

平成27年度  
包括外部監査の結果報告書  
(概要版)

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



## 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

公認会計士3名、公認情報システム監査人3名、弁護士1名、

## 第2 外部監査の結果

監査結果のうち、合規性等についての指摘事項（指摘）は32件、経済性・効率性等に関する意見を述べた事項（意見）は15件であった。

### 1 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、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。

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。

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。

### (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。

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。

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。

## 2 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

##### 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）

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。）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。

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、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。

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

##### 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があった。

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

##### 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。

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

### 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。

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、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。

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。

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。

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。

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、随意契約により業者が選定されている。

サーバ等機器の設置に係る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。

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。

才 情報システム等の導入及び変更管理について

a 情報システム導入およ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。

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。

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。

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。

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。

## 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

### 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。

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。

図書館は、図書館システムの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

### 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。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。

したがって、対象システムの各所管課は、リース期間にかかるわらず利用端末をOSのサポート期間内に更新する必要がある。

ク ベータ版ソフトウェアの導入について

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、調達に係る手続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。

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 隨意契約の対象範囲について

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。

当該契約の対象のうち、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。

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付加しており、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。

当該契約の対象のうち、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、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、随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

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）

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、映像中継装置等が5台追加購入され、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った。

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、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に係る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った。

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

#### 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）

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。

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） 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タ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）  
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。

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) 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。

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、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) 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ィ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。

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。

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ます

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、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、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) 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）

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。

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。

したがって、情報システム管理台帳の管理状況について、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) 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支援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。

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。

したがって、各所管課は、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) 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）
- 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。

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) 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。

情報システムにおいては、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。

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つた。

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。

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 が使用可能な状況で残存していた。

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。

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。

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) 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。

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。

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。

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、利用可能な状況にしていた。

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。

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。

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。

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) 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。

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) 「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）

時間外処理連絡票を閲覧した結果、日次処理の取消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。

そのため、適切な夜間バッチ処理を実行する観点から、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) 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）

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。

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) 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）

執務室内に設置された端末に導入された更新ツールは、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。

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。

#### (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）

ポイント発行端末の読み取りエラーが認められた場合、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続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。

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續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) 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。

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。

#### (カ) システムのデータのバックアップについて

##### (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。

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。

### (キ) 緊急時用のバックアップシステムについて

#### (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）

住民記録情報システム及び総合窓口システムのバックアップツールは、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。

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。

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) 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ター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、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。

各所管課は、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。

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) 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。

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。

(ウ) コンピュータウイルス対策ソフトについて

(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。

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。

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、プラネタリウム投影システムの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。

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。

したがって、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する必要がある。

(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、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。

したがって、スポーツ課は、当該端末による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。