入札説明書等配布一覧表

山形県税務総合電算システム運用支援業務

No	名　　称	部数等
1	入札説明書 （添付様式） ・一般競争入札参加資格確認申請書 ・一般競争入札参加資格審査申請書提出書 ・競争入札に関する質問書 ・入札書 ・委任状	１部
2	委託仕様書	１部
3	委託契約書（書式）	１部
4	山形県情報システム導入標準ガイドライン	１部
5	山形県情報セキュリティポリシー	１部

（注）上記内容について、落丁等がないか確認してください。

山形県総務部税政課

資料番号1

山形県税務総合電算システム運用支援業務

入札説明書

令和７年 10 月
山　形　県

入　札　説　明　書

山形県税務総合電算システム運用支援業務の調達に係る入札公告に基づく一般競争入札については、関係法令及び山形県財務規則（昭和39年３月県規則第９号。以下「規則」という。）に定めるもののほか、この入札説明書によるものとする。

１　担当部局等

(1) 契約及び仕様書に関する事務を担当する部局等（以下「契約担当部局」という。）

〒990-8570

山形市松波二丁目８番１号

山形県総務部税政課税務システム担当　電話番号：023(630)2096

２　入札参加者の資格

(1) 「山形県競争入札参加資格者指名停止要綱に基づく指名停止措置を受けていないこと」とは、入札参加資格審査日（一般競争入札参加資格確認申請書又は競争入札参加資格審査申請書（以下「申請書」という。）の提出期限の日）から開札日までの期間中のいずれの日においても指名停止措置を受けていないことをいう。

(2) 公告で指定された期限までに申請書を提出しない者及び入札参加資格が無いと認められた者は、本件入札に参加することができない。

３　入札参加資格の審査等

(1) 本件入札に参加を希望する者は、入札公告の「入札参加者の資格」を有することを証するための申請書及び添付書類（以下「申請書等」という。）を、公告で指定された提出場所へ提出し、入札参加資格の審査を受けなければならない。

(2) 提出書類

①　入札参加者の資格に関する書類

(ｱ) 競争入札参加資格者名簿（物品及び役務の調達）に登載されている者

ａ　一般競争入札参加資格確認申請書（別紙様式第１号）

(ｲ) 競争入札参加資格者名簿（物品及び役務の調達）に登載されていない者

ａ　競争入札参加資格審査申請書提出書（別紙様式第１－１号）

ｂ　競争入札参加資格審査申請書及び添付書類(会計局が別に定める物品等競争入札参加資格審査申請要領による)

(3) 上記(2)の書類郵送で提出する場合は、書留郵便に限る。

(4) 申請書を提出した者は、入札日の前日までに添付書類に関し説明又は協議を求められた場合はこれに応じるものとし、必要な場合には添付書類の追加に応じるものとする。なお、その指示に応じないときは、入札参加資格がないものとみなす。

(5) 申請書の作成及び提出に係る費用は、申請者の負担とする。

4　入札参加資格審査結果の通知

(1) 入札参加資格の審査は、その提出期限の日を基準日として行うものとし、その結果は令和７年11月21日（金）までに通知する。

(2) 本件入札への参加は、前項の通知により、入札参加資格を有する者のみ行うことができるものとする。

5　仕様書に関する質問等

(1) 仕様書に関し質問がある場合は、令和７年11月14日（金）午後３時までに契約担当部局に一般競争入札仕様書等に関する質問書（別紙様式第７号）により持参又は郵送（書留郵便に限る。）で提出すること。なお、郵送による場合は、上記期限まで契約担当部局に到達しなければならない。

(2) (1)の質問に対する回答は、質問者あて書面により行うとともに、その回答書は、当該回答を行った日の翌日から入札執行の日時までの期間、山形県総務部税政課において閲覧に供する。

6　入札の辞退等

(1) 入札参加者は、入札書を提出するまでの間は、いつでも入札を辞退することができる。入札を辞退する場合は、書面により行うものとする。この場合は、辞退する役務の名称、入札日、辞退する者の氏名又は名称、辞退する理由を記載した書面に代表者印を押印し、入札を執行する日時までに提出するものとする。

(2) 入札参加者が入札執行時刻に遅れた場合は、本件入札を棄権したものとみなす。

7　入札

(1) 入札書の様式は、入札書（別紙様式第８号）による。

(2) 入札書は入札公告の「入札の場所及び日時」に持参するものとするが、郵送による提出も認める。（書留郵便に限る。）

(3) 入札書は封筒に入れて厳封し、表に「氏名又は名称」及び「物品等の名称」を記載すること。

(4) 入札書を郵便により提出する場合は二重封筒とし、入札書を中封筒に厳封の上、上記(3)の内容を記載し、表封筒に「入札書在中」と朱書きすること。なお、令和７年12月３日（水）午後５時までに契約担当部局に必着とし、当該日時までに到達しなかった場合は棄権とみなす。

(5) 入札者は名刺を提出し、代理人をして入札に関する行為をさせようとする者は、委任状（別紙様式第９号）を作成し提出させること。

(6) 入札者又は入札者の代理人は、当該入札に関する他の入札者の代理をすることはできない。また、法人の代表者（支店長等の受任者を含む。）が自ら入札する場合は、当該入札に関して他の入札者となることはできない。

(7) 入札価格には、役務の遂行に必要な打合せ等の付随業務に係る旅費、日当、使用料、その他一切の諸経費を含む総額とする。

(8) 入札に際し、入札書に記載される入札金額並びに契約期間における年度ごと及び月ごとに対応した積算内訳書を提出すること。

8　開札

入札者又はその代理人は開札に立ち会うものとする。入札者又はその代理人が立ち会わない場合においては、入札事務に関係のない山形県職員を立ち合わせて開札を行う。

開札に立ち会わない入札者は、開札結果の通知に必要な返信用封筒に、受取人の住所、氏名又は名称等を明記のうえ、所定の料金の切手を貼ったものを入札書とともに提出しなければならない。

9　入札の無効

次に掲げる入札は無効とする。

(1) 入札公告に示した入札参加資格のない者（入札参加資格があることを確認された者で、開札時において入札公告に示した入札参加資格を満たさなくなった者を含む。）のした入札

(2) 申請書に虚偽の記載をした者のした入札

(3) 委任状を持参しない代理人のした入札

(4) 入札の公正な執行を妨げ、又は公正な価格の成立を害し、若しくは不正の利益を得るため連合したと認められる入札

(5) 同一の事項につき２通以上の入札書を契約担当者に提出した入札

(6) 金額、氏名等の入札要件が確認できない入札書、記名押印を欠く入札書又は入札金額を訂正した入札を契約担当者に提出した入札

(7) その他入札に関する条件に違反した入札

10　再度入札

予定価格の制限の範囲内の価格の入札がないときは、直ちに再度の入札を行う場合がある。

再度の入札を辞退するときは、入札書に「辞退」と記載し、提出すること。

入札を一度辞退した者は、当該入札案件の再度の入札に参加することはできない。

11　落札者の決定方法

(1) 規則第 120 条第１項の規定により作成された予定価格の範囲内で最低の価格をもって入札（有効な入札に限る。）を行った者を落札者とする。

(2) 落札となるべき同価の入札をした者が二人以上あるときは、直ちに当該入札者にくじを引かせて落札者を決定する。この場合において、当該入札者のうち立ち会わない者又はくじを引かない者があるときは、当該入札執行事務に関係のない山形県職員にこれに代わってくじを引かせ落札者を決定する。

(3) 落札者の決定の時までに入札参加資格を満たさなくなった者は落札者としない。

12　その他

(1) 申請書に虚偽の記載をした場合においては、山形県競争入札参加資格者指名停止要綱に基づく指名停止措置を行うことがある。

(2) 入札参加者の連合、その他の理由により入札を公正に執行することができないと認められるときは、当該入札参加者を入札に参加させず、又は入札の執行を延期し、若

しくは取り止めることがある。
(3) 入札をした者は、入札後、契約条項又は入札条件等の不明を理由として異議を申立てることができない。
(4) 落札者は予約完結権を他に譲渡することができない。
(5) 入札者又はその代理人は、即日口頭落札決定通知を受領するための印鑑（入札書に使用する印鑑に限る。ただし、代理人の場合は当該代理人の印鑑とする。）を持参すること。なお、当該印鑑を持参できない場合は、入札執行時の指示により落札決定を通知する。
(6) 本件契約の条項は、別に示す契約書（書式）による。
(7) その他必要とする入札に関する条件については、入札執行時の指示による。

様式第１号（一般競争入札参加資格確認申請書）

年　　月　　日

山形県知事　吉村　美栄子　殿

住所又は所在地
氏名又は名称
代表者氏名

一般競争入札参加資格確認申請書

下記役務の調達に係る入札参加資格について確認されたく申請します。
なお、公告された資格を有すること並びに添付書類の内容については事実と相違ないことを誓約します。

記

１　調達役務の入札公告日及び名称
(1) 入札公告日　令和７年 10 月 24 日
(2) 役務の名称　山形県税務総合電算システム運用支援業務

２　添付書類

※登録番号	※確認印

※申請者は記入しないでください。

様式第１－１号（競争入札参加資格者名簿未登載者用）

年　　月　　日

山形県知事　吉村　美栄子　殿

住所又は所在地
氏名又は名称
代表者氏名

一般競争入札参加資格審査申請書提出書

下記役務の調達に参加したいので、別添のとおり競争入札参加資格審査申請書を提出します。

なお、公告された資格を有すること並びに添付書類の内容については事実と相違ないことを誓約します。

記

１　調達役務の入札公告日及び名称

(1) 入札公告日　令和７年 10 月 24 日

(2) 役務の名称　山形県税務総合電算システム運用支援業務

２　添付書類

※登録番号	※確認印

※申請者は記入しないでください。

様式第７号（一般競争入札仕様書等に関する質問書）

年　　月　　日

山形県知事　吉村　美栄子　　殿

住所又は所在地
氏名又は名称
代表者氏名

競争入札に関する質問書

下記役務の調達に係る仕様書等について、下記のとおり質問します。

記

１　調達役務の入札公告日及び名称
(1) 入札公告日　令和７年 10 月 24 日
(2) 役務の名称　山形県税務総合電算システム運用支援業務

２　質問事項等

様式第８号（入札書）

入　札　書

年　月　日

山形県知事　吉村　美栄子　殿

入札者　住所又は所在地※1

氏名又は名称及び代表者名

㊞

〔 代理人氏名※2 ㊞ 〕

山形県財務規則及び本件契約の条項により入札条件を承認し、下記のとおり入札します。

記

入札金額	￥
入札保証金額	免　除
役務の名称及び規格	山形県税務総合電算システム運用支援業務 （規格は仕様書のとおり）
数量	仕様書のとおり
納入場所又は引渡場所	仕様書のとおり
履行期間又は履行期限	令和８年１月１日から令和 10 年 12 月 31 日まで
摘要	

※１　入札者の「住所又は所在地」並びに「氏名又は名称及び代表者名」は、必ず記載すること。（代理人が入札する場合であっても、記載すること。その場合、押印は不要。）

※２　代理人が入札する場合は、※１の記載に加え、〔　〕欄に記名・押印のうえ入札すること。

様式第９号（委任状）

委　　任　　状

年　　月　　日

山形県知事　吉村美栄子　殿

住所又は所在地
氏名又は名称
代表者氏名　　㊞

私は　　を代理人と定め、下記の権限を

（使用印鑑　　）

委任します。

記

１　山形県税務総合電算システム運用支援業務の入札並びに見積に関する一切の件

２　委　任　期　間

年　　月　　日　から

年　　月　　日　まで

資料番号2

山形県税務総合電算システム運用支援業務

委託仕様書

令和７年 10 月
山　形　県

1　委託業務の名称

山形県税務総合電算システム運用支援業務

2　委託期間

令和8年1月1日から令和 10 年 12 月 31 日まで

3　履行場所

・山形県山形市松波二丁目8番1号　山形県庁舎内

・その他発注者が指定する場所

4　委託業務の概要

山形県税務総合電算システムの安定的な運用のための運用支援業務を委託するもの

5　システムの概要

図1　システム機能概要図

本システムは、県税（対象税目：個人県民税、個人事業税、法人二税、県民税三割、不動産取得税、自動車税、軽油引取税、ゴルフ場利用税、県たばこ税、鉱区税、狩猟税、産業廃棄物税、その他税）の賦課徴収業務を行うシステムである。

本システムは、課税システム、収納管理、収入計算書、滞納整理システム、外部連携、共通システム（宛名管理、共通マスタ・コード、EUC）から構成されている。（参照：図1　システム機能概要図）

本システムは、稼動基盤を県庁外部のインターネットデータセンター（以下「iDC」という。）に構築し、専用回線によって県基幹高速通信ネットワークと接続している。

県税に係る事務を行う県庁及び各公所（総務部税政課、村山総合支庁課税課・納税課・漆山分

室・西村山税務室・北村山税務室、最上総合支庁税務課、置賜総合支庁税務課・西置賜税務室及び庄内総合支庁税務課・押切分室）の職員は、情報系パソコン及びシステム専用端末のWEBブラウザから、県基幹高速通信ネットワークを経由して本システムを利用している。

（4） 用語の定義

用語	定義
県基幹高速通信ネットワーク	県の公所約 160 拠点及び県内市町村が接続されたネットワークであり、インターネット接続、電子メール利用、イントラ情報システム等各種業務システム利用、県ホームページ公開等を行う電子県庁推進の基盤として運用しているもの。
情報系パソコン	本県の情報主管課が一括で購入し、職員が業務で利用するPCの総称。税務担当者は原則的にこのPC（約 190 台）から本システムにアクセスする。基本的な仕様は次のとおり。 OS：Windows11 Pro　ブラウザ：Edge
システム専用端末	情報系パソコンとは別に、システム専用端末として調達するクライアント用PCの総称。27台が配備され、主に各公所の窓口業務用及びシステム運用管理用に利用されている。基本的な仕様は次のとおり。 OS：Windows11 Pro　ブラウザ：Edge　CPU：2.5Ghz　メモリ：8GB　SSD：500GB
稼動基盤	本システムを稼動させるために必要な、サーバ機器、ネットワーク機器、各種ソフトウェア及び IDC とその接続回線をいう。 山形県大規模システム統合基盤として庁内 3 システム（財務、総務事務、人事給与）と共有しており、情報主管課で運用管理している。

6 委託作業の内容

設計書及び各種手順書等の記載内容に基づき、山形県税務総合電算システムの運用管理支援業務を行うこと。主な業務は(1)から(4)のとおり。

(1) 運用状況の分析監視

・システム改善要望に対する技術的検討及び決定された改善内容に係るシステム修正（業務委託期間において、想定される作業工数が 12 月あたりおおむね3人月以上となる改修については対象外とする。）。 なお、山形県税務総合電算システムの改修について、発注者が別途調達を行う場合には、本番稼動までの試験等の検証作業について支援すること。

・定期的な意見交換によるシステム分析

(2) 税務関係職員に対する研修の実施と研修支援

・総務部税政課職員が利用者を対象に実施するシステム研修の支援

・システム運用の研修

(3) 運用・サポート

・システムで保有するデータの抽出・加工

・自動車保有関係手続のワンストップサービス（OSS）都道府県税共同利用化システムの運用管理のサポート（税制改正時のシステム更新作業、課税標準額ファイル更新、カレンダーファイル更新、申告データ等抽出、不要ファイル削除等）

(4) 管理業務

・ドキュメントの整備

・稼動基盤運用に関する支援

・運用状況の月次報告会の開催

7 作業の実施に関する要件

（1） 運用・保守に関する要件

① 運用期間

令和8年 1 月 1 日から令和 10 年 12 月 31 日までとする。

② 運用時間

本システムのオンラインサービス提供時間（山形県の開庁日の午前 8 時 30 分から午後 5 時 15 分まで）を基準とし、県が示すスケジュールや運用上の必要に応じて延長運用を行うものとする。

③ 障害対応

業務委託期間中における緊急事態に備えた連絡体制を整備し、委託業務の遂行上問題・事故等が発生した場合は、受注者は速やかに発注者に報告すること。

④ サービス品質

SLAに関しては、現行の SLA 定義書を踏まえたうえで、県と検討の上決定すること。

⑤ 運用業務の引き継ぎ

(ｱ) 委託期間開始前

令和7年 12 月 31 日で契約期間が満了する現行の運用支援業務受注者から業務についての引継ぎを受け、令和8年 1 月 1 日の業務開始に備えること。

業務の引継ぎ期間及びスケジュールについて、現行の運用支援業務受注者と協議のうえ決定し、発注者に対し事前に報告すること。なお、この業務引継ぎに要する経費は本業務の受注者が負担すること。

(ｲ) 委託期間満了時

委託期間満了等により、受注者が本委託業務の受注者でなくなる場合、受注者は、次期受注者に対し、本委託業務に関して十分な引き継ぎを行うこと。

業務引き継ぎは、委託期間満了日までに完了することとし、次期受注者が円滑に業務を実施できるようサポートすること。

なお、この業務引き継ぎに要する経費は次期受注者の負担とする。

(ｳ) 委託期間満了後

委託期間満了後、発注者及び次期受注者から業務に関し照会があったときは、それに応じること。

（2） その他全般的事項

① 作業環境等

・特に断りのない場合、受注者の作業場所及び業務の実施に必要な設備・機器については、県から別途指示がない限り、受注者の責任において確保すること。

・県庁舎内において作業を行う場合は、「山形県庁内管理規則」等の県庁舎管理に係る規定を遵守し、場所の使用に係る一切の事項について県の指示に従うとともに、作業従事者の品位の保持に努めること。
・開発時に使用する稼動環境等の管理者パスワードについては、必要な開発者以外に周知しないこと。また、開発者が使用するアカウントについても十分注意して管理し、不要なアカウントを発行しないようにすること。これらのアカウント・パスワードは、本稼動前に必ず削除もしくは変更すること。
・本システムとのリモート接続は認めない。

② 費用負担等

・業務に必要な経費（交通費等）は原則として委託業務に含むものとする。
・山形県税務総合電算システムに接続するパソコン等は、発注者が別途調達した機器を利用するものとする。
・その他業務の実施に必要な機器や消耗品等については、発注者から別途指定等のない限り、受注者の責任において準備すること。
・本業務の実施にあたり、関係事業者（システム開発事業者、県ネットワーク関係事業者、大規模システム統合基盤関係事業者等）の支援が必要な場合には、各事業者に要請できるものとするが、それにかかる費用については、本業務の委託費の中に含んでいるものとする。

③ 使用物件・資料

・業務の実施にあたり必要と認められる資料等については貸与する。ただし善良な注意義務をもってこれを保持し、発注者の承諾なく第三者に公表または貸与してはならない。
・受注者は、県が使用させる資料及び帳票等の管理体制及び業務従事者以外の者に使用させないための対策を提示すること。なお、情報漏えい防止の観点から、情報の管理状況を県が定期的又は随時確認する場合があるため、これに対応すること。
・業務完了等により県が使用させた資料及び帳票等が不要になった場合、当該資料を県に返還すること。資料等を複写している場合は複写物を廃棄するとともに、廃棄した旨を書面で報告すること。
・本システムは個人情報を扱っており、実データについては本システム外には持ち出しできないものである。
・開発時に使用するデータ、特に個人情報に係るものは基本的にダミーデータを用意するものとし、テスト等で稼動環境に近いデータが必要な場合は、個人が特定できないように加工するなど、個人情報漏えいが起こらないようにすること。

④ 情報セキュリティの確保

・山形県情報セキュリティポリシーを遵守すること。
・業務従事者に対しセキュリティ教育を実施すること。
・業務上知り得た情報の守秘義務を遵守すること。
・委託業務終了時は情報資産の返還、廃棄等を確実に行うこと。
・発注者がセキュリティ監査等を実施する場合には、監査・検査を受け入れすること。

⑤ その他

・本委託業務の実施にあたっては、「山形県情報システム導入標準ガイドライン」を理解し、遵守すること。

9 作業実施体制等に関する要件

（1） 要員配置

受注者は税務関連の法令用語を理解する者で、次の要件を満たす要員を配置し、契約締結後に業務実施体制を書面にて発注者に提出すること。

なお、運用SEは、原則的に山形県総務部税政課内に合せて3名以上を専任で常駐させ業務を遂行することとし、この要員を変更する場合は、変更する1ヶ月前までに交代する後任者の報告を県に行い、了承を得ること。要員の交代の際には、本業務に支障を来たさないように十分な訓練を行った後、後任者に引継ぎを行うこと。

要員名称	役割・資格要件
運用管理責任者	過去5年以内に、都道府県税務システムに係る運用管理業務に従事した経験を有し、かつ、省令に規定するITサービスマネージャ試験に合格した者又は同等以上の資格若しくは能力を有する者で、税務総合電算システムの性能・障害・セキュリティ管理及び業務要件を踏まえた安定的・効率的な運用管理、関係者の調整・管理能力を有すること。
運用SE	税務総合電算システムを維持管理するための監視業務や、障害発生時の迅速な切り分けができ、軽微なシステム改修やシステム内を調査するために Java、COBOL 言語を習得し、Shell を操作できる能力を有する者で、過去5年以内に、都道府県税務システムに係る運用支援業務又は開発業務に従事した経験を有すること。

（2） 作業環境

受注者が作業を実施するための作業環境に係る要件は以下のとおりとする。作業を実施する上で県が用意する環境の使用に当たって、十分な注意を払い、適切に使用すること。また、受注者は、これらをシステム運用支援作業以外の目的に利用しないこととするが、県の承認があった場合、システム運用支援に影響を与えない範囲で、本業務のシステム移行作業で利用することができる。

① 県が用意する環境

・システム運用支援用スペース（県庁舎内）

・システム運用管理用機器及びツール類（本システム用運用管理端末、プリンタ等）

② 受注者において用意する環境

作業を実施する上で上記①以外に必要となる環境。

（3） 委託業務従事者の適正な労働条件の確保

① 受注者は、従事者の雇用にあたっては、労働基準法、最低賃金法及び労働安全衛生法等の労働関係法令を遵守すること。

② 受注者は、業務の責任者（管理者、主任者）については、正規職員や社会保険被保険者を配置すること。

10 別途調達する業務

次に調達する業務などは発注者が別途調達を行うが、本委託業務の適正かつ円滑な実施及びシステムの安定運用の確保のため、以下に示す業務の受注者等と情報共有・相互連携の上、本業務を遂行すること。

① 山形県大規模システム統合基盤関係業務（稼働基盤・情報主管課所管）

② 山形県税務総合電算システム利用環境導入及び運用管理業務

③ その他連携を行う外部システム・収納チャネル

- ・地方税ポータルシステム（電子申告、国税連携システム、共通納税システム）
- ・自動車保有関係手続きのワンストップサービスシステム（OSS）
- ・コンビニ収納システム
- ・山形県財務会計システム
- ・山形県認証認可システム
- ・軽油流通情報システム
- ・自動車税分配情報システム
- ・自動車税納税状況 Web 確認システム

11 成果品等

受注者は、本委託業務における成果物のドキュメントの内容及び体裁、部数、納入時期について、県とあらかじめ十分協議し、その承認を受けたのち、指定された様式等で作成すること。

なお、現在想定している成果物及び提出時期は下表のとおり。

	ドキュメント名	提出時期
1	運用実績報告書	月次（翌月速やかに）
2	SLA 報告書	月次（翌月速やかに）
3	その他業務中に作成した各種ドキュメント	随時

12 その他

受注者は、本仕様書に定めのない事項、本仕様書に定める業務の実施にあたって必要な詳細事項及び本仕様書の解釈に疑義が生じたときは、遅滞なく県と協議して定めるものとする。

業 務 委 託 契 約 書（書式）

資料番号３

委託業務の名称　　山形県税務総合電算システム運用支援業務

委　託　期　間　　令和８年１月１日から令和 10 年 12 月 31 日まで

業 務 委 託 料　　金　　円（うち消費税及び地方消費税の額　　円）

契 約 保 証 金　　契約金額の 100 分の 10 に相当する金額以上の額とする。
ただし、山形県財務規則第 135 条各号のいずれかに該当する場合は免除する。

頭書業務の委託について、委託者 山形県知事 吉村　美栄子を発注者とし、受託者 ○○○○ を受注者とし、次の条項により委託契約を締結する。

（総則）

第１条　受注者は、別紙「山形県税務総合電算システム運用支援業務委託仕様書」（以下「委託仕様書」という。）に基づき、頭書の業務委託料（以下「委託料」という。）をもって、頭書の委託期間の終期（以下「履行期限」という。）までに頭書の委託業務（以下「委託業務」という。）を実施し、その結果（以下「成果品」という。）を発注者に引き渡すものとする。

２　前項の「委託仕様書」に明記されていない仕様があるとき又は明記されていない仕様が必要となった場合は、発注者、受注者協議して定める。

（業務遂行上の義務）

第２条　受注者は、委託業務に従事する者（以下「従事者」という。）に、委託業務の遂行に必要な技術を習得させ、委託業務の遂行に万全を期するものとする。

２　受注者は、委託業務を遂行するために、発注者の事務室等に立ち入る場合には、安全管理・秩序維持等に関する発注者の諸規則を遵守するものとする。

（従事者の管理）

第３条　受注者は、契約締結後すみやかに従事者の氏名を発注者に通知するものとする。

２　受注者は、従事者の管理について、一切の責任を負う。

３　発注者は、従事者のうち不適当と認められる者があるときは、受注者に対してその交替を求めることができる。

（秘密の保持等）

第４条　受注者は、委託業務の遂行上直接若しくは間接に知り得た秘密を外部に漏らし、又は他の目的に利用してはならない。

２　受注者は、この契約に係る受注者の従事者及びその他の者に、発注者の秘密を保持することの重要性を認識させ、故意又は過失による漏洩防止対策を講ずるとともに、漏洩防止対策を徹底させる

ため、あらゆる機会を通じ、絶えず教育・訓練を行う等の前項の義務を遵守させるために必要な措置を講じなければならない。

３　前２項の規定は、この契約が終了し、又は解除された後においても同様とする。

（個人情報の保護）

第５条　受注者は、この契約による事務を行うため個人情報を取り扱う場合は、別記「個人情報取扱特記事項」を遵守しなければならない。

（山形県情報セキュリティポリシー遵守義務）

第６条　受注者は、この契約による業務を実施するに当たっては、山形県情報セキュリティポリシーを遵守しなければならない。

（監督及び指示並びに調査及び報告）

第７条　受注者は、この契約に基づく委託業務の実施について、発注者の監督及び指示に従わなければならない。

２　発注者は、必要があるときは、受注者に対し委託業務の実施状況について実地に調査し、又は書面による報告を求めることができる。

（責任者）

第８条　発注者及び受注者は、本契約締結後すみやかに、各自の責任者をそれぞれ選任し、互いに書面により、相手方に通知する。なお、成果品として定められた資料等において双方の体制図を定め、当該体制図に当該責任者を記載することをもって通知に代えることができるものとする。

２　発注者及び受注者は、事前に書面により相手方に通知することにより、責任者を変更できるものとする。

（資料等）

第９条　発注者は、受注者が委託業務を実施する過程で必要となる発注者の帳票、関係資料等（以下「資料等」という。）を受注者に使用させるものとする。なお、使用期間、使用条件等については、必要に応じて、発注者、受注者協議のうえ取り決めるものとする。

２　受注者は、前項の資料等について、紛失・破損しないように、保管・管理を厳重にしなければならない。

３　受注者は、次の各号に該当する場合は、第１項の資料等を速やかに発注者に返却するものとする。

(1) 業務が完了した場合

(2) 使用期間が経過した場合

(3) その他合理的な理由により発注者が返却を要求した場合

（損害賠償）

第10条　受注者は、委託業務の処理に関し、故意又は過失により、発注者又は第三者に損害を与えたときは、その損害を賠償しなければならない。

２　前項の規定による賠償額は、発注者、受注者協議により定めるものとする。

（権利及び義務の譲渡禁止）

第11条　受注者は、この契約によって生ずる権利及び義務を第三者に譲渡し、又は承継させてはならない。ただし、あらかじめ書面により発注者の承認を得たときは、この限りでない。

（再委託の禁止）

第12条　受注者は、委託業務の全部又は一部を第三者に委託してはならない。ただし、あらかじめ書面により発注者の承認を得たときは、この限りでない。

２　受注者は、前項の規定に基づき第三者へ委託する場合は、当該第三者に対し第４条に規定する秘密の保持及び第５条に規定する個人情報の保護、第６条に規定する山形県情報セキュリティポリシー遵守義務、第19条に規定する成果品に関する権利の帰属に関する義務を負わせるものとする。

（契約内容の変更等）

第13条　発注者は、必要がある場合には、委託業務の内容を変更し、又は委託業務を一時中断することができる。この場合において、委託料又は履行期限を変更する必要がある場合は、発注者、受注者協議して書面によりこれを定めるものとする。

２　前項の場合において、受注者が損害を受けたときは、発注者は、その損害を賠償しなければならない。この場合の賠償額は、発注者、受注者協議して定める。

（契約の解除）

第14条　発注者は、受注者が次の各号のいずれかに該当する場合においては、この契約を解除することができる。

(1) この契約に違反し、又は違反するおそれがあると認めたとき。

(2) この契約の履行について、不正の行為があったとき。

(3) 正当な理由がなく、この契約の履行を怠ったとき。

(4) 故意又は過失により発注者に重大な損害を与えたとき。

(5) 受注者が次のいずれかに該当するとき。

イ　役員等（受注者が個人である場合にはその者を、受注者が法人である場合にはその役員又はその支店若しくは契約を締結する事務所の代表者をいう。以下この号において同じ。）が暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）第２条第６号に規定する暴力団員（以下この号において「暴力団員」という。）又は暴力団員でなくなった日から５年を経過しない者（以下この号において「暴力団員等」という。）であると認められるとき。

ロ　暴力団（暴力団員による不当な行為の防止等に関する法律第２条第２号に規定する暴力団をいう。以下この号において同じ。）又は暴力団員等が経営に実質的に関与していると認められるとき。

ハ　役員等が自己、自社若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもって、暴力団又は暴力団員等を利用する等したと認められるとき。

ニ　役員等が、暴力団又は暴力団員等に対して資金等を供給し、又は便宜を供与する等直接的あるいは積極的に暴力団の維持及び運営に協力し、又は関与していると認められるとき。

ホ　役員等が暴力団又は暴力団員等と社会的に非難されるべき関係を有していると認められるとき。

ヘ　下請契約又は資材、原材料の購入契約その他の契約に当たり、その相手方がイからホまでのいずれかに該当することを知りながら、当該者と契約を締結したと認められるとき。

ト　受注者が、イからホまでのいずれかに該当する者を下請契約又は資材、原材料の購入契約その他の契約の相手方としていた場合（へに該当する場合を除く。）に、発注者が受注者に対して当該契約の解除を求め、受注者がこれに従わなかったとき。

2　発注者は、前項各号に規定する場合のほか、特に必要があるときは、この契約を解除することができる。この場合において、受注者が損害を受けたときは、発注者は、その損害額を負担するものとする。この場合の損害額は、発注者、受注者協議して定める。

3　第１項第１号から第３号まで又は第５号の規定によりこの契約を解除する場合には、契約保証金は、発注者に帰属するものとする。ただし、契約保証金が免除されている場合には、受注者は、発注者に対し解除違約金として契約金額の100分の10に相当する金額を納付しなければならない。

4　第１項第４号の規定によりこの契約を解除する場合には、受注者は、発注者に与えた損害を賠償しなければならない。この場合の賠償額は、発注者、受注者協議して定める。

5　発注者は、この契約を解除しようとするときは、その理由を記載した書面により受注者に通知するものとする。

6　発注者は、翌年度以降において、本契約に係る歳入歳出予算の当該金額について減額又は削除があった場合は、この契約を解除する。

（談合等に係る契約解除）

第15条　前条に定める場合のほか、発注者は、この契約に関して次の各号のいずれかに該当する場合においては、この契約を解除することができる。

(1) 受注者が私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54号。以下「独占禁止法」という。）第７条第１項若しくは第２項（第８条の２第２項及び第20条第２項において準用する場合を含む。）、第８条の２第１項若しくは第３項、第17条の２又は第20条第１項の規定による命令を受け、当該命令に係る抗告訴訟（行政事件訴訟法（昭和37年法律第139号）第３条第１項に規定する抗告訴訟をいう。以下この条において同じ。）を提起しなかったとき。

(2) 受注者が独占禁止法第７条の２第１項（第８条の３において読み替えて準用する場合を含む。）、第７条の９第１項若しくは第２項又は第20条の２から第20条の６までの規定による命令を受け、当該命令に係る抗告訴訟を提起しなかったとき。

(3) 受注者が前２号に規定する抗告訴訟を提起し、当該抗告訴訟について棄却又は却下の判決が確定したとき。

(4) 受注者（法人の場合にあっては、その役員又はその使用人）が刑法（明治40年法律第45号）第96条の６若しくは第198条又は公職にある者等のあっせん行為による利得等の処罰に関する法律（平成12年法律第130号）第４条の規定による刑に処せられたとき。

２　受注者は、この契約に関して前項各号のいずれかに該当するときは、発注者が契約を解除するか否かを問わず、賠償金として、契約金額の100分の10に相当する額を発注者の指定する期間内に支払わなければならない。ただし、発注者が特に認める場合は、この限りでない。

３　この契約の履行後に、受注者が第１項各号のいずれかに該当することが明らかになった場合についても、前項と同様とする。

４　第２項の規定は、同項の規定に該当する原因となった違反行為により発注者に生じた実際の損害額が同項に規定する賠償金の額を超える場合においては、発注者がその超える部分に相当する額につき賠償を請求することを妨げるものではない。

（事故発生の通知）

第16条　受注者は、委託業務の処理に関し事故が生じたときは、直ちに発注者に対し通知するとともに、遅滞なくその状況を書面をもって発注者に報告し、事故処理等に関する今後の方針案を提出しなければならない。

（業務完了報告等）

第17条　受注者は、月ごとの委託業務を完了したときは、遅滞なく発注者に対して業務完了報告書を提出しなければならない。この場合において、業務完了報告書への押印は不要であり、電子メールでの提出も可能とする。

２　発注者は、前項の業務完了報告書を受理したときには、その日から起算して10日以内に成果品について検査を行わなければならない。この場合において、発注者は、当該検査の結果を書面により受注者に通知するものとする。

３　前項の検査の結果不合格となり、成果品について補正を命ぜられたときは、受注者は、発注者の指定する期日までに遅滞なく当該補正を行い、発注者に補正完了の届けを提出して再検査を受けなければならない。この場合において、再検査の期日については、同項を準用する。

４　発注者は、検査合格の通知を受けたときは、遅滞なく当該成果品を発注者に引き渡すものとする。

（委託料の支払）

第18条　受注者は、前条の検査に合格したときは、発注者に対し別表「支払計画書」に掲げる月額の請求書を提出するものとする。この場合において、請求書への押印は不要であり、電子メールでの提出も可能とする。

２　発注者は、前項の規定による請求を受けたときは、その日から起算して30日以内に委託料を受注者に支払うものとする。

（成果品に関する権利の帰属）

第19条　成果品に係る著作権（著作権法（昭和45年法律第48号）第21条から第28条までに規定するものをいう。）及び所有権は、すべて発注者に帰属するものとする。ただし、成果品に含まれる受注者が従来より権利を有していた受注者固有の知識、技術に関する権利及び第三者が権利を有する著作物等については受注者又は当該第三者に留保される。この場合において、受注者は、当該著作権につ

いて、発注者及びその指定する者が必要とする範囲で、発注者及びその指定する者に対し、無償で利用することを許諾するものとする。

２　受注者は、前項に基づき発注者に著作権を移転し、あるいは発注者及びその指定する者に無償で著作権法に基づく利用が許諾された契約目的物に関し、著作権法第18条、第19条及び第20条第１項に規定する権利を行使しないものとする。

３　受注者は、成果品が第三者の著作権その他の権利を侵害していないことを保証し、万が一第三 者からの権利侵害に関する訴えが生じた場合には、受注者の責において解決するものとする。

（遅延利息）

第20条　受注者は、発注者の責めに帰する理由により第18条の規定による契約金額等の支払が遅れた場合においては、未受領金額につき、遅延日数に応じ、年2.5%の割合で計算した額の遅延利息の支払を発注者に請求することができる。この場合において、遅延利息の額が100円未満であるときは、発注者はこれを支払わないものとし、その額に100円未満の端数があるときは、その端数を切り捨てるものとする。

２　発注者は、その責めに帰する理由により第17条第２項に規定する期間内に検査をしないときは、その期間満了の日の翌日から検査をした日までの期間の日数を第18条第２項に規定する支払期間の日数から差し引くものとし、また、その遅延期間が支払期間の日数を超えるときは、支払期間は満了したものとみなし、その超える日数に応じ、前項の遅延利息を支払うものとする。

（発注者の履行追完請求権等）

第21条　成果品がこの契約の内容に適合しないときは、発注者は、その不適合を知った時から１年以内にその旨を受注者に通知した上で、当該不適合を理由として、履行の追完の請求、委託料の減額の請求、損害賠償の請求及び契約の解除をすることができる。

（履行遅滞違約金）

第22条　受注者がその責めに帰すべき事由によって、履行期限までに委託業務を完了することができない場合において、当該履行期限後相当の期間内に完了する見込みがあると認められるときは、発注者は、受注者から違約金を徴収して当該履行期限を延長することができる。

２　前項の違約金の額は、委託料から既成部分又は既成部分相当額を控除した額に対して、遅延日数に応じ、年2.5%の割合で計算した額とする。

（履行不能の場合の措置）

第23条　受注者は、天災その他その責めに帰することができない事由により、この契約の全部又は一部を履行することができないときは、発注者の承認を得て当該部分についての義務を免れるものとし、発注者は、当該部分についての委託料の支払を免れるものとする。

（疑義についての協議）

第24条　この契約に定めのない事項及びこの契約に関し疑義の生じた事項については、必要に応じ、発注者、受注者協議して定めるものとする。

発注者と受注者は、各々対等な立場における合意に基づいて、上記の条項によって業務委託契約を締結し、信義に従って誠実にこれを履行するものとする。

この契約の締結を証するため、本書２通を作成し、発注者、受注者記名押印の上、各自１通を保有する。

令和７年　　月　日

発注者　山形市松波二丁目８番１号
山形県知事　　吉　村　美栄子

受注者　○○○○○○○○○
○○○○○○○○○
○○○○○○○○○

別記

個人情報取扱特記事項

（基本的事項）

第１　受注者は、個人情報（個人に関する情報であって、特定の個人が識別され、又は識別され得るものをいう。以下同じ。）の保護の重要性を認識し、この契約による事務を行うに当たっては、個人の権利利益を侵害することのないよう、個人情報の取扱いを適正に行わなければならない。

（秘密の保持）

第２　受注者は、この契約による事務に関して知り得た個人情報を他に漏らしてはならない。この契約が終了し、又は解除された後においても同様とする。

（収集の制限）

第３　受注者は、この契約による事務を行うために個人情報を収集するときは、その目的を明確にし、　目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

２　受注者は、この契約による事務を行うために個人情報を収集するときは、本人から収集し、本人以外から収集するときは、本人の同意を得た上で収集しなければならない。ただし、発注者の承諾があるときは、この限りでない。

（漏えい、滅失及び毀損の防止）

第４　受注者は、この契約による事務に関して知り得た個人情報について、漏えい、滅失及び毀損の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

（目的外利用・提供の禁止）

第５　受注者は、この契約による事務に関して知り得た個人情報を当該事務の目的以外の目的に利用し、又は第三者に提供してはならない。

（複写又は複製の禁止）

第６　受注者は、発注者の承諾があるときを除き、この契約による事務を行うために発注者から提供された個人情報が記録された資料等を複写し、又は複製してはならない。

（事務従事者への周知）

第７　受注者は、この契約による事務に従事している者に対し、在職中及び退職後においても当該事務に関して知り得た個人情報を正当な理由なく他人に知らせ、又は当該事務の目的以外の目的に使用してはならないこと、山形県個人情報保護条例により罰則が適用される場合があることなど、個人情報の保護に必要な事項を周知させるものとする。

（再委託の禁止）

第８　受注者は、発注者の承諾があるときを除き、この契約による事務を第三者に委託してはならない。

（資料等の返還等）

第９　受注者は、この契約による事務を行うために、発注者から提供を受け、又は受注者自らが収集し、若しくは作成した個人情報が記録された資料等は、この契約の終了後直ちに発注者に返還し、又は引き渡すものとする。ただし、発注者が別に指示したときは当該方法によるものとする。

（調査）

第10　発注者は、受注者がこの契約による事務を行うに当たり取り扱っている個人情報の状況について、 随時調査することができる。

（事故発生時における報告）

第11　受注者は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに発注者に報告し、発注者の指示に従うものとする。

別表

支　払　計　画　書

年度	年	月	委託料（税抜）	消費税及び地方消費税	計	摘要
令和７年度	8	1	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		2	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		3	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	計		○,○○○,○○○	○○○,○○○	○,○○○,○○○	
令和８年度	8	4	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		5	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		6	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		7	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		8	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		9	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		10	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		11	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		12	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	9	1	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		2	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		3	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	計		○,○○○,○○○	○○○,○○○	○,○○○,○○○	
令和９年度	9	4	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		5	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		6	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		7	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		8	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		9	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		10	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		11	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		12	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	10	1	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		2	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		3	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	計		○,○○○,○○○	○○○,○○○	○,○○○,○○○	
令和10年度	10	4	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		5	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		6	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		7	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		8	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		9	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		10	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		11	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
		12	○,○○○,○○○	○○○,○○○	○,○○○,○○○	
	計		○,○○○,○○○	○○○,○○○	○,○○○,○○○	
合計			○,○○○,○○○	○○○,○○○	○,○○○,○○○	

資料番号４

山形県情報システム導入標準ガイドライン

令和4年 10 月 25 日

山形県みらい企画創造部やまがた幸せデジタル推進課

目次

第1 ガイドライン策定の背景について

本県では、「山形県情報システム開発・運用基本指針（平成 20 年3月策定、平成 26 年3月改定）に基づき、費用対効果の向上に留意しつつ、業務と情報システムの効率化に関する諸施策を推進してきました。

具体的には、県庁全体の視点から情報システムに係る費用の適正化と業務の効率化を図ることを目的に、平成 17 年 11 月に「山形県情報システム全体最適化計画」を策定し、大型汎用機を利用した情報システムを中心に効率的な情報システムへの移行及び再構築に取り組んできました。

また、平成 22 年度からは「山形県情報システム全体最適化計画（第二次）」に基づき、情報システム間の機器の共有化や構築済みの機能の再利用を図る効率的なシステム開発・運用へと移行するため、情報資産を管理するデータベースの構築を行うとともに、「山形県情報システム開発・運用ガイドライン（平成 23 年 3 月策定、平成 29 年3月改定）」を定め、情報システムの企画、開発、運用の各工程について、標準的な手順を示すことで品質の高い情報システムの構築等が行えるよう努めてきました。当該ガイドラインでは、共通基盤の利用による費用低減や、適正な情報セキュリティが確保されるよう、平成 29 年度に改定したところです。

さらに、平成 25 年度からは「山形県情報システム全体最適化計画（第三次）」に基づき ICT 環境の変化に的確に対応するために、情報システムの構築ルールの策定・見直しや、PDCA サイクル推進体制の強化、統一的な災害対策対応の実施に係る ICT-BCP 策定等の施策推進により、情報システムを活用した業務効率化の促進や費用削減などにも取り組んできました。

続いて、平成 28 年3月からは「山形県情報システム全体最適化計画（第四次）」に基づき、これまでの取組み状況についての課題及び情報システムを取り巻く環境の変化等を踏まえ、これまでの取組をより実効的に進めるため、県庁全体で情報システムに係る費用の適正化と業務の効率化を図ってきました。

加えて、クラウドサービスを利用することで、情報システム開発や機器導入、維持管理に要する経費の削減、システム保守や資産管理に係る利用者負担の軽減等といった効果が期待されることから、「山形県クラウドサービス導入活用指針（平成 26 年3月策定、平成 29 年3月改定）」を定め、適時に情報通信技術の進展に対応してきました。

本県においては、前述の情報システム等の導入について、「全体最適化計画」等の各種計画や指針等に基づき、基幹サーバや大規模システム統合基盤についてサーバの共通化を行いました。また、「やまがたｅ申請」を用いた県内市町村との電子申請・届出や施設予約システムの共同利用も推進してきました。さらに、WEB 会議や議事録作成、システム所管課が管理及び運用する情報システム等について、クラウドサービスの活用を図ってきました。

以上のことから、本県が定めた「全体最適化計画」等の各種指針と計画等に基づいた諸施策が情報システムに係る費用の適正化に一定の成果を得ることができました。

一方で、これまで本県が策定した情報システム導入等に関する各種指針と計画は、国の動

向や情報通信技術の進展の都度、整備を行っており、複数の計画と指針があったことから各業務担当課が情報システム等の導入の際に適時に、必要な指針等を確認しづらい状況にありました。そのため、情報システム導入等に関するノウハウが県庁全体に蓄積しているとは言いがたい状況です。

また、デジタル技術やデータを活用した、より一層の行政サービスの向上が求められています。そのため、業務の効率化をさらに図るために、業務及び情報システムの標準化や共通化も求められているところです。

以上のことから、情報システム導入等に関し、「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」や「デジタル社会の実現に向けた重点計画」及び「自治体デジタル・トランスフォーメーション（DX）推進計画」等の国が示している計画や指針等を参考にしながら、これまで本県が策定した各種計画や指針等を一元的に整理し、情報システム導入等における一連のプロセスをより一層の効率化を推進するため、その手続き・手順に関する基本的な方針を定める県の共通のルールを、「山形県情報システム導入標準ガイドライン」（以下「ガイドライン」という。）として策定しました。

なお、本県では、誰もがデジタル化の恩恵を受けられ、誰一人として取り残さない包摂的な社会づくりを基本理念として県の各分野においてデジタル化を推進することとしております。行政のデジタル化を進めるうえでも、この考え方を踏まえて情報システムの導入が行われるよう留意願います。

第2 情報システム導入における基本原則

情報システムは、ネットワーク化による利便性の向上、それに伴う脅威の増大等、以前にも増して多様化、複雑化してきています。また、情報システムの導入にあたっては、従来のような独自導入機器、独自開発ソフトウェアやパッケージソフトウェアに加えて、クラウドサービスの利用も一般的になりつつあります。本県においても、共通基盤等のプライベート・クラウド[1]の構築及び運用を推進してきました。今後もより一層の情報システムに係る費用の適正化と業務の効率化をさらに推進するため、以下の4原則のもと、情報システムを導入することを基本とします。

1 クラウド・バイ・デフォルト原則

クラウド・バイ・デフォルト原則とは、情報システムを導入する際に、クラウドサービスの利用を第一候補として検討を行うことです。国は「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（令和2年 7 月 17 日閣議決定）」及び「デジタル・ガバメント実行計画（令和2年 12 月 25 日閣議決定）」を策定し、当該原則を徹底することとしました。具体的にはクラウドサービスを利用することで、従来のオンプレミス[2]の情報システムに比べ、リソースの迅速な配備と柔軟な増減が可能となり、整備・変更に係る期間を短縮でき、自動化された運用による高度な信頼性や複数地域へのリソース配置による可用性の確保、サービスが提供する管理機能等を活用することによる運用負荷の低減を図ることを通じて、情報システムに係る費用を削減しつつ高品質な情報システムを整備することを目的としています。

本県でも、情報システムを導入する際には、クラウド・バイ・デフォルト原則を徹底し、共通基盤等のプライベート・クラウドの利用を含めて、クラウドサービスの利用を第1候補として検討します。

また、クラウドサービスの利用にあたっては、総務省が公表する「地方公共団体における情報セキュリティポリシーに関するガイドライン」を踏まえた本県の情報セキュリティポリシーを遵守し、情報セキュリティを確保する必要があります。具体的には、「政府情報システムのためのセキュリティ評価制度（ISMAP）[3]」及び、ISO/IEC27017[4]並びに SOC 報告書等のクラウドセキュリティ認証[5]等を取得しているクラウドサービスを利用することや、クラウドセキュリティ認証等と

---

[1] 情報システムのインフラをサービスとして遠隔から利用できるようにしたクラウド環境のうち、組織が自庁システムでの利用のためだけに用意した環境。

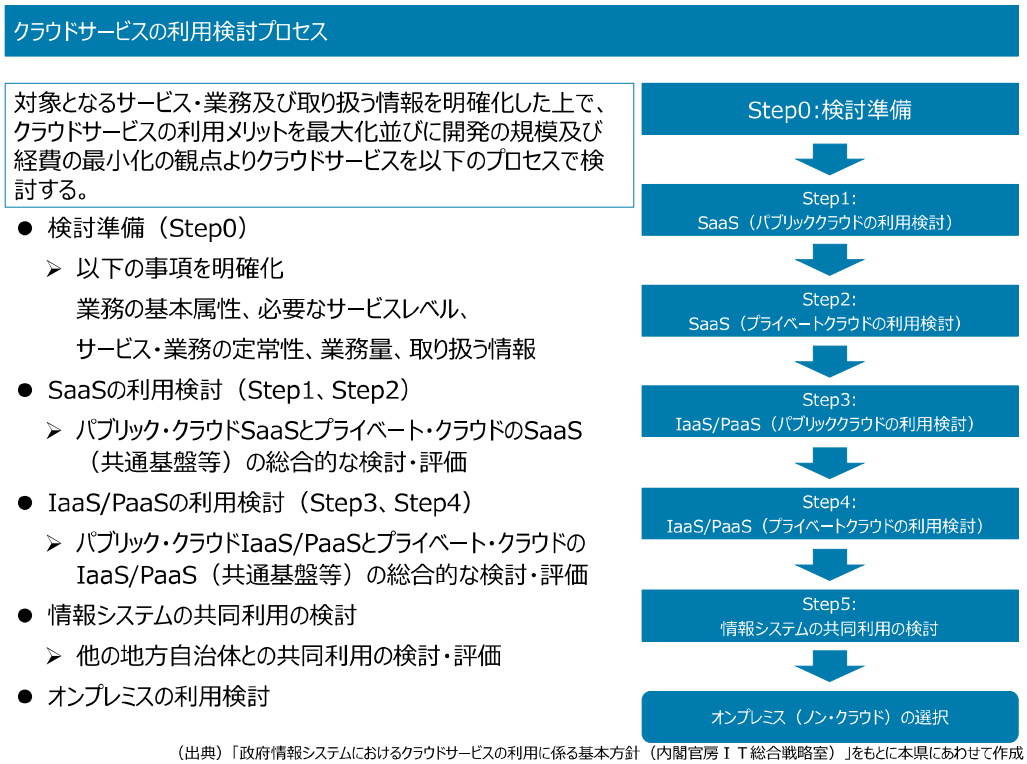
[2] 従来型の構築手法で、アプリケーションごとに個別の動作環境（データセンター、ハードウェア、サーバ等）を準備し、自らコントロールするもの。

[3] 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。

[4] 情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC27001 の取り組みをベースとして、クラウドサービスに関する情報セキュリティ管理策の強化を図ったガイドライン規格。

[5] クラウドサービスの情報セキュリティ機能の実態を利用者が個別に詳細に調査することは困難であるため、情報セキュリティ対策の有効性について第三者による認証や各クラウドサービスの提供している監査報告書を利用することが重要である。

同等の情報セキュリティ対策を行っているクラウドサービスを利用し、情報セキュリティ対策の維持及び向上を図ります。



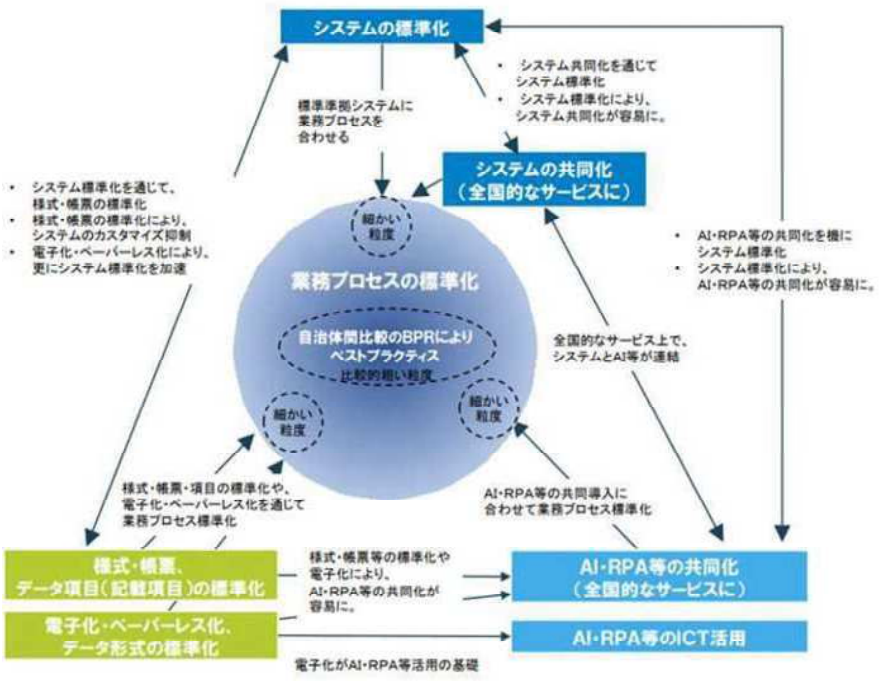
（出典）「政府情報システムにおけるクラウドサービスの利用に係る基本方針（内閣官房ＩＴ総合戦略室）」をもとに本県にあわせて作成

図 1 クラウドサービスの利用検討プロセス

2　業務の標準化とパッケージ導入及びノンカスタマイズ原則

国では、「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（令和2年 7月 17 日閣議決定）」及び「デジタル・ガバメント実行計画（令和2年 12 月 25 日閣議決定）」において、地方公共団体のデジタル化を推進するとともに、業務プロセス及び情報システムの標準化も推進しています。

本県でも、「全体最適化計画」に基づき、情報システムの独自開発の低減に努めてきました。しかしながら、県業務の独自性や業務の複雑性等から、一部で独自開発ソフトウェアの運用が行われています。今後も費用の適正化と業務の効率化に向け、他の都道府県等の業務の標準化の動向を参考にしつつ、本県における独自の業務について削減を進めることで、業務の標準化を図ります。また、情報システムの導入の際には、パッケージソフトウェアの導入可否の検討を実施することとし、パッケージ導入を基本とします。加えて、パッケージソフトウェアを導入する際には、情報システムに係る経費を抑制する観点から、ノンカスタマイズを原則とします。



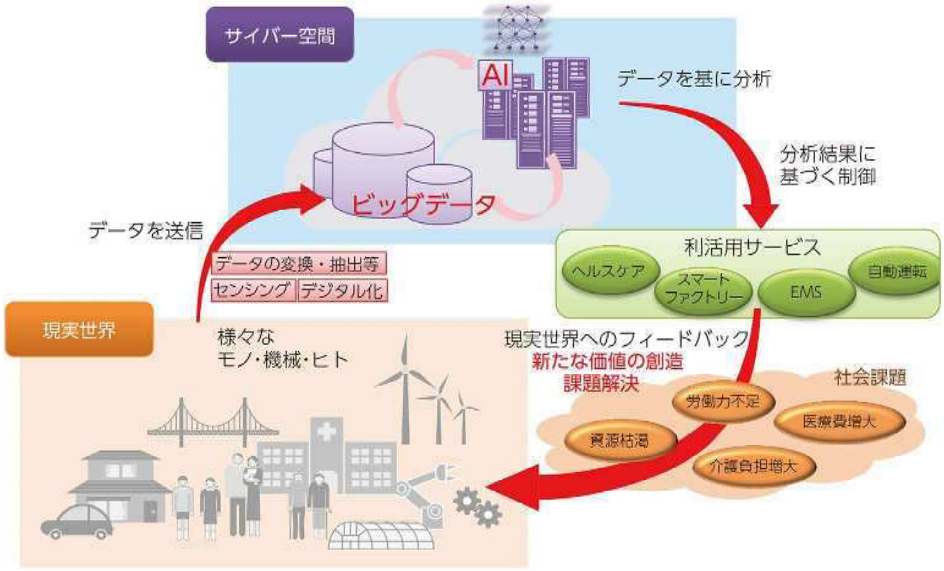
（出典）「地方自治体における業務プロセス・システムの標準化及びAI・ロボティクスの活用に関する研究会報告書（総務省）」

図 2　業務の標準化のイメージ図

3 先端技術の活用

本県でも、人口減少に伴い職員数の減少が進む一方、職員に求められる業務はむしろ増加傾向にあります。また、働き方改革などを背景に、労働生産性の向上はあらゆる組織において喫緊の課題となっています。このような状況を踏まえ、国は「自治体デジタル・トランスフォーメーション（DX）推進計画（令和2年 12 月 25 日）」を策定し、自治体の AI[6]・RPA[7]の利用を推進する方針です。本県でも、本格的な人口減少社会となる 2040 年頃を見据え、希少化する人的資源を本来注力するべき業務に振り向けるため、従来から職員が行ってきたシステム化されていない定型的な業務を中心として、AI・RPAを活用することを検討する等、先端技術の活用を基本とします。

加えて、先端技術を活用することのできる職員の育成を行います。



（出典）総務省「平成29年版 情報通信白書」

図 3 先端技術の活用イメージ図

[6] 人工知能のこと。Artificial Intelligence の略。
[7] ソフトウェア上のロボットによる業務工程の自動化のこと。Robotic Process Automation の略。

4　情報セキュリティポリシーの遵守

本県は、法令等に基づき、県民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供しています。また、本県の業務の多くに情報システムを用いています。

国や本県が推進する各種手続のオンライン利用の推進や情報システムの高度化等、電子自治体を進展することにより、情報システムの停止等が発生した場合、多くの業務が継続できなくなり、県民生活や地域の社会経済活動に重大な支障が生じる可能性も高まることが想定されます。

また、サイバー攻撃が複雑・巧妙化している中、個人情報の流出などにより、行政の信頼低下等の重大な影響を与える可能性も想定されます。県民生活や地域の社会経済活動を保護するため、情報セキュリティ対策を講じ、その保有する情報を守り、業務を継続することが必要となっています。

そのため、情報システムを導入、運用を行う際には、本県が定める情報セキュリティポリシーを遵守し、適切な情報セキュリティマネジメント体制を確保します。また、本県が定める情報セキュリティポリシーに従って、各種手順書等も適時に見直すこととします。

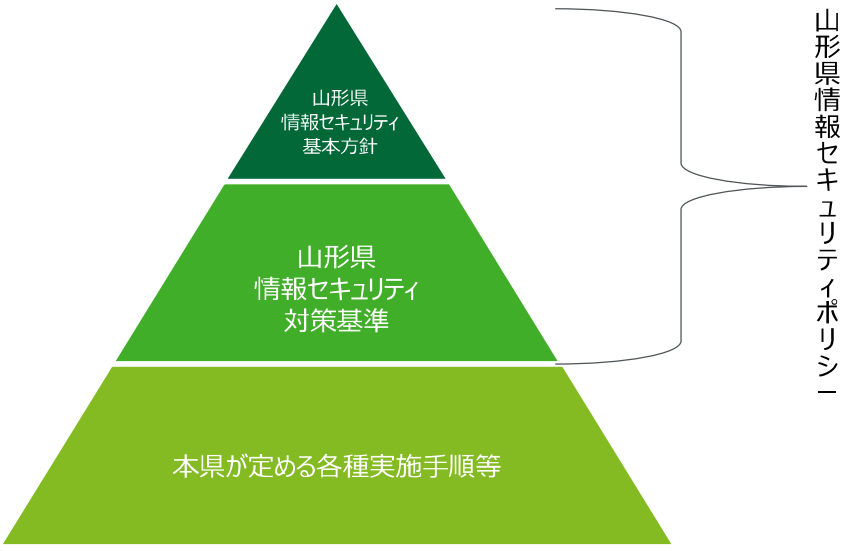
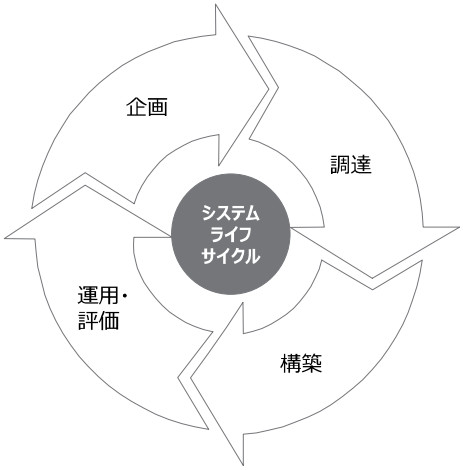


図 4 本県の情報セキュリティポリシーに関する体系図

第3 情報システム導入における調達プロセス

1 情報システム調達プロセス

情報システムは、ハードウェアやソフトウェアのサポート期限等にあわせて定期的な見直しが必要であり、企画から運用評価までの一連の流れをシステムライフサイクルと呼びます。各プロセスの名称や内容には様々な考え方がありますが、本県での定義を下図に示します。



■ 企画

事業の目的や目標を達成するために、構築するシステムの要求事項やシステム化の方針を明確にし、予算要求に必要な資料を準備する活動。

■ 調達

調達内容や予算額を確定し、委託事業者を決定するまでのプロセス。調達仕様書の作成、入札、契約等の活動。

■ 構築

情報システムを実際に開発していくプロセスで、基本設計、詳細設計、プログラミング、テストまでを含む活動。

■ 運用・評価

情報システムを運用する中で発生する障害への対応、各種ニーズや業務内容の変更に伴う改修、ハード・ソフトの利用環境の変化に伴う改修等の活動や、次期システムに向けたシステムの評価の活動。

図 5 情報システムにおけるライフサイクル

後年度負担の発生や職員負担の増加を低減し、情報システム調達を成功させるためには、企画段階及び調達段階において、十分な準備を行うことが重要であり、本ガイドラインは、企画・調達の内容に重点を置いています。

2 調達の分類

情報システムの調達は、下図の分類とします。情報システムの調達の分類に合わせて、調達に向けた準備作業を実施する必要があります。

調達の分類	概要
①新規システム	従来システム化していない業務を新たにシステム化する。（既存システム無し）
②システム更改	契約満了に伴い、次期システムや機器を置き換える。（既存システム有り）
③システムの改修	既存システムのプログラムを変更する。
④運用・保守	定期保守や障害対応など、システム導入後の維持管理を実施する。
⑤機器の調達	パソコンやプリンタ、スマートデバイス等の機器を単独購入する。（※購入にはリース提供も含める）
⑥再リース	既存の機器・ソフトウェアを一定期間延長してリースする。
⑦コンサルティング	企画段階の業務分析や調達仕様書作成の支援などを委託する。
⑧その他	分担金・負担金（定められた金額）の支払いや通信役務（インターネット回線料・閉域網使用料）など。

図 6 情報システム等の調達分類

3 調達協議

情報システムに係る調達協議とは、情報システムの構築、改修、リースなどの IT に関する調達を予定するシステム所管課が、調達計画や仕様書などを情報主管課と協議するものです。システム所管課は、本ガイドラインで定める「システム開発計画書」、「システム構築調書」、「統一見積書」及び「予算検証チェックリスト」（以下、調達協議資料と言います。）等を情報主管課に提出し、情報主管課及び ICT マネージャ等から技術的な助言や仕様書等の作成サポートを受けることができます。

調達協議には、当初予算要求時の IT 調達協議（以下、「要求時協議」と言います。）があります。要求時協議は財政課に予算要求を実施する際に必須であり、財政課は情報主管課の審査結果を踏まえて予算査定等を実施します。

なお、業務の再構築（BPR[8]）等を伴う大規模なシステム開発については、事務効率化推進委員会に諮り、システム開発の方針の的確性や費用対効果等についての妥当性を全庁的に検討することが必要なことに留意してください。

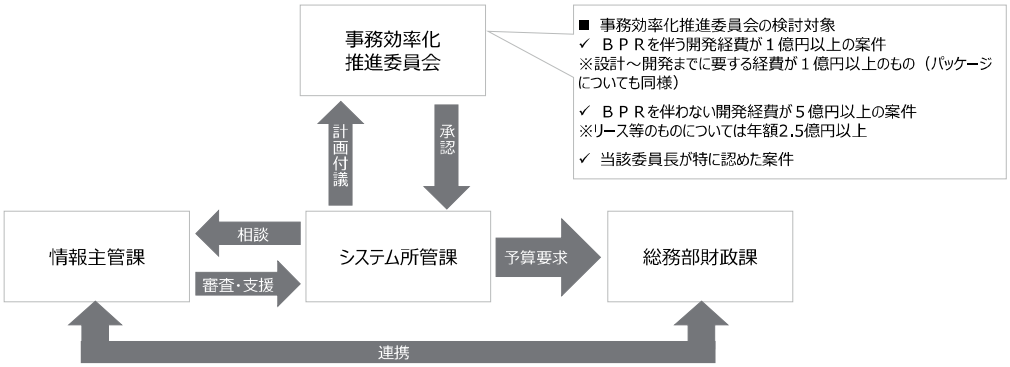


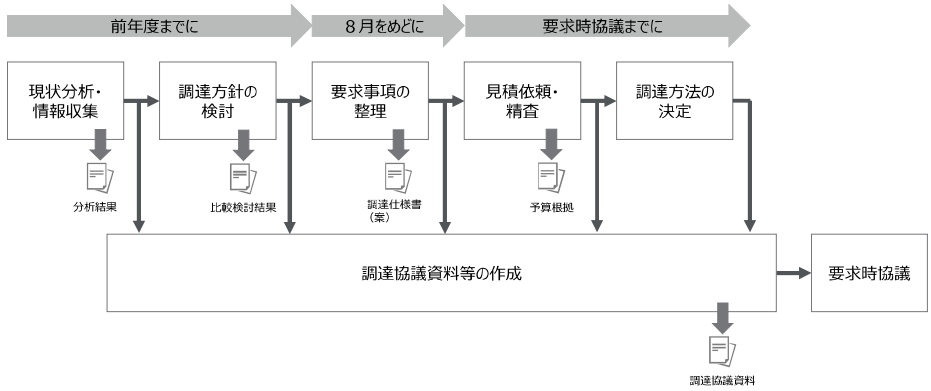
図 7 予算要求の流れ

[8] 既存の業務プロセスを詳細に分析して課題を把握し、ゼロベースで全体的な解決策を導き出すことにより、業務負担を軽減するとともに、業務処理の迅速化・正確性の向上を通じた利便性の向上を図る取組のこと。Business Process Reengineering の略。

4 企画段階における全体の流れ

(1) 企画段階の流れ

企画段階では、現状分析・情報収集等を通じて企画内容を整理し、企画内容を基に原則複数者から参考見積り等を取得します。企画段階で収集・整理した内容について「システム開発計画書」等に取りまとめ、要求時協議を行います。



既存システムの改修など随意契約が妥当と思われる場合であっても、他の都道府県などの情報（改修費等）を取得してください。
企画段階では積極的にシステム事業者や他の都道府県との情報交換を行うなど、情報収集に努めてください。

図 8 企画段階の流れ

(2) 調達協議資料等の作成

情報システムに関する予算要求にあたっては、次頁以降の作業で作成する「調達協議資料」を一式、情報主管課へ提出します。なお、当該資料の添付資料である「統一見積書」は事業者へ作成を依頼します。

情報システムに関する予算要求の流れは下図の通りです。

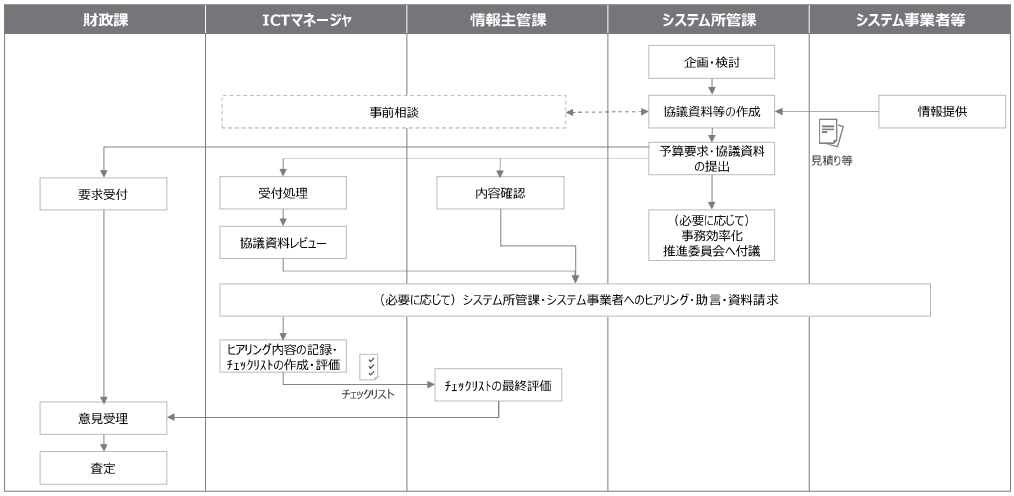


図 9 予算要求の流れ

(3) 企画段階における調達の分類ごとの作業内容

企画段階における調達の分類ごとの作業対象を下図に示します。作業内容の参考にしてください。

○：必須、△：案件次第（必要に応じて）、－：対応不要

作業工程		①新規	②更改	③改修	④運用	⑤機器	⑥再ﾘｰｽ	⑦ｺﾝｻﾙ	⑧その他
現状分析・情報収集	現状分析	○	△	－	－	－	－	－	－
	情報収集情報収集（新たなシステムや機能）	○	○	△	－	－	－	△	△
調達方針の検討	比較検討結果の作成	○	○	△	－	－	○	－	－
要求事項の整理	RFIの実施	△	△	－	－	－	－	－	－
	運用保守実績の評価	－	－	－	○	－	△	－	－
	既存事業者との協議	－	○	○	○	－	○	－	－
	調達仕様書（案）の作成	○	○	○	○	○	○	○	○
見積り依頼・精査	見積り依頼	○	○	○	○	○	○	○	○
	見積り精査	○	○	○	○	○	○	○	○
	予算根拠資料の作成	○	○	○	○	○	○	○	○
調達方法の決定		○	○	○	○	○	○	○	○
システム開発計画書等の作成		○	○	○	○	○	○	○	○
要求時協議		○	○	○	○	○	○	○	○

図 10 企画段階における調達の分類ごとの作業内容（例）

(4) 現状分析

要求事項の整理に向けて、業務プロセス及び情報システムを分析し、課題を整理します。業務プロセス及び情報システムの分析は、下図の流れで実施します。なお、②更改（機器のみの更改（ハードウェアリプレース））の場合は原則として、実施不要です。

業務を観察する

現場の業務を観察し、業務実態について、事実を詳細に把握する。事実の把握は、「平均、合計ではなくばらつきを見る」ことや「推測ではなく、現場で起こっている事実を見る」ことを意識して実施する。現場への問合せや情報システムの改善要望などを日常的に取得している場合は、その情報を活用する。

現行システムを評価する

システム導入の目的(KGI・KPI等)に対する実績の確認や、システム利用者へのアンケート等により、現行システムを評価する。評価に当たっては、アクセス数やユーザ登録数、障害発生件数、ピーク時のレスポンスタイムなど定量的な実績データを活用して分析を行い、改善点を抽出する。
※システム更改の予算要求を行う場合は、現行システムの評価を実施していることを前提とする。

業務を可視化する

業務の流れを示す業務フローの作成や業務単位での業務量調査等により、業務情報を可視化する。可視化することで、業務のどの部分に改善が必要なのかを客観的に示すことができる。

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック　第4章

図 11 現状分析のイメージ（例）

(5) 情報収集

情報収集の方法は以下を参考に実施してください。なお、企画段階では積極的に事業者と情報交換を行ってください。また、各部局内の実績や他都道府県の導入事例、「競争入札参加資格者名簿」、「IT資産総合管理データベース」等を参考に情報収集を行ってください。

ア　国等の動向の情報収集

情報システムや機能に関連する国等の動向（補助金、交付金等を含む）や社会情勢を把握してください。なお、情報収集に当たっては国等の Web サイト、iJAMP、J-LIS などの書籍なども活用してください。

イ　他団体への照会

同規模自治体・近隣自治体に、企画内容に関連する情報（取組、仕様書、費用、調達方法、広域での共同利用等）を照会してください。なお、③改修で全国一律の制度対応等であっても、ベンダ毎に対応方法やコストが異なるため原則として、実施してください。

ウ　庁内への照会

以下を例として、庁内へ照会してください。

(ア) 全庁最適化の視点から、類似案件や情報システムの有無等を調査し、類似システムについては共同利用や統合を検討してください。

(イ) 共通基盤利用、マイナンバー利用事務、外部のクラウドサービスを利用予定の場合は、早期に情報主管課に相談してください。

(ウ) 本県が保有する個人情報の外部提供を行う際は、山形県情報公開・個人情報保護審査会の対象となる場合があるため、所管部署に事前に相談してください。

エ　事業者への照会

企画内容に合致する開発実績のある事業者に対し、情報システムのデモンストレーションや製品カタログ、参考見積書の提出などを事業者に依頼し、市場に流通している同種のパッケージシステムやクラウドサービスの情報を収集します。事業者への照会に当たっては、情報の偏りを防ぐため、複数の事業者に対して照会を行ってください。

(6) 調達方針の検討

調達の分類(注)ごとに下図を例とした、企画の方向性について比較検討を行ってください。その上で、案件に応じた調達方針を決定します。

なお、案件の比較検討に当たっては、各実施方法について、費用、効果、メリット・デメリットを整理した、比較検討結果を原則、作成します。また、共同利用の検討が可能なシステムについては、実施方法の 1 つとして比較検討を実施します。

調達の分類	実施方法
①新規	新システム導入 ・ 既存システムの拡張 ・ システム化以外 （外部委託等） ・ ツール （RPA等） 等
②更改	更改 ・ 契約延長 （再リースを含む） ・ 廃止 等
③改修	システムの改修 ・ RPA等を含むツール・運用対応 等 ※制度対応など対応が必須の場合は実施不要
⑥再リース	更改 ・契約延長 （再リースを含む） ・ 廃止 等

図 12 現状分析のイメージ(例)

注）調達分類については、図 6 情報システム等の調達分類を参照してください。

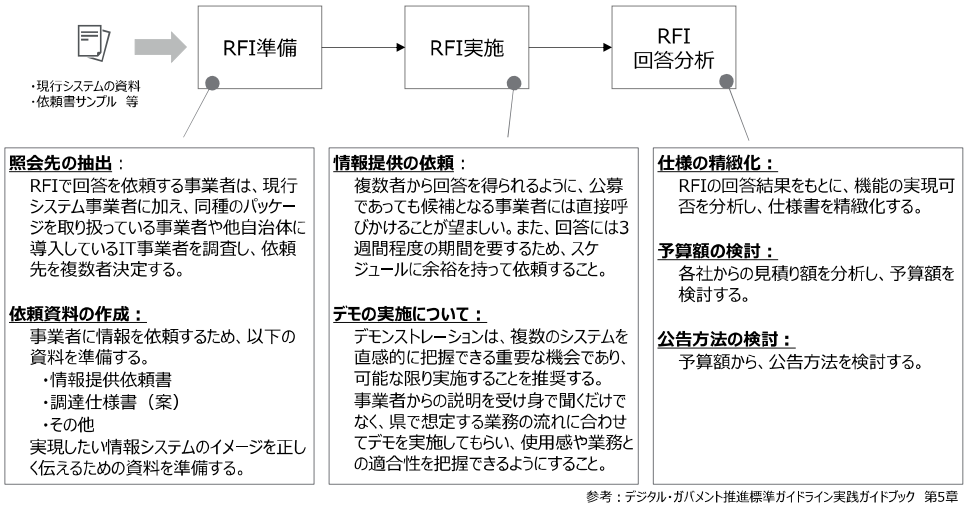
なお、情報システムの構築に際して、「山形県基幹高速通信ネットワーク」の利用を想定している場合には、「業務システム等の山形県基幹高速通信ネットワークへの接続に関する手続について（通知）（ICT第464号、令和3年1月27日）」をご参照ください。

(7) RFI の実施

RFI とは、Request For Information の略であり、入札や調達の事前準備として、事業者から情報提供を受けるために実施するものです。具体的には、想定する要求事項の実現可否や概算見積などの情報提供を受けます。RFI の照会先は可能な限り2者以上に実施してください。RFI の実施に当たっては、付録の「付録 2_情報提供依頼書(RFI)(例)」を参考にしてください。

ア RFI の進め方

下図を例とした RFI を実施し、要求事項を整理します。

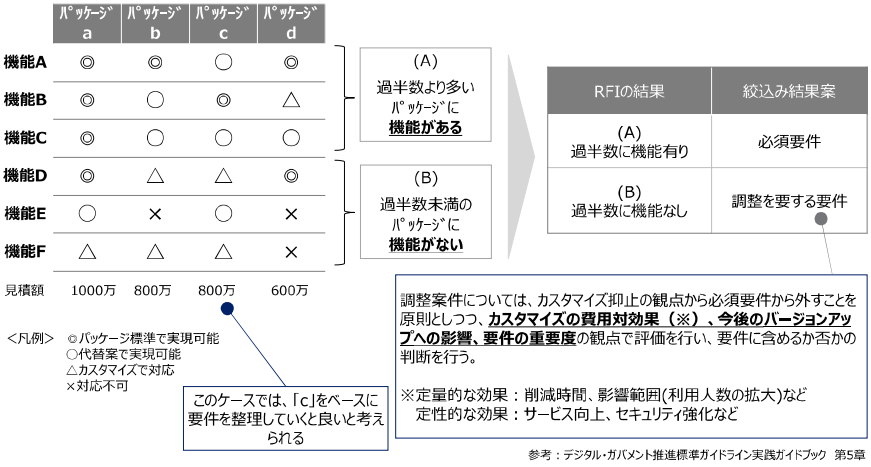


参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第5章

図 13RFI の進め方

イ RFI 結果の分析

事業者から得られた RFI 回答をもとに下図を参考とした分析を行い、仕様書の精緻化、予算額の検討、調達方法の検討を行います。



参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第5章

図 14RFI 結果の分析イメージ(例)

(8) 運用保守実績の評価

現行の保守業務の報告書等をもとに障害件数や保守工数等の各種保守業務の実績を分析し、費用や仕様に対する評価を行います。仕様と作業実績の間にギャップがある場合は、下図を例とした保守仕様や費用の見直しを行います。

なお、保守料は情報システムの安定稼働を目的としたいわゆる「固定部分」と、作業員が都度実施する「変動部分」で構成されますが、「固定部分」の見直しは、保守の品質低下を招く恐れがあるため、原則当初の契約期間中の見直しは行わないことが望ましいと考えられます。

また、「変動部分」についても、1年単位で交渉するのではなく、2～3年を例とした複数年平均で見直しを行うことが望ましいと考えられます。

項番	概要	仕様・見積	実績	見直し案
1	障害対応件数	障害対応件数として、20件/月を想定した工数が計上されている。	障害対応件数は、月平均5件であった。	仕様の想定障害対応件数及び工数（費用）の見直しを行う。
2	保守費用内の改修	保守費用内での軽微な改修として2人月の工数が計上されている。	保守範囲内の改修工数は、１人月未満であった。	想定改修工数と費用の見直しを行う。
3	サポートデスク対応	24時間365日のサポートデスク窓口が設定されている。	サポートデスク窓口の利用時間は開庁時間のみであった。	システムの重要度、障害発生時の影響度を踏まえ、サポートデスク窓口の対応時間を開庁時間内とする。

図 15 運用保守実績の評価方法（例）

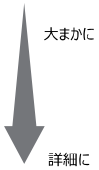
(9) 既存事業者との協議

改修案件については、業務要件を実現するための改修方法について現行事業者と協議し、調達仕様書を作成します。ただし、システムライフサイクルコストの適正化の観点から、改修方法の妥当性や将来コストの適正化を検討してください。

(10) 調達仕様書(案)の作成

収集した情報をもとに情報システムに求められる要求事項を整理し、調達仕様書(案)として取りまとめます。企画段階で調達仕様書を完成させる必要はありませんが、見積りの精度を向上させるために、必要な要件を可能な限り詳細に記載するようにします。見積り要求段階での仕様の粒度は、下図を参考としますが基本的には、「6　調達仕様書の作成」の記載に準拠した調達仕様書を作成するように努めてください。

調達の分類	記載イメージ
①新規	主要な機能の単位で記載する。詳細な実現方法等については、機能の向上やコストの低減を含めて、事業者からの提案の余地を残す。
②更改、③改修（※１）、⑦ｺﾝｻﾙ	現行システムの機能を踏襲するようなところは詳細に記載しつつ、新たに追加する機能や法改正の詳細条件が不明な場合などは、可能な範囲で記載する。
③改修（※２）、④運用、⑤機器、⑥再リース	必要となる作業が明確であるため、案ではなく最終版のレベルで作成する。



※１　制度が未確定など企画段階で要件が確定していない改修案件
※２　企画段階で要件が確定している改修案件

図 16 調達仕様書(案)の記載イメージ(例)

なお、要件等に未確定の事項がある場合には、以下に留意してください。

- ✓ 見積りを依頼する要件の中で詳細が未確定な箇所には、未確定である旨、その理由、どのタイミングで詳細化できる予定であるかを調達仕様書(案)内に記述します。
- ✓ 未確定な箇所については、できるだけ複数の対応案を示し、それぞれの対応案に対して見積り金額を把握できるよう配慮します。その上で、見積り前提が変わった際の影響範囲(見積り金額だけでなく、工期や連携先情報システムへの影響等を含めた全体的な影響)について事業者に確認します。
- ✓ 未確定な箇所を機能別に一覧にまとめ、巻末等に記載します。

(11) 見積書の依頼

要求事項の整理後、予算要求に向けて下図の点を考慮しながら事業者に見積りを依頼します。特に大規模な情報システムに関する見積り依頼にあたっては、発注者の意図を事業者に正しく伝えるための説明会の開催や見積根拠を把握するためのヒアリングなど、積極的にコミュニケーションを図ることが求められます。

考慮ポイント	詳細
要件が未確定な部分を明確にする。	要件に未確定な部分が残っている場合は、対象箇所を明確にする。 なお、要件が明確になったうえで再度見積りを取得し、精緻化を図ること。
複数者から見積を取得する。	見積の精度を高めるとともに入札の不調のリスクを低減するため、既存システムの改修や再リースなど、特定の事業者にしか実施できない場合を除き、可能な限り複数者から見積を取得する。
初期費用だけでなく、 ランニング費用についても取得する。	情報システムにかかる費用については、初年度の開発費用だけでなく、次年度以降にも発生する費用（ライセンス費用、保守費用等）についても取得する。
見積の内訳を明確にする。	情報システムには様々な見積手法が存在し、事業者ごとに考え方が異なる。見積手法そのものを指定することは、事業者の負担を増加させ、協力が得られない恐れがあるため避けるべきだが、機能や作業単位ごとの工数、単価、リースの場合は賃貸借料と保守料の内訳、見積根拠を明記するように依頼する。
見積フォーマットを指定する。	フォーマットの指定は、複数事業者の見積を同じレベルで比較する場合や項目の抜け漏れの抑止に有効である。 見積り依頼時は、原則本県で準備している見積フォーマットを活用する。
現行システム移行費用を取得する。	データ移行が発生する場合は、既存事業者に対してデータ抽出の見積を依頼すること。なお、現行契約にデータ抽出の要件が含まれている場合は不要である。
撤去費用を確認する。	既存の機器がある場合は、機器の撤去費用や原状回復費用、データ消去費用について見積りに含めること。なお、現行契約に含まれている場合は、見積もりは不要である。
連携先の費用を確認する。	他システムとの連携がある場合は、連携先の情報システム側にも費用(システム改修、連携テスト等)が発生しないか確認すること。
ライセンス等の更新費用を確認する。	サポートサービス提供期限が運用期間内に終了する製品(ソフトウェア等)が含まれる場合は、更新費用についても確認すること。

図 17 見積り取得時の主な確認事項(例)

(12) 見積書の精査

見積書の精査に当たっては、見積チェックリストの回答を踏まえ、下図のような点を確認します。

チェック項目	概要
ハードウェア・ソフトウェア費用	ハードウェア・ソフトウェアの選定理由や、リースの場合はリース料率、再リース価格の根拠が明確になっているか確認する。
人件費 (アプリケーション構築・改修費用)	必要な機能が漏れていないか、必要のない改修や優先度の低い改修が含まれていないか、成果品は十分か、要件が不明瞭な箇所は明確になっているかを確認する。また、類似案件（毎年実施される定例的な制度対応等）がある場合は、類似案件と比較して調達金額に乖離がないか確認する。
運用保守費用	想定している保守条件となっているか、2年目以降の場合は過去の保守実績を反映した費用になっているか等を確認する。
その他	見積書の前提条件を確認する。また、他社と比べて金額が極端に乖離した見積がある場合は、ヒアリング等により原因の確認（※）を行う。 ※一社のみが仕様を詳細に理解し精度の高い見積を作成することにより、結果として金額が高くなっている等が考えられるため、逸脱している見積が正しくないとは限らない。そのため、ヒアリングでの原因確認が必要となる。

図 18 見積り精査の主な観点(例)

なお、見積の精査は、単に見積金額を低減させられればいいというものではないという点に留意してください。発注者が見積の内容を十分に理解し、前提条件や取りうる選択肢を把握した上で、実現させたい機能と価格のバランスをとることが重要になります。

精査の前提として、明確な仕様による精度の高い見積りが必要であるが、金額の妥当性については、当該情報システムに最も精通しているシステム所管課の協力も欠かせないものであり、対応内容とコストの比較や当該情報システムの過去の改修実績との比較などをシステム所管課の視点で実施することが有効であると考えられます。

(13) 予算要求用資料の作成

複数者の見積り結果や現行の費用を踏まえ、予算要求額を決定します。予算要求額の決定に当たっては、予算根拠資料を作成してください。

事業者名	A者	B者	C者	D者	現行
■初期費用計	**3,000,000**	**2,500,000**	**4,500,000**	**5,000,000**	**3,500,000**
ハードウェア関連費	2,000,000	1,600,000	2,000,000	2,500,000	1,500,000
ソフトウエア関連費	500,000	500,000	1,000,000	1,500,000	1,300,000
導入作業	500,000	400,000	1,500,000	1,000,000	700,000
■経常費用計	**100,000**	**120,000**	**80,000**	**120,000**	**80,000**
ハードウェア保守費	30,000	40,000	25,000	35,000	20,000
ソフトウエア保守費	30,000	60,000	45,000	45,000	15,000
運用費	40,000	20,000	10,000	40,000	45,000
■総合計	**9,000,000**	**9,700,000**	**9,300,000**	**12,200,000**	**8,300,000**
特徴	・拠点は仙台である。 ・他県にて類似内容の開発実績あり。	・拠点は東京のみあり、基本的にはリモート保守ある。 ・類似の開発実績はなし。	・拠点は山形市内である。 ・類似の開発実績はなし。	・拠点は山形市内である。 ・他県にて類似内容の開発実績あり。	・拠点は山形市内である。 ・他県にて類似内容の開発実績あり。

要求予算額：	9,300,000

根拠：	回答のあった４者から費用の低い３者を抽出し、３者の平均額と３者の中間の費用のうち費用の低い者を採用した。

図 19 予算要求額の決定(例)

予算要求額の決定方法は、複数事業者から収集した見積りの中での最低額を予算額とする考え方が一般的ですが、プロポーザル方式等で価格以外の要素を評価する必要がある場合、最高額と最低額を除外した平均値を取得する方法(3 点見積り)などの方法も一案です。

(14) システム方式の検討

システムの構築方法としては、クラウドサービスの利用とオンプレミス[9]に大別されます。情報システム導入における基本原則に則り、クラウドサービスの利用や共同利用を第1とし、クラウドサービスの活用が難しい場合は、オンプレミスを検討します。

導入方法	クラウドサービス	オンプレミス（自己所有）
概要	情報システムの一部、またはすべてについて、事業者の提供する**サービスを利用**する方法	情報システムをすべて自庁で**保有**（リース含む）する方法
設置場所	データセンター	自庁・データセンター
事業者によるサービス提供の範囲	IaaS / PaaS / SaaS（ASP） アプリケーション / データ / ミドルウェア（DB等） / OS / ハードウェア	単独導入 アプリケーション / データ / ミドルウェア（DB等） / OS / ハードウェア

自己所有　事業者によるサービス提供

図 20 オンプレミスとクラウドサービスの違い

(15) 外部サービス利用時における留意点

システム所管課においては、クラウドサービス等の外部サービスを利用する場合には、「外部サービスの利用（機密性2以上の情報を取り扱う場合）に関する実施手順」及び「外部サービスの利用（機密性2以上の情報を取り扱わない場合）に関する実施手順」を遵守して導入・運用してください。

[9] オンプレミスとは、情報システムの設置形態の分類で、庁内やデータセンターに機器を設置して情報システムを導入・運用すること。クラウドサービスの対義語である。

(16) 調達単位の検討

情報システムの調達にあたっては、履行可能性、ライフサイクルコスト、技術的妥当性、複数の関連調達間の整合性・効率性等[10]を考慮の上、競争性が確保されコストが低減されるよう合理的な調達単位[11]を検討することが重要です。

情報システムに係る調達においては、一括発注や過度な又は不適切な調達単位の組み合わせに起因するいわゆるベンダーロックインや過度な分割調達による作業の増加や重複によるコストの増加を防ぎ、かつ、競争性・透明性を確保することで、プロジェクトの目的・目標の達成に向けて、より効果的・効率的な提案を受けられるよう、調達の単位を検討する必要があります。また、調達単位を適切に保つことは、調達の競争性を高め、より良い提案を受ける可能性を高めることにつながります。

一方で、調達単位を分割しすぎることで、発注者側の調達に係る負担や事業者の管理・調整に係る負荷が増大することから、プロジェクトの実効性が損なわれないよう留意する必要もあります。

このため、情報システムの調達における計画段階で、プロジェクトのライフサイクルを通したコストの低減、各活動の効率的・効果的な履行、プロジェクトの目的・目標の確実な実現等の観点を基に、当該プロジェクトにとって合理的な調達単位を検討し、要件定義等による調達内容の具体化・詳細化と合わせて、調達単位を決定する必要があります。

なお、合理的な調達単位の検討に当たっては、過去の事例や他の自治体の事例及び専門的な知識を有する外部人材から助言を受けることも一案です。

調達の単位の検討にあたっては、図 21～図 23も参考にしてください。

---

10 「複数の関連調達間の整合性・効率性」とは、当該調達に関連する他の調達との間に、調達対象となる作業や物品の漏れや重複がなく整合が取れており、調達を分割することで全体のコスト削減や事務処理の軽減に繋がることを指します。調達を分割することで、整合性や効率性が低下するのであれば、まとめて調達することも検討する必要があります。

11 「合理的な調達単位」とは、次の図 21 に掲げる調達単位を基本し、プロジェクトの規模や技術的要素、実施体制や予算等を踏まえ、競争性及び透明性を確保した上で、基本となる調達単位を組み合わせ、又は調達単位を工程や機能単位等に分割し、当該プロジェクトにとって最適であると合理的かつ客観的に判断できる調達単位を指します。

項番	基本となる調達単位
1	調査研究又は要件定義作成支援
2	プロジェクト管理支援
3	設計・開発（設計・開発の内容が細分化できる場合であっても、必ずしも調達単位を分割する必要はない。）
4	クラウドサービス利用
5	ハードウェアの賃貸借又は買取り
6	ソフトウェア製品の賃貸借又は買取り
7	回線
8	アプリケーションプログラムの保守
9	ハードウェアの保守
10	ソフトウェア製品の保守
11	運用
12	運用サポート業務
13	業務運用支援
14	施設の賃貸借
15	施設の整備等
16	システム監査（情報セキュリティ監査を含む。）

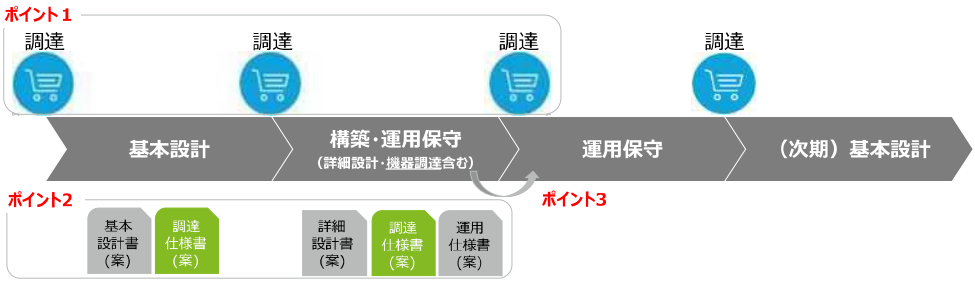
出典：「デジタル・ガバメント推進標準ガイドライン　解説書（第３編第６章　調達）」

図 21 調達単位(例)

なお、調達単位の検討に当たっては、調達の透明性・公正性の確保及び相互牽制、監査の独立性及び客観性の確保の観点等から、入札制限等も踏まえて、検討する必要があります。

また、調達単位の計画はプロジェクトの全体像との関連を明確に示すことで、第三者がその内容を確認・把握できるようにするとともに、本県の情報システムの調達事例として活用できるようにすることも重要です。

分離調達においては、発注者が複数の事業者間の調整を実施する責任があることに留意する必要があります。



ポイント1

- 調達が分割されており、スケジュールの制約の中で調達事務に係る負荷が高い状況にある。
- 前フェーズが確定しない状態で、次フェーズの予算要求を行うことになり、過度にリスクを見込んだ見積りとなる可能性が高まる。

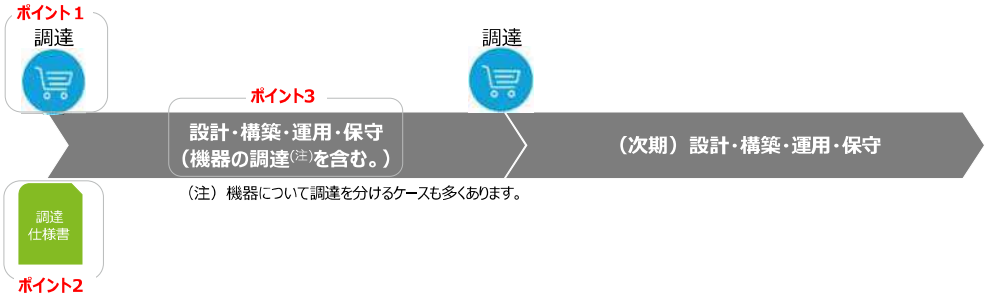
ポイント2

- 前フェーズで調達仕様書案などの作成が役務になっており、次フェーズに対する独立性が十分ではない。

ポイント3

- 運用保守工程の引継ぎが難しい。（前工程と同一事業者でないと、安定的な運用保守が難しい。）

図 22 分離調達の例



ポイント1

- 調達は１回を基本とし、調達事務に係る負荷を軽減する。
- 事業者は当初から設計・構築・運用・保守を一貫して行うことを想定できるため、別事業者が設計したシステムに基づき、構築・運用・保守を行うリスクを排除できるため、見積りの精度が高まる。

ポイント2

- 調達仕様書は県職員が作成するか、コンサルティング事業者に委託し、後工程との独立性を確保する。

ポイント3

- 構築と運用保守を同一事業者にすることで運用保守の安定化を図る。

図 23 一括調達の例

(17) 買取・リース・サービス利用

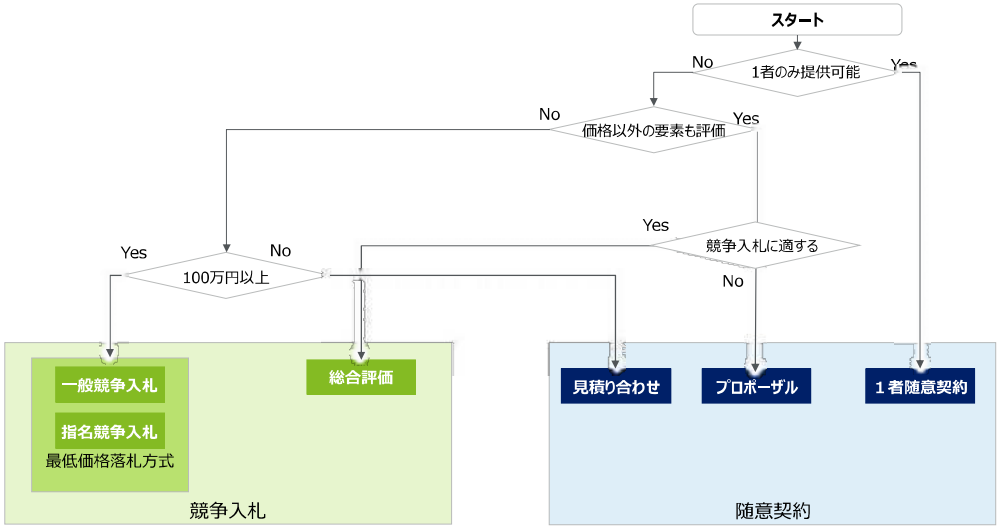
情報システムの調達方法としては、買取・リース・サービス利用に大別できます。それぞれのメリット及びデメリットは下図のとおりです。利用期間や調達するシステムの特性を考慮し、選択してください。

調達形態	買取	リース	サービス利用
定義	機器等を購入すること。	期間を定め、システム事業者から機器等を借り受けること。	事業者のサービス（クラウド、回線利用料）の提供を受けること。
メリット	長期利用の場合、リースより割安となる場合が多い。	初期費用が抑えられる。経費計上が可能である。	構築期間の短縮を図ることが可能。 契約や約款等において、サービスレベルを明示できる場合が多い。
デメリット	初期費用が高い。また、廃棄費用が生じる。所属によっては、固定資産税が別途必要となる場合がある。	中途解約は原則不可である。 修理費用は負担する必要がある。	カスタマイズが困難である。 長期利用の場合、割高になる可能性がある。

図 24 情報システムの調達方法の比較

(18) 調達方式の検討

情報システムの調達については、下図を参考に調達方式を検討してください。



出典：「業務委託における総合評価一般競争入札実施要領」

図 25 調達方式の検討(例)

	一般競争入札		随意契約	
	最低価格落札方式	総合評価方式	随意契約	プロポーザル方式（随意契約の一種）
メリット	• 価格という分かりやすい指標で落札者が決定するため、公平性が確保されやすい。 • 応札者が作成する書類が少ないため、一般的に応札者が多くなると考えられ、競争性が確保しやすい。 • 入札関係書類が他の調達方式に比べて少なく、事務手続きの負担が少ない。	• 価格に加えて、技術（提案）面を含めて評価する。 • 情報システムの要件について、各事業者の提案内容を比較することができる。 • 必須でない要件について、契約額とのバランスを考慮して、実装するかどうか提案を受けることができる。 • 事業者の意欲、品質管理、実績等を総合的に評価することができる。 • 実績や経験がある事業者を評価することができる。	• 緊急の調達が必要な場合等で、短期間で調達できる。	• 一般的に価格よりも技術（提案）に重きを置いて評価する。 • 情報システムの要件について、各事業者の提案内容を比較することができる。 • 必須でない要件について、契約額とのバランスを考慮して、実装するかどうか提案を受けることができる。 • 事業者の意欲、品質管理、実績等を総合的に評価することができる。 • 実績や経験がある事業者を評価することができる。 • 評価後、優先交渉を決定し、随意契約として、柔軟に契約を進めることができる。
デメリット	• 情報システムの要件について、事前に調査し、精緻な仕様書を作成する必要がある。 • 調達仕様書以上の提案を求められないため、必要な機能を網羅する必要がある。 • 価格のみで決定するため、仕様書が不十分な場合、低品質の情報システムが納入されるおそれがある。	• 評価基準作成・審査に時間を要する。 • 提案書の作成で事業者に負担が生じるため、入札参加者が少なくなりやすい。 • 提案書の作成に慣れた事業者が有利。 • 調達事務が煩雑となる。	• 以下の場合に限定される ✓ 少額の契約（100万円以下） ✓ その性質又は目的が競争入札に適しない契約 ✓ 特定の施設等から物品を買入れ又は役務の提供を受ける契約 ✓ 新規事業分野の開拓事業者からの新商品の買入契約 ✓ 緊急の必要によるもの ✓ 競争入札に付することが不利なもの ✓ 時価に比して著しく有利な価格で契約ができるもの ✓ 競争入札に付し入札者又は落札者がない ✓ 落札者が契約を締結しないとき	• 評価基準作成・審査に時間を要する。 • 提案書の作成で事業者に負担が生じるため、入札参加者が少なくなりやすい。 • 提案書の作成になれた事業者が有利。 • 調達事務が煩雑となる

図 26 調達方式のメリット及びデメリット（例）

一般競争入札 （最低価格落札方式）	一般競争入札 （総合評価方式）	随意契約	随意契約 プロポーザル方式
• 機器や機能の固定したソフトウェアの調達等、仕様どおりの物品の納入を求める場合 • 機能や運用の仕様が定まっており、機能・品質上の評価や提案の必要性がない場合 • 緊急に調達の必要性がある場合	• 価格に加えて、技術（提案）を評価することが適当である場合 • 実現方法が複数想定される状況下にあり、実現方式によりメリット、デメリットの比較（評価）が必要な場合（クライアントサーバ方式、Ｗｅｂ方式、クラウド方式等） • 実現可能性や費用対効果を踏まえた上で、必須ではない機能（任意機能）がある場合 • 機能の実現方法、保守・運用方法、品質管理方法について提案を求める場合 • 新技術のため委託業者の開発実績を考慮する必要がある場合	• 少額の契約 • 改修等で、特定の事業者のみが対応可能で、競争入札に適しない契約 • 緊急の調達が必要であるもの • 競争入札に付することが不利なもの（例：競争入札に付した場合の方が、入札価格が上昇することが見込まれる場合等） • 時価に比して著しく有利な価格で契約ができるもの • 競争入札に付し入札者又は落札者がない場合 • 落札者が契約を締結しないとき	• 価格よりも技術（提案）に重きを置いて評価する必要がある場合 • 実現方法が複数想定される状況下にあり、実現方式によりメリット、デメリットの比較（評価）が必要な場合（クライアントサーバ方式、Ｗｅｂ方式、クラウド方式等） • 実現可能性や費用対効果を踏まえた上で、必須ではない機能（任意機能）がある場合 • 機能の実現方法、保守・運用方法、品質管理方法について提案を求める場合 • 新技術のため委託業者の開発実績を考慮する必要がある場合

図 27 調達方式に応じた案件（例）

(19) 随意契約について

随意契約とは、競争入札によらずに任意で決定した相手と契約を締結すること、及び締結した契約です。随意契約の場合、下図の地方自治法や山形県財務規則に則った運用が求められることに留意してください。

号	内容
第1号	売買、賃借、請負その他の契約でその予定価格（本県の場合、100万円以下）が別表第5に定める額の範囲内において普通地方公共団体の規則で定める額を超えないものをするとき。
第2号	不動産の買入れ又は借入れ、普通地方公共団体が必要とする物品の製造、修理、加工又は納入に使用させるため必要な物品の売払いその他の契約でその性質又は目的が競争入札に適しないものをするとき。
第3号	障がい者支援施設等で製作された物品を買い入れる契約、シルバー人材センター、母子・父子福祉団体等から役務の提供を受ける契約をするとき。
第4号	新商品の生産により新たな事業分野の開拓を図るものとして知事の認定を受けた者が生産する物品を買い入れる契約をするとき。
第5号	緊急の必要により競争入札に付することができないとき。
第6号	競争入札に付することが不利と認められるとき。
第7号	時価に比して著しく有利な価格で契約を締結することができる見込みのあるとき。
第8号	競争入札に付し入札者がないとき、又は再度の入札に付し落札者がないとき。
第9号	落札者が契約を締結しないとき。

図 28 地方自治法施行令第 167 条の 2 第 1 項にて定める随契理由

5 調達段階における全体の流れ

(1) 調達段階の流れ

調達段階では、企画段階で準備した資料をもとに、調達に必要な資料を作成します。その後、公告から契約までを執り行います。

調達仕様書の作成については、「6 調達仕様書の作成」をご参照ください。

また、調達関連資料の作成については「7 調達仕様書作成後の流れ」、「調達関連資料の作成」をご参照ください。

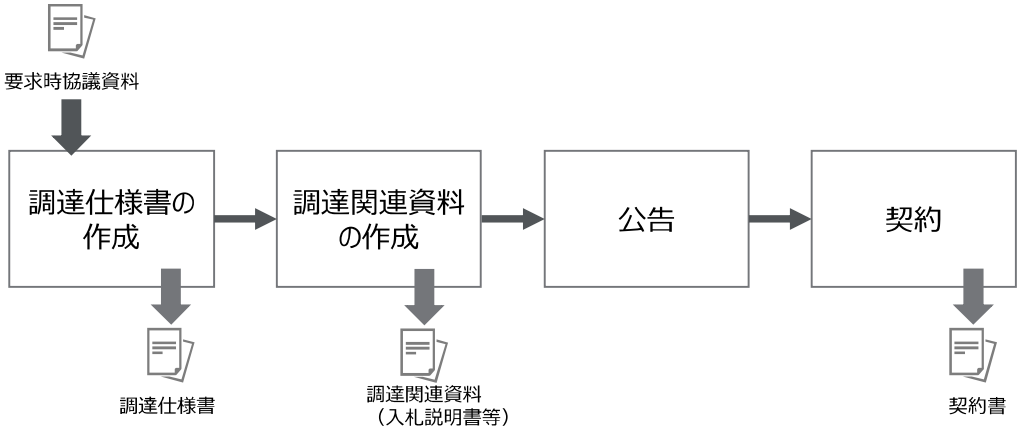


図 29 調達段階の流れ

6 調達仕様書の作成

(1) 調達仕様書の構成

調達仕様書は機能要件や帳票要件、非機能要件といった情報システムに必要な機能を定義するドキュメントです。調達仕様書の主な構成と目次案は下図の通りです。あわせて付録の付録1の「付録調達仕様書(例)」をご参照ください。

なお、外部サービス(クラウドサービス等)により情報システムを導入する場合には、外部サービスの利用(機密性2以上の情報を取り扱う場合)に関する実施手順及び外部サービスの利用(機密性2以上の情報を取り扱わない場合)に関する実施手順を遵守してください。

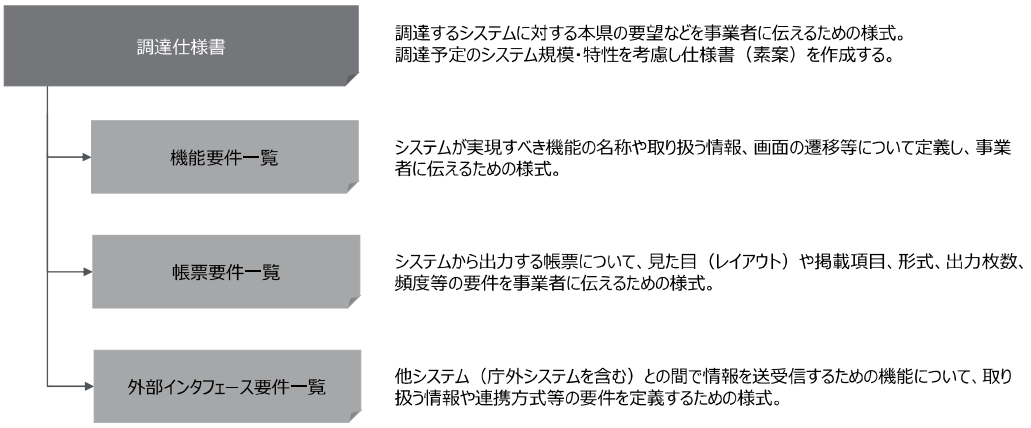


図 30 調達仕様書の構成(例)

目次項目	記載項目（例）
1．概要	✓ 調達件名 ✓ 調達の背景、目的及び期待する効果 ✓ 業務・情報システムの概要 ✓ 契約期間 ✓ 作業スケジュール ✓ 補足
2．前提条件	✓ 構築条件
3．作業内容	✓ 作業の内容
4．１機能要件 4．２非機能要件	✓ 機能要件 ✓ 非機能要件
5．成果品	✓ 成果品の範囲、納品期日等 ✓ 成果品の納入場所 ✓ 成果品の検収
6．プロジェクト管理	✓ プロジェクト管理
7．作業の実施に当たっての遵守事項	✓ 秘密保持等
8．再委託に関する事項	✓ 再委託の承認手順等
9．その他特記事項	✓ その他特記事項

図 31 調達仕様書の目次(例)

(2) 調達の分類ごとの記載事項

調達仕様書の各要件項目に対する調達の分類ごとの記載要否は下図のとおりです。各項目の記載内容については、下図以降を参照してください。

○：必須、△：案件次第、－：不要

調達仕様書の目次	①新規	②-1 ｼｽﾃﾑ更改	②-2 機器更改	③改修	④運用	⑤機器	⑥再ﾘｰｽ	⑦ｺﾝｻﾙ	⑧その他
1 調達案件の概要	○	○	○	○	○	○	○	○	○
2 前提条件	△	△	△	△	△	△	△	△	△
3 作業内容	○	○	○	○	○	○	○	○	○
4 機能要件	○	○	－	○	－	－	－	－	△
5 非機能要件	○	○	○	△	－	△	○	－	△
6 SLA	○	○	○	△	△	○	△	△	△
7 情報システムの稼働環境	○	○	○	△	－	○	○	－	△
8 テスト要件	○	○	○	○	－	－	－	－	△
9 移行要件	△	○	○	△	－	－	－	－	△
１０ 教育・研修要件	○	△	△	△	△	－	－	－	△
１１ 運用・保守要件	○	○	○	△	○	○	○	－	△
１２ 成果品	○	○	○	○	○	○	○	○	△
１３ プロジェクト管理	○	○	○	○	○	○	○	○	△
１４ 留意事項	○	○	○	○	○	○	○	○	△

※「１４ 留意事項」には「付録1_調達仕様書（例）」の「第７ 作業の実施に当たっての遵守事項」、「第８ 再委託に関する事項」及び「第９ その他特記事項」を含みます。

図 32 調達の分類ごとの調達仕様書記載事項（例）

(3) 調達案件の概要

調達情報システムについての背景、委託期間といった概要を記載します。詳細は「付録 1_調達仕様書（例）」をご参照ください。

(4) 機能要件

業務要件を満たすために情報システムの機能として求められる要件を定義します。機能要件としては、機能、画面、帳票、情報・データ、外部インタフェースの5つを定義します。また、システム評価に向けて、アクセス数やレスポンスタイム等のデータ出力機能を要件として設定しておくことも重要です。情報システムの種類毎に必要な要件は異なる点に留意してください。

機能要件の項目	概要	記載箇所
1　機能要件	機能とは情報システムが外部に価値を提供する一連の動作のまとまりのことであり、「入力」「演算（処理）」「出力」で構成される。ボタン操作による画面の動きやバッチ処理による印刷なども一つの機能である。	調達仕様書、機能要件一覧
2　画面要件	画面上で取り扱う情報の種類、画面を構成する要素の配置を指す。事業者の作業規模の見積や、具体的なレイアウト・画面遷移を設計するにあたって必要な情報であり、詳細部分まで決定する必要はない。	調達仕様書
3　帳票要件	業務で使用する為に情報システムから出力した紙やPDF形式等の電子帳票である。帳票を生成する方式（カーボンコピー用紙を使用する等）や出力先も要件に取り入れる。	調達仕様書、帳票要件一覧
4　情報・データ要件	情報・データを一覧化し、処理の形式や内容、データ構造に関する情報を明確にする。異なる画面や帳票でも、同じ情報を表示することがあるため、重複をなくして管理する情報・データを明確にする必要がある。	調達仕様書
5　外部インタフェース要件	情報システムが、他の情報システムと連携して情報を受け渡すために、連携内容や形式、仕組みを明確に定義する。連携先の情報システムの都合もあるため、双方の要件をすり合わせる必要がある。	調達仕様書、 外部インタフェース要件一覧

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック　第５章　Step.5

図　33 機能要件（例）

(5)　非機能要件

情報システムの開発に際して定義される要件のうち、機能面以外のものを指し、性能や信頼性、拡張性、セキュリティなどに関する要件を定義します。改修や運用など既に存在する場合は定義不要ですが、新規等の場合は基本的に全ての項目を定義してください。

非機能要件の項目	概要	記載内容（例）
1　ユーザビリティ アクセシビリティ	利用者がミスなく効率的に行うための必要事項、目的の情報への辿り着きやすさを示す。	十分な視認性のあるフォント及び文字サイズを用いること
2　規模	ユーザの数や取り扱う情報量を指す。機器やデータ等の量について整理し、想定可能な最大値を要件として示す。	利用者：最大100人、常時80人 利用時間帯：平日8時～18時
3　性能	応答性能やスループット（処理性能）等の、情報システムの能力について、費用と性能のバランスをとって定義する。	レスポンスタイム：定常時1秒以内、ピーク時3秒以内、応答時間達成率
4　信頼性	可用性と完全性について示す。情報システムが持つ故障への耐性の度合いや、機器の破損への対策やログの取得等について示す。	平均故障間隔、平均修復時間
5　拡張性	利用者やデータ量の増加に備えて、情報システムの処理性能を維持するための対処方針を要件として定量的に示す。	仮想サーバやストレージ等のリソースについて、柔軟な増減が可能であること
6　上位互換性	OSやソフトウェアのバージョンアップがあったときに、古いバージョンの製品が利用できることを示す。	必要な調査及び作業を実施し、実行環境のバージョンアップに対応可能な情報システムとすること
7　中立性	将来的に他の製品への乗り換えが困難にならないよう、中立性の観点から問題がないことを示す。	特定の事業者や製品に依存することなく、他者に引き継ぐことが可能なシステム構成であること
8　継続性	災害時における復旧目標時間やデータのバックアップ、冗長性等について記載する。	稼働率、目標復旧時点、目標復旧時間
9　情報セキュリティ	情報システムが満たすべきセキュリティの要件を記載する。認証、ログ、暗号化、不正プログラム対策等。	アクセスログの取得、通信の暗号化、不正プログラム対策

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック　第５章　Step.6

図　34 非機能要件（例）

(6)　SLA

SLA（サービスレベルアグリーメント）とは、事業者と発注者が契約を締結するにあたり、サービス内容及びサービス品質についての基準を明文化したものです。下表を参考にSLAを設定することが望ましいと考えられます。なお、設定した SLA 項目については、以下の3つのいずれかの方法で締結します。これらの中でも、自治体の情報システムについては、仕様書にお

いて定めることが一般的です。仕様書において SLA を定める場合、非機能要件や運用・保守要件を中心に、設定した目標値を定めることとなります。

- 契約書の条文に SLA 項目を記載し、締結する方法
- 仕様書において定め、契約書と一体で締結する方法
- 契約書とは別に、覚書を締結する方法

項目		概要	記載例
サービス品質	サービス稼働率	サービス稼働保証時間において、稼働予定時間に対して実際に稼働した時間(稼働時間)の割合	・ 稼働率は99.9%とする。 ・ 運用時間は原則、開庁日の開庁時間（8:30～17:15）とする。
システム性能	基準応答時間達成率	システムの応答時間を計測し、そのうち基準応答時間内に応答できた割合	・ 基準応答時間達成率は95.0%以上とすること。
システムの運用保守	障害受付時間	障害発生報告を受理するまでの時間	・ システムに障害が発生した場合、電話、メール等による対応を行ない受付時間については、開庁日の開庁時間（8:30～17:15）までとする。
	目標復旧時間	障害発生の報告を受けてから、障害対応完了までの時間	・ 保守要員を発注者の要請後、概ね6時間以内に現場に派遣し、6時間以内に保守作業を行うこと。
セキュリティ	セキュリティ監視	システムの脆弱性（不正アクセス、ウイルス感染 など）を検知してから、状況を報告、対応を実施するまでの時間	・ システム等の脆弱性を発見した場合は、1日以内に報告し、その対策を報告日から１週間以内に提案すること。
	OS等のパッチ適用、パターンファイル更新	OSのセキュリティパッチやウイルス対策ソフトのパターンファイルが公開されてから適用までの時間	・ OS等のパッチがリリースされた場合、サーバについてはリリースされた日から１日以内に適用すること。ウイルス対策ソフトのパターンファイルは、ベンダーリリースから1日以内に適用すること。

参考：公共IT におけるアウトソーシングに関するガイドライン(総務省)
地方公共団体におけるASP･SaaS導入活用ガイドライン(総務省)

図 35 SLA の例

また、上記の他、基準を満たすことができなかった場合の対応策についても以下を参考に明文化してください。

- サービスレベルが未達成の場合、その状況に応じて、受託者の負担でリソースの増強など具体的な対策を本県と協議の上、実施すること。
- 受託者は、上記のサービスレベルの結果対応を本県から求められた場合、速やかに業務への影響や緊急性を考慮し、暫定的、中長期的に必要な措置を講じなければならない。

(7) 情報システムの稼働環境

調達仕様書に情報システムの稼働環境を示す必要があります。具体的には、情報システムに係るサーバ要件、端末要件、ネットワーク要件等を指します。情報システム稼働環境における、構成要素の内容を下図に示します。

稼働環境に係る要件	概要	記載例	
サーバ要件	サーバについて、クラウド、共通基盤、オンプレミスのいづれかを選択することを示す	クラウドサービスを利用する場合	• クラウドサービスの利用を前提とする。
		共通基盤を利用する場合	• 別途、情報主管課に確認すること。
		オンプレミスを利用する場合	• サーバの設置場所は、XXXとする。
端末要件	ユーザが使用する端末に必要な機能、スペック、ソフトウェア等を示す	• 利用目的を満たすことのできる機器を選定すること。	
ネットワーク要件	冗長構成の有無、暗号化の有無、通信回線装置におけるアクセス制御の設定有無等、ネットワークに関する要件を示す	• ネットワーク帯域：XX • 冗長構成：有/無 • 通信回線装置におけるアクセス制御の設定：有/ 無 • 暗号化：有/無 • 通信プロトコル XX	

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第５章 Step.6

図 36 情報システムの稼働環境の例

(8) テスト要件

情報システムの品質を確保するために必要なテストの種類や目的、方法、実施内容、範囲、報告書等の要件を記載します。受入テストは、システム所管課側のテストであるため、事業者の支援内容について記載します。テストの実施に当たっては、テスト計画書を作成し、実施期限や役割分担を明確にした上で実施してください。

テスト要件の項目	概要	記載例	本県の役割（例）
1 単体テスト	アプリケーションを構成する最小の単位で実施するテストであり、設計通りに動作するかを事業者が機能単位で確認する。	開発環境にて、テスト用に作成したデータを使用する。	事業者において当該テストを実施していることを確認する。
2 結合テスト	複数の機能を連結させて動作を確認するテストであり、業務毎に設計通りに動作するかを事業者が確認する。	検証環境にて、テスト用に作成したデータを使用する。	事業者において当該テストを実施していることを確認する。
3 総合テスト（システムテスト）	システム全体が設計通りに動作することを確認するテストであり、業務を組み合わせたフローに沿って業務が行えることを機能面や非機能面の観点から事業者が確認する。	検証環境にて、テスト用に作成したデータ、または本番データから作成した疑似データを使用する。	• データ作成支援 • シナリオ作成支援
4 受入テスト（ユーザテスト）	納品されるシステムが要件通りに動作することを確認するテストであり、一連の業務が滞りなく行えることを所管課が確認する。事業者と協力して進める。	検証環境または本番環境にて、本番データまたは本番データから作成した疑似データを使用する。	• データ作成 • シナリオ作成 • テスト実施

図 37 各テストの概要

(9) 移行要件

情報システムの移行には、データ移行、システム移行及び業務運用移行の3つの要素があります。大規模な情報システムにおいては、段階的に移行を行うこともありますが、中小規模の情報システムにおいては、情報システムが利用されていない夜間や休日にすべての移行を実施する場合もあります。移行にあたっては、現行システム事業者と協議し、移行に係る作業範囲を明確化しておくことや、業務に支障がないように移行計画を立て、コンティンジェンシープラン（予期せぬ事態に備えて予め定めておく緊急時対応計画）を策定しておくことも望まれます。

移行要件の項目	概要	記載例
1 データ移行	現行システムから新システムへ移行するデータの量や、種類、期間等の情報を示す。	xx月xx日業務終了後時点のデータを移行する。 移行データは法定の過去5年分とする。 移行対象データは、マスタ・トランザクション・月次締めデータとする。（※1）
2 システム移行	システムの切り替え方法やタイミング、他社との連携がある場合の切り替え方法について示す。	本稼働はxx月xx日とする。 旧システムは参照のみ可能とする。
3 業務運用移行	業務フローが新しくなる場合、どのような手順で新フローに切り替えるかを示す。	xx月xx日から1か月は試行運用期間とし、xx月xx日から1か月間を並行稼働期間とする。

<データ移行内容記載例（※1）>

NO	移行元	移行対象データ	件数	提供方法
1	○○システム	○○テーブル	XX	CSV形式
2	○○システム	○○届出ファイル	XX	CSV形式
3	○○システム	○○申請情報	XX	CSV形式

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第５章 Step.6

図 38 移行要件の例

ア データ移行

参考として、データ移行における現行事業者と次期システム事業者の作業範囲や作業内容の考え方を下図に示します。なお、次期システム更改時における移行費用の高騰やベンダロックを抑止するため、仕様書には以下のような要件を記載することが望まれます。

◆ 仕様書記載（例）

・ 本調達で導入を行うシステムにおいては、保有する全てのデータに関して契約終了後、CSV データ等の可読性の高いレイアウトでのデータ提出を行うこと。その際のデータ抽出に係る費用は、全て調達範囲に含めること。

・ 次期システムへの移行のために必要な技術情報の提供を行うこと。

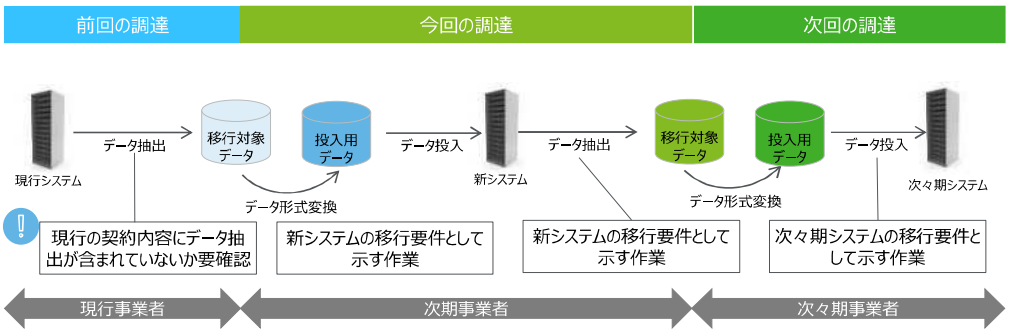
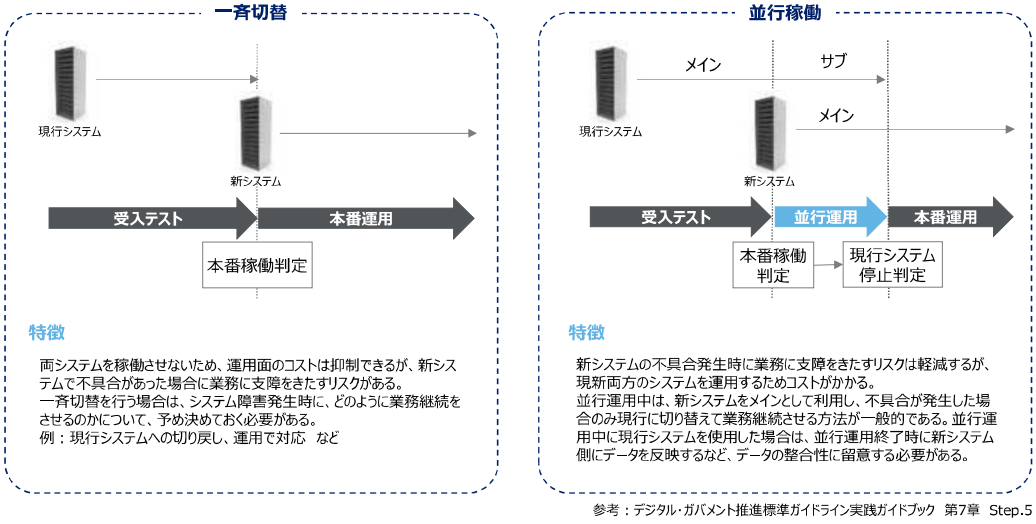


図 39 データ移行の基本的な考え方の例

イ　システム移行

システム移行とは、受入テストが終わったシステムを本番環境にリリースする作業です。移行の種類は、現行システムと新システムの並行稼働期間を設けず、ある時点で一斉に切り替える「一斉切替」と、現行システムと新システムを一定期間並行稼働させる「並行稼働」があります。原則は一斉切替を実施しますが、システムが稼働できない場合に影響が大きいなど重要度が高いシステムは、並行稼働を実施する場合もあります。



参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック　第7章　Step.5

図 40 システム移行の基本的な考え方の例

総合テスト(システムテスト)においては、調達仕様書に記載した要件を確認することが重要です。

観点	確認内容の概要	テスト仕様書の記載例
可用性	機器が冗長化されているか、バックアップセンターが設置されているか。切替テストを実施しているか。災害時に備えて、復旧体制が確立されているか。	サーバダウンを想定し、スタンバイしているサーバへの切替テストを実施すること。
性能・拡張性	性能目標値にあった性能を有している機器やシステムであるか。境界値確認を実施しているか。業務で増加するデータ量を想定した機器構成であるか。	最大利用者数での負荷テストを行い、性能目標を達成していること。
運用保守性	監視手段、バックアップ体制が確立されているか。問題発生時の役割分担、体制、訓練、マニュアルを整備しているか。	ログが記録され、都度確認ができること。 バックアップとリストアが可能であること。
移行性	次期システムにデータを容易に移行できるデータ出力機能を有しているか。出力テストは実施しているか。	データの出力を可能とすること。
セキュリティ	データにアクセス可能な者が限定されているか。権限設定に応じたアクセスができることを確認しているか。不正アクセスやウイルス感染を防止できる仕組みがあるか。	一般ユーザがデータを直接更新できないような仕組みとすること。
緊急時対応計画との整合性	山形県が定める事業継続計画やコンティンジェンシープランに則り緊急時の対応手順が整備されているか。	（必要に応じて）災害や事故など想定外の事態発生時の対策訓練を実施すること。

図 41 総合テスト(システムテスト)における確認のポイント例

(10) 教育・研修要件

情報システムの利用者が情報システムに実装された機能を理解し、効率的に運用していくために、利用者に対するマニュアルや操作研修の内容について定義します。人事異動等に備え定期的に研修を実施することや、マニュアル等についても工夫が必要である点に留意してください。

教育・研修要件の項目	概要	記載例
1 マニュアル	管理者用、ユーザ用のシステム操作マニュアルの作成要件を示す。	管理者・ユーザ向けの情報システムの操作マニュアルを作成すること。また、業務マニュアルのシステム関連部分の作成についても支援する。
2 研修	導入前、導入後の定期的な研修について、目的、対象者、内容、回数などを示す。	全職員に対するシステム管理者・ユーザトレーニングを導入前に実施すること。年に1度、集合研修を実施すること。

■マニュアルの要件（例）

マニュアル	概要	対象者
操作手順書	• 利用者区分ごとに操作手順書の内容を分割するなど、利用しやすいように工夫すること • 個々の業務に沿った画面の流れを中心に作成すること	○○入力担当者
システム管理者用操作手順書	• 管理者権限のみが操作可能な機能に特化したシステム管理用操作手順書を作成すること	○○決裁者

■研修の要件（例）

研修対象者の範囲	内容	実施時期	方法	マニュアル	対象者数
○○入力担当者	窓口業務における操作	運営開始前準備等	集合研修：○○研修所	操作手順書	○名程度
○○決裁者	決裁における操作及び分析	人事異動時	オンライン研修：各職員が日常使用している端末PC	システム管理者用操作手順書	○名程度

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第５章 Step.6

図 42 教育・研修要件(例)

(11) 運用・保守要件

運用・保守要件は、情報システムが滞りなくサービス提供できるよう監視やバックアップ等の定型化されたオペレーションを実施する「運用」と、不具合対応等システムの改修や調整を実施するための「保守」に大別されます。

「運用」では、システム評価に向けたログ解析等のサポートを要件として設定しておくことも重要です。共通基盤を利用する場合は、共通基盤の機能やサービスを活用することで、コスト削減や業務の効率化を図ることができます。

要件	概要	記載例
運転管理・監視等	ログ管理、ジョブ（スケジュール）管理、バックアップ・リストア管理、システム監視、構成管理、変更管理、マスタ管理	• ログは原則１年分（※）保管すること。 • スケジュール外のジョブの実行やマスタの変更については、作業依頼書を取り交わした上で作業すること。 • 必要に応じてRPA等のツールを活用すること。
運用サポート	ヘルプデスク業務、研修、ログ解析	• 運用について不明点がある場合は、電話またはメールにてヘルプデスクに問合せること。 • アクセスログの解析を行い、利用状況の報告を行うこと。

※平成23年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書参照

図 43 運用要件(例)

要件	概要	記載例
予防	セキュリティ管理、利用者管理、バージョンアップ対応	• セキュリティソフトのバージョンアップは、パッチリリース後1週間以内に実施すること。 • OSバージョンアップが不要の場合は、その旨を記載すること。
障害対応	問題発生時の調査、分析、暫定・恒久対応、防止策の策定等	• 障害発生時、原因の究明、暫定対応、恒久対応を行い、障害内容や対処内容、再発防止策を記載した障害報告書を提出すること。

参考：デジタル・ガバメント推進標準ガイドライン実践ガイドブック 第５章 Step.6

図 44 保守要件(例)

(12) 成果品

各作業の目的を明確にするため、各作業項目に対する成果品を明示します。実績の明確化だけでなく、見積金額の根拠となる各工程の成果品の想定ボリュームと、実際の成果品のボリュームを比較することで、見積金額の妥当性判断にも利用することができます。

項番	概要	内容	内訳
1	計画資料	構築、運用、保守に係る計画、実施スケジュール、実施体制を記載した資料	プロジェクト計画書、作業スケジュール、体制図 等
2	設計書	システム構築に係る資料	要件定義書、内部設計書、外部設計書、データ項目定義書、連携インターフェース仕様書 等
3	テスト計画及び結果	事業者側のテスト計画及びその結果や、ユーザ側のテスト計画資料	総合テスト計画書及びテスト結果、受入テスト（ユーザテスト）計画、システム連携テスト計画及び結果、データ移行計画及びテスト結果 等
4	報告書	障害対応や保守運用対応の実績資料	障害対応一覧及び対応結果、保守運用報告書 等
5	マニュアル	システムの操作手順や管理手順を記載した資料	操作マニュアル(管理者用、利用者用)、業務マニュアル、FAQ 等

※必要に応じて、ハードウェアやソフトウェアを成果品に追加すること。

図 45 成果品(例)

(13) 情報の消去及び廃棄

令和元年に他県において、リース契約等により返却した物品からの情報流出事案が発生しました。当該事案は、リース契約満了後、当該契約の相手方であるリース会社から作業を請け負った事業者の従業員によるハードディスクの横領によるものでした。

本県の情報セキュリティポリシーにおいても、電磁的記録媒体の廃棄に関するルールは記載されているところですが、仕様書の作成に当たっては、契約完了時のデータ消去及び廃棄方法について必ず明記する必要があります。記載に当たっては、具体的な消去及び廃棄の方法を指定することや、消去及び廃棄したことを確認できる方法について記載することが望ましいと考えられます。

クラウドサービス等を活用する場合は、電磁的記録媒体の物理破壊を指定することは困難であることが想定されるため、データの取扱方法については、事業者の規約等を十分に確認する必要があります。

なお、調達仕様書に記載する情報の消去及び廃棄に関する要件の記載例は付録の「付録1_調達仕様書(例)」を参考にしてください。また、上記事案を踏まえた本県の対応について、「情報システム機器廃棄時等のデータ消去等に係る適正な取扱いについて(通知)(情政第480号、令和2年2月13日)」もあわせてご参照ください。

(参考)

◆ 山形県情報セキュリティ対策基準(抜粋)

第3章 情報資産の分類と管理

3．3　情報資産の管理

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産の取り扱いについて管理方法を定め、情報資産の分類又はその内容に応じその取り扱いを制限しなければならない。また当該情報資産について、所属する職員等に対し、次に掲げるところ及び別に定める実施手順により取り扱うよう指導しなければならない。

(5)情報資産の廃棄

情報資産を廃棄する場合は、次に掲げるところにより行うこと。

①当該媒体を所管する情報セキュリティ管理者又は情報システム管理者の許可を得ること。

②記録されている情報の機密性に応じ、当該機器等の情報を復元できないように処置した上で廃棄すること。

③行った処理について、日時、担当者及び処理内容等を記録すること。

第5章　物理的セキュリティ

5．1　機器等の管理

(7)機器の廃棄

サーバ等機器及び電磁的記録媒体の廃棄又はリース返却をする場合は、当該機器等から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。また、これに係る廃棄等の記録を作成し保管しなければならない。

7 調達仕様書作成後の流れ

(1) 調達仕様書のレビュー

調達仕様書の内容の妥当性を確認するため、所属内レビューやシステム関係者レビュー、再 RFI などを実施します。

ア 所属内レビュー

所属長（必要に応じて部局長）を含めた管理職同席のもと、システム導入目的や期待効果、業務フローなどのシステム導入における前提事項や、システム機能の具体的な内容についてレビューを行います。

イ システム関係者レビュー

当該システムの連携先や情報部門などの関係者を交え、連携先システムのデータ形式、データの出力タイミング（時点）、システム連携テストのスケジュール、全体フローの確認等の、システムの連携方式や運用等についてレビューを行います。

ウ 再 RFI の実施

作成した仕様の対応可否について、候補となる事業者に確認します。すでに RFI を実施した案件については、回答のあった事業者に対して再確認を依頼します。

(2) 調達仕様書に基づいた RFI の再実施

調達仕様書の作成後、仕様についての実現性や公平性の確認、システム構築及び運用コストを把握するために、入札公告に先立ち、広く事業者から意見を求めるものです。RFI の実施基準は、初回に実施した RFI に準ずることとします。また、RFI 実施事業者に調達仕様書を公開することは差し支えありません。RFI を実施していない場合は、原則「競争入札参加資格者名簿」等から、2者以上の事業者を選定します。

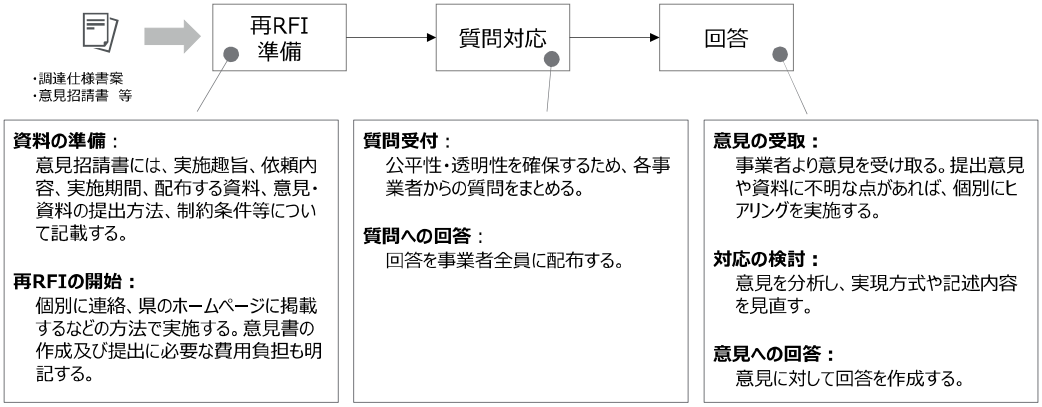


図 46 再 RFI の進め方（例）

なお、RFI の回答については、以下の点について留意してください。

・ 事業者からの追加仕様案には、特定の事業者に有利な仕様が含まれている場合があ

るため、採用には注意すること。

・　全ての事業者の回答に対応できるようにすると、必要な機能を除外せざるを得なくなる可能性があるため、業務上必須の機能については対応できない事業者がいても仕様上残すことを検討すること。

(3) 調達関連資料の作成

調達に向けて、下図を参考に調達方式に応じた資料を準備してください。

項番	資料	一般競争入札	総合評価	プロポーザル	随意契約
1	入札説明書	○	○	－	－
2	提案実施要領	－	－	○	－
3	仕様書	○	○	○	○
4	審査要領	－	○	○	－
5	契約書案	○	○	○	○
6	見積依頼書	－	－	－	○
7	落札者決定基準	－	○	○	－

図 47 調達方式毎の作成資料(例)

なお、契約書案は、原則として学事文書課が毎年示している「業務委託契約書」のひな形を利用してください。また、委託業務内で情報漏えい等に代表される情報セキュリティインシデントが発生することを防止するため、契約書において、本県の情報セキュリティポリシーを示したうえで、遵守することを義務付けてください。契約書への追記例は以下の通りです。

■ 追記例

(山形県情報セキュリティポリシー遵守義務)

第 X 条 受注者は、この契約による業務を実施するに当たっては、山形県情報セキュリティポリシーを遵守しなければならない。

また、委託業務の中で、個人情報を取扱う可能性がある場合には、「個人情報取扱特記事項」も契約書の別添として締結することに留意してください。

さらに、情報システムや取扱う情報の重要性といった特性等を踏まえて、情報セキュリティに関する認証資格を要件に含める場合は、入札公告等に以下を参考に必要な要件を記載してください。

- 受注者は、プライバシーマーク[12]又は ISO/IEC27001[13](情報セキュリティマネジメントシステム)相当の認証を取得していること
- 当該システムがクラウドサービスである場合には、受注者は、ISO/IEC27017 相当の認証を取得していること

なお、地域経済の振興の観点から、本県内事業者といった要件や上記の情報セキュリティに認証資格以外の要件を加える場合には、その旨を記載してください。

[12] 個人情報について適切な保護措置を講ずる体制を整備しているかについて、第三者が評価する制度。
[13] 情報セキュリティに関する国際規格の1つで、情報セキュリティマネジメントシステムの確立と継続的な改善を要求する規格。

(4) 評価基準

調達方式を総合評価とする場合は、別途、評価基準を定めます。評価基準における配点の一般的な考え方は下図を参照し、検討してください。

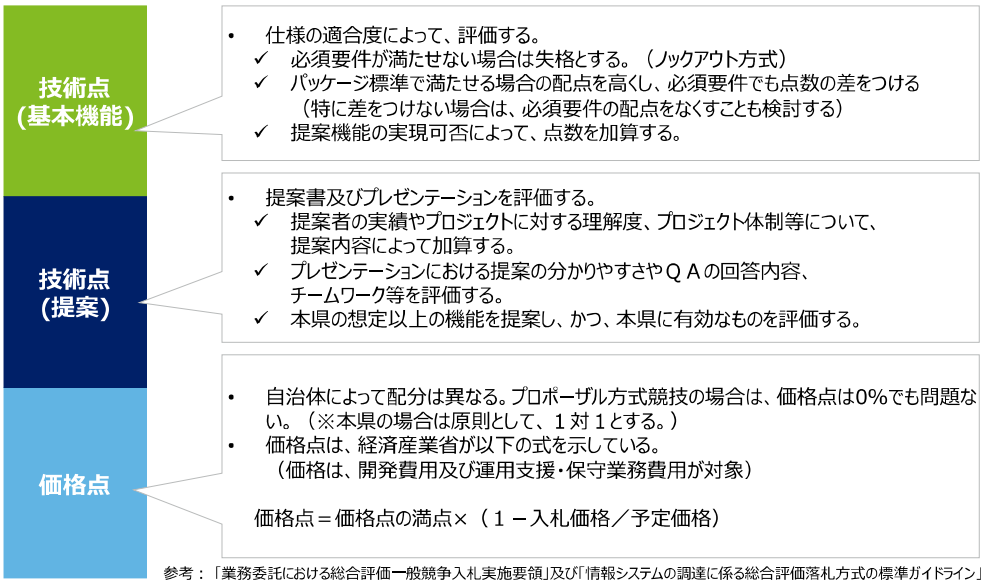


図 48 評価基準の考え方(例)

(5) 公告・契約

調達関連資料の作成が終わり次第、公告に向けて準備します。なお、公告から契約に向けた流れは下図の通りです。

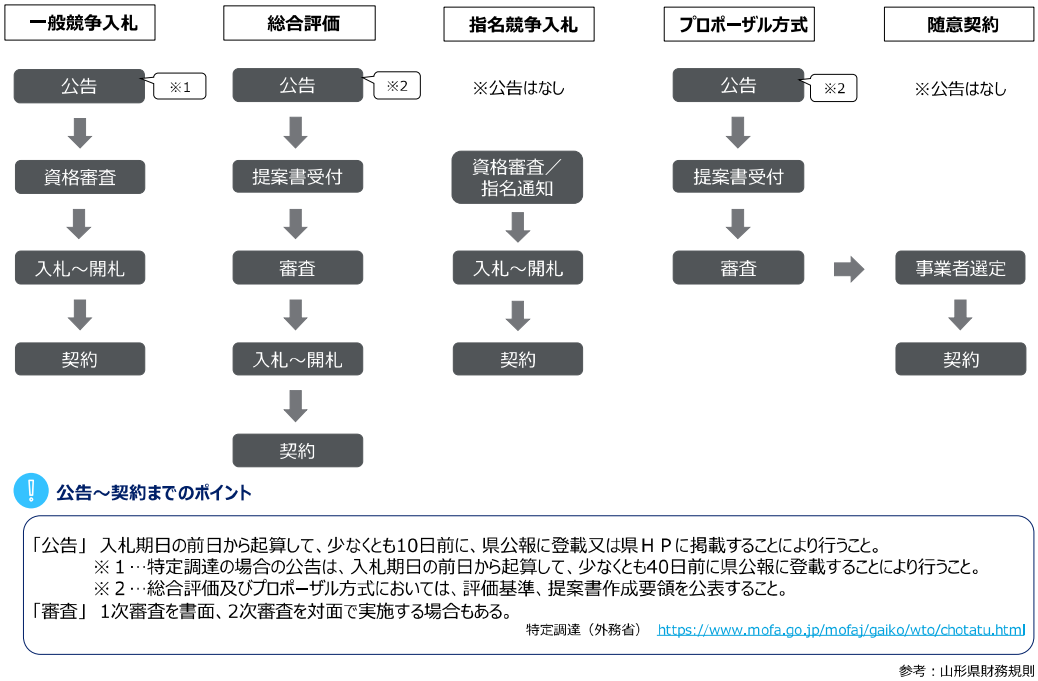


図 49 公告から契約までの流れ

なお、自治体が情報システムをプロポーザル方式で調達を行う際の一般的なスケジュールは下図の通りです。事業者の提案書準備期間や審査日数等の各作業の期間が短いと、熟度の高い提案を受けることができない、十分な審査ができない等、結果として低品質な情報システムが納入されてしまうといった影響が懸念されるため、余裕のある作業スケジュールを設定することが重要です。

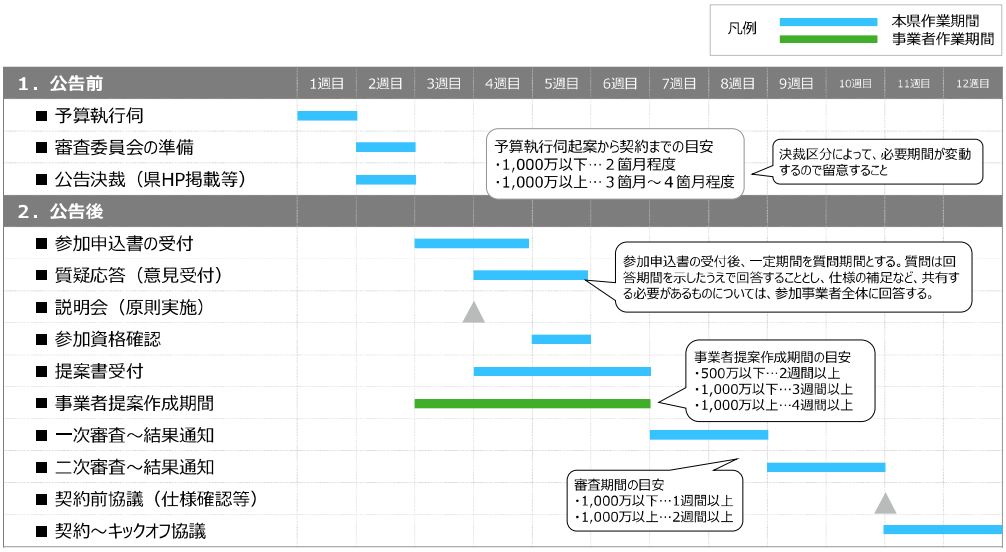


図 50 プロポーザル方式における一般的なスケジュール（例）

(6) 審査結果の通知

プロポーザル方式を採用した際は、業務委託における公募型プロポーザル方式実施要領第6条第4項に基づき審査結果を参加者に通知します。通知の内容については、概ね以下のとおりとします。

ア　すべての参加者に共通して通知する項目

(ア) 参加者数

(イ) 当該参加者の総得点

(ウ) 当該参加者の各審査項目（1　全体的事項、2　委託業務内容、3　体制、その他の事項等）の得点

イ　2位以下の参加者に共通して通知する項目

(ア) 1位の参加者の総得点

(イ) 1位の参加者の各審査項目（1　全体的事項、2　委託業務内容、3　体制、その他の事項等）の得点

8 その他契約書及び仕様書に関する留意事項

(1) その他留意事項

契約書及び仕様書の作成にあたっては、以下についても留意してください。なお、これらは調達後のリスクを軽減するために重要な事項である一方、過度な要求はコスト増につながる可能性があることにも留意してください。

ア 機密保持、資料の取扱い

業務で知り得た情報や、資料の取扱いについて、受託者による目的外の利用の禁止や契約期間終了後に適切に返却・廃棄することを仕様書に定める必要があります。記載例は付録の「付録 1_調達仕様書(例)」を参考にしてください。

イ 法令等の遵守

調達する案件の履行に際して、特に遵守が求められる法律等がある場合には以下の例を参考に契約書に定める必要があります。

■ 記載例

● 当該調達案件の業務遂行に当たっては、XX 法、XX 法等を遵守し履行すること。

また、本県においては、調達仕様書等に労働関係法令の遵守を明記することとしているため、必ず記載してください。

上記に加えて、調達する案件の履行に応じて、法令や本県が定める条例、規則等の遵守が求められる場合には上記と同様に、契約書に定めることについて、留意してください。

ウ 契約不適合担保責任(旧瑕疵担保責任)

契約不適合担保責任とは、納品された情報システムに不具合があるなど、納品された成果物に何らかの欠陥があった場合の、システム事業者に対して、履行追完請求権・代替物提供請求権(改正民法 562 条 1 項)、代金減額請求権(改正民法 563 条)、損害賠償請求権及び解除権(改正案 564 条)を指します。契約不適合責任が発生する期間について、民法では発注者側が契約不適合を知ってから 1 年以内とされている点に留意してください。(改正民法 566 条)

エ 検収

検収は成果品や提供された役務について、要求事項を満たしているか確認する重要な行為です。契約書及び仕様書をもとに、確認を実施する点に留意してください。検収に関する仕様書への記載例は、付録の「付録 1_調達仕様書(例)」を参考にしてください。

オ 再委託に関する制限

再委託については、以下の3つの考え方があります。

(ア) 原則、認めない

(イ) 発注者の承認により認める

(ウ) 原則、自由とする

再委託は、コストや業務の効率化の面でのメリットが見込まれる一方、再委託先による情報漏えいのリスクが懸念されます。そのため、再委託は原則禁止とします。一方、委託業務が効果的に遂行できるとすれば、発注者の承認のもと再委託を認めることとする「(イ)発注者の承認により認める」方法も一案です。ただし、業務の大半を委託するようなケースや個人情報を取り扱うような業務では、再委託を認めないことが望ましいと考えられます。なお、再委託に当たっては、書面によって承認証跡を残すことに留意してください。再委託に関する仕様書への記載例は、付録の「付録 1_調達仕様書(例)」を参考にしてください。

カ　知的財産権の帰属

委託業務で開発したソフトウェアの著作権は、原則として本県が保有します。ただし、著作権は、「成果物を作成した人(あるいは組織)に帰属する権利」になるため、契約書上で特に定めがない場合は、ソースコードを作成した技術者、あるいはシステム開発会社が著作権を持つことになることから、権利の帰属や譲渡等について、契約書に明記する必要があるかについても検討してください。

※一般的に契約書の記載によって著作権を保有できるものは、独自仕様で作成したプログラムやカスタマイズした内容等であり、汎用ミドルウェアやパッケージ製品そのものについては対象にできない点に留意します。

9 構築段階

(1) プロジェクト管理

ア キックオフ時の協議事項

キックオフ会議は、基本的にはプロジェクトの実施計画を精査する重要な場であるため、十分な資料準備と会議時間確保に努めてください。実施計画の主な内容としては、スケジュール、体制、プロジェクトの進め方の3つについて、認識を合わせる必要があります。キックオフ会議は、契約後速やかに開催し、一定レベルの責任者(発注者:所属長等、事業者:プロジェクトマネージャー以上)が同席することが重要です。

項目	内容	参照する資料（例）
スケジュール	個別のスケジュールの妥当性や、マイルストーンの抜け漏れを確認する。特に、スケジュールは事業者の目線で作られることが多く、発注者側のマイルストーン（発注者側の決裁期間や上席への説明会など）が漏れるリスクがあるため、発注者側で納品までに行う必要がある作業やイベントに漏れがないか確認する。	作業スケジュール
体制	何名体制で、どのレベルの担当者が参画しているのか、どれくらいの頻度で誰が現場に来るのかを確認する。体制図には多数の担当者の記載があるにも関わらず、実際には担当者1名で対応する等もあるため、体制図と実運用の差異を確認する。	体制図
プロジェクトの進め方	各作業に関してどのような進め方をするのかを確認する。特にどのように品質確保をする（社内のレビュー体制など）のかを把握する。また、コミュニケーションの取り方(連絡の窓口、連絡方法(メール等))を確認する。	プロジェクト計画書

図 51 キックオフ会議における確認事項(例)

イ プロジェクトにおける管理事項

プロジェクト管理とは、プロジェクトが成功するようにマネジメントすることであり、PMBOK[14]では 10 の知識エリアで構成されると定義されています。各知識エリアでの分析を元に、プロジェクト全体の視点で計画を見直す等、部分最適や個別最適ではなく、全体最適の視点が求められます。

[14] プロジェクトマネジメントの概念や用語、手法、工程などを体系化した標準の1つ。Project Management Body of Knowledge の略。

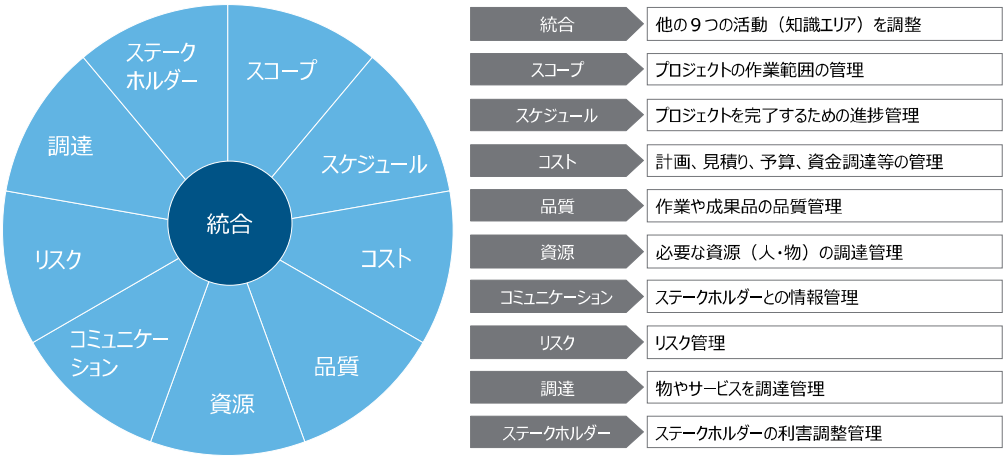


図 52 プロジェクト管理における 10 の知識エリア

ウ　スケジュール（進捗）管理

プロジェクトは、有期性という特性から、時間という制約が生まれます。単に最終的な納期を守るという条件だけでは、きめ細やかな管理が困難なため、スケジュールを作成して、コントロールを行う必要があり、PMBOK では「プロジェクトを所定の時期に完了させるためのプロセス」と定義されています。代表的な進捗管理の手法としては、「マスタ・スケジュール」、「WBS」、「進捗報告書」等の資料をもとに確認し、進捗遅れやそのリスクがある場合は、原因分析と対策を検討する方法が挙げられます。なお、受注事業者の WBS は事業者目線で作成されており、県側の作業時間が考慮されていない場合があります。作業の抜け漏れを防止するためには、システム所管課側でもスケジュールを作成する方法も有効です。

NO	チェックポイント	確認の目的
1	作業ごとに現在の進捗がわかるWBSになっているか。	作業ごとの進捗を把握することで、関連する作業（例えば、他システムとの連携テスト等）への影響を把握できる。
2	定例会議や稼働判定会議等のイベントを記載しているか。	会議体を記載することで、いつまでに誰が、何を（例えば、テスト結果等の成果品）作成するかを明示することができる。
3	作業や成果品に抜け漏れがないか。	作業や成果品に抜け漏れがある場合、作業の着手遅れの原因につながってしまう。
4	作業や成果品に重複がないか。	無駄な作業がある場合、進捗遅れを招きやすくなってしまう。
5	成果品等の承認作業を記載しているか。	いつまで誰が、何を（例えば、テスト結果等の成果品）、承認しなければならないかを明示することができる。
6	成果品等の承認（確認）期間が十分か。	成果品等（例えば、テスト結果等の成果品）の承認（確認）期間が十分でない場合、バグ等を発見できないおそれがある。

図 53 マスタ・スケジュールや WBS を利用する際の確認ポイント（例）

(ア) マスタ・スケジュール

マスタ・スケジュールとは、プロジェクトの開始から完了までに必要な作業をすべて洗い出し、それらを順序付けたものがマスタ・スケジュールです。大まかな進捗管理を行うために活用します。

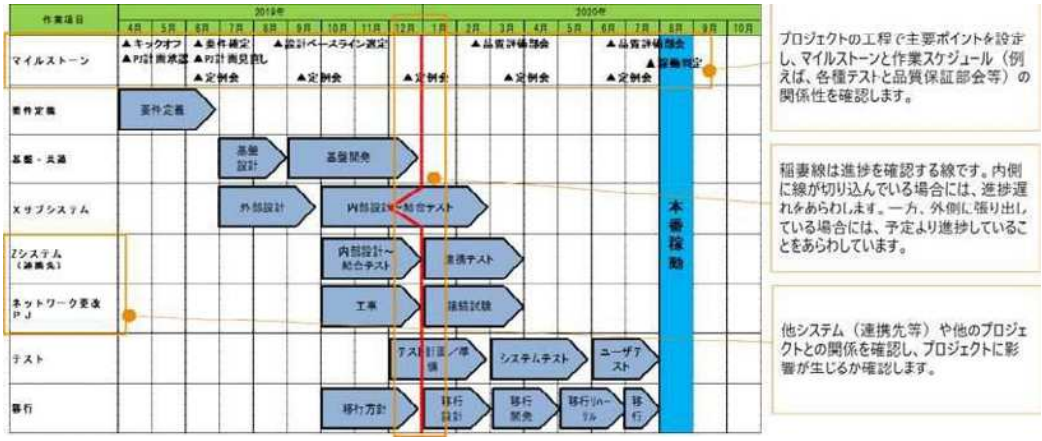
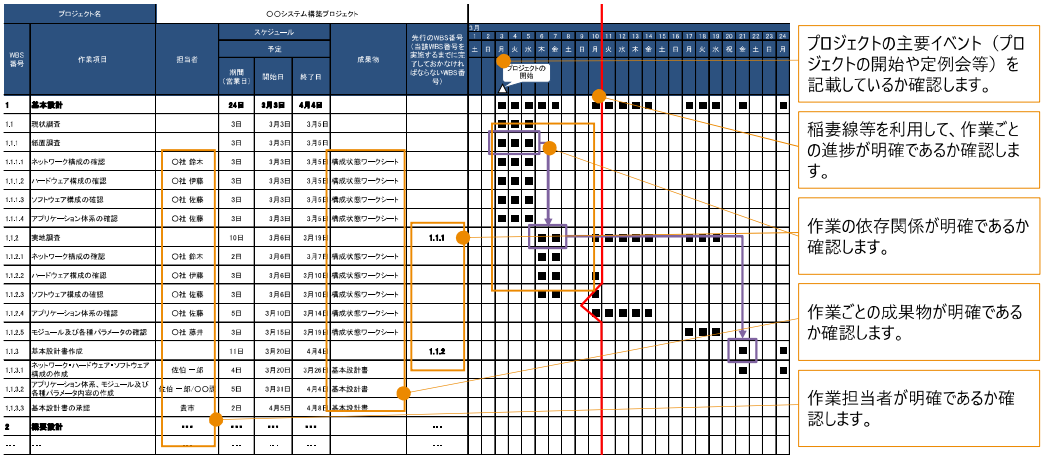


図 54 マスタ・スケジュールの活用イメージ(例)

(イ) WBS(Work Breakdown Structure)

WBS とは、プロジェクト等の目的を達成するために必要な作業(Work)を漏れなく分解(Breakdown)し、構造化(Structure)したものです。進捗管理のほか、抜け漏れ、重複を防止するために活用します。



エ　ウォーターフォール型開発（V 字モデル）

官公庁の情報システムでは、開発に際して主にウォーターフォール型開発を採用しています。ウォーターフォール型の開発において、システム開発が開始してから終了するまでの流れにおける開発工程とテスト工程を表したモデルがV字モデルです。

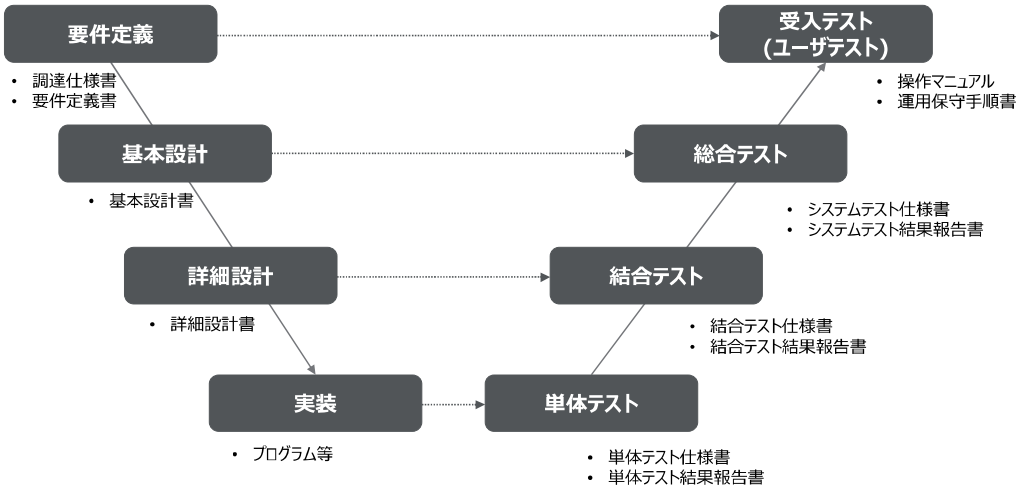


図 55 ウォーターフォール型開発のイメージ図

(ｱ) ウォーターフォール型開発において発注者が注意する点

ウォーターフォール型開発の情報システムを発注した際、発注者は、総合テスト及び受入テスト(ユーザテスト)について、主に下図の観点でテストが実施されているかを重点的に確認します。

○：メイン、△：レビュー

種別	目的	実施主体		注意する点（例）
		県	事業者	
単体テスト	・ プログラムを構成する比較的小さな単位（ユニット）が個々の機能を満たしているかどうかをテストする。	－	○	✓ 実施体制（例えば、開発者とテスト担当者が同一になっていないか）が妥当であるか。 ✓ テスト結果を受領した上で、ヒアリングし、単体テストをシナリオ通りに実施しているか。
結合テスト	・ 開発したプログラムが他のプログラムと連動して、機能として正しく動作するかどうかをテストする。	△	○	✓ 実施体制（例えば、開発者とテスト担当者が同一になっていないか）が妥当であるか。 ✓ テスト結果を受領した上で、ヒアリングし、結合テストをシナリオ通りに実施しているか。
総合テスト	・ 求められている機能が正しく動作するかをテストする。 ・ システムが非機能要件を満たしているかテストする。	△	○	✓ 基本設計書の機能を網羅しているか。 ✓ 異常系のケースもテストを実施しているか。 ✓ 本番運用を想定した十分なデータの処理件数でテストが行われているか。
受入テスト（ユーザテスト）	・ 実際に操作して、要件定義で定めた仕様が実現されているかについて、実際に業務遂行上の問題点がないかテストする。	○	△	✓ 職員が直接、システムを操作し、操作性や機能性について問題がないか。 ✓ 異常系のケースもテストを実施しているか。 ✓ 現行システムと出力結果が一致するか。

図 56 ウォーターフォール型開発における確認ポイント(例)

オ　アジャイル型開発

アジャイル型開発とは、大きな単位でシステムを区切ることなく、イテレーションと呼ばれる小単位(1 週間～4 週間程度)で設計からテストを繰り返して開発を進める手法です。近年、早期に開発後のイメージを確認できることから、HP 等の Web 系システムで採用することが多く、官公庁の情報システムの開発手法でも採用されつつあります。

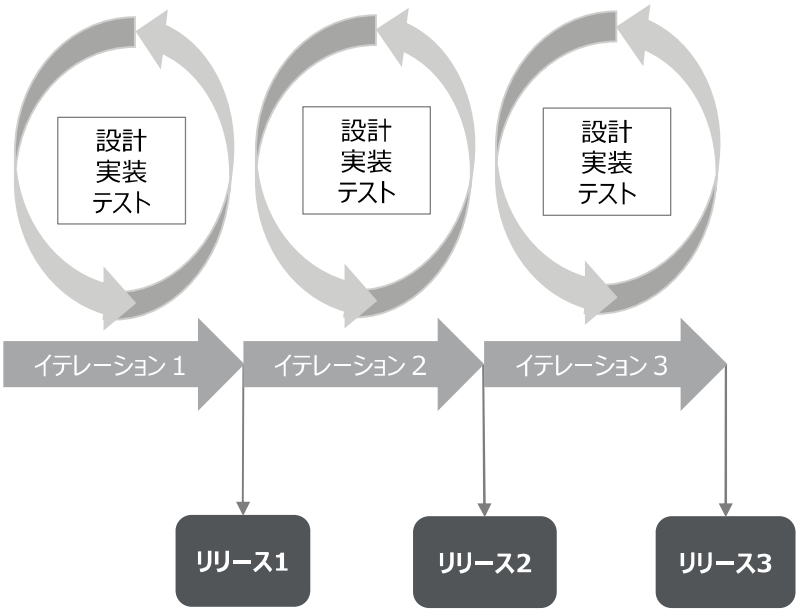


図 57 アジャイル型開発のイメージ図

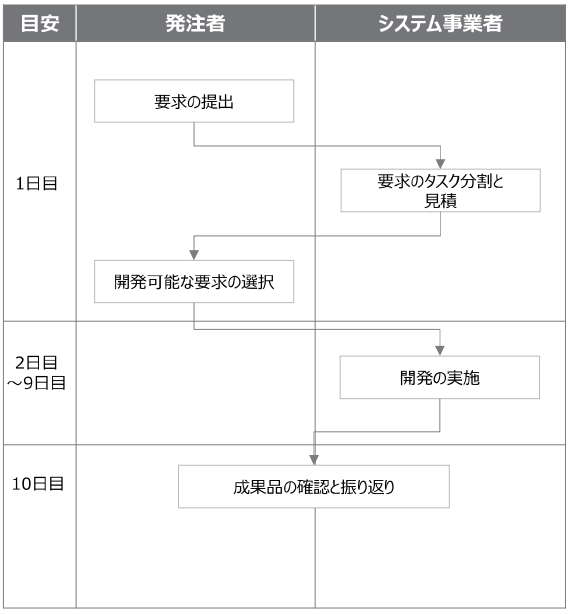


図 58 イテレーションでの作業フローイメージ図

(ｱ) アジャイル型開発において発注者が注意する点

アジャイル型開発の情報システムを発注した際、発注者は、各イテレーションでのスケジュール管理やマイルストーンの設定について、注意します。またアジャイル型開発では、計画を詳細に立案しないことから、スケジュールや進捗具合が把握しにくくプロジェクトの遅延のリスクがあるため、開発スケジュールに対する進捗確認を行うことが重要です。

工程	概要	注意する点（例）
要求の提出	• イテレーション単位で実施したい内容を事業者へ提出する。	✓ 事業者へ正確にインプットできるよう、要件を整理したうえで十分なコミュニケーションをとっているか。
要求の選択	• 要求を基に事業者が作成した見積を確認し、実現したい要求を選択する。	✓ 事業者が作成した見積をもとに、イテレーション内でこなせる作業量に収まるよう要求を取捨選択して、事業者に作業を依頼しているか。
成果品の確認と振り返り	• 仕様通りにシステムが動くか確認する。 • 次のイテレーションに向けて要件を再整理し、全体のスケジュール管理を行う。	✓ 仕様通りにシステムが動かなかった場合は、要求の変更点と次のイテレーションに向けた新規の要求から、優先順位を再設定しているか。 ✓ 最終的な目標を意識した上で、イテレーションごとの要求事項を整理し、スケジュールに遅延がないか確認しているか。

図 59 アジャイル型開発における確認ポイント(例)

(2) 検収

検収とは、納品物が仕様通りの内容であるか確認し受け取ることであり、受託者から発注者に責任が移る分岐点となる重要な作業です。下図を参考に、検収を実施してください。

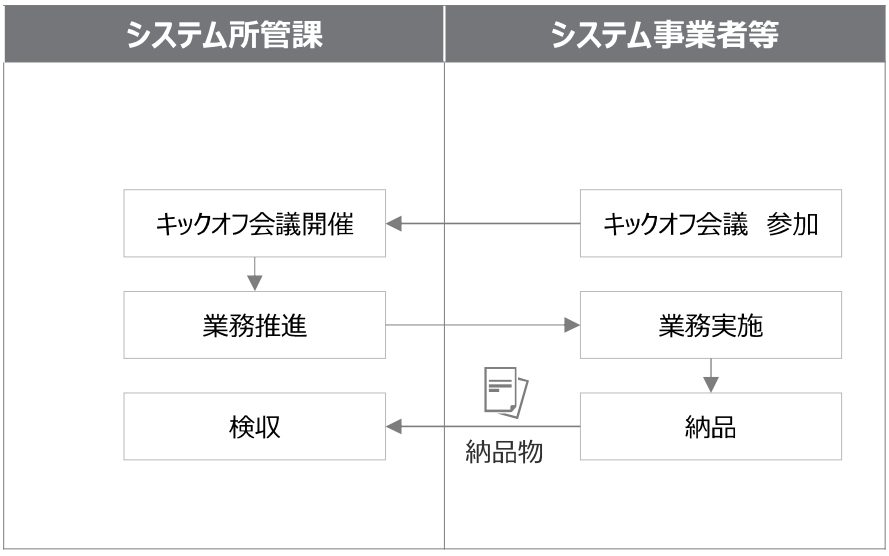


図 60 検収の流れ

ア　検収におけるチェック内容

検収に当たっては、下図のチェック観点を活用し、検収を実施してください。

チェックタイミング	内容
要件定義フェーズ終了時	仕様書の内容が成果品に抜け漏れなく記載されているか、改修の場合は、成果品のバージョン管理(改訂履歴)がなされているかを確認する。
設計フェーズ終了時	仕様書の内容が成果品に抜け漏れなく記載されているか、改修の場合は、成果品のバージョン管理(改訂履歴)がなされているかを確認する。
事業者側テストフェーズ終了時	仕様書や提案書、テスト計画書等に記載されている全てのテストを実施しているか、他システム連携がある場合は、連携テストは実施したか等を確認する。
受入テスト終了時	仕様の内容が全て実現されているか、残課題や未実施のTODOが残存していないか等を確認する。
納品時	仕様書に記載の成果品は漏れなく作成されているか、見積に見合ったボリュームで成果品は作成されているか等を確認する。

図 61 検収におけるチェックの観点例

10 運用・評価

(1) 運用保守の実施

運用保守は、情報システムを維持管理していくための業務であり、大きく製品保守とシステム保守が存在します。システム保守には、障害対応、予防保守、運用作業、ヘルプデスク、小規模改修などの業務が含まれます。運用保守の成果物は、システムの運用状況を把握するためのものであり、その実績(障害対応件数、運用作業実績など)は、運用保守仕様の定期的な見直しに利用します。

分類	保守内容	概要	成果物
製品保守	ハードウェア	定期点検、メンテナンス、障害対応（修理・交換） など	-
	ソフトウェア	ソフトウェアのアップデートパッチ提供、製品の不具合情報の通達、製品に関するヘルプデスク対応 など	-
	クラウドサービス ※1	HW/SWの保守、システム保守全般	-
システム保守	予防保守	システムの監視・点検、異常検出時の通知・対応 など	システム稼働状況報告書 など
	障害対応	障害発生時の原因追求や復旧作業 など	障害報告書 など
	運用作業	バッチ処理の実行、システムの設定変更、SWのアップデート作業、アプリ更新作業 など	運用作業実績 など
	ヘルプデスク	ユーザからの日々の問合せへの対応	問合せ対応状況 など
	小規模改修 ※2	仕様変更や機能追加等に伴う軽微な改修作業	仕様書 設計書 など

※1 クラウドサービスの場合、システム保守作業（小規模改修を除く）はサービス料に含まれることが一般的である。
※2 大規模システムで毎年一定の改修が発生するものに限定し、実績に応じて工数の見直しを行う必要がある。

図 62 運用保守の分類

運用保守のほか、障害の発生を未然に防ぐことを目的とした予防保守を行うこともあります。予防保守の概要は下図のとおりです。

分類		監視対象
サービス	プロセス監視	サービスやプロセスの稼働状況
	ポート監視	待ち受けポートへの接続可否や応答時間
リソース	CPU監視	CPU使用率
	メモリ監視	メモリの使用状況／空き状況
	ディスク監視	ハードディスクの使用状況／空き容量
ログ	システムログ	BIOSやOS等が出力するシステムログ
	イベントログ	windowsイベントログ情報
	アプリケーションログ	アプリケーションから出力されるログ情報
ネットワーク	トラフィック監視	ネットワークのトラフィック量
	アクセス監視	該当システムへのアクセス情報 （Googleアナリティクス等を利用したアクセス解析を含む）

図 63 予防保守の例

(2) 障害対応

発生した障害を迅速に解決するためには、どのような理由で障害が発生する可能性があるのか理解しておくことや、障害が発生した場合に備えて必要な準備をしておくことが重要です。

障害が発生する要因としては、以下のようなケースが考えられます。

- ✓ 自然現象・・・地震、台風、火災などの災害等
- ✓ 人的要因・・・操作ミス等
- ✓ 環境要因・・・機器故障、ソフトウェアのバグ、停電等
- ✓ 情報セキュリティ・・・不正アクセス等

なお、障害発生に備えて準備しておくべきものとしては、下図のようなものが考えられます。なお、大規模災害時は ICT-BCP ガイドラインを参照してください。

種別	記載内容
コミュニケーションプラン	システム事業者等関係者の連絡先や連絡手法について整理しておく。ＨＷとＳＷの事業者が分かれている場合など複数の事業者が関与する場合は、役割分担を明確にしておくことも重要である。
障害分析手法	エラーコードに関するマニュアルや事象別の想定原因など、障害発生後の原因究明を迅速に実施するために有効な情報を整理しておく。
オペレーションマニュアル	システムの停止・起動やバックアップからのリストア方法など、障害の復旧に向けて実施する可能性のある主なオペレーション方法について整理しておく。
インシデント管理手順	発生した障害について原因や対応方法をまとめるための一覧表や、ＳＬＡとの整合など障害を評価し、必要に応じて事業者に是正を求めるための体制等について整理しておく。

図 64 障害対応に備えて予め準備する事項

ア 障害対応の流れ

障害発生時は、障害対応に備えて予め準備した資料を活用しながら、概ね下図の流れで対応します。

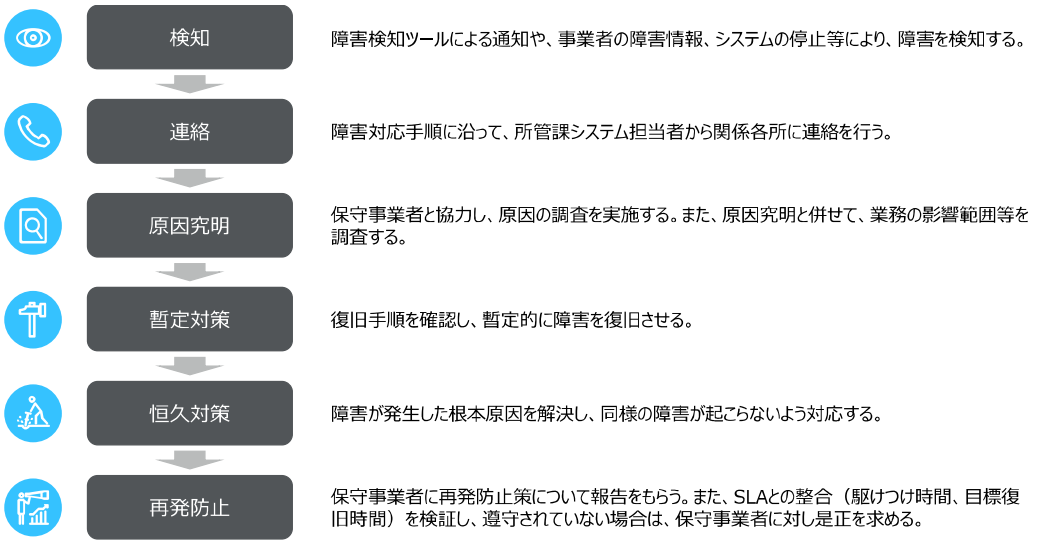


図 65 障害対応フローの例

(3) 評価の実施

情報システム運用中の場合、年次や月次等のタイミングで、事業者との定例会や定例レポート等をもとに運用実績の取りまとめを行い、運用保守の業務内容の過不足や費用の妥当性について評価を行います。情報システムの導入によって、企画段階で期待した効果が出ているかどうか、また今後の方針等を検討します。評価の目的は、情報システムの改善点を把握することであり、無理に高い評価をすることが目的ではないことを念頭に置いて検討します。

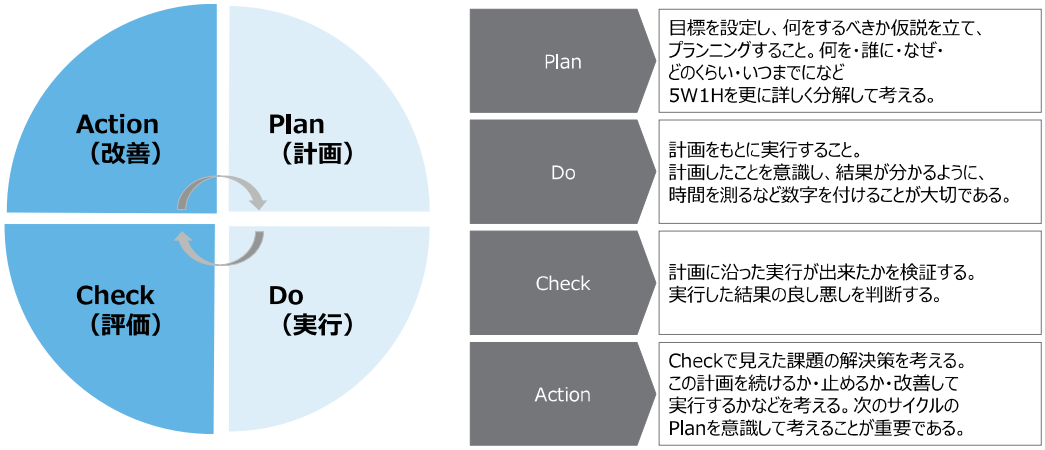


図 66 評価の概要

本ガイドライン策定に際して参考とした文献・計画・指針等

(1) 国が公表する文献等

ア 世界最先端デジタル国家創造宣言・官民データ活用推進基本計画(令和2年 7 月 17 日閣議決定)

イ デジタル社会の実現に向けた改革の基本方針(令和2年 12 月 25 日)

ウ デジタル・ガバメント実行計画(令和2年 12 月 25 日閣議決定)

エ デジタル・ガバメント推進標準ガイドライン(2020 年(令和2年)11 月 27 日最終改定)

オ デジタル・ガバメント推進標準ガイドライン実践ガイドブック(2020 年(令和 2 年)3 月 31 日)

カ 政府情報システムにおけるクラウドサービスの利用に係る基本方針(2018 年(平成 30 年)6 月 7 日、各府省情報化統括責任者(CIO)連絡会議決定)

キ 自治体デジタル・トランスフォーメーション(DX)推進計画(令和2年 12 月 25 日)

ク 地方自治体における業務プロセス・システムの標準化及び AI・ロボティクスの活用に関する研究会報告書(令和元年(2019 年)5月)

ケ 情報通信白書(平成 29 年～令和2年)

コ 公共 IT におけるアウトソーシングに関するガイドライン(平成 15 年 3 月)

サ 地方公共団体における ASP・SaaS 導入活用ガイドライン(平成 22 年4月)

シ 情報システムの調達に係る総合評価落札方式の標準ガイドライン(平成 25 年7月 19 日)

ス デジタル社会の実現に向けた重点計画(令和4年6月7日)

(2) 本県が整備した計画・指針等

ア 山形県情報システム開発・運用基本指針(平成 20 年3月策定、平成 26 年3月改定)

イ 山形県情報システム全体最適化計画(平成 17 年 11 月)(計画期間:平成 17 年度～平成 21 年度)

ウ 山形県情報システム全体最適化計画(第二次)(計画期間:平成 22 年度～平成 24年度)

エ 山形県情報システム全体最適化計画(第三次)(計画期間:平成 25 年度～平成 27年度)

オ 山形県情報システム全体最適化計画(第四次)(計画期間:平成 28 年度～令和2年度)

カ 山形県情報システムフレームワーク(平成 17 年 11 月策定、平成 26 年3月改定)

キ 山形県情報システム開発・運用ガイドライン(平成 23 年 3 月策定、平成 29 年3月改定)

ク 山形県クラウドサービス導入活用指針(平成 26 年3月策定、平成 29 年3月改定)

ケ 山形県クラウドサービス導入活用ガイドライン(平成 29 年4月)

コ 山形県情報セキュリティ基本方針(平成 14 年 4 月 1 日施行、平成 20 年 4 月 1 日改正

施行）

サ　山形県情報セキュリティ対策基準（平成 20 年4月１日施行、令和3年Ｘ月Ｘ改正施行）

シ　山形県財務規則（昭和 39 年3月県規則第9号）

様式集（別添）

- ✓ システム開発計画書
- ✓ システム構築に関する調書
- ✓ 統一見積書
- ✓ 予算検証チェックリスト

付録(別添)

- ✓ 付録 1_調達仕様書(例)
- ✓ 付録 1 調達仕様書別紙_様式_機能一覧(例)
- ✓ 付録 1_調達仕様書別紙_様式_帳票一覧(例)
- ✓ 付録 1_調達仕様書別紙_様式_連携インタフェース一覧(例)
- ✓ 付録 2_情報提供依頼書(RFI)(例)

資料番号５

山形県情報セキュリティポリシー

山形県情報セキュリティ基本方針

本県は、自らＩＴ社会の模範たる構成員となり、ＩＴ社会の健全な発展に寄与するとともに、本県が保有する県基幹高速通信ネットワークをはじめとする情報システム及び電子情報（以下「本県の情報資産」という。）の管理を適正に実施し、県民の権利、利益を守り、行政の安定的継続的な運営を実現するため、ここに山形県情報セキュリティ基本方針を制定する。

１　職員一人一人がＩＴ社会における模範となるよう努める。

２　適切な技術的施策を講じ、本県の情報資産に対する不正な侵入、改ざん、破壊、利用妨害などが発生しないよう、また、これが漏えいなどすることのないよう努める。

３　外部の情報資産に対して不正な侵入、改ざん、破壊、利用妨害などをすることがないよう努める。

４　本県の情報資産にセキュリティ上問題が発生した場合、その原因を迅速に究明し、その被害を最小限に止めるよう努める。

５　本県の情報資産のうち特に重要なものについては、必要なとき確実に利活用できるよう十分な備えに努める。

６　上記の活動を継続的に実施し、かつ、新たな脅威にも対応できるよう、情報セキュリティ管理体制を確立する。

平成14年4月1日　施行
平成20年4月1日　改正施行

山形県情報セキュリティ対策基準

目次

第１章　総則

１．１　目的

山形県情報セキュリティ対策基準（以下「本対策基準」という。）は、山形県情報セキュリティ基本方針（以下「基本方針」という。）に基づき、本県が保有する情報資産を脅威から保護するための情報セキュリティ対策を実施するにあたっての組織体制、管理方法、遵守すべき事項及び判断基準等について基本的な事項を定めることを目的とする。

１．２　用語の定義

本対策基準における主な用語の定義は以下のとおりとする。

（1）情報セキュリティポリシー

基本方針及び本対策基準をいう。

（2）情報資産

次に掲げるもので、本県が保有又は契約により使用等するものをいう。

① 下記（3）から（7）に掲げるもの

② ①で取り扱う情報（これらを印刷した帳票及び文書を含む。）

③ ①にアクセス又は管理区域へ出入りするために用いる IC カード、USB トークン及びこれらに類するもの（以下「IC カード等」という。）

④ 情報システムの仕様書、ネットワーク構成図及び開発・保守に関する資料等の文書

（3）パソコン等機器

パソコン、モバイルノートパソコン、スマートフォン及びタブレット型コンピュータ等の機器並びにこれらに含まれる電磁的記録媒体をいう。

（4）サーバ等機器

情報を格納しているサーバ及びこれに含まれる電磁的記録媒体並びに通信回線装置等のネットワークを構成する基幹機器をいう。

（5）電磁的記録媒体

磁気ディスク、光学ディスク、磁気テープ及びフラッシュメモリ記憶装置等（スマートフォン及びタブレット型コンピュータ等の機器に含まれるものを含む。）のデータを記録・保持するための媒体又は装置全体をいう。

（6）ネットワーク

パソコン等機器又はサーバ等機器（以下「パソコン・サーバ等」という。）を相互に利用するための通信回線網及びこれを構成する基幹機器をいう。

（7）情報システム

パソコン・サーバ等、電磁的記録媒体、ネットワーク、クラウドサービス（インターネット上で利用できるアプリケーション等のサービスをいう。）及びソフトウェアで構成された情報処理又は通信に用いる機器及び仕組みをいう。

（8）脅威

次に掲げるもの及びこれに類するもので、情報資産に係るものをいう。

① 部外者等の無断侵入、窃取、不正アクセス、不正プログラム（不正かつ有害な動作を行う意図で作成された悪意のあるプログラム等をいう。）による攻撃及び標的型攻撃等の意図的要因並びに委託

事業者等の過失等の非意図的要因による情報資産の漏えい・破壊・改ざん・消去等

② 職員等の情報セキュリティポリシーに係る違反行為等の意図的要因並びにプログラム上の欠陥、人為的ミス（誤操作、電子メールの誤送信、紛失等をいう。）及び故障等の非意図的要因による情報資産の漏えい・破壊・改ざん・消去等

③ 地震、落雷及び火災等の災害並びにサービス不能攻撃等の予期しない大量アクセス等による情報システムの停止等

（9）情報セキュリティ

情報資産について、次に掲げるものを維持することをいう。

① 機密性（Confidentiality）

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

② 完全性（Integrity）

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

③ 可用性（Availability）

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(10) 情報セキュリティインシデント

単独又は一連の脅威のうち、情報セキュリティを脅かす又はその確率が高い事象をいう。

(11) 職員

常勤の職員をいう。

(12) 職員等

職員、非常勤職員をいう。

(13) 事業継続計画

自然災害等の問題発生シナリオに基づいて具体的な作業手順を定め、事業などが停止する時間を可能な限り少なくする目的で作られる管理策や計画をいう。

(14) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(15) LGWAN 接続系

人事給与、財務会計及び文書管理等LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

(16) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(17) 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(18) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピューターウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

(19) 標準準拠システム等

地方公共団体情報システムの標準化に関する法律（令和３年法律第40号）第６条第１項及び第7条第１項に規定する標準化基準に適合する基幹業務システム及び関連システム等の業務システムをいう。

１．３　適用範囲

（１）組織の範囲

本対策基準が適用される行政機関は、知事部局、教育委員会、議会事務局、選挙管理委員会、人事委員会、監査委員、公安委員会、警察本部、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会、企業局及び病院事業局（以下「各部局」という。）とする。

（２）情報資産の範囲

本対策基準は、各部局が管理する情報資産を対象とする。ただし、第３章以下の規定は、警察本部が管理する情報資産について、及び山形県県立学校教育情報セキュリティ対策基準が対象とする情報資産は、第６章の６．６情報セキュリティインシデントの報告及び対応等を除き適用しない。

第２章　組織体制

２．１　組織・管理体制

山形県デジタル化推進本部設置要綱により設置された山形県デジタル化推進本部（以下「本部」という。）を情報セキュリティポリシーに関する最高意思決定機関として、本県における情報セキュリティに係る方針を決定し、その維持及び向上を図るとともに、次の体制により情報セキュリティ対策を推進する。

（１）最高情報セキュリティ責任者（Chief Information Security Officer、以下「CISO」という。）

副知事を、CISO とする。CISO は、次に掲げる権限と責任を有する。

① 本県における情報セキュリティ対策全般に関する統括的な権限と責任を有する。

② 情報セキュリティを含む情報管理全般に関する専門的な知識及び経験を有する専門家をアドバイザーとして置くことができる。

③ CISO が不在の場合は、統括情報セキュリティ責任者がその権限を代行する。

（２）統括情報セキュリティ責任者

みらい企画創造部長を、統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、次に掲げる権限と責任を有する。

① CISO を補佐する。

② 情報セキュリティ責任者に対して、情報セキュリティに関する指導及び助言を行う。

③ 情報セキュリティインシデント（軽微なものを除く。）が発生した場合は、CISO の指示のもと、必要かつ十分な措置を行う。

（３）副統括情報セキュリティ責任者

みらい企画創造部次長を、副統括情報セキュリティ責任者とする。副統括情報セキュリティ責任者は、次に掲げる権限と責任を有する。

① 統括情報セキュリティ責任者を補佐する。

② 情報セキュリティインシデント（軽微なものを除く。）が発生した場合において、CISO及び統括情報セキュリティ責任者が不在の場合はこれに代わり必要かつ十分な措置を行う。

（4）情報セキュリティ責任者

本部の本部員（以下「部局長」という。）を、情報セキュリティ責任者とする。情報セキュリティ責任者は、次に掲げる権限と責任を有する。

① 各部局の情報セキュリティに関する統括的な権限と責任を有する。

② 各部局の情報セキュリティ管理者及び情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う。

（5）情報セキュリティ管理者

各所属長を、各所属における情報セキュリティ管理者とする。情報セキュリティ管理者は、各所属における情報セキュリティについて次に掲げる権限と責任を有する。

① 各所属における情報セキュリティ対策に関して、適切な運用及び管理を行う。

② 所管する情報資産を適正に管理するとともに、情報セキュリティポリシーの適切な運用に関して、所属する職員等に指導を行う。

（6）情報システム管理者

各情報システムを所管する所属の長を、情報システム管理者とする。情報システム管理者は、所管する情報システムについて次に掲げる権限と責任を有する。

① 著しく不適切な利用等が認められる者がある場合は、その者の利用を制限又は停止する事ができる。

② 所管する情報システムの情報セキュリティに関する維持管理を行う。

③ 情報システムに関する実施手順の策定及び維持管理を行うとともに、情報主管課長と連携し、緊急時の連絡体制について利用する職員等に周知徹底を図る。

（7）情報主管課長等

情報セキュリティポリシーの運用を適切に実施するため、情報主管課を定めるものとし、みらい企画創造部ＤＸ推進課を情報主管課とし、同部ＤＸ推進課長を情報主管課長とする。情報主管課長は、次に掲げる権限と責任を有する。

① 県としての情報セキュリティの考え方・取組みを明確にする。

② 情報セキュリティポリシーに基づき、山形県として満たすべき情報セキュリティの基準を明確にし、それを実現し、維持するため、本対策基準に基づき実施手順を整備する。

③ 情報セキュリティインシデントが発生した際に迅速な対応ができるよう、各部局との連携のもとに山形県としての組織体制や連絡網を確立するとともに、山形県全体の情報セキュリティ管理体制の統括事務を所掌する。

④ 軽微な情報セキュリティインシデントが発生した場合は、自らの判断により必要かつ十分な措置を行うことができる。

（8）山形県情報セキュリティ等監査員班

統括情報セキュリティ責任者は、情報資産における情報セキュリティ対策状況について確認するため、山形県情報セキュリティ等監査員班長を指名し、山形県情報セキュリティ等監査員班を組織するものとする。

（9）情報化推進・セキュリティ委員会

情報セキュリティ責任者は、情報セキュリティポリシーを各部局の日常業務の中で具体的に運用す

るため、各部局、各総合支庁ごと情報化推進・セキュリティ委員会を組織するものとする。

(10)情報セキュリティインシデント対策班(Computer Security Incident Response Team､以下｢CSIRT｣という。)

情報セキュリティインシデントの防止に向けた取組みを行うとともに、発生時において、その状況等を正確に把握し、被害拡大の防止、復旧及び再発防止等の対策を迅速かつ的確に行うため、次に掲げるところにより CSIRT の体制を整備するものとする。

① 統括情報セキュリティ責任者、副統括情報セキュリティ責任者、情報主管課長及び情報主管課を CSIRT とする。

② 統括情報セキュリティ責任者を CSIRT 責任者、副統括情報セキュリティ責任者を CSIRT 副責任者、情報主管課長を CSIRT 管理者とする。

③ CSIRT 責任者は、情報セキュリティインシデントに対し必要かつ十分な措置を CSIRT 管理者に指示する。

④ CSIRT 副責任者は、CSIRT 責任者を補佐する。また、情報セキュリティインシデントの公表について、情報セキュリティインシデントが発生した部局（以下「インシデント発生部局」という。）に対し指示及び支援を行う。

⑤ CSIRT 管理者は、CSIRT 責任者の指示のもと、情報セキュリティインシデントに対し必要かつ十分な措置を行う。

⑥ CSIRT 管理者は、情報セキュリティに関して県内市町村、関係機関及び委託事業者等との情報共有を行う。

⑦ CSIRT 管理者は、県内市町村から情報セキュリティインシデントの報告を受けた場合は、必要に応じ回復のための支援を行う。

(11) 標準準拠システム等をクラウドサービス上で利用する際の組織体制

情報主管課長及び情報システム管理者は、標準準拠システム等をクラウドサービス上で利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

第３章　情報資産の分類と管理

３．１　情報資産の管理責任

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について管理責任を有する。

３．２　情報資産の分類

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について、別に定める実施手順に基づき、表１、表２及び表３に定める機密性、完全性、可用性に関する基準により分類を行うものとする。

表１　機密性による情報資産の分類

分類	分類基準
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する情報資産

機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産
機密性１	機密性２又は機密性３の情報資産以外の情報資産

表２　完全性による情報資産の分類

分類	分類基準
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適正な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
完全性１	完全性２の情報資産以外の情報資産

表３　可用性による情報資産の分類

分類	分類基準
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失、又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
可用性１	可用性２の情報資産以外の情報資産

３．３　情報資産の管理

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産（クラウドサービスに保存される情報資産も含む。）の取り扱いについて管理方法を定め、情報資産の分類又はその内容に応じその取り扱いを制限しなければならない。また当該情報資産について、所属する職員等に対し、次に掲げるところ及び別に定める実施手順により取り扱うよう指導しなければならない。

（１）取り扱い制限の遵守

取り扱い制限のある情報資産を取り扱う場合は、これを遵守すること。

（２）情報の秘匿

情報をパソコン等機器又は電磁的記録媒体に保存する場合は、当該情報の情報資産の分類等に応じて、パスワード等による暗号化又は当該機器等の管理区域への保管等の方法によりこれを秘匿すること。

（３）作成途中の情報の管理

機密性２以上の情報について、作成途中であっても紛失や流出等を防止し、作成途中で不要になった場合は、これを消去すること。

（４）他所属が所管する情報資産の取り扱い

他の所属が所管する情報資産について、当該他所属が定めた情報資産の分類に基づき取り扱うこと。

（５）情報資産の廃棄等

情報資産を廃棄やリース返却等を行う場合は、次に掲げるところにより行うこと。

① 当該媒体を所管する情報セキュリティ管理者又は情報システム管理者の許可を得ること。

② 記録されている情報の機密性に応じ、情報資産の情報を復元できないように処置すること。
③ 行った処理について、日時、担当者及び処理内容等を記録すること。
④ 標準準拠システム等のクラウドサービス上での利用における全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理すること。

３．４　パソコン等機器、電磁的記録媒体及びソフトウェアの管理

（1）パソコン等機器、電磁的記録媒体及びソフトウェアの管理

情報セキュリティ管理者及び情報システム管理者は、所管するパソコン等機器、電磁的記録媒体及びソフトウェアの管理について、次に掲げるところにより行うものとする。

① パソコン等機器及び電磁的記録媒体の貸出及び返却について、記録を作成し保管しなければならない。
② ソフトウェアについて、そのライセンスを適切に管理しなければならない。また、開発元のサポートが終了したソフトウェアについては、原則として速やかにその使用を終了しなければならない。さらに、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。
③ パソコン等機器を情報主管課が所管する山形県基幹高速通信ネットワーク（以下「基幹ネットワーク」という。）に接続しようとする場合は、情報主管課長の承認を得なければならない。
④ マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。
⑤ その他情報セキュリティの確保のために必要な措置を講じなければならない。

第４章　情報システム全体の強靭性の向上

４．１　マイナンバー利用事務系

（1）マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWANを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

（2）情報のアクセス及び持ち出しにおける対策

① 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

② 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（3）マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、他の領域とはネットワークを分離しなければならない。

（4）マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

４．２　LGWAN 接続系

（1）LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

① サニタイズ処理方式（ファイルを一旦分解した上で、ウィルスが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し分解前と同様のファイル形式に復元する方法）

② インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

（2）LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をLGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

４．３　インターネット接続系

（1）インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びLGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

第５章　物理的セキュリティ

情報システム管理者は、所管する情報システムに係る物理的セキュリティを確保するため、次に掲げるところにより対策を講じるものとする。

５．１　機器等の管理

（1）機器の設置場所

サーバ等機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除

した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（2）サーバの冗長化等

① 可用性２の情報を格納しているサーバについて、仮想基盤上で稼動させる等により、物理サーバに障害が発生した際にも情報システムの運用停止時間を最小限にする措置を講じなければならない。

② 完全性２又は可用性２の情報を格納しているサーバ等機器又は電磁的記録媒体について、ミラーリング（データの複製を別の場所に同期させ保存することをいう。）等により当該情報を保持しなければならない。

（3）機器の電源

サーバ等機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電源を供給する容量の予備電源を備え、落雷等による過電流に対して情報を保護するための措置を講じなければならない。

（4）通信ケーブル等の配線

① 通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収容管を使用する等必要な措置を講じなければならない。

② 主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合は、速やかに修復等の対応を行わなければならない。

（5）機器の定期保守及び修理

① 可用性２の情報を格納しているサーバ等機器については、定期保守を実施しなければならない。

② サーバ等機器又は電磁的記録媒体を事業者等に修理させる場合は、内容を消去した状態で行わせなければならない。内容を消去できない場合は、修理にあたり、当該事業者等と守秘義務契約を締結する他、秘密保持体制の確認等を行わなければならない。

（6）庁舎外への機器の設置

庁舎外にサーバ等機器を設置する場合は、情報主管課長の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（7）機器の廃棄

① サーバ等機器及び電磁的記録媒体の廃棄又はリース返却をする場合は、当該機器等から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。また、これに係る廃棄等の記録を作成し保管しなければならない。

② パソコン等機器及びサーバ等機器を廃棄する場合は、山形県財務規則（昭和 39 年山形県規則第９号）のほか、関係法令等を遵守するよう留意すること。

③ 標準準拠システム等のクラウドサービス上での利用におけるクラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする場合は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

５．２　管理区域の管理

（1）管理区域の構造等

① 管理区域とは、機密性２以上、可用性２又は完全性２の情報を取り扱う情報システムを設置し、管理及び運用を行うための部屋又は機密性２以上の情報が記録された電磁的記録媒体を保管する場所

をいう。

② 管理区域の出入り口は必要最小限とし、鍵等によって許可されていない立ち入りを防止しなければならない。

③ 管理区域内のパソコン・サーバ等に、転倒及び落下防止等の措置を講じなければならない。

（2）入退室管理

① 管理区域の出入りについて、IC カード等又は入退室簿への記載等により管理しなければならない。

② 管理区域へ入る者に対し、身分が識別できるよう、ネームプレートの着用等を義務付けなければならない。

③ 機密性２以上の情報を取り扱う情報システムを設置している管理区域について、管理区域へ入る者に対し、当該情報システムに関する業務に不要なパソコン等機器、通信回線装置及び電磁的記録媒体等（当該者が所管するものを含む。）を持ち込ませないようにしなければならない。

（3）機器の搬入出

① 管理区域へ搬入するパソコン・サーバ等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。

② 管理区域のパソコン・サーバ等及び電磁的記録媒体の搬入出について、職員を立ち会わせなければならない。

５．３　ネットワークの管理

（1）関連文書の保管

ネットワークに関連する文書を適切に保管しなければならない。

（2）ネットワーク接続の制限

外部のネットワークへの接続を必要最低限に限定し、可能な限り接続ポイントを減らすよう努めなければならない。

（3）通信回線の選択及び情報の暗号化

機密性２以上の情報を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（4）機密性及び完全性の確保

機密性２以上又は完全性２の情報を取り扱う情報システムのネットワークに使用する回線について、伝送途上で情報が破壊・盗聴・改ざん・消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（5）可用性の確保

可用性２の情報を取り扱う情報システムが接続される通信回線について、求められる安定性を満たすものを選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない

第６章　人的セキュリティ

６．１　職員の遵守事項

（1）職員の遵守事項

職員は、次に掲げる項目を遵守するものとする。

① 情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシー及び実施手順等を遵守するとともに自らの役割及び責任を意識しなければならない。

② 業務上必要のない情報を作成・入手・利用してはならない。

③ 業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールの使用及びインターネットへのアクセスを行ってはならない。

④ 機密性２以上又は完全性２の情報資産を外部に持ち出し、又は送信等する場合は、当該情報資産を所管する情報セキュリティ管理者又は情報システム管理者の承認を得た上で取り扱い制限に従うとともに、格納されている情報の暗号化等の処理を行わなければならない。

⑤ 庁舎外で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得なければならない。

⑥ 庁舎外から持ち帰ったパソコン等機器をネットワーク及び情報システムに接続する前に、不正プログラム対策ソフトウェアによるチェックを行なわなければならない。

⑦ 私物のパソコン・サーバ等又は電磁的記録媒体を、ネットワーク及び情報システムに接続してはならない。ただし、在宅勤務職員がリモート接続システムにより接続する場合は、実施手順に従い利用することができる。

⑧ パソコン等機器を公衆無線 LAN 等（不特定多数に利用させることを目的に提供されている無線 LAN 環境をいう。）へ接続してはならない。

⑨ パソコン等機器について、その仕様を変更又はソフトウェアをインストールする場合は、当該機器を所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。

⑩ 情報主管課からパソコン等機器の情報セキュリティに関する修正プログラムが配布された場合は、速やかに当該パソコン等機器へ適用しなければならない。

⑪ ソフトウェアを不正に利用してはならない。

⑫ 電磁的記録媒体等をパソコン・サーバ等に接続する際は、不正プログラム対策ソフトウェアによる当該媒体のチェックを行わなければならない。

⑬ 使用しているパソコン等機器が不正プログラムに感染した場合は、直ちに LAN ケーブルの取り外し又は通信を行わない設定への変更等によりネットワークから切り離すとともに、「6.6.情報セキュリティインシデントの報告及び対応」に掲げるところにより報告等を行わなければならない。

⑭ 情報資産を第三者に使用閲覧等されることがないよう、離席時にはパソコン等機器のスクリーンセーバー設定及び操作のロックを行わなければならない。また、電磁的記録媒体及び文書等を容易に閲覧等されない場所に保管しなければならない。

⑮ 電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに当該情報を消去（消去できない場合は当該媒体内の全ての情報について保存される必要がなくなった時点で破棄）しなければならない。

⑯ 入出力した文書をコピー機、ＦＡＸ又はプリンタ等に放置してはならない。

⑰ 差出人が特定できない又は不自然なファイルが添付されている等の不審な電子メールを受信した場合は、「6.6.情報セキュリティインシデントの報告及び対応」に掲げるところにより報告等を行わなければならない。

⑱ 自動転送機能を用いて、電子メールを転送してはならない。

⑲ 業務上必要のない送信先に電子メールを送信してはならない。

⑳ 複数人に電子メールを送信する場合は、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
㉑ 異動、退職等により業務を離れる場合は、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

６．２　非常勤職員への対応

（１）非常勤職員への適用

情報セキュリティポリシーは、非常勤職員に対しても適用するものとする。

（２）非常勤職員への対応

情報セキュリティ管理者は、非常勤職員の情報セキュリティポリシーの遵守について、次に掲げるところにより行うものとする。

① 採用の際は、情報セキュリティポリシーのうち、非常勤職員が守るべき内容を理解させなければならない。
② 採用の際は、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めなければならない。

６．３　情報セキュリティのポリシー等の掲示

CISOは、職員等が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならない。

６．４　委託事業者に対する説明

情報システム管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

６．５　情報セキュリティに関する研修

（１）研修の実施

① 統括情報セキュリティ責任者は、山形県組織全体の情報セキュリティ向上のため、山形県として必要な教育内容・研修計画を定め、教育・啓発活動を実施しなければならない。
② 統括情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施しなければならない。

（２）研修の受講

① 職員等は、情報セキュリティ教育の重要性を認識し、必要と定められた研修を受講しなければならない。
② 情報セキュリティ管理者は、所属職員等に対し、その業務に応じた情報セキュリティ教育・啓発に関する研修等を受講できる環境づくりに努めなければならない。

６．６　情報セキュリティインシデントの報告及び対応等

情報セキュリティインシデントが発生した場合の報告及び対応等は、次に掲げるところにより行うものとする。

（１）情報セキュリティインシデントの報告及び対応

① 職員等は、情報セキュリティインシデントを認知した場合は速やかに自らが所属する情報セキュリティ管理者に報告し、その指示に従わなければならない。
② 情報セキュリティ管理者は、情報セキュリティインシデントを認知した場合は速やかに情報主管課長に報告するとともに、当該インシデントが情報システムに関連する場合は、速やかにこれを所管する情報システム管理者に報告しその指示に従わなければならない。また、緊急性及び重要性に応じて情報セキュリティ責任者に報告しなければならない。
③ 情報システム管理者は、情報セキュリティインシデントを認知した場合は、速やかに情報主管課長にその旨を報告するとともに、情報主管課長の指示のもと、適切な対応に努めなければならない。また、緊急性及び重要性に応じて情報セキュリティ責任者に報告しなければならない。
④ 情報主管課長は、情報セキュリティインシデントを認知した場合は、その状況を確認し、緊急性及び重要性に応じて統括情報セキュリティ責任者及び副統括情報セキュリティ責任者に報告を行うとともに、統括情報セキュリティ責任者の指示又は自らの判断のもと、当該インシデントに係る情報セキュリティ管理者及び情報システム管理者に対し、被害拡大防止及び復旧のための対策を指示し、又は自らこれを講じなければならない。
⑤ 統括情報セキュリティ責任者は、情報セキュリティインシデントの報告を受けた場合はその状況を確認し、被害拡大防止及び復旧のための対策について情報主管課長に対し指示しなければならない。また、その内容についてCISOに報告しなければならない。

（2）情報セキュリティインシデントの公表

情報セキュリティインシデントについて外部公表を行う場合は、次に掲げるところにより行うものとする。
① 副統括情報セキュリティ責任者は、インシデント発生部局における「山形県広報広聴事務取扱要綱」の規定による報道監（以下「発生部局の報道監」という。）に対し、外部公表に係る指示及び支援を行わなければならない。
② 外部公表は、発生部局の報道監が行うものとし、その内容について副統括情報セキュリティ責任者に報告しなければならない。
③ 副統括情報セキュリティ責任者は、公表した内容について統括情報セキュリティ責任者に報告しなければならない。

（3）関係機関等との連携

情報主管課長は、当該情報セキュリティインシデントが不正アクセス禁止法違反等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との密接な連携に努めなければならない。

（4）情報セキュリティインシデントの原因究明・記録等

情報主管課長並びに発生した情報セキュリティインシデントに係る情報セキュリティ管理者及び情報システム管理者は、互いに連携して当該インシデントの原因を究明するとともに、その内容、原因、処理結果等を記録し、適切に保存しなければならない。

（5）情報セキュリティインシデントの再発防止

① CISOは、情報セキュリティインシデントの報告を受けた場合は、その内容を確認し、統括情報セキュリティ責任者に対し再発防止策を実施するために必要な措置を指示しなければならない。
② 統括情報セキュリティ責任者は、CISO の指示のもと、再発防止のための対策について情報セキュリティ責任者に対し指示し、又は自らこれを行わなければならない。また、その内容についてCISO

に報告しなければならない。

③ 情報セキュリティ責任者は、再発防止の対策について指示を受けた場合はこれを実施し、その内容について統括情報セキュリティ責任者へ報告しなければならない。

６．７　ＩＤ及びパスワード等の取り扱い

職員等は、ID、パスワード及びICカード等の取り扱いについて、次に掲げるところにより行うものとする。

（１）ID及びパスワードの取り扱い

① 自己の管理するＩＤ及びパスワードを、他人に利用させてはならない。

② 情報システム等でやむを得ずＩＤ及びパスワードを共用利用する場合は、共用利用者以外に利用させてはならない。

③ パスワードは秘密にし、パスワードを記載したメモ等を第三者が容易に閲覧できる場所に掲示等してはならない。また、業務上必要がなくなった場合は速やかにこれを廃棄しなければならない。

④ パスワードは十分な長さとし、文字列は他人が容易に想像できないものにしなければならない。

⑤ ID及びこれに係るパスワードが流出した、又はそのおそれがある場合は、速やかにパスワードを変更するとともに、「6.6.情報セキュリティインシデントの報告及び対応」に掲げるところにより報告等を行わなければならない。

⑥ 情報システム管理者から与えられた仮のパスワード（初期パスワード含む）について、情報システムへ初めてログインした時点で変更しなければならない。

⑦ パソコン等機器のパスワードの記憶機能について、情報主管課より提供された以外のものを使用してはならない。

（２）ICカード等の取り扱い

① ICカード等を業務上必要のない者に貸し出してはならない。

② ICカード等をパソコン等機器に接続したまま離席してはならない。

③ ICカード等を紛失した場合は、「6.6.情報セキュリティインシデントの報告及び対応」に掲げるところにより報告等を行わなければならない。

第７章　技術的セキュリティ

７．１　機器及びネットワークの管理

（１）機器及びネットワークの管理

情報システム管理者は、所管する情報システムについて、次に掲げるところにより機器及びネットワークの管理等を行うものとする。

① 業務システムのデータベースやサーバ等機器に記録された情報について、当該機器の冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。また、標準準拠システム等のクラウドサービス上での利用において、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が要件を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、

自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

② 情報システムの運用において実施した作業について、作業記録を作成し適切に管理しなければならない。

③ 情報システムの変更等の作業を行った場合は、作業内容について記録を作成するとともに、これを漏えいし、又は改ざん若しくは消去等されないよう適正に管理しなければならない。

④ 情報システムの仕様書及びネットワーク構成図について、記録媒体に関わらず、業務上必要とする者以外の者の閲覧、紛失等がないよう、適正に管理しなければならない。

⑤ 各種ログ及び情報セキュリティの確保に必要な情報を取得するとともに、これを改ざん及び誤消去されないよう必要な措置を講じた上で、一定の期間保管しなければならない。

⑥ ログとして取得する項目、保存期間及び取り扱い方法等について定め、適正にログを管理しなければならない。

⑦ 悪意ある第三者等からの不正侵入及び不正操作等の有無について、取得したログを必要に応じて点検又は分析しなければならない。なお、標準準拠システム等をクラウドサービス上での利用の際には、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

⑧ 標準準拠システム等のクラウドサービス上での利用において、情報セキュリティ監査等のために必要となった場合のクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

⑨ 職員等からの情報システムに関する障害の報告及びその処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

⑩ フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等の設定情報を管理しなければならない。

⑪ 不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

７．２　外部ネットワーク等との接続

（１）外部ネットワーク等との接続

情報システム管理者は、所管する情報システムについて外部のネットワーク及び情報システム（以下「外部ネットワーク等」という。）との接続を行う場合は、次に掲げるところにより行うものとする。

① 基幹ネットワークを外部ネットワーク等と接続する場合は、情報主管課長の承認を得た上でこれを行わなければならない。

② 接続しようとする外部ネットワーク等に係るネットワーク構成、機器構成及び情報セキュリティ技術等を調査しなければならない。

③ 接続した外部ネットワーク等の管理者の瑕疵によりデータの漏えい・破壊・改ざん・消去等又は情報システムの停止等による業務への影響が生じた場合に対処するため、当該外部ネットワーク等の管理者による損害賠償責任を契約上担保しなければならない。

④ ウェブサーバ等をインターネット上に公開する場合、庁内ネットワークへの侵入を防御するため

に、ファイアウォール等を外部のネットワークとの境界に設置した上で接続しなければならない。

⑤ 接続した外部ネットワーク等のセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合は、速やかに当該外部ネットワークを遮断しなければならない。

７．３　無線 LAN の盗聴対策

情報システム管理者は、所管する情報システムにおいて無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

７．４　電子メールのセキュリティ管理及び利用制限

情報主管課長が所管する電子メールのセキュリティ管理及び利用制限は、次に掲げるところによるものとする。

（１）電子メールのセキュリティ管理

情報主管課長は、電子メールのセキュリティ管理等について、次に掲げるところにより行うものとする。

① 権限のない利用者により、基幹ネットワークを経由した外部から外部への電子メールの中継処理が行われることを不可能とするよう、メールサーバの設定を行わなければならない。

② スパムメール等が内部から送信されていることを検知した場合は、必要に応じてメールサーバの運用を停止しなければならない。

③ 電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ 所管するドメインについて、外部の者により詐称されないよう送信ドメインの認証を行わなければならない。

⑤ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取込む場合は無害化しなければならない。

（２）電子メールの利用制限

情報システムの開発、運用又は保守等のため庁舎内に常駐している委託事業者等による電子メールアドレスの利用は原則禁止とする。ただし、業務上やむを得ないと情報主管課長が認めた場合はこの限りではない。

７．５　Web 会議サービスの利用時の対策

Web 会議サービスの利用にあたっては、別に定める実施手順に従い、情報セキュリティ対策を実施しなければならない。

７．６　ソーシャルメディアサービスの利用

ソーシャルメディアサービスの利用にあたっては、別に定める実施手順を遵守しなければならない。

７．７　アクセス制御

（１）情報システム管理者によるアクセス制御等

情報システム管理者は、所管する情報システムへのアクセス制御等について、次に掲げるところに

より行うものとする。

① 情報システムで取り扱う情報資産の分類又はその内容に応じ、アクセス権限を有する職員等及びその権限の内容を、必要最小限としなければならない。

② アクセスする権限のない職員等がアクセスできないよう、IC カード等又はユーザ ID 等によりシステム上制限しなければならない。

③ 利用者の登録、変更及び抹消等の情報管理並びに職員等の異動、出向及び退職等に伴うユーザ ID の取り扱い等の方法を定めなければならない。

④ 管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID 及びこれに係るパスワードの漏えい等が発生しないよう厳重に管理しなければならない。

⑤ 職員等の認証に関する情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

⑥ 認証情報の不正利用を防止するための措置を講じなければならない。

⑦ 所管する情報システムの情報資産の分類又はその内容に応じて、適正な強度のログインパスワードを設定し、定期的に変更しなければならない。

⑧ 外部のネットワークからのアクセスを認める場合、通信途上の盗聴を防御するために通信の暗号化等の措置を講じなければならない。

⑨ 特権によるネットワーク及び情報システムへの接続時間を必要最小限とするよう努めなければならない。

（2）職員等による外部からのアクセス等の制限

情報セキュリティ管理者は、職員等による外部のネットワークからのアクセス等について、次に掲げるところにより行わなければならない。

① 職員等に外部からネットワーク又は情報システムへアクセスさせる場合は、当該システムを所管する情報システム管理者の承認を得なければならない。

② ネットワーク又は情報システムに対する外部からのアクセスを、これを必要とする合理的理由を有する最小限の者に限定しなければならない。

７．８　システム開発・導入・保守等

情報システム管理者は、情報システムの開発・導入・保守等について、次に掲げるところにより行うものとする。

（1）情報システムの調達

① 情報システムに係る開発・導入・保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 機器又はソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（2）情報システムの開発

① 開発に使用する ID を適切に管理し、開発完了後に不要となる場合は、これを消去しなければならない。

② 開発に用いるハードウェア及びソフトウェアについて、情報セキュリティ上問題のないことを確認しなければならない。

③ 利用を認めた以外のソフトウェアが情報システムに導入されている場合は、これを消去しなければならない。

（3）情報システムの導入

① 情報システムの開発、保守及びテスト環境と運用環境を可能な限り分離しなければならない。

② 情報システムの開発・保守計画の策定時にシステム運用環境への移行の手順を明確にしなければならない。

③ 移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う業務への影響が最小限になるよう配慮しなければならない。

④ 導入する情報システム又はサービスに求められる可用性を満たすことを確認した上で導入しなければならない。

⑤ 導入する情報システム又はサービスを既に稼動している情報システムに接続する前に十分な試験を行わなければならない。またこの場合において、機密性２以上の情報を試験に使用してはならない。

（4）情報システムの開発・保守に関する資料の保管

情報システムの開発・保守に関する資料を適正に整備・保管しなければならない。

（5）入出力データの正当性の確保

① 情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列の入力を除去する機能が組み込まれるよう、情報システムを設計しなければならない。

② 故意又は過失による情報の漏えい・破壊・改ざん・消去等のおそれがある場合に、これを検出するチェック機能が組み込まれるよう、情報システムを設計しなければならない。

③ 情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるよう、情報システムを設計しなければならない。

（6）変更管理

情報システムの変更をした場合は、プログラム仕様書等の変更履歴を作成しなければならない。

（7）開発・保守用のソフトウェアの更新等

開発・保守用のソフトウェアを更新又はこれにパッチを適用する場合は、関連する他の情報システムへ影響を与えることがないよう、その整合性を確認しなければならない。

（8）システム更新又は統合時の検証等

情報システムを更新又は統合する際は、長時間停止や誤作動による業務への影響が生じないよう、更新等の前にその体制及び計画等について検証等を行わなければならない。

７．９　不正プログラム対策

（1）情報主管課長による対策

情報主管課長は、不正プログラム対策について、次に掲げるところにより行うものとする。

① 外部ネットワーク等から送受信するファイルは、基幹ネットワークのゲートウェイにおいて不正プログラムのチェックを行い、これの基幹ネットワークへの侵入及び外部への拡散を防がなければならない。

② 不正プログラムに関する情報を収集し、必要に応じ職員等に対して注意喚起を行わなければならない。

（2）情報システム管理者による対策

情報システム管理者は、所管する情報システムの不正プログラム対策について、以下に掲げるところにより行うものとする。

① ネットワーク接続を要する情報システムにおいて、パソコン・サーバ等に、不正プログラム対策ソフトウェアを常駐させるとともに、不正プログラムのパターンファイル等を常に最新の状態に保たなければならない。

② ネットワークに接続しない情報システムにおける電磁的記録媒体の使用について、使用を認めた以外のものを職員等に利用させてはならない。

③ ネットワークに接続しない情報システムにおいて、不正プログラムの感染及び侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

④ 不正プログラム対策ソフトウェアを導入しているパソコン・サーバ等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

⑥ 標準準拠システム等のクラウドサービス上での利用において、仮想マシンを設定する際には不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

7．10　不正アクセス対策

（1）基幹ネットワークの不正アクセス対策

情報主管課長は、基幹ネットワークの不正アクセス対策について、次に掲げるところにより行うものとする。

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を消去又は停止しなければならない。

③ 情報システムに攻撃を受けることが明確になった場合は、「5.6.情報セキュリティインシデントの報告及び対応等」に準じ、報告等及び情報システムの停止を含む必要な措置を講じるとともに、関係機関と連絡を密にして情報の収集、提供を行わなければならない。

④ 基幹ネットワーク内のパソコン・サーバ等に対する攻撃及びこれらからの外部ネットワーク等に対する攻撃を監視しなければならない。

⑤ 標準準拠システム等をクラウドサービス上で利用するにあたって、情報セキュリティポリシーにおける不正アクセス対策に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑥ 標準準拠システム等をクラウドサービス上で利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑦ パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、情報セキュリティポリシーを満たすことを確認しなければならない。

（2）サービス不能攻撃対策

情報システム管理者は、外部のネットワークからアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（3）標的型攻撃対策

電子メールに係る情報システムを所管する情報システム管理者は､所管するネットワークについて、標的型攻撃による不正プログラムの侵入を防止するために、自動再生無効化等の入口対策を講じなければならない。また、侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

7．11　セキュリティ情報の収集

（1）セキュリティ情報の収集

情報主管課長及び情報システム管理者は、セキュリティ情報の収集について、次に掲げるところにより行うものとする。

① セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

② 情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認知した場合は、情報セキュリティインシデントを未然に防止するための対策を速やかに講じなければならない。

③ 標準準拠システム等をクラウドサービス上での利用する際には、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

（2）不正プログラム情報の収集

情報主管課長は、不正プログラムに関する情報等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

第８章　遵守状況の確認

8．1　情報システムの監視

（1）情報システムの監視

情報システム管理者は、所管する情報システムの監視について、次に掲げるところにより行うものとする。

① セキュリティに関する事案を検知するため、情報システムを常時監視し、その記録を保存しなければならない。

② 重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

③ 標準準拠システム等をクラウドサービス上での利用する際には、必要となるリソースの容量・能力

が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

④ 標準準拠システム等をクラウドサービス上での利用する際には、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑤ 標準準拠システム等をクラウドサービス上での利用する際には、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

８．２　情報セキュリティポリシー遵守状況の確認

（１）情報セキュリティポリシー遵守状況の確認

① 情報セキュリティ管理者は、定期的又は必要に応じ所属職員等の情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合は、速やかに情報主管課長に報告しなければならない。

② 情報主管課長は、発生した問題について、適正かつ速やかに対処しなければならない。

③ 情報システム管理者は、ネットワーク及びサーバ等機器のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的又は必要に応じ確認を行い、問題がある場合は適正かつ速やかに対処しなければならない。

（２）機器等の利用状況調査

情報主管課長は、不正アクセス及び不正プログラム等の確認のため、パソコン等機器、電磁的記録媒体のログ及び電子メールの送受信記録等の利用状況を調査することができる。

第９章　障害時の対応

９．１　緊急時対応計画の策定

情報システム管理者は、緊急時対応計画の策定について、次に掲げるところにより行うものとする。

（１）緊急時対応計画の策定

① 情報セキュリティインシデントが発生した場合において連絡、証拠保全、被害拡大の防止、影響範囲の特定、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、発生時には当該計画に従って適正に対処しなければならない。

② 標準準拠システム等をクラウドサービス上での利用する際には、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従

って適正に対処しなければならない。

（2）緊急時対応計画に定める事項

緊急時対応計画には、次に掲げる内容を定めなければならない。

① 関係者の連絡先
② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

（3）緊急時対応計画の見直し

情報セキュリティを取り巻く状況の変化や組織体制の変動等に対し、必要に応じて緊急時対応計画の規定を見直さなければならない。

9．2　事業継続計画との整合

県が事業継続計画を整備する場合、本部は、当該計画と情報セキュリティポリシー等の整合性を検討し、必要に応じ情報セキュリティポリシーの見直しを行うものとする。

第10章　業務委託と外部サービスの利用

10．1　業務委託等

情報システム管理者は、業務委託等について、次に掲げるところにより行うものとする。

（1）委託等事業者の選定

① 委託等事業者の選定にあたり、委託等の内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。
② 情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託等事業者を選定しなければならない。

（2）契約時のセキュリティ要件

重要な情報資産を取扱う業務を委託する場合は、委託等事業者との間で必要に応じて次の情報セキュリティ要件を契約に含めなければならない。

① 山形県情報セキュリティポリシー及び実施手順の遵守
② 当該事業者の責任者、委託等の内容、作業者の所属、作業場所の特定
③ 提供されるサービスレベルの保証
④ 当該事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）での管理方法
⑤ 業務従事者に対する情報セキュリティ教育の実施
⑥ 提供された情報の目的外利用及び当該事業者以外の者への提供の禁止
⑦ 業務上知り得た情報の守秘義務
⑧ 再委託等に関する制限事項の遵守
⑨ 業務終了時の情報資産の返還、廃棄等
⑩ 業務の定期報告及び緊急時報告義務
⑪ 県による情報セキュリティに関する監査・検査の受け入れ

⑫ 情報セキュリティインシデント発生時の県による公表に対する同意
⑬ 情報セキュリティポリシーを遵守しなかったこと及び当該事業者の瑕疵による損害賠償等

（3）セキュリティ教育の実施状況の確認

委託先を含む関係者については委託先等で情報セキュリティに関する教育が行われていることを確認しなければならない。

10．2　外部サービスの利用（機密性２以上の情報を取り扱う場合）

外部サービスの利用（機密性２以上の情報を取り扱う場合）にあたっては、別に定める実施手順を遵守しなければならない。

10．3　外部サービスの利用（機密性２以上の情報を取り扱わない場合）

外部サービスの利用（機密性２以上の情報を取り扱わない場合）にあたっては、別に定める実施手順を遵守しなければならない。

第 11 章　法令遵守

11．1　法令遵守

（1）法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか、関係法令を遵守し、これに従わなければならない。

① 地方公務員法(昭和 25 年 12 月 13 日法律第 261 号)
② 著作権法（昭和 45 年法律第 48 号）
③ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
④ 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）
⑤ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
⑥ サイバーセキュリィティ基本法（平成 26 年法律第 104 号）
⑦ 個人情報の保護に関する法律施行条例（令和４年 12 月県条例第 37 号）

（2）情報システム管理者は、標準準拠システム等をクラウドサービス上での利用する際に、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

第 12 章　違反時の対応等

12．1　違反時の対応及び処分等

（1）違反時の処分

職員等の情報セキュリティポリシーに係る違反行為が認められるときは、当該職員等は発生した事

案の状況等に応じて、懲戒処分その他の処分の対象となる。

（2）違反時の対応

違反行為への対応は、次に掲げるところによるものとする。

① 職員等は、他の職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、速やかに当該職員等が所属する情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

② 情報セキュリティ管理者は、所属する職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、速やかに情報主管課長及び当該違反行為に係る情報システム管理者に報告するとともに、当該職員等に是正の指導を行わなければならない。

③ 情報主管課長及び当該違反行為に係る情報システム管理者は、所管する情報システムに関して職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、当該職員等が所属する情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

④ 情報セキュリティ管理者の指導によっても改善されない場合、情報システム管理者は、所管する情報システムについて、当該職員等の利用を停止することができる。

第13章　評価・見直し

13．1　情報セキュリティ監査

（1）情報セキュリティ監査の実施

情報セキュリティ監査は、次に掲げるところにより行うものとする。

① 山形県情報セキュリティ等監査員班は、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わなければならない。

② 山形県情報セキュリティ等監査員班は、情報セキュリティ監査に係る実施要綱を定めなければならない。

③ 被監査所属の情報セキュリティ管理者及び監査対象の情報システムを所管する情報システム管理者は、情報セキュリティ監査の実施に協力しなければならない。

13．2　自己点検

（1）自己点検の実施

情報セキュリティ対策に関する自己点検は、次に掲げるところにより行うものとする。

① 情報セキュリティ管理者は、情報セキュリティポリシーの運用及び管理状況について、定期的又は必要に応じ自己点検を行わなければならない。

② 情報システム管理者は、所管する情報システムについて、定期又は必要に応じ情報セキュリティ対策状況に関する自己点検を行わなければならない。

③ 情報セキュリティ管理者及び情報システム管理者は、自己点検実施後は点検結果と改善策を取りまとめ、自己の権限の範囲内で改善を図った上で、情報主管課長に報告しなければならない。

④ 情報主管課長は、報告を受けた点検結果について、情報セキュリティポリシーの見直しに活用しなければならない。

13．3　情報セキュリティポリシーの見直し

本部は、必要があると認めた場合は、情報セキュリティポリシーの運用状況を確認するとともに、その結果及び情報セキュリティに係る環境の変化等を踏まえ、その見直しを行うものとする。

第 14 章　例外措置

14．１　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合は、統括情報セキュリティ責任者の承認を得て、例外措置を講じることができる。

14．２　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、災害対応等行政事務の遂行に緊急を要し、例外措置をとることが避けられない場合は、事後速やかに統括情報セキュリティ責任者に報告しなければならない。

14．３　例外措置の記録

統括情報セキュリティ責任者は、情報セキュリティ管理者又は情報システム管理者により例外措置がとられた場合は、その内容について記録し、一定期間保管しなければならない。

第 15 章　実施手順

15．１　実施手順

本対策基準に定める事項のほか、情報セキュリティポリシーの運用にあたって遵守すべき実施手順のうち情報主管課長が所管するものは、別表のとおりとする。

15．２　実施手順の公開等

（１）実施手順の公開等

① 実施手順は、公にすることにより本県の行政運営に重大な支障を及ぼすおそれがあることから原則として非公開とする。

② 職員等以外の者がその業務の遂行上実施手順を参照する必要がある場合は、その者に対してのみこれを開示することができ、その者はこれに関して守秘義務を負うものとする。

第 16 章　委任

16．１　情報主管課長への委任

（１）情報主管課長への委任

次に掲げる事項については、情報主管課長に委任する。

① 県の組織に関する条例又は規則の改正に伴う本対策基準の規定の整備及び見直し

② 本対策基準別表の整備及び見直し

③ 本対策基準別表に掲げる実施手順の整備及び見直し

附則

本規程は、平成 20 年４月１日から施行する。

附則

本規程は、平成 21 年４月１日から施行する。

附則

本規程は、平成 22 年４月１日から施行する。

附則

本規程は、平成 23 年４月１日から施行する。

附則

本規定は、平成 28 年４月１日から施行する。

附則

本規定は、平成 29 年４月１日から施行する。

附則

本規定は、平成 31 年４月１日から施行する。

附則

本規定は、令和２年４月１日から施行する。

附則

本規定は、令和３年４月１日から施行する。

附則

本規定は、令和４年 10 月 25 日から施行する。

附則

本規定は、令和５年４月１日から施行する。

附則

本規定は、令和５年 10 月 11 日から施行する。

別表　実施手順

大分類	小分類	実施手順
情報資産	分類管理	情報資産の分類と管理に関する実施手順 （H23.3.31（H29.4.1 最終改正））
		電子情報の持ち出しに係る取扱基準 （H20.12.1（R5.4.1 最終改正））
物理的セキュリティ 人的セキュリティ 技術的セキュリティ	端末管理	情報系パソコン運用管理手順 （H22.8.31（H29.11.6 最終改正））
	イントラ情報システム	山形県庁イントラ情報システム利用要綱 （H20.8.14（R2.2.1 最終改正））
		山形県庁イントラ情報システム「サービス利用者の認証」

		の利用手順 （R2.4.1 最終改正）
		山形県庁イントラ情報システム「電子メール」の利用手順 （R2.2.1 最終改正）
		山形県庁イントラ情報システム「インターネット」の利用手順 （R4.12.22 最終改正）
		山形県庁イントラ情報システム「文書管理」の利用手順 （H26.4.1 最終改正）
		山形県庁イントラ情報システム「共有ワークスペース」の利用手順 （R2.2.1 最終改正）
		イントラ情報システム「セキュアファイル交換」の利用手順 （R2.2.1）
		インターネット接続に係る特定通信の利用手順 （R2.2.1）
		仮想ＰＣ運用管理手順 （R2.2.1）
	ネットワーク管理	山形県基幹高速通信ネットワーク外部機関利用要綱 （H16.9.10（R3.4.1 最終改正））
		山形県基幹高速通信ネットワーク外部機関接続要綱 （H17.7.1（R3.4.1 最終改正））
	テレワーク	テレワークにおける情報セキュリティ対策実施手順 （R2.12.14）
		在宅勤務制度(試行含む)に係るパソコン貸し出し要綱 （H29.8.1（R2.1.1 最終改正））
		山形県サテライトオフィス（試行含む）に係るパソコン貸し出し要綱 （R29.8.1（R2.1.1 最終改正））
		リモート接続システム利用要領 （R2.1.1（R5.4.1 最終改正））
		短期モバイル端末貸出要領 （H29.9.14（R5.4.1 最終改正））
		長期モバイル端末貸出要領 （H29.8.1（R5.4.1 最終改正））
	Web 会議サービス	Web 会議ツール「Zoom」利用要領 （R2.5.12（R5.4.1 最終改正））
	ソーシャルメディアサービス	山形県ソーシャルメディアサービスの利用に関する実施手順 （H28.4.1（H29.4.1 最終改正））
障害時の対応	情報システムの対応	情報資産に関する危機管理方針 （H14.3）
		山形県基幹高速通信ネットワーク障害対応マニュアル （H22.3.30（R3.4.1 最終改正））

外部サービスの利用	外部サービス	外部サービスの利用（機密性２以上の情報を取り扱う場合）に関する実施手順 （R5.10.11）
		外部サービスの利用（機密性２以上の情報を取り扱わない場合）に関する実施手順 （R5.10.11）
評価・見直し	情報セキュリティ監査	山形県情報セキュリティ監査実施要綱 （R4.7.11）

（参考資料）情報セキュリティポリシー関連規程について

情報セキュリティの確保のため特に遵守又は参照すべき主な関連規程について、下記に示す。

（1）関連規程のうち、情報主管課が所管するもの

大分類	小分類	関連規程
組織体制		山形県デジタル化推進本部設置要綱 （H12.9.26（R2.11.19最終改正））
情報資産	文書管理	山形県行政手続等における情報通信の技術の利用に関する条例 （H18.12.19）
物理的セキュリティ 人的セキュリティ 技術的セキュリティ	システム調達	山形県情報システム導入標準ガイドライン （R3.4.1（R4.10.25最終改正））

（2）関連規程のうち、情報主管課以外が所管するもの

大分類	小分類	関連規程
情報資産	情報公開	山形県情報公開条例 （H9.12.22（R4.12.23最終改正）、総務部）
	個人情報	個人情報の保護に関する法律施行条例 （R4.12.23、総務部）
	文書管理	山形県公文書管理規程 （R2.3.27（R5.4.1最終改正）、総務部）
		文書事務の手引 （H7.3.31（R2.11最終改正）、総務部）
		総合行政ネットワークにおける電子公文書取扱要領 （H16.1.6（R2.4.1最終改正）、総務部）
		電子メール及び電子掲示板を利用した電子文書取扱要領 （H16.1.6（R2.4.1最終改正）、総務部）
物理的セキュリティ 人的セキュリティ 技術的セキュリティ	インシデント対応	山形県広報広聴事務取扱要綱 （H9.4.1（R5.4.1最終改正）、総務部）
障害時の対応	危機管理	山形県危機管理要綱 （H17.4.1（R4.4.1最終改正）、防災くらし安心部）
		山形県大規模災害発生時の災害対策本部事務局活動マニュアル （R4.6最終改正、防災くらし安心部）
外部サービスの利用	ソーシャルメディアサービス	ソーシャル・ネットワーキング・サービスを利用した山形県広報活動ガイドライン （H28.2.17総務部）
違反時の対応	懲戒処分	懲戒処分の基準（R2.10.1最終改正、総務部） 懲戒処分の基準（R2.7.1最終改正、教育委員会）