

令和8年度いしかわ環境情報サイトリニューアル等委託業務仕様書

1 業務概要

1.1 委託業務名

いしかわ環境情報サイトリニューアル等委託業務

1.2 業務期間

契約締結日から令和9年3月19日(金)まで

1.3 業務の目的

石川県では、環境総合計画の改定を機に、いしかわ環境情報サイトをリニューアル再構築し、かつ本サイトに子ども向けコンテンツを追加し、学校教育等の場で活用することで、環境意識の醸成を図り、もって環境教育・環境学習を推進する。

1.4 業務概要

既存の石川県の環境ポータルサイト「いしかわ環境情報サイト」(URL:<https://ishikawa-ecoweb.pref.ishikawa.lg.jp/>)のリニューアル再構築と子ども向けコンテンツの追加等を行う。

本業務の遂行にあたっては、企画・情報設計、コンテンツ及び教材の制作、デザイン、システム開発、広報に至る一連の工程を統括する責任者が一元的に管理するものとする。

①既存サイトのリニューアル

- ・既存サイトを全面リニューアルする
- ・複数システムで運用されているコンテンツ管理機能を統合し、管理者が単一の管理画面で更新及び管理できる構成とすること。
- ・パソコン、タブレット、スマートフォンに対応したデザインとすること
- ・子どもから大人まで幅広い利用者が親しみやすいデザインとすること。
- ・利用者が「知る」「学ぶ」「体験する」行動につながる導線設計を行うこと。

②子ども向けコンテンツの追加

- ・教職員の指導を受け、授業の中で補助教材等として活用することを念頭に置き「地球温暖化対策」、「廃棄物・リサイクル対策」、「自然環境・生物多様性」、「生活環境の保全」の4分野毎に環境学習の教材を制作
- ・児童等が自主学習を行う際の使用できる教材やデータ、参考資料の紹介
- ・主に小学校高学年を想定

③広報・周知

(1)学校等への広報・周知

学校等教育機関の利用促進を図る観点で、SNS、チラシ、ポスター、メディア(テレビ、ラジオ、新聞など)を活用するなど、本サイトを効果的に広報・周知する方法を検討し、実施すること。なお、周知方法や内容については、事前に石川県と協議すること。

(2)市町、県民、企業、環境団体等への広報・周知

サイトのリニューアルを周知する観点で、SNS、チラシ、ポスター、メディア(テレビ、ラジ

オ、新聞等)を活用するなど、本サイトのリニューアルを効果的に広報・周知する方法を検討し、実施すること。なお、周知方法や内容については、事前に石川県と協議すること。

2 既存サイトのリニューアル

2.1 環境情報、イベント情報、活動報告の統合

- ・現在それぞれ別のコンテンツで管理している「環境情報」「イベント情報」「活動報告」を一つのコンテンツ基盤で管理できる構成とすること。
- ・カテゴリ・タグ・状態管理(下書き・公開・公開終了・掲載期間)等を活用し、内容に応じた表示制御を行える仕組みとすること

2.2 活動団体

- ・活動団体をジャンルごとに分類できること
- ・ジャンルを各所属と紐付けて管理できること。
- ・管理権限に応じた編集制御ができること。

2.3 既存サイトからコンテンツの移行

- ・既存サイトのコンテンツを新サイトへ移行すること。
- 移行対象・件数・方法(手動／自動)を提案書に明示すること。
- ・旧URLから新URLへのリダイレクト設定(石川県で実施)をすることから、検索エンジン評価・外部リンク・お気に入り等を可能な限り維持すること。

2.4 外部システム統合

現在、別システムで運用されているフードドライブ及び食べきり協力店について、次の要件を満たすこと。

- ・他コンテンツと管理画面を統一すること
- ・本サイトで一元管理できる構成とすること
- ・現在のシステムのデータ移行方針、地図、検索表示の方法を提案すること。

2.5 管理機能・権限管理

- ・管理者画面を統一し、運用負荷の低減を図ること
- ・管理者を所属単位で区分し、所属ごとに管理権限を設定すること。対象は現時点で4課(環境政策課、カーボンニュートラル推進課、資源循環推進課、自然環境課)。
- ・将来の組織改編(所属の統廃合・名称変更・追加)に対し、プログラム改修を要さず、設定操作のみで権限体系を追加・変更できること。

2.6 投稿申請・承認機能等

(1) 次の各コンテンツについて、サイト上で市町・団体等が投稿や登録申請が行え、管理者の承認後掲載される仕組みとすること。

- ・イベント情報: 市町・各団体等が投稿申請 → 管理者承認後に掲載
- ・活動団体 → 管理者承認後に掲載

- ・施設情報 → 管理者承認後に掲載
- ・食べきり協力店 → 企業・団体等が登録・更新申請 → 管理者承認後に掲載
- ・フードドライブ → 企業・団体等が登録・更新申請 → 管理者承認後に掲載

(2)管理者承認後、トップページに最新情報を自動表示する「新着表示機能」を実装すること。

- ・公開日が新しい順にトップページへ表示する。
- ・表示件数は最新5件とし、各記事のタイトルおよび公開日を表示する。
- ・新着情報は登録・更新後、自動的にトップページへ反映する。
- ・市町・団体・企業等による投稿又は登録申請から管理者承認・公開までのワークフローを、コンテンツ種別ごとに設定・運用できること。差戻し、修正依頼及び承認履歴の管理を含むこと。

2.7 意見募集フォーム(既存サイトにおける「みんなの広場」)

- ・スパム投稿対策、不正アクセス対策、自動送信対策を考慮した仕様を提案すること
- ・投稿の公開範囲、掲載可否(掲載前のチェック有無)とモデレーション運用を明示すること
- ・CAPTCHA 等を用いる場合も、Cookie、プライバシーへの配慮及び代替手段を確保すること。
- ・投稿データ(個人情報を含む場合)の取扱い・保管を明示すること

3 環境学習コンテンツの追加

3.1 環境学習の定義

環境教育等による環境保全の取組の促進に関する法律(平成 15 年法律第 130 号)第2条第3項における「環境教育」の定義による。

当サイトで提供するコンテンツは下記を想定している。

- ・主として小学校高学年が環境の授業等で利用する
- ・各分野ごとにクイズを作成する。

(各 10 問(20 ページ程度)をランダムに表示。内容は各所属と協議し決定すること。)

- ・問題の追加・修正は、県担当者が管理画面から行えること。

・石川県より提供する児童向けの環境動画3本(①石川県の大気と水、②カーボンニュートラルについて知ろう③石川の美しい海を守るために)を掲載するコンテンツを作成すること。

- ・児童が身近に感じられるよう、石川県における話題・地名等を取り上げること

・動画やイラスト等の視覚表現を活用し、児童の関心を引き出し、内容の理解を深めるようなものとする

- ・GIGA スクール構想によって整備された 1 人 1 台の学習者用端末情報やスマートフォン等から利用する際の親和性を考慮すること

・内容については、学校の教育現場での活用も想定していることから、環境分野の知識や指導方法に精通した者と連携して作成すること

- ・石川県の環境関連施設の紹介、県民の環境意識向上につながる構成を提案すること

4 利用目的別の導線設計

利用者の目的に応じて適切なコンテンツへ誘導するため、サイトの入口で「環境学習」と既存のポータルサイト機能である「環境情報検索」の2つの利用目的を明示的に分岐させること。

画面仕様(例)

- ・トップページのファーストビューに、以下の2つの主要導線を配置する
環境学習をしたい方
環境情報を調べたい方
- ・利用者が選択した目的に応じて、関連するコンテンツ一覧ページへ遷移できる構成とする
- ・2つの導線はボタンまたはカード形式で視覚的に識別しやすく配置し、利用者がサイトの主な利用目的を直感的に選択できるデザインとする

5 システム要件

5.1 利用する環境については以下のとおりとすること。

(1) 端末性能

一般的に販売されている端末(パソコン、タブレット、スマートフォン)の標準的な性能で本サイトを利用できること。

(2) OS

<パソコン>

サポート(延長サポートを含む。)継続中の Microsoft Windows、Mac OS のバージョンで利用できること。また、契約期間中に新しいバージョンがリリースされた場合、追加費用無しで対応できること。

<タブレット、スマートフォン>

iOS、Android の最新バージョンで利用できること。また、契約期間中に新しいバージョンがリリースされた場合、追加費用無しで対応できること。

(3) ブラウザ

「(2) OS」で標準搭載されるブラウザ及び国内シェアのあるブラウザ(Microsoft Edge、Google Chrome、Safari など)の最新バージョンで幅広く利用できること。また、契約期間中に新しいバージョンがリリースされた場合、追加費用無しで対応できること。

(4) ソフトウェア

原則として、ブラウザのみで本サービスを利用できることとし、事前に特別なアプリケーションをインストールする必要があること(スマートフォン利用者向けにアプリケーションのインストールが必要な場合を除く。)

一般的に公開されている各種プラグインのインストールが必要な場合は、その旨を明記し、併せて設定方法も明示すること。

(5) ディスプレイ

解像度 1280×768 以上のディスプレイで最適に表示できること。

(6) 同時アクセス

学校授業での利用を想定し、大量の同時アクセス(最大 150 人程度を想定)に対応できるものとする

(6)ドメイン要件等

一般的な利用環境において、5 秒以内にページを表示できるパフォーマンスを確保すること。

メンテナンス時間を除き、24 時間 365 日稼働すること。

24 時間監視体制が整備されていること。

システム用ドメインについては、県が指定するドメインを使用すること。

5.2 デザイン・コンテンツ制作

・アクセシビリティ、ユーザビリティに配慮し、サイトの利用者が見やすく使いやすい構成・デザインとすること。

アクセシビリティについては、日本産業規格 (JISX 8341-3:2016 高齢者・障害者等配慮設計指-情報通信における機器、ソフトウェア及びサービス-第3部:ウェブコンテンツ) の適合レベル AA に準拠すること。

- ・総務省「みんなの公共サイト運用ガイドライン」を踏まえること
- ・音声読み上げ・キーボード操作・色とコントラスト・文字拡大に対応すること
- ・公開前にアクセシビリティ試験を実施し、結果報告書を提出すること
- ・効果的な SEO 対策 (サーチエンジン最適化) を行うこと
- ・作成にあたって、階層図案とサイトマップ案を提出し、適宜、情報共有すること。
- ・将来的な事情変更への柔軟な対応を可能とするため、各コンテンツの軽微な修正は、各所属のシステム管理者が設定画面等から実施できる仕組みを提供すること。
- ・上記変更の際し、プログラム改修やベンダーによる作業を原則不要とすること。
- ・上記変更の際し、アクセシビリティ基準を満たしているか、各所属のシステム管理者が更新時に確認できる仕組みを提供すること
- ・ポータル部分と環境学習部分を通じて、配色・書体・キャラクター・図版のトーン&マナーを統一し、全体として一貫した世界観を構築すること。
- ・提案時に、トップページのデザイン案を1案以上提示すること。デザイン案は、本サイトが児童向け環境学習コンテンツと県民向け環境情報ポータルの双方の性格を有することを踏まえ、イラスト、図版、写真等の視覚表現を効果的に用い、児童にとって直感的に理解しやすく、学習意欲を喚起する構成とすること。あわせて、県民、教職員、企業、団体、市町等の幅広い利用者が利用する公共性の高いサイトであることに配慮し、過度に幼児的又は娯楽的な表現に偏ることなく、信頼性、視認性、情報探索性及び行政サイトとしての品位を備えたデザインとすること。

5.3 保守について

・サイトの構築にあたっては、保守管理経費が必要最低限となるよう配慮すること。提案の際には、次年度 (令和9年度) の保守予定額を明示すること。保守予定額には、OS 及びサーバ側プログラムの更新対応費用、監視体制運営費用、問合せ対応費用及び障害発生時の原因調査・復旧対応費用を含めること。

- ・毎月1日から月末までのサイト閲覧数、ページ毎・カテゴリー毎のアクセス数等のログの集計、ユニークユーザー数、滞在時間、参照元、ページビュー数等を把握できるようにすること
- ・構築したサイトについて、管理者(県担当者)用のマニュアルを作成すること
- ・要件定義書、設計書、保守期間、障害対応時間(受付・復旧目標＝SLA)を提案すること
- ・問合せ窓口、エスカレーション体制を掲示すること
- ・業務終了後、県において、軽微なサイト構成の変更が行えるよう、可変性を持たせた構成とすること。
- ・再委託を行う場合は、その範囲・相手方・理由を提案書に明示すること。企画、情報設計、システムの設計・開発及び主要コンテンツの制作その他の中核的業務については、原則として受託者自らが実施すること。また、構築期間中及び保守期間中、県との対面による協議・打合せに柔軟に対応できる体制を有すること。

5.4 その他

(1) 個人情報の保護

- ・本業務の遂行にあたって、個人情報の滅失、漏洩又は既存の防止その他個人情報保護に必要な措置を講ずるとともに、別記「個人情報の取扱いに係る特記事項」を遵守するものとする。
- ・ただし、業務の実態に即して、契約締結時に協議のうえ、適宜必要な事項を追加し、また不要な事項を削除するものとする。

(2) セキュリティ

- ・本業務の遂行にあたっては、別記「石川県情報調達共通特記仕様書(令和8年6月版)」および「石川県サーバ統合基盤利用仕様書(令和5年8月版)」を遵守すること。今年度中に統合基盤の移行が予定されているため、「新サーバ統合基盤移行マニュアル」を参照して対応すること。(別途送付するため、必要な場合は連絡すること)
- ・脆弱性診断の実施、WAF・不正アクセス対策、ログ取得・保全を行うこと
- ・個人情報を取り扱う機能(各種申請・フォーム)について、取得・利用・保管・廃棄の方針を明示すること
- ・データのバックアップ方針(頻度・保存世代・復旧目標)を明示すること
- ・セキュリティパッチ・CMS バージョンアップ対応の方針を提案すること
- ・本業務で採用するCMSその他のソフトウェア(オープンソースソフトウェアを含む。)について、受託者は、当該ソフトウェア自体に起因する不具合・脆弱性を含め、構築するシステム全体の動作保証及び契約不適合責任を負うこと。プラグイン、テーマ、ライブラリ等の第三者が開発したコンポーネントを利用する場合も同様とし、責任をCMS開発元等の第三者に転嫁しないこと。
- ・採用するCMS及び利用する全コンポーネントについて、契約期間及び次年度以降の保守期間を通じ、セキュリティパッチ及びバージョンアップを継続的に提供・適用できる体制を確保すること。サポートが終了し、又は更新提供が不確実なコンポーネントに依存しないこと。
- ・採用するCMSの選定理由、ライセンス条件、サポート提供元及び脆弱性情報の入手経路を提案書に明示すること。脆弱性発見時の対応手順並びに初動及び恒久対応の目標時間(SL

A)を提案書に示すこと。

- ・情報セキュリティ事象の記録(ログ等)を取得し、保管期限は1年以上とすること。

(3)業務完了報告

- ・要件定義書、設計書、テスト報告書、操作マニュアル、公開サイト一式、移行結果報告書等を提出すること。

- ・管理者向けの操作研修を実施すること(回数、形式は提案者の任意)

- ・令和9年3月19日に業務完了報告書を提出すること

個人情報の取扱いに係る特記事項

(趣旨)

第1 乙は、個人情報の保護の重要性を認識し、この契約による事務の実施に当たっては、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 乙は、この契約による事務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。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。

2 乙は、この契約による事務に従事している者に対して、在職中及び退職後においてもこの事務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならないことその他個人情報の保護に関し必要な事項を周知するものとする。

(取得の制限)

第3 乙は、この契約による事務を行うため個人情報を取得するときは、その事務の目的を明確にし、当該目的の達成のために必要な範囲内で、適法かつ適正な方法により取得しなければならない。

(適正管理)

第4 乙は、この契約による事務に関して知り得た個人情報の漏えい、滅失又はき損の防止その他の個人情報の適切な管理のために個人情報の取扱責任者の設置等の管理体制の整備など、必要な措置を講じなければならない。

(従事者の監督)

第5 乙は、その従事者に個人情報を取り扱わせるに当たっては、当該個人情報の適正な管理が図られるよう、当該従事者に対する必要な監督を行わなければならない。

(目的外利用及び提供の禁止)

第6 乙は、この契約による事務に関して知り得た個人情報を、契約の目的以外の目的のために利用し、又は第三者に提供してはならない。ただし、あらかじめ甲の書面による指示又は承諾を受けたときは、この限りではない。

(複写又は複製の禁止)

第7 乙は、この契約による事務を行うため甲から提供を受け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。ただし、あらかじめ甲の書面による承認を受けたときは、この限りでない。

(再委託の禁止)

第8 乙は、この契約による個人情報を取り扱う事務について、第三者に再委託し、又は下請させてはならない。ただし、あらかじめ甲の書面による承認を受けたときは、この限りではない。

2 乙は、甲の承諾により第三者に個人情報を取り扱う事務を再委託し、又は下請させる場合には、甲が乙に求めた個人情報の保護に関し必要な措置と同様の措置を当該第三者に書面により求めるものとする。

(資料等の返還等)

第9 乙は、この契約による事務を行うため甲から提供を受け、又は乙自らが取得し、若しくは作成した個人情報が記録された資料等は、本契約終了後直ちに甲へ返還しなければならない。ただし、甲が書面により別に指示したときは、その指示に従うものとする。

2 乙は、この契約による事務により保有する個人情報については、本契約終了後直ちに消去し、又は廃棄しなければならない。ただし、甲が書面により別に指示したときは、その指示に従うものとする。

(管理状況の報告等)

第10 甲は、乙がこの契約による事務を行うに当たり、個人情報の取扱責任者の設置及びその他個人情報の管理状況について報告を求め、又は調査をすることができるものとする。

(事故報告)

第11 乙は、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、直ちにその状況を甲に通知し、適切な措置をとらなければならない。また、調査結果を遅滞なく甲に報告しなければならない。

(指示)

第12 甲は、乙がこの契約による事務を行うために取り扱っている個人情報の管理状況について、不適切と認められるときは、乙に対して必要な指示を行うことができる。

注1 「甲」は、委託者である知事、「乙」は受託者をいう。

2 委託の事務の実態に即して、適宜必要な事項を追加し、また不要な事項を削除するものとする。

石川県情報調達共通特記仕様書（令和 8 年 6 月版）

1	目的	2
2	情報の管理	2
3	受託者の持込機器	3
4	教育	3
5	監査	3
6	パッチ適用	3
7	脆弱性対応（開発）（保守）	4
8	コンピュータウイルス対策	4
9	アクセス制御（開発）	4
10	パスワード（開発）	5
11	セッション管理（開発）	5
12	認可処理（開発）	5
13	アカウント管理（開発）	6
14	ログイン状態にある利用者の意図に反した機能実行の防止（開発）	7
15	ログ（開発）（保守）	7
16	暗号化（開発）	9
17	調達	9
18	外部ネットワーク接続	10
19	ネットワーク管理	11
20	外部とのデータ交換	11
21	互換性（開発）	11
22	アクセシビリティ	12
23	生成 AI	12
24	契約時	13
25	プロジェクト立ち上げ	13
26	基本設計（開発）	13
27	システム開発（開発）	14
28	テスト（開発）	14
29	研修	15
30	移行（開発）	16
31	検収	16
32	運用（保守）	16
33	事故時の対応	17
34	契約終了時	18
35	著作権の帰属	18
36	著作権の紛争	18
37	契約不適合責任	19
38	その他	19

1 目的

- (1) 本特記仕様書（以下「本書」という。）は、ハードウェア（パソコン、サーバ等）、ソフトウェアライセンス、情報システム等の調達（購入のみならずリースや委託を含む）及び保守を行う際、石川県情報セキュリティポリシーに基づき、調達仕様書（以下「仕様書」という。）に加え、遵守すべき項目を定めるものである。受注者は本書に従わなくてはならない。
- (2) 本書に記載のない仕様に関しては仕様書による。契約書及び仕様書の記載が本書と異なる場合は、本書を優先する。ただし、以下の場合は、本書の該当項番を適用しない。
 - ・ 契約書または仕様書に本書の項番及び選択した項番を適用しない旨が記載されている場合
 - ・ システム開発を伴わない場合、項目名に（開発）と注記されている項目内の項番
 - ・ システムの運用・保守を伴わない場合、項目名に（保守）と注記されている項目内の項番
 - ・ 契約内容と無関係の項番（例えば、**Web** アプリケーションでないシステムを納品する場合の **Web** アプリケーションに関する項番）

2 情報の管理

- (1) 受注者は、県有施設以外で、個人情報等、石川県情報公開条例に定める非公開情報（以下「非公開情報」という。）を取り扱う場合、以下のとおり管理しなければならない。
 - ・ 非公開情報を受け取った際、預り証を提出すること。
 - ・ 非公開情報の保管場所は施錠した保管庫又は施錠若しくは入退室管理を行っている部屋とすること。
 - ・ 保管場所を事前に書面により報告すること。
 - ・ 保管場所を追加または変更する場合は、事前に書面により報告すること。
 - ・ 非公開情報を保管場所から持ち出さないこと。ただし、県の施設または県が指定した場所へ持ち出す場合を除く。
 - ・ 非公開情報を電子データで移送する場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。また、ウイルス対策ソフトの最新のパターンファイルによりスキャンが実施されていること。
 - ・ 非公開情報を複製又は複写しないこと。ただし、事前に県の承認を受けて、業務に必要最小限の範囲で行う場合を除く。
 - ・ 非公開情報を電子データで保管する場合、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの完全性について、定期的に点検すること。
 - ・ 非公開情報を管理するための台帳を整備し、利用者、保管場所、利用期間等を当該台帳に記録すること。

- ・非公開情報の紛失、漏洩、改ざん、破損その他の事故（以下「情報セキュリティ事故」という。）を防ぎ、真正性、見読性及び保存性の維持に責任を負うこと。
 - ・作業場所に、個人所有のパソコンまたは外部記録媒体を持ち込んで、非公開情報を扱う作業を行わないこと。
 - ・非公開情報を利用する作業を行うパソコンに、ファイル交換ソフト等、業務に関係のないアプリケーションをインストールしないこと。
 - ・県から非公開情報の状況について報告を求められた際、直ちに報告すること。
- (2) 開発及び運用で使用する媒体及び資料は、利用する資格のない者が利用できないよう施錠した保管庫又は施錠若しくは入退室管理を行っている部屋に保管すること。
 - (3) 受注者のうち、アクセス権限のない者は、重要な情報（非公開情報を含む）にアクセスしてはならない。
 - (4) 受注者のうち、アクセス権限を有する者は、業務上の目的以外の目的で重要な情報（非公開情報を含む）にアクセスしてはならない。

3 受託者の持込機器

- (1) 受注者の情報機器を県のネットワークに接続する場合は、以下に掲げる項目を守らなければならない。
 - ・県の許可を得ること。
 - ・必要な情報セキュリティ対策（ウイルス対策ソフトの導入、セキュリティパッチの適用等）を実施し、実施状況を確認すること。
 - ・個人所有の情報機器を接続しないこと。

4 教育

- (1) 作業責任者及び作業従事者全員に対して以下の事項を教育すること。
 - ・個人情報の保護
 - ・情報セキュリティ対策
 - ・その他本書に定める遵守事項
- (2) 作業責任者及び作業従事者を変更する場合も上記の教育を実施すること。
- (3) 受注者は、県の承諾を得て委託業務の一部を再委託するときは、再委託先の作業責任者及び作業従事者に対し、上記の教育を実施しなければならない。

5 監査

- (1) 県は、契約書、仕様書及び本書の履行に係る県の情報の取扱いについて、契約書、仕様書及び本書に基づき必要な措置が講じられているかどうか検証及び確認するため、受注者及び再委託先に対して、監査又は検査を行うことができる。

6 パッチ適用

- (1) システムの OS、ミドルウェア、ソフトウェア部品（ライブラリ等）、アプリケー

ションは以下の要件を満たすこと。

- ・当該ソフトウェアのメーカーにおけるサポートライフサイクルポリシーにおいて、メーカーから、契約期間中、脆弱性修正パッチ（以下「パッチ」という。）の開発及び提供がされること。
- ・新たに発見された脆弱性に関する情報やパッチのリリース情報（以下「パッチ情報」という。）が遅滞なくインターネットに公開または県に情報提供されること。

(2) 納品時点で提供されているパッチは全て適用した状態で納品すること。

7 脆弱性対応（開発）（保守）

- (1) Web アプリケーションの場合、独立行政法人 情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の「チェックリスト」に示されている脆弱性がないこと。
- (2) システムの場合、契約期間中に発見された脆弱性への対処について、以下の場合には追加費用なしで修補（パッチの開発・提供）すること。なお、修補以外の代替案によって可用性の低下を伴わずに脆弱性の影響を回避でき、かつ県の実情を得た場合、代替案による対処も可とする。
 - ・Web アプリケーションの場合、独立行政法人 情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の「チェックリスト」に含まれる脆弱性。
 - ・修補せずに運用を継続すると情報セキュリティ事故が発生する可能性のある脆弱性
 - ・本書によらず、受注者が追加提案として修補を約束した脆弱性。

8 コンピュータウイルス対策

- (1) ネットワーク接続の有無に関わらず、全てのパソコン及びサーバにソフトウェアまたはアプライアンス製品の導入によりウイルス対策を施すこと。
- (2) パソコン及びサーバの用途上必要のない OS のサービスは停止し、必要のないソフトウェアは削除すること。

9 アクセス制御（開発）

- (1) 利用者の認証方式はパスワード認証とすること。
- (2) 利用者認証を経していない者は本システムの利用者認証を要する機能（画面）を利用できないこと。
- (3) 利用者認証を要する機能（画面）は、セッションが終了した後は利用できないこと。
- (4) システム管理者の操作等、重要な情報の処理はアクセス可能な端末を限定すること。

10 パスワード（開発）

- (1) パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第2要素（ワンタイムパスワード生成器の生成するパスワードなど）はこの限りでない。
 - ・パスワードに利用できる文字種は、英字（大文字、小文字を区別）、数字、記号の3種とし、それぞれ自由に利用できること。
 - ・パスワードに利用する文字数は8文字未満を受け付けないようにすること。また、少なくとも64文字のパスワードは受け入れられること。
- (2) 初期パスワードまたは仮パスワードを発行する場合、パスワードは英字大文字、英字小文字、数字、記号を含み、12文字以上とすること。
- (3) ログインフォームはパスワードの入力欄は入力した文字を伏字にする（Webアプリケーションの場合、input要素においてtype属性の値にpasswordを指定すること）。または、伏字にする・しないを選択できる機能を持つこと。
- (4) パスワード認証に失敗した際に、利用者IDの間違いか、パスワードの間違いかが区別できるメッセージを表示しないこと。
- (5) パスワードを連続して一定回数間違った場合は、当該アカウントを一定時間ロックすること。特に仕様書に明示されていない場合、一定回数は10回、一定時間は30分間とする。
- (6) パスワードは平文で保存せず、ソルトつきハッシュの形で保存すること。ソルトは利用者毎に別々に設定し、最低5文字以上とすること。

11 セッション管理（開発）

- (1) Webアプリケーションの場合、利用者のセッション管理にはプログラミング言語やWebアプリケーション実行環境の備えるセッション管理機構を用いること。
- (2) Webアプリケーションの場合、ログイン状態にある利用者のセッション識別のための情報（セッションID）は、クッキーを用いて保持すること。
- (3) セッションはログイン処理成功後に開始すること。
- (4) セッションの有効期間を設定すること。特に仕様書に明示されていない場合、インターネットに公開するシステムの場合、有効期間を30分、インターネットに公開しないシステムは3時間とすること。
- (5) 次の場合はセッションを終了し、セッション情報を破棄すること。
 - ・利用者がログアウト機能呼び出した場合（ログアウトボタンを押す等）
 - ・最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合

12 認可処理（開発）

- (1) 認可処理は以下のとおり文書化し、求めがあった際に提出すること。
 - ・認可処理の必要な機能、情報を識別して、認可処理の必要な画面には、画面遷移図上に識別マーク等をつけること。
 - ・各ロールと権限を一覧表（権限マトリックス）に整理すること。
- (2) Webアプリケーションの場合、各利用者の権限確認には、セッション変数に保

存された利用者識別情報（利用者 ID 等）を基準とすること。

- (3) 認可を要する情報表示や機能実行をする前に、実行中の利用者が、当該情報の表示や機能を実行するための権限を有していることを画面毎に確認すること。
- (4) 認可されなかった場合は、適切なエラー表示をすること。

13 アカウント管理（開発）

- (1) 利用者 ID により、利用者を個別に識別できること。
- (2) 利用者 ID が重複しないよう、チェック処理を行うこと。
- (3) 情報システム管理者が、パスワードをリセットできること。
- (4) 利用者がパスワードを変更できること。
- (5) パスワード変更機能の実行前に、現在のパスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
- (6) 情報システム管理者が、利用者アカウントを追加及び削除できること。
- (7) 情報システム管理者が、利用者アカウントを一時的に利用停止できること。
- (8) システムに利用者のメールアドレスが登録されている場合、利用者がパスワードを失念した場合の対処機能は以下の①、②いずれかの方式とし、③または④の要件を満たすこと。（利用者確認の手段として、予め登録したメールアドレスに宛てたメールが受信できることを用いる。）
 - ①パスワードリセット機能を利用するための URL を登録メールアドレスにメール送付する方式
 - ②仮パスワードを発行し、メールで通知する方式（仮パスワードでログインした場合は、パスワード変更機能のみが利用できるものとする）
 - ③①の機能の実装に際して、第三者がパスワードリセット機能を使えないように、URL には十分長い乱数による秘密情報（トークン）をつけること。
 - ④②の機能に対する総当たり攻撃対策を施すこと。
- (9) インターネットに公開し、利用者登録が可能なシステムの場合、以下を遵守すること。
 - ・利用者登録時にメールアドレスを登録させること。
 - ・利用者によって登録されたメールアドレスに対してメールを送付し、登録メールアドレスが利用者に利用されているアドレスであることを確認する処理を実装すること。
 - ・登録メールアドレスが利用者に利用されているアドレスであると確認できた後に本システムにおける利用者登録を完了（登録の確定）とし、利用者登録の完了を経ってからアカウントを作成すること。
 - ・登録されたメールアドレスに対してメールを送付する際に、利用者が登録したパスワードを記載しないこと。
 - ・利用者が登録したメールアドレスを変更する機能を実装すること。
 - ・メールアドレス変更機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
 - ・メールアドレス変更機能の実行後は、利用者登録時と同様の処理を経ること。

- ・変更前のメールアドレス（旧メールアドレス）にも登録メールアドレスが変更された旨の通知をメール送付すること。
- ・パスワード変更機能の実行後に、登録されているメールアドレスへ、パスワードが変更された旨の通知をメール送付すること。
- ・利用者による自身のアカウント削除機能を提供すること。
- ・アカウント削除機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
- ・アカウント削除機能の実行後、登録されていたメールアドレスにアカウントが削除された旨の通知をメール送付すること。

14 ログイン状態にある利用者の意図に反した機能実行の防止（開発）

- (1) Web アプリケーションの場合、外部リンク等により本システムの画面（機能）に遷移することにより、本システムの機能がログイン状態にある利用者の意図に反して実行されることを防止すること。なお、ここで言う「ログイン状態にある利用者の意図に反した機能実行の防止」とは、クロスサイト・リクエスト・フォージェリ（以下「CSRF」という。）対策及びクリックジャッキング対策を指す。
- (2) Web アプリケーションの場合、CSRF 対策及びクリックジャッキング対策を施すべき画面（機能）を洗い出し、求めがあった際に提出すること。なお、当該機能のページは POST メソッドで呼び出すようにすること。
- (3) Web アプリケーションの場合、対策対象の画面（機能）を実行する前のページにて十分長い乱数による秘密情報（トークン）を生成して埋め込み、処理を実行する際は、その値が正しい場合のみ実行すること。
- (4) Web アプリケーションの場合、対象画面の 1 つ手前の画面にて、次のいずれかの HTTP レスポンスヘッダを出力すること。なお、対象画面以外にも出力してよい。
 - ・X-FRAME-OPTIONS: DENY
 - ・X-FRAME-OPTIONS: SAMEORIGIN

15 ログ（開発）（保守）

- (1) システム監査、情報セキュリティ事故調査を目的として以下のログを出力及び保管すること。
 - ・Web アプリケーションの場合、Web サーバのアクセスログ
 - ・メールの送受信を行う場合、メールの送受信ログ
 - ・ファイアウォールを設置する場合、ファイアウォールのアクセスログ
 - ・データベースを使用する場合、データベースのアクセスログ
 - ・アプリケーションログ
 - ・エラーログ

- (2) デバッグログについては、構築時、動作テスト時には出力してよいが、本番稼働時までには無効にしておくこと。ただし、システム検証やトラブル対応のために、認めた場合は除く。
- (3) 以下のイベントをアプリケーションログにて取得すること。なお、以下に記載していない他のイベントも取得してもよい。
- ・ログイン（成功・失敗問わず）
 - ・ログアウト
 - ・アカウントロック
 - ・利用者登録・登録削除
 - ・利用者の登録内容更新
 - ・利用者のパスワード変更
 - ・非公開情報の参照
 - ・その他重要な操作（Web アプリケーションの場合、CSRF 対策の対象となる操作は必須）
- (4) 以下の情報をログに含めること。なお、これ以外の情報を含めても良い。
- ・アクセス日時（年、月、日、時、分、秒）
 - ・Web アプリケーションの場合、アクセス元 IP アドレス（IPv4 又は IPv6）
 - ・利用者 ID
 - ・アクセス対象（Web アプリケーションの場合、URL 又はページ番号等）
 - ・操作内容
 - ・操作対象（利用者 ID、文書 ID など）
 - ・実行結果（成功あるいは失敗、処理件数など）
- (5) パスワードはログの項目として取得しないこと。
- (6) ログが不正に参照・変更・削除されないよう保護すること。
- (7) ログから非公開情報が漏えいすることを防ぐため、ログの目的（監査、情報セキュリティ事故調査）を妨げない範囲で非公開情報を含めない処理又は非公開情報の一部のみ出力（マスク処理）をすること。
- (8) ログは 3 年間保管すること。ただし、ファイアウォール等、ハードウェアの仕様によりこの保管期限を達成できない場合は、最大限保管すればよいものとする。
- (9) ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。

16 暗号化（開発）

- (1) システムで送受信する情報のうち、非公開情報に該当するものを要件定義時に一覧表にまとめ、求めがあった際に提出すること。
- (2) インターネットに公開する **Web** アプリケーションの場合、利用者と本システム間で非公開情報を送受信する際に利用する画面（機能）を **SSL/TLS** の利用対象とすること。
- (3) インターネットに公開する **Web** アプリケーションの場合、サーバ証明書はブラウザで警告の出ないものを使用し、証明書の発行先名は、運営者の名称とする。
- (4) **Web** アプリケーションの場合、**SSL2.0** は使用しない設定にすること。
- (5) 非公開情報をデータベースまたはファイルに保存する際は暗号化を施すこと。
- (6) 非公開情報をデータベースまたはファイルに保存する際の暗号化アルゴリズムは **CRYPTREC**「電子政府における調達のために参照すべき暗号のリスト」に記載されたアルゴリズムを用いること。
- (7) 県から求めがあった場合、暗号鍵の管理方法を提出すること。

17 調達

- (1) パソコンを調達する場合、コンシューマー向け製品ではなく、業務に関係のないプリインストールソフトが少ない法人向け製品を選定すること。
- (2) 機器を調達する場合、重要な機器は、障害発生を想定し、必要に応じて二重化等を行うこと。
- (3) ソフトウェアライセンス（以下「ライセンス」という。）を調達する場合、県の定める様式に従って以下の事項を報告すること。ただし、県が不要と判断した場合はこの限りではない。
 - ・ソフトウェア名
 - ・版（アカデミック版、アップグレード版等）
 - ・種類（プリインストール、パッケージ、ボリュームライセンス等）
 - ・メーカー
 - ・導入可能数
 - ・特筆すべき使用許諾条件
 - ・プログラムの追加と削除（プログラムと機能）での表示

- (4) ライセンスを調達する場合、ユーザ登録またはライセンス登録は事前に県に登録内容の了解を得てから実施すること。
- (5) ライセンスを調達する場合、障害や互換性を考慮すること。複数のライセンスを調達するとき、メーカーからボリュームライセンスが提供されている場合は、OSを除き原則としてボリュームライセンスを調達すること。特段の理由によりボリュームライセンスを選択しない場合は、事前に県の了解を得ること。
- (6) ライセンスを調達する場合、県が既に保有しているライセンスの使用許諾条件の制約を考慮すること。
- (7) 賃貸借契約でライセンスを調達する場合、使用許諾条件上問題がないか確認すること。
- (8) 更新前の機器で利用していたライセンスを更新後の機器で利用する場合、更新後の機器及び利用形態等が当該ライセンスの使用許諾条件を満たすか確認し、必要に応じてライセンスの調達を行うこと。
- (9) システムを調達する場合、ハードディスクの一部に障害が発生したときもデータが保全されるよう定期的にバックアップを取得すること。重要システムの場合、RAID 構成やホットスペアの配置等により、ハードディスクの一部に障害が発生したときも運用が継続できること。
- (10) 契約書、仕様書及び本書に定める納品物に第三者が権利を有する著作物（ソフトウェアライセンスを除く。）が含まれている場合、当該著作物の使用に必要な費用の負担及び使用許諾契約に係る一切の手続を行うこと。
- (11) 機器等の調達にあたり、機器等の開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること。

18 外部ネットワーク接続

- (1) 外部ネットワーク（インターネットを含む。）と接続する場合、以下の項目を遵守すること。
 - ・外部のネットワークを経由した接続において非公開情報を取り扱う場合、利用者 ID とパスワードによる利用者の認証を行うこと。
 - ・外部の端末からネットワークを経由した重要な操作が行われる場合は、アクセス可能な外部端末を限定すること。
 - ・外部の端末からネットワークを経由した重要な操作が行われる場合は、暗号化された転送プロトコル（SSL、SSH、SFTP 等）を使用するよう努めること。
 - ・総合行政ネットワーク等の外部機関が管理するネットワークとの接続を行う場合は、そのネットワーク接続仕様に従った対策を行うこと。
 - ・外部の端末からネットワークを経由した重要な操作を実施する場合は、専用線や IP-VPN といった閉域網を利用すること。やむを得ず、インターネット等の公衆通信網を利用する場合は、暗号化された通信プロトコル（IPsec/SSL/SSH/SFTP 等）を使用すること。

- ・外部の端末からネットワークを経由した重要な操作が行われる場合は、利用者 ID とパスワードによる認証だけでなく、IP アドレス制限や二要素認証等を実施すること。
- ・ファイアウォールを構築し、情報機器を保護すること。
- ・ファイアウォール及びルータにおいて、次に掲げる内容を定め、求めがあった際に提出すること。
 - ① 通過させるポート番号、通信方式、接続先、通信の方向
 - ② 通過させる理由

19 ネットワーク管理

- (1) ネットワークを構築または管理する場合、以下の項目を遵守すること。
 - ・次に掲げる管理資料を作成し、不備または変更があった場合は修正すること。
 - ① ネットワークの構成図
 - ② ネットワークの運用管理方法
 - ③ ネットワーク接続基準
 - ④ ネットワーク障害時の対応方法
 - ・重要なネットワーク回線及びネットワーク機器は、障害発生を想定し、必要に応じて二重化等を行うこと。

20 外部とのデータ交換

- (1) ネットワークを利用して外部とのデータ交換を行う場合、以下の項目を遵守すること。
 - ・使用する回線及び通信方法等の手順を定め、遵守すること。
 - ・決められた保存領域で行い、別の領域を使用しないこと。
 - ・ファイルサイズ又はデータの一部を交換前のデータと比較する等の確認をすること。
 - ・交換相手、交換日時、交換方法、交換データの内容等について記録すること。
 - ・非公開情報を交換する場合は、データを暗号化すること。

21 互換性（開発）

- (1) システムを開発する場合、納品時にマイクロソフトがサポート中の **Windows** クライアント OS 及び納品から 5 年の間に販売される **Windows** クライアント OS に対応すること。
- (2) **Web** アプリケーションの場合、納品時にマイクロソフトがサポート中の **Microsoft Edge** 及び納品から 5 年の間に提供される **Microsoft Edge** に対応すること。
- (3) **Web** アプリケーションの場合、互換性を考慮し **Microsoft Edge** 以外でも使用可能であることが望ましい。

22 アクセシビリティ

- (1) インターネットに公開する場合、公開する全ての URL について、JIS X 8341-3:2016 のレベル AA に配慮すること。ここでの「配慮」とは、情報通信アクセス協議会ウェブアクセシビリティ基盤委員会「ウェブコンテンツの JIS X 8341-3:2016 対応度表記ガイドライン - 2016 年 3 月版」で定められた表記による。なお、既存の PDF、動画及び音声ファイルは対象外とする。
- (2) インターネットに PDF ファイルを公開する場合、提供する情報はできるだけページ本文内に HTML 形式でも掲載すること。また、PDF ファイルは文書ファイル等から変換して作成するものとし、例外的にスキャンして作成した PDF ファイルを掲載する場合は、JPEG 形式のファイルでも公開すること。なお、既存の PDF ファイルは対象外とする。
- (3) インターネットに表形式データを公開する場合、CSV 形式も公開すること。なお、既存の Excel ファイルは対象外とする。

23 生成 AI

- (1) 契約により指定された個人情報の取り扱いが AI にも適用される。クラウドサービスの AI を利用する場合、クラウドサービスのデータ処理規約（DPA）等の法的書面により、個人情報の取り扱いに関する要求事項が全て満たされることを確認すること。
- (2) 処理対象データが AI モデルの学習（ファインチューニングを含む。）に利用されないこと。クラウドサービスの AI を利用する場合、AI モデルの学習に利用されないことがデータ処理規約等の法的書面に明記されていること。
- (3) AI がインターネット検索機能（グラウンディング検索機能を含む。）を利用しないこと。利用目的の達成のためにこれらの機能を利用する必要がある場合は、事前に県に通知し、承認を得ること。
- (4) AI を提供する事業者の所在国及びデータの処理地域を県に通知すること。
- (5) 国外に所在するクラウドサービス事業者の AI を利用する場合、当該国の個人情報保護制度等を確認し、個人情報の取り扱いに関する要求事項が実効的に履行される環境にあることを確認すること。
- (6) データの処理地域が国外の場合、当該国の個人情報保護制度等を確認し、個人情報の取り扱いに関する要求事項が実効的に履行される環境にあることを確認すること。
- (7) クラウドサービスの AI を利用する場合、処理対象データの保存期間が当該サービスの機能の範囲内で最短となるよう設定すること。
- (8) クラウドサービスの AI を利用する場合、クラウドサービス事業者のデータ処理規約その他の法的書面の内容を定期的に確認し、重大な変更があることを認知した際は、速やかに県に通知すること。
- (9) AI を提供する事業者の所在国またはデータの処理地域を変更する際は、事前に県に通知し、承認を得ること。
- (10) 安全管理措置の履行状況を確認するために必要な情報（クラウドサービス事業者

の公式ドキュメント、データ処理規約、設定画面のスクリーンショット等)を県の求めに応じ提供すること。

- (11) クラウドサービスの AI を利用する場合、当該クラウドサービスが ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストに掲載されていること。

24 契約時

- (1) 受注者は、契約締結後、遅滞なく以下の書類を提出しなければならない。
- ・ 契約金額内訳書
 - ・ 連絡先（緊急連絡先を含む少なくとも第三順位者までの氏名、常時連絡可能な電話番号及びメールアドレス）

25 プロジェクト立ち上げ

- (1) システム開発や設定を伴う機器調達の場合、プロジェクト立ち上げ時に以下の書類を県と協議のうえ作成、提出すること。また、これらの書類の記載事項を変更する場合、県と協議の後、変更後の書類及び変更点を記した文書を提出すること。
- ・ 作業工程表
 - ・ 体制図（再委託先及び下請け先を含む作業責任者、作業従事者の氏名等）
- (2) システムの開発を行う場合、以下の事項を含むプロジェクト方針書を県と協議のうえ作成、提出すること。協議に際し、県と受注者双方で決定事項、検討事項、リスク要因を明確にし、現時点で不明点がないようにすること。プロジェクト方針書について概ねの合意ができた時点で基本設計に着手すること。
- ・ 前提条件と制約条件
 - ・ 仕様等を決定・変更する場合の合意の手順、報告の頻度
 - ・ 県と受注者の役割と責任分担
 - ・ 現状の課題と想定されるリスク
 - ・ 変更管理計画
 - ・ 仕様管理計画
 - ・ 進捗管理計画
 - ・ 品質管理計画
 - ・ 問題管理計画

26 基本設計（開発）

- (1) 基本設計時には以下の事項を遵守すること。
- ・ 県と認識の違いが発生しないよう、連絡を密にすること。
 - ・ 県から口頭で説明を受けた場合、文書化（図、表なども活用）したものを作成し確認を求めるなどして正確な情報把握に努めること。
 - ・ 少量の例外的な処理をシステム化するよう依頼を受けた場合は、システム化により得られるメリットと、システムの複雑化に伴う開発期間及び開発費用の増加並びに拡張性及びメンテナンス性の低下等のデメリットとを比較説明

し、県の判断を仰ぐこと。

- (2) 基本設計時には以下の事項を含む基本設計書を県と協議のうえ作成、提出すること。

- ・システム（ネットワーク含む）構成
- ・情報セキュリティの確保
- ・性能や信頼性（故障検出や故障対応等）
- ・処理方式や他システムとの連携方式
- ・将来の処理能力強化などの拡張性
- ・画面・帳票の種類やレイアウト（設計方針も含む）
- ・業務機能（利用者管理機能、利用状況確認機能等も含む）
- ・総合テスト、研修、移行などシステム導入に向けて必要な作業の概要
- ・システム導入（運用開始）後の業務運用や保守作業の概要

27 システム開発（開発）

- (1) システム開発時には以下の事項を遵守すること。

- ・定期的な報告会または臨時会議を実施し、作業状況を県に報告すること。
- ・問題・課題やリスクと思われる事項は初期段階のうちに県に報告するとともに、原因の分析や処置方法の検討、スケジュールへの反映、類似問題有無の確認などを行うこと。
- ・業務で実際に使用しているデータをテストデータとして使用しないこと。ただし、業務上やむを得ず使用する場合は、利用範囲及び利用目的を限定して、県の許可を得た上で必要な保護対策を実施すること。
- ・開発した情報システムの導入により、既存システムに影響を及ぼさないことを確認すること。
- ・海賊版や偽造品、その他ライセンスの保有を対外的に示すことができないソフトウェアを用いて開発を行わないこと。
- ・システム開発の責任者及び作業者に対して、適切なアクセス権を設定し、使用する ID を管理すること、また、開発完了後、開発用 ID を削除すること。
- ・システム開発の責任者及び作業者は、使用するハードウェア及びソフトウェアを特定し、県に報告すること。県が利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから速やかに削除すること。
- ・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、出力されるように情報システムを開発すること。

28 テスト（開発）

- (1) 県から求めがあった場合、テストの成果物を提出すること。
- (2) 以下の場合は強化試験を実施するなどの処置を施すこと。
- ・障害発生率が基準値より多い
 - ・障害発生率が基準値より極端に少ない

- ・基本的な事項で障害を検出した
- (3) インターネットに公開する場合、ウェブアクセシビリティ基盤委員会の示す「JIS X 8341-3:2016 試験実施ガイドライン」に基づく試験を実施すること。この試験は、抽出により実施してよい。
- (4) Web アプリケーションの場合、独立行政法人 情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の別冊「ウェブ健康診断仕様」により検査すること。この検査は抽出により実施してよい。
- (5) 総合テスト時には以下の事項を含む総合テスト計画書を県と協議のうえ作成、提出すること。
 - ・テスト環境
 - ・検証ツール
 - ・テスト項目（性能や信頼性、安全性、運用性、作成した媒体（CD-ROM やテープなど）の二次利用、他のシステムとの連携を含む）
 - ・テストデータ
 - ・テスト手順
 - ・結果確認方法
 - ・仕様書の要求事項を満たしていることの確認
 - ・品質判定基準
- (6) 総合テスト後、総合テスト成績書を県に提出すること。

29 研修

- (1) 研修を行う場合、以下の事項を含む研修計画書を県と協議のうえ作成、提出すること。
 - ・スケジュール
 - ・県と受注者との役割分担、体制
 - ・対象者（一般利用者、システム管理者等）
 - ・研修内容
 - ・研修で使用する環境やデータの準備
 - ・研修用マニュアル（操作マニュアル等）の作成
 - ・研修結果アンケートの実施
- (2) 研修結果アンケートにより操作マニュアル等の記載内容やわかりやすさに課題が見つかった場合は、運用開始前に改善すること。
- (3) 研修結果アンケートにより習熟度が不足している場合は、追加の研修実施を行う等の対策をとること。

30 移行（開発）

- (1) 既存システムからの移行を行う場合、データ移行において必要となる既存システムに関する調査、既存システムの保守業者等との調整、移行の際に必要なシステムの設計・開発等、移行作業に関する全ての作業を行うこと。また、以下の事項を含む移行計画書を県と協議のうえ作成、提出すること。

- ・スケジュール
- ・県と受注者との役割分担、体制
- ・業務や利用中のシステムを停止しなければならない期間、範囲
- ・外部機関や他システムへの影響
- ・事前の周知、調整
- ・移行当日の体制（連絡方法や要員配置（出先機関などの対応も含む））
- ・移行の詳細な手順（移行後の確認手順も含む）
- ・移行の成功／失敗の判断基準
- ・旧システムへの戻し手順
- ・運用開始直後の支援体制、状況確認会議の実施

31 検収

- (1) 検収のために、以下のものを提出すること。

- ・完了報告書
- ・システムの場合、システム一式及び付帯資料（設計書、マニュアル、報告書等）
- ・県が求めた場合、納品物が契約書や仕様書の要求事項を満たすことを確認するための補足説明資料
- ・その他、契約書や仕様書で定めた納品物

32 運用（保守）

- (1) 事前に以下の事項を含む運用計画書を県と協議のうえ作成、提出すること。

- ・定常的な作業とその実施頻度
- ・定常的な作業以外の特別対応
- ・稼働状況、故障状況、利用状況等の把握
- ・作業報告
- ・発生しうる問題とその対応

- (2) 契約期間中は以下の事項を遵守すること。

- ・作業の実施状況を記録し、定期的に報告書を提出すること。
- ・設計書、機器構成、データ仕様、システム間連携仕様等、各種書類の変更管理を行い、変更があった場合、県に最新版の書類を提出すること。
- ・運用計画どおりに安定的にシステムが利用されているか確認すること。
- ・運用計画と相違が生じた場合に、対処を検討し、必要な是正処置をとること。
- ・作業の記録及び保管を行うこと。
- ・契約に基づき実施する情報セキュリティ対策の履行状況を定期的に報告する

こと。

- ・ウイルス対策ソフトウェアのパターンファイルを最新の状態に保つこと。
- ・最新のパターンファイルを利用して、定期的にコンピュータウイルスの検査を行うこと。
- ・パッチリリース後 1 週間以内にパッチ適用・非適用の方針を決め、その判断理由について報告すること。なお、パッチを適用しないことによりセキュリティ上の問題がある場合、パッチを適用しなければならない。
- ・パッチリリース後 2 週間以内に追加費用なしでパッチ適用(動作検証を含む。)を行うこと。また、適用作業終了後は、正常動作を確認し、パッチ適用状況(適用の成功・不成功、動作への影響有無等)を報告すること。
- ・開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認すること

(3) トラブル発生時には以下の事項を遵守すること。

- ・二次災害の発生や影響の拡大防止を優先すること。
- ・重大な障害発生時には、作業担当者だけで対応するのではなく、組織的に取り組むこと。
- ・利用者への影響を確認し、県に対し状況や復旧予定を速やかに連絡すること。
- ・県へ報告する際は、事実と推測を区別すること。
- ・暫定的な処置を施すことで業務遂行が可能となるような方法も検討すること。

(4) 県が求めた際、以下の電子データを提出すること。

- ・ソースコード（受注者または第三者がツール等として従前から著作権を有している場合を除く）
- ・全件分のデータ（汎用的なデータ形式とすること）
- ・データのレイアウト、コード表など次期システムの参考となる資料
- ・次期システムにおいて設計上考慮すべき事項

(5) 次期システムの計画が生じた場合は、円滑なデータ移行を実現するための調査等を県の求めに応じて誠実に実施すること。

33 事故時の対応

(1) 契約書、仕様書及び本書の履行に関し情報セキュリティ事故が発生した場合、その事故の発生に係る帰責の如何に関わらず、直ちに県に対して、以下の事項を報告し、適切な措置をとること。また、調査結果を遅滞なく県に報告すること。

- ・当該事故に関わる情報の内容
- ・件数
- ・事故の発生場所
- ・発生状況

- (2) 情報セキュリティ事故が発生した場合、県は必要に応じて当該事故に関する情報を公表することができる。
- (3) 情報セキュリティ事故による影響の拡大を防止した後、県へ原因の調査結果、回復方法及び再発防止策について報告すること。

34 契約終了時

- (1) 機器を廃棄またはリース返却する場合には以下の事項を遵守すること。
 - ・記憶装置を物理的に破壊、又は磁氣的に破壊し、情報を復元不可能な状態にすること。また、庁舎内で職員立ち会いのもと破壊する等、確実な履行を担保すること。
 - ・データ消去証明書を県へ提出すること。
 - ・県が所有するソフトウェアを削除すること。
 - ・機器の廃棄またはリース返却の記録を保管すること。
- (2) 賃貸借契約の場合、追加費用なしで撤去すること。
- (3) 賃貸借契約の場合、県名義で調達したライセンスを県に無償譲渡すること。ただし県が不要と判断したものを除く。
- (4) 契約期間を通じてセキュリティ対策が適切に実施されたことを確認し、報告すること。

35 著作権の帰属

- (1) 受注者は、成果品（契約の履行過程において得られた記録、契約終了時に提出される移行データ等を含む。）を他人に閲覧させ、複写させ、又は譲渡してはならない。ただし、県の承諾を得たときは、この限りでない。
- (2) 前項の成果品に関し、著作権及び意匠権等のすべての権利は、受注者または第三者がツール等として従前から著作権を有している場合を除き、県に帰属するものとする。
- (3) 受注者は、県に著作権を譲渡し、または県に著作権法に基づく利用を許諾した成果品に関し、著作者人格権を行使しないものとする。

36 著作権の紛争

- (1) 契約書、仕様書及び本書に定める納品物に関し、第三者との間に著作権（ライセンスを除く。）に係る権利侵害の紛争等が生じたときは、当該紛争の原因が県の責めに帰す場合を除き、受注者の責任及び負担において一切を処理するものとする。この場合、県は、当該紛争等の事実を知ったときは受注者に通知し、受注者は必要な範囲で訴訟上の防衛を県のために講じなければならない。
- (2) 契約書、仕様書及び本書に定める納品物に関し、第三者との間にライセンスに係る権利侵害の紛争等（必要ライセンス数の不足の指摘を含む。）が生じたときは、県が納品物を紛失した場合を除き、受注者の責任及び負担において一切を処理するものとする。この場合、県は、当該紛争等の事実を知ったときは受注者に通知し、受注者は必要な範囲で訴訟上の防衛（不足ライセンスの追加調達を含む。）

を県のために講じなければならない。

37 契約不適合責任

- (1) 契約書、仕様書及び本書に定める納品物について契約の内容に適合しないもの（バグも含む。以下「契約不適合」という。）が発見された場合、県は受注者に対して当該契約不適合の修正を請求することができ、受注者は、修正するものとする。
- (2) 受注者がかかる修正責任を負うのは、以下のいずれかの期間内に県から請求された場合に限るものとする。
 - ・ 検収完了後 1 年以内
 - ・ 個々の機能に関しては、運用開始以降、当該機能の初動操作が正常に稼働してから 6 ヶ月以内
- (3) 受注者が納品物の一部を修正した場合、関連する他の納品物も遅滞なく修正し、再提出すること。例えばシステムを修正した場合で設計書も納品していた場合、設計書も修正し、再提出すること。

38 その他

- (1) 受注者は、本書に定めるもののほかに、業務内容に応じて、適切な情報セキュリティ対策を実施すること。
- (2) 契約書、仕様書または本書に定めのない事項については、必要に応じて県と受注者とが協議して定める。

石川県サーバ統合基盤利用仕様書

令和5年8月

石川県総務部デジタル推進課

目次

1.1. 本書の位置づけ	3
1.2. 背景および目的	3
2. 統合基盤の概要	3
2.1. 統合基盤の特徴	3
2.2. 統合基盤から提供されるもの	4
2.3. 原課側で用意、対応する必要があるもの	5
2.4. 統合基盤と原課の役割分担	5
2.5. 統合基盤のシステム構成	6
2.6. ハードウェア仕様	6
2.6.1. ストレージ	6
2.6.2. ネットワーク	6
2.7. ソフトウェア仕様	7
3. 統合基盤の利用支援	7
3.1. システム移行	7
3.1.1. 移行手順	7
3.1.2. 移行方法	8
3.1.3. 移行端末	8
3.2. 障害対応	8
3.3. 問い合わせ対応	9
3.4. 運用ポータルサイト	9
4. 利用に当たっての留意事項	9
4.1. 統合基盤で利用出来ないもの	9
4.2. システムリソースの最適化	9
4.3. 統合基盤の適正利用	9
4.4. 統合基盤の Oracle の利用について	9
4.5. その他	9

1. はじめに

1.1. 本書の位置づけ

情報システムを所管する部署が「石川県サーバ統合基盤」（以下、「統合基盤」という。）を利用するにあたり、その仕様や提供サービスを確認するためのドキュメントである。

1.2. 背景および目的

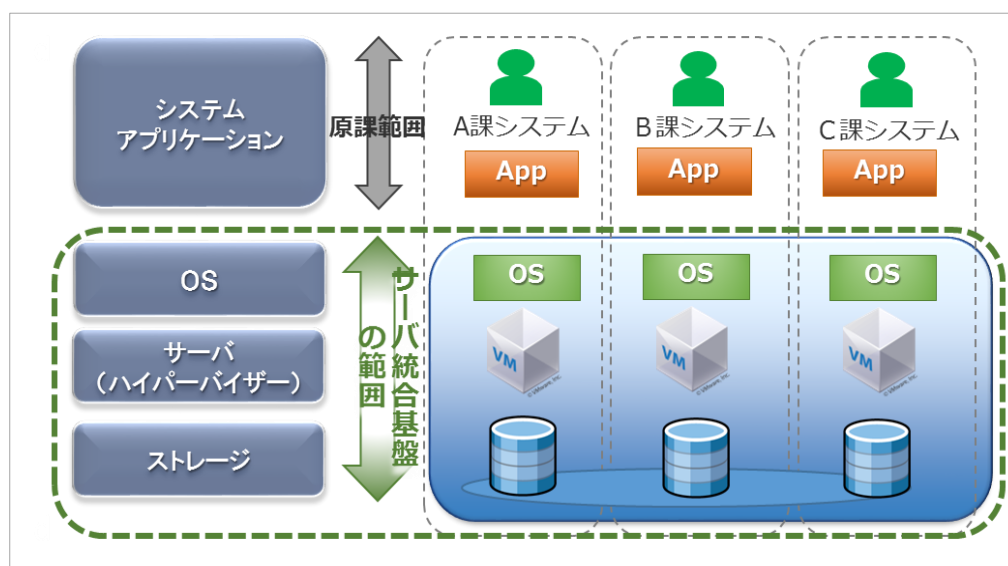
本県では、情報システムの全体最適化の取り組みとして、システムの稼働環境を集約・一元化する統合基盤を導入した。複数のシステムで統合基盤を共用することにより、システム機器の利用効率を高めるとともに、統合基盤のバックアップやセキュリティ対策等の維持管理業務を一元化することで、以下の3点を実現する。

- ・システムの機器コスト削減
- ・システムの保守・運用業務の負荷軽減
- ・システムの信頼性およびセキュリティの向上

2. 統合基盤の概要

2.1. 統合基盤の特徴

- ・仮想化ソフト（VMware 社の vSphere）によるプライベートクラウド環境を提供。（Oracle 専用基盤は既に利用しているシステムにのみ提供）
- ・ハードウェア（OS 含む）は統合基盤で提供されるため、当該部分の構築・維持にかかる予算低減や負荷軽減が可能。
- ・原則として 24 時間 365 日利用可能。
- ・冗長化構成により、高可用性、高信頼性を実現。
- ・庁内でバックアップを実施。
- ・県庁舎 7F ネットワーク管理室に設置。（静脈認証による入退室管理でセキュリティ確保）
- ・統合基盤側と原課側での責任範囲は以下の通り。



注）業務システム独自の OS やハードウェアが必要な場合はこの限りではない

2.2. 統合基盤から提供されるもの

No.	項目	内容	備考
(1)	サーバリソース	CPU、メモリ、ディスク	割りリソース量はシステム移行時に応相談
(2)	ネットワークリソース	論理ネットワークインタフェースカード	帯域：10Gbps（共用利用） ネットワーク構成は応相談
(3)	ソフトウェアライセンス（OS）※ ¹	Windows Server 2016 Windows Server 2019 Windows Server 2022 Red Hat Enterprise Linux 7/8 以上	左記以外の WindowsOS および Red Hat Enterprise Linux のバージョンについては応相談。それ以外については基本的に不可。
(4)	ファイアウォール機能※ ²	レイヤ 4 以下のパケットフィルタリング機能	UTM 機能は提供不可
(5)	負荷分散機能※ ³	Web アプリケーションのトラフィックロードバランシング機能	分散方式はラウンドロビン、リーストコネクション方式の 2 通りから選択 データベース負荷分散機能は提供不可
(6)	バックアップ・リストア機能※ ⁴	一括バックアップ 仮想サーバ全体のイメージバックアップ	3 世代前（最大 3 日前）の状態に復元可能
		個別バックアップ※ ⁵ 仮想サーバ内のフォルダ、ファイル単位のバックアップ	1 世代前の状態に復元可能
		スナップショット※ ⁶ サーバメンテナンス前に一時的に取得し、万一の時に即時にロールバックする機能	常時保存は不可（別途定めるルールに則り利用後は速やかに削除）
(7)	監視機能	仮想サーバに対して ICMP による死活監視を実施し、NG 時に管理者にメール通知する機能	リソース、プロセス、サービス、ログ監視は未提供
(8)	ウイルス対策機能※ ⁷ ※ ⁸	提供 OS に対するアンチウイルス機能により、インシデント発生時はウイルス駆除、隔離までを基盤側で行い、その情報を管理者にメール通知する機能	ソフトウェア名 Windows Server：Deep Security Virtual Appliance ウイルス対策 RHEL：Deep Security Agent ウイルス対策
(9)	管理機能※ ⁹	運用管理端末の利用 ネットワーク管理室に設置する端末から仮想サーバをメンテナンスすることが可能	・リモート接続（RDP/telnet/ssh） ・電源 off/on、再起動 ・CD/DVD ドライブ、USB メモリの接続 ・コンソール接続 ・仮想サーバリソース状況確認
(10)	問い合わせ（ヘルプデスク）サービス※ ¹⁰	問い合わせや相談を受付、応対するサービス	・統合基盤が提供する機能の内容 ・運用管理端末の利用方法 ・障害発生時の問い合わせ など
(11)	運用ポータルサイト	統合基盤を利用する上で有用な情報をブラウザから閲覧出来る機能	・統合基盤利用に必要なマニュアル ・申請資料一式 ・よくある問い合わせ など
(12)	システム移行に必要な端末貸与	物理サーバを仮想サーバに変換するために必要な端末を用意	端末数には限りがあるため、移行日程が重複する場合、別途日程調整要

※¹ 提供以降の OS に対する更新プログラムの適用は原課側の責任において行うものとします。

※² オプション提供となります。仮想サーバ側でフィルタリング可能な場合は提供不可。

※³ オプション提供となります。高度な負荷分散機能が必要な場合（例えば、ラウンドロビン以外の負荷分散）は提供出来ない場合があります。

※⁴ バックアップソフトウェア名：「Veeam Backup & Replication Standard Edition」

※⁵ 本機能のリストア対応は原課側作業となります。

バックアップ設定は基盤運用受託業者へご依頼ください。

※⁶ 本機能は原課側に解放されますので、スナップショット取得、削除対応は原課側作業となります。

※⁷ インシデント発生後の調査、対策は原課側で実施下さい。

※⁸ 統合基盤側で用意する RHEL 用ウイルス対策機能にはライセンス数の上限があります。登載するシステム数によってはライセンスが不足する可能性もあるため、予算段階では原課側にてその費用を盛り込んでください。（費用についてはデジタル推進課ネットワーク G に連絡ください）

※9 県庁外からのリモート接続については応相談。

※10 電話受付時間（基盤運用受託業者）：開庁日 8:30～17:45、メール受付：24 時間 365 日

上記の他、以下のものは利用（移行）出来ません。

- ・ SSL アクセラレータ、VPN ルータ等のネットワーク機器
- ・ バックアップ専用ストレージ（NAS）
- ・ テープドライブ等の外部記憶装置
- ・ コールドスタンバイ構成における、スタンバイ側サーバの移行（アクティブ側サーバのみ移行対象）

2.3. 原課側で用意、対応する必要があるもの

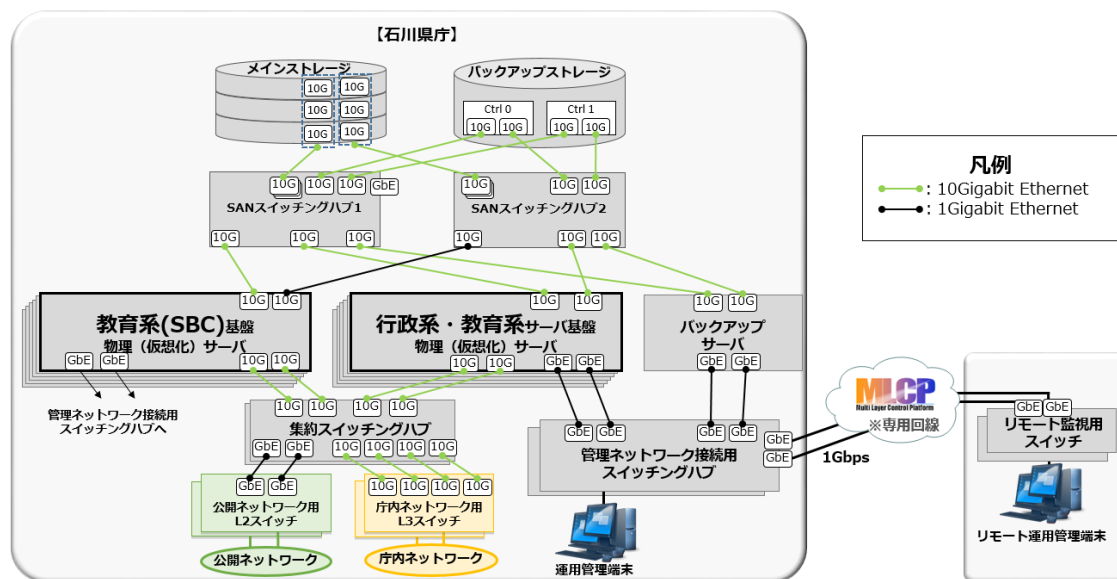
- ・ 業務アプリケーション機能
- ・ データベースなど静止点を必要とするバックアップ機能（必要時、当方が提供する個別バックアップ機能との結合試験を実施すること）
- ・ システム移行後の既存システム機器の撤去
- ・ その他、「2.2 統合基盤から提供されるもの」を逸脱する機能

2.4. 統合基盤と原課の役割分担

種別		統合基盤	原課
アプリケーション		・ VMwareToolsインストール ・ バックアップソフトインストール（個別バックアップ希望時） ・ ウイルス対策ソフトインストール(Linux) (Deep Security Agent)	・ 左記以外のアプリケーションの調達・導入・検証
ミドルウェア			・ インストール、設定、運用、管理
ウイルス対策	Windows (エージェントレス型)	・ ウイルスチェック、運用、管理 ・ インシデント発生時の処理が隔離の場合、感染ファイルの削除	・ インシデント発生時の対策
	Linux (エージェント型)	・ OSへのアプリインストール、テスト、ウイルスチェック、運用、管理 ・ インシデント発生時の処理が隔離の場合、感染ファイルの削除	・ インシデント発生時の対策
バックアップ	一括	・ バックアップ、リストア対応	
	個別 (任意)	・ 初期ソフトウェアインストール	・ バックアップスケジュールの設定、リストア
	スナップショット (任意)	・ スナップショット権限付与	・ スナップショットの取得・削除
OS		・ OSライセンス提供 (Windows / Linux) ・ 初期インストール (ネットワーク設定(IPアドレスのみ)、IPフィルタリング初期設定)	・ 必要なソフトウェアインストール、設定 ・ IPフィルタリングの適切な管理 ・ OSの運用 (OSに対するアップデート対応)
仮想化環境		・ 仮想サーバ作成・削除・変更 ・ 統合基盤全体のリソース管理	・ 仮想サーバ単体のリソース管理 ・ 運用管理端末を用いた仮想サーバ単体の設定
ハードウェア		・ 統合基盤の運用・保守、および運用管理端末の提供	・ 業務専用端末の調達（必要時のみ）

2.5. 統合基盤のシステム構成

統合基盤の構成機器を、県庁舎内ネットワーク管理室、監視センタに設置。



2.6. ハードウェア仕様

2.6.1. ストレージ

- ・メインストレージはオールフラッシュ/SolidfireHelix 構成(独自冗長方式)
- ・バックアップストレージは SSD+NL-SAS/RAID TEC 構成

2.6.2. ネットワーク

仮想サーバが接続可能なネットワークは以下の3種類。

(1) 公開系ネットワーク

- ・システムをインターネットに公開する場合のネットワーク。
- ・従来の DMZ と同じネットワーク。(ネットワークアドレスは固定)

(2) 庁内系ネットワーク

- ・システムを庁内のみで利用する場合のネットワーク。
- ・基本的に従来のネットワークと同じ。(既存システムが本ネットワークと異なる場合は、原則移行する必要あり)

(3) 仮想サーバ専用ネットワーク

- ・構築する仮想サーバ専用のネットワーク。
- ・上記のネットワークとは隔離されているためセキュア。(ネットワークアドレスは指定可能)

2.7. ソフトウェア仕様

VMware のバージョンは以下の通り。

コンポーネント	バージョン	用途
ESXi(vSphere)	6.7.0, 13006603	ハイパーバイザー (仮想化機能)
vCenter Server	6.7.0.31000	ESXi、仮想サーバの一元管理

3. 統合基盤の利用支援

3.1. システム移行

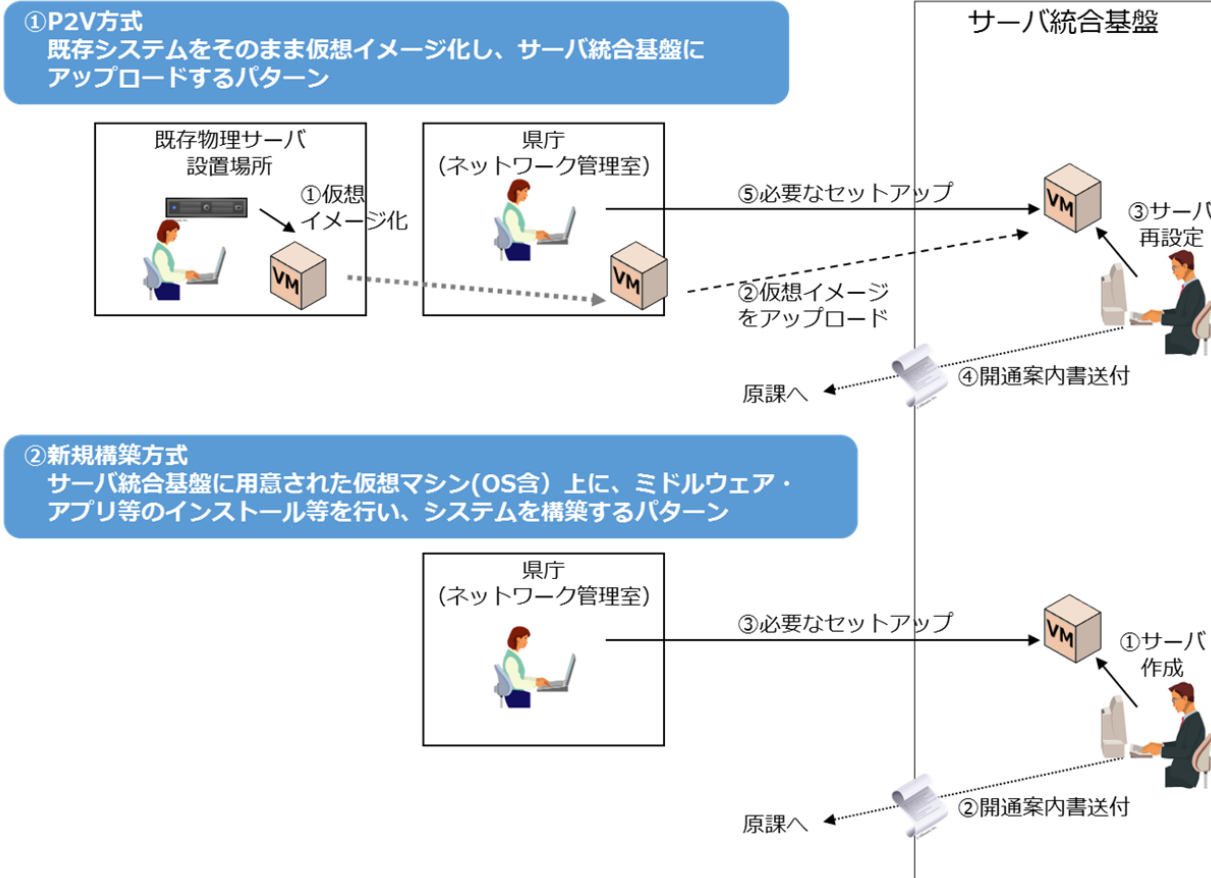
3.1.1. 移行手順

以下の手順で移行を実施する。

- ① 原課は、システム移行計画をデジタル推進課に提出
- ② 原課、デジタル推進課、統合基盤運用者の三者で事前協議を実施
(協議内容)
 - ・ 基盤への移行方法の決定 (P2V 方式 / 新規構築方式)
 - ・ 適切なサーバリソースサイズの決定
 - ・ 開発・検証環境の利用有無を決定 等
- ③ 原課は、事前協議で合意した仮想サーバリソースで利用申請書を提出
- ④ 統合基盤運用者は、利用申請書に基づき、仮想サーバを作成
- ⑤ 原課は、開発・検証環境を利用した動作検証を実施
- ⑥ 問題が無ければ、統合基盤運用者は、本番環境を設定
- ⑦ 原課は、本番環境で最終的な動作確認を行い、問題が無ければ、本番運用開始

3.1.2. 移行方法

以下の2通りから最適な移行方法を選択する。



3.1.3. 移行端末

- ・物理サーバを仮想サーバに変換するために必要な移行端末をデジタル推進課から貸与。
- ・変換ソフトは「VMware vCenter Converter Standalone」を利用。
- ・端末数には限りがあるため、使用する際はデジタル推進課と要調整。

3.2. 障害対応

- ・統合基盤において障害が発生した場合は、統合基盤運用者から影響がある原課に（自動）障害通知メール後に、電話またはメールで連絡する。
- ・統合基盤運用者から連絡が無い場合でも、仮想サーバの動作が遅いなど 異常を感じた場合は、障害受付窓口（24時間365日対応）まで連絡すること。
- ・障害箇所の確認を行い、障害原因の一次切り分けを行う。
- ・障害原因が統合基盤にある場合は、速やかに復旧作業を実施し、復旧後連絡を行う。
- ・原課は、復旧連絡受領後、システムの正常性確認を行うこと。

3.3. 問い合わせ対応

- ・ヘルプデスクを設置し、統合基盤が提供する機能や、運用管理端末の利用方法など、統合基盤に係る質問や相談への対応を行う。
- ・対応時間は、平日（土日祝日および年末・年始を除く）の 8 時 30 分から 17 時 45 分までとする。
- ・ヘルプデスクに連絡する前に、運用ポータルサイトの F A Qを確認し、知りたい情報が掲載されていないか確認の上、問い合わせること。

3.4. 運用ポータルサイト

統合基盤を利用する上で有用な情報をブラウザから閲覧出来る機能であり、以下の情報を開示。

- ・マニュアル類
- ・申請資料一式
- ・障害・メンテナンス情報
- ・よくある問い合わせ（FAQ）

4. 利用に当たっての留意事項

4.1. 統合基盤で利用出来ないもの

- ・SSL アクセラレータ、VPN ルータ等のネットワーク機器
- ・バックアップ専用ストレージ（N A S）
- ・テープドライブ等の外部記憶装置
- ・コールドスタンバイ構成における、スタンバイ側サーバの移行（アクティブ側サーバのみ移行対象）

4.2. システムリソースの最適化

- ・統合基盤では、各仮想サーバのリソース（CPU、メモリ、ディスク）稼働状況を採取し、定期的に分析を行う。
- ・稼働状況の実績に応じて、原課と協議のうえ、仮想サーバのリソースの割り当てを変更することがある。

4.3. 統合基盤の適正利用

利用システムの稼働状況およびセキュリティ対策等において統合基盤の安全かつ安定的な運用に支障が生じる状況が明らかとなった場合は、デジタル推進課からの指示に従い、適切に対応すること。

4.4. 統合基盤の Oracle の利用について

仮想化基盤での Oracle Database 利用は推奨しない。特別な理由がある場合は、デジタル推進課と協議を行い決定すること。

4.5. その他

統合基盤の利用および統合基盤へのシステム移行の実施にあたり、本仕様書に記載のない事項または疑義が発生した場合は、速やかにデジタル推進課と協議を行い、その内容について合意すること。