報告監４の第２号
令和４年２月25日

大阪市監査委員　森　伊吹
同　森　恵一
同　片山一歩
同　明石直樹

令和３年度監査委員監査結果報告の提出について

（統合型ＧＩＳ及び大阪市立斎場予約受付システムにおける情報セキュリティ対策に係る事務）

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

統合型ＧＩＳ及び大阪市立斎場予約受付システムにおける情報セキュリティ対策に係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

統合型ＧＩＳ及び大阪市立斎場予約受付システムにおける情報セキュリティ対策に係る事務

・　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

計画調整局(注)及び環境局

（注）令和３年11月１日に都市計画局から局名変更

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　システム所管部署等の情報セキュリティ管理体制が構築されているか。	指摘事項２ 指摘事項３
	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。	指摘事項２
（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４
	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５
	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。	―
	エ　情報システム室の自然災害や火災等に対する物理的対策は適切か。	―
（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
	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 指摘事項５
	ウ　外部委託先とのＳＬＡ等により、運用時のサービス内容、サービス品質、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３

（注）１　監査の結果欄の「ー」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。

３　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。

４　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。

5　ＳＬＡとは、Service Level Agreement の略で、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。

なお、大阪市立斎場予約受付システムについては、外部委託による脆弱性診断(注)を併せて実施した。

(注)　専用の診断ツールを使用し、診断実施環境からインターネット経由で対象システムにアクセスし、外部の攻撃者からインターネット経由で攻撃を受ける可能性があるかといった観点で、脆弱性の有無を調査すること

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　計画調整局に対してアクセスログの分析について是正を求めたもの

【ルール、あるべき状況等】

大阪市情報セキュリティ対策基準(注)1（平成 31 年４月１日）によれば、業務管理者(注)2、サーバ等管理者及びネットワーク管理責任者は、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、定期にまた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、統合型ＧＩＳ情報セキュリティ実施手順(注)3（令和３年３月 19 日）によれば、外部委託業者はシステムの各操作に関してログを取得するとされており、そのログを５年間保存し、月に１回又は随時に、侵害及びその兆候がないかどうか分析するとされており、発見時には連絡体制に基づき報告することとなっている。

(注) 1　本報告書　参考 1 本市の情報セキュリティ対策の概要（1）情報セキュリティポリシー参照

2　業務管理者は、システムの開発及び運用、保守の実施並びに管理を担い、当該システムに係る業務を所管する課等のリーダー又は長をもって充てるとされている。

3　本報告書　参考 1 本市の情報セキュリティ対策の概要（2）情報セキュリティ実施手順参照

【現状】

監査において、統合型ＧＩＳ（庁内向け）(注)の職員及び外部委託業者のログイン状況を確認した。職員については、外部委託業者から毎月報告されるユーザー別ログ統計（令和元年 12 月から令和３年４月まで）から、ログインしている状況が、外部委託業者については、上記期間中の作業記録から、ログインして作業を実施している状況が確認できた。

しかし、外部委託業者が、ログを取得し、月１回又は随時に実施すべきとされている「侵害及びその兆候がないかどうかの分析」について、都市計画局（調査時）に確認したところ、「外部委託業者にてシステム監視・分析が行われており、その監視・分析の結果、これまでの委託

期間において侵害及びその兆候が認められていない」との回答であったが、その作業実績、分析結果は確認できなかった。

（注）　本報告書　参考 2　統合型ＧＩＳの概要参照

【問題発生の原因】

アクセスログを分析し、不正アクセスや不正操作等の有無を確認することについて、その分析結果が確認できないのは、定期的な報告がなく、侵害及びその兆候が認められた際にのみ報告を受けるという手順に留まっていたことが原因と考えられる。

【リスク】

現状では、不正アクセスや不正操作等を見逃し、個人情報等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］

業務管理者は、不正アクセスや不正操作等の有無を確認するため、外部委託業者に対して、職員及び外部委託業者自身のＩＤも含めた全体のログについて、侵害及びその兆候がないかどうか分析した結果を定期的に提出するよう指示し、その分析結果を確認すること。

２　環境局に対して指定管理者の業務について是正及び改善を求めたもの

【ルール、あるべき状況等】

大阪市情報セキュリティ対策基準によれば、情報システム室管理責任者（当該システムの運用管理を所管する課等のリーダー等）は、許可を受けた者が情報システム室へ入室するときは、次の事項等を記録しなければならないとされている。

- 入室年月日
- 入退室時分
- 所属または団体名及び氏名
- 入室目的
- その他情報システム室管理責任者が必要と認める事項

大阪市立斎場予約受付システム(注)1（以下「斎場予約受付システム」という。）の情報システム室は環境局所管の斎場に設置されており、その斎場は、指定管理者(注)2により管理されている。

当該業務に関する指定管理者募集要項によれば、指定管理者は、情報資産に関する情報セキュリティの履行に際して、大阪市情報セキュリティ管理規程及び大阪市情報セキュリティ対策基準並びに情報セキュリティ実施手順を遵守することとされている。

（注）１　本報告書　参考 3　大阪市立斎場予約受付システムの概要参照

２　指定管理者制度は、地方自治法第 244 条の２により公の施設（地方自治法第 244 条第１項に規定する公の施設をいう。）について、地方公共団体が指定する指定管理者に管理を代行させる制度

【現状】

情報システム室の入退室は「サーバー室入退室管理簿」に記録され、指定管理者の責任者により確認された上で、月例報告により環境局斎場霊園担当課長へ報告する運用となっていた。また、情報システム室の入退室に必要な鍵は指定管理者によって管理されていた。

しかし、次のような事実が確認された。

■　大阪市立斎場予約受付システム情報セキュリティ実施手順(注)（平成 29 年８月１日）を確認したところ、情報システム室管理責任者についての記載はなく、情報システム室の入退室記録や鍵の管理について具体的な運用方法が明記されていなかった。また、指定管理者の業務に関する仕様書にも、情報システム室の管理について記載はされていなかった。

■　指定管理者から提出された 12 か月間（令和２年４月から令和３年３月まで）の「サーバー室入退室管理簿」を確認したところ、様式に「入室目的」を記載する欄が設けられていなかった。また、上記期間中の入退室 41 件のうち、入室について所属の記載がないものが 20 件、氏名の記載がないものが 11 件あった。

（注）　本報告書　参考 1 本市の情報セキュリティ対策の概要（2）情報セキュリティ実施手順参照

【問題発生の原因】

上記の状況が発生した原因として、以下のことが考えられる。

■　平成 29 年に指定管理者制度を導入した際に、情報システム室の管理に関して、情報セキュリティ実施手順や指定管理者の業務に関する仕様書に記載すべき内容が十分に検討されていなかった。

■　入退室管理に関する様式を定める際に、大阪市情報セキュリティ対策基準の内容と適合しているか確認できていなかった。また、入退室管理簿の記載に関して、関係者への周知が徹底されていなかった。

【リスク】

現状では、情報システム室の入退室管理について指定管理者が行う業務が不明確であることから、業務が適正に履行されているかが確認できず、入退室管理が適正に行われずに本市の重要な情報資産が損なわれるリスクがある。

したがって、以下のとおり指摘する。

［指摘事項２］

1.　業務管理者は、情報セキュリティ実施手順や指定管理者の業務に関する仕様書に、情報システム室の管理に関する指定管理者の業務について追記し、指定管理者に実施させること。

2.　業務管理者は、情報システム室の入退室管理に関する様式に「大阪市情報セキュリティ対策基準」に定められた項目を適切に反映するとともに、入退室時の記録に関する要領を定めて関係者に周知し、適切に運用されていることを確認すること。

３　環境局に対して外部委託の扱いについて是正及び改善を求めたもの

【ルール、あるべき状況等】

本市職員が主体性を持って運用保守業務（外部委託）を実施していくために最も重要なことは「委託業者に作業内容や作業結果の報告を求め、承認・確認すること」と、システム運用保守における委託管理の手引き（令和２年４月１日　ＩＣＴ戦略室）に記載されている。

また、同手引きによると、本市は、委託業者が運用保守計画に基づき適切に作業しているかを管理するとされている。本市職員は、委託業者から作業実施前に作業内容の詳細について説明を求め、その作業内容と安全性を確認した上で作業実施を承認し、作業後には委託業者から作業結果や作業の実績工数等の報告を求め、正しく作業が完了したか確認するとされている。

【現状】

現在の外部委託の状況を確認したところ、斎場予約受付システムのソフトウェア及び機器一式は、いずれも借入契約（「リース契約」と同義）を結んでいた。

令和３年度に締結された借入契約の「大阪市立斎場予約受付システムソフトウェア借入仕様書」及び「大阪市立斎場予約受付システム用機器一式借入仕様書」を確認したところ、図表－１に示すとおり、過年度と同様、いずれも保守サポート業務を含んでいることが確認できた。

図表－１　各借入契約の仕様書に記載されている保守サポート業務の内容

	大阪市立斎場予約受付システム ソフトウェア借入仕様書	大阪市立斎場予約受付システム用 機器一式借入仕様書
保守内容	（１）平常時保守サポート ①ヘルプデスクサービス ②データベース保守 ③バージョンアップ対応 （２）緊急時対応サポート ①リモートメンテナンス保守 ②パッケージの不具合対応 ③サーバ障害時の復旧対応	（１）障害時連絡対応、問診 （２）障害切り分け作業 （３）予備品の用意 （４）ソフトウェアサポート ①ソフトウェア、ファームウェア、 ドライバ、パッチ等の改良版の提供 ②マニュアル改訂版の提供 ③保守、技術情報等の提供 ④各種技術支援 （５）保守サービス一覧 ①ハードウェア ・サーバ関連機器 ・セキュリティ関連機器 ②ソフトウェア ・ソフトウェア関連保守 ・ライセンス保守

（注）　１　環境局提供資料「大阪市立斎場予約受付システムソフトウェア借入仕様書」「大阪市立斎場予約受付システム用機器一式借入仕様書」を参照し、監査部において抜粋した。

２　「大阪市立斎場予約受付システム用機器一式借入仕様書」の保守内容にあるソフトウェアには、ミドルウェアに分類されるものを含んでいる。ミドルウェアとは、ＯＳとアプリケーションの間で、両者の機能を補佐するために動くソフトウェアである。

前述の借入契約のほかに、令和２年度にはミドルウェア等の更新作業の実施のため、「ミドルウェア等業務」を外部委託しており、その受託者は、ソフトウェア借入契約の受託者と同一業者であった。

上記各契約の実施体制を整理し、図表－２に示す。

図表－２　各契約の実施体制

	ソフトウェア 借入契約	機器一式 借入契約	ミドルウェア等 業務委託契約
受託者	業者Ａ	業者Ｂ	業者Ａ
実作業担当（窓口）	業者Ａ	業者Ａ	業者Ａ

■　図表－２のとおり、機器一式借入契約に含まれる保守サポート業務の体制として、ソフトウェア借入契約の受託者（業者Ａ）が窓口を担当している。本来、業者Ａを窓口とすることについて、機器一式借入契約の受託者（業者Ｂ）から報告を受けるべきものであるが、環境局は、業者Ａから報告を受けていた。

■　機器一式借入契約における「大阪市立斎場予約受付システム用機器一式借入仕様書」を確認したところ、本市に保守体制、サポート内容・方法について文書として提示する旨の規定は設けられていなかった。また、保守サポート業務の実施状況を本市に報告することを求める規定は、確認できなかった。

■　ソフトウェア借入契約における「大阪市立斎場予約受付システムソフトウェア借入仕様書」の規定により、毎月提出されている業者Ａからの完了報告書（令和２年４月から令和３年５月まで）を確認したところ、保守作業内容の記述がどの完了報告書においても全く同じであり、ヘルプデスクサポートの工数等、詳細な実施状況を確認できる記載はなかった。

■　前述の完了報告書とは別に、業者Ａから提出された作業完了報告書(注)（令和２年度分、17 件）を確認したところ、全件について、どの契約に関するものか明示されていなかった。記載されている作業内容により、どの契約に関するものか判断できる作業完了報告書もあったものの、詳細な作業内容が書かれていないため、どの契約に関するものか明確となっていないものが４件含まれていた。

（注）　情報システム室で実施された作業に関して、都度提出される報告書

【問題発生の原因】

実質的に、ソフトウェア借入契約、機器一式借入契約及びその他システムに関する業務委託契約の窓口を同一業者が担当しているという状況において、実施される作業内容等を、契約毎に確認し、管理しなければならないという認識が不十分であったことが原因と考えられる。

【リスク】

現状では、契約している保守サポート業務が確実に実施されないことにより、システムの可用性(注)が十分に確保されないリスク、保守作業内容等に関する詳細な情報が記録されないこ

とにより、情報セキュリティインシデント発生時に追跡調査ができず障害管理等が適正に行われなくなるリスクがある。

したがって、以下のとおり指摘する。

(注)　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること

［指摘事項３］

1.　業務管理者は、機器一式借入契約の保守サポート体制に関して、機器一式借入契約の受託者から提示を受けるよう改めること。

2.　業務管理者は、委託業者を適切に管理するため、機器一式借入契約の業務仕様書を改訂するとともに、作業完了報告書等を提出させる際は、どの契約に基づくものか分かるように契約名称を記載させ、作業内容等についても明確な記載を求めて、その内容を定期的に確認すること。

４　環境局に対してＩＤ、パスワードの管理について改善を求めたもの

【ルール、あるべき状況等】

大阪市立斎場予約受付システム情報セキュリティ実施手順によれば、システムを管理・利用する職員（指定管理者を含む。）はパスワードの使用に際して、次の項目等に留意し管理することとされている。

■　初回ログイン時に配布された仮のパスワードは、最初のログイン時に変更する。

■　６か月に１回、パスワードを変更する。

【現状】

斎場予約受付システムには、一定期間を経過するとパスワードが無効となる機能が実装されていなかった。そのため、パスワード管理として、月例報告会において指定管理者に定期的にパスワードを変更するよう指示していたが、指定管理者のパスワード変更実施を確認できなかった。

【問題発生の原因】

パスワードの管理がシステム利用者に委ねられており、変更実施を確認する仕組みが確立されていないことが原因と考えられる。

【リスク】

現状では、パスワードの変更が確認できず、パスワードが長期間変更されないことにより、退職者などシステムを利用してはならない者に不正ログインされ、重要情報にアクセスされるリスクがある。

したがって、以下のとおり指摘する。

［指摘事項４］

業務管理者は、パスワードが確実に変更されるようシステムに機能を追加するか、若しくは変更実施を確認できる仕組みを構築し、その実施状況を確認すること。

５　環境局に対して脆弱性診断結果に係る対応について是正及び改善を求めたもの

【ルール、あるべき状況等】

大阪市立斎場予約受付システム情報セキュリティ実施手順によれば、「業務管理者及びシステム運用管理者は、定期的にＪＰ／ＣＥＲＴ(注)1やＩＰＡセキュリティセンター(注)2・Microsoft 等のホームページからセキュリティに関する情報を定期的に収集し、最新の動向を把握する」とされている。

（注）１　ＪＰＣＥＲＴ／ＣＣは、コンピュータセキュリティの情報収集、対応の支援、コンピュータセキュリティ関連情報の発信などを行う、特定の政府機関や企業からは独立した中立の組織である。

２　ＩＰＡは独立行政法人情報処理推進機構の略。セキュリティセンターは、国内外の関係機関と連携し、民間では収集が困難な情報収集、分析とそれらの知見の一般化を行う。

【現状】

今回の監査において、斎場予約受付システムに対して脆弱性診断を実施したところ、緊急に対策を要する脆弱性が１件、その他に緊急度は低いものの情報セキュリティインシデントに繋がる恐れがある脆弱性が７件検出された。

【問題発生の原因】

セキュリティに関する情報を定期的に収集し、最新の動向を把握するための具体的な手法、手続が確立されておらず、新たに発見された脆弱性に関する情報を、所管する情報システムに反映できていなかったことが原因と考えられる。

【リスク】

現状では、外部からの攻撃により重要な情報が流出し、本市の信用を失墜するリスクがある。したがって、以下のとおり指摘する。

［指摘事項５］

1.　業務管理者は、検出された脆弱性のうち、特に緊急度の高い脆弱性について速やかに対策を決定し、実行すること。また、それ以外の脆弱性についても改善に向けた方針を決定すること。

2.　業務管理者は、情報セキュリティに関する脆弱性の情報について、定期的に収集し最新の動向を把握するとともに、適切に対応するための仕組みを構築すること。

第７　その他

なし

参考

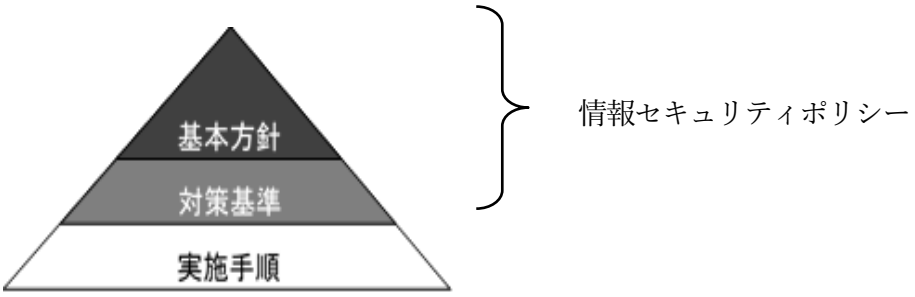
１　本市の情報セキュリティ対策の概要

（１）情報セキュリティポリシー

地方公共団体における情報セキュリティ対策については、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（令和２年 12 月 28 日改定　総務省）により、その徹底のために対策を組織的に統一し、明文化された情報セキュリティポリシーを定めなければならないとされ、図表－３の体系が提示されている。

情報セキュリティポリシーは、当ガイドラインにおいて「組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう」とされている。

図表－３　情報セキュリティポリシーに関する体系図



基本方針：情報セキュリティ対策における基本的な考え方を定めたもの

対策基準：基本方針に基づいて全ての情報システムに共通の情報セキュリティ対策の基準を定めたもの

実施手順：対策基準を、具体的なシステムや手順、手続に展開して個別の実施事項を定めたもの（情報セキュリティポリシーの下位文書）

上記を踏まえ、本市では、基本方針として大阪市情報セキュリティ管理規程（令和３年４月１日改正）を、対策基準として大阪市情報セキュリティ対策基準（平成 31 年４月１日改正）を定め、セキュリティポリシーとして運用している。

（２）情報セキュリティ実施手順

本手順は情報セキュリティポリシーの下位文書として、所管する情報システム又は情報通信ネットワーク単位に、情報セキュリティ対策の実施に関し必要となる事項を定めることとされている。

２　統合型ＧＩＳの概要

（１）システムの概要

システムの概要を図表－４に示す。

図表－４　統合型ＧＩＳの概要

		統合型ＧＩＳ（市民向け） 通称：マップナビおおさか	統合型ＧＩＳ（庁内向け）
所管	局等名	計画調整局	
	部課等名	企画振興部統計調査担当	
運用保守業者		株式会社パスコ	
システムの概要		【目的】市民サービスの向上やアカウンタビリティの向上を図るなど、市民参加のまちづくりの推進につなげる。 【機能】電子地図上にわかりやすく行政情報を掲載、配信するなど、情報発信機能を強化するとともに、双方向に情報交換できる環境を整備	【目的】庁内横断的に活用し、各部署における地図データ整備の重複の解消、データ作成費用の削減等、経費の削減、業務の効率化を図る。 【機能】背景図となる共通電子地図と各部署の保有する行政情報を関連付け、これらをシステムにより一元的に管理
運用開始年月		平成 22 年４月にクラウドサービスを利用して運用開始 平成 25 年４月に委託業者変更	平成 22 年１月に運用開始 平成 26 年 11 月に委託業者変更
		令和元年 11 月に統合型ＧＩＳとして再構築（庁内向けもクラウドサービスに移行）	
利用者		市民、企業・団体、職員	職員
サービス時間帯		毎日　00：00～24：00	
サーバ設置場所		クラウド事業者のデータセンター	

（注）　クラウドサービスとは、従来は利用者が手元にあるコンピュータに導入していたようなソフトウェアやデータを、インターネットなどのネットワーク経由で利用者に提供するサービスをいう。

（２）取り扱うデータ

大阪市情報セキュリティ対策基準による重要性分類Ⅰ（個人情報及び業務上必要とする最小限のもののみが扱うデータ）のデータとして、住民情報、法人情報を取り扱う。

３　大阪市立斎場予約受付システムの概要

（１）システムの概要

システムの概要を図表－５に示す。

図表－５　大阪市立斎場予約受付システムの概要

大阪市立斎場予約受付システム		
所管	局等名	環境局
	部課等名	総務部施設管理課（斎場霊園担当）
運用保守業者		都築電気株式会社（システムソフトウェア） 株式会社ＪＥＣＣ（システム用機器一式）
システムの概要		【目的】市立５斎場(北・佃・鶴見・小林・瓜破)の予約受付等を、ＩＤを付与した葬儀取扱事業者が行う。 【機能】火葬、式場、遺体預りの予約受付、予約状況・空き状況の確認、葬儀取扱事業者登録・確認、各種帳票の印刷、炉の故障や設備不調による使用可否状況等の情報提供など
運用開始年月		平成 21 年４月に運用開始
利用者数		職員　　：８名 指定管理者　　：12 名 葬儀取扱事業者：約 500 社
サービス時間帯		毎日　00：00～24：00
サーバ設置場所		本市施設内

（注）　システムソフトウェア、システム用機器一式については、借入契約を行っており、運用保守も借入契約受注者の業務に含まれている。なお、システムソフトウェアはパッケージソフトを本市仕様にカスタマイズしたものである。

（２）取り扱うデータ

大阪市情報セキュリティ対策基準による重要性分類Ⅰ（個人情報及び業務上必要とする最小限のもののみが扱うデータ）のデータとして、使用者（葬儀取扱事業者）の個人・法人情報を取り扱う。

また、重要性分類Ⅱ（公開することを予定していないデータ及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼすデータ）としては、故人の氏名(注)、死亡日等を取り扱う。

（注）　大阪市個人情報保護条例（平成７年３月 16 日条例第 11 号）により、個人情報とは生存する個人に関する情報とされている。

監査結果に関する措置状況報告書

報　告　番　号：報告監４の第２号

監 査 の 対 象：令和３年度監査委員監査　統合型ＧＩＳ及び大阪市立斎場予約受付システムにおける情報セキュリティ対策に係る事務

所　管　所　属：計画調整局

通知を受けた日：令和４年３月15日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
1	１　計画調整局に対してアクセスログの分析について是正を求めたもの 監査において、統合型ＧＩＳ（庁内向け）の職員及び外部委託業者のログイン状況を確認した。職員については、外部委託業者から毎月報告されるユーザー別ログ統計（令和元年12月から令和３年４月まで）から、ログインしている状況が、外部委託業者については、上記期間中の作業記録から、ログインして作業を実施している状況が確認できた。 しかし、外部委託業者が、ログを取得し、月１回又は随時に実施すべきとされている「侵害及びその兆候がないかどうかの分析」について、都市計画局（調査時）に確認したところ、「外部委託業者にてシステム監視・分析が行われており、その監視・分析の結果、これまでの委託期間において侵害及びその兆候が認められていない」との回答であったが、その作業実績、分析結果は確認できなかった。 [指摘事項１] 業務管理者は、不正アクセスや不正操作等の有無を確認するため、外部委託業者に対して、職員及び外部委託業者自身のＩＤも含めた全体のログについて、侵害及びその兆候がないかどうか分析した結果を定期的に提出するよう指示し、その分析結果を確認すること。	（是正内容） ・これまで外部委託事業者にてシステム侵害及びその兆候を発見した場合に報告を受ける手順となっていたが、9月8日の外部委託事業者との保守定例会（月次開催）にて、業務管理者が外部委託事業者に対して、システム侵害及びその兆候の有無に関わらず分析した結果を月次報告するよう指示した。 ・以後、毎月の保守定例会時に報告を受け分析結果の確認を行っている。 （再発防止策） ・統合型GIS情報セキュリティ実施手順において、令和3年11月1日付けで、不正アクセス対策として、外部委託事業者が収集したログについて侵害及びその兆候がないかどうかの分析結果を報告する旨を追記する改正を行った。	措置済	令和3年11月1日

監査結果に関する措置状況報告書

報　告　番　号：報告監４の第２号

監 査 の 対 象：令和３年度監査委員監査　統合型ＧＩＳ及び大阪市立斎場予約受付システムにおける情報セキュリティ対策に係る事務

所　管　所　属：環境局

通知を受けた日：令和５年５月２日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
２	２　環境局に対して指定管理者の業務について是正及び改善を求めたもの 　情報システム室の入退室は「サーバー室入退室管理簿」に記録され、指定管理者の責任者により確認された上で、月例報告により環境局斎場霊園担当課長へ報告する運用となっていた。また、情報システム室の入退室に必要な鍵は指定管理者によって管理されていた。 　しかし、次のような事実が確認された。 ■　大阪市立斎場予約受付システム情報セキュリティ実施手順（平成29年８月１日）を確認したところ、情報システム室管理責任者についての記載はなく、情報システム室の入退室記録や鍵の管理について具体的な運用方法が明記されていなかった。また、指定管理者の業務に関する仕様書にも、情報システム室の管理について記載はされていなかった。 ■　指定管理者から提出された12か月間（令和２年４月から令和３年３月まで）の「サーバー室入退室管理簿」を確認したところ、様式に「入室目的」を記載する欄が設けられていなかった。また、上記期間中の入退室41件のうち、入室について所属の記載がないものが20件、氏名の記載がないものが11件あった。 [指摘事項２] 1. 業務管理者は、情報セキュリティ実施手順や指定管理者の業務に関する仕様書に、情報システム室の管理に関する指定管理者の業務について追記し、指定管理者に実施させること。 2. 業務管理者は、情報システム室の入退室管理に関する様式に「大阪市情報セキュリティ対策基準」に定められた項目を適切に反映するとともに、入退室時の記録に関する要領を定めて関係者に周知し、適切に運用されていることを確認すること。	【1】【2】 ・「斎場予約受付システム情報セキュリティ実施手順」を令和３年12月15日に改正し、情報システム室管理責任者（業務管理者）及び情報システム室の管理に係る事項を追記した。また、入退室時の記録に関し、「大阪市立斎場情報システム室入退室管理要領」を定めて関係者に周知のうえ、実施している。 ・情報システム室の管理に関して指定管理者が実施する業務内容について、「大阪市立北斎場及び大阪市立鶴見斎場指定管理者募集要項変更合意書」を令和３年12月28日に締結し、令和４年１月より業務を実施させている。なお、同合意書において規定する「情報システム室入退室管理簿」の様式については、「大阪市情報セキュリティ対策基準」に定められた項目を反映させたものとしている。 ・上記合意書に基づいて指定管理者から報告される月例報告により、令和４年１月以降、情報システム室への入退室管理及び施錠管理が適切に運用されていることを確認している。	措置済	令和4年2月7日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
3	３　環境局に対して外部委託の扱いについて是正及び改善を求めたもの 　外部委託の状況を確認したところ、斎場予約受付システムのソフトウェア及び機器一式は、いずれも借入契約を結んでいた。令和３年度に締結された借入契約の「大阪市立斎場予約受付システムソフトウェア借入仕様書」及び「大阪市立斎場予約受付システム用機器一式借入仕様書」を確認したところ、いずれも保守サポート業務を含んでいることが確認できた。 　借入契約の他に、令和２年度には「ミドルウェア等業務」を外部委託しており、その受託者は、ソフトウェア借入契約の受託者と同一業者であった。 ■　機器一式借入契約に含まれる保守サポート業務の体制として、ソフトウェア借入契約の受託者（業者Ａ）が窓口を担当している。本来、業者Ａを窓口とすることについて、機器一式借入契約の受託者（業者Ｂ）から報告を受けるべきものであるが、環境局は、業者Ａから報告を受けていた。 ■　機器一式借入契約における「大阪市立斎場予約受付システム用機器一式借入仕様書」を確認したところ、本市に保守体制、サポート内容・方法について文書として提示する旨の規定は定められていなかった。また、保守サポート業務の実施状況を本市に報告することを求める規定は、確認できなかった。 ■　ソフトウェア借入契約における「大阪市立斎場予約受付システムソフトウェア借入仕様書」の規定により、毎月提出されている業者Ａからの完了報告書（令和２年４月から令和３年５月まで）を確認したところ、保守作業内容の記述がどの完了報告書においても全く同じであり、ヘルプデスクサポートの工数等、詳細な実施状況を確認できる記載はなかった。 ■　前述の完了報告書とは別に、業者Ａから提出された作業完了報告書（令和２年度分、17件）を確認したところ、全件について、どの契約に関するものか明示されていなかった。記載されている作業内容により、どの契約に関するものか判断できる作業完了報告書もあったものの、詳細な作業内容が書かれていないため、どの契約に関するものか明確となっていないものが４件含まれていた。 [指摘事項３] 1. 業務管理者は、機器一式借入契約の保守サポート体制に関して、機器一式借入契約の受託者から提示を受けるよう改めること。 2. 業務管理者は、委託業者を適切に管理するため、機器一式借入契約の業務仕様書を改訂するとともに、作業完了報告書等を提出させる際は、どの契約に基づくものか分かるように契約名称を記載させ、作業内容等についても明確な記載を求めて、その内容を定期的に確認すること。	【1】 ・機器一式借入契約の受託者から、機器一式借入契約の保守サポート体制に関して、令和３年10月に保守サポート体制表を提出させている。 【2】 ・作業完了報告書等の提出にあたり、契約名称を記載するとともに、作業内容等について明確に記載するよう指示し、令和３年11月以降、実施している。その際、報告書等に作業内容等が明確に記載されているかを確認している。 ・令和４年度の大阪市立斎場予約受付システム用機器一式借入仕様書に上記内容について、明記した。	措置済	令和4年3月3日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
4	４　環境局に対してＩＤ、パスワードの管理について改善を求めたもの 斎場予約受付システムには、一定期間を経過するとパスワードが無効となる機能が実装されていなかった。そのため、パスワード管理として、月例報告会において指定管理者に定期的にパスワードを変更するよう指示していたが、指定管理者のパスワード変更実施を確認できなかった。 [指摘事項４] 業務管理者は、パスワードが確実に変更されるようシステムに機能を追加するか、若しくは変更実施を確認できる仕組みを構築し、その実施状況を確認すること。	・当該システムは、令和４年度の再構築において、一定期間を経過するとパスワードが無効となる機能を実装し改善する予定とし、改善までの間については、月例報告会等において指定管理者等に定期的にパスワードの変更を指示し、令和４年２月に、管理者権限でパスワードが変更されていることを確認した。 ・令和５年４月１日からの新システムの稼働に伴いパスワード設定６か月後に、パスワードが無効となる機能を実装した。	措置済	令和５年３月31日
5	５　環境局に対して脆弱性診断結果に係る対応について是正及び改善を求めたもの 今回の監査において、大阪市立斎場予約受付システムに対して脆弱性診断を実施したところ、緊急に対策を要する脆弱性が１件、その他に緊急度は低いものの情報セキュリティインシデントに繋がる恐れがある脆弱性が７件検出された。 [指摘事項５] 1. 業務管理者は、検出された脆弱性のうち、特に緊急度の高い脆弱性について速やかに対策を決定し、実行すること。また、それ以外の脆弱性についても改善に向けた方針を決定すること。 2. 業務管理者は、情報セキュリティに関する脆弱性の情報について、定期的に収集し最新の動向を把握するとともに、適切に対応するための仕組みを構築すること。	【１】 ・指摘された脆弱性のうち、特に緊急度の高い脆弱性を含む７件については、令和４年３月15日に当該システムの改修により対応を完了した。 ・残る１件の脆弱性については、令和４年度のシステム再構築により、対応を完了した。 【２】 ・令和４年度の大阪市立斎場予約受付システムＯＳ更新業務委託仕様書に、情報セキュリティに関する脆弱性の情報を定期的に報告する旨を追加し、最新の動向を把握するとともに、緊急度及び深刻度に応じて、システムの動作検証を行ったうえで緊急アップデートを行うなど、システムの安定稼働とセキュリティ対応の両面から適切に対応できる仕組みとした。 （令和４年７月28日　第１回報告）	措置済 措置済	令和５年３月31日 令和４年７月28日

報告監５の第８号
令和５年３月15日

大阪市監査委員　森　伊吹
同　森　恵一
同　杉村幸太郎
同　森山よしひさ

令和４年度監査委員監査結果報告の提出について

（住まい情報センター管理運営システム及び道路橋梁（きょうりょう）総合管理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

住まい情報センター管理運営システム及び道路橋梁総合管理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

住まい情報センター管理運営システム（都市整備局所管）及び道路橋梁総合管理システム（建設局所管）における情報セキュリティ対策に係る事務に関する事務

・　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

都市整備局及び建設局

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。	指摘事項１
	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。	指摘事項１
（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 指摘事項２
	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。	－
	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
	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 指摘事項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１
	ウ　外部委託先とＳＬＡ等により、運用時のサービス内容、サービス品質、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。	－

（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。

３　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。

４　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。

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。

なお、住まい情報センター管理運営システムについては、外部委託による脆弱性診断(注)を併せて実施したところ、サイバー攻撃のリスクとなるような脆弱性は検知されなかった。

（注）　専用の診断ツールを使用し、診断実施環境からインターネット経由で対象システムにアクセスし、外部の攻撃者からインターネット経由で攻撃を受ける可能性があるかといった観点で、脆弱性の有無を調査すること

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　情報セキュリティ実施手順の整備について是正及び改善を求めたもの

【都市整備局及び建設局に対して】

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、情報セキュリティ実施手順（以下「実施手順」という。）の作成や見直しについて、次のとおりとされている。

- 業務管理者(注)1は、セキュリティポリシー(注)2に基づき、当該システムにおける情報セキュリティ対策の実施に関し必要となる事項を定めた実施手順を作成し、局等情報セキュリティ責任者(注)3の承認を得なければならない。
- 局等情報セキュリティ責任者は、所管するシステム及びネットワークについて、ポリシーの変更並びに情報セキュリティをめぐる情勢の変化等に伴い、適宜情報セキュリティ対策の見直しを行ない、必要があると認めるときは、当該システム及びネットワークの実施手順の変更を行わなければならない。

（注）１　業務管理者は、システムの開発及び運用、保守の実施並びに管理を担い、当該システムに係る業務を所管する課等のリーダー又は長をもって充てるとされている。

２　セキュリティポリシーとは、大阪市情報セキュリティ管理規程及び大阪市情報セキュリティ対策基準をいう。

３　局等情報セキュリティ責任者は、情報セキュリティに関する連絡体制の構築並びに職員に対するポリシーの遵守に関する指導、助言及び研修その他局等における情報セキュリティの確保のために必要な措置を行い、局長等をもって充てるとされている。

しかし、今回の監査において、両システムの実施手順の作成、見直しの状況について確認したところ、次の状況が生じていた。

＜住まい情報センター管理運営システム：都市整備局＞

■　当該システムの実施手順は、平成 16 年３月 24 日に作成されており、その見直し、変更は業務管理を担う住宅政策課長が行うこととされている。

■　改定状況を確認したところ、当該システムの実施手順の最終改定は平成 25 年８月 30 日であり、大阪市情報セキュリティ対策基準がそれ以降に複数回改定されている（直近の改定は令和４年４月１日）にもかかわらず実施手順が改定されておらず、以下の例のとおり、現状との不整合や、大阪市情報セキュリティ対策基準に準拠していない項目がある。

・　管理体制の内容が、大阪市情報セキュリティ対策基準に定められている、システムに係る管理体制・役割の内容と異なる。
・　連絡体制の役職名が、現行の組織体制と異なる。
・　データの重要性分類の明文化がされていない。
・　情報システム室に関する記載がない。

■　以下の例のとおり、当該システムの実施手順と現在の運用に不整合が見られる項目がある。

・　当該システムの実施手順の名称は大阪市住宅情報提供システム情報セキュリティ実施手順であるが、システムの名称は機能改修に伴い、大阪市住宅情報提供システムから、住まい情報センター管理運営システムに変更している。
・　実施手順では、バックアップについて、１年に１回、ＤＡＴ(注)を新しいものに交換しなければならないとされているが、現在はＤＡＴを使用せず、バックアップサーバによるデータバックアップを行っている。
・　実施手順では、パスワードは月に１回変更すること及び十分な長さ（４文字以上）とすることとしているが、専用端末へのログインのパスワードについて、設定では、90 日に１回の変更及び８文字以上とするようになっている。また、各サブシステムのパスワードについては変更の時期、長さ、複雑性について運用上の定めがない。
・　実施手順では、アクセス制御は住宅政策課長が実施することとなっているが、実際は、システムを運用・利用する指定管理者の権限付与者が、ユーザＩＤ及びアクセス権限を付与している。
・　実施手順では、各サブシステムに指定管理者職員ごとのユーザＩＤを登録し、このユーザＩＤを割り振られた職員のみが、当該サブシステムにアクセスできるよう設定することとなっているが、実際は、相談対応サブシステムは指定管理者職員ごとのユーザＩＤを登録しているものの、図書検索システムは共用ＩＤで運用している。（指摘事項３後述）
・　実施手順では、業務管理者である住宅政策課長は指定管理者の住まい情報センター所長に対し、サーバ上の重要データへのアクセス及び端末機へのログインのアクセスログの取得と、必要な分析結果の提出を要求すると記載されているが、運用上は住まい情報センター所長に対し定期的な報告を求めておらず、端末機へのログインは共用ＩＤを使用しており、アクセスログの取得及び分析ができていない。（指摘事項３後述）
・　外部媒体について、指定管理者は当該システムに関する業務でＵＳＢメモリを使用する

ことがあるが、実施手順において、データをやり取りする場合は、必ず事前にウイルスチェックを実施するものとするとの記載に留まり、外部媒体の具体的な管理や取扱いに関する記載がない。

（注）　ＤＡＴとは、データを記録する磁気テープの規格のことをいう。

＜道路橋梁総合管理システム：建設局＞

■　当該システムの実施手順は、平成 25 年 12 月 27 日に作成されており、その見直し、変更は運用管理を担う工務課長が行うこととされている。

■　改定状況を確認したところ、当該システムの実施手順の最終改定は平成 26 年４月１日であり、大阪市情報セキュリティ対策基準がそれ以降に複数回改定されている（直近の改定は令和４年４月１日）にもかかわらず実施手順が改定されておらず、以下の例のとおり、現状との不整合や、大阪市情報セキュリティ対策基準に準拠していない項目がある。

・　管理体制の内容が、大阪市情報セキュリティ対策基準に定められている、システムに係る管理体制・役割の内容と異なる。
・　連絡体制の役職名が、現行の組織体制と異なる。
・　データの重要性分類の明文化がされていない。

■　以下の例のとおり、当該システムの実施手順と現在の運用に不整合が見られる項目がある。

・　実施手順では、機器集中管理室 (注) の入退室について、機器集中管理室責任者である工務課長の属する課等の職員を除き、情報処理機器集中管理室入室許可申請書及び作業計画報告書（以下「申請書」という。）を用いて機器集中管理室責任者の許可を得なければならないとされているが、現状は、工務課以外の職員も、各所属からの報告により電子錠の開錠が可能な情報を職員証に登録することで入退室しており、申請書は提出させていない。また、保守業者は、年度当初に機器集中管理室への長期間入退室を伴う作業計画書を提出させ、電子錠の開錠が可能な入退室カードを日々、入退室管理及びカード貸出簿に記載した上で貸し出すこととしており、申請書は提出させていない。

（注）　実施手順において、機器集中管理室には、当該システムのサーバ等の機器又はネットワークの根幹機器を設置するとしている。

これらは、本市ポリシーに準じて実施手順を整備すること、また実施手順に基づいてシステムを運用することの重要性に対する理解が不十分であったことが原因と考えられる。

現状では、実施手順が適切に改定されないことにより、当該システムにおける情報セキュリティ対策が適切に実施されず、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.　都市整備局及び建設局は、当該システムの実施手順について、本市ポリシーに準拠し、かつ現在のシステム運用に則した内容となるよう改定されたい。

2.　都市整備局及び建設局は、実施手順の定期的な点検・見直しの重要性や必要性を理解し、当該システムの実施手順の改正漏れを防ぐ仕組みを構築されたい。

２　情報システム室への端末機等の持込みの管理について是正を求めたもの

【都市整備局に対して】

大阪市情報セキュリティ対策基準によれば、情報システム室管理責任者(注)は、当該情報システム室に関係しない端末機、通信回線装置、記録媒体等（以下「端末機等」という。）を持ち込ませないようにしなければならないとされている。

（注）　サーバ等の機器又はネットワークの基幹機器を設置する情報システム室の管理責任については、当該システム又はネットワークの運用管理を所管する課等のリーダー等（情報システム室管理責任者という。）が担うとされている。

しかし、今回の監査において、情報システム室への端末機等の持込みの状況について確認したところ、次のような状況が生じていた。

■　当該システムの保守業務を委託している委託事業者が、保守業務に必要となる端末機等を情報システム室に持ち込む場合がある。

■　情報システム室への入退室を管理している指定管理者は、来館者の事務室への入退室を管理している入退受付票及び情報システム室への入退室を管理しているサーバー室入室許可管理簿により委託事業者の入退室を確認している。

■　しかし、情報システム室への端末機等の持込みに関しては、入室に際して口頭での申告を受けているものの、書面による記録は行っていない。

これは、情報システム室への端末機等の持込みの管理が、不正アクセス対策の一つであるという理解が不十分であったことが原因と考えられる。

現状では、情報システム室に持ち込まれる端末機等の管理が適切に行われず、不正アクセス等による重要な情報の流出等の情報セキュリティインシデントが発生するリスク、また、その場合に、過去に遡って原因を追究することが困難となるリスクがある。

したがって、以下のとおり指摘する。

［指摘事項２］

都市整備局は、当該システムの情報システム室への端末機等の持込みについて、事前に入退室受付票やサーバー室入室許可管理簿等に記載させる等により、持ち込まれる端末機等の管理を行われたい。

３　アクセスログの分析について是正を求めたもの

【都市整備局に対して】

大阪市情報セキュリティ対策基準によれば、業務管理者、サーバ等管理者及びネットワーク管理責任者は、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、都市整備局が定めている当該システムの実施手順によれば、業務管理者である住宅政策課長が、システムを運用・利用する指定管理者の住まい情報センター所長に対し、アクセスログの取得及び必要な分析結果の提出を要求すること、当該アクセスログの確認において侵害及びその兆候を発見した場合には、連絡体制に基づき報告しなければならないこととされている。

しかし、今回の監査において、アクセスログの取得状況及び必要な分析結果の提出状況について確認したところ、次のような状況が生じていた。

- 住まい情報センター所長がサーバのアクセスログを障害等の発生時に取得し確認しているが、そもそも当該システム専用端末へのログインには、指摘事項１に記載のとおり職員ごとにＩＤを付与せず、ユーザ共用ＩＤを使用しており、個人のログイン状況を確認できない。
- サブシステムである相談対応サブシステム及び図書検索システムは、アクセスログが記録される仕様となっておらず、サブシステムごとのアクセスログは確認できない状況となっている。
- 住宅政策課長は、住まい情報センター所長に対して必要な分析結果の提出を求めておらず、アクセスログの確認を行っていない。

これらは、アクセスログの取得及び分析の必要性について理解が不十分であったことが原因と考えられる。

現状では、不正アクセスや不正操作等を見逃し、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３］

1.　都市整備局は、当該システムについて、職員ごとのアクセスログが確認できるように、専用端末機へのログインを個人ＩＤに改められたい。
2.　都市整備局は、当該システムのサブシステムについて、職員ごとのアクセスログを確認するかにつき、関係所属と調整し、調整の結果に応じた運用とされたい。
3.　都市整備局は、当該システムへの侵害及びその兆候を発見するために、アクセスログの分析結果を確認できる仕組みを構築されたい。

第７　その他

なし

監査結果に関する措置状況報告書

報　告　番　号：報告監５の第８号

監 査 の 対 象：令和４年度監査委員監査（住まい情報センター管理運営システム及び道路橋梁総合管理システムにおける情報セキュリティ対策に係る事務）

所　管　所　属：都市整備局

通知を受けた日：令和５年４月24日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
1	情報セキュリティ実施手順の整備について是正及び改善を求めたもの 住まい情報センター管理運営システムの実施手順の作成、見直しの状況について確認したところ、次の状況が生じていた。 ■ 当該システムの実施手順は、平成16年３月24日に作成されており、その見直し、変更は業務管理を担う住宅政策課長が行うこととされている。 ■　改定状況を確認したところ、当該システムの実施手順の最終改定は平成25年８月30日であり、大阪市情報セキュリティ対策基準がそれ以降に複数回改定されている（直近の改定は令和４年４月１日）にもかかわらず実施手順が改定されておらず、現状との不整合や、大阪市情報セキュリティ対策基準に準拠していない項目がある。 ■　当該システムの実施手順と現在の運用に不整合が見られる項目がある。 【指摘事項】 １．都市整備局は、当該システムの実施手順について、本市ポリシーに準拠し、かつ現在のシステム運用に則した内容となるよう改定されたい。 ２．都市整備局は、実施手順の定期的な点検・見直しの重要性や必要性を理解し、当該システムの実施手順の改正漏れを防ぐ仕組みを構築されたい。	【１】 実施手順の改定案を令和４年12月に作成し、デジタル統括室との協議を経て、令和５年１月30日付けで改定を行った。 【２】 実施手順の改正漏れを防ぐため、本市ポリシー改定時には必ず改定の必要性を判断して決裁または供覧を行うこととするとともに、デジタル統括室からの「情報セキュリティ検査」実施指示の時期に合わせて実施手順の内容について点検を行い、その点検結果について決裁を行うこととし、これらの手続方法について明文化した。また、確実にこの手続が継続されるよう引継文書に添付することとした。	措置済 措置済	令和５年１月30日 令和５年１月30日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
２	情報システム室への端末機等の持込みの管理について是正を求めたもの 情報システム室への端末機等の持込みの状況について確認したところ、次のような状況が生じていた。 ■　当該システムの保守業務を委託している委託事業者が、保守業務に必要となる端末機等を情報システム室に持ち込む場合がある。 ■　情報システム室への入退室を管理している指定管理者は、来館者の事務室への入退室を管理している入退受付票及び情報システム室への入退室を管理しているサーバー室入室許可管理簿により委託事業者の入退室を確認している。 ■　しかし、情報システム室への端末機等の持込みに関しては、入室に際して口頭での申告を受けているものの、書面による記録は行っていない。 【指摘事項】 都市整備局は、当該システムの情報システム室への端末機等の持込みについて、事前に入退室受付票やサーバー室入室許可管理簿等に記載させる等により、持ち込まれる端末機等の管理を行われたい。	令和５年１月30日付けで策定した大阪市立住まい情報センター情報システム室入退室管理要領において、情報システム室入室許可管理簿に端末機持込の有無についての記載項目を設定することにより、持ち込まれる端末機等の管理を行うよう改めた。	措置済	令和５年１月30日
３	アクセスログの分析について是正を求めたもの アクセスログの取得状況及び必要な分析結果の提出状況について確認したところ、次のような状況が生じていた。 ■　住まい情報センター所長がサーバのアクセスログを障害等の発生時に取得し確認しているが、そもそも当該システム専用端末へのログインには、職員ごとにＩＤを付与せず、ユーザ共用ＩＤを使用しており、個人のログイン状況を確認できない。 ■　サブシステムである相談対応サブシステム及び図書検索システムは、アクセスログが記録される仕様となっておらず、サブシステムごとのアクセスログは確認できない状況となっている。 ■　住宅政策課長は、住まい情報センター所長に対して必要な分析結果の提出を求めておらず、アクセスログの確認を行っていない。 【指摘事項】 １．都市整備局は、当該システムについて、職員ごとのアクセスログが確認できるように、専用端末機へのログインを個人ＩＤに改められたい。 ２．都市整備局は、当該システムのサブシステムについて、職員ごとのアクセスログを確認するかにつき、関係所属と調整し、調整の結果に応じた運用とされたい。 ３．都市整備局は、当該システムへの侵害及びその兆候を発見するために、アクセスログの分析結果を確認できる仕組みを構築されたい。	【１】 システムの専用端末機へのログインを個人ＩＤに改めて設定を行った。 （令和５年１月27日　設定完了確認） 【２】 サブシステムにおけるアクセスログの確認方法について、デジタル統括室と調整を行った結果、上記【１】の対応により、専用端末機へのアクセスログの確認をもってサブシステムへのアクセスログを確認することが可能と判明したことから、専用端末機へのログインには個人ＩＤを利用するよう実施手順に定めた。 【３】 業務管理者は、必要時にアクセスログの分析を行えるよう、アクセスログを１年間保管することとし、その旨を実施手順に定めた。	措置済 措置済 措置済	令和５年１月27日 令和５年１月30日 令和５年１月30日

監査結果に関する措置状況報告書

報　告　番　号：報告監５の第８号

監 査 の 対 象：令和４年度監査委員監査（住まい情報センター管理運営システム及び道路橋梁総合管理システムにおける情報セキュリティ対策に係る事務）

所　管　所　属：建設局

通知を受けた日：令和５年４月28日

指摘No.	指摘等の概要	措置内容又は措置方針等	措置分類	措置日 （予定日）
1	情報セキュリティ実施手順の整備について是正及び改善を求めたもの 道路橋梁総合管理システムの実施手順の作成、見直しの状況について確認したところ、次の状況が生じていた。 ■　当該システムの実施手順は、平成25年12月27日に作成されており、その見直し、変更は運用管理を担う工務課長が行うこととされている。 ■　改定状況を確認したところ、当該システムの実施手順の最終改定は平成26年４月１日であり、大阪市情報セキュリティ対策基準がそれ以降に複数回改定されている（直近の改定は令和４年４月１日）にもかかわらず実施手順が改定されておらず、現状との不整合や、大阪市情報セキュリティ対策基準に準拠していない項目がある。 ■　当該システムの実施手順と現在の運用に不整合が見られる項目がある。 【指摘事項】 １．建設局は、当該システムの実施手順について、本市ポリシーに準拠し、かつ現在のシステム運用に則した内容となるよう改定されたい。 ２．建設局は、実施手順の定期的な点検・見直しの重要性や必要性を理解し、当該システムの実施手順の改正漏れを防ぐ仕組みを構築されたい。	【１】 当該システムの実施手順について、令和５年１月26日にデジタル統括室に情報セキュリティ実施手順変更報告書を提出し、令和５年２月24日に承諾を受け、令和５年２月28日付けで情報セキュリティ実施手順を改定し令和５年３月１日より運用している。 【２】 ・当該システム担当の引継文書として、情報セキュリティ実施手順の改定の流れを明文化し、本市ポリシーの改定及び所管システムの運用を変更した際に既存の情報セキュリティ実施手順に影響がある場合は、改定を行うことを記載した。 ・年に１度、局所管の全システム担当者に対して、情報セキュリティに関する研修を実施し、情報セキュリティ実施手順の定期的な点検・見直しの重要性や必要性に関する内容を含めるとともに、情報セキュリティに関する研修と合わせて、各システムの実施手順と、本市ポリシー及び現在のシステム運用と不整合がないかを確認する。令和４年度については、令和５年２月20日に実施した。 ・令和５年２月20日より、週に１度、ＩＣＴ担当者間の情報共有を行う担当内会議を設け、会議においてメールの確認を行うことにより、デジタル統括室からの本市ポリシーの改定等、各システムの実施手順の改定に関係する通知等の確認漏れを防ぐ。	措置済 措置済	令和５年２月28日 令和５年２月20日

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

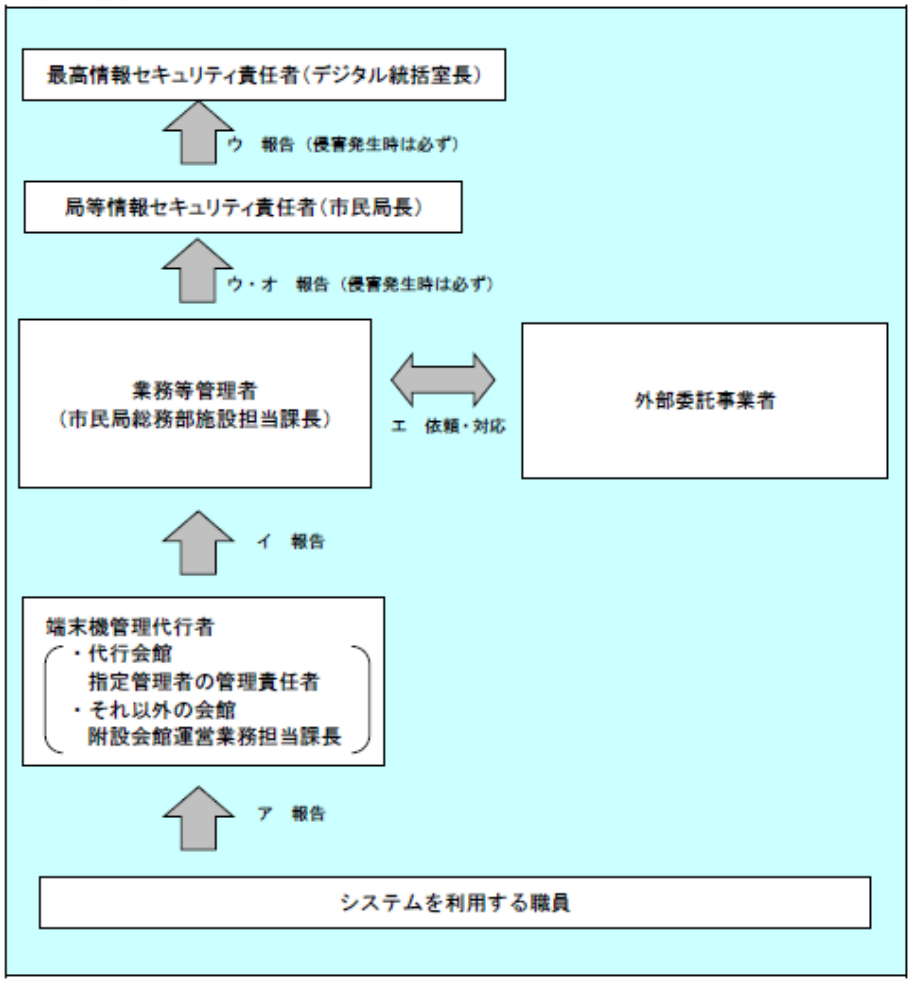
【市民局（施設担当）に対して】

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。

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