報告監 28 の第 31 号
平成 28 年 10 月 19 日

大阪市監査委員　貴　納　順　二
同　阪　井　千鶴子
同　辻　　淳　子
同　西　﨑　照　明

平成 27 年度随時監査等結果報告の提出について

（統合基盤システムの開発、変更管理、運用管理等に関する事務）

地方自治法（昭和 22 年法律第 67 号）第 199 条第２項及び第５項の規定による平成 27 年度随時監査等を実施し、同条第９項の規定により監査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　監査の概要

１　監査の対象および選定理由

（１）監査の対象

統合基盤システムの開発、変更管理、運用管理等に関する事務

（２）選定理由

本市では、住民基本台帳等事務システム、税務事務システム、総合福祉システム等の住民情報系基幹システムに係る経常経費の削減を目的として、平成 27 年１月から、これらのシステムを基幹系システム統合基盤（以下「統合基盤システム」という。）に連携させ、認証、印刷、システム間の連携等の基本的かつ共通する機能を集約している。

統合基盤システムは、連携する住民情報系基幹システムのネットワークや認証機能等の重要機能を受け持つこととなり、確実な運用の確保と情報セキュリティの両面から、極めて重要な役割を担っている。

そのため、統合基盤システムを所管する総務局行政部ＩＴ統括課を監査対象として、ＩＣＴ監査を実施することとした。

なお、監査実施時に統合基盤システムを所管していた総務局行政部ＩＴ統括課は、平成 28 年４月１日実施の組織改正により、新設されたＩＣＴ戦略室にＩＣＴ統括担当として移管された。

２　監査の目的と範囲

統合基盤システムの開発、変更管理、運用管理等に係る重要リスクに対する内部統制の整備状況及び運用状況等を監査し、その有効性を評価するとともに、当該事務の関係法令及び

規程等への準拠性、適正性、効果性ならびに効率性につき、証ひょう書類等の査閲、関係職員への質問等の監査手続を通じて検証することを目的とした。

平成 28 年３月１日を監査基準日とし、監査範囲は次の項目とした。

ア　統合基盤システムの開発・運用体制

イ　統合基盤システムのセキュリティ確保

ウ　統合基盤システムの災害対策

エ　中央情報処理センター（以下「センター」という。）の運用状況（統合基盤システムや前述の住民情報系基幹システムはセンターで運用管理されているため、セキュリティ確保や災害対策の項目についてはセンターも監査範囲に含めた。）

３　重要リスク及び監査の着眼点

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
（1）システムの開発、変更、保守に支障が生じ、システムの信頼性を損なうリスク	ア　プログラムの変更は、変更管理手順に基づき、本市の責任者の承認を得て実施されているか。
	イ　プログラムのテスト結果は、委託先や本市の責任者が承認しているか。
	ウ　システム開発の各工程の完了判定やリリース(注)1判定などは、責任者によって適切に実施されているか。
	エ　開発又は変更されたプログラムを本番環境に登録する前に、本市の責任者が適切に承認しているか。
（2）システムの運用、管理に支障が生じ、システムの信頼性を損なうリスク	ア　運用業務委託、保守業務委託及び直営作業の役割分担は明確になっているか。
	イ　運用業務及び保守業務の業務フローは文書化され、明確になっているか。
	ウ　障害復旧方針は、各基幹システムの対応方針と整合するように定められているか。
	エ　障害管理に係るルールが定められ、全ての障害が記録されているとともに、原因分析や再発防止策が実施されているか。
	オ　各サーバにおける障害に対し、対策は準備されているか。
	カ　運用業務や保守業務について、サービスレベル契約を締結し、適切に運用されているか。
（3）システムの安全性を損なうリスク	ア　アカウント管理（登録、変更、削除、権限付与、パスワード変更等）は適切に運用されているか。
	イ　サーバ操作、端末操作等のログ(注)2を取得し、定期的に確認しているか。
	ウ　ウイルス対策は適切に運用されているか。
	エ　管理者用アカウント（特権ＩＤ）は適切に管理され、使用状況がログ等で確認できるように運用されているか。

	オ　センターの入退館管理やコンピュータ室の入退室管理について、入館者・入室者の特定、禁止物品の持込みや持出しの防止が適切に行われているか。
	カ　システムのバックアップ・リストア(注)3機能は適切に設計され、運用されているか。
(4)障害時・災害時に市民サービスに支障をきたすリスク	ア　障害・災害発生時の代替措置、復旧手順及び対応方法についてマニュアルを作成し、周知しているか。
	イ　障害・災害発生時に、関係者へ迅速かつ正確に連絡する手段は整備されているか。
	ウ　障害・災害時により統合基盤システムに重大な損害が発生し、稼働できなくなった場合を想定した、住民サービス業務の遂行に向けた緊急時対応計画は策定されているか。
	エ　システムやデータをバックアップした保存媒体は、遠隔地に保管するなど、適切な保管場所が選定されているか。
	オ　センターは、耐震対策、浸水対策等の災害対策が取られているか。
(5)統合基盤システムが当初目的のとおりに機能しないリスク	ア　ＩＴ資産や機能の最適配置は進められているか。
	イ　運用管理業務の簡素化、効率化は実現しているか。

(注) 1　リリースとは、プログラムを本番環境に反映し、使用できる状態にすることをいう。

2　ログとは、ある機器やソフトウェア、システムについて、その起動や停止、エラーや障害の発生、利用者による操作や設定の変更、外部との通信など、稼働中に起こった出来事の内容を日時などとともに時系列に記録したものをいう。

3　リストアとは、バックアップした保存媒体を用いて、データを元の状態に戻すことをいう。

4　監査の期間

平成 28 年３月１日から同年同月 15 日まで

第２　事務の概要

１　統合基盤システムの概要

本市は、基幹系システムの最適化において、システム機器や機能の共有化による効率的なシステム構成やシステムの技術刷新による安定稼働の維持を着実に実現するには、共通的なＩＴ基盤を新たに整備し、整備したＩＴ基盤上にシステムを再構築することが効果的であるとして、平成 23 年度から、本市基幹系システムを中心に共通的に利用する統合基盤システムを構築し、平成 27 年１月に本番運用を開始した。

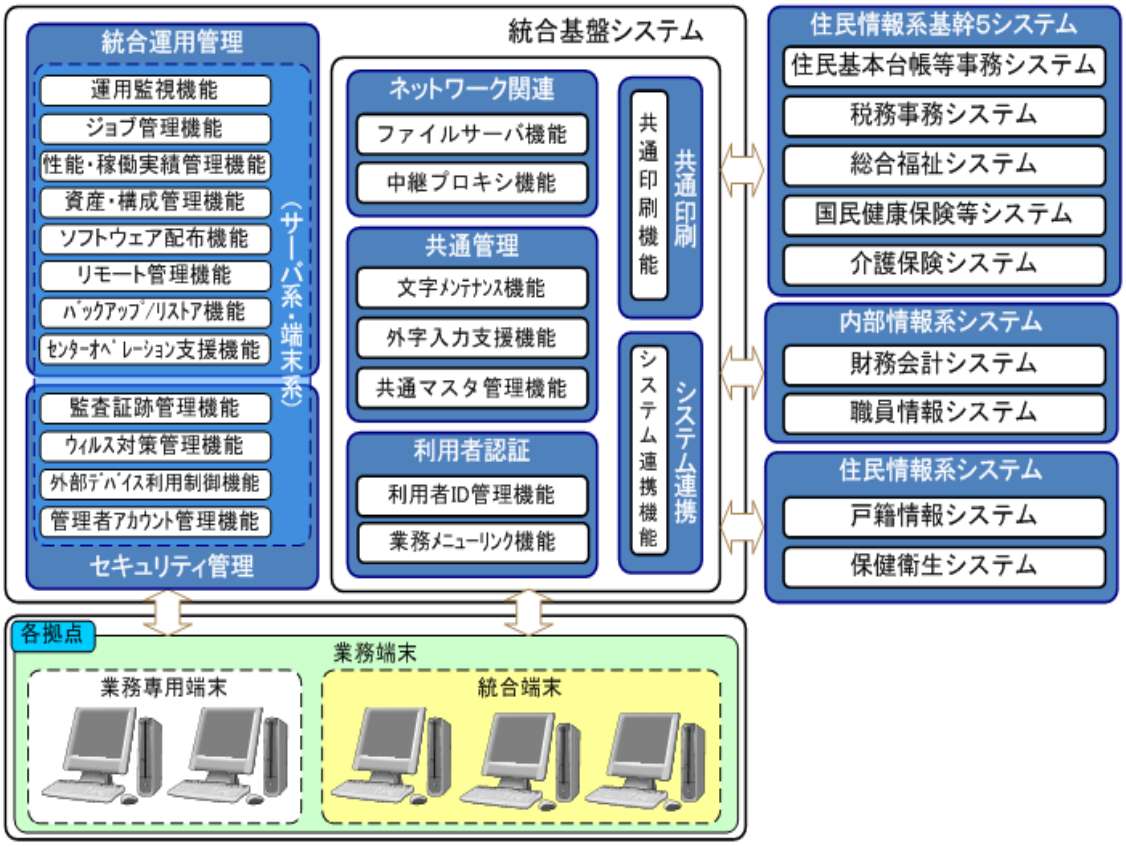
（１）実装機能の概要

統合基盤システムにおいて実装する機能と、統合基盤システムを利用する業務システムとの関連を示した全体概念図は、図－１のとおりとなっている。

また、実装する機能は、①利用者認証、②共通印刷、③システム連携、④統合運用管理、⑤セキュリティ管理、⑥共通管理及び⑦ネットワーク管理の大きく７つに整理されている。

図－１　統合基盤システムと業務システムとの関連を示した全体概念図

（「大阪市基幹系システム統合基盤　開発・運用保守業務委託」調達仕様書より）



（２）住民情報系基幹システムの利用開始時期

住民情報系の５つの基幹システムが、統合基盤システムに対応するように再構築される時期を表－１に示す。

表－１　住民情報系基幹システムの再構築時期

（「大阪市基幹系システム統合基盤　開発・運用保守業務委託」調達仕様書より編集）

システム名	再構築後利用開始時期
住民基本台帳等事務システム	平成 27 年１月
税務事務システム	平成 27 年１月
総合福祉システム	平成 27 年１月
国民健康保険等システム	平成 29 年１月
介護保険システム	平成 29 年１月

（３）統合基盤システムの開発、運用・保守業務に係る主な役割

統合基盤システムの開発、運用・保守業務に係る主な役割は表－２のとおりである。

表－２　統合基盤システムの開発、運用保守業務に係る主な役割（平成 28 年３月現在）

組織	主な役割	備考
ＩＴ担当 （総務局行政部ＩＴ統括課）	統合基盤システム運用全般の管理、統括を行う担当又はその職員。 統合基盤システムの運用保守管理を行う本委託業務の発注担当であり、統合基盤システムの運用保守業務の管理及び各関係先との調整等を行う。	
業務管理者 （総務局行政部ＩＴ適正化担当課長）	統合基盤システムの開発、運用及び保守の実施並びに管理を担う。	
統合基盤システム開発・保守業者 （株式会社　エヌ・ティ・ティ・データ関西）	統合基盤システムを開発し、保守業務を行う業者。 運用保守に関する要件を踏まえ、各関係先と調整や保守作業を行う。	開発・保守業務 （H23～30 年度） 789,924 千円 改修業務（H27 年度） 186,150 千円
基盤系機器保守業者 （サーバ、端末等） （日立キャピタル株式会社）	統合基盤システムのサーバ機器や端末等の保守を行う業者。 各関係先との調整や納入したハードウェア及びソフトウェアの保守を行う。	機器リース額 （年額概算） 202,604 千円

２　統合基盤システム等が稼働している中央情報処理センターの概要

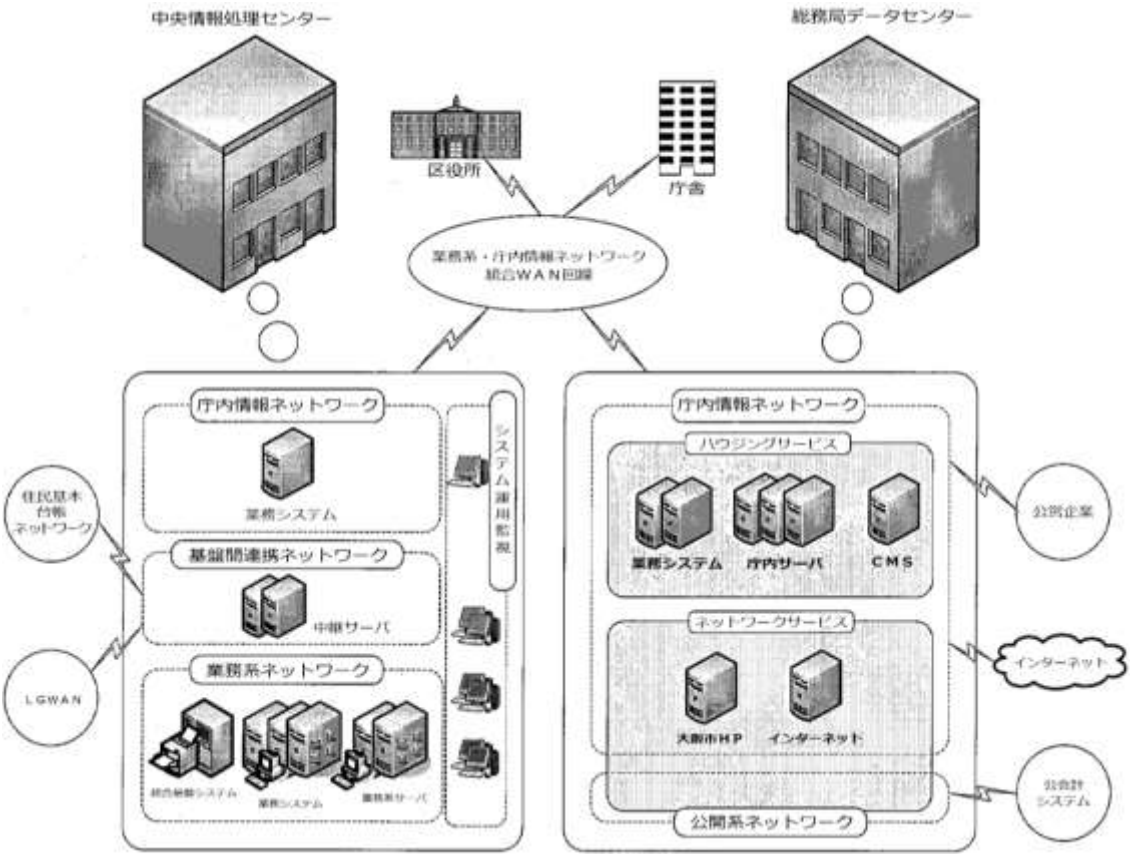
（中央情報処理センター管理要綱 Ver.1.0（平成 26 年７月　総務局行政部ＩＴ統括課）から抜粋・編集）

（１）センターの概要

センターは、総務局が設置する情報システム室であり、一部の基幹系システムのサーバ等の機器及び本市通信ネットワークの基幹機器を設置し、これらの運用管理を行っている。

センターの概要は、図－２のとおりである。

図－２　センターの概要図



（２）センターに係る管理体制

センターにおける運用管理業務を適切かつ円滑に管理するための体制は、表－３のとおりである。

表－３　センターに係る管理体制

管理者	役割
市副情報統括責任者 (注) （総務局ＩＴ統括担当部長）	センターの運用管理に関する事務を掌理する。
センター管理責任者 （ＩＴ統括課長）	センターの施設及び設備に関する管理責任を有するとともに、センターにおいて運用する業務システムのサーバ等の機器及び大阪市情報通信ネットワークの基幹機器等について管理責任を有する。
運用代行受託業者 （アクセンチュア株式会社）	センターで稼働する各業務システムや統合基盤システムの運用業務を行う業者。 運用作業全体を管理し、システム維持運用、オペレーション作業を実施する。
警備業務受託者 （三和管財株式会社）	センターの入退館管理等の警備業務を行う業者。

(注) 平成28年４月の規程改定により、市副情報統括責任者はＩＣＴ適正利用統括責任者に名称変更となり、ＩＣＴ戦略室ＩＣＴ統括担当部長が就くこととなった。

第３　監査の結果

今回監査を実施したところ、次のとおり是正、改善すべき点が認められたので、これらに留意し、適正で効率的かつ効果的な事務の執行に一層努力されたい。

１　情報システムに関する業務継続計画を早急に策定するよう求めたもの

地方公共団体におけるＩＣＴ部門の業務継続計画（以下「ＢＣＰ(注)1」という。）策定に関するガイドライン（平成20年８月　総務省）によれば、地方公共団体は、災害時に地域住民の生命、身体の安全確保、被災者支援等のために、災害応急業務、復旧業務及び平常時から継続しなければならない重要な業務を実施していく責務を負っており、これらの業務の継続を確保するために不可欠な情報システムが災害時に稼働していることは極めて重要であるとされている。そのため、同ガイドラインにおいては、ＩＣＴ部門は率先して情報システムに関する業務継続計画(注)2（以下「ＩＣＴ－ＢＣＰ」という。）を策定し、業務の継続力を高めていかなくてはならないとされている。

しかし、本市のＩＣＴ－ＢＣＰの策定状況を確認したところ、次に示す事態が認められた。

- 本市のＩＣＴ部門である総務局行政部ＩＴ統括課は、大規模災害発生を想定したＩＣＴ－ＢＣＰを策定できていなかった。（平成27年４月１日現在、政令市20都市の中でＩＣＴ－ＢＣＰが未策定であったのは本市を含む３市のみ(注)3）
- 平成28年３月に策定された大阪市業務継続計画（第１版）や大阪市ＩＣＴ戦略においても、ＩＣＴ－ＢＣＰ作成に向けた検討を進めていくとし、南海トラフ巨大地震による影響調査や対策の検討に着手していたものの、作成時期を平成29年度末としていたなど、緊急性を考慮した策定プランとなっていなかった。

このような事態が生じているのは、本市の最高情報統括責任者(注)4（以下「本市ＣＩＯ」という。）及び本市のＩＣＴ部門であるＩＴ統括課において、ＩＣＴ－ＢＣＰの策定は本市全体のＢＣＰとの整合性を確保するため、大阪市業務継続計画を踏まえて取り組むべきものであるという認識から、ＩＣＴ部門の最優先課題としていなかったことが原因である。

ＩＣＴ－ＢＣＰが未策定のまま大規模災害が発生すると、情報システムの機能維持や回復に甚大な影響を及ぼすリスクがある。

したがって、以下のとおり勧告する。

［改善勧告］

本市ＣＩＯ及びＩＣＴ戦略室は、ＩＣＴ－ＢＣＰの重要性を再認識し、本市全体のＢＣＰを所管する危機管理室と連携して、全市的な検討体制を構築して早急にＩＣＴ－ＢＣＰを策定するとともに、継続的に見直し、実効あるものにするための運用管理体制を構築すること。

（注）１　ＢＣＰとは、Business Continuity Planの略で、業務継続計画のこと。

２　情報システムに関する業務継続計画とは、情報システム部門（ＩＣＴ部門）において、災害や事故を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に復旧させるためのＩＣＴ部門が対

応する業務継続計画をいう。

3　地方自治情報管理概要　～電子自治体の推進状況（平成27年4月1日現在）～　（総務省 自治行政局地域情報政策室　平成28年3月）に基づく。

4　最高情報統括責任者とは、Chief　Information　Officer の訳語で、組織の情報通信技術に関する事務を統括する役割を担う。

2　中央情報処理センターの情報セキュリティ対策を抜本的に見直すよう求めたもの

竣工から20年以上経過した本市所有ビル内に配置されたセンターは、本市の基幹系システムのサーバ機器等が設置され運用が行われているとともに、重要な個人情報等のデータを取り扱うことから、入退館管理等の物理的セキュリティを含め万全なセキュリティ対策が求められる。これらの対策は、最新の技術動向やセキュリティ事故やその対策等を参考に、適時充実・強化させていくことが求められる。

たとえば、入退館（室）管理におけるセキュリティでは、生体認証等と連動したセキュリティゲート、共連れ防止機能(注)1、入退室カードによる入退室管理システム（履歴の管理）などの機能は、最近のデータセンターのセキュリティとしては必要不可欠な機能となりつつある。

また、センターの電源設備等については、災害を受けるおそれの少ない場所に設置することが原則とされ、諸般の事情から災害を受けるおそれのある場所に止むを得ず設置する場合は被害防止に必要な対策を講じることなどが求められている。

しかし、センターの入退館（室）に係るセキュリティを確認したところ、センターにおいては、入退館におけるセキュリティゲートや入退室における共連れ防止機能が装備されていないなど、最近のデータセンターに求められる設備面やシステム面での対応が十分でなく、入退館（室）にかかるセキュリティの多くを警備員等の人手による統制に依存していたことによって引き起こされたと考えられる事態が、次に示す（1）及び（2）のとおり生じていた。

また、電源設備の設置状況についても、（3）に示す事態が認められた。

（1）定常的にセンター内での作業が発生する者の入退館管理について

入退館管理にあたっては、情報システムの保守要員等のように定常的にセンター内で作業する者と、設備関係業者のように非定常的にセンター内で作業する者とを区分した入退館手続としている。

定常的にセンター内での作業する者については、入館及び退館の都度、ＩＤ入力と静脈情報による生体認証の二要素認証を行わせるとともに、その結果を生体認証ログとして記録している。

しかし、二要素認証による認証行為を必要としているものの、1階受付には、認証結果によって物理的に入退館を制限するセキュリティゲート等の設備が設けられておらず、警備員が認証結果のランプを目視確認して入退館を認めるといった警備員の人的対応に依存した運用ルールとなっている。

なお、平日昼間と夜間・休日では警備体制の違いから、入退館手続が次のとおり異なっている。

■　平日昼間は１階受付に２名の警備員が配置されており、入館者は、１階受付で入退館時の認証を行う。

■　夜間・休日は警備員が１名体制となるため、警備員は４階の警備員室に常駐し、１階は機械警備を行う。入館者はインターホンで警備員室に連絡を取って機械警備の解除を依頼し、警備員によって機械警備が解除された後入館し、４階に移動して警備員室で認証を行う。（認証結果の確認手続については、１階受付と同じ。）

ＩＴ統括課は、認証エラー等について、警備員から日次で報告を受けるとともに、不適正な記録の有無について定期的に生体認証ログを確認するとしている。

しかし、平成 27 年 12 月の生体認証ログ 14,433 件をもとに、その運用状況を確認したところ、次に示す事態が認められた。

■　平日昼間の入館において、１階受付の認証で、認証エラーのまま入館していた記録が１件認められた。

この１件は、警備員の目視確認が十分でなかったことによるものであった。

■　夜間・休日時の入館において、４階警備員室の入館認証をしなかった結果、退館時に認証エラーとなっていた記録が３件認められた。

この３件は、夜間・休日の入館者は必ず最初に４階にて入館認証を受けるというルールであるにもかかわらず、情報システムの保守要員等がそのルールを遵守していなかったこと及び警備員が夜間・休日の入館者に対して認証を確実に行わせるような手続となっていなかったことによるものであった。

■　警備員は上記のエラーの発生状況をＩＴ統括課に報告していなかった。

■　ＩＴ統括課は、生体認証ログの定期的な確認を行っていなかった。

（２）センター内の重要区画の入退室管理について

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は、許可を受けた者が情報システム室へ入室するときは、入室年月日、入退室時分、所属又は団体名及び氏名、入室目的等を記録しなければならないとされている。

センター内のサーバ等を設置している重要区画の入退室管理は、電子錠を通じて入室管理装置により管理・施錠されており、ＩＤカードにより認証し、入室の許可とともにそのＩＤと時刻を記録する仕組みとなっている。

しかし、入室管理装置は、共連れ防止機能を有するものでなく、認証装置は入室側にしか設けられていないものとなっていた。

また、ＩＤカードは、ＩＤごとに入室可能な扉が入室管理装置に登録されており、入室が許可された者に貸与される。ＩＤカードは、本市ＩＴ統括課職員及びセンター運用業者に対しては常時貸与され、各情報システムの保守要員等に対しては、事前に提出された作業計画書に基づいて入館時に貸与され、退館時に返却を受けることとしている。

上記のとおり、センターの重要区画への入退室については、共連れ防止機能によるアクセスコントロールがないことから、入室者の運用に依存した統制となっているため、入退室に係る記録の整備やそのモニタリングが重要な統制の手段と考えられる。

しかし、センターの入退室管理状況を確認したところ、次に示す状況が認められた。

- ■　重要区画の入室については、作業計画書によって、入室目的等が、また入室時の認証行為によって入室年月日等が記録されることになっているが、退室についてはその記録が作成されていなかった。
- ■　ＩＴ統括課において、入室ログと作業計画書を突合するなど、入退室の記録を定期的に確認していなかった。
- ■　入室管理装置におけるＩＤカード全500枚の入室権限付与の登録状況を確認したところ、扉１か所の権限解除が反映されていないもの及び扉１か所の権限設定が反映されていなかったものがそれぞれ１枚ずつ見られた。
- ■　入室管理装置におけるＩＤカードの入室権限付与の登録事務については、明文化された手続がなく、センター管理責任者等によるチェックも行われていなかった。

（３）電源設備の災害対策状況について

大阪府が平成25年８月に公表した南海トラフ巨大地震の被害想定によれば、センターの周辺は津波により最大１メートル程度の浸水が発生するおそれがあるとされている。

しかし、センターの浸水対策状況を確認したところ、非常用発電設備や主要配電設備が地下１階に設置されているにもかかわらず、浸水リスクへの対策として電源設備の上階移設等を検討していたものの、建物内部への浸水から防護する防水施設の設置やセンター内が浸水した場合の対策は講じられていなかった。

これら（１）～（３）の事例は、センターのセキュリティ対策の脆弱性を端的に示すものであり、本市の重要なデータセンターである中央情報処理センターのセキュリティ対策が、時代の流れに適応できていない状況を示すものと考えられる。

この背景には、重要な情報システムやデータを取り扱う本市のデータセンターに関連するセキュリティリスクと災害リスクに対して、本市ＣＩＯ、市副情報統括責任者及びＩＴ統括課の認識が低かったことがある。

現状では、平常時及び大規模災害発生時において、データセンターとしてのセキュリティの確保や重要な基幹システムの継続運用の確保を阻害するリスクがある。

したがって、以下のとおり勧告する。

［改善勧告］

本市ＣＩＯ、ＩＣＴ適正利用統括責任者及びＩＣＴ戦略室においては、入退館（室）に係るリスクの総点検を行うとともに、巨大地震発生時にも影響の小さい地域に立地する民間のデータセンターの活用を含め、設備面、システム面、立地面から必要なセンターのセキュリティ対策を抜本的に見直すこと。

なお、見直しにあたっては、ＮＰＯ法人日本データセンター協会(注)[2]作成のデータセンターのファシリティ(注)[3]を評価・格付する基準や、公益財団法人金融情報システムセンター(注)[4]作成の「金融機関等コンピュータシステム安全対策基準」等の客観的に示された評価基準を参考に、大量の個人情報を扱う本市のデータセンターに相応しいセキュリティの達成水準

を明確に定めて取り組むこと。

また、新データセンター構築など、上記の対策実施に長期間を要する場合は、短期的対策として下記の事項を早急に実施すること。

1. 入退館管理について

ア センターの入退館管理に係る運用ルールを再点検し、セキュリティ上のリスクを洗い出し、そのリスク対策を反映した新たな入退館運用ルールを構築し実施すること。

また、本センターの施設及び設備に関する管理責任を有するセンター管理責任者が、リスクに応じて必要なモニタリング項目と頻度を定め、モニタリングを実施すること。

イ 新たな入退館運用ルールを、各入館者や警備業務受託者へ周知・徹底すること。

2. センター内の重要区画への入退室管理について

ア 重要区画への入退室管理にかかる運用ルールを再点検し、セキュリティ上のリスクを洗い出し、そのリスク対策を反映した新たな入退室運用ルールを構築し実施すること。

また、本センターの施設及び設備に関する管理責任を有するセンター管理責任者が、リスクに応じて必要なモニタリング項目と頻度を定め、モニタリングを実施すること。

イ 新たな入退室運用ルールを、ＩＤカード貸与者や警備業務受託者へ周知・徹底すること。

ウ 重要区画の在室時間を把握できるよう検討・実施すること。

エ ＩＤカードの入室権限付与の登録事務やＩＤカードの現物確認の手続を見直し、センター管理責任者等が入室権限の適切性をリスクに応じた頻度で確認するような手続とすること。

3. 電源設備等に係る浸水対策について

津波によるセンターの電源設備の浸水事態について、重要な情報システムの継続計画を策定するなど、具体的な対応策を検討すること。

（注）１ 共連れとは、一人のＩＤ認証で解錠した扉を複数の者が通過してしまうことをいい、その防止機能は入室路を通常の扉ではなく１人ずつしか通行ができないゲートの設置やシステムとしてのアンチパスバック機能（入室する際のＩＤ認証の記録がないと退室時の認証を許可しない仕組み）などによって実現される。

２ 日本データセンター協会は、データセンター事業者と主要データセンター関連事業者が参加する組織を形成し、各事業者が水平的垂直的に協力してＩＴ立国の基盤を支えるデータセンターのあるべき姿を追求することを目的として設立された団体で、アメリカの民間団体（UPTIME INSTITUTE）が作成した基準（Tier：ティア）をもとに、日本の実情に即したファシリティ評価基準を策定している（ティア１～４の段階ごとに、求められるレベルを定めている）。

３ ファシリティとは、施設や設備等の固定的な物的資産について、総称していう。

４ 金融情報システムセンターは、主に金融情報システムの諸問題を調査・研究しており、「金融機関等コンピュータシステム安全対策基準」は昭和60年12月、金融機関等の自主基準として策定されて以来、現在まで金融情報システムに関する安全対策の共通のよりどころとして広く活用されている。

３ 統合基盤システムにおける利用者等のアカウント管理について改善を求めたもの

（１）利用者のアカウント管理について

本市情報セキュリティ対策基準では、業務管理者はアクセス権限の把握、管理を適切に

行うこととされている。

一方、統合基盤システムの情報セキュリティ実施手順では、90 日以内毎にユーザＩＤのパスワードを変更させることを求めている。

しかし、統合基盤システムにおいて登録されている 144 個のユーザＩＤの管理状況を確認したところ、次のような実態が認められた。

- 民間委託・短期嘱託職員用の２個の利用者ＩＤは、使用予定がないにも関わらず、これらのＩＤで各種プログラムの動作確認を実施するため、テスト用として登録されたままとなっていた。
- 人事異動の際に使用するためとしていた１個の臨時のユーザＩＤが、使用期間終了のため本来は無効化されるべきものがそのまま放置されていた。
- 90 日以上もパスワードが変更されていないユーザＩＤが 87 個あった。

（２）特権ＩＤのパスワード管理について

広範なアクセス権限を有する特権ＩＤの管理にあたっては、一般利用者のユーザＩＤと比べて更に厳重な管理が求められ、統合基盤システム設計書によれば、特権ＩＤのパスワードについては定期的変更運用を行うことが求められていることから、ユーザＩＤのパスワードと同等かより短い周期で変更すべきことが期待される。

しかし、統合基盤システムにおける特権ＩＤのパスワード変更状況について確認したところ、次のような実態が認められた。

- 統合基盤システムの情報セキュリティ実施手順等において、特権ＩＤのパスワードについて変更頻度を定めていなかった。
- パスワード変更の対象となる延べ 36 の特権ＩＤを確認したところ、平成 27 年１月の本番環境の稼働開始以降、一度もパスワードが変更されていなかった。

これら（１）～（２）の事態が生じているのは、アクセス制御における重要な手段であるユーザＩＤ等の管理やパスワードの定期的変更という基本的リスク認識が、業務管理者に欠けていたことが原因と認められる。

現状では、ユーザＩＤ等が不正に使用されるリスクがある。

したがって、以下のとおり勧告する。

[改善勧告]

統合基盤システムの業務管理者は、次の点に留意し、利用者等のアカウント管理を徹底するとともに、開発・保守業者に対しても指導・徹底を行うこと。

1. ユーザＩＤの定期的な棚卸しを実施し、使用予定のないＩＤが放置されないようにすること。
2. 利用者に対しパスワードを定期的に変更するよう指導するとともに、パスワードの変更状況を適時確認すること。
3. 情報セキュリティ実施手順等において、特権ＩＤのパスワードの変更頻度を定め、定期的に変更すること。