６．情報システム

（１）概要

①情報システムの概要

情報システムの監査は、企業会計及び料金システム（以下「企業会計システム等」）を対象範囲とした。

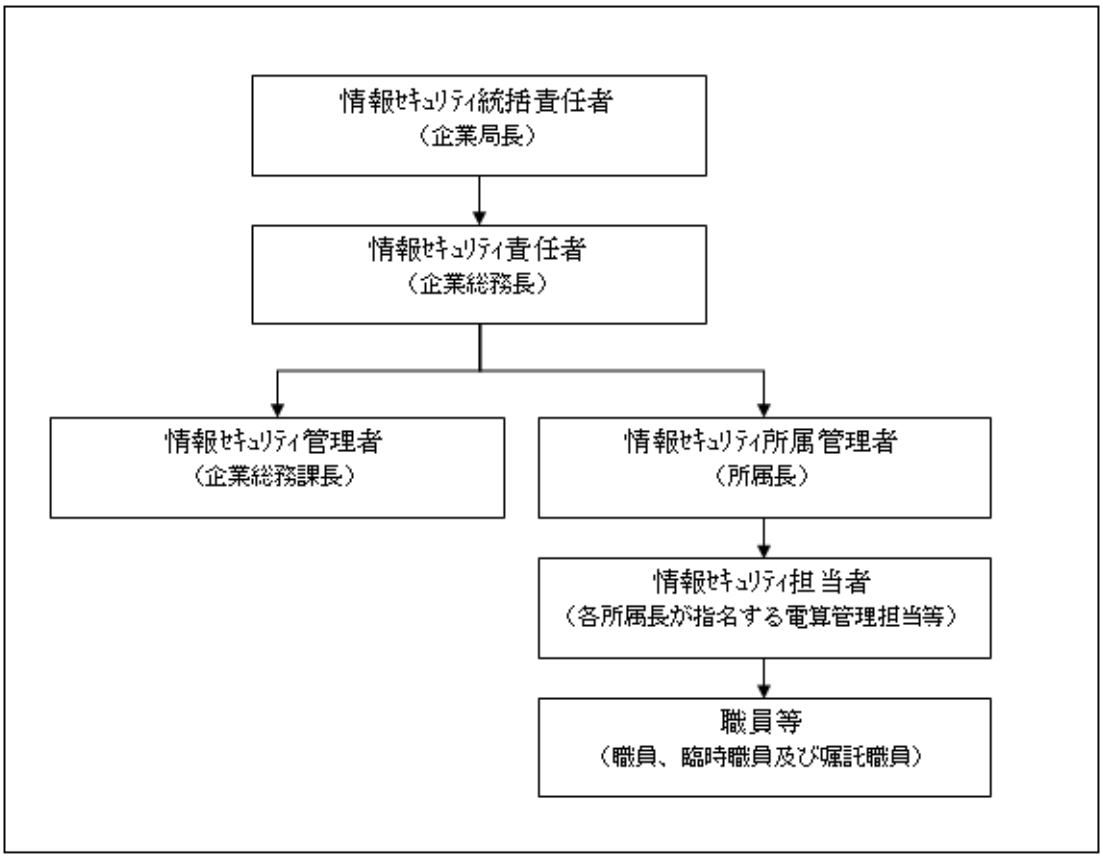
企業局では、主なシステムとして、基本的業務（新設改造工事、開閉栓申込、検針、調定、収納、未収整理）、メンテナンス業務（ガス安全点検、修繕工事、メーター定期取替）、及び還付業務等を扱う料金システムと、予算編成業務、収入管理業務、支出管理業務、決算管理業務等を扱う企業会計システムを利用している。料金システムから企業会計システムへはデータの自動連携を行っていない。

なお、料金システムとは、水道・ガス・下水道料金システム、未収金管理システム、オーダーシステム、水道・ガス修繕工事管理システム、ガス安全点検システム、汎用集計システム、用途別水道統計システム、ガス使用量実績表作成システム、ガス事業統計システム、ガス試算システムの総称である。

②情報システムの管理体制

（ア）情報システムに関する組織体制

情報システム（情報セキュリティ）に関する組織体制は、以下のとおりである。



注：平成 27 年度における組織体制を記載している。

（イ）情報資産の管理

情報資産の範囲と情報資産の例は以下のとおりである。

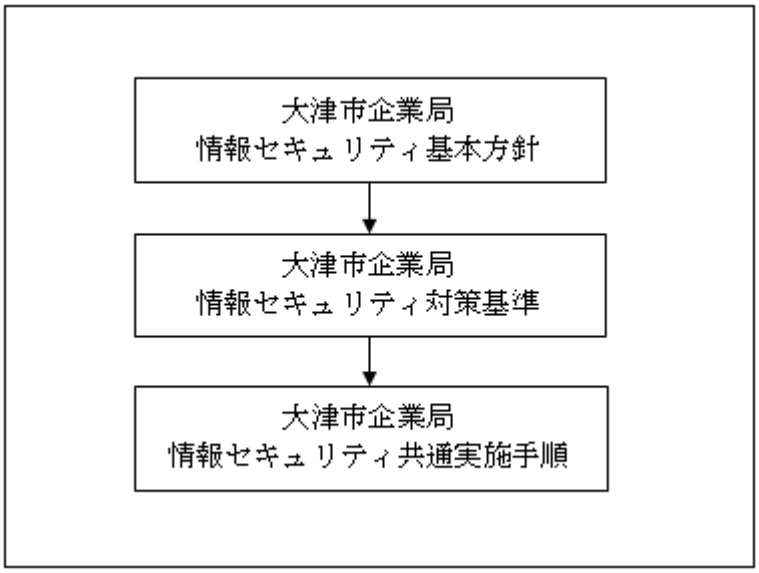
情報資産の種類	情報資産の例
ハードウェア	サーバ、クライアント（パソコン）、ハンディターミナル、プリンタ、記録媒体等
ソフトウェア	オペレーティングシステム、業務プログラム等
ネットワーク	通信回線、ルータ、ハブ等の通信機器
情報システム等	ハードウェア・ソフトウェア・ネットワークに掲げる情報資産で構成され、業務処理を行う仕組（等とは、人の知識や経験「人的資産」）
これらに関する施設及び設備	新館４階、５階のサーバ室及びその他コンピュータ室、通信分岐盤、配電盤、通信ケーブル
記録媒体	CD-R、DVD-R、USB メモリー、MO、LTO 等
ネットワーク及び情報システムで取り扱う情報	ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

注：平成 27 年度における情報資産の種類・例を記載している。

③情報セキュリティ

（ア）規程の体系

情報セキュリティに関する規程の体系は次のとおりである。



④物理的セキュリティ

（ア）サーバ室の入退室管理等

サーバ室へは、IC カードにより許可された者のみ入室できるように制限を行っている。また、サーバ室には、停電等による電源供給の停止に備えた予備電源が備え付けられ、定期的な点検を実施している。さらに、サーバ室には、耐震、防火、防水、温湿度管理等の対策を実施している。

⑤人的セキュリティ

（ア）パソコン等の持ち出し等による情報処理作業の制限等

企業局が保有するパソコン及び記録媒体等を庁舎外に持ち出してはならない。業務上必要な場合は、情報セキュリティ所属管理者及び情報セキュリティ管理者の許可を得るようにしている。

また、私物のパソコン及び記録媒体等を庁舎内に持ち込み情報処理作業を行ってはならない。業務上必要な場合は、情報セキュリティ所属管理者及び情報セキュリティ管理者の許可を得るようにしている。

⑥技術的セキュリティ

（ア）ユーザ ID 及びパスワード管理

システムへのログインには、ユーザ ID 及びパスワードによる認証が要求される仕組となっている。ユーザ ID ごとに権限設定を行っており、共用 ID は設定していない。

（イ）プログラム変更管理

プログラムを変更する場合には、依頼票等に基づき外部委託先が実施しており、対応内容については、定例会等において確認している。

（ウ）バックアップデータの保管及び復旧体制

企業会計システム等の情報について、定期的にバックアップを行っており、バックアップテープについては遠隔地で保管している。

⑦システム運用

（ア）障害管理

障害等が発生した場合には、外部委託先に対応を依頼するため、依頼票等を作成しており、対応内容については、定例会等において確認している。

⑧外部委託先管理

（ア）契約書及び仕様書

情報システムの運用、保守等を外部に委託する場合は、委託事業者との間で必要に応じて、次の情報セキュリティ要件を明記した契約を締結しなければならないとされている（「大津市企業局情報セキュリティ対策基準」7-4 外部委託）。

（ⅰ）情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
（ⅱ）委託先の責任者、委託内容、作業者、作業場所の特定
（ⅲ）提供されるサービスレベルの保証
（ⅳ）従業員に対する教育の実施
（ⅴ）提供された情報の目的外利用及び受託者以外の者への提供の禁止
（ⅵ）業務上知り得た情報の守秘義務
（ⅶ）再委託に関する制限事項の遵守
（ⅷ）委託業務終了時の情報資産の返還、廃棄等
（ⅸ）委託業務の定期報告及び緊急時報告義務

（ｘ）企業局による監査、検査
（xi）企業局による事故時等の公表
（xii）情報セキュリティポリシーが遵守されなかった場合の規定

企業会計システム等に関する運用・保守等の委託契約においては、再委託又は下請の禁止、情報管理担当者の指定、秘密の保持、業務遂行の方法等が規定されている。また、個人情報取扱特記事項を明記しており、秘密の保持、個人情報取得の制限、適正管理、情報の廃棄、目的外利用及び提供の禁止、再委託の禁止、資料等の返還、従事者への周知、個人情報取扱いの状況調査、事故報告などについて定められている。

（イ）定期的な報告に対する確認
外部委託先との定例会等において、外部委託先の業務内容について定期的な報告を受け、確認を行っている。

⑨情報システムの調達
（ア）料金システムの調達予定
料金システムは、平成 16 年の運用開始から 10 年以上経過しており、度重なるシステム改修により、システム仕様の複雑化・ブラックボックス化やシステム改修リスクの増大、また情報システムの維持・管理に係るコストの高止まり、業務自体の非効率化など多くの課題を抱えている。システム改修のリスク低減や経常的な運用コストの削減、事務の効率化を図るため、料金システムの再構築を実施している。
料金システムの調達における主な概要は以下のとおりである。

実施範囲	料金システムの基本的業務（新設改造工事、開閉栓申込、検針、調定、収納、未収整理）、メンテナンス業務（ガス安全点検、修繕工事、メーター定期取替）、還付（過誤納）等の機能が実施範囲である。企業会計システム及びマッピングシステムとの連携に係る部分を含む。
調達スケジュール	平成 29 年 1 月から稼働開始とする。
システム開発方針	導入するシステムはパッケージソフトで構築することが望ましい。

カスタマイズ方針	原則、ノンカスタマイズとすることにより、システム導入・維持費用の低減、パッケージソフトの品質と保守性を担保する。
ハードウェア方針	原則、既存クライアント端末及びプリンタ、ハンディターミナルを利用すること。

（イ）企業会計システムの調達予定

企業会計システムは平成 16 年に運用を開始しており、次期システムの調達は、平成 31 年４月を予定しており（平成 30 年 10 月から一部利用開始予定）、次期システムの調達に関する仕様等は、検討中である。

（２）実施した監査手続

企業会計システム等を対象に、所定の質問書に基づき、担当者への質問、及び関連証憑の閲覧、実機観察、サーバ室の視察を実施した。確認項目、質問内容、手続の概要は、以下のとおりである。

確認項目	質問内容	手続
情報システムの管理体制	情報システムについて、組織体制、権限及び責任が明確となっているか。 情報資産について、重要度に応じた分類がなされ、分類に応じた適切な管理が行われているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問
情報セキュリティの評価見直し	情報セキュリティポリシーや対策基準に基づき、自己点検や監査が行われているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問
物理セキュリティ	情報システム室への入退室が制限されているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問 ・サーバ室の視察
人的セキュリティ	電磁的記録媒体、情報資産及びソフトウェアを、外部に持ち出す、もしくは外部から持ち込む場合、責任者により許可を得ているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問

確認項目	質問内容	手続
技術的セキュリティ	ユーザ ID 及びパスワードの管理が適切に行われているか。オペレーティングシステムの ID など管理者権限を有する ID について、外部委託先が常時利用できないよう制限しているか。 プログラム変更時に必要なドキュメントが保管されているか。 定期的なバックアップが実施され、バックアップ媒体が遠隔地等に適切に保管されているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問 ・実機観察
システム運用	障害が発見された場合、職員等によって、直ちに責任者に報告されているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問
外部委託先管理	外部委託事業者との間で締結される契約書に、必要に応じた情報セキュリティ要件が明記されているか。 外部委託事業者におけるセキュリティ対策の確保が確認され、必要に応じ業務委託契約に基づく措置が講じられていることを定例報告等により確認しているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問
情報システムの調達	情報システムの調達に関する手続の流れが明確となっているか。必要とされる技術的な要件（目的、機能要件、運用・保守要件、セキュリティ要件等）が調達仕様書に明記されているか。 購入やリース等の調達方法、競争入札や随意契約等の調達方式の検討をどのように行っているか。 ライフサイクルコストを意識した導入を行っているか。情報システム調達後の効果測定をどのように行っているか。	・規程類、証憑類の閲覧 ・質問書に基づく質問 ・次期システムの調達仕様書の閲覧、及び質問

（3）監査の結果及び意見

①情報資産の台帳管理の不備について（結果）

「大津市企業局情報セキュリティ対策基準」（以下、「対策基準」という）において、企業局における情報資産は、機密性、完全性及び可用性により、以下の重要性分類に従って分類することとされている。

分類区分	内容
Ⅰ	個人情報及びセキュリティ侵害が市民・お客様の生命、財産等への重大な影響を及ぼす情報
Ⅱ	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報
Ⅲ	外部に公開する情報のうち、セキュリティ侵害が行政事務の執行等に微妙な影響を及ぼす情報
Ⅳ	上記以外の情報

更に、対策基準においては、上記の分類区分に応じた具体的な管理方法が定められている。

上述のように、情報資産について重要性に応じた分類を行い、その分類に応じた適切な管理を実施するためには、その前提として、企業局において、どのような情報資産が存在するのかを網羅的に把握することが必要であるが、USB メモリーに関する台帳が作成されているのみであり、情報資産を網羅的に把握した台帳等は作成されていない。

そのため、情報資産の分類が行われず、管理体制等が不十分な場合、情報の漏えいや紛失等の情報セキュリティ事故の発見が遅れる、気付かないなどの事態が生じる可能性がある。

重要性分類、及び分類に応じた適切な管理を行うため、情報資産の台帳を作成するなど網羅的に情報資産を把握する必要がある。

②情報セキュリティに関する監査及び自主点検の未実施について（結果）

対策基準において、情報セキュリティに関する監査や自主点検が次のとおり規定されている。

(監査)

情報セキュリティ責任者は、情報セキュリティ監査責任者を指名し、ネットワークや情報システム等の情報資産における情報セキュリティ対策状況について、定期的に監査を行わなければならない。

（自主点検）

情報セキュリティ管理者及び情報セキュリティ所属管理者は、所管するネットワークや情報システム等の情報資産について、定期的又は必要に応じて自主点検を実施しなければならない。

対策基準において、監査及び自主点検を実施すべきとなっているが、対策基準を制定して以降、一度も実施されていない。

そのため、情報セキュリティポリシーの遵守状況の確認が適時に実施されず、情報セキュリティ対策が徹底されない状態や、情報セキュリティ対策が業務運用にそぐわない状態が継続する可能性がある。

情報セキュリティに関する監査及び自主点検について、実施時期を定めた上で、計画的に実施する必要がある。

③パスワード変更に関する周知の不徹底について（意見）

対策基準において、パスワードの取扱いが以下のとおり規定されている。

①	職員等は、パスワードは、他者に知られないように管理しなければならない。
②	職員等は、自己の管理するパスワードを秘密にし、パスワードの照会等には一切応じてはならない。
③	職員等は、パソコン等のパスワードの記憶機能を利用してはならない。
④	職員等は、パスワードは定期的に、又はシステムへのアクセス回数に基づいて変更しなければならない。また、他人に解読されないよう想像しにくいものにしなければならない。
⑤	職員等の間でパスワードを共有してはならない。
⑥	仮のパスワードは、最初のログイン時点で変更しなければならない。
⑦	複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑧	パスワードが流出した恐れがある場合は、速やかに情報セキュリティ所属管理者に報告し、パスワードを変更しなければならない。

パスワードの変更に関しては、④において、定期的に、又はシステムへのアクセス回数に基づいて変更しなければならないとされており、⑥において、仮のパスワードは、最初のログイン時点で変更しなければならないとされている。現行のシステムでは、有効期限を設定し定期的にパスワードを強制変更させる機能や、初回ログイン時に強制変更する機能が備わっていない。利

用者に対してパスワード変更の周知徹底は行っているが、利用者に対して変更した旨の確認までは実施していない。

そのため、パスワードの変更が行われておらず、仮に漏洩した場合、情報システム等が不正に利用される可能性がある。

システム上の機能として備わっていない場合には、利用者に対して周知徹底した上で、利用者に対して変更した旨の確認を行うなど業務運用上の措置を講じる必要がある。なお、次期システムの要件を検討する際には、システム上の機能として具備できるように対処する必要がある。

④料金システムにおけるプログラム変更時のドキュメント保管について（意見）

現行の料金システムでは、システム導入時において、プログラム変更時に保管すべき文書が明確に決まっていなかったこともあり、システム導入時からのプログラム改訂履歴が網羅的に残されていない。

そのため、次期システムに要求する機能要件を洗い出す際に、調査に時間がかかるなどの支障が生じている。

次期システムの導入時には、プログラム変更時に保管すべき文書を外部委託先と明確に定めた上で、プログラム改訂履歴を適切に保管すべきである。

⑤情報システムの調達について

（ア）情報システムの調達に関する規程の整備（意見）

情報システムの調達に関して、企業局電子計算組織の利用及び管理に関する事務取扱要領第 14 条及び第 15 条に基づき、「電算化・OA 機器導入に伴う事務フロー図」（以下「フロー図」という）が作成されている。フロー図では、事務の流れについては明確になっているものの、標準的に具備すべきシステム要件や、保管すべき文書等、具体的な手順までは記載されていない。

そのため、情報システムの調達に関する手続が属人的になり、標準的に具備すべきシステム要件等が仕様に盛り込まれない可能性がある。

手続が属人的になることを避け、標準的に具備すべきシステム要件等が仕様に確実に盛り込まれることを担保するため、情報システムの調達に関する規程を作成すべきである。

（イ）情報システムの調達における効果測定（意見）

情報システムの調達においては多額のコストがかかることが想定され、平成 29 年１月に調達された料金システムにおいては、平成 27 年度から平成 36 年度までの 10 年間で、導入時の初期費用及び運用保守費用込みで、約２億６千万円の支出が見込まれている。

情報システムの調達では、システム調達後、当初期待した調達コストに見合う効果が上がっているかどうかを検証すべきである。その結果、期待した効果が上がっていない場合には、その原因を分析し、次期システムの調達に役立てることが有用である。なお、検証方法については、利用者に対してアンケートを取るなどの方法が考えられる。

⑥委託契約における駐在社員の情報セキュリティ対策の不徹底について（結果）

企業局では、お客様センター業務を株式会社ジェネッツに委託しており、検針業務、窓口収納・受付業務及び関連業務、電話応対業務、ハンディターミナルデータ処理業務、滞納整理業務並びに給水停止及びガス供給停止業務を委託している。受託者の駐在社員は、個人情報などの情報資産を取り扱っているが、契約書において個人情報取扱特記事項が定められているだけである。一方、企業局の職員に対しては、対策基準において、物理的セキュリティ、人的セキュリティ、技術的セキュリティなど、個人情報の取扱を含む情報セキュリティに関する遵守事項が詳細に定められている。受託契約における駐在社員は、企業局の職員と同様に情報資産を取り扱っているため、両者において情報セキュリティに関するリスクに大きな差異はない。

駐在社員に対して、企業局の職員と同等の情報セキュリティポリシーを適用すべきところ、対策基準において、情報セキュリティポリシーの遵守主体は、職員、臨時職員及び嘱託職員とされており、駐在社員については明確に記載されておらず、不明確な取扱いとなっている。また、駐在社員について、誓約書を提出させているが、個人情報保護の遵守に関する誓約であり、企業局の職員と同等の情報セキュリティポリシーを遵守させることを担保するものではない。

そのため、駐在社員による情報資産の管理が適切に実施されなかった場合、情報の漏えいやセキュリティ事故が生じる可能性がある。

駐在社員についても、企業局の職員と同等の情報セキュリティポリシーを適用する必要がある。

⑦情報システム関連費用の市との一括調達について（意見）

一般的に、調達に係る契約を締結する場合、調達数量が多くなるほどスケールメリットが生じるため調達価格が低減すると考えられる。市長部局と企業局とが一括調達することによって、スケールメリットが生じるような情報システム関連費用の調査を実施した。ウィルス対策ソフトやネットワークセキュリティ統合管理ツールについては一括調達済であったが、以下の案件については一括調達がなされていなかった。

（単位：千円）

件名	金額	備考
一人一台端末	12,471	一括調達は実施されていない。 平成 24 年度実績ベースでの試算額を記載している（企業局試算）。
プリンタ（複合機）	3,404	一括調達は実施されていないが、平成 29 年度から市長部局・企業局で一括調達することが決定している。 平成 26 年度実績ベースでの試算額を記載している（企業局試算）。
サーバールームの空調機電気代	919	一括調達は実施されていない。 設置機器の定格容量を基にインターネットを用いて試算した金額を記載している（企業局試算）。

OA 機器（一人一台端末、プリンタ、サーバや通信機器等）については、一括調達は実施されていなかった。

市と OA 機器の一括調達を実施することにより経費削減が見込める可能性があるため、経費削減効果を試算し、OA 機器の一括調達について市長部局と協議を進めるべきである。また、サーバールームについても、市長部局と統合することで、空調に係る経費（電気代・保守）並びに入退室管理システムに係る経費（保守）の削減効果が見込めることから、市長部局と協議を進めるべきである。