報告監７の第９号
令和７年３月26日

大阪市監査委員　森　　伊吹
同　森　　恵一
同　岡田妥知
同　福田武洋

令和６年度監査委員監査結果報告の提出について

（大阪市行政オンライン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

大阪市行政オンラインシステム(注)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。

(注)　デジタル統括室が所管する大阪市行政オンラインシステムは、個人や事業者が、マイナンバーカードを用いた公的個人認証やクレジットカード等による手数料の電子決済を利用して、住民票の写しの請求や行政手続の申請など、パソコンやスマートフォンから簡単に手続等を行えるクラウドサービス（ＬＧＷＡＮ-ＡＳＰ対応）である。令和２年８月から利用を開始し、オンライン申請できる手続数の増加に伴い、利用する職員数も増加しており、全庁的に利用されている（令和６年12月末時点での職員アカウント数　約１万件）。

２　対象所属

デジタル統括室、総務局、政策企画室、水道局、及び行政委員会事務局（選挙部除く）

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。	－
（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。	－
	イ　ＩＤ及び権限が適切に管理されているか。	指摘事項１
	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　ユーザＩＤの管理等について

【デジタル統括室、政策企画室及び行政委員会事務局に対して】

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によれば、業務管理者は、システムのアクセス権限の把握、管理を適切に行わなければならないとされている。

また、大阪市行政オンライン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、管理体制及びアクセス制御について次のとおり定められている。

≪管理体制≫

- 業務管理者は、デジタル統括室デジタルサービス担当課長が担当し、本システムの運用、保守の実施並びに管理を担い、本システムが正常に稼働するよう、安全性に十分配慮し適切な運用管理を担う。
- 利用所管管理者については本システムを利用する職員等が所属する課等の長が担当し、円滑に業務処理が実施されるよう本システムの利用管理を担う。

≪アクセス制御≫

- 業務管理者および利用所管管理者は、本システムへのアクセス権限の把握、管理を適切に行う。特に職員等の異動や退職時にともない発生する不要なユーザＩＤは速やかに消去する。
- 業務管理者および利用所管管理者は、利用されていないユーザＩＤが放置されないよう１年に１回点検する。

なお、上記ユーザＩＤの追加・削除等の設定及び点検に関して、職員の異動に伴うシステムの利用開始を円滑に行うため令和６年３月１日付けで図表－１のとおり実施手順を改正することについて、令和６年２月 28 日付けでデジタル統括室から各所属あてに通知された（以下「取扱変更通知」という）。

図表－１　実施手順の改正内容

	改正後	改正前
実施手順の規定	①　業務管理者および利用所管管理者は、本システムへのアクセス権限の把握、管理を適切に行う。特に職員等の異動や退職時にともない発生する不要なユーザＩＤは速やかに消去する。 ②　業務管理者および利用所管管理者は、利用されていないユーザＩＤが放置されないよう１年に１回点検する。	①　業務等管理者は、本システムへのアクセス権限の把握、管理を適切に行う。特に職員等の異動や退職時にともない発生する不要なユーザＩＤは速やかに消去する。 ②　業務等管理者は、利用されていないユーザＩＤが放置されないよう、１年に１回点検する。

今回の監査において、各利用課及びデジタル統括室における、実施手順改正後のユーザＩＤの管理状況についてそれぞれ確認したところ、次のとおりであった。

（１）利用課である政策企画室におけるユーザＩＤの管理について改善を求めたもの

政策企画室（広報担当、報道担当）において、当該システムを利用する職員のユーザＩＤの点検が実施されていなかった。

また、令和６年度当初に利用所属職員が人事異動により他所属へ移った後も、不要となったユーザＩＤが削除されず登録されたままとなっていた。

当該事実を受け、政策企画室において取扱変更通知がどのように周知されていたか確認したところ、庶務担当部署である秘書課から各利用課へ取扱変更通知が伝達されておらず、各利用課が取扱いの変更について認識できていなかったことが判明した。

秘書課は、所属内への照会・周知事項に関して各課へ漏れなく伝達できるよう、日頃から組織として進捗を管理していたものの、取扱変更通知については見落としたとのことであった。

また、各利用課においても、当該システムを操作する主たる担当者に異動がなかったため実務上支障がなく、毎年度、デジタル統括室へ手続を依頼していたユーザＩＤの追加・削除等を令和６年度は実施していないことについて疑問を感じず、確認を行っていなかった。

これは、取扱変更通知が所属内で周知されていなかったという実態はありつつも、当該システムの利用に当たって、利用課として利用する職員とユーザＩＤが適正か常日頃から点検・管理するという意識を十分に持てていなかったことが原因である。

現状では、正式な権限のない職員により不要となったユーザＩＤが使用され、不正な操作が行われることや、情報が持ち出されることにより、重要な情報の流出等の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（１）］

政策企画室は、利用課としての役割を認識した上で、当該システムに係るユーザＩＤの権限設定及び点検について、実施者や実施時期を明文化して組織として引き継ぐなど、規定に基づき実施できるよう仕組みを構築し、運用されたい。

（２）利用課である行政委員会事務局におけるユーザＩＤの管理について改善を求めたもの

行政委員会事務局（任用調査課任用担当）において、当該システムを利用する職員のユーザＩＤの点検が実施されていなかった。

また、令和６年度当初に利用所属職員が人事異動により他所属へ移った後も、不要となったユーザＩＤが削除されず登録されたままとなっていた。

これは、取扱変更通知について、所属内で周知はされていたものの、繁忙時期であったため精読できておらず、利用課として自らユーザＩＤの権限設定等を実施するよう取扱いが変更されたことを十分認識できていなかったことが原因である。

現状では、正式な権限のない職員により不要となったユーザＩＤが使用され、不正な操作が行われることや、情報が持ち出されることにより、重要な情報の流出等の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（２）］

行政委員会事務局は、利用課としての役割を認識した上で、通知の確認を徹底し、当該システムに係るユーザＩＤの権限設定及び点検について、実施者や実施時期を明文化して組織として引き継ぐなど、規定に基づき実施できるよう仕組みを構築し、運用されたい。

（３）業務管理者であるデジタル統括室におけるユーザＩＤの点検や利用所属への通知について改善を求めたもの

改正後の実施手順においても、デジタル統括室は業務管理者としてユーザＩＤの点検を行うことが定められている。

デジタル統括室によれば実施手順改正前後の役割分担は図表－２のとおりであり、改正後は、ユーザＩＤの点検について各利用課が実施する形となっており、業務管理者として点検状況を把握する仕組みとなっていなかった。

図表－２　実施手順改正前後の役割分担

	改正後	改正前
デジタル統括室	①　部課に「利用課の長」がいない場合や、大量の職員登録が必要な場合といった例外的なケースについて、各利用課から提出される依頼書に基づき、ユーザＩＤの追加・削除等の設定を実施する。 ②　実施手順の周知を行う。	①　各利用課から提出される依頼書に基づき、ユーザＩＤの追加・削除等の設定を一括して実施する。 ②　５～６月を目途に、その時点で登録済のユーザＩＤ一覧を各利用課に展開し、削除対象について報告を受け、その内容に基づき一括で削除する。
各利用課	①　組織改正や人事異動に伴い、各利用課の「利用課の長」が、ユーザＩＤの追加・削除等の設定を実施する。 ②　実施手順に基づき、１年に１回（任意のタイミングで）、自所属のユーザＩＤの点検（棚卸）を実施する。	①　組織改正や人事異動に伴い、デジタル統括室に、ユーザＩＤの追加・削除等の設定を依頼する。 ②　展開されたユーザＩＤ一覧を確認し、デジタル統括室に削除対象職員を報告する。

また、今回の監査において、２所属で不備が検出されたユーザＩＤの権限設定等について、図表－１のとおり実施手順には明記されているものの、取扱変更通知は「利用課の長の権限設定を変更したことにより、所管部課における職員情報の照会及び編集（追加・削除等）が可能となります。」との記載に留まっており利用課として果たさなければならない役割が十分伝わらない表現となっていた。

さらに、各利用課でも年に１回実施することとなったユーザＩＤの点検について、取扱変更通知にその旨の記載はなく、実施手順を遵守する旨の記載があるのみであったことや、令和６年４月の人事異動以降のタイミングにおいて、デジタル統括室から各利用課へ点検実施の通知が行われておらず、各利用課が確実に点検を実施できる効果的な通知ができていたとは言いがたい状況となっていた。

デジタル統括室によると、実務上、各ユーザＩＤが不要であるか否かは各利用課でしか正確に把握できないことから、上記の対応で十分と考えていたとのことであるが、業務管理者としての役割の一つであるユーザＩＤの点検という事項については一部その役割を果たせているとは言えない状況であった。

これは、ユーザＩＤの点検に関して、実施手順改正前後での業務管理者としての役割を具体的に整理できていなかったことが原因である。

現状では、（１）（２）で記載したとおり各利用課で適切にユーザＩＤの点検が行われず、正式な権限のない職員により不要となったユーザＩＤが使用され、不正な操作が行われることや、情報が持ち出されることにより、重要な情報の流出等の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（３）］

デジタル統括室は、業務管理者としての役割を改めて認識した上で、当該システムに係るユーザＩＤの点検について、各利用課から結果の報告を受けて状況を確認するなど、規定に基づき適切に実施できるよう仕組みを構築し、運用されたい。

また、各利用課が自らの役割を正確に認識した上で、実施手順に基づきセキュリティ対策を講じられるように、当該システムに係る取扱変更や実施手順の改正に当たっては、周知の時期や記載内容、方法を検討するなど工夫して、的確に伝わるよう取り組まれたい。

第７　その他

特になし