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