荒川区情報セキュリティ

監査報告書

（概要版）

平成３０年１月

1　監査目的

平成２９年１１月に社会保障・税番号制度における情報連携が開始されました。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	介護保険課	介護保険システム

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29年 9月27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29年11月21日	実地監査 資料事前送付	監査資料の内容等の確認
平成29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（対象課：介護保険課）
平成30年 1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		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

ア　全体

監査の結果は、情報セキュリティの機密性、完全性、可用性の特性のほか、その付加的な特性としての真正性、責任追跡性、否認防止、信頼性の４点についても、全体として適正に管理されているところです。

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・迅速に対応されることを期待します。

イ　情報資産管理について

監査対象の業務の特性から、情報資産の種別は多種多様にわたっています。その前提条件のもとで、情報資産管理台帳は、情報セキュリティ対策の把握の基本台帳として、適切に管理される必要があります。その内容は、情報資産名をはじめ、格納媒体、保管場所、利用者の範囲等にも及んでいるところです。

監査結果としては、この整備状況は、全体としてよく整備されており、推奨されるべき方向といえます。

ウ　業務フロー図について

情報資産管理台帳と関連性の深い監査対象ドキュメントとして、業務フロー図があります。この業務フロー図の作成には、実務的には多種多様であり、一般に困難を伴うものと思考されます。そのため、多くの関係職員の協力が、求められるところであります。

しかし、それが実施された場合の成果は、チームワークの醸成、業務の標準化や改善策の発見、業務やリスクの透明化、職員への普及啓発等、直接・間接に効果が大きいものです。

監査の結果は、作成の負担を克服し良く整備されており、その取組みは高く評価されるものです。今後は、その充実に一層の取り組みが期待されるところです。

エ　今後に期待したい事項

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、次の事項について改善を求められるところです。

・一次的保管の情報記録媒体の管理

情報記録媒体のうち業務の特性から、USB メモリや支払いデータのように、一時的に保管されるものに対し、情報資産管理台帳に記載が省略されているものがあります。これらはリスク管理の視点からも、重要な管理対象となるものです。そのため情報資産管理台帳に掲載し、管理責任、利用者の範囲、保管場所等について明確化する必要があるところです。

・室内ケーブルの補完

室内のケーブルのカバーが短く、束ねた各種のケーブルが一部表面に露出しているところが見受けられました。これはセキュリティ対策の面から看過できない点であり、カバーの補完を期待したいところです。

・一般用プリンターの管理

プリンターについて、業務用と一般用に区別され利用されています。この中で一般用について、利用による使用、配布、廃棄等について、情報の印刷による活用面から、その記録をとり、適正な管理を期待したいところです。