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

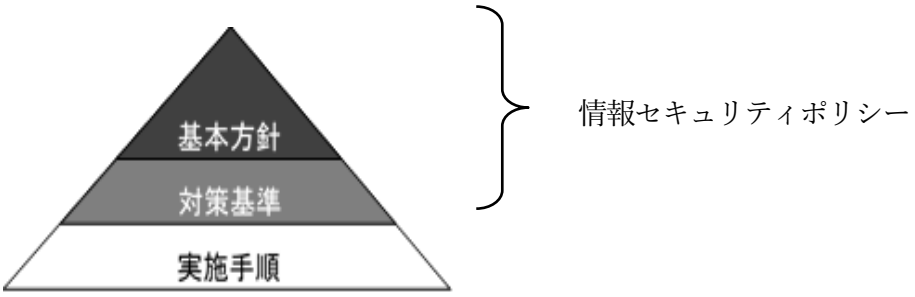
１　本市の情報セキュリティ対策の概要

（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。