平成２９年度

包括外部監査結果報告書

【概要版】

「情報システムに関する事務の執行について」

平成３０年３月

和歌山県包括外部監査人

公認会計士　坂井俊介

目次

1　包括外部監査の概要

1.1　外部監査の種類

地方自治法第 252 条の 37 第１項及び第２項に基づく包括外部監査

1.2　選定した特定の事件（テーマ）

情報システムに関する事務の執行について

1.3　特定の事件（テーマ）を選定した理由

行政運営の効率的・効果的な執行のためには、情報システムの活用が必要不可欠となっている。また、和歌山県においては、南海トラフ地震や土砂災害をはじめとする自然災害への対応のために各種の情報システムが整備されており、その果たすべき役割は非常に重要なものとなっている。そのため、情報システムの整備については毎年多額の投資を要し、その保守管理についても多くの予算が割り振られている。

しかしながら、自治体の組織構造及び予算制度に起因して、各種の情報システムの整備・運用については各所管部署任せになっており全庁的な調整が行われていないこと、情報システムの機能設定や保守内容等についてベンダー任せになっていること等が懸念される。

さらに、情報化が加速し続けている現在の社会環境においては、情報システムへの不正アクセスやサイバー攻撃等により蓄積されたデータの改ざん・個人情報の漏えい等のリスクも拡大しており、情報セキュリティ対策の重要性が高まっている。県が取り扱う情報には、県民の個人情報のみならず行政運営上重要な情報などが含まれており、漏洩、損傷等の事故があった場合は極めて重大な結果を招きかねない。そのため、県は、平成 16 年に和歌山県情報セキュリティポリシーを策定するとともに、全職員の使用するパソコンデータを集中管理する情報システム（シンクライアントシステム）を導入し、情報セキュリティに関する先進的な対応を行ってきたところである。

しかしながら、情報セキュリティに関する認識が全庁的に統一されていなければ、重大なセキュリティ事故を招く可能性がある。

県は、全国でも深刻な少子高齢化の状況にあり、その対応のために財政負担が今後増大することが予想されるが、そのような状況の中で情報システム関連費用はこれからのＡＩ社会の到来により更に増大していく恐れもある。また、さらなる情報化の加速により情報管理に関する重要性が高まっていくと考えられる。そのため、情報システムの調達・保守・情報管理等に関する事務の執行について、経済性、効率性及び有効性の観点から監査を行うことは県民にとって有意義であると判断し、特定の事件として選定する。

1.4　包括外部監査対象期間

平成 28 年度（自平成 28 年４月１日　至平成 29 年３月 31 日）

ただし、必要に応じて過年度及び平成 29 年度の一部についても監査対象とした。

1.5　外部監査の方法

1.5.1 監査の要点及び視点

県が保有する各情報システムの調達及び運用保守に関する財務事務、及び、各情報システムのセキュリティ対応について、法令等への準拠性、有効性、効率性の視点を中心に、以下の事項を監査の視点とした。

- 情報システムの調達に関する財務事務が、関係法令、条例、規則等に準拠して適切に行われているか
- 情報システムの調達が、支出額に見合った成果を収めているか
- 情報システムの運用保守に関する財務事務が、関係法令、条例、規則等に準拠して適切に行われているか
- 情報システムの運用保守が、支出額に見合った成果を収めているか
- 情報システムのセキュリティ対応について、想定されるリスクを勘案して適切に行われているか

1.5.2 主な監査手続

- 全庁レベルでの情報システムの調達や運用保守に関するルール及び情報システムのセキュリティ対応の状況に関して
  - 県が定める情報処理関連の諸規程等を閲覧し、県が取り組んでいる情報システムの調達や運用保守に関する事務手続、職務分掌、モニタリング方法等を把握する。
  - 情報システム施策の知事部局における統括部署である情報政策課に対して情報システムの調達、運用保守に関する事務手続及び内部統制の整備・運用状況をヒアリングする。
  - 県が保有する 126 件の情報システムの概要、予算の執行、調達及び保守における事務執行、セキュリティ管理の状況等について各所管部署に対し「調査票」を配布し、個々の情報システムの管理状況を把握する。
- 調査票の回答を吟味し、金額的重要性、情報の機密度、内部統制の観点等から情報システム 12 件を抽出し、個別にヒアリング及び関係書類閲覧による調査を実施する。また特に必要と認めた場合は、情報システムの管理状況について現地視察を行う。

1.6　外部監査の実施時期

平成 29 年４月１日から平成 30 年３月 31 日まで

1.7　外部監査人補助者の資格と名称

公認会計士	坂井俊介
公認会計士	池田学
ＩＴコーディネータ	西脇弘
公認会計士	駒井健二郎
公認会計士	前橋佑也
公認会計士試験合格者	永田祐司

1.8　利害関係

包括外部監査の対象とした事件につき、地方自治法第 252 条の 29 に規定する利害関係はない。

1.9　本報告書の取り扱い

本報告書は地方自治法第 252 条の 37 第５項の規定に基づく包括外部監査の結果を記したものである。同 252 条の 31 第１項の趣旨に基づき、特定のテーマを選定し、包括外部監査人の視点から限られた時間と予算の中で調査を実施し、その結果検出した事項の範囲で結果及び意見を述べたものであり、事務執行全般について何らかの保証を与えるものではない。

2　調査票による個別システムの概要調査

2.1　調査対象及び調査票の内容

県が保有する情報システムの件数が多いことから、全てのシステムを対象に深度ある監査を実施することが困難である。そこで、平成 28 年度末において、県が所有する情報システム全件について、所管部署に調査票を配布し、情報システムの概要及び調達や運用保守の状況、セキュリティ等の状況についての概要を把握することとした。当該調査票による概要調査の結果を踏まえ、詳細な監査を実施する個別システムの選定を行い、効果的・効率的な監査に結び付けていく趣旨である。

2.2　詳細な監査対象として選定する際の観点

以下のような特徴を１つ以上有する情報システムを詳細な監査対象として選定した。

(ア)情報システムの当初の開発投資額が大きい。
(イ)情報システムに対して、近年大きな改修を行っている。
(ウ)情報システムの開発時期が古い。
(エ)情報システムの管理体制にセキュリティ上のリスクがある。
(オ)情報システム内で個人情報を保管していると考えられる。

上記の観点について補足説明する。

(ア)情報システムの当初の開発投資額が大きい。

情報システムの開発投資額の大半は、システム開発要員の人件費である。開発投資額が大きい情報システムは、システム開発要員が多数関与していることが多く、当該システムは大規模かつ複雑なものであると推測される。

大規模かつ複雑な情報システムは、県にとっての重要性が大きいことから、当該情報システムの管理状況について検討する必要性は大きいと考えられる。

なお、情報システムによっては当初の開発投資額に関する資料が保管されておらず、開発投資額を確認できないものもある。

(イ)情報システムに対して、近年大きな改修を行っている。

開発と同様、改修額が大きい場合、大規模かつ複雑な機能追加を実施している可能性がある。したがって当該改修は、県にとっての重要性が大きいことから、当該情報システムの管理状況について検討する必要性は大きいと考えられる。

(ウ)情報システムの開発時期が古い。

情報システムの中には、20 年以上前に開発されたものもある。このような開発時期が古い情報システムは、時代の変化に対応できておらず、情報システムが十分に活用できていないおそれがある。また、時間の経過により仕様書や設計書などの情報システムにとって重要な書類の保管が適切に実施されていないおそれもある。

したがって開発時期が古い情報システムを検討する必要性は大きいと考えられる。

(エ)情報システムの管理体制にセキュリティ上のリスクを有する可能性がある。

情報システムによって容易に大容量のデータを保有し活用することができる。しかし、情報システムの管理体制にセキュリティの状況が適切でなければ、データ流出のおそれがある。

県が保有する情報システムで取り扱うデータが外部に流出すれば、社会的な影響が大きく、情報システムのセキュリティは重要である。

したがってセキュリティ上のリスクを有する情報システムに対して、詳細な検討を実施する必要性は大きいと考えられる。

(オ)情報システム内で個人情報を保管していると考えられる。

前述のとおり、情報システムにはデータ流出のリスクがあるが、仮に当該情報システムが個人情報を有していれば、データが流出した際の社会的な影響がさらに大きくなると考えられる。

したがって個人情報を保有している情報システムは、詳細な検討を実施する必要性は大きいと考えられる。

詳細調査対象として以下の 12 の情報システムを選定している。

No.	所管部署	システム名称
1	人事課	人事管理システム
2	人事課職員厚生室	職員健康管理システム
3	情報政策課	シンクライアントシステム
4	情報政策課	県立情報交流センター情報システム
5	福祉保健総務課	生活保護システム
6	障害福祉課	身体障害者手帳等交付管理システム
7	財政課	新地方公会計システム
8	税務課	県税運営システム
9	教育庁総務課	校務支援システム
10	教育庁学校人事課	人事管理電算処理システム
11	道路保全課	道路情報管理システム
12	会計課	財務会計システム

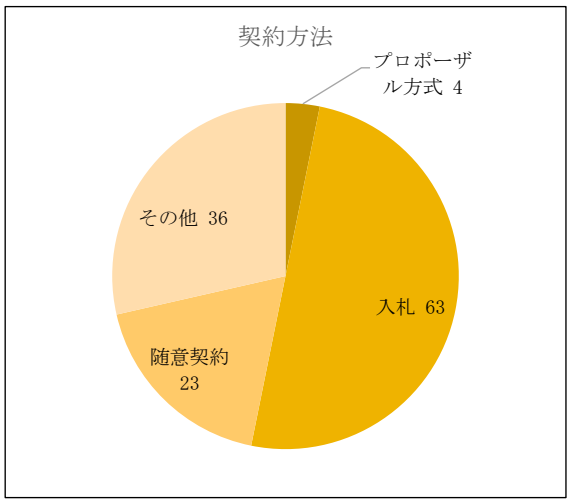
なお、調査票の回答内容をもとに監査人の判断で該当の有無を判断したものであり、例えば、上述（エ）に該当があるからと言って、実際にセキュリティ上のリスクがあるというわけではない。セキュリティ上のリスクが検出された情報システムについては、後の監査の結果及び意見の項で詳述する。

調査票に記載した質問項目は以下のとおりである。

項目	細目
1.情報システムの概要	・ 情報システムの名称 ・ 導入目的 ・ 開発時期（期間）及び供用開始日 ・ 導入時の支出額 ・ これまでの改修・更新の概要及び金額 ・ その他説明
2.最近５年間の情報システムに関する予算の執行状況	－
3.調達	・ 意思決定の方法 ・ 調達にあたっての費用対効果の検証 ・ システム調達費用の決定方法 ・ 契約方法 ・ 検収方法
4.保守	・ 契約内容 ・ システム保守費用の決定方法 ・ システム導入当初の契約方法 ・ 検収方法
5.物理的・論理的セキュリティ管理	・ 最近３か年で生じた運用上の障害 ・ 障害・災害への対応方針 ・ ＩＤ管理 ・ パスワード管理 ・ 情報漏えいへの対応 ・ プログラム管理
6.その他	・ 情報システム監査の実施の有無 ・ 有効活用 ・ 改修・更新の要望（追加で必要と考える機能） ・ その他

2.3　主な調査項目の集計結果

①　平成 28 年度新規調達システムの契約方法



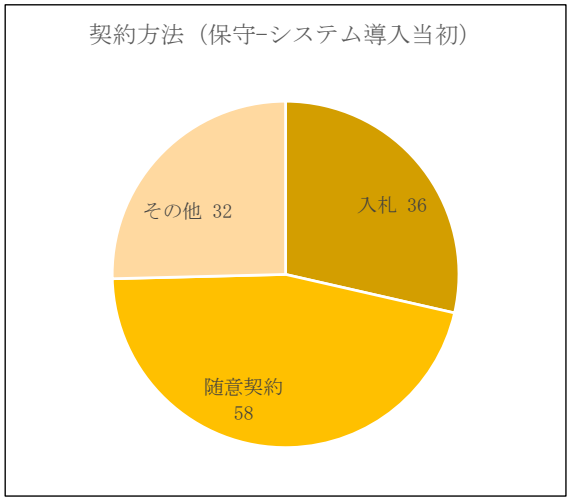
プロポーザル方式	4 件
入札	63 件
随意契約	23 件
その他	36 件
合計	126 件

調達の契約方法は、63 件（50.0%）が入札であり、随意契約は 23 件（18.3%）であった。その他 36 件（28.6%）は導入年度が古く、保存年限が経過しており導入方法が不明であるもの等である。

②　調達の検収方法

検収担当者は、課内の職員とする回答が大半であった。

③　保守の契約方法（システム導入初年度）

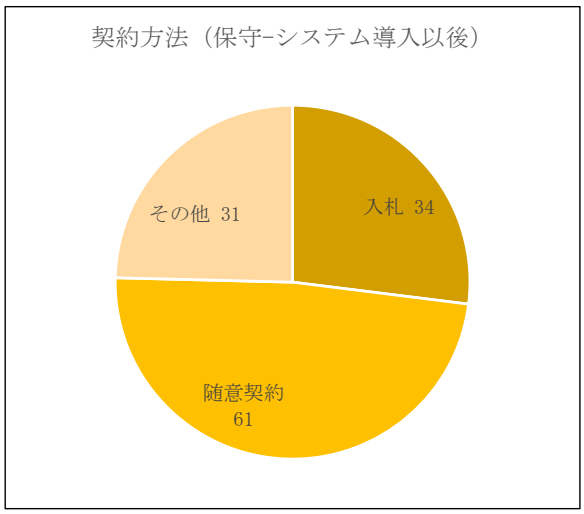


入札	36 件
随意契約	58 件
その他	32 件
合計	126 件

システム導入後の初年度における保守の契約方法は、36 件（28.6%）が入札であり、随意契約は 58 件（46.0%）であった。その他 32 件（25.4%）は導入年度が古く、保存年限が経過しており導入方法が不明であるもの等である。

システム調達に比べ保守については随意契約の割合が大きくなっている。

④　保守の契約方法（システム導入年度以降）



入札	34 件
随意契約	61 件
その他	31 件
合計	126 件

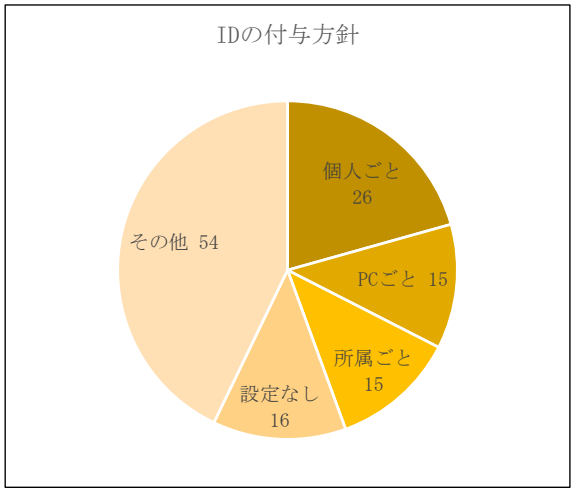
随意契約が 61 件（48.4%）と導入当初に比べ若干割合が高まっている。

⑤　検収方法

検収担当者は、課内の職員とする回答が大半であった。

⑥　ＩＤ管理

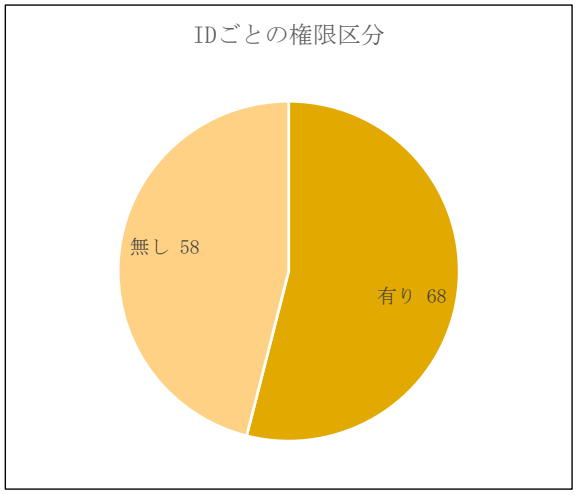
（ア）ＩＤの付与方針



個人ごと	26 件
ＰＣごと	15 件
所属ごと	15 件
ＩＤの設定なし	16 件
その他	54 件
合計	126 件

ＩＤの付与は各所管部署で実施することになっているが、個人ごと 26 件(20.6%)、パソコン（以下、「ＰＣ」という。）ごと 15 件（11.9%)、所属ごと 15 件(11.9%)、ＩＤの設定なし 16 件（12.7%）との回答であった。その他 54 件（42.9%）は、ＩＤが共有されている等の回答となっている。

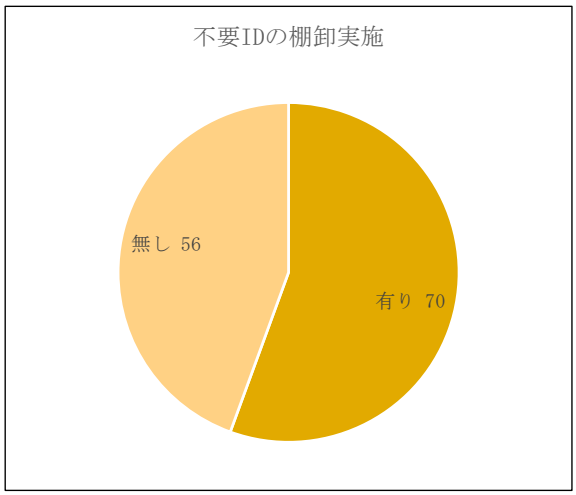
（イ）ＩＤごとの権限区分



有り	68 件
無し	58 件
合計	126 件

ＩＤごとの権限区分については、有りが 68 件（54.0%）、無しが 58 件（46.0%）となっており、ＩＤに権限区分が付されていない場合が半数近くある。

（ウ）不要ＩＤの棚卸実施

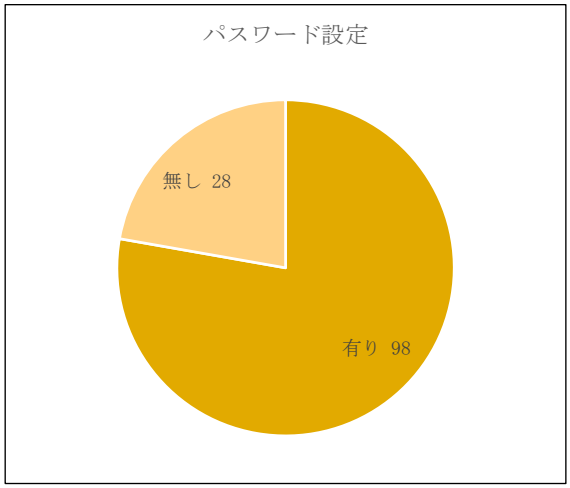


有り	70 件
無し	56 件
合計	126 件

不要ＩＤの棚卸が定期的に実施されていないシステムが 56 件（44.4%）あった。

⑦　パスワード管理

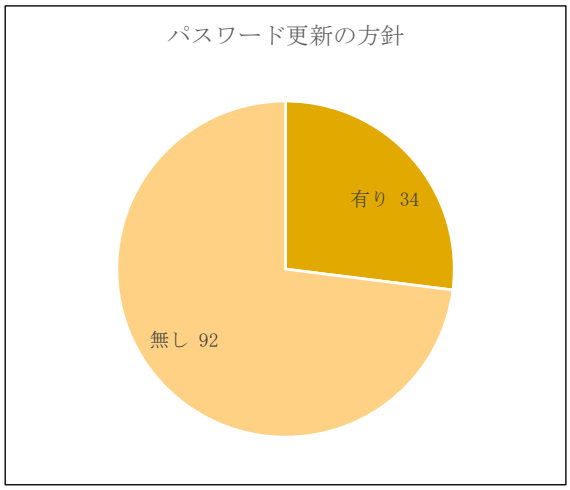
（ア）パスワード設定



有り	98 件
無し	28 件
合計	126 件

パスワード設定が無いとの回答が 28 件（22.2%）あった。

（イ）パスワード更新の方針

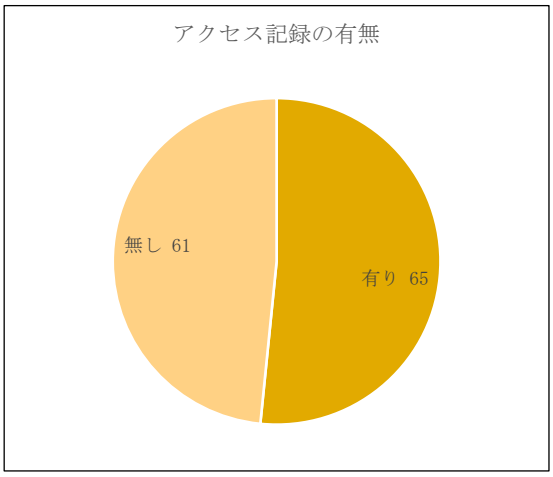


有り	34 件
無し	92 件
合計	126 件

パスワード更新の方針が無いとの回答が 92 件（73.0%）あった。

⑧　情報漏えいへの対応

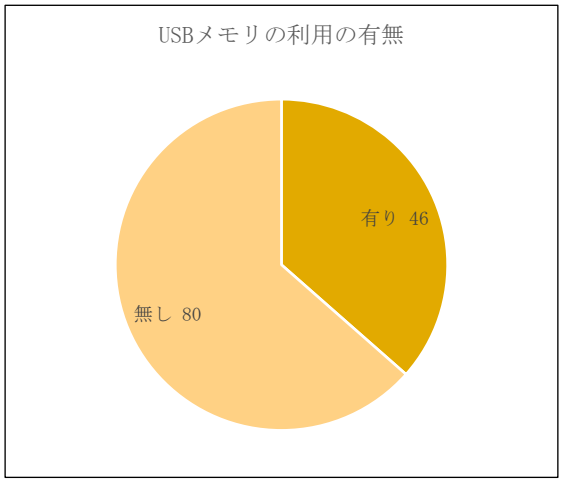
（ア）アクセス記録の保存



有り	65 件
無し	61 件
合計	126 件

アクセス記録の保存について、無しとの回答が 61 件（48.4%）あった。

（イ）ＵＳＢメモリの利用の有無



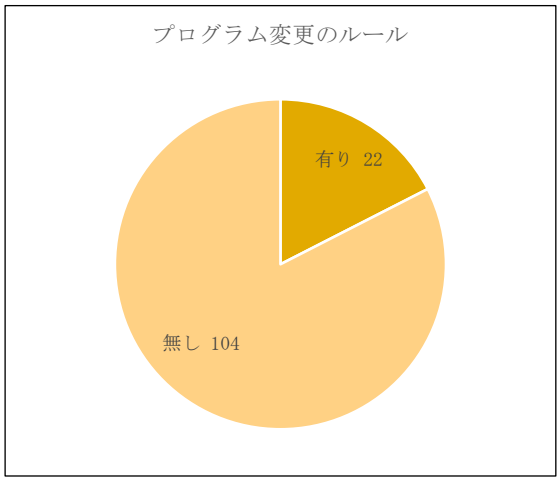
有り	46 件
無し	80 件
合計	126 件

ＵＳＢメモリの利用については 46 件（36.5%）が有りと回答している。

ＵＳＢメモリの管理方法については個別システムの詳細調査により実情を確認した。

⑨　プログラム変更

（ア）プログラム変更のルール



有り	22 件
無し	104 件
合計	126 件

プログラム変更のルールは所管部署においては無いとの回答が 104 件（82.5%）であった。

2.4　調査票に基づく調査の結果

上記の調査票の回答状況を分析した結果、情報セキュリティ対策が徹底されていない状況が散見された。

①　ＩＤ管理について【結果】

調査票の回答結果によると、ＩＤの付与は「個人ごと」以外に「ＰＣごと」「所属ごと」「ＩＤの設定なし」の状況も見られた。事務の特性等によって共有ＩＤを使用せざるを得ない状況もあると思われ、県は共有ＩＤを利用する場合の対策を定めてはいるものの、その運用状況を踏まえると十分機能しているとは言えない。

また、調査票アンケートによると「不要ＩＤの棚卸実施」も徹底されておらず、異動等で不要になったＩＤについて速やかに登録を抹消しているかの担保が得られない。その場合、当該不要ＩＤを第三者が入手した場合、情報漏えいするリスクが考えられる。

ＩＤ管理については全庁的なルールは定められているがそれらは業務所管課において浸透・徹底されていない状況を踏まえ、情報漏えいリスクに万全を期すべきである。

②　パスワード管理について【意見】

「ユーザ認証」には、以下のようないくつかの方法があり、パスワードによるユーザ認証は一般的な認証方法として広く使用されているがその他にもＩＣカード認証や指紋認証といったさまざまな方法がある。また最近ではそれ１種類の方法のみによる認証ではなく、複数の方法を組み合わせた二要素認証等が普及してきており、県においても技術的対策として重要な情報資産を扱う全端末については二要素認証が既に導入されている。

・ユーザのみが知っているもの(パスワード)

・ユーザが所有するもの(鍵やカード)

・ユーザの特徴を表すもの(指紋などのバイオメトリックス)

しかし、調査票アンケートによると、一般的な認証方法である「パスワード設定」さえないものも見られた。

情報へのアクセスを制御するため、適切なユーザ認証を用い、本人確認の徹底を検討される必要がある。

③ アクセス記録の保管について【結果】

県においては技術的対策として、外部からの不正アクセスについてはサイバー攻撃対策を講じている。

しかし、調査票の回答結果によると、半数近くのシステムでアクセス記録を保存していないとのことであった。

アクセス記録が保存されていない場合、不正なアクセスがあっても長期間にわたり気づくことができず、被害が拡大するリスクがある。また、後日検証もできないため不正アクセスを助長することにもなりかねない。これら不正アクセスや情報漏えい等のリスクを軽減するためにもアクセス記録を保存する必要がある。

④ システム変更管理[1]について【結果】

調査票の回答結果によると、大半のシステムでは、プログラム変更のルールは無いとのことであった。

情報システムの変更管理は非常に重要な活動である。例えば、職員からの電話１本でＩＴ事業者のシステム・エンジニア（ＳＥ）がシステムを変更しているような場合、その変更の記録は何も残らず、またその変更の影響によって障害が発生した場合、その原因追究は非常に困難なものになる恐れがある。

情報システムの運用保守においては、一定「情報システム調達ガイドライン」において定められているが、以下のようなポイントを踏まえ、より詳細な変更管理手順を整備・運用すべきである。

- 変更管理手順が定められ、それに則り運用されていること
- 変更管理手順において適切に職務分掌がなされていること
- 変更が事前に計画され、その内容が承認されていること
- 変更の内容がテストされており、その結果が承認されていること　等

1 すべての変更を効率的かつ迅速に取り使うために、標準化された方法、手順が使われることを確実にすることと、それによって変更に起因するインシデントがサービス品質に与える影響を最小限にし、組織の日々の運用を改善すること（出典：「ITIL v2」）

3　個別の情報システムに関する結果及び意見

3.1　詳細調査の選定対象

調査票による概要調査の結果に基づき、以下のような特徴を１つ以上有する情報システムについて、個別にヒアリング及び関係資料閲覧による詳細調査の対象として選定した。

(ア)情報システムの当初の開発投資額が大きい。

(イ)情報システムに対して、近年大きな改修を行っている。

(ウ)情報システムの開発時期が古い。

(エ)情報システムの管理体制にセキュリティ上のリスクがある。

(オ)情報システム内で個人情報を保管していると考えられる。

前述２．２のとおり、詳細調査対象として以下の 12 の情報システムを選定している。

No.	所管部署	システム名称
1	人事課	人事管理システム
2	人事課	職員健康管理システム
3	情報政策課	シンクライアントシステム
4	情報政策課	県立情報交流センター情報システム
5	福祉保健総務課	生活保護システム
6	障害福祉課	身体障害者手帳等交付管理システム
7	財政課	新地方公会計システム
8	税務課	県税運営システム
9	教育庁総務課	校務支援システム
10	教育庁学校人事課	人事管理電算処理システム
11	道路保全課	道路情報管理システム
12	会計課	財務会計システム

3.2　個別の情報システムに関する結果及び意見の概要

個別システムの詳細調査により発見された結果及び意見の検出状況は以下のとおりである。

No	システム名	結果及び意見の種類		
		コスト	セキュリティ	その他
1	人事管理システム	意見：2	意見：2 結果：2	意見：1
2	職員健康管理システム	意見：1	－	意見：1
3	シンクライアントシステム	意見：5	意見：1	－
4	県立情報交流センター情報システム	意見：1	意見：1	－
5	生活保護システム	意見：2 結果：1	意見：2 結果：1	－
6	身体障害者手帳等交付管理システム	意見：2	意見：1 結果：1	－
7	新地方公会計システム	意見：2	－	－
8	県税運営システム	－	意見：1	意見：1
9	校務支援システム	意見：1	意見：3	－
10	人事管理電算処理システム	－	意見：4	－
11	道路情報管理システム	結果：1	意見：2 結果：1	意見：1
12	財務会計システム	意見：1	－	－

3.3　主な個別の情報システムに関する結果及び意見（抜粋）

①　コスト

- 業者から入手した見積書について、作業工数が明確でないものがあった。積算根拠を明確化するために、作業明細の粒度を細かくし、その明細ごとの作業工数×単価が記載された見積書を入手することが望ましい。
- 県の「情報システム調達ガイドライン」や「システム導入（変更・委託）事前協議要領」では、情報システム導入時の事前協議において費用対効果の検証が求められているが、費用対効果の検証を行っていない情報システムがあった。これらについては県の規程に従い、費用対効果の検証を行うべきである。
- 保守契約等について、業者から提出される完了報告書に実績工数の記載がなく、当初見積り工数との予実分析が困難なものがあった。業者に対して保守作業完了時に実績工数の報告を求め、予実分析により工数見積りの妥当性を検討し、次回の価格設定に活かしていくことが望ましい。

②　セキュリティ

- 情報システムのバックアップ作業を業者が行っている場合で、仕様書等に当該バックアップ作業の記載がないものがあった。このような状況では、バックアップデータの滅失や情報漏えい等の発生時に責任の所在が不明確となる恐れがある。そのため、バックアップについては職員が実施するか、当該作業も含めた適切な保守契約を締結することが望ましい。
- 特定個人情報を扱っている情報システムにおいて、定期的なアクセスチェックを実施していないものがあった。特定個人情報については、個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」でアクセス状況の定期的な確認の実施が望まれているため、定期的なアクセスチェックを行うことが望ましい。
- パスワードの更新に関する方針が設けられていない、又はパスワードの変更実績がない情報システムがあった。職員異動が定期的に行われる環境下でパスワード変更が実施されていなければ、継続して使用されているパスワードが複数の職員の間で共有されることになり、システム管理者の管理が及ばないところでの情報漏えい等のリスクが回避困難なため、パスワード更新に関する方針を定め、定期的なパスワード変更を実施すべきである。

③　その他

- 県の公文書管理規程に基づいて各所管部署で作成される「公文書分類表」により、情報システムの仕様書や設計書などは５年で廃棄されている。そのため、仕様書等を含め開発時の文書が残っていない情報システムがあったが、システム開発時の文書は今後のシステム改修・更新・運用保守時において有用な情報となるため、文書保存期間を過ぎたとしても保存しておくことが望ましい。

➢ 県の「情報システム調達ガイドライン」では、情報システム受入時の各テストにおける県側の関与度合いについて下記のとおり示されているが、県側でテストが実施されていない情報システムがあった。要求に見合った機能が適切に運用できるか等の検証を県側で実施すべきである。

4.4.2 役割分担

テスト段階における県側の関与の度合いは開発体制、契約内容等により異なるが、一例をあげると以下のとおりである。

	テスト計画書	テストデータ作成	テスト実施	テスト結果検証
単体テスト	開発業者	開発業者	開発業者	開発業者
結合テスト	開発業者	開発業者	開発業者	開発業者
総合テスト	開発業者	開発業者	県／開発業者	県／開発業者
運用テスト	県／開発業者	県	県	県

4　全庁レベルにおける情報システムに関して発見された監査の意見

（以下、知事部局に対する意見とするが、教育庁においてもこれらを参考にされたい。）

4.1　ＩＣＴ運営について

4.1.1県の現状と今後の方向性【意見】

ＩＣＴ（インフォメーション・コミュニケーション・テクノロジー：情報通信技術）活用が、県の行政改革上の戦略や政策の実現にさらに貢献するためには、行政改革の視点をより多く取り入れたＩＣＴ施策の策定・実行が求められるところである。県ＩＣＴが全庁レベルの目標の達成に貢献するためには、組織のより幅広い戦略や政策の計画に整合した短期的及び中長期的な施策の策定・実行が行われる必要がある。

近年、ＩＣＴを活用した県民サービスや業務手続きの簡素化・簡便化の推進や各種情報システムの高度化によるサービス充実化が求められている。また今後は、県の働き方改革の推進においても、テレワーク[2]やＡＩ[3]・ＲＰＡ[4]の活用含め、ＩＣＴ活用がより重要になってくる。しかしその一方、県のＩＣＴ運営には以下のような現状が見られた。

- 行政経営とＩＣＴ施策の連携に課題がある。
- 全庁的な課題に対して統制を取る組織機能とＩＣＴを活用した有効な検討の対応に課題がある。

現状の情報政策課の機能はＩＣＴ基盤やセキュリティ等の技術的な支援機能が中心であるが、上述２点のような現状課題を解消するためには、行政改革の視点をより取り入れた上で、行政経営や事業におけるＩＣＴ活用を推進するために、行政経営とＩＣＴの橋渡しを行う機能が別途必要となる。

既に、多くの都道府県や政令市では、以下のような目的のために、ＣＩＯ（最高情報責任者）をトップとしたＩＣＴ運営体制が構築・常設されており、行政経営とＩＣＴの連携強化を図っている。

①　ＩＣＴ戦略・ガバナンスの推進

県の戦略や政策と整合のとれたＩＣＴ施策を策定し、それら施策を実現するためのＩＣＴガバナンス（統治の仕組み）を確立する。

②　ＩＣＴ投資・コストの最適化

県の全体最適化の視点でＩＣＴ投資の最適化を進めるとともに、メリハリの効いたＩＣＴ投資が行えるよう不要・余分なＩＣＴコストは適正化する。

③　ＩＣＴリスクへの対応

---

[2] ICT を活用した、場所や時間にとらわれない柔軟な働き方のこと。「tele = 離れた所」と「work = 働く」をあわせた造語。（出典：一般社団法人　日本テレワーク協会　ＨＰ）

[3] 人工知能（artificial intelligence）の略。大まかには「知的な機械、特に、知的なコンピュータプログラムを作る科学と技術」と説明されているものの、その定義は研究者によって異なっている状況にある。

[4] ロボティック・プロセス・オートメーション(Robotic Process Automation)の略。これまで人間のみが対応可能と想定されていた作業、もしくはより高度な作業を人間に代わって実施できるルールエンジンや AI、機械学習等を含む認知技術を活用した業務を代行・代替する取り組み。人間の補完として業務を遂行できることから、仮想知的労働者（Digital Labor）とも言われる。（出典：一般社団法人日本 RPA 協会　ＨＰ）

ＩＣＴ活用を通じて発生する情報セキュリティリスク（個人情報漏えい、システム障害等による業務停止等のリスク）を識別し、その対策を講じる。

情報政策課は、ネットワークやセキュリティ、システム開発・運用等に通じているが、一方で（一般職員には難解である）ＩＣＴを、経営や業務所管課の視点で説明するスキルや、業務所管課間で利害衝突の発生しやすい全庁的なＩＣＴ施策やＩＣＴ投資等を取りまとめるリーダーシップが求められる上記①②には十分な対応ができていない。上記③についても、全庁的な情報セキュリティ対策が業務所管課には十分には浸透・徹底していない。（後述５．３「情報セキュリティについて」参照）

4.1.2 中期計画について【意見】

県において和歌山県長期総合計画が策定されており、「長期総合計画の実現」と「将来にわたる持続可能な行財政運営の確保」を両立するために、今後５年間（平成 29 年度～平成 33 年度）の行財政運営の方向性を定めた「中期行財政経営プラン」において、長期総合計画に掲げた将来像を実現するため、計画に掲げた目標の達成度を注視しながら、毎年度、知事をトップにした新政策会議をプラットフォームにした「新政策プロセス」において施策を創出している。この新政策プロセスに則り、各部局において具体的計画を策定し実行している。

和歌山県長期総合計画には様々な目標や施策が掲げられているが、それらを実現するためにＩＣＴがどのように貢献すべきか、という点が不明瞭である。例えば、情報政策課による中長期的な施策の一つである「超高速ブロードバンドや新たな通信技術・サービスの導入の促進」は具体的に、どのような目的で、誰が、何を、どのように、どのようなスケジュールで実施されるかが不明瞭である。県が積極的に関与し、進捗管理ができる施策を新政策プロセス等で具体化していくことが望ましい。

前述のとおり、例えば、今後は県の働き方改革の推進においてもＩＣＴ活用がより重要になってくる。情報政策課だけで新政策が完結しないよう、行政改革の視点をより多く取り入れた上で、行政経営や事業の改善に資する「超高速ブロードバンドや新たな通信技術・サービスの導入の促進」が計画され、また、ＩＣＴを取り巻く急激な環境変化にも十分に対応できるよう柔軟に見直しを行うことができる仕組みが必要である。

4.1.3 業務・システム最適化推進委員会について【意見】

県にとって重要なシステム投資を決定する業務・システム最適化推進委員会は、議論すべき事項が発生したときのみ招集することになっているが、直近では１年半程度開催されておらず、県やＩＣＴを取り巻く環境が目まぐるしく変化していることを鑑みると、これらを定期的に開催する必要がある。県やＩＣＴを取り巻く環境の変化に対応すべく、能動的に問題を提起し機能させるべきである。また、同委員会においては、行政改革課と情報政策課とが共同して、業務見直し・システム整備を同時に進めていくことが効率的であると考える。

県は現在、汎用機システムからオープン系システムへの全庁的なシステム変革期にある。汎用機からオープン系への移行自体は手段に過ぎず、オープン系への移行等を通じて解決すべき課題や方向性、得られる成果や具体的な取組み等に関する業務・システム最適化計画が、本委員会によって十分な審議を経て承認され、その後、当該計画に則り実行されているかの進捗状況等についても定期的に監視されるべきである。

4.1.4 シンクライアントに接続されていないシステムやサーバの管理について【意見】

シンクライアントに接続されていないシステムやサーバについても、事前協議の中で情報政策課が審査し、納入時の検収や導入後の運営維持管理は各課が責任をもって対応すべきとされている。しかし、効率的にＩＣＴが利活用できるようにする、あるいは、情報セキュリティ事故等を未然に防止する観点からは、ネットワークやセキュリティ等に通じた情報政策課の担当者が、外部からの不正侵入等に備えるネットワークに関する技術的対策のみでなく、各課のシステムについても必要に応じてシステムの導入支援やサーバー（個人情報等）の管理状況のチェック等をより広く実施すべきである。庁内における責任の所在がどこにあるかは県民には関係なく、万が一の個人情報漏えい等のセキュリティ事故等が発生した場合、県は加害者の一旦を担うことになるリスクさえもあり、その際に被害を受けるのは県民である。これらを未然に防止すべく、庁内における責任の所在の如何に関わらず情報政策課を中心としたオール和歌山県でセキュリティ強化の対策を講じるべきである。

4.2　情報システムの調達・保守について

4.2.1 事前協議・執行前協議について【意見】

情報政策課は事前協議や執行前協議において、庁内のシステム投資やＰＣやプリンタなどのシステム機器の購入案件に対して、ネットワークやセキュリティの技術的な観点から問題がないかを一元的に審査している。しかし、各課の情報システムに関する投資の調査の結果、効率性の観点からの審査が不十分であると考えられるため、費用対効果などの観点からの審査を強化すべきである。

- 情報政策課は、既存システムの保守運用に関して、工数×単価の観点でのコストの妥当性の検証はあまり実施しておらず、また財政課ではその（ＩＣＴコスト特有の事項に関する）知見不足から情報システムのコストの妥当性を検証することは困難である。そのため、各システム所管課でのコスト削減に関する意識が薄くなり、業者の見積書を入手し、ネットワークやセキュリティの技術的な観点さえクリアすれば、比較的容易に支出が行われてしまうリスクがある。
- 事前協議において業者からの見積書を徴してその内容を検討することとしているが、既存システムの保守運用に関する見積書の内訳では、作業項目の粒度が粗く、また明細ごとの工数×単価の積み上げ形式になっていないケースが多く見られた。システム所管課では当該見積書を入札時の予定価格算定の基礎資料としている。また、当該見積書を参考にして財政課による予算配分が行われている。第三者の専門家でも検証が行えるような、粒度が細かく、明細ごと工数×単価が明記された精度の高い見積書を徴することは、コスト削減につなげる第一歩であり、情報政策課は指導性を発揮すべきである。
- とくに、新規開発・再構築、大規模なシステム改修で発生する一時経費や契約変更（金額増加）等については、（上述のような見積書の精査に留まらず、）情報政策課だけでなくＣＩＯをトップとした政策審議や、行政改革、財政等も含めた業務・システム最適化推進委員会等で、当該調達について、技術面のみではなく、行政運営面からもその必要性及び費用対効果等の審査・承認を行う仕組みを整備・運用すべきである。

4.2.2 システム導入の事後評価について【意見】

情報システム調達ガイドラインにおいては、システムを導入した年度末に、事後報告（事後評価）を実施することになっているが、実施されていないものがある。効果的・効率的なシステムが導入されたかどうかの検証のために、事後報告はルールに従い実施する必要がある。また、導入年度以降に保守コストも生じることから、評価については導入年度のみではなく、継続して定期的に実施する必要がある。

4.2.3 システム受領の検収について【意見】

検収は各システム所管課で実施することになっている。各課の検収の中には、発注先が提示する機能評価の確認に依存しており、各課がテストシナリオを主体的に検討しているとはいえず、ユーザ受入れ（検収）テストといえるほどの水準には達していないものもある。

情報システム調達ガイドラインには一定求められているが、とくに重要なシステム投資については、検収の精度をより向上させるために、情報政策課もユーザ受入れ（検収）テストに関与することが望ましい。

4.2.4 システム仕様書や設計書の保存について【意見】

情報システムが運用中にも関わらず、一部のシステムにおいて、当該情報システムの仕様書や設計書などが廃棄されている。システム改修・更新・運用保守時の利便性を考慮し、システム構築時の仕様書等は残しておくことが望ましい。

4.2.5 システムのバックアップについて【意見】

情報セキュリティの可用性を高める意味において、情報資産のバックアップは非常に重要である。例えば、万が一ウイルス感染等によってシステム利用が不能となった場合においても、迅速にバックアップからシステム復旧できさえすれば、システム障害に伴う業務停止時間は最小限に抑えることができる。

しかし、職員の個人情報等の重要性の高い情報のバックアップが１箇所のみで保存されているケースがあるため、各システムの管理者は不測の事態に備え、費用対効果も考慮した上で、これらバックアップデータの副本化や保管場所の分散（庁舎内・庁舎外）を検討するべきである。

4.3　情報セキュリティについて

4.3.1 ＩＣＴに関する外部環境の変化

情報セキュリティに関する脅威の高度化、多様化やクラウド技術の進展、ＳＮＳ[5]の普及などのＩＣＴに関する外部環境の急激な変化は、県の情報セキュリティにも大きな影響を及ぼすこととなる。

官公庁においても近年、日本年金機構や堺市役所で大規模な情報漏えい事故が発生しており、官公庁における情報セキュリティリスクの影響度や発生可能性、住民の注目度は大きく上昇している。いまや、個人情報漏えい等の情報セキュリティ事故は官公庁における最大の経営リスクの一つと言ってよい状況にある。

[5] ソーシャル・ネットワーキング・サービスのこと。人と人とのつながりを支援するインターネット上のサービスを指す

4.3.2情報セキュリティに関する実効性の不足【意見】

前述の３．３に見られる県情報セキュリティに関する実効性の不足は、一連のＰＤＣＡサイクルにおけるＣ（チェック）、Ａ（改善）の弱さがその一因であると推察される。

情報セキュリティに関するＰＤＣＡサイクルを回すための組織的対策として、情報セキュリティ基本方針に点検・監査に関する規定がある。例えば、情報政策課は情報セキュリティポリシーが遵守されていることを検証するため、定期的に情報セキュリティ監査を実施することになっており、毎年度実施することが望ましい。また、所属内点検を毎年度実施しているが、前述の３．３を踏まえると、それらが十分機能しているとは言い難く、実効性を高めるための改善余地がある。

県は、総務省の「新たな自治体情報セキュリティ対策の抜本的強化について」で示されている高度なセキュリティ対策に沿って、内外からの不正侵入に対しては庁内ネットワークはじめ様々な技術的対策を施しており、個別システムは当該ネットワークに組み込まれている。

しかし、各課の所管する個別システムにおいては、情報セキュリティ対策に関する不備が見受けられ、前述３．３で判明したＩＤ、パスワード等の管理に関する情報漏えいリスクが存在している。とくに、個人情報のような機密性の高い情報資産に求められるＩＤ管理やユーザ認証、外付けハードディスクやＵＳＢメモリ等のような持ち運びのできる電子記録媒体の取り扱い等については十分な情報セキュリティ対策（コントロール）[6]の実行は喫緊の課題であり、これらの実行を担保する仕組みの構築が求められる。

また、情報セキュリティに関するＰＤＣＡサイクルを回すための人的対策として重要な役割を担う教育・研修についても、毎年度実施されてはいるものの、前述の３．３を踏まえると、上記規定にある「情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上」の目的が達成されているとは言い難く、実効性を高めるための改善余地がある。

第３章　情報セキュリティポリシー等の取扱い
第４節　点検
情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行う。
第５節　情報セキュリティ監査
情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を行う。

第４章　人と組織
第３節　セキュリティに関する教育
情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育プログラムを策定し、それを実施する。

（出典：「和歌山県情報セキュリティ基本方針」）

[6] 大別すると抑止、予防、検知、復旧の４つのセキュリティ管理策のことをいう。

5　総括

情報システムをいかに効果的に活用するかが現在及び将来の行政経営の良し悪しにつながることは、今日の情報化社会において当然のことである。特に県は急激な人口減少という深刻な課題に直面しており、将来的に行政職員の確保さへ危ぶまれる可能性がある。

一方で、少子高齢化、インバウンド需要の増大、ＡＩの進歩、在宅・遠隔地勤務等社会や住民のニーズは多様化し、多数エリアが見えにくくなりロングテール型の需要構造の中、ニッチなニーズにも幅広く対応していくことが求められていく。情報をいかに活用し、住民ニーズにマッチングさせて行くかは、県の施策の効果を高めるだけでなく、住民満足度、ひいては住民定着度を高める重要なカギとなる。

県は、平成16年に和歌山県情報セキュリティポリシーを策定するとともに、全職員の使用するパソコンデータを集中管理する情報システム（シンクライアントシステム）を先進的に導入し、最近でも情報システムの共通基盤への統合集約化をはかるなど、情報セキュリティに関する積極的な取組みを行ってきた点は評価できる。

また、県では、長期総合計画及び新政策会議をプラットフォームにした「新政策プロセス」において毎年度、情報通信基盤の整備を中心によりスムーズに、よりスピーディに行政経営を展開できるように、情報システム投資により業務効率を高める施策を進めているところであるが、本監査において、「４　個別の情報システムに関して発見された監査の結果及び意見」「５全庁レベルにおける情報システムに関して発見された監査の結果及び意見」にあるように、いくつかの課題が検出された。

(1)　情報セキュリティ基本方針及び調達ガイドライン実現担保の仕組み
(2)　システム導入・保守コストの妥当性検証の仕組み
(3)　各所管レベルのセキュリティ管理の強化

(1) 情報セキュリティ基本方針及び調達ガイドライン実現担保の仕組み【意見】

県は情報セキュリティ基本方針の序文において、

「不正アクセス、コンピュータウィルスなどの外部からの脅威も日々増大かつ高度化しており、また内部職員又は業務受託業者による機密情報又は県民の個人情報の漏洩・悪用の可能性も皆無とはいえずセキュリティ管理の重要性が高まっています。」

と述べ、情報システム調達ガイドラインではその策定の目的として、

「今後もＩＴを活用することで行政サービスの高度化や業務の効率化・迅速化を図る必要がある一方、一旦システム化すれば継続的な経費を伴うことから、適正にかつ効率的に投資することで最少の費用で、最大の効果（業務効率の向上）を発揮するようなシステム導入が求められているところである。」

と規定している。

しかし、これらの規定の趣旨を実現するための枠組みに課題があると考える。情報セキュリティ及びシステム調達等に関する情報政策課と各所管の責任分担及び管理責任の範囲について見直しの検討が必要と考える。

情報政策課は事前協議段階において、主としてネットワークへの接続を含めた技術的な視点や見積書徴収等に関する手続的な視点等から審査を実施し、導入初年度末において導入月のいかんに係らず

事後的な効果検証を行っているが、システム導入価格の専門的な妥当性検証や履行検収時の技術的な検証は十分ではない。システム保守についても同様の状況にある。

各所管の担当者にとっては初めてのシステム導入になるケースも多く、情報システム独特の相場観も少なく、また技術的な面での検収能力が乏しい状況にあることを勘案すると、価格検証や機能テスト検証評価が各所管の担当者任せの部分が大きく、最少のコストで最適のシステムを導入するという趣旨からすると、全庁的にその趣旨の実現担保ができているとは言い難い。

また、システム導入後のデータ管理等のセキュリティ管理は各所管で行うことになっているが、情報セキュリティ基本方針等に基づいた運用ができているかどうかのモニタリングは十分に機能していない。情報セキュリティ監査や研修を定期的に実施することになっているが、これも実効性に不足があり十分には機能していない。

情報政策課と各所管、行政改革課や財政課等が、どの程度、情報システムの導入や保守契約について、最適システムの導入や最小コストの観点、セキュリティの観点から関与すべきかについて、行政改革の視点も取り入れた上でこれら枠組み論に関し再度検討が必要と考える。

(2)　システム導入・保守コストの妥当性検証の仕組み【意見】

情報システムの導入、保守コストについては、複数の事業者からの見積書を入手することが定められており、その規定を遵守することで競争に関する透明性の確保は図られている。当該見積書に基づいて予定価格等が算定され、調達が行われる。

しかしながら、予定価格等算定の重要な根拠となっている見積書については、

・ 導入・保守コストの内訳項目がない（あるいは粗い）

・ 工数や単価等の積算根拠がない（あるいは少ない）

といったケースが頻出しており、価格の妥当性検証をどのように行っているか外部監査の立場からは不明な場合が多かった。各所管へのヒアリングを通じて確認したところ、情報政策課が相談にのって助言した事例もごく少数であった。

履行検収においても、実際に要した工数実績を入手していないケースが多数あった。これでは、ＰＤＣＡサイクルを回してコストを最適化する術がなく、各所管の担当者任せの交渉術に頼ることになりかねない。

システム導入・保守については、見積書徴収段階から工数単価等の積算根拠を明記したものを入手し、情報政策課の関与も含めたＰＤＣＡサイクルの仕組みを構築し、コストの最適化を図る全庁的な対応が必要である。

(3)　各所管レベルのセキュリティ管理の強化【意見】

県が保有する情報システムは、総務省の「新たな自治体情報セキュリティ対策の抜本的強化について」で示されている高度なセキュリティ対策に沿って、内外からの不正侵入に対しては庁内ネットワークはじめ様々な技術的対策を施している。一方で、個別システムの運用・管理については、情報セキュリティポリシーおよび関係規程等に基づき、各システムの所管部署でセキュリティ管理が行われている。県職員には、地方公務員法により守秘義務が課せられていることは前提となるが、前述３．３で示した以下の項目に関連する問題点があった。

・物理的アクセス
・データのバックアップ
・アクセスログの管理
・ＩＤ、パスワード管理
・ＵＳＢ管理

各所管が扱うシステムやデータは高い機密性や完全性、可用性が求められるものが多く、漏洩事件が発生した場合の影響度が大きい。出先機関も含め、取扱いルールが浸透していなかったり、徹底されていなかったりという現状が見受けられ、早急に改善が必要と思われる。これについては、セキュリティ管理が各所管において情報セキュリティ基本方針等に基づいた運用ができているかどうかのモニタリング機能が弱いことも一つの大きな原因である。

モニタリング方法を含め、セキュリティ管理を実効性あるものにするための方策を検討される必要がある。

監査過程で検出した事項を集約して、上記３つの観点から県の情報システムに関する事務の執行に関する課題を総括したところであるが、これらは調査対象とした 12 件の個別システムの問題ではなく、知事所管以外の部局も含め全庁的に共通する課題であると認識していることを念のため付言する。

行政経営へのＩＣＴ活用に係る中長期的なビジョンについて【意見】

最後に、ＡＩの進歩が今後どのようになるかは現時点で未知の部分も多いが、行政経営の中でＩＣＴが果たす役割は今後さらに大きくなると思われる。

県の長期総合計画（2017～2026 年度）のなかで、情報通信技術の発達の恩恵を享受できる環境を整えるため情報通信基盤の整備を進めていく方向性と具体的施策が示されている。併せて行政経営の有効性向上の視点からもＩＣＴ活用の中長期的なビジョンを示し、施策の方向性を提示すべきと考える。

以　上