

平成27年度
包括外部監査の結果報告書

情報システムに関する財務事務の執行について

豊田市包括外部監査人
公認会計士 湯本秀之

目 次

第1 外部監査の概要 ······ ······ ······ ······ ······ ······	1
1 外部監査の種類 ······ ······ ······ ······ ······ ······ ······	1
2 選定した特定の事件（テーマ） ······ ······ ······ ······ ······ ······	1
3 事件を選定した理由 ······ ······ ······ ······ ······ ······ ······	1
4 外部監査の方法 ······ ······ ······ ······ ······ ······ ······	2
5 監査テーマに対する市民の意見募集 ······ ······ ······ ······ ······	4
6 外部監査の実施期間 ······ ······ ······ ······ ······ ······ ······	4
7 外部監査人補助者 ······ ······ ······ ······ ······ ······ ······	4
8 その他 ······ ······ ······ ······ ······ ······ ······	4
第2 情報システムの概要 ······ ······ ······ ······ ······ ······	5
1 市において利用している情報システム ······ ······ ······ ······ ······	5
2 情報システム課の役割 ······ ······ ······ ······ ······ ······	6
3 各情報システムの所管課等の役割 ······ ······ ······ ······ ······	7
4 情報システムに関する規則類 ······ ······ ······ ······ ······	8
5 情報セキュリティに関する取組 ······ ······ ······ ······ ······	10
第3 外部監査の結果 ······ ······ ······ ······ ······ ······	13
1 実施手続の概要 ······ ······ ······ ······ ······ ······	13
2 総括的事項 ······ ······ ······ ······ ······ ······	32
(1) 情報システムの調達に係るガイドラインの整備 ······ ······	32
(2) 情報システムの調達における総合評価方式の導入 ······ ······	33
(3) 情報セキュリティ対策に係る監査の実施 ······ ······	35
(4) 情報セキュリティ基本要綱・共通実施手順の定期的な見直し	35
(5) 情報セキュリティ対策会議の定期的な開催 ······ ······	36
3 個別的事項 ······ ······ ······ ······ ······ ······	38
(1) 情報システムの調達に係る事務手続について ······ ······	38
ア 情報システムの管理責任について ······ ······ ······	38
イ 情報システムの情報資産管理状況について ······ ······	41
ウ 稼働中の情報システムの契約書類について ······ ······	44

エ	情報システム調達時の契約方法について ······	45
オ	情報システム等の導入及び変更管理について ······	48
カ	業務の外部委託におけるセキュリティの確保について ···	54
キ	サポート期間の考慮について ······	59
ク	ベータ版ソフトウェアの導入について ······	63
(2)	情報システムの調達・運用に係る経済性・効率性・有効性について ······	66
ア	随意契約の対象範囲について ······	66
イ	調達コストの適正化について ······	71
ウ	市が保管するデータのホームページによる一般公開の状況について ······	73
(3)	情報システムの運用に係る安全性について ······	75
ア	セキュリティ関連の書類管理等について ······	75
(ア)	個別実施手順について ······	75
(イ)	インターネットの利用について ······	81
(ウ)	障害報告について ······	84
(エ)	情報資産管理状況の定期的な監査の実施について ·····	89
イ	ユーザ ID の管理状況について ······	91
(ア)	システム利用時のアクセス許可について ······	91
(イ)	ID 及びパスワードの管理について ······	94
(ウ)	ユーザ登録状況の確認について ······	96
(エ)	システム利用時におけるアクセス権限について ······	101
ウ	データの管理状況について ······	105
(ア)	データ修正手続について ······	105
(イ)	時間外のバッチ処理について ······	106
(ウ)	一般業務ユーザにおける管理コマンドの実行状況について ······	108
(エ)	アプリケーションシステムのデータへのアクセスについて ······	110
(オ)	外部記録媒体の管理状況について ······	113
(カ)	システムのデータのバックアップについて ······	116
(キ)	緊急時用のバックアップシステムについて ······	119
エ	脅威への対策について ······	120
(ア)	情報処理装置の保護について ······	120
(イ)	無線 LAN の利用について ······	124
(ウ)	コンピュータウイルス対策ソフトについて ······	128

(4) 用語集	134
第4 利害関係	138

- ・報告書中の数値は、端数処理の関係で、総額と内訳の合計とが一致していない場合がある。
- ・外部監査の結果のうち、合規性等について指摘した事項については（指摘）として表記し、経済性、効率性、有効性等について意見を述べた事項については（意見）として表記している。

第1 外部監査の概要

1 外部監査の種類

地方自治法第252条の37第1項に基づく包括外部監査

2 選定した特定の事件（テーマ）

（1）外部監査対象

情報システムに関する財務事務の執行

（2）外部監査対象期間

平成26年度及び必要に応じ遡及する年度並びに一部平成27年度

3 事件を選定した理由

市は、多くの情報システムを利用して行政活動を実施している。市民の利便性の向上を図り、効率的・効果的な行政運営を実現するため、情報システムの利用は必要不可欠なものといえる。一方で、市の財政事情を考慮し、情報システムの開発及び運用経費の負担を軽減する観点から、効果的な開発及び経費の削減が要請されている。また、平成25年5月に社会保障・税番号制度関連法が成立し、個人情報保護を始めとする情報セキュリティの確保は、市民にとって重要な関心事となっている。

市の情報システムは、汎用機による情報システムとそれ以外（クライアント・サーバ型システム、アプリケーションサービスプロバイダ、スタンドアロン等を含む。）による情報システムに大別される。前者は、情報システム課の内製により開発・管理されているのに対し、後者は、委託業者により開発され、使用する所管課で管理されているという違いがある。また、これらの情報システムの中には、市民の個人情報を始めとする重要な情報を多数保有しているものがある。

このような状況において、市におけるこれまでの情報システムの財務事務の執行がどのようなものであり、今後、どのような課題があるのかを検証することは意義が大きいものと判断されることから、特定の事件として選定する。

4 外部監査の方法

(1) 監査の視点

情報システムに関する財務事務の執行に係る主な監査の視点は次のとおりである。

- ア 情報システムの調達に係る事務手続が、関係する法令、条例等に準拠しているかどうか（合規性）。
- イ 情報システムの調達・運用が、3E（経済性・効率性・有効性）の観点から適切に実施されているかどうか。
- ウ 情報システムの運用が、安全性の観点から適切に実施されているかどうか。

(2) 主な監査手続

- ア 関連書類一式を閲覧し、合規性の検証のため、関連規則等との照合を実施した。
- イ 経済性、効率性等の検証のため、どのような事務処理、業務改善等がなされているかについて、担当部署に対するヒアリング及び関連書類の調査、分析等を行った。
- ウ 情報セキュリティに関する法制度、総務省、経済産業省等の基準及びシステム監査基準を踏まえ、担当部署に対するヒアリング及び関連書類の調査、分析等を行った。
- エ 必要に応じて施設等の現場視察を行った。

(3) 監査対象

ア 監査対象項目

本監査では、市が使用している情報システムの中から、金額的及び質的な重要性を考慮した上で対象システムを選定した。

また、対象システムの所管課のほか、情報システム課、財政課及び契約課を対象とした。

なお、今回の監査結果は、監査結果を記載していない情報システムにおいても、当該情報システムの導入、開発、運用等について、参考にしてい

ただきたい。

イ 監査対象部署

本調査の対象とした情報システムに係る所管部課等は、以下のとおりである。

表 1-1 本調査の対象とした所管部課等

部局名等	課名等
経営戦略室	市政発信課
総務部	人事課
	契約課
	情報システム課
	技術管理課
	用地審査課
税務財産部	資産税課
社会部	交通安全防犯課
	生涯学習課
	防災対策課
環境部	環境政策課
市民福祉部	総務課
	市民課
	地域福祉課
	介護保険課
健康部	健康政策課
都市整備部	交通政策課
	建築相談課
建設部	幹線道路推進課
	河川課
上下水道局	経営管理課
	料金課
	水道整備課
	水道維持課
	下水道施設課
教育行政部	スポーツ課
	図書館

学校教育部	学校教育課
	保健給食課
消防本部	指令課
	予防課

5 監査テーマに対する市民の意見募集

包括外部監査のテーマについては、市が、平成27年4月に広報とよた及び市ホームページを活用して市民からの意見を募集したが、市民からの意見はなかった。

6 外部監査の実施期間

自 平成27年6月29日 至 平成28年2月16日

7 外部監査人補助者

齋 藤 英 喜（公認会計士、システム監査技術者、公認情報システム監査人）

北 川 裕 和（公認会計士）

田 中 豪 明（公認会計士、公認情報システム監査人）

深 見 圭 司（公認情報システム監査人）

大 山 満（公認情報システム監査人）

後 藤 由 兼（公認情報システム監査人）

山 田 麻 登（弁護士）

8 その他

情報システムに関する専門的な用語集を本報告書の末尾に記載しているので、参考にしていただきたい。

第2 情報システムの概要

1 市において利用している情報システム

市において利用している情報システムは、図 2-1 に示すとおり汎用機上で稼働するもの、グループウェア上で稼働するもの及び庁内ネットワーク又はインターネット上で稼働するもの並びに各所管課で個別に導入したもののが4つに大別される。

	情報システム名	責任部署
汎用機系	●財務情報システム ●住民登録情報システム ●国民健康保険情報システム ●国民年金システム ●市県民税システム など	情報システム課
グループウェア	●人事関係申請システム ●会議室予約システム ●旅費申請システム ●情報システム資産管理台帳システム など	情報システム課
インターネット・イントラネット	●豊田市例規集 ●豊田市議会議事録 ●統合型地図情報システム など	各所管課
個別導入システム	●人事管理システム ●契約管理システム ●統合型GIS ●災害対策本部システム ●戸籍総合システム など	各所管課

図 2-1 市において利用している情報システム

このうち、汎用機上で稼働する情報システムは、プログラムの開発・保守及び運用管理を情報システム課で実施しているため、当該システムの開発及び保守費用は、情報システム課の人員費として発生する。

汎用機上で稼働する情報システムは、信頼性・安定性が高く、複数業務の並行稼働性、大規模バッチ処理、大規模帳票出力業務等に優れる一方で、他の情報処理基盤との互換性に乏しく、対応するハードウェアやオペレーティングシステムを提供する特定の業者への依存度が高まりやすいなどの問題を

有する。

グループウェア上で稼働する情報システムは、市の内部における情報共有のためのソフトウェアとして、職員同士の情報の交換や共有、各種申請手続の申請や承認を電子的に実現するものであり、情報システム課が所管する。

また、庁内ネットワーク又はインターネット上で稼働する情報システムは、インターネット等の技術を用いることを前提として、ホームページを含む様々な形で情報を提供するものであり、各情報の担当部課等が所管する。

個別導入システムは、汎用機、グループウェア及び庁内ネットワーク又はインターネットのように全庁的に利用される情報システム基盤以外のものであり、各所管課で調達及び運用管理が行われる。これに含まれる情報システム基盤の種類や規模は様々であり、スタンドアロン、クライアント・サーバ型等の形態で利用されている。各所管課における費用は、実施政策ごとに集計されているため、情報システムに関連する費用のみを抽出して総額を把握することは困難である。

2 情報システム課の役割

情報システム課の事務分掌は、次のとおりとされる。

- (1) 電子計算組織の利用計画、総合調整、新規適用業務開発、管理運用及び適用業務の維持に関すること
- (2) OAに係る運用指導及び研修に関すること
- (3) 情報化の推進に関すること
- (4) データ保護に関すること

また、情報システム課における体制は、図 2-2 情報システム課組織構成のとおりである。

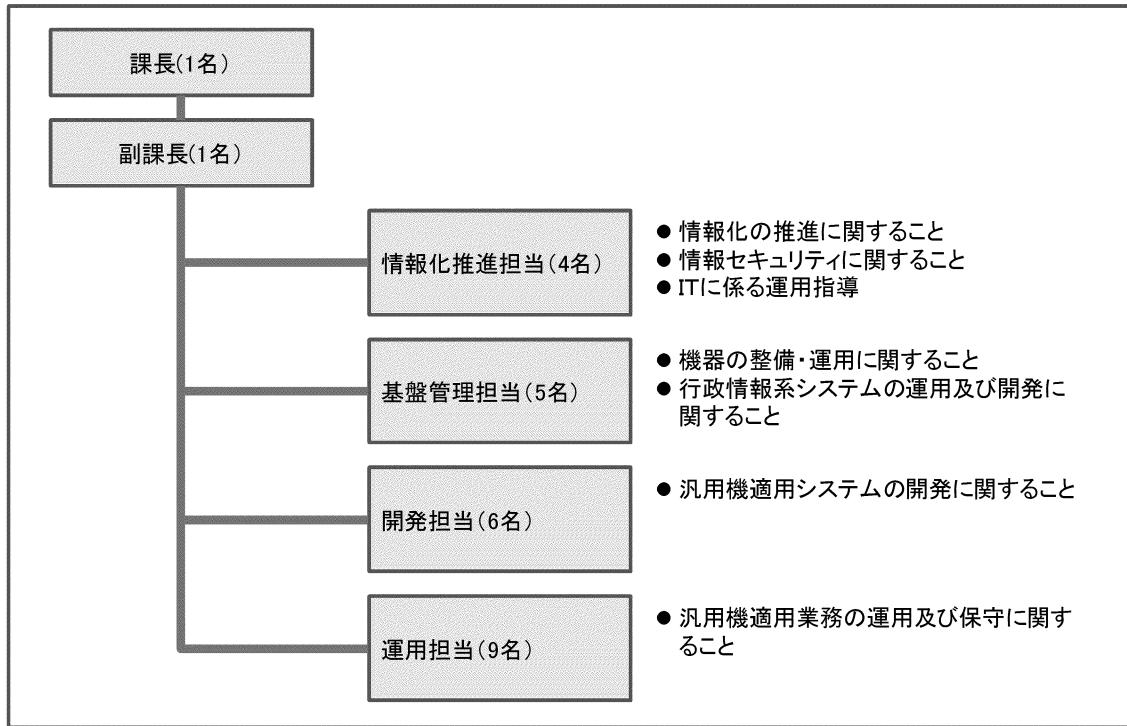


図 2-2 情報システム課組織構成

情報システム課では、前記の事務分掌に従い、汎用機系の情報システムの開発・運用を行うとともに、全序的に利用される情報資産の管理、情報化推進、情報セキュリティ管理及び情報システムに係る各課等への指導を行っている。

また、情報システム課の予算は、所管する汎用機及び全序的に利用される情報システムに係るものも含め、財政課の査定を経て配分される。

3 各情報システムの所管課等の役割

個別導入システムについては、各所管課において、企画、予算、機能設計、発注・調達、開発、運用・保守、関連帳票の管理等を行う。

情報システム課が管理するネットワーク基盤等を使用しない場合については、必要となるインフラについても整備を行っている。

また、情報システムの調達、開発及び運用・保守に係る業務を外部へ委託する場合は、外部委託業者の管理も各所管課が行う。

各所管課における情報システムに関する予算は、必要に応じて情報システム課の支援を受けつつ各所管課において策定し、財政課の査定を経て配分される。

4 情報システムに関する規則類

市においては、情報システムの調達に関する規則類として、「豊田市契約規則」、「物品契約事務の手引」及び「豊田市プロポーザル実施ガイドライン」を定めている。

また、市では、汎用機で稼働する情報システムについて内製を行っているため、「豊田市の情報処理～システム開発の手引き～」が作成され、情報セキュリティに関する規則類としては、「情報セキュリティ基本方針」、「情報セキュリティ基本要綱」、「共通実施手順」等が定められている。

以下に、各規則類の概要について述べる。

(1) 「豊田市契約規則」

市は、情報システムの調達についても、一般的な契約事務に基づき処理を行っている。そのため、地方自治法施行令第173条の2の規定に基づき、契約の締結、契約の履行、監督及び検査等、契約に関し必要な事項を「豊田市契約規則」として定めている。

(2) 「物品契約事務の手引」

契約課物品担当により作成されている業務マニュアルとして「物品契約事務の手引」が定められている。

同手引は、豊田市契約規則、豊田市物品管理規則及び豊田市物品検査要綱並びに豊田市物品管理事務細則に基づき作成され、市における物品購入及び借入れに関する契約事務の手順が定められている。

(3) 「豊田市プロポーザル実施ガイドライン」

情報システムの調達に際し、市が想定する契約締結方法は、一般競争入札、指名競争入札及び随意契約の3種類である。

このうち、随意契約により契約を締結する場合に、性質や目的上、品質を追求する必要がある契約において、公募等により提案書の提出を受け、当該契約の履行に最も適した契約の相手方を特定する方式（プロポーザル方式）を採用することがある。

「豊田市プロポーザル実施ガイドライン」では、当該方式による契約の相手方の選定手続について、公平性、透明性及び客観性を確保するために必要

な事項が定められている。

(4) 「豊田市の情報処理～システム開発の手引き～」

市では、情報システムの導入は必ずしも外部からの調達という手段によることなく、財務情報システムを始め、汎用機上で稼働するアプリケーションシステムの多くを情報システム課職員の手により内製している。

そのため、情報システム課に配属された職員に対するガイダンスとして、あるいは情報システム課職員が開発作業を進めるに当たり、従うべき作業手順として、「豊田市の情報処理～システム開発の手引き～」が定められている。

(5) 「豊田市電子計算機処理管理運営規程」

市では、主に汎用機による処理の管理運営について必要な事項を「豊田市電子計算機処理管理運営規程」として定めている。

同規程には、データ保護、汎用機上で実行する処理の依頼手順、端末装置の操作制限、電子計算機室の立入制限及び保安措置等の事項が定められている。

(6) 「情報セキュリティ基本方針」

市は、個人情報を始めとして市が保有する重要な情報及びその情報を扱う情報システムについて、職員が守るべき基準を「豊田市情報セキュリティ基本方針」として定めている。

当該基本方針は、国等において「情報セキュリティポリシー」と呼ばれるものに相当する。

市のホームページでは、市が保有する情報や情報システムの安全性を維持向上するため、当該方針に基づき以下の総合的かつ体系的な情報セキュリティ対策を進めるとされている。

- ア 情報セキュリティに関し実施すべき項目を網羅した基本要綱と、具体的対策を確実に実行するための実施手順を定め、実践する。
- イ 基本要綱、実施手順は、実践結果の検証などにより定期的に見直し、情報セキュリティ対策の継続的な改善を進める。

ウ 市長を始めすべての職員が情報セキュリティの重要性を認識し、基本要綱と実施手順を継続的に実践するための研修、訓練を実施する。

(7) 「豊田市情報セキュリティ基本要綱」

市は、「豊田市情報セキュリティ基本方針」に基づき、市の機関が実施すべき情報セキュリティ対策に関する必要な事項を「豊田市情報セキュリティ基本要綱」として定めている。

同要綱では、情報セキュリティ組織及び体制、情報セキュリティ文書の管理、情報資産の分類と管理のほか、物理的セキュリティ、技術的セキュリティ等に関する事項が定められている。

(8) 「共通実施手順」

「共通実施手順」は、「豊田市情報セキュリティ基本要綱」に基づき、共通して遵守すべき事項及び基準を定めている。

当該手順の内容には、情報処理装置保護基準、パスワード管理基準を中心とする複数の管理基準等が含まれる。

(9) 「個別実施手順」

「個別実施手順」は、「豊田市情報セキュリティ基本要綱」及び「共通実施手順」に基づき、個別の情報資産に関し遵守すべき事項を定めている。

5 情報セキュリティに関する取組

(1) 規程類

市が定める情報セキュリティに関する規程としては、上述のとおり「豊田市情報セキュリティ基本方針」、「豊田市情報セキュリティ基本要綱」、「共通実施手順」、「個別実施手順」等が定められている（以下これらの規程を「セキュリティ文書」という。）。

なお、「豊田市情報セキュリティ基本要綱」、「共通実施手順」及び「個別実施手順」は、本監査の実施期間中である平成27年9月に大幅な改定がなされている。本監査の対象期間は平成26年度を基本としているため、本報告書において特段の記載がない場合は、平成26年度当時に存在した改定前のものを

示している。

(2) 組織体制

市は、情報セキュリティに係る管理及び運営を行うため、図 2-3 のとおり組織体制を整備している。

市長は、情報セキュリティに関する最高責任者として情報セキュリティ統括責任者を担当し、副市長、教育長及び事業管理者が情報セキュリティ副統括責任者としてその補佐を行う。

また、総務部長は、情報セキュリティを適切に維持管理するため、情報セキュリティ文書の運営管理責任者として情報セキュリティ管理者を担当し、総務部副部長が情報セキュリティ副管理者としてその補佐を行う。

各部局等において所管する情報資産の統括的な管理責任者である情報セキュリティ部門管理者は、各部局の副部長等が担当し、具体的な情報セキュリティ対策を実施する情報セキュリティ責任者は、担当課長等が担当する。

情報セキュリティ委員会は、情報セキュリティに関し、市政全般の視点から基本方針及び基本要綱の制定及び改正について審議を行うものであり、市長の主宰の下に、副市長並びに教育長、事業管理者、部長、消防長、上下水道局長及び部長権限を持つ政策監で構成される。

情報セキュリティ対策会議は、上述のような情報セキュリティに関する規程類の制定及び改定のほか、情報処理施設、情報処理装置及び情報システムの導入及び変更並びに情報処理に関する委託契約の締結の審議又は検討を行うものであり、総務部長、総務部副部長及び情報セキュリティ責任者である各所属長で構成される。

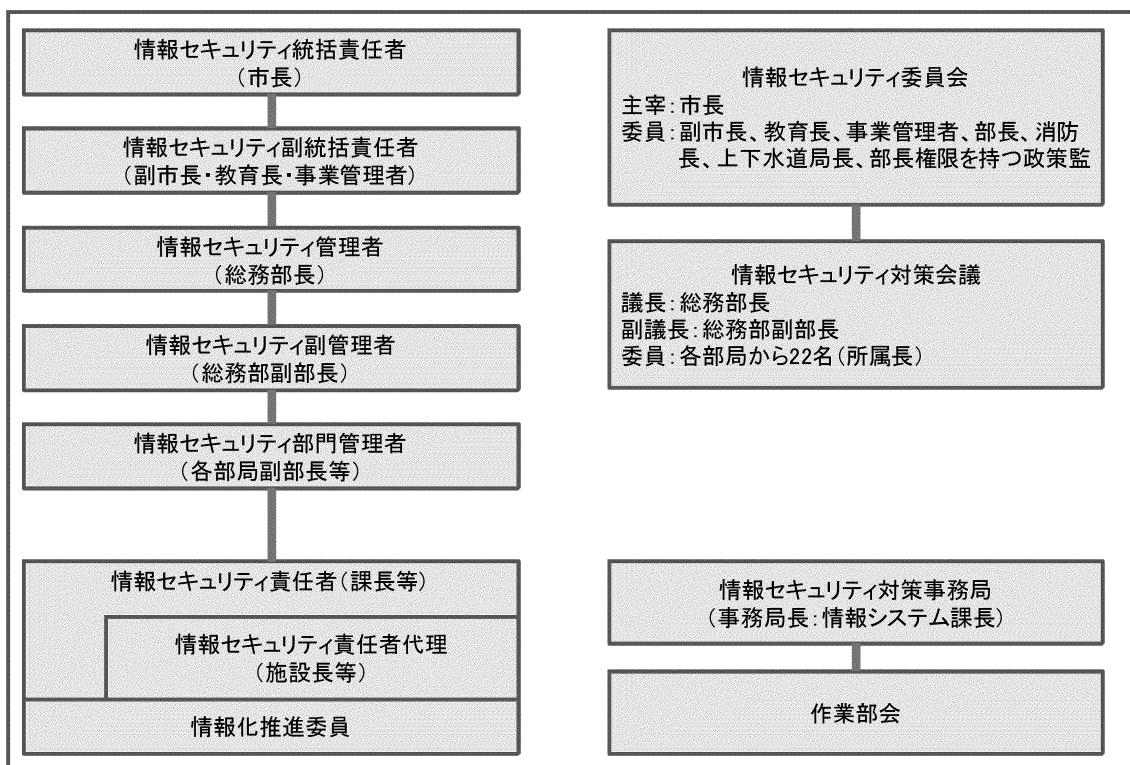


図 2-3 市のセキュリティ組織体制

(3) 研修・訓練

情報セキュリティに関する教育研修は、新規採用職員研修を中心に隨時実施し、情報セキュリティの意識向上を図っている。

(4) 監査

平成 24 年度から平成 26 年度までにおいて、情報セキュリティ管理に関する内部監査は実施されていない。過去において情報セキュリティに関する状況調査として、情報システム課から各所管課に対するヒアリングが行われた例がある。

外部監査としては、平成 17 年度から平成 26 年度までにおいて、あいち電子自治体推進協議会による共同セキュリティ監査が毎年実施されている。

第3 外部監査の結果

1 実施手続の概要

本監査では、まず、アンケートにより市で使用される情報システムについて予備調査を行い、金額及び各情報システムの使用状況に関する情報を収集し、その後に、本調査として対象とした情報システムについて質問、資料の閲覧等を実施した。

以下に各手順について述べる。

(1) アンケートによる情報システムに関する予備調査

市で使用される情報システムには、情報システム課が所管する汎用機及びグループウェア上で稼働するもののほか、各課で個別に導入したものが存在する。

今回の調査においては、市で使用される情報システムの中で金額的又は質的に重要なものを対象とする狙いから、情報システムの概要のほか、情報システムの調達、情報システムの経済性・効率性・有効性及び情報システムの安全性に関するアンケートを作成した（表3-1参照）。

アンケートの配布対象は、情報システム課が整備する情報システム資産管理台帳を基に、平成26年度において投資が計画されていたもの、個人情報を取り扱うとされるもの等を条件として抽出した。

当該アンケートは、64部局（情報システムの数にして136件）を対象に配布し、その全件を回収した。

表3-1 アンケート項目

アンケート項目
情報システムID
情報システム名
情報システムの概要
所管課の名称
稼働開始日
情報システムの開発形態
情報システムの運用形態
情報システムの開発事業者
情報システムの改修事業者

情報システムの運用事業者
情報システムの利用部課等
情報システム利用者の人数
市民の利用状況
概算のアクセス件数
ハードウェアの設置場所
初期導入費用の金額
運用費用の金額

(2) 本調査の対象とする情報システムの選定基準

上記アンケートの回答に基づき、平成 24 年度から平成 26 年度までにおける初期導入費用及び保守費用の金額的な重要性又は今回の監査の視点から考慮すべき質的な重要性を勘案し、本調査の対象を選定した。

(3) 本調査

本調査の対象として選定された情報システム及び部課等は次のとおりである。当該情報システムを対象として、質問、資料の閲覧等を実施した。

表 3-2 本調査の対象として選定された情報システム及び部課等

No.	部局名等	課名等	情報システム名
1	経営戦略室	市政発信課	豊田市ホームページ管理システム
2	総務部	人事課	人事管理システム
3	総務部	契約課	契約管理システム
4	総務部	情報システム課	汎用機上で稼働する情報システム
5	総務部	情報システム課	統合型 GIS
6	総務部	技術管理課 用地審査課(*)	土地開発基金管理システム
7	税務財産部	資産税課	固定資産地図情報システム
8	社会部	交通安全防犯課	ネットワーク防犯カメラシステム
9	社会部	生涯学習課	とよた科学体験館プラネタリウム投影システム
10	社会部	防災対策課	災害対策本部システム
11	社会部	防災対策課	映像中継システム

12	社会部	防災対策課	気象情報システム
13	社会部	防災対策課	防災行政無線システム
14	環境部	環境政策課	とよたエコポイントシステム
15	市民福祉部	総務課	電子カルテシステム
16	市民福祉部	総務課	医用画像管理システム
17	市民福祉部	総務課	乙ヶ林診療所コンピューテッドラジオグラフィーシステム
18	市民福祉部	市民課	戸籍総合システム
19	市民福祉部	市民課	住基ネットシステム
20	市民福祉部	地域福祉課	地域包括支援センターシステム
21	市民福祉部	介護保険課	介護保険指定期間等管理システム
22	健康部	健康政策課	特定健診等データ入力システム
23	都市整備部	交通政策課	バス位置情報提供サービスシステム
24	都市整備部	建築相談課	指定道路台帳システム
25	建設部	幹線道路推進課	大気データ処理システム
26	建設部	河川課	工損費用算定システム
27	上下水道局	経営管理課	公営企業会計システム
28	上下水道局	料金課	検針収納システム
29	上下水道局	水道整備課	水道管網解析システム
30	上下水道局	水道維持課	上水道地図情報システム
31	上下水道局	下水道施設課	下水道地図情報・排水設備情報ファイリングシステム
32	教育行政部	スポーツ課	豊田市スポーツ施設利用システム
33	教育行政部	図書館	図書館システム
34	学校教育部	学校教育課	学校図書館管理システム
35	学校教育部	保健給食課	学校給食管理システム
36	消防本部	指令課	消防指令システム
37	消防本部	予防課	防災学習センター用システム

※ 平成 26 年度から用地審査課が新設され、技術管理課から事務が移管されている。

(4) 調査対象とする情報システムの概要

調査対象として選定した情報システムの概要は、次のとおりである。

ア 豊田市ホームページ管理システムについて

豊田市ホームページ管理システムは、市民に対する行政サービスの情報提供及び市内外に向けた広報（情報発信）のための Web サイト構築に用いるシステムであり、平成 21 年 12 月に導入され、平成 27 年 7 月に更改されている。

当該システムは、市政発信課の所管とされ、システムの利用者数は、市政発信課等の職員約 20 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-3 豊田市ホームページ管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
25,712	22,653	20,345	18,182

イ 人事管理システムについて

人事管理システムは、職員の入事情報を管理するシステムであり、平成 10 年 10 月に導入されている。

当該システムは、人事課の所管とされ、システムの利用者数は、人事課の職員約 20 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-4 人事管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	7,528	5,996	4,533

※リース契約のため、初期導入費用は発生していない。

ウ 契約管理システムについて

契約管理システムは、契約事務の執行に係る帳票の作成及び契約情報のデータを管理するシステムであり、平成 21 年 3 月に導入されている。

当該システムは、契約課の所管とされ、システムの利用者数は、市の職員約 3,200 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-5 契約管理システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	10,537	15,587	5,516

※リース契約のため、初期導入費用は発生していない。

エ 統合型 GIS について

統合型 GIS (Geographic Information System) は、全庁で利用され、豊田市全域が網羅されている地理情報システムであり、平成 16 年 3 月に導入されている。

当該システムは、情報システム課の所管とされ、システムの利用者数は、市の職員約 3,200 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-6 統合型 GIS の初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
9,135	2,455	2,455	4,878

オ 土地開発基金管理システムについて

土地開発基金管理システムは、土地・物件所有者情報等を管理するシステムであり、平成 17 年 4 月に導入された。

当該システムは、当初、技術管理課の所管とされていたが、平成 26 年度からは用地審査課の所管とされている。当該システムの利用人数は、街路課、幹線道路推進課、土木課、河川課、地域建設課、業務課及び公園課の職員約 50 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-7 土地開発基金管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
5,000	202	202	2,263

カ 固定資産地図情報システムについて

固定資産地図情報システムは、資産税に関する図面情報とデータベース情報を統合利用する地図情報システムであり、平成 24 年 4 月に導入されている。

当該システムは、資産税課の所管とされ、システムの利用者数は、資産税課の職員約 50 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-8 固定資産地図情報システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
13,020	50,030	56,385	65,772

キ ネットワーク防犯カメラシステムについて

ネットワーク防犯カメラシステムは、市内に設置された防犯カメラの映像をネットワークを通じて参照することが可能なシステムであり、平成 25 年 12 月に導入されている。

当該システムは、交通安全防犯課の所管とされ、システムの利用者数は、ネットワーク式カメラを導入する各課の管理責任者及び指定された取扱者約 160 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-9 ネットワーク防犯カメラシステムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	—	1,442	21,640

※外部委託業者から機器及びシステムを借り受けているため、初期導入費用は発生していない。また、当該システムは平成 25 年 12 月に導入されているため、平成 24 年度の運用費用は発生していない。

ク とよた科学体験館プラネタリウム投影システムについて

とよた科学体験館プラネタリウム投影システムは、プラネタリウム投影及び映像を管理するシステムであり、平成 20 年 3 月に導入された。

当該システムは、生涯学習課の所管とされ、システムの利用者数は、とよた科学体験館の職員約 5 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-10 とよた科学体験館プラネタリウム投影システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
446,000	6,647	6,647	6,837

ケ 災害対策本部システムについて

災害対策本部システムは、災害時等における情報の一元化・集約化を図るためのシステムであり、平成 27 年 4 月に導入されている。

当該システムは、防災対策課の所管とされ、システムの利用者数は、市の職員約 3,200 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-11 災害対策本部システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
59,283	—	—	—

※当該システムは平成 27 年 4 月に導入されているため、平成 24 年度から平成 26 年度までの運用費用は発生していない。

コ 映像中継システムについて

映像中継システムは、被災現場等からの映像を動画で中継するシステムであり、平成 27 年 7 月に導入されている。

当該システムは、防災対策課の所管とされ、システムの利用者数は、防災対策課と各出張所の職員約 180 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-12 映像中継システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
14,227	—	—	—

※当該システムは平成 27 年 7 月に導入されているため、平成 24 年度から平成 26 年度までの運用費用は発生していない。

サ 気象情報システムについて

気象情報システムは、雨量・水位・風向風速・震度情報を管理とともに、ウェブサイトで情報提供するためのシステムであり、平成 18 年 2 月に導入されている。

当該システムは、防災対策課の所管とされ、システムの利用者数は、防災対策課の職員約 15 名である。

また、当該システムで管理される情報は一般公開され、下記 URL から閲覧可能である。

雨量情報

<http://www2.city.toyota.aichi.jp/weather/rain/rain01h.html>

震度情報

<http://www2.city.toyota.aichi.jp/shindo/index.html>

当該システムに係る過年度の費用は、下表のとおりである。

表 3-13 気象情報システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	9,014	8,049	8,415

※初期導入費用は、契約書類等が保存されていないため不明である。

シ 防災行政無線システムについて

防災行政無線システムは、災害時等の緊急情報の伝達・情報収集・相互通信を行うためのシステムであり、平成20年10月に導入されている。

当該システムは、防災対策課の所管とされ、システムの利用者数は、市の職員約3,200名である。

当該システムに係る過年度の費用は、下表のとおりである。

表3-14 防災行政無線システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成24年度	平成25年度	平成26年度
4,406,358	110,250	98,700	113,400

ス とよたエコポイントシステムについて

とよたエコポイントシステムは、とよたエコポイントの管理をするためのシステムであり、平成21年6月に導入されている。

当該システムは、環境政策課の所管とされ、システムの利用者数は、環境政策課の職員約5名である。

当該システムに係る過年度の費用は、下表のとおりである。

表3-15 とよたエコポイントシステムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成24年度	平成25年度	平成26年度
1,575	5,266	4,795	6,935

セ 電子カルテシステムについて

電子カルテシステムは、豊田地域医療センターにおける患者の診療及び診療録を管理するシステムであり、平成23年3月に導入されている。

当該システムは、市民福祉部総務課の所管とされ、システムの利用者数は、豊田地域医療センターの職員約500名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-16 電子カルテシステムの初期導入費用及び運用費用
(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
181,620	18,659	18,659	18,659

ソ 医用画像管理システムについて

医用画像管理システムは、豊田地域医療センターにおける放射線・生理・内視鏡画像及びレポートを保存し、統合的に参照するシステムであり、平成 24 年 3 月に導入されている。

当該システムは、市民福祉部総務課の所管とされ、システムの利用者数は、豊田地域医療センターの職員約 500 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-17 医用画像管理システムの初期導入費用及び運用費用
(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
151,800	6,720	6,720	6,720

タ 乙ヶ林診療所コンピューテッドラジオグラフィーシステムについて

乙ヶ林診療所コンピューテッドラジオグラフィーシステムは、乙ヶ林診療所におけるレントゲン画像診断システムであり、平成 27 年 3 月に更改されている。

当該システムは、市民福祉部総務課の所管とされ、システムの利用者数は、乙ヶ林診療所の職員 1 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-18 乙ヶ林診療所コンピューテッドラジオグラフィーシステムの初期導入費用及び運用費用

(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
13,446	—	—	—

※当該システムは平成 27 年 3 月に導入されているため、平成 24 年度から平成 26 年度までの運用費用は発生していない。

チ 戸籍総合システムについて

戸籍総合システムは、戸籍及び戸籍に関する事務を管理するためのシステムであり、平成 10 年 10 月に導入されている。

当該システムは、市民課の所管とされ、システムの利用者数は、市民課と各出張所の職員約 140 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-19 戸籍総合システムの初期導入費用及び運用費用

(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	25,407	22,890	25,173

※リース契約のため、初期導入費用は発生していない。

ツ 住基ネットシステムについて

住基ネットシステムは、住民基本台帳法に基づき、住民基本台帳を管理するシステムであり、平成 14 年 8 月に導入されている。

当該システムは、市民課の所管とされ、システムの利用者数は、市民課と各支所等の職員約 120 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-20 住基ネットシステムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
4,725	7,085	6,767	6,696

テ 地域包括支援センターシステムについて

地域包括支援センターシステムは、地域包括支援センターと情報共有を行うためのシステムであり、平成 24 年 3 月に更改されている。

当該システムは、地域福祉課の所管とされ、システムの利用者数は、地域福祉課、地域包括支援センター及び基幹包括支援センターの職員約 120 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-21 地域包括支援センターシステムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	8,113	8,113	8,113

※リース契約のため、初期導入費用は発生していない。

ト 介護保険指定期間等管理システムについて

介護保険指定期間等管理システムは、介護保険指定事業者の管理に用いるシステムであり、平成 24 年 4 月に導入されている。

当該システムは、介護保険課の所管とされ、システムの利用者数は、介護保険課の職員約 10 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-22 介護保険指定期間等管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	1,564	1,354	2,851

※リース契約のため、初期導入費用は発生していない。

ナ 特定健診等データ入力システムについて

特定健診等データ入力システムは、医療機関から受領した特定健診等の結果をデータ化するためのシステムであり、平成 20 年 4 月に導入されている。

当該システムは、健康政策課の所管とされ、システムの利用者数は、健康政策課及び豊田加茂医師会の職員約 5 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-23 特定健診等データ入力システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	1,654	1,670	2,311

※初期導入費用は、契約書類等が保存されていないため不明である。

ニ バス位置情報提供サービスシステムについて

バス位置情報提供サービスシステムは、とよたおいでんバスの現在位置等について、インターネットを介してパソコンや携帯電話に情報提供を行うシステムであり、平成 21 年 4 月に導入されている。

当該システムは、交通政策課の所管とされ、システムの利用者数は、交通政策課の職員約 15 名である。また、当該システムで管理される情報は一般公開され、下記 URL 内の「バス位置情報提供サービス」から閲覧可能である。

<http://michinavitoyota.jp/portal/index.html>

当該システムに係る過年度の費用は、下表のとおりである。

表 3-24 バス位置情報提供サービスシステムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	8,134	7,333	7,726

※外部委託業者から借り受けているため、初期導入費用は発生していない。

ヌ 指定道路台帳システムについて

指定道路台帳システムは、建築基準法施行規則の改正により、指定道路台帳を整備し、照会や確認を円滑にするシステムであり、平成 23 年 4 月に導入されている。

当該システムは、建築相談課の所管とされ、システムの利用者数は、建築相談課及び土木管理課の職員約 15 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-25 指定道路台帳システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
170,876	3,203	4,200	5,022

ネ 大気データ処理システムについて

大気データ処理システムは、大気観測局から送られてくる大気データを処理し、豊田市のウェブサイトで随時公開するシステムであり、平成 16 年 12 月に導入されている。

当該システムは、幹線道路推進課の所管とされ、システムの利用者数は、幹線道路推進課の職員 2 名である。また、当該システムで処理される情報は一般公開され、下記 URL から閲覧可能である。

<http://www2.city.toyota.aichi.jp/dourokankyou/index.html>

当該システムに係る過年度の費用は、下表のとおりである。

表 3-26 大気データ処理システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	15,501	8,021	9,839

※機器設置等の初期導入費用は、国と愛知県が負担している。

ノ 工損費用算定システムについて

工損費用算定システムは、河川での工事に際し、工事現場周辺で発生する事業損失費用を算定するシステムであり、平成 27 年 1 月に導入されている。

当該システムは、河川課の所管とされ、システムの利用者数は、河川課の職員 3 名である。

当該システムはベータ版のソフトウェアであり、当該システムの導入及び運用に係る費用は発生していない。

ハ 公営企業会計システムについて

公営企業会計システムは、上下水道事業の財務、契約事務、固定資産、貯蔵品等を管理するためのシステムであり、平成 9 年 11 月に導入されている。

当該システムは、経営管理課の所管とされ、システムの利用者数は、経営管理課及び水道局各課の職員約 150 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-27 公営企業会計システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	12,925	12,925	12,985

※リース契約のため、初期導入費用は発生していない。

ヒ 検針収納システムについて

検針収納システムは、水道業務に使用するハンディターミナルのデータ入出力等を管理するためのシステムであり、平成 26 年 8 月に導入されている。

当該システムは、料金課の所管とされ、システムの利用者数は、料金課の職員約 10 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-28 検針収納システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
15,418	—	—	2,510

※当該システムは平成 26 年 8 月に導入されているため、平成 24 年度から平成 25 年度までの運用費用は発生していない。

フ 水道管網解析システムについて

水道管網解析システムは、上水道管の流量、流速等を解析し、緊急時における断水シミュレーション等に使用するシステムであり、平成 11 年度に導入されている。

当該システムは、水道整備課の所管とされ、システムの利用者数は、水道整備課及び水道維持課の職員約 25 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-29 水道管網解析システムの初期導入費用及び運用費用

(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
276	2,447	3,245	10,833

ヘ 上水道地図情報システムについて

上水道地図情報システムは、上水道施設の維持管理業務及び窓口業務の効率化を図るシステムであり、平成 12 年 4 月にシステム更改されている。

当該システムは、水道維持課の所管とされ、システムの利用者数は、水道維持課、水道整備課、上水運用センター、水道料金課、地域水道課、上下水道総務課及び一般財団法人豊田市水道サービス協会の職員約 180 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-30 上水道地図情報システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
440,780	33,694	29,494	31,193

ホ 下水道地図情報・排水設備情報ファイリングシステムについて

下水道地図情報・排水設備情報ファイリングシステムは、道路等の工事に際し、周辺の下水道や排水設備の設置状況の調査に用いるシステムであり、下水道地図情報システムは平成 11 年 2 月に、排水設備情報システムは平成 15 年 6 月に導入され、平成 26 年 2 月に更改されている。

当該システムは、下水道施設課の所管とされ、システムの利用者数は、下水道施設課、下水道建設課及び料金課の職員約 50 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-31 下水道地図情報・排水設備情報ファイリングシステムの初期導入費用及び運用費用

(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	21,658	21,165	21,806

※リース契約のため、初期導入費用は発生していない。

マ 豊田市スポーツ施設利用システムについて

豊田市スポーツ施設利用システムは、市内スポーツ施設の予約、管理等の業務に使用するためのシステムであり、平成 17 年 4 月からインターネットによる一般利用が可能となった。

当該システムは、スポーツ課の所管とされ、システムの利用者数は、スポーツ課の職員約 20 名である。また、当該システムは一般公開され、下記 URL から利用可能である。

<https://www.cm1.epss.jp/TOSS/index.html>

当該システムに係る過年度の費用は、下表のとおりである。

表 3-32 豊田市スポーツ施設利用システムの初期導入費用及び運用費用
(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	22,452	22,452	23,051

※機器はリース契約であり、システムは外部委託業者から借り受けているため、初期導入費用は発生していない。

ミ 図書館システムについて

図書館システムは、豊田市中央図書館の蔵書や貸出しを管理するシステムであり、昭和 60 年 10 月に導入され、平成 25 年 1 月に更改されている。

当該システムは、図書館の所管とされ、システムの利用者数は、図書館及び交流館の職員約 250 名である。また、当該システムで管理されている情報は一般公開され、図書館内に設置された端末の他、下記 URL から利用可能である。

<http://www.library.toyota.aichi.jp/>

当該システムに係る過年度の費用は、下表のとおりである。

表 3-33 図書館システムの初期導入費用及び運用費用
(単位：千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	48,294	35,020	35,356

※リース契約のため、初期導入費用は発生していない。

ム 学校図書館管理システムについて

学校図書館管理システムは、学校図書館における蔵書や貸出しを管理するシステムであり、平成 21 年 2 月に導入されている。

当該システムは、学校教育課の所管とされ、システムの利用者数は、学校教育課の職員約 30 名である。また、各学校の教職員や児童・生徒も、図書の貸出手続において利用している。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-34 学校図書館管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	31,566	29,837	11,940

※リース契約のため、初期導入費用は発生していない。

メ 学校給食管理システムについて

学校給食管理システムは、市立の学校で提供される給食を管理するシステムであり、平成 26 年 7 月に導入されている。

当該システムは、保健給食課の所管とされ、システムの利用者数は、保健給食課、保育課、給食センター等の職員約 40 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-35 学校給食管理システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
8,610	9,607	7,578	8,749

モ 消防指令システムについて

消防指令システムは、市の消防本部が、消防活動等を迅速かつ効率的に実施するため、119 番通報の受付から出動指令まで及び現場活動支援から事案終了までを迅速かつ確実に管理するためのシステムであり、平成 21 年 12 月に導入されている。

当該システムは、指令課の所管とされ、システムの利用者数は、消防本部の職員約 500 名である。

当該システムに係る過年度の費用は、下表のとおりである。

表 3-36 消防指令システムの初期導入費用及び運用費用
(単位 : 千円)

初期導入費用	運用費用		
	平成 24 年度	平成 25 年度	平成 26 年度
—	228,324	228,051	189,337

※リース契約のため、初期導入費用は発生していない。

ヤ 防災学習センター用システムについて

防災学習センター用システムは、豊田市防災学習センターの各種体験コーナーを来館者が利用するためのシステムであり、平成18年4月に導入されている。

当該システムは、予防課の所管とされ、防災学習センターの各種体験コーナーで稼働している。

当該システムに係る過年度の費用は、下表のとおりである。

表3-37 防災学習センター用システムの初期導入費用及び運用費用
(単位:千円)

初期導入費用	運用費用		
	平成24年度	平成25年度	平成26年度
234,255	8,040	6,968	8,808

2 総括的事項

(1) 情報システムの調達に係るガイドラインの整備(意見)

市の情報システムの調達に関するルールとしては、一般的な契約事務に関する規則である豊田市契約規則、一般的な物品調達に関する手引である物品契約事務の手引等が作成されているのみであり、情報システムの調達に係る手順等について直接的に記述したものは存在していない。

情報システムの調達においても、競争原理を働かせ、投資コストの適正化を図ることが期待されるものである。情報システムの調達に際しては、情報システムのライフサイクル、契約単位及び品質管理並びに情報セキュリティ等の専門的・技術的な知識が必要となる場面も想定される。

一方、市においては、情報システムの調達において考慮すべきライフサイクル、契約単位及び品質管理に係る検討は、調達を行う各所管課において行っている。情報セキュリティ等については情報システム課による審査が行われるが、ライフサイクルや契約単位の検討については、情報システム課の担当事務を外れるため、各所管課で個別に判断を行っている。

そのため、情報システムの保守費用を見直す機会がないまま長年にわたり継続的に使用している例、契約単位の検討が担当者の判断に依存している例、

購入により調達した場合に実施する検収等による品質確認が、リース契約により調達する場合には実施されていない等、一般的な物品調達に関する手順だけでは対処することができない例等が見受けられた。

情報システムの調達に関する直接的なルールが定められていない背景としては、財務情報システム、税務関係システム等市政の根幹に関わる重要な情報システムを情報システム課で内製しているため、各所管課においては、比較的小規模で、導入に伴うリスクが小さい簡易なパッケージソフトウェア等の情報システムを調達する場合が多いためと考えられる。

しかし、近年、情報システム技術の進展に伴い、従来の汎用機からクライアント・サーバ型システムへの移行等、情報システムの利用環境も大きく変化してきている。そのため、各所管部署において調達する情報システムのライフサイクルや契約形態にも徐々に変化が生じている。また、現在使用している汎用機についても、技術的な基盤の変更又は委託開発等による外製システムへの移行を行わざるを得ない状況が生じる可能性がある。

このような環境の変化に対応しつつ、情報システムの調達に係るコストの適正化を図り、必要な品質を確保するための基本的な考え方及び事務手順の整備を検討されたい。

(2) 情報システムの調達における総合評価方式の導入（意見）

市において、情報システムを調達する際の契約方式は、価格のみを考慮する場合は、最低価格落札方式による一般競争入札又は指名競争入札が採用される。

一方で、調達対象の性質又は目的が競争入札に適さないものは、随意契約が採用される。

また、随意契約のうち、「広範かつ高度な知識、専門的な技術又は豊かな経験を必要とするとき」等、調達対象の価格だけでなく性能面についても考慮する必要がある場合は、公募等により提案書の提出を受け、当該契約の履行に最も適した相手方を選定するプロポーザル方式が実施される。

このうち、一般競争入札については、最低価格落札方式のほかに、総合評価落札方式が用いられる場合がある。

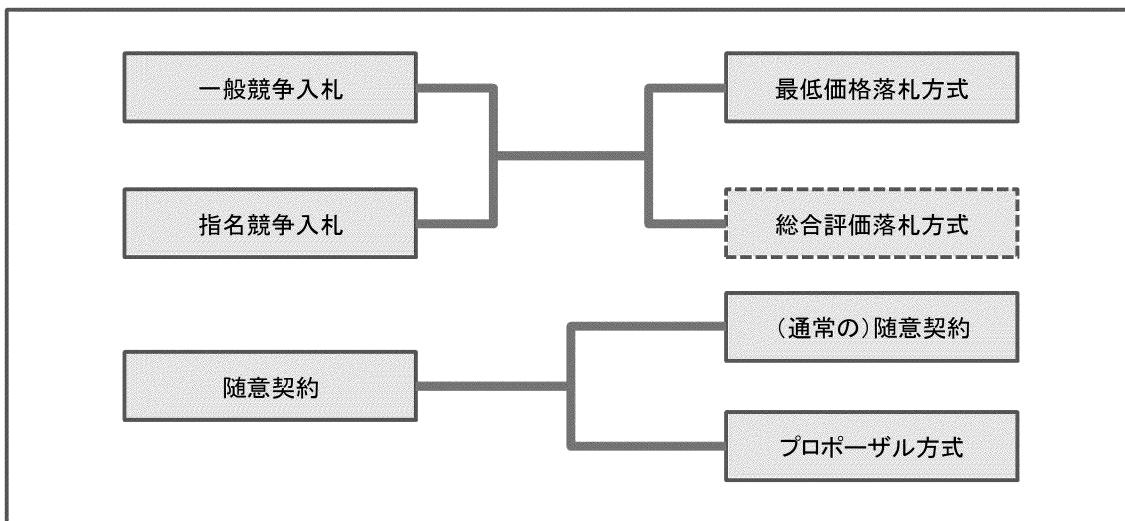


図 3-1 契約方法の分類

総合評価落札方式とは、地方自治法施行令第167条の2の規定に基づき、価格のほかに、価格以外の技術的な要素を評価の対象に加え、品質や施工方法等を総合的に評価し、価格と技術力及び信頼性・社会性の両面から最も優れたものをもって申込みをした者を落札者とする方式をいい、市にあっては「豊田市業務委託総合評価方式実施要綱」において要件、手順等が定められている。ただし、市において総合評価落札方式を採用する場合、「人件費割合の高い業務委託」であることを運用上の条件とし、さらには、「人件費割合が高い業務委託」は、清掃業務、警備業務、植物管理及び受付に限定され、情報システムの調達は対象に含まれていない。

そのため、結果的に、市において情報システムを調達する場合に、総合評価落札方式による一般競争入札を実施することはない」とされている。

また、現状では、プロポーザル方式が採用される具体的な条件が不明であり、提案内容における性能面と価格面の比重について明確な定めがないため、情報システムの調達において、性能と価格の両面を考慮した上で情報システム調達コストを最適化する方法が、十分に整備されていないと考えられる。

総合評価落札方式は、国においては「情報システムの調達に係る総合評価落札方式の標準ガイドライン」（平成25年7月19日調達関係省庁申合せ）が取りまとめられ、各地方自治体においても広く採用されている方式であり、価格だけでなく、性能面及び技術面の評価を考慮すべき情報システムの調達に馴染むものといえる。

もっとも、総合評価落札方式による場合、プロポーザル方式等と比較して落札者決定基準の設定等追加的な手續が必要となり、小規模な案件に適用する場合は、事務工数が増加することによる不効率を生じる可能性がある。

しかし、大規模な案件においては、価格面だけでなく性能面及び技術面を総合的に評価するメリットは大きいため、情報システムの調達についても、総合評価落札方式を採用する要件及び手順の整備を検討されたい。

(3) 情報セキュリティ対策に係る監査の実施（指摘）

豊田市情報セキュリティ基本要綱第81条では、セキュリティ文書に従って情報資産が適切に管理運用されていることを定期的に確認するものと定められている。市では、各所管課に対する状況調査のヒアリング及びあいち電子自治体推進協議会による共同セキュリティ監査は実施されていたものの、内部監査、自主点検等が実施された例はないとされる。

個別的事項として後述する項目の中には、セキュリティ文書に定めた事項が遵守されていない事例も散見され、情報セキュリティ対策の改善が十分に図られているとはいえない。

情報セキュリティ対策に係る実践結果を検証するため、内部監査、自主点検等を実施する必要があると考える。

今後は、情報セキュリティ対策の継続的な改善を行う観点から、セキュリティ文書に従って情報資産が適切に管理運用されていることを定期的に確認する必要がある。なお、市は平成27年度に情報セキュリティ対策事務局による内部監査を実施し、この点を確認している。

(4) 情報セキュリティ基本要綱・共通実施手順の定期的な見直し（指摘）

豊田市情報セキュリティ基本方針では、基本要綱、実施手順は、実践結果の検証などにより定期的に見直し、情報セキュリティ対策の継続的な改善を進めるとされている。

しかし、豊田市情報セキュリティ基本要綱の改定日は平成25年4月1日、共通実施手順の改定日は平成27年3月23日であるものの、過去数年間において、いずれも実質的な見直しは行われていなかった。

平成27年9月の改定によって、セキュリティ文書の定めを実態に沿った形で大幅に見直したものと推察するが、情報資産の管理状況が長年チェックされていなかつたことは問題である。

今後は、セキュリティ文書に従って情報資産が適切に管理運用されていることを定期的に確認し、当該結果を受けてセキュリティ文書の見直しを行うことにより、情報セキュリティ対策の継続的な改善を行う必要がある。

(5) 情報セキュリティ対策会議の定期的な開催（指摘）

平成 24 年度以降における情報セキュリティ委員会及び情報セキュリティ対策会議の開催実績は、下表のとおりである。

表 3-38 情報セキュリティ委員会の開催実績（平成 24 年度～）

開催日	議題
平成 27 年 8 月 17 日	情報セキュリティポリシーの改正について（審議）

表 3-39 情報セキュリティ対策会議の開催実績（平成 24 年度～）

開催日	議題	標題
平成 26 年 5 月 26 日	該当なし	平成 26 年度豊田市情報セキュリティ対策会議委員の選任及び業務用パソコンのソフトウェア瑕疵等を改善する仕組みに関する意見について（照会）
平成 27 年 3 月 3 日	該当なし	共通実施手順「業務の外部委託等における情報セキュリティの確保に関する基準」及び「外部記録媒体管理基準」の改正案に関する意見について（照会）
平成 27 年 4 月 24 日	該当なし	平成 27 年度豊田市情報セキュリティ対策会議委員の選任について（通知）
平成 27 年 7 月 27 日	(1) 情報セキュリティポリシーの改正について（審議） (2) 情報セキュリティ組織内点検の実施について（意見照会） (3) アクセスログの活用について（意見照会） (4) 電子メール添付ファイルの暗号化について（意見照会）	該当なし

	(5) 部門サーバ室及び部門仮想サーバの運用について (報告)	
	(6) 市の情報セキュリティに関する現状について (報告) (7) 今後の予定について	
平成 27 年 10 月 22 日	(1) 情報セキュリティ組織内点検の実施について (意見照会) (2) 外部記録媒体の利用制限について (意見照会) (3) データセンターの利用について (意見照会) (4) 電子メール添付ファイルの暗号化について (意見照会) (5) マイナンバー制度に伴う 庁内ネットワークの再構築について (報告) (6) あいち電子自治体推進協議会 共同セキュリティ監査結果 (速報) について (報告) (7) 情報セキュリティ研修の実施について (報告) (8) 今後の予定について	該当なし

情報セキュリティ基本要綱第 22 条第 1 項によれば、セキュリティ管理者及びセキュリティ責任者は、セキュリティ文書について、毎年定期的に見直しを行うものとされ、セキュリティ文書の改正に係る審議には、情報セキュリティ対策会議による審議又は検討が必要とされる。

しかし、前項に記載のとおり、過去数年においてセキュリティ文書の実質的な見直しが行われていなかったため、平成 24 年度及び平成 25 年度においては、情報セキュリティ対策会議は開催されなかった。

そのため、今後は前項に記載したセキュリティ文書の定期的な見直しの実施と合わせて、総務部長及び所管課長等による情報セキュリティ対策会議を毎年開催する必要がある。

3 個別的事項

(1) 情報システムの調達に係る事務手続について

ア 情報システムの管理責任について

(ア) 概要

市には、公益財団法人豊田地域医療センター（以下「医療センター」という。）に無償で貸与している土地、家屋、その他附帯構造物及び医療機器その他の備品が存在している。当該医療機器その他の備品の中には情報システムも含まれており、当該情報システムには電子カルテシステム及び医用画像管理システムが含まれている。

市有財産としての情報システムを第三者に貸与する場合、市には資産管理責任がある。したがって、市は、第三者が市から貸与されている情報システムについて業者と契約を締結する場合にも、適切な契約がなされるよう管理する必要がある。

また、当該情報システムを貸与されている医療センターには、市とは異なる独自のルールとして「職務権限規程」が存在し、契約（予定価格の決定、契約の締結、契約金額の変更、契約内容の変更及び契約の解除）の決定権限について以下のとおり定められている。

表 3-40 契約の決定権限

決定権限者	決定区分
理事長	1件 3,000万円以上
副理事長、常務理事	1件 1,000万円以上 3,000万円未満
院長、事務局長	1件 500万円以上 1,000万円未満
事務長、部長、室長	1件 100万円以上 500万円未満
課長、科長	1件 100万円未満
備考	1,000万円以上のものは事務局長合議 500万円以上 1,000万円未満のものは事務長合議

	100 万円以上 500 万円未満のものは総務課長合 議
--	---------------------------------

また、これから述べる内容に関連して、地方自治法第 244 条の 2 に定められた指定管理者制度がある。指定管理者制度とは、公の施設の管理について、民間事業者等が有するノウハウを活用することにより、住民サービスの質の向上を図り、施設の設置の目的を効果的に達成するため、平成 15 年 9 月に施行された制度である。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘及び意見を述べることとする。

a 情報システムの管理責任について（意見）

（対象）

市民福祉部総務課（電子カルテシステム及び医用画像管理システム）

医療センターは、市から電子カルテシステム及び医用画像管理システムを無償で貸与されているが、当該情報システムの保守費については医療センターが負担している。また、平成 26 年度の保守契約の当事者は、医療センター及び外部委託業者のみであり、当該情報システムの所有者である市は含まれていなかった。

これは、市と医療センターとの間で締結されている「市有財産使用貸借契約書」第 7 条において、「乙（医療センター）は、貸付物件について維持保存、改良その他の経費を要するときは、これを負担するものとする。」と規定され、当該条項に基づき、医療センターが当該情報システムに係る保守契約の主体となり得るとの解釈に基づき、運用されていたものである。

この点につき、指定管理者制度においては、市と指定管理者との間で締

結する基本協定書の中に以下の条項を定めることとされ、市からの指定管理業務再委託承認通知書による承認後に、契約が締結されている。

(第三者への委託の制限)

(中略)

2 指定管理者は、管理運営業務のうちの主たる業務を除く業務を第三者へ委託し、又は請け負わせようとするときは、業務内容、業者名、契約金額を書面により甲に提出し、甲の承認を得なければならない。

(以下略)

当該条項が設けられた趣旨は、指定管理者制度に基づいて市の事業に係る管理運営業務が委託される場合、第三者への再委託が適切なものであるかどうかについて市が判断し、当該業務が適切に行われるよう監督する責任を有しているためと考えられる。

このような趣旨に鑑みれば、市の事業に係る管理運営業務を第三者に再委託する場合は、指定管理者制度に基づくか否かにかかわらず、市の承認を得ることが必要と考えられる。

電子カルテシステム及び医用画像管理システムに係る保守契約は、指定管理者制度ではなく市有財産使用貸借契約に基づくものであるが、市が所有する情報システムの保守業務を第三者に委託しようとするものであるため、指定管理者制度と同程度の対応を行うことが望ましい。

したがって、医療センターは、電子カルテシステム及び医用画像管理システムに係る保守契約を締結する際に、業務内容、業者名及び契約金額について、書面により市の承認を得ることを検討されたい。

b 契約の決定に係る職務権限について（指摘）

(対象)

市民福祉部総務課（電子カルテシステム及び医用画像管理システム）

医療センターにおいて、電子カルテシステム及び医用画像管理システムに係る平成26年度の保守契約は、理事長の決定に基づく正式な契約の締結後に、取引業者の都合から、所管課長の決定により再度締結されていた。

当該契約は、年間34,174,872円（税込）の支出を伴う契約であり、医療センターの職務権限規程では、理事長の決定がなければ契約を締結できないことになっている。これについて二重支払等の不利益は認められなかつ

たが、公印が押印された契約書が二度にわたり交付されていたものである。

契約の締結に係る職務権限が遵守されない場合、契約関係に係る対外的な権利及び義務が組織として認められた範囲を逸脱する可能性があり、適切ではない。

したがって、課長決定に基づく契約の締結は適切ではなく、また、公印を適切に管理する観点からも、職務権限規程を遵守する必要がある。

イ 情報システムの情報資産管理状況について

(ア) 概要

豊田市情報セキュリティ基本要綱第26条では、以下のとおり、各所管課等において情報資産を分類の上、情報資産台帳に登録するものとされている。

＜豊田市情報セキュリティ基本要綱（抜粋）＞

（情報資産の分類及び登録）

第26条 セキュリティ管理者は、業務における必要性又はセキュリティ事故等が発生した場合 の影響度に応じ、情報資産の分類基準を共通実施手順に定めるものとする。

- 2 セキュリティ管理者は、情報資産を分類し、登録するための手順を共通実施手順に定めるものとする。
- 3 セキュリティ責任者は、所管する情報資産を適切に管理するため、第1項の分類基準及び前項の手順に従い、所管する情報資産を分類し、情報資産台帳に登録するものとする。

（以下略）

平成26年度までの共通実施手順の「情報資産の分類及び登録手順」では、各所属が導入した情報システムは、情報システム台帳にて管理するよう規定されている。

情報システム課は、情報システム台帳を紙の状態で管理する一方で、新しく情報システム資産管理台帳システムを平成26年度から立ち上げ、情報資産についてはこちらに登録するよう各課に指示をしていた。したがって、調査時点では、管理台帳が二重に存在している状況であった。

また、紙の情報システム台帳を実際に調査したところ、数年前から最新の状態に加除されていない状況であった。

(イ) 手続

情報資産の管理・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

a 情報システムの情報システム台帳への登録状況について（指摘）

（対象）

情報システム課（全般的な内容）

調査対象システムのうち、紙の情報システム台帳が存在していないものをまとめた結果は、以下のとおりである。なお、いずれの情報システムも、平成26年度末においては、情報システム資産管理台帳システムに登録済みであった。

表 3-41 情報システム台帳が存在しない情報システムの一覧

所属名	システム名
市政発信課	豊田市ホームページ管理システム
人事課	人事管理システム
情報システム課	統合型 GIS
情報システム課	「豊田市電子計算機組織」の汎用機系に分類される全てのシステム
情報システム課	「豊田市電子計算機組織」のグループウェアに分類される全てのシステム
情報システム課	「豊田市電子計算機組織」のインターネット・庁内ネットワークに分類される全てのシステム
用地審査課	土地開発基金管理システム
交通安全防犯課	ネットワーク防犯カメラシステム

生涯学習課	とよた科学体験館 プラネタリウム投影システム
防災対策課	災害対策本部システム
防災対策課	映像中継システム
防災対策課	気象情報システム
防災対策課	防災行政無線システム
環境政策課	とよたエコポイントシステム
市民福祉部総務課	電子カルテシステム
市民福祉部総務課	医用画像管理システム
市民福祉部総務課	乙ヶ林診療所コンピューテッドラジオグラフィーシステム
地域福祉課	地域包括支援センターシステム
介護保険課	介護保険指定期間等管理システム
健康政策課	特定健診等データ入力システム
建築相談課	指定道路台帳システム
幹線道路推進課	大気データ処理システム
河川課	工損費用算定システム
経営管理課	公営企業会計システム
学校教育課	学校図書館管理システム

情報資産に係る管理台帳への登録が網羅的でない場合、当該台帳に基づき市が実施する保護措置等の対象に、本来保護すべき情報資産が含まれない可能性がある。

平成27年9月に改定された共通実施手順では、情報システム台帳で行っていた情報資産の管理を、情報システム資産管理台帳で行うよう変更している。

改定前の共通実施手順では、「各所属において導入した情報システム及び当該システムで扱うすべてのデータ」となっていた箇所が、改定後は、「購入、賃貸借、無償貸与、無償譲渡等調達方法の別にかかわらず、各課等において導入した情報システム及び当該システムを構成する情報資産」に変更されている。いずれの共通実施手順においても、市が管理責任及び使用責任を有する全ての情報資産を登録対象とするものである。

そのため、セキュリティ責任者（情報システムに係る各所管課課長）は、各課等において導入した情報資産の全てを情報システム資産管理台帳に登録するとともに、定期的に棚卸しを実施し、適正に管理する必要がある。

また、情報システム課においても、各課等が共通実施手順どおりに情

報資産を登録し、棚卸しを実施しているかどうかについて管理する必要がある。

ウ 稼働中の情報システムの契約書類について

(ア) 概要

市における文書事務に関する必要な事項を定められた文書事務の手引には、以下のとおり定められている。

<文書事務の手引（抜粋）>

第5章第1節11 保存期間

(2) 文書の保存期間の種類と取扱い

文書の保存期間は、文書分類表により標準フォルダごとに定められている。豊田市では、保存期間を法令に特別の定めのあるものを除き、「30年、10年、5年、3年」の4種類に分けている。

また、文書の保存期間は、組織としての最低保存期間を示すものであり、保存継続の必要性の見直しを保存期間満了時点で実施し、廃棄できないものであれば継続保存をすることができる。主管課長は、文書の保存期間基準に定める保存期間を超えて保存する必要があると認める文書等については、文書事務担当課長と協議の上、その必要な期間当該文書等を保存することができる。

（以下略）

※下線は包括外部監査人により記載

上記手引に基づき、各所管課長等は、文書の保存期間満了時に、当該文書の廃棄又は継続保存のいずれかを検討することが求められることとなる。

(イ) 手続

情報システムの調達・運用に係る資料入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

a 契約書類の廃棄について（意見）

（対象）

防災対策課（気象情報システム）

気象情報システムは、平成18年2月から稼働しているものの、当初の導入に係る契約書類が保管されていなかった。これは、契約書類の保存期間とする5年を経過したため、廃棄されたものとされる。

稼働中の情報システムに係る導入時の契約書が保管されていない場合、当該システムに係る契約内容及び権利義務関係が不明となる可能性がある。

また、文書事務の手引に定められる文書の保存期間は、組織としての最低保存期間を示すものとされ、主管課長が必要と判断したものについては、文書事務担当課長と協議の上、保存を継続することができるとされている。

そのため、稼働中の情報システムに係る契約書類については、文書事務担当課長と協議し、保存を継続することが望ましい。

したがって、主管課長である防災担当課長は、今後において、稼働中の情報システムに係る導入時の契約書類等の保存を継続することを検討されたい。

エ 情報システム調達時の契約方法について

（ア）概要

豊田市契約規則第27条においては、以下のとおり、随意契約による場合も見積競争によることが望ましいとされ、コストの低減を図ることが期待されている。

<豊田市契約規則（抜粋）>

（見積書の徴収）

第27条 契約担当者は、随意契約によろうとするときは、なるべく2人以上の者から見積書（様式第3号）又はこれに類する書類を徴さなければならない。ただし、法令によって価格の定められているものその他市長が特に認めたものは、見積書の徴収を省略することができる。

(以下略)

また、情報システムに係るハードウェアの法人税法上の耐用年数は 5 年と定められ、自社利用目的のソフトウェアも同様とされる。そのため、法定耐用年数を超えて使用する可能性はあるものの、情報システムの一般的な更新期間は、5 年程度を目安に検討することが想定されるといえる。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

a 隨意契約によるシステム調達について（意見）

（対象）

交通安全防犯課（ネットワーク防犯カメラシステム）

ネットワーク防犯カメラシステムは、平成 25 年 12 月から稼働し、平成 26 年度における費用は 20,037 千円（税抜）であった。

当該導入に係る契約は、光ファイバーのシステム配線を市内全域に整備している市内で唯一の業者であること、市内にサーバを設置することで少人数による短時間でのデータ等の確認及び取扱いが可能であること、防犯カメラの設置とネットワークの運営が単一であるため、メンテナンス及び障害に対する対応が円滑及び迅速であること等を理由として、随意契約により業者が選定されていた。

しかし、データ等の確認や災害・障害発生時の対応に迅速性等を求めることが、必ずしも市内にサーバを設置する根拠とはならず、市内の業者であることを要件とする必然性に乏しい。

また、交通安全防犯課では、光ファイバーのシステム配線を市内全域に整備している選定業者以外の業者について、費用面、機能面から検討した

ことを示す具体的な記録は残されていなかった。

本来は、このような情報システムの調達においても一般競争入札によるべきであり、業者選定の透明性を確保する必要がある。

そのため、交通安全防犯課は、今後において、情報システム又は情報機器を調達する場合、随意契約を採用する根拠を慎重に吟味した上で、その記録を残すことを検討されたい。

(対象)

水道維持課（上水道地図情報システム）

上水道地図情報システムは、平成 12 年から稼働し、運用業務委託に係る費用は、平成 24 年度が 33,694 千円、平成 25 年度が 29,494 千円、平成 26 年度が 31,193 千円であった。

当該運用業務委託に係る契約は、パッケージソフトのデータ保守であることを理由として、随意契約により業者が選定され、平成 12 年の導入以降、情報システムの更新及び業者の変更について検討された記録は残されていなかった。

長年にわたり同一の業者を随意契約で選定する場合、保守費用等の関連コストが高止まりする可能性がある。そのため、情報システムの調達コストを適正化する観点から、導入後一定期間を経過した情報システムについては、情報システムの更新及び業者の変更の要否を含めて、費用とサービス内容を比較検討する必要がある。

また、情報システムの更新サイクルは 5 年程度とされることが一般的であるため、これに合わせて上記検討を行うことが望ましい。

したがって、水道維持課は、上水道地図情報システムに係る費用とサービス内容を比較し、情報システムの更新及び業者の変更の要否を検討されたい。

(対象)

スポーツ課（豊田市スポーツ施設利用システム）

豊田市スポーツ施設利用システムは、平成 22 年 1 月から稼働し、当該情報システムに係るサービス提供について、平成 21 年度及び平成 26 年度の契約は、随意契約により業者が選定されていた。

随意契約の根拠となる平成 27 年 1 月 16 日付けのメーカー選定理由書では、数社から提案を受けた旨の記載はあるものの、具体的な選定の根拠は

示されておらず、添付資料もなかった。また、情報システム更新時の仕様書にも、比較の根拠となる機能要件は明記されていなかった。

長年にわたり同一の業者を随意契約で選定する場合、保守費用等の関連コストが高止まりする可能性がある。そのため、情報システムの調達コストを適正化する観点から、導入後一定期間を経過した情報システムについては、情報システムの更新及び業者の変更の要否を含めて、費用とサービス内容を比較検討する必要がある。

また、情報システムの更新サイクルは 5 年程度とされることが一般的であるため、これに合わせて上記検討を行うことが望ましい。

したがって、スポーツ課は、豊田市スポーツ施設利用システムに係る費用とサービス内容を比較し、情報システムの更新及び業者の変更の要否を検討したうえで、その記録を残すことを検討されたい。

(対象)

学校教育課（学校図書館管理システム）

学校図書館管理システムに係るサーバ等機器は、外部委託業者が管理しているデータセンターに設置され、平成 27 年度における費用は 11,228 千円（税抜）であった。当該契約は、随意契約により業者が選定されている。しかし、随意契約として業者を選定した際の詳細な検討記録はなかった。

サーバ等機器の設置に係るハウジングサービス契約は、施設、設備、警備体制、機能要件、サービスレベル等の仕様に基づいて選定されるのが一般的であり、提供業者の特殊な技術力を要するものではないと考えられる。

また、地方自治法第 234 条に定められるとおり、契約締結の方法は一般競争入札が原則とされるため、一定の要件を満たさない限り、随意契約によるべきではない。

そのため、ハウジングサービス契約については随意契約とする理由に乏しく、考慮すべき特段の理由がない場合は、一般競争入札により業者を選定する必要がある。

当該契約は、上記のようなハウジングサービス契約に該当するといえるため、学校教育課は、一般競争入札により業者を選定することを検討されたい。また、庁内には、情報システム課が所管する電算室もあるため、サーバ等機器を当該場所に設置することも検討する余地がある。

才 情報システム等の導入及び変更管理について

（ア）概要

情報システムの調達は、いくつかの工程に分けて把握することが可能であり、例えば、「情報システムに係る政府調達の基本指針」（平成19年3月1日各府省情報化統括責任者（CIO）連絡会議決定）では、以下のとおり定められている。

<情報システムに係る政府調達の基本指針（抜粋）>

第2章 全般的事項

II 情報システムに係る工程

情報システムに係る工程を、次のとおりとする。

情報システムに係る工程

工程の名称	工程で行う作業内容
1. 情報システム化計画の策定	「業務・システム最適化指針（ガイドライン）」（平成18年3月31日各府省情報化統括責任者（CIO）連絡会議決定。以下「最適化指針」という。）の「現行体系の作成」、「業務・システムの見直し方針の作成」、「将来体系の作成」及び「最適化計画の作成」に相当する作業をいう。
2. 要件定義等	最適化指針の「仕様書（要件定義書）の作成」に相当する作業及び調達計画書の作成に係る作業をいう。
3. 設計・開発	最適化指針の「設計・開発」に相当する作業をいう。
4. 結合・総合テスト等	最適化指針の「結合・総合テスト等」に相当する作業をいう。
5. 受入テスト	最適化指針の「受入テスト」に相当する作業をいう。
6. 移行	最適化指針の「移行」に相当する作業をいう。
7. 運用	情報システムの運用及び利用者に対する支援を行う。
8. 保守	情報システムの問題発生、改善要求等に対応して、情報システムを修正する作業をいう。

このうち、受入テストは、ユーザとして要求する仕様及び品質を満たしているかどうかの判定を行う工程であり、移行は、開発段階にある情報システムを本番の環境へ移行する工程であると理解され、それぞれについて

適切な管理者による承認が行われるべきものと考えられる。

市における物品契約事務の手引には、物品借入の事務手続として、下記のとおり契約事務のフロー図が定められている。

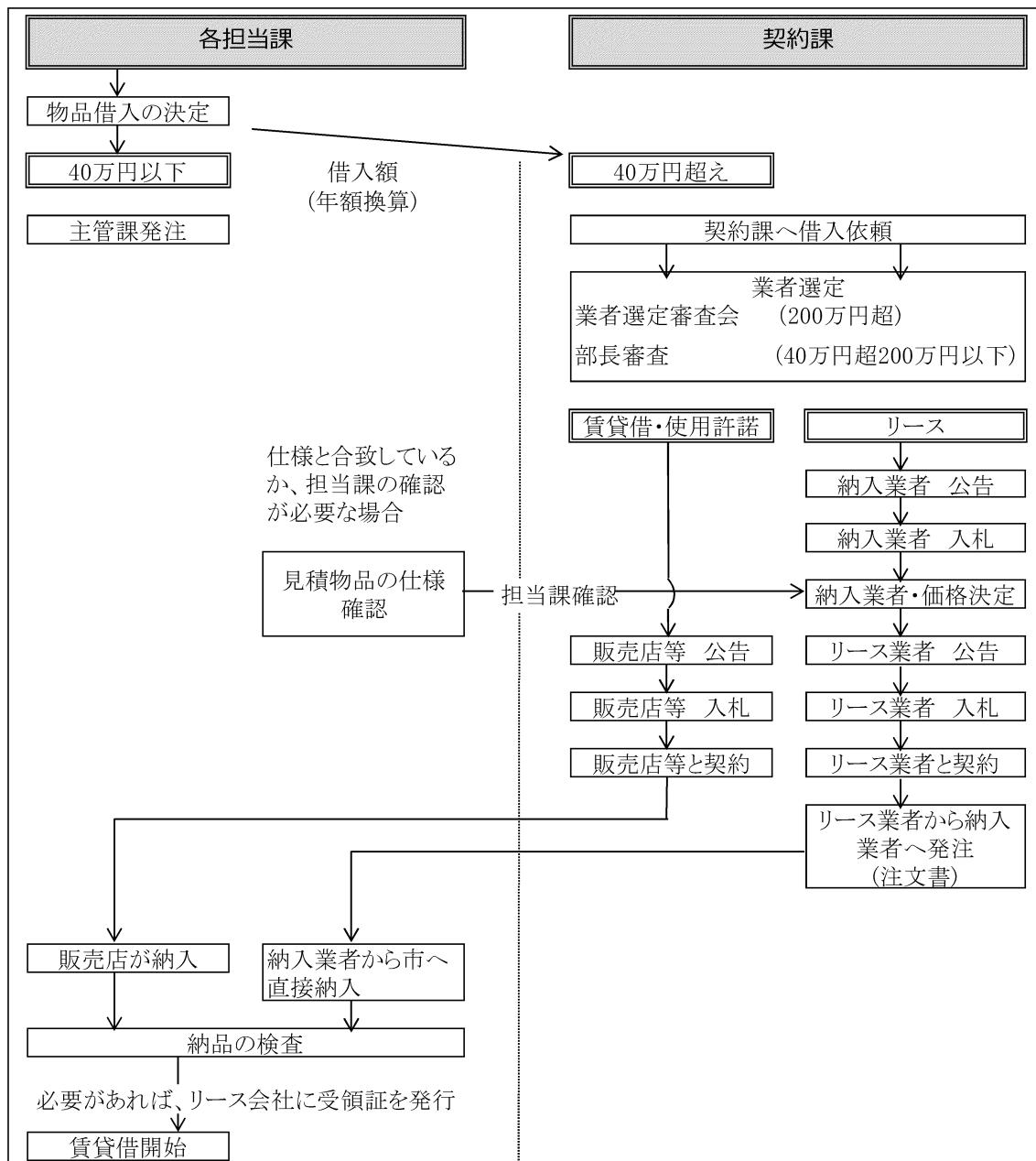


図 3-2 契約事務のフロー図

上記フロー図上では納品された際に検査を行う旨が示されているものの、具体的な手順に係る定めはない。

そのため、市では平成 24 年度から平成 27 年度にかけて以下のようない

報システムの導入又は更新が行われているが、受入テストや本番移行に係る記録等が残されていなかった。

表 3-42 平成 24 年度から平成 27 年度にかけて導入又は更新された情報システム

情報システム名	所管課等	時期	内容
人事管理システム	人事課	平成 25 年 10 月	ソフトウェア、サーバ、プリンタ等機器の更新
土地開発基金管理システム	用地審査課	平成 26 年 12 月	ソフトウェアのバージョンアップ及びプログラム変更
ネットワーク防犯カメラシステム	交通安全防犯課	平成 25 年 12 月	新規導入
住基ネットシステム	市民課	平成 25 年 10 月	ソフトウェア、サーバ、プリンタ、業務端末等機器の更新
特定健診等データ入力システム	健康政策課	平成 27 年 1 月、3 月	ソフトウェアのバージョンアップ及びプログラム変更
検針収納システム	料金課	平成 26 年 9 月	ソフトウェア、ハンディターミナル、プリンタ等機器の更新
図書館システム	図書館	平成 25 年 1 月	ソフトウェアのバージョンアップ及びプログラム変更
学校図書館管理システム	学校教育課	平成 27 年 3 月	ソフトウェア、サーバ、プリンタ、業務端末等機器の更新

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘及び意見を述べることとする。

a 情報システム導入及び更新時のユーザ受入テストの承認について（意見）

（対象）

- 人事課（人事管理システム）
- 用地審査課（土地開発基金管理システム）
- 市民課（住基ネットシステム）
- 健康政策課（特定健診等データ入力システム）
- 交通政策課（バス位置情報提供サービスシステム）
- 料金課（検針収納システム）
- 図書館（図書館システム）
- 学校教育課（学校図書館管理システム）

検針収納システムについては、プログラム変更案件に係る受入テストの記録及び本番移行に係る所管課長等の承認記録が残されていなかった。また、検針収納システム以外の対象システムについては、各システム導入時における受入テストの記録及び本番移行に係る所管課長等の承認記録が残されていなかった。

なお、物品契約事務の手引に定められた契約事務のフロー図には、納品の検査を行う旨が示されているものの、その具体的な手順、書式、承認等については定められていない。

情報システム導入又はプログラム変更に係る受入テスト、本番移行等の各工程において十分な管理が行われない場合、要求する仕様及び品質を満たしているか否かの判定が適切に行われず、情報システム導入又はプログラム変更の品質が不十分となる可能性がある。

また、情報システム導入又はプログラム変更の各工程において実施すべき手順が定められていない場合、管理水準が担当者の能力に依存することとなり、当該水準が一定以上に保たれない可能性がある。加えて、各工程におけるテスト結果や承認記録が残されていない場合、当該意思決定に係る責任の所在が不明確となる可能性がある。

市が定める共通実施手順の情報システム等の導入及び変更管理基準では、セキュリティ責任者は、情報システムの導入又は変更を完了後速やかに情報システム導入・変更完了報告書を対策事務局長である情報システム課長

に提出するものとされ、当該報告書の様式には、稼働テストの結果を記載する欄が設けられている。しかし、ここでの報告は本番移行後に事後的に実施されるものと考えられ、上記のような受入テスト又は本番移行に係る承認とは異なるものといえる。そのため、情報システム導入又はプログラム変更の各工程において実施すべき具体的な手順、書式、承認等について定め、これに基づいて管理を行う必要があると考えられる。

したがって、市は、情報システム導入又はプログラム変更の各工程における具体的な管理手順等を定め、各所管課等において受入テストの記録、本番移行に係る所管課長等の承認記録を残すことを検討されたい。

b システム導入の完了報告について（指摘）

（対象）

交通安全防犯課（ネットワーク防犯カメラシステム）

ネットワーク防犯カメラシステムは、平成25年度の導入に係る情報システム導入・変更完了報告書が作成されておらず、情報システム課長及び総務部長への所定の報告が行われていなかった。

情報システムの導入又は変更に係る完了報告は、共通実施手順の情報システム等の導入及び変更管理基準において、個別実施手順の作成又は改正のきっかけとなるなど、その後の情報資産管理を行う上で必要とされているものである。

したがって、交通安全防犯課は、ネットワーク防犯カメラシステムの導入に係る情報システム・変更完了報告書を対策事務局長である情報システム課長に提出する必要がある。

c プログラム変更の承認について（指摘）

（対象）

用地審査課（土地開発基金管理システム）

健康政策課（特定健診等データ入力システム）

土地開発基金管理システムに係るプログラム変更は頻繁に行われているが、情報システム導入・変更承認願は作成されていなかった。

また、特定健診等データ入力システムは、平成27年度の健診事業の実施に伴うプログラム変更が行われていたものの、情報システム導入・変更承

認願は作成されていなかった。

これらのプログラム変更案件には、情報システムの処理結果に影響を与えない軽微なものであることを理由として、各所管課長への報告記録が残されていないものもあった。

プログラム変更の要件について、セキュリティ責任者の承認を受けない場合、適切かつ十分であることの検証が行われず、本来実施すべき変更が行われない、又は、実施すべきでない変更が行われる可能性がある。

また、共通実施手順の情報システム等の導入及び変更管理基準では、情報システムを変更する場合、セキュリティ責任者は、情報システム導入・変更承認願を作成し、対策事務局長の承認を受けることとされている。プログラム変更は、情報システムの機能を変更することが可能となるものであり、情報システムの変更に当たるものと考えられるため、上記基準に基づき、情報システム導入・変更承認願の作成対象となるものと考えられる。

そのため、所管課長等は、プログラム変更案件について情報システム導入・変更承認願を対策事務局長に提出することが原則といえる。

また、プログラム変更の程度が軽微であり、情報システムの変更に当たらないとして、情報システム導入・変更承認願の提出を省略する場合であっても、その判断はセキュリティ責任者である所管課長等によりなされるべきである。

したがって、用地審査課及び健康政策課の各課長は、土地開発基金管理システム及び特定健診等データ入力システムに係るプログラム変更について、情報システム導入・変更承認願を作成し、情報システム課長の承認を受ける必要がある。また、情報システムの処理結果に影響を与えない軽微なプログラム変更の要件については、少なくとも用地審査課長又は健康政策課長により承認された記録を残す必要がある。

カ 業務の外部委託におけるセキュリティの確保について

(ア) 概要

市では、情報システムの導入、構築及び保守業務を外部に委託する場合がある。この場合、当該委託業務について、受託者と業務委託契約が締結される。契約の締結に当たり、受託者が遵守すべき市の情報セキュリティに係る特記事項を、当該契約書等にその一部として添付している。

また、平成27年度からは、情報セキュリティ上必要な事項がまとめられた遵守項目確認表に基づいて、受託者の情報セキュリティに関する遵守状

況を確認することとしている。

これらの市における外部委託に係る情報セキュリティ対策に関し、必要な事項を定めた豊田市情報セキュリティ基本要綱には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（適用範囲）

第3条 この要綱の適用範囲は、市長、教育委員会（豊田市が設置する小学校、中学校及び特別支援学校（以下「学校」という。）を含む。）、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会、事業管理者、消防長、議会及び豊田市土地開発公社（以下「適用機関」という。）が所管する情報資産（適用機関が、適用機関以外のものに貸与し、もっぱら当該適用機関以外のものの業務を処理するための情報資産を除く。以下同じ。）及び当該情報資産に接するすべての当該適用機関の職員（非常勤特別職員、特別任用職員及び適用機関が外郭団体に派遣した職員並びに学校の教員を含む。以下「職員等」という。）とする。

（中略）

（業務の外部委託業者等）

第30条 セキュリティ責任者は、所管する情報処理施設等の保守又は管理若しくは所管する情報システムの操作、管理、保守又は開発を外部の者に委託する場合は、外部委託を受ける業者及び当該業者の要員が遵守すべき事項を、当該外部委託に係る契約書に明記するものとする。

（以下略）

また、市の所管する各システムに対して、共通して遵守すべき事項又は基準を定めた共通実施手順には、以下のとおり定められている。

<共通実施手順（抜粋）>

業務の外部委託等における情報セキュリティの確保に関する基準

1 趣旨

基本要綱第30条の規定に基づき、業務の外部委託等における情報セキュリティの確保に関する基準を定める。

2 対象

セキュリティ責任者は、次に掲げる内容を伴う業務を外部委託等により

発注する場合は、3に定める基準を満たさなければならない。

ア 情報システムの導入、構築、保守等市が所管する情報システムを設定し、操作し、又は保守する業務

(中略)

3 基準

- (1) 適用機関と適用機関以外の者との間で委託契約書等の契約書類を作成するものについては、情報セキュリティに関する特記(以下「特記」という。)を契約書等にその一部として添付すること。
- (2) 適用機関と適用機関以外の者との間で委託契約書等の契約書類を作成しないものについては、情報セキュリティに関する覚書(以下「覚書」という。)を締結すること。ただし、短期間の簡易な業務で覚書の締結がふさわしくないと当該業務を所管するセキュリティ責任者が認めた場合は、覚書の内容を受託者に提示することにより、覚書の締結を省略できるものとする。
- (3) 受託者が情報セキュリティ上必要な事項を遵守しているかどうかを遵守項目確認表に基づき確認すること。

(中略)

情報セキュリティの確保に関する特記事項

乙の要員(乙自身が要員として業務を行う場合も含む。以下「乙要員」という。)が、この契約による業務(以下「契約業務」という。)に従事するに当たって、甲の情報セキュリティを確保するため、次の事項を遵守しなければならない。

(中略)

(誓約書の提出)

第3 乙は、乙要員に、甲に対して誓約書(別記様式)を提出させなければならない。ただし、甲の判断により業務開始時の提出に代えることができる。

(以下略)

※下線は包括外部監査人により記載

この点について、平成27年9月に改定された豊田市情報セキュリティ基本要綱では、以下のとおり定められている。

<施行：平成27年9月1日 豊田市情報セキュリティ基本要綱（抜粋）>

(外部委託等)

第50条 セキュリティ管理者は、情報システムの操作、構築、管理、保守又は開発を外部の者に委託する場合並びにデータの作成及び加工を外部の者に委託する場合に、データの漏えい、盗難、不正複製、き損及び滅失並びにシステムの停止を防ぐため、外部委託等を受ける事業者及び当該事業者の要員が遵守すべき事項について、外部委託等に関する基準を定める。

(以下略)

なお、平成27年9月に共通実施手順も改定されているが、改定後においては、豊田市情報セキュリティ基本要綱の改定に応じて、根拠となる条項が第30条から第50条に変更されているものの、上記に抜粋した記載内容については変更されていない。

市は、図書館システムの管理運営において、システムと機器の借入に係る賃貸借契約と、図書館システムの保守業務を委託する委託契約を締結している。また、賃貸借契約における「図書館システムに係るシステム及び機器借入仕様書 19 問合わせ支援」の変更にあたり、平成25年6月1日付で覚書が取り交わされている。

変更後の「図書館システムに係るシステム及び機器借入仕様書」の内容は以下のとおりである。

<図書館システムに係るシステム及び機器借入仕様書（抜粋）>

19 問合せ支援

- (1) 毎週火曜日・木曜日・土曜日に豊田市中央図書館に常駐し、電算機器障害・情報システム全般の運用管理業務支援に対応すること。
ただし、平成25年12月28日から平成26年1月3日の間は除く。
ネットワーク障害・機器障害・システム障害の切り分け、その他運用管理支援業務ができる担当者を配置すること。

(以下略)

市は、賃貸借契約に基づき、図書館システムのデータのバックアップ取得状況の確認やバッチ処理のチェック等運用業務を外部業者に委託している。

委託契約では、委託内容として、図書館からのシステム改善要望に対応したプログラム修正、機能追加、システム障害時の対応、月次、年次処理のサポート作業、ファイルの最適化作業及びデータ整備作業が定められている。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

a 外部業者のセキュリティ確保について（指摘）

（対象）

図書館（図書館システム）

図書館システムは、リース会社を経由して調達され、賃貸借契約が締結されている。当該システム導入時の物品借入決定書では、個人情報保護欄及び情報セキュリティ欄が非該当とされていたため、当該契約には、情報セキュリティに関する特記が契約書に添付されていなかった。なお、図書館は、当該契約について情報セキュリティを考慮すべきとの判断に基づき、平成27年4月1日に委託先業者と個人情報の取扱い及び情報セキュリティに関する覚書を締結し、情報セキュリティに関する特記を契約書に添付した場合と同水準の取決めを行った。

しかし、当該覚書に定められる秘密保持に関する誓約書の受領、遵守項目確認表に基づく情報セキュリティに係る状況確認が行われておらず、定期的な報告も受けていなかった。

情報セキュリティ上の必要事項が確認されない場合、外部委託業者における管理が市の要求水準と比較して不十分となり、情報資産が適切に取り扱われない可能性がある。共通実施手順の業務の外部委託等における情報セキュリティの確保に関する基準では、情報システムの導入、構築、保守等市が所管する情報システムを設定し、操作し、又は保守する業務などについて、外部委託先との間で情報セキュリティに係る取決めを行うことを求めている。

具体的には、情報セキュリティに関する特記又は覚書に基づき、受託者

において情報セキュリティ上必要な事項を遵守しているかどうかを遵守項目確認表に基づき確認させるとともに、結果について報告を受けることが定められている。

また、平成 27 年 9 月改定後の共通実施手順においても同様の趣旨に基づく定めがある。以上から、情報システムの保守等に係る委託契約等については、秘密保持に関する誓約書を受領し、情報セキュリティ上必要な事項の遵守を確認させるとともに、定期的な報告を受ける必要があると考えられる。

図書館システムに関する契約は、直接の契約相手がリース会社であるため賃貸借契約であるが、当該契約に係る仕様を定めた図書館システムに係るシステム及び機器借入仕様書では、システム保守が含まれている。そのため、当該契約は、共通実施手順の業務の外部委託等における情報セキュリティの確保に関する基準の適用対象と考えられるため、必要な対応を行うべきである。

すなわち、図書館は、図書館システムの賃貸借契約に係る個人情報の取扱い及び情報セキュリティに関する覚書に基づき、委託先業者から秘密保持に関する誓約書を受領し、遵守項目確認表に基づく確認を行わせるとともに、定期的な報告を受ける必要がある。

キ サポート期間の考慮について

(ア) 概要

情報システムの利用端末として使用されるパソコン類には、オペレーティングシステム（以下「OS」という。）というソフトウェアが搭載され、機器の基本的な管理や制御のための機能が実装されている。

広く使用される代表的な OS として、Microsoft 社が開発する Windows シリーズがある。なかでも、平成 13 年に発表された Windows XP は高い普及率であったため、サポート期間が延長されていたが、平成 26 年 4 月に延長サポートが全て終了することとなった。

市では、平成 25 年 9 月に、Microsoft 社製品 WindowsXP 及び Office2003 のメーカーサポート終了への対応について、以下のとおり方針が定められている。

<Microsoft 社製品 WindowsXP 及び Office2003 のメーカーサポート終了への対応>

1 趣旨

Microsoft 社製品 WindowsXP 及び Office2003 のメーカーサポート終了に伴い、情報セキュリティ確保の観点から、当該製品使用 PC の対応方針を定める。

2 対応方針

Microsoft 社製 OS の内「WindowsXP」もしくはそれ以前の古い OS を使用しているパソコン及び「Microsoft Office2003」もしくはそれ以前の古いOffice ソフトウェアを使用しているパソコンについては、利用形態に応じて以下のとおり対応する。

(1) インターネット接続パソコン

- ・メーカーサポート終了となる平成 26 年 4 月 9 日までに、OS については「Windows7」「Windows8」など、Office ソフトウェアについては「Microsoft Office2007」「Microsoft Office2010」「Microsoft Office2013」などメーカーサポートが存続しているソフトウェアへバージョンアップする

(2) インターネット非接続パソコン

- ・原則として、インターネット接続パソコンと同様に平成 26 年 4 月 9 日までに OS 及び Office ソフトウェアをバージョンアップする
- ・平成 26 年 4 月 9 日までのバージョンアップが困難な場合、使用している OS へのサポートを平成 26 年度中は継続する事が明らかとなっており、インターネット非接続環境でもウィルス定義の更新が可能なウィルス対策ソフトを導入したうえで、平成 27 年 3 月 31 日までに OS 及び Office ソフトウェアをバージョンアップする

3 例外対応

やむをえない事由により 2-(1)-(2) の対応ができない PC については、セキュリティ責任者は当該 PC の継続使用に関し、その理由とウィルス対策等必要な措置を付して、セキュリティ管理者の承認を得るものとする。

制定:平成 25 年 9 月 18 日 施行:平成 25 年 9 月 18 日

また、平成 27 年 9 月に改定された共通実施手順に含まれるソフトウェア

の瑕疵及び不具合対策基準には、以下のとおり定められている。

<ソフトウェアの瑕疵及び不具合対策基準>

1 趣旨

基本要綱第47条の規定に基づき、ソフトウェアの瑕疵及び不具合への対策に関する基準を定める。

2 概要

セキュリティ責任者は、所管する情報システムに使用するソフトウェアについて3に定める基準を満たさなければならない。

3 基準

- (1) メーカー等によりセキュリティパッチの提供、バージョンアップ版の提供等のサポートサービス(以下「サポート」という。)が提供されているソフトウェアを選定し、使用すること。
- (2) 業務に影響のない限り、最新のセキュリティパッチを適用して使用すること。
- (3) メーカー等によるサポートの終了が計画されている場合は、サポートの終了する日までに、サポートが継続して提供されるバージョン又は他製品への移行を行い、サポートが提供されていないソフトウェアを使用しないこと。
- (4) 前項の規定にかかわらず、サポート終了の予告からサポート終了までの期間が1年未満の場合又はサポート終了の予告なしにサポートが終了された場合は、サポート終了後速やかにサポートが継続して提供されるバージョン又は他製品への移行を行うこと。

制定:平成27年8月17日 施行:平成27年9月1日

(イ) 手續

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続(閲覧、突合、分析、質問、観察等)を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

a 情報システム利用端末更新時におけるサポート期間の考慮について（指摘）

（対象）

- 用地審査課（土地開発基金管理システム）
- 健康政策課（特定健診等データ入力システム）
- 経営管理課（公営企業会計システム）
- 予防課（防災学習センター用システム）

対象システムに係る利用端末のOSには、平成26年4月9日にサポートが終了しているWindows XPが使用されていた。当該端末は、いずれも外部ネットワークからは遮断された環境で使用されているものの、サードパーティ製のセキュリティ更新プログラムも適用されていなかった。

なお、当該端末は、監査実施日現在においては、以下のとおり更新されていた。

表 3-43 サポートが終了したOSが利用端末に使用されていたシステム

対象システム	端末の種類	更新時期
土地開発基金管理システム	業務用パソコン	平成26年12月
特定健診等データ入力システム	業務用パソコン	平成26年10月
	専用パソコン	平成27年3月
公営企業会計システム	業務用パソコン	平成27年1月
防災学習センター用システム	専用パソコン	平成27年3月

これは、各所管課において、リース期間内であることを理由に更新されず残されていたためとされる。サポート期間が終了したOSを継続して使用する場合、利用者はサポート期間終了以降に発見された脆弱性を把握することができないため、その脆弱性を利用した攻撃から情報システムを保護することができない。そのため、サポート期間が終了したOSを搭載した利用端末は、常に脆弱性を抱えた状態といえ、マルウェアとよばれるウイルスやコンピュータに被害をもたらすプログラムの感染や攻撃者による侵入に対する防御が十分ではないといえる。

また、このような利用端末を使用する場合、外部ネットワークから遮断されていたとしても、USB メモリ等を媒介してマルウェアに感染する可能性は残される。

Microsoft 社製品 Windows XP 等のメーカーサポートが終了する製品を使用する端末については、メーカーサポートが存続しているソフトウェアへのバージョンアップ等の対応が求められ、例外措置として使用を継続する場合はウイルス対策等の必要な措置を講じた上でセキュリティ管理者の承認を得るものとされていた。

また、平成 27 年 9 月改定後の共通実施手順のソフトウェアの瑕疵及び不具合対策基準には、メーカー等によるサポートの終了が計画されている場合は、サポートの終了する日までに、サポートが継続して提供されるバージョン又は他製品への移行を行い、サポートが提供されていないソフトウェアを使用しないことと定められているため、サポート期間が終了した OS の使用は禁止されているといえる。

そのため、情報セキュリティを確保する観点から、情報システムの利用端末は、OS のサポート期間内に更新すべきであり、サポート終了後には使用すべきではないと考えられる。

したがって、対象システムの各所管課は、リース期間にかかわらず利用端末を OS のサポート期間内に更新する必要がある。また、やむを得ず、利用端末の更新がサポート期間の終了に間に合わなかった場合は、ウイルス対策等の必要な措置を講じた上でセキュリティ管理者である総務部長の承認を得る必要がある。

ク ベータ版ソフトウェアの導入について

(ア) 概要

共通実施手順では、以下のとおり、情報システム導入時に仕様及び情報セキュリティ上の問題点の有無を確認するものとされている。

<共通実施手順（抜粋）>

情報システム等の導入及び変更管理基準

1 趣旨

基本要綱第62条及び第63条の規定に基づき、情報システムの導入及び変更（追加、更新を含む。以下同じ。）の管理に関する基準を定める。

（中略）

4 導入・変更管理

(1) 導入・変更の承認

セキュリティ責任者は、情報システムを導入する場合、又は所管する情報システムを変更する場合は、事前に、(2)に掲げる手続きに従い、次の表に掲げる区分に応じた審議・承認を得なければならない(中略)。

(2) 承認手順

①セキュリティ責任者は、事前に、「情報システム導入・変更承認願」に、次に掲げる事項について記載した文書(様式自由)を添付して、対策事務局長へ提出する。

導入	変更
<ul style="list-style-type: none">・事業の概要及び目的・システムの概要・システム構成図・アプリケーション一覧・取扱データ項目一覧・ネットワーク構築方法 (利用通信回線等)・ウィルス対策・データ保護対策 (入力データ・出力帳票の正確性確保、バックアップ等)・アクセス管理方法 (利用者制限・識別)・設置場所・保守体制・緊急時の対応・予算額及び積算金額(積算書)又は作業人工・導入スケジュール・担当者名	<ul style="list-style-type: none">・変更の内容及び目的・予算額及び積算金額(積算書) 又は 作業人工・変更作業スケジュール・担当者名

なお、「事前に」とは、次に掲げるとおりとする。

	契約課発注案件	契約課へ依頼する前
--	---------	-----------

業者発注分	上下水道局総務課 発注案件	上下水道局総務課が発注する前
	主管課発注案件	発注する前
職員作成分		要件定義完了後でプログラム作成着手前

②対策事務局長は、記載内容をチェックし、個人情報保護条例を始めとした法令、基本要綱及び共通実施手順に反する事項、その他の情報セキュリティ上の問題点の有無を確認する。

③対策事務局長は、記載内容のチェックにより問題点があったときは、セキュリティ責任者に対し改善を求める。

④対策事務局長は、問題点が無い場合は、(1)の区分に従った手続きを行う。

⑤対策事務局長は、セキュリティ管理者の承認を得た場合又は自ら承認した場合は、承認願を提出したセキュリティ責任者に対して、速やかにその旨を回答する。

⑥対策事務局長は、自ら承認した場合は、直近の対策会議に報告する。

(3)完了報告

セキュリティ責任者は、情報システムの導入又は変更を完了した場合は、次に掲げる手続きに従い、セキュリティ管理者に導入又は変更の完了を報告しなければならない。

①セキュリティ責任者は、情報システムの導入又は変更の完了後速やかに「情報システム導入・変更完了報告書」を対策事務局長に提出する。

②対策事務局長は、完了報告書の提出があったときは、記載事項のチェックを行い、直近の対策会議に報告するものとし、この報告によりセキュリティ管理者に報告されたものとする。

(以下略)

しかし、所管課等において、ソフトウェア開発業者の試作版のソフトウェア（以下「ベータ版」という。）が無償で提供された場合は、支出に係る決裁が不要なため、上記のような確認を経ずに利用することができる気になる。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

（ウ）監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

a ベータ版ソフトウェアの導入について（指摘）

（対象）

河川課（工損費用算定システム）

工損費用算定システムは、ソフトウェア開発会社から無償で提供されたベータ版であるため、調達に係る手續が行われていなかった。これは、従来、外部委託していた工損費用算定業務を河川課で引き継いだ際に、委託業者から当該システムの紹介を受け、これを使用するに至ったものである。

ベータ版は、製品版を作成することを目的とした試作版としての性格を有し、その処理結果は開発業者によって保証されていない。このような性格を有するベータ版を市の業務に供することは不適切である。

また、職員がベータ版の操作方法に習熟していることを理由として、随意契約により当該システムの製品版を選定することも考えられるため、調達の透明性を確保する観点からも適切ではない。

市の業務に供する情報システムについてはベータ版を使用せず、適切な契約手続に従い製品版のソフトウェアを調達する必要がある。

したがって、河川課は、工損費用算定システムのベータ版を中止し、市の規程等に従い製品版の情報システムを導入すべきである。

（2）情報システムの調達・運用に係る経済性・効率性・有効性について

ア 随意契約の対象範囲について

（ア）概要

情報システムに係る費用には、保守費用や関連するソフトウェアのライセンス使用料等のように、使用する期間を通じて継続的に発生するものが含まれている。

このような費用を伴う契約については、ソフトウェアのソースプログラム、著作権又は開発環境を保有していることから、導入時の外部委託業者を随意契約により選定する場合が少なくない。

しかし、地方自治法第 234 条においては以下のとおり規定され、原則的な契約方法は一般競争入札とされている。

<地方自治法（抜粋）>

（契約の締結）

第 234 条 売買、貸借、請負その他の契約は、一般競争入札、指名競争入札、随意契約又はせり売りの方法により締結するものとする。

2 前項の指名競争入札、随意契約又はせり売りは、政令で定める場合に該当するときに限り、これによることができる。

（以下略）

したがって、調達の競争性、透明性を確保し、コストの合理化を図るとともに、より良いサービスを求める観点から、随意契約とする範囲は最低限とすべきであると考えられる。

情報システムの調達においても、特定の業者に委託する必然性のないものについては一般競争入札により調達すべきであり、やむを得ず随意契約とする場合は、できる限り契約単位を分離して、その範囲を最低限とすることが求められる。

例えば、「情報システムに係る政府調達の基本指針」（平成 19 年 3 月 1 日各府省情報化統括責任者（CIO）連絡会議決定）では、大規模なプロジェクトを一括調達することなく、適切な規模に分離して調達することにより、事業者への競争参加機会の拡充を図り、また、複数の事業者の参入により競争性が高まることによるコストの低減を図る趣旨から、情報システムの機能ごとの分離調達、ハードウェアとソフトウェアの分離調達、設計・開発から移行までの工程、運用の工程及び保守の工程の分離調達等が推奨されている。

<情報システムに係る政府調達の基本指針（抜粋）>

第3章 調達プロセスに係る指針

I 企画

1. 調達計画書の作成

(2) 調達計画書に記載すべき内容

②設計・開発の工程における分離調達の内容

大規模なプロジェクトを一括調達することなく、プロジェクトを適切な規模に分離して調達（分離調達）することにより、事業者への競争参加機会の拡充が図られ、また、複数の事業者の参入により競争性が高まることによってコストの低減が期待される。

このため、調達担当課室は、特定情報システムの設計・開発の工程については、情報システムの方式の検討結果を踏まえて、原則として、共通基盤システム、各個別機能システムの単位で分離調達を行う。

なお、①(i)の情報システムの方式を採用した場合において、設計・開発に先立って当該情報システム全体の設計に係る基本的事項の整理を行う必要がある場合は、共通基盤システムの設計・開発の調達を先行して実施し、当該事業者において基本的事項の整理を行う。個別機能システムの設計・開発に係る調達は、当該基本的事項を明らかにした上で実施する。

調達計画書には、それらの内容を記載する。

③ハードウェアとソフトウェアとの分離調達の内容

調達担当課室は、特定情報システムについては、原則として、ハードウェア(OS等のハードウェアと不可分な既製のソフトウェアを含む。)とソフトウェア(設計・開発を行うソフトウェアに限る。)とは分離して調達することとし、その内容を調達計画書に記載する。

④設計・開発から移行までの工程、運用の工程及び保守の工程の分離調達の内容

運用及び保守の工程について、随意契約によるものが9割以上にも上り、競争性が確保されているとは言い難い状況を踏まえ、特定情報システムについては、調達担当課室は、設計・開発から移行まで(以下「設計・開発等」という。)の工程、運用の工程、保守の工程は、原則として、それぞれ一般競争入札により分離して調達することとし、その内容を調達計画書に記載する。なお、構築する情報システムに係るコスト全体の評価を行う観点から、設計・開発等の工程の調達に際しては、将来

の運用及び保守の工程を含めたライフサイクルコストに基づく技術評価を行うことが望ましい。

(以下略)

当該基本指針は、地方自治体に直接適用されるものではないが、同様の趣旨により、契約単位はできる限り分離することが望ましい。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

a システム調達における契約単位の区分について（意見）

（対象）

情報システム課（グループウェア）

平成 26 年度において、情報システム課は、グループウェアとウイルス対策ソフト等のライセンス契約を一括して契約していた。当該契約は、必要となる権利等を有する者が他にいないことを理由として、随意契約により業者が選定されていた。なお、見積書に添付されていた明細によれば、ライセンス使用料のうち、当該業者が開発・販売している製品に係るものは 15,748 千円、それ以外に係るものは 4,221 千円であった。

当該契約の対象のうち、グループウェア、DBMS 等は、当該業者が開発・販売している製品であるため、これらに係るライセンス使用料の支払について、上記随意契約の理由は合致する。しかし、ウイルス対策ソフト等は別の業者が開発を行い、販売代理店も複数存在するため、これらの契約単位を一括し、随意契約により業者を選定することについては、その合理性に問題があるといえる。

随意契約による場合、簡略な手続により、事務作業や経費の負担が少な

いといった点で有利である。しかし、市が利用している既存のサービス提供業者に対し、他のサービスを随意契約としてまとめて発注した場合、特定の業者への依存度が高まるとともに、その他の業者の参入を阻害する可能性がある。また、発注者にとって、より良質で低廉な情報システム関連サービスを受ける機会を逸してしまう可能性がある。

ソフトウェアのライセンス使用料のうち、市が要求する仕様が市販される一般的な製品で対応できる場合は、提供する業者の技術力、経験等を考慮する必要性が低く、地方自治法第 234 条において原則的な契約方法とされる一般競争入札による調達に馴染むと考えられる。

そのため、情報システムの調達に当たっては、属性の異なるソフトウェアのライセンスについては契約単位を分離し、それらのうち複数業者が提供可能なものについては、随意契約によらず、一般競争入札により業者を選定すべきである。

したがって、情報システム課は、調達コストの合理化を図る観点から、当該契約の対象のうち、ウイルス対策ソフト等に係るライセンスについてはグループウェア等と分離する等、随意契約とする範囲の見直しを検討されたい。

(対象)

資産税課（固定資産地図情報システム）

平成 26 年度において、資産税課は、固定資産地図情報システムに係る保守作業、地形データ更新作業、課税検証図面出力作業等を一括して契約していた。当該契約は、当該システムを導入した業者しか作業できないこと、及び市の仕様により独自プログラムを附加しており、その改定・更新は当該業者以外の作業が困難であることを理由として、随意契約により業者が選定されていた。なお、平成 26 年度における費用は 60,900 千円（税抜）であった。

当該契約の対象のうち、業務システムの保守作業等は、当該業者が開発・販売している製品であり、市の要望に基づきカスタマイズを行ってきたノウハウもあることから、上記随意契約の理由に合致する。

しかし、地形データ更新作業及び課税検証図面出力作業については、当該情報システムの導入業者以外でも作業できるため、上記随意契約の理由に合致せず、一般競争入札での調達が可能と考えられる。

したがって、資産税課は、調達コストの合理化を図る観点から、当該契約の対象のうち、業務システムの保守作業等とそれ以外を分離する等、隨

意契約とする範囲の見直しを検討されたい。

イ 調達コストの適正化について

(ア) 概要

情報システムに係る費用として、設計、開発、データ移行、機器設置等のイニシャルコスト、アプリケーションソフトウェア保守、機器保守及び機器（賃貸借の場合）等の稼動後に発生するランニングコストが挙げられる。このようなシステムの構築開始から利用終了までのコストの全体を、ライフサイクルコストという。

アプリケーションソフトウェア保守及び機器保守に係る費用がランニングコストに含まれていない場合、当該システムのライフサイクルコストに係る正確な費用の把握ができず、コスト低減の考慮時において、誤ったライフサイクルコストを算出してしまう可能性がある。

また、入札時において、アプリケーションソフトウェア保守及び機器保守に係る費用が含まれていない場合、入札後の保守契約の締結を前提に、意図的に入札金額を下げるなど、契約の公平性、透明性及び客観性が確保されない可能性がある。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

a 調達コストの適正化（意見）

（対象）

防災対策課（災害対策本部システム）

平成 27 年 4 月に導入された災害対策本部システムには、映像中継装置等の購入（2 台）が含まれ、一般競争入札により業者が選定されていた。その後、平成 27 年 6 月に、映像中継装置等が 5 台（7,776 千円）追加購入され、他の業者が映像中継装置を増設した場合、一元的な保守管理ができないこと等を理由として、当初の導入に係る業者が随意契約により選定されていた。

これらの映像中継装置等は、いずれもメーカー保証期間中であったため、当該装置に係る保守契約は、平成 28 年度に上記導入業者と随意契約により締結することが検討され、それぞれの購入時の契約対象には含まれていなかつた。

情報システム又は情報機器の調達に係る費用は、初期導入時にのみ発生するものではなく、導入後の保守作業についても発生するため、そのライフサイクルを通じた全体的な調達コストの適正化を考慮する必要があると考えられる。

また、機器の追加購入を行う場合も、原則的な契約方法は一般競争入札によるべきであり、随意契約による場合の理由については慎重に検討すべきである。

したがって、防災対策課は、今後において、情報システム又は情報機器を調達する場合、初期導入費用だけでなく保守費用も含めて価格を比較し、業者を選定することを検討されたい。また、追加購入を行う場合も、調達コストの適正化を図る観点から、随意契約によらず、一般競争入札によることを検討されたい。

（対象）

市民福祉部総務課（乙ヶ林診療所コンピューテッドラジオグラフィーシステム）

市民課（住基ネットシステム）

乙ヶ林診療所コンピューテッドラジオグラフィーシステムは、平成 27 年 3 月から稼働し、導入費用は 12,450 千円（税抜）であった。また、住基ネットシステムに係るハードウェアは、平成 25 年 10 月から賃借し、平成 26 年度の費用は 1,262 千円であった。

これらの情報システム及び情報機器は、いずれもメーカー保証期間中であったため、保守契約は当初の一般競争入札の対象には含まれていなかつた。

情報システム又は情報機器の調達に係る費用は、初期導入時にのみ発生

するものではなく、導入後の保守作業についても発生するため、そのライフサイクルを通じた全体的な調達コストの適正化を考慮する必要があると考えられる。

したがって、市民福祉部総務課及び市民課は、今後において、情報システム又は情報機器を調達する場合、初期導入費用だけでなく保守費用も含めて価格を比較し、業者を選定することを検討されたい。

ウ 市が保管するデータのホームページによる一般公開の状況について

(ア) 概要

沿道環境が環境保全目標（環境基準を準用する。）を達成及び維持するために定められた豊田市若園地区における第二東名高速道路と県道名古屋岡崎線の沿道環境保全に関する協定書には、以下のとおり定められている。

<豊田市若園地区における第二東名高速道路と県道名古屋岡崎線の沿道環境保全に関する協定書（抜粋）>

(目的)

第1条 第二東名と県道の併用後、沿道環境が環境保全目標を達成及び維持するため、大気・騒音等の必要項目の測定（以下、「環境測定」という。）及びその測定値が第二東名と県道に起因して環境保全目標を達成できない。と認められる場合に実施する沿道環境の保全対策（以下、「環境保全対策」という。）について定める。

(環境測定及び環境保全対策の実施者)

第2条 第二東名と県道の環境測定設備（以下、「常時測定局」という。）における測定は、市が行うものとする。

（中略）

(環境測定)

第3条

（中略）

5. 常時測定局の測定項目については、市が管理するホームページで測定された一時間平均値（速報値）を一般公開するものとする。

（以下略）

※下線は包括外部監査人により記載

当該協定書の定めを受けて、市は、大気、気象及び騒音測定結果（時間値）のデータをホームページ上で公開している。

しかし、当該データ閲覧のための推奨環境の一部に係るサポート期間は、平成 27 年 4 月 30 日に終了していた。

(イ) 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

(ウ) 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

a 大気データ閲覧における推奨環境について（指摘）

（対象）

幹線道路推進課（大気データ処理システム）

大気データ処理システムは、市民に大気測定結果のデータを公開するためのシステムである。

所管課に設置されたインターネット接続端末から当該データの閲覧を試みたところ、エラーメッセージが表示され、当該データを閲覧することができなかった。その原因は、当該システムの閲覧には、端末側に特定のソフトウェアが必要であるものの、上記端末では当該ソフトウェアが既にアップグレードされていたことから、有効に機能しなかったためである。なお、当該ソフトウェアのサポート期間は、平成 27 年 4 月 30 日に終了している。

市民への情報提供を目的とする情報システムを利用するため必要なソフトウェアのサポート期間が終了している場合、一般には情報セキュリティ上の問題を回避するためにアップグレードされていることが見込まれるため、市民が当該サービスを享受する機会は制限されていると考えられる。このような情報システムをあえて利用するために、サポートが終了しているソフトウェアへダウングレードした場合、市民は情報セキュリティ上の

リスクを負うことになる。

また、平成 27 年 9 月改定後の共通実施手順のソフトウェアの瑕疵及び不具合対策基準では、メーカー等によるサポートの終了が計画されている場合は、サポートの終了する日までに、サポートが継続して提供されるバージョン又は他製品への移行を行い、サポートが提供されていないソフトウェアを使用しないことと定められているため、サポート期間が終了したソフトウェアを前提とする情報システムの使用環境は改善されるべきであると考えられる。

そのため、情報システムの使用環境にサポート期間が終了したソフトウェアが含まれる場合、所管課はサポートが継続して提供されるバージョン又は他製品への移行を速やかに行う必要がある。

したがって、幹線道路推進課は、市民へのサービスを充実させる観点から、大気データシステムについて改修を行うべきである。

(3) 情報システムの運用に係る安全性について

ア セキュリティ関連の書類管理等について

(ア) 個別実施手順について

a 概要

市では、豊田市情報セキュリティ基本要綱及び共通実施手順において、個別の情報資産に関し遵守すべき具体的な措置等の事項を個別実施手順に定めることとする条項が複数存在する。

また、豊田市情報セキュリティ基本要綱では、情報資産の定義及び個別実施手順を定める者について、以下のとおり定めている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（定義）

第2条 この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（中略）

（5）情報システム 電子計算機、端末装置及び記録媒体、情報を伝送するための機器及び電気通信回線並びにこれらの用に供するプログラム等からなるシステムをいう。

(中略)

(7) 情報資産 情報処理施設等、情報処理装置、情報システム及び情報システムで扱う全てのデータをいう。

(中略)

(9) データ 電子計算機で扱うことができる形にした文字、数値、記号、音声、静止画、動画等をいう。

(中略)

(情報セキュリティ責任者)

第10条 課又はそれに相当する組織（以下「課等」という。）が所管する情報資産に関する情報セキュリティ対策を適切に実施し、維持するため、情報セキュリティ責任者（以下「セキュリティ責任者」という。）を置く。

(中略)

3 セキュリティ責任者は、課等の長をもって充てる。

(中略)

(個別実施手順)

第 20 条 個別実施手順は、基本要綱及び共通実施手順に基づき、個別の情報資産に関し遵守すべき事項を定める文書とする。

2 個別実施手順は、情報資産を所管するセキュリティ責任者が、対策会議の意見を聴いて策定し、セキュリティ管理者が承認する。

3 前項の規定に関わらず、個別実施手順の字句の修正等の軽微な改正に当たっては、対策会議からの意見聴取を省略し、又はセキュリティ管理者に代わって対策事務局長が承認できるものとする。

(以下略)

また、下表は、豊田市情報セキュリティ基本要綱において、個別実施手順に定めるべきとされる条項をまとめたものである。

表 3-44 個別実施手順に定めるべきとされる項目

個別実施手順条文	内容	関連する共通実施手順
第 28 条 (研修)	研修の種類、対象者、実施方法等を定める研修計画	該当なし
第 29 条(第三者のアクセスに対する保護)	第三者が情報処理施設等へアクセスする場合の、当該アクセスに係る情報セキュリティを	該当なし

	確保するために講ずべき必要な措置	
第 31 条(情報処理装置の保護)	災害等環境上の脅威、許可されない物理的アクセス、電源異常又は通信ケーブル等の配線の損傷等から情報処理装置を守るための、所管する情報処理装置について講ずべき必要な措置	・情報処理装置保護基準
第 37 条(管理区画の保護)	管理区画内の情報資産に対する災害等環境上の脅威、許可されない物理的アクセス、電源異常又は通信ケーブル等の配線の損傷等から守るための、所管する管理区画について講ずべき必要な措置	・特別保護情報資産及び管理区画の指定
第 38 条 (入退管理)	職員等及び第三者の管理区画への入退の管理方法等	・特別保護情報資産及び管理区画の指定
第 39 条(管理区画内作業の管理)	職員等が管理区画内で行う作業に関して講ずべき措置	・特別保護情報資産及び管理区画の指定
第 40 条 (受渡場所)	情報処理に係る物品の受渡場所について、当該物品の盗難、改ざん等を防止するための講ずべき措置	該当なし
第 42 条(アクセス許可基準)	業務上及び情報セキュリティ上の必要に応じ、所管する情報資産に係るアクセス許可基準	該当なし
第 48 条(アクセス制御措置)	所管する情報システムのネットワーク、オペレーティングシステム、アプリケーションソフトウェアについて、業務上必要なアクセス制御措置	・インターネット接続に係るセキュリティ対策基準 ・リモートメンテナンスに関する基準
第 50 条(情報処理施設等の作業の監視)	所管する情報処理施設等における職員等及び第三者の作業等を監視するための手順	該当なし

第 51 条(携帯型電子計算機等によるアクセスに係る保護)	職員等が携帯型電子計算機等を利用し、重要な情報システムへアクセスする場合、又は職員等に対し遠隔地からのコンピュータ操作を許可する場合の、不正アクセス等を防止するために講ずべき措置	該当なし
第 68 条(ネットワークの保護)	ネットワークへの不正アクセスの防止又はネットワークにより送信されるデータの機密性を守るために、所管するネットワークについて講ずべき必要な措置	<ul style="list-style-type: none"> ・インターネット接続に係るセキュリティ対策基準 ・ネットワーク保護基準
第 72 条(データ等の移送時の保護)	データ等を他の機関又は事業者へ移送する場合の盗難、損傷等を防止するための、データ等の移送時に講ずべき措置	該当なし
第 75 条(ホームページの保護)	ホームページに掲載された情報が、故意又は不注意な操作により改ざん又は削除をされたための措置	<ul style="list-style-type: none"> ・ホームページによる情報の公開基準
第 76 条(コンピュータウィルス対策)	所管する情報システムをコンピュータウィルス等不正なソフトウェアから保護するために必要な措置	<ul style="list-style-type: none"> ・コンピュータウィルス対策基準
第 77 条(一般開放インターネットパソコンの保護)	所管する公共施設等に一般開放インターネットパソコンを設置する場合は、当該一般開放インターネットパソコンを不正利用等から保護するための必要な措置	<ul style="list-style-type: none"> ・一般開放インターネットパソコン保護基準

これに対し、平成 27 年 9 月に改定された豊田市情報セキュリティ基本要綱及び共通実施手順では、以下のとおり定められている。

<施行：平成27年9月1日 豊田市情報セキュリティ基本要綱（抜粋）>

（個別実施手順）

- 第24条 個別実施手順は、基本要綱及び共通実施手順に基づき、個別の情報システムに関し遵守すべき事項を定める文書とする。
- 2 セキュリティ管理者は、個別実施手順の策定及び管理に関する手順を定める。
 - 3 個別実施手順は、前項の規定による手順により、情報システムを所管するセキュリティ責任者が策定し、対策事務局長の承認を得るものとする。
 - 4 前項の規定にかかわらず、個別実施手順の用語の整理その他の軽微な改正に当たっては、対策事務局長の承認を省略し決定できるものとし、改正後速やかに対策事務局長に報告するものとする。

（以下略）

<施行：平成27年9月1日 共通実施手順（抜粋）>

個別実施手順策定・管理手順

1 趣旨

基本要綱第24条第2項の規定に基づき、個別実施手順の策定及び管理に関する手順を定める。

2 策定対象

個別実施手順は、次の各号のいずれかに該当する情報システムについて策定する。

- (1) 機密性重要度3に分類される情報システム
- (2) 完全性重要度2に分類される情報システム
- (3) 可用性重要度2に分類される情報システム

（以下略）

従来、個別実施手順の策定対象は、導入された全ての情報システムとされていたが、上記の改定に伴い、情報システムに係る重要度の分類に応じて策定するよう変更された。

b 手続

情報システムの調達・運用に係る資料入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事

務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 個別実施手順の策定について（指摘）

（対象）

- 市政発信課（豊田市ホームページ管理システム）
- 人事課（人事管理システム）
- 契約課（契約管理システム）
- 用地審査課（土地開発基金管理システム）
- 資産税課（固定資産地図情報システム）
- 交通安全防犯課（ネットワーク防犯カメラシステム）
- 環境政策課（とよたエコポイントシステム）
- 市民福祉部総務課（乙ヶ林診療所コンピューテッドラジオグラフィーシステム）
- 地域福祉課（地域包括支援センターシステム）
- 介護保険課（介護保険指定期間等管理システム）
- 健康政策課（特定健診等データ入力システム）
- 交通政策課（バス位置情報提供サービスシステム）
- 建築相談課（指定道路台帳システム）
- 幹線道路推進課（大気データ処理システム）
- 河川課（工損費用算定システム）
- 料金課（検針収納システム）
- 水道整備課（水道管網解析システム）
- 水道維持課（上水道地図情報システム）
- 下水道施設課（下水道地図情報・排水設備情報ファーリングシステム）
- スポーツ課（豊田市スポーツ施設利用システム）
- 図書館（図書館システム）
- 学校教育課（学校図書館管理システム）
- 予防課（防災学習センター用システム）

料金課（検針収納システム）を除いた上記対象システムについて、個別

実施手順が策定されていなかった。また、料金課では、検針収納システムについて個別実施手順は作成されていたものの、検針収納システムの更新に伴う修正が行われていなかった。

豊田市情報セキュリティ基本要綱第20条では、情報セキュリティ対策について、個別の情報資産に関し遵守すべき事項を個別実施手順として定めるものとしている。これは、平成27年9月に改定された基本要綱第24条においても同様の趣旨とされる。

平成26年度中においては、各情報システムについて必須とされていた個別実施手順の策定が不十分な状況にあり、市が実施すべき情報セキュリティ対策について適切に整備されていなかった。平成27年9月に改定された共通実施手順の個別実施手順策定・管理手順では、各情報システムの重要度に応じて個別実施手順を策定するものとしている。

そのため、情報システムの重要度を明確にし、必要に応じて個別実施手順を策定すべきである。

(イ) インターネットの利用について

a 概要

市では、インターネットを情報発信や情報収集を廉価に効率良く実現する手段として利用を促進している。一方で、インターネットは悪意ある集団や個人も利用しており、マルウェア、迷惑メール等の様々なリスクがあることを念頭に活用する必要がある。

市では、所管する情報資産、情報システム、ネットワーク等をこれらのリスクから保護するため、職員が情報システムを利用して業務を行うための府内ネットワークと、インターネット等の外部へ接続されるネットワークの2種類を分離して構築し、業務を行うための府内ネットワークが外部から侵入攻撃されないよう対策を講じている。

インターネット等の外部に接続されるパソコンの安全性を管理する方法として、インターネットへの接続状況や接続内容を監視・制限する方法があり、現在では多くの企業でも実施されている。

基本要綱第27条では、以下のとおり、安全確保と適切利用の2つの目的を持って、インターネットパソコンに対する管理・制限について定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（職員等の責務）

第27条 職員等は、セキュリティ文書に定められた事項を遵守する義務を負うとともに、その役割と責任において、協力して豊田市全体の情報セキュリティの確保に努めなければならない。

- 2 職員等は、豊田市が保有する情報資産を、職務の遂行以外に使用してはならない。

（以下略）

これに基づき、インターネット利用の監視及び業務処理を行うパソコンについて共通して遵守すべき事項を定めた共通実施手順のインターネット利用の監視等に関する基準には、以下のとおり定められている。

<共通実施手順（抜粋）>

業務用パソコン以外のパソコンでの業務処理の禁止

（中略）

2 業務用パソコン以外のパソコンでの業務処理の禁止

- (1) 職員等は、業務用として貸与されたパソコン以外のパソコンで業務処理を行ってはならない。
(2) 職員等は、インターネットに接続されたパソコンでは、絶対に業務処理を行ってはならない。

（中略）

4 やむを得ずインターネットに接続されたパソコンで業務処理を行う場合の手続き等

- (1) 2(2)の規定に関わらず、やむを得ずインターネットに接続されたパソコンで業務処理を行う場合、セキュリティ責任者は事前に、様式「インターネットパソコン利用承認書」を対策事務局長に提出する。
(2) 対策事務局長は、記載内容をチェックし、個人情報保護条例を始めとした法令、基本要綱及び共通実施手順に反する事項、その他の情報セキュリティ上の問題点の有無を確認する。
(3) 対策事務局長は、記載内容のチェックにより問題点があったときは、セキュリティ責任者に対し改善を求める。
(4) 問題点がない場合は、対策会議の意見を聞いてセキュリティ管理者が承認する。

(以下略)

※下線は包括外部監査人により記載

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) インターネットに接続されたパソコンによる業務処理の承認について（指摘）

（対象）

介護保険課（介護保険指定期間等管理システム）
スポーツ課（豊田市スポーツ施設利用システム）

介護保険課及びスポーツ課は、インターネットに接続されたパソコンで各業務システムを利用していた。しかし、介護保険課及びスポーツ課は、情報システム課長にインターネットパソコン利用承認書を提出しておらず、インターネットに接続されたパソコンで業務システムを利用するについて、情報セキュリティ管理責任者である総務部長の承認を受けていなかった。

その原因は、共通実施手順の業務用パソコン以外のパソコンでの業務処理の禁止に定められている手順が周知されていなかったためである。

市では、インターネットに接続されたパソコンで業務処理を行うことは、盗聴や改ざんの危険があるため原則として禁止されており、やむを得ずインターネットに接続されたパソコンで業務処理を行う場合は、インターネットパソコン利用承認書を対策事務局長に提出し、情報セキュリティ上の問題点の有無を確認した上で、セキュリティ管理者により使用が許可されるという手順が定められていた。

平成27年9月の改定後の共通実施手順においては、業務用パソコン以外

のパソコンでの業務処理の禁止に係る定めが削除され、ルール上は問題がないとも考えられる。しかし、改定後の共通実施手順では、インターネット接続に関する基準において情報セキュリティ対策を定め、データ保管基準において保管するデータの重要度に応じてインターネットへの接続を禁止している。

そのため、インターネットに接続されたパソコンで業務システムを利用する場合、改定後の共通実施手順に沿った情報セキュリティ対策が講じられていること及び保管するデータの重要度が市として許容し得る程度であることを確かめる必要がある。

したがって、介護保険課及びスポーツ課では、インターネットに接続されたパソコンに係る情報セキュリティ対策及び保管するデータの重要度を確かめた上で、情報セキュリティ上の問題点の有無を確認する必要がある。

(ウ) 障害報告について

a 概要

豊田市情報セキュリティ基本要綱第78条には、以下のとおり、情報システムの故障、不正確な処理等の不具合に対応する旨が定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（情報セキュリティ事故等への対応）

第78条 職員等は、情報システムの故障、不正確な処理、情報の漏洩、改ざん等の情報セキュリティに係る事故又はソフトウェアの誤動作（以下「セキュリティ事故等」という。）を発見した場合は、直ちにセキュリティ責任者に報告するものとする。

- 2 セキュリティ責任者は、セキュリティ事故等が発生した場合又は発生する恐れがある場合は、次条の規定に基づく緊急対応計画に従い、当該セキュリティ事故等への対応を行うものとする。
- 3 セキュリティ責任者は、セキュリティ事故等の原因を究明し、再発防止策を講じなければならない。
- 4 セキュリティ責任者は、セキュリティ事故等について、セキュリティ管理者に報告するものとする。

（以下略）

このうち、共通実施手順のセキュリティ事故等報告手順では、重大なセ

セキュリティ事故等が発生した場合の報告手順について、以下のとおり定められている。

<共通実施手順（抜粋）>

セキュリティ事故等報告手順

- 1 趣旨 基本要綱第78条第4項の規定に基づき、情報システムの故障、不正確な処理、情報の漏洩、改ざん等の情報セキュリティに係る事故又はソフトウェアの誤動作（以下「セキュリティ事故等」という。）があつた場合の報告の手順を定める。
 - 2 報告手続き
 - (1) セキュリティ責任者は、所管する情報資産に重大なセキュリティ事故等が発生した場合は、速やかに部門管理者に報告し、合わせて対策事務局長に報告しなければならない。
 - (2) セキュリティ責任者は、次に掲げる事故等が発生した場合は、当該事故等が収束した後速やかに、様式「情報セキュリティ事故等報告書」によりセキュリティ管理者に報告しなければならない。
 - ・市民に影響を与えたもの又は与える可能性があったもの
 - ・市の事務処理に広範囲の影響を与えたもの又は与える可能性があったもの
 - ・収束に1人日以上の人工又は5万円以上の経費がかかったもの
 - (3) セキュリティ責任者は、事故等の収束に時間がかかると予想される場合は、必要に応じて中間報告をしなければならない。
（中略）
 - (5) セキュリティ管理者は、事故等報告書の提出があったときは、当該事故等の原因等を分析し、必要に応じてセキュリティ文書の見直し、職員等への注意の喚起等を行わなければならない。
- （以下略）

また、市では「事務ミス発生時の対応ルール」として、事務処理のミス発生時に、その影響度に応じた報告手順が定められている。

<事務ミス発生時の対応ルール（抜粋）>

原則として、事務ミスの影響度によって初期情報共有、原因分析・対策立

案・公表、事後の情報共有・再発防止への対応の区分を分け、影響度が高いものは原則公表するとともに事務改善委員会に報告し、再発防止を徹底することとします。

レベル1 市民への影響がなく、他課への影響や市に金銭的被害がないもの

(1) 初期情報共有

- ・口頭又はメモにより、事務ミスの概要を副課長まで報告する。

(2) 原因分析・対策立案・公表

- ・事務ミスが発生した業務の担当長が事務ミス事案の原因分析及び対策を検討した上で副課長へ報告する（口頭可）。

- ・危機管理担当、議会への報告なし

- ・公表なし

(3) 事後の情報共有、再発防止への対応

- ・課内打合せ・回覧等で課内における情報共有を行う。

- ・必要に応じて業務マニュアルを修正する。

(4) 情報の蓄積

- ・特になし

レベル2 市民への影響はないが他課への影響があるもの

(1) 初期情報共有

- ・口頭又はメモにより、事務ミスの概要を課長まで報告する。

- ・必要に応じて部長、副部長及び影響を受けた部署へ情報提供を行う。

(2) 原因分析・対策立案・公表

- ・事務ミスが発生した業務の担当長が事務ミス事案の原因分析及び対策を検討した上で、課長に報告する（事務ミス報告様式の使用は副課長の判断により、口頭でも可とする。事務ミス報告様式を使用する場合は①の部分を記載し、課長決定を取る）。

- ・必要に応じて部長・副部長に報告を行う。

- ・危機管理担当、議会への報告なし

- ・公表なし

(3) 事後の情報共有、再発防止への対応

- ・課内打合せ・回覧等で課内における情報共有を行う。

- ・必要に応じて部長、副部長及び影響を受けた部署へ情報提供を行う。

- ・必要に応じて業務マニュアルを修正する。

(4) 情報の蓄積

- ・課共有フォルダ等で情報を蓄積する。

- ・必要に応じて部共有フォルダにも情報を蓄積する。
(以下略)

情報システム課が所管する汎用機システムでは、市民や他部署に影響のあるシステム障害が情報システム課起因により発生した場合、実務上はトラブル報告書を作成し、必要な報告を行う運用となっていた。一方で、影響範囲が情報システム課内のみで、かつ軽微なシステム障害については、トラブル報告書が作成されていなかった。

例えば、異常終了したバッチ処理に対して再実行することにより対応が完了する場合、本番環境にリリースした直後のプログラムを起因とする障害・不具合が、軽微なプログラム修正で対応が完了する場合等については、トラブル報告書が作成されない。

このようなトラブル報告書の作成基準は、規程等には明文化されていないため、市民や他部署に影響のない軽微なシステム障害と判断された事象については、どのような内容で、いつ発生したかといった記録は残されていない。

また、トラブル報告書が作成された場合においても、いつ、誰に報告されたかについては記録されていなかった。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

(a) システム障害の記録について（意見）

（対象）

情報システム課（全般的な内容）

市では、障害記録に関連するルールとして、共通実施手順のセキュリテ

イ事故等報告手順及び事務ミス発生時の対応ルールが定められている。しかし、当該ルールはいずれも何らかのトラブルに関する報告について定めたものであり、影響の程度が低いものも含めた障害記録について定めたものではない。

また、汎用機上で稼働する業務システムに係るプログラム開発及び運用保守においては、プログラムの不具合に対応することを目的とした軽微なプログラム変更が行われる場合、全く記録が残されない場合もある。

障害発生時に、発生状況、対応策等の関連する情報を蓄積することにより、当初は無関係に思えた複数の障害から共通の傾向や規則性を発見し、根本的な原因の解消又は予防措置を検討する材料として活用することが可能となる。また、業務システムを組織内部で開発している場合には、当該システムの不具合に直接対応することになるため、障害情報を記録することの有用性は高いといえる。

そのため、各情報システムの所管課長等は、障害記録をプログラムに係る不具合又は操作ミスを含むオペレーション管理に活用する観点から、業務システムの使用のみでは解決できないような状況が発生した場合は、これを障害として取り扱い、関連する情報を記録すべきと考えられる。

したがって、市は、業務システムに係る障害記録の様式を含めた手順を定め、各情報システムの所管課長等は、トラブル報告書等の作成要件を満たさないものについても、障害記録を残すことを検討されたい。特に情報システム課においては、軽微なプログラム修正についても記録を残すことを検討されたい。

(b) トラブル報告書の報告記録について（意見）

（対象）

情報システム課（汎用機上で稼働する情報システム）

トラブル報告書の様式には、報告日及び報告先に係る記載欄が用意されていなかった。また、サンプルとして閲覧したトラブル報告書にも、それらに係る記録は残されていなかった。そのため、当該報告書について、適切に報告されたか否かを確かめることができなかった。

情報システムの障害を含むトラブル発生時には、その事実、発生原因及び再発防止策等を関係者に伝達し、二次的なトラブルを防止するとともに、組織全体として適切な対応を取ることができるよう、情報共有を図る必要がある。

また、トラブル報告書に係る取扱手順とされる事務ミス発生時の対応ルールでは、事務ミスの影響度に応じて報告先を区別している。

そのため、事務ミスの影響度を切り分けるとともに、所定の報告先に報告されたことを示す記録を残す必要があると考えられる。

したがって、トラブル報告書の様式において、報告日及び報告先に係る記載欄を設けるとともに、事務ミスの影響度に応じた所定の報告先に報告されたことを示す事実を記録することを検討されたい。

(エ) 情報資産管理状況の定期的な監査の実施について

a 概要

豊田市情報セキュリティ基本要綱第81条では、以下のとおり、情報セキュリティ対策に係る定期的なチェックを行う旨が定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（監査）

第81条 セキュリティ管理者は、セキュリティ文書に従って情報資産が適切に管理運用されていることを定期的に確認するものとする。

2 セキュリティ管理者は、前項の確認に客観性を持たせるため、第三者による監査を受けるものとする。

（以下略）

また、平成27年9月に改定された共通実施手順に含まれる情報資産登録管理基準には、情報資産の確認について以下のとおり定められている。

<施行：平成27年9月1日 共通実施手順（抜粋）>

（情報資産登録管理基準）

4 登録・管理手順

（中略）

（10）情報資産の確認

セキュリティ責任者は、所管する情報資産の実態と資産管理台帳記載の内容との整合性について定期的に確認を行い、確認した事実の記録を行うものとする。

（以下略）

しかし、市においては、当該条項に基づく情報セキュリティ対策に係るチェック行為が行われていなかった。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 情報資産の定期的な確認状況について（指摘）

（対象）

情報システム課（全般的な内容）

市では、平成 27 年 5 月に情報システム資産管理台帳の登録状況に係る確認が行われているものの、平成 26 年度以前においては、情報資産の管理状況について、定期又は不定期にかかわらず確認がなされていなかった。

市の資金を投じて調達した情報システム及び各種サーバ機器、各種ネットワーク機器、電子記録媒体等の情報資産は、情報システム管理台帳に登録されている。当該情報システム管理台帳の登録状況が適切に管理されているか否かの確認が定期的に行われない場合、不適切な管理状況にある情報資産の発見ができない、又は放置される状況が継続してしまう可能性がある。当該状況が継続することにより、情報資産における機密性及び可用性が低下する、又は誤った管理方法による情報漏えい等のリスク等を高める要因となり得ることが考えられる。

また、平成 27 年 9 月に改定された共通実施手順の情報資産登録管理基準 4 (10) では、セキュリティ責任者は、所管する情報資産の実態と資産管理台帳記載内容との整合性について定期的に確認を行い、確認した事実の記録を行うものとされている。

したがって、情報システム管理台帳の管理状況について、基本要綱第 81 条における「定期」について具体的な期間を定めた上で、セキュリティ管

理者による定期的な確認を行う必要がある。

イ ユーザ ID の管理状況について

(ア) システム利用時のアクセス許可について

a 概要

平成 26 年度当時は、豊田市情報セキュリティ基本要綱において、以下のとおり、情報資産に係るアクセス許可基準は個別実施手順へ定めるものとされていた。

<豊田市情報セキュリティ基本要綱（抜粋）>

(アクセス許可基準)

第42条 セキュリティ責任者は、業務上及び情報セキュリティ上の必要に応じ、所管する情報資産に係るアクセス許可基準を個別実施手順に定めるものとする。

(アクセスの許可)

第43条 セキュリティ管理者は、セキュリティ責任者が情報資産へのアクセスを許可する手順を定めるものとする。

2 セキュリティ責任者は、前条の基準及び前項の手順に従い、所管する情報資産へのアクセスを許可するものとする。

(以下略)

平成 27 年 9 月に改定された「豊田市情報セキュリティ基本要綱」及び「共通実施手順」では、以下のとおり各情報システムで管理すべきアクセス権限に関する基準が定められている。

<施行：平成 27 年 9 月 1 日 豊田市情報セキュリティ基本要綱（抜粋）>

(アクセス制御)

第42条 セキュリティ管理者は、情報システム又はデータへの不正アクセスを防ぐため、アクセス権の制御に関する基準を定める。

2 セキュリティ責任者は、前項の基準に基づき、所管する情報システム及び情報資産へのアクセスを制御し、必要最低限のアクセスのみを許可するものとする。

(以下略)

<施行：平成27年9月1日 共通実施手順（抜粋）>

アクセス制御基準

1 趣旨

基本要綱第42条の規定に基づき、アクセス権の制御に関する基準を定める。

2 IDの管理

セキュリティ責任者は、所管する情報システム及び情報資産へアクセスするために発行するID等について、以下の手順に基づき管理しなければならない。

3 ID等の発行等に関する手順

(1) ID等の種別

セキュリティ責任者は、発行するID等について、次に掲げる種別により区分して管理するものとする。

ア 利用者ID

イ 特権ID

ウ 一時的作業者ID

(2) 利用者ID等の発行申請

情報システムを使用しようとする職員等が所属する課等のセキュリティ責任者は、当該情報システムを管理するセキュリティ責任者に対して、次に掲げる項目を記した発行申請書によりID等の発行を申請するものとする。

ア 使用する情報システムの名称

イ 情報システムを使用する者の所属

ウ 情報システムを使用する者の役職

エ 情報システムを使用する者の氏名

オ 情報システムを使用する目的

カ 情報システムを使用する期間

キ 必要な機能・権限

(3) 利用者ID等の発行

前項の規定により申請を受けたセキュリティ責任者は、申請内容を審査し、当該ID等の発行が適切であると判断した場合は、ID等を発行し、前項の規定により申請された発行申請書について、当該ID

等が有効な期間保管するものとする。
(以下略)

また、平成 27 年 9 月に改定された共通実施手順では、ユーザ ID 及びパスワードの取扱いについて、以下のとおり定められている。

<施行：平成 27 年 9 月 1 日 共通実施手順（抜粋）>

（ID・パスワード取扱い基準）

3 基準

（中略）

（2）職員等は、情報システムを利用するためには発行されたパスワードについて、次の各号に掲げる内容を遵守すること

（中略）

ク 入力短縮のためのパソコン上でのパスワード保存機能を利用しないこと。

（以下略）

※下線は包括外部監査人により記載

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

（a）システム利用時のユーザ認証について（指摘）

（対象）

人事課（人事管理システム）

交通安全防犯課（ネットワーク防犯カメラシステム）

人事管理システムのサーバには、データベースの設定変更、データの変

更及び参照が可能となる支援ツールがインストールされ、当該ツール起動時に要求されるユーザ ID 及びパスワードが保存されていた。また、ネットワーク防犯カメラの業務システム起動時にユーザ認証として入力が要求されるユーザ ID 及びパスワードが、当該業務システムに保存されていた。これにより、ユーザ ID 及びパスワードを把握していない者であっても、ログインボタンを押すだけで業務システムの起動が可能な状態であった。

ユーザ認証は、アクセスを要求してきた者が情報システムの正当な権限者であることを確かめるための機能である。そのため、ユーザ ID 及びパスワードが当該システムに保存されている場合、無権限者によるアクセスが制御されず、未承認のデータ参照、情報漏えい等が行われる危険がある。

従来の共通実施手順では、パスワード保存機能の利用禁止に係る特段の定めはなかった。しかし、平成 27 年 9 月に改定された共通実施手順の ID・パスワード取扱い基準では、入力短縮のためのパソコン上でのパスワード保存機能を利用しないことが明記されている。

したがって、各所管課は、対象システムについて、ユーザ認証に係るユーザ ID 及びパスワードを支援ツール又は業務システムに保存させず、ログインの都度入力を求めるように設定する必要がある。

(イ) ID 及びパスワードの管理について

a 概要

市では、権限を有する者のみが情報システムを利用できるよう制御するため、ユーザ ID 及びパスワードによる認証を行うことを方針としている。

「豊田市情報セキュリティ基本要綱」では、パスワードの管理について以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

(利用者等の登録等及びパスワード管理の手順)

第44条 セキュリティ管理者は、情報システムを利用できる者（以下「利用者」という。）及び情報システムの設定等を行う運用担当者（以下「運用担当者」という。）の登録及び登録の抹消並びにパスワードの管理に関する手順を定めるものとする。

（中略）

（パスワードの管理）

第46条 利用者及び運用担当者は、第44条の規定により定められた手順に

従い、パスワードを管理するものとする。
(以下略)

また、市では共通実施手順のパスワード管理基準において、パスワード設定方針を含む管理基準を定めている。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 端末OS又は業務システムに係るパスワードの定期的な変更について
(指摘)

(対象)

市政発信課（豊田市ホームページ管理システム）
人事課（人事管理システム）
契約課（契約管理システム）
情報システム課（汎用機上で稼働する情報システム）
用地審査課（土地開発基金管理システム）
交通安全防犯課（ネットワーク防犯カメラシステム）
環境政策課（とよたエコポイントシステム）
市民福祉部総務課（医用画像管理システム）
地域福祉課（地域包括支援センターシステム）
介護保険課（介護保険指定期間等管理システム）
健康政策課（特定健診等データ入力システム）
幹線道路推進課（大気データ処理システム）
経営管理課（公営企業会計システム）
下水道施設課（下水道地図情報・排水設備情報ファイリングシステム）
スポーツ課（豊田市スポーツ施設利用システム）

図書館（図書館システム）
学校教育課（学校図書館管理システム）
保健給食課（学校給食管理システム）
指令課（消防指令システム）

対象システムに係るユーザ認証時に要求されるパスワードが、定期的に変更されていなかった。また、対象システムの中には、パスワードの強度が共通実施手順に示される基準に満たないものもあった。

パスワードが長期間にわたり変更されていない場合や、パスワードの強度が十分でない場合、第三者により推測される可能性が高まり、なりすましによる情報システムの不正な使用が行われる危険がある。また、共用しているユーザIDに係るパスワードが変更されていない場合、異動又は退職により担当を外れた職員等による情報システムの使用を、ユーザ認証機能で制御することができない。

共通実施手順のパスワード管理基準では、パスワードの設定方針として定期的な変更あるいは一定の強度を保持すべく所定のルールを定めている。

したがって、各所管課は、共通実施手順に従い、対象システムに係るユーザ認証時に要求されるパスワードを定期的に変更するとともに、パスワードの強度を一定以上とする必要がある。

（ウ） ユーザ登録状況の確認について

a 概要

情報システムは、使用者をIDで管理している。

IDは使用者個人と結びつけられることが一般的で、IDを活用して操作履歴を記録することもできる。

記録された履歴は、IDから誰が操作したかを調べることが可能であり、不正使用の調査等で活用することができる。

IDは現在の使用者のみを登録し、職務権限を失った者のIDは削除するか、無効にすることが一般的である。また、システムによっては、ID数に応じてソフト料金が異なるものもあり、使用者数に応じた適正なシステム価格が求められる。

市における情報セキュリティ対策に関し、必要な事項を定めた「豊田市情報セキュリティ基本要綱」には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（利用者等の確認）

第47条 セキュリティ責任者は、所管する情報資産の利用者及び運用担当者の登録について、定期的に確認するものとする。

（以下略）

また、平成27年9月に改定された共通実施手順には、以下のとおり定められている。

<施行：平成27年9月1日 共通実施手順（抜粋）>

（ID・パスワード取扱い基準）

（中略）

3 基準

(1) 職員等は、情報システムを利用するため発行されたID等について、次の各号に掲げる内容を遵守すること。

ア ID等を他人に教えないこと。

イ ID等を他人に貸さないこと。

（中略）

カ 当該情報システムを使用する必要がなくなり、ID等が不要となった場合、当該情報システムを管理する課等が定める手順により、ID等を返却すること。

（中略）

（アクセス制御基準）

（中略）

4 ID等の管理に関する基準

（中略）

(5) セキュリティ責任者は、ID等の発行状況について、最低1年間に一度の頻度で定期的に見直し、不要なID等が存在した場合は、これを削除又は無効化し、使用不可能な状態としなければならない。

（以下略）

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事

務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) ユーザ ID の利用状況の管理について（指摘）

（対象）

人事課（人事管理システム）

人事管理システムでは、ライセンス契約により使用が許諾されている 20 個のユーザ ID を、複数の職員で共用していた。そのため、操作履歴に残されたユーザ ID では、実際に誰が操作したか確認することができない状況にある。

ユーザ認証は、アクセスを要求してきた者が情報システムの正当な権限者であることを確かめるための機能である。また、情報システムにおいては、ユーザ ID をキーとした操作ログ等を収集し、必要に応じて操作者を追跡及び特定することがある。そのため、ユーザ ID を個人別に付与できる環境においては、ユーザ ID を共用せず個人別に付与することが望ましい。

平成 27 年 9 月に改定された共通実施手順の ID・パスワード取扱い基準では、ID 等を他人に教えないこと及び他人に貸さないこととされている。また、アクセス制御基準では、取り扱うデータの重要度によってはユーザ ID の共用を禁止し、ユーザ ID を個人別に付与すべきとされている。

そのため、ユーザ ID は、情報システムの環境が整っている場合、複数の職員により共用することなく、個人別に設定する必要があると考えられる。

したがって、人事課は、人事管理システムに係る十分な個数のユーザ ID を使用することができるため、共用せず個人別に設定すべきである。

(b) ユーザ ID の登録状況の確認について（指摘）

（対象）

図書館（図書館システム）

保健給食課（学校給食管理システム）

指令課（消防指令システム）

対象システムに係るユーザ ID には、導入時のテスト用等、現在使用していないものが使用可能な状態で存在していた。また、各所管課等では、対象システムについて、不要なユーザ ID の有無を確かめる等の定期的な見直しが行われていなかった。

不要なユーザ ID が使用可能な状態で残存している場合、そのユーザ ID を不正に利用することで、本来許可されない情報システムに対する操作が行われる可能性がある。

平成 27 年 9 月に改定された共通実施手順の ID・パスワード取扱い基準では、情報システムを使用する必要がなくなり、ID 等が不要となった場合、ID 等を返却することとされている。また、共通実施手順のアクセス制御基準によれば、ID 等の発行状況について、最低 1 年間に一度の頻度で定期的に見直すこととされる。

したがって、各所管課では、対象システムについて現在使用していないユーザ ID を削除又は無効化する必要がある。また、セキュリティ責任者である各所管課長は、今後において、定期的にユーザ ID の見直しを行う必要がある。

(c) 情報システムを使用しないユーザの登録状況について（指摘）

（対象）

情報システム課（汎用機上で稼働する情報システム）

汎用機上で稼働する情報システムのうち、市県民税システム及び収納口座情報システムについて、既に情報システムを使用しない状況にあるユーザの ID が使用可能な状態で残存していた。

市県民税システムについては、情報システム課がユーザ登録作業等を行う操作員管理システム（汎用機系システムのユーザ ID を統合的に管理するシステム）でユーザを管理しており、現在は別の課に所属している特別任用職員が、市民税課に所属していた際に使用していたユーザ ID が 1 件残存していた。これは、当該特別任用職員が平成 27 年 4 月から市民税課で勤務した際に、業務上必要があるとして市県民税システムのユーザ登録を行い、同年 6 月に契約満了となった時点でユーザ登録を削除しないまま、現在に至ったものである。なお、市県民税システムが使用可能な端末は限られており、現在所属する課に設置された端末からシステムを使用することはできないが、市民税課等に設置された端末からの使用は可能な状態である。

一方、収納口座情報システムについては、同システム内で独自にユーザ管理を行い、ユーザ登録作業も納税課が主体となって行っているが、過去に存在した所属で登録された特別任用職員のユーザ ID が 2 件残存していた。この 2 件についても、当該特別任用職員が契約満了となった際にユーザ登録の削除をしないまま、現在に至ったものである。

使用可能なユーザ ID が残存する場合、なりすましにより当該ユーザ ID が不正に使用され、データの機密性及び信頼性が損なわれる可能性がある。また、両システムとも市民の個人情報を扱うシステムであるため、情報の機密性については特に注意を払う必要がある。

豊田市情報セキュリティ基本要綱第 47 条において、利用者及び運用担当者の登録に係る見直しについて定められた趣旨からすれば、使用されないユーザ ID については登録状況を見直し、削除又は無効化する等の措置を取るべきである。また、退職、人事異動等によりユーザがシステムを使用しなくなった場合には、ユーザ ID を無効化する等、不要なアクセス権限を停止する必要があると考えられる。

したがって、汎用機系システムのユーザ権限を管理する情報システム課及び収納口座情報システムのユーザ権限を管理する納税課は、年度の途中においても、職員等の退職、人事異動等に伴い、ユーザ ID を削除又は無効化する等、不要なアクセス権限を停止する措置を講じる必要がある。

(d) 退職者の ID に付与されたアクセス権限について（指摘）

（対象）

指令課（消防指令システム）

消防指令システムは、異動又は退職した利用者のユーザ ID に退職者フラグを設定して残していた。

これらの ID は、新規データの登録が制限されているものの、既に登録されたデータの参照及び変更が可能な状態にあった。

異動又は退職した職員のユーザ ID によりデータの参照及び変更ができる場合、そのユーザ ID を不正に利用することで、本来許可されない情報システムに対する操作が行われる可能性がある。

平成 27 年 9 月に改定された共通実施手順のアクセス制御基準によれば、情報システムを使用する必要がなくなり、ID の返還が適切であると判断した場合は、情報システムの利用を終了する日の経過後直ちに当該 ID 等を削除又は無効化し、使用不可能な状態にするものとされている。

そのため、異動又は退職した職員のユーザ ID については、データの参照及び変更ができないように設定する必要がある。

したがって、指令課は、消防指令システムにおけるユーザ ID のうち、退職者フラグが設定されたものについて、全ての操作ができないようにする必要がある。

(エ) システム利用時におけるアクセス権限について

a 概要

一般的に、情報システムでは利用者を識別するため、ユーザ ID が設定されている。ユーザ ID は、端末 OS の利用又は情報システムの利用において設定され、それぞれ異なるユーザ ID が必要となる。

また、各ユーザ ID には権限が付与され、その権限によって利用可能な機能や扱うことのできるデータの範囲を制御することが可能となる。

このうち、高いレベルの権限を持った ID は、特権 ID と呼ばれる。例えば、端末 OS に係るユーザ ID に管理者権限が付与された特権 ID では、任意のソフトウェアのインストールが可能であり、また、特定のアプリケーションにおいて高いレベルの権限を持った特権 ID では、通常業務では使用しない機能が利用可能となる。

平成 27 年 9 月に改定された豊田市情報セキュリティ基本要綱には、アクセスの制御について以下のとおり定められている。

<施行：平成 27 年 9 月 1 日 豊田市情報セキュリティ基本要綱（抜粋）>

（アクセス制御）

第42条 セキュリティ管理者は、情報システム又はデータへの不正アクセスを防ぐため、アクセス権の制御に関する基準を定める。

2 セキュリティ責任者は、前項の基準に基づき、所管する情報システム及び情報資産へのアクセス権を制御し、必要最低限のアクセスのみを許可するものとする。

（以下略）

また、平成 27 年 9 月に改定された共通実施手順に含まれるアクセス制御基準には、以下のとおり定められている。

<施行：平成 27 年 9 月 1 日 共通実施手順（抜粋）>

(アクセス制御基準)

3 ID等の発行等に関する手順

(1) ID等の種別

セキュリティ責任者は、発行するID等について、次に掲げる種別により区分して管理するものとする。

ア 利用者ID

イ 特権ID

ウ 一時的作業者ID

(中略)

(7) 返還された利用者ID等の削除又は無効化

前項の規定により返還申請を受けたセキュリティ責任者は、当該ID等の返還が適切であると判断した場合は、情報システムの利用を終了する日の経過後直ちに当該ID等を削除又は無効化し、使用不可能な状態とするものとする。

(8) 特権ID等の管理

特権IDは、発行対象を原則として当該情報システムを所管する課等における当該情報システムの管理担当職員のみに限定し、発行等に関する手続は(2)から(7)により行うものとする。

(以下略)

また、市では、外部委託先との間で委託契約書等の契約書を作成する場合、情報セキュリティに関する特記を契約書等に添付することとしている。当該特記の様式には、外部委託先が管理する情報システムについて遵守しなければならない事項として、以下のとおり定められている。

<情報セキュリティに関する特記（抜粋）>

(システムの管理)

第11条 乙（受託者）は、本業務において、業務の実施又はサービスの提供に使用する、乙が管理する情報システムについて、次の各号に定める内容を遵守しなければならない。

(中略)

(3) 業務に使用するパソコンに、業務に関係のないアプリケーションをインストールしないこと。

(以下略)

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘及び意見を述べることとする。

(a) 端末 OS の管理者権限の付与について（意見）

（対象）

スポーツ課（豊田市スポーツ施設利用システム）

豊田市スポーツ施設利用システムに係る管理者端末において、OS 上のユーザ ID には全て管理者権限が付与され、これを通常業務に使用していた。

当該端末には、年に 2、3 回程度、外部に設置されたサーバから更新プログラムが配信される。このとき、スポーツ課職員が各拠点に出向くことなくプログラムの更新を行うため、上記管理者権限を付与しているとされる。しかし、管理者権限を使用することにより、動作検証の行われていないソフトウェアがインストールされ、システムが利用できなくなる障害が発生している。

OS の管理者権限を使用する場合、端末に任意のソフトウェアをインストールすることが可能であるため、市が許可していないソフトウェアのインストールが行われる可能性があるほか、マルウェアに感染するなどの危険性も高まる。

また、職員が各拠点に出向くことなくプログラムの更新を行うことは、遠隔操作ソフトウェアを導入することでも対応可能であり、各拠点のユーザに管理者権限を付与する必然性はない。

平成 27 年 9 月に改定された共通実施手順のアクセス制御基準では、特權 ID の発行対象を所管課等における当該情報システムの管理担当職員に限定している。この趣旨からすれば、ユーザに付与する権限は必要最小限に限定すべきものと考えられる。

したがって、スポーツ課は、豊田市スポーツ施設利用システムに係る各拠点の利用端末について、OS の管理者権限の使用者を限定し、各拠点の業

務担当者による使用を制限することにより、ソフトウェアをインストールできないよう制御することを検討されたい。

(b) サーバにおける業務外の作業について（指摘）

（対象）

料金課（検針収納システム）

検針収納システムの保守を行う外部委託業者は、料金課の執務室に常駐し、当該システムが稼働するサーバOS以外でも行える勤怠管理等、当該システムの保守管理とは関係のない作業を、当該システムが稼働するサーバOSに特権IDでアクセスして行っていた。

業務システムが稼働するサーバにおいて業務と関係のない処理が行われた場合、業務システムの稼働状況に影響を与える可能性があり、また、業務システムのデータを誤って削除するなどのセキュリティ事故の発生につながる可能性もある。

外部委託業者から入手すべき誓約書には、業務に使用するパソコンに、業務に関係のないアプリケーションをインストールしない旨の定めがあり、これは、市側の情報システムのリソースを業務に関係のない作業に使用させない趣旨であると考えられる。そのため、業務システムが稼働するサーバにおいて、保守管理とは関係のない作業を行うべきではない。

したがって、料金課は、当該サーバでの外部委託業者による勤怠管理等の作業を禁止し、外部委託業者に対し適切な対応を求める必要がある。

(c) ユーザIDに付与されたアクセス権限について（指摘）

（対象）

人事課（人事管理システム）

人事管理システムには、利用者IDのほか、データのバックアップや利用者IDの操作ロックの強制解除機能を有する特権IDが存在する。人事課では、当該システム利用者全員に特権ID及びパスワードを周知し、利用可能な状況についていた。

業務システムの管理者権限が必要な範囲を越えて付与された場合、未承認の設定変更が行われる可能性がある。

平成27年9月に改定された豊田市情報セキュリティ基本要綱第42条で

は、所管する情報システムのアクセス権を制御し、必要最低限のアクセスのみを許可するものとされている。

したがって、人事課は、人事管理システムに係る特権 ID の使用者を管理担当職員に限定し、当該 ID に係るパスワードを変更するなどの措置を講じる必要がある。

(対象)

指令課（消防指令システム）

指令課は、消防指令システムのサブシステムである消防 OA システムに係るユーザ ID 登録作業を警防救急課に依頼していた。当該システムでは、ユーザ ID に付与する権限を細かく設定することができ、依頼した作業に必要な権限のみを付与することも可能である。

しかし、両課では、相互に職員が異動する場合があるため、警防救急課において、本来は指令課のみが使用すべき特権 ID が共用され、これを使用して当該システムのユーザ ID 登録作業を行っていた。上記で述べたとおり、付与するアクセス権限は必要最小限とするべきである。

したがって、指令課では、警防救急課に使用させるユーザ ID に依頼した作業に必要な権限のみを付与し、特権 ID の使用者を限定する必要がある。

ウ データの管理状況について

(ア) データ修正手続について

a 概要

市では、汎用機システムのデータベースに登録されたデータについて、担当課の依頼に基づき、情報システム課の職員が直接修正する場合がある。

これらのデータ修正依頼については記録を残しているところ、記録の残し方には、以下に示すとおり、主に 2 つのパターンが存在する。

- (a) 担当課から、修正内容が記載されたオンライン画面の写しと合わせて、依頼者の確認印が押された申請を情報システム課で受け取り、修正後、作業者が作業完了の確認印を押す。
- (b) 担当課と情報システム課のみが使用可能なファイルサーバにおいて、データ修正依頼に係る管理ファイルを置き、当該ファイル上に、

依頼日、依頼内容、依頼者、修正者、修正後確認者等の依頼に係る情報を記録する。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

(a) データ修正に係る責任者の承認について（意見）

（対象）

情報システム課（汎用機上で稼働する情報システム）

汎用機上で稼働する業務システムには、一般ユーザ向けの操作メニューでは登録したデータの修正が不可能な場合がある。現行の事務では、データ修正の申請方法が担当課によって違い、修正記録の残し方も一様ではない。加えて、修正依頼の承認者も担当課によって異なっている。

しかし、いずれの場合も、当該承認は口頭により行われ、所管部局及び情報システム課の各責任者により承認されたことを示す記録は残されていない。また、上記運用に係る明文化されたルールは定められていない。

通常の操作メニューを介しないデータ修正に係る依頼及び承認等に係るルールを定めない場合、これらの手順が不明確となり、不適切な処理が行われる可能性がある。

したがって、情報システム課は、通常の操作メニューを介しないデータ修正に係るルールを定めたうえで、修正の記録を残すことを検討されたい。

（イ）時間外のバッチ処理について

a 概要

大量のデータをまとめて一括処理することをバッチ処理と呼ぶ。市では、汎用機において、常にバッチ処理を実施しているが、特に勤務時間中にオンライン等で更新されたさまざまなデータ等を夜間に一括で処理することが多い。バッチ処理は、機械操作専門のオペレーター（委託業者）が実行するため、それを指示するための「作業依頼書」を情報システム課職員が作成し、指示する。夜間は、「作業依頼書」のみでなく「時間外処理連絡票」と呼ばれる夜間バッチ処理一覧表に指示が記載され、実行される。毎日実施する日次処理は、「時間外処理連絡票」にあらかじめ印刷された状態になっていて、それ以外の月次処理などを追記している。

まれに日次処理を実施しない日があるが、その場合、「時間外処理連絡票」にあらかじめ印刷されている処理名に、担当者が取消線を記入することをもって、処理を実行しない決定としている。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

(a) 「時間外処理連絡票」について（意見）

（対象）

情報システム課（汎用機上で稼働する情報システム）

サンプル資料である時間外処理連絡票（2015年6月3日（水））を閲覧した結果、日次処理のうち、「No.2：業務処理名（済通消込み）」、「No.7：業務処理名（園児 済通消込み）」については、取消線が記入され、実行対象から除外されていた。また、取消線の記入に係る明文化されたルールは存在せず、処理を実行しない理由、担当者等は連絡票のみでは分からなかった。

バッチ処理の取消しに関するルールが明文化されていない場合、日次の定例処理の取消しの際に必要な確認項目が網羅されないまま日次処理の取

消しが実行される可能性がある。また、本来取消しに係る決定権がない者であっても、取消線を記入することでバッチ処理を実施しない決定が行われてしまう可能性がある。

そのため、適切な夜間バッチ処理を実行する観点から、処理の取消線を記入する場合、担当者、承認者及び実行しない理由の記録を残すこと、並びに当該手順に係るルールを明文化することを検討されたい。

(ウ) 一般業務ユーザにおける管理コマンドの実行状況について

a 概要

豊田市情報セキュリティ基本要綱では、以下のとおり、プログラムソースの保護措置について定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（プログラムソースライブラリーへのアクセス管理）

第57条 セキュリティ責任者は、所管する情報システムへのソフトウェア導入に当たり、作業実施者の当該情報システムのプログラムソースライブラリー（電子計算機におけるプログラムを保存した領域をいう。）へのアクセスを適切に管理するものとする。

（プログラム等の変更作業の管理）

第58条 セキュリティ責任者は、所管する情報システムのプログラム等の変更作業を実施する場合は、当該情報システムの情報セキュリティを確保するため、必要な措置を講ずるものとする。

（以下略）

データの保護措置に関し必要な事項を定めた「豊田市電子計算機処理管理運営規程」には、以下のとおり定められている。

<豊田市電子計算機処理管理運営規程（抜粋）>

（端末装置に係るデータの保護措置）

第25条 情報システム課長は、端末装置から事務処理に必要なデータ以外のデータの検索及び改ざんが行われないよう、必要な技術的措置を講じなければならない。

2 端末装置管理者及び端末装置操作員は、端末装置の操作に際して、個人情報の保護に万全の注意を払わなければならない。

(以下略)

汎用機系システムを操作する際は、OS のユーザ ID が必要となる。また、OS のユーザ ID は、ユーザプロファイルと呼ばれる権限設定ファイルの内容に依存する。そのため、OS のユーザ ID ごとに使用可能な権限が異なる。

例えば、ユーザプロファイルの設定項目には、OS のユーザ ID ごとに OS にログインした直後に起動するプログラムを指定する項目（以下「初期起動プログラム」という。）、OS のユーザ ID ごとのユーザプロファイルの設定内容を修正できる権限項目等が存在する。

なお、後者の修正権限を有するユーザプロファイルを持つ OS のユーザ ID の使用者は、情報システム課の基盤管理担当職員の一部にのみ割り当てられている。

また、汎用機系のシステムは市の情報システム課にて内製されているため、情報システム課の職員が使用する OS のユーザ ID は、一人につき一般業務用のユーザ ID とシステムメンテナンス用のユーザ ID の 2 種類が設けられている。

システムメンテナンス用のユーザ ID の初期起動画面では、業務システムの管理に必要な管理コマンドである各種プログラムの生成や、各種オブジェクトの作成、変更、削除等を実行可能なメニューが表示されるように設定されている。

一方、一般業務ユーザ ID の初期起動画面では、業務システムへのログイン画面が表示されるのみであり、上記のような管理コマンドが実行可能なメニューは表示されないように設定されている。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 一般業務ユーザのプログラム及びデータに対する操作権限について

(指摘)

(対象)

情報システム課（汎用機上で稼働する情報システム）

情報システム課では、情報システムのプログラム及びデータに係るセキュリティを確保するため、汎用機システムに係るプログラムやデータベースファイル等の更新が可能な管理コマンドの実行メニューを、情報システム課の開発担当者と運用担当者のみに初期起動プログラムによって割り当てている。

しかし、実際には、情報システム課職員以外の一般業務ユーザであっても、特定の操作を行うことにより上記メニューが表示され、管理コマンドの実行が可能な状態であった。

一般業務ユーザにより管理コマンドが実行可能な場合、誤操作等によりプログラム修正又は削除が行われ、処理結果の信頼性が損なわれる可能性がある。同様に、不適切なデータの入力又は修正が行われることにより、データの信頼性も損なわれる可能性がある。

このうち、「情報セキュリティ基本要綱」第 57 条では、プログラムソースライブラリーへのアクセスを適切に管理するものとされ、また、「豊田市電子計算機処理管理運用規程」第 25 条 1 項では、情報システム課長は、端末装置から事務処理に必要なデータの検索及び改ざんが行われないよう、必要な技術的装置を講じなければならないとされている。

そのため、情報システムのプログラムソースライブラリー及びデータ保護の観点から、一般業務ユーザが管理コマンドを使用できないような技術的措置を講ずる必要があると考えられる。

したがって、情報システム課長は、一般業務ユーザによる管理コマンドの使用を制限する等の技術的措置を実施することにより、汎用機システムに係るプログラム及びデータベースファイルの保護を図るべきである。

(エ) アプリケーションシステムのデータへのアクセスについて

a 概要

市における情報セキュリティ対策に関して必要な事項を定めた「豊田市情報セキュリティ基本要綱」には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

(データ等の取扱い)

第70条 セキュリティ管理者は、データ、データを記録した記録媒体及び情報処理により出力された帳票(以下本節において「データ等」という。)の完全性を確保し、データ等の漏洩、盗難、不正複製等を防止するため、データ等の取扱いに関する保護基準及び手順を定めるものとする。

2 職員等は、データ等の取扱いについて、前項の規定により定められた保護基準及び手順に従うものとする。

(以下略)

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘及び意見を述べることとする。

(a) 更新ツールの設定状況について（意見）

(対象)

指令課（消防指令システム）

指令課は、受付時に目標物と呼ばれる場所を特定するための情報を参照、更新するために、指令課執務室内に設置された端末に導入されたツール（以下「更新ツール」という。）を使用している。更新ツールは、消防指令システムを導入した外部業者によって作成されたデータベース編集プログラムであり、目標物等の情報が保存されたサーバに接続し、データの参照及び更新を可能とするものである。当該更新ツールは、指令課職員のうち目標物データの入力及び修正作業を行う4名の担当者のみが使用する。

当該更新ツールは、特定の操作を行うことでプログラムの編集が可能であり、個人情報を含む全てのデータに対して参照、修正及び削除が可能な

状況にあった。

未承認のプログラム変更が行われた場合、本来意図しない処理が行われる可能性がある。また、未承認のデータ修正又は削除が行われた場合、データ間の整合性が損なわれるなど、いずれも業務に影響を与える可能性がある。さらに、データの参照が可能であり、かつ、操作履歴も残されることから、容易に個人情報をコピーすることが可能であるため、個人情報の漏えいも懸念される。

豊田市情報セキュリティ基本要綱第70条によれば、データの完全性を確保し、不正な処理が行われないように手順を定め、職員はその手順に従うものとされている。一方で、更新ツールにおいては、最低限不要な処理が行われないよう対応することが求められる。

したがって、指令課では、外部業者に対して、利用者がプログラムや不要なデータを修正できないよう更新ツールの修正を依頼されたい。また、次期システムにおいては、更新が予定されるマスタデータの編集メニューをアプリケーションの機能に組み込むなどの対応が望まれる。

(b) データの直接修正を行う際の手続について（指摘）

（対象）

環境政策課（とよたエコポイントシステム）

環境政策課では、ポイント発行端末の読み取りエラーが認められた場合、外部業者に依頼してポイントを付与するため、業務システムを介さずに、外部業者に依頼してデータベースを直接修正する対応が取られている。しかし、データベースを直接修正する際の手続は定められていない。このため、環境政策課から外部業者へのデータの修正依頼は口頭で行われ、修正内容及び修正行為について、環境政策課の責任者によって事前に承認された記録は残されていなかった。

データを直接修正する際の手續が定められていない場合、未承認のデータ修正が恣意的に行われる可能性があるため、データの直接修正は、責任者の許可を得た上で行う必要がある。

また、平成27年9月に改定された豊田市情報セキュリティ基本要綱第45条では、データの漏えい、不正複製、毀損及び滅失を防ぐため、データの取扱いに関する基準を定めることとし、共通実施手順の個別実施手順策定・管理手順では、情報資産の重要度に応じ、これらの技術的セキュリティについて、個別実施手順として定めることとしている。

とよたエコポイントは、利用者である市民にとって、地元の特産品や商品券等と交換できる等の利用価値があり、そのデータには一定の完全性や可用性を確保する必要があると考えられる。

したがって、環境政策課では、とよたエコポイントのデータベースを直接修正する際の承認及び依頼に係る手続を個別実施手順として定め、その記録を残すとともに、定期的に当該承認記録と外部委託業者からの作業報告を照合する必要がある。

(オ) 外部記録媒体の管理状況について

a 概要

市では、情報システムで扱うデータのバックアップや配布に際して、CD(CD-R等を含む。)やDVD(DVD-R等を含む。)等の媒体を用いることがある。このような情報システム外にデータ等を記録するためのものを外部記録媒体という。

外部記録媒体に記録された情報の中身は、肉眼で確認することが不可能であり、管理を容易にするには、当該外部記録媒体に貼付したラベルにタイトル、管理番号等を記載して他と区別する必要がある。中身を忘れる前にタイトル等を記載することが望ましいが、一時的な使用では、すぐに捨てる等の理由でタイトル等を記載しない場合もある。

市では、個別の外部記録媒体のラベルにタイトル等を記載することのほかに、外部記録媒体を管理するため、外部記録媒体管理台帳を作成し、台帳による管理も実施している。

市における外部記録媒体の管理に関し、必要な事項を定めた豊田市情報セキュリティ基本要綱には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（データ等の取扱い）

第70条 セキュリティ管理者は、データ、データを記録した記録媒体及び情報処理により出力された帳票（以下本節において「データ等」という。）の完全性を確保し、データ等の漏洩、盗難、不正複製等を防止するため、データ等の取扱いに関する保護基準及び手順を定めるものとする。

2 職員等は、データ等の取扱いについて、前項の規定により定められた保護基準及び手順に従うものとする。

（以下略）

上記第70条に掲げるデータ等の取扱いに関する保護基準は、共通実施手順が該当する。共通実施手順には、具体的な保護基準及び手順として以下のとおり定められている。

<共通実施手順（抜粋）>

外部記録媒体管理基準

- 1 趣旨 基本要綱第70条の規定に基づき、外部記録媒体の管理に関する基準を定める。
- 2 対象 登録及び管理を行う対象は、各課等において保有する外部記録媒体とする。ただし、データを追記することができず、かつ、次に掲げる以外のデータが記録されている外部記録媒体は、登録を不要とすることができる。
 - (1) 機密性が侵害されることにより、市民の生命・財産に影響を及ぼすおそれがあるデータ
 - (2) 機密性が侵害されることにより、行政運営に重大な影響を及ぼすおそれがあるデータ
 - (3) 直ちに一般に公表することを前提としていないデータ
- 3 登録及び管理の方法 セキュリティ責任者及びセキュリティ責任者代理（以下「セキュリティ責任者等」という。）は、登録及び管理の対象となる外部記録媒体について、外部記録媒体管理台帳（以下「媒体管理台帳」という。）に登録し、所管する課等及び個々に識別できる番号を表示したラベルを貼付して管理するものとする。
また、2により登録を不要とした外部記録媒体については、所管する課等及び登録外であることを表示したラベルを貼付するものとする。なお、登録外の外部記録媒体については、媒体への貼付ではなくケースや箱等にまとめてラベルを貼付することも可とする。

（以下略）

市における外部記録媒体の取得及び廃棄については、一元管理を行う目的から、情報システム課に置かれている情報セキュリティ対策事務局（以下「対策事務局」という。）が一括して当該業務を担当している。対策事務局から各部署に配付した後の外部記録媒体は、各部署の責任において管理・運用され、セキュリティ責任者により、個々に識別できる重複しない

番号が記載されたラベルが外部記録媒体に貼付される。これらは外部記録媒体管理台帳において管理される。

また、各部署に配付された外部記録媒体は、月に一度外部記録媒体管理台帳に記録されたラベルの番号を元に、実際の外部記録媒体との突合作業が実施され、配布された外部記録媒体の紛失チェックが実施されている。

b 手続

外部記録媒体の調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) ラベルの貼付されていない外部記録媒体について（指摘）

（対象）

情報システム課（全般的な内容）

情報システム課が所管するマシン室において、個々に識別できる番号が記載されたラベル又は登録外であることが表示されたラベルのいずれも貼付されていない外部記録媒体が9個存在した。当該外部記録媒体のうち、2個については外部記録媒体管理台帳への登録が必要なデータを含む媒体であったが、登録されていなかった。

当該外部記録媒体の内訳については、以下のとおりである。

表 3-45 ラベルの貼付されていない外部記録媒体の内訳

No.	媒体	記録された情報の概要	存在した場所
1	CD-R 1枚	税関係台帳情報	ラック内にある段ボール
2	CD-R 1枚	公開情報	
3	CD-R 6枚	公開情報	
4	DVD-RW 1枚	職員写真情報	机上にある書類ケース

外観の目視確認のみでは記録されている情報の概要又は重要性が把握できない外部記録媒体が存在した場合、思い込み等により登録管理対象外として認識し、外部に持ち出してしまう等により情報漏えいにつながるリスクが高い。

外部記録媒体管理基準 2 には、登録及び管理を行う対象が定められており、また管理・登録対象外とする基準も定められている。その上で、同基準 3において、登録を不要とした外部記録媒体については、所管課等及び登録外であることを表示したラベルを貼付することが定められている。一方で、同基準 3においては、登録外の外部記録媒体については、媒体への貼付ではなく、ケースや箱等にまとめてラベルを貼付することも可とすることが定められている。

以上のことから、外部記録媒体に関して登録の要否を確認の上、ラベルを貼付し、必要であれば外部記録媒体管理台帳に登録を行うべきと考えられる。また、同基準 3 のとおり、登録対象外であれば媒体にラベルを貼付しないことも認められているため、仮に登録すべき情報が格納された外部記録媒体が発見された場合でも、発見者によっては当該外部記録媒体の内容は同基準 3 に示すラベルを貼付しない場合に該当するものであると思い込むことは十分に考えられる。

よって、各課においてラベルが貼付されていない外部記録媒体やそのケース、箱等が存在することは、外部記録媒体の適切な管理又は登録ができているとはいえない。

したがって、ラベルの貼付されていない外部記録媒体やそのケース、箱等が存在した場合は、登録の要否を確認の上、必ずラベルを貼付し、必要に応じて外部記録媒体管理台帳に登録を行うべきである。

例えば、月次で行われている外部記録媒体管理台帳と、配布された外部記録媒体との突合によるチェック作業において、外部記録媒体管理台帳に記載された情報を基軸にしてチェックを行うのではなく、配布された外部記録媒体の現物を基軸にして外部記録媒体管理台帳と突合を行う等により、外部記録媒体管理台帳に登録されていない外部記録媒体が存在した場合でも検出可能なチェック方法を検討されたい。

(カ) システムのデータのバックアップについて

a 概要

一般的に情報システムでは、大量の情報がコンピュータ内にデータとし

て保存される。コンピュータ内に保存されたデータは、ハードウェア障害、操作ミス、災害、又はマルウェア等の不正プログラムの感染等により消失する可能性がある。

こうした事態に備えて、外部記録媒体にバックアップデータを保存することで、コンピュータ内のデータを保護し、データが消失した場合にも情報システムを復旧することができる。

これらの外部記録媒体には、情報システムのデータが保管されていることから、情報システムと同様に適切に管理する必要がある。

バックアップデータの取得について、豊田市情報セキュリティ基本要綱には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

（ソフトウェア等の複製）

第65条 セキュリティ責任者は、重要な情報システムのソフトウェア及びデータについて、当該情報システム又はデータに障害が発生した場合に迅速に復旧するため、定期的に複製を作成し、常に使用できる状態で保管するものとする。

（以下略）

また、平成27年9月に改定された共通実施手順に含まれる外部記録媒体管理基準には、外部記録媒体の保管について以下のとおり定められている。

<施行：平成27年9月1日 共通実施手順（抜粋）>

（外部記録媒体管理基準）

4 登録及び管理手順

（中略）

（3）外部記録媒体の保管

セキュリティ責任者等は、外部記録媒体を鍵のかかるロッカーに保管しなければならない。

（以下略）

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について意見を述べることとする。

(a) バックアップデータの保管状況の確認について（意見）

（対象）

人事課（人事管理システム）
料金課（検針収納システム）
水道維持課（上水道地図情報システム）

対象システムのバックアップデータは、人事管理システム及び上水道地図情報システムについては磁気テープに、検針収納システムについては、ネットワークを通じてアクセスできる外部記憶装置にそれぞれ保存していた。各バックアップ媒体は、各情報システムのサーバと同一の場所に保管され、職員が退庁する際も施錠された書棚へ保管する等の物理的な保護措置は講じられていなかった。

バックアップ媒体がサーバと同一の場所に保管されている場合、火災、地震等の災害によってサーバ上のデータが損失した際に、バックアップデータも損失し、データの復元が不可能となる可能性がある。

また、バックアップ媒体の紛失等を防止する観点から、施錠可能な書庫等に保管する必要があると考えられる。豊田市情報セキュリティ基本要綱第65条によれば、重要な情報システムのデータは、障害発生時に備え、常に使用できる状態で保管するものとされている。また、平成27年9月に改定された共通実施手順の外部記録媒体管理基準では、外部記録媒体を鍵のかかるロッカー等に保管しなければならないとされており、情報システムの重要度に応じてバックアップ媒体についても物理的な保護措置を図ることが想定されている。

対象システムは、職員の入事情報、水道使用量及び料金等が含まれるものであり、直ちに一般公表することが予定されていないことから、一定の機密性を確保すべきと考えられる。

したがって、対象システムに係るバックアップ媒体のうち、磁気テープ等については施錠可能な書棚等へ保管し、ネットワークを通じてアクセスできる外部記憶装置については施錠可能な専用の棚へ設置する等の措置を

講ずる必要がある。また、情報セキュリティの観点から、データの重要度に応じて、耐火耐震区画、遠隔地等への保管を検討されたい。

(キ) 緊急時用のバックアップシステムについて

a 概要

市では、住民記録情報を管理する住民記録情報システム及び諸証明を発行する総合窓口システムにおいて、市民の異動処理証明書の発行、納税情報等の更新業務及び住民票等の出力業務を実施している。

これらの業務システムについては、市民に対する行政サービスの維持の観点から、住民票等の参照・出力に機能を限定したツールを作成し、当該システムが停止した場合も業務を遂行することが可能となるよう対策を講じている。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 住民記録情報システムの緊急時用バックアップツールについて（指摘）

(対象)

情報システム課（汎用機上で稼働する情報システム）

汎用機上で稼働する情報システムである住民記録情報システム及び総合窓口システムには、災害時対応用のバックアップツールが用意されていた。当該ツールは、前日までに登録された住民記録情報が保存されたサーバに接続することで、データの閲覧を可能とするものである。

当該ツールは、市民課及び情報システム課に所属する正規職員及び特別任用職員の全員により常時使用可能な状態であった。

当該ツールの使用時にはパスワードが要求されるものの、ユーザ ID は設定されていない。そのため、当該ツールを使用すれば、操作ログ等の使用記録を残さずに市民の個人情報である住民記録情報を閲覧することが可能であった。

なお、業務システムを操作した場合は、汎用機のログにより、誰がどのような操作を行ったのかを追跡することが可能である。住民記録情報のような高い機密性が要求される情報を扱う業務システムについて操作者が必要な範囲に限定されない場合、情報漏えいが発生する等、機密性が損なわれる可能性が十分に低減されない。また、バックアップシステムにおいても、取り扱われる情報の機密性は業務システムと同程度のセキュリティ水準が要求されるのが本来である。

そのため、バックアップシステムは、平常時において使用する必要がなく、操作者を限定したとしても支障はないことから、所管部局において、平常時におけるバックアップシステムの使用者を必要な範囲に限定し、業務システムと同程度のセキュリティ水準を維持する必要があると考えられる。

したがって、市民課及び情報システム課は、平常時における当該ツールの使用者を必要な範囲に限定する等の措置を講じるとともに、業務システムと同様に操作ログ等の使用記録を残すことにより、使用状況を確認できる体制を整える必要がある。

エ 脅威への対策について

(ア) 情報処理装置の保護について

a 概要

情報システムを構成するハードウェアは、精密機器であり、物理的な衝撃で故障する可能性がある。また、ノート型パソコンのような小さな物については、紛失・盗難が発生する可能性が高いことから、保管方法に注意を払う必要がある。

市における情報セキュリティ対策に関し、必要な事項を定めた豊田市情報セキュリティ基本要綱には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

(情報処理装置の保護)

第31条 セキュリティ管理者は、災害等環境上の脅威、許可されない物理的アクセス、電源異常又は通信ケーブル等の配線の損傷等から情報処理装置を守るため、情報処理装置に係る保護基準を定めるものとする。

2 セキュリティ責任者は、前項の情報処理装置に係る保護基準に基づき、所管する情報処理装置について講ずべき必要な措置を個別実施手順に定め、実施するものとする。

(以下略)

また、市の所管する各システムに対して、共通して遵守すべき事項又は基準を定めた共通実施手順には、以下のとおり定められている。

<共通実施手順（抜粋）>

情報処理装置保護基準

1 趣旨

基本要綱第31条の規定に基づき、情報処理装置の保護基準を定める。

2 パソコン保護基準

(1) セキュリティ責任者は、所管するデスクトップ型パソコンには、必要に応じて転倒防止策を講じなければならない

(2) セキュリティ責任者(第25条第2項責任者、セキュリティ責任者代理)は、ノート型パソコンについては、職員等の帰宅時にはできる限りロッカ等の施錠できる場所に保管又はワイヤーロックで設置場所に固定する等の盗難防止措置を講じなければならない。

(以下略)

なお、上記共通実施手順は、平成27年9月1日に以下のとおり改正されている。

<施行：平成27年9月1日 共通実施手順（抜粋）>

情報処理装置の設置環境に関する基準

(中略)

3 基準

(1) 機密性重要度3のデータを保管する機器を設置する区画等については、

次に掲げる基準を満たすこと。

- ア 外部からの侵入が容易にできないよう、外壁は無窓であること。
 - イ 外部に通ずるドアは必要最小限とし、施錠可能であること。
 - ウ 入退室を許可された者にのみ制限すること。
 - エ 入退室記録を取得すること。
 - オ 入室中は身分証明書等を携帯すること。
 - カ 当該区画等を管理する課等の職員等以外の者が入室する場合は、当該区画等を管理する課等の職員等が付き添うこと。ただし、監視カメラ等により区内の状況が確認できる場合は、その限りではない。
 - キ 当該区画等に設置された情報システムに関連しない情報資産の持ち込みを禁止すること。
- (2) 機密性重要度2以上のデータを保管する機器は、セキュリティーワイヤー、ネジ止め等による盗難防止対策を行うこと。
- (3) 機密性重要度2以上のデータへアクセス可能な機器は、外部の者が自由に出入りすることができず、職員等が監視可能な場所に設置すること。
- (4) 機密性重要度1のデータを保管する機器又は機密性重要度1のデータへのみアクセスする機器を外部の者が自由に出入りすることができる場所へ設置する場合は、セキュリティーワイヤー、ネジ止め等による盗難防止対策を行うこと。
- (5) 可用性重要度2の情報システムを構成する機器のうち、当該機器が停止することでシステム全体の停止となる機器を設置する区画等については、次に掲げる基準を満たすこと。
- ア 耐震又は免震機能を持つこと。
 - イ 自家発電設備と接続され、落雷等による過電流に対する防護機能を持った無停電電源設備を持ち、停電時にも無停止で安定した電源供給機能を保つこと。
 - ウ 不活性ガス等による消火設備を持ち、火災発生時に機器の破損がないこと。
 - エ 冗長化された空調設備により、温度及び湿度を一定に保つこと。
- (6) 可用性重要度2の情報システムを構成する機器のうち、当該機器が停止することでシステム全体の停止となる機器の設置については、次に掲げる基準を満たすこと。
- ア ベルト、ビス等により固定し、転倒及び衝突防止対策を行うこと。
 - イ バンド、チューブ等によりケーブル類を結束し、地震や引っ掛け等によるケーブル抜けを防ぐこと。

(以下略)

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) サーバ等機器の設置状況について（指摘）

（対象）

人事課（人事管理システム）

市民福祉部総務課（乙ヶ林診療所コンピューテッドラジオグラフィーシステム）

料金課（検針収納システム）

水道維持課（上水道地図情報システム）

下水道施設課（下水道地図情報・排水設備情報ファイリングシステム）

保健給食課（学校給食管理システム）

対象システムのサーバ等の機器は、平成27年9月に改定された共通実施手順の情報処理装置の設置環境に関する基準に照らし、適正な場所に設置されていなかった。業務に関連のない職員がサーバ等に容易に接近することが可能であり、過失により物理的な衝撃が与えられる可能性がある状況であった。

従来の共通実施手順では、利用端末に係る物理的な保護措置について定められていたものの、サーバ等の機器については特段の定めがなかった。しかし、平成27年9月に改定された共通実施手順の情報処理装置の設置環境に関する基準では、情報処理装置の設置環境に係る基準を定め、情報資産の重要度の区分に応じて、機器を設置する区画等への入退室、盗難、衝突防止等の対策を講じることとしている。

したがって、各所管課は、改定後の共通実施手順に従い、対象システム

の重要度の区分に応じて、サーバ等の機器を適正な場所に設置し直す等物理的な措置を講じる必要がある。

(b) 情報システム処理装置の設置状況について（指摘）

（対象）

河川課（工損費用算定システム）

工損費用算定システムが稼働するノート型パソコンは、施錠可能な書庫等に保管されず、ワイヤーロック等の盗難防止措置も講じられていないかった。

職員の不在時において施錠可能な書庫等への保管が行われていない、あるいはワイヤーロック等の盗難防止対策が施されていない場合、利用端末が不正に持ち出される等により、当該端末を利用していた職員の業務に支障を来す可能性がある。

また、当該システムの特性としてスタンドアロンであることから、当該利用端末内部に本番データが格納されているため、当該利用端末が紛失し、又は盗難に遭った場合、当該システムの情報が外部に漏えいする可能性がある。

共通実施手順の情報処理装置保護基準2によれば、搭載された情報システムにかかわらず、セキュリティ責任者が所管するノートパソコンを対象として、職員等の帰宅時にはできる限りロッカー等の施錠できる場所に保管し、又はワイヤーロックで設置場所に固定する等の盗難防止措置を講じなければならないとされている。

平成27年9月に改定された共通実施手順の情報処理装置の設置環境に関する基準では、情報処理装置の設置環境に係る基準を定め、情報資産の重要度の区分に応じて、機器を設置する区画等への入退室、盗難及び衝突防止等の対策を講じることとしている。

したがって、河川課は、改定後の共通実施手順に従い、対象システムの重要度の区分に応じて、利用端末に対する物理的な保護措置を講じる必要がある。

(イ) 無線LANの利用について

a 概要

無線 LAN とは、電波を使って無線 LAN の機能を持つパソコンとアクセスポイントと呼ばれる中継機器との間で通信を行うネットワーク環境のことである。無線 LAN を利用することで、パソコンにネットワークケーブルを接続する必要が無く、電波の届く範囲でネットワークに接続することが可能となる。

電波は一定の範囲内であれば壁や建物等の障害物を越えて届くため、不正アクセスや通信内容が盗み見られないよう通信データを暗号化するなど適切なセキュリティ対策を講じる必要がある。

市では、無線 LAN の利用について、共通実施手順に以下のとおり定めており、その利用を原則禁止していた。

<共通実施手順（抜粋）>

ネットワーク保護基準

(4) 無線LANの利用の禁止

①セキュリティ責任者は、ネットワークを構築するにあたっては、次のいずれかに該当する場合を除き、無線LANを用いてはならない。

- ・ネットワーク上を流れるデータに、将来にわたって個人情報が含まれないと想定される場合
- ・小規模のネットワークで、不正侵入、データ漏洩の可能性が極めて低い場合
- ・ネットワークを敷設するにあたって有線とすることが極めて困難な場合
- ・インターネットに接続するための専用回線の場合

②セキュリティ責任者は、無線LANを利用する場合には、無線LAN上を流れるデータの重要度に応じて必要なセキュリティ対策を定め、情報セキュリティ対策会議の意見を聴いて、セキュリティ管理者の承認を得なければならない。

（以下略）

※下線は包括外部監査人により記載

また、平成 27 年 9 月に改定された共通実施手順に含まれるネットワーク管理基準には、無線 LAN の使用について以下のとおり定められ、取り扱うデータの重要度に応じて無線 LAN の使用を禁止している。

<施行：平成 27 年 9 月 1 日 共通実施手順（抜粋）>

(ネットワーク管理基準)

6 基準

(中略)

(4) 無線ネットワークの使用に関する基準

ネットワークに無線ネットワークを使用する場合は、次に掲げる対策を講ずること。

ア 機密性重要度2以上又は完全重要度2のデータが流通するネットワークについては、無線ネットワークは使用してはならない。

(以下略)

ネットワーク防犯カメラシステム及び豊田市スポーツ施設利用システム利用端末のうち、庁舎内に設置された利用端末では、インターネット回線に接続する際に無線LANを利用している。

ネットワーク防犯カメラシステムは、豊田市の全域を網羅する専用のネットワークで接続され、庁内に設置された端末からは、設置された全てのカメラの映像を確認することができる。

豊田市スポーツ施設利用システムは、外部に設置されたサーバとの接続に、通信内容を暗号化した上でインターネット回線を利用している。

ネットワーク防犯カメラシステムでは、画像データに個人が特定される映像が含まれる可能性があり、豊田市スポーツ施設利用システムは、施設予約情報等の個人情報を取り扱っている。

対象システムは、サーバと端末がインターネット経由で接続されるため、暗号化技術を用いて通信データが暗号化され、一定の情報セキュリティ対策が講じられている。

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) 無線 LAN の利用について（指摘）

（対象）

交通安全防犯課（ネットワーク防犯カメラシステム）

スポーツ課（豊田市スポーツ施設利用システム）

対象システムは、庁舎内に設置された利用端末からインターネット回線に接続する際に無線 LAN を利用することについて、いずれもセキュリティ管理者である総務部長の承認を得ていなかった。

無線 LAN の利用において、セキュリティの設定が不十分な場合、通信内容が傍受される可能性や、不正アクセスによるネットワーク上を流れるデータの流出又は接続された端末を踏み台にした不正な操作が行われる可能性がある。

改正前の共通実施手順のネットワーク保護基準では、原則として無線 LAN の使用が禁止され、例外的に認められるケースであっても、セキュリティ管理者の承認を得なければならないとされていた。

また、平成 27 年 9 月に改定された共通実施手順のネットワーク管理基準では、上記承認手続についての定めは削除されているものの、一定以上の重要度に区分されたデータが流通するネットワークについて、無線ネットワークの使用が禁止されている。

そのため、平成 26 年当時としては、無線 LAN の使用についてセキュリティ管理者の承認が必要であり、また、共通実施手順改定後においては、一定以上の重要性が認められるデータが流通するネットワークについて無線 LAN を使用してはならないと考えられる。

対象システムについては、無線 LAN の利用について情報セキュリティ管理責任者である総務部長の承認を得ておらず、適切な手順を経ないでこれを利用していたものと考えられる。

また、ネットワーク防犯カメラシステムは、導入時の検討において個人情報保護の対象とされ、豊田市スポーツ施設利用システムは各施設の予約情報等の個人情報が取り扱われることが明らかである。個人情報は、直ちに一般に公表することを前提としていない情報資産に該当すると考えられるため、これを含むデータが流通するネットワークに無線ネットワークの使用を禁止する改定後の共通実施手順のネットワーク管理基準にも合致しないといえる。

したがって、対象システムについては、無線 LAN の使用を中止し、有線でのネットワークを構築する必要がある。

なお、一定以上の重要度に区分されたデータが流通するネットワークであっても、セキュリティ対策を講じることによりリスクを十分に低減できる場合には、無線 LAN の使用を一律で排除する必要性はないと考えられるため、実態に応じてルールを緩和することも検討されたい。

(ウ) コンピュータウイルス対策ソフトについて

a 概要

不正な動作を行う意図で作成された悪意のあるソフトウェアであるいわゆるマルウェアは、ネットワーク、コンピュータ、記録装置媒体等のあらゆる環境で感染する可能性がある。例えば、メールの添付ファイルや USB メモリ等の外部記録媒体にマルウェアが含まれていた場合、ファイルを開いた際に感染することがある。

こうしたマルウェアの対策としては、ウイルス対策ソフトの導入が効果的とされている。ウイルス対策ソフトは、マルウェア等の不正なプログラムのパターンを収録したウイルス定義ファイルと検査対象のファイルを照合（スキャン）し、パターンとの一致が見られた場合、該当するマルウェアを検出又は駆除することができる。

なお、ウイルス対策ソフトは、ウイルス定義ファイルを最新の状態に保つことで、最新のマルウェアに対応することが可能となる。

市における不正なソフトウェアへの対策に関し必要な事項を定めた「豊田市情報セキュリティ基本要綱」には、以下のとおり定められている。

<豊田市情報セキュリティ基本要綱（抜粋）>

(コンピュータウイルス対策)

第76条 セキュリティ管理者は、情報システムをコンピュータウイルス等不正なソフトウェアから保護するため、コンピュータウイルス対策基準を定めるものとする。

2 セキュリティ責任者は、前項のコンピュータウイルス対策基準に従い、所管する情報システムをコンピュータウイルス等不正なソフトウェアから保護するため必要な措置を個別実施手順に定め、実施するものとする。

（以下略）

また、市の所管する各システムに対して、共通して遵守すべき事項又は

基準を定めた「共通実施手順」には、以下のとおり定められている。

<共通実施手順（抜粋）>

インターネット利用の監視等に関する基準

1 趣旨

基本要綱第27条第2項の規定に基づき、インターネット端末の職員等の不正利用の防止及び職員等の不正サイト閲覧によるコンピュータウィルス感染の防止のため、インターネットの利用の監視及び制限(以下「監視等」という。)に関する基準を定める。

2 インターネット利用の監視等

インターネット端末又はインターネットLANを所管するセキュリティ責任者は、当該インターネット端末又はインターネットLANを利用する職員等のホームページの閲覧及び電子メール(インターネットのメールに限る。)の送受信の監視等をすることができる。

3 監視等の方法

監視等の方法は、対策事務局長が、対策会議の意見を聴いて、別に定める。

4 監視結果の報告

- (1) 対策事務局長は、監視の結果、不正利用等が確認された場合は、セキュリティ管理者に報告しなければならない。
- (2) セキュリティ管理者は、監視結果を不正利用等が確認された所属のセキュリティ責任者に通知し、適切な措置を求めなければならない。
(中略)

コンピュータウィルス対策基準

1 趣旨

基本要綱第76条第1項の規定に基づき、コンピュータウィルス対策についての基準を定める。

2 実施すべき事項

(中略)

(2) 情報セキュリティ責任者

- ①所管するパソコン又はサーバ(以下「パソコン等」という。)にウィルス対策ソフトを導入し、次に掲げる事項を設定すること。

- ・リアルタイムスキャン機能を有効にすること。
 - ・ウィルス定義ファイルを常に最新のものに更新できる仕組みを構築すること。
 - ・システムの完全ウィルススキャンを最低月1回実行すること。
- (以下略)

※下線は包括外部監査人により記載

b 手続

情報システムの調達・運用に係る資料を入手し、必要と考えられる監査手続（閲覧、突合、分析、質問、観察等）を実施することにより、当該事務手続の合規性等を検証した。

c 監査結果

上記の監査手続を実施した結果、次の事項について指摘を述べることとする。

(a) コンピュータウイルス定義ファイルの更新について（指摘）

(対象)

経営管理課（公営企業会計システム）

水道整備課（水道管網解析システム）

下水道施設課（下水道地図情報・排水設備情報ファイリングシステム）

対象システムの利用端末において、ウイルス対策ソフトのコンピュータウイルス定義ファイルが最新のものに更新されていなかった。

いずれも外部ネットワークに接続されていないため、外部記録媒体等を使ってコンピュータウイルス定義ファイルを更新する必要があるが、当該作業が行われていなかったものである。

コンピュータウイルス定義ファイルには、各セキュリティ対策ソフトのメーカー等が発見したコンピュータウイルスの情報が登録されている。コンピュータウイルス定義ファイルが更新されていない場合、新しいコンピュータウイルスやその亜種の情報が登録されず、E-mail や USB メモリ等から新しいコンピュータウイルス等が侵入した場合に、それを検知することができず、感染してしまう可能性がある。

共通実施手順のコンピュータウイルス対策基準では、所管するパソコンにウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新のものに更新できる仕組みを構築すること及びシステムの完全ウイルススキャンを最低月1回実行することとされている。

このため、外部ネットワークに接続されていない環境であっても、運用にてウイルス定義ファイルの更新が求められると考える。

したがって、各所管課は、対象システムに係る端末について、定期的にウイルス定義ファイルの更新を行う必要がある。

(b) コンピュータウイルス対策ソフトの導入について（指摘）

(対象)

交通安全防犯課（ネットワーク防犯カメラシステム）

生涯学習課（とよた科学体験館 プラネタリウム投影システム）

ネットワーク防犯カメラシステムは、当該システム利用端末にコンピュータウイルス対策ソフトが導入されていなかった。交通安全防犯課では、当該システム導入時において、防犯カメラ映像の閲覧のみを想定し、利用端末に外部記録媒体を接続することは想定していなかった。しかし、映像データを警察に提供する場合等、外部記録媒体が接続される可能性はあると思われる。

また、とよた科学体験館のプラネタリウム投影システムの利用端末にも、コンピュータウイルス対策ソフトが導入されていなかった。そのため、外部委託業者よりプラネタリウム番組データの提供を受ける際、受領したUSBメモリ等のウイルススキャンを実施せずに、プラネタリウム投影システムの利用端末に接続していた。

情報システム利用端末にコンピュータウイルス対策ソフトが導入されていない場合、マルウェアに感染した外部記録媒体が接続されることにより、利用端末がマルウェアに感染し、コンピュータ内にあるデータの消失、書換え、情報漏えい等の被害を受ける可能性がある。

豊田市情報セキュリティ基本要綱第76条2項では、セキュリティ責任者は、コンピュータウイルス対策基準に従い、所管する情報システムをコンピュータウイルス等不正なソフトウェアから保護するために必要な措置を個別実施手順に定め、実施するものとされている。また、共通実施手順のコンピュータウイルス対策基準では、所管するパソコンにウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新のものに更新できる仕組

みを構築するとともに、システムの完全ウイルススキャンを最低月 1 回実行することとされている。

したがって、各所管課は、対象システムに係る利用端末にウイルス対策ソフトを導入し、常に最新のパターンファイルに更新された状態で、月 1 回以上のウイルススキャンを実行するとともに、外部委託業者から受領した USB メモリを使用する前にウイルススキャンを行う必要がある。

(c) 個別システムパソコンにおけるインターネット利用の監視について
(指摘)

(対象)

スポーツ課（豊田市スポーツ施設利用システム）

豊田市スポーツ施設利用システム管理者端末が設置されている拠点は、以下のとおりである。

表 3-46 豊田市スポーツ施設利用システム管理者端末の設置拠点

No.	設置場所
1	高岡コミュニティセンター
2	高橋コミュニティセンター
3	東山体育センター
4	高岡公園体育館
5	スカイホール豊田
6	柳川瀬公園体育館
7	豊田地域文化広場
8	平戸橋いこいの広場
9	毘森公園管理事務所
10	豊田市運動公園体育館
11	豊田市運動公園陸上競技場
12	豊田市五ヶ丘運動広場
13	猿投棒の手ふれあい広場
14	西部体育館
15	井上公園水泳場
16	藤岡体育センター
17	緑の公園管理事務所

18	足助トレーニングセンター
19	下山トレーニングセンター
20	旭総合体育館
21	稻武ふれあい子ども館
22	逢妻交流館
23	朝日丘交流館
24	井郷交流館(猿投コミュニティセンター)
25	石野交流館
26	梅坪台交流館
27	上郷交流館(上郷コミュニティセンター)
28	猿投北交流館
29	猿投台交流館
30	末野原交流館
31	崇化館交流館
32	高橋交流館
33	豊南交流館
34	保見交流館
35	前林交流館
36	益富交流館
37	松平交流館(松平コミュニティセンター)
38	美里交流館
39	竜神交流館
40	若園交流館
41	若林交流館
42	西部コミュニティセンター
43	市役所(スポーツ課)

豊田市スポーツ施設利用システムに係る管理者端末は、各拠点に設置され、いずれもインターネットに接続されている。しかし、スポーツ課では、当該端末によるインターネット利用の監視が行われていなかった。

端末によるインターネット利用の監視等が行われていない場合、職員等の不正な利用、マルウェアへの感染によるデータ漏えいが検知されない可能性がある。

また、共通実施手順のインターネット利用の監視等に関する基準では、セキュリティ責任者は、インターネット利用の監視等を行い、不正利用等

が確認された場合は、セキュリティ管理者に報告しなければならないとされる。

したがって、スポーツ課は、当該端末によるメールの送受信履歴やホームページの閲覧履歴等インターネット回線を流れる通信内容を記録するツールを導入し、不正利用等が発見された場合は、セキュリティ責任者であるスポーツ課長を通じてセキュリティ管理者である総務部長へ報告する仕組みを整備すること又は当該端末からインターネットへの接続を取りやめることのいずれかの対応をとる必要がある。

(4) 用語集

用語	説明	出典
ASP サービス	インターネット上でアプリケーションを提供するサービスの提供者（事業者）から提供されるソフトウェアやサービスのこと。 ASP とは、Application Service Provider（アプリケーションサービスプロバイダ）の略	3
DBMS	DataBase Management System の略 データベースを管理し、データに対するアクセス要求に応えるソフトウェア	1
OS	Operating System（オペレーティング・システム）の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。	2
URL	インターネット上の情報資源の場所とその属性を指定する記述方式 情報資源の種類やアクセス方法、情報を提供するウェブサーバの識別名、ファイルの所在を指定するパス名などで構成される。	5
アプリケーション	コンピュータの OS 上で動作するソフトウェアのこと。	3
ウイルススキャン	コンピュータがウイルスに感染していないかどうかを検査すること。	3
ウイルス対策ソフト	コンピュータをウイルスから防御するためのソフトウェアのこと。「アンチウイルスソフト」とも呼ばれる。	3
カスタマイズ	ソフトウェアの設定や設計を調整し、ユーザの好みに合わせて作り変えること。	4

管理者権限	サーバの全ての機能を利用できる権限	5
クライアント・サーバ型	<p>情報を提供するサーバと、情報の提供を受けるクライアントから構成されるネットワークによるシステム形態のひとつ。</p> <p>クライアント（顧客）がサーバ（提供者）に対して、要求した情報を受け取ることで、さまざまなサービスを提供する方式である。</p>	3
グループウェア	組織や企業で LAN を活用して情報共有やコミュニケーションの効率化を図り、グループで作業することを支援するソフトウェアの総称	3
サーバ	<p>ネットワーク上で情報やサービスを提供するコンピュータのこと。</p> <p>逆に、サーバに対して、情報やサービスを要求するコンピュータをクライアントという。</p>	3
情報セキュリティ	<p>情報の機密性、完全性及び可用性を確保すること。</p> <p>機密性とは、ある情報へのアクセスを認められた人だけがその情報にアクセスできる状態を確保すること。完全性とは、情報が破壊、改ざん又は消去されていない状態を確保すること。可用性とは、情報へのアクセスを認められた人が、必要時に中断することなく情報にアクセスできる状態を確保すること。</p>	3
スタンドアロン	コンピュータを他のコンピュータと接続せずに単独で利用する形態	4
脆弱性	コンピュータやネットワークにおいて、情報セキュリティ上の問題となる可能性がある弱点のこと。	3
電子カルテ	診療録等に記録された診療情報(診療の過程で得られた患者の病状や治療経過等の情報)を電子化し、保存された診療録	6
統合型 GIS	<p>ネットワーク環境のもとで、庁内で供用できる空間データを「共用空間データ」として一元的に整備・管理し、各部署において活用する庁内横断的なシステム（技術・組織・データの枠組）</p> <p>GIS とは、地理的位置を手がかりに、位置に関する情報を持ったデータ（空間データ）を総合的に管理・加工し、視覚的に表示し、高度な分析や迅速な判断を可能とする技術</p>	10

特権 ID	サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID	5
ハウジングサービス	主にファシリティに関するサービスの提供を行うものの。代表的なサービス例は、スペース提供(フロア提供、設備警備等)、電源空調設備の提供	7
バックアップ	データの写しを取って別の記録媒体に保存すること。	8
パッケージソフトウェア	CD-ROM や DVD などのメディアに記録され、マニュアルなどとともに包装されて店頭で販売されているソフトウェア製品又は市販ソフトウェア製品のこと。最近ではインターネットからダウンロード販売されるものもある。	3
バッチ処理	コンピュータのデータ処理方法で、データを一定期間あるいは一定量まとめてから、一括して処理を行う方式のこと。	4
パッチ	完成したプログラムに対して、脆弱性等をなくすために後から配布される修正プログラムのこと。	3
汎用機	ホストコンピュータ、メインフレーム、汎用コンピュータ、エンタープライズサーバ等と呼ばれるベンダ独自仕様 OS を搭載する大型電子計算機を備えた情報処理システム	9
マルウェア	malicious software の短縮された語。コンピュータウイルスのような有害なソフトウェアの総称	2
無線 LAN	ケーブル線の代わりに無線通信を利用してデータの送受信を行う LAN システム。IEEE802.11 諸規格に準拠した機器で構成されるネットワークのことを指す場合が多い。	2

1 「平成 19 年情報通信白書」(総務省)

2 「平成 26 年情報通信白書」(総務省)

3 「国民のための情報セキュリティサイト」(総務省)

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

4 「自治体 E A 一業務・システム刷新化の手引きー」(総務省)

http://www.soumu.go.jp/denshijiti/system_tebiki/dict/content_a.h

tml

- 5 「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」（平成 27 年 3 月 27 日一部改訂）（総務省）
- 6 「標準的電子カルテ推進委員会 最終報告」（平成 17 年 5 月 17 日）（厚生労働省）
- 7 「公共 IT におけるアウトソーシングに関するガイドライン」（平成 15 年 3 月）（総務省）
- 8 「地方公共団体における行政情報化の推進状況調査結果」（平成 27 年 3 月）（総務省）
- 9 「電子自治体の取組みを加速するための 10 の指針」（平成 26 年 3 月 24 日）（総務省）
- 10 「地方自治情報管理概要～電子自治体の推進状況（平成 26 年 4 月 1 日現在）～」（平成 26 年 4 月 1 日）（総務省）

第4 利害関係

包括外部監査の対象としての特定の事件につき、私には地方自治法第 252 条の 29 に規定されている利害関係はない。