荒川区情報セキュリティ

監査報告書

（概要版）

平成３１年３月

1　監査目的

情報セキュリティ外部監査は、組織の重要な情報資産に対する情報セキュリティ対策が適切に整備･運用されているかどうかを第三者の専門的な立場から検証･評価を行い、助言等を与えることです。区では平成21年度より実施しており、監査結果をもとに情報セキュリティ対策の更なる改善と徹底を図っています。

2　監査内容

監査対象とするシステムについて、情報資産の管理状況や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、現行の取扱い等の問題点を確認のうえ、改善方法等について助言、指導を行います。

3　監査対象

監査対象課	監査対象システム
生活福祉課	生活保護システム
	中国残留邦人等支援システム
	レセプト管理システム
障害者福祉課	障害者福祉システム

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等の視察
（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30年10月 4日	実施方法打合せ	情報セキュリティ監査の実施方法
平成30年11月16日	実地監査 資料事前送付	監査資料の内容等の確認
平成30年12月 5日	実地監査	監査証拠確認、執務室視察、職員へのインタビュー
平成31年 2月 1日	監査報告会	監査結果を踏まえた監査対象課への指導助言

6　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		項　　目
監査項目	組織的・人的管理	（１）職員の遵守事項 （２）事故・欠陥等の報告 （３）緊急時対応計画 （４）外部委託 （５）自己点検
	技術的管理	（６）通信ケーブルの配線 （７）通信回線 （８）パスワードの取扱い （９）アクセス記録の管理取得等 （１０）アクセス制御・利用者ＩＤの取扱い （１１）不正プログラム対策 （１２）ソフトウェアの更新
	物理的管理	（１３）情報資産の管理 （１４）機器の廃棄 （１５）機器の定期保守及び修理 （１６）パソコン等の管理 （１７）サーバー等の機器の管理 （１８）外部記憶媒体の利用

8　適用基準等

（１）適用基準

ア　荒川区電子情報システム管理運営規程

イ　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

ウ　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

エ　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

ア　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（総務省）

イ　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（総務省）

ウ　クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）

エ　特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編（個人情報保護委員会））

9　監査結果

（1）総評

監査を行った結果､全体としてリスクコントロールがリスクアセスメントに基づいて、適切に整備・運用されていることが確認されました。しかし、一部に改善を求められるところがあります。今後も、業務執行時に潜むリスクについて十分理解し、事故前提社会の理念に立ち、的確にフォローアップされることを期待します。

（2）緊急時対策の対応について

緊急時一次対応手順に、情報システム部門の追加が求められるところです。今日の情報システムは、ネットワーク技術も進展し、その管理運営は高度化・複雑化してきている状況です。このため緊急時一次対応手順には、情報システム部門の担当者の参加なくては、原因、対策、復旧等について、迅速且つ十全の対応がしきれない分野が多くなっています。これらの状況を考慮すると、緊急時一次対応には、情報システム部門の担当者の追加を求めることが、適正と考えられるところです。

また、緊急時対応を的確に行うために、訓練を実施しておくことが重要です。緊急時対応訓練の実施計画を作成し、実地又は図上での訓練を実施することを期待します。その実施計画の中には、システムの復旧が長時間に及ぶ場合を想定した緊急時の業務体制に関しても盛り込むことが重要です。

（3）内部牽制システムについて

情報システムにおける真正性の確保による、故意や過失による事故の未然防止対策として、内部牽制システムの組み込みが求められるところです。

※内部牽制システムとは

業務や機能のあるまとまり単位について、業務の配分や機能の分化を図り、故意や過失があれば、相互に異なった角度から、自然に発見される方式のことです。

（4）情報資源管理の電子化等による減量化について

情報資源管理で保存されている文書（紙）が、たいへん多いのが、今回の対象課の特徴といえます。現状は、的確に管理されている現状ですが、ファイリングキャビネットが満杯の状態のところも見受けられました。

情報資源管理として、適正な管理の障害になることが想定されるため、ファイルの移し替え等を図り、情報資源管理の適切な運用管理を期待します。さらに、文書資料の電子化による減量化についても検討をお願いします。

（5）通信ケーブルの保護対策について

通信ケーブルをモール等で保護をしている事務室については、一部モールが損傷し、通信ケーブルが露出した状態となっている箇所がありました。これらは、通信ケーブル切断の可能性もあるため、早急に対策をとる必要があります。