荒川区情報セキュリティ

監査報告書

（概要版）

平成２８年１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ているものです。区の業務執行に重要な各種情報を取扱う情報システムの利用現場を対象に、個人情報やプログラム等の重要電子データ及び情報機器等の情報資産の管理やセキュリティ対策が適切に行われているかを第三者の専門的な視点から確認し、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ることを目的としています。

2　監査テーマ

監査対象とする情報システムについて、情報資産の管理状況や情報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上、改善方法等について助言、指導を行いました。

また、委託業務のあるシステムにおいては、保守契約内容及び委託業務の管理・監督状況について確認を行い、ホームページで住民に対して公開を行っているシステムにおいては、改ざん・不正アクセス等の対策について確認しました。

3　監査範囲

番号	監査対象課	監査対象システム
1	荒川清掃事務所	粗大ごみ収集・受付システム
2		有料ごみ処理券管理システム
3		東京２３区廃棄物情報管理システム
4	清掃リサイクル課	東京２３区廃棄物情報管理システム
5	経営支援課	中小企業融資管理システム

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27年 9月24日	実施方法打合せ	情報セキュリティ監査の実施方法、内容等事前打合せ
平成27年11月10日	実地監査①	監査証拠確認、執務室視察、職員へのインタビュー　対象課（荒川清掃事務所・清掃リサイクル課）
平成27年11月17日	実地監査②	監査証拠確認、執務室視察、職員へのインタビュー　対象課（経営支援課）
平成27年12月17日	監査結果報告書取りまとめ	監査結果に関する意見交換、監査報告書、調書の作成
平成28年 1月 7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	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

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

④ＩＣＴ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）

③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）

９　監査結果

（１）　総評

（日本年金機構の情報漏えい事件を受けて）

セキュリティ監査にあたって、最初に対象情報システムの各管理者にヒアリングを行いました。日本年金機構へのサイバー攻撃で、個人情報の大量漏えいが発生したことについて、明らかにされた重要な点は、組織内における事故の状況認識や情報共有化の欠如であったことです。

これは管理者の認識として、業務とセキュリティ対策の双方が、バランスよく遂行されるよう、日常から配慮しているかが重要な鍵となるものです。ひいては職場へのセキュリティ文化の浸透や、その認識を確認することが必要であったためです。幸い監査の対象となった各管理者には、今日のセキュリティ問題の認識のもと、それぞれが業務の特性に立って、取組まれている姿勢が確認できました。

（セキュリティ対策の管理状況の把握）

システム監査にあたっては、もとより「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」によって行うことですが、具体的には、その情報システムの特性をふまえ、組織的・人的、技術的、物理的のそれぞれの管理面での対応策について把握したところです。具体的事項は本報告の区分別項目を参照してください。

総じては、推奨される点は、次のとおりです。

・組織的・人的管理面では、「事故・欠陥等の報告」「緊急時対応計画の策定」「自己点検の実施」
・技術的面では、「通信回線の機密性」「不正プログラム対策」
・物理的面では、「情報資産の維持管理」「機器の廃棄」「機器の定期保守」「パソコン等の管理状況」

また、改善が求められる点として、次の事項があります。

・組織的・人的管理面では、「緊急時対応計画の再点検」「外部委託仕様書のセキュリティ要件の記載」
・技術的面では、「パスワードの取扱い」「アクセス制御・利用者IDの取扱い」
・物理的面では、「情報資産の管理への記載対象の再検討等」

（監査結果を踏まえて）

以上に、述べました推奨する点は、監査の結果、信頼性・可用性の面から適正に管理していると見られる点で、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するものです。

また、改善を求められるとした点は、直ちに情報セキュリティの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理解した上で、改善を要望するものです。

本報告は、監査時点で適正に管理されていると判断したものです。情報セキュリティ環境の変化は激しい分野だけに、各管理者はじめ関係者におかれては、その変化に対応するよう努められることが求められます。そのため区としては、それらに係る情報提供について、一層の充実を図られることを期待したいところです。

（２）推奨する点

① 対応及び適切な連絡体制が定められていました。
② 保守事業者の対応窓口が明確にされていました。
③ 緊急時対応計画が定められていました。
④ 毎年度、全職員対象の自己点検が実施され、情報セキュリティ対策状況が確認されていました。
⑤ 機密性に配慮した適切な回線が使用されていました。
⑥ 不正プログラムへの感染が疑われる場合に、直ちに通信ケーブルを取り外し、情報システム課に連絡する対処ができるよう研修等を通じて周知徹底されていました。
⑦ 契約書類、受付書類等は適切に鍵のかかるキャビネットに保管されていました。
⑧ データ消去証明書が保管されていました。
⑨ 保守契約により、定期的な保守が実施されていました。
⑩ 端末等はセキュリティワイヤで固定され、適切に管理されていました。
⑪ 各システムはログイン時にパスワードの入力が必須となっていました。
⑫ 主要な端末では重要データの持ち出しができないよう外部記録装置の利用が制限されていました。

（３）改善を求める点

① 緊急時の対応フロー図がすべてのシステムにおいてほぼ同じ対応の流れとなっており、各所属・システムごとの実情に即した実効性があるか疑わしいものでした。
② 仕様書にあるセキュリティ要件の記載の一部にシステムの形態との不一致がありました。
③ 一部のシステムで、パスワードを長期間変更していない、または変更が利用者任せになっていました。
④ 一部のシステムで、利用者ＩＤを複数担当者間で共有していました。
⑤ 担当でなくなった職員のＩＤが削除されていないシステムがありました。
⑥ ＯＡパソコンが配布された各課においては情報資産管理台帳に記載されていませんでした。
⑦ 情報資産管理台帳に、データ量の記載がありませんでした。
⑧ データの保存期間について、一部で客観的な基準が無い状態となっていました。
⑨ 一部の所属で、情報資産管理台帳に記載している書類が一般の書類と混在する形で保管されていました。