荒川区情報セキュリティ

監査報告書
（概要版）

平成２４年２月

1　監査目的

今回の監査は、助言型の情報セキュリティ監査として実施したものです。

本監査では、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さら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。この再検証をとおして、現行の取り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	福祉部生活福祉課	・生活保護法及び中国残留邦人等支援法等の経理及び統計に関する業務 ・法外援護企画、調整及び実施に関する業務 ・生活相談に関する業務 ・路上生活者の自立支援に関する業務 ・被保護世帯及び中国残留邦人等に係る個別的援護事務に関する業務 ・法外援護事務の調査に関する業務
2	教育委員会事務局 学務課	・区立学校及び区立子ども園の設置廃止に関する業務 ・学齢児童生徒の就学に関する業務 ・学級編成及び学齢簿に関する業務 ・学校運営に関する業務 ・学校保健に関する業務 ・就学援助に関する業務 ・奨学資金に関する業務
3	選挙管理委員会事務局	・選挙の管理、執行に関する業務 ・選挙人名簿の調整に関する業務 ・明るい選挙の啓発に関する業務
4	健康部保健予防課	・エイズ、結核その他の感染症の予防等に関する業務 ・健康危機管理対策に関する業務 ・公害健康被害補償の認定及び補償給付の支給に関する業務 ・大気汚染障害者認定に関する業務 ・衛生上の試験及び検査に関する業務

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 23 年 12 月 15 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 24 年 1 月 17、23 日	本調査	監査対象課の執務室の視察と職員へのインタビュー
平成 24 年 2 月 9 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 24 年 2 月 23 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）緊急時一次対応

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 荒川区電子情報システムに係わる緊急時対応マニュアル

（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

今回で３回目となる情報セキュリティ監査ですが、セキュリティに関する基本的な対応については各課で的確に履行されており、これまでの監査結果が着実に各所管課へ浸透していることがうかがえます。

今後、更なるセキュリティの向上を図るために、情報資産管理台帳の充実や緊急時一次対応手順の実効性の担保に加え、標的型メール攻撃等のセキュリティ上の脅威に対する対策の充実を図ることを期待いたします。

（2）優れている点

今回の監査の結果、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 個人情報等が保管されているキャビネットは施錠できるようになっており、鍵も適正に管理されていた。
② システム利用者の ID は各職員ごとに設定され、適正に管理されていた。
③ 不正プログラムはインストールできない環境になっていた。
④ 窓口等の端末機の設置場所は、個人情報に配慮した配置となっていた。
⑤ 受付窓口における申請書などの個人情報を含む資料の放置は認められなかった。

（3）指摘事項及び改善事項

指摘事項等は、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、確実にご対応ください。

① 情報資産管理台帳の更なる整備充実を図ること。
② 各職員の机上に設置されている専用端末以外の事務用端末に重要な記録等が残らない方法を検討すること。
③ パスワード変更の期間を短縮すること。
④ 印刷委託業者の現場視察を検討するとともに、不要な帳票類の処理及び廃棄の記録を残すよう仕様書等に明記すること。
⑤ 緊急時一次対応手順の有効性を検証するとともに、各職員への周知を徹底すること。