めるため、第三者機関による監査を実施します。**
- **○　セキュリティ事故事例や技術動向を踏まえ、情報漏えい防止対策の徹底等情報セキ**

[10] http://www.city.meguro.tokyo.jp/gyosei/keikaku/keikaku/koso/kihonkeikaku/kihonkeikaku/index.html

ュリティ対策の強化・充実を図ります。

以上のとおり、目黒区は基本計画において、一方において情報公開を推し進めることを、他方において電子自治体推進のため、人材育成、電子的方法による支払いの拡充、職員自身による定期的評価・改善体制の確立、第三者機関による情報システム監査、情報セキュリティ対策の強化・充実を施策として行うことを、高らかに宣言した。なお、情報化推進計画は基本計画の補助計画という位置づけを失っていない。また、（８）で述べた情報化推進計画の各目標における目標、取組方針、施策をみれば基本計画の施策５とほぼ同じであることが理解できる。

（１０）目黒区実施計画（平成２２年３月）[11]

基本計画の改定を受けて、目黒区は平成２２年３月に目黒区実施計画（以下、「実施計画」という）を策定した。実施計画は基本計画に掲げている施策を計画的に実現するための５ヵ年の事業計画で各年度の予算編成に当たっての指針となるものであり、「実効性を確保する観点から、財源の裏付けを図り、平成２２年度からの５ヵ年に具体化すべき主要な事業の事業量・実施時期等」を明らかにしたもの」である。また、実施計画は、施策の重要性・緊急性を考慮し計画年度中の財源を確保するものである。

ところで、基本計画で「身近な政府としての自治体運営の確立」という項目に関する６つの施策（①地方政府としての自治・財政権の拡充、②透明で開かれた区政の推進、③住民参加の仕組みの拡充、④行財政改革の推進、⑤電子自治体の推進、⑥公共施設の計画的配置・整備）のうち、実施計画では⑤と⑥の項目しか掲げられていない。また、電子自治体の推進のためになすべき施策として掲げられた①電子自治体の推進体制の整備と有効活用できる人材の確保・育成、②電子的方法による支払いの拡充、③費用対効果の高い情報システムの導入・業務の見直し、④職員自身による定期的評価・改善体制の確立、⑤第三者機関による情報システム監査、⑥情報セキュリティ対策の強化・充実のうち、実施計画に入った項目は③のみであった。目黒区の説明によれば、実施計画の策定の段階では５年間の財源の裏づけが必要なものを絞り込み「住民記録系情報システムの再構築」を提出したが、所要経費として１０億円程度が見込まれる同事業は厳しい財政状況にあるという理由で実施計画事業としては認められなかった。

そのかわり、庁内情報処理体制の基盤強化として、「庁内ネットワークの高度利用を促進するため、クライアントＰＣ管理システム移行によりイントラネット・システムの基盤を強化するとともに、個別システム最適化のための共通基盤を強化する。」として平成２２年度から平成２６年度まで１億１５１万５０００円の事業費が計上されている。しかし、これも財政状況を理由に当初検討されて

[11] http://www.city.meguro.tokyo.jp/gyosei/keikaku/keikaku/koso/jisshi_keikaku/jissikeikaku/index.html

いた規模よりも縮小されて計上されたものである。

基本計画の電子自治体の推進のために掲げられた人材育成、電子的方法による支払いの拡充、職員自身による定期的評価・改善体制の確立、第三者機関による情報システム監査、情報セキュリティ対策の強化・充実については、施策実現のためのロードマップは作成されておらず、また事業費用化もされていない状況であるが、目黒区からは基本計画の補助計画である情報化推進計画の施策にも掲げられており、７割程度は着手している状況であるという説明を受けている。その状況の評価は、本件監査の一部をなすことになる。

（１１）外部監査

目黒区の行政改革では、「ＩＴを活用した電子自治体の構築」が平成１６年度から行政改革の目標項目として掲げられ、当該項目の細項目の一つとして、「個人情報の保護等、情報セキュリティの充実」を実行するとされていた。「平成１６年度～平成２０年度目黒区行革白書」[12]では、平成１６年度から平成１８年度までは継続して実施中と報告されており、また、平成１９年度・２０年度の年次別推進プラン項目別取組状況についても「平成１６年度にホストコンピューターによる住民記録（住基ネットを含む)、税務、国保システム等の第三者による情報セキュリティ監査を実施し、１７年度からは、全庁的な自己点検や内部監査を実施しております。」と報告されている。

また、目黒区行革計画（平成２１年３月）[13]では、ＰＤＣＡマネジメントサイクルを実現するための仕組みとして「情報システム評価の実施」が掲げられ、「区の情報システムについて職員によるシステム評価と第三者によるシステム監査を実施し、情報システムが適切に運用されているかどうかを検証します。」（所管は情報課）と記述されている。そして、平成２１年度には、「職員によるシステム評価」「第三者によるシステム監査（内部情報システム)」（後に「職員によるシステム評価の検討」に変更された。）平成２２年度には「職員によるシステム評価」「第三者によるシステム監査（イントラネット＝庁内ネットワーク)」（後に「職員によるシステム評価の検討及び試行」に変更され、かつ、「第三者によるシステム監査」は削除された）を計画していた。

これらの計画に基づいて、実施された第三者による外部監査は、以下のとおりであるが、いずれも全面的な情報システム監査とはいえず、システム監査項目のうち限られた項目を対象としている部分的監査（なお以下の②は監査ではないことに留意）である。

① 平成１６年度のホストコンピューターによる住民記録（住基ネットを含む)、税務、国保システム等の第三者による情報セキュリティ監査

[12] http://www.city.meguro.tokyo.jp/gyosei/keikaku/keikaku/kaikaku/gyoukakuhakusyo/index.html

[13] http://www.city.meguro.tokyo.jp/gyosei/keikaku/keikaku/kaikaku/gyoukakukeikakushin/index.html

② 平成２０年度の内部情報システムを対象として実施されたシステム評価（目黒区内部情報システム評価報告書（平成２１年３月））

③ 平成２１年度のシステム監査（目黒区内部情報システム・システム監査報告書（平成２２年３月））

２ 現在の情報セキュリティ管理体制の概要

（１）基本規程

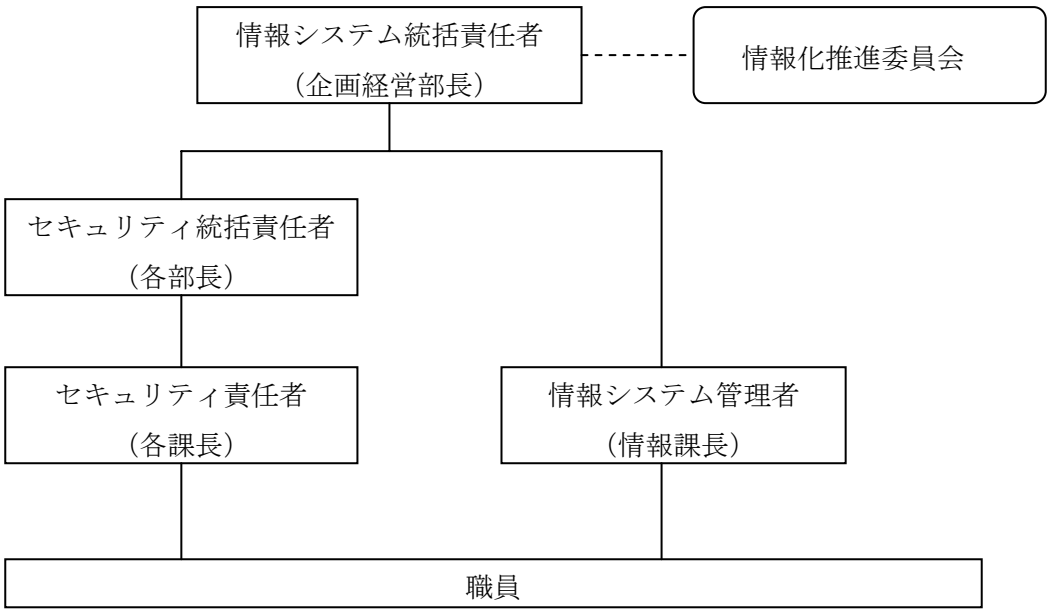
目黒区では電子情報処理規則を制定し、区における電子情報処理に関する基本的な事項を定めている。そして、同規則第１１条第２項に基づき、区の電子情報を災害、障害、過失及び不正といったリスクから保護し、その高度な安全性を確保することを目的として、情報セキュリティ基本方針が定められている。さらに、かかる基本方針に基づく情報セキュリティ対策に係る基準として、上記規則第１１条第３項に基づき、情報セキュリティ対策基準が定められている。

個別システムの管理運用に関しては、まず、情報統括責任者が個別システムの管理運用に係る共通基準を定め、かかる基準に基づき、各部長が部の所管する個別システムごとにその管理運用に係る基準を定めることとされている（電子情報処理規則第１６条第３項、情報セキュリティ基本方針４（３））。このほか、各課長は、個別システムにおける情報セキュリティ対策の実際の手順等について定める実施基準を定めることとされる（電子情報処理規則第１２条）。個別システムの管理運用基準と情報セキュリティ実施基準は、個別システムによってはまとめて（単一の文書として）制定されている（「介護保険システム管理運用基準及びセキュリティ実施基準」など）。

（２）管理体制

目黒区では、上記（１）の基本規程に基づき、情報セキュリティに関して、次のような組織体制が採られている。すなわち、まず区の計画的な情報化施策の推進及び適正かつ安全で効率的な電子情報処理の実現を図るためとして、情報化推進委員会を設置している（電子情報処理規則第９条第１項）。その上で、電子情報処理の管理運用を総合的に行うため、企画経営部長を情報システム統括責任者とし、情報セキュリティ対策の推進及び総合的な管理に係る事務に当たらせるとともに（同第５条第１項、第６条）、企画経営部情報課長を情報システム管理者とし、情報システム統括責任者の補佐及び電子情報処理の管理運用の具体的な推進事務を行わせている（同第５条第２項、第６条）。また、各部長をセキュリティ統括責任者とし、部が所管する電子情報のセキュリティ対策や個別システムの開発及び管理運用について責を負わせている（同第５条３項、第７条）。さらに、各セキュリティ統括責任者を補佐し、各課において所管する業務にかかる情報セキュリティ対策を実施するためとして、各課長をセキュリティ責任者に任じてい

る。以下は、これらの情報セキュリティ管理体制を図示したものである。



（３）内部監査体制

情報セキュリティ基本方針の実施状況について定期的に監査や自己点検が行われることは、総務省セキュリティポリシーガイドラインでも、情報セキュリティ対策を徹底するために必要とされている[14]。目黒区では、情報セキュリティ監査及び職員による自己点検が実施されている。また、平成１９年には「情報セキュリティ監査実施要綱」が定められ、平成１７年度以降、職員を監査人とする情報セキュリティ内部監査が当該要綱に基づき実施されるようになった。

（４）教育体制

情報セキュリティの教育・研修の実施は、総務省セキュリティポリシーガイドラインでも、情報セキュリティの人的セキュリティの一内容として重要とされている[15]。目黒区では、情報システム統括責任者は定期的に情報セキュリティに関する研修を実施することとされ、またセキュリティ責任者は、所管の情報資産の情報セキュリティについて必要な研修を実施することとされている。

[14] 総務省セキュリティポリシーガイドライン３．８参照。
[15] 同３．５．２参照。

第３　外部監査の結果及び意見

１　国保年金課

（１）監査対象部課の業務の内容

区民生活部国保年金課は、国民健康保険料の収納推進業務を担当している。その業務は、国民健康保険料収納対策の一環として、保険料未納世帯に対し、個別訪問して保険料の徴収や口座振替の勧奨、生活実態調査、住居・資格確認調査を行うことであり、収納推進員支援システムは保険料の収納率の向上を図ることを目的に、平成１３年度から採用した収納推進制度とともに導入された。

収納推進員は専務的非常勤職員であり、現金取扱員として保険料の徴収等の業務を行う。収納推進員は日曜から土曜の１週間中５日勤務し、訪問計画の作成、日々の現金収納及び結果入力を行っている。土日に勤務した場合は、翌週の初日にすぐ収納整理を行う。

（２）監査の対象システムの概要

名称	国保収納推進員システム
目的	国民健康保険料の訪問徴収世帯の管理
システムの取扱い業務	訪問カードの出力、訪問結果の入力、収納推進員の管理の各業務
導入年度	平成１３年度
登録データ	訪問の有無、訪問の日時、接触の有無、保険料の徴収状況（現年・滞繰）、口座振替依頼の有無、居住調査の有無、資格調査の有無、留意事項等

国保収納推進員システムを用いた事務のフローは別紙３のとおりである。

（３）情報セキュリティ体制

セキュリティ責任者	国保年金課長
システム担当者[16]	納付相談係収納推進員担当職員
システム使用者[17]	納付相談係収納推進員担当（非常勤）４名

[16] 個別システムの管理運用基準及びセキュリティ実施基準においてセキュリティ責任者によって指定されると定められている当該個別システムの担当者をいう。

[17] セキュリティ責任者によって個別システムの使用が認められている者をいう。個別システムによっては「操作者」と称されている。

情報セキュリティ実施基準等	「標準個別システム管理運用基準及びセキュリティ実施基準」（平成１６年１月２０日制定、平成２２年４月１日改正）「収納推進員システムトラブル時対応手順」
システムの構成	パソコン３台、プリンタ２台
盗難防止他	「標準個別システム管理運用基準及びセキュリティ実施基準」の盗難防止措置欄において、「ア最後に使用した者が引き出しを施錠、イ最後に使用した者がキャビネットを施錠、ウ常時盗難防止用ワイヤー設置、エその他」の選択肢があるが、「エその他」を選択している。
バックアップ体制	システム担当者が定期的に電磁的記録媒体にバックアップする。
外部との接触	当該システムに必要なホストシステム上の資格・住記個人データ・世帯データ、収納データを定期的に電磁的記録媒体によって取り込む
障害時対応	「収納推進員システムトラブル時対応手順」が作成されている。
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	過去実施なし

（４）指摘事項

ア　パスワードの定期的な変更の未実施

現在の「標準個別システム管理運用基準及びセキュリティ実施基準」で規定しているセキュリティ実施基準では、パスワードの定期的な変更についての記載がないため、平成１３年度に導入して以来、定期的なパスワードの変更の実施は行っていない。アクセス権限の徹底の観点より、適切なセキュリティ対策基準として定期的なパスワードを変更するよう「標準個別システム管理運用基準及びセキュリティ実施基準」の見直しを行うことが必要である。

イ　盗難防止措置の不十分な規定

「標準個別システム管理運用基準及びセキュリティ実施基準」では、同システムに使用されるパソコンの盗難防止措置に関する規定が不十分であるため、関連する規程について再度見直しを行い、具体的な防止措置について文書化することが必要である。なお、現場では、施錠等の盗難防止策が実施されている。

（５）監査人の意見

ア　区外転出者の国民健康保険料未納額の回収を

監査の過程で発見した項目で情報セキュリティに関連しないが、平成１８年

度の包括外部監査においても当該国民健康保険料の未納額について取り上げられており、一市区町村では解決できない課題もあり、その重要性を考え、意見として以下に記載する。

市区町村は、国民皆保険制度のもとで医療の給付又は医療費の支給等をする健康保険の制度の一つとして、国民健康保険法に基づき、加入者（被保険者）が納める保険料や国などの補助金により国民健康保険を運営している。そのため国民健康保険料の未納の問題は、国民健康保険制度の運営の重要な課題となっている。目黒区でも約１３億円の滞納金額があり、回収に向けて活動を行っているところである。

①目黒区の滞納状況と欠損処理状況

目黒区における「年度別滞納件数と金額（２月催告件数と金額)」、「年度別収納推進員直接収納金額」及び「年度別欠損処理額」は以下のとおりである。

【年度別滞納件数と金額】　（金額単位：円）

年度	区内件数	金額	区外件数	金額	合計件数	合計金額
平成２０年度	11,003	1,196,718,838	2,137	148,399,170	13,140	1,345,118,008
平成２１年度	10,892	1,148,055,188	2,251	162,479,781	13,143	1,310,534,969

【年度別収納推進員直接収納金額】

年度	直接収納金額（単位：円）
平成２０年度	41,586,668
平成２１年度	47,286,246

【年度別欠損処理額】　（金額単位：円）

年度	現年度分(注１)		過年度分(注２)		不納欠損合計	
	世帯数	金額	世帯数	金額	世帯数	金額
平成２０年度	6,629	485,425,163	494	59,330,123	7,123	544,755,286
平成２１年度	6,701	483,834,672	695	72,987,258	7,396	556,821,930

注１・・当年度に時効が到来すること等で欠損処理したもの

注２・・時効中断等による未納額を欠損処理したもの

②未納健康保険料回収の検討課題

目黒区内における健康保険料の滞納については、収納推進員が直接訪問して収納することができるが、収納推進員が対象とするのは、あくまでも目黒

区内の未納者でかつ社会保険加入・生活保護加入などの資格喪失者及び分納中を除外した世帯であり、目黒区外へ転出した未納保険者への訪問による回収は対象外となっている。つまり、健康保険料未納のままで目黒区外へ転出した場合には、目黒区内の未納健康保険料への回収活動に比べると回収への取り組みが弱いと言える。

他方、他の地方自治体での未納健康保険料がある被保険者が目黒区に転入した場合、目黒区の未納健康保険料ではないため目黒区が回収する債権の対象とはなっていない。このような未納健康保険料に対する対応状況を考えれば、地方自治体間の相互協力が未納健康保険料の回収には不可欠である。

健康保険料は国民皆保険制度を担う財源であり、その維持・運営を図るためには自治体間で協力して未納健康保険料を回収する方法を模索することが望まれる。

2　戸籍住民課

（1）監査対象部課の業務の内容

戸籍住民課は、住民登録や戸籍、印鑑登録、外国人登録などの居住・身分関係に関連する業務を所掌している。監査では、同課の所管する「戸籍情報システム」を対象として監査を行った。同システム利用による業務フローは別紙４のとおりである。

（2）監査の対象システムの概要

戸籍住民課においては、戸籍証明係の所掌する戸籍に関する証明書発行業務、戸籍届出係の所掌する戸籍関係の届出処理業務の２つの業務を、「戸籍情報システム」という１つのシステムで取り扱っている。

名称	戸籍情報システム
目的	戸籍事務をコンピュータで取り扱うことにより、住民サービスの向上と事務の省力化を図る
システムの取扱い業務	主に届出処理、証明発行、郵送処理等を含む戸籍事務
導入年度	平成１９年６月（平成１９年１０月全面稼動）
登録データ	現在戸籍附票、除籍改製原戸籍及び平成改製原戸籍、記載不要届出書のイメージデータ、受附帳イメージデータ等

（3）情報セキュリティ体制

戸籍情報システムの情報セキュリティ体制の概要は以下のとおりである。

セキュリティ責任者	戸籍住民課長
システム担当者	課長の指定する職員
システム使用者	戸籍届出係、戸籍証明係、住民記録係の担当職員（非常勤含む）
情報セキュリティ実施基準等	「戸籍情報システムに係る管理運用基準」（平成１８年１２月２８日制定） 「戸籍情報システムに係るセキュリティ実施基準」（平成１８年４月２４日制定）
システムの構成	メインサーバ１台、バックアップサーバ１台、住基連携サーバ１台、クライアント１６台（戸籍証明係６台、戸籍届出係１０台）、イメージスキャナ１台、プリンタ８台（戸籍証明係４台、戸籍届出係４台）
バックアップ体制	データ:定期に電磁的記録媒体等にバックアップが作成されるシステム：年に１度外部委託業者がバックアップを作成する
外部との接触	当該システムに必要なホストシステム上の住民記録データ等を電磁的記録媒体によって取り込む このほか、毎年１回法務局にデータを持参
障害時対応	「土日・夜間の窓口対応時に機械のトラブルが生じた場合の対応について」（平成１７年５月１７日） 「戸籍システム障害時の事務の代替手順」
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	平成１７年度に実施。戸籍情報システムの導入前であるため、同システムを対象とするものではなかったが、課内における情報処理に関して職員のセキュリティ知識レベルの引上げとセキュリティ事故への対応・準備が必要との指摘がなされた。

（４）指摘事項

ア　定期的なパスワード更新の不徹底

戸籍情報システムにおいては、各職員にそれぞれの利用権限に応じたパスワードが配属時に付与される。かかるパスワードについては、定期的な更新が義務付けられており、かかるパスワードの変更は各職員の裁量による管理に任されているところ、職員アンケート及びヒアリングによれば、パスワードを更新していない職員が複数おり、またセキュリティ責任者及びシステム担当者も特に各職員のパスワード更新の状況を把握しておらず、注意喚起等もしていないという状況であった。また、セキュリティ責任者は質問票に対する回答においては「パスワードの変更を指示している」としていたが、事後のヒアリングにおいては、特に定期的には変更を指示しておらず、自身も定期的な変更は行っていないとの回答がなされた。

ついては、上記基準どおりの運用が徹底されるよう、周知の徹底や、定期的

なパスワードの更新を義務付ける機能を当該システムにおいて導入することも視野に入れ、実効性のある対策を講じるべきである。この点、「定期的なパスワードの更新を義務付ける機能」については、当初のヒアリングでは「システムの追加的なカスタマイズが必要」と説明されていたが、監査期間中に、システム中にパッケージの一部として当該機能が実装されていたがこれまで利用されていなかったことが判明したとの報告を受けた。今後は当該機能を活用したパスワードの定期的な更新が確保されるべきである。

イ　バックアップデータの区外の施設における保管の未検討

戸籍情報は、区にとってきわめて重要性の高い個人情報であるため、滅失した場合に備え、定期的にバックアップデータの保管を行うことが必要である。戸籍データについては、上記（３）のとおり、平日はバックアップが行われているが、これらのバックアップはいずれも庁内のみで保管されるものであるため、広域災害等で戸籍データが滅失するといった事変には対応していない。また、戸籍法第７５条に基づき、毎年一度管轄法務局である東京法務局に戸籍データのバックアップが送付されているが、年に一度のみの更新では、かかるバックアップから最新のデータを復元するのは容易ではないと考えられる。

目黒区では、「特に重要な」電子データのバックアップについては区外の施設において保管すべき旨が定められている。なお、東京法務局へのヒアリングによれば、戸籍データのバックアップを一定の頻度（２週間など）で庁外の遠隔施設において保管することは、戸籍法の運用上特に問題とはならず、実際に庁外保管を行っている例は存在するという。目黒区でも、戸籍データが「特に重要な」データに該当するか再度検討を行った上で、区外の施設において戸籍データのバックアップの保管を行うことを検討すべきである。

ウ　システムを取り扱う職員の情報セキュリティ研修の不十分な受講状況

上記（３）の表のとおり、平成１７年度の情報セキュリティ内部監査では、セキュリティポリシーや規程類に対する職員の理解度の低さが指摘されている。また、ヒアリングによれば、新たに同課に配属された職員や非常勤職員に対しては戸籍住民課長による研修のほか情報課の実施する研修を受ける義務があり、また課内のセキュリティ責任者、ＩＴリーダーにもセキュリティ研修を受ける義務があるが、システム担当者を含む他の職員に対しては特に継続研修は義務付けられていないとのことである。ヒアリングによれば、全職員対象の情報課の開催する研修会やｅラーニングを利用した情報セキュリティ研修を自発的に受けている職員はいるが、窓口対応により中断を余儀なくされる中で研修を受けるという難点からか、受講する職員は多くはないとのことである。また、ｅラーニングを受講している職員の数についても、特に課としては把握

していないとのことである。

当該システムで取り扱う情報の重要性に鑑み、戸籍情報システムを利用して業務を取り扱う職員（非常勤含む）については、定期的に（たとえば２年間に１度など）情報セキュリティに関する研修を受けさせるなどの対策を採るべきである。また、職員の研修の受講に際しては、研修室の利用を促すなど、集中して効率的に研修を受けられるように配慮するべきである。

エ　住民基本台帳法に基づく居住実態調査中の個人情報持ち出しに関する管理の不徹底

本監査期間中の１１月１６日、西部地区サービス事務所の職員が住民基本台帳法に基づく居住実態調査を実施中、個人情報の記載された文書を紛失するという事故が発生した。かかる紛失が報告されたのは、紛失から２日後の１１月１８日になってからであった。紛失した文書は４世帯分の「実態調査票」及び「住民記録システム個人現状照会画面の画面コピー」であり、これら書類には住所、氏名、性別、生年月日、前住所、本籍等の個人情報が記載されていたとのことである。上記「住民記録システム個人現状照会画面の画面コピー」は、適正な管理が要求される帳票等に当たると考えられるところ、当該コピーが外部調査中に紛失したこと、紛失の発覚が遅れたという事故は、所属部長である区民生活部長が認めているとおり、その管理に以下のような不徹底があったことによるものである。すなわち、当該業務に関し、帰庁時のチェック体制等を含め、携帯する個人情報を厳選し、最小限の情報所持による事務執行が可能となる体制作りが不徹底であった。監査人団は、上記事故が監査対象の課の所管の範囲内であることに鑑み、本件事故への対応に関し追加的な監査を行った。

監査において明らかとなった事実は以下のとおりである。すなわち、上記事故について職員から報告を受けた西部地区サービス事務所長（セキュリティ責任者）は、「目黒区危機管理指針」に記載の対応方法に基づき、所属部長である区民生活部長（セキュリティ統括責任者）、企画経営部長（情報システム統括責任者）、情報課長（情報システム管理者）及び広報課長に当日中に報告を行い、その翌日には区議会に対しても報告を行うとともに、報道機関への連絡と区ホームページへの掲載を行っている。その一方で、戸籍住民課及び各地区サービス事務所は、一旦居住実態調査を休止して再発防止のための対策を検討し、住民基本台帳実態調査の取扱いとして①調査に持ち出す書類を調査対象者のみとし、個人情報の項目も必要最小限とすること、②実態調査及び事務処理終了後には、関係書類は直ちに鍵付の保管庫等に保管すること、③関係書類は散逸しにくいファイル（リング付ファイルなど）を利用するとともに、書類の盗難や落下に注意すること等が確認された。実態調査が再開されたのは、本件事故の３週間後、これら事項の確認についての通知が戸籍住民課長により行われてからであった。これらの対応に関しては「目黒区危機管理指針」に従った

対応が行われたとの評価が可能であるが、居住実態調査を担当する職員が携帯する情報の重要性に鑑み、今後も戸籍住民課及び各地区サービス事務所において今回確認されたような取扱いが徹底されるべきである。

3　健康福祉計画課

（1）監査対象部課の業務の内容

健康福祉計画課は、健康福祉事業に係る情報の一元管理・共有化を図ることで福祉の各事業の連携を容易にし、事務事業の一層の効率化を実現するために保健福祉情報システムを導入し、その維持管理を担っている。その保健福祉情報システムを高齢者福祉課、地域ケア推進課、障害福祉課、生活福祉課、子ども政策課が活用している。その活用している業務内容は以下のとおりである。

①　高齢福祉課

高齢者に対するサービスを提供している。そのうち、保健福祉情報システムを使用して以下の事業を実施している。

〔提供するサービス〕

ひとりぐらし等高齢者登録、電話訪問、家具転倒防止器具取付、理美容サービス、寝具乾燥消毒サービス、高齢者自立支援住宅改修給付、紙おむつの支給、おむつ代の支給、福祉電話の設置、高齢者火災安全システム、緊急通報システム、非常通報システム、訪問食事サービス、週一食事サービス、養護老人ホーム入所、特別養護老人ホーム入所

②　障害福祉課

障害福祉サービス、相談支援及び地域生活支援事業の提供体制を確保している。そのうち、保健福祉情報システムを使用して以下の事業を実施している。

〔提供するサービス〕

心身障害者福祉手当、特別障害者手当、障害児福祉手当、経過的福祉手当、心身障害者医療費助成、福祉タクシー券、自動車燃料費助成、リフト付き福祉タクシー、リフト付き福祉小型バス、紙おむつ支給、寝具乾燥消毒、点字新聞購読料補助、原爆被爆者見舞金、電話使用料助成、理美容サービス

③　生活福祉課

災害、病気、入学などで急に資金が必要になり、しかも調達が困難な区民に対する資金の貸付に保健福祉情報システムを使用している。

④　子ども政策課

２０歳未満の児童を扶養している配偶者のない女子に対し、その経済的支援と生活意欲の助長を図り、あわせてその扶養している児童の福祉を増進するための母子福祉資金の貸付、女性の経済的自立と生活意欲の助長を図り、福祉の増進に寄与するために、事業の開始、継続、就職などのために資金を必要とする女性で、一定の要件を満たす方を対象にする女性福祉資金の貸付に保健福祉情報システムを使用している。

⑤　地域ケア推進課

地域包括支援の後方支援としての相談業務において保健福祉情報システムを使用している。

（２）監査の対象システムの概要

名称	保健福祉情報システム
目的	保健福祉事業における保健福祉サービス利用者の管理・通知作成
システムの取扱い業務	健康福祉関連業務
導入年度	平成１０年度
登録データ	氏名、住所、税、国保、総合登録サブシステム関連データ、援護サブシステム関連データ、施設入所サブシステム関連データ、医療サブシステム関連データ、資金貸付サブシステム関連データ、手当サブシステム関連データほか

保健福祉情報システムを用いた事務のフローは別紙５のとおりである。

（３）情報セキュリティ体制

セキュリティ責任者	健康福祉計画課長
システム担当者	健康福祉計画課保健福祉計画担当係長のうちから、健康福祉計画課長が若干名を指定
システム使用課と使用者	健康福祉部の地域ケア推進課、高齢福祉課、障害福祉課、生活福祉課、子育て支援部の子ども政策課で８６名
情報セキュリティ実施基準等	「保健福祉情報システム管理運用基準及びセキュリティ実施基準」（平成１６年３月１０日制定、平成２１年３月２７日改正） 「保健福祉情報システム障害時対応マニュアル」
システムの構成	サーバ２台、パソコン３３台他

盗難防止他	サーバ機は、サーバ室に設置し、その開閉扉の鍵はシステム担当者が管理する。サーバ機の周辺機は盗難防止対策を講じている。各課で使用するパソコンは、各課で対応する。
バックアップ体制	定期的に電磁的記録媒体にバックアップを行う
外部との接触	当該システムに必要なホストシステム、介護システムの情報を定期的に電磁的記録媒体によって取り込む。包括支援システムに対して保健福祉情報システムの情報を 定期的に電磁的記録媒体で提供する。
障害時対応	「保健福祉情報システム障害時対応マニュアル」が作成されている。
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	平成１８年度に実施され以下の項目の指摘が行われている。 １．保健福祉計画係にあるイントラネットパソコンが、容易にカウンターから見えてしまうことについて ２．保健福祉情報システムパスワードの更新頻度の検討について ３．パスワードの種類が多く、煩雑のためメモで書いておいてしまうことについて ＜改善状況＞ ２．のパスワードの変更については、事業の実施課の業務を考慮している。１．と３．の指摘事項については、改善されている。

（４）指摘事項

特になし

（５）監査人の意見

ア　高齢福祉課は委託事業会社保有の個人情報の取扱いの検討を

監査の過程で発見した項目で情報セキュリティに関連しないが重要性を考えて記載している。

目黒区では、高齢者に対して区独自の福祉サービスを提供している。その過程で業務の必要性により個人情報を提供することになる。例えば、高齢者在宅配食、紙おむつの供給、寝具乾燥消毒等の事業委託については、氏名、住所等の情報が提供されなければ事業の委託はなしえない。そこで、提供される個人情報の取扱いについて、契約書、仕様書を入手して個人情報に関する取扱いの記載について確認したところ、守秘義務に関する一般的な規定はあるものの、委託事業の終了に伴う資料の返還については特に規定されていなかった。

このような個人情報の取扱いは、委託する事業会社が変更しない場合には問

題は生じないが、委託事業会社の変更がある場合、個人情報が事業会社に保有し続ける現状の取り扱いでよいか検討が必要と考える。目黒区作成の「目黒区職員のための個人情報保護・情報セキュリティハンドブック」では、委託事業については、委託先への要求事項として事業終了後の資料の返却を記載している。また、障害福祉課の仕様書では提供した名簿は契約期間満了後の返却を記載している。高齢福祉課も秘密の保持の観点から委託事業の終了に伴う名簿等の個人情報の返還について契約書、仕様書の見直しが望まれる。

4　地域ケア推進課

（1）監査対象部課の業務の内容

地域ケア推進課は、介護保険法（平成１８年４月改正法施行）に基づき、地域支援事業として、介護予防事業、包括的支援事業（総合相談・支援事業、権利擁護事業、包括的・継続的ケアマネジメント事業、介護予防ケアマネジメント事業）、及び任意事業を行い、このうち包括的支援事業は地域包括支援センター（以下「包括支援センター」という。）を設けて実施する。包括支援センターは北部・東部・中央・南部・西部の５ケ所があり、それぞれ以下の受託法人に対して１年単位で包括的支援事業等を委託している。

北部包括支援センター	株式会社やさしい手
東部包括支援センター	社会福祉法人目黒区社会福祉事業団
中央包括支援センター	社会福祉法人目黒区社会福祉事業団
南部包括支援センター	社会福祉法人目黒区社会福祉協議会
西部包括支援センター	社会福祉法人目黒区社会福祉事業団

（2）監査の対象システムの概要

名称	包括支援業務支援システム
目的	・包括支援センターの相談支援業務、申請受付業務等に必要な行政情報の提供 ・包括支援センターの申請受付業務等を処理するための書面伝送機能
システムの取扱い業務	同上
導入年度	平成２１年４月
登録データ	住民記録情報、外国人登録情報、介護保険情報、高齢者登録情報、障害情報等

包括支援業務支援システムを用いた事務のフローは、別紙６のとおりである。

（３）情報セキュリティ体制

セキュリティ責任者	地域ケア推進課長
システム管理者	地域ケア推進係及び相談支援係のうちから課長の指定する職員２名
システム担当者	地域ケア推進課の各係、介護保険課、高齢福祉課及び各包括支援センターにおいて課長が指定する各１名
操作者	次の者及び地域ケア推進課長が特に認めた者 ・地域ケア推進課の職員 ・介護保険課、高齢福祉課の職員のうち、業務上システムを操作する必要があると所属長が認め、地域ケア推進課長が指定した者 ・各包括支援センターの職員（臨時職員を除く。）
情報セキュリティ実施基準等	「包括支援センターシステム管理運用基準及びセキュリティ実施基準」（平成２１年４月１日制定）
システムの構成	サーバ１台[18]、クライアントＰＣ１６台（地域ケア推進課・介護保険課・高齢福祉課に各２台、包括支援センター各２台）、スキャナ１３台（地域ケア推進課・介護保険課・高齢福祉課に各１台、包括支援センター各２台）、プリンタ３台（地域ケア推進課・介護保険課・高齢福祉課に各１台）
バックアップ体制	データ： 定期的に作成している。 システム： バージョンアップ及び設定変更を行った際に、運用保守受託事業者において行う。
外部との接触	ホストシステム、介護保険システム及び保健福祉情報システム上のデータを定期的に電磁的記録媒体によって取り込む。
障害時対応	「包括支援センターシステム管理運用基準及びセキュリティ実施基準」（平成２１年４月１日制定）
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	・地域ケア推進課を対象とする内部監査は、平成２２年度に実施される予定。 ・地域ケア推進課が平成２２年９月６日及び７日に、各包括支援センターに対して、情報セキュリティ監査（包括支援センターシステムに限定せず、各包括支援センターにおける情報セキュリティ全般を対象とするもの）を実施し、受託者設

[18]管理サーバ、データベースサーバ、セキュリティサーバ、ファイルサーバの４種類セットで１台を意味している。

	置システムについて一部ウィルス対策ソフトが導入されていないため、インターネットに接続していない場合でも導入すべきこと（南部包括支援センター）等を指摘。

（４）指摘事項

ア　規程の不十分な周知状況

各包括支援センターにおいては、システムについては地域ケア推進課が策定した「包括支援センターシステム管理運用基準及びセキュリティ実施基準」が適用されるものであるが、西部包括支援センターでは当該基準を保管してはいたものの、直ちには見つけ出すことができず、職員への適切な周知が行われているとは言い難い状況であった。セキュリティ責任者は職員が常に情報セキュリティ関係規程等を閲覧できるようにしなければならないとされているから、規程類の保管場所につき職員に周知し、必要に応じて閲覧できる体制を整えるべきである。

（５）監査人の意見

ア　キャビネットの鍵の管理の工夫を

各包括支援センターでは、相談記録等の個人情報の含まれた書類をファイル等で保管し、それらを鍵のかかるキャビネットの中に置いている。キャビネットは施錠し、その鍵は鍵のかかる場所に保管してあるが、当該鍵のかかる場所の鍵は夕方の職員退出時から明朝の出勤時までは、それぞれ職員間で合意された施錠されていない場所に置かれている。各包括支援センターで扱う相談記録等は守秘性の高い個人情報を多く含んでいることからすると、最終的に施錠がされていない状況は好ましくなく、たとえばダイヤル式の金庫を購入して夜間や休日はこれに鍵を保管する等の工夫が望まれる。

５　介護保険課

（１）監査対象部課の業務の内容

介護保険課は、介護保険法（平成１８年４月改正法施行）に基づき、被保険者資格記録管理、保険料納付記録管理、受給者管理、納付実績管理等の業務を行っている。目黒区の地区サービス事務所のうち東部地区サービス事務所を除く４ケ所（西部・南部・北部・中央）は、介護保険被保険者証の交付、保険料の収納等の業務を行っている。

（２）監査の対象システムの概要

名称	介護保険システム
目的	・区が運営する介護保険の被保険者の資格管理及び保険料納付管理 ・介護保険サービス受給者の受給者管理及び給付実績管理 ・介護サービスの低所得利用者負担軽減補助事務執行 ・要介護認定情報の管理 ・主治医意見書作成料等の支払事務執行
システムの取扱い業務	同上
導入年度	平成１７年３月
登録データ	住民記録情報、外国人登録情報、住民税情報、医療保険情報

目黒区介護保険システムを用いた事務の概要は、別紙７のとおりである。

（３）情報セキュリティ体制

セキュリティ責任者	介護保険課長
システム管理者	介護保険課介護保険管理係のうちから課長の指定する職員２名
システム担当者	介護保険課各係・各地区サービス事務所・高齢福祉課・地域ケア推進課・生活福祉課職員から課長が指定する各１名
操作者	次の者及び介護保険課長が特に認めた者 ・介護保険課職員のうち、介護保険課長が指定する者（現在６９名） ・地区サービス事務所（東部を除く）、高齢福祉課、地域ケア推進課及び生活福祉課に属する職員のうち、業務上システムを操作する必要があると所属長が認め、介護保険課長が指定した者
情報セキュリティ実施基準等	「介護保険システム管理運用基準及びセキュリティ実施基準」（平成１６年１月２７日制定、同２１年４月１日改正）、「ＩＣカード取扱基準」（平成１８年８月１８日制定）
システムの構成	サーバ６台、クライアントＰＣ３８台（うち地域ケア推進課・高齢福祉課・生活福祉課に各１台、地区サービス事務所に各１台）、スキャナ６台、プリンタ１７台（うち地区サービス事務所に各１台）
バックアップ体制	データ： 定期的に作成している。 システム：バージョンアップ及び設定変更を行った際に行う。

外部との接触	・ホストシステムから住民記録情報等を受取り、介護情報の提供を行う。 ・保険給付の審査・支払業務のために、国民健康保険団体連合会との間で給付実績、受給者情報等の受取及び受渡を行う。 ・介護保険料等の特別徴収のために、国民健康保険団体連合会を通じて年金保険者との間で特別徴収情報の受取及び受渡を行う。 ・保険給付、介護保険料還付金、主治医意見書作成料等の支払い、介護保険料口座振替のために、金融機関との間で電磁的記録媒体によって支払・収納データの受取及び受渡を行う。 ・介護保険課から都道府県に対して、事業状況報告（月報・年報）として統計データを提出する。（個人情報は含まれない。） ・介護保険課は、認定審査会が要介護審査・認定を行うにあたって必要な情報を提出する。（紙データのみで、かつ個人情報はマスキングして認定審査会に提出し、審査終了後直ちに回収する。）
障害時対応	「介護保険システム障害時対応マニュアル」
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	・介護保険課を対象とする監査人による内部監査は、平成１８年度に実施された。サーバルームの監視カメラのうち１台の故障等の指摘があったが、その後対処された。 ・平成１７年に、北部地区サービス事務所、中央地区サービス事務所、南部地区サービス事務所、西部地区サービス事務所を対象として、情報セキュリティ内部監査を実施した。セキュリティ実施手順などの規定の理解度が低いこと等が指摘され、その対策として、職員への規定の周知等を行った。

（４）指摘事項

ア　電磁的記録媒体の不十分な管理

介護保険課は、サーバ保管庫の鍵のかかるキャビネット内において、電磁的記録媒体を１年間保管している。ただ、電磁的記録媒体の一覧表が作成されていないため、仮に保管されている電磁的記録媒体の一部を誰かが持ち出したとしても、どの電磁的記録媒体がいつ持ち出されたかが把握できないこととなる。従って、電磁的記録媒体の一覧表を作成し、定期的にその保管を確認すべきである。

イ　不要な紙類の不適切な管理

介護保険課は、不要になった紙類（保険料納入にかかる催告状、督促状などが多い。）は段ボールに入れておいて、１ケ月に一度溶解処理に出しているが、その保管している１ケ月の間は鍵のない棚において保管されており、近くの者は誰でもこれを見たり取り出したりすることが可能な状況にある。介護保険課にて扱う書類は個人情報を含むものも多いため、不要になった書類の保管・処分については情報漏えい対策を徹底すべきである。具体的には、たとえば小型のシュレッダーを購入して不要な書類が出るたびにシュレッダーにかけることが望ましいと考えるが、シュレッダーの購入・配置が困難だとしても、少なくとも鍵のかかるキャビネットにおいて不要な紙類を保管すべきである。

ウ　パスワードの変更の不実施

「介護保険システム管理運用基準及びセキュリティ実施基準」によれば、パスワードはシステム管理者が年に一度以上変更し通知することとされている。しかし、実際には平成１７年３月のシステム導入以来パスワードは変更されていないとのことである。セキュリティ責任者及びシステム管理者のヒアリングにおいてその理由を聞いたところ、変更手続きとしては、セキュリティ責任者である介護保険課長から指定されているシステム管理者が対象者のパスワードを決定し、それを各人のイントラネットのメールアドレスに通知するという方法を取ることになるが、現在対象者が合計で１８８人おり、この全てにつきシステム管理者が行うのは事務手続き上極めて大変とのことであった。また、２０１１年２月か３月にハードがバージョンアップされる時に、個人がそれぞれのパスワードを変更しうるように機能が変更される可能性が高いため、現在はこのバージョンアップの内容等を外部の保守委託先に問い合わせているところとのことであった。

しかし、システム導入以来パスワードが変更されていないという状況は、「介護保険システム管理運用基準及びセキュリティ実施基準」の規定に違反し、業務懈怠の状態にあるのであるから、セキュリティ責任者及びシステム管理者は、かかる状況が情報セキュリティを危うくしていることを危機感をもって認識し、事務手続きの困難を理由にせずに、直ちに各人のパスワードを変更し通知すべきである。ただ、変更手続にかなりの負担を要するのも理解できるところであるため、次回のバージョンアップ時に、各人がパスワードを変更できる機能が追加されるべきであろう。

（５）監査人の意見

ア　キャビネットの鍵の管理の工夫を

介護保険課では、未収台帳をキャビネットの中に置き、キャビネットは施錠し、その鍵は鍵のかかる場所に保管してあるが、当該鍵のかかる場所の鍵は夕

方の職員退出時から、明朝の出勤時までは、一定の職員間で合意された施錠されていない場所に置かれている。介護保険課で扱う情報は守秘性の高い個人情報を多く含んでいることからすると、最終的に施錠がされていない状況は好ましくなく、夜間や祝日はダイヤル式の金庫に入れる等の工夫が望まれる。

6　選挙管理委員会事務局

（1）監査対象部課の業務の内容

選挙管理委員会事務局（以下、「選管事務局」という）は、公正な選挙を行うために設置された選挙管理委員会（独立行政委員会）の職務を補助執行する機関である。その業務は、①選挙管理委員会に関する事務、②選挙執行に関する事務、③選挙人名簿の調整に関する事務、④裁判員及び検察審査会審査員候補者の選定に関する事務等である。

（2）監査の対象システムの概要

名称	選挙人名簿・期日前投票システム
目的	選挙人名簿の管理・運用及び選挙時における期日前（不在者）投票の管理・運用
システムの取扱い業務	同上
導入年度	平成１６年導入。平成２０年度には裁判員制度の施行により、平成２１年度には国民投票制度の施行により改修が加えられ、現在に至る。
登録データ	住所、氏名、性別、生年月日、世帯構成、本籍地、転入日、転入届出日、転出日、転出届出日、転出先、選挙人名簿登録有無、投票人名簿登録有無及び投票情報。 なお、平成２２年９月２日現在の選挙人名簿登録者数は２２０，８９７名。

選挙人名簿・期日前投票システムを用いた事務のフローは別紙８のとおりである。

（3）情報セキュリティ体制

セキュリティ責任者	選管事務局次長
システム担当者	課長が指定する選挙係所属の者１名

システム使用者	【名簿管理システム】 システム担当者メニューはシステム担当者のみ、ユーザーメニューは選管事務局に所属する者全て 【期日前投票システム】 担当者メニューは選管事務局に所属する者、ユーザーメニューは選挙時における期日前投票従事職員及び選挙時における期日前投票委託社員
情報セキュリティ実施基準等	「選挙人名簿・期日前投票システム管理運用基準及びセキュリティ実施基準」（平成２２年６月１日制定） 「選挙人名簿・期日前投票システムの緊急時対応について」
システムの構成	【平常時及び選挙時（事務局内)】 サーバ２台、ＭＯドライブ１台、外部記録装置１台、プリンタ２台 【選挙時（期日前投票所)】 上記システムに加えて、クライアントＰＣ１１台、プリンタ７台
盗難防止他	【情報セキュリティ関連文書の内容に及ぶため省略】
バックアップ体制	バックアップサーバに自動的に記録
外部との接触	ホストシステム上の住民記録データ上を定期的に電磁的記録媒体によって取り込む
障害時対応	「選挙人名簿・期日前投票システムの緊急時対応について」

過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	平成１９年度に実施され、以下の指摘がなされている。 １．「情報セキュリティに関する規定（ママ）やマニュアルについて、周知度が低かった。また、システム操作時の基本的な注意事項について、一部、理解の不足している状況が見受けられた。」との選管事務局の「セルフチェック」の結果報告を受けて、「課における話し合いでは、セキュリティ対策面で理解度の低い項目（緊急対応における手順の確認）などにテーマを絞ったほうが効果的ではないかとの助言を行った。また、セキュリティに関する研修や話し合いは、これを機会に継続し、選挙の無い閑散期を選んで毎年実施してほしい旨要望した。」との助言及び要望がなされた。 ２．開票管理システムにつき、「データ保存する電磁手記録媒体をより安全性の高いものへの変更を検討されるよう要請」された。 ＜改善状況＞ １．につき、選管事務局から情報セキュリティに関する確認会を平成２０年２月１５日に実施した旨の報告があった。また、「今後も継続的に確認会を実施していくことを全職員に周知した。なお、内容についてはテーマを絞って実施することとした。」との報告がなされたが、かかる継続的な確認会は行われていない（後記（４）エ参照）。 ２．につき、選管事務局から平成２０年４月からデータ保存媒体を変更予定である旨の報告がなされたが、その後、変更はもとより、保存媒体の変更についての検討も行われていない（後記（４）オ参照）。

（４）指摘事項

ア　不適切なパスワード管理

ＩＤ及びパスワード管理に関連する規定によれば、本件システムを運用するために必要なパスワードは、論理上、５種類が考えられる。そして、「選挙人名簿・期日前投票システム管理運用基準及びセキュリティ実施基準」（以下「選挙システムセキュリティ実施基準」という。）上、パスワードは１年に１度以上変更するものとされている。

しかしながら、ヒアリングの結果、次の事実が確認された。

①　パスワードが起動用のものを除き、全て同一であること

パスワードは、起動用を除いて、全て同一である。

すなわち、パスワードは、システム管理者用パスワードを除き、ライアント機及びシステム起動時を含めて、全て同一である。なお、これを同一にしなければならない理由はない。

② 目黒区職員のみならず、派遣社員もそのパスワードを知っていること

クライアント起動のパスワードは、目黒区職員のみならず、派遣会社からの派遣社員も行っている。

期日前投票においては、目黒区の応援として派遣された職員のみでなく、派遣会社の派遣社員もまた、投票所の業務に従事している。そして、かかる派遣社員に対して、投票期間前の研修の際に、パスワードを教授している（この点、起動は選管事務局が行うものとする選挙システムセキュリティ実施基準の関連規定に違反している。）。

③ 本件システムの導入後、パスワードが一度も変更されていないこと

このようなパスワードは、本件システムの導入後、１回も変更されたことがない。

これは、前記の選挙システムセキュリティ実施基準に明らかに違反する運用である[19]。

なお、ヒアリングに先立つ質問票に対しては、選管事務局は定期的に変更している旨を、事務局次長は定期的に変更するよう指示している旨を回答してきた。しかしながら、ヒアリングにおいて、監査人補助者の指摘を受けて回答者自らが右回答が誤りであることを認めるという、極めて遺憾な監査経緯があったことを指摘する。

平成１６年の本件システム運用時から継続されてきた上記の運用は、セキュリティ実施基準に違反するというばかりでなく、実質的にも極めて危険であると言わざるを得ない。

すなわち、投票所は、期日前投票で６箇所、投票日で３８箇所存在し、各投票所において、本件システムの起動に関わる可能性がある者は３名以上存在する。これらは、上記のとおり、目黒区の他部署からの応援や、派遣会社の職員であって、入れ替わりがあるものである。選挙は年に数回あるのが通常であるから、平成１６年以降で見ても、累計で数百名が本件システムの起動に関わっていると合理的に推定することができる。

しかしながら、平成１６年の本件システム運用開始から一度もパスワードは

[19] 総務省ガイドラインにおいても、パスワードが定期的に変更されているか否かについては、必須監査項目とされている（別紙１参照）。

変更されておらず、また、新規に選挙事務に関わる区職員及び派遣社員に対しては、事前研修の場においてパスワードを教授しているというのであるから、累計で同様に数百名が本件システムの起動パスワードを知っているということになる。

このような、いわば「公開されたパスワード」は、もはやセキュリティ対策としてのパスワードとしての機能を喪失し、システム立上げプロセスのための一手間にしか過ぎない状態になっていると言える。

パスワードが同一のものがあり、しかもそれが平成１６年以来一度も変更されておらず、目黒区職員外の者を含む累計数百名がそれを知っていることについてのリスクは、もはや具体的に例示する必要もない。

選挙システムセキュリティ実施基準に従って定期的な変更を行うとともに、選挙ごとに（できれば、さらに投票所ごとに）異なるパスワードを設定するなど、適切な対処を早急に取る必要がある（なお、選管事務局より、平成２２年１２月１０日、全てのパスワードを変更し、以後セキュリティポリシーどおりにパスワード管理を行う旨の報告があった。）。

なお、平成１９年度の情報セキュリティ内部監査においては、このようなパスワードの不適切な管理状況は指摘されておらず、むしろ、全体としてセキュリティ管理が問題なく進められているとの講評が付されているほどであり、現在の内部監査体制及び方法による内部監査の限界を露呈していると言える。

イ　不適切なサーバ管理

選管事務局においては、現状、鍵付きの小型ラックにメインサーバ及びバックアップサーバの双方を収納している。

往査において、次の事実及び問題点が認められた。

①　不適切なバックアップサーバ収納場所

バックアップサーバをメインサーバとともに同じラックに収納しているのであるから、災害時（とくに火災時）の物理的環境もまた同じとなる。したがって、災害時には、両サーバにともに、データ喪失を含む障害が生じてしまう可能性がある。さらには、選挙人名簿（紙媒体）は、両サーバに近い耐火性のないロッカーに収納されているため、火災の際には、両サーバとともに消失されるおそれがあり、その場合には、目黒区の選挙人名簿作成・保管事務のみならず、選挙という民主主義の根幹をなす制度の遂行に極めて重大な支障が生じること必至である。

情報処理機器及び電磁的記録媒体の取付けを行う場合には、火災、水害、ほこり、振動、温度及び湿度等の影響を考慮しなければならないとされてお

り[20]、また、セキュリティ責任者は、必要に応じて電子データのバックアップ処理を行うとともに、特に重要なものに関しては、区以外の施設において保管及び管理をする等の措置を行うものとされている。

したがって、バックアップサーバは遠隔地に置く等して、サーバとバックアップサーバは別の場所に分けて格納すべきである。

② 熱対策の不徹底

サーバが格納してあるサーバラックは、ファンが付いているものの、スリット等の開口箇所が少なく、必ずしも熱対策に優れたものでないと認められる。実際、往査時、ラックの扉が開かれ、２台のサーバに扇風機の風が当てられている状態であった。

メインサーバとバックアップサーバが隣り合って設置している状況で、双方に熱による障害が発生したときは、目黒区の選挙人名簿作成事務に支障が生じるおそれがある。そして、前記のとおり情報処理機器及び電磁的記録媒体の取付けを行う場合には、温度及び湿度等の影響を考慮しなければならないとされているところである。

メインサーバとバックアップサーバは、分けて格納するほか、熱対策を十分に施した設備・方法によって設置をすることが必要である。

③ 不適切な施錠管理

上記のとおり往査時、サーバに扇風機の風をあてる等、熱対策のために、サーバのラックに鍵がかけられず、扉が開いていることが確認された。

これは、サーバを施錠格納し、システム担当者以外の者が開閉できないようにすべきとする選挙システムセキュリティ実施基準に抵触するおそれがある。システム担当者は、施錠は執務時間外になされればよいと限定解釈して運用しているが、鍵のかけ忘れというヒューマンエラーの発生可能性に加えて、選管事務局における杜撰なパスワード管理の結果、多数の者がシステムを立ち上げ、選挙人名簿を閲覧し、プリントアウトすることが事実上可能な状態になっていることを併せ考えると、選挙人名簿の流出可能性に対する配慮に欠ける運用と言える。

サーバの物理的な格納方法について早急に検討して実施するとともに、サーバ収納庫に対する几帳面な鍵の開け閉めと鍵自体の管理を徹底されたい。

ウ 選挙人名簿及び選挙人名簿にかかるデータの不適切な管理

[20] 総務省ガイドラインにおいても、「サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置」されているか否かの点は必須監査項目とされている（別紙１参照）。

上記イで述べたとおり、現在、選挙人名簿は紙媒体で耐火性のないロッカーに置かれ、選挙人名簿にかかるデータは同一のラックに格納されたメインサーバ及びバックアップサーバに記録されているのみであり、その他の方法では選挙人名簿にかかるデータは保管されていない。

ところで、選挙人名簿の登録は、３月、６月、９月及び１２月の年４回、各々２日に行われ、各月１日現在で引き続き３ケ月以上その区市町村の住民基本台帳に記録されている人が登録される。したがって、選挙人名簿は、特定の単一の日の住民基本台帳上の記録からでは作成できないのであって、選管事務局が、火災等の災害によって一度サーバ内の選挙人名簿にかかるデータ及び紙媒体での選挙人名簿をともに失ったときは、その後３ケ月以内の選挙の実施に重大な支障を及ぼすことになる。

よって、①選挙人名簿を耐火性のある収納庫に保管する、②バックアップサーバの保管場所を遠隔地に変更する、又は③定期的に選挙人名簿データのバックアップを電磁的記録媒体等に記録し、当該記憶媒体を他所にて保管する、といった適切な情報保護対策を取ることが必要である[21]。

エ　情報セキュリティ研修を継続的に行うべきとする過去の内部監査における指摘に対する不適切な対応

選管事務局は、平成１９年度情報セキュリティ内部監査において、セキュリティに関する研修を毎年継続的に行うべきとの指摘ないし意見を受けた。そして、選管事務局では、それに対して、情報セキュリティに関する「確認会」を行ったほか、以後も継続的に確認会を実施する旨を回答した。

しかし、「確認会」は平成２０年２月１５日に１回だけ行われたのみで、それ以降は全く行われておらず、その具体的な予定もない。

上記ア及びイで指摘した事実関係に鑑みれば、選管事務局は、今回外部監査の対象となった他の部署に比べて情報セキュリティに対する意識が著しく低いと言わざるを得ず、それゆえに、情報セキュリティに関する研修の機会を継続的に設けるべきとの内部監査における指摘ないし意見は正当である。しかし、選管事務局が、それに対して真摯に向かう意識があったのか甚だ疑問である（また、上記のとおり包括外部監査人の質問票に対しても事実に反する回答を行ってきたことに鑑みれば、自己の回答に対する責任感が欠けているのではないかとの印象を否定できない。）。

今回の外部監査を契機に、情報セキュリティ対策とその意識の徹底をはかる

[21] 情報セキュリティ対策基準には、必要に応じて電子データのバックアップ処理を行い、特に重要なものは区以外の施設において保管及び管理をすべきとの関連規定があるほか、情報化推進計画の施策８－１－２でも区の情報システムが扱うデータの重要度や業務の種類を考慮した外部データセンターの活用を図るとされている。既述のとおり、選挙人名簿にかかる情報が特に重要なものであることには疑いはない。

ことが求められる。

オ　電子記録の保管方法に関する過去の内部監査における指摘に対する不適切な対応

平成１９年度情報セキュリティ内部監査においては、開票管理システム（監査対象として明記したシステムではないが、情報管理一般の問題として取り上げる。）にかかるデータ保存の方法について、データ破損が生じ易い電磁的記録媒体ではなく、より安全性の高いものへの変更を検討されるよう要請された。これに対し、選管事務局は、平成２０年４月から変更予定と回答した。

しかし、現在に至るも、データ保存は従来どおりの媒体で行っている。媒体の変更が不可能ということでもなく、それが実現できないことについて検討されたこともない。

この点も、内部監査における指摘に対して真摯に向かう意識があったのか（また、自己の回答に対する責任感が欠けているのではないかとの）疑問を抱かせるものであり、早急に、保存媒体の変更について検討を進めるべきである。

7　生活福祉課

（１）監査対象部課の業務の内容

生活福祉課は、社会福祉法に定める「福祉に関する事務所」の所掌事務のうち、生活保護法が定める援護に関する事務を行う実施機関である。

生活福祉課は、健康福祉部内の課であり、課長以下、管理係、相談援護係、保護第一係、保護第二係及び保護第三係で構成されている。

その具体的な事務は、生活保護法に基づく事務のほか、低所得者や路上生活者に対する相談や支援、「中国残留法人等の円滑な帰国の促進及び永住帰国後の自立の支援に関する法律」に基づく支援給付、行旅病人及び行旅死亡人取扱法、及び墓地埋葬法に基づく事務等を行っている。

（２）監査の対象システムの概要

名称	生活保護システム
目的	生活保護にかかる保護の決定、医療扶助事務及び経理事務を効果的・効率的に処理する。
システムの取扱い業務	相談管理、ケース管理、医療管理及び経理管理等
導入年度	平成１２年に導入、その後平成１７年及び平成２２年に更新し、現在に至る。
登録データ	住所、氏名、性別、生年月日、世帯構成、本籍地、収入の状

	況等。なお、平成２２年８月平均の対象者は、生活保護被保護者２，５２１人、被保護世帯２，１１８世帯。

生活保護システムを用いた事務のフローは別紙９のとおりである。

（３）情報セキュリティ体制

セキュリティ責任者	生活福祉課長
システム担当者	課長が指定する者３名
システム使用者	相談管理メニュー　相談援護係に属する者 ケース管理共通メニュー　保護係に属する者 統計・医療・介護・経理管理メニュー　管理係に属する者 システム管理・継続メニュー　指定されたシステム担当者
情報セキュリティ実施基準等	「生活保護システム管理運用基準およびセキュリティ実施基準」（平成１８年３月３１日制定） 「生活保護システム障害時対応マニュアル」（同日制定）
システムの構成	ドメイン／ＡＰサーバ１台、ＡＰサーバ２台、クライアントＰＣ４３台、プリンタ１１台
盗難防止他	サーバ機、クライアント機は保管場所を施錠する。 サーバルーム及びサーバ保管庫は施錠し、鍵の管理はシステム担当者が行う。
バックアップ体制	定期的にバックアップを実行。
外部との接触	なし
障害時対応	「生活保護システム障害時対応マニュアル」（同日施行）
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	平成１８年度に実施され、以下の指摘がなされている。 １．情報セキュリティに関する規程の理解や研修への参加が不十分であった。 ２．新聞や牛乳等の業者が、執務時間外や昼休みなど監視が行き届かない時間帯に事務室内に入ってくるところがあった。 ３．事務スペースの狭隘により、良好なセキュリティ確保が困難な所属があった。 ４．調査等の外出の際に、対象区民の生活保護記録等の持ち出しが行われているが、個人情報の持出しに関してルールがなく管理されていない。 ５．生活保護システムのサーバ室が、他の用途の部屋と兼用になっており、サーバの鍵が同じ部屋にある。

	６．事務スペースの一部の入り口は、外部の者が容易に入室可能であり、また死角になったキャビネットの書類等を持ち出すことも可能な状態にある。 ＜改善状況＞ １．につき、その後、課内研修会を開催するとともに、継続的に係長会において個人情報管理体制の具体化について検討している。 ２．及び３．につき、レイアウトの変更により改善済み。 ４．につき、「持出し管理簿」を作成することとしたが、その運用上の問題点について後記（５），アを参照。 ５．につき、平成１８年１２月１５日に鍵をサーバ室とは別の部屋で管理することとした旨の回答がなされたが、それが徹底されていなかった（後記（４），ウを参照)。
設置場所	生活福祉課は、廊下を挟んで管理係・相談援護係スペースと保護係スペースに分かれているため、当該システムも２か所に設置されている。 管理係・相談援護係スペースは、専用フロアとなっており、休日・夜間は、窓口シャッターを閉じ、出入口は施錠管理している。保護係スペースは、他課との共用フロアにあり、休日・夜間は、窓口シャッターを閉じ、出入口は施錠管理している。

（４）指摘事項

ア　不適切な文書ファイル保管

生活保護受給者に関するファイル（ケースファイル）の管理方法について、従前より、生活福祉課においては、それを扱う保護係の職員が帰庁時に、各自が使用したファイルを専用の鍵付キャビネットに収納し、全て施錠するものとの運用方針を有していた。

しかし、往査時において、かかる運用は全く行われておらず、ケースファイルのキャビネットが施錠されることは日常的にはないことが確認された。

たしかにキャビネットは極めて多数に上るうえ、目黒区役所の出入口のみならず生活福祉課の執務場所も、執務時間後にシャッターが閉じられていることから、毎日の鍵の開閉を厭う現場の意向も理解できなくもない。

しかし、当該執務場所は保護係以外の者を含む多数の職員で共同して使用するものであること及びケースファイル記載の情報は、生活保護受給者に関する極めて高度な個人情報であることに鑑みれば、保有個人情報の漏洩、滅失、改ざん、き損その他の事故を防止するために必要な措置を講じなければならないとする個人情報保護条例第１０条第１項第２号に従い、生活福祉課のそもそも

の運用方針どおりに、ケースファイルは執務終了時には施錠管理するのが相当である。

なお、往査時にこの事実が生活福祉課長にも認識されたところ、平成２２年１２月１０日、生活福祉課より、ファイリングキャビネットについて、退庁時に鍵をかけるよう各係に周知徹底し、これを毎日確認することとした旨の報告があった。

イ　不要な紙類についての不十分な管理

現在、生活福祉課では、個人情報が記載されたメモや印刷物等の文書で不要なものが出ると、課内の所々に置かれたダンボール箱に随時入れていき、それを１か月ごとにまとめて文書庫に運ぶという方法で廃棄している（総務課ではそれを溶解処理により廃棄している。）。このダンボール箱は、大きく上部の口を開いたうえ、判別可能なように目印を付けているものである。

廃棄文書についてこのような処理をしているため、文書は、かかるダンボール箱の中で、最長１か月間放置されることになる。

しかし、廃棄文書は、誰にも管理されないものであるため、それが紛失しても誰も気付かないという問題がある。溶解処理をするという前提でダンボール箱に入れられるものであるため、要保護性が高い情報が記載されたものであっても同じである。

よって、個人情報保護条例第１０条第１項第２号に従い、例えば、取出し困難なポスト型の専用箱を設置するなど、さらに適切な個人情報保護対策を取る必要がある。

ウ　サーバ保管庫についての不適切な管理

サーバ室の往査において、サーバは鍵のかかるラックに保管されているが、その鍵がラックの上部に置かれる運用であることが確認された。そして、生活福祉課では、このような運用をしなければいけない必然性はないとのことであった。

かかる運用は、サーバ保管庫を施錠すべしとする生活保護システム管理運用基準およびセキュリティ実施基準に実質的に抵触するものと思われる。

よって、サーバ保管庫の鍵は、より適切な場所に保管すべきである。

なお、往査時に包括外部監査人補助者がこの旨の見解を述べたところ、その日から改善するとの回答があり、その後のヒアリングにおいて、改善が認められた。

エ　個人情報関連文書の持ち出しに関する管理の不徹底

各ケースワーカーは、「訪問計画表」と題する文書に各自の訪問計画を記載したうえで戸別訪問を行っている。この訪問計画表には、各ケースの氏名、住

所、電話番号、家賃等についての情報が集約されており、個人情報の管理上、極めて重要なものである。戸別訪問の業務を遂行するためには、全ケースワーカーがこれを携行する必要性は認められる。

しかし、訪問計画表の記載内容が上記のような生の情報を集約しているものであるため、万が一紛失したときの影響は極めて大きい。実際に、住民基本台帳法に基づく居住実態調査中に、個人情報が記載された書面が紛失するという事故が西部地区サービス事務所において発生している現状から見ると、その管理方法について、見直す必要がある。

例えば、訪問計画表上は、氏名と住所について記号・番号で表し、氏名等との対照表を作成して、別の場所（例えば、訪問計画表が鞄の中であれば、対照表は衣服の内ポケット等別の場所）に入れて携行するといった対応も考えられるところである。このような処理をするのに、システムを変更する必要もなく、持出用の書類だけ、プリントアウトした書類を分割（裁断）し、記号番号を付記するなどの工夫で十分可能ではないかと考えられる。

（５）監査人の意見

ア　ケースファイル持出管理についてさらに検討を

書類の持出しに関しては、平成１８年度情報セキュリティ内部監査において、調査等の外出の際に生活保護記録等の持ち出しが行われており、個人情報の持ち出しに関してルールがなく管理されていないことが指摘され、個人情報持ち出し管理簿・台帳への記入等の対策を採ることが要請されたこと受けて、その受戻しについての記録として、持出し管理簿が作成されている。この持出し管理簿は、各保護係の分が一括してキャビネットに置かれている。

しかし、平成２２年１０月２７日の往査時に、次の事実及び問題点を認めた。

①　訪問計画表についての持出し記録が不十分であること

訪問計画表については、ケースワーカー全員分について、毎年１回、４月時点での記録について、持出しを許可する旨の記録を作成するだけとなっている。そして、４月以降に追加訂正されたケースにかかる記載は、手書きにより訪問計画表に記載される運用であった。

したがって、４月以降の情報の更新分については手続を欠くものであると言える。

②　記載不備

その他のケースファイル中の記録については、同日の往査時点において２件のみ持ち出した旨の記録があったが、持出時の係長の決裁印もなく、日数がかなり経過した記録であったにもかかわらず、返却された旨の記載もなかった。

これらからして、平成１８年度情報セキュリティ内部監査の指摘を受けて造

られた現在の制度が正しく機能しているとは認められなかった。

ケースファイル中の記録について、必ず係長の許可を得て持ち出し、返却する運用なのであれば、係長が持出し管理簿を保管し、その場で記録を作成する方が実効性があるはずであるし、訪問計画表に関する持出し管理簿の作成頻度を上げることも可能なはずである。また、持出しに関する明文の規則を作成するのが望ましい。

イ　点検中レセプトの管理方法について検討を

生活保護受給者が病院・診療所において診察を受けると、病院・診療所から診療報酬請求書（レセプト）が生活福祉課に届き、管理係において診療代支払の事務を行うこととなる。

かかるレセプトの点検業務は、業務委託契約に基づき、専用のレセプト点検室にて、委託業者が月に数日間行い処理している。同点検室は、生活福祉課の執務場所の一角をパーテーションで区切って設置されたものであり、２つの出入口の１つは鍵があり、もう１つは更にパーテーションで区切られた打合せスペースと繋がり、そのスペースと生活福祉課の執務場所の間の出入口は施錠可能となっている。これらの２つの鍵は、日中は施錠されていない。

そして、点検中のレセプトは、レセプト点検室内の机や床のダンボール箱の中に置かれている。したがって、点検中のレセプトは、日中鍵がかからないレセプト点検室に、点検が完了するまでの期間、継続して、施錠管理されずに置かれているという状態である。

しかし、レセプト点検は毎日の業務ではないため、直ちに紛失に気付かないおそれがある。そして、紛失したときに、生活福祉課が責任を負うべきか、受託業者が責任を負うべきかという、責任の所在も不明確となっている。

設置スペースの問題があるようではあるが、個人情報保護条例第１０条第１項第２号に従って、レセプト点検室に点検中のレセプトを保管する専用鍵付きロッカーを置く等、さらに安全な情報管理対策について検討されたい。

８　子育て支援課

（１）監査対象部課の業務の内容

子育て支援課は、奨学資金貸付や私立幼稚園補助に係る子育て支援業務、児童館や学童保育に係る児童館運営業務、子どもに関連する各種手当・医療費助成業務を所掌している。また、平成２２年４月から施行されている「子ども手当法」に基づく子ども手当の支給事務も同課が所掌している。

（２）監査の対象システムの概要

監査団は、子育て支援課の手当・医療係の所管する「児童扶養手当システム」

を対象として監査を行った。同システムの概要は以下のとおり、同システムを利用した業務フローは別紙１０のとおりである。

名称	児童扶養手当システム
目的	児童扶養手当の受給資格者情報の管理及び関連事務の処理をコンピュータシステムで扱うことにより省力化を図る
システムの取扱い業務	①児童扶養手当の受給資格管理・照会、②現況届処理、証書・各種一覧・通知作成、③支給、支給明細、各種一覧作成
導入年度	平成１３年度（本稼動は平成１４年８月）

（３）情報セキュリティ体制

児童扶養手当システムの情報セキュリティ体制の概要は以下のとおりである。

登録データ	受給資格者に関する情報、支給実績等
セキュリティ責任者	子育て支援課長
システム担当者	課長の指定する手当・医療係の職員
システム使用者	手当・医療係の担当職員４名（入力処理権限あり）、その他１２名（閲覧権限のみ）
セキュリティ実施基準等	「児童扶養手当個別システムセキュリティ管理規程」（平成１６年１１月制定）
システムの構成	パソコン１台、プリンタ１台
バックアップ体制	データ： 定期的に電磁的記録媒体にバックアップを作成。このほか、バックアップデータを外部施設で保管している
外部との接触	ホストシステム上の住民記録データとの確認を紙媒体で行っている。このほか、定期的に、税務データと住民記録データの突合を電磁的記録媒体により行っている。税の年度が変わる時期には新年度の税務データが一括して更新される。 金融機関に対する手当の支払い指示は電磁的記録媒体により行う
障害時対応	システムセキュリティ管理規程により規定
過去の情報セキュリティ内部監査の実施状況、その際の指摘事項	平成１８年度に実施。個人情報を含む紙文書の発生が多いため、個人情報を含む文書等の保管・施錠管理に工夫が必要との指摘あり

（４）指摘事項

ア　パスワードの更新に関するセキュリティ実施手順の不備、定期的なパスワード更新の不徹底

児童扶養手当システムにおいては、各職員にそれぞれの利用権限に応じた２種類のパスワードを付与している。しかし、ヒアリングによれば、これらのパスワードは数年に１度変更されるのみであるという。また、「児童扶養手当個別システムセキュリティ管理規程」には、システムへのアクセスのために必要なパスワードについて、変更頻度などの手順が定められていない。目黒区では、この点について、権限を有しない職員がアクセスできないように、実施手順等において必要事項を定めたうえ、設定を行うべきこととされている。

ついては、「児童扶養手当個別システムセキュリティ管理規程」や実施手順を見直した上で、最低でも年に一度のパスワードの変更を規定すると同時に、その時期や方法についても定めを置き、運用上もパスワード管理の徹底を行う必要がある。

（５）意見

ア　書類の保管方法の改善を

子育て支援課手当・医療係では、上記のとおり児童扶養手当のほか、医療費助成、子ども手当その他の手当の給付に係る業務を所掌しているところ、法改正に伴う事務量の増加に伴い、課内で保管する文書量も増加している。他方で、同課の利用するスペースには限りがあり、子ども手当関連の事務処理には庁内の別室を一時的にあてがう、隣接する別の課のスペースの一部を譲り受けるなどの対応が行われている。そのため、保管すべき書類が課内の複数のキャビネットに分散して保管されているほか、課内のスペースは数多くのファイルや備品等で雑然としている。子ども手当導入等のような法改正が行われた場合に、係外を含めて複数の場所に分散して保管せざるを得ない場合があることは理解できるものの、このような状態では、個人情報の含まれる書類の管理不徹底なども懸念される。

この点に関しては、日々の業務で参照頻度がそれほど高くない文書は庁舎地下の書庫において保管し、特に紙媒体としての保管が求められていない文書については電子データによる保管に切り替えるなど、限られたスペースを有効に利用するための工夫が行われることが望ましい。

イ　システム間の登録データの互換性確保によるシステム利用の効率化を

児童扶養手当の受給資格者は、育成手当、ひとり親家庭等医療費助成等の受給対象と重なる場合が多い。もっとも、児童扶養手当システムがスタンドアロンのパソコンにより単独で管理運用されているのに対し、育成手当及びひとり親家庭等医療費助成についてはホストシステム上のシステムを利用した管理運用が行われている。ヒアリングによれば、児童扶養手当とこれら２事業については、業務上相互に参照する必要性が比較的高いものの、児童扶養手当のデ

ータ形式が異なるため、ホストシステム上へのデータ反映は手動入力での対応とならざるを得ない状態にあるという。手動入力の頻度が増えれば、それだけ人的ミスの介在が懸念されるところである。したがって、システム利用の効率化という観点から、情報を相互に利用する複数のシステム間でデータの互換性を向上させる（たとえば、MO等による相互のデータのやり取りを可能にする）などの効率化を、コストの点にも留意しつつ検討していくことが望まれる。

ウ　職員別のパスワードの付与を

上記（４）で述べたとおり、児童扶養手当システムでは、システムにアクセスするためのパスワードとして権限に応じた２種類のパスワードが担当職員に付与されているが、職員別のパスワード付与は行っていない。このような運用を前提とすると、仮に同システム上、不正処理（データの誤入力修正、消滅取消等の職権処理）が行われたとしても、アクセスログから当該不正が行われた者を特定することができないという問題がある。コスト負担の観点から可能であれば、各担当職員別にそれぞれの権限に応じた個別パスワードを付与することが望ましい。

9　情報課

（１）監査対象部の情報セキュリティ関連業務の内容

情報課の情報セキュリティ関連業務については、電子情報処理規則、情報セキュリティ基本方針等に規定されている。これらの規程によれば情報課は、ホストシステムの電子情報のセキュリティ対策を専属して担当するほかに、①情報システムの管理者としての業務（「（４）目黒区電子情報処理規則」の記載箇所を参照）、②内部監査に関する庶務の業務（「（６）内部監査と目黒区情報セキュリティ監査実施要綱」の記載箇所を参照）等を担っている。

①　情報システムの管理者としての業務

情報システム管理者の主な業務内容には、情報資産に対する脅威が発生した場合又は脅威のおそれがある場合において必要な措置を行うこと、セキュリティ責任者に対して情報セキュリティ対策に関する助言、指導及び調査等を行うこと、セキュリティ責任者と連携して情報セキュリティ関係規定等に沿った情報セキュリティ対策の状況について職員に自己点検を行わせること等が含まれる

各部に置かれている個別システムは各部がその責任を負うが、情報課は情報に係る専門性を有していることより、情報システム管理者としてセキュリティ責任者（各課長）に助言、指導及び調査等を行うことが求められている。つまり、セキュリティ責任者の業務が情報資産を適切に管理するために物理

的セキュリティ、人的セキュリティ、技術的セキュリティの各項目について対処すること、自己点検を実施すること等のため、情報課が実施する助言等の内容もこれらのセキュリティ責任者の業務に対する助言、指導及び調査等を行うことになる。例えば、情報課が助言等のなかで実施している情報セキュリティについての研修は、人的セキュリティを通じて、自己点検は職員が実施する情報システムの適正な評価を通じて、情報セキュリティ対策の強化を図ることになる。

情報課は、このような助言等を情報システムの管理者の業務として実施している。

② 内部監査に関する庶務の業務

情報セキュリティの内部監査は、情報システム統括責任者が行うことになっているが、内部監査に関する庶務は情報課の責任とされている。したがって、実効性のある内部監査の実現は、内部監査に関する情報課の庶務の実施内容により、具体的には企画経営部情報課がどのような監査計画、監査実施計画、報告等を行うかにかかっている。

情報課は、このように情報セキュリティ対策の強化の一環として内部監査に係る庶務業務を担当している。

（2）指摘事項

ア 情報セキュリティ研修の不十分な管理

情報セキュリティ対策基準においては、情報セキュリティの研修を「人的セキュリティ」と位置付け、情報統括システム責任者により情報セキュリティ関連規定等の周知及び情報セキュリティ対策の重要性についての啓発、情報セキュリティに関する研修の実施が行われること、またセキュリティ責任者により研修が実施されることが規定されている。

そこで、情報セキュリティ研修の受講状況を確認したところ以下の【情報セキュリティ研修の受講状況】のような状況であった。

【情報セキュリティ研修の受講状況】

平成２２年度	職員数（人）	うち管理職（人）
４月１日現在職員数	２，２１４	８２
講義形式研修受講者数	２６５	５２
E－ラーニング受講者数	７５	1
イントラネット及び内部情報システム操作研修（セキュリ	７６	－

ティを含む)		
受講者数計	４１６	５３

情報課へのヒアリングの結果、以下の情報セキュリティ研修参加状況の管理と研修受講履歴管理が不十分なことが認められた。すなわち、各課では、研修に参加したセキュリティ責任者等が各課に戻って課内研修を行うなどが行われているが、現状の職員数に対する受講者数（受講者数÷職員数で計算した受講率は１８．８%)、管理職の受講者数（受講率６４．６%）は、研修への受講結果としては満足できるものではない。また、人的セキュリティが機能する前提は、情報セキュリティの上で必要となる知識、技能、態度等を十分に認識し、習得しているという一定の質を維持していることである。研修はそのための方法であるにもかかわらず、研修受講履歴を管理する等の仕組みは考えられておらず、質の把握ができていない。

研修を通じた人的セキュリティの機能や質を維持していくために情報システム統括責任者及び情報システム管理者は研修参加状況の管理、研修参加者の受講履歴管理等を行うことが必要である。

イ　情報セキュリティ内部監査の実施方法の欠陥

情報セキュリティ監査の責任者は企画経営部長であるが、企画経営部長の下で情報課が監査業務の庶務を担い、監査人に対して情報セキュリティ内部監査の手順等の説明を行っている。しかし、監査説明資料やヒアリング等によれば、情報セキュリティ内部監査における監査の質疑応答は約３０分程度で、質問事項はあらかじめ事務局（情報課）が作成した質問項目を参考に監査人が取捨選択すること、質問項目についてはまだ見直しは行われていないが、その理由は監査対象がまだ一巡していないからとのことであった。

情報セキュリティの内部監査は、情報セキュリティ監査実施要綱の目的で記載のとおり「区の情報セキュリティの維持・向上を図ることを目的とする。」ことにあるが、現状の内部監査では監査目的で記載している区の情報セキュリティの維持・向上を図ることは困難である。

情報課へのヒアリングの結果、以下の問題点が認められた。

①　内部監査時でのヒアリング項目の適時かつ適切な見直しが必要

内部監査の目的を達成するためには、内部監査におけるヒアリング項目を最近生じた情報セキュリティの事件や内部監査結果により、適時にかつ適切に追加や修正することが必要である。それは、内部監査を実施した結果で指摘すべき問題事項がある場合は、その問題の性質により速やかにヒアリング

項目に追加する、情報セキュリティの事故が発生した場合には、当該発生した項目をヒアリング項目とするなどヒアリング項目の見直しを随時に行うことを意味している。

情報課が主張している監査が一巡するまで内部監査時でのヒアリング項目の更新をしないことは、当該目的を達成できないことになり問題である。

② 最低限実施すべきヒアリング項目を定めることが必要

監査では、監査結果の質を維持するためや監査意見を取りまとめるために、必ず検討や確認しなければならない項目があるのが通常である。セキュリティ内部監査という監査においても同様である。しかし、現状の内部監査の実施方法は、ヒアリング項目の選択を監査人に一任している。このような実施方法では情報セキュリティの維持・向上を図ることは困難である。

内部監査時に必ず検討や確認しなければならないヒアリング項目を、総務省ガイドラインの必須監査事項１１０項目も参照して定めることにより、現状よりも充実させることが必要である。

ウ 情報セキュリティの内部監査計画の欠陥

内部監査の過去の実施状況に関するヒアリング等によれば、情報セキュリティ内部監査は平成１７年度以降に実施されているところ、平成１７年度にはホスト系システムのみが監査対象とされ、前年に実施された外部監査を受けて内部統制としての監視（点検・改善指導を行う）体制、良好な情報セキュリティの維持が確認され、翌平成１８年度以降はそれ以外の各所属が保有する個別システムを監査対象とし、情報セキュリティ規程類の遵守状況や個人情報の管理状況等について確認がなされたとのことであった。

このような情報課の説明より、以下の問題点が認められた。すなわち、平成１７年に実施された内部監査では、ホスト系システムが優先されたため、同年に内部監査の対象となった国保年金課が保有していた個別システムである国保収納推進員システムについては、数年をかけて順次各課の保有するシステムを内部監査の対象にするという内部監査計画（以下、「ローテーション監査」という）と相まって、内部監査がいまだに行われていない。このような内部監査の対象からの「漏れ」が生じていることは、内部監査の計画自体に問題があったことを示している。

また、ローテーション監査を前提とする場合には、長期にわたり内部監査が行われないシステムが必然的に生じるため、その隙間を補う制度を整備しておくことが必要となる。この点、目黒区では、内部監査を補完する制度として「自主点検」という制度を設けている。ローテーション監査においては、内部監査を補完する自主点検が内部監査と一体となり車の両輪の如く機能することで、

初めて情報セキュリティの維持・向上を期待できるものである。しかし、目黒区においては、下記１０（１）ウで指摘しているとおり、この自主点検制度は機能が十分に果たされていない状況であって、かかる不完全な自主点検制度のもとでのローテーション監査は、この点においても、その制度設計ないし監査計画自体に欠陥があるといわざるを得ない。したがって、自主点検の実施については下記１０（１）ウで指摘している点を検討し、適切な見直しを行うとともに、内部監査計画については、早急な見直しを実行すべきである。その見直しの内容としては、内部監査の対象となっていない個別システムの洗上げ及び速やかな内部監査の実施が必須である。また、内部監査についても下記１０（１）エに指摘した問題について対処すべきである。

エ　「個別システム共通基準」及び「標準個別システム管理運用基準」の未改定

情報セキュリティ基本方針及び情報セキュリティ対策基準は平成２２年７月３０日付けで改定されているが、これに関連する「個別システム共通基準」及び個別システム管理運用基準の作成例である「標準個別システム管理運用基準」については、いまだ対応する改定がなされていない。このうち、「標準個別システム管理運用基準及びセキュリティ実施基準」の改定については、企画経営部長（情報システム統括責任者）から作成例を後日通知する旨が各課長（セキュリティ責任者）宛てに通知されているが、情報課へのヒアリングによれば、この改定は平成２２年度中を目処に行うことを予定しているという。また、個別システムを所有するいずれの所管課においても、「個別システム管理運用基準」や「セキュリティ実施手順」等の見直しは行われていないという。

平成２２年度の情報セキュリティ基本方針及び情報セキュリティ対策基準の改定は、情報資産のリスク分類など新たに加えられた内容が多く、各個別システムの所管課においても、早急に個別システムごとの管理運用基準やセキュリティ実施手順を見直す必要が生じていると考えられる（情報セキュリティ基本方針１２）。また、これら管理運用基準やセキュリティ実施手順の改定には、情報セキュリティに関する一定の専門性が要求されると考えられ、その意味でも、情報課が早急に共通基準や基準の作成例を作成し、各個別システムの所管課における情報セキュリティ対策において指導的役割を果たすことが強く求められている（電子情報処理規則第１６条２項、第６条（３）、（７）等）。個別システムの管理運用基準やセキュリティ実施手順の見直しは、一義的には個別システムを所有する課の所属部長（セキュリティ統括責任者）や課長（セキュリティ責任者）に責任があるとはいえ、その相談や指導に当たる情報課においても、当該見直し作業が支障なく行われるよう、早急に共通基準や作成例を制定の上周知するとともに、各所管課に対し十分な指導を行うことが必要である。

１０　統括的指摘事項、包括外部監査人の意見並びに提言

各課に対する個別の指摘事項から、目黒区における個人情報を取り扱う情報セキュリティの管理体制、運用及び検証体制の現状には、共通した問題と課題があることが浮かび上がってくる。

その現状を短く言い表せば、管理体制にかかる上位のセキュリティ対策基準等の規程類の整備や体制づくりは進捗してはいるが、セキュリティ対策基準にはやや手直しが必要な点も見受けられる一方、個別システムのそれの見直し作業は進んでおらず、その運用は課によって遵守レベルのばらつきがあって重大な基準違反も発生しており、また、職員同士で行う独自の内部監査や自己検証にはかなりの問題がある状態といえる。また、管理体制自体にもガバナンス向上やＰＤＣＡの促進から検討すべき点がある。

これらの点については、以下に、具体的に統括的指摘事項として指摘し、そのような事態を発生させている原因となっている事実として指摘すべきものや関連する事実、さらに対策として行うべきことを記述する。また、原因とまでは断言できない又は指摘事項として改善を要すべき事項とまでは言い切れないが、監査チームが監査を通じて観察したところから目黒区において検討すべきであると思われる点を、意見又は提言として指摘事項の次に掲げることとする。

（１）　目黒区に対する統括的指摘事項

ア　情報セキュリティ対策基準の不明確な規定

基本計画や情報化推進計画では、情報セキュリティ対策の強化をとるべき施策として宣言し、リスク分析の考え方を取り入れて情報資産を重要性に応じて分類した対策をとるとしており、これに基づいて、情報セキュリティ基本方針及び情報セキュリティ対策基準が平成２２年７月に改定されている。

その内容をみると、総務省ガイドラインの情報セキュリティの基本的観点をかなりとりこんでいることがわかる。特に情報セキュリティ対策基準は、情報資産を重要性に応じて分類している。これは、情報資産を機密性による分類[22]、完全性による分類[23]、可用性による分類[24]という三つの分野で分類し、それぞれの項目ごとにリスクに応じた対策基準及び取扱いの条件や制限等をセキュリティ責任者が設定するという考え方である。ここで分類に応じて設定すべきであるとされている基準や取扱いの条件には、以下のようなものを含むとされ

[22] 情報資産がどの程度の機密性を要するかによって、アクセス権限の設定や情報の漏えい対策を行うべきかのレベルを決定するという整理である。

[23] 業務遂行上、正確性や完全性がどの程度求められるかによって、対策のレベルを決定するという整理である。

[24] その情報の利用が出来なくなることが業務遂行にどのような支障を及ぼすかによって、対策のレベルを決定するという整理である。

ている。

大　項　目	小　項　目
情報資産の管理	機器の据付、重要な情報処理システムの可用性の向上、電子データの管理及び保管、機器の電源、ネットワークケーブル等の配線、外部事業者に情報処理機器を取り扱わせる場合の留意事項、情報処理機器等の廃棄
情報資産の設置場所の管理	管理区域の設定・構造・入退出管理、管理区域への搬出入管理、管理区域外での物理的措置（ワイヤーによる固定など）、管理保管設備の必要条件と点検等、管理区域又は管理保管設備の運用、管理又は保管する担当者の指定
人的セキュリティ	職員が遵守すべき事項、研修等
技術的セキュリティ	アクセス権限、不正プログラムへの対策、アクセスログの取得、障害対応、外部ネットワークとの接続制限、電子署名・暗号化など

しかしながら、情報資産による分類を行った場合に、どのレベルの対策が原則として適切なのかの例示がないので、セキュリティ責任者が的確な判断ができるかどうか疑問であり、またセキュリティ責任者の考え方による対応となるので、全庁的に対策のレベルが統一できずまちまちになるおそれがある。

例えば、住民基本台帳記載の個人情報は機密性も完全性も可用性も最高レベルのものであることに疑いはないであろうが、そうであるとすれば、そのような情報が記録されている個別システムは、当該システムが据え付けられる管理区域が地震・火災等の危機管理の上からも安全と思われる場所に設定され、管理区域の立ち入りには承認されている人間しか許されず、また、管理区域の入り口にはセキュリティロックがされている等、物理的セキュリティにおいて最高レベルの管理が適切と考えられるし、人的セキュリティ・技術的セキュリティにおいても高度のレベルの管理が必要とされるであろう。しかし、情報セキュリティ対策基準では、管理の方針が具体的に分からない。すなわち、

① 火災、水害、ほこり、振動、温度及び湿度等の影響を考慮の上、情報資産の分類に応じた対策を施した場所に設置するとともに、容易に取り外せないよう固定する等の措置を講じるべき旨のみ規定されており、分類のレベルでどの程度の措置を取るべきかは方針としても示されておらず、例示もない。

② どの分類の情報資産について管理区域の設定をすべきかについてはまったく指針が示されていないため、どの分類の情報資産について管理区域を設定すべきかの方針が不明確となっている。

③ 特に重要な電子データに関しては区以外の施設において保管及び管理をする措置を行うとしているが、「特に重要なもの」とは、機密性、完全性、

可用性の観点からみてどのレベルのものなのかの例示もなく不明確である。

④　物理的セキュリティについて、機密性２、可用性２については特に規定されている項目があるが、その他の項目について分類について指定がない場合には、すべての分類にあてはまる方針であるのかが不明確である。

⑤　人的セキュリティ及び技術的セキュリティについては分類について特に指定した項目がないが、技術的セキュリティに関してはアクセス権限、障害対策、外部ネットワークとの接続制限の各点について情報資産の分類によって対応の方針が異なることも考えられるから、この点についてもいま少し検討が必要に思われる。

⑥　改定前の情報セキュリティ対策基準では情報システムで作成された帳票の管理についての規定があったが、現在の情報セキュリティ対策基準では情報資産の定義にも含まれておらず、また個別の規定も設けられていない。この原因は、情報システムで作成された帳票が情報セキュリティ基本方針における情報資産の定義に含まれなかったためと推測されるが、運用面の対策として情報セキュリティ対策基準には規定を設けるべきではないかと思われる。

以上のように、情報セキュリティ対策基準の記述は、指針として不明確な点がいくつかあるといわざるを得ないので、さらなる検討が必要である。

また、情報セキュリティ対策基準では、人的セキュリティについて、職員及び委託事業者等の遵守すべき事項、研修、事故及び欠陥等への対応が掲げられているが、当該項目はすべて職員に対するものとして記述されており、委託事業者に対するものなのか規定上は明らかでないため、明確化する必要がある。

イ　個別システムの情報セキュリティ管理運用基準及びセキュリティ対策基準の見直しの未実施

上記のとおり、改定された情報セキュリティ対策基準が情報資産の分類にしたがった管理という考え方に変ったのであるから、個別システムのセキュリティ責任者は、情報資産の分類にしたがった個別システムの情報セキュリティ管理運用基準及びセキュリティ対策基準の見直しにすみやかに着手すべきであるが、監査終了日現在においても、見直しに着手している部は皆無である。

しかし、上位規程が改正されて施行されているのに、下位の規程の見直し作業が着手さえされていないのは怠慢のそしりを免れるものではない。

平成２２年６月２８日に開催された情報化推進委員会では、情報セキュリティポリシーの改定案についての説明があり、情報課が管理運用基準及び対策基準の作成例を出す予定であるとの説明がなされている。また、その後の企画経営部長（情報システム統括責任者）による各課長（セキュリティ責任者）宛て通知においても、「標準個別システム管理運用基準及びセキュリティ実施基準」の作成例については後日通知する旨が記載されている。この点について、情報

課が作成例を出していないことは情報課に対する指摘事項で述べたところであるが、個別システムの情報セキュリティ管理運用基準及び対策基準を整備する責任はあくまで各個別システムのセキュリティ責任者（各課長）にあるのであって、作成例がないため何もしないということでは、その責任を果たしたことにはならない。平成２２年１０月の情報化推進委員会では作成例が示されていないことや、個別システムの基準等の改定が進んでいないことについてのセキュリティ統括責任者（各部長）からの発言は皆無であって、目黒区における個別システムの基準等の改定の必要性に対する感覚はかなり鈍いといわざるを得ない。

目黒区は全庁の個別システムにおいて情報課が一刻もはやく作成例を決定し、かつ、各セキュリティ統括責任者（各部長）及びセキュリティ責任者（各課長）において速やかに見直しを行うよう、情報化推進委員会において適切に指導し推進すべきである。

なお、その際に、とりあえず、現行の情報セキュリティ対策基準によって情報資産について機密性、完全性、可用性の観点で分類し、これらについてレベルが最も高いシステムと思われるのに管理区域の設定・構造・入退出管理、管理区域への搬出入管理の項目等の物的セキュリティ対策や、その他の人的・技術的セキュリティ対策が欠けるといったことのないように、各セキュリティ責任者が作成する管理運用基準及びセキュリティ対策基準が真に情報資産の分類に適合しているかを検討することが重要である。現状の管理体制の枠組からみると情報化推進委員会の承認事項とすることは手続的には重過ぎると思われるが、専門的知識を有する情報課においてそのレベルを全庁的に統一する方向で働きかけることは可能であると考えられるので、例えば、各課が作成した改定案について情報課の同意をとりつけないと決定ができないようなやり方を検討すべきである。また、情報化推進委員会が遅くとも今後数ヶ月以内に改定が終了するように改定の進捗状況を監視し、適時、指導することも必要である。なお、本報告書で情報セキュリティ対策基準の不明確性を指摘したからといって、その改定をまって個別システムの情報セキュリティ管理運用基準及び対策基準の見直しを行うような解決の先延ばしをすべきではないことはいうまでもない。

ウ　自主点検の機能不全

目黒区では、平成１７年度から全庁的なセルフチェックを実施している。すなわち、情報課が一般職員用と課長用のセルフチェックシートを準備して、個々の職員がチェックシートへの回答を記入してセキュリティ責任者である課長に提出し、課長においてその内容を検討させ、その結果と各課の情報セキュリティ対策を提出させる形式の自主点検を行っている。

しかしながら、今回の監査では、監査対象部課から多数の問題が発見されて

おり、発見されたものには、チェックシートに質問項目があるのに問題が指摘されたパスワード不変更の事例、チェックシートに質問項目がない物理的セキュリティに関する問題が指摘された事例、自主点検や内部監査で発見された指摘事項に対する対策をとるといいながら対策が現実にはとられておらず問題が放置されていた事例や、さらには質問自体に対する虚偽の回答が見られた事例が含まれている。自ら問題を発見し、自ら対策を考え、自ら対策を実施するという自主点検の目的や、問題点の集約を情報課で行い、全庁的な対策の参考とするという目的は達せられていないというほかない。

この原因は、自主点検の進め方と自主点検で発見された全庁的課題について対策の決定と実行に関する統制が十分でないことにあると思われる。自主点検が機能するには、個々の職員の遵守状況を十分把握するに必要な主要なポイント（前記①に記載の小項目の主要なもの）をカバーする質問表が用意され、セルフチェックの結果について問題があれば、セキュリティ責任者が当該課の中で発見された問題を課内でまず共有化させ、さらに見落としている問題がないかどうかを洗い出すプロセスを踏んで、当該問題の原因を探り、発見された原因に対して適切な対策を講じるという一連のプロセスが必要で、このようなプロセスにしないとセルフチェックの目的を十分達せられない場合が多い。この観点からみると、現在の自主点検の体制や運営には以下のような問題がある。

① 平成２１年度までの自主点検のための質問表はあまりにも質問項目が少なく、また、質問も抽象的なものが含まれており十分ではない。例えば、「個人情報の扱いについては、常に個人情報保護条例の規定を念頭においている」、「セキュリティパッチを更新することの重要性を知っている」、「電子情報だけではなく、紙媒体からの情報漏えい等にも常に注意している」という抽象的な質問ではセルフチェックの用は十分なさないから、質問をもっと具体的なものにする必要性がある。

② セキュリティ統括責任者及びセキュリティ責任者にセルフチェックのプロセスで何が重要かを十分理解させる必要があるが、情報課からの各課への依頼文書「情報セキュリティに関するセルフチェックの実施について（依頼)」では、課で集計したときに問題が発見された場合、適切であるときには課の内部で共有化するというガイダンスは欠けているし、セキュリティ責任者である課長に対策の検討を依頼してはいるが課の内部で何をすべきかの指導がないため、セキュリティ責任者は単に集計作業とそれに対する対策を提出するという作業のみを行って終了している可能性があり、課の中での職員による自発的なＰＤＣＡサイクルの向上に必ずしも結びついていない。

③ セキュリティ統括責任者及びセキュリティ責任者だけで十分な対策をと

ることができない場合は、全庁的な分析と全庁共通の対応を行うべきかを上位機関で検討し、対策を決定して各セキュリティ責任者に実行させるべきであるが、情報課から自主点検の集計報告を受けている情報化推進委員会がそのイニシアチブをとったという例がみられない。たとえば、パスワードの定期的変更がないという問題は各課において、繰り返しかつ長期にわたって発生しており今回の監査でも発見されている問題であるが、パスワード変更そのものはセキュリティ責任者が適切に行われているか監視すべきものでセキュリティ責任者の職務が適切に遂行されていない可能性や、セキュリティ責任者が多数の職員の個別パスワードを定期的に作って変更するという手続の実行が難しい可能性もある。したがって、パスワードを変更するように課所属職員に促すだけではその対策として十分ではないし、また人の自覚による規程遵守という方法に限界がある疑いがあるから、一定期間経過すると自動的にパスワード変更を促すスクリーンが出て、パスワードを変更しなければログインできなくなるというシステム的な対応が必要であるかもしれない。このような検討が情報化推進委員会でみられないのは、情報集約や分析が十分でない等の自主点検のプロセス管理が不十分である可能性がある。

④　なお、平成２２年度のセルフチェックの質問事項は情報セキュリティ基本方針及び情報セキュリティ対策基準が改定されたため、その理解度を測るものであった。しかし、当該質問事項は新たな基準の理解ができているかを計測するためには有効・有用であるが、現に情報セキュリティ運用基準及び対策基準がそのとおりに運用されているかという点をチェックするための質問事項ではないので、自主点検の本来意図している目的達成には有用ではない。このような質問事項のセルフチェックは、改定された情報セキュリティ基本方針及び情報セキュリティ対策基準についての講習を行った後に、その理解度を測るために実施するのがむしろ適当である。

以上から、目黒区は、自主点検の質問事項や、セキュリティ統括責任者及びセキュリティ責任者が行うべき手順や、情報課が問題を集約した後の情報化推進委員会での検討と全庁的対応の必要性を検討して対策を実行させるプロセスを、今一度確立する必要がある。

エ　不適切な内部監査体制及びその機能不全

目黒区の内部監査の体制は、設計が不完全で、運用も不適切であり、早急に改善する必要がある。以下にその理由を述べる。

目黒区の内部監査は、監査計画を情報課が策定し、その計画に基づいて、監査対象から独立している者ではなく情報課が依頼する他の部の課長（セキュリティ責任者）が監査人となって情報課が用意した資料、手順、質問事項によっ

て監査を行うという体制である[25]。この体制には、監査としての独立性だけでなく、監査の専門性や監査の実効性の欠如から発生する監査リスク（監査手続において重要な問題を見落とすリスク）の問題が本質的に存在する。

すなわち、内部監査は各課の持ち回りであるから、ある年に監査対象になる（あるいはなった）課の課長が監査人となって行うものであり、他の部課の監査を行ったときの課長が自分の課の内部監査の担当になるかもしれず、監査のお手盛が起きるリスクがあるし、また監査対象となる課のセキュリティ責任者である課長では独立した監査人とは言えない。

また、監査人であるセキュリティ責任者は、監査対象となる個別システムに通じているわけでもなく、監査の専門家でもないから、重要な問題点を見落とすリスクがあるだけでなく、監査人となった者の知識・経験や監査の取組み姿勢で実際の監査の質に大きなばらつきが発生する可能性がある。

この点、情報課によると、内部監査人に選ばれた者は情報課が行う１時間の内部監査に係る監査人説明会を受講しなければならず、これによって対策をとっているとしている。この説明会では情報課が用意した資料を使用して、情報セキュリティ内部監査の概要説明、監査実施手順（ヒアリング、実地調査）の説明、質疑応答が行われるが、平成２１年度情報セキュリティ内部監査説明資料（以下、「説明資料」という）を検討すると、以下のような問題を指摘することができる。

① ヒアリングは被監査課長が５分程度で資料に基づく説明を行い、ヒアリングは事務局があらかじめ作成した質問事項を参考にして約２５分程度行うとされ、進行役である事務局（情報課課員）は時間管理を行い、主任監査人は既定の時間になったらヒアリングの終了を宣言すると説明されている。実地調査も１５分から２０分が目安とされており、全体でも１時間以内の監査時間とされている。また、業務に支障を来さないようにとの注意喚起がある。１時間の監査では表面的な監査にとどまってしまう可能性が非常に高いし、説明資料に書かれている指示は監査人が懐疑をもっても時間をかけた監査を行うという意欲をそぐ方向に働く[26]。なぜこのような短い時間しか監査しないのかについて、情報課は、監査人となる課長の日常業務から考えて１時間以上の時間を確保するのは困難であり、また、資料に目をとおしての準備と監査調書の作成を含めて数時間以上使うことを強いることはできないと説明している。このように最初から、監査資料も限定され実査も時間的に限定するフレームワークとなっているだけでなく、全庁に内部監査は短い時間

[25] 第２の１（６）でのべた情報セキュリティ監査実施要綱に関する説明を参照。

[26] 監査論では、職業的懐疑心をもって監査を行うことは、監査人の職業倫理として当然であり必要なこととされており、常識である。

ですませるという暗黙の合意を形成させている可能性がある。

② ヒアリング質問事項は情報課が準備しているが、これは毎年同じものが使われており、自主点検や過去の内部監査を考慮して質問事項をアップデートするということは行われていない。また、総務省ガイドラインの必須監査事項１１０項目に比較すると、極めて限定された範囲の事項しか質問事項として列挙されていない。

③ 個別システムの管理運用基準やセキュリティ実施基準は、事前に資料として監査人に送付されているようであるが、ヒアリング質問事項に対する回答は、監査対象の各課における管理運用基準やセキュリティ実施基準を参照しなければ、問題があるのかどうか正確には評価できないものがあるし、さらに管理運用基準やセキュリティ実施基準そのものが十分な内容のものであるかどうかもわからない。例えば「オンライン端末やパソコンの設置場所について、何か留意している点がありますか。」というヒアリング質問事項があるが、これでは各課における個別システムの運用基準やセキュリティ対策基準が守られているかどうかというポイントをつく質問事項にはなっておらず、また、今回の監査対象となった各課の内部監査ではヒアリング質問事項を個別システムの運用基準やセキュリティ対策基準が遵守されているかどうかということについてチェックが十分されているかどうか疑わしい状態である。また、情報セキュリティ対策基準では、セキュリティ責任者が情報資産の分類により個別システムのセキュリティ実施基準に盛り込むべき項目とされているから、個別システムのセキュリティ実施基準に照らして対策が十分か監査人が判断すべきであるところ、この質問事項ではそれができないし、またそれが行われた形跡は一切無い。むしろそのような個別システムの管理運用基準やセキュリティ実施基準が十分かどうかは監査人の考慮するところではないものとなっている。

④ また、質問事項に対する回答のみでは重要なリスクが発見できない形式的な質問も含まれている。例えば、システムの障害時の手順について、質問は「システムがダウンして使用不能になった場合、代替処理などの手順を定めていますか」となっているが、各個別システムのセキュリティ実施基準では別途対応マニュアルによるとしている例が多く、したがって答えがイエスであれば形式的なマニュアルの整備は問題なしとされてしまう。しかし、マニュアルを見なければ、障害時の対応として十分なものが整備されているかどうかは実はわからない。

また、これまでの各課の指摘で明らかなとおり、ヒアリング質問事項や実地

調査チェックリストに含まれているのに見落とされている問題点や質問事項に含まれない重大な問題が今回発見されており、内部監査人によってばらつきや監査の質に大きな差があることがあり、問題である。特に選管事務局における指摘事項は、その多くは内部監査で指摘可能であったと思われるのに、まったく見逃されていた。

さらに、情報課は内部監査では事務局的役割を果たしているのであるから、上記のような監査の実態からみれば、情報課に対する内部監査は、他の課長が監査人になるとはいえ、実質的には自己監査にすぎないものである。これは、内部監査の独立性、客観性の観点からみて、適切とは思えない。この点、第三者による目黒区内部情報システム・システム監査報告書（平成２２年３月）においても、システム監査について情報課に対する監査が多く、被監査部門が監査の事務局を担当することは監査における独立性、客観性の観点から問題が多く、区がシステム監査を推進する上でその推進体制について再検討すべきとの提言がなされている。

以上のような内部監査手続の実態からみれば、現在の内部監査制度は自己点検の一形態と呼ぶほうが正確であり、内部監査というのは不正確である。総務省ガイドラインも内部監査が被監査部門から独立した監査人等が行うことが必要としている点を踏まえれば、情報課からも独立した情報セキュリティ監査チームを設置すべきである。独立した課を設置するのが理想的であるが、それが無理であるならば監査事務局にそのようなスタッフを補充することは可能であろう。また、内部監査の実施要綱の見直し、監査項目や質問項目の見直しや年次における重点監査項目の制定など、内部監査の充実に努める必要がある。

この点、今後の情報セキュリティ監査の実施について、情報課の考えとして、①内部監査と外部監査双方のメリットが活かせるよう隔年ごと交互に行う等の実施が望ましく、また内部監査の実施においても、監査事務局等、区長部局とは独立した部署による専門的な監査の実施が望ましいが、いずれも現在の財政状況、人材の確保の困難さという点から実施が困難な状況にあること、②過去の内部監査は、各課長が自所属におけるセキュリティ対策について理解を深めるきっかけとなった面もあること、③来年度以降は個別システム単位で監査を実施する方法が考えられるが、その規模や対象所属が大きく異なることから検討が必要であること、④庁外施設については今回６施設のみの実施にとどまったが、情報セキュリティ規程類の遵守状況や個人情報の管理状況等について確認もできることから、来年度についても数施設程度は実施したいこと、⑤監査対象の抽出、実施方法については効率的・効果的な方法を検討していくこと、の５点が表明された。

情報課も監査法人等への委託による監査の実施を含め効率的・効果的な方法を検討している状況である。財政状況等の問題を考えるならば、監査事務局等

による内部監査と自己点検を実施するほかないであろう。ただし、効率的・効果的に実施するには、以上の指摘事項の改善が不可欠である。目黒区が十分対応できるのであるならば問題はないが、自ら対応できない場合には、監査法人等の専門家へ内部監査の実施方法（ヒアリング項目も含む）や自己点検に関する質問票の見直しについてのアドバイスや当該業務を委託することなど、第三者機関の能力を活用して対応することが有用である。

また、情報課から内部監査の報告を受けている情報化推進委員会がそのイニシアチブをとったという例がみられない。情報化推進委員会に対する平成２０年度及び２１年度の内部監査報告では２年連続してパスワードの不変更が報告されているが、情報化推進委員会は全庁的な点検の指示や改善の指示は出していない。これでは上位機関としてＰＤＣＡを促進する機能を十分果たしたことにはならない。

オ　情報セキュリティ関連文書の非公開に関する手続の不備

目黒区は情報セキュリティ関連文書を第三者に開示するにあたり、覚書を締結し、情報セキュリティ関連文書を指定し、右文書で「第三者が業務上知り得た区の人事、技術、事務手続等の情報」を機密情報として区の同意が無い限りその利用と公開を禁止している。今回の包括外部監査にあたり、包括外部監査人は覚書の締結を要求されたので締結したが、目黒区はかかる運用の根拠規程はないがそのように運用していると説明している。しかし、かかる運用は情報公開条例第４条第１項で定められている保有情報の公表及び提供のための施策を整備するという規定の趣旨に反する疑いがあるし、基本計画に表明されている情報公開の促進という施策とも逆方向であるので、手続規程の整備を行う必要がある。

包括外部監査人が監査にあたり目黒区から締結することを要求された覚書は、情報セキュリティ関連文書があまりに広く指定されているため、その内容の引用やその運用にかかる事項は、機密情報に該当するものが多々ある。情報セキュリティに問題がある場合に、包括外部監査人には報告書に監査結果とその認定にいたった事実関係を適切に記載すべき義務が包括外部監査契約上あるので、説明義務を尽くした監査報告書を作成するには必然的に機密情報に該当する事項を記載せざるを得ない。

また、包括外部監査報告書は、地方自治法第２５２条の３７第５項で区長、議会、監査委員、関係行政委員会に提出が義務付けられ、同法第２５２条の３８第３項により監査委員は提出を受けた報告書を公表することとなっている。さらに、地方自治法２４２条に基づく住民監査請求[27]がなされた場合、または、

[27] ただし、住民監査請求の対象は、公金の支出、財産（土地、建物、物品などの取得・管理・処分、契約（工事請負、購買など）の締結・履行、債務その他の義務の負担（借り入れなど）、公

目黒区包括外部監査契約に基づく監査に関する条例第３条により区民が個別監査請求をした場合には、住民監査請求の結果報告又は個別監査報告には監査結果についての適切な説明がなされなければならず、そのためには覚書の機密情報に該当する情報を記載しなければ十分説明ができない場合もありうる。

他方、情報セキュリティに関する監査報告書には、情報資産や情報システム等の脆弱性に関する情報が含まれており、情報セキュリティ確保の観点からはすべてを公開することは適当ではないことがあることも事実であり、区として公開を制限する措置を取るべき場合もありうる。

この点、総務省ガイドラインでは、「各地方公共団体の制定する情報公開条例の「不開示情報」の取扱いなどを踏まえ、適切な範囲で公開していく必要がある」としており、基本的には情報公開条例の枠内での運用が適切であると指摘しており、監査人としてもそのような運用が適切であると考える。

そこで、情報公開条例第４条第１項で定められている保有情報の公表及び提供のための施策を整備するという規定の趣旨に従い、規則を整備し、情報セキュリティ関連文書とその中に含まれる機密情報を適切に定義し、機密情報の非公開の手続を定める根拠規程を設けるべきである。

カ　個人情報を含む電子データの保存年限を定めた文書保存・廃棄基準に違反する状況

個人情報保護条例第１０条第２項で「保有個人情報を保有する必要がなくなったときは、速やかに消去しなければならない」と規定されていることから、関係各課の文書保管年数状況や作成データの参照の可能性等その他を考慮して、電子データの保管期間を決めることが必要であるが、目黒区の文書管理規定に基づく文書保存・廃棄基準によると、「文書」は、「区における事務の執行につき必要なすべての書面及び電磁的記録をいう」と規定され、保存年限については「文書の保存年限は別表に定める基準に基づき、次の各号に掲げる区分に従って課長及び所長（全庁的に共通して存在する文書の保存年限にあっては、主管部局の長）が決定する。」等と定められている。しかるところ、今回監査対象としたすべての課において、個人情報を含む電磁的記録の保管期間は定められていないと認識されており、これらの電磁的記録は保管期間を超えた時に消去するという運用がなされていないことが発見された。

文書保存・廃棄基準の文言上は電磁的記録についても保存年限の規定の適用があるとみるほかないので、この事態は文書保存・廃棄基準違反である。他方、個人情報を記録している電磁的記録はさまざまであり、その内容によって一律保存年限を過ぎたものを文書保存・廃棄基準どおりに消去すべきなのか、さら

金の賦課・徴収を怠る事実（都税の徴収を怠る場合など）、財産の管理を怠る事実（損害賠償請求を怠る場合など）に限定されるから、情報セキュリティに関してもこれらの範囲に限定される。

に消去するという運用が妥当かどうかは疑問がある。たとえば、保健福祉情報システムは、多くの福祉関係課が使用しており、一律に保管期限を決めることはできない。したがって、文書保存・廃棄基準の見直しも含め、電磁的記録の内容や利用状況を考慮した柔軟な保存年限と消去の手続に関する規程を整備する必要がある。

（２）　意見並びに提言

ア　情報化推進委員会委員長と情報セキュリティ統括責任者には副区長レベルを

情報セキュリティに関する目黒区の体制は、情報化推進委員会を頂点としているが、情報化推進委員会は内部監査や自主点検の結果報告を受けても何ら全庁的な対策を打ち出したことはなく、ＰＤＣＡの推進という観点から機能は十分はたされているとは言い難いと思われる。また、企画経営部長のもとにある財政課が全庁的に区の財政に責任を有しており、同じ部長のもとで情報課が基本計画や補助計画である情報化計画に基づいて予算要求をしてもそれが認められないことも多々あるようである。

ＩＴガバナンス体制については、第三者による目黒区内部情報システム・システム監査報告書（平成２２年３月）においても、情報化推進計画を確実に実行するＰＤＣＡのサイクルを確実に展開する体制を整備することが提言されていることを考えると、全庁的な事項について権限がある者（副区長レベル以上）が情報推進化委員会を主催し、優先順位を決断し政策実行についての適切な指示が全庁に対して発せられるようにすべきではないかと考えられる。総務省の調査[28]でも、区長が情報セキュリティ統括責任者となっている区は２、副区長がなっている区は１５であり、部長級がなっているのは４区である。人口２０万人以上の地方自治体１０８団体では、首長レベルが１０、副知事等のナンバー２が７１であるのに、部長クラスは７しかない。ＩＴガバナンスを重視している地方自治体が多いことを考慮すると、目黒区においても体制の一層の強化を検討することを提言する。

イ　基本計画を骨抜きにしないためのプロセスの検討を

基本計画で情報セキュリティの重要性にふれ、補助計画である情報化推進計画でも施策として実行を約束している一方、実施計画では施策として掲げられた事項についての事業予算化が十分なされず、また、政策実現のロードマップも整備されていない状況がある。基本計画が骨抜きになってしまっていることは否定しようのない事実である。

これはなにも情報セキュリティに限った話ではないが、そもそも１０年もの

[28] http://www.soumu.go.jp/denshijiti/chousah22.html

長期にわたる基本計画を策定するならば、そこには相当のコミットメントがなければならないが、変化の激しい現代で１０年もの長期計画をぶち上げることに果たしてどれだけの実現可能性があるのか疑わしい。基本計画でいくら美辞麗句を並べても、実行がともなわなければ何の意味もないのである。

他方において実施計画や補助計画は５年間とされている。５年実施してみて次の５年で残りの施策を全部実施できるかは、そのときの財政状況次第なのであるから、もともと基本計画を修正することを予定しているようなものであるといわれても反論できないのではないだろうか。

基本計画も実施計画も区長の任期（１期または２期）にあわせ、基本計画で施策として掲げた事項をどのタイミングでどのようにして実現するのかについて、ロードマップを示すべきではないだろうか。そしてそのロードマップにあわせた実施計画を策定すべきではないか。そうでないと、基本計画は単なる美辞麗句の政治的マニフェストに堕し、実施計画策定の時期の部局間の予算の調整の中で施策実行はあやふやになり、基本計画の施策の多くが実現できない項目の塊になってしまう。区民がロードマップに基づいて政策が実現されていくのかをチェックできるような工夫が必要であると考える。

ウ　目黒区にＰＤＣＡを働かせるための意識改革を

監査人は昨年度の監査報告書で、区職員の意識改革を区長や上級職員のイニシアチブで実現するように提言した。本年においても、なおこのことを特に強調して提言したい。

今回の監査では、監査人団が用意した質問票や質問に対して事実と異なる回答を行った例がいくつかみられた。極めて残念な事態というほかない。監査に対する虚偽の回答は、監査の破壊である。それであるがゆえに、例えば金融庁の行う金融検査では場合によって検査忌避罪を構成し刑事罰の対象となる悪質な行為である。

これらの事実に反する回答は監査人チームとの比較的簡単な問答によって正確な回答を引き出すことができている。したがって、事実に反する回答を行った職員が監査妨害の意図を有していたという印象を監査人団はもっていない。しかし、とりあえず自分には問題がないことを質問票に対しては回答しておいて、監査人補助者に少し問い詰められるとあっさりと本当のことを告白するという態度を目撃している。すなわち、軽い気持ちで事実に基づかない回答を行った場合であっても監査を破壊する可能性があることが理解できていないのである。これは、監査の機能の無理解の顕れというほかはない。

監査の機能の理解という点については、情報セキュリティ対策の要ともいえる情報課においても十分ではないと感ずる点があったのは前述したところであるが、さらに、監査人団は監査外でもその印象を強く持つ出来事があった。本件監査が進行中に、目黒区は財政難を理由として緊急対策を打ち出し、３６

項目の事業を廃止、延期、縮小又は改善に分け、包括外部監査は廃止される２事業の一つに選ばれた。財政難からやむをえない措置ではあろうが、問題はその理由付けである。廃止は事業存続の意義が薄れているものと分類されているところ、包括外部監査については監査テーマの主要なものは実施され指摘事項も概ね改善されており、制度としての一定の役割は果たしたというのが廃止の理由である。ここにみられる意識は、監査という制度に対する相当の理解のなさを表している。毎年の包括外部監査で多くの問題が指摘され続けてきている実情は、目黒区におけるＰＤＣＡがまだまだ十分機能していないことの証左であり、目黒区職員の監査に対する意識の低さが一因であると監査人団は考えている。この廃止の理由はまさにそれを示した事例であろうし、今回の監査において職員に見られた意識とまったく同質である。

平成２１年度包括外部監査報告書でも指摘したところであるが、監査委員の監査や包括外部監査における指摘のみを改善していけば、組織がよくなるかというとそうではないことは明らかである。もともと地方自治体においても内部統制があるはずであって、よりよい行政を実現するために常に区職員が問題点を認識し改善につとめてこそ、始めてＰＤＣＡサイクルが機能し始めるのである。また、包括外部監査の役割は、行政の監視という意味ももちろんあるが、そのような組織の自律機能を援助する仕組みでもある。区職員が行政事務の改善に主体的・継続的に取り組むことこそが、内部統制の要なのである。したがって、問題点の発見から、原因を分析し、改善策を策定し、実行していくのは、本来的に区の職員の仕事であり、包括外部監査はそれを援助するものと捉えるべきであって、このような主体的改善活動の自覚がないと、包括外部監査の指摘に対する根本原因にさかのぼった改善案の立案・実行に至らなかったり、あるいは長期間にわたり改善活動を停滞させるといった弊害が現れる。今回の監査で改善に自発的に取り組もうとしている課も見られたところではあるが、全体として目黒区の職員の意識レベルは、まだまだ指摘されるまでは改善活動を自らは行わないというレベルから脱していないのではないかと懸念している。

目黒区は真剣に職員の意識改革に取り組むべきである。

以　上

別紙一覧

別紙１： 総務省「地方公共団体における情報セキュリティ監査に関するガイドライン」（平成１５年策定、平成１９年改定）の「必須１１０項目」の抜粋

別紙２： 個別システムの概要

別紙３： 国保年金課 国保収納推進員システム

別紙４： 戸籍住民課 戸籍情報システム

別紙５： 健康福祉計画課 保健福祉情報システム

別紙６： 地域ケア推進課 包括支援業務支援システム

別紙７： 介護保険課 介護保険システム

別紙８： 選挙管理委員会事務局 選挙人名簿・期日前投票システム

別紙９： 生活福祉課 生活保護システム

別紙１０： 子育て支援課 児童扶養手当システム

別紙1:【目黒区外部包括監査参考用】「地方公共団体の情報セキュリティ監査ガイドライン」必須項目110

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
1. 対象範囲		(1)行政機関の範囲	1	○	**ⅰ）行政機関の範囲** 最高情報統括責任者によって、情報セキュリティポリシーを適用する行政機関の範囲が定められ、文書化されている。	□情報セキュリティポリシー	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーを適用する行政機関の範囲が文書化され、正式に承認されているか確かめる。	3.1.(1)	5.1.1	
		(2)情報資産の範囲	2	○	**ⅱ）情報資産の範囲** 最高情報統括責任者によって、情報セキュリティポリシーを適用する情報資産の範囲が定められ、文書化されている。	□情報セキュリティポリシー	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーを適用する情報資産の範囲が文書化され、正式に承認されているか確かめる。	3.1.(2)	5.1.1	・ネットワーク、情報システムで取扱うデータを印刷した文書及びシステム関連文書以外の文書は、文書管理規程等により適切に管理する必要がある。情報セキュリティ対策が進んだ段階では、すべての文書を情報セキュリティポリシーの対象範囲に含めることが望ましい。
2. 組織体制		(1)組織体制、権限及び責任	3	○	**ⅰ）組織体制、権限及び責任** 最高情報統括責任者によって、情報セキュリティ対策のための組織体制、権限及び責任が定められ、文書化されている。	□情報セキュリティポリシー □権限・責任等一覧	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティ対策に係る権限、責任、連絡体制、兼務の禁止が文書化され、正式に承認されているか確かめる。	3.2.(1)～(6)、(8)	6.1.1 6.1.3	
		(2)情報セキュリティ委員会	4	○	**ⅰ）情報セキュリティ委員会の設置** 最高情報統括責任者によって、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されている。	□情報セキュリティポリシー □情報セキュリティ委員会設置要綱	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されているか確かめる。	3.2.(7)①	6.1.2	
3. 情報資産の分類と管理方法		(1)情報資産の分類	5	○	**ⅰ）情報資産の分類に関わる基準** 統括情報セキュリティ責任者及び情報セキュリティ責任者によって、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いが定められ、文書化されている。	□情報セキュリティポリシー □情報資産分類基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いが文書化され、正式に承認されているか確かめる。	3.3.(1)	7.2.1	
		(2)情報資産の管理	6	○	**ⅰ）情報資産の管理に関わる基準** 統括情報セキュリティ責任者及び情報セキュリティ責任者によって、情報資産の管理に関わる基準が定められ、文書化されている。	□情報セキュリティポリシー □情報資産管理基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、情報資産の管理に関わる基準が文書化され、正式に承認されているか確かめる。	3.3.(2)	7.1.2 7.1.3	
			7	○	**ⅱ）情報資産管理台帳の作成** 情報セキュリティ管理者によって、重要な情報資産について目録(情報資産管理台帳)が作成されている。	□情報資産管理基準 □情報資産管理台帳	監査証拠のレビューと情報セキュリティ管理者へのインタビューにより、重要な情報資産について目録(情報資産管理台帳)が作成され、定期的に見直されているか確かめる。	3.3.(2)(ｱ)	7.1.1	
4. 物理的セキュリティ	4.1. サーバ等の管理	(1) 機器の取付け	8	○	**ⅱ）機器の取付け** 情報システム管理者によって、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度等の影響を可能な限り排除した場所に設置し、容易に取外せないように固定するなどの対策が講じられている。	□機器設置基準/手続 □建物フロアレイアウト図 □管理区域(情報システム室等)のレイアウト図 □機器設置記録 □情報資産管理台帳	監査証拠のレビューと情報システム管理者へのインタビュー及び管理区域の視察により、サーバ等の機器が設置されているか確かめる。	3.4.1.(1)	9.1.4 9.2.1	・情報資産管理台帳などに、機器の設置場所や設置状態などを明記しておくことが望ましい。

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(2)サーバの二重化	9	○	**iii）サーバ障害対策基準** 統括情報セキュリティ責任者又は情報システム管理者によって、メインサーバに障害が発生した場合の対策基準及び実施手順が定められ、文書化されている。	□サーバ障害対策基準 □サーバ障害対応実施手順	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、サーバに障害が発生した場合の対策基準及び実施手順が文書化され、正式に承認されているか確かめる。	3.4.1.(2) ②	10.5.1 13.1.1 14.1.4	
		(3)機器の電源	10	○	**ii）予備電源装置の設置及び点検** 情報システム管理者によって、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的に点検されている。	□機器電源基準 □システム構成図 □機器設置記録 □機器保守点検記録 □障害報告書	監査証拠のレビューと情報システム管理者へのインタビュー及び管理区域の視察により、UPS（無停電電源装置）などの予備電源が設置されているか確かめる。また、停電時や瞬断時に起動し、当該機器が適切に停止するまでの間に十分な電力を供給できる容量があるかなど、定期的に点検されているか確かめる。	3.4.1.(3) ①	9.2.1 9.2.2 13.1.1 14.1.4	・設置した予備電源が、サーバ等の増設に対して十分な電力供給能力があるのかを定期的に確認しておくことが望ましい。
		(4)通信ケーブル等の配線	11	○	**ii）通信ケーブル等の保護** 統括情報セキュリティ責任者及び情報システム管理者によって、通信ケーブルや電源ケーブルの損傷等を防止するための対策が講じられている。	□通信ケーブル等配線基準/手続	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビュー及び執務室や管理区域の視察により、通信ケーブルや電源ケーブルが配線収納管に収納されるなど、損傷から保護されているか確かめる。	3.4.1.(4) ①	9.2.3 9.2.4	・情報処理設備に接続する通信ケーブル及び電源ケーブルは、可能ならば施設内の地下に埋設するか又はそれに代わる十分な保護手段を施すことが望ましい。 ・ケーブルの損傷等を防止するために、配線収納管を使用することが望ましい。 ・ケーブル用途（電源、通信等）で分離して配線することが望ましい。また、通信ケーブルを2重化している場合は、それぞれを別ルートで配線することが望ましい。
		(5)機器の定期保守及び修理	12	○	**ii）サーバ等の機器の定期保守** 情報システム管理者によって、サーバ等の機器の定期保守が実施されている。	□機器保守・修理基準/手続 □保守機器管理表 □保守体制図 □作業報告書 □障害報告書 □機器保守点検記録	監査証拠のレビューと情報システム管理者へのインタビューにより、保守対象機器、保守実施時期、保守内容、保守担当が明確になっているか、保守が適切に行われているか確かめる。また、実際にサーバ等機器の障害が発生している場合は、保守に問題がなかったか確かめる。	3.4.1.(5) ①	9.2.4	
			13	○	**iii）記憶媒体を内蔵する機器の修理** 記憶媒体を内蔵する機器を外部の事業者に修理させる場合、情報システム管理者によって、情報が漏えいしない対策が講じられている。	□機器保守・修理基準/手続 □保守機器管理表 □保守体制図 □作業報告書 □機密保持契約書	監査証拠のレビューと情報システム管理者へのインタビューにより、記憶媒体を内蔵する機器を外部委託の事業者に修理させる場合にデータを消去した状態で行わせているか確かめる。データを消去できない場合は、修理を委託する事業者との間で守秘義務契約を締結し、秘密保持体制等を確認しているか確かめる。	3.4.1.(5) ②	6.2.1 6.2.2 6.2.3 9.2.4 15.1.1 15.2.1	
		(7)機器の廃棄等	14	○	**ii）記憶装置の情報消去** 情報システム管理者によって、廃棄又はリース返却する機器内部の記憶装置からすべての情報が消去され、復元が不可能な状態にされている。	□機器廃棄・リース返却基準 □機器廃棄・リース返却手続 □情報資産管理台帳 □記憶装置廃棄記録	監査証拠のレビューと情報システム管理者へのインタビューにより、機器内部の記憶装置からすべてのデータが復元が不可能なように消去されているか確かめる。	3.4.1.(7)	9.2.6	・委託契約等により、サービス提供を受けている業務においても留意する必要がある。
	4.2. 管理区域（情報システム室等）の管理	(1) 管理区域の構造等	15	○	**iii）管理区域への立ち入り制限機能** 統括情報セキュリティ責任者及び情報システム管理者によって、管理区域への許可されていない立ち入りを防止するための対策が講じられている。	□建物フロアレイアウト図 □敷地図面 □管理区域（情報システム室等）のレイアウト図	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビュー及び管理区域の視察により、外部へ通じるドアを必要最低限とし、鍵、監視機能、警報装置等が設けられているか確かめる。	3.4.2.(1) ③	9.1.1	・外部へ通じるドアを必要最小限とするにあたり、消防法に違反しないよう留意する必要がある。

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			16	○	**ⅳ）情報システム室内の機器の耐震、防火、防水対策** 統括情報セキュリティ責任者又は情報システム管理者によって、情報システム室内の機器等に耐震、防火、防水等の対策が施されている。	□建物フロアレイアウト図 □敷地図面 □管理区域（情報システム室等）のレイアウト図	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビュー及び情報システム室の視察により、機器等に耐震、防火、防水等の対策が実施されているか確かめる。	3.4.2.(1) ④	9.1.1 9.1.4	
		(2) 管理区域の入退室管理等	17	○	**ⅱ）管理区域への入退室制限** 情報システム管理者によって、管理区域への入退室が制限され管理されている。	□管理区域入退室基準/手続 □管理区域入退室記録 □認証用カード管理記録	監査証拠のレビューと情報システム管理者へのインタビュー及び管理区域の視察により、入退室管理基準に従って管理区域への入退室を制限しているか確かめる。 また、ICカード、指紋認証等の生体認証、又は入退室管理簿への記録による入退室管理を行っているか、及びICカード等の認証用カードが管理・保管されているか確かめる。	3.4.2.(2) ①	9.1.2	・ 入退室手続に業者名、訪問者名等の個人情報を記述しているような場合は紛失、覗き見等が生じないように管理する。 ・ICカードや指紋等生体認証の入退管理システムを導入した場合、故障等により入退に支障が生じるのを未然に防止するため、定期的に保守点検することが望ましい。 ・必要以上の入退室や通常時間外の入退室など、不信な入退室を確認する必要がある。
		(3) 機器等の搬入出	18	○	**ⅲ）機器等の搬入出時の立会い** 情報システム管理者によって、管理区域への機器の搬入出の際は、職員を立ち合わせている。	□機器搬入出基準/手続 □管理区域入退室記録 □機器搬入出記録	監査証拠のレビューと情報システム管理者へのインタビューにより、機器等の搬入出の際に職員が立会っているか確かめる。	3.4.2.(3) ②	9.1.5 9.1.6	
	4.3. 通信回線及び通信回線装置の管理		19	○	**ⅱ）通信回線及び通信回線装置の管理** 統括情報セキュリティ責任者又は情報システム管理者によって、庁内の通信回線及び通信回線装置が管理基準に従って管理されている。	□ネットワーク管理基準 □通信回線敷設図 □結線図	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、通信回線及び通信回線装置、管理状況について確かめる。 また、執務室や管理区域の視察により、ネットワークの配線状況を確かめる。	3.4.3.①	10.6.1 11.4.1	
	4.4. 職員等のパソコン等の管理		20	○	**ⅲ）ログインパスワード設定** 情報システム管理者によって、情報システムへのログイン時にパスワード入力をするよう設定されている。	□パソコン等管理基準	監査証拠のレビューと情報システム管理者へのインタビュー及び執務室等のパソコン等のサンプリング確認により、パソコン等にログインする時にパスワード入力をするよう設定されているか確かめる。	3.4.4.②	11.5.1 11.5.2 11.5.3	・パスワードの管理及び取扱いについては、No.119～126、207～208も関連する項目であることから参考にすること。 ・ログイン時のシステム設定については、No.206も関連する項目であることから参考にすること。
5. 人的セキュリティ	5.1. 職員等の遵守事項	(1) 職員等の遵守事項 (ア) 情報セキュリティポリシー等の遵守	21	○	**ⅰ）情報セキュリティポリシー等遵守の明記** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が情報セキュリティポリシー及び実施手順を遵守しなければならないことが定められ、文書化されている。	□情報セキュリティポリシー □職員等への周知記録	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等の情報セキュリティポリシー及び実施手順の遵守や、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合に職員等がとるべき手順について文書化され、正式に承認されているか確かめる。また、承認された文書が職員等に周知されているか確かめる。	3.5.1.(1) (ア)	5.1.1	
			22	○	**ⅱ）情報セキュリティポリシー等の遵守** 職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策について不明な点や遵守が困難な点等がある場合、速やかに情報セキュリティ管理者に相談し、指示を仰げる体制になっている。	□情報セキュリティポリシー □実施手順	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、情報セキュリティポリシー及び実施手順の遵守状況を確かめる。また、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合、職員等が速やかに情報セキュリティ管理者に相談し、指示を仰げる体制が整備されているか確かめる。必要に応じて、職員等へのアンケート調査を実施し、周知状況を確かめる。	3.5.1.(1) (ア)	5.1.1	・職員等の情報セキュリティポリシーの遵守状況の確認及び対処については、No.271～279も関連する項目であることから参考にすること。

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(1) 職員等の遵守事項 (イ) 業務以外の目的での使用の禁止	23	○	**ⅱ）情報資産等の業務以外の目的での使用禁止** 職員等による業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていない。	□端末アクセス記録 □電子メール送受信ログ □ファイアウォールログ	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスが行われていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (イ)	6.1.4	
		(1) 職員等の遵守事項 (ウ) パソコン等の端末の持ち出し及び外部における情報処理	24	○	**ⅱ）情報資産等の外部持出制限** 職員等がパソコン等の端末、記録媒体、情報資産及びソフトウエアを外部に持ち出す場合、情報セキュリティ管理者により許可を得ている。	□端末等持出・持込基準/手続 □庁舎外での情報処理作業基準/手続 □端末等持出・持込申請書/承認書	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等がパソコン等の端末や記録媒体、情報資産及びソフトウエアを外部に持ち出す場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (ウ)②	9.2.5 11.7.1 11.7.2	・紛失、盗難による情報漏えいを防止するため、暗号化等の適切な処置をして持出すことが望ましい。
			25	○	**ⅲ）外部での情報処理業務の制限** 職員等が外部で情報処理作業を行う場合は、情報セキュリティ管理者による許可を得ている。	□庁舎外での情報処理作業基準/手続 □庁舎外作業申請書/承認書	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部で情報処理作業を行う場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (ウ)③	9.2.5 11.7.1 11.7.2	・情報漏えい事故を防止するため、業務終了後は速やかに勤務地に情報資産を返却することが望ましい。
			26	○	**ⅳ）私物パソコンの使用制限** 職員等が外部で情報処理作業を行う際に私物パソコンを用いる場合、情報セキュリティ管理者による許可を得ている。また、機密性の高い情報資産の私物パソコンによる情報処理作業は行われていない。	□庁舎外での情報処理作業基準/手続 □私物パソコン等使用申請書/承認書	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部で情報処理作業を行う際に私物パソコンを用いる場合、情報セキュリティ管理者の許可を得ているか確かめる。また、機密性3の情報資産の情報処理作業を行っていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (ウ)④	9.2.5 11.7.1 11.7.2	
		(1) 職員等の遵守事項 (エ) パソコン等の端末等の持込	27	○	**ⅱ）私物パソコン等の持込制限** 情報セキュリティ管理者による許可なく、職員等による私物パソコン及び記録媒体の庁舎内への持ち込みは行われていない。	□私物パソコン等使用申請書/承認書	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、私物パソコン及び記録媒体が庁舎内に持ち込まれていないか確かめる。持ち込まれている私物パソコン及び記録媒体がある場合は、情報セキュリティ管理者による許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (エ)	6.1.4	
		(1) 職員等の遵守事項 (オ) 持ち出し及び持ち込みの記録	28	○	**ⅱ）端末等の持出・持込記録の作成** 情報セキュリティ管理者によって、端末等の持ち出し及び持ち込みの記録が作成され、保管されている。	□端末等持出・持込基準/手続 □端末等持出・持込申請書/承認書	監査証拠のレビューと情報セキュリティ管理者へのインタビューにより、端末等の持ち出し及び持ち込みの記録が作成され、保管されているか確かめる。	3.5.1.(1) (オ)	6.1.4	・記録を定期的に点検し、紛失、盗難が発生していないか確認することが望ましい。
		(1) 職員等の遵守事項 (キ) 机上の端末等の管理	29	○	**ⅱ）机上の端末等の取扱** 離席時には、パソコン等の端末や記録媒体、文書等の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられている。	□クリアデスク・クリアスクリーン基準	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビュー、執務室の視察により、端末の画面ロックや文書等の容易に閲覧されない場所への保管といった、情報資産の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.1.(1) (キ)	11.3.3	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(3) 情報セキュリティポリシー等の掲示	30	○	**ⅱ）情報セキュリティポリシー等の掲示** 情報セキュリティ管理者によって、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるように掲示されている。	□職員等への周知記録	監査証拠のレビューと情報セキュリティ管理者へのインタビュー及び執務室の視察により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるよう、イントラネット等に掲示されているか確かめる。	3.5.1.(3)	5.1.1	
		(4) 外部委託事業者に対する説明	31	○	**ⅱ）外部委託事業者に対する情報セキュリティポリシー等遵守の説明** ネットワーク及び情報システムの開発・保守等を外部委託業者に発注する場合、情報セキュリティ管理者によって、情報セキュリティポリシー等のうち、外部委託事業者及び外部委託事業者から再委託を受ける事業者が守るべき内容の遵守及びその機密事項が説明されている。	□業務委託契約書 □外部委託管理基準	監査証拠のレビューと情報セキュリティ管理者へのインタビューにより、ネットワーク及び情報システムの開発・保守等を発注する外部委託事業者及び外部委託事業者から再委託を受ける事業者に対して、情報セキュリティポリシー等のうち外部委託事業者等が守るべき内容の遵守及びその機密事項が説明されているか確かめる。	3.5.1.(4)	6.2.3	・再委託は原則禁止であるが、例外的に再委託を認める場合には、再委託先の業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認した上で許可しなければならない。 ・外部委託事業者に対して、契約の遵守等について必要に応じ立ち入り検査を実施すること。 ・外部委託に関する事項ついては、No.284～288も関連する項目であることから参考にする
	5.2. 研修・訓練	(1) 情報セキュリティに関する研修・訓練	32	○	**ⅱ）情報セキュリティ研修・訓練の実施** 最高情報統括責任者によって、定期的にセキュリティに関する研修・訓練が実施されている。	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、定期的に情報セキュリティに関する研修・訓練が実施されているか確かめる。	3.5.2.(1)	8.2.2	
	5.3. 事故、欠陥等の報告		33	○	**ⅰ）情報セキュリティ事故等の報告手順** 統括情報セキュリティ責任者によって、情報セキュリティに関する事故、システム上の欠陥及び誤作動を発見した場合の報告手順が定められ、文書化されている。	□情報セキュリティ事故等報告手順	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等が情報セキュリティに関する事故、システム上の欠陥及び誤作動を発見した場合、又は住民等外部からの事故等の報告を受けた場合の報告ルート及びその方法が文書化され、正式に承認されているか確かめる。	3.5.3.(1) ～(3)	13.1.1 13.1.2	・報告ルートは、団体の意思決定ルートと整合していることが重要である。
		(1) 庁内からの事故等の報告	34	○	**ⅰ）庁内からの情報セキュリティ事故等の報告** 庁内で情報セキュリティに関する事故、システム上の欠陥及び誤作動が発見された場合、報告手順に従って関係者に報告されている。	□情報セキュリティ事故等報告手順 □情報セキュリティ事故等報告書	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、職員等へのインタビューにより、報告手順に従って遅滞なく報告されているか確かめる。	3.5.3.(1)	13.1.1 13.1.2	
	5.4. ID及びパスワード等の管理	(1) ICカード等の取扱い	35	○	**ⅲ）認証用ＩＣカード等の放置禁止** 認証用ICカード等を業務上必要としないときは、カードリーダーやパソコン等の端末のスロット等から抜かれている。	□ICカード等取扱基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビュー及び執務室の視察により、業務上不要な場合にカードリーダーやパソコン等の端末のスロット等から認証用のICカードやUSBトークンが抜かれているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.4.(1) (ｱ)②	11.2.1 11.5.2	
			36	○	**ⅳ）認証用ＩＣカード等の紛失時手続** 認証用ICカード等が紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせている。	□ICカード等取扱基準 □ICカード紛失届書	監査証拠のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンが紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせているか確かめる。	3.5.4.(1) (ｱ)③	11.2.1 11.5.2	
			37	○	**ⅴ）認証用ＩＣカード等の紛失時対応** 認証用ICカード等の紛失連絡があった場合、統括情報セキュリティ責任者及び情報システム管理者によって、当該ICカード等の不正使用を防止する対応がとられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、紛失した認証用のICカードやUSBトークンを使用したアクセス等が速やかに停止されているか確かめる。	3.5.4.(1) (ｲ)	11.2.1 11.5.2	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			38	○	**vi）認証用IＣカード等の回収及び廃棄** ICカード等を切り替える場合、統括情報セキュリティ責任者及び情報システム管理者によって、切替え前のカードが回収され、不正使用されないような措置が講じられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンを切り替える場合に切替え前のICカードやUSBトークンが回収され、破砕するなど復元不可能な処理を行った上で廃棄されているか確かめる。	3.5.4.(1) (ウ)	11.2.1 11.5.2	・回収時の個数を確認し、紛失・盗難が発生していないか確実に確認することが望ましい。
		(3) パスワードの取扱い	39	○	**ii）パスワードの取扱い** 職員等のパスワードは当該本人以外に知られないように取扱われている。	□パスワード管理基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、職員等のパスワードについて照会等に応じたり、メモに記録したり、他人が容易に想像できるような文字列に設定したりしないように取扱われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.4.(3) ①～③	11.3.1	・最短6文字以上で、次の条件を満たしていることが望ましい。 ①覚えやすいこと ②当人の関連情報（例えば名前、電話番号、誕生日等）から、他の者が容易に推測できる事項又は容易に得られる事項に基づかないこと。 ③連続した同一文字又は数字だけ若しくはアルファベットだけの文字列でないこと。
			40	○	**iii）パスワードの不正使用防止** パスワードが流出したおそれがある場合、不正使用されない措置が講じられている。	□パスワード管理基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、パスワードが流出したおそれがある場合、速やかに情報セキュリティ管理者に報告され、パスワードが変更されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.4.(3) ④	11.3.1	
			41	○	**iv）パスワードの定期的な変更** パスワードが定期的に変更されている。	□パスワード管理基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、パスワードが定期的に、又はアクセス回数に基づいて変更されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.4.(3) ⑤	11.3.1	・機密性の非常に高い情報資産を取扱う情報システムのパスワードは、古いパスワードを再利用させないことが望ましい。
			42	○	**vii）パスワード記憶機能の利用禁止** パソコン等の端末のパスワード記憶機能が利用されていない。	□パスワード管理基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビュー、執務室の視察により、パソコン等の端末のパスワード記憶機能が利用されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.5.4.(3) ⑧	11.3.1	
6. 技術的セキュリティ	6.1. コンピュータ及びネットワークの管理	(1) 文書サーバの設定等	43	○	**iii）文書サーバの構成** 情報システム管理者によって、文書サーバが課室等の単位で構成され、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように設定されている。	□文書サーバ設定基準	監査証拠のレビューと情報システム管理者へのインタビュー及びパソコン等の端末からの操作により、文書サーバが課室等の単位で構成され、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように設定されているか確かめる。	3.6.1.(1) ②	11.1.1 11.4.7 11.6.1	
			44	○	**iv）文書サーバのアクセス制御** 情報システム管理者によって、特定の職員等しか取扱えないデータについて、担当外の職員等が閲覧及び使用できないような措置が講じられている。	□文書サーバ設定基準	監査証拠のレビューと情報システム管理者へのインタビュー及びパソコン等の端末からの操作により、住民の個人情報や人事記録といった特定の職員等しか取扱えないデータについて、担当外の職員等によって閲覧及び使用できないよう、別途ディレクトリを作成する等のアクセス制御が行われているか確かめる。	3.6.1.(1) ③	11.1.1 11.6.1	

項目	No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
(2) バックアップの実施	45	○	**ⅱ）バックアップの実施** 情報システム管理者によって、ファイルサーバ等に記録された情報について定期的なバックアップが実施され、バックアップ媒体が適切に保管されている。	□バックアップ基準 □バックアップ手順 □バックアップ実施記録 □リストア手順 □リストアテスト記録	監査証拠のレビューと情報システム管理者へのインタビュー及び管理区域あるいは執務室の視察により、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、必要に応じて定期的にバックアップが実施されているか確認かめる。また、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、リストアテストによる検証が行われているか確かめる。	3.6.1.(2)	10.5.1	・サーバの二重化については、No.21～24も関連する項目であることから参考にすること。
(4) システム管理記録及び作業の確認	46	○	**ⅱ）情報システム運用の作業記録作成** 情報システム管理者によって、所管する情報システムの運用において実施した作業記録が作成されている。	□システム運用基準 □システム運用作業記録	監査証拠のレビューと情報システム管理者へのインタビューにより、所管する情報システムの運用において実施した作業記録が作成され、管理されているか確かめる。	3.6.1.(4) ①	10.10.4	
(5) 情報システム仕様書等の管理	47	○	**ⅱ）情報システム仕様書等の管理** 統括情報セキュリティ責任者又は情報システム管理者によって、情報システム仕様書等が管理されている。	□情報システム関連文書管理基準 □システム仕様書等 □プログラム仕様書等	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビュー及び管理区域の視察により、ネットワーク構成図、情報システム仕様書等の情報システム関連文書を業務上必要でない者からの閲覧や、紛失等がないよう、施錠したキャビネットへの保管やフォルダへのアクセス制限などによって管理されているか確かめる。	3.6.1.(5)	10.7.4	
(6) アクセス記録の管理取得等	48	○	**ⅱ）アクセス記録等の取得及び保存** 統括情報セキュリティ責任者及び情報システム管理者によって、各種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が取得され、保存されている。	□システム運用基準 □アクセス記録 □システム稼動記録 □障害時のシステム出力ログ	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、各種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が取得され、一定期間保存されているか確かめる。	3.6.1.(6) ①	10.10.1 10.10.2	
(7) 障害記録	49	○	**ⅱ）障害記録の保存** 統括情報セキュリティ責任者及び情報システム管理者によって、障害記録が記録され、保存されている。	□障害対応基準 □障害報告書 □障害時のシステム出力ログ	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題が記録され、適切に保存されているか確かめる。	3.6.1.(7)	10.10.3 10.10.5	
(8) ネットワークの接続制御、経路制御等	50	○	**ⅱ）ファイアウォール、ルータ等の設定** 統括情報セキュリティ責任者によって、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等が設定されている。	□ネットワーク設定基準 □ネットワーク構成図	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定しているか確かめる。	3.6.1.(8) ①	10.6.1 10.6.2	・設定の不整合とは、例えば、通信機器間で通信経路の設定や通信パケットの通過ルールに齟齬がある等の場合をいう。
	51	○	**ⅲ）ネットワークのアクセス制御** 統括情報セキュリティ責任者によって、ネットワークに適切なアクセス制御が施されている。	□ネットワーク設定基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施しているか確かめる。	3.6.1.(8) ②	10.6.1 10.6.2 11.4.1	

項目		No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
(10) 外部ネットワークとの接続制限等		52	○	**ⅱ）外部ネットワーク接続の申請及び許可** 情報システム管理者が所管するネットワークを外部ネットワークと接続する場合、最高情報統括責任者及び統括情報セキュリティ責任者から許可を得ている。	□外部ネットワーク接続基準 □外部ネットワーク接続手続 □外部ネットワーク接続申請書/承認書	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、情報システム管理者が所管するネットワークを外部ネットワークと接続する場合、最高情報統括責任者及び統括情報セキュリティ責任者から許可を得ているか確かめる。	3.6.1.(10) ①	11.4.1 11.4.6	
		53	○	**ⅴ）ファイアウォール等の設置** ウェブサーバ等をインターネットに公開している場合、統括情報セキュリティ責任者又は情報システム管理者によって、外部ネットワークとの境界にファイアウォール等が設置されている。	□ネットワーク管理基準 □通信回線敷設図 □結線図	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するため、外部ネットワークとの境界にファイアウォール等が設置されたうえで接続されているか確かめる。	3.6.1.(10) ④	11.4.5 11.4.6 11.4.7	
(11) 無線LAN及びネットワークの盗聴対策		54	○	**ⅱ）無線LAN利用時の暗号化及び認証技術の使用** 無線LANを利用する場合、統括情報セキュリティ責任者又は情報システム管理者によって、暗号化及び認証技術が使用されている。	□ネットワーク管理基準 □ネットワーク設計書	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、無線LANを利用する場合には解読が困難な暗号化及び認証技術が使用され、アクセスポイントへの不正な接続が防御されているか確かめる。	3.6.1.(11) ①	11.4.1 11.4.2 11.4.5	
(12) 電子メールのセキュリティ管理		55	○	**ⅱ）電子メール転送制限** 統括情報セキュリティ責任者によって、電子メールサーバによる電子メール転送ができないように設定されている。	□電子メール管理基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、権限のない者による外部から外部への電子メール転送（電子メールの中継処理）が行えないよう、電子メールサーバの設定が行われているか確かめる。	3.6.1.(12) ①	10.8.1 10.8.4	
(13) 電子メールの利用制限		56	○	**ⅵ）フリーメール、ネットワークストレージサービス等の使用禁止** ウェブで利用できるフリーメール、ネットワークストレージサービス等は使用されていない。	□電子メール利用基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、外部への不正な情報の持ち出し等を防止するため、ウェブで利用できるフリーメール、ネットワークストレージサービス等が使用されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(13) ⑤	10.8.1 10.8.4	
(15) 無許可ソフトウエアの導入等の禁止		57	○	**ⅱ）ソフトウエアの無断導入の禁止** パソコン等の端末に無断でソフトウエアが導入されていない。	□ソフトウエア導入基準/手続	監査証拠のレビューと情報システム管理者及び職員等へのインタビュー、パソコン等の端末の確認により、パソコン等の端末に許可なくソフトウエアが導入されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(15) ①	10.4.1	
		58	○	**ⅲ）ソフトウエア導入の申請及び許可** 業務上必要なソフトウエアがある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウエアが導入されている。	□ソフトウエア導入基準/手続 □ソフトウエア導入申請書/承認書	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、業務上必要なソフトウエアがある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウエアが導入されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(15) ②	10.4.1	
		59	○	**ⅳ）不正コピーソフトウエアの利用禁止** 不正にコピーされたソフトウエアは利用されていない。	□ソフトウエア導入基準/手続	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、不正にコピーされたソフトウエアが利用されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(15) ③	10.4.1 15.1.2	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(16) 機器構成の変更の制限	60	○	**ⅲ）機器の改造及び増設・交換の申請及び許可** 業務上パソコン等の端末に対し機器の改造及び増設・交換の必要がある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て行われている。	□端末構成変更基準/手続 □端末構成変更申請書/承認書	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、業務上パソコン等の端末に対し機器の改造及び増設・交換の必要がある場合、統括情報セキュリティ責任者及び情報システム管理者の許可を得て行われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(16) ②	10.1.2	
		(17) 無許可でのネットワーク接続の禁止	61	○	**ⅰ）ネットワーク接続の禁止** 統括情報セキュリティ責任者の許可なく、パソコン等の端末がネットワークに接続されていない。	□ネットワーク利用基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者及び職員等へのインタビュー、執務室及び管理区域の視察により、統括情報セキュリティ責任者の許可なく、職員等や外部委託事業者がパソコン等の端末をネットワークに接続していないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(17)	10.6.1	
		(18) 業務以外の目的でのウェブ閲覧の禁止	62	○	**ⅰ）業務以外の目的でのウェブ閲覧禁止** 業務以外の目的でウェブが閲覧されていない。	□ネットワーク利用基準	監査証拠のレビューと情報システム管理者及び職員等へのインタビューにより、業務以外の目的でウェブが閲覧されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.1.(18)	11.4.1 11.4.6	
6. 技術的セキュリティ	6.2. アクセス制御	(1) アクセス制御 (ア) アクセス制御	63	○	**ⅰ）アクセス制御に関わる方針及び基準** 統括情報セキュリティ責任者又は情報システム管理者によって、アクセス制御に関わる方針及び基準が定められ、文書化されている。	□アクセス制御方針 □アクセス管理基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、所管するネットワーク又は情報システムの重要度に応じたアクセス制御方針や、業務上の必要性や権限に応じた許可範囲等のアクセス管理基準が文書化され、正式に承認されているか確かめる。	3.6.2.(1) (ア)	11.1.1 11.2.1 11.2.2 11.2.3 11.2.4	・開発、運用等を外部委託しており、重要な情報資産へのアクセスを許可している場合は、アクセス制御方針やアクセス管理基準等に外部委託に関するアクセス制御の事項が記述されていることが望ましい。
		(1) アクセス制御 (イ) 利用者IDの取扱い	64	○	**ⅰ）利用者ＩＤの取扱に関わる手続** 統括情報セキュリティ責任者及び情報システム管理者によって、利用者IDの登録、変更、抹消等の取扱に関わる手続が定められ、文書化されている。	□利用者ID取扱手続 □利用者ID登録・変更・抹消申請書 □利用者ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、利用者IDの登録、変更、抹消等の取扱に関わる手続が文書化され、正式に承認されているか確かめる。	3.6.2.(1) (イ)①	11.2.1	
			65	○	**ⅱ）利用者ＩＤの登録・権限変更の申請** 業務上においてネットワーク又は情報システムにアクセスする必要あるいは変更が生じた場合、当該職員等によって、統括情報セキュリティ責任者又は情報システム管理者に当該利用者IDを登録又は権限を変更するよう申請されている。	□利用者ID登録・変更・抹消申請書 □利用者ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者及び職員等へのインタビューにより、ネットワーク又は情報システムにアクセスする業務上の必要あるいは権限変更が生じた場合、当該職員等によって、利用者IDの登録、権限変更を申請しているか確かめる。	3.6.2.(1) (イ)①	11.2.1	・単に利用者IDの登録及び変更の手続の有無を確認するのではなく、承認者の妥当性などを確認することが望ましい。
			66	○	**ⅲ）利用者ＩＤの抹消申請** 業務上においてネットワーク又は情報システムにアクセスする必要がなくなった場合、当該職員等によって、統括情報セキュリティ責任者又は情報システム管理者に当該利用者IDを抹消するよう申請されている。	□利用者ID登録・変更・抹消申請書 □利用者ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者及び職員等へのインタビューにより、ネットワーク又は情報システムにアクセスする業務上の必要がなくなった場合、当該職員等によって、利用者IDの抹消を申請しているか確かめる。	3.6.2.(1) (イ)②	11.2.1	・単に利用者IDの抹消の手続の有無を確認するのではなく、承認者の妥当性などを確認することが望ましい。
			67	○	**ⅳ）利用者ＩＤの点検** 統括情報セキュリティ責任者及び情報システム管理者によって、利用されていないIDが放置されてないか点検されている。	□利用者ID棚卸記録 □利用者ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、人事管理部門と連携し、利用者IDを定期的に棚卸して、必要のない利用者IDが登録されてないか、過剰なアクセス権限を付与していないかなどを定期的に点検しているか確かめる。	3.6.2.(1) (イ)③	11.2.4	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(1) アクセス制御 (ウ) 特権を付与されたIDの管理等	68	○	**ⅰ）特権I Dの取扱に関わる手続** 統括情報セキュリティ責任者及び情報システム管理者によって、管理者権限等の特権を付与されたIDの取扱に関わる手続が定められ、文書化されている。	□特権ID取扱手続 □特権ID認可申請書 □特権ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、管理者権限等の特権を付与されたIDの取扱に関わる手続が文書化され、正式に承認されているか確かめる。	3.6.2.(1) (ウ)	11.2.2	
			69	○	**ⅱ）特権I D及びパスワードの管理** 統括情報セキュリティ責任者及び情報システム管理者によって、特権IDを付与する者が必要最小限に制限され、当該ID及びパスワードが厳重に管理されている。	□特権ID取扱手続 □特権ID管理台帳	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、必要以上に特権IDを付与していないか、当該ID及びパスワードが厳重に管理されているか確かめる。	3.6.2.(1) (ウ)①	11.2.2	
			70	○	**ⅴ）特権I Dの外部委託事業者による管理の禁止** 統括情報セキュリティ責任者及び情報システム管理者によって、特権を付与されたID及びパスワードの変更を外部委託事業者には行わせていない。	□特権ID取扱手続	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、外部委託事業者に特権ID及びパスワードの変更を行わせていないか確かめる。	3.6.2.(1) (ウ)④	11.2.2	
		(2) 職員等による外部からのアクセス等の制限	71	○	**ⅰ）外部からのアクセスに関わる方針及び手続** 統括情報セキュリティ責任者によって、外部から内部のネットワーク又は情報システムにアクセスする場合の方針及び手続が定められ、文書化されている。	□リモートアクセス方針 □リモート接続手続	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、外部からのアクセスに関わる方針及び手続が文書され、正式に承認されているか確かめる。	3.6.2.(2)	11.4.1 11.4.2 11.7.1 12.3.1	
			72	○	**ⅱ）外部からのアクセスの申請及び許可** 外部から庁内ネットワークに接続する必要のある場合、当該職員等によって、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得ている。	□リモート接続許可申請書／許可書	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、職員等が外部から庁内ネットワークに接続する必要のある場合、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得ているか確かめる。	3.6.2.(2) ①	11.4.1	・外部からのアクセスを認める場合であっても、外部から庁内ネットワークに接続する必要性などを確認することが望ましい。
			73	○	**ⅳ）外部からのアクセス時の本人確認機能** 外部からのアクセスを認める場合、統括情報セキュリティ責任者によって、外部からのアクセス時の本人確認機能が設けられている。	□ネットワーク設計書 □システム設計書	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、外部からのアクセスを認める場合、本人確認機能が設けられているか確かめる。	3.6.2.(2) ③	11.4.2	
			74	○	**ⅵ）外部からのアクセス用端末のセキュリティ 確保** 外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、統括情報セキュリティ責任者及び情報システム管理者によって、セキュリティ確保の措置が講じられている。	□リ モート 接続手続	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保の措置が講じられているか確かめる。	3.6.2.(2) ⑤	11.7.1	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			75	○	**vii）外部から持ち込んだ端末のウイルス確認等** 外部から持ち込んだ端末を庁内ネットワークに接続する場合、当該職員等によって、接続前にコンピュータウイルスに感染していないことや、パッチの適用状況等が確認されている。	□端末接続時手続	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者及び職員等へのインタビューにより、外部から持ち込んだ端末を庁内ネットワークに接続する場合、接続前に当該端末がコンピュータウイルスに感染していないことや、セキュリティホールや不正プログラムに対する適切なパッチが適用されていることが確認されているか確かめる。	3.6.2.(2) ⑥	11.7.1	
		(5) パスワードに関する情報の管理	76	○	**ⅰ）パスワードファイルの管理** 統括情報セキュリティ責任者又は情報システム管理者によって、職員等のパスワードファイルが厳重に管理されている。	□アクセス制御方針 □アクセス管理基準	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、職員等のパスワードの暗号化やオペレーティングシステム等のセキュリティ強化機能等でパスワードファイルが厳重に管理されているか確かめる。	3.6.2.(5) ①	11.5.3	・職員等によるパスワードの取扱いについては、No.119～126も関連する項目であることから参考にすること。
	6.3. システム開発、導入、保守等	(1) 情報システムの調達	77	○	**ⅱ）セキュリティ機能の明記** 情報システムを調達する場合、統括情報セキュリティ責任者及び情報システム管理者によって、必要とする技術的なセキュリティ機能が調達仕様書に明記されている。	□調達仕様書	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、情報システム開発、導入、保守等の調達にあたり、アクセス制御機能やパスワード設定機能、ログ取得機能、データ暗号化等、必要とする技術的なセキュリティ機能が調達仕様書に明記されているか確かめる。	3.6.3.(1) ①	12.1.1 12.5.5	
		(2) 情報システムの開発	78	○	**ⅱ）システム開発における責任者及び作業者の特定** 情報システム管理者によって、システム開発の責任者及び作業者が特定されている。	□システム開発体制図	監査証拠のレビューと情報システム管理者へのインタビューにより、システム開発の責任者及び作業者が特定されているか確かめる。	3.6.3.(2) (ア)	12.1.1 12.5.5	
			79	○	**ⅳ）システム開発の責任者及び作業者のアクセス権限設定** 情報システム管理者によって、システム開発の責任者及び作業者のアクセス権限が設定されている。	□アクセス権限設定書 □開発用ID管理台帳	監査証拠のレビューと情報システム管理者へのインタビューにより、システム開発の責任者及び作業者のアクセス権限が設定されているか確かめる。	3.6.3.(2) (イ)②	11.1.1 11.2.1 11.2.2 12.4.3	
		(3) 情報システムの導入 (イ) テスト	80	○	**ⅰ）導入前のテスト実施** 新たに情報システムを導入する場合、情報システム管理者によって、既に稼動している情報システムに接続する前に十分な試験が行われている。	□システムテスト計画書／報告書	監査証拠のレビューと情報システム管理者へのインタビューにより、新たに情報システムを導入する場合、既に稼動している情報システムに接続する前に十分な試験が行われているか確かめる。	3.6.3.(3) (イ)①	10.3.2	
			81	○	**ⅲ）個人情報及び機密性の高い生データの使用禁止** 個人情報及び機密性の高い生データは、テストデータとして使用されていない。	□システムテスト計画書／報告書 □ユーザテスト計画書／報告書	監査証拠のレビューと情報システム管理者へのインタビューにより、個人情報及び機密性の高い生データを、テストデータとして使用していないか確かめる。	3.6.3.(3) (イ)③	10.3.2 12.4.2	
		(4) システム開発・保守に関連する資料等の保管	82	○	**ⅱ）資料等の保管** 情報システム管理者によって、システム開発・保守に関連する資料及び文書が適切に保管されている。	□システム開発基準 □システム仕様書等 □プログラム仕様書等	監査証拠のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、ファイルサーバ等の確認により、システム開発・保守に関連する資料及び文書が紛失したり改ざん等されないように保管されているか確かめる。	3.6.3.(4) ①	10.7.4	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			83	○	**iii）テスト結果の保管** 情報システム管理者によって、テスト結果が一定期間保管されている。	□システム開発基準 □システムテスト計画書／報告書	監査証拠のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、ファイルサーバ等の確認により、テスト結果が一定期間保管されているか確かめる。	3.6.3.(4) ②	10.7.4	
			84	○	**iv）ソースコードの保管** 情報システム管理者によって、情報システムに係るソースコードが適切に保管されている。	□システム開発基準 □ソースコード	監査証拠のレビューと情報システム管理者へのインタビュー又は管理区域及び執務室の視察、サーバ等の確認により、情報システムに係るソースコードが誤消去や改ざん等されないような方法で保管されているか確かめる。	3.6.3.(4) ③	12.4.3	
		(6) 情報システムの変更管理	85	○	**ii）変更履歴の作成** 情報システム管理者によって、情報システムを変更した場合、プログラム仕様書等の変更履歴が作成されている。	□システム開発基準 □システム仕様書等 □プログラム仕様書等	監査証拠のレビューと情報システム管理者へのインタビューにより、情報システムを変更した場合、システム仕様書やプログラム仕様書等の変更履歴が作成されているか確かめる。	3.6.3.(6)	10.1.2 12.5.1	
6. 技術的セキュリティ	6.4. 不正プログラム対策		86	○	**i）不正プログラム対策に関わる基準及び手順** 統括情報セキュリティ責任者及び情報セキュリティ責任者によって、不正プログラム対策に関わる基準及び手順が定められ、文書化されている。	□不正プログラム対策基準 □不正プログラム対策手順	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、不正プログラム対策に関わる基準及び手順が文書化され、正式に承認されているか確かめる。	3.6.4.	10.4.1 10.4.2 12.6.1	
		(1) 統括情報セキュリティ責任者の措置事項	87	○	**v）パターンファイルの更新** 統括情報セキュリティ責任者によって、不正プログラム対策ソフトウエアのパターンファイルが最新のパターンファイルに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフトウエアのログ	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビュー、サーバ及びパソコン等の確認により、不正プログラム対策ソフトウエアのパターンファイルが最新のパターンファイルに更新されているか確かめる。	3.6.4.(1) ⑤	10.4.1 10.4.2 12.6.1	
			88	○	**vi）不正プログラム対策ソフトウエアの更新** 統括情報セキュリティ責任者によって、不正プログラム対策ソフトウエアが最新のバージョンに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフトウエアのログ	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビュー、サーバ及びパソコン等の確認により、導入された不正プログラム対策ソフトウエアが最新のバージョンに更新されているか確かめる。	3.6.4.(1) ⑥	10.4.1 10.4.2 12.5.1 12.6.1	
		(2) 情報システム管理者の措置事項	89	○	**ii）パターンファイルの更新** 情報セキュリティ管理者によって、不正プログラム対策ソフトウエアのパターンファイルが最新のパターンファイルに更新されている。	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフトウエアのログ	監査証拠のレビューと情報システム管理者へのインタビュー、サーバ及びパソコン等の確認により、不正プログラム対策ソフトウエアのパターンファイルが最新のパターンファイルに更新されているか確かめる。	3.6.4.(2) ②	10.4.1 10.4.2 12.6.1	
		(3) 職員等の遵守事項	90	○	**ii）データ等取り入れ時のチェック** 外部からデータ又はソフトウエアを取り入れる場合、職員等によって、不正プログラム対策ソフトウエアによるチェックが行われている。	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフトウエアのログ	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部からデータ又はソフトウエアを取り入れる場合、不正プログラム対策ソフトウエアによるチェックが行われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.4.(3) ②	10.4.1 10.4.2 10.8.1	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			91	○	**iii）出所不明なファイルの削除** 差出人不明又は不自然に添付されたファイルを受信した場合、職員等によって、速やかに削除されている。	□電子メール利用基準 □不正プログラム対策基準 □不正プログラム対策手順	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が差出人不明又は不自然に添付されたファイルを受信した場合、速やかに削除されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.4.(3) ③	10.4.1 10.4.2 10.8.1	
			92	○	**iv）不正プログラム対策ソフトウエアによるフルチェックの定期的実施** 職員等の使用する端末に対して、職員等によって、不正プログラム対策ソフトウエアによるフルチェックが定期的に実施されている。	□不正プログラム対策基準 □不正プログラム対策手順 □不正プログラム対策ソフトウエアのログ	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等の使用する端末に対して、不正プログラム対策ソフトウエアによるフルチェックが定期的に実施されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.4.(3) ④	10.4.1 10.4.2	
			93	○	**vii）不正プログラムに感染した場合の対処** 不正プログラムに感染した場合、職員等によって、LANケーブルの即時取外し又は機器の電源が遮断されている。	□不正プログラム対策基準 □不正プログラム対策手順 □情報セキュリティ事故等報告書	監査証拠のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、不正プログラムに感染した場合、LANケーブルの即時取外し又は機器の電源が遮断されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	3.6.4.(3) ⑦	13.2.1	・侵害時の対応についてはNo.280～283も関連する項目であることから参考にすること。
6. 技術的セキュリティ	6.6. セキュリティ情報の収集	(1) セキュリティホールに関する情報の収集・共有及びソフトウエアの更新等	94	○	**ii）ソフトウエアの更新** 統括情報セキュリティ責任者及び情報システム管理者によって、セキュリティホールの緊急度に応じてパッチが適用され、ソフトウエアが更新されている。	□パッチ適用情報 □パッチ適用記録	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、セキュリティホールの緊急度に応じてパッチが適用され、ソフトウエアが更新されているか確かめる。	3.6.6.(1)	12.6.1	
7. 運用	7.1. 情報システムの監視		95	○	**iv）外部接続システムの常時監視** 統括情報セキュリティ責任者及び情報システム管理者によって、外部と常時接続するシステムが常時監視されている。	□システム運用基準 □監視記録	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、外部と常時接続するシステムが常時監視されているか確かめる。	3.7.1.③	10.2.2 10.10.2	
	7.2. 情報セキュリティポリシーの遵守状況の確認	(1) 遵守状況の確認及び対処	96	○	**iii）発生した問題への対処** 最高情報統括責任者によって、情報セキュリティポリシー遵守上の問題に対して、適切かつ速やかに対処されている。	□情報セキュリティ事故等報告手順 □情報セキュリティ事故等報告書	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、最高情報統括責任者に報告された情報セキュリティポリシー遵守上の問題に対して、適切かつ速やかに対処されているか確かめる。	3.7.2.(1) ②	13.2.1 15.2.1	

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
			97	○	**ⅳ）システム設定等における情報セキュリティポリシーの遵守状況の確認及び問題発生時の対処** 統括情報セキュリティ責任者及び情報システム管理者によって、システム設定等における情報セキュリティポリシーの遵守状況について定期的に確認が行われ、問題が発生していた場合には適切かつ速やかに対処されている。	□情報セキュリティポリシー □システム運用基準 □情報セキュリティ事故等報告手順 □情報セキュリティ事故等報告書 □自己点検実施基準 □自己点検結果	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について定期的に確認が行われ、問題が発生していた場合には適切かつ速やかに対処されているか確かめる。	3.7.2.(1) ③	13.1.1 13.1.2 13.2.1 15.2.2	
		(3) 職員等の報告義務	98	○	**ⅱ）情報セキュリティポリシー違反発見時の報告** 情報セキュリティポリシーに対する違反行為が発見された場合、職員等によって、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告されている。	□情報セキュリティ事故等報告手順 □情報セキュリティ事故等報告書	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ管理者、職員等へのインタビューにより、情報セキュリティポリシーに対する違反行為が発見された場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告されているか確かめる。	3.7.2.(3) ①	13.2.1	
			99	○	**ⅲ）発見された違反行為に対する対処** 情報セキュリティポリシーに対する違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合、統括情報セキュリティ責任者によって、緊急時対応計画に従った対処が行われている。	□情報セキュリティ事故等報告手順 □情報セキュリティ事故等報告書 □緊急時対応計画	監査証拠のレビューと統括情報セキュリティ責任者及び情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーに対する違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合、緊急時対応計画に従った対処が行われているか確かめる。	3.7.2.(3) ②	13.2.1	・緊急時対応計画については、No.280～283も関連する項目であることから参考にすること。
	7.3. 侵害時の対応	(1) 緊急時対応計画の策定	100	○	**ⅱ）緊急時対応計画の策定** 情報セキュリティ委員会によって、緊急時対応計画が定められている。	□緊急時対応計画 □情報セキュリティ委員会議事録	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、緊急時対応計画が定められているか確かめる。	3.7.3.(1)(2)	13.2.1 14.1.3	
	7.4. 外部委託	(1) 外部委託先の選定基準	101	○	**ⅰ)外部委託事業者の選定基準** 情報セキュリティ管理者によって、外部委託先選定の際、委託内容に応じた情報セキュリティ対策が確保されていることが確認されている。	□外部委託選定基準 □サービス仕様書(サービスカタログ)	監査証拠のレビューと情報セキュリティ管理者へのインタビューにより、外部委託先選定の際、委託内容に応じた情報セキュリティ対策が確保されていることを確認しているか確かめる。	3.7.4.(1) ①	6.2.1 10.2.1 12.5.5	・外部委託選定基準には、「コンプライアンスに関してその管理体制、教育訓練等の対策が取られ、従業員が理解しているか」、「委託業務内容に即した技術、要員が確保されているか」などの項目が含まれていることが望ましい。

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(2) 契約項目	102	○	**ⅰ)外部委託事業者との契約** 情報システムの開発あるいは運用等を外部委託する場合、外部委託事業者との間で締結される契約書に、必要に応じた情報セキュリティ要件が明記されている。	□業務委託契約書	監査証拠のレビューと情報セキュリティ責任者又は情報システム管理者へのインタビューにより、外部委託事業者との間で締結される契約書に必要に応じて次の情報セキュリティ要件が明記されているか確かめる。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 綴委託先の責任者、委託内容、終業者、終業場所の特定 ・提供されるサービスレベルの保証 ・従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 綴業務上終り得た情報の守秘義務 綴終委託に関する制限事項の遵守 綴委託業務終了時の情報資産の返還、廃棄等 綴委託業務の定終報告及び緊急時報告義務 綴委託終団体による監査、検査 綴委託終団体による事故時等の公表 ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)等	3.7.4.(2)	6.2.3	・再委託は原則禁止であるが、例外的に再委託を認める場合には、再委託先の業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認した上で許可しなければならない。 ・契約書において、再委託先の監督についても規定されていることが望ましい。
	7.4. 外部委託	(3) 確認・措置等	103	○	**ⅰ)外部委託事業者のセキュリティ対策の確認と報告** 情報セキュリティ管理者によって、外部委託事業者におけるセキュリティ対策の確保が確認され、必要に応じ業務委託契約に基づく措置が講じられている。また、確認した内容が統括情報セキュリティ責任者に報告され、さらにその重要度に応じて最高情報統括責任者に報告されている。	□外部委託管理基準 □作業報告書 □改善要望書 □改善措置実施報告書	監査証拠のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、外部委託事業者においてセキュリティ対策が確保されているか定期的に確認され、必要に応じ業務委託契約に基づいた改善要求等の措置が講じられているか確かめる。また、確認された内容が統括情報セキュリティ責任者に報告され、さらにその重要度に応じて最高情報統括責任者に報告されているか確かめる。	3.7.4.(3)	10.2.2 10.2.3	・外部委託事業者の情報セキュリティポリシー等の遵守事項については、No.93～94も関連する項目であることから参考にすること。 ・契約事項の遵守状況の他、十分なセキュリティ対策がとられていることを確認する必要があり、特に、再委託の制限、情報の持ち出しの禁止、業務終了後のデータの返還・廃棄、私物パソコンの使用について、違反がないか確認することが必要である。

項目			No.	必須	監査項目	監査証拠の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
	7.5. 例外措置	(1) 例外措置の許可	104	○	**ⅰ)例外措置の申請及び許可** 情報セキュリティ関係規定の遵守が困難な状況で行政事務の適正な遂行を継続しなければならない場合、情報セキュリティ管理者及び情報システム管理者によって、最高情報統括責任者の許可を得たうえで例外措置が取られている。	□例外措置申請書/許可書 □例外措置実施報告書	監査証拠のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、情報セキュリティ関係規定の遵守が困難な状況で行政事務の適正な遂行を継続しなければならない場合、遵守事項とは異なる方法を採用すること又は遵守事項を実施しないことについて合理的な理由がある場合に限り、最高情報統括責任者の許可を得たうえで例外措置が取られているか確かめる。	3.7.5.(1)	6.1.2	
		(2) 緊急時の例外措置	105	○	**ⅰ)緊急時の例外措置** 行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、情報セキュリティ管理者及び情報システム管理者によって、事後速やかに最高情報統括責任者に報告されている。	□例外措置実施報告書	監査証拠のレビューと情報セキュリティ管理者又は情報システム管理者へのインタビューにより、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、例外措置実施後速やかに最高情報統括責任者に報告されているか確かめる。	3.7.5.(2)	6.1.2	
	7.7. 懲戒処分等	(1) 懲戒処分	106	○	**ⅰ) 懲戒処分の対象** 統括情報セキュリティ責任者によって、情報セキュリティポリシーに違反した職員等及びその監督責任者が地方公務員法による懲戒処分の対象となることが定められ、文書化されている。	□情報セキュリティポリシー	監査証拠のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーに違反した職員等及びその監督責任者が、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象となることが文書化され、正式に承認されているか確かめる。	3.7.7.(1)	8.2.3	
8. 評価・見直し	8.2. 自己点検	(1) 実施方法	107	○	**ⅰ)ネットワーク及び情報システムに関わる自己点検の実施** 統括情報セキュリティ責任者及び情報システム管理者によって、所管するネットワーク及び情報システムについて、定期的又は必要に応じて自己点検が行われている。	□自己点検実施計画 □自己点検結果報告書	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、所管するネットワーク及び情報システムについて、定期的又は必要に応じて自己点検が行われているか確かめる。	3.8.2.(1) ①	15.2.1 15.2.2	
			108	○	**ⅱ)各部局の自己点検の実施** 情報セキュリティ責任者及び情報セキュリティ管理者によって、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度又は必要に応じて自己点検が行われている。	□自己点検実施計画 □自己点検結果報告書	監査証拠のレビューと情報セキュリティ責任者又は情報セキュリティ管理者へのインタビューにより、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度又は必要に応じて自己点検が行われているか確かめる。	3.8.2.(1) ②	15.2.1 15.2.2	
		(2) 報告	109	○	**ⅰ)自己点検結果の報告** 統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者によって、自己点検結果と自己点検結果に基づく改善策が取りまとめられ、情報セキュリティ委員会に報告されている。	□自己点検結果報告書 □改善計画 □情報セキュリティ委員会議事録	監査証拠のレビューと統括情報セキュリティ責任者又は情報システム管理者及び情報セキュリティ責任者へのインタビューにより、自己点検結果と自己点検結果に基づく改善策が取りまとめられ、情報セキュリティ委員会に報告されているか確かめる。	3.8.2.(2)	6.1.2 15.2.1 15.2.2	
	8.3. 情報セキュリティポリシーの見直し		110	○	**ⅱ)情報セキュリティポリシーの見直し** 情報セキュリティ委員会によって、情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシーの見直しが行われている。	□情報セキュリティポリシー □情報セキュリティ委員会議事録 □職員等への周知記録	監査証拠のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティ委員会において、情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況の変化等をふまえ、必要に応じて情報セキュリティポリシーの見直しが行われているか確かめる。また、見直された場合に、その内容が職員等や外部委託事業者に周知されているか確かめる。	3.8.3.	5.1.2	

7　個別システムの概要　（平成２２年3月３１日現在）

No.	システム名	所属	業務概要等	機器構成	稼動年度
1	ＤＴＰ	広報課	広報紙等編集作業	パソコン 6 台	平成 13
2	ホームページ保守	広報課	ホームページ保守	パソコン 3 台	平成 13
3	ＣＭＳ	広報課	ホームページコンテンツの作成・管理	サーバー1 台、パソコン 1 台	平成 19
4	区政情報コーナー蔵書管理	広報課	図書管理、貸出管理	パソコン 1 台	平成 14
5	大型情報ディスプレイ	広報課	ロビーでのフロア配置・区議会日程等の案内	パソコン 8 台	平成 14
6	広聴	広報課	広聴案件処理データベース	サーバー1 台、端末は庁内イントラネットパソコン利用	平成 17
7	庁内イントラネット	情報課	庁内イントラネット・システム、グループウエア	サーバー9 台、パソコン 1866 台	平成 15
8	ＬGWAN	情報課	ＬGWAN制御	サーバー1 台、サービス提供設備１台	平成 16
9	電子申請	情報課	電子申請（東京電子自治体共同運営システム利用）	庁内イントラネットパソコン利用	平成 16
10	内部情報システム	情報課	内部情報システム（文書管理、庶務事務、財務情報、共通基盤）	サーバー14 台及びパソコン 10 台端末は庁内イントラネットパソコン利用	平成 19
11	例規集データベース	総務課	例規集データベース	サーバー1 台、端末は庁内イントラネットパソコン利用	平成 16
12	男女平等センター資料室蔵書管理	人権政策課	蔵書管理、新着案内・ホームページ作成	パソコン 1 台	平成 6
13	男女平等センター資料室貸出管理	人権政策課	貸出・返却管理	パソコン 1 台	平成 15
14	人事給与	人事課	人事管理、給与計算	サーバー3 台、パソコン 6 台	平成 19
15	研修情報	人事課	研修情報処理	パソコン 1 台	平成 13
16	健康管理支援	人事課	健康管理支援	サーバー1 台、パソコン 1 台	平成 19
17	公共料金	契約課	公共料金領収書管理	パソコン 1 台	平成 17
18	電子調達	契約課	業者登録、電子入札（東京電子自治体共同運営システム利用）	サーバー1 台、パソコン 1 台	平成 16
19	施設保全管理	施設課	ＣＡＤ設計図作成、施設データ作成	サーバー1 台、パソコン 18 台	平成 6
20	災害情報	防災課	罹災情報管理、備蓄物資・街頭消火器管理	サーバー3 台、パソコン 17 台	平成 10

No.	システム名	所属	業務概要等	機器構成	稼動年度
21	啓発用機器制御	防災課	地震の学習館啓発用機器の制御	パソコン 5 台	平成 10
22	緊急地震速報	防災課	気象業務支援センターから受け取る地震情報の周知	パソコン 2 台、送信機 5 台・受信機 75 台	平成 19
23	統計調査支援	地域振興課	指定統計調査に係る調査員管理・調査区管理	パソコン 2 台	平成 13
24	地方税ポータルシステム（エルタックス）審査システム	税務課	給与支払報告書、所得税申告書の電子データの提出・受領	パソコン 1 台	平成 21
25	コンビニ収納	国保年金課	コンビニ収納の収納金管理	パソコン 1 台	平成 16
26	特定健診等データ管理	国保年金課	特定健診等データ管理	パソコン 3 台	平成 20
27	国保収納推進員	国保年金課	保険料未納者情報による訪問事務	パソコン 3 台	平成 13
28	画像レセプト情報管理	国保年金課	国保連合の画像レセプト情報管理システム利用端末	パソコン 6 台	平成 17
29	国保調整交付金事業報告	国保年金課	国保事業の国都支出金・年報・報告	パソコン 1 台	平成 5
30	後期高齢者医療広域連合電算処理システム	国保年金課	後期高齢者医療広域連合電算処理	パソコン 5 台	平成 19
31	中小企業融資	産業経済課	中小企業融資管理	パソコン 2 台	平成 3
32	東京都中小企業総合支援	産業経済課	中小企業の仕事の受発注斡旋	パソコン 1 台	平成 3
33	消費者相談情報直接入力	産業経済課	消費者相談受付事務、消費者相談情報入力	パソコン 4 台	平成 16
34	消費者相談情報検索	産業経済課	消費者相談情報検索サービス	パソコン 1 台	平成 3
35	消費生活センターインターネット検索	産業経済課	消費生活センターインターネット	パソコン 1 台	平成 13
36	企業情報検索	産業経済課	企業情報提供用	パソコン 2 台	平成 19
37	中小企業センターIT講習用	産業経済課	中小企業向け IT 講習用	サーバー1 台、パソコン 21 台	平成 21
38	公的個人認証サービス	戸籍住民課	公的個人認証サービス	パソコン 1 台、登録専用機 1 台	平成 15
39	CS ログ管理	戸籍住民課	CS サーバーのログ管理	パソコン 1 台	平成 15
40	戸籍住民証明発行集計	戸籍住民課	戸籍住民証明発行集計、レジ集計	パソコン 1 台	平成 14
41	戸籍事務	戸籍住民課	戸籍事務	サーバー4 台 パソコン 16 台	平成 19
42	集会施設予約	東部地区サービス事務所	集会施設予約事務	サーバー2 台、パソコン 97 台	平成 18
43	保健福祉情報	健康福祉計画課	福祉事務処理	サーバー2 台、パソコン 34 台	平成 10
44	特定健康診査・がん検診受診状況管理	健康推進課	がん検診・医療機関名簿管理、生活改善指導者データ管理	サーバー 1 台、パソコン 3 台	平成 13

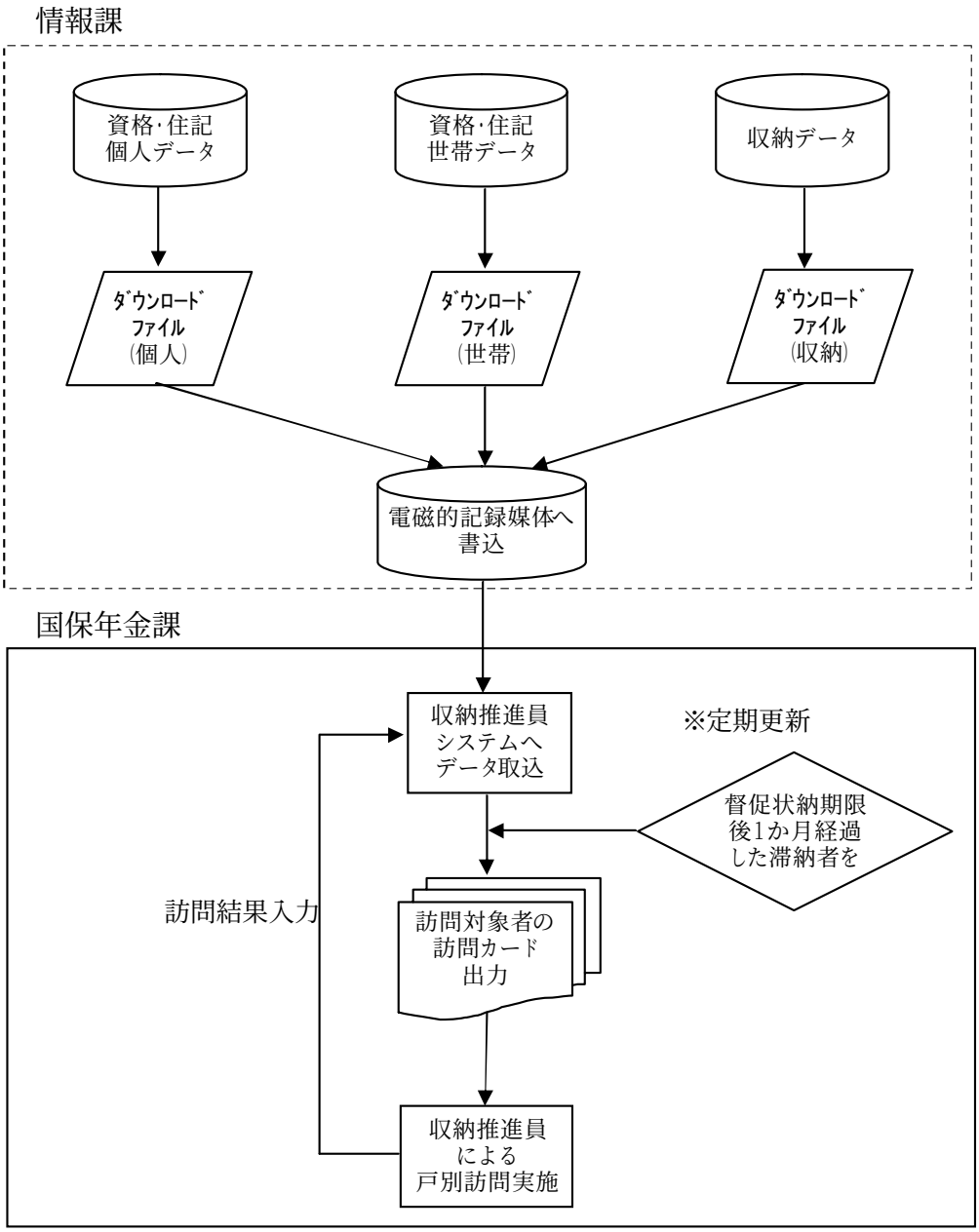
No.	システム名	所属	業務概要等	機器構成	稼動年度
45	栄養表示推進事業	健康推進課	飲食店等のメニューの栄養成分計算	パソコン 1 台	平成 12
46	公害補償・大気汚染	健康推進課	公害補償認定・給付事務、大気汚染申請・認定情報データベース	サーバー1 台、パソコン 4 台	平成 13
47	食品衛生台帳管理	生活衛生課、碑文谷保健センター	食品衛生事業者等の情報管理	サーバー1 台、パソコン 5 台	平成 4
48	食品保健総合	生活衛生課	厚生労働省に接続し報告等（ＷＩＳＨ）	パソコン 1 台	平成 10
49	犬登録管理・給水施設管理	生活衛生課	狂犬病予防法の犬台帳管理、水道法の施設台帳管理	パソコン 1 台	平成 7
50	給水台帳管理・井戸台帳管理	生活衛生課	水道法の施設台帳管理	パソコン 1 台（犬登録管理・給水施設管理と兼用）	平成 13
51	Ｘ線デジタル画像処理	保健予防課、碑文谷保健センター	胸部Ｘ線撮影の画像データ処理	サーバー1 台、パソコン９台	平成 15
52	結核登録者情報システム	保健予防課	結核感染者情報の登録と情報送信（厚生労働省・東京都・他自治体）	パソコン 1 台	平成 18
53	検査機器温度管理	碑文谷保健センター	検査用恒温機器の温度管理	パソコン 1 台（食品衛生台帳管理と兼用）	平成 13
54	包括支援業務支援システム	地域ケア推進課	地域包括支援センターへの行政情報の提供および書面伝送	サーバー1 台、パソコン 16 台	平成 21
55	介護保険	介護保険課	介護保険被保険者資格管理、保険料納付管理、受給者管理、給付実績管理	サーバー6 台、パソコン 38 台	平成 11
56	認定支援ネットワーク	介護保険課	認定情報送信（厚生労働省・東京都）	パソコン 1 台	平成 11
57	国保連伝送	介護保険課	国保連受給者情報交換	パソコン 1 台	平成 14
58	特別養護老人ホーム入所調整	高齢福祉課	特別養護老人ホーム入所調整	パソコン 1 台	平成 13
59	福祉工房利用者用	障害福祉課	福祉工房製品作成、機関紙編集	パソコン 4 台	平成 14
60	支援費システムパンチ入力用	障害福祉課	支援費システムパンチ入力用	パソコン 1 台	平成 16
61	障害区分判定	障害福祉課	自立支援法対応障害区分判定資料作成、対象者管理	パソコン 1 台	平成 17
62	障害者自立支援給費等請求	障害福祉課	障害者自立支援給費等請求事務	パソコン 4 台	平成 19
63	栄養計算	障害福祉課	栄養計算（すくすくのびのび園）	パソコン 1 台	平成 16
64	生活保護	生活福祉課	生活保護法施行に要する一般事務、生活保護法外の援護事務全般	サーバー5 台、パソコン 47 台	平成 3
65	中国残留邦人支援給付	生活福祉課	中国残留邦人支援給付に要する一般事務、法外の援護事務全般	サーバー1 台(端末は生活保護システムと兼用)	平成 20

No.	システム名	所属	業務概要等	機器構成	稼動年度
66	私立幼稚園補助金	子育て支援課	私立幼稚園補助金業務支援	パソコン 1 台	平成 16
67	学童保育料管理	子育て支援課	学童保育料管理	パソコン 2 台	平成 16
68	児童扶養手当管理	子育て支援課	児童扶養手当事務	パソコン 1 台	平成 12
69	奨学資金管理システム	子育て支援課	奨学資金貸付・償還管理	パソコン 1 台	平成 21
70	子育てポータルサイト入力用	子ども政策課	子育てポータルサイト（めぐろ子ども・子育てネット）入力用	パソコン 1 台	平成 19
71	保育所入所管理	保育課	保育所入所管理	サーバー1 台、パソコン 8 台	平成 20
72	都市計画用ＧＩＳ	都市計画課	都市計画業務 GIS	パソコン 2 台	平成 15
73	道路管理	道路管理課	道路占用許可事務、道路工事調整事務	パソコン 2 台	平成 3
74	道路管理支援	道路管理課、都市整備課	道路台帳現況平面図・土地境界確定図等閲覧及び証明書作成	サーバー1 台、パソコン 4 台	平成 18
75	駐輪場管理	道路管理課	駒場東大前駅外５駐輪場管理	パソコン 6 台	平成 10
76	駐輪場管理監視	道路管理課	自由が丘駅南口駐輪場場内管理	パソコン 1 台	平成 20
77	放置自転車撤去台帳	道路管理課	放置自転車撤去事務	パソコン 5 台	平成 19
78	水位情報	土木工事課	水位情報監視	パソコン 1 台	平成 16
79	水防監視	土木工事課	雨量・水位データの収集	サーバー2 台、パソコン 5 台	平成 2
80	気象情報提供	土木工事課	ウェザーニュースからの気象情報取得	パソコン 1 台	平成元
81	土木積算	土木工事課、みどりと公園課	土木（公園）工事積算	パソコン 4 台	平成 4
82	図面印刷	土木工事課	図面印刷管理	パソコン 1 台	平成 17
83	みどりの条例	みどりと公園課	みどりの条例事務、緑化事業管理	庁内イントラネットパソコン利用	平成 4
84	構造計算	建築課	構造計算	パソコン 1 台	平成 18
85	共同住宅 GIS データベース	住宅課	共同住宅 GIS	パソコン 1 台	平成 20
86	住宅統合管理	住宅課	住宅の統合管理	サーバー1 台、パソコン 1 台	平成 15
87	大気汚染データ収集	環境保全課	大気汚染データ収集・整理	パソコン 2 台	平成 16
88	工場情報管理	環境保全課	公害関係法令の工場等の認可届出事務、指導立入検査事務	パソコン 2 台	平成 13
89	有料ごみ処理券管理	清掃リサイクル課	有料ごみ処理券の管理	サーバー1 台、パソコン 1 台	平成 12

No.	システム名	所属	業務概要等	機器構成	稼動年度
90	粗大ごみ受付	清掃リサイクル課、清掃事務所	粗大ごみ収集管理、受付	サーバー1台、パソコン4台(サーバー1台は共同運営)	平成14
91	２３区廃棄物情報	清掃リサイクル課、清掃事務所	２３区清掃事務のネットワーク	サーバー1台、パソコン3台(サーバー1台は一部事務組合)	平成12
92	資源回収業務管理	清掃事務所	資源回収事務支援	パソコン1台	平成12
93	清掃事業所車両管理	清掃事業所	収集車両管理	パソコン1台	平成12
94	選挙開票管理	選挙管理委員会事務局	候補者管理、開票の集計・統計	パソコン2台	平成4
95	在外選挙人管理	選挙管理委員会事務局	在外選挙人名簿調製	パソコン1台	平成13
96	選挙人名簿・期日前投票	選挙管理委員会事務局	選挙人名簿調製、期日前投票管理事務	サーバー1台、パソコン10台	平成10
97	投票所名簿管理	選挙管理委員会事務局	投票所名簿管理	パソコン78台	平成17
98	区議会会派控室用インターネット	区議会事務局	区議会会派控室用インターネット	パソコン8台	平成15
99	区議会会議録検索	区議会事務局	区議会会議録検索	パソコン1台	平成15
100	音声認識会議録作成	区議会事務局	音声認識会議録作成	パソコン5台	平成18
101	区議会映像配信	区議会事務局	区議会映像インターネット配信	サーバー1台	平成18
102	区議会会議室音声制御	区議会事務局	会議室音声制御	パソコン4台	平成21
103	学校緊急情報通報	企画調整課	緊急情報等の配信	サーバー3台	平成18
104	小中学校給食管理・栄養計算	学務課	給食管理・栄養計算	パソコン1台	平成12
105	小中学校情報教育	指導課	小中学校情報教育、児童生徒教材作成	パソコン6台	平成14
106	科学教室	めぐろ学校サポートセンター	理科実験計測データ分析	パソコン8台	平成11
107	学習支援教室生徒指導用	めぐろ学校サポートセンター	学習支援教室生徒指導用	パソコン9台	平成10
108	視聴覚教材作成	めぐろ学校サポートセンター	視聴覚ライブラリー	パソコン2台	平成18
109	教職員研修	めぐろ学校サポートセンター	教職員研修用	パソコン15台	平成21
110	歴史資料館資料管理・閲覧検索	地域学習課	歴史資料館の資料管理及び閲覧検索	サーバー1台、パソコン9台	平成20
111	文化財データベース	地域学習課	文化財問合せ回答データ保存、資料の作成・保存	パソコン2台	平成13
112	放課後フリークラブ支援	地域学習課	子ども教室事務用	パソコン5台	平成19

No.	システム名	所属	業務概要等	機器構成	稼動年度
113	スポーツ施設予約	スポーツ振興課	スポーツ施設予約管理、利用台帳管理	サーバー2 台、パソコン 20 台	平成 17
114	スポーツ講座申込み	スポーツ振興課	スポーツ教室・講習会の受付	ＡＳＰ	平成 20
115	体力診断	スポーツ振興課	区民体力診断	パソコン 1 台	平成 14
116	図書館情報	八雲中央図書館	図書館資料の管理業務、利用者用インターネット	サーバー13 台、パソコン 194 台	平成 3

別紙3：国保収納推進員システム業務フロー図

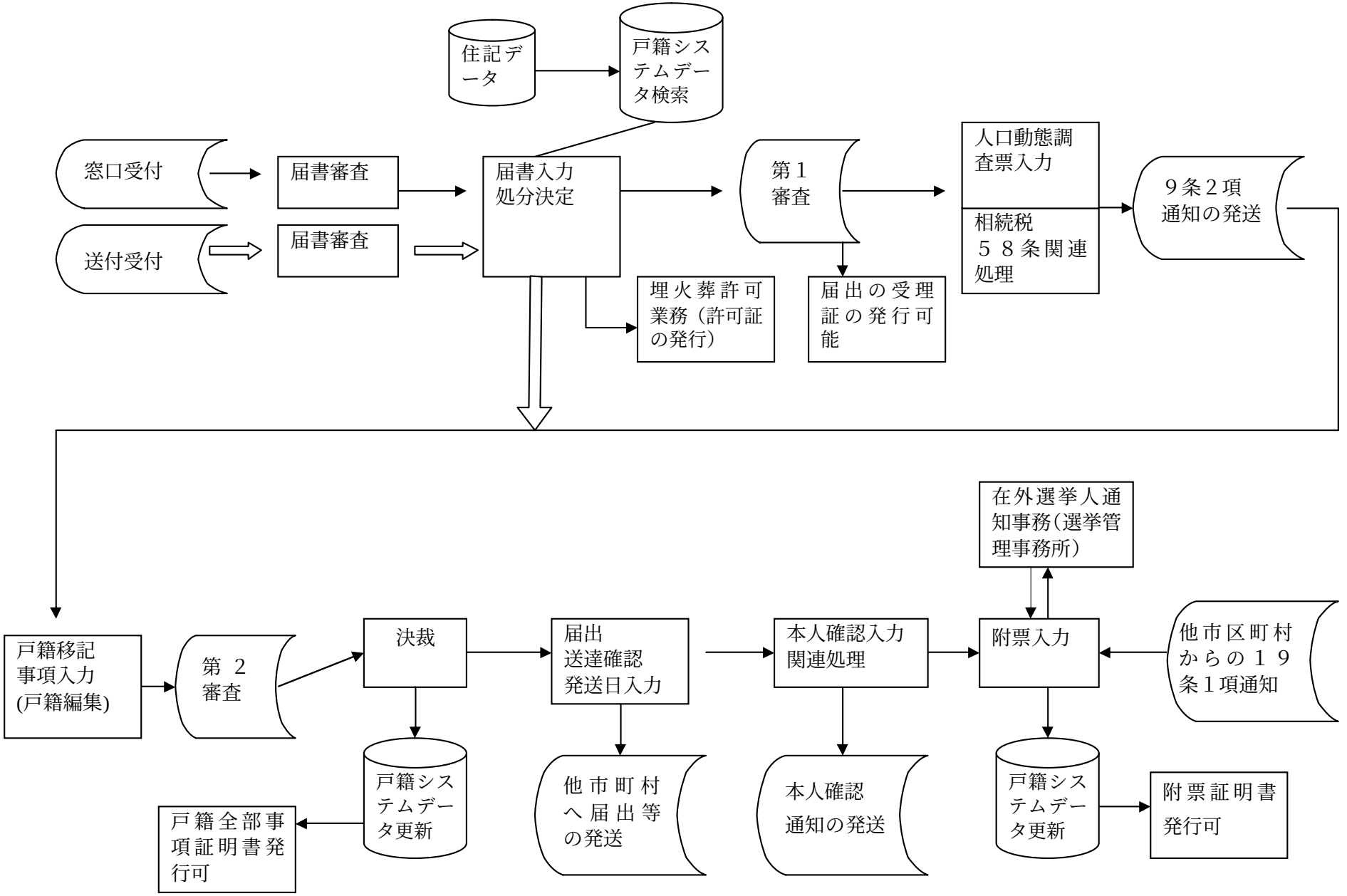


情報課で住記、資格個人･世帯、収納などのＤＢからダウンロードファイルを定期に作成、ファイルを電磁的記録媒体に書き込んだものを国保年金課に引き渡す。収納推進員システム担当者が、そのファイルを収納推進員システムに取り込み、データ更新を行う。

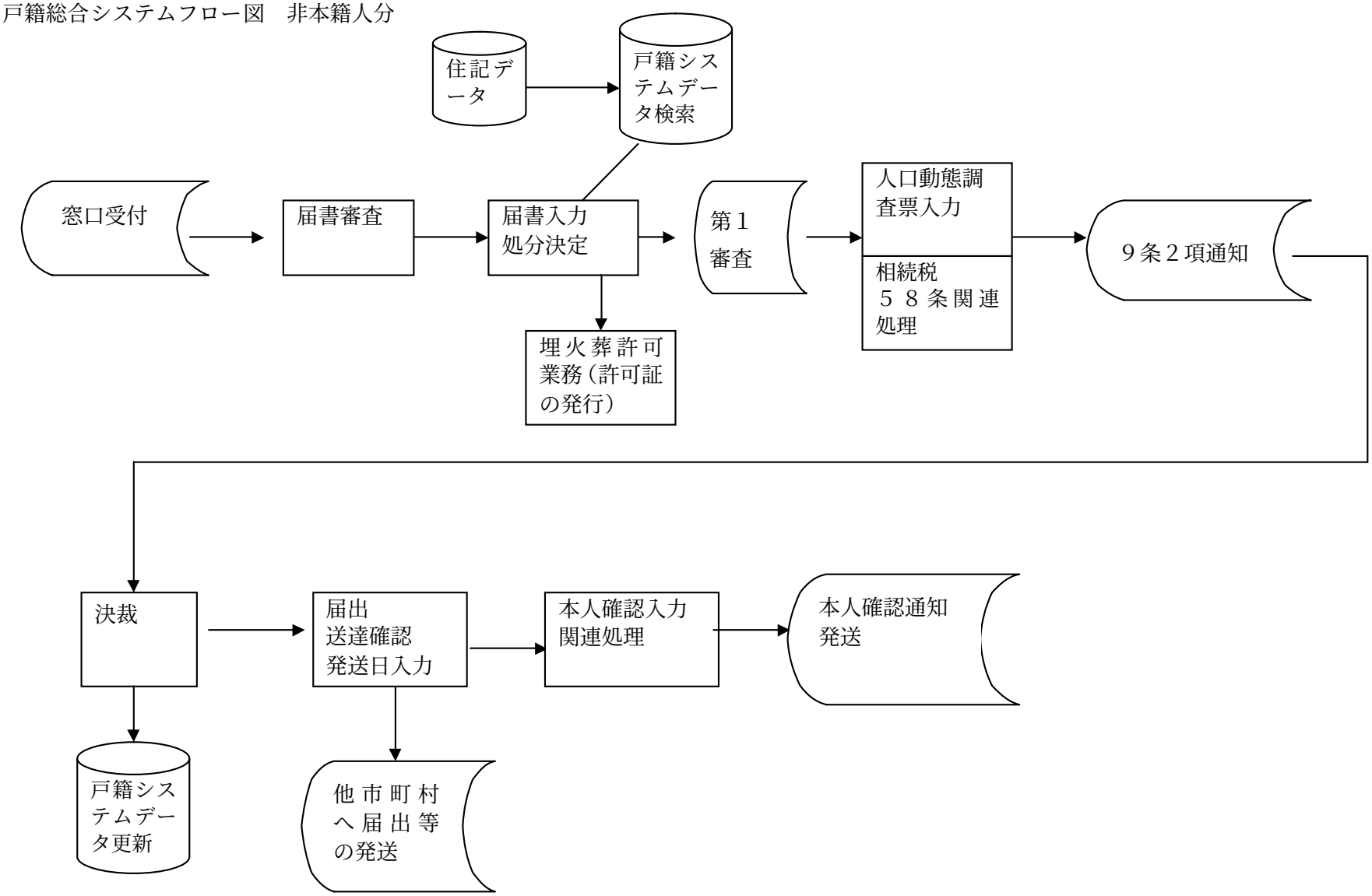
督促状を送付し、納期限を1か月以上経過した未納保険料がある世帯を抽出して、訪問カードを出力、4名の収納推進員が割り当てられた担当地区を2～3か月の頻度で訪問する。訪問終了後、訪問時の対応等を結果入力することにより、次回訪問カードに情報として記載される。

訪問カードの出力から結果入力までの処理は、収納推進員が行っている。

別紙４： 戸籍総合システムフロー図　本籍人分



戸籍総合システムフロー図　非本籍人分



別紙５：保健福祉情報システム
システム概要

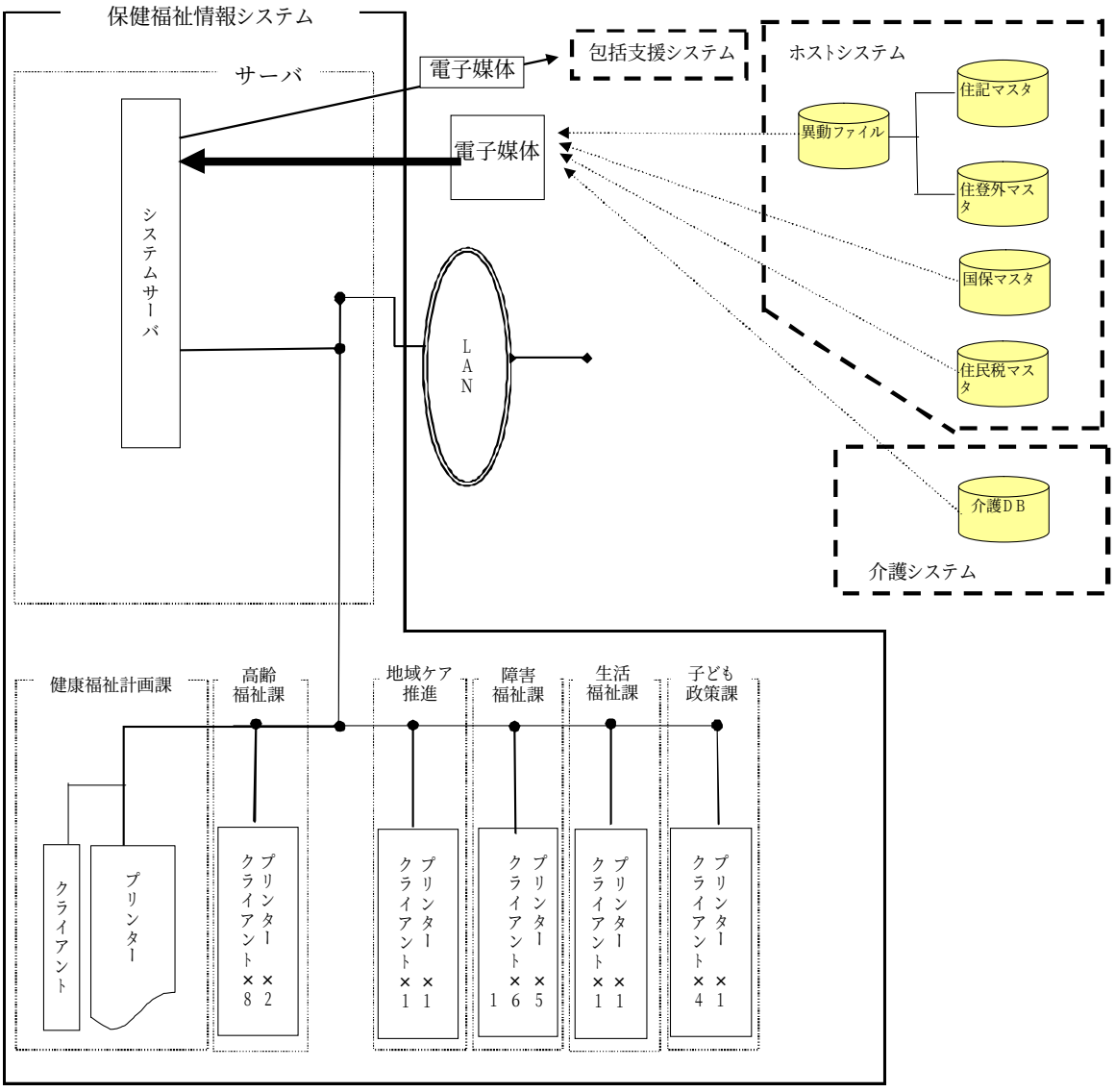
１．導入目的

健康福祉計画課では、保健福祉事業に係る情報の一元的管理・共有化を図ることで各事業の連携を容易にし、事務事業の一層の効率化を実現するため、平成 10 年に保健福祉情報システムを導入した。

２．システム構成

保健福祉情報システムは、パッケージ・ソフトウエアをベースとして構成されている。なお、本システムは、ホストシステム及び介護システムとは結合していないため、電子媒体を使用して住記データや介護データ等を定期的に保健福祉情報システムへの取り込みを行っている。また、平成 21 年 4 月から包括支援システムに対して保健福祉に関する情報を電子媒体により定期的に提供している。

図１　システム構成概要



３．機能構成

システム機能構成概要

保健福祉情報システム

1 共通管理サブシステム

システム管理	共通管理

2 総合登録サブシステム

高齢者台帳	高齢
身体障害者（児）手帳の交付	障害
愛の手帳の交付	障害
電話訪問	高齢
家具転倒防止器具取付	高齢･障害
理美容サービス	高齢
重度心身障害者(児）手当	障害
心身障害者扶養年金/心身障害者扶養共済制度	障害
交通災害共済	障害
寝具乾燥消毒	高齢･障害
緊急一時在宅保護	障害
リスト付き福祉小型バス貸出	障害
リフト付き福祉タクシー	障害
原爆被爆者見舞金支給	障害
防災用障害者名簿管理	障害
福祉工房	障害
自立支援住宅改修給付	高齢
入浴サービス	障害
点字図書の給付	障害

3 援護サブシステム

日常生活用具給付・貸与	障害
補装具交付・修理/人口肛門・膀胱等補助	障害
ホームヘルプサービス	障害
住宅設備改善費の給付	障害
おむつ支給･おむつ代支給	高齢･障害
福祉電話貸与・料金助成	高齢･障害
火災安全システム	高齢
緊急通報システム・非常通報システム	高齢･障害
食事サービス(週一回、配食代金補助)	高齢
判定依頼	障害
自動車燃料費助成/福祉タクシー券	障害
65歳以上難病認定	障害
脳性マヒ・筋萎縮症	障害

4 福祉医療サブシステム

心身障害者(児）医療費助成	障害

5 手当サブシステム

心身障害者福祉（区）手当支給	障害
特別障害者（国）手当支給	障害
障害児福祉（国）手当支給	障害
経過的福祉（国）手当支給	障害

6 資金貸付サブシステム

母子福祉資金	子ども政策
女性福祉資金	子ども政策
応急福祉資金	生活福祉

7 施設入所サブシステム

養護老人ホーム入所	高齢
特別養護老人ホーム入所	高齢

8 自立支援給付サブシステム

障害者自立支援給付(18.10版、施設、居宅)	障害
地域生活支援日常生活用具	障害
自立支援補装具	障害

包括支援センターシステムの概要

【システムの機能】
①包括支援センターの相談支援業務、申請書受付業務等のための行政情報の提供　②包括支援センターの申請受付業務等を処理するための書面伝送機能

各システムとのデータ連携

保健福祉情報システム

高齢者の保健福祉サービス利用状況、障害者手帳情報等

介護保険システム

高齢者（65歳未満要介護者含む。）の介護度、認定期間、主治医、担当ケアマネジャー等

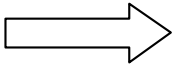
住民記録ホストシステム

高齢者及びその同居家族の住民基本4情報、世帯情報

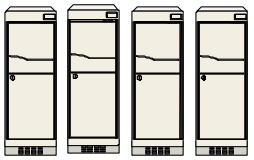
高齢者の相談支援業務、申請受付業務等に必要な範囲のデータを抽出

地域ケア推進課

職員がデータ更新用の端末で照会用データを更新する。



サーバ



①各システムから抽出したデータを保管。端末からは照会のみ可能。
②センターから伝送された申請書データを保管。各課の端末で出力。

個人認証管理・操作ログ履歴管理
ウィルス対策・不正アクセス防止対策等

ネットワーク

包括支援センター(5か所)

所長の職責
・センター職員の業務を監督
・区の情報セキュリティ基準等の遵守
・研修等による個人情報保護教育等

所長

社会福祉士　保健師 看護師　主任ケアマネジャー

（従事事職員数５センター計５８人）

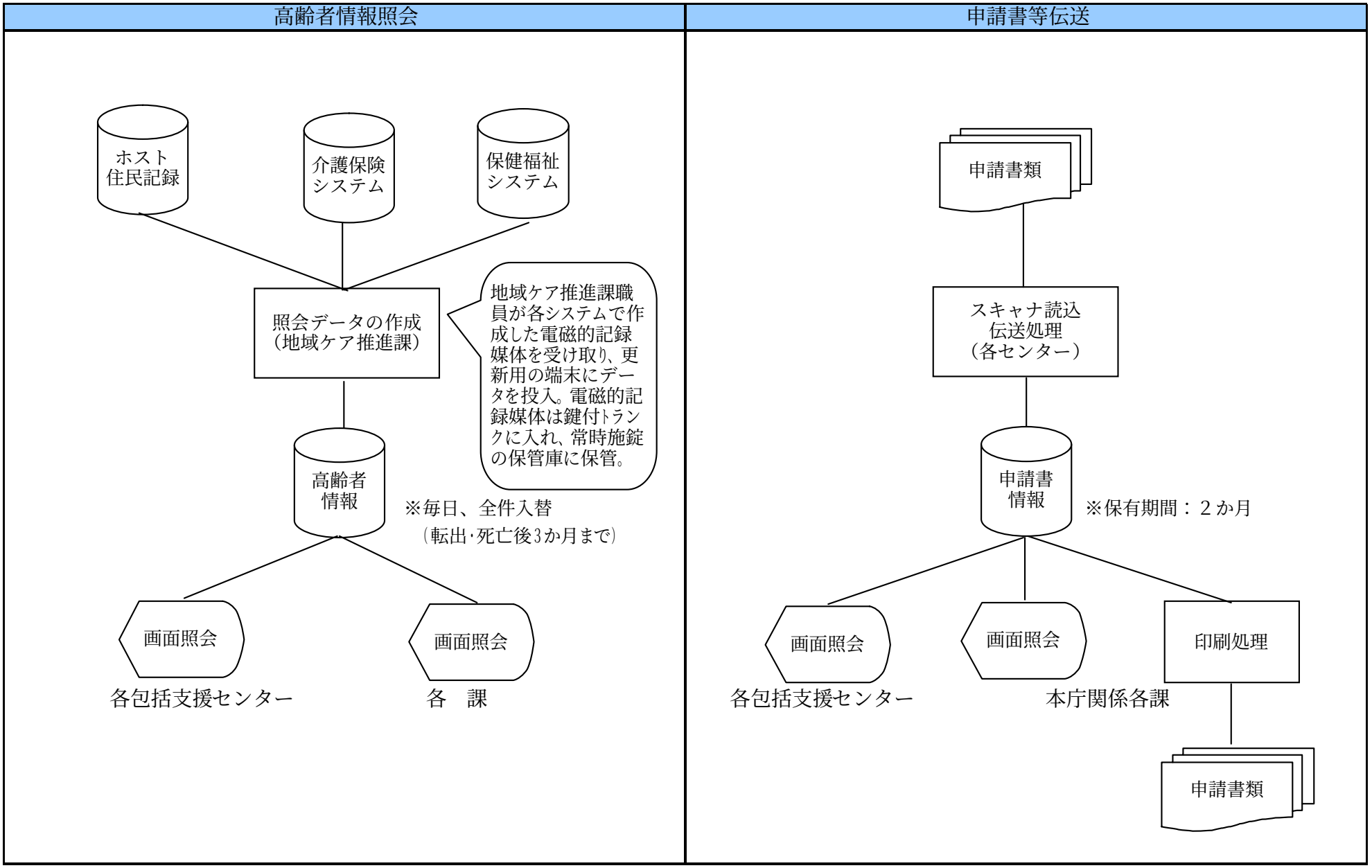
○システム端末（各2台）＋スキャナ(各2台)

本庁関係各課

介護保険課
高齢福祉課
地域ケア推進課

○システム端末（各2台）＋スキャナ（各1台）＋プリンタ（各1台）

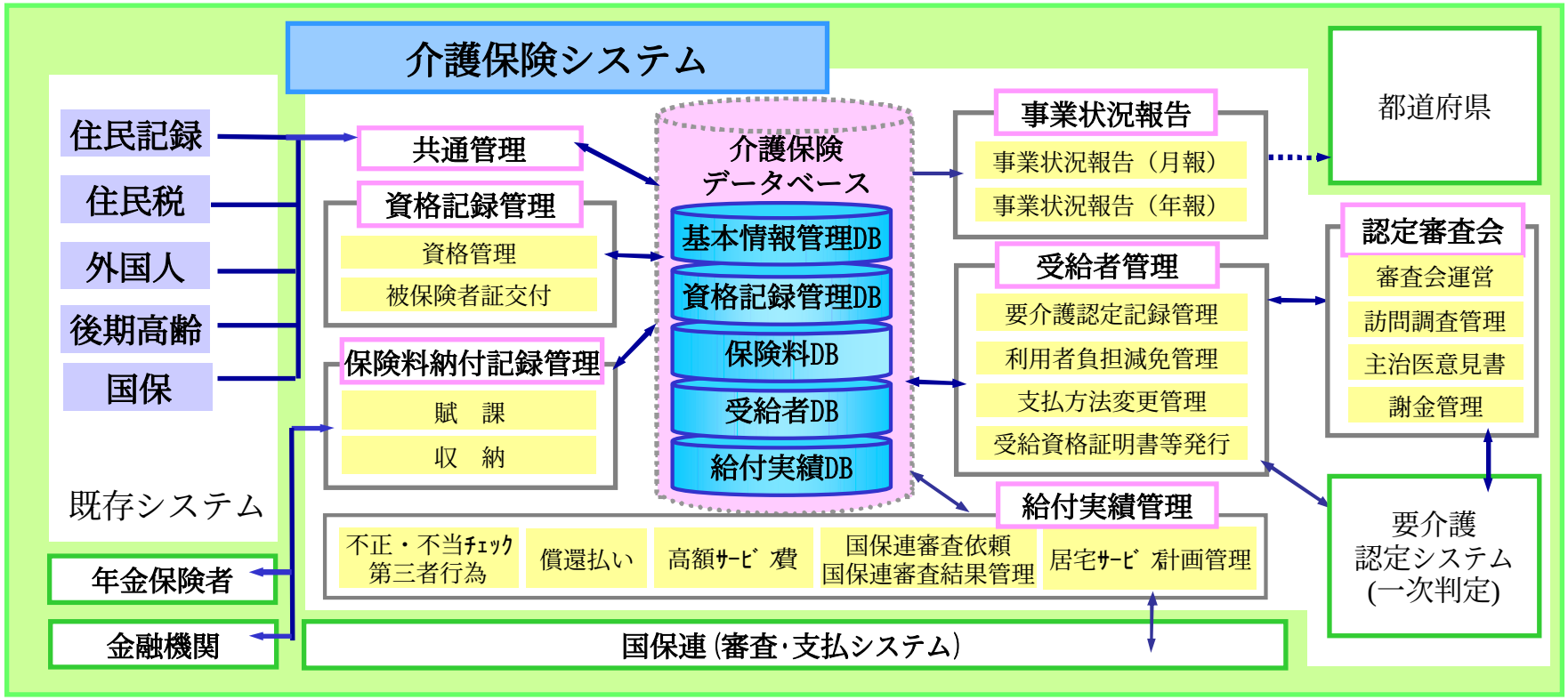
包括支援センターシステム・処理フロー図



別紙7：

介護保険システム概要

『介護保険システム』は、厚生労働省より提示の介護保険事務処理システム仕様に準拠し、資格記録管理／保険料納付記録管理／受給者管理／給付実績管理／認定審査会の各業務が一体となったシステム



別紙8：選挙管理委員会　処理フロー

（平常時及び定時登録時）※定時登録（3月、6月、9月、12月）

【平常時】

住民記録異動情報
（電磁的記録媒体）

情報課より
住民記録異動情報の格納された媒体を受領し,選挙人名簿システムに取り込む。

選挙人名簿システム
（サーバー）へ取り込み

【定時登録時】

選挙人名簿定時登録処理

（新規登録者、抹消者の抽出）
（選挙人名簿登録者の確定）

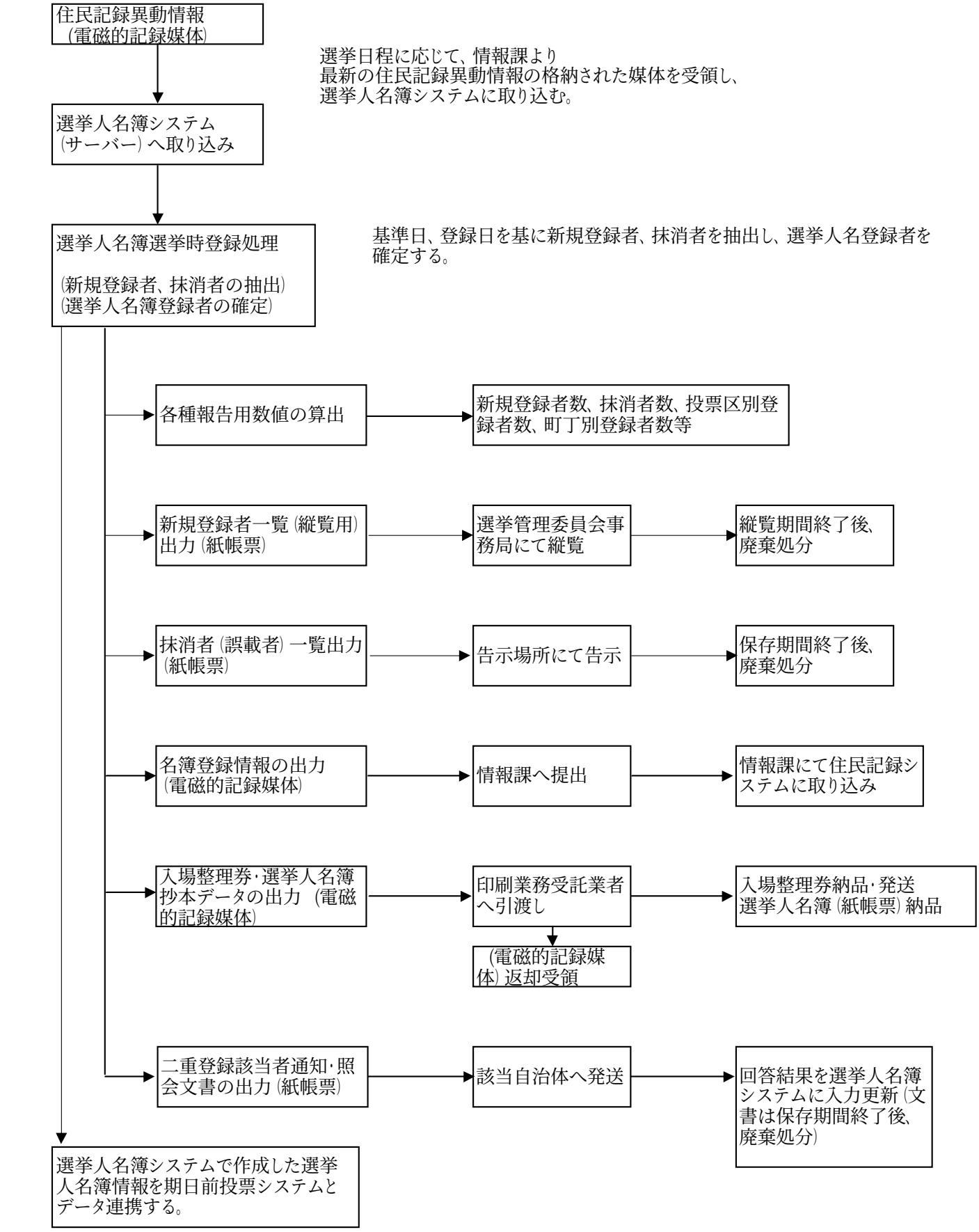
毎年3、6、9、12月の定時登録処理を行う。
基準日、登録日を基に新規登録者、抹消者を抽出し、選挙人名登録者を確定する。

- 各種報告用数値の算出 → 新規登録者数、抹消者数、投票区別登録者数、町丁別登録者数等
- 新規登録者一覧（縦覧用）出力（紙帳票） → 選挙管理委員会事務局にて縦覧 → 縦覧期間終了後、廃棄処分
- 選挙人名簿抄本出力（紙帳票） → 投票区毎にファイルし施錠保管 → 次回定時登録処理後、廃棄処分
- 抹消者（誤載者）一覧出力（紙帳票） → 告示場所にて告示 → 保存期間終了後、廃棄処分
- 選挙資格情報の出力（電磁的記録媒体） → 情報課へ提出 → 情報課にて住民記録システムに取り込み
- （9月のみ）裁判員・検察審査員候補者予定者名簿作成用データ出力 → 裁判員名簿調製プログラムへ取込・調製 → 裁判所・検察審査会に使送

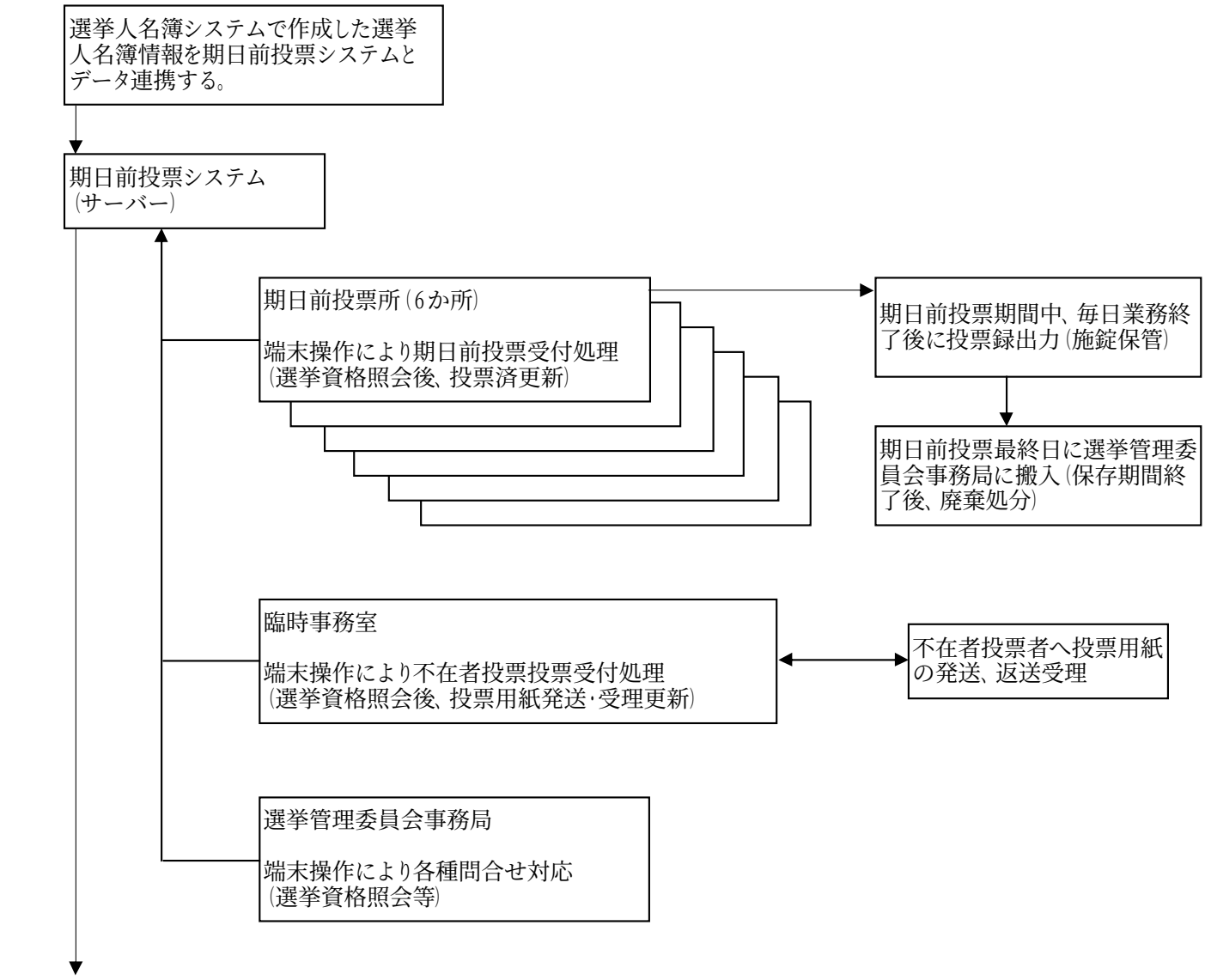
処理フロー

（選挙時）

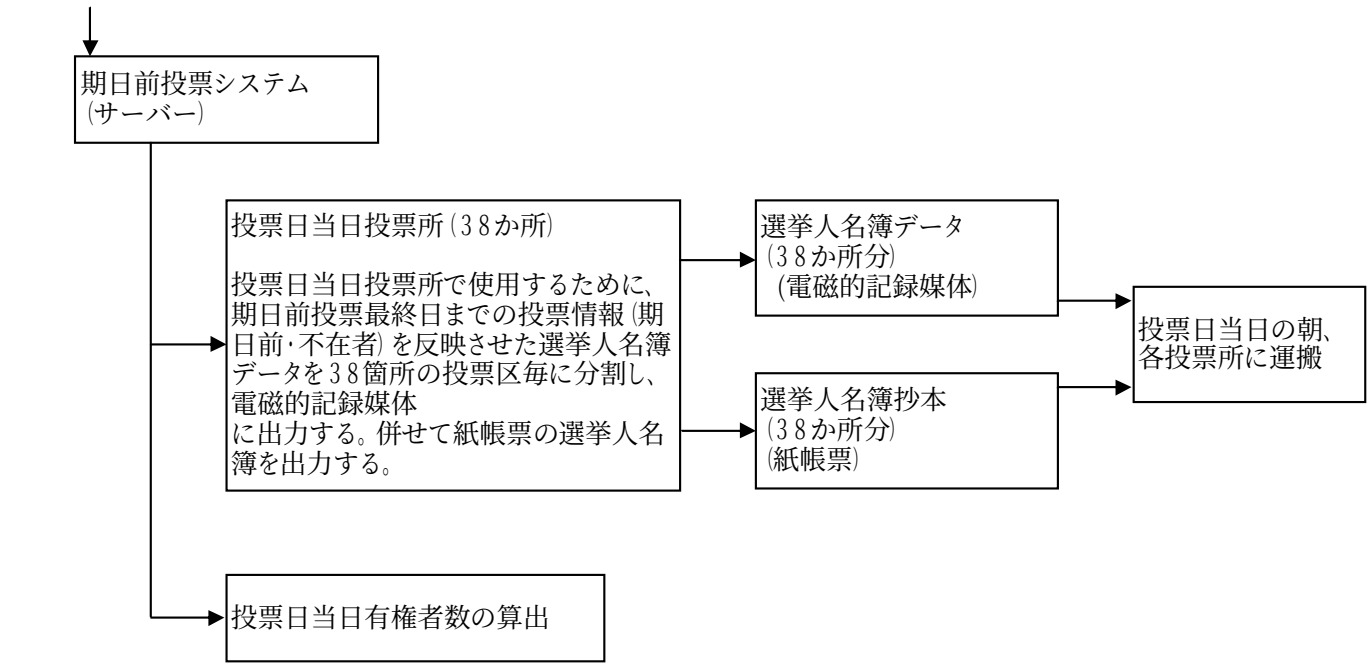
【選挙時登録】



【期日前（不在者）投票期間】

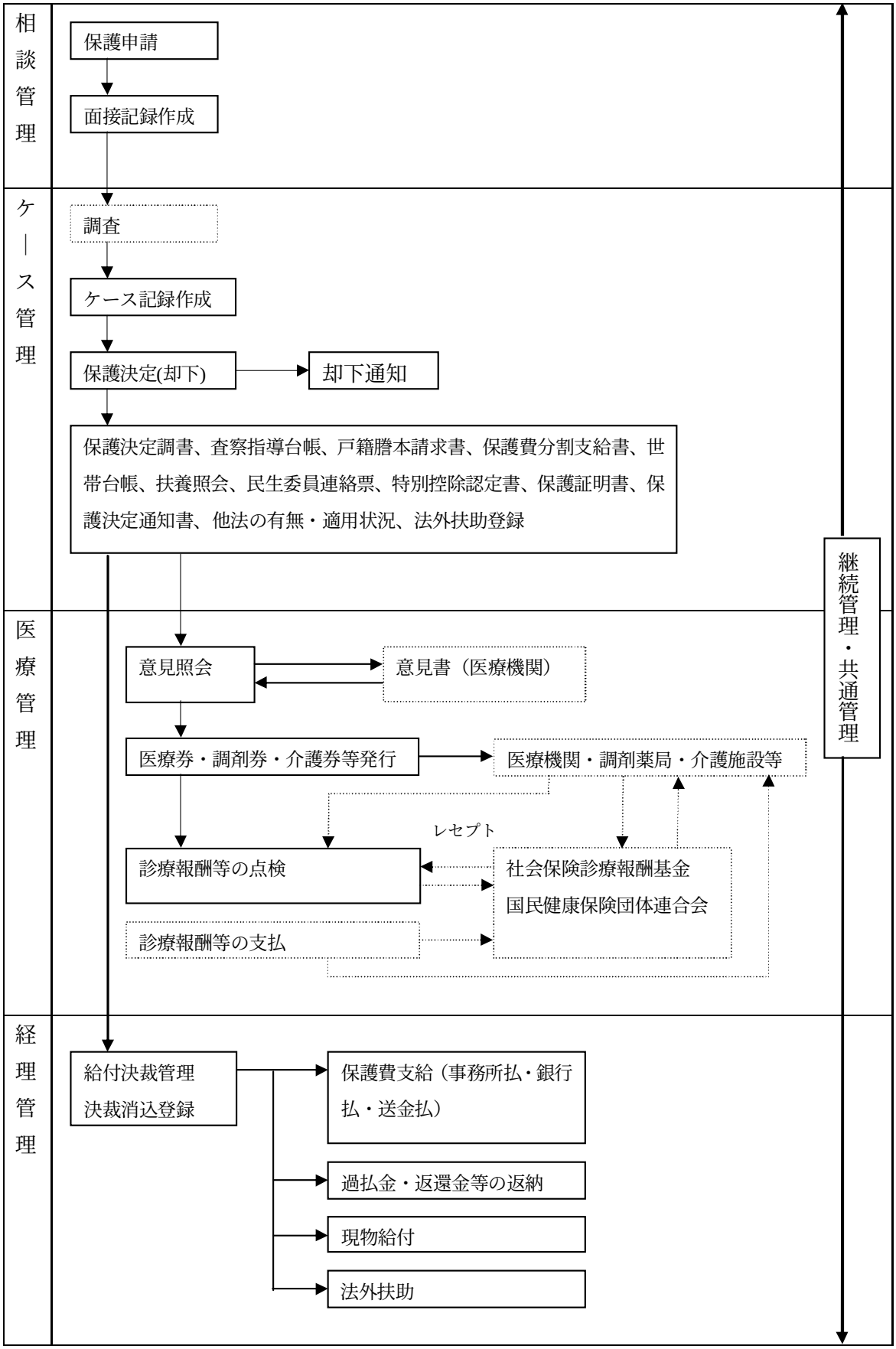


【期日前投票最終日業務終了後】



別紙９：

生活保護システム事務処理フロー



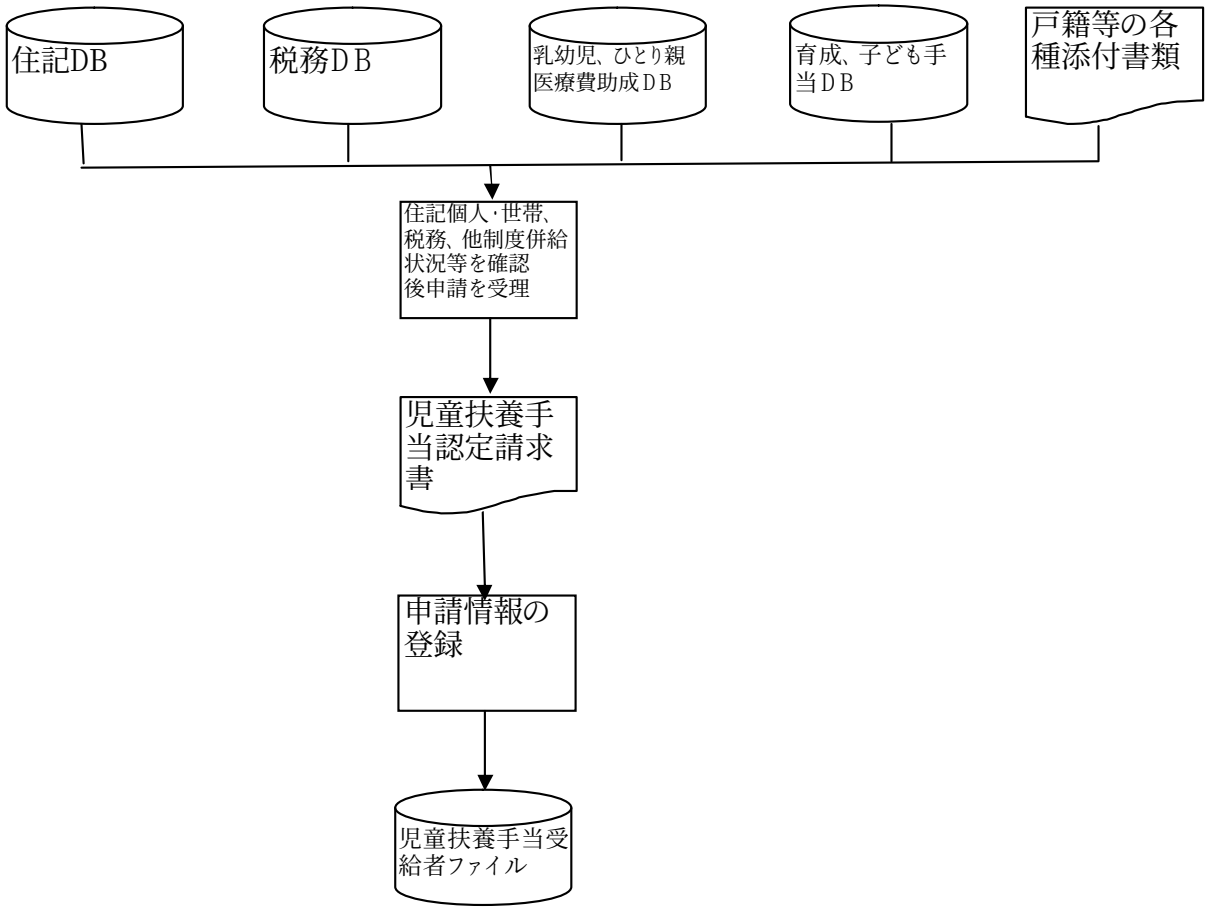
児童扶養手当事務フロー

別紙10：児童扶養手当処理フロー

【新規申請受付】

児童扶養手当の申請の申し出をいただいた時点で、まず、戸籍・受理証明書等の、事前に準備が必要な書類の内容を確認。次いで、住記・税務・育成手当等の各手当・医療費助成ＤＢの状況を確認し、申請可能であると判断された時点で、児童扶養手当認定請求書を記入していただく。申請を受理した場合、住記異動を確認するために、受給者ファイルへ情報を登録する。

提出された認定請求書、及び各種添付書類は、別途、年金受給資格確認等の作業を経た上で、認定、あるいは却下の処理を行なう。



児童扶養手当事務フロー

【新規認定】

受理した認定請求に関して、受給資格要件審査、及び公的年金受給資格確認等の各関連審査を行なった上で、「認定」「却下」の判定を行なう。
却下者については、個別システムに却下内容を入力し、却下通知を送付。認定者については、個別システムに受給資格を入力、決裁処理を行なった上で、受給者宛に各種通知を発送。
あわせて、受給者ファイルへも認定･却下の情報を登録する。