荒川区情報セキュリティ

監査報告書

（概要版）

平成２６年１２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系システムの利用現場を対象に、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上、改善方法等について助言、指導を行いました。

また、委託事業者の管理下に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ました。

3　監査範囲

番号	監査対象課	監査対象システム
1	環境課	省エネ管理システム
2		公害苦情処理システム
3	職員課	人事給与システム
4	情報システム課	職員ポータル・グループウェア
5		文書管理システム

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26年 9月18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26年10月15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（環境課）
平成26年10月29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（職員課、情報システム課）
平成26年11月20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26年12月24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	（１）情報資産の管理（２）通信ケーブル等の配線 （３）機器の定期保守及び修理（４）通信回線（５）パソコン等の管理 （６）机上端末の管理（７）事故・欠陥等の報告（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）緊急時対応計画 （１２）外部委託（１３）自己点検

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

① 情報資産管理台帳について

「バックアップデータ」や「アクセスログデータ」も重要な情報資産です。各職場の情報資産管理台帳に載せておく必要があります。一般に情報資産としての認識が薄いのですが、一旦何等かの事故が発生した場合、必要不可欠のものです。

次ぎに、情報資産の名称について、媒体の特性が理解しやすいように、表記することが望ましい点が見うけられました。情報資産管理台帳を整備することは、情報セキュリティリスクを洗い出すという点で非常に重要です。正しい情報資産管理台帳を作成することが、適切なセキュリティ対策のスタートです。統一的なルールのもとに、その充実が期待されます。

②利用者ＩＤ・パスワードについて

監査対象のなかで､パスワードを定期的に変更していないシステムがありました。定期的にパスワード変更を行う運用への改善を求めます｡更に良い対応策としては、「一定期間を過ぎたパスワードは無効にするなど､システム上での仕様追加を行う」ことも検討することが有効です。

また、パスワードをファイルにて保存、管理する場合は、パスワードロックを行い、管理責任者のみがそのパスワードを管理する体制が必要となります。システム管理を業務委託し、作業を受託業者が実施する場合においても、区側で責任をもって管理してください。

③緊急時対応計画について

各課とも緊急時における手順を作成し、明確にしていた点は評価できます。緊急時対応手順を基に、いざという時にすぐに対応できることが重要であるため、更に実効性を高めるためには、その内容の定期的な確認と、緊急時を想定した訓練の実施等を行うことが望まれます。

また、緊急時には、当然想定しきれないケースが多々あるため、事象検知後に、その影響度合に応じた対応手順や連絡ルート等を確立しておくことが重要だと考えます。その点で、荒川区で定めているＩＣＴ－ＢＣＰがありますので、これを参考にして、各システムが必要な部分を抜粋し緊急時の対応手順や連絡ルート等を確立してください。

④外部委託について

システム管理・保守の業務委託については、委託先について実質的に管理・監督することが重要です。主に保守作業等の報告が定期的にある場合は、その機会にいろいろと質問するなど、コミュニケーションを密にして、実態を把握することが有効です。

次に、インターネット上のサービスを利用するシステムの利用契約においては、稼働率や復旧時間等のような品質やサービスの内容について、達成できなかった場合のルールを定めた合意書を作成し、委託事業者との間でお互いに基準とその状況を確認していくことが望ましいと考えます。

また、荒川区において、外部委託契約時には、基本的に再委託を禁止していますが､やむなく必要な場合は､「再委託の届出」により承認をもらうことはもちろんのこと、契約書上に､「再委託先の管理」という項目を追加し、再委託先を区は管理、監督する環境を整備しておくことが重要です。

（２）推奨する点

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。
②外部記憶媒体への書き込みが容易に行えないよう適切な措置が講じられていました。
③適切な連絡体制が定められ事業者の問合せ窓口が明確にされていました。
④端末での操作ログは、全て取得されており、過去１年以上長期にわたってログ閲覧が可能な状態でした。

（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バックアップデータとアクセスログデータについても重要な情報を含む資産です。情報資産管理台帳へ追記してください。

②荒川区が定めるＩＣＴ－ＢＣＰを基に、各システムにおいて必要な部分を抜粋し、障害の種類による影響度合に応じた手順を策定してください。

③外部委託事業者が作業者から受領した誓約書については、内容を確認し、区側でも写しを取得し保管しておくことが望まれます。