報告監６の第７号
令和６年３月27日

大阪市監査委員　森　伊吹
同　森　恵一
同　ホンダ　リエ
同　辻　義隆

令和５年度監査委員監査結果報告の提出について

（区役所附設会館等予約システム及び公害健康被害補償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次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

区役所附設会館等予約システム及び公害健康被害補償システムにおける情報セキュリティ対策に関する事務に対する当該監査は、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

区役所附設会館等予約システム（市民局所管）及び公害健康被害補償システム（健康局所管）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　対象所属

市民局、健康局、両システムの利用所属として住之江区及び住吉区
上記に加え、情報セキュリティ検査(注)等業務をとりまとめているデジタル統括室を対象とした。

(注)　大阪市情報セキュリティ管理規程（平成19年達第19号）に基づき、各情報システムにおいて情報セキュリティ対策が適切かつ確実に実施されているかどうかを検証するため、各所属が自己点検を実施し、その内容についてデジタル統括室が検査を実施している。

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	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　システム所管部署内の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、本市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　情報システム室等の入退室やシステム利用者のＩＤ及び権限が適切に管理されているか。	指摘事項１（１）
	イ　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。	指摘事項２（１） 指摘事項２（２）
	ウ　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。	指摘事項１（２）
	エ　情報システム室等の自然災害や火災等に対する物理的対策は適切か。	－
	オ　情報資産を廃棄、リース返却等をする際に適切な措置を講じているか。	－
(3)情報セキュリティに係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を見逃すリスク	ア　システムのアクセスログが取得され、定期的に分析されているか。	指摘事項１（３）
	イ　情報セキュリティ管理に係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。	指摘事項２（１）
	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。	指摘事項１（４） 指摘事項２（３）
(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　情報システム室とは、情報システムのサーバが置かれている室のことをいう。

４　アクセスログとは、情報システムに対する操作について日時、利用者等の情報を記録したものをいう。

５　ＳＬＡ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次のとおりである。

１　区役所附設会館等予約システムについて

市民局が所管する区役所附設会館等予約システムは、区役所附設会館及びクレオ大阪の施設・附属設備、並びにクレオ大阪の講座の予約を管理するためのシステムである。

区役所附設会館に関することは市民局施設担当が、クレオ大阪に関することは市民局男女共同参画課が、それぞれ事務を担当している。

（１）区役所附設会館におけるユーザＩＤの管理について改善を求めたもの

【市民局（施設担当）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「本市対策基準」という。）によれば、業務管理者等は、システム及びネットワークへ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、当該システムの「情報セキュリティ実施手順（以下「実施手順」という。）」（区役所附設会館版）(注) には、アクセス制御について次のとおり定められている。

（注）　区役所附設会館等予約システムの実施手順は、区役所附設会館（指定管理者施設及び直営会館）については区役所附設会館版、クレオ大阪５館についてはクレオ大阪版の２種類をそれぞれ作成し、運用している。

・　業務等管理者は、システムへのアクセス権限の把握、管理を適切に行う。特に職員の異動や退職に伴い発生する不要なユーザＩＤは速やかに消去する。
・　業務等管理者は、利用されていないＩＤが放置されないよう、６か月に１回点検する。

しかし、今回の監査において、ユーザＩＤ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。

■　市民局（施設担当）では、市民局職員以外の各施設でのユーザＩＤの管理について、各施設に管理を任せており、ＩＤ登録等の状況について把握できていなかった。
■　市民局（施設担当）は、システムに不具合が起きたときに誰がいつ操作したかのログ確認を可能とするため、個人ごとにシステム利用者ＩＤを登録・利用することを各施設に求めているが、共用ＩＤを登録し、利用していると思われる施設があり、個人のログイン状況を確認できない状況となっていた。

■　区役所附設会館において、同一名称のユーザＩＤが複数登録されている施設があるなど、不要なＩＤが削除されずそのままとなっていた。
■　市民局（施設担当）では、実施手順に定める６か月に１回の点検を実施していなかった。

これは、本市対策基準の理解が不十分であったことから、市民局として自らアクセス権限の把握、管理を実施しなければならないという認識が不足していたため、ユーザＩＤの管理・運用に関する手続を具体的に整理しておらず、本市対策基準や実施手順に基づきアクセス権限の把握、管理を実施できる仕組みがなかったことが原因である。

現状では、不正アクセスや不正操作等の履歴を確認できず、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、以下のとおり指摘する。

［指摘事項１（１）］
市民局は、本市対策基準の趣旨を踏まえた上で、ユーザＩＤの管理・運用に関する手続を具体的に整理し、所属内や各施設に対して周知徹底されたい。
また、点検結果を記録として残すなど、アクセス権限について組織として把握・管理できる仕組みを構築されたい。

（２）区役所附設会館における連絡体制について改善を求めたもの

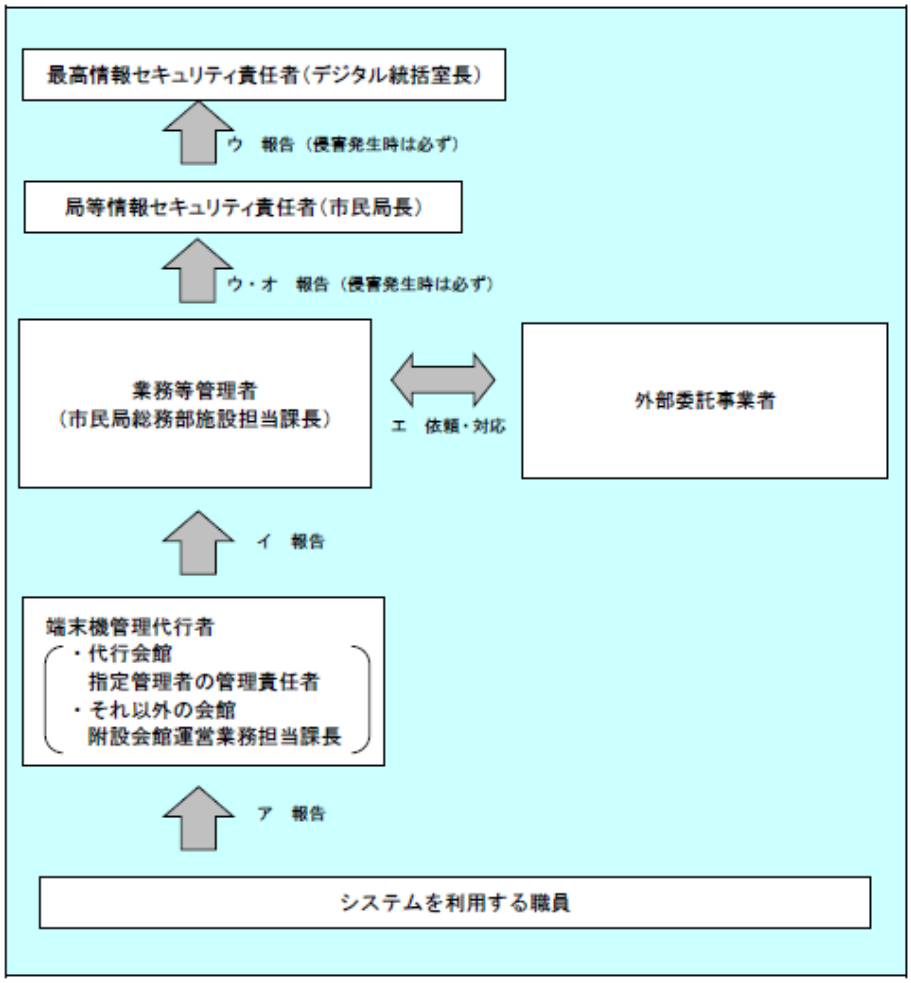
【市民局（施設担当）に対して】

本市対策基準によれば、局等情報セキュリティ責任者（局長等）は局等における情報資産に関する情報セキュリティ対策の連絡体制を設置し、関係者等と連絡調整を行うとされている。

区役所附設会館（指定管理者施設）では、区役所及び指定管理者施設の職員が当該システムを利用しており、システムに関係する連絡・通知等については、市民局（施設担当）から区役所へ、区役所から指定管理者へ、という体制がとられている。

しかし、実施手順（区役所附設会館版）では、障害・侵害時の連絡体制図を図表－１のとおり定めており、区役所の関与については記載がなかった。

図表－１　連絡体制図（区役所附設会館版）



（注）　実施手順（区役所附設会館版）を監査部において加工（外部委託事業者連絡先等を削除）

これは、所管するシステムの実態を考慮せず実施手順を定めていたことが原因である。

現状では、連絡体制について関係者の中で認識の相違が起き、当該システムにおける障害・侵害時の連絡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、以下のとおり指摘する。

［指摘事項１（２）］

市民局は、運用実態を考慮した上で適切な連絡体制を定め、実施手順に反映されたい。

（３）区役所附設会館及びクレオ大阪におけるアクセスログの分析について改善を求めたもの

【市民局（施設担当及び男女共同参画課）に対して】

本市対策基準によれば、業務管理者等は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存し、定期に又は随時に分析するために必要な措置を講じなければならないとされている。

また、当該システムの実施手順（区役所附設会館版・クレオ大阪版）によれば、業務等管理者が各種ログを取得し、随時に、侵害及びその兆候がないかどうか分析を行うこととされている。

しかし、今回の監査において、各種ログの取得・分析状況について確認したところ、次のとおりであった。

■　市民局（施設担当及び男女共同参画課）は、各種ログについて、システム運用事業者において一括で保管・分析させ、一定回数のログイン失敗など不正ログインの疑いがある場合は報告させることとしているが、市民局として各種ログの取得・分析を行っておらず、実施手順と異なった運用となっていた。
■　市民局（施設担当）に確認したところ、区役所附設会館はかなりの数があることから、各種ログの取得・分析を自ら行うことは現実的に困難との認識であった。

これは、所管するシステムの実態を考慮せず実施手順を定めていたことが原因である。

現状では、現実的には実行できない手続を実施手順に記載することで実施手順が形骸化し、適切な手続が引き継がれずに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、以下のとおり指摘する。

［指摘事項１（３）］
市民局は、本市対策基準の趣旨を踏まえ、デジタル統括室と協議した上で、現実的に実行できる適切な各種ログの取得・分析の実施方法について検討し、速やかに実施手順を改正・運用されたい。

（４）事業者が講じるセキュリティ対策の実施状況の確認について改善を求めたもの

【市民局（施設担当及び男女共同参画課）に対して】

本市対策基準によれば、システム保守等の外部委託での管理については、事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ契約に基づき措置しなければならないとされている。
また、当該システムの実施手順（区役所附設会館版・クレオ大阪版）には、事業者への管理、指導について次のとおり定められている。
・　業務等管理者は、サービス提供事業者に対して、実施手順に準拠した情報管理体制、情報セキュリティ対策を講じるよう要求し、その運用状況について必要なセキュリティ対策が確保されているか随時に確認、調査を行う。また、月次報告等にてＳＬＡ実施状況等の情報セキュリティ対策状況の確認を行う。

しかし、今回の監査において、事業者によるセキュリティ対策の実施状況について確認し

たところ、次のとおりであった。

■　市民局（施設担当及び男女共同参画課）は、事業者から提出される保守点検報告書等により、サーバの稼働状況やバックアップの取得状況等のＳＬＡ実施状況について、毎月確認していたが、同じくＳＬＡで定められているウイルス対策やセキュリティパッチの更新については報告書に記載がなく、それらが実際に講じられているか把握できていなかった。

これは、今まで運用上特に問題が起こっていなかったことから、事業者において当然に上記セキュリティ対策が講じられているものとして、事業者任せとなっていたことが原因である。

現状では、当該システムにおけるウイルス対策等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、以下のとおり指摘する。

［指摘事項１（４）］
市民局は、事業者にウイルス対策等の実施状況について報告を求めることなどにより、セキュリティ対策が実施されていることを確認できる仕組みを構築されたい。

２　公害健康被害補償システムについて

健康局が所管する公害健康被害補償システムは、公害健康被害認定患者の情報をデータベース化し、診療報酬等支払いデータや各種帳票の作成等をするためのシステムである。

（１）ウイルス対策ソフトの更新について是正を求めたもの

【健康局に対して】

本市対策基準によれば、業務管理者等は、システムがインターネットに接続していない場合、定期的にウイルスチェック用のソフトウェア及びパターンファイルの更新を実施しなければならないとされている(注)。

(注)　同じく本市対策基準によれば、システムがインターネットに接続している場合は、ウイルスチェック用のソフトウェア及びパターンファイルを常に最新の状態に保つように努めなければならないとされている。

また、当該システムの実施手順によれば、ウイルス対策ソフトのパターンファイルは、入手した定義ファイルをもとに、四半期ごとに手動で更新するとされている。

しかし、今回の監査において、ウイルス対策ソフトの更新状況について確認したところ、次のとおりであった。

■　ウイルスチェック用のソフトウェア及びパターンファイルの更新について、令和４年１月の機器更新以降実施されていなかった。

■　健康局は、本件について、令和３年度に実施した情報セキュリティ検査（自己点検）において「定期的なウイルスソフトの更新が実施されていない」と「×」の自己評価をし、改善策として「端末業者と調整し、四半期に一度を目安に、今後、定期的に更新を実施する」ことを、とりまとめ担当であるＩＣＴ戦略室（現デジタル統括室）に報告していた。

その後、令和４年度にデジタル統括室から本件に対してフォローアップがあった際には、上記端末機器更新時にウイルス対策ソフトが最新化されたことをもって「改善完了」として報告していたが、定期的に更新する仕組みが構築されないままとなっていた。

これは、ウイルス対策ソフトの更新の必要性自体は認識していたものの、当該システムがインターネットに接続しておらず、今までの運用上ウイルス感染等の問題も特に起こっていなかったことから、早急に対応が必要な案件として認識しておらず、仕組みの構築を先送りにしていたことが原因である。

現状では、当該システムにおけるウイルス対策ソフトの更新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、以下のとおり指摘する。

［指摘事項２（１）］

健康局は、ウイルスチェック用のソフトウェア及びパターンファイルについて定期的な更新を行うことができる仕組みを早急に構築されたい。

（２）記録媒体の管理について改善を求めたもの

【健康局に対して】

本市対策基準によれば、記録媒体等の管理について、台帳を整備・記録することとされている。

また、当該システムの実施手順によれば、記録媒体等によりデータをやり取りする場合には、必ず事前にウイルスチェックを実施すること、情報セキュリティ責任者は別途定める「記録媒体等取扱マニュアル」(注) に基づき記録媒体等を適切に管理することとされている。

（注）　当該システムにおいては、デジタル統括室が作成する「記録媒体等取扱マニュアル（サンプル）」を準用しているとのことであり、当該マニュアルでは、担当内で使用する記録媒体等の全てを一元的に管理するために記録媒体等を管理簿へ登録することや、ウイルスチェックを実施することなどが定められている。

しかし、今回の監査において、記録媒体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。

■　保有する記録媒体（ＵＳＢ）５本のうち４本については、担当課において受渡簿を作成することで、受け渡す相手方、日時等については一定の管理を行っていたものの、情報セキュリティ責任者への報告・管理簿への登録がされないまま、日常的に利用されている状況であった。
■　保有する記録媒体（ＵＳＢ）５本について、ウイルスチェックが実施されていなかった。

これは、本市対策基準や記録媒体に関する情報セキュリティ対策の理解が不十分であったことから、上記の運用による管理で足りると認識していたことが原因である。

現状では、記録媒体に関する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、以下のとおり指摘する。

［指摘事項２（２）］
健康局は、本市対策基準や記録媒体に関する情報セキュリティ対策の趣旨を踏まえた上で、当該システムにおいて保有する記録媒体を速やかに管理簿へ登録し、ウイルスチェックを徹底するなど適切な情報セキュリティ対策が確保できる仕組みを構築されたい。

（３）運用保守業務委託における事業者の管理・監督について改善を求めたもの

【健康局に対して】

本市対策基準によれば、システムの運用、保守を所管する業務管理者等は、これらの業務の全部又は一部を事業者に委託しようとする場合の留意事項として、調整・管理機能、スケジュール等業務全体の遂行を左右する重要な要件や機能を本市のコントロール下におくこととされている。
また、公害健康被害補償システム保守業務委託仕様書には、障害管理や障害保守などの詳細については本市と協議の上決定し、事業者が作成する業務計画書に明記することが記載されており、健康局として、業務計画書の内容を承認した上で、事業者が業務計画書に基づき保守業務を実施しているかを管理・監督する必要がある。

しかし、今回の監査において、事業者から提出された業務計画書等を確認したところ、次のとおりであった。

■　健康局は、毎月開催される定例会で事業者から業務報告を受けることで、障害管理等が一定実施されていることを事後的には確認していたものの、業務実施前に提出される業務計画書には、障害管理や障害保守などの実施方法、内容、実施サイクル、対応策、報告等の詳細についての記載がなく、事業者が実施すべき保守業務の内容・手法等が明確になっていなかった。

これは、今まで運用上特に問題が起こっていなかったことから、事業者において当然にセキュリティ対策が講じられるものとして、事業者任せとなっていたことが原因である。

現状では、当該システムにおける障害管理等の情報セキュリティ対策が適切に実施されず、システム障害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、以下のとおり指摘する。

［指摘事項２（３）］

健康局は、事業者に対し、仕様書に基づく業務計画書の作成・提出を求め、障害管理の方法や内容などの業務要件の詳細を承認し、業務計画書に基づき事業者を適切に管理・監督されたい。

第７　その他

留意すべき事項（市民局及び健康局に対して）

今回の監査では、各システムにおいて本市対策基準や実施手順に基づいた情報セキュリティ対策が実施できていない事項について、上述のとおり指摘した。

個別具体的に改善を求める事項については、各指摘事項に記載したところであるが、市民局及び健康局は、当該事項を改善した後も、各システムの情報セキュリティ対策が適切に実施されているか、規定と運用に乖離がないかなど、定期的に確認するよう取り組まれたい。

留意すべき事項（全庁的なセキュリティ体制の確保・強化について）

大阪市情報セキュリティ管理規程によれば、情報セキュリティに係る体制として、本市に最高情報セキュリティ責任者を置き、デジタル統括室長をもって充てること、また、最高情報セキュリティ責任者は、本市における情報セキュリティを総括し、情報セキュリティ対策の統一的な実施に必要な指導、助言又は調整を行うことが規定されている。

デジタル統括室においては、これまでも、全庁的な情報セキュリティ研修の実施や、各所属における情報セキュリティ検査（自己点検）を実施する仕組みの整備、所属ごとの支援担当窓口の設置など、各所属の支援に取り組んでいる。

しかし、この間、情報セキュリティに関する事務を対象として監査委員監査を実施している中では、監査対象としたシステムにおける情報セキュリティ対策が十分とは言えないとして、例年、同様の指摘をしており、監査の対象となっていないシステムにおいても同じような状況にあることが懸念される。

本市は、令和５年３月に「大阪市ＤＸ戦略」を策定し、安全・安心かつ安定的な行政サービス

を実現するために、情報セキュリティ対策をＤＸと同時に推進していくことを基本的な考え方の一つとして掲げて取組を進めているところであり、今後ますます、情報セキュリティ対策の実効性の確保と対策レベルの向上に向けた取組が必要不可欠となる。

デジタル統括室は、監査委員監査の結果等も踏まえ、各所属が所管するシステムにおいて、規定に基づき適切に情報セキュリティ対策が実施できているか等を確認できるように、情報セキュリティ検査（自己点検）の検査項目を工夫されたい。

また、各システムの所管所属や、本市の情報セキュリティを総括しているデジタル統括室は、現行の仕組みにとらわれることなく、監査委員監査で検出されているような、規定等の見落としや判断誤り等による人的セキュリティリスクをできる限り排除できる仕組みづくりを進め、全庁的なセキュリティ体制の確保・強化を目指されたい。