報告監８の第１号
令和８年１月30日

大阪市監査委員　森　伊吹
同　森　恵一
同　大橋一隆
同　土岐恭生

令和７年度監査委員監査結果報告の提出について

（財政局所管システムにおける情報セキュリティ対策に関する事務）

地方自治法（昭和22年法律第67号）第199条の規定による監査を実施し、その結果に関する報告を以下のとおり決定したので提出する。

第１　大阪市監査委員監査基準への準拠

本監査は、大阪市監査委員監査基準に準拠して実施した。

第２　監査の種類

地方自治法第199条第１項及び第５項の規定に基づく財務監査
地方自治法第199条第２項の規定に基づく行政監査

第３　監査の対象

１　対象事務

財政局所管システムにおける情報セキュリティ対策に関する事務

・　主に直近事業年度及び進行事業年度を対象とした。

２　対象システム

税務事務システム(注)

（注）　財政局が所管する税務事務システムは、各税目の賦課、収納管理、滞納整理に至る税務事務を処理し、オンライン処理による情報の一元管理と共有化、バッチ処理による「大量データの一括処理」、「大量帳票外部媒体出力処理」等の処理形態を取り、事務処理の効率化などを実現するシステムである。

３　対象所属(注)

財政局、デジタル統括室、中央区役所及び城東区役所

（注）　財政局は税務部、あべの市税事務所及び弁天町市税事務所を対象とする。

第４　監査の着眼点

監査の実施に当たり、重要リスク及び監査の着眼点を次のとおり設定した。

重要リスク	監査の着眼点	監査の結果
（1）情報セキュリティ管理体制が十分でなく、適切な情報セキュリティ対策が実施されず、重大な情報セキュリティインシデントが発生するリスク	ア　対象システムにおける情報セキュリティ管理体制が構築されているか。	－
	イ　情報セキュリティ実施手順は、情報セキュリティポリシー等に準拠して作成され、対策基準の変更等に対応して適宜見直されているか。また、関係者に周知徹底されているか。	指摘事項１
（2）情報セキュリティ対策の整備・運用状況が適切でなく、重大な情報セキュリティインシデントが発生するリスク	ア　情報資産等の管理が適切に実施されているか。	指摘事項２
	イ　ＩＤ及び権限が適切に管理されているか。	－
	ウ　ＯＳ等のバージョンアップやセキュリティパッチの適用、ウイルス対策ソフト等の対応が適切に実施されているか。	－
	エ　システム障害発生時に、緊急度や影響度を判断し、対応するための手順が策定されているか。また、障害管理が適切に行われているか。	－
（3）情報セキュリティに関するモニタリングが有効に機能せず、重大な情報セキュリティインシデントが発生するリスク	ア　各種ログは適切に取得され、定期的に分析されているか。	－
	イ　情報セキュリティに関する自己点検が実施され、不備事項についての改善措置が適時実施されているか。	－
	ウ　外部委託先とＳＬＡ等により、情報セキュリティの管理状況等について定期的にモニタリングし、評価しているか。	－
（4）過去に実施した監査で指摘した事項が実行・改善されず、業務が有効又は適正に実施されないリスク	ア　過去に実施した監査で指摘した事項が実行・改善されているか。	－

（注）１　監査の結果欄の「－」の項目については、今回の監査の対象範囲において試査等により検証した限り、指摘に該当する事項が検出されなかったことを示すものである。

２　情報セキュリティインシデントとは、情報セキュリティを脅かす事件や事故及びセキュリティ上好ましくない事象・事態のことをいう。

３　ＳＬＡ（Service Level Agreement）とは、事業者が利用者に対しサービスをどの程度の品質で提供するのか明示した契約のことをいう。

第５　監査の主な実施内容

監査手続は試査を基本とし、質問・閲覧等の手法を組み合わせて実施した。

第６　監査の結果

第１から第５までの記載事項のとおり監査した限り、重要な点において、監査の対象となった事務が法令に適合し、正確に行われ、最少の経費で最大の効果を挙げるようにし、その組織及び運営の合理化に努めていることがおおむね認められた。

ただし、是正又は改善が必要な事項は以下のとおりである。

１　実施手順の周知について改善を求めたもの

【財政局に対して】

デジタル統括室が定めている大阪市情報セキュリティ対策基準（以下「対策基準」という。）によれば、局等情報セキュリティ責任者は、局等における情報セキュリティの連絡体制を利用し、情報セキュリティ責任者その他必要と認める者に対し、ポリシー及び実施手順の周知徹底を行わなければならないとされている。また、局等が実施する研修等により、所属員に対しポリシー及び実施手順の遵守について啓発しなければならないとされている。

また、税務事務システム・電子申告システム情報セキュリティ実施手順（以下「実施手順」という。）には、管理体制及び役割について次のとおり定められている。

≪管理体制及び役割≫

情報セキュリティ責任者は、所管する情報資産の情報セキュリティ対策が適切かつ確実に実施されるよう必要な措置を行う。また、職員等に対するセキュリティポリシー及び実施手順の遵守に関する指導、助言又は研修その他情報セキュリティ確保のために必要な措置を行う。

なお、実施手順は令和６年４月１日付けで改正されており、令和６年３月 27 日付けでシステム所管所属の財政局税務部情報統括管理者からシステム利用所属あてに、全対象職員に対して周知する旨の内容が記載された通知文により通知された。

【令和６年４月１日実施手順の改正内容（抜粋）】

「情報セキュリティ対策」へ以下項目の追加

■ 組織・体制及び役割・責任

システムの情報資産について、全庁的な組織・体制及び役割・責任に基づき情報セキュリティ対策を行う。

■ 点検・評価及び見直し

点検・評価を実施し運用改善を行い、必要に応じて適宜情報セキュリティポリシーの見直しを行う対策を講じるものとする。

「セキュリティポリシー及び実施手順等の遵守状況の確認」へ以下の追加

セキュリティポリシー及び実施手順に違反した職員等及びその監督責任者は、その重大性、発生した事象の状況等に応じて、地方公務員法及び大阪市職員基本条例に基づき懲戒処分の対象となる場合がある。

今回の監査において、実施手順の周知状況について確認したところ、次のとおりであった。

財政局（弁天町市税事務所管理担当）において、令和６年４月１日の実施手順改正について、担当内のシステム利用職員に改正内容の周知を行っていなかった。
管理担当に確認したところ、令和６年３月 27 日付けで通知のあった実施手順の改正について、改正内容を確認したものの、担当内のシステム利用職員に周知が必要な改正内容ではないと判断し周知を行わなかったことが判明した。

これは、本件通知について、管理担当が改正内容の確認を行った際に、改正内容はシステム利用職員が遵守すべき事項にかかる内容ではなく、システム利用職員に周知する必要はないものと判断したことが原因である。

現状では、実施手順の改正内容を熟知していないシステム利用職員により、適切な情報セキュリティ対策が実施されず、重大な情報セキュリティインシデントを招くリスクがある。
したがって、次のとおり指摘する。

［指摘事項１］
財政局は、実施手順の改正の通知があった場合は、改正内容の確認を徹底するとともに、システム利用職員まで確実に周知されるよう、情報セキュリティ責任者の下、規定に基づき実施されたい。

２　外部記憶デバイスの管理について改善を求めたもの

【財政局に対して】

デジタル統括室が定めている対策基準によれば、情報セキュリティ責任者は、データの重要性が容易に識別できるよう、ファイルが格納された記録媒体等の保管について台帳整備し、所定の場所において適切に管理しなければならないとされている。
さらに、外付けハードディスクや外付けＳＳＤ等のサーバなどパソコン等の端末機の外に置きケーブル等で接続するタイプの記憶装置の場合は、これら外付けハードディスク等の現物と台帳に記録された識別番号について定期的に照合点検しなければならないとされている。

また、実施手順には、情報資産の管理について次のとおり定められている。
≪情報資産の管理≫
外部記憶デバイスは、施錠できるロッカー等にて保管し、紛失・盗難がないように適切に管理しなければならない。また、情報セキュリティ責任者は常に使用されている外部記憶デバイスの所在を把握し、紛失・盗難がないか確認し、少なくとも１年に１回は外部デバイス管理簿へ確認結果を記録すること。

今回の監査において、外部記憶デバイスの管理状況について確認したところ、次のとおりであった。

財政局（課税課個人課税グループ）において、外部記憶デバイスとしてＵＳＢメモリを３本登録し使用していたが、情報セキュリティ責任者による１年に１回以上実施すべき、外部記憶デバイスの所在確認は行っていたものの、管理簿への確認結果の記録を行っていなかった。

また、ＵＳＢメモリ３本のうち１本については、ＵＳＢメモリ自体にラベル等の貼付けがなく、台帳（管理簿）に記録された識別番号と容易に照合点検できない状態であることから、適切に管理しているとは言い難い状況であった。

これは、実施手順における外部記憶デバイスの管理方法の理解が不十分であったことが原因である。

また、システム所管所属策定の外部記憶デバイスの管理方法等を取りまとめた「税務事務システム等外部記憶デバイスの取扱手順」において、ＵＳＢメモリへのラベル等の貼付けによる管理方法が記載されていなかったことが原因である。

現状では、当該システムの運用において、情報セキュリティ対策が適切に実施されず、情報セキュリティインシデントを招くリスクがある。

したがって、次のとおり指摘する。

［指摘事項２］

財政局は、１年に１回以上の外部記憶デバイスの所在確認及び管理簿への確認結果の記録について、情報セキュリティ責任者の下、規定に基づき実施されたい。

また、デジタル統括室が定めている対策基準に基づき外部記憶デバイスが適切に管理されるよう、「税務事務システム等外部記憶デバイスの取扱手順」にラベル等の貼付けによるＵＳＢメモリの管理方法について追記し周知されたい。

第７　その他

特になし