荒川区情報セキュリティ

監査報告書
（概要版）

平成２５年２月

1　監査目的

本監査は、助言型の情報セキュリティ監査として実施し、今年度で 4 回目を迎えました。

本監査では、住民記録や税など、区民の重要な個人情報を取り扱う業務系システムの利用現場において、情報資産の管理等が適切に実施されていることを第三者の専門的立場から点検、評価するとともに、監査の結果をもとに、業務系システム利用現場における情報セキュリティ対策の更なる改善と徹底を図ることを目的としました。

2　監査テーマ

監査対象とする課の情報資産について、所管業務の事務処理フロー及び情報資産のライフサイクル（発生から廃棄まで）に即し、それぞれの局面におけるリスク分析の視点を踏まえ、情報資産の管理状況や業務系システムの利用状況、情報セキュリティ対策の実施状況等を再検証しました。この再検証を通して、現行の取扱い等の問題点を確認の上、改善方法等について助言、指導を行いました。

3　監査範囲

No	監査対象課	主な業務内容
1	区民生活部地域振興課 （町屋区民事務所）	・住民基本台帳、印鑑の登録及び証明に関する業務 ・特別区民税及び軽自動車税の収納・証明に関する業務 ・国民健康保険の届書の受理並びに被保険者証の発行及び訂正並びに保険料の収納に関する業務 ・介護保険の被保険者証の発行及び訂正並びに保険料の収納に関する業務 ・国民年金の届書の受理及び年金手帳の訂正に関する業務 ・畜犬登録届等の受付及び登録料の収納に関する業務 ・ひろば館及びふれあい館の使用に関する業務 ・担当地域の地域振興事業の実施に関する業務
2	福祉部福祉推進課	・社会福祉統計に関する業務 ・介護保険施設の計画及び調整に関する業務 ・民生委員推薦会及び民生委員・児童委員に関する業務 ・生業資金及び応急資金に関する業務 ・区営住宅に関する業務
3	福祉部国保年金課	・国民健康保険の被保険者の資格取得及び喪失、被保険証に関する業務 ・後期高齢者医療に関する業務 ・国民健康保険料及び後期高齢者医療保険料の徴収・滞納整理に関する業務 ・国民年金の給付、被保険者の資格取得及び喪失に関する業務 ・国民年金保険料の免除及び学生納付特例制度に関する業務
4	子育て支援部児童青少年課	・学童クラブ事業及び放課後子どもプランの運営及び調整に関する業務 ・青少年問題に関する関係機関との連絡調整に関する業務 ・青少年の健全育成に関する業務

4　監査方法

（1）事前確認

・情報セキュリティ関連規程と監査証拠のレビュー

（2）本調査

・監査対象課の執務室の視察

・監査対象課の職員へのインタビュー

5　監査実施日程

実施日	区　分	内　　容
平成 24 年 12 月 17 日	事前確認	情報セキュリティ関連規程と監査証拠のレビュー（本調査に関する事前打合せを含む）
平成 25 年 1 月 25 日	本調査①	監査対象課（福祉推進課、国保年金課）の執務室の視察と職員へのインタビュー
平成 25 年 1 月 29 日	本調査②	監査対象課（地域振興課町屋区民事務所、児童青少年課）の執務室の視察と職員へのインタビュー
平成 25 年 2 月 4 日	監査報告書の取りまとめ	監査調書の作成と監査結果に関する意見交換
平成 25 年 2 月 18 日	監査報告会	監査結果を踏まえた監査対象課への助言、指導

6　監査実施体制

［監査人］　都市情報システム研究所　茶 谷 達 雄

西城技術士事務所　西 城 秀 雄

7　監査項目

区　分	内　　容
監査項目	(1) 情報資産の管理、(2) 通信ケーブルの配線、(3) 機器の定期保守及び修理、(4) 管理区域の構造、(5) 入退室の管理、(6) パソコン等の機器管理、(7) 職員の遵守事項、(8) パスワードの取扱い、(9) アクセス制御、(10) 不正プログラム対策、(11) 個人情報保護、(12) 緊急時対応、(13) その他

8　適用基準等

（1）適用基準

① 荒川区電子情報システム管理運営規程

② 荒川区電子情報システムに係る情報セキュリティ対策基準

③ 荒川区庁内ネットワーク利用に係るセキュリティ実施手順

④ 荒川区ＩＣＴ部門における業務継続計画

（2）参考基準

① 地方公共団体情報セキュリティ監査ガイドライン（総務省）

② 地方公共団体情報セキュリティセルフチェックリスト（総務省）

９　監査結果

（１）総評

① 情報資産管理台帳について

情報資産管理台帳に記載されている情報資産が、現在キャビネットに保管している資産に限られており、移送データやシステム連携データを格納した記録媒体、バックアップデータ、パソコン等の機器が情報資産管理台帳に記載されていませんでした。今後は、全庁的な統一基準の下で、更に情報資産管理台帳の精度を高めていくことを期待いたします。

② 緊急対応手順について

今回監査を行った各課では、緊急時の対応者が明確に記載されるなど詳細な情報セキュリティに係る緊急時対応手順が整備されており、各課の管理者がセキュリティに関する高い意識を持って課内の職員に対する啓発を行っていました。今後は、机上訓練（シミュレーション）の実施等を検討し、具体的に訓練を実施することで、対応手順の有効性を検証し、緊急対応能力の向上を図ることが重要です。

③ データの誤入力防止対策について

監査を行った各課とも、チェックリストによるチェックを実施し、二重チェックを行うなど、誤入力防止対策を実施していましたが、チェックリストやチェック体制は、まだ検討の余地があるものと思われます。ヒューマンエラーを最小限に抑える観点から、改めて体制の強化が望まれます。

（２）推奨する点

今回の監査の結果、特に優れていると見られる点は以下のとおりです。今後も、引き続き情報セキュリティ対策を徹底することを推奨します。

① キャビネットの施錠について、最終退出者が確認を行い、記録を残すなど適正であった。

② 他自治体にＣＤを渡す際や、金融機関とＦＤの受け渡しをする際に、証書等による授受の記録を各課で残しており適正であった。

③ 外部の者が立ち入ることができないよう抑制措置がとられており、適正であった。

④ 業務系システム及びスタンドアロンシステムは、個人単位での指静脈によるログイン認証により、限られた人しかログインできず、適正であった。

⑤ ＵＳＢメモリ等の記録媒体は、原則使用できないようになっていた。

⑥ 人事異動に伴うパスワード等の変更は、情報システム課と連携し、的確・迅速に対応されていた。

⑦ 利用者はユーザー権限でないとログインできない仕組みになっており、不正ソフト等はインストールできない環境になっていた。

（３）改善を求める点

直ちに情報セキュリティ事故につながる内容ではありませんが、業務執行時に潜むリスクについて十分に理解した上で、改善するようにしてください。

① 一部の情報資産で、保管場所は把握していたが、ファイリングが適切でないものがあったため、情報資産のファイリングを適切に行うこと。

② 情報資産の廃棄は、シュレッダーを使用するなど適切に行われていたが、今後は「いつ」「誰が」「何を」廃棄したかがわかるよう、記録を残すこと。

③ パスワードの変更が行われていない、あるいは不定期に行われているシステムがあったが、今後は定期的にパスワードの変更を実施すること。

④ 入力チェックについて、システムを扱っている職員が主に１人であり、区の職員間で二重チェックを行っていないケースがあったので、今後は担当者を２人にして二重チェックを行う等、各課で組織的に対応すること。

⑤ 委託契約に関し、データ消去義務を明記するなど、より情報保護に配慮した内容にするとともに、プライバシーマークの取得を受託条件にすることを検討すること。