荒川区情報セキュリティ

監査報告書

（概要版）

平成２９年１月

1　監査目的

平成２９年７月に社会保障･税番号制度における情報連携が開始します。これに伴い、特定個人情報をはじめとする重要な各種情報を取り扱う業務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確認します。また、監査結果をもとに、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うえ、改善方法等について助言、指導を行います。

また、特定個人情報を使用する業務については、上記を確認のうえ、関係法令、基準に従い適切に管理、運用されているかどうか確認します。

3　監査範囲

番号	監査対象課	監査対象システム
1	税務課	税務システム
2		税滞納整理支援システム
3	戸籍住民課	住民記録システム
4		住民基本台帳ネットワークシステム
5		戸籍システム

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28年9月20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28年10月26日	実地監査 事前打合せ	監査資料の内容等の確認
平成28年11月30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（対象課：税務課、戸籍住民課）
平成29年1月26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

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

オ　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

カ　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

キ　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

ク　荒川区個人番号の利用等に関する条例

ケ　荒川区個人番号の利用等に関する条例施行規則

コ　荒川区特定個人情報取扱基準

サ　荒川区特定個人情報取扱手順

（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

ア 全体

監査の結果は、情報セキュリティの要件としての機密性、完全性、可用性の面から全体として、適正に管理していると見ることができます。しかし、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、一部に改善が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た上で、引き続き情報セキュリティ対策を徹底されることを期待するところです。

イ 監査対象ドキュメント

監査対象となった関係ドキュメントは、多種多量にわたっています。これらの整備状況は一般的に良好で、業務主管課と情報システム部門との協力により、よく整備されているといえます。これらの整備過程で、担当部門の情報セキュリティに対する内部監査的要素や普及啓発効果も考えられ、推奨されるべき方向といえます。

ウ 業務委託契約にあたっての対応

区における業務委託契約の標準的条項は､現在､再委託は原則禁止としていますが､IT 業界の産業構造から再委託は避けられない状況といえます｡このため業務委託契約にあたっては、再委託についての対応を検討していく必要があるといえます。

具体的には、マイナンバー制度のもとでの再委託の要件として「委託者の許諾を得た場合に限り、再委託をすることができる」とし、又、再委託先への「間接的な監督義務を負うこととなる」としています。特に、再委託の許諾を与える際には、特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断しなければならないとしていることに留意が必要です。

更に、この５月から施行される改正個人情報保護法においても、そのガイドラインで､再委託の場合､「委託先から事前報告を受け又は承認を行うこと、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等」により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が適切に安全管理措置を講ずることを十分に確認するよう求めている状況です。

これらのことから業務委託契約にあたって、再委託に係る事項を明確にし、その適正化について検討が求められるところです。

エ 緊急時対応の組織的対応

緊急対策の中心が情報システムに偏重しているように見られる点が懸念されるところです。現在の事故対策は、従来のように単に情報システムにとどまらず、業務全般に及ぼすようになってきており、極めて多様な対応策が求められるといえます。

具体的には、これまでのセキュリティ事故の調査分析や復旧にとどまらず、庁内関係システムとの調整、業務が中断したときの影響分析と再開計画、国や都等公的部門への報告と調整、住民やマスコミ等への広報、復旧に伴う短期・長期の必要な財政措置と法的対応、業務委託事業者・セキュリティ専門事業者との調整、再発防止策等々です。

このためには、事故発見時点の早期から経営層や関係部門長からなる緊急対策会議

（仮称）を立ち上げて、事故対策の万全と被害の最小化に対応する必要があるところです。

（２）推奨する点

ア　利用者IDについて、台帳が作成されており、適正に管理されていました。また、人事異動等により、システムにアクセスする必要がなくなった場合に対象となる利用者IDの削除を迅速に行っており、利用権限のない者からの不正アクセスに対する対応が適正にとられていました。

イ　重要な情報資産について、台帳で適正に管理するとともに、その取り扱い状況が業務フロー図により明らかにされていました。

ウ　システムのログインは生体認証又はIDとパスワードによる認証が必須とされていました。

エ　端末機から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を制限し、庁内ネットワークを介して管理するための仕組みが組み込まれていました。

（３）改善を求める点

ア　現在、パスワードを１年に１回の変更とされていますが、定期的に変更する運用へ切り替えるよう検討してください。

イ　情報資産管理台帳の記載内容について、作成者によって記載が異なる点がみられるので、統一性の確保について検討される必要があります。