画は立案されておらず、不十分である。

②　指摘事項及び意見

スキルの明確化や年度別教育研修計画を立案し、実行していくことが望まれる。また、京都府内での研修体制の構築が難しい場合には、外部で開催される研修なども組み合わせて実施することを検討すべきである。

(7)　情報システムに関する責任者への報告体制について

①　現状

情報システムの開発・変更、運用などについて、年度ごとに計画・実行・評価を行う必要がある。その結果を政策企画部長や担当副知事に定期的に報告することで、中長期的な観点から情報システムをコントロールすることができる。

ところが、実際にはそのような定期的な報告等は実施されていない。

②　指摘事項及び意見

情報システムの開発・変更、運用などについて、定期的な報告体制の整備を検討する必要がある。

2.3　各システムの監査について

2.3.1　システム監査の着眼点と実施した手続について

監査の着眼点については、「(1)　情報システムの開発・変更管理」「(2)　情報システムの運用管理」「(3)　情報システムのセキュリティ管理」「(4)　災害対策、業務継続計画」という４つの観点から実施した。それぞれを監査対象とした理由及び具体的な実施項目は下記のとおりである。

(1)　情報システムの開発・変更管理

情報システムの開発・変更とは、例えばシステムの新規開発やプログラムの変更のことを言う。開発・変更時にプログラム上に欠陥が発生した場合、システム障害の発生による業務の停止や、データ改ざん・データ漏洩等が発生する可能性がある。

そのため、開発・変更管理は情報システム管理上重要なものであり、包括外部監査の目的にも適すると判断したため、監査対象とした。

なお、本項目については次の事項に沿って検討を進めた。

①ルールの整備状況（ルールとは、規程や手順を指す。以下同じ。）

②開発・変更作業の実施状況

③開発・変更作業の管理及び承認

④テスト実施状況の管理

⑤本番移行の管理

(2)　情報システムの運用管理

情報システムの運用とは、プログラム実行・処理のことを言い、プログラムが問題なく実行・処理されるための管理が必要となる。運用管理には、定例的なプログラム実行が問題なく行われていることの管理や、不正処理につながるようなプログラム実行が行われないことの管理、障害発生によるプログラム実行が停止したときの対応等が含まれる。

プログラムが正しく実行されない場合、システム障害の発生による業務の停止、不正処理の実行によるデータ改ざん・データ漏洩等が発生する可能性がある。

そのため、運用管理も同様に監査対象とした。

なお、本項目については次の事項に沿って検討を進めた。

①ルールの整備状況

②システム運用状況の管理（障害管理・例外処理実行管理・不正プログラム実行防止含む）

③ソフトウェア・ハードウェア・ネットワークの構成、調達管理

(3)　情報システムのセキュリティ管理

情報システムのセキュリティとは、データ改ざん・データ漏洩等を防止するものである。そのため、これも情報システム管理上重要なものであり、監査対象とした。

なお、本項目については次の事項に沿って検討を進めた。

①ルールの整備状況

②情報セキュリティに関する教育・訓練

③アクセス管理１（ID・パスワード等のアクセス制限による技術的な管理）

④アクセス管理２（データ改ざん、不正持ち出し等の防止）

⑤アクセス管理３（サーバルームやマシンルームへの立ち入りの管理）

(4)　災害対策、業務継続計画

災害発生時の情報システムのダウン防止、もしくはダウンしたとしても適時の復旧は、情報システムを使用する

上で重要であり、災害発生時に情報システムが使用できない場合、京都府の業務や府民生活に重大な影響を及ぼす可能性がある。そのため、これも監査対象とした。

なお、本項目については次の事項に沿って検討を進めた。

①災害のリスク分析の状況

②業務継続計画の策定

③復旧対策の現状（バックアップ体制等）

着眼点毎に、詳しい内容と実施した手続を、以下で記載する。

また、外部委託事業者も情報システムの管理に重要な役割を果たしているため、外部委託事業者担当者にもヒアリングする他、必要に応じて外部委託事業者が保管している資料の閲覧を行っている。

外部委託事業者の管理状況は「2.4 外部委託事業者の管理について」で検討を行う。

（参考）各システムの外部委託事業者は下記のとおりである。

【図表2.3.1】

システム	外部委託事業者
新人事給与	オムロンパーソネル㈱
	㈱ワークスアプリケーションズ
人事	㈱ケーケーシー情報システム
教職員人事電算	㈱ジェーワンシステム京都支店 ケイアイエスユー㈱
税務支援	日本電気㈱京都支社
行政事務支援	㈱大塚商会京都支店
	㈱アルファネット （㈱大塚商会の連結子会社）
統合財務	㈱オーイーシー
総務事務	富士電機㈱関西支社
	㈱グローバルソフトウェア
衛星通信系防災情報	沖電気工業㈱京都支店
	㈱OKIソフトウェア（沖電気工業㈱の連結子会社）
	㈱沖電気カスタマアドテック （沖電気工業㈱の連結子会社）

2.3.2　情報システムの開発・変更管理について

⑴　ルールの整備状況

①　現状

情報システムの開発・変更管理に関する規程として、対策基準「6⑸システム開発、導入、保守等」がある。

情報システムの開発・変更管理に関する事項が、下記のとおり規定されている。

ア　情報システムの調達
㋐　情報システムの調達（更新を含む。）を実施する場合、情報システム管理者は予算要求前、調達実施前、運用開始前の各段階で、セキュリティ確保方法についてIT推進本部と協議しなければならない。
㋑　情報システム管理者は、情報システムの機器及びソフトウェアの調達に伴う仕様書の作成については、情報セキュリティ対策上支障が生じるおそれのある内容を記載しないようにすること。
㋒　情報システム管理者は、機器及びソフトウェアを調達する場合は、当該製品の安全性及び信頼性を確認すること。
イ　情報システムの開発
情報システムの開発を行う場合、次の事項を実施するものとする。
㋐　情報システムの開発、保守等に関する事故及び不正行為に係るリスク（危険性）について十分検討を行うこと。
㋑　プログラム、設定等のソースコードを整備すること
㋒　セキュリティの確保に支障が生じるおそれのあるソフトウェアは使用しないこと。
㋓　情報システムの開発及び保守に係る記録を作成するとともに、運用、管理等に必要な説明書等の書類を定められた場所に保管すること。
㋔　不要になったユーザ名、パスワード等は、速やかに抹消すること。
ウ　ソフトウェアの更新及び保守
情報システム管理者は、独自開発ソフトウェア及びOS等を更新又は修正プログラムを導入する場合は、不具合が無いこと及び他のシステムとの適合性の確認を行った上で、計画的に更新又は導入すること。
エ　管理記録
情報システム管理者は、所管する情報システムにおいて行ったシステム変更等の作業については、記録を作成し適切に管理を行うものとする。

②　指摘事項及び意見
この内容及びその他の規程を閲覧・検討した結果、ルールの整備状況について、下記の問題点が発見された。
㋐　具体的な規程が未整備である（８システム共通）
対策基準においてシステムが正常に稼動するために、例えば「情報システムの開発、保守等に関する事故及び不正行為に関するリスク（危険性）について十分検討を行うこと」「プログラム、設定等のソースコードを整備すること」といった、当然に守られるべき事項が記載されている。しかし、対策基準に定めた事項が遵守されるための、具体的な管理事項を定めた規程がない。
少なくとも、以下の事項を規程に定める必要がある。
（規程化すべき事項）
・開発・変更に関する依頼方法及び依頼内容の保存方法
・開発・変更にかかる記録（テスト結果や承認記録）の結果の保存方法
・検証環境と本番環境の分離
・本番移行の管理方法（誰が本番移行作業を行い、誰が移行作業に立ち会うか等）
・開発・変更結果を承認するにあたり検討すべき事項
などである。
なお、以下において各システムの実際の管理状況を検討したが、各システムの管理水準は統一されていない事項があり、その要因として上記事項を定めた規程がないことが考えられる。
㋑　外部委託事業者における規程が未整備である（教職員人事電算システム）
上記㋐で指摘したとおり、京都府において規程を適切に整備していない状況であるが、一方で京都府の情報システムの開発・変更を担う外部委託事業者も、業務の適切な遂行を考慮すれば当然に関連規程を整備する必要がある。京都府も外部委託事業者に対してそのように指導すべきであり、外部委託事業者において少なくとも京都府が要求する水準の管理体制を整えるよう監視する必要がある。
そのため、外部委託事業者に対しても、社内における規程の整備状況についてヒアリングを行い、また、可能な限り社内資料を閲覧して、京都府が要求する水準を満たすような規程の整備が行われているか確認した。
結果、大半の外部委託事業者では社内で規程を整備している状況にあったが、教職員人事電算システムにかかる外部委託事業者（㈱ジェーワンシステム）は、社内で規程を整備していないとの回答であった。
なお、この状況について教職員課に見解を確認したところ、京都府教職員人事電算システムに関する情報セキュリティ実施手順を遵守させており、問題ないとの回答であった。しかし、当実施手順には開発・変更に関する事項は何ら規定されていないため、外部委託事業者において開発・変更に関する規程は存在しないと言わざるを得ない（詳細については「2.5教職員課について」で後述する。）。

⑵　情報システムの開発・変更作業の実施状況について
①　開発・変更依頼について
ⅰ　現状

変更依頼については、適切な変更要求（例えば業務遂行に不要な変更要求、不正処理を目的とした要求ではないこと。）が行われ、かつ、依頼に基づいた作業が行われたことを記録する必要がある。

京都府の各システムでは、各所管部署が外部委託事業者に開発・変更を依頼し、外部委託事業者が作業を行う。そのため、京都府から外部委託事業者への依頼方法及び依頼文書の保存状況について検討した。

（注）下記において「京都府担当者」といった表現を行っているが、これは情報システム管理者及び情報システム責任者以外の京都府職員という意味で用いている。

【図表2.3.2-1】

システム	実施状況
新人事給与	当システムでは、外部委託事業者(オムロンパーソネル㈱)と業務所管課（情報政策課・給与厚生課など）との調整の上、バージョンアップ対応のみ行っているため、京都府からの変更依頼によるものはない。
人事	京都府人事課担当者が、「要件確認書兼質問確認連絡書」に変更依頼内容を記載して、メールで外部委託事業者（㈱ケーケーシー情報システム）に変更依頼を行っている。 （参考） 開発は人事異動時期に合わせて、例年３月に集中する。
教職員人事電算	京都府教職員課担当者が、連絡票に変更依頼内容を記載して、メールで外部委託事業者（㈱ジェーワンシステム）に変更依頼を行っている。 （参考） 開発は人事異動時期に合わせて、例年３月に集中する。
税務支援	京都府税務課担当者が、連絡票に変更依頼内容を記載して、メールで外部委託事業者（日本電気㈱）に変更依頼を行っている。
行政事務支援	京都府情報政策課担当者が、メールに変更依頼内容を記載して、外部委託事業者（㈱大塚商会京都支店）等に変更依頼を行っている。
統合財務	業務所管課（情報政策課、会計課など）担当者が口頭もしくはメールで依頼を行うが、後日、業務所管課担当者と外部委託事業者（㈱オーイーシー）が変更内容について打ち合わせを行い、その内容を議事録として外部委託事業者が取りまとめており、その議事録を情報システム管理者が確認している。
総務事務	京都府情報政策課担当者がメールで外部委託事業者（富士電機㈱）に変更依頼を行っている。
衛星通信系防災情報	変更の都度、外部委託事業者（沖電気工業㈱）と契約を締結していることから、契約内容の打合せ等を通じて、具体的な変更依頼を行っている。

ii　指摘事項及び意見

㈠　依頼方法等が不統一である（８システム共通）

情報システムの開発・変更依頼は、各所管部署で共通の方法によることが望ましい。なぜなら、情報システムの開発・変更を束ねる情報政策課が迅速かつ的確に開発・変更の内容を把握するためには、共通の方法で依頼が行われている必要があるからである。また、職員の異動がある際、部署ごとに異なる開発・変更依頼方法であれば、部署ごとの方法に慣れるまでの時間が無駄である。

ところが京都府においては、上記のとおり、変更依頼はメールによるものが多かったが、依頼方法は各システムで統一されておらず、また、依頼文書の保存も統一されていなかった。これでは、情報政策課による一元管理が非効率になり、また、職員の異動の際に部署ごとの方法に習熟するまでの時間も無駄になり、問題がある。

依頼方法及び依頼文書の保存は各システムで統一させることが望ましい。

(ｲ)　変更依頼内容の管理が不十分である（８システム共通）

いつ、誰が、どのような、情報システムの開発・変更依頼を行ったかについては、漏れなく管理している必要がある。そうしなければ、どの開発・変更依頼が完了し、どれが未了かを迅速・正確に把握することができないからである。

ところが、京都府においては、メールだけによる変更依頼及び依頼文書の保存しか、行っていない。メールだけによる依頼及び依頼文書の保存を行った場合、変更依頼したメールが他のメールと紛れてしまって、後々依頼内容を確認することが困難になるおそれがあり、問題である。

そのため、変更依頼の一覧表を京都府で作成して、後日外部委託事業者から報告される変更内容と突合できる状態にすることが望ましい。

②　作業実施手順について

ｉ　現状

開発・変更作業を実施する際に、案件に応じた作業実施手順を策定し、これに基づいて作業を行うことが必要であり、その際には担当者による確認が必要である。そのため、各システムにおける手順策定状況を検討した。

【図表2.3.2-2】

システム	手順の設定状況
新人事給与	当システムでは、京都府からの変更依頼はなく、外部委託事業者（㈱オムロンパーソネル）の現場担当責任者がバージョンアップ対応要否を判断して、必要な項目のみアップデート対応を行っている。なお、アップデート前に業務所管課（情報政策課、給与厚生課など）担当者及び再委託先（㈱ワークスアプリケーションズ）と協議を行った上でテスト内容やスケジュールを決定し、業務所管課担当者の承認を得た上でアップデート作業を実施している。
人事	案件の都度、外部委託事業者（㈱ケーケーシー情報システム）が作業手順を決定している。また、京都府人事課への報告資料（要件確認書兼質問確認連絡書や業務報告書）などに作業手順を記載し、京都府人事課担当者がその手順を確認している。
教職員人事電算	案件の都度、手順を外部委託事業者（㈱ジェーワンシステム）で決定している。なお、京都府教職員課では作業手順の確認は行っていない。
税務支援	外部委託事業者（日本電気㈱）が手順を決定し、京都府税務課担当者がその手順を確認している
行政事務支援	外部委託事業者（㈱大塚商会）が手順を決定し、再委託先（㈱アルファネット）の現場担当責任者が承認を行う。 なお、京都府情報政策課担当者がその手順を確認している。
統合財務	外部委託事業者（㈱オーイーシー）が作業手順を決定する。また、業務所管課（情報政策課、会計課など）担当者と外部委託事業者が変更内容とともに作業手順について打ち合わせを行い、その中で業務所管課担当者が確認している。
総務事務	外部委託事業者（富士電機㈱）が作業手順を決定する。 開発・変更の都度、仕様を京都府情報政策課担当者と合意しながら進めるため、その打ち合わせの際に京都府情報政策課担当者が作業手順も確認している。
衛星通信系防災情報	外部委託事業者（沖電気工業㈱）が作業手順を決定する。また、開発・変更に係る契約内容の打合せ時に、京都府防災・原子力安全課担当者が作業手順を確認している。

ii　指摘事項及び意見

(ｱ)　担当者が作業実施手順を確認していないケースがある。(教職員人事電算)

情報システムの開発・変更を行う際の作業実施手順は、各所管部署の担当者が十分に把握していなければならない。なぜなら、作業開始から終了までのスケジュールが他の業務に与える影響については、外部委託業者には十分には把握できないからである。また、作業実施手順の内容を確認することで、不必要な作業等があることがわかり、当初の見積りが過大であったことがわかる可能性もあるからである。さらに、当初計画していたスケジュールどおりに情報システムの開発・変更が完了するかどうかを把握することも大切である。

ところが、教職員人事電算システムにおいては、各所管部署の担当者が作業手順の確認を行っていなかった。これでは、他の業務に影響を与える作業の有無を把握することができないし、不要な作業の有無もわからない。また、当初の計画通りのスケジュールで開発・変更が完了するかどうかも分からない。

よって、作業手順については担当者も確認を行い、不要な作業が行われていないか確認するよう改善が必要である。

(ｲ)　担当者が本質的な確認が出来ていないおそれがある（８システム共通）

各所管部署における情報システム担当者が、情報システムの開発・変更を把握し、作業実施手順の内容の妥当性を判断するためには、相応の知識・能力・経験が必要である。具体的には、情報政策課が実施する研修を修了した情報セキュリティ操作認定者であることが、その最低条件であると考えられる。

ところが、情報政策課以外で所管しているシステムについて、担当者の中には情報セキュリティ操作認定者でない者がおり、情報システムの開発・変更を把握し、作業実施手順の内容の妥当性を判断することが困難なものと考えられる（「2.3.4　情報システムのセキュリティ管理について　(2)　情報セキュリティに関する教育・訓練（現状及び問題点）」の問題点２を参照いただきたい。）。

そのため、各所管部署の担当者は、最低限、情報政策課の研修を修了した情報セキュリティ操作認定者とするよう改善が必要である。

ただし、情報システムの開発・変更の内容によっては、情報セキュリティ操作認定者であるだけでは未だ知識・能力・経験が不足しており、開発・変更の内容を把握し作業実施手順の内容の妥当性を確認するのが困難なケースもあると思われる。

そのため、作業手順の確認は情報システムに精通した情報政策課職員が確認することが望ましい。また、この問題点は下記の開発・変更作業の管理及び承認、テスト実施状況の管理、本番移行の管理にも該当するため、開発・変更過程の要所において情報政策課が関与することを検討されたい。

(3)　開発・変更作業の管理及び承認について

①　現状

手順等が存在していても、実際にその手順どおりに作業されていなければ、不正な開発・変更が行われる可能性がある。そのため、その管理・承認状況について確認を行った。

【図表2.3.2-3】

システム	実施状況
新人事給与	開発・変更作業は、再委託先の開発元業者（㈱ワークスアプリケーションズ）で行う。作業結果の承認は外部委託事業者(オムロンパーソネル㈱)の現場責任者が承認している。 当該システムでは、上述のとおり京都府からの変更依頼はなく、外部委託事業者の業務責任者がバージョンアップ対応要否を判断して、必要な項目のみアップデート対応を行っている。アップデート前に業務所管課（情報政策課、給与厚生課など）担当者及び再委託先（㈱ワークスアプリケーションズ。開発・変更作業を担当）と協議を行った上でテスト内容やスケジュールを決定し、担当者の承認を得た上でアップデート作業を実施している。
人事	開発・変更作業は外部委託事業者（㈱ケーケーシー情報システム）が行う。承認は京都府人事課担当者が、動作確認を行ったうえで行っている。
教職員人事電算	開発・変更作業は外部委託事業者（㈱ジェーワンシステム）が行う。承認は京都府教職員課担当者が、動作確認を行ったうえで行っている。
税務支援	開発・変更作業は外部委託事業者（日本電気㈱）が行う。承認は京都府税務課担当者が行っている。
行政事務支援	開発・変更作業及び変更結果の承認は、外部委託事業者（㈱大塚商会）の各担当者が行う。承認は京都府情報政策課担当者が動作確認を行ったうえで行っている。
統合財務	開発・変更作業は外部委託事業者（㈱オーイーシー）が行う。承認は業務所管課（情報政策課、会計課など）担当者が、動作確認を行ったうえで行っている。
総務事務	開発・変更作業は外部委託事業者（富士電機㈱）が行う。承認は京都府情報政策課担当者が、動作確認を行ったうえで行っている。
衛星通信系防災情報	変更の作業状況管理は外部委託事業者（沖電気工業㈱）が行う。承認は京都府防災・原子力安全課担当者が動作確認を行ったうえで行っている。

② 指摘事項及び意見

ⅰ 情報システムの開発・変更に情報政策課の承認がなく規程に違反している（８システム及びその他のシステム共通）

「京都府電子計算組織等運用管理規程」において、各所管部署の「課長等は、その所掌する業務を電子計算組織を使用して新たに電算処理しようとするときは、適用業務システム開発協議書により情報政策課長の承認を受けなければならない」（第５条第１項）し、また「業務システムを変更又は廃止しようとするときは、適用業務システム変更（廃止）協議書により情報政策課長の承認を受けなければならない」（第７条）とされる。

したがって、情報政策課所管のシステムについて開発・変更する際は情報政策課長の承認を受けなければならないのはもちろんのこと、その他の所管部署のシステムについて開発・変更する際にも、情報政策課長の承認を所定の様式に従い受けなければならない。

ところが、実際の情報システム開発・変更の際には、情報政策課長の承認を必ずしも受けておらず、「京都府電子計算組織等運用管理規程」に反しているため、問題がある。情報システムの所管が情報政策課以外であったとしても、「京都府電子計算組織等運用管理規程」にしたがって情報政策課の承認を受けるように改善しなければならない。

また、「京都府電子計算組織等運用管理規程」には定められていないが、実際の運用においては、開発・変

更作業プロセスの要所では情報政策課も各課担当者とともに作業内容の確認を行うことを検討されたい。

なお、当該問題点について情報政策課に見解を確認したところ、「京都府電子計算組織等運用管理規程」がホストコンピュータを使用していたときの規程であることから、規程が実態に即したものとはなっておらず、そのため規程を見直した上で規程を遵守する方針である、とのことであった。

⑷　テスト実施状況の管理

①　現状

テスト実施状況の管理は「⑶開発・変更作業の管理及び承認」の一環ではあるが、開発・変更作業のなかでも特に重要な手続きであるため、別途テストの実施状況について検討した。

【図表2. 3. 2-4】

システム	実施状況
新人事給与	ⅰ 再委託先の開発元業者（㈱ワークスアプリケーションズ）が府庁内の開発環境（本番環境とは異なる環境）でテストを行う（そのため、府庁外部へのデータ持ち出しはなし。）。 ⅱ 業務所管課（情報政策課、給与厚生課など）担当者とテスト方法を協議した後に、テストを実施。 ⅲ 開発元業者、業務所管課担当者、外部委託事業者（オムロンパーソネル㈱）の３者がテスト結果を確認。テスト結果の検証方法として、①実際の過去データを用いた計算結果が、変更前と一致するかをテストし、また、②変更点に関する仮データを作成してテストを実施。検証は担当者と委託先が分担を決めて検証している。 ⅳ テスト結果は開発元業者が保管
人事	ⅰ 外部委託事業者（㈱ケーケーシー情報システム）が自社の開発環境でテストを行う。 ⅱ テストの実施方針は、外部委託事業者で定めており、京都府人事課担当者は、実施方針を確認していない。 ⅲ テスト実施に際しては、実在するデータとは異なるテスト用データを利用して府庁内にある外部委託事業者の開発環境で作業を行い、その後、庁内LANを利用して府庁内の予備サーバに作業データを移してテストを行っている。 ⅳ 外部委託事業者の担当者がテスト結果の承認を行っている。京都府人事課担当者も動作確認によりテスト結果を確認している。
教職員人事電算	ⅰ 外部委託事業者（㈱ジェーワンシステム）が自社の開発環境でテストを行う。 ⅱ テストの実施方針を外部委託事業者で定め、京都府教職員課担当者も、実施方針を確認している。 ⅲ テスト実施に際しては、実在するデータを利用しており、人事システムの本番環境からUSBメモリで持ち出し、このデータを外部委託事業者の開発環境に取り込んで作業している（USBメモリ使用時の問題点については、後述の「2.3.4 情報システムのセキュリティ管理⑷アクセス管理 2（データ改ざん、不正持ち出しの防止」に記載している。）。 ⅳ 外部委託事業者の担当者がテスト結果の承認を行っている。京都府教職員課担当者は、自身が本番移行作業を行う際に確認している。

税務支援	ⅰ 外部委託事業者（日本電気㈱）が、府庁内の開発環境でテストを行う（そのため、府庁外部へのデータ持ち出しはなし。）。 ⅱ 京都府税務課担当者とテスト方法を協議した後に、テストを実施。 ⅲ テスト実施に際しては、実際のデータ（テスト実施時点から約１ヶ月前のデータ）を開発環境にコピーして行っている。 ⅲ 京都府税務課担当者及び外部委託事業者（開発担当者及び運用担当者）がテスト結果を確認。 ⅳ テスト結果は開発元業者が保管。
行政事務支援	ⅰ 外部委託事業者（㈱大塚商会）が、自社の開発環境でテストを行う。 ⅱ 京都府情報政策課担当者とテスト方法を協議した後に、テストを実施。 ⅲ テスト実施に際しては、開発環境にテストケースを想定したデータを作成したうえで、テストを行っている（そのため、府庁外部へのデータ持ち出しはなし。）。 ⅳ 京都府情報政策課担当者、外部委託事業者（開発担当者）及び再委託先（㈱アルファネット。システム運用を担当。）がテスト結果を確認。 ⅴ テスト結果は外部委託事業者が保管 ⅵ 本番移行前に事前にピーク負荷のテストを実施。
統合財務	ⅰ 外部委託事業者（㈱オーイーシー）が、自社の開発環境及び府庁内の開発環境でテストを行う。 ⅱ 業務所管課（情報政策課、会計課など）担当者とテスト方法を協議した後に、テストを実施。 ⅲ テスト実施に際しては、開発環境にテストケースを想定したデータを作成したうえで、テストを行っている（そのため府庁外部へのデータ持ち出しはなし。）。 ⅲ 業務所管課担当者、外部委託事業者の開発担当者及び運用担当者がテスト結果を確認。 ⅳ テスト結果は外部委託事業者が保管。 ⅴ 本番移行前に事前にピーク負荷のテストを実施。
総務事務	ⅰ 外部委託事業者（富士電機㈱）が社内の開発環境でテストを行う。 ⅱ 京都府情報政策課担当者とテスト方法を協議した後に、テストを実施。 ⅲ 京都府情報政策課担当者、外部委託事業者の開発担当者及び自社内の試験管理担当者がテスト結果を確認。 ⅳ テスト結果は外部委託事業者が保管。 ⅴ 本番移行前に事前にピーク負荷のテストを実施。

衛星通信系防災情報	ⅰ 外部委託事業者（沖電気工業㈱）が自社の開発環境でテストを行う。 ⅱ テストの実施方針は、外部委託事業者で定めており、京都府防災・原子力安全課担当者は実施方針を確認していない。 ⅲ テスト実施に際しては、開発環境にテストケースを想定したデータを作成したうえで、テストを行っている（そのため府庁外部へのデータ持ち出しはなし。）。ただし、外部委託事業者の開発環境から府庁内の本番環境へテスト結果データを USB メモリで取り込んでいる。この、USB メモリ使用時の問題点については、後述の「2.3.4 情報システムのセキュリティ管理(4)アクセス管理２(データ改ざん、不正持ち出しの防止」に記載している。 ⅳ 外部委託事業者の担当者がテスト結果の承認を行っている。京都府防災・原子力安全課担当者も動作確認によりテスト結果を確認している。

② 指摘事項及び意見

ⅰ テスト実施手順の確認が行われていない（人事）

開発・変更した情報システムについて、本番移行させる前に開発環境等でテストを実施する。これは、万が一、開発・変更した情報システムに不備があるにもかかわらず本番移行させた場合に、業務に重大なトラブルを生じさせてしまうからである。したがって、開発環境等におけるテストは、正しい手順により実施し、本番移行させても問題が発生しないかどうか細心の注意を払わなければならない。

ところが、人事システムにおいてテスト実施手順の確認が行われていなかったため、問題がある。テストが正しく実施されているか確認するために、テスト実施手順を確認する必要がある。

(5) 本番移行の管理

① 現状

開発・変更作業によって適正なプログラムが作成されたとしても、システムへの本番移行時に異なるプログラムを容易に移行できるような状況である場合、不正なプログラムや誤ったプログラムが混入する可能性がある。そのため、京都府の各システム担当者が本番移行作業を行うか、または本番移行作業に立ち会って作業状況を確認する必要がある。各システムにおける本番移行管理の状況について検討した。

【図表2.3.2-5】

システム	実施状況
新人事給与	開発元業者（㈱ワークスアプリケーションズ）が本番移行を行っている。また、本番運用開始までに業務所管課（情報政策課、給与厚生課など）において、本番移行作業に立ち会って状況確認を行っている。
人事	外部委託事業者（㈱ケーケーシー情報システム）が本番移行を行い、京都府人事課担当者（運用担当者）が本番移行作業に立ち会って状況確認を行っている。
教職員人事電算	京都府教職員課担当者（運用担当者）が本番移行作業を行っている。
税務支援	外部委託事業者（日本電気㈱）が本番移行を行い、京都府税務課担当者（運用担当者）が本番移行作業に立ち会って状況確認を行っている。
行政事務支援	再委託先（㈱アルファネット）の運用担当者が本番移行を行い、京都府情報政策課担当者及び外部委託事業者（㈱大塚商会）の開発担当者が本番移行作業に立ち会って状況確認を行っている。
統合財務	外部委託事業者（㈱オーイーシー）の運用担当者が本番移行を行い、業務所管課（情報政策課、会計課など）担当者が本番移行作業に立ち会って状況確認を行っている。
総務事務	外部委託事業者（㈱富士電機）の運用担当者が本番移行を行い、京都府情報政策課担当者が本番移行作業に立ち会って状況確認又は京都府情報政策課担当者が翌日に結果の確認を行っている。
衛星通信系防災情報	外部委託事業者（沖電気工業㈱）が本番移行を行い、京都府防災・原子力安全課担当者（運用担当者）が本番移行作業に立ち会って状況確認を行っている。

検討の結果、本項について問題点はなかった。

2.3.3　情報システムの運用管理について

⑴　ルールの整備状況

①　システム運用状況の管理に関するルール

対策基準「７運用及び緊急時におけるセキュリティ対策」において運用管理に関する事項が、下記のとおり規定されている。

⑴　情報システムの監視
ア　情報システム管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視し、障害が起きた際は速やかに対応するものとする。
イ　情報システム管理者は、外部ネットワークと常時接続するするシステムについては、ネットワーク侵入監視装置を設置する等厳重な監視を行うものとする。
ウ　情報システム管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視を行うものとする。
エ　情報システム管理者は、監視した結果を正確に記録するとともに、消去や改ざんをされないよう必要な措置を講じ、安全な場所に保管するものとする。
⑵　対策基準の遵守状況の確認
ア　職員等は、この対策基準に違反した場合又は違反事実を確認した場合は、直ちに情報セキュリティ責任者に報告するものとする。
イ　情報セキュリティ責任者は、対策基準の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めた場合には速やかに情報システム管理者及びIT推進本部に報告するものとする。
なお、情報システム管理者が支障を確認した場合には、迅速かつ適切に対処するものとする。

（注）「職員等」とは「情報資産に関する業務に携わるすべての職員（非常勤職員及び臨時職員等を含む。）及び委託等を受けて携わる者」を言う。以下「職員等」を対策基準において用いている場合は、同じ意味を指す。

また、具体的な管理手順については電子計算機運用管理要領や委託契約書の業務仕様書で定めているが、詳細は以下において検討する。

②　ソフトウェア・ハードウェア・ネットワークの構成管理及び調達管理に関するルール

対策基準「４⑴情報システム」において下記のとおり規定されている。

ウ　ネットワーク
㋐　ネットワーク回線は、傍受・損傷が受けることがないよう、可能な限りの措置を講じること。
なお、情報システム管理者等の許可無く、ネットワーク回線を変更、又は追加できないようにすること。
㋑　原則として無線LANの使用を禁止する。ただし、他の方法によることができない場合は、特殊な暗号処理を施す等の計画書を作成し、事前にIT推進本部の承認を受けるものとする。
６　技術的セキュリティ対策
⑴　機器構成変更の禁止
職員等は、情報システムの端末等に対して機器の増設、改造又はプロトコル（通信手順）の設定変更等を行わないものとする。
ただし、業務を円滑に遂行するためやむを得ない理由がある場合で、かつ情報システム管理者に申請し、事前の了解を得た場合についてはこの限りではない。
⑵　アクセス制御
ア　情報システム管理者は、情報システムにおけるアクセス制御について次の事項を遵守するものとする。
㋐　アクセス権限の許可は必要最低限とすること。
㋑　不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォールの設置等の適切なネットワーク経路制御を講じること。
㋒　アクセス方法等は職員等の真正性が確保できるものにすること。
イ　接続した情報通信機器についてセキュリティ上の問題があり、情報資産を脅かすおそれがあると認められる場合には、速やかに当該情報通信機器をネットワークから物理的に隔離するものとする。
⑶　外部ネットワークとの接続
府の情報システムと府以外の機関の情報システム（以下「外部ネットワーク」という。）との接続については、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を検討し、府の情報資産に影響が生じないことをIT推進本部が確認した上で接続を認めるものとする。
なお、接続に当たって、情報システム管理者は、次の事項を遵守するものとする。
ア　不正アクセスを防止するためのファイアウォールの設置や職員等の認証、論理的なネットワークの分割等適切なネットワーク経路制御を講じること。
イ　外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれが発生した場合は、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

⑵　システム運用状況の管理（障害管理・例外処理実行管理・不正プログラム実行防止含む）

①　運用計画の策定状況及び運用計画に基づく運用監視状況

ｉ　現状

システムを正常に運用するためには、予め運用計画（運用のスケジュール）を定めることにより、どのようなプログラムを実行するかを決定し、運用計画に基づくプログラム実行が正常に終了したことを確認する必要

がある。

そのため、各システムの状況について担当者及び外部委託事業者にヒアリングし、必要に応じて管理資料の検討を行った。

【図表2.3.3-1】

システム	実施状況
新人事給与	（運用計画） システムの仕様書に運用計画を定めている。この他、仕様書に記載されていない事項については、業務所管課（情報政策課、給与厚生課など）が定めた運用日程に基づいて実施。 （運用監視） 外部委託事業者（オムロンパーソネル㈱）が、常時障害発生有無の確認を行っている。
人事	（運用計画） システム操作手引書において定めている。 （運用監視） 京都府人事課担当者が、常時障害発生有無の確認を行っている。
教職員人事電算	（運用計画） 基本設計書において定めている。 （運用監視） 外部委託事業者（㈱ジェーワンシステム）が、府庁を訪れた際に障害発生有無の確認を行っているのみである（毎日の監視が行われていない）。
税務支援	（運用計画） 外部委託事業者（日本電気㈱）が京都府税務課と協議の上で運用計画を策定しており、変更する場合も外部委託事業者が京都府税務課と協議の上で変更する。 （運用監視） 日本電気㈱（外部委託事業者）が、常時障害発生有無の確認だけではなく、各処理が正常に行われたことを、各処理終了の段階で確認している。
行政事務支援	（運用計画） 開発当初に策定した運用マニュアルにおいて定めている。 （運用監視） 外部委託事業者の再委託先（㈱アルファネット）が障害発生有無の確認及び負荷の発生状況を確認している。
統合財務	（運用計画） 外部委託事業者（㈱オーイーシー）が業務所管課（情報政策課、会計課など）と協議の上で運用計画を定めている。 （運用監視） 外部委託事業者が、常時障害発生有無の確認を行うほか、各処理が正常に行われたことの各処理終了段階での確認、負荷の発生状況を確認している。

総務事務	（運用計画） 基本設計書において定めている。 （運用監視） 外部委託事業者の再委託先（㈱グローバルソフトウェア）が、障害発生有無の確認だけではなく、各処理が正常に行われたことを、各処理終了の段階で確認している。
衛星通信系防災情報	（運用計画） 基本設計書において定めている。 （運用監視） 京都府防災・原子力安全課担当者が障害発生有無の確認を行っている。

ii　指摘事項及び意見

㈠　情報システムの運用に情報政策課の承認がなく規程に違反している（８システム及びその他のシステム共通）

「電子計算機運用管理要領」において、業務主管課の長は「電子計算機の利用を希望するときは、あらかじめ電子計算機オープン利用申請書を情報政策課に提出し、承認を受けなければならない」（第４条第１項）し、また「所掌する適用業務の電算処理に当たっては、別に定める期日までに年間電算処理予定表を情報政策課長に提出しなければならない」（第５条第２項）。また、「電算処理スケジュールを変更する必要が生じたときは、速やかに電算処理スケジュール変更協議書により情報政策課長に協議しなければならない」（第６条第１項）。

したがって、情報政策課所管のシステムについて運用する際は情報政策課長の承認を受けなければならないのはもちろんのこと、その他の所管部署について運用する際にも、情報政策課長の承認を所定の様式に従い受けなければならない。

ところが、実際の情報システムの運用の際には、情報政策課長の承認を必ずしも受けておらず、「電子計算機運用管理要領」に反しているため、問題がある。

情報システムの所管が情報政策課以外であったとしても、「電子計算機運用管理要領」にしたがって情報政策課の承認を受けるように改善しなければならない。

なお、当該問題点について情報政策課に見解を確認したところ、「京都府電子計算組織等運用管理規程」がホストコンピュータを使用していたときの規程であることから、規程が実態に即したものとはなっておらず、そのため規程を見直した上で規程を遵守する方針である、とのことであった。

㈡　運用監視が不十分な状況にある（教職員人事電算）

システムを安定的に稼動させるためには、通常は障害発生時にはアラームがシステム管理担当者に通知されるなど、常時の監視が必要である。そうしなければ、障害が発生しているにもかかわらず長時間放置され、結果として業務に重大な支障が発生しかねないからである。

しかしながら、教職員人事電算システムでは、㈱ジェーワンシステム担当者が府庁を訪れた際に障害発生有無の確認を行っているのみであり、十分とはいえず問題がある。障害発生時には担当者にアラームが通知されるなど、最低限の管理を行う必要がある。また、教職員人事電算システム以外のシステムにおいて、障害発生有無の管理しか行っていないシステムがあるが、正常終了確認や負荷発生状況等も監視することが望ましい。

②　障害管理及び例外処理実行管理

i　現状

運用計画で定めたプログラム実行が適正に行われれば良いが、実際には障害発生によってプログラム実行が停止することがあり（そのため上述のとおり障害発生有無の確認が行われている。）、そのための対応が別途必要となることがある。また、各種業務の状況によっては運用計画以外のプログラム実行（例外処理実行）が必要となることがある。

そのため、障害管理及び例外処理実行管理の各システムの状況について担当者及び外部委託事業者にヒアリングし、必要に応じて管理資料の検討を行った。

【図表2.3.3-2】

システム	実施状況
新人事給与	（障害管理） 障害対応作業は外部委託事業者（オムロンパーソネル㈱）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応結果については、週次及び月次で行われる業務所管課（情報政策課、給与厚生課など）担当者等とのミーティングで報告される。 （例外処理実行管理） 例外処理は行われていない。
人事	（障害管理） 障害対応作業は外部委託事業者（㈱ケーケーシー情報システム）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応の都度、外部委託事業者から京都府人事課担当者に報告される。 （例外処理管理） 例外処理は、京都府人事課担当者から外部委託事業者へメールで依頼される。例外処理の内容についても、処理前に外部委託事業者から京都府人事課担当者に報告される。
教職員人事電算	（障害管理） 障害対応作業は外部委託事業者（㈱ジェーワンシステム）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応の都度、外部委託事業者から京都府教職員課担当者に報告される。 （例外処理管理） 例外処理は、京都府教職員課担当者から外部委託事業者へメールで依頼される。例外処理の内容についても、処理前に外部委託事業者から担当者に報告される。
税務支援	（障害管理） 障害対応作業は外部委託事業者（日本電気㈱）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応の都度、外部委託事業者から京都府税務課担当者に報告される。 （例外処理管理） 例外処理は、京都府税務課担当者から外部委託事業者への連絡票で依頼される。例外処理の内容についても、処理前に外部委託事業者から担当者に報告される。
行政事務支援	（障害管理） 障害対応作業は外部委託事業者（㈱大塚商会）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応結果については、週次及び月次で行われる担当者等とのミーティングで報告される。 （例外処理管理） 例外処理は、京都府情報政策課担当者から外部委託事業者へのメールで依頼される。例外処理の内容についても、処理前に外部委託事業者から担当者に報告される。

統合財務	（障害管理） 障害対応作業は外部委託事業者（㈱オーイーシー）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応結果については、週次及び月次で行われる担当者等とのミーティングで報告される。 （例外処理管理） 例外処理は、業務所管課（情報政策課、会計課など）担当者から外部委託事業者へのメールで依頼される。例外処理の内容についても、処理前に外部委託事業者から担当者に報告される。
総務事務	（障害管理） 障害対応作業は外部委託事業者（㈱グローバルソフトウェア）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応結果については、週次及び月次で行われる京都府情報政策課担当者等とのミーティングで報告される。 （例外処理管理） 例外処理は、担当者から外部委託事業者へのメールで依頼される。例外処理の内容についても、処理前に外部委託事業者から担当者に報告される。
衛星通信系防災情報	（障害管理） 障害対応作業は外部委託事業者（沖電気工業㈱）において行われ、障害発生の都度、作業内容及び対応結果を文書化し、保管する。また対応の都度、外部委託事業者から京都府防災・原子力安全課担当者に報告される。 （例外処理管理） 例外処理は行われていない。

ii　指摘事項及び意見

例外処理に情報政策課の承認がなく規程に違反している（８システム及びその他のシステム共通）

「電子計算機運用管理要領」において、業務主管課の長は「適用業務に係る電算処理において、当該業務の年間電算処理スケジュール及び月間電算処理スケジュールで予定されていない電算処理を行う必要が生じたときは、予定外電算処理協議書により情報政策課長に協議しなければならない」（第７条第１項）とされる。

したがって、情報政策課所管のシステムについて例外処理を実行する際は情報政策課長の承認を受けなければならないのはもちろんのこと、その他の所管部署について例外処理を実行する際にも、情報政策課長の承認を所定の様式に従い受けなければならない。

ところが、実際の例外処理の実行の際には、情報政策課長の承認を必ずしも受けておらず、「電子計算機運用管理要領」に反しているため、問題がある。

情報システムの所管が情報政策課以外であったとしても、「電子計算機運用管理要領」にしたがって情報政策課の承認を受けるように改善しなければならない。

なお、当該問題点について情報政策課に見解を確認したところ、「京都府電子計算組織等運用管理規程」がホストコンピュータを使用していたときの規程であることから、規程が実態に即したものとはなっておらず、そのため規程を見直した上で規程を遵守する方針である、とのことであった。

⑶　ソフトウェア・ハードウェア・ネットワークの構成管理及び調達管理

①　構成管理及び調達管理

i　現状

㋐　ソフトウェア及び機器類の台帳管理状況について

情報政策課に対して台帳管理状況についてヒアリングしたところ、「機器等接続申請書」に基づき、各システム所管部署から情報政策課長に対して接続申請が行われているものについては、台帳管理の対象となっているとの事であった。また、機器の廃止については、「個別業務〔システム〕（廃止）申請書」に基づき、各システム所管部署から情報政策課長に対して廃止申請が行われたものについては、台帳から抹消している

との事であった。

(ｲ)　ネットワークの状況について

外部ネットワークとの接続状況について、情報政策課にヒアリングしたが、今まで接続申請を受けたことはないとの回答であった。

また、各システムのネットワーク図を閲覧したが、外部ネットワークとの接続と見受けられるようなものはなかった。

(ｳ)　システム構成について

各システムのシステム構成について各所管部署にヒアリングするとともに、必要に応じてシステム構成図の閲覧を行った。

合わせて、現在使用していないシステムの有無についても確認したが、使用していないシステムはない、とのことであった。

ii　指摘事項及び意見

契約書の記載項目の見直し（８システム共通）

システム改修委託契約書や軽微なシステム改修を含む保守管理契約が存在する。これらについては、修正したプログラムの権利が誰に帰属するかについて、契約書に明記しておくべきである。なぜなら、契約書に明記していないその権利が誰に帰属するか判然とせず、万が一、契約先の企業が倒産した場合などに、その権利の帰属が問題になることがあるからである。

ところが、情報システムに関する契約書を閲覧すると、修正したプログラムの権利が誰に帰属するか明記されていないものが散見された。

契約書の記載項目の見直しを行い、プログラムの権利が誰に帰属するかを明示するべきである。

2.3.4　情報システムのセキュリティ管理について

京都府では、個人情報など府民生活に重要な影響を与える情報が保管されており、万が一その情報が流出した場合には、計り知れない影響を及ぼす。そのため、情報セキュリティは一定水準を保つ必要があり、そのためにしかるべき管理を行う必要がある。

管理方法としては、(1)　ルールの整備状況、(2)　情報セキュリティに関する教育・訓練、(3)　アクセス管理１（ID・パスワード等のアクセス制限による技術的な管理）、(4)　アクセス管理２（データへの不正アクセス、改ざん、不正持ち出し等の防止）、(5)　アクセス管理３（サーバルームやマシンルームへの立ち入りの管理）、を行うことが考えられる。したがって、京都府における情報セキュリティの体制、技術的な管理方法、物理的な管理方法について監査を行った。

(1)　ルールの整備状況（全般的なセキュリティ管理方針）

①　現状

京都府情報セキュリティ対策基準において、その管理方針が下記のとおり定められている。

> ４　物理的セキュリティ
> (1)　情報システム
> ア　機器の設置等
> 機器の設置等に当たっては、次に掲げる措置を講じるものとする。
> (ｱ)　温度、湿度、ほこり等の環境の影響を可能な限り排除した場所に設置すること。
> (ｲ)　必要に応じ、容易に取り出せないようにするなど適切な措置を講じること。
> (ｳ)　情報システムの重要度に応じて、機器の二重化や地震対策運用環境を考慮すること。
> (ｴ)　ネットワークに接続できない等の事由でセキュリティを維持できない機器については、USB ポート等の外部機器と接続可能なインターフェイスを封印すること。
> イ　電源
> (ｱ)　サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えること。
> (ｲ)　落雷等による過電流に対してサーバ等の危機を保護するための措置を講じること。
> ウ　ネットワーク（上述のため、省略）
> (2)　管理区域
> ア　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等又は情報資産の管理並びに運用を行うための区域（以下「管理区域」という。）は、水害対策及び確実な入退室管理を行うために、地階又は１階に設けることは可能な限り避けること。
> また、外部からの侵入が容易にできないように管理区域は可能な限り無窓の外壁等に囲まれた区域とすること。
> イ　管理区域から外部に通じる出入口は１箇所のみとし、IC カード等による入退室管理、入退室管理簿の記載、監視機能、鍵、警報装置等によって許可されていない立入りを防止すること。
> ウ　管理区域には、ビデオカメラ等の監視機能を設置すること。

エ　管理区域内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を講じること。
なお、管理区域内の機器類の配置は、緊急時に円滑に避難できるように配慮すること。
オ　管理区域を囲む外壁等の床下開口部はすべて塞ぐこと。
カ　消火剤は、機器及び記録媒体に影響を与えないものであること。
(3)　機器等を庁舎外に設置しようとする場合
情報システムを庁舎外に設置しようとする場合は、IT 推進本部の承認を受けるものとする。
(4)　情報資産の管理方法
ア　情報資産に関する業務に携わるすべての職員（非常勤職員及び臨時職員等を含む。）及び委託等を受けて携わる者（以下「職員等」という。）が業務上やむを得ず記録媒体を持ち出す場合、情報セキュリティ責任者は管理簿を設けるなど適切に管理するものとする。
イ　記録媒体の管理
(ｱ)　取り出しが可能な記録媒体は、盗難や損傷の防止等のため適切な管理を行うこと。取り出しが可能な記録媒体は、盗難や損傷、ウイルス被害防止等のため、ウイルスチェックを行うなど適切な管理を行うこと。
(ｲ)　記録媒体に納められた情報資産のうち、重要な情報資産は、別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管すること。
(ｳ)　重要な情報資産を記録した記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管すること 。
(ｴ)　記録媒体が不要となった場合は、データを復元できないように消去を行った上で廃棄すること。また、消去及び廃棄を行った日時、処理者及び処理内容を記録すること。
5　人的セキュリティ対策
(1)　職員等の責任
ア　情報セキュリティ対策の遵守義務
(ｱ)　職員等は、基本方針及び対策基準に定められている事項を遵守すること
(ｲ)　情報セキュリティ対策について不明な点、遵守することが困難な点が発生したときは、速やかに情報セキュリティ責任者に連絡すること。
(ｳ)　情報システム管理者は、次のイに該当する利用が行われていると認める場合は、当該職員等に対して情報システムの利用を停止することができる。
イ　情報システム利用上の注意事項
職員等は、情報システムの利用に当たって次の行為を行ってはならない。
(ｱ)　業務目的以外で情報システムを利用すること。
(ｲ)　情報資産を執務室外に持ち出すこと。ただし、情報資産を別の記録媒体に保存するなどやむを得ない理由のある場合で、かつ情報セキュリティ責任者の事前の了解を得た場合を除く 。
(ｳ)　情報システム管理者の許可を得ずにソフトウェアを導入すること。
(ｴ)　利用する端末や記録媒体について、許可のない第三者に利用又は閲覧され得る状態にすること。
(ｵ)　情報セキュリティ責任者の許可なく、府の情報システム以外のパソコン並びに USB メモリ、メモリカード等の外部記憶装置及び外部記憶媒体（以下「機器等」という。）を庁舎内に持ち込むこと。
(ｶ)　府の情報システムに機器等を接続する場合、情報セキュリティ責任者、IT 推進員又は情報セキュリティ操作認定者がウイルスチェックを実施した後、直接又はその指揮の下で職員が行うものとする。
ウ　その他
職員等は、知り得た情報資産を漏えいしてはならない。その職を退いた後も、また、同様とする。
(2)　パスワード及び IC カードの管理
ア　職員等は、パスワードに関し、次に掲げる事項を遵守すること。
(ｱ)　他の職員等のユーザ名を使わないこと
(ｲ)　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ないこと。
(ｳ)　パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。
(ｴ)　パスワードは定期的に変更し、古いパスワードの再利用はしないこと。
(ｵ)　パスワードの盗用や漏えいがあった場合は、直ちに情報システム管理者に連絡すること。
(ｶ)　その他、ユーザ名及びパスワードの適正な管理を行うこと
イ　情報システム管理者のパスワード管理
情報システム管理者は、職員等のパスワードに関する情報を厳重に管理するものとする。
ウ　IC カードの管理
(ｱ)　職員等は、IC カード等を紛失した場合は、速やかに情報セキュリティ責任者及び情報システム管理者に連絡すること。
(ｲ)　情報システム管理者は連絡があり次第速やかに当該 IC カードを利用したアクセス等を停止すること。
(3)　教育・訓練
ア　IT 推進本部は、情報セキュリティに対する意識を醸成し保つため、職員等及び関係する者に対し普及啓発するとともに、職員等に対し情報セキュリティに関する理解が深まるよう教育・訓練を行うものとする。
イ　情報システム管理者は、情報システムに不測の事態が発生した場合に備えた訓練を行うものとする。

ウ　情報セキュリティ責任者、IT推進員及び情報セキュリティ操作認定者は、毎年定められたセキュリティ対策に係る研修を受講しなければならない。なお、情報セキュリティ操作認定者が研修を受講しなかった場合、その指定を取り消すものとする。

(4)　事故、欠陥に対する報告

ア　職員等は、情報資産の流出、漏えい、改ざん、情報システムの障害及び誤作動等の事故(以下「事故等」という。)の発生及び発生の危険性を発見した場合には、直ちに情報セキュリティ責任者に報告し、その指示に従い必要な措置を講じるものとする。

イ　情報セキュリティ責任者は、事故等の報告を受けた場合は、直ちに当該事故等の内容を情報システム管理者及びIT推進本部に報告するものとする。

(5)　外部委託に関する管理（「2.4外部委託事業者の管理について」に記述のため、省略）

6　技術的セキュリティ対策

(1)　アクセス記録の取得等

ア　情報システム管理者は、重要な情報システムについて、各種アクセス記録及び情報セキュリティ対策に必要な記録を取得し、１年以上の期間を定めて、保存するものとする。

イ　情報システム管理者は、重要な情報システムについて、定期的にアクセス記録等を分析、監視するものとする。

ウ　情報システム管理者は、アクセス記録等が窃盗、改ざん、消去されないように必要な措置を講ずるものとする。

(2)　機器構成変更の禁止（上述のため省略）

(3)　アクセス制御（上述のため省略）

(4)　外部ネットワークとの接続（上述のため省略）

(5)　システム開発、導入、保守等（上述のため省略）

(6)　コンピュータウイルス

ア　情報システム管理者は、コンピュータウイルスによる情報システムの安全性を確保するため、次の事項を実施するものとする。

(ｱ)　外部ネットワークからデータを受け入れる際には、ファイアウォールを適切に設定するとともに、メールサーバ等においてウイルスチェックを行いシステムへの侵入を防止すること。

(ｲ)　外部ネットワークへデータを送信する際にも、(ｱ)と同様のウイルスチェックを行いシステムへの侵入を防止すること。

(ｳ)　コンピュータウイルス情報について職員等に対する注意喚起を行うこと。

(ｴ)　端末においてウイルス対策用のソフトウェアを導入すること。

(ｵ)　ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

(ｶ)　コンピュータウイルスに対する修正プログラムを入手し、サーバ及び端末に速やかに適用すること。

イ　職員等は、次の事項を遵守しなければならない

(ｱ)　外部からデータ又はソフトウェアを取り入れる場合には、必ずウイルスチェックを行うこと。

(ｲ)　差出人が不明のファイル及び不自然に添付されたファイルは、速やかに削除すること。

(ｳ)　ウイルスチェックの実行を途中で止めないこと。

(ｴ)　情報システム管理者が提供するウイルス情報を常に確認すること。

(ｵ)　添付ファイルのあるメールを送受信する場合は、必ずウイルスチェックを行うこと。

(7)　不正アクセス対策

ア　情報システム管理者は、不正アクセスを防止するため、次に掲げる対策を講じるものとする。

(ｱ)　ソフトウェアの不備に伴うセキュリティホールに対しては、速やかに修正プログラムを適用すること。

(ｲ)　情報システム上の不要なユーザ名は、速やかに削除すること。

(ｳ)　重要な情報システムの設定に係るファイル等について、当該ファイルの改ざんの有無を検査すること。

(ｴ)　不正アクセスを受けるおそれが認められる場合には、情報システムの停止を含む必要な措置を講じること。

(ｵ)　利用終了又は利用される予定のない不要なポートは閉めること。

イ　職員等は、不正アクセスを受けた場合には、直ちに情報セキュリティ責任者及び情報システム管理者に連絡し、その指示に従うものとする。

ウ　情報システム管理者は、不正アクセスを受けた場合は、直ちにIT推進本部及び関係機関に連絡を行い、情報の復旧等必要な措置を講じなければならない。

(8)　セキュリティ情報の収集

ア　情報システム管理者は、情報セキュリティに関する情報を収集し、情報システムについてソフトウェアに修正プログラムを適用する等、セキュリティ対策上必要な措置を講じるものとする。

イ　IT推進本部は、前項の情報を情報システム管理者及び情報セキュリティ責任者に通知するものとする。

なお、京都府では平成21年６月に、庁内のコンピュータにウイルスが感染したことを受けて、セキュリティ対策の強化方法を講じている。強化方法の内容等は、下記のとおりである（「セキュリティ対策の強化について（平成21年６月政策企画部）」を基に記述。）。

1　原因及びセキュリティ強化対策のポイント

原因	強化対策
職員及び受託事業者のセキュリティ意識の低さ	セキュリティ操作認定者の新設並びにセキュリティ研修の実施及び受講の徹底
USB メモリ、独自導入パソコン等の情報機器の不適切な管理	・公用で USB メモリ等を接続する場合のルール確立 ・セキュリティ対策に問題のあるパソコンの統合
運用管理を業者委託する際に、セキュリティ対策の指示が遺漏又は不徹底	現場における連絡、復旧対策の再確認・強化及び IT 推進本部協議の義務付け

2　対策の概要

①　セキュリティ操作認定者の新設並びにセキュリティ研修の実施及び受講の徹底

○所属長（セキュリティ責任者）：管理職研修時に研修実施の方向で調整
○IT 推進員：責任者を補佐し、操作認定者の指導・支援。研修を速やかに実施。
○セキュリティ操作認定者：資格要件に研修受講を設定　研修を速やかに実施

（注）セキュリティ操作認定者・・・公用で USB メモリを接続できる等、通常の職員と比較してセキュリティに関する権限が与えられている。

②　公用で USB メモリ等を接続する場合のルール確立

○USB メモリ等の接続をセキュリティ責任者、IT 推進員、セキュリティ操作認定者に限定
○USB メモリ等の接続に係るガイドライン申請を徹底

・USB メモリ等はウイルスを媒介するおそれがあるものの、業務運営上必要である現状に鑑み、その接続操作を情報セキュリティ責任者と情報セキュリティ操作認定者に限定し、管理を徹底。なお、情報セキュリティ操作認定者の資格継続要件として毎年の研修受講を設定。

③　セキュリティ対策に問題のあるパソコンの統合

○十分なセキュリティ対策ができないパソコンは、事務支援パソコンに統合。

・現地、現場での講演、説明会のためにはモバイルパソコンを貸与し、統合を推進。
・継続利用がやむを得ない場合は、USB 接続口等を封印して使用 。

④　現場での連絡、復旧対策の再確認・強化及び IT 推進本部協議の義務付け

○事業継続を可能とするため、非常時連絡網の再チェック及び復旧体制の強化を実施
○予算要求から調達、運用開始までの各段階で、IT 推進本部への協議を義務付け

・各所属において、保守事業者との非常時連絡網、復旧体制及び保守物品の確認を始めとする点検を実施するとともに、IT 推進本部による内部監査を実施。
・セキュリティ攻撃が高度化し、また原課にセキュリティ対策のノウハウが蓄積されていないことから、予算要求段階から対策を実施するまで IT 推進本部の関与が必要。
・包括的対策の徹底及び全体最適化を推進するため、すべてのシステム、パソコン等が協議対象。

3　その他の対策

・職員の私物、受託業者等の USB メモリ等（納品物を除く）の持込を禁止。
・庁内における派遣会社からの人材受入増、アウトソーシングの進展に対応し、派遣社員、アウトソーサーにも職員と同様の対応を求める。
・外部の専門家によるシステム監査等を実施。

②　指摘事項及び意見

「セキュリティ対策の強化について」の各規程への未反映

「セキュリティ対策の強化について」は、京都府の正式な規程ではなく、通達のような性格を持つものである。通達も規程と同様に京都府職員が遵守すべきものであるものの、京都府職員に遵守事項を徹底させるためには、「セキュリティ対策の強化について」の内容を各規程に反映させ、「セキュリティ対策の強化について」及び各規程で遵守事項を一致させる必要がある。

(2)　情報セキュリティに関する教育・訓練

①　現状

上述のとおり対策基準「５(3)教育・訓練」において規程が定められているが、実際には、下記のとおり訓練や

教育研修の実施が徹底できていない状況にある。情報セキュリティに関する教育・訓練は、セキュリティの水準を一定以上に保つためには最も重要なものであり、必要な訓練もしくは研修実施を徹底する必要がある。

②　指摘事項及び意見

ⅰ　情報システム管理者が訓練を行っていない（８システム及び全システム共通）

そもそも「不測の事態」が明確になっていないため、まずは「不測の事態」（大規模災害発生、ウイルス感染、不正アクセス等）を定義し、これに沿った訓練を行う必要がある。

ⅱ　セキュリティ対策に係る研修を受講していない者がいる（教職員人事電算）

平成23年度及び平成24年度のセキュリティ研修は、USB メモリ使用者（セキュリティ操作認定者）に対しては出席を義務付けているが、受講者一覧を閲覧した結果、教職員課において USB メモリ使用者の名前がなかった。

セキュリティ研修への出席を義務付けている以上、該当者には必ず研修を受講させる必要がある。

また、USB メモリを使用していない他の各システムの担当者についても、研修受講の義務付けを検討されたい。

⑶　アクセス管理１（ID・パスワード等のアクセス制限による技術的な管理）

①　現状　～一般 ID と特権 ID の使用状況について～

一般 ID（※１）と特権 ID（※２）に分けて、権限付与状況等を各担当者（外部委託事業者含む）にヒアリングした。なお、一般 ID のパスワードポリシーについては「③現状　～一般 ID のパスワードポリシー～」を参照。

（※１）一般 ID：通常の操作が可能な権限。

（※２）特権 ID：全データの閲覧・改ざん、プログラム変更など重要な処理が可能な権限。そのため、使用状況の管理が特に重要となる。

【図表2. 3. 4-1】

システム	実施状況
新人事給与	ⅰ一般 ID の状況 ⑺給与担当者のみがアクセス可能。 ⑴職員番号及び利用者のパスワードによりアクセス管理を行っている。 ⅱ特権 ID の状況 ⑺特権 ID は 13 あり。外部委託事業者（㈱オムロンパーソネル）及びその再委託先（㈱ワークスアプリケーションズ）の担当者は全員特権 ID が使用可能。 ⑴特権 ID の使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない。
人事	ⅰ一般 ID ⑺人事課と人事関係課以外の職員はアクセスできない。 ⑴職員番号及び利用者のパスワードで管理。 ⅱ特権 ID ⑺特権 ID は４つあり、それぞれ京都府人事課人事担当と外部委託事業者（㈱ケーケーシー情報システム）がそれぞれ２つずつ使用可能。 ⑴特権 ID の使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない（人事システムは、使用者が限られていること、使用場所も人事課の隣室であると限定的であることから、他のシステムと比較して不正使用の可能性は低いと考えているためである。）。 ⅲその他（作業室への入室管理） 外部委託事業者が京都府庁内で作業する際には、京都府人事課の監視のもと作業室に入室する。

教職員人事電算	ⅰ一般ID (ｱ)教育委員会以外の職員はアクセスできない。 (ｲ)職員番号及び利用者のパスワードにより、アクセス管理を行っている。 (ｳ)人事電算専用端末を操作する場合は、指紋認証による管理を行っている。ただし、教職員課において、指紋認証装置の不具合を理由として指紋認証を使用していない事例があった。 ⅱ特権ID (ｱ)特権IDは10あり、京都府教職員課人事担当と外部委託事業者（㈱ジェーワンシステム）が使用可能。 (ｲ)特権IDの使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない。 (ｳ)使用されていない特権IDが残っている。
税務支援	ⅰ一般ID (ｱ)府税に関する業務に携わる職員がアクセス可能。具体的には、総務部税務課、各府税事務所、自動車税管理事務所、各広域振興局の企画総務部税務室、各府税出張所の各職員であり、合計で約280名の職員がアクセス可能である。 (ｲ)職員番号及び利用者のパスワードでアクセス管理している。 (ｳ)一般IDで全納税者の情報を閲覧可能である。 ⅱ特権ID (ｱ) 特権IDは5つ。外部委託事業者（日本電気㈱）が使用可能。 (ｲ) 特権 ID の使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない。 ⅲその他 ログイン記録は、一般ID含めて稼動時から保持しているが、どの情報にアクセスしたか等のオペレーションログの記録が残っていない。
行政事務支援	ⅰ一般IDの状況 (ｱ) 全ての京都府職員（教育委員会のうちの、市町村立小中学校は除く）、公立大学法人職員、京都地方税機構の職員がアクセス可能。 (ｲ) ユーザーＩＤ及び利用者のパスワードによりアクセス管理している。 ⅱ特権IDの状況 (ｱ) 特権IDは３つ。外部委託事業者（㈱大塚商会）担当者１名及びその再委託先（㈱アルファネット）担当者３名のみが特権ID及びそのパスワードを把握している。 (ｲ) 特権 ID の使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない。

統合財務	ⅰ一般IDの状況 (ｱ) 全ての京都府職員（教育委員会のうちの、市町村立小中学校は除く）がアクセス可能。 (ｲ) 外部に対して資金が支払われる伝票を起票する職員は、職員番号、利用者のパスワード及びICカードによりアクセス管理を行っている。それ以外の職員（予算の登録や各種検索）は、職員番号及び利用者のパスワードによりアクセス管理を行っている。 ⅱ特権IDの状況 (ｱ) 特権IDは４つ。外部委託事業者（㈱オーイーシー）担当者のうち、常駐している者は全員特権IDを使用可能。 (ｲ) 特権 ID の使用状況の監視については、毎朝外部委託事業者がログを確認している。
総務事務	ⅰ一般IDの状況 (ｱ) 全ての京都府職員（公安委員会、及び教育委員会のうちの、市町村立小中学校は除く）がアクセス可能。 (ｲ) 行政事務支援システムからのシングルサインオン（行政事務支援システムからログインする。）のため、当該システムにユーザーが自らＩＤ及びパスワードの入力は行われていない。 ⅱ特権IDの状況 (ｱ) 特権IDは３つ。外部委託事業者（富士電機㈱）の担当者２名と再委託先（㈱グローバルソフトウェア）の担当者１名が使用可能。 (ｲ) 特権 ID の使用状況の監視については、ログイン履歴のログを保管するのみで、不正等に用いられているかまでは確認していない。
衛星通信系防災情報	ⅰ一般ID (ｱ) 京都府職員すべてがアクセス可能。 (ｲ) 京都府職員すべてが同一の ID とパスワードでアクセス可能。すなわち、京都府職員の誰がアクセスしたかを管理していない。 （理由） 当該システムは、全職員が災害発生時に迅速に利用できることを前提としているため。ただし、IP アドレスにより操作できるPCを限定しているため、京都府外から当該システムを利用することはできない。 (ｳ) 各市町村に設置の専用端末にも、それぞれに ID とパスワードを付与しており、専用端末にて閲覧・書き込みすることができる。 ⅱ特権ID 特権IDは一つ。普段は京都府防災・原子力安全課担当者が管理しており、外部委託事業者（沖電気工業㈱）が保守作業を行う際に、特権IDの使用権限を付与している。

②　指摘事項及び意見　～一般IDと特権IDの使用状況について～

ⅰ　一般ID

(ｱ)　権限付与が広範である（税務支援）

府税に関する業務に携わる職員が、全納税者の情報を閲覧できる状態にあり、あまりにも、幅広い権限が

与えられ過ぎているといえる。

そのため、府民サービスの低下や未納防止などの取り組みを考慮した上で、各部署で閲覧できる権限を狭める（例えば、納税者の地域で閲覧権限を区分けするなど。）ことを検討されたい。

㈠　簡易検索が可能なオペレーションログが残っていない（税務支援）

オペレーションログが残らないシステムとなっている。「稼働ログ」と「データベースのアクセス記録」の組み合わせにより必要なオペレーションが記録されるシステムとなっており調査に時間を要するため、費用対効果の検討は必要であるが、オペレーションログを記録するための改修を検討されたい。

㈡　指紋認証の実施を怠っている（教職員人事電算）

「京都府教職員人事電算システムに関する情報セキュリティ実施手順」において、人事電算専用端末を操作する職員の認証は、ユーザ ID 及び指紋情報にて行うこととされている。

しかし、実際には、教職員課において指紋認証装置の不具合を理由としてユーザ ID のみのアクセス制御となっている事例があり、規程に反した運用となっているため問題がある。これに関する問題点については、「2. 5教職員課について」においても記述する。

㈢　非効率な ID 登録・削除・権限変更（税務支援）

上記では記載していないが、異動時期になると、税務課は東府税事務所、西府税事務所、南府税事務所、自動車税管理事務所、山城広域振興局企画総務部税務室、山城南府税出張所、南丹広域振興局企画総務部税務室、中丹広域振興局企画総務部税務室、中丹西府税出張所、丹後広域振興局企画総務部税務室に、どの職員がどの部署に異動したかをそれぞれ問い合わせている。そのうえで、ID の登録・削除・権限変更を行っている。

実務的には、この問い合わせ業務が非常に煩雑であるという。各部署に問い合わせるのに時間がかかるうえ、その内容を迅速に ID 登録・削除・権限変更に反映しなければ業務に支障が出る。

そもそも人事異動については、人事システムから出力できるはずであるから、それをなぜ活用していないかを聞いたところ、人事システムから出力されるデータには、異動情報以外の個人情報が多く含まれているから使用できないとのことであった。

人事システムから出力されるデータの形式を変更することは、比較的容易であると考えられるので、データ出力形式の変更による業務効率化を検討されたい。

ⅰ　特権 ID

㈠　削除すべき特権 ID が残っている（教職員人事電算）

特権 ID は必要なものだけを作成し、不要なものは削除しなければならない。なぜなら、不要な特権 ID が不正に使用されるリスクが存在するからである。

ところが、教職員人事電算システムにおいては、不要な ID がそのまま削除されずに残っているため、問題である。

速やかに不要な特権 ID を削除することが望まれる。

㈡　特権 ID の使用状況を管理していない（新人事給与、人事、教職員人事電算、税務支援、行政事務支援、総務事務、衛星通信系防災情報）

統合財務システムでは、特権 ID のログ履歴を毎日確認しているとのことであったが、他のシステムではログ履歴を保管するのみで、履歴の確認は行われていない。上述のとおり、特権 ID は管理に特に注意を要するものであることから、定期的にログ履歴を確認し、不正使用が行われていないか、確認する必要がある。

③　現状　～一般 ID のパスワードポリシーについて～

各システムのパスワードポリシーは下記のとおりである。

【図表2. 3. 4-2】

システム	根拠規程等	実施状況
全庁的パスワードポリシー	京都府情報セキュリティ対策基準	【規程の抜粋】 ⅰパスワードの長さ等について パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。 ⅱパスワードの変更について パスワードは定期的に変更。 ⅲパスワードの再利用について 古いパスワードの再利用はしない。

新人事給与	新人事給与システムセットアップ手順書	【規程の抜粋】 ⅰパスワードの長さ等について 半角６文字以上 ⅱパスワードの変更について １年程度の期間で定期的に変更。 ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について 上記以外のパスワードはシステム上設定できない。 ⅱパスワードの変更について システム上、強制することはできない。 ⅲパスワードの再利用について システム上制限は無い。
人事	なし	【規程の抜粋】 ⅰパスワードの長さ等について なし ⅱパスワードの変更について なし ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について パスワードは英数半角、大文字・小文字・数字を組み合わせた８桁以上の文字列以外のパスワードはシステム上設定できない。 ⅱパスワードの変更について システム上、強制することはできない。（長期間同じパスワードを使用できる。） ⅲパスワードの再利用について システム上、制限はない。
教職員人事電算	京都府教職員人事電算システムに関する情報セキュリティ実施手順	【規程の抜粋】 ⅰパスワードの長さ等について パスワードは英数半角、大文字・小文字・数字を組み合わせた６桁以上の文字列 ⅱパスワードの変更について なし ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について 上記以外のパスワードはシステム上設定できない。 ⅱパスワードの変更について 規程にはないが、システム上１年ごとにパスワードの変更を強制しており、変更しなければロックされる。 ⅲパスワードの再利用について システム上、古いパスワードは使用できない設定となっている。

税務支援	税務電算トータルシステムセキュリティ対策実施手順	【規程の抜粋】 ⅰパスワードの長さ等について パスワードは５文字以上とし、数字及びアルファベットを混在させるなど容易に推定できないものとすること。 ⅱパスワードの変更について パスワードは毎年度変更すること。 ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について 制限なし（システム制限検討中） ⅱパスワードの変更について 制限なし（システム制限検討中） ⅲパスワードの再利用について 制限なし（システム制限検討中）
行政事務支援	行政事務支援システム用管理要領 及び 行政事務支援システム運用ルール	【規程の抜粋】 ⅰパスワードの長さ等について 自らが定めたパスワードを使用（運用管理要領） ⅱパスワードの変更について (ｱ)パスワードの適切な管理を定めている（運用管理要領） (ｲ)6ヶ月を目安に定期的に変更（運用ルール） ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について 半角６文字以上14文字以内 ⅱパスワードの変更について パスワード設定日から６ヶ月で変更を求める（変更しないと情報政策課でロックする） ⅲパスワードの再利用について 過去10回分は使用できない
統合財務	統合財務システム管理運営要領	【規程の抜粋】 ⅰパスワードの長さ等について 利用者が設定 ⅱパスワードの変更について 利用者が変更及び管理を行う ⅲパスワードの再利用について なし 【システム上の対応】 ⅰパスワードの長さ等について 半角英数字で最大15文字以内 ⅱパスワードの変更について システム上、制御することはできない。 ⅲパスワードの再利用について 制限なし

総務事務	なし	【規程の抜粋】 行政事務支援システムとシングルサインオンとなっているため規程はない。 【システム上の対応】 ⅰパスワードの長さ等について 半角英数の文字を組み合わせ 10 文字以上のものを利用。 ⅱパスワードの変更について 行政事務支援システムとシングルサインオンとなっているため、総務事務システムのパスワードをユーザが入力することはなく、変更も不要。 ⅲパスワードの再利用について パスワードの再利用は可能。ただし、行政事務支援システムとシングルサインオンとなっているため、パスワードをユーザが入力することはない。
衛星通信系防災情報	なし	【規程の抜粋】 なし 【システム上の対応】 ⅰパスワードの長さ等について パスワードの長さについて規制はない。（運用上は８文字以上で設定している。） ⅱパスワードの変更について　パスワードの変更期限の設定はない。 ⅲパスワードの再利用について パスワードの再利用制限の設定はない。

④　指摘事項及び意見　～一般 ID のパスワードポリシー～

ⅰ　類似のパスワードポリシーが散見され、必要性が不明確である（教職員人事電算、税務支援、行政事務支援、統合財務）

パスワードポリシーに関する規程が、京都府内で複数存在しており、それぞれに微妙な差異がある。パスワードポリシーを定めた規程は、「京都府情報セキュリティ対策基準」「京都府教職員人事電算システムに関する情報セキュリティ実施手順」「税務電算トータルシステムセキュリティ対策実施手順」「行政事務支援システム運用管理要領」「統合財務システム管理運営要領」の５つである。このうち、「京都府情報セキュリティ対策基準」は他の４つの上位に位置するパスワードポリシーを示していると考えられる。

したがって、「京都府情報セキュリティ対策基準」以外の規程においては、これよりも要件を加重する場合、もしくは緩和する場合にのみパスワードポリシーを記載すればよい。しかし、類似のパスワードポリシーが散見されるのが実情であり、各所管部署が統一感なくパスワードポリシーを策定しているように見受けられる。実質的に必要性のないパスワードポリシーは、「京都府情報セキュリティ対策基準」のパスワードポリシーに統一することを検討すべきである。

ⅱ　パスワードポリシーを遵守するためのシステム上の制約がない（新人事給与、人事、税務支援、統合財務、衛星通信系防災情報）

パスワードポリシーを定めた以上は、このパスワードポリシーに沿わないパスワードについては、システム上認めないように設定すべきである。それができなければ、実質的にはパスワードポリシーは機能しなくなるからである。

しかし、例えば人事システムにおいては、パスワードポリシーをシステム上完全な強制はできない。「㈠パスワードの定期的な変更は、システム上強制的に実施するようになっていない。㈡古いパスワードでもシステム上、使用できるようになっている。」のである。パスワードポリシーに反するパスワードが設定されたとしても防ぎようがない。結果としてセキュリティが弱体化してしまっている。

システム改修が必要になるため、費用対効果を考慮しながら、パスワードポリシーに反するパスワードが設

定できないようなシステム変更を検討すべきである。

そもそも、そのようなシステム改修を行うために費用が発生するうえ、今後パスワードポリシーが変更になったときには８つのシステムそれぞれにおいてパスワードポリシーを順守するためのシステム改修を行わなければならず費用がかさむ。

以上のことを考慮すると、パスワードポリシーを全庁的なパスワードポリシーである「京都府情報セキュリティ対策基準」に集約した上で、職員のポータルサイトである行政事務支援システムでの一元管理（シングルサインオン）とすることを検討すべきである。

⑷　アクセス管理２（データ改ざん、不正持ち出し等の防止）

データマスターそのものへの不正アクセスにより改ざん等を行う場合は、ネットワーク管理や特権 ID の管理が主となり、これらの管理状況については既に記載しているため、ここでは、USB メモリ等の媒体によるデータの持ち出しやメールによるデータ持ち出しの管理状況について検討する。

①　現状について

ｉ　USB メモリ等の媒体について

㋐　ルールの整備状況

上述の「セキュリティ対策の強化について（平成21年６月政策企画部）」によると、ガイドライン申請による申請及び承認が必要としている。USB メモリ以外の外部記憶装置についても「セキュリティ対策の強化について」において、図表のとおり規定されている。

【図表2.3.4-3】

外部記憶装置	管理方針
USB メモリ	・接続をセキュリティ責任者、操作認定者に限定 ・ガイドライン申請の徹底
メモリカード類（注２）	USB メモリと同様の扱い （プリンタ内ドライブは封印対応も可）
光学ドライブ （CD-R 等）	講演等でのデータ持ち出し用に接続承認
外付け HDD	システムバックアップに限定して接続承認

（注１）上記は府庁内各課に関するものであるが、この他、職員私物や業者持込については、原則接続禁止とし、例外対応として業者納品物は接続を認めている（ただし、この接続時の申請要否については定められていない。）

（注２）メモリカード類とは、カードリーダライタ、デジタルカメラ、プリンタ内ドライブ、IC レコーダ等を指す。

㋑　使用状況

教職員人事電算システム、総務事務システム、衛星通信系防災情報の各システムにおいて、外部委託事業者がシステム変更作業時に USB メモリを用いてデータを持ち出し、もしくはデータを取り込んでいる。（詳細は「2.4.1外部委託事業者への委託業務内容及び管理状況⑴委託業務の内容」を参照いただきたい。）。

㋒　承認状況

これについて、ガイドライン申請による申請及び承認が必要となる（上述の「セキュリティ対策の強化について（平成21年６月政策企画部）」を参照。）が、各所管部署に承認状況を確認した結果、担当者の口頭による承認が行われているのみである、とのことであった。また、その担当者のセキュリティ研修の受講状況を確認したが、教職員課及び防災・原子力安全課の一部の担当者において受講を示すものはなかった。

㋓　未承認使用防止の状況

USB メモリの未承認使用を防ぐために、例えば USB 接続を行わないときは接続口を封印し使用時のみこれを解除することが考えられるが、各所管部署にヒアリングしたところ、そのような対応は行われていないとの事であった。

また、接続口の封印・解除が煩雑であれば、事後的に使用状況を確認することによって、未承認使用への牽制を行う方法があり、例えば USB メモリの接続ログを定期的に確認する方法が考えられるが、所管部署にヒアリングしたところ、事後的な確認も行われていないとの事であった。

ⅱ　メールの使用状況について

メールは府庁内部でも頻繁に使用されているが、情報セキュリティの観点からは、特に外部とのデータ送受に際して適切な管理が行われているかが重要となるため、これについて検討する。

㈠　ルールの整備状況

メールの使用方法等に関する規程は存在するものの、情報セキュリティの観点から定められた規程はない。

㈡　使用状況

監査対象となった８システムについては、外部とのデータ送受を行っている事例はなかった。

㈢　未承認使用防止の状況

システム上において外部との送信時に何らかの承認設定（例えば情報セキュリティ責任者の承認後に送信する設定）があるか情報政策課にヒアリングしたが、システム上での設定は無いとのとのことであった。

②　指摘事項及び意見

ⅰ　USB メモリ等の媒体について

㈠　規程が十分でない（８システム共通）

「セキュリティ対策の強化について」と各規程の内容を一致させるべきであることについては、「2.3.4(1)ルールの整備状況（セキュリティ管理全体）」に記述のとおりである。また、この他に、業者持込時の USB メモリ使用に関して具体的に誰が承認すべきか明確になっていないため、これを明確にする必要がある。具体的には府庁内各課で使用するときと同様に、ガイドライン申請の徹底、及び情報セキュリティ責任者または情報セキュリティ操作認定者立会の下で、USB メモリを使用するように徹底する必要がある。

また、システムによっては USB メモリの使用自体を禁じる場合もあると考えられる。この場合は、USB メモリの使用を規程において禁じたうえで、USB メモリ等の媒体の差込口を物理的にロックする等の対応を規程化しなければならない。

㈡　業者使用時の適切な承認・立会が行われていない（８システム共通）

上述のとおり、業者が USB メモリを使用する場合でも、ガイドライン申請の徹底、及び情報セキュリティ責任者または情報セキュリティ操作認定者立会いの下で、USB メモリを使用するように徹底する必要がある。

しかし、実際には担当者による口頭承認のみで、担当者が立会の下で業者（外部委託事業者）が USB メモリを使用しているため、適切な承認・立会の下で使用されるように改善する必要がある。

㈢　未承認使用防止が不十分（８システム共通）

仮に USB メモリ使用時のガイドライン申請を徹底したとしても、未承認使用の防止が不十分であるため、申請の徹底が USB メモリ不正使用防止にはつながらない可能性がある。そのため、未使用時の接続口封印や接続ログの事後確認などにより、未承認使用防止の対策を講じる必要がある。

ⅱ　メール送信について

㈠　情報セキュリティの観点からの規程がない（８システム共通）

メールは USB メモリ以上に大量のデータを持ち出すことが可能であり、USB メモリ等と同様の管理が必要である。しかしながら、メールに関して情報セキュリティの観点からの規程がない。

そのため、まずはどのような管理が必要かを検討した上で、規程化が必要である。その際には、下記㈡も参照されたい。

㈡　未承認使用防止が十分ではない（８システム共通）

上述のとおり、外部とのメール送信時に、情報セキュリティ責任者による承認がなくてもシステム上は送信可能となっており、未承認使用の防止が不十分な状況にある。メールにより大量のデータを持ち出すことが可能なため、特にデータ送信を行う場合は、情報セキュリティ責任者の承認を経た上で送信が行われるようにする必要がある。

管理方法としては、例えば、送信の都度 USB メモリと同様のガイドライン申請を行った上で、事後的に外部とのメール履歴を確認する方法があるが、それよりも、外部送信時には必ず情報セキュリティ責任者の承認が行われるようにシステム上設定する方法がより有効かつ効果的であると考えられる。

⑸　アクセス管理３（サーバルームやマシンルームへの立ち入りの管理）

①　現状～サーバ室の状況～

各サーバ室の状況は下記のとおりである。

ⅰ　監視・認証・ラック設置状況

【図表2. 3. 4-4】

	データセンター	府庁電算室	府庁（防災情報サーバ室）
有人監視	監視員室で24時間常時監視あり	なし	なし
監視カメラ	データセンター入口、データセンターフロア内に監視カメラ設置	サーバ室入口、サーバ室内に監視カメラ設置	設置されていない。
認証方法	IC カード＋バイオメトリクス認証（血流）共連れ防止ドアの採用	ICカードによる認証。	なし
ラックの施錠	ラックを個別に施錠ラック鍵を 24 時間365日、監視員室で設置	情報政策課が管理しているサーバには施錠されていない。	なし

ii　建物耐震の状況

【図表2. 3. 4-5】

データセンター	府庁電算室	府庁（防災情報サーバ室）
日本建築防災協会の耐震性能評価Ⅰ級（最上級）	地震の震動及び衝撃に対して倒壊し、又は崩壊する危険性が低いとするレベル。(旧建設省の告示（平成７年12月25日）に基づいた判定。)	地震の震動及び衝撃に対して倒壊し、又は崩壊する危険性が低いとするレベル。(旧建設省の告示（平成７年12月25日）に基づいた判定。)

iii　停電対策の状況

【図表2. 3. 4-6】

データセンター	府庁電算室	府庁（防災情報サーバ室）
・24時間365日無瞬断無停電運用可 ・UPS：無停電電源供給装置（90分保持） ・非常用発電機２基 ・移動電源車を京都市内某所に配置 ・備蓄燃料で24時間運転可	・UPS（無停電電源装置）が 30 分程度の停電であれば稼動を継続する。 ・UPSが稼動の間に、自家用発電装置が稼動（自家用発電装置は2～10分で供給可能となる。）	・UPS（無停電電源装置）が 30 分程度の停電であれば稼動を継続する。 ・UPSが稼動の間に、自家用発電装置が稼動（自家用発電装置は１分以内で供給可能となる。）

iv　消火設備

【図表2. 3. 4-7】

データセンター	府庁電算室	府庁（防災情報サーバ室）
ハロンガス	ハロンガス	ハロンガス

② 府庁電算室・府庁が使用できないときの対応

府庁電算室・府庁が災害等で使用できない場合に備えて、西日本電信電話㈱の施設を利用するための契約を当社と締結している（京都府と西日本電信電話株式会社京都支店は、大規模災害等の緊急事態における拠点施設である地方公共団体の庁舎の代替施設を事前に確保するため「緊急時における西日本電信電話株式会社施設の使用に関する協定」を締結しており、その一環である。）

③ 指摘事項及び意見

各サーバ室を視察した結果、以下の問題点が発見された。

i 府庁電算室

㈠ 窓がある

「京都府情報セキュリティ対策基準」によれば、情報システムの設置場所は、外部からの侵入が容易にできないように管理区域は可能な限り無窓の外壁等に囲まれた区画とすることとされる。しかし、実際には侵入が容易でない場所に設置されているが窓ガラスのある部屋であり、「京都府情報セキュリティ対策基準」を十分には満たしていない。

㈡ 出入口が二つある

「京都府情報セキュリティ対策基準」によれば、情報システムの管理区域から外部に通じる出入口は１箇所のみとしなければならない。しかし、実際には出入口が２箇所（廊下に別のドアがある）あるため、「京都府情報セキュリティ対策基準」に違反しているおそれがある。廊下側のドアについては、機器搬入や停電時などの出入口機能確保のため設置されているが、情報政策課で施錠について管理もされ、通常は利用されていないため、違反しているとまでは言い切れない。しかしながら、違反の懸念がある状態は少なくとも適切ではなく、規程の見直しも含めて検討されたい。

㈢ 施錠されていないラックがある。

カギのかけられていないラックがある（情報政策課管理分）。重要な機器があるためラックに管理している以上は、施錠を行い、厳重に管理する必要がある。

㈣ 保管状態が適切でないものがある。

情報資産の保管状態について、下記２点の問題点が発見された。

・バックアップデータの一部が、ラック外に保管されている。

・運用監視 PC もラック外にある。

これらはともに、重要な情報資産であるため、ラック内にて厳重に保管する必要がある。

㈤ 整理状態が悪い

廃棄予定の備品が多数あるなど、整理状況が不十分であるので、整理整頓されたい。

㈥ 部外者入室時の担当者立会不徹底

部外者が入室しているときに情報政策課職員が常に立ち会っているか確認したが、立ち会っていないときがあるとのことであった。情報政策課の事務室とは離れた場所にあるため、例えば、入室許可を受けた者が不許可者を入室させる可能性がある。そのため、常に立ち会うことが望ましいが、少なくとも必要に応じて監視カメラによる監視等の措置が必要である。

ii 府庁（防災情報サーバ室）

府庁（防災情報サーバ室）にも、下記のとおり、府庁電算室と同様の問題が発見された。

㈠ 窓がある。

問題点の内容は府庁電算室と同様であるため、詳細は省略する。

また、この他に当該サーバー室独自の問題点として、下記事項が発見された。

㈡ サーバ室の奥が職員ロッカーとなっている。

㈢ サーバ室が施錠されていない。

これらの問題も、当該サーバ室のセキュリティ上問題であるため、改善を検討されたい。

（サーバ室の視察の状況については「4.1サーバルームの状況」を参照いただきたい。）

2.3.5 災害対策・業務継続計画について

平成23年３月に東日本大震災が発生し、また、平成24年８月に、内閣府から南海トラフの巨大地震の被害想定が公表されるなど、災害対策・業務継続計画の重要性はますます高くなるものと思われる。そのため、災害発生時に復旧・稼動維持を優先すべきシステムを中心に、京都府の ICT における災害対策・業務継続計画の策定状況について検討した。

⑴ 現状　～災害のリスク分析状況～

「京都府地域防災計画」において、大規模災害の想定（風水害・震災・原子力発電所関連・各種事故）及び災害分析を行っており、京都府ホームページにも公表されている。

⑵ 現状　～業務継続計画の策定～

業務継続計画とは、「地方公共団体におけるICT部門の業務継続計画（BCP）策定ガイドライン」によると、「災害・事故で被害を受けても、重要業務をなるべく中断させず、中断してもできるだけ早急に（あるいは、許容される中断時間内に）復旧させる「業務継続」を戦略的に実現するための計画である。」とある。京都府では業務継続計画に関して下記の５規程を定めている。

①　京都府業務継続基本指針（平成21年９月策定）

府民生活に密着する行政サービスの提供や府の基幹業務などの「継続の必要性の高い通常業務」（以下「重要継続業務」という。）を、危機発生時においても継続もしくは早期復旧するための基本的な考え方を定めたものである。

②　京都府新型インフルエンザ対応マニュアル～社会対応版～（平成20年11月策定）

新型インフルエンザ発生に備えて、重要業務の継続ができるよう、京都府業務継続基本指針に基づき定めたものである。

③　京都府庁地震業務継続マニュアル（全庁版）（平成23年２月改正）

地震発生時においても適正に業務を執行するためのものであり、京都府業務継続基本指針に基づく地震対応版の業務継続計画（BCP）として定めるものである。

④　部局マニュアル、広域振興局（支部）マニュアル

京都府新型インフルエンザ対応マニュアル～社会対応版～、京都府庁地震業務継続マニュアル（全庁版）に基づいて、各部局・広域振興局で新型インフルエンザ対応版、地震対応版のBCPを定めたものである。

なお、京都府業務継続基本指針及び京都府庁地震業務継続マニュアル（全庁版）は京都府ホームページにおいて公表されているが、これらの規程において、情報システムに関して定めている内容を下記に記述する。

①　京都府業務継続基本指針

ⅰ　業務継続の基本方針

業務継続の基本方針については、下記のとおり定められている。

> ・府は、いかなる危機発生時においても、府民の生命・身体・財産を保護し、被害を最小限にとどめることを第一の責務としていることから、応急対策業務を中心とした、非常時優先業務を最優先に実施する。
> ・非常時優先業務に必要となる人員や資機材等の資源の確保・配分は、全庁横断的に調整する。
> ・非常時優先業務の実施に必要となる人員や資機材を確保するため、重要継続業務以外の通常業務については、積極的に休止・縮小する。その後、非常時優先業務に影響を与えない範囲で、順次再開する。

ⅱ　対象としている危機事象

本指針では特定の危機を想定せず、府庁の業務継続に影響を与えるすべての危機事象を対象とする。しかし、事象により業務継続に対する影響は大きく異なるため、代表事例として、「大地震の発生」と「新型インフルエンザのまん延」に係る業務継続対策について記述している（※１）。

（※１）危機事象の代表事例について

「地方公共団体におけるICT部門の業務継続計画（BCP）策定ガイドライン」によると、「大地震の発生」は「わが国ではどの地域でも発生の懸念のある大地震を想定した場合、火災等の二次災害及び電力途絶等事態も想定して対処することが求められることや、施設・設備等の損壊がテロ等の他の原因であっても対応が類似しているため、応用が容易である。」とされている。このことを考えると、「大地震の発生」は代表事例としては適当なものと考えられる。

また、「新型インフルエンザのまん延」は、当時は新型インフルエンザの対応が世間一般に大きく取り上げられていたときであることから、これを代表事例としている。現時点において新型インフルエンザそのものが、業務継続に重大な影響を及ぼす可能性があるかどうかは議論の余地があるものの、ある特定の伝染病を想定することによって、今後新たな伝染病が流行したときの対策にも用いることができるため、「新型インフルエンザのまん延」を想定することも適当なものと考えられる。

ⅲ　庁舎機能の確保

庁舎機能の確保については、下記のとおり定められている。

(ｱ)　電源の確保
(A)　非常用発電機の状況
電力の供給が途絶えた場合に備え、本庁、総合庁舎及び防災行政無線用として、非常用発電設備を備えている。各庁舎管理者等は、平素から発電設備用の燃料を確保する。
(B)　停電時の業務継続
各所属は、停電時に非常用電源に切り替わった場合に、業務の継続が可能となるよう、非常電源系統の差込口の所在を確認しておく。（本庁１号館のみ）
(ｲ)　通信手段の確保
電話回線の不通・輻輳などにより、通話が困難である場合、府防災行政無線や災害優先電話等を活用し、被災情報の収集・連絡、応急対策の調整等を行う。
(A)　電話回線（NTT 回線）の確保
本庁舎の停電や庁内電話交換機が損壊しても、電話回線が切断されない限り、各部局に配置されている災害時優先電話を直結することで最低限の電話回線（NTT 回線）が確保可能となっている。
また、災害時優先扱いの公用携帯電話を一定数保有している。
(B)　府防災行政無線の利用
府防災行政無線は、府庁、総合庁舎、市町村、防災関係機関等の防災拠点施設を結ぶ府独自の通信網であり、「京都デジタル疏水ネットワーク」を利用した地上系と、自治体衛星機構の通信衛星を利用した衛星系で２ルート化している。更に、地上系の回線についての二重化を進めている（※２）。(21年度「みやこネットワーク（仮称）整備」)
(C)　非常通信の利用
府防災行政無線のほか、携帯電話、衛星携帯電話、京都市防災行政無線、消防庁消防無線、国土交通省マイクロ回線等により、国やライフライン事業者等との通信を確保している。

（「(※２)」は監査人が追記したものである。）

(※２) 地上系の回線

京都府業務継続計画基本指針では、「地上系の回線についての二重化を進めている」とあるが、「第３監査の結果及び意見　１監査対象システムの概要　1.10衛星通信防災情報システム【図1.10.１京都デジタル疏水ネットワーク概念図】に記述のとおり現時点において二重化は完了している。

ⅳ　情報ネットワークシステムの維持

情報ネットワークシステムの維持について、下記のとおり定められている。

(ｱ)　体制の確保
(A)　運用委託事業者との関係
情報システムを所管する所属（以下「システム所管所属」という。）は、危機発生に備え、情報システムの運用を委託している事業者の体制を確保する。
・運用委託事業者の担当者と24時間連絡がとれる連絡体制
・運用委託事業者の担当者に不測の事態が発生した場合に備えた応援態勢
また、システム所管所属は、運用委託事業者からの支援が受けられない事態に備えて、府職員だけで最低限運用できる項目を洗い出し、緊急時運用マニュアルとして整備する。
(B)　代替職員の確保
システム所管所属は、各情報システムを担当する府職員が出勤できない事態に備えて、あらかじめ代替の職員を指名し、連絡体制を整える。
(C)　重要データ等のバックアップ
システム所管所属は、サーバが破損する事態に備えて、データ及びシステムのバックアップを庁舎内と庁舎外で保管する。
(ｲ)　障害発生時の対応
(A)　システムの状況確認
システム所管所属は、情報システム運用の可否、情報機器の破損状況等を把握するとともに、主管課を通じて業務推進課に報告する。
(B)　復旧対応
システム所管所属は、情報システムに障害が発生した場合、速やかに運用委託業者に連絡して復旧を求めるとともに、主管課を通じて業務推進課に報告する。
(C)　本部事務局の報告
業務推進課（※３）は、(A)及び(B)で把握した情報及び京都デジタル疏水ネットワークの状況等について本部事務局に報告する。

ⅴ　庁舎の代替施設の検討

(ｱ)　代替施設検討の必要性
本庁及び総合庁舎は、府の災害拠点施設であり、電源や通信手段の確保策を講じているが、現時点で予見できない不測の事態により使用ができない場合に備え、代替施設の確保を検討する。
(ｲ)　業務の一部の代替施設の候補
庁舎が被災した場合に備え NTT 施設の使用について NTT 西日本と協定を結んでいる。（※４）

（「（※３）」、「（※４）」は監査人が追記したものである。）

（※３）業務推進課

現在の情報政策課のことである。なお、京都府庁地震業務継続マニュアル（全庁版）にも業務推進課のまま、古い部署名が残っている。

（※４）代替施設の候補

代替施設の候補については、上述のとおり西日本電信電話株式会社（NTT 西日本）と「緊急時における西日本電信電話株式会社施設の使用に関する協定」を締結している。

② 京都府庁地震業務継続マニュアル（全庁版）

「８　情報ネットワークシステムの確保」に下記のとおり定められている。

i　現状

㈠　業務推進課が管理している全庁的な基盤となる京都デジタル疏水ネットワークや全庁的な情報システム（グループウェア、ファイルサーバ、文書事務、総務事務、統合財務等）については、サーバを府庁電算室とデータセンターに設置しているが、それぞれ耐震性の確保、転倒防止対策等を図っている。

㈡　電気の配電については、通常の配線と同様に施行されているため、断線の可能性は残っている。

㈢　府庁停電時においては、自家用発電機により京都デジタル疏水ネットワークをはじめ、各種情報システムは優先配電される。

㈣　情報システムの運用については、障害発生時には、各システムの運用委託事業者の担当者と24時間対応可能な連絡体制を確保している。

㈤　各情報システムに係るデーターについては、バックアップ体制は構築されている。

主なシステム	概要	サーバ等設置場所	停電時等
京都デジタル疏水ネットワーク	行政、防災、教育、医療等の各分野に広範囲に利用する、府の基幹となる情報ネットワーク （下表の情報システム全てがこの疏水ネットワークを利用） ※ UPS：無停電電源装置（30分程度の停電であれば稼動を継続する。）	・データセンター ・京都府庁 ・各振興局 ・各地域機関等	・データセンターは電源冗長化（センター内は電気回路を二重化） ・回線を NTT とケイオプティコムの二重化 ・他施設については、UPS の設置により停電に対応 ・ネットワーク機器の転倒防止対策を実施
行政事務支援システム	行政事務の効率化、高度化等を図るためのグループウェア（掲示板、メール）及びファイルサーバ等の事務処理支援システム	府庁電算室	・電算室内の UPS にて対応 ・サーバの転倒防止対策を実施
施策推進支援システム	府の施策に関する情報を共有するためのシステム		
新人事給与システム	給与関連事務の効率化、省力化等を目的とした、人事システムと給与システムが一体化したシステム		
電子申請システム	インターネットから、府・市町村あてに申請・届出（処理状況の公開を含む）手続を行えるシステム		
公共施設案内予約システム	インターネットや携帯電話から、府・市町村の公共施設の施設情報の閲覧、空き状況の確認、予約・抽選申込等が行えるシステム		
文書事務支援システム	起案、決裁、保管、廃棄まで文書のライフサイクル全般を管理する Web 方式のシステム	データセンター	・電源冗長化により稼働（センター内は電気回路を二重化） ・サーバの転倒防止対策を実施
統合財務システム	予算、歳出、歳入及び物品管理を行う財務システム		
総務事務システム	休暇・旅費など職員の各種申請手続を行うシステム		
e-ラーニングシステム	職員がいつでも学習できるシステムとして開発。また、府民向けにスポーツ生涯学習室がコンテンツを用意し、対府民向けの学習講習も実施		

統合型GIS	位置に関する情報を持ったデータ（空間データ）を一元的に整備・管理し、庁内横断的に共同利用するシステムで、視覚的に表示したり、高度な分析等を行うことができるシステム		
市町村・共同ポータルシステム	インターネットから、府・市町村あてにイベント参加申込の受付、各種申請書のダウンロード、行政情報等の提供を行えるシステム		

ii　課題

(ｱ)　基幹であるデジタル疏水ネットワークシステムが停止すると、全府庁の情報システム（地上系防災情報システムを含む）にも支障が生じるため、府庁舎での電気断線の保護対策等、より一層の稼働確保対策が必要である。

(ｲ)　情報システムの施設・設備の管理・運用については、特に専門性が高いこと、各情報システムごとに府情報システム担当者が相違し、また運用委託業者も相違していることから、府情報システム担当職員が出勤不可の場合の対応、業者から支援が受けられない事態への対応などが必要である。

(ｳ)　非常用電源を効率に使用するため、デジタル疏水ネットワークシステムなど災害時に使用するシステムを限定しておく必要がある。

iii　対策

(ｱ)　基幹であるデジタル疏水ネットワークシステムについて、府庁舎での電気回線の二重化などの断線保護対策等を進める。

(ｲ)　障害発生時における、府情報システム担当職員の参集方法、事前の代替職員の指名、府職員だけで最低限できる項目の洗い出しなど、情報システム運用確保のマニュアルやチェックシートを整備し、情報システム担当職員全員が共有する。

(ｳ)　運用委託業者に対して、緊急時の連絡体制だけではなく、参集時間・方法などを確認し、より確実な障害対策を調整・整理する。

(ｴ)　情報システム所管の部局においては、各種情報システムが使用できないことを想定し、手処理でも重要業務が執行できる体制を整える。

③　業務継続計画の見直しの状況

平成24年８月22日に京都BCP検討会議（注）が開催されるなど、東日本大震災等を踏まえた見直しの検討が、現在進められている。

（注）京都BCP検討会議

京都BCP検討会議とは、経済団体や電気、ガス事業者、大学等研究者が参加し、地震や水害、感染症などに見舞われても企業や府民の活動が継続できるよう、京都府全体でカバーしあう仕組みの構築を目指すための会議である。

④　指摘事項及び意見

上記の規程の内容について検討した結果、下記問題点が発見された。

i　緊急時運用マニュアルがない。

京都府庁地震業務継続マニュアル（全庁版）にも「情報システム運用確保のマニュアルやチェックシートを整備し、情報システム担当職員全員が共有する。」とあり、業務継続計画が着実に実行されるためには、作業内容を示したマニュアルが必要であるが、実際には、このようなマニュアル等は制定されておらず、早急に制定が必要である。

ii　主要なシステムが全て業務継続計画に反映されていない。

京都府庁地震業務継続マニュアル（全庁版）には、情報政策課所管分しか記載されておらず、他部署で所管しているシステムについては記述されていない。

情報政策課が所管しているシステム以外にも、主要なシステムは業務継続計画に反映して復旧対策等を講じる必要がある。

iii　サーバ設置場所が公表されていること

監査人が京都府ホームページを閲覧した際、京都府庁電算室及びデータセンターの設置場所が特定できる内容が公表されていた。

当然ながらデータセンターやサーバの設置場所は、セキュリティ上の観点からは秘匿すべき事項であるが、一方で法令等によって府民に対して公表せざるを得ない場合もある。

したがって、まずは可能な限り設置場所は秘匿することとし、止むを得ず公表する場合は、情報政策課は公表される内容を公表前に十分に確認し、セキュリティ上問題のない範囲での公表かを検討する必要がある。ま

た、併せて公表されることを十分に考慮して、強固な情報セキュリティ管理を行う必要がある。

ⅳ　府庁電算室・府庁（防災情報サーバ室）の脆弱性

上記「2.3.4(5)　アクセス管理３（サーバルームやマシンルームへの立ち入りの管理）」でも記載したとおり、府庁電算室及び府庁（防災情報サーバ室）は情報資産管理の観点から不十分な状況にある。特に府庁電算室は、その存在が公表されてしまった前提で考えると、あまりにも脆弱と言わざるを得ない。

そのため府庁電算室は特に、府庁に設置しているサーバを全てデータセンターに移管することにより、より強固な管理体制下に置くことを検討されたい。

ⅴ　京都府庁地震業務継続マニュアル（全庁版）の見直しが不十分

京都府庁地震業務継続マニュアル（全庁版）に記載の内容が、最新のものとはなっていないものがある。具体的には、地上系回線の二重化が完了していることが反映されていないこと、また、情報政策課が旧の部署名（業務推進課）となっていることがある。

大規模災害発生時に不要な混乱を無くすためにも、当マニュアルの内容を最新のものに更新する必要がある。

(3)　復旧対策の現状について

業務継続計画等については上記のとおりであるが、一方で復旧対策の現状についても検討している。今回の監査では、復旧・稼動維持を優先すべきシステムの選定状況とシステムのバックアップ体制について検討した。

ⅰ　現状１　～復旧・稼動維持を優先すべきシステムの選定状況～

上記のとおり、京都府業務継続基本指針４(1)ウ重要データ等のバックアップにおいて、「システム所管所属は、サーバが破損する事態に備えて、データ及びシステムのバックアップを庁舎内と庁舎外で保管する。」とある。

そのため、京都府において、復旧・稼動維持を優先すべきシステムを選定しているかを情報政策課にヒアリングした。その結果、情報政策課では選定していないとのことであった。また他のシステムの所管部署にも選定状況を確認したが、明確に定義されていない状況であった。ただし、実際に優先復旧が必要か否かを考慮している所管部署があったため、考慮している部署については、実状もヒアリングした。

（回答状況）

【図表2. 3. 5-1】

所管部署	管理対象システム	回答
情報政策課	新人事給与 行政事務支援 統合財務 総務事務	復旧等を優先すべきシステムは、情報政策課では定義していない。 ただし、防災関係及び府民向けシステム（例えば税務支援システムや衛星通信系防災情報システム）については、復旧等を優先すべきシステムと考えている。
人事課	人事	復旧等を優先すべきか明確に定義していない。 ただし、実際には当該システムは復旧等を優先すべきシステムとまでは考えていない。 （理由） 京都府職員の人事情報に関するものであるが、住所等連絡先など、災害発生時に必要となる情報は別途把握可能であり、その他のデータについては災害時に優先してまで復旧等をすべきものはない。
教職員課	教職員人事電算	復旧等を優先すべきか明確に定義していない。ただし、実際には当該システムは復旧等を優先すべきシステムとまでは考えていない。 （理由） 京都府内の教職員に関する人事情報であり、災害発生時に必要となる情報は別途把握可能である。また、その他の情報については災害時に優先して復旧すべきものではない。
税務課	税務支援	復旧等を優先すべきか明確に定義していない。 ただし、当該システムは復旧等を優先すべきと考えている。 （理由） 税務支援システムに保管している課税情報や収納情報等、個人情報に関するデータは府民にとって非常に重要な情報であり、優先復旧等が必要と考えている。
防災・原子力安全課	衛星通信系防災情報	復旧等を優先すべきか明確に定義していない。 ただし、当該システムは復旧等を優先すべきと考えている。 （理由） 災害情報を府民に提供するなど、災害発生時には重要なシステムであるため。

ⅱ　現状　～バックアップ体制について～

各システムのバックアップ体制は、下記のとおりである。

㈠　バックアップ頻度

【図表2.3.5-2】

システム	バックアップ頻度
新人事給与	（データ） 日次で実施。 （システム） 毎年１回定期メンテナンス時に実施。
人事	（データ） 日次で実施。 （システム） 人事異動の都度実施の他、システム改修の都度、改修部分をバックアップしている。
教職員人事電算	（データ） 週次で実施。このほか、データに変更のあった部分を日次で実施。 （システム） バックアップは、年間４～５回の頻度で実施。
税務支援	（データ） データ全体については、週次で実施。このほか、データに変更のあった部分を日次で実施。 （システム） 週次で実施。
行政事務支援	（データ） データ全体については、週次で実施。このほか、データに変更のあった部分を日次で実施。 （システム） データと同時にバックアップを実施。
統合財務	（データ） 日次で実施。 （システム） OS やミドルウェアのバージョンアップ等のシステム設定変更時に実施（当該システム稼働時から設定変更はないものの、平成23年度の機器更新時にバックアップを実施。）。
総務事務	（データ） 日次で実施。 （システム） ４か月毎に実施。
衛星通信系防災情報	（データ） 当該システムの主な目的が、災害情報を府民に公表することであることから復旧すべきデータはなく、バックアップは実施していない。 （システム） プログラム変更時に実施。

㈠　バックアップ保管場所

【図表2. 3. 5-3】

システム	バックアップファイル保管場所
新人事給与	府庁電算室に保管。
人事	府庁電算室に保管。
教職員人事電算	府庁電算室に保管。
税務支援	（データ） データセンターに保管。 （システム） 外部委託事業者（日本電気㈱京都支社）にて保管。
行政事務支援	府庁電算室に保管。
統合財務	データセンターに保管。
総務事務	データセンターに保管。
衛星通信系防災情報	外部委託事業者（沖電気工業㈱京都支店）にて保管。

㈡　リストアテストの実施状況

【図表2. 3. 5-4】

システム	リストアテストの実施状況
新人事給与	システム構築時に実施したが、それ以降は実施していない。
人事	（データ） 人事異動時（毎年３月）に実施。 （システム） 実施していない。
教職員人事電算	実施していない。
税務支援	（データ） 月１回の頻度で実施。 （システム） 開発時に実施したが、それ以降は実施していない。
行政事務支援	システム構築時に実施したが、それ以降は実施していない。
統合財務	システム稼動時及び平成23年度機器更新時に実施
総務事務	システム導入時に実施したが、それ以降は実施していない。
衛星通信系防災情報	プログラム変更時のみ実施。

（注）リストアテスト

リストアとはバックアップデータを用いてデータを元の状態に戻すことをいい、リストアテストとはバックアップデータが正常に元の状態に復元できることを確かめるために実施するテストをいう。

ⅲ　指摘事項及び意見

㈠　復旧等優先すべきシステムが明確に定義・認識されていない

上記のとおり、復旧を優先すべきシステム・データが明確に定義されていないが、大規模災害発生時に速やかな対応を図るためにも、明確に定義し、京都府庁地震業務継続マニュアル（全庁版）に状況を記述することが必要である。

㈡　バックアップが庁舎外保管されていない

本監査での検討対象としたシステムの多くでバックアップデータが庁舎外保管されていなかった。しかしながら、業務継続計画基本指針に定めているとおり、バックアップデータは庁舎外にも保管し、庁舎に大きな被害が発生した場合でもシステム復旧・データ復旧をできるようにする必要がある。

㈢　定期的にリストアテストを実施していない（人事、教職員人事電算、税務支援、衛星通信系防災情報）

リストアテストは、開発当初に実施したのみで、それ以降は実施していないシステムがある（人事システム、

教職員人事電算システム、税務支援システム、衛星通信系防災情報システム）。また、衛星通信系防災情報システムはプログラム変更の都度、リストアテストを実施しているのみである。

少なくとも、復旧を優先すべきシステム及びデータについては定期的にリストアテストを行い、いつ大規模災害が発生しても適時に復旧できるよう備える必要がある。

2.4　外部委託事業者の管理について

2.4.1　外部委託事業者への委託業務内容及び管理状況

⑴　委託業務の内容

京都府では、情報システムに関係する作業や管理の多くを外部委託事業者に委託している。

そのため、情報システムに関する管理状況の検討を行うにあたり、担当者にヒアリングするほか、外部委託事業者にもヒアリングを実施し、京都府が適切に外部委託事業者に対する委託管理を行っているか検討した。

（各システムの外部委託事業者（再掲））

【図表2.4.1-1】

システム	外部委託事業者
新人事給与	オムロンパーソネル㈱
	㈱ワークスアプリケーションズ（再委託先）
人事	㈱ケーケーシー情報システム
教職員人事電算	㈱ジェーワンシステム京都支店(注1)
税務支援	日本電気㈱京都支社
行政事務支援	㈱大塚商会京都支店
	㈱アルファネット（再委託先）(注2)
統合財務	㈱オーイーシー
総務事務	富士電機㈱関西支社
	㈱グローバルソフトウェア（再委託先）
衛星通信系防災情報	沖電気工業㈱京都支店
	㈱OKIソフトウェア（再委託先）(注3)
	㈱沖電気カスタマアドテック（再委託先）(注3)

（注１）㈱ジェーワンシステム京都支店は、実質的にはケイアイエスユー㈱の本社であり、形式上はケイアイエスユー㈱代表者が㈱ジェーワンシステム従業員として㈱ジェーワンシステム京都支店を運営している。なお、機器保守対応はケイアイエスユー㈱が実質的に再委託の状態で行っている。この問題点は、「2.5教職員課について」「3.4教職員人事電算管理システム構築業務、運用業務」を参照いただきたい。

（注２）㈱アルファネットは㈱大塚商会の連結子会社である。

（注３）㈱OKIソフトウェア及び㈱沖電気カスタマアドテックは、沖電気工業㈱の連結子会社である。

（業務内容・業務形態等）

【図表2.4.1-2】

システム	外部委託事業者	業務内容、業務形態
新人事給与	オムロンパーソネル㈱	（業務内容） ・システムの運用監視 ・給与計算、会計仕訳処理 ・帳票の出力 ・帳票の管理や帳票設計 ・運用管理 ・システムへの論理的アクセスの権限付与 （業務形態） 京都府庁に常駐して作業している。 （再委託先の管理状況） 変更管理については、作業の都度、外部委託事業者が検証を行って、適切な処理が行われているか確認している。
	㈱ワークスアプリケーションズ	（業務内容） オムロンパーソネル㈱から再委託を受け、開発・変更作業、障害対応等を行っている。 （業務形態） 普段は京都府庁には駐在しておらず、作業実施時に京都府庁に駐在して作業している。 （その他） ㈱ワークスアプリケーションズは当該システムを開発した業者である。
人事	㈱ケーケーシー情報システム	（業務内容） ・開発・変更作業 ・障害対応　など （業務形態） 普段は京都府庁には駐在していないが、作業発生の都度、本社（京都市内）で作業を行っている。
教職員人事電算	㈱ジェーワンシステム京都支店	（業務内容） ・開発・変更作業 ・障害対応 （業務形態） 当社は、普段は京都府庁には駐在しておらず、作業も本社（東京都内）で行っている（ケイアイエスユー㈱も普段は京都府庁には駐在していない。）。 障害発生時には、ケイアイエスユー㈱が㈱ジェーワンシステム事務担当者として京都府からの連絡を受け、ケイアイエスユー㈱が障害原因を分析する。システムに原因がある場合は㈱ジェーワンシステム担当者が対応し、機器に原因がある場合はケイアイエスユー㈱が対応する。 なお、機器保守はケイアイエスユー㈱が行っている。 (その他 セキュリティに関する事項) 作業に必要なデータは、当該システムからUSBメモリで抜き取り、本社に持ち帰って作業している。

税務支援	日本電気㈱ 京都支社	（業務内容） ・運用監視 ・開発、変更作業 ・障害対応　など （業務形態） 京都府庁に常駐して作業している。
行政事務支援	㈱大塚商会 京都支店	（業務内容） ・開発、変更作業 （業務形態） 京都府庁に常駐して作業している。
	㈱アルファネット	(業務内容) ・運用監視 ・障害対応 ・京都府職員のヘルプデスク（当該システムを操作するときの質問対応等） (業務形態) 京都府庁に常駐して作業を行っている。 (委託契約に関する事項) ヘルプデスク対応はパートナー契約を締結している個人に再委託している。
統合財務	㈱オーイーシー	(業務内容) ・運用監視 ・開発、変更管理 ・障害対応 （業務形態） 運用監視担当者は常駐。変更担当者は普段は京都府庁には駐在しておらず、関西支社（京都市内）で作業を行っている。 (その他 セキュリティに関する事項) 変更作業を行う場合は、一旦は当社関西支社でテストを実施するが、その際に京都府のシステムからデータを持ち出さず、当社でテスト用データを用いて作業している。また、当社で行ったテスト結果についても京都府のシステムに移行させず、京都府のテスト環境において、再度変更作業を行っている。
総務事務	富士電機㈱ 関西支社	(業務内容) ・開発、変更管理 (業務形態) 業務担当者は東京都内の事業所に駐在している。 (その他 セキュリティに関する事項) 作業に必要なデータは、運用管理端末からUSBメモリに抜き取り、京都府の各システムとは遮断されている環境から、パスワードをかけてメールで送っている。
	㈱グローバルソフトウェア	(業務内容) ・運用監視 ・障害対応 ・例外処理対応 (業務形態) ・京都府庁に常駐して作業を行っている。

衛星通信系防災情報	沖電気工業㈱京都支店 ㈱OKI ソフトウェア ㈱沖電気カスタマアドテック	(業務内容) ・開発、変更管理 ・障害対応 (業務形態) 沖電気工業㈱京都支店及び㈱沖電気カスタマアドテックの業務担当者は京都市内の事業所に駐在している。 ㈱OKI ソフトウェアの業務担当者は東京都内の事業所に駐在している。 (その他 セキュリティに関する事項) 作業に必要なデータ・プログラムは、沖電気工業㈱で保管しており、沖電気工業㈱の品質保証審査を経てUSBメモリもしくはCDに保存して、当該システムに移管する。したがって、当該システムからデータ等をコピーすることはない。 このような媒体は、沖電気工業㈱から持ち出すときと持ち帰ったときにウイルスチェックを行っている。

⑵　外部委託事業者の管理状況

対策基準及び契約書により、業務の全部又は一部の処理を再委託する場合は、書面により京都府の承諾が必要と規定されている。また、外部委託事業者と再委託を受ける事業者との契約を締結する場合においても対策基準5⑸外部委託に関する管理について明記することが定められている。そのため再委託を行っている業者について情報政策課及び防災・原子力安全課にヒアリングした。

なお、教職員人事システムも実質的に保守対応を再委託しているが、これについては、「2.5教職員課について」に記述した。

【図表2.4.1-2】

システム	再委託先との契約締結状況
新人事給与	再委託承認はしていない。 （理由） 当該システムの運用保守作業は、オムロンパーソネル㈱がシステム利用に必要なライセンスを㈱ワークスアプリケーションズから取得しており、基本的にオムロンパーソネル㈱が運用保守作業を実施。 ただし、バージョンアップなど比較的大きな作業が発生した際に、スポット的に㈱ワークスアプリケーションズが作業を実施している程度であるため、再委託との認識はしていない。
行政事務支援	再委託承認はしていない。 （理由） ㈱アルファネットは、㈱大塚商会の連結子会社であることから、実質的に㈱アルファネット担当者は㈱大塚商会の従業員と同等であること、また、IT業界ではよく見られる派遣のような形態であることから、再委託との認識はしていない。
総務事務	再委託承認はしていない。 （理由） ㈱グローバルソフトウェアは、富士電機㈱のいわゆる協力会社の立場にあり、実質的に㈱グローバルソフトウェア担当者は富士電機㈱の従業員と同等であること、また、IT業界ではよく見られる派遣のような形態であることから、再委託との認識はしていない。
衛星通信系防災情報	再委託承認は行っている。

2.4.2　指摘事項及び意見

⑴　委託契約書に改善の必要がある

対策基準５⑸外部委託に関する管理において、その管理方針が下記のとおり定められている。

> ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、下記の事項を明記した契約を締結するものとする。
> ア　基本方針及び対策基準の遵守
> イ　業務上知り得た情報の守秘義務
> ウ　府から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
> エ　府から提供された情報の返還義務
> オ　外部委託事業者の責任者や業務に携わる社員の名簿の提出
> カ　基本方針及び対策基準が遵守されなかった場合の損害賠償等の規定

（下線は監査人が追記。）

しかしながら下記のとおり、委託契約書締結時に対策基準を遵守していない事項があるため、改善する必要がある。

ｉ　外部委託事業者が京都府の規程を確認していない（８システム共通）

契約書に付随する業務仕様書に、外部委託事業者が「京都府電子計算組織等運用管理規程等関係規程を遵守すること。」としている契約があるが、外部委託事業者ではこれを確認していない。または、このような規程の遵守すら明記していない契約がある。

外部委託事業者に、京都府の情報セキュリティに関する事項を確実に遵守させるためには、外部委託事業者に

関連規程を十分に説明する必要がある。また、その説明時には、外部委託事業者からも管理状況について、京都府が要求する管理水準を保持しているか報告させるとともに、外部委託事業者の規程等を確認すること必要である。

ii　京都府による監査を受け入れることを明記していない（８システム共通）

そもそも対策基準に契約書に明記することを定めていないことが問題であるが、京都府が要求する管理水準を外部委託事業者に確保させるために、状況に応じて、京都府が外部委託事業者に対して監査を行うことを契約書に明記する必要がある。

なお、当該監査は京都府職員が直接行うほか、システム監査の専門家（監査法人など）に監査を委託することが考えられる。

iii　作業場所を特定していない（人事、教職員人事電算、税務支援、統合財務）

委託契約書において、外部委託事業者の作業場所を特定してない。作業場所を特定しない場合、情報資産の紛失の可能性が高まるため、作業場所を特定して情報資産の適切な管理等を外部委託事業者に実施させる必要がある。

iv　外部委託事業者の従業員であることを確認していない（８システム共通）

「オ　外部委託事業者の責任者や業務に携わる社員の名簿の提出」に関する事項が契約書に明記されておらず、実際に外部委託事業者から正規の名簿（委託契約書において、外部委託事業者を代表する者から提出された名簿）の提出を受けていない。そのため、外部委託事業者の従業員であることを対策基準に従って適切に確認できていない状況にある。

v　契約書全体の不備（教職員人事電算）

基本方針及び対策基準に規定されている事項のうち大半が、契約書に記載されておらず、情報セキュリティに関連する事項としては個人情報保護に関する事項が記載されているのみである。

vi　業務仕様書の不備（新人事給与、人事）

基本方針及び対策基準に規定されている事項の主要部分が、業務仕様書において遵守すべき事項として記載されているものの、基本方針及び対策基準において規定されている事項が完全に網羅されていない。

⑵　再委託承認が行われていない（新人事給与、行政事務支援、総務事務）

上述のとおり、対策基準及び契約書により、業務の全部又は一部の処理を再委託する場合は、書面により京都府の承諾が必要と規定されている。しかしながら、新人事給与、行政事務支援、総務事務の３システムにおいては、いずれの再委託先とも京都府の承諾が行われていない。

京都府において再委託を承認する際には、対策基準に示される「ア　基本方針及び対策基準の遵守、イ　業務上知り得た情報の守秘義務、ウ　府から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、エ　府から提供された情報の返還義務、オ　外部委託事業者の責任者や業務に携わる社員の名簿の提出、カ　基本方針及び対策基準が遵守されなかった場合の損害賠償等の規定」について、委託先と再委託先との間で適切に取り決められているかどうか、また、再委託先が反社会的勢力（注）等問題のある組織ではないか否かが、判断のポイントになる。

ここで断っておきたいが、再委託については上述の情報政策課の見解にもあるとおり、IT 業界ではよくあることであり、再委託そのものを否定するものではない。

しかしながら、過去に他の某地方公共団体において、再委託先が個人情報を不正使用したケースや流出させたために某地方公共団体に損害が発生した例や、平成24年11月に民間企業（金融機関）でも、某システム会社の再委託先従業員によるデータ不正使用が発覚している事例もあり、再委託先が問題を起こしている事例が多数あることも事実である。

この３システムは、他地方公共団体等の問題事例と比べて扱っているデータの重要性が異なるなど、一律に比較できるものではない。しかし、対策基準等で定められている以上、京都府が上記の判断ポイントに沿って確認の上で、再委託の承諾を行うことが必要である。また、判断ポイントを規程等のかたちで明文化することも検討が必要である。

ただ、外部委託事業者が①京都府に対して再委託の事実を意図的に伝えない場合や、②再委託承諾を回避するために派遣の形態を取る場合など、外部委託事業者が悪意を持てば、京都府としては再委託承諾の徹底が困難であることも事実である。しかしながら、これが再委託承諾を行わない理由にはなりえず、外部委託事業者が（再委託、派遣等契約の形態に関わらず）他の外部者に業務をさせる場合には、外部委託事業者に対して京都府の承諾を義務付ける必要がある。また、外部委託事業者が他の外部者に業務をさせていないと主張する場合には、その旨の念書を別途入手することも検討されたい。

なお、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成21年３月総務省）に、本件に関して参考となる記述があったため、下記に抜粋する。

外部委託事業者に対する個人情報の管理の在り方については、本検討において地方公共団体が実施すべき対策の具体的な方法論を提供をしたところであるが、この方法論の実践に関連した次のような解決困難な課題が存在する。
＜再委託についての課題＞
外部委託事業者からの個人情報の漏洩が増加している要因の一つには、外部委託事業者がコスト削減のため受託業務の遂行に当たって必要な要員を自社よりも低コストである社外に求めていることがあげられる。ICT 業界においては、冒頭で述べたとおり、再委託・再々委託という形で業務が取り扱われていることが常態化している。
現状では、元々社内にあったエンジニア部門や保守部門などを子会社化している、開発のために必要な技術者を案件に応じて外部から調達しているといったように、業務の再委託・再々委託は外部委託事業者の事業戦略に関わる場合が多く、一律に再委託・再々委託を禁止すると、委託先が確保できないといった事態が生じるおそれが高い。したがって、個人情報の取り扱い上問題が発生しやすい再委託・再々委託といった形態を一律に禁止するかどうかについては、今後も慎重な検討が必要である。
しかしながら、業務の再委託・再々委託は原則禁止であると契約上確実に明記し、契約に反して再委託・再々委託が行われた場合には厳格に事業者の責任を追及するといった対応・事例を確実に積み上げることにより、安易な再委託・再々委託を消滅させる不断の努力が必要である。

（注）反社会的勢力について
反社会的勢力とは、暴力団員及び暴力団員と社会的に非難されるべき関係を有する者を言う。なお、京都府暴力団排除条例第６条において、「府は、公共工事その他の府の事務又は事業により暴力団を利することとならないよう、暴力団員及び暴力団員と社会的に非難されるべき関係を有する者について、府が実施する入札に参加させない等の必要な措置を講じるものとする。」と定められている。

⑶　データのやりとりが対策基準に沿っていない（教職員人事電算、総務事務、衛星通信系防災情報システム）
上述のとおり、一部の外部委託事業者において、USB メモリにデータを保管して、これを持ち運びしているケースがあるが、その際のデータのやりとりが、対策基準に沿っていない。具体的には、情報セキュリティ責任者の許可なく USB メモリが庁舎内に持ち込まれており、また、京都府によるウイルスチェックが未実施のまま、USB メモリの接続が行われている。このような状況において、万が一事故が発生した場合、責任があいまいとなるおそれがあるため、対策基準を適切に遵守する必要がある。
（対策基準再掲。下線は監査人が付けたものである。）

・情報セキュリティ責任者の許可なく、府の情報システム以外のパソコン並びに USB メモリ、メモリカード等の外部記憶装置及び外部記憶媒体（以下「機器等」という。）を庁舎内に持ち込むこと。
・府の情報システムに機器等を接続する場合、情報セキュリティ責任者、IT 推進員又は情報セキュリティ操作認定者がウイルスチェックを実施した後、直接又はその指揮の下で職員等が行うものとする。

⑷　府による監査が行われていない（８システム共通）
上述のとおり、そもそも契約書に明記されていないためではあるが、外部委託事業者に対する監査が実施されておらず、定期的に実施する必要がある。特に府庁に常駐していない外部委託事業者に対しては、優先的に監査を行い、外部委託事業者の管理状況を確認する必要がある。

2.5　教職員課について（規程遵守の不徹底等）
教職員課による教職員人事システムの管理状況については、多数の問題点が発見されたが、その根本的な原因は、教職員課で定めた「情報セキュリティ実施手順」を適切に遵守すべきとの意識の低さが原因であると言える。それを示す教職員課の回答について以下に記載する。

⑴　指紋認証を使用していないことについての回答
教職員課担当者が実際に指紋認証を使用していないことについて、なぜ使用していないか質問を行った際にも「各教育局では指紋認証を使用しており問題ない。」との回答を得た。指紋を読み取れないという指紋認証装置の不具合が発生していたために業務に支障を来たすことが原因とのことであるが、不具合は直ちに修正すれば良いだけのことである。そもそも各教育局に実施手順の遵守を指導すべき立場にある教職員課が適切に実施手順を遵守していないことは、その立場上からも問題である。

⑵　実質的な再委託の問題
ケイアイエスユー㈱は機器保守対応を行っているが、これは機器賃借にかかるリース契約締結時にケイアイエスユー㈱が保守契約のサポート体制として書類提出されているためである。
したがって、リース会社からケイアイエスユー㈱に再委託されている状況にある。対策基準等で定められている以上、京都府による承諾は必要であり、再委託の承諾が行われていないことは上述の再委託に関する事項と同様に問題である。

⑶　外部委託事業者の契約代表者の形骸化

平成24年４月１日に㈱ジェーワンシステムと締結した委託契約書を確認したところ、㈱ジェーワンシステムの契約代表者は京都支店長となっている。しかしながら、そもそも京都支店は実質的に存在していない。すなわち、実質的に会社を代理する権限の無い者と契約締結を行っている状態にあるため問題である。契約そのものの有効性に関わる問題であり、㈱ジェーワンシステム代表取締役を契約代表者として契約締結を行う必要がある。

⑷　実施手順に開発・変更に関する事項がないことについての回答

監査の過程で㈱ジェーワンシステムの社長及びケイアイエスユー㈱社長（㈱ジェーワンシステム従業員も兼ねている。）に開発・変更に関する規程・手順等の制定状況についてヒアリングを行ったところ、「当社では、開発・変更に関する規程等を定めていないが、そもそも教職員課の実施手順に開発・変更に関する規程がないので、規程等を定める意味がない。」との回答であった。また、当該回答時に同席していた教職員課の見解を確認したが「実施手順に準拠しており、外部委託事業者の管理状況に問題がない。」との回答であった。

包括外部監査は、外部委託事業者の管理体制そのものを監査するものではないため、本来的には外部委託事業者の管理体制等に対して指摘するものではない。だが、外部委託事業者に規程等がないことは、情報システム管理上問題である上に更に、それを社長自ら問題と感じていないことは、地方公共団体のシステムを開発する業者としては不適切と言わざるを得ない。

また、教職員課は、このような回答を行った外部委託事業者に対して、何ら指摘を行わなかったが、通常は外部委託事業者に対し、その場で指導を行うべきである。問題点が発見されれば、これを良き機会と捉えて、改善につなげようとする意識が最も大切であると考える。

なお、教職員課の問題点については「3.4　教職員人事電算管理システム構築業務、運用業務」を参照いただきたい。

3　契約の状況

3.1　調達方式の概要

地方公共団体での契約方式については、大別すると入札（一般競争又は指名競争）と随意契約（企画提案公募方式又は単独随意契約）の２種類に区別される。

一般競争入札が調達方式の原則であるが、システム開発のように価格のみでなく特殊な技術等の評価を必要とする契約においては、企画提案公募方式も多く採用される。

企画提案公募方式は、外部委員等を交えた厳正な審査結果に基づいて受託業者を決定するのであるが、価格だけで入札する形式での契約でないため随意契約に区分される。随意契約においては、「なぜ競争入札によらなかったのかという」理由が必要である。

監査対象としたシステムの契約方式については、①一般競争入札、②企画提案公募方式、③単独随意契約の３種類が採用されている。開発業務については、企画提案公募方式を採用するケースが多く、一般競争入札は８契約中１件のみであった。

＜企画提案公募方式とは＞

企画提案公募において特定決定された者から見積書を徴し、当該見積金額が予定価格の範囲内であれば地方公共団体の物品等又は特定役務の調達手続の特例を定める政令（平成７年政令372号）第10条第１項第１号の規定により、その者と随意契約を締結する方法。

＜随意契約が行える場合＞

既に調達をした物品等（以下「既調達物品等」という。）又は既に契約を締結した特定役務（以下「既契約特定役務」という。）につき、交換部品その他既に調達物品等に連接して使用する物品等の調達をする場合又は既契約特定役務に連接して提供を受ける同種の特定役務の調達をする場合であって、既調達物品等又は既契約特定役務の調達の相手方以外の者から調達をしたならば既調達物品等の使用又は既契約特定役務の便益を享受することに著しい支障が生ずるおそれがあるとき。

3.2　監査対象とした個別契約（開発、運用保守）

今回の監査対象である８システムについて、①その開発業務と、②その後の運用保守業務について、契約手続の適切性を検討する。

監査対象となる個別契約の主な内容は、以下の通りである。

⑴　人事システム開発業務、保守運用支援業務
⑵　教職員人事電算管理システム構築業務、運用業務
⑶　新税務電算トータルシステム開発業務、運用業務
⑷　衛星通信系防災情報システム整備工事、保守管理業務
⑸　内部事務アウトソーシング導入業務、運用業務／人事給与システム開発業務、運用業務
⑹　行政事務支援システム開発業務、運用業務

⑺　統合財務システム開発業務、運用業務
⑻　総務事務システム開発業務、運用業務

3.3　人事システム開発業務、保守運用支援業務
3.3.1　契約の概要（【図表3.3.1】）

【図表3.3.1】人事システムの契約概要

システム名	人事システム					
所管部署	知事直轄（職員長）／人事課					
運用開始	平成18年10月					
監査対象契約	①人事システム開発業務　　平成18年2月契約					
	②人事システム保守運用業務　　平成18年10月契約以降					
入札契約方式	①開発	企画提案公募方式（運用業務のトータルコストを考慮する）				
	②運用	随意契約				
経費	（単位：千円）					
	年度	開発	改修	保守運用	機器賃借 端末	合計
	H18年	83,790			22,681	106,471
	H19年			3,675		3,675
	H20年			5,250		5,250
	H21年			5,250		5,250
	H22年		2,719	5,250		7,969
	H23年		9,871	5,250	9,463	24,584
	H24年			5,250		5,250
	合計	83,790	12,590	29,925	32,144	158,449

3.3.2　システムの概要
現行のクライアントサーバ型の旧システムを見直し、総務事務システム、給与電算システム等関連システムとの容易なデータ連携を可能とするとともに、GUI、庁内 LAN の活用等により人事業務の効率化、ペーパーレス化を図るため、新たな人事電算システムを構築・導入するものである。
また、開発に当たっては、汎用パッケージソフトウェアをベースに、京都府の人事業務に合わせたカスタマイズを行うこと、端末側に専用ソフトを必要とせず、インターネットブラウザのみで動作可能な Web 型方式を採用するなどにより、低コスト化を図った。
新たな人事システムは、従来同様に職員情報の管理、職員の採用、退職、異動等人事業務の支援、組織管理、各種帳票作成を行うことに加え、総務事務・給与電算等他システムと職員に関するデータを相互に連携することで、人事関連業務を効率的・効果的に行うことを目指すものである。

3.3.3　開発の契約手続の適切性の検討
⑴　契約方式は適切に選択されているか
業者選定は、運用等のトータルコストも考慮した企画提案公募方式が採用された。
企画提案コンペ説明会への参加業者は13社、うち12社が辞退し、企画提案に参加した業者は１社であった。
（随意契約とする理由）
低コストのシステム開発を目的としており、平成18年度以降の開発、運用等の経費も提示させることにより、トータルコストを踏まえた業者選定を行う必要がある。
最新の技術を用いた開発を行うため、当該システムの開発等を行うに足る技術力やノウハウの有無を的確に見極める必要がある。
当該システムは、総務事務システム、給与電算システム等関連システムとのデータ連携を前提にしており、その円滑な導入に向けての調整が必要である。
別添仕様書にて要求する機能、性能を有する人事システムを開発させるものであり、特殊な技術が求められる特定役務に該当する。
⑵　予定価格は適切な積算根拠に基づき設定されているか
システム開発に係る経費積算内訳において、人件費の単価は、一律「900千円／人月」として積算が行われている。

また、改修業務についての経費積算についても、同様の一律単価による積算が行われている。業務内容に応じて人員の単価は異なるのであるから、詳細な人員別工数の見積を行うとともに、その設定単価については、実勢価格の把握に努めることが必要である。

一律単価の妥当性について、人事課に質問を行ったが、「全庁的に予算要求単価が一律「900千円／人月」であるため、妥当であると考えている。」との回答であった。これは、人事課だけの問題ではなく、システム開発等の経費積算に当たって全庁的に考慮すべき事項であり、経費積算の緻密なルールの検討が望まれる。

⑶　実施された業者選定手続、契約手続はルールに準拠して行われているか

企画提案への参加業者は１社のみである。企画提案の評価は、９名の評価者により行われ、京都府電子府庁推進委員会の評価結果を踏まえて採用が決定された。

企画提案書の評価一覧及び評価概要の記述において、採択に疑問を生じるものはなく、また、契約手続においても指摘すべき事項はない。

⑷　その他検討した事項

①平成18年度の当初の機器賃貸借及び機器保守の契約、平成23年度の機器更新において行われた機器賃貸借及び機器保守の契約は、汎用機器の調達であることから一般競争入札によって行われており、指摘すべき事項はない。

②平成22年度及び23年度において、システムの改修業務が生じており、この契約は開発業者と単独随意契約で行われているが、これらの契約の随意契約理由や契約手続において、特に指摘すべき事項はない。

⑸　指摘事項及び意見

（予定価格積算における人件費単価について）

予定価格の積算において、人件費の単価が一律「900千円／人月」として積算されているが、業務内容に応じて人員の単価は異なるのであるから、詳細な人員別工数の見積を行うとともに、その設定単価については、実勢価格の把握に努めることが必要である。

一律単価の問題は、システム開発等の経費積算に当たって全庁的に考慮すべき事項であり、経費積算の緻密なルールの検討が望まれる。

3.3.4　運用の契約手続の適切性の検討

⑴　契約方式は適切に選択されているか

システムの保守運用業務については、システムの開発業者と単独随意契約による委託契約が締結されており、システム運用開始（平成19年10月）から現在に至るまで、１年契約で毎年更新されている。

（随意契約の根拠と理由）

人事システム本体の保守や運用に係る支援を円滑かつ確実に履行することができるのは、当該システムを独自に開発し、その内容に精通している開発業者が唯一の業者であるため。

⑵　予定価格は適切な積算根拠に基づき設定されているか

運用経費については、システム開発時の企画提案書において提示された年間5,250千円で毎年契約が更新されている。

ただし、平成24年度以降は、当初の契約から５年間を超える更新となる。企画提案においては、５年間の運用経費の提案となっていることから、今後の更新に当たっては、運用内容についての工数見積や単価設定について、新たに詳細な人員別工数の見積を求めるとともに、その設定単価についても提示を求め、経費積算の妥当性を検討する必要がある。

⑶　実施された業者選定手続、契約手続はルールに準拠して行われているか

指摘すべき事項はない。

⑷　その他検討した事項

該当事項なし

⑸　指摘事項及び意見

（運用業務の経費積算について）

保守運用業務について、企画提案においては５年間の運用経費の提案となっていることから、６年目以降となる今後の更新に当たっては、新たに詳細な人員別工数の見積を求めるとともに、その設定単価についても提示を求め、経費積算の妥当性を検討する必要がある。

3.4　教職員人事電算管理システム構築業務、運用業務

3.4.1　契約の概要（【図表3.4.1】）

【図表3.4.1】教職員人事電算管理システムの契約概要

システム名	教職員人事電算管理システム				
所管部署	教育委員会／教職員課				
運用開始	平成16年8月				
監査対象契約	①教職員人事電算管理システム構築業務　平成15年11月契約				
	②教職員人事電算管理システム運用業務　平成16度契約以降				
入札契約方式	①開発	企画提案公募方式			
	②運用	随意契約			
経費	（単位：千円）				
	年度	開発	運用	機器賃借	合計
	H16年	25,200	2,880	15,555	43,635
	H17年		4,363		4,363
	H18年		4,363		4,363
	H19年		4,363		4,363
	H20年		4,363		4,363
	H21年		4,363	17,646	22,009
	H22年		4,363		4,363
	H23年		4,363		4,363
	H24年		4,363		4,363
	合計	25,200	37,784	33,201	96,185

教職員人事電算管理システムは、平成18年度公務員制度改革に伴う教職員評価制度への活用や人事作業に伴う業務量の軽減を図るため、京都府内の市町（組合）立小学校及び中学校（京都市立を除く。）並びに府立高等学校及び特別支援学校の教職員の人事情報をデータベースサーバにより一元管理し、人事管理業務を電算処理するためのシステムである。

①開発の契約方式は、企画提案公募方式で行われ、②その後の運用業務は、保守の技術的能力の見地から開発の請負業者と随意契約が行われて現在に至っている。

3.4.2　システムの概要

⑴　基本仕様

①京都府教職員人事データシステム上の人事データについて管理業務を実施

②本システムは府行政事務支援システム上に構築

③教育庁内に管理者専用端末を設置し、データの入力、修正、帳票出力を実施

④府内５箇所の教育局に本システム専用端末を設置し、データの入力、修正、帳票出力を実施

⑵　事業概要

教職員の人事情報は手書きのカード等を用いて管理しているが、データ入力及び参照、分類等の作業効率や、カードの保管等のセキュリティ面において改善の余地がある。これに対応するため、人事情報をデジタルデータとして保管することとし、現在「教職員人事データベースシステム構築業務」によりデータベーススキーマ設計及びデータ入力作業、データ確認作業を行っている。

同業務により作成されたデータベースを活用し、人事異動作業をコンピュータ上行うことで、業務の簡素化及び信頼性の向上を図るとともに、様々な帳票の作成及び出力を可能にする。また、適材適所の人事配置の実現に向け、研修記録等、府内教育機関に分散している情報の一元管理を行う。

3.4.3　開発の契約手続の適切性の検討

⑴　契約方式は適切に選択されているか

業者選定は、企画提案公募方式（随意契約）により行われた。

（随意契約による理由）

システム開発に必要な業務調査や設計業務は、教職員人事の実態を的確に把握し、関係する多種多様な技術的知識を組み合わせることができる総合力が不可欠であり、単に表面的な技術力の有無や価格で判断できるものではな