

荒川区情報セキュリティ

監査報告書（概要版）

平成22年4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、住民記録や税など、区民の重要な個人情報を取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	区民生活部戸籍住民課	<ul style="list-style-type: none">・住民基本台帳に関する業務・印鑑登録に関する業務・戸籍に関する業務・外国人登録に関する業務・公的個人認証サービスに関する業務
2	福祉部介護保険課	<ul style="list-style-type: none">・介護給付に関する業務・要介護認定に関する業務・被保険者の資格取得及び喪失に関する業務・介護保険料に関する業務
3	子育て支援部計画課	<ul style="list-style-type: none">・私立専修学校、私立各種学校及び私立幼稚園に関する業務・児童手当、児童扶養手当、特別児童手当及び児童育成手当に関する業務・ひとり親家庭及び子どもの医療費の助成に関する業務・母子生活支援、母子相談、婦人相談及び家庭相談に関する業務・母子家庭自立支援関連事業給付金等の給付に関する業務・ひとり親家庭ホームヘルプ、ひとり親休養ホームに関する業務・母子自立支援プログラム策定事業に関する業務・入院助産措置に関する業務
4	健康部健康推進課	<ul style="list-style-type: none">・健康づくりの推進に関する業務・母子保健に関する業務・栄養指導に関する業務・歯科保健に関する業務・予防接種に関する業務・医療助成等に関する業務・成人健診に関する業務・腸内細菌検査に関する業務・エックス線検査に関する業務

4 監査方法

- (1) 関係規程及び監査証拠のレビュー
- (2) 監査対象課の執務室の視察
- (3) 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 22 年 1 月 21 日	事前確認	情報セキュリティ関連規程と監査証拠の事前確認 (本調査に関する事前打合せを含む)
平成 22 年 2 月 1、2 日	本調査	監査対象課の執務室の視察
平成 22 年 3 月 11 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 22 年 3 月 24 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) IC カード等の取扱い、(9) パスワードの取扱い、 (10) アクセス制御、(11) 不正プログラム対策、(12) 個人情報保護、 (13) 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
- ⑤ 荒川区住民基本台帳ネットワークシステム管理運営規程
- ⑥ 荒川区住民基本台帳ネットワークシステムの適正管理等に関する条例
- ⑦ 荒川区住民基本台帳ネットワークシステムの適正管理等に関する条例施行規則

(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

今回の監査では、情報セキュリティに関して優れている点も多く見受けられましたが、指摘事項等があったことも事実です。

本報告書の内容をもとに検討の上、今後の情報セキュリティ向上の取組みにご活用いただければ幸いです。

(2) 優れている点

今回の監査で優れている点は、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 執務室のレイアウト図に情報資産を保管しているキャビネット番号等が記載され、的確に管理されていた。また、セキュリティワイヤの装着及びクリアスクリーンの運用が適正に行われていた。
- ② ICカードは、管理台帳により、ID番号等が適切に管理されており、6か月に1回、定期的にパスワード変更を実施していた。合わせて、指静脈認証等を活用した適切なアクセス制御が行われていた。
- ③ 端末機に不正プログラムがインストールできないよう、指静脈認証等を活用して管理者権限を適正に制限していた。
- ④ 端末機の設置場所や窓口の構成が、申請者等の個人情報やプライバシーの保護に配慮されたものとなっていた。
- ⑤ 緊急時一次対応手順が職員に周知徹底されていた。責任者が明確にされており、責任者はリスクをよく認識していた。

(3) 指摘事項及び改善事項

直ちに情報セキュリティ事故につながる内容の指摘事項はありませんでした。今後も、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。

なお、情報セキュリティの一層の向上を図るため、以下の事項の実施をご提案いたします。

- ① 情報資産管理台帳の一層の整備充実を図ること。
- ② 定期的な業務フロー等の再点検により、リスクの「見える化」に努めること。
- ③ 通信ケーブルの敷設環境の改善に努めること。
- ④ キャビネット類の計画的な入れ替えを検討すること。
- ⑤ 区全体に係る事故時の対応手順に、個人情報漏えい事故を想定した対応を追加すること。