荒川区情報セキュリティ

監査報告書

（概要版）

平成２６年３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、業者選定の方法、契約内容及び委託業務の管理・監督状況について、ホームページ等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も合わせ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	広報課	区公式ホームページ
2	子育て支援課	あらかわ子育て応援サイト
3	教育総務課	学校情報配信システム
4	南千住図書館	図書館システム

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25年12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26年 1月29日	実地調査	監査証拠確認、執務室視察、職員へのインタビュー　対象課（子育て支援課、広報課）
平成26年 1月30日	実地調査	監査証拠確認、執務室視察、職員へのインタビュー　対象課（教育総務課、南千住図書館）
平成26年 2月18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 3月13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

パソコン、プリンター等の機器類の記載漏れが散見されました。また、課ごとに記載方法が不統一であったほか、システム関連文書の保存期間の考え方にも検討の余地が感じられました。

正しい情報資産管理台帳を作成することが、適切な情報資産の管理につながりますので、統一的なルールを確立するなど、今後の充実が期待されます。

②利用者ＩＤ・パスワードについて

多くのシステムで利便性を重視するあまり、利用者のＩＤ・パスワードの共用が見られました。個人ごとに専用の利用者ＩＤ・パスワードを付与する運用に改めることを検討してください。

また、システムにおける誤入力チェックについて、セキュリティの面から、パスワードのみ誤った場合でも、そのことを特定されないようなメッセージにするなどの配慮も必要です。

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及びフロー図を作成し、明確にしていた点は評価されますが、その内容については、実行性に疑問を感じる部分がありました。

局所化と一報までを想定される障害状況ごとに明確化し、より実践的なものとすべきです。

また、手順に従って訓練を実施するなど、緊急時対応に対する職員一人一人の意識を向上させる方策についても検討してください。

④外部委託について

今回の監査対象としたシステムでは、導入選定時にセキュリティ対策の評価のウエイトが低いように感じられました。導入選定時にも一定程度考慮するようにしてください。

ウェブシステムについては、委託先と十分な連携の下、外部からの攻撃の監視、異常事象発見の際の対応策を明確にすることを検討してください。

また、インターネット上のサービスを利用するシステムでは、サービスの内容や品質を達成できなかった場合のルールを定めた合意書を作成することを推奨します。

（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通信回線はセキュリティ水準に見合った適切な回線が使用されていました。

②カウンターの端末は利用者から画面が見えないよう配慮されていました。

③不正プログラム対策として、ウィルス対策ソフトウェアが導入され、自動的に最新のパターンファイルに更新されていました。

④委託先業者との契約において、基本的なセキュリティ要件はすべてのシステムで契約条項に明記されていました。

（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情報資産管理台帳について、記載誤りや記載漏れがありました。

②システムの利用者ＩＤが共用されていました。責任追跡性の観点から個人ごとの利用者ＩＤでの運用を検討してください。

③委託先業者の選定時には業務受託実績や機能を重視し、決定していました。今後は、これらに加えて、具体的な情報セキュリティ対策の実施状況について確認することや必要に応じて認証取得状況等を選定条件とすることを検討してください。