
三重県情報システムの整備及び管理 に関する標準ガイドライン

第2編 ITガバナンス

目 次

第1章 はじめに	1
1 IT ガバナンスとは	1
第2章 支援・審査・評価	2
1 支援・審査・評価の基本的な考え方	2
2 支援・審査・評価に係る組織体制.....	2
3 予算要求前審査・支援	3
4 契約前審査・支援	4
5 プロジェクト管理支援.....	5
6 システム評価	5
7 課題解決支援.....	5
第3章 情報システムに関する情報の管理	6
1 情報システム基礎調査の提出.....	6
第4章 人材の育成	8
1 本ガイドラインの活用	8
2 支援・審査・評価の活用	8
3 研修の受講等	8
第5章 情報セキュリティ.....	9
1 三重県電子情報安全対策基準の制定	9
2 三重県電子情報安全対策基準の遵守	9
3 情報セキュリティ実施手順の作成・見直し.....	9
第6章 情報システムに関する業務継続計画.....	10
1 情報システムに関する業務継続計画.....	10
2 「情報システムに関する業務継続計画」の策定	10
第7章 監査の指摘事項に基づく対応	11
1 監査の概要	11
2 包括外部監査.....	11
3 情報セキュリティの運用に関する監査.....	14

第1章 はじめに

1 IT ガバナンスとは

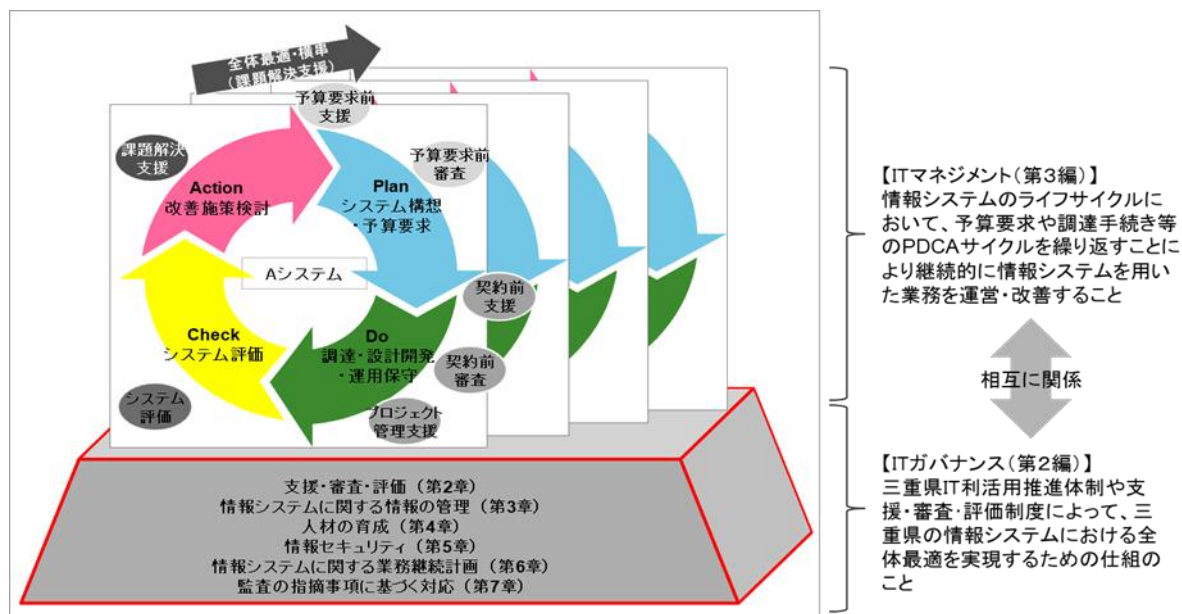
三重県情報システムにおけるITガバナンスとは、デジタル戦略推進委員会等の三重県IT利活用推進体制、予算要求前審査及びシステム評価等の支援・審査・評価制度によって、三重県の情報システムにおける全体最適を実現するための仕組みのことをいいます。

本編では、こうしたITガバナンスにおける支援・審査・評価制度の概要に加えて、情報システムの管理、人材育成、情報セキュリティ、情報システムに関する業務継続計画、監査の指摘事項に基づく対応などのシステム担当所属が取り組むべき規定や方針を示しています。

主な記載内容は以下のとおりです。

- ・ 支援・審査・評価
- ・ 情報システムの管理
- ・ 人材の育成
- ・ 情報セキュリティ
- ・ 情報システムに関する業務継続計画
- ・ 監査の指摘事項に基づく対応

IT ガバナンスのイメージは、以下の図(第1編の再掲)の赤枠の部分になります。



第2章 支援・審査・評価

1 支援・審査・評価の基本的な考え方

(1) 支援・審査・評価の目的

三重県において、情報システムの調達・運用はシステムごとに各部局のシステム担当所属で実施していますが、システム担当所属の担当者がシステム調達・運用の知識・経験について必ずしも十分とはいえないことがあります。これにより情報システムのライフサイクルにおける取組が独自の手続・手順によるものになったり、県全体方針と必ずしも合致しない個別最適なものになったりすることがあります。

支援・審査・評価は、このような状況に対応して、情報システムのライフサイクルに対応したPDCAサイクルを確立することにより情報システムの全体最適化を推進することを目的として行うものです。

支援・審査・評価に関する全体イメージ及び年間スケジュールについては、以下を参照してください。

- ・【別紙 I -2】予算要求前及び契約前における支援・審査の全体イメージ
- ・【別紙 I -3】予算要求前支援・審査及び契約前支援・審査に係る年間スケジュール(概要)

(2) 支援の範囲

予算要求前支援は審査に必要な資料の作成方法の助言、指導までが範囲となります。予算要求前審査では、特に新規開発や機能追加の場合、説明が不十分であれば、支援を十分に受けたシステムであっても、非承認もしくは再審査となる場合もあります。

2 支援・審査・評価に係る組織体制

(1) 支援・審査・評価組織

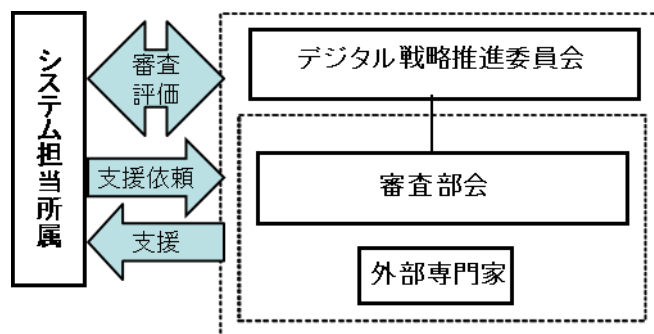
情報システムの支援・審査・評価組織体制は次の図のとおりです。

「三重県デジタル戦略推進委員会設置要領」第 1 条において、「三重県行財政改革・デジタル戦略推進本部の下部組織として、三重県デジタル戦略推進委員会を設置する。」と規定されており、同要領第4条に基づいて審査部会が設置されています。

システム担当所属は情報システム整備の実施主体であり、必要に応じて支援依頼を行います。

審査部会は、システム担当所属の依頼に基づく支援の実施と予算要求前審査、契約前審査、システム評価を実施します。

デジタル戦略推進委員会は、審査部会の審査・評価が、適切な方法で行われたことを確認します。



3 予算要求前審査・支援

(1) 予算要求前審査

ア 予算要求前審査の概要

予算要求前審査は、デジタル戦略推進委員会が行う各所属の情報システム関連調達に係る予算要求案件の審査で、システム化の必要性、仕様書の適切性、経費積算の妥当性などを確認することを目的として行うものです。システム担当所属は、情報システム関連予算について、デジタル戦略推進委員会の予算要求前審査を受審することが、予算要求の前提となっています。

イ 予算要求前審査の実施時期

予算要求前審査全体のスケジュールはおおむね次のとおりです。7月初めにデジタル戦略推進委員会が開催され、システム担当所属は予算要求前審査実施通知を受領します。8月中下旬の期限までに審査資料を審査部会に提出し、その後、9月から10月にかけて審査が行われ、必要に応じて聞き取りが行われます。その後、審査の結果が10月下旬のデジタル戦略推進委員会に報告されるという流れになります。デジタル戦略推進委員会の確認を受けた後、各システム担当所属に審査結果が通知されます。

(2) 予算要求前支援

ア 予算要求前支援の概要

システムの新規開発や再構築等における調達計画(長期計画)の作成及び調達案件全般における予算要求資料の作成の支援を受けることができます。このプロセスにおける主な支援対象は以下のとおりです。

手続	支援対象となる主なシステム担当所属の作業
システム企画	<ul style="list-style-type: none"> ・現状調査、事例調査 ・システム化範囲、目的の設定 ・システム概要の作成 ・費用分析
調達計画の作成	<ul style="list-style-type: none"> ・開発・運用の全体スケジュールの作成 ・調達方針の検討(スクラッチ、パッケージ、使用機器、契約の分割等) ・契約方法の検討(一般競争入札、総合評価一般競争入札、企画提案コンペ、随意契約等)
予算要求資料の作成	<ul style="list-style-type: none"> ・見積依頼資料の作成 ・見積書徴取、情報提供依頼の実施(WTO 案件等) ・見積書評価、要求額確定 ・予算要求前審査資料作成(予算調査表等)

イ 予算要求前支援の実施時期

審査部会の事務局において、毎年2月頃に個別支援の支援希望調査が行われます。その他必要に応じて適宜支援依頼を行うことができます。支援希望のあったシステムについては確認打合せを行い、必要と認められた場合に個別支援を受けられます。

4 契約前審査・支援

(1) 契約前審査

ア 契約前審査の概要

契約前審査は、各所属の情報システム関連調達に係る契約案件の審査で、発注時における公平性・透明性・競争性の確保や調達仕様書等の適切性を確認することを目的として行うものです。資料準備状況、予算要求時からの変更点、スケジュール、仕様書の記載、設計金額等の観点により審査が実施されます。

イ 契約前審査の実施時期

契約前審査は、各情報システムの調達に応じて、随時、年間を通して行います。

(2) 契約前支援

ア 契約前支援の概要

システムの契約事務における契約計画の作成から調達仕様書等の作成の支援を受けられるものです。このプロセスにおける主な支援対象は以下のとおりです。

手続	支援対象となる主なシステム担当所属の作業
契約準備	・契約手続実施スケジュールの作成
契約手続の実施	・調達仕様書・設計書作成 ・意見招請の実施(WTO 案件等) ・落札者決定基準の作成(総合評価一般競争入札)

5 プロジェクト管理支援

システム担当所属の希望により、契約後のプロジェクト管理についても、必要に応じて、「プロジェクト管理支援」の形で、支援を受けることができます。主な支援対象は以下のとおりです。

手続	支援対象となる主なシステム担当所属の作業
契約の執行	・プロジェクト管理
成果物の受領	・納品・検査

6 システム評価

(1) システム評価の概要

システム評価は、システム開発や再構築時に想定した目的や創出される効果が、運用後に期待通りに発揮されているかどうかを検証し、改善に生かしていく取組です。原則、実施を希望するシステムに対して、システム評価を実施します。併せて、システム評価の実施を推奨するシステムに対して、デジタル戦略企画課から声掛けを行います。システム評価を実施したシステムのシステム担当所属は、システム評価結果に基づいた改善を行います。

(2) システム評価の目的

システム評価の目的は以下のとおりです。

- ・ 現行システムの問題点の可視化、改善
- ・ 次期システムの方向性の明示

7 課題解決支援

全体最適化の方針に即した次期システムの実現を図るための支援として、課題解決支援を実施する場合があります。

第3章 情報システムに関する情報の管理

情報システム基礎調査は、各情報システムに関する基礎情報として、現行システムの整備目的、構築時期、導入経費・運用費用、現行システムにおける問題点等の情報を記載するものです。情報システム基礎調査で得られた情報を分析して、各システム担当所属はシステム担当者の引継ぎや次期システムの構想検討に活用します。また、情報システム基礎調査は、予算要求前審査やシステム評価においても利用される資料であり、各制度で使用するシステム概要の資料を共通化することで、資料作成の効率化や各システム間での比較分析や全庁横断的な施策等の立案に活用されます。

1 情報システム基礎調査の提出

(1) 情報システム基礎調査票の作成、提出

各システム担当所属は、情報システム基礎調査票を入力し、提出します。情報システム基礎調査票は、毎年度基礎調査の実施時期に新しい情報に更新した上で、デジタル戦略企画課に提出する必要があります。

新規に情報システムを構築する場合も、予算化に先立って、情報システム基礎調査票に必要項目を入力し、提出します。

(2) 情報システム基礎調査の対象システム

情報システム基礎調査は、県行政内部の効率的な事務処理や、県民への質の高い行政サービスの提供を行う仕組みを有する、大規模システム(共通基盤を含む)と中小システムの両方が対象です。

なお、システムは、中小システムと大規模システムに種別されます。大規模システムの定義は以下のとおりです。それ以外のシステムは、中小システムに分類されます。

- | |
|--|
| <ul style="list-style-type: none">・ 過去5年間のシステム投資額が1億円以上となるシステム・ 庁内システムに対して共通的にサービスを提供するシステムを共通基盤と位置付け、前述5年間の投資額にかかわらず、大規模システムとして扱う。 |
|--|

(3) 情報システム基礎調査の記入要領

情報システム基礎調査の様式や要領等の資料は情報システム基礎調査票サポートサイトに掲載されている「情報システム基礎調査 記入要領」を参照してください。

【情報システム基礎調査票サポートサイト】

http://dkint22/plus/h20_288/kiso.htm

【三重県情報システム基礎調査票の例】

1.回答日	平成30年7月26日
2.管理番号	99-999
3.登録状態	1稼働中
4.システム名称等	〇〇事務処理システム
5.基本事業番号	0
6.情報関連予算名	〇〇〇化推進事業費
7.情報セキュリティ実施手順の作成	1対象
8.システム評価の実施年度	平成24年度
9.システム評価結果	4実施済(●)
10.課題対応方針	9なし
11.情報システム関係資料(実施手順、課題対応方針)	http://ss110035/dbbox/view/index.asp?INFO=TXI3ME5UWXXNhekF5TURBME1BPT0%288D
12.担当部局	地域連携部
13.担当所属	〇〇課
14.所属コード(k+6桁)	k999999
15.担当者名	三重 賢
16.職員コード(m+6桁)	m000000
17.連絡先	999-999-9999
18.システム種別	2中小システム
19.システムの概要・機能	サーバを〇〇課に設置し、〇〇課と地域機関が〇〇業務を実施する上で利用するシステムである。 各ユーザは専用端末から行政WANを介してサーバにアクセスして、〇〇登録や〇〇依頼書、〇〇報告書、統計資料の作成等の処理を行う。
20.システム整備の目的・必要性	〇〇法に基づき、〇〇事業を実現する上で、〇〇業務を実施する為に必要な事務作業を支援するシステムである。 〇〇業務は、〇〇登録や、〇〇依頼書、〇〇報告書、統計資料の作成等を実施するものであり、その年間〇〇〇〇件程度の処理を、地域機関を含めた〇〇人で実施している。また、旧来は1件あたり〇時間程度を必要としていたが、システム化により〇分程度で処理可能となっており、業務を遂行する上で不可欠なシステムとなっている。

第4章 人材の育成

情報システムを整備し、運用するに当たっては、単に情報システムに関する専門的・技術的な知識・能力だけでなく、企画立案、プロジェクト管理等の能力も重要となります。

しかしながら、すべての分野において十分な技能や経験を持つ人材を育成・確保することは容易なことではないため、各人が不足する技能や経験をそれぞれで補い合いながら、個別の職務に当たることが必要となります。

デジタル社会推進局では、情報システムを整備するプロジェクトを適切に遂行し、かつ、運用管理ができる人材を育成するために、以下のような取組を実施しており、システム担当所属はこれらを活用することができます。

1 本ガイドラインの活用

システム担当所属は、情報システムの整備及び管理を推進するに当たって、担当する情報システムに関する業務の遂行に必要な知識・能力を習得する必要があります。

本ガイドラインは、情報システムのライフサイクルに対応したPDCAサイクルを推進するために、システム担当所属が参考とするべき標準的な手順や仕様書ひな形等の各種様式例をまとめたものです。そのため、システム担当所属が担当する情報システムに関する業務を遂行するための最初の取組として、ガイドラインや関連文書の記載内容を理解することが求められます。

2 支援・審査・評価の活用

システム担当所属は支援・審査・評価を受けることにより、支援・審査・評価対象となった取組を改善するだけでなく、そこで受けた支援内容や指摘事項を理解し、本ガイドラインや研修により補完することで、担当する情報システムの整備及び管理を推進するための知識を習得することが可能です。

3 研修の受講等

システム担当所属は本ガイドラインの内容や支援・審査・評価結果を理解し、業務に生かすために、必要に応じて研修を受講し、必要な知識・能力の習得に努めることが求められます。知識・能力の習得は研修の受講に限らず、書籍やインターネットからの情報収集や外部セミナーの受講、他県調査の実施等、様々な手段により継続的に自己研さんに努めることが重要です。

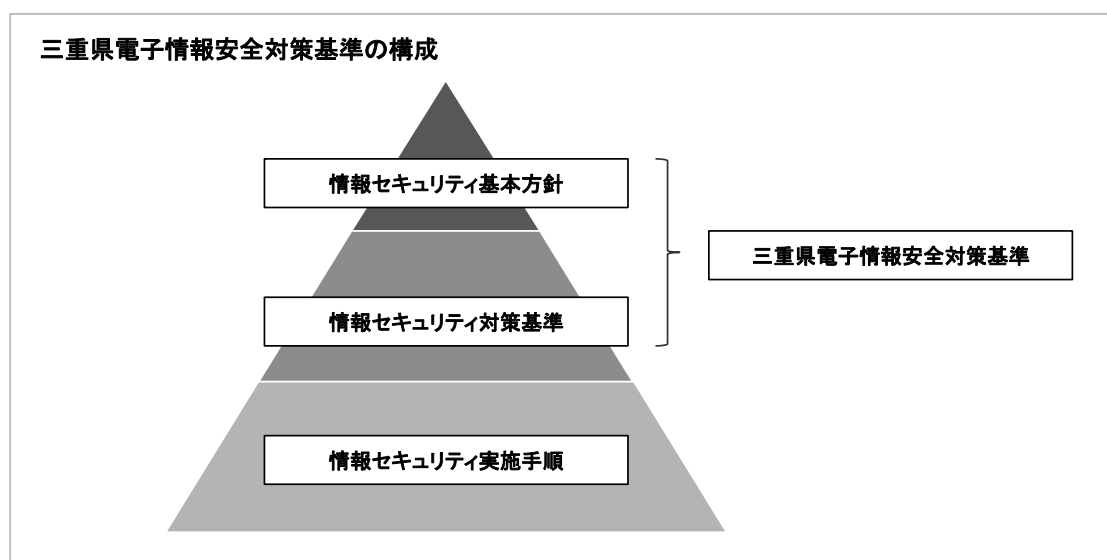
なお、デジタル社会推進局では、システム担当者が本ガイドラインや関連文書を理解するために、各種必要な研修メニューの提供を行っています。また、情報システムに関する知識を深めるために、IT技術トレンド等の外部環境や三重県の状況を踏まえたテーマを選定して勉強会を開催しています。

第5章 情報セキュリティ

1 三重県電子情報安全対策基準の制定

三重県の各情報システム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等、部外に漏えいした場合に極めて重大な結果を招く情報が多数含まれています。

これらの情報及び情報を取り扱う情報システムを様々な脅威から防御し、県民の財産、プライバシー等を守るとともに、事務の安定的な運営を行い、県民からの信頼の維持向上を図るため、三重県電子情報安全対策基準(情報セキュリティポリシー)が定められています。



2 三重県電子情報安全対策基準の遵守

三重県電子情報安全対策基準は、三重県が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、電子情報に関する情報セキュリティ対策の頂点に位置するものです。

したがって、三重県知事をはじめとして三重県が所掌する情報資産に関する業務に関わるすべての職員及び外部委託事業者等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって本基準を遵守する義務を負うものと定められています。

3 情報セキュリティ実施手順の作成・見直し

情報システム管理者等は、情報システムごとに情報セキュリティ実施手順を作成する必要があります。

情報セキュリティ実施手順とは、三重県電子情報安全対策基準に基づいた各システムにおける具体的な対策として、①セキュリティ範囲定義書、②情報資産マトリックス兼セキュリティ対策定義書、③活動内容報告書、④緊急時対応計画を取りまとめたものです。情報セキュリティ実施手順はすべての情報システムについて作成が義務付けられており、毎年、定期的に見直しが必要となります。

第6章 情報システムに関する業務継続計画

1 情報システムに関する業務継続計画

「業務継続計画」とは、大規模な災害、事故、事件等や感染症の発生により県の庁舎、職員等が相当の被害を受けた結果、ヒト、モノ、情報及びライフライン等利用できる資源に制約がある状況下において、適切な業務執行を行うことを目的に、「非常時優先業務(※)」を特定し、業務継続に必要な資源の確保・配分や、そのための手続の簡素化、指揮命令系統の明確化等について必要な措置等の計画について県が策定するものです。

それら大規模な災害、事故、事件等の発生時に県の「非常時優先業務」を実施・継続させるためには、関連する情報システムやネットワーク等の稼働が必要不可欠となります。

なお、情報システムやネットワーク等は、大規模な災害、事故、事件等の発生後から対策を始めるのでは、稼働できないことはもとより早期復旧も困難であるという特性を持つため、平常時から周到な備えが不可欠となります。

そこで、大規模な災害、事故、事件等の発生時に最低限必要な情報システムやネットワーク等の稼働維持あるいは早期復旧を図るべく情報システムに特化した「業務継続計画」として、「情報システムに関する業務継続計画」が必要とされています。

※災害応急対策業務、優先度の高い復旧・復興対策業務、及び継続性の高い通常業務

2 「情報システムに関する業務継続計画」の策定

(1) 計画の策定

非常時優先業務に関連する情報システムやネットワーク等を所管するシステム担当所属は、「情報システムに関する業務継続計画」を策定し、そこで業務継続のために必要となる情報システムの基礎的対策計画を定める必要があります。

基礎的対策計画には、緊急時対応体制や行動計画、システム機器設置場所並びにその他のリソースの現状とバックアップ等の状況からシステムリスクを洗い出し、システムの目標復旧時間と停止時の影響と代替手段等について記載します。

(2) 計画の見直し

システム担当所属は、次に掲げる事項の状態になった場合「情報システムに関する業務継続計画」の見直しをする必要があることから、定期的(年1回以上の頻度)な見直しを実施します。

- ・対象となる非常時優先業務に係る計画等が改定される場合
- ・組織体制もしくは委託事業者に変更があり連絡体制表等に変更の必要が生じた場合
- ・災害訓練の結果、見直しが必要な場合
- ・対象の情報システムの更新や新規構築があった場合
- ・国、県の制度変更があった場合
- ・知事等から見直しするように指示があった場合

第7章 監査の指摘事項に基づく対応

1 監査の概要

三重県において、情報システムに関する監査には、包括外部監査人による包括外部監査、内部監査人及び外部専門家による情報セキュリティ監査、等があります。

包括外部監査制度は、監査委員の監査に加え、より専門的、独立的な立場から、さらには、信頼性、透明性の確保の観点から監査機能を向上させようとするもので、選定された包括外部監査人により毎年特定のテーマを選定して監査する制度です。

情報セキュリティ監査は、三重県電子情報安全対策基準に基づき、電子情報の適切な管理・運用体制の構築や安全対策の維持向上を図ることを目的に実施されます。

2 包括外部監査

(1) 概要

近年、自治体の行政運営にとって情報システムは不可欠のものとなっております。行政事務は情報システムに大きく依存しており、また、情報システムは、事故や災害によりその機能が麻痺した場合、行政事務や県民の生活に与える経済的、質的な損失が非常に大きいものとなります。さらに、情報セキュリティに不備があると、個人情報等重要な情報が漏えいする可能性もあります。このような情報システムの重要性から包括外部監査のテーマとして選定されたり、特定の監査テーマの中で情報システムを利用した事務や情報システムに係る取引が対象として選定されたりすることがあります。

次に掲げる事項は、これまでの包括外部監査において指摘を受けた代表的なものであり、継続的に取組が必要な事項として留意する必要があります。

(2) 包括外部監査における指摘事項

ア 情報システムの調達の適切性について

- ・ 契約書の適切な記載が行われていないものがある。
- ・ 随意契約の妥当性についての検討が不十分なものや、検討過程を文書等で残していないため検討が適切に実施されたか確かめられないものがある。
- ・ 業務の再委託に関する承認過程が不明確になっているものがある。

調達手続の適正化は、事業者の公正な競争を促し、調達コストの低減だけでなく、より有効に活用できるシステムの取得・開発にもつながります。調達手続の際には、適正な手続の実施だけでなく検討過程の文書化やその文書の保管等一層の公平性・透明性を確保していくことが求められます。

(本ガイドラインで留意が必要な箇所)

- ・ 第3編第2章 第5 システム企画書の作成
- ・ 第3編第3章 第4 2 予算要求前審査の提出資料作成
- ・ 第3編第4章 第3 調達仕様書作成

イ 情報セキュリティについて

- ・ 情報システムのパスワードについて定期的な変更がなされていないものがある。
- ・ 委託事業者に対する情報セキュリティ管理等の実施状況について、十分な確認がなされていないものがある。
- ・ バックアップ媒体の保管が適切に実施されていないものがある。

情報システムには、県民の個人情報のみならず行政運営上重要な情報が含まれます。情報セキュリティの不備は、短時間に膨大な情報を漏えいする等極めて重大な問題を生じさせる原因となります。また、情報システムの不適切な使用等により障害が発生した場合には、行政事務が滞り、県民生活に多大な影響を与えます。したがって、情報セキュリティについては、不備の改善はもとより一層の管理体制の強化が望まれます。

(本ガイドラインで留意が必要な箇所)

- ・ 第3編第4章 第3 2【調達仕様書目次の例】3 非機能要件

ウ 情報システムの有効性、経済性、効率性について

- ・ 委託業務内容に応じた適切な単価の設定がなされていないものがある。
- ・ 情報システム導入・変更による効果測定が十分になされていないものがある。

情報システムは、整備、運用に多額のコスト(支出)を伴いますが、一方で、一度導入をするとそれ以降はその導入効果を検討しないまま毎年度経常費用として一定金額を支出し続ける場合が多く見られます。導入後も委託事業者に委託する業務内容に応じた適切な単価を設定した上で、実績等を勘案して、委託金額の適正性を定期的に検討する必要があります。また、情報システムの導入・変更の有効性、効率性の評価・審査を確実に実施することができるよう、効果・目標値の設定や到達度の測定の仕組みを整備することが望まれます。

(本ガイドラインで留意が必要な箇所)

- ・ 第3編第3章 第3 2 (3)費用対効果分析について
- ・ 第3編第7章 第2 5 (1)運用及び保守作業の改善
- ・ 第3編第8章 第4 2 現行システムに対する評価の観点

エ 情報システムの予定価格の設定に係る積算について

- ・ 予定価格の設定に係る積算について、積算根拠が不明確であるものや積算時の検討が必ずしも十分とはいえないもの等が散見される。

予定価格について、三重県会計規則運用方針では、取引の実勢価格や市場価格等を考慮して予定価格を設定することとされています。予定価格の設定に係る積算においては、以下のような対応を行うことが望まれます。

予定価格は、原則として業務に必要な工数を見積ることで積算し、業務実施後に見積工数と実績工数を比較して工数を見直し、翌年度の工数の見積に反映することで、予定価格の精度を高めていくことが求められます。運用業務については運用・保守事業者の実績工数を提出させ、次年度必要となる工数の見積精度を高めるといった取組が求められます。

すべての契約において工数を見積ることは実務的に困難であるため、そうした場合においては、複数の参考見積書により算定する方法を採用することが求められます。

単独の参考見積書により算定する方法によらざるを得ない場合においても、事業者より入手した参考見積書の金額をそのまま使用するのではなく、たとえ一部分であっても単価や工数を検証することができないかを検討することが必要です。また、実勢価格等と比較しやすいように参考見積書の様式を工夫する等、様々な視点から検討を行うことが求められます。例えば、労働時間数×時間単価＝人件費、という形式で記載した場合には、時間単価について実勢価格との比較がある程度可能になります。

(本ガイドラインで留意が必要な箇所)

- ・第3編第3章 第2 見積依頼書作成
- ・第3編第3章 第3 1 見積依頼の実施
- ・第3編第7章 第2 5 (1)運用及び保守作業の改善

オ 委託業務の履行確認について

- ・システム開発の委託業務において、テスト報告書等により、委託先が実施したテストの内容及び結果について確認が十分とはいえない事例が散見される。
- ・検査担当者が動作確認を行った結果について、具体的にどのような項目をどれだけ動作確認を行ったかが記録に残されていない。

システム開発の委託業務において、履行確認は、委託先から受領する業務完了報告書と成果品である詳細設計書、テスト報告書、改修プログラム等を検査することで行われます。検査担当者は調達仕様書にて定義した業務を適切に実施できることを確認するため、委託先が実施したテストの内容及び結果について確認を行う必要があります。

さらに、検査担当者による委託先の報告書の確認だけでなく、調達仕様書にて定義した業務を適切に実施できるかを、ユーザ観点からテストします。テスト結果について、具体的にどのような項目をどれだけ動作確認したかを記録に残す必要があります。

(本ガイドラインで留意が必要な箇所)

- ・第3編第6章 第2 3 第一次工程レビュー(次工程の開始判定)
- ・第3編第6章 第3 3 第二次工程レビュー(次工程の開始判定)

- ・第3編第6章 第4 2 受入テストの実施
- ・第3編第6章 第4 3 受入テスト結果の確認

3 情報セキュリティの運用に関する監査

(1) 概要

三重県において、情報セキュリティの運用に関する監査には、内部監査人等による情報セキュリティ監査(以下、「内部監査」といいます。)があります。

内部監査は、三重県電子情報安全対策基準に基づき、平成29年度に試行され、平成30年度から実施されています。

この内部監査は、三重県職員から選任される内部監査人及び外部専門家により、各所属における三重県電子情報安全対策基準の運用状況を中心として情報セキュリティに関する問題点を確認するとともに、改善方法の検討を行う「助言型監査」を実施することで、電子情報の適切な管理・運用体制の構築や安全対策の維持向上を図ることを目的に実施されます。また、内部監査の結果は、三重県電子情報安全対策基準の実効性について評価し、見直しを行うことにも活用されます。

次に掲げる事項は、これまでの内部監査において指摘を受けた代表的なものであり、継続的に取組が必要な事項として留意する必要があります。

(2) 内部監査における指摘事項

ア 使用しないソフトウェアの削除について

- ・インストールが認識されていないソフトウェアが、最新の状態にアップデートされていない事例が多数の所属で確認された。

業務に必要なソフトウェアは、所属長の許可を得てインストールすることができますが、パソコンの利用者が異動等により変更になり、後任の職員が、どのようなソフトウェアがインストールされているか知らないままパソコンを利用する場合があります。ソフトウェアが最新状態にアップデートされていないと、標的型攻撃に利用される可能性があるため、継続して使用しないソフトウェアは削除(アンインストール)する必要があります。

(本ガイドラインで留意が必要な箇所)

- ・特になし

イ 不要になった情報資産の消去について

- ・消去した重要性分類特Aの情報資産が、NASの「ゴミ箱」に復元可能な状態で残っていた。

業務で作成・入手した情報資産は、その重要性に応じて保管し、不要になれば消去する必要があります。

一般的にパソコンやNASでは、誤操作による削除を防ぐため「ゴミ箱」が設定されており、「ゴミ箱を空にする」操作により消去する必要があります。

また、消去しても、パソコンやサーバ、NAS等で使用されるHDD等の記録媒体上から情報資産を復元することも可能であり、これらの機器を廃棄・返却する場合には、記録媒体を物理的に破壊する、又は、一定の要件を保証する完全消去用ソフトウェアを使用して情報資産を消去する必要があります。

さらに、情報システムの運用・保守を委託する際は、情報資産の消去についても調達仕様書で定める必要があります。

(本ガイドラインで留意が必要な箇所)

- ・第3編第2章 第5 システム企画書の作成
- ・第3編第3章 第4 2 予算要求前審査の提出資料作成
- ・第3編第4章 第3 調達仕様書作成
- ・第3編第7章 第2 6 ハードウェア、ソフトウェア製品などの廃棄

ウ 約款による外部サービスの利用について

- ・許可を得ないで約款による外部サービス(LINE)が利用されていた。

約款による外部サービスの利用は、昨今のクラウド化の流れから、利用の増加が見込まれるシステムの運用形態ではありますが、オンプレミスとは異なる情報セキュリティ上のリスクがあることを認識したうえで、取り扱う情報資産の重要性分類に応じて、事前に統括情報セキュリティ責任者や情報セキュリティ管理者の許可を得る必要があります。(オンプレミスが安全で、クラウドが危険なわけではないことに注意が必要です。)

(本ガイドラインで留意が必要な箇所)

- ・第3編第2章 第5 システム企画書の作成
- ・第3編第3章 第4 2 予算要求前審査の提出資料作成
- ・第3編第4章 第3 調達仕様書作成