令和８年度

防災情報ネットワーク事業

システム要件定義書作成業務

仕様書（案）

農林水産省　関東農政局

目　次

第１章 総　則

第 1-1 調達件名

令和８年度　防災情報ネットワーク事業システム要件定義書作成業務

第 1-2 調達背景

現行の国営造成土地改良施設防災情報ネットワークシステム（以下「現行システム」という。）は、国営造成土地改良施設の有する水位等の観測情報や気象情報を迅速に収集、伝達、蓄積及び分析整理するためのシステムとして平成 21 年度に開発したものであり、令和７年度にリホストによるクラウド移行を行ったところである。

しかしながら、オンプレミスサーバー時のシステム構成を踏襲したことによりクラウドの特性を十分に活用できておらず、情報セキュリティの確保やシステムの運用・保守に要する年間費用について課題を抱えている。また、現行システムが抱えるデータ容量等の制限の最適化や、最新デバイスに適応した閲覧情報の改良など、ユーザビリティを向上させるための改善が求められている。

このため、現行システムを刷新し、新たな防災情報ネットワークシステム（以下「新システム」という。）を構築する必要があり、本業務は新システムの要件定義書を作成するものである。

平成 30 年６月には、「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」が決定（最終改定は、令和７年５月 27 日）された。この中で、「クラウド・バイ・デフォルトの原則」が政府方針として出されている。これらの状況を踏まえ、本システムはパブリッククラウドを利用する。

第 1-3 調達目的及び調達の期待する効果

本業務は、現行システムで課題となっている機能や、新たに活用したい機能の要件を整理し、優先順位を付けて新システムの要件定義書を作成することを目的とする。

これにより、システムのクラウドネイティブ化に伴う情報セキュリティの向上及び運用コストの低減並びに操作性・利便性の向上が図られるほか、将来の改修が容易となる新システムの構築が可能となる。

第 1-4 調達範囲

本調達では、新システムに係る要件定義書一式を作成する業務を行うものとし、受注者の責任範囲は、必要機能の整理から要件定義書一式の作成までの一連の要件定義全てとする。

なお、上記は責任分界の基本である。責任範囲の調整が必要となった場合には、発注者と協議の上、決定することとする。

第２章 作業概要

第 2-1 作業概要

主な作業概要は以下のとおりであり、詳細な作業内容は第 5 章に示す。

（1）業務実施計画書の作成
（2）現状の調査及び課題整理
（3）要件定義書一式の作成

(4) 設計・開発及び運用・保守に係る概算費用

(5) 定例会

(6) 業務結果報告書の作成

第 2-2 スケジュール

本業務の期間は、令和 8 年 4 月 24 日から令和 8 年 10 月 30 日とし、発注者が想定している作業スケジュール（案）は図１のとおりである。主なマイルストーンは（2）現状の調査及び課題整理の取りまとめ時点及び(3)要件定義書一式の作成に関する中間報告時点である７月中に設定する。

なお、本業務の対応は、土曜、日曜、国民の祝日に関する法律（昭和 23 年法律第 178 条）に規定する休日及び年末年始（令和 8 年 12 月 29 日から令和 9 年 1 月 3 日）を除く 8 時 30 分から 17 時 15 分を原則とするが、システム障害などの緊急時の対応は、監督職員の指示により、上記時間外に実施する場合がある。

作業概要	2026 年（R8）									2027 年（R9）			備考
	4	5	6	7	8	9	10	11	12	1	2	3	
(1)業務実施計画書の作成													
(2)現状の調査及び課題整理					マイルストーン								
(3)要件定義書一式の作成													
(4)設計・開発及び運用・保守に係わる概算費用													
(5)定例会													
(6)業務結果報告書の作成													
※関連スケジュール													
設計・開発業務（R9 年度予定）						見積依頼		調達仕様書等作成			調達手続き		

図１　作業スケジュール（案）

第 3 章 防災情報ネットワークシステムの概要

第 3-1 システムの概要

防災情報ネットワークシステムは、別紙１「防災情報ネットワーク対象地区一覧表」に示すとおり、令和７年３月時点で 185 地区において運用されている。

現行システムの利用環境は別紙３「システム利用環境等」に示すとおりであり、（別図１）「現行の国営造成土地改良施設防災情報ネットワークシステム概念図」及び（別図２）「現行の国営造成土地改良施設防災情報ネットワークシステム機器構成図」により、気象情報提供者から調達する気象情報を取り込むほか、全国の各国営事業地区の中央管理所で個別に開発導入されたデータ転送システムを通じて、中央管理所の計測情報・状態監視情報を取り込み、利用者に提供するとともに、内閣府が運用する総合防災情報システムに情報提供している。

新システムでは、システムのクラウドネイティブ化を図り、ガバメントクラウドで稼働する環境に移行する。

第 3-2 現状の課題

現行システムの操作性・利便性に関する内容において、現状抱えている課題として把握している内容は以下のとおり。

(1)機能上の課題

①現行システムのメール配信登録は１件ずつ入力する必要があるが、入力ミス防止の観点から外部

メールサービスを併用しており、クラウドシステム上のメールサービスとの一貫性がない。
②ブラウザバックによる戻る操作により、表示エラーが頻繁に発生し作業が中断される。
③スマートフォン等の最新デバイスでの操作閲覧が困難。
(2)非機能上の課題
①観測値をダウンロードする際、データ量が大きい場合にダウンロードエラーが生じるため、ユーザー側でダウンロードサイズを想定した観測期間等の設定を試行する必要がある（性能）。
②オンプレミスサーバー時のシステムでは、サーバ容量等から登録地区数を制限していたが、現行システムでも登録地区数の制限が踏襲されている（拡張性）。
③バックアップシステムへの切替え・切戻し作業において、現行システムでは切替え開始後３営業日間の時間を要している（継続性）。

第 4 章 作業条件

第 4-1 業務実施場所等

本業務は原則として受注者側拠点で行うものとする。本業務の作業場所及び作業に当たり必要となる設備、備品、消耗品等については、受注者の責任において用意すること。また、必要に応じて担当職員が現地確認を実施することができるものとする。

第 4-2 新システムのクラウドサービス環境

新システムで用いるクラウドサービスはガバメントクラウドとする。ガバメントクラウドの詳細は、デジタル庁 HP の GCAS Guide（https://guide.gcas.cloud.go.jp/）を参照すること。ガバメントクラウドのクラウドサービスプロバイダーは、AWS、Azure、Google cloud、Oracle Cloud の４種類である。

なお、現行システムのクラウドサービス環境は Amazon Web Services（以下「AWS」という。）東京リージョンを基盤（2AZ（アベイラビリティゾーン）構成）であり、クラウド構成図は、別紙３のとおりである。

第 4-3 使用する機器等

受注者側の拠点において本業務を実施するための機器、ＯＳ、開発ツール等の環境は受注者によって整備するものとする。

第 4-4 情報セキュリティ

(1) 受注者は、別に貸与する「農林水産省における情報セキュリティの確保に関する規則」（平成 27 年 3 月 31 日農林水産省訓令第４号）及び「国営造成土地改良施設防災情報ネットワークシステムのセキュリティ確保について（案）」に記載された関連項目を遵守し業務を実施しなければならない。なお、「農林水産省における情報セキュリティの確保に関する規則」及び「国営造成土地改良施設防災情報ネットワークシステムのセキュリティ確保について（案）」が改定された場合には、それらに基づき実施すること。

(2) 別紙４「情報セキュリティの確保に関する共通基本仕様」に基づき作業を行うこと。なお、「情報セキュリティの確保に関する共通基本仕様」が改定された場合には、それらに基づき実施すること。

(3) 本業務の実施に当たっては、セキュリティ上問題となりうるおそれのあるソフトウェアを使用してはならない。

(4) 本業務で使用する全ての情報に関して、アクセス制限を明確にしなければならない。
(5) 本業務で知り得た情報は、業務の遂行に使用する以外に使用し、又は提供してはならない。
(6) 業務を行う上で預託した情報については、業務完了時に返還（又は廃棄）しなければならない。
(7) 監督職員の求めに応じ、情報の管理状況について報告又は監査することを許諾すること。
(8) 業務実施期間中に情報セキュリティに関わる事項に違反した場合は、契約を打ち切り損害賠償の請求を行うことがある。
(9) 受注者は本業務で、システムの設置場所へ機器の搬入出を行う場合には、監督職員の立会いのもと行うと共に、内容の確認を受けなければならない。
(10) 本業務に従事する全ての者に対して、退職後も有効な守秘義務契約を個別に締結すること。
(11) マニュアル類は定められた場所に保管し、業務を遂行するに当たり知り得た情報は第三者に漏らしてはならないものとする。業務において知り得た情報の漏洩等の事案が発生した際には、発注者に電話、口頭等による報告を行うとともに、書面にて提出すること。なお、事案の発生後は事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。
(12) 「農林水産省における情報セキュリティの確保に関する規則」は、政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受注者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。
　また、適切な措置が講じられていることを確認するため、遵守状況の報告を求めることや、必要に応じて発注者による実地調査が実施できること。
(13) 生成 AI システム特有のリスクケース等が発生した場合、受注者は関係するデータの提供、調査等に協力すること。
(14) 本業務の開発・運用において、ソースコード解析やソースコード生成、ソースコードの管理を行う際には、セキュリティ・バイ・デザイン（DS-200）を元に、情報セキュリティ対策の責任者を定め、開発環境や開発工程等も含めたすべてのライフサイクルに対してぬけ漏れなく情報セキュリティ対策を実行すること。
(15) クラウドアーキテクストのベストプラクティス（AWS の場合 Well-Architected Framework、Azure の場合 Azure Well-Architected Framework、Google Cloud の場合 Google Cloud Architecture Framework、Oracle の場合 Well-architected framework for Oracle Cloud Infrastructure）及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 別冊クラウド設計・開発編」に準拠すること。
(16)以下の現行システムのセキュリティ対策要件を参照し、システムのセキュリティ対策要件を点検すること。
・AWS 設定確認リスト（別紙５）
・Web システム／Web アプリケーションセキュリティ要件書（別紙６）

第 4-5 業務責任者及び業務担当者等
(1) 受注者は本業務の実施に当たり業務責任者、チームリーダー及び業務担当者を定め、発注者に通知するものとする。また、業務責任者を変更するときは発注者の承認を得ること。
(2) 受注者は、本業務の業務責任者及び担当者等の役割に応じて次に示すスキル・経験を持つ人員を充て、プロジェクト全体として全ての要件を満たす作業実施体制とすること。
(3) 業務責任者は契約図書等に基づき、業務の技術上の管理及び統轄を行うものとする。
(4) 業務責任者は、情報処理技術者試験のうちプロジェクトマネージャ試験の合格者、PMI 本部が認

定するＰＭＰ資格又は技術士（情報工学部門又は総合技術監理部門（情報工学を選択科目とする者））の資格を有すること。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、農林水産省の理解を得ること）。なお、業務期間中に業務責任者を専任で支援する要員が保有していることでも可とする。

(5) 業務責任者及び業務担当者は、情報ネットワークのシステム構築業務又はシステム改良業務などの経験を１件以上有するものとする。

(6)チームリーダー及び業務担当者は以下の資格を有するものを含めること。

チームリーダーは、パブリッククラウドに係る全ての技術領域において当該提案予定のクラウドサービスプロバイダーの認定技術者としての上級資格[*1]を有する者を 1 名以上配置すること。

なお、チームリーダーの資格はパブリッククラウド上での情報システム構築期間中に専任でチームリーダーを支援する要員が保有していることでも可とする。または、クラウドサービスプロバイダーが提供するサポートサービス（AWS プロフェッショナルサービス、Azure 有償サポート、PSO プロフェッショナルサービス、Oracle プロフェッショナルサービス）の利用での対応も可とする。

業務担当者は、パブリッククラウドに係る全ての技術領域において当該クラウドサービスプロバイダーの認定技術者としての中級資格[*2]以上を有する者を 1 名以上配置すること。

例として、以下のような資格が挙げられる。

*1 AWS Certified Solutions Architect - Professional / Microsoft Certified: Azure Solutions Architect Expert / Google Cloud Professional Cloud Architect / Oracle Cloud Infrastructure 2024 Certified Architect Professional

*2 AWS Certified Solutions Architect - Associate / Microsoft Certified:Azure Administrator Associate Google Cloud Associate Cloud Engineer / Oracle Cloud Infrastructure 2024 Certified Architect Associate

(7) 本業務を行う担当者は、業務を効率的、効果的に推進するために求められる業務遂行能力を有すること。

・情報や意見を的確に交換できるコミュニケーション能力
・課題・改善点を識別し、改善する能力
・担当する職務に応じた技術力（クラウド業務を実施する場合は、AWS 等のスキル）

(8) 本仕様書に記載されている監督職員との協議事項等を業務責任者に委任しない場合は、書面により発注者に報告しなければならない。

第 4-6 提出書類

受注者は、発注者が指定した様式により、契約締結後に本仕様書及び契約書類に示す書類について、監督職員を経て発注者に遅延無く提出しなければならない。

受注者が発注者に提出する書類で様式が定められていないものは、受注者において様式を定め、提出するものとする。ただし、発注者がその様式を指示した場合は、これに従わなければならない。

第 4-7 業務実施計画書の作成

(1) 受注者は、契約締結後 14 日以内に業務実施計画書及び業務実施要領の案を作成し、監督職員の承認を受けること。

なお、業務実施計画書及び業務実施要領の記載内容は、「デジタル・ガバメント推進標準ガイドライン」（以下「標準ガイドライン」という。）「第７章設計・開発」で定義されている事項を踏まえ、以下の内容を記述し、作業実施計画書の内容に変更の必要が生じた場合は、変更の理由及び変更内容とともに修正された作業実施計画書を担当部署に書面にて届け出て承認を得ること。また、標準ガイドラインの改定があった場合には、これに対応すること。

また、受注者は、承認を得た作業実施計画書に基づき、本業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

① 全体スケジュール（作業工程名、各作業工程の実施内容、実施期間、作業担当、各作業工程の完了条件を含む。）
② WBS 及び詳細スケジュール（作成した WBS を元に、各作業の関連性（作業間の依存関係が明確になるようにスケジュールをガントチャートとして記述し、明確にすること。）、作業担当、開始･完了日等の制約、各作業項目の作業内容と成果物の関係を踏まえ整理するもの。）
③ プロジェクト体制図（要員数、要員の経験・スキル、連絡先、作業計画と要員配置との対応関係も含む。）
④ 会議体ルール
⑤ 要件定義手法
⑥ コミュニケーション管理（手段、様式を含む。）
⑦ 本業務の成果物を詳細に定義したドキュメント体系
⑧ ドキュメント管理（採番ルール、版数管理を含む。）
⑨ 情報セキュリティ管理（委託先等を含む。）
⑩ 作業体制の管理手法
⑪ 品質管理、品質基準の設定
⑫ リスク管理
⑬ 課題管理
⑭ 変更管理
⑮ その他（実施における前提条件、時間、予算等の制約条件等）

(2) 受注者は、業務計画書の内容を変更する場合には、監督職員に了解を得ることとし、重要な内容の変更をする場合には、その都度監督職員に変更業務計画書を提出しなければならない。

(3) 受注者は、監督職員が指示した事項については、さらに詳細な業務実施計画書に係る資料を提出しなければならない。

第 4-8 制限事項

本業務を遂行するにあたり、知り得た情報は外部に漏らしてはならない。

第 4-9 調達案件及び関連調達案件の調達単位、調達方式等

本調達案件及び関連する調達案件の調達単位、調達方式、実施時期等は表 1 のとおりである。

表１　関連する調達案件

No	調達案件名(予定)	調達の方式	実施時期(予定) 又は受注者名
1	防災情報ネットワーク事業 システム要件定義書作成業務（本業務）	一般競争入札 （総合評価落札方式）	入札公告：R8.1 月頃 ※調整中 落札者決定：R8.4 月頃
2	防災情報ネットワーク事業 システム運用・保守・クラウドサービス提供業務 （履行期間 R8.4.1-R9.3.31 予定）	一般競争入札 （総合評価落札方式）	入札公告：R7.12 月頃 落札者決定：R8.3 月頃
3	防災情報ネットワーク事業 気象情報利用業務（履行期間 R8.4.1-R9.3.31 予定）	一般競争入札 （最低価格落札方式）	入札公告：R8.3 月頃 落札者決定：R8.3 月頃

また、表１に示す調達案件以外の関連業務が発生した場合、関連業務契約の都度、監督職員より通知するものとする。

第 4-10 作業の実施体制・方法

本件受注者に求める作業実施体制は図２及び表２のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上見直しを行うが、業務実施にあたり、別途契約の受注者の協力が必要な場合は、発注者が受注者間の調整を行う。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

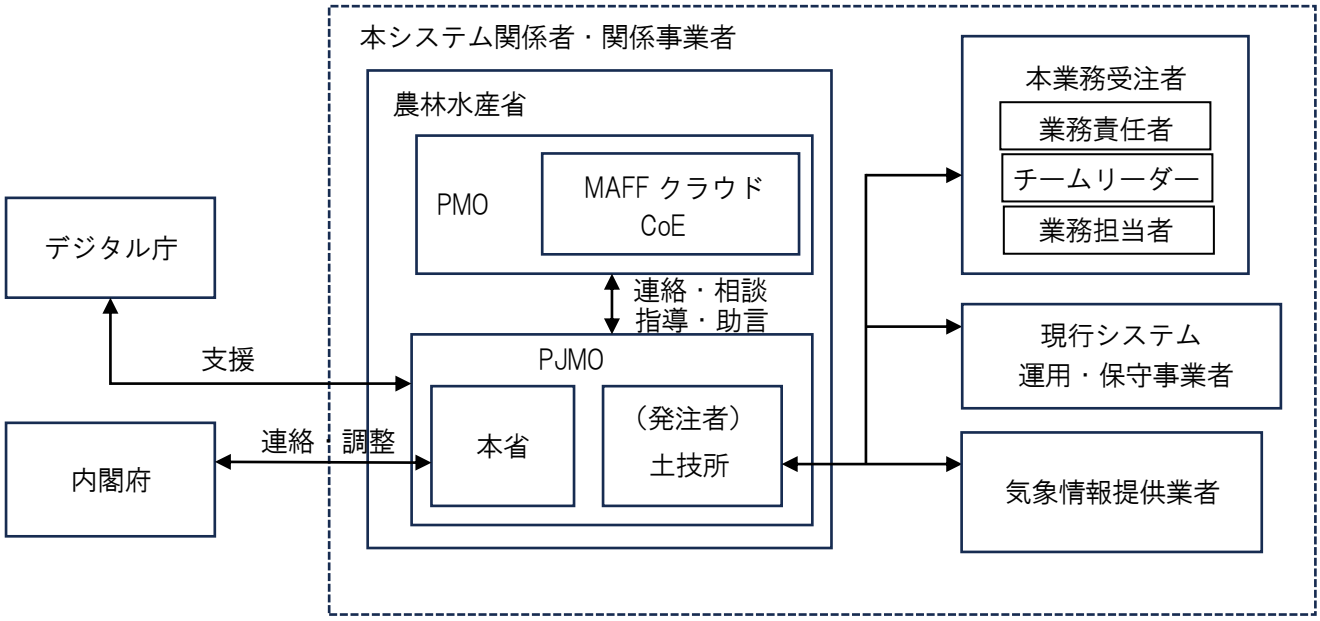


図２　作業実施体制

表２　組織または要員の役割

No	組織または要員	役　割
1	担当部署	防災情報ネットワークシステムの管理組織として、本業務の進捗等を管理する。
2	本業務受注者	本業務を実施する。
3	現行システム運用・保守事業者	現行システムの運用保守を行う。
4	気象情報提供業者	防災情報ネットワークシステムへ気象データの提供を行う。
5	内閣府総合防災情報システム担当課	総合防災情報システムと防災情報ネットワークシステム間の情報連携に当たり、担当部署と調整、情報共有等を行う。
6	PMO	農林水産省の全体管理組織。クラウド利用を含む情報システムに関する各 PJMO からの問い合わせを受け、対応、助言・指導等を行う。
7	MAFF クラウド CoE	担当部署・受注者に対してパブリッククラウド全般及び MAFF クラウド利用に係る技術的な支援を行う。 利用システムに対して、全体クラウド CoE から提示された方針や基準を実施できるように支援を行う。

No	組織または要員	役　割
8	デジタル庁	ガバメントクラウドの所管組織。全体クラウド CoE として、以下の 3 つの役割を担う。 ・ガバメントクラウドの方針や基準等の戦略を立案し、各府省クラウド CoE に提示を行う。 ・政策優先度の高いプロジェクトに対して、ガバメントクラウドの方針や基準を実施できるように支援を行う。 ・各府省クラウド CoE 体制不足時の支援を行う。
9	業務責任者	本業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。
10	チームリーダー	作業状況の監視・監督を担う。
11	業務担当者	要件定義の作業を担当する。

第 4-11 情報資産管理標準シートへの情報提供

(1) 受注者は、標準ガイドラインの「別紙３ 調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」に基づく情報資産管理を行うために必要な事項を記載した情報資産管理標準シートを提出すること。

(2) 受注者は、標準ガイドラインの「別紙２ 情報システムの経費区分」に基づき区分等した契約金額の内訳が記載されたエクセルの電子データを契約締結後速やかに提出すること。なお、人件費については人件費単価ごとに工数を提示すること。再委託先がある場合は再委託先の法人番号と再委託金額を提示すること。最大何次請負、再委託総額、累計契約額(前年度まで)、年度契約金額を提示すること。

第 4-12 クラウドサービス利用時の情報システムの保護に関する事項

(1) 情報システム、情報システムで取り扱うデータ等の情報資産の所有権その他の権利がクラウドサービスプロバイダーに帰属せず、また、発注者からクラウドサービスプロバイダーに移転されるものでないこと。

(2) クラウドサービスの利用にあたり、情報資産が漏えいすることがないよう、必要な措置を講じること。

(3) 現在利用しているクラウドサービスの解約に伴うデータの削除については、クラウドサービスプロバイダーが定めるデータ消去の方法で、データ削除し、削除したことを証明する資料を提出すること。なお、クラウドサービスの契約を移管する場合は当たらない。

第 5 章 業務実施内容

第 5-1 業務内容

本業務における業務内容は以下のとおりである。

(1) 現状の調査及び課題整理

1) 現行システムの現状・課題の整理

受注者は、発注者が提供する現行システムの操作マニュアル、各種設計書等の既存資料の情報や利用者の要望事項を基に本システムの現状と課題を把握し、整理する。

なお、本作業においては、課題の詳細を把握するため、現行システム利用者（５団体程度）へのヒアリングを実施する。

2）課題に対する対応方針の検討

受注者は、上記 1)で整理した現状と課題を踏まえ、それぞれの課題への対応方針を検討する。

3）検討結果の取りまとめ

受注者は、上記 1)～2)の整理及び検討結果をもとに、課題改善後の新たな業務フロー図及びシステム化範囲等を検討し、要件定義書一式の基礎資料となるよう取りまとめる。

(2) 要件定義書一式の作成

受注者は、上記(1) の結果を基に、新システムに必要な要件（業務要件、機能要件、非機能要件）について検討する。

本業務において検討したリファレンスアーキテクチャによる実装方式は、発注者と協議の上、決定する。また、必要に応じ MAFF クラウド CoE と事前協議すること。

これらの結果を要件定義書一式として取りまとめ具体的な内容を記載するとともにシステム構成図を作成する。

要件定義書一式の作成に当たっては、政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（2023 年 9 月 29 日版）、及び GCAS Guide への準拠を前提に、標準ガイドライン」、「デジタル・ガバメント推進標準ガイドライン解説書」、「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」及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2022 年 7 月 29 日 内閣サイバーセキュリティセンター)」を用いて要件定義内容をチェックするとともに別紙７ の様式で記載する。

また、要件定義書一式は、新システムの設計・開発の調達仕様書作成において重要な基礎資料となることから、マイルストーンを設置し要件定義書一式に関する中間報告書を作成する。

併せて中間報告会を 7 月中に実施し、方向性の確認を行う。

(3) 設計・開発及び運用・保守に係る概算費用

受注者は、上記(2) の成果を基に、設計・開発及び運用・保守に必要な概算費用について自社のこれまでの実績から算出する。

(4) 定例会

受注者は、進捗会議を隔週に１回開催し、業務の進捗状況等を報告すること。

なお、開催方法は対面形式又はリモート会議形式を状況に応じて適宜決定する。

発注者から要請があった場合、又は、受注者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

受注者は、会議終了後、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、発注者の承認を受けること。

定例会の参加者は、以下のメンバーとする。

・農林水産省関東農政局土地改良技術事務所（発注者）

・農林水産省農村振興局整備部防災課 災害・減災対策室

・農林水産省大臣官房デジタル戦略グループ情報管理室

なお、初回の定例会において、受注者は実施計画書に基づき説明を行い、土地改良技術事務所から現行システムの説明を受けること。

(5) 業務結果報告書の作成

受注者は、以下の内容を含む業務結果報告書を作成し、発注者の承認を得ること。

・本調達の概要
・上記(1)～(4) で作成した資料

第 5-2 業務実施に当たっての留意点

(1) 本業務の遂行に当たっては、「デジタル社会推進標準ガイドライン群」のうち標準ガイドライン（政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント）に該当する以下の①から⑥に基づくこと。また、具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン解説書」を参考とすること。なお、デジタル社会推進標準ガイドライン群が改定された場合は、最新のものを参照し、その内容に従うこと。

① DS-100 デジタル・ガバメント推進標準ガイドライン
② DS-310 政府情報システムにおけるクラウドサービスの適切な 利用に係る基本方針
③ DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン
④ DS-900 Web サイト等の整備及び廃止に係るドメイン管理ガイドライン
⑤ DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い
⑥ DS-920 行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン

(2) インターネット公開するシステムは原則として政府系ドメイン（go.jp）を用いること。

(3) 本業務の遂行に当たっては、農林水産省が定めるプロジェクト計画書との整合を確保して行うこと。また、本業務における検討結果をプロジェクト計画書に適宜反映するとともに、プロジェクト計画書を段階的詳細化し、内容変更の支援をすること。

(4) 新たな要件の策定にあたっては、政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針記載の留意事項等を参考に、クラウドサービスの利用に適した刷新に向け、適切に作業を進めること。

(5) アーキテクチャ実装方式を検討する際、CI/CD を原則とする開発・運用方式を検討すること。

(6) 合理的な調達単位の検討において、CI/CD 実施による開発と運用保守の一体化等、担当部署による調達単位の整理を技術的観点から支援すること。

(7) アーキテクチャ実装方式を検討する際、以下の１）から３）の観点に基づき、実装方式を検討（又は見直し）すること。その際、ガバメントクラウドが用意するリファレンスアーキテクチャ等を積極的に活用すること。ただし、デジタル庁ＨＰ（https://guide.gcas.cloud.go.jp/）に掲載されている GCAS Guide の「リファレンスアーキテクチャ」に記載された構成を参考に各ブロックを単純に組み合わせたり、アーキテクチャイメージを単純に踏襲したりするだけでなく、本システムに最適化された構成での提案を行うこと。なお、当該提案内容は、各府省におけるシステム品質向上のため、ベストプラクティスとして共有されうる旨留意すること。
また、UX を担うフロントエンドと業務処理を担うバックエンドは独立的に検討すること。
上記検討内容は、発注者に加え、必要に応じて MAFF クラウド CoE と事前協議すること。

１）旧来技術からの脱却
旧来型のセキュリティ対策、多階層の大規模な画面構成、クライアントサーバ方式、Web 三層モデル、シンクライアント（VDI 等）、法定帳票以外の多数の帳票、夜間バッチ、紙での月次運用報告等、人海戦術的な運用作業等の排除を検討すること
２）システムやアプリケーションのモダン化
３）アジャイルと CI/CD を原則とする開発・運用方式のモダン化

(8) 合理的な調達単位の検討において、CI/CD 実施による開発と運用保守の一体化等、担当部署によ

る調達単位の整理を技術的観点から支援すること。

(9) 費用見積について、開発及び運用に係る概算見積を作成すること。当該見積りには、ガバメントクラウドに係るクラウド利用料も含めること。

(10) ガバメントクラウド利用には、デジタル庁の技術審査が必要とされる。加えて、「設計・開発、運用・保守に係る概算費用」に基づく投資対効果の分析の結果、ガバメントクラウドに係るクラウド利用料変動が生じる場合、デジタル庁の承認が必要となる。また、当省 PMO（MAFF クラウド CoE）は、当省内各システムによる予算要求の取りまとめ、モダナイズを通じたコスト適正化及び進捗管理を実施しており、新システム構築に向けて調整等を実施することが求められる。
上記を踏まえ、担当部署がデジタル庁、当省 PMO その他の関係者と調整等を実施する際、資料作成、会議参加等必要な支援を行うこと。

(11)「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2025 年 7 月 1 日国家サイバー統括室）」の点検を行い、要件定義書に反映すること。

(12) 受注者は、要件定義の作業経緯、残存課題等を文書化し、担当部署に対して確実な引継ぎを行うこと。

(13) 当該調達案件の業務の管理に当たっては、農林水産省が定めるプロジェクト管理要領との整合を確保して行うこと。

(14) 情報システム監査の実施

本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために、農林水産省が情報システム監査の実施を必要と判断した場合は、農林水産省が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を受注者は受け入れること（農林水産省が別途選定した事業者による監査を含む。）。

情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担当部署と協議し、指示された期間までに是正を図ること。

(15) 当該調達案件の業務遂行に当たっては、担当部署が定めるプロジェクト計画書との整合を確保して行うこと。

(16) 当該調達案件の業務の管理に当たっては、担当部署が定めるプロジェクト管理要領との整合を確保して行うこと。

(17) 受注者は、要機密情報を取り扱う場合、クラウドサービス選定においては「政府情報システムにおけるセキュリティバイデザインガイドライン　別紙 5 政府情報システムにおけるクラウドセキュリティ要件策定、審査手順」に従い、クラウドサービスの選定を行うこと。

(18) パブリッククラウド上に保管されたデータについては、ISMAP で規定された方法でデータが消去されていること、それが正しく運用されているか第三者による監査により証明されていること。

(19) パブリッククラウド利用時の情報システムの構成やインスタンスタイプ、利用するマネージドサービスが記載されているか。MAFF クラウド CoE に相談し、事前に方針を確認すること。

(20)ガバメントクラウドについて不明点等がある場合は、担当部署及び全体クラウド CoE と協議の上、作業を進めること。

(21) 農林水産省が本システムの更改を行う際には、次期の情報システムにおける要件定義支援事業者及び設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

(22) その他特記事項

本調達仕様書と契約書の内容に齟齬が生じた場合には、本調達仕様書の内容が優先すること。

第 6 章 貸与資料等

貸与資料等は下記のとおりであり、監督職員の請求があった場合はその時点で、それ以外は完了検査時に一括返納しなければならない。

第 6-1 貸与資料

(1)「農林水産省における情報セキュリティの確保に関する規則」(平成 27 年３月 31 日農林水産省訓令第４号)

(2) 国営造成土地改良施設防災情報ネットワークシステムのセキュリティ確保について（案）

(3) 現行システムの関係資料

1) 令和 2 年度国営造成土地改良施設防災情報ネットワーク事業システム改良業務　報告書

（現行システムの「システム要件定義書」、「ソフトウェア方式設計書」、「切替え・切戻し手順書」を含む）

2) 令和 7 年度防災情報ネットワーク事業 システム運用・保守・クラウドサービス提供業務　報告書（現行システムの「運用・保守計画」、「運用・保守実施要領」を含む）

3) その他関係資料は以下のとおりである。

- 平成 19 年度 国営造成土地改良施設防災情報ネットワークの構築に係る業務・システム最適化計画の策定等委託業務 報告書
- 平成 20 年度 国営造成土地改良施設防災情報ネットワークの構築に係る調査検討・実証等委託業務報告書
- 国営造成土地改良施設防災情報ネットワーク防災中央データセンターシステム開発業務 報告書
- 国営造成土地改良施設防災情報ネットワーク情報提供システムデータ等整備業務 報告書
- 国営造成土地改良施設防災情報ネットワーク防災中央データセンターシステム連携開発業務 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワークシステム運用業務 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワークシステム保守業務 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワークシステム運用支援業務（その１） 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワーク事業
- 国営造成土地改良施設防災情報ネットワークシステム機能検討業務（その１） 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワーク事業
- 国営造成土地改良施設防災情報ネットワークシステム機能検討業務（その２） 報告書
- 平成 23 年度国営造成土地改良施設防災情報ネットワーク事業
- 国営造成土地改良施設防災情報ネットワークシステム機能検討業務（その３） 報告書
- 平成 24 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
- 平成 24 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
- 平成 24 年度国営造成土地改良施設防災情報ネットワーク事業 システム接続支援業務 報告書
- 平成 24 年度国営造成土地改良施設防災情報ネットワーク事業 システム改良検討業務 報告書
- 平成 25 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
- 平成 25 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
- 平成 25 年度国営造成土地改良施設防災情報ネットワーク事業 システム改良検討業務 報告書
- 平成 26 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書

・平成 26 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 26 年度国営造成土地改良施設防災情報ネットワーク事業 システム詳細設計業務 報告書
・平成 27 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
・平成 27 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 27 年度国営造成土地改良施設防災情報ネットワーク事業 システム開発業務 報告書
・平成 28 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
・平成 28 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 28 年度国営造成土地改良施設防災情報ネットワーク事業 情報活用検討業務 報告書
・平成 29 年度国営造成土地改良施設防災情報ネットワーク事業 システム設定業務 報告書
・平成 29 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
・平成 29 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 30 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
・平成 30 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 30 年度国営造成土地改良施設防災情報ネットワーク事業 システム詳細設計業務 報告書
・平成 31 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・平成 31 年度国営造成土地改良施設防災情報ネットワーク事業 システム設定業務 報告書
・令和元年度国営造成土地改良施設防災情報ネットワーク事業　防災情報ネットワークシステム改良業務 報告書
・令和元年度国営造成土地改良施設防災情報ネットワーク事業　防災情報ネットワーク接続支援業務 報告書
・令和 2 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用業務 報告書
・令和 2 年度国営造成土地改良施設防災情報ネットワーク事業 システム保守業務 報告書
・令和 2 年度国営造成土地改良施設防災情報ネットワーク事業 システム改良業務 報告書
・令和 2 年度国営造成土地改良施設防災情報ネットワーク事業 接続支援業務 報告書
・令和 3 年度国営造成土地改良施設防災情報ネットワーク事業 システム運用・保守業務 報告書
・令和 4 年度防災情報ネットワーク事業 システム運用・保守業務 報告書
・令和 5 年度防災情報ネットワーク事業 システム運用・保守業務 報告書
・令和 5 年度防災情報ネットワーク事業 防災情報ネットワークシステムデータベースのクラウド移行に向けた検討業務 報告書
・令和 6 年度防災情報ネットワーク事業 システム運用・保守業務 報告書
・令和 6 年度防災情報ネットワーク事業 防災情報ネットワークシステム設定業務 報告書
・令和 7 年度防災情報ネットワーク事業 システム運用・保守・クラウドサービス提供業務 報告書
・令和 7 年度防災情報ネットワーク事業　システム改修業務　報告書
・令和 7 年度防災情報ネットワーク事業　システム改良検討業務　報告書

(4) 閲覧に当たっては、複写や写真撮影等による閲覧内容の記録は禁止する。また、閲覧を希望する資料によっては、情報セキュリティ確保等の観点から閲覧できない場合がある。

ガバメントクラウドを利用する場合は、以下の GCAS サイトにアクセスし情報を確認してください。

https://guide.gcas.cloud.go.jp/

閲覧に供する資料の例を次に示す。

・プロジェクト計画書、プロジェクト管理要領
・プロジェクト標準（標準コーディング規約、セキュアコーディング規約等）
・農林水産省クラウド利用ガイドライン及び関係資料
・関連する他の情報システムの操作マニュアル、設計書、各種プロジェクト標準

第 7 章 成果物

第 7-1 成果物

本業務の成果物は、以下のとおりであり、改定の無い文書も添付する。

なお、成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受注者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書等にて権利譲渡不可能と示されたもの以外は、全て発注者に帰属するものとする。

受注者に帰属する知的財産権を利用して本業務を行う場合、発注者及びシステム利用者に受注者の知的財産権の利用を許諾する範囲及び制約を受注者が周知すること。

発注者は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、受注者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により発注者がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

本調達に係る成果物の権利（著作権法第 21 条から第 28 条までに定める全ての権利を含む。）及び所有権は、検収に合格した成果物の引渡しを受けたとき受注者から発注者に移転するものとする。

納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受注者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続きを行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前に発注者の承認を得ることとし、発注者は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら発注者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こと。この場合、発注者は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

受注者は発注者に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

受注者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

生成 AI を活用したシステムを構築・運用する場合、生成 AI で作成したアウトプットや本業務で作成した生成 AI 向けの指示文については、農林水産省に権利が帰属するものとする。

受注者は、本業務の改修要件を満たすための詳細設計を行い、既存の各種設計書類に反映をし、成果物について担当部署の承認を得ること。

受注者に帰属する知的財産権を利用して本業務を行う場合、発注者及びシステム利用者に受注者の知的財産権の利用を許諾する範囲及び制約を受注者が周知すること。

（1）業務報告書

成果物は以下に示すとおり計画しているが、成果物に追加・削除が生じた場合は、監督職員と協議するものとする。

表4 成果物一覧

No.	成果物名	内容及び納品数量	納品期日
1	本業務での起票シート	一式	令和8年10月30日
2	作業報告一覧表		
3	協議の記録等		
4	リリースノート		
5	契約金額の内訳		契約締結日から14日以内
6	業務実施計画書		
7	情報資産管理標準シート		担当部署から依頼された場合、速やかに提出
8	業務フロー		令和8年10月30日
9	業務結果報告書		

第 7-2 成果物の納品方法等

（1）成果物の納品方法

1） 成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

2） 用字・用語・記述符号の表記については、「公用文作成の考え方（令和 4 年 1 月 11 日内閣官房長官通知）」を参考にすること。

3） 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。

4） 作成した成果物は担当部署が指定したサーバへ納品（例：PrimeDrive 又は SharePoint 等）すること。なお、納品の際は、検収が終了したファイル一式を時点がわかるような形式（例：zip 等）で提出すること。

5） サーバ納品について、Microsoft Office 又は PDF のファイル形式で作成すること。

6） 納品後、農林水産省において改変が可能となるよう、図表等の元データも併せて納品すること。

7） 成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。

8） 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

9） 不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

10）上記に加えて紙媒体についても作成し、発注者から特別に示す場合を除き、原則紙媒体は２部を納品すること。

11）紙媒体による納品について、用紙のサイズは、原則として日本産業規格 A 列４番とする

が、必要に応じて日本産業規格 A 列３番を使用すること。

(2) 成果物の納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、発注者が納品場所を別途指示する場合はこの限りではない。

〒332-0026
埼玉県川口市南町 2-5-3
農林水産省関東農政局土地改良技術事務所　防災・災害対策技術課
（電話：048-278-4683）

(3) 契約不適合責任

1) 農林水産省は検収（「検査」と同義。以下同じ。）完了後、納入された成果物について調達仕様書との不一致（バグも含む。以下「契約不適合」という。）が発見された場合、受注者に対して当該契約不適合の修正等の履行の追完（以下「追完」という。）を請求することができる。この場合において、受注者は、当該追完を行うものとする。ただし、農林水産省が追完の方法を指定して追完を請求した場合であって、農林水産省に不相当な負担を課するものでないときは、受注者は農林水産省が指定した方法と異なる方法による追完を行うことができる。

2) 前記 1)の場合において、追完の請求にも関わらず相当の期間内に追完がなされないときは、農林水産省は、その不適合の程度に応じて支払うべき金額の減額を請求することができる。

3) 前記 2)の規定にかかわらず、次に掲げる場合には、農林水産省は、相当の期間の経過を待つことなく、直ちに支払うべき金額の減額を請求することができる。

ア 追完が不能であるとき。

イ 受注者が追完を拒絶する意思を明確に表示したとき。

ウ 特定の日時又は一定の期間内に履行をしなければ本調達の目的を達することができない場合において、受注者が追完をしないでその時期を経過したとき。

エ アからウまでに掲げる場合のほか、農林水産省が追完の請求をしても追完を受ける見込みがないことが明らかであるとき。

4) 農林水産省は、当該契約不適合（受注者の責めに帰すべき事由により生じたものに限る。）により損害を被った場合、受注者に対して損害賠償を請求することができる。

5) 当該契約不適合について、追完の請求にもかかわらず相当期間内に追完がなされない場合又は追完の見込みがない場合であって、当該契約不適合により本契約の目的を達することができないときは、農林水産省は本契約の全部又は一部を解除することができる。

6) 前記 1)から 5)までの規定にかかわらず、受注者が種類又は品質に関して契約の内容に適合しない成果品を農林水産省に引き渡した場合において、農林水産省が検収完了後１年以内に当該契約不適合について通知しないときは、農林水産省は、本仕様書に定める契約不適合責任に係る請求をすることができない。ただし、成果品を納入した時において受注者が当該契約不適合を知り、若しくは重過失により知らなかったとき、又は当該契約不適合が受注者の故意若しくは重過失に起因するときはこの限りでない。

7) 前記 1)から 5)までの規定にかかわらず、契約不適合が農林水産省の与えた指示によって生じたときは適用しないこと。ただし、受注者がその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りでない。

(4) 検収

1) 本業務の受注者は、成果物等について、納品期日までに農林水産省に内容の説明を実施して検収を受けること。

2） 検収の結果、成果物等に不備又は、誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について農林水産省に説明を行った上で、指定された日時までに再度納品すること。

第 8 章 入札参加資格に関する事項

第 8-1 競争参加資格

ア　予算決算及び会計令第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

イ　公告日において令和７・８・９年度全省庁統一資格の「役務の提供等」の「A」、「B」、「C」又は「D」の等級に格付けされ、競争参加資格を有する者であること。

第 8-2 公的な資格や認証等の取得

ア　入札参加者は、品質マネジメントシステムに係る以下のいずれかの条件を満たすこと。

（ア）品質マネジメントシステムの規格である「JIS Q 9001」又は「ISO9001」（登録活動範囲が情報処理に関するものであること。）の認定を、業務を遂行する組織が有しており、認証が有効であること。

（イ）上記と同等の品質管理手順及び体制が明確化された品質マネジメントシステムを有している事業者であること（管理体制、品質マネジメントシステム運営規程、品質管理手順規定等を提示すること。）。

イ　入札参加者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。

（ア）情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC27001」又は「ISMS」の認証を有しており、認証が有効であること。

（イ）一般財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けているか、又は同等の個人情報保護のマネジメントシステムを確立していること。

（ウ）個人情報を扱うシステムのセキュリティ体制が適切であることを第三者機関に認定された事業者であること。

第 8-3 受注実績等

入札参加者は、以下の要件をすべて満たしていること。

ア　入札参加者は、パブリッククラウドサービス上に、システムの要件定義又は Web アプリケーションの設計・開発、運用保守に係る業務実績を過去５年以内に有すること。

イ　入札参加者は、レガシーシステムをモダンなアプリケーションへの刷新に向けた基本構想策定又は要件定義を支援した実績を過去５年以内に有すること。

第 8-4 複数事業者による共同入札

ア　複数の事業者が共同提案する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

イ　共同提案を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事

項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

ウ　共同提案を構成する全ての事業者は、本入札への単独提案又は他の共同提案への参加を行っていないこと。

エ　共同事業体の代表者は、品質マネジメントシステム及び情報セキュリティに係る要件について満たすこと。その他の入札参加要件については、共同事業体を構成する事業者のいずれかにおいて満たすこと。

第 8-5 入札制限

ア　本業務に関連する調達間での入札制限は設けない。

イ　本業務を直接担当する農林水産省 IT アドバイザー（デジタル統括アドバイザーに相当）、農林水産省全体管理組織（ＰＭＯ）支援スタッフ及び農林水産省最高情報セキュリティアドバイザーが、その現に属する事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」　（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社並びに請負先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。

第 9 章 契約変更

請負契約書に規定する発注者と受注者による協議事項は次のとおりとする。ただし、軽微な変更については、協議の上契約変更しないものとする。

(1) 第 4 章に示す「作業条件」に変更が生じた場合

(2) 第 5 章に示す「業務実施内容」に変更が生じた場合

(3) 第 7 章に示す「成果物」に変更が生じた場合

(4) 履行期間に変更が生じた場合

第 10 章 再請負に関する事項

(1) 再請負の制限及び再請負を認める場合の条件

ア　本業務の受注者は、業務を一括して又は主たる部分を再請負してはならない。

イ　受注者における業務責任者を再請負先事業者の社員や契約社員とすることはできない。

ウ　受注者は再請負先の行為について一切の責任を負うものとする。

エ　再請負先における情報セキュリティの確保については受注者の責任とする。

オ　再請負を行う場合、再請負先が「8-5 入札制限」に示す要件を満たすこと。

(2) 承認手続

ア　本業務の実施の一部を合理的な理由及び必要性により再請負する場合には、あらかじめ再請負の相手方の商号又は名称及び住所並びに再請負を行う業務の範囲、再請負の必要性及び契約金額等について記載した別添の再請負承認申請書を農林水産省に提出し、あらかじめ承認を得ること。

イ　前項による再請負の相手方の変更等を行う必要が生じた場合も、前項と同様に再請負に関する書面を農林水産省に提出し、承認を得ること。

ウ　再請負の相手方が更に請負を行うなど複数の段階で再請負が行われる場合（以下「再々請負」という。）には、当該再々請負の相手方の商号又は名称及び住所並びに再々請負を行う業務の範囲を書面で報告すること。

(3) 再請負先の契約違反等

再請負先において、本仕様書の遵守事項に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、農林水産省は、当該再請負先への再請負の中止を請求することができる。

第 11 章 環境関係法令等の遵守

第 11-1 環境法令の遵守

受注者は、物品・役務（委託事業を含む）の提供に当たり、関連する環境関係法令を遵守するものとする。

(1) エネルギーの節減

・エネルギーの使用の合理化及び非化石エネルギーへの転換等に関する法律（昭和 54 年法律第 49 号）

(2) 廃棄物の発生抑制、適正な循環的な利用及び適正な処分

・廃棄物の処理及び清掃に関する法律　（昭和 45 年法律第 137 号）

・国等による環境物品等の調達の推進等に関する法律　（平成 12 年法律第 100 号）

・プラスチックに係る資源循環の促進等に関する法律（令和３年法律第 60 号）

(3) 環境関係法令の遵守等

・労働安全衛生法　（昭和 47 年法律第 57 号）

・地球温暖化対策の推進に関する法律　（平成 10 年法律第 117 号）

第 11-2 環境負荷低減に係る遵守事項

受注者（受注者）は、役務（委託事業を含む）の提供に当たり、新たな環境負荷を与えることにならないよう、事業の最終報告時に別紙８の様式を用いて、以下の取組に努めたことを、環境負荷低減のクロスコンプライアンス実施状況報告書として提出すること。なお、全ての事項について「実施した／努めた」又は「左記非該当」のどちらかにチェックを入れるとともに、ア～エの各項目について、一つ以上「実施した／努めた」にチェックを入れること。

(1) 環境負荷低減に配慮したものを調達するよう努める。

(2) エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

(3) 廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

(4) みどりの食料システム戦略の理解に努める。

第 11-3 行政の進化と革新のための生成 AI の調達・利活用に係るガイドラインへの対応

本業務の遂行に当たっては、生成 AI を活用する場合、「デジタル社会推進標準ガイドライン DS-920　行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン 別紙３調達チェックシート」の基本項目を満たすこと。本業務においては、国民等による農林水産省外利用の場合、個人情報、プライバシー、知的財産を取り扱う場合の要件についても対応すること。行政の進化と革新のための生成 AI の調達・利活用に係るガイドラインが改定された場合は、最新のものを参照し、その内容に従うこと。

第 11-４ IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ

本業務の遂行に当たっては、生成 AI を活用する場合、納入候補となる機器・役務等について、令和８年３月５日（又は提案書、証明書等の提出期限）までに、担当部署へ機器等リスト（区分（ノート PC 等)、業者・役務実施業者名、製造業者の法人番号、製品名・役務実施場所、型番等を記載したリスト）を提出することとし、農林水産省においてサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、速やかに担当部署に確認した上で、代替品の選定等、納入候補となる機器・役務等を見直すこと。

第 12 章 定めなき事項

本仕様書に定めのない事項又は、本業務の施行に当たり疑義が生じた場合は、必要に応じて、監督職員と速やかに協議しなければならない。

本調達仕様書と契約書の内容に齟齬が生じた場合には、本調達仕様書の内容が優先するものとする。

別紙1　防災情報ネットワーク対象地区一覧表

局名	県名	地区名	現況
東北	青森	津軽北部	運用中
東北	青森	浪岡川	運用中
東北	青森	平川	運用中
東北	青森	岩木川左岸	運用中
東北	青森	小田川	運用中
東北	青森	八戸平原	運用中
東北	青森	浅瀬石川	運用中
東北	岩手	山王海	運用中
東北	岩手	藤沢	運用中
東北	岩手	豊沢川	運用中
東北	岩手	馬淵川沿岸	運用中
東北	岩手	岩手山麓	運用中
東北	岩手	雫石川沿岸	運用中
東北	宮城	迫川上流（荒砥沢ダム）（小田ダム）	運用中
東北	宮城	迫川上流（一の堰頭首工）	運用中
東北	宮城	旧迫川	運用中
東北	宮城	中田	運用中
東北	宮城	角田	運用中
東北	宮城	大崎	運用中
東北	宮城	鳴瀬川	運用中
東北	秋田	男鹿東部	運用中
東北	秋田	能代開拓	運用中
東北	秋田	仙北平野	運用中
東北	秋田	旭川水系	運用中
東北	山形	寒河江川農水	運用中
東北	山形	白川	運用中
東北	山形	最上川下流沿岸	運用中
東北	山形	新庄	運用中
東北	山形	最上川中流	運用中
東北	山形	泉田川	運用中
東北	山形	月山山麓	運用中
東北	山形	米沢平野二期	運用中
東北	山形	赤川	運用中
東北	福島	郡山東部	運用中
東北	福島	会津宮川	運用中
東北	福島	会津北部	運用中
東北	福島	雄国山麓	運用中
東北	福島	白河矢吹	運用中
東北	福島	阿武隈上流	運用中
東北	福島	安積疏水（新安積）	運用中
東北	福島	請戸川	運用中
東北	福島	母畑	運用中
関東	栃木	鬼怒中央	運用中
関東	栃木	那須野原	運用中
関東	栃木	芳賀台地	運用中
関東	群馬	渡良瀬川中央・沿岸	運用中
関東	群馬	鏑川（大塩貯水池･竹沼貯水池）	運用中
関東	群馬	鏑川（丹生貯水池）	運用中
関東	茨城	那珂川沿岸	運用中
関東	茨城	霞ヶ浦用水	運用中
関東	埼玉	大里	運用中
関東	山梨	釜無川	運用中
北陸	新潟	新川流域／西蒲原	運用中
北陸	新潟	亀田郷	運用中
北陸	新潟	白根郷	運用中
北陸	新潟	刈谷田川右岸	R7予定
北陸	新潟	関川	運用中
北陸	新潟	阿賀野川用水	運用中
北陸	新潟	阿賀野川右岸	運用中
北陸	新潟	信濃川下流	運用中
北陸	新潟	新津郷	運用中
北陸	新潟	佐渡	運用中
北陸	新潟	柏崎周辺	運用中
北陸	新潟	加治川	運用中
北陸	新潟	苗場山麓第一	運用中
北陸	新潟	苗場山麓第二	運用中
北陸	富山	氷見	運用中
北陸	富山	常願寺川沿岸	運用中
北陸	富山	小矢部川	運用中
北陸	石川	河北潟	運用中
北陸	石川	手取川	運用中
北陸	石川	珠洲第二	運用中

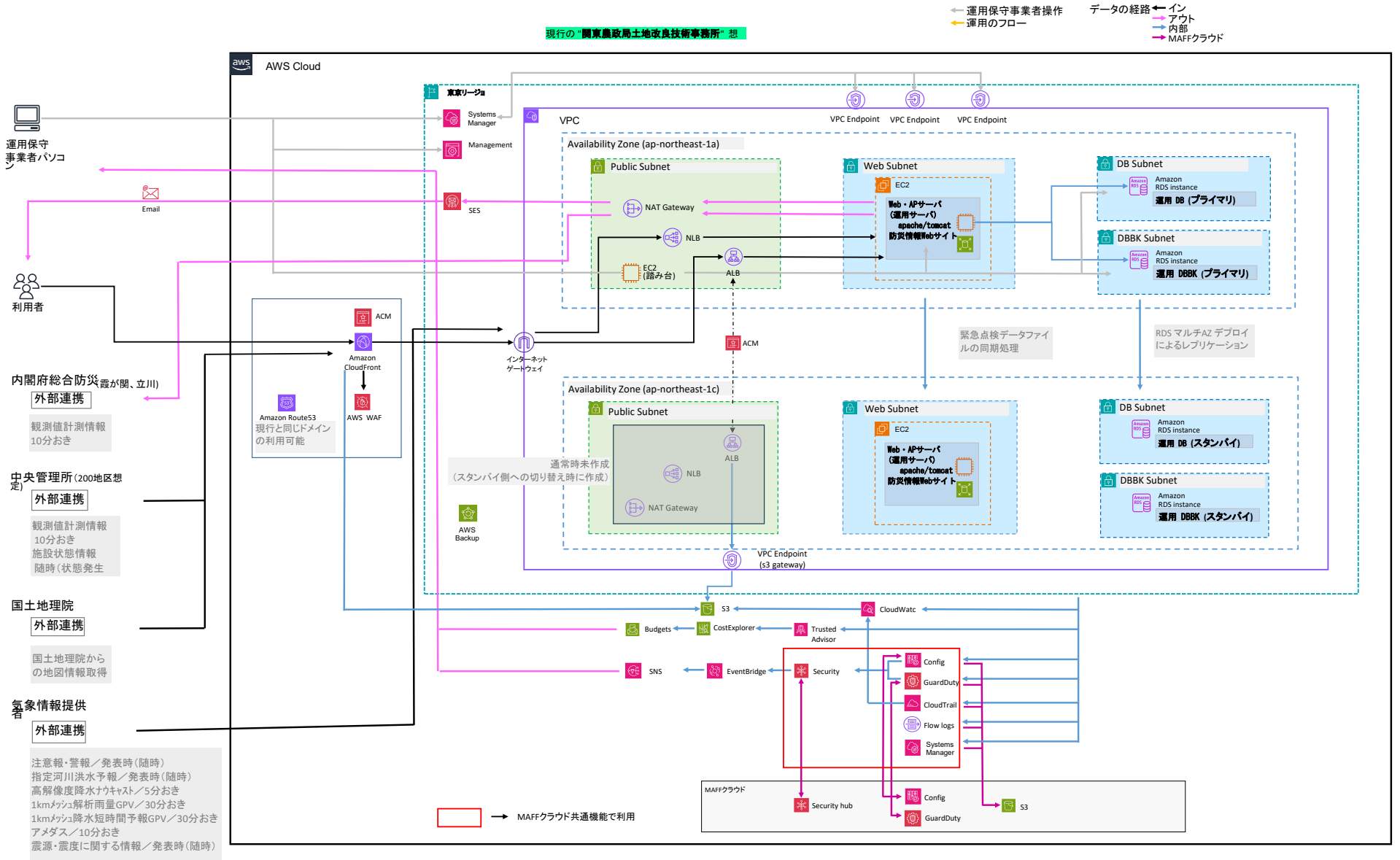
局名	県名	地区名	現況
北陸	石川	珠洲	R7予定
北陸	福井	日野川用水（一期）（二期）	運用中
東海	愛知	新矢作川用水	運用中
東海	愛知	新濃尾	運用中
東海	岐阜	西濃用水第二期	運用中
東海	三重	中勢用水	運用中
東海	三重	宮川用水第二期	運用中
近畿	滋賀	野洲川	運用中
近畿	滋賀	日野川	運用中
近畿	滋賀	湖北	運用中
近畿	滋賀	愛知川	運用中
近畿	京都	巨椋池	運用中
近畿	兵庫	北淡路	運用中
近畿	兵庫	東条川	運用中
近畿	兵庫	加古川	運用中
近畿	奈良	大和高原北部	運用中
近畿	奈良	十津川紀の川	運用中
近畿	奈良	五条吉野	運用中
近畿	和歌山	南紀用水	運用中
中四	鳥取	大山山麓	運用中
中四	鳥取	東伯	運用中
中四	岡山	児島湾周辺・岡山（海岸保全）	運用中
中四	岡山	笠岡湾	運用中
中四	岡山	勝英	運用中
中四	岡山	小阪部川	運用中
中四	広島	広島中部台地	運用中
中四	広島	芦田川	運用中
中四	島根	横田	運用中
中四	愛媛	南予	運用中
中四	愛媛	道前道後　道後平野地区	運用中
中四	愛媛	道前道後　面河地区	運用中
中四	愛媛	道前道後　道前平野地区	運用中
九州	福岡	耳納山麓	運用中
九州	福岡	筑後川中流　床島地区	運用中
九州	福岡	筑後川中流　山田地区	運用中
九州	佐賀	佐賀中部	運用中
九州	佐賀	上場	運用中
九州	佐賀	嘉瀬川	運用中
九州	佐賀	多良岳	運用中
九州	長崎	諫早湾	運用中
九州	熊本	八代平野	運用中
九州	大分	駅館川	運用中
九州	大分	大野川上流	運用中
九州	宮崎	大淀川右岸	運用中
九州	宮崎	大淀川左岸	運用中
九州	宮崎	一ツ瀬川	運用中
九州	宮崎	都城盆地	運用中
九州	宮崎	尾鈴	運用中
九州	宮崎	西諸	運用中
九州	鹿児島	出水平野	運用中
九州	鹿児島	曽於東部	運用中
九州	鹿児島	曽於南部	運用中
九州	鹿児島	曽於北部	運用中
九州	鹿児島	笠野原	運用中
九州	鹿児島	肝属中部	運用中
九州	鹿児島	徳之島用水	運用中
九州	鹿児島	南薩	運用中
北海	北海道	幌向川	運用中
北海	北海道	音江山（芦別北部）	運用中
北海	北海道	新雨竜（一期）（二期）	運用中
北海	北海道	雨竜川中央	運用中
北海	北海道	北空知	運用中
北海	北海道	樺戸（二期）	運用中
北海	北海道	多度志	運用中
北海	北海道	恵岱別	運用中
北海	北海道	当別	運用中
北海	北海道	南月形	運用中
北海	北海道	幌新	運用中
北海	北海道	幌加内	運用中
北海	北海道	野花南	運用中
北海	北海道	高岡シップ	運用中
北海	北海道	北檜山右岸	運用中

局名	県名	地区名	現況
北海	北海道	上磯	運用中
北海	北海道	厚沢部川	運用中
北海	北海道	渡島中央	運用中
北海	北海道	駒ヶ岳	運用中
北海	北海道	知内	運用中
北海	北海道	双葉	運用中
北海	北海道	共和	運用中
北海	北海道	北後志	運用中
北海	北海道	余市	運用中
北海	北海道	ペーパン	運用中
北海	北海道	神居	運用中
北海	北海道	共栄近文	運用中
北海	北海道	フラヌイ　フラヌイ二期	運用中
北海	北海道	空知川右岸	運用中
北海	北海道	ぴっぷ	運用中
北海	北海道	しろがね	運用中
北海	北海道	当麻	運用中
北海	北海道	美瑛川	運用中
北海	北海道	風連（御料ダム、風連ダム）	運用中
北海	北海道	ふらの	運用中
北海	北海道	温根別	運用中
北海	北海道	天塩川上流	運用中
北海	北海道	早来	運用中
北海	北海道	三石	運用中
北海	北海道	鵡川沿岸	運用中
北海	北海道	勇払東部	運用中
北海	北海道	十勝川左岸	運用中
北海	北海道	芽室	運用中
北海	北海道	幕別	運用中
北海	北海道	中士幌	運用中
北海	北海道	札内川	運用中
北海	北海道	女満別	運用中
北海	北海道	斜里	運用中
北海	北海道	斜里（二期）	運用中
北海	北海道	雄武中央（一期）（二期）	運用中
北海	北海道	北見	運用中
北海	北海道	西網走	運用中
北海	北海道	苫前	運用中
北海	北海道	天塩沿岸	運用中
北海	北海道	羽幌	運用中
北海	北海道	羽幌二股	運用中
沖縄	沖縄	石垣島	運用中
沖縄	沖縄	羽地大川	運用中

運用中	185地区
Ｒ７接続予定	2地区

別紙２ クラウド構成図

AWS 1リージョン 2AZ・RDS構成



別紙３　システム利用環境等

１　システムの利用環境

本システムの利用環境は下表のとおりである。

（１）利用者

本システムの利用者は、以下のとおりである。

利用者	主な利用目的
①　関東農政局土地改良技術事務所	全国の防災情報の収集と提供、 防災中央システム／バックアップシステムの管理
②農林水産本省	全国の防災情報の参照
③地方農政局等（北海道開発局、 沖縄総合事務局含む）	関係地区の防災情報の参照
④土地改良調査管理事務所等 （北海道開発局各開発建設部含む）	関係地区の防災情報の参照
⑤道府県	関係地区の防災情報の参照
⑥市町村	関係地区の防災情報の参照
⑦施設管理者	関係地区の防災情報の参照
⑧内閣府	全国の防災情報の収集 （内閣府総合防災情報システム）

（２）システム環境

データ転送システム（中央管理所）のシステム環境は、地区により異なるため未記載とする。

（３）ソフトウェア環境

ソフトウェア環境は、以下のとおりとする。

システム名	サーバ名	構　成	内　　容
防災中央システム／バックアップシステム	Web・アプリケーションサーバ	OS Web サーバ アプリケーションサーバ Java	Red Hat Enterprise Linux8（64bit） Apache HTTP Server 2.4 Apache Tomcat 9.0 Amazon Corretto 17
	データベースサーバ	サービス DBMS	Amazon RDS PostgreSQL 15
	データベース（ダウンロード用）兼バックアップサーバ	サービス DBMS	Amazon RDS PostgreSQL 15
データ転送システム（中央管理所）	転送サーバ	OS	Windows Server 2022 Standard Windows Server 2019 Standard Windows Server 2016 Standard

（４）システム概念図

システム概念図は別図１に示すとおり。

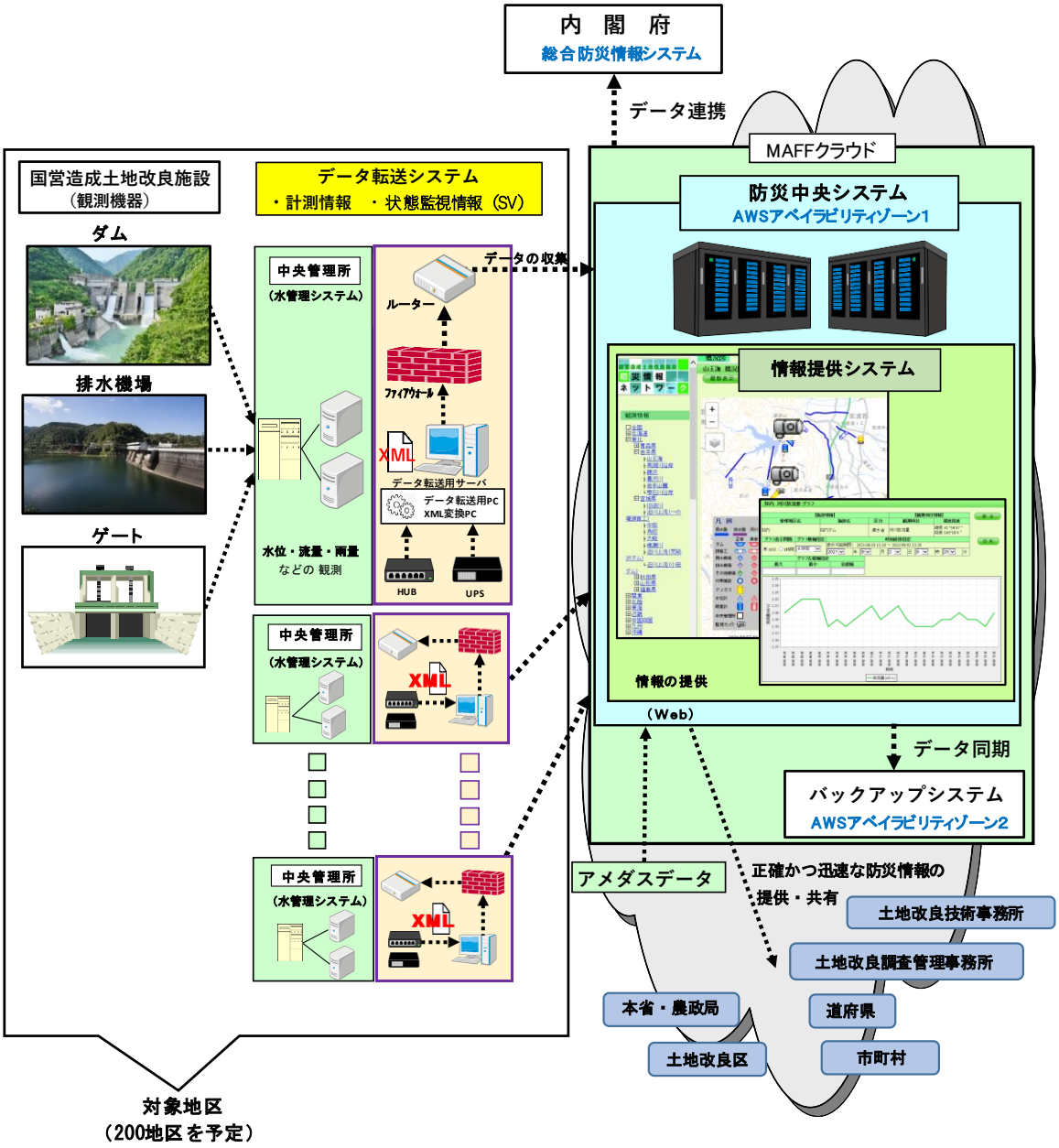
2　用語の定義

本業務で使用する主な用語の定義は、次のとおりとする。

用語	定　　義
AWS	MAFF クラウド上で稼働するクラウドサービス。「Amazon Web Services」の略。東京リージョンを基盤（2AZ（アベイラビリティゾーン）構成）とする。
データ転送システム	既存の国営造成土地改良施設に設置されている中央管理所から防災情報をインターネット経由で防災中央システムへ転送するためのシステム。
情報提供システム	データ転送システムで転送されてきた各国営造成土地改良施設固有の情報を表示するシステムであり、防災中央システム上で稼動する。
防災中央システム	AWS の東京リージョンアベイラビリティゾーン１に設置され、中央管理所から転送された防災情報を迅速かつ、一元的に管理し、収集した防災情報を別紙３の１（１）に記載された利用者へ情報を提供するためのシステム。
バックアップシステム	AWS の東京リージョンアベイラビリティゾーン２に設置され、防災中央システムが被災し機能が停止した場合、代わってシステムを稼働させるバックアップシステム。
中央管理所	国営造成土地改良施設の情報を一元的に管理し、施設管理者が国営造成土地改良施設の遠隔操作を行うことを目的に各国営地区に設置された施設。
国営造成土地改良施設	農業用ダム、頭首工、排水機場等の基幹的土地改良施設
水管理システム	中央管理所で国営造成土地改良施設の情報を監視・制御するシステム
総合防災情報システム	防災機関が横断的に共有すべき防災情報の形式を標準化し、国、地方公共団体等の各機関や住民等の情報を共通のシステムに集約する共通基盤
気象情報提供者	気象情報及び地震情報を提供する者
計測情報	国営造成土地改良施設の操作、制御とそれに伴う施設の状況変化を把握するために必要な情報　　例）水位、雨量、ポンプ翼開度など
状態監視情報（SV）	国営造成土地改良施設の状態、操作モード、警報関係などの情報 例）ゲート開・閉、ゲート故障、水位異常など

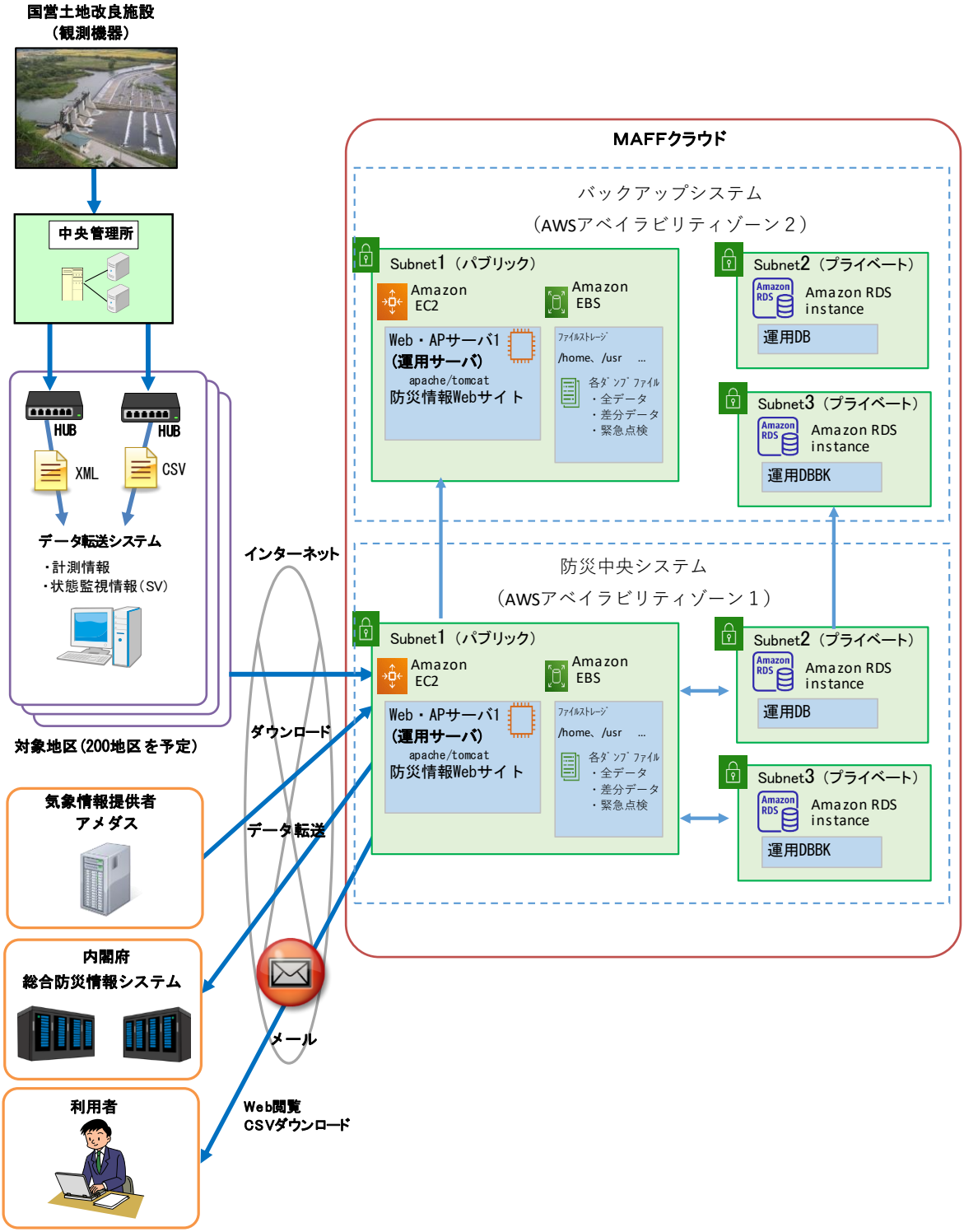
（別図１）

国営造成土地改良施設防災情報ネットワークシステム概念図



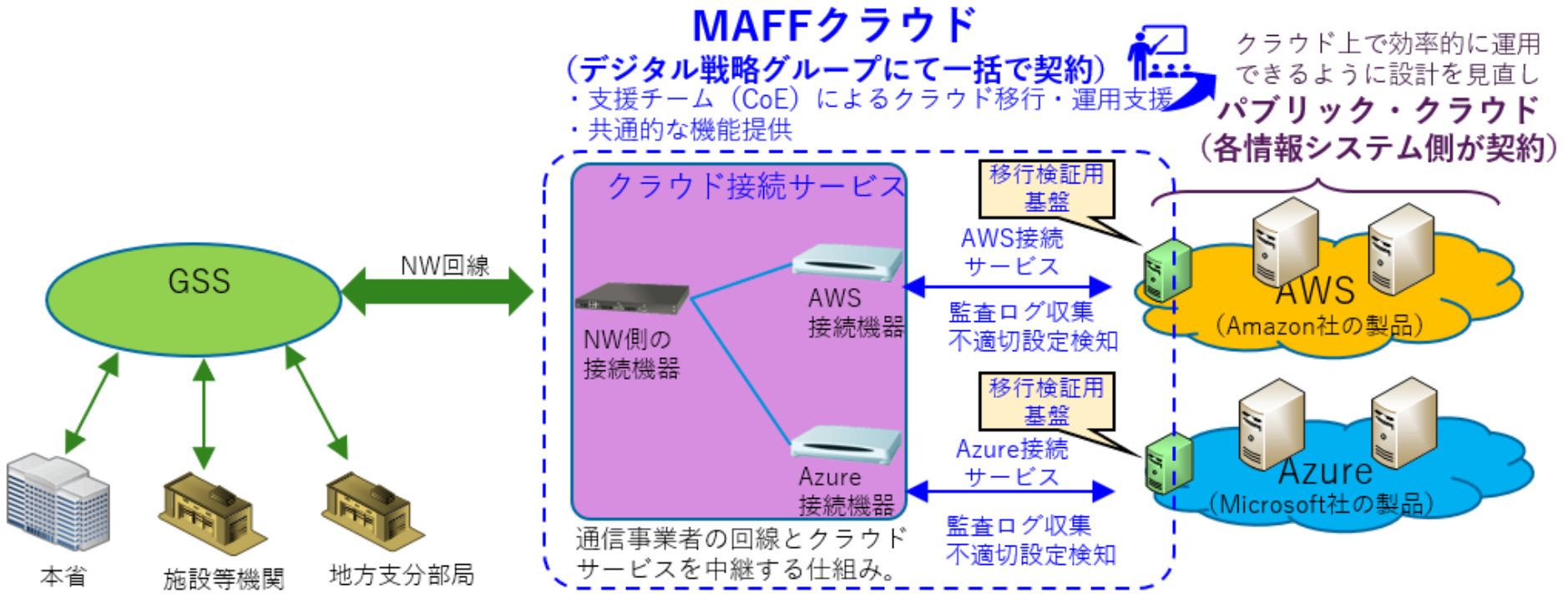
（別図２）

国営造成土地改良施設防災情報ネットワークシステム機器構成図



（別図３）

MAFFクラウド構成イメージ



別紙４　　情報セキュリティの確保に関する共通基本仕様

Ⅰ　情報セキュリティポリシーの遵守

１　受託者は、担当部署から農林水産省における情報セキュリティの確保に関する規則（平成27 年農林水産省訓令第４号。以下「規則」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。

なお、規則は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

２　受託者は、規則と同等の情報セキュリティ管理体制を整備していること。

３　受託者は、本業務の従事者に対して、規則と同等の情報セキュリティ対策の教育を実施していること。

Ⅱ　応札者に関する情報の提供

１　応札者は、応札者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を提出すること。

なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（〇〇国籍の者が△名（又は□%）等）を記載すること。また、この場合であっても、担当部署からの要求に応じて、可能な限り要員に関する情報を提供すること。

２　応札者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

（1）ISO/IEC27001 等の国際規格とそれに基づく認証の証明書等

（2）プライバシーマーク又はそれと同等の認証の証明書等

（3）独立行政法人情報処理推進機構（IPA）が公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が4に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書

Ⅲ　業務の実施における情報セキュリティの確保

１　受託者は、本業務の実施に当たって、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。

（1）本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても、第三者に開示し、又は本業務以外の目的で利用しないこと。

（2）本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。

（3）本業務に係る情報を適切に取り扱うことが可能となるよう、情報セキュリティ対策の実施内容及び管理体制を整備すること。なお、本業務実施中及び実施後において検証が可能となるよう、必要なログの取得や作業履歴の記録等を行う実施内容及び管理体制とすること。

（4）本業務において、個人情報又は農林水産省における要機密情報を取り扱う場合は、当該情報（複製を含む。以下同じ。）を国内において取り扱うものとし、当該情報の国外への送信・保存や当該情報への国外からのアクセスを行わないこと。

（5）農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、農林水産省又は農林水産省が選定した事業者による立入調査等の情報セキュリティ監査（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 26 条第1項第2号に基づく監査等を含む。以下同じ。）を受け入れること。また、担当部署からの要求があった場合は、受託者が自ら実施した内部監査及び外部監査の結果を報告すること。

（6）本業務において、要安定情報を取り扱うなど、担当部署が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。

（7）本業務において、第三者に情報が漏えいするなどの情報セキュリティインシデントが発生した場合は、担当部署に対し、速やかに電話、口頭等で報告するとともに、報告書を提出すること。また、農林水産省の指示に従い、事態の収拾、被害の拡大防止、復旧、再発防止等に全力を挙げること。なお、これらに要する費用の全ては受託者が負担すること。

2　受託者は、委託期間を通じて以下の措置を講ずること。

（1）情報の適正な取扱いのため、取り扱う情報の格付等に応じ、以下に掲げる措置を全て含む情報セキュリティ対策を実施すること。また、実施が不十分の場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。

ア　情報セキュリティインシデント等への対処能力の確立・維持

イ　情報へアクセスする主体の識別とアクセスの制御

ウ　ログの取得・監視

エ　情報を取り扱う機器等の物理的保護

オ　情報を取り扱う要員への周知と統制

カ　セキュリティ脅威に対処するための資産管理・リスク評価

キ　取り扱う情報及び当該情報を取り扱うシステムの完全性の保護

ク　セキュリティ対策の検証・評価・見直し

（2）本業務におけ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。

（3）本業務において情報セキュリティインシデントの発生、情報の目的外使用等を認知した場合、直ちに委託事業の一時中断等、必要な措置を含む対処を実施すること。

（4）私物（本業務の従事者個人の所有物等、受託者管理外のものをいう。）の機器等を本業務に用いないこと。

（5）本業務において取り扱う情報が本業務上不要となった場合、担当部署の指示に従い返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

3　受託者は、委託期間の終了に際して以下の措置を講ずること。

（1）本業務の実施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書面等により報告すること。

（2）成果物等を電磁的記録媒体により納品する場合には、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処するとともに、確認結果（確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等）を成果物等に記載又は添付すること。

（3）本業務において取り扱われた情報を、担当部署の指示に従い返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

4　受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、担当部署に報告し、協議の上、対策を講ずること。

Ⅳ　情報システムにおける情報セキュリティの確保

1　受託者は、本業務において情報システムに関する業務を行う場合には、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。

（1）本業務の各工程において、農林水産省の意図しない情報システムに関する変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること。）。

（2）本業務において、農林水産省の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入調査等、農林水産省と連携して原因を調査し、排除するための手順及び体制（例えば、システムの操作ログや作業履歴等を記録し、担当部署から要求された場合には提出するなど）を整備していること。

2　受託者は、本業務において情報システムの運用管理機能又は設計・開発に係る企画・要件定義を行う場合には、以下の措置を実施すること。

（1）情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、情報システム運用時に情報セキュリティ確保のために必要となる管理機能や監視のために必要な機能を本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

ア　情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

イ　情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

（ア）農林水産省外と通信回線で接続している箇所における外部からの不正アクセスやサ

ービス不能攻撃を監視する機能

（イ）不正プログラム感染や踏み台に利用されること等による農林水産省外への不正な通信を監視する機能

（ウ）端末等の農林水産省内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能

（エ）農林水産省内通信回線への端末の接続を監視する機能

（オ）端末への外部電磁的記録媒体の挿入を監視する機能

（カ）サーバ装置等の機器の動作を監視する機能

（キ）ネットワークセグメント間の通信を監視する機能

（2）開発する情報システムに関連する脆（ぜい）弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

ア　既知の脆（ぜい）弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

イ　開発時に情報システムに脆（ぜい）弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

ウ　セキュリティ侵害につながる脆（ぜい）弱性が情報システムに存在することが発覚した場合に修正が施されること。

エ　ソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を提供すること。

（3）開発する情報システムに意図しない不正なプログラム等が組み込まれないよう、以下を全て含む対策を本業務の成果物に明記すること。

ア　情報システムで利用する機器等を調達する場合は、意図しない不正なプログラム等が組み込まれていないことを確認すること。

イ　アプリケーション・コンテンツの開発時に意図しない不正なプログラム等が混入されることを防ぐための対策を講ずること。

ウ　情報システムの構築を委託する場合は、委託先において農林水産省が意図しない変更が加えられないための管理体制を求めること。

（4）要安定情報を取り扱う情報システムを構築する場合は、許容される停止時間を踏まえて、情報システムを構成する要素ごとに、以下を全て含むセキュリティ要件を定め、本業務の成果物に明記すること。

ア　端末、サーバ装置及び通信回線装置等の冗長化に関する要件

イ　端末、サーバ装置及び通信回線装置並びに取り扱われる情報に関するバックアップの要件

ウ　情報システムを中断することのできる時間を含めた復旧に関する要件

（5）開発する情報システムのネットワーク構成について、以下を全て含む要件を定め、本業務の成果物に明記すること。

ア　インターネットやインターネットに接点を有する情報システム（クラウドサービスを含

む。）から分離することの要否の判断及びインターネットから分離するとした場合に、分離を確実にするための要件

イ　端末、サーバ装置及び通信回線装置上で利用するソフトウェアを実行するために必要な通信要件

ウ　インターネット上のクラウドサービス等のサービスを利用する場合の通信経路全般のネットワーク構成に関する要件

エ　農林水産省外通信回線を経由して機器等に対してリモートメンテナンスすることの要否の判断とリモートメンテナンスすることとした場合の要件

3　受託者は、本業務において情報システムの構築を行う場合には、以下の事項を含む措置を適切に実施すること。

（1）情報システムのセキュリティ要件の適切な実装

ア　主体認証機能

イ　アクセス制御機能

ウ　権限管理機能

エ　識別コード・主体認証情報の付与管理

オ　ログの取得・管理

カ　暗号化機能・電子署名機能

キ　暗号化・電子署名に係る管理

ク　監視機能

ケ　ソフトウェアに関する脆（ぜい）弱性等対策

コ　不正プログラム対策

サ　サービス不能攻撃対策

シ　標的型攻撃対策

ス　動的なアクセス制御

セ　アプリケーション・コンテンツのセキュリティ

ソ　政府ドメイン名（go.jp）の使用

タ　不正なウェブサイトへの誘導防止

チ　農林水産省外のアプリケーション・コンテンツの告知

（2）監視機能及び監視のための復号・再暗号化

監視のために必要な機能について、2（1）イの各項目を例として必要な機能を設けること。また、必要に応じ、監視のために暗号化された通信データの復号化や、復号されたデータの再暗号化のための機能を設けること。

（3）情報セキュリティの観点に基づくソフトウェアの選定

情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう可能な限り最新版を選定し、利用するソフトウェアの種類、バージョン及びサポート期限に係る情報を農林水産省に提供すること。

ただし、サポート期限が公表されていないソフトウェアについては、情報システムのライフサイクルを踏まえ、ソフトウェアの発売等からの経過年数や後継となるソフトウェアの有無等を考慮して選定すること。

（4）情報セキュリティの観点に基づく試験の実施

ア　ソフトウェアの開発及び試験を行う場合は、運用中の情報システムとの分離

イ　試験項目及び試験方法の決定並びにこれに基づいた試験の実施

ウ　試験の実施記録の作成・保存

（5）情報システムの開発環境及び開発工程における情報セキュリティ対策

ア　変更管理、アクセス制御、バックアップの取得等、ソースコードの不正な変更・消去を防止するための管理

イ　調達仕様書等に規定されたセキュリティ実装方針の適切な実施

ウ　セキュリティ機能の適切な実装、セキュリティ実装方針に従った実装が行われていることを確認するための設計レビュー及びソースコードレビューの範囲及び方法の決定並びにこれに基づいたレビューの実施

エ　オフショア開発を実施する場合の試験データに実データを使用することの禁止

（6）政府共通利用型システムの利用における情報セキュリティ対策

ガバメントソリューションサービス（GSS）等、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程等に基づき、政府共通利用型システムの情報セキュリティ水準を低下させることがないように、適切なセキュリティ要件を実装すること。

4　受託者は、本業務において情報システムの運用・保守を行う場合には、以下の事項を含む措置を適切に実施すること。

（1）情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。

ア　情報システムの運用環境に課せられるべき条件の整備

イ　情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

ウ　情報システムの保守における情報セキュリティ対策

エ　運用中の情報システムに脆（ぜい）弱性が存在することが判明した場合の情報セキュリティ対策

オ　利用するソフトウェアのサポート期限等の定期的な情報収集及び報告

カ　「デジタル・ガバメント推進標準ガイドライン」（デジタル社会推進会議幹事会決定。最終改定：2025 年 5 月 27 日）の「別紙3 調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」に基づく情報資産管理を行うために必要な事項を記載した情報資産管理標準シートの提出

キ　アプリケーション・コンテンツの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポートを継続しているバージョンでの動作検証及び当該バージ

ョンで正常に動作させるためのアプリケーション・コンテンツ等の修正

（2）情報システムの運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。

ア　情報セキュリティに関わる運用保守体制の整備

イ　運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

ウ　情報セキュリティインシデント（可能性がある事象を含む。以下同じ。）を認知した際の対処方法の確立

（3）情報システムのセキュリティ監視を行う場合には、以下の内容を全て含む監視手順を定め、適切に監視運用すること。

ア　監視するイベントの種類や重要度

イ　監視体制

ウ　監視状況の報告手順や重要度に応じた報告手段

エ　情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順

オ　監視運用における情報の取扱い（機密性の確保）

（4）　情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか定期的に見直しを行うこと。

（5）　情報システムにおいて定期的に脆（ぜい）弱性対策の状況を確認すること。

（6）情報システムに脆（ぜい）弱性が存在することを発見した場合には、速やかに担当部署に報告し、本業務における運用・保守要件に従って脆（ぜい）弱性の対策を行うこと。

（7）要安定情報を取り扱う情報システムについて、以下の内容を全て含む運用を行うこと。

ア　情報システムの各構成要素及び取り扱われる情報に関する適切なバックアップの取得及びバックアップ要件の確認による見直し

イ　情報システムの構成や設定の変更等が行われた際及び少なくとも年１回の頻度で定期的に、情報システムが停止した際の復旧手順の確認による見直し

（8）ガバメントソリューションサービス（GSS）等、本業務の調達範囲外の政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを運用する場合は、政府共通利用型システム管理機関との責任分界に応じた運用管理体制の下、政府共通利用型システム管理機関が定める運用管理規程等に従い、政府共通利用型システムの情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

（9）不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

5　受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。

（1）情報システム更改時の情報の移行作業における情報セキュリティ対策

（2）情報システム廃棄時の不要な情報の抹消

Ⅴ　情報システムの一部の機能を提供するサービスに関する情報セキュリティの確保

応札者は、要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除くものとし、以下「業務委託サービス」という。）に関する業務を実施する場合は、業務委託サービス毎に以下の措置を講ずること。

1　業務委託サービスの中断時や終了時に円滑に業務を移行できるよう、取り扱う情報の可用性に応じ、以下を例としたセキュリティ対策を実施すること。

（1）業務委託サービス中断時の復旧要件

（2）業務委託サービス終了または変更の際の事前告知の方法・期限及びデータ移行方法

2　業務委託サービスを提供する情報処理設備が収容されているデータセンターが設置されている独立した地域（リージョン）が国内であること。

3　業務委託サービスの契約に定める準拠法が国内法のみであること。

4　ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

5　業務委託サービスの利用を通じて農林水産省が取り扱う情報について、目的外利用を禁止すること。

6　業務委託サービスの提供に当たり、業務委託サービスの提供者若しくはその従業員、再委託先又はその他の者によって、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること）。

7　業務委託サービスの提供者の資本関係、役員等の情報、業務委託サービスの提供が行われる施設等の場所、業務委託サービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

8　業務委託サービスの提供者の情報セキュリティ水準を証明する、Ⅱの2で掲げる証明書等または同等以上の国際規格等の証明書の写しを提出すること。

9　情報セキュリティインシデントへの対処方法を確立していること。

10　情報セキュリティ対策その他の契約の履行状況を確認できること。

11　情報セキュリティ対策の履行が不十分な場合の対処方法を確立していること。

12　業務委託サービスの提供者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について業務委託サービスの提供者と合意し、定められた手順により情報を取り扱うこと。

Ⅵ　クラウドサービスに関する情報セキュリティの確保

応札者は、本業務において、クラウドサービス上で要機密情報を取り扱う場合は、当該クラウドサービスごとに以下の措置を講ずること。また、当該クラウドサービスの活用が本業務の再委託に該当する場合は、当該クラウドサービスに対して、Ｘの措置を講ずること。

１　サービス条件

（１）クラウドサービスを提供する情報処理設備が収容されているデータセンターについて、設置されている独立した地域（リージョン）が国内であること。

（２）クラウドサービスの契約に定める準拠法が国内法のみであること。

（３）クラウドサービス終了時に情報を確実に抹消することが可能であること。

（４）本業務において要求されるサービス品質を満たすクラウドサービスであること。

（５）クラウドサービス提供者の資本関係、役員等の情報、クラウドサービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）のうち農林水産省の情報又は農林水産省が利用するクラウドサービスの環境に影響を及ぼす可能性のある者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

（６）ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

（７）原則として、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（以下「ISMAP クラウドサービスリスト等」という。）に登録されているクラウドサービスであること。

（８）ISMAP クラウドサービスリスト等に登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（３桁の番号で表現される項目）及び末尾にＢが付された詳細管理策（４桁の番号で表現される項目）を原則として全て満たしていることを証明する資料を提出し、農林水産省の承認を得ること。

２　クラウドサービスのセキュリティ要件

（１）クラウドサービスについて、以下の要件を満たしていること。

ア　クラウドサービス提供者が提供する主体認証情報の管理機能が農林水産省の要求事項を満たすこと。

イ　クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること。

ウ　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作が特定されていること。

エ　クラウドサービス内及び通信経路全般における暗号化が行われていること。

オ　クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合、ソフトウェアのクラウドサービス上におけるライセンス規定に違反していないこと。

カ　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合、その機能を確認していること。

キ　暗号鍵管理機能をクラウドサービス提供者が提供する場合、鍵管理手順、鍵の種類の情報及び鍵の生成から廃棄に至るまでのライフサイクルにおける情報をクラウドサービス提供者から入手し、またリスク評価を実施していること。

ク　利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていること。

ケ　クラウドサービス提供者が提供するバックアップ機能を利用する場合、農林水産省の要求事項を満たすこと。

（2）クラウドサービスで利用するアカウント管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス提供者が付与し、又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

イ　クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者に対する、強固な認証技術による認証

ウ　クラウドサービス提供者が提供する主体認証情報の管理機能について、農林水産省の要求事項を満たすための措置の実施

（3）クラウドサービスで利用するアクセス制御に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス上に保存する情報やクラウドサービスの機能に対する適切なアクセス制御

イ　インターネット等の農林水産省外通信回線から農林水産省内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合の適切なセキュリティ対策

（4）クラウドサービスで利用する権限管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス利用者によるクラウドサービスに多大な影響を与える誤操作の抑制

イ　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（5）クラウドサービスで利用するログの管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの管理

（6）クラウドサービスで利用する暗号化に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス内及び通信経路全般における暗号化の適切な実施

イ　情報システムで利用する暗号化方式の遵守度合いに係る法令や農林水産省訓令等の関連する規則の確認

ウ　暗号化に用いる鍵の保管場所等の管理に関する要件

エ　クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理

（7）クラウドサービスを利用する際の設計・設定時の誤り防止に関して、以下のセキュリティ要件を満たしていること。

ア　クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策

イ　クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

ウ　クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用

エ　クラウドサービスの設定の誤りを見いだすための対策

（8）クラウドサービス運用時の監視等に関して、以下の運用管理機能要件を満たしていること。

ア　クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

イ　利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

ウ　クラウドサービス内における時刻同期の方法

エ　利用するクラウドサービスの不正利用の監視

（9）クラウドサービス上で要安定情報を取り扱う場合は、その可用性を考慮した設計となっていること。

（10）クラウドサービスにおいて、不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施を含む、情報セキュリティインシデントが発生した際の復旧に関する対策要件が策定されていること。

3　クラウドサービスを利用した情報システム

クラウドサービスを利用した情報システムについて、以下の措置を講ずること。

（1）導入・構築時の対策

ア　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス利用のための責任分界点を意識した利用手順

（イ）クラウドサービス利用者が行う可能性がある重要操作の手順

イ　情報システムの運用・監視中に発生したクラウドサービスの利用に係る情報セキュリティインシデントを認知した際の対処手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス提供者との責任分界点を意識した責任範囲の整理

（イ）クラウドサービスのサービスごとの情報セキュリティインシデント対処に関する事項

（ウ）クラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

ウ　クラウドサービスが停止し、又は利用できなくなった際の復旧手順を実施手順として整

備すること。なお、要安定情報を取り扱う場合は十分な可用性を担保した手順とすること。

（2）運用・保守時の対策

ア　クラウドサービスの利用に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービス提供者に対する定期的なサービスの提供状態の確認

（イ）クラウドサービス上で利用するIT資産の適切な管理

イ　クラウドサービスで利用するアカウントの管理、アクセス制御、管理権限に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

（イ）クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

ウ　クラウドサービスで利用する機能に対する脆（ぜい）弱性対策を実施すること。

エ　クラウドサービスを運用する際の設定変更に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（イ）クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

（ウ）クラウドサービス利用者が行う可能性のある重要操作に対する監督者の指導の下での実施

オ　クラウドサービスを運用する際の監視に関して、以下の内容を全て含む対策を実施すること。

（ア）クラウドサービスの不正利用の監視

（イ）クラウドサービスで利用しているデータ容量、性能等の監視

カ　クラウドサービスを運用する際の可用性に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）不測の事態に際してサービスの復旧を行うために必要なバックアップの確実な実施

（イ）要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る定期的な訓練の実施

（ウ）クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

キ　クラウドサービスで利用する暗号鍵に関して、暗号鍵の生成から廃棄に至るまでのライフサイクルにおける適切な管理の実施を含む情報セキュリティ対策の実施

（3）更改・廃棄時の対策

ア　クラウドサービスの利用終了に際して、以下の内容を全て含む情報セキュリティ対策

を実施すること。

（ア）クラウドサービスで取り扱った情報の廃棄

（イ）暗号化消去が行えない場合の基盤となる物理機器の廃棄

（ウ）作成されたクラウドサービス利用者アカウントの削除

（エ）利用したクラウドサービスにおける管理者アカウントの削除又は返却

（オ）クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

Ⅶ Web システム／Web アプリケーションに関する情報セキュリティの確保

受託者は、本業務において、Web システム／Web アプリケーションを開発、利用または運用等を行う場合、別紙「Web システム／Web アプリケーションセキュリティ要件書 Ver.4.0」の各項目について、対応可、対応不可あるいは対象外等の対応方針を記載した資料を提出すること。

Ⅷ 機器等に関する情報セキュリティの確保

受託者は、本業務において、農林水産省にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等（以下「機器等」という。）を納品、賃貸借等をする場合には、以下の措置を講ずること。

1 納入する機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

2 機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、農林水産省と受託者が連携して原因を調査・排除できる体制を整備していること。

3 機器等の設置時や保守時に、情報セキュリティの確保に必要なサポートを行うこと。

4 利用マニュアル・ガイダンスが適切に整備された機器等を採用すること。

5 脆（ぜい）弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。

6 ISO/IEC 15408 に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

7 情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新版を採用するとともに、ソフトウェアの種類、バージョン及びサポート期限について報告すること。なお、サポート期限が事前に公表されていない場合は、情報システムのライフサイクルを踏まえ、販売からの経過年数や後継ソフトウェアの有無等を考慮して選定すること。

8 機器等の納品時に、以下の事項を書面で報告すること。

（1）調達仕様書に指定されているセキュリティ要件の実装状況（セキュリティ要件に係る試験

の実施手順及び結果）

（2）機器等に不正プログラムが混入していないこと（最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等）

Ⅸ 管轄裁判所及び準拠法

1 本業務に係る全ての契約（クラウドサービスを含む。以下同じ。）に関して訴訟の必要が生じた場合の専属的な合意管轄裁判所は、国内の裁判所とすること。

2 本業務に係る全ての契約の成立、効力、履行及び解釈に関する準拠法は、日本法とすること。

Ⅹ 業務の再委託における情報セキュリティの確保

1 受託者は、本業務の一部を再委託（再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託を含む。以下同じ。）する場合には、受託者が上記Ⅱの1、Ⅱの2、Ⅲの1及びⅣの1において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、農林水産省の許可を得ること。

2 受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、農林水産省又は農林水産省が選定した事業者による再委託先への立入調査等の監査を受け入れるものとすること。

3 受託者は、担当部署からの要求があった場合は、再委託先における情報セキュリティ対策の履行状況を報告すること。

Ⅺ 資料等の提出

上記Ⅱの1、Ⅱの2、Ⅲの1、Ⅳの1、Ⅴの6、Ⅴの7、Ⅴの8、Ⅵの1（5）、Ⅵの1（6）、Ⅵの1（8）、Ⅷの1及びⅧの6において提出することとしている資料等については、最低価格落札方式にあっては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式及び企画競争方式にあっては提案書等の評価のための書類に添付して提出すること。

Ⅻ 変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅳ、Ⅴ、Ⅵ、Ⅶ、Ⅷ及びⅩに関して、農林水産省に提示した内容を変更しようとする場合には、変更する事項、理由等を記載した申請書を提出し、農林水産省の許可を得ること。

別紙５

AWS/Azure設定確認リスト　　凡例：〇：責任者、△：サポート

【PaaS/IaaS】基本的な設定すべきセキュリティ対策（AWS/Azure）	担当		役割分担に関する補足
	MAFFクラウド管理者(PMO)	PJMO	
IDおよびアクセス管理			
組織が許可したアカウントの管理		〇	
管理者アカウントに対する多要素認証の利用	△	〇	多要素認証を設定していない限りあらゆるAWS/Azureリソースの操作が出来ないよう設定
管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し	△	〇	年度末に実施
必要最低限の管理者権限の割当て	△	〇	AWS：Configを利用して実施 Azure：Azure Policyを利用して実施
グループを利用した権限の設定		〇	
管理者アカウントに関する復旧手段の確保		〇	
すべてのアカウントへのパスワードポリシーの適用	△	〇	AWS：Configを利用して実施 Azure：Azure Policyを利用して実施
アクセスキー、サービスアカウントキー等の適切な管理		〇	
管理者アカウントと日常的に使用するアカウントの分離		〇	ユーザーの払い出しはPJMO管理
アカウント・権限・認証情報の定期的な見直し		〇	年度末に実施
AWSにおいて考慮すべき設定			
AWS サポートセンターへのアクセス設定		〇	
IAMに保存されているサーバ証明書の管理		〇	
IAM Access analyzerの有効化		〇	
Azureにおいて考慮すべき設定			
Microsoft Azure サポートセンターへのアクセス設定		〇	
Azure App Serviceに保存されているサーバ証明書の管理		〇	
ログの記録と監視			
ログの有効化及び取得	△	〇	MAFFクラウド管理者側で有効化の為の手順を作成し、PJMOに配布
ログの一元管理	△	〇	
ログの保護	△	〇	管理者アカウントで保管
ログの監視/通知の設定	△	〇	AWS：アクセスログなどは管理者アカウント側でGuardDutyを用いて対応。 Azure：アクセスログなどは管理アカウント側でMicrosoft Defender for Cloudを用いて対応。 そのほかのログについてはPJMOに一任。
ネットワーク			
ロードバランサの接続設定		〇	
仮想マシン			
最新のOSパッチの適用確認		〇	
不正プログラム対策ソフトウェアの導入		〇	
攻撃対象となるネットワークポートへのアクセス制限		〇	
ストレージ			
匿名/公開アクセスの禁止	△	〇	不適切設定を有効化し、管理者アカウントで監視
ストレージアクセスの通信設定	△	〇	不適切設定を有効化し、管理者アカウントで監視
AWSにおいて考慮すべき設定			
Amazon RDSの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視
MFA Deleteの有効化	△	〇	不適切設定を有効化し、管理者アカウントで監視
Amazon EBSの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視
Azureにおいて考慮すべき設定			
Azure Databaseの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視
MFA Deleteの有効化	△	〇	不適切設定を有効化し、管理者アカウントで監視
Azure Disk Storageの暗号化	△	〇	不適切設定を有効化し、管理者アカウントで監視

別紙6

項目		見出し		要件		備考	必須可否
1	認証・認可	1.1	ユーザー認証	1.1.1	特定のユーザーや管理者のみに表示・実行を許可すべき画面や機能、APIでは、ユーザー認証を実施すること	特定のユーザーや管理者のみにアクセスを許可したいWebシステムでは、ユーザー認証を行う必要があります。また、ユーザー認証が成功した後にはアクセス権限を確認する必要があります。そのため、認証済みユーザーのみがアクセス可能な箇所を明示しておくことが望ましいでしょう。 リスクベース認証や二要素認証など認証をより強固にする仕組みもあります。不特定多数がアクセスする必要がない場合には、IPアドレスなどによるアクセス制限も効果があります。 OpenIDなどIdP(ID Provider)を利用する場合には信頼できるプロバイダであるかを確認する必要があります。IdPを使った認証・認可を行う場合も他の認証・認可に関する要件を満たすものを利用することが望ましいです。	必須
				1.1.2	上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ（非公開にすべきデータは直接URLで指定できる公開ディレクトリに配置しない）では、ユーザー認証を実施すること		必須
				1.1.3	多要素認証を実施すること	多要素認証（Multi Factor Authentication: MFA）とは、例えばパスワードによる認証に加え、TOTP（Time-Based One-Time Password：時間ベースのワンタイムパスワード）やデジタル証明書など二つ以上の要素を利用した認証方式です。手法については NIST Special Publication 800-63B などを参照してください。	推奨
		1.2	ユーザーの再認証	1.2.1	個人情報や機微情報を表示するページに遷移する際には、再認証を実施すること	ユーザー認証はセッションにおいて最初の一度だけ実施するのではなく、重要な情報や機能へアクセスする際には再認証を行うことが望ましいでしょう。	推奨
				1.2.2	パスワード変更や決済処理などの重要な機能を実行する際には、再認証を実施すること		推奨
		1.3	パスワード	1.3.1	ユーザー自身が設定するパスワード文字列は最低 8文字以上であること	認証を必要とするWebシステムの多くは、パスワードを本人確認の手段として認証処理を行います。そのためパスワードを盗聴や盗難などから守ることが重要になります。	必須
				1.3.2	登録可能なパスワード文字列の最大文字数は64文字以上であること	パスワードを処理する関数の中には最大文字数が少ないものもあるので注意する必要があります。	必須
				1.3.3	パスワード文字列として使用可能な文字種は制限しないこと	任意の大小英字、数字、記号、空白、Unicode文字など任意の文字が利用可能である必要があります。	必須
				1.3.4	パスワード文字列の入力フォームはinput type="password"で指定すること	基本的にinputタグのtype属性には「password」を指定しますが、パスワードを一時的に表示する可視化機能を実装する場合にはこの限りではありません。	必須
				1.3.5	ユーザーが入力したパスワード文字列を次画面以降で表示しないこと（hiddenフィールドなどのHTMLソース内やメールも含む）		必須

項目	見出し		要件		備考	必須可否
			1.3.6	パスワードを保存する際には、平文で保存せず、Webアプリケーションフレームワークなどが提供するハッシュ化とsaltを使用して保存する関数を使用すること	関数が存在しない場合にはパスワードは「パスワード文字列＋salt（ユーザー毎に異なるランダムな文字列）」をハッシュ化したものとsaltのみを保存する必要があります。（saltは20文字以上であることが望ましい） パスワード文字列のハッシュ化をさらに安全にする手法としてストレッチングがあります。	必須
			1.3.7	ユーザー自身がパスワードを変更できる機能を用意すること		必須
			1.3.8	パスワードはユーザー自身に設定させること システムが仮パスワードを発行する場合はランダムな文字列を設定し、安全な経路でユーザーに通知すること		推奨
			1.3.9	パスワードの入力欄でペースト機能を禁止しないこと	長いパスワードをユーザーが利用出来るようにするためにペースト機能を禁止しないようにする必要があります。	推奨
			1.3.10	パスワード強度チェッカーを実装すること	使用する文字種や文字数を確認し、ユーザー自身にパスワードの強度を示せるようにします。またユーザーIDと同じ文字列や漏洩したパスワードなどのリストとの突合を行う必要があります。手法については NIST Special Publication 800-63B などを参照してください。	推奨
	1.4	アカウントロック機能について	1.4.1	認証時に無効なパスワードで10回試行があった場合、最低30分間はユーザーがロックアウトされた状態にすること	パスワードに対する総当たり攻撃や辞書攻撃などから守るためには、試行速度を遅らせるアカウントロック機能の実装が有効な手段になります。アカウントロックの試行回数、ロックアウト時間については、サービスの内容に応じて調整することが必要になります。	必須
			1.4.2	ロックアウトは自動解除を基本とし、手動での解除は管理者のみ実施可能とすること		推奨
	1.5	パスワードリセット機能について	1.5.1	パスワードリセットを実行する際にはユーザー本人しか受け取れない連絡先（あらかじめ登録しているメールアドレス、電話番号など）にワンタイムトークンを含むURLなどの再設定方法を通知すること	連絡先については、事前に受け取り確認をしておくことでより安全性を高めることができます。 使用されたワンタイムトークンは破棄し、有効期限を12時間以内とし必要最低限に設定してください。	必須
			1.5.2	パスワードはユーザー自身に再設定させること		必須
	1.6	アクセス制御について	1.6.1	Web ページや機能、データをアクセス制御（認可制御）する際には認証情報・状態を元に権限があるかどうかを判別すること	認証により何らかの制限を行う場合には、利用しようとしている情報や機能へのアクセス（読み込み・書き込み・実行など）権限を確認することでアクセス制御を行うことが必要になります。 画像やファイルなどのコンテンツ、APIなどの機能に対しても、全て個別にアクセス権限を設定、確認する必要があります。 これらはアクセス権限の一覧表に基づいて行います。 CDNなどを利用してコンテンツを配置するなどアクセス制御を行うことが困難な場合、予測が困難なURLを利用することでアクセスされにくくする方法もあります。	必須

項目		見出し		要件		備考	必須可否
				1.6.2	公開ディレクトリには公開を前提としたファイルのみ配置すること	公開ディレクトリに配置したファイルは、URLを直接指定することでアクセスされる可能性があります。そのため、機微情報や設定ファイルなどの公開する必要がないファイルは、公開ディレクトリ以外に配置する必要があります。	必須
		1.7	アカウントの無効化機能について	1.7.1	管理者がアカウントの有効・無効を設定できること	不正にアカウントを利用されていた場合に、アカウントを無効化することで被害を軽減することができます。	推奨
2	セッション管理	2.1	セッションの破棄について	2.1.1	認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側のセッションを破棄しログアウトすること	認証を必要とするWebシステムの多くは、認証状態の管理にセッションIDを使ったセッション管理を行います。認証済みの状態にあるセッションを不正に利用されないためには、使われなくなったセッションを破棄する必要があります。セッションタイムアウトの時間については、サービスの内容やユーザー利便性に応じて設定することが必要になります。また、NIST Special Publication 800-63B などを参照してください。	必須
				2.1.2	ログアウト機能を用意し、ログアウト実行時にはサーバー側のセッションを破棄すること	ログアウト機能の実行後にその成否をユーザーが確認できることが望ましい。	必須
		2.2	セッションIDについて	2.2.1	Webアプリケーションフレームワークなどが提供するセッション管理機能を使用すること	セッションIDを用いて認証状態を管理する場合、セッションIDの盗聴や推測、攻撃者が指定したセッションIDを使用させられる攻撃などから守る必要があります。 また、セッションIDは原則としてcookieにのみ格納すべきです。	必須
				2.2.2	セッションIDは認証成功後に発行すること 認証前にセッションIDを発行する場合は、認証成功直後に新たなセッションIDを発行すること		必須
				2.2.3	ログイン前に機微情報をセッションに格納する時点でセッションIDを発行または再生成すること		必須
				2.2.4	認証済みユーザーの特定はセッションに格納した情報を元に行うこと		必須
		2.3	CSRF（クロスサイトリクエストフォージェリー）対策の実施について	2.3.1	ユーザーにとって重要な処理を行う箇所では、ユーザー本人の意図したリクエストであることを確認できるようにすること	正規ユーザー以外の意図により操作されては困る処理を行う箇所では、フォーム生成の際に他者が推測困難なランダムな値（トークン）をhiddenフィールドやcookie以外のヘッダーフィールド（X-CSRF-TOKENなど）に埋め込み、リクエストをPOSTメソッドで送信します。フォームデータを処理する際にトークンが正しいことを確認することで、正規ユーザーの意図したリクエストであることを確認することができます。 また、別の方法としてパスワード再入力による再認証を求める方法もあります。 cookieのSameSite属性を適切に使うことによって、CSRFのリスクを低減する効果があります。SameSite属性は一部の状況においては効果がないこともあるため、トークンによる確認が推奨されます。	必須
3	入力処理	3.1	パラメーターについて	3.1.1	URLにユーザーID やパスワードなどの機微情報を格納しないこと	URLは、リファラー情報などにより外部に漏えいする可能性があります。そのため URLには秘密にすべき情報は格納しないようにする必要があります。	必須

項目		見出し		要件		備考	必須可否
				3.1.2	パラメーター（クエリーストリング、エンティティボディ、cookieなどクライアントから受け渡される値）にパス名を含めないこと	ファイル操作を行う機能などにおいて、URL パラメーターやフォームで指定した値でパス名を指定できるようにした場合、想定していないファイルにアクセスされてしまうなどの不正な操作を実行されてし まう可能性があります。	必須
				3.1.3	パラメーター要件に基づいて、入力値の文字種や文字列長の検証を行うこと	各パラメーターは、機能要件に基づいて文字種・文字列長・形式を定義する必要があります。入力値に想定している文字種や文字列長以外の値の入力を許してしまう場合、不正な操作を実行されてしまう可能性があります。サーバー側でパラメーターを受け取る場合、クライアント側での入力値検証の有無に関わらず、入力値の検証はサーバー側で実施する必要があります。	必須
		3.2	ファイルアップロードについて	3.2.1	入力値としてファイルを受け付ける場合には、拡張子やファイルフォーマットなどの検証を行うこと	ファイルのアップロード機能を利用した不正な実行を防ぐ必要があります。画像ファイルを扱う場合には、ヘッダー領域を不正に加工したファイルにも注意が必要です。	必須
				3.2.2	アップロード可能なファイルサイズを制限すること	圧縮ファイルを展開する場合には、解凍後のファイルサイズや、ファイルパスやシンボリックリンクを含む場合のファイルの上書きにも注意が必要です。	必須
		3.3	XMLを使用する際の処理について	3.3.1	XMLを読み込む際は、外部参照を無効にすること	手法についてはXML External Entity Prevention Cheat Sheetなどを参照してください。 https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html	必須
		3.4	デシリアライズについて	3.4.1	信頼できないデータ供給元からのシリアライズされたオブジェクトを受け入れないこと	デシリアライズする場合は、シリアライズしたオブジェクトにデジタル署名などを付与し、信頼できる供給元が発行したデータであるかを検証してください。	必須
		3.5	外部リソースへのリクエスト送信について	3.5.1	他システムに接続や通信を行う場合は、外部からの入力によって接続先を動的に決定しないこと	外部から不正なURLやIPアドレスなどが挿入されると、SSRF(Server-Side Request Forgery)の脆弱性になる可能性があります。外部からの入力によって接続先を指定せざるを得ない場合は、ホワイトリストを基に入力値の検証を実施するとともに、アプリケーションレイヤーだけではなくネットワークレイヤーでのアクセス制御も併用する必要があります。	推奨
4	出力処理	4.1	HTMLを生成する際の処理について	4.1.1	HTMLとして特殊な意味を持つ文字（< > " ' &）を文字参照によりエスケープすること	外部からの入力により不正なHTMLタグなどが挿入されてしまう可能性があります。「<」→「<」や「&」→「&」、「"」→「"」のようにエスケープを行う必要があります。スクリプトによりクライアント側でHTMLを生成する場合も、同等の処理が必要です。実装の際にはこれらを自動的に実行するフレームワークやライブラリを使用することが望ましいでしょう。また、その他にもスクリプトの埋め込みの原因となるものを作らないようにする必要があります。 XMLを生成する場合も同様にエスケープが必要です。	必須
				4.1.2	外部から入力したURLを出力するときは「http://」または「https://」で始まるもののみを許可すること		必須

項目	見出し		要件		備考	必須可否
			4.1.3	<script>...</script>要素の内容やイベントハンドラ（onmouseover=""など）を動的に生成しないようにすること	<script>...</script>要素の内容やイベントハンドラは原則として動的に生成しないようにすべきですが、jQueryなどのAjaxライブラリを使用する際はその限りではありません。ライブラリについては、アップデート状況などを調べて信頼できるものを選択するようにしましょう。	必須
			4.1.4	任意のスタイルシートを外部サイトから取り込めないようにすること		必須
			4.1.5	HTMLタグの属性値を「"」で囲うこと	HTMLタグ中のname="value"で記される値(value)にユーザーの入力値を使う場合、「"」で囲わない場合、不正な属性値を追加されてしまう可能性があります。	必須
			4.1.6	CSSを動的に生成しないこと	外部からの入力により不正なCSSが挿入されると、ブラウザに表示される画面が変更されたり、スクリプトが埋め込まれる可能性があります。	必須
	4.2	JSONを生成する際の処理について	4.2.1	文字列連結でJSON文字列を生成せず、適切なライブラリを用いてオブジェクトをJSONに変換すること	適切なライブラリがない場合は、JSONとして特殊な意味を持つ文字（ " ￥ , : { } [ ] ）をUnicodeエスケープする必要があります。	必須
	4.3	HTTPレスポンスヘッダーについて	4.3.1	HTTPレスポンスヘッダーのContent-Typeを適切に指定すること	一部のブラウザではコンテンツの文字コードやメディアタイプを誤認識させることで不正な操作が行える可能性があります。これを防ぐためには、HTTPレスポンスヘッダーを「Content-Type: text/html; charset=utf-8」のように、コンテンツの内容に応じたメディアタイプと文字コードを指定する必要があります。	必須
			4.3.2	HTTPレスポンスヘッダーフィールドの生成時に改行コードが入らないようにすること	HTTPヘッダーフィールドの生成時にユーザーが指定した値を挿入できる場合、改行コードを入力することで不正なHTTPヘッダーやコンテンツを挿入されてしまう可能性があります。これを防ぐためには、HTTPヘッダーフィールドを生成する専用のライブラリなどを使うようにすることが望ましいでしょう。	必須
	4.4	その他の出力処理について	4.4.1	SQL文を組み立てる際に静的プレースホルダを使用すること	SQL文の組み立て時に不正なSQL文を挿入されることで、SQLインジェクションを実行されてしまう可能性があります。これを防ぐためにはSQL文を動的に生成せず、プレースホルダを使用してSQL文を組み立てるようにする必要があります。 静的プレースホルダとは、JIS/ISOの規格で「準備された文(Prepared Statement)」と規定されているものです。	必須
			4.4.2	プログラム上でOSコマンドやアプリケーションなどのコマンド、シェル、eval()などによるコマンドの実行を呼び出して使用しないこと	コマンド実行時にユーザーが指定した値を挿入できる場合、外部から任意のコマンドを実行されてしまう可能性があります。コマンドを呼び出して使用しないことが望ましいでしょう。	必須
			4.4.3	リダイレクタを使用する場合には特定のURLのみに遷移できるようにすること	リダイレクタのパラメーターに任意のURLを指定できる場合（オープンリダイレクタ）、攻撃者が指定した悪意のあるURLなどに遷移させられる可能性があります。	必須
			4.4.4	メールヘッダーフィールドの生成時に改行コードが入らないようにすること	メールの送信処理にユーザーが指定した値を挿入できる場合、不正なコマンドなどを挿入されてしまう可能性があります。これを防ぐためには、不正な改行コードを使用できないメール送信専用のライブラリなどを使うようにすることが望ましいでしょう。	必須

項目		見出し		要件		備考	必須可否
				4.4.5	サーバ側のテンプレートエンジンを使用する際に、テンプレートの変更や作成に外部から受け渡される値を使用しないこと	サーバ側のテンプレートエンジンを使用してテンプレートを組み立てる際に不正なテンプレートの構文を挿入されることで、任意のコードを実行される可能性があります。 外部から渡される値をテンプレートの組み立てに使用せず、レンダリングを行う際のデータとして使用する必要があります。 また、レンダリング時にはクロスサイトスクリプティングの脆弱性が存在しないか確認してください。	必須
5	HTTPS	5.1	HTTPSについて	5.1.1	Webサイトを全てHTTPSで保護すること	適切にHTTPSを使うことで通信の盗聴・改ざん・なりすましから情報を守ることができます。次のような重要な情報を扱う画面や機能ではHTTPSで通信を行う必要があります。 ・入力フォームのある画面 ・入力フォームデータの送信先 ・重要情報が記載されている画面 ・セッションIDを送受信する画面 HTTPSの画面内で読み込む画像やスクリプトなどのコンテンツについてもHTTPSで保護する必要があります。	必須
				5.1.2	サーバー証明書はアクセス時に警告が出ないものを使用すること	HTTPSで提供されているWebサイトにアクセスした場合、Webブラウザから何らかの警告がでるということは、適切にHTTPSが運用されておらず盗聴・改ざん・なりすましから守られていません。適切なサーバー証明書を使用する必要があります。	必須
				5.1.3	TLS1.2以上のみを使用すること	SSL2.0／3.0、TLS1.0／1.1には脆弱性があるため、無効化する必要があります。使用する暗号スイートは、7.2.1を参照してください。	必須
				5.1.4	レスポンスヘッダーにStrict-Transport-Securityを指定すること	Hypertext Strict Transport Security(HSTS)を指定すると、ブラウザがHTTPSでアクセスするよう強制できます。	必須
6	cookie	6.1	cookieの属性について	6.1.1	Secure属性を付けること	Secure属性を付けることで、http://でのアクセスの際にはcookieを送出しないようにできます。特に認証状態に紐付けられたセッションIDを格納する場合には、Secure属性を付けることが必要です。	必須
				6.1.2	HttpOnly属性を付けること	HttpOnly属性を付けることで、クライアント側のスクリプトからcookieへのアクセスを制限することができます。	必須
				6.1.3	Domain属性を指定しないこと	セッションフィクセイションなどの攻撃に悪用されることがあるため、Domain属性は特に必要がない限り指定しないことが望ましいでしょう。	推奨
7	その他	7.1	エラーメッセージについて	7.1.1	エラーメッセージに詳細な内容を表示しないこと	ミドルウェアやデータベースのシステムが出力するエラーには、攻撃のヒントになる情報が含まれているため、エラーメッセージの詳細な内容はエラーログなどに出力するべきです。	必須

項目	見出し		要件		備考	必須可否
	7.2	暗号アルゴリズムについて	7.2.1	ハッシュ関数、暗号アルゴリズムは『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（CRYPTREC暗号リスト）』に記載のものを使用すること	広く使われているハッシュ関数、疑似乱数生成系、暗号アルゴリズムの中には安全でないものもあります。安全なものを使用するためには、『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（CRYPTREC暗号リスト）』や『TLS暗号設定ガイドライン』に記載されたものを使用する必要があります。	必須
	7.3	乱数について	7.3.1	鍵や秘密情報などに使用する乱数的性質を持つ値を必要とする場合には、暗号学的な強度を持った疑似乱数生成系を使用すること	鍵や秘密情報に予測可能な乱数を用いると、過去に生成した乱数値から生成する乱数値が予測される可能性があるため、ハッシュ関数などを用いて生成された暗号学的な強度を持った疑似乱数生成系を使用する必要があります。	必須
	7.4	基盤ソフトウェアについて	7.4.1	基盤ソフトウェアはアプリケーションの稼働年限以上のものを選定すること	脆弱性が発見された場合、修正プログラムを適用しないと悪用される可能性があります。そのため、言語やミドルウェア、ソフトウェアの部品などの基盤ソフトウェアは稼働期間またはサポート期間がアプリケーションの稼働期間以上のものを利用する必要があります。もしアプリケーションの稼働期間中に基盤ソフトウェアの保守期間が終了した場合、危険な脆弱性が残されたままになる可能性があります。	必須
			7.4.2	既知の脆弱性のないOSやミドルウェア、ライブラリやフレームワーク、パッケージなどのコンポーネントを使用すること	利用コンポーネントにOSSが含まれる場合は、SCA（ソフトウェアコンポジション解析）ツールを導入し、依存関係を包括的かつ正確に把握して対策が行えることが望ましいでしょう。	必須
	7.5	ログの記録について	7.5.1	重要な処理が行われたらログを記録すること	ログは、情報漏えいや不正アクセスなどが発生した際の検知や調査に役立つ可能性があります。認証やアカウント情報の変更などの重要な処理が実行された場合には、その処理の内容やクライアントのIPアドレスなどをログとして記録することが望ましいでしょう。ログに機微情報が含まれる場合にはログ自体の取り扱いにも注意が必要になります。	必須
	7.6	ユーザーへの通知について	7.6.1	重要な処理が行われたらユーザーに通知すること	重要な処理（パスワードの変更など、ユーザーにとって重要で取り消しが困難な処理）が行われたことをユーザーに通知することによって異常を早期に発見できる可能性があります。	推奨
	7.7	Access-Control-Allow-Originヘッダーについて	7.7.1	Access-Control-Allow-Originヘッダーを指定する場合は、動的に生成せず固定値を使用すること	クロスオリジンでXMLHttpRequest (XHR)を使う場合のみこのヘッダーが必要です。不要な場合は指定する必要はありませんし、指定する場合も特定のオリジンのみを指定する事が望ましいです。	必須
	7.8	クリックジャッキング対策について	7.8.1	レスポンスヘッダーにX-Frame-OptionsとContent-Security-Policyヘッダーのframe-ancestors ディレクティブを指定すること	クリックジャッキング攻撃に悪用されることがあるため、X-Frame-Optionsヘッダーフィールドに DENYまたはSAMEORIGINを指定する必要があります。 Content-Security-Policyヘッダーフィールドに frame-ancestors 'none' または 'self' を指定する必要があります。 X-Frame-Options ヘッダーは主要ブラウザーでサポートされていますが標準化されていません。CSP レベル 2 仕様で frame-ancestors ディレクティブが策定され、X-Frame-Options は非推奨とされました。	必須

項目		見出し		要件		備考	必須可否
		7.9	キャッシュ制御について	7.9.1	個人情報や機微情報を表示するページがキャッシュされないよう Cache-Control: no-store を指定すること	個人情報や機密情報が含まれたページはCDNやロードバランサー、ブラウザなどのキャッシュに残ってしまうことで、権限のないユーザーが閲覧してしまう可能性があるためキャッシュ制御を適切に行う必要があります。	必須
		7.10	ブラウザのセキュリティ設定について	7.10.1	ユーザーに対して、ブラウザのセキュリティ設定の変更をさせるような指示をしないこと	ユーザーのWebブラウザのセキュリティ設定などを変更した場合や、認証局の証明書をインストールさせる操作は、他のサイトにも影響します。	必須
		7.11	ブラウザのセキュリティ警告について	7.11.1	ユーザーに対して、ブラウザの出すセキュリティ警告を無視させるような指示をしないこと	ブラウザの出す警告を通常利用においても無視させるよう指示をしていると、悪意のあるサイトで同様の指示をされた場合もそのような操作をしてしまう可能性が高まります。	必須
		7.12	WebSocketについて	7.12.1	Originヘッダーの値が正しいリクエスト送信元であることが確認できた場合にのみ処理を実施すること	WebSocketにはSOP (Same Origin Policy)という仕組みが存在しないため、Cross-Site WebSocket Hijacking(CSWSH)対策のためにOriginヘッダーを確認する必要があります。	必須
		7.13	HTMLについて	7.13.1	html開始タグの前に<!DOCTYPE html>を宣言すること	DOCTYPEで文書タイプをHTMLと明示的に宣言することでCSSなど別フォーマットとして解釈されることを防ぎます。	必須
				7.13.2	CSSファイルやJavaScriptファイルをlinkタグで指定する場合は、絶対パスを使用すること	linkタグを使用してCSSファイルやJavaScriptファイルを相対パス指定した場合にRPO (Relative Path Overwrite) が起きる可能性があります。	必須
8	提出物	8.1	提出物について	8.1.1	サイトマップを用意すること	認証や再認証、CSRF対策が必要な箇所、アクセス制御が必要なデータを明確にするためには、Webサイト全体の構成を把握し、扱うデータを把握する必要があります。そのためには上記の資料を用意することが望ましいでしょう。	必須
				8.1.2	画面遷移図を用意すること		必須
				8.1.3	アクセス権限一覧表を用意すること	誰にどの機能の利用を許可するかまとめた一覧表を作成することが望ましいでしょう。	必須
				8.1.4	コンポーネント一覧を用意すること	依存しているライブラリやフレームワーク、パッケージなどのコンポーネントに脆弱性が存在する場合がありますので、依存しているコンポーネントを把握しておく必要があります。	推奨
				8.1.5	上記のセキュリティ要件についてテストした結果報告書を用意すること	自社で脆弱性診断を実施する場合には「脆弱性診断士スキルマッププロジェクト」が公開している「Webアプリケーション脆弱性診断ガイドライン」などを参照してください。	推奨

別紙 7

要件仕様書標準テンプレート
（2024/08/27）

【凡例】
黒字：標準記載
多くの案件で汎用的に利用できる文章
青字：任意追加記載
調達案件の内容、条件に応じて追記する文章

令和 XX 年度

XXX システム

要件定義書

令和 XX 年 XX 月

農林水産省

1. 業務要件定義

1.1. 業務実施手順

(1) 業務範囲

本システムは原則として現行システムが対象とする業務範囲を踏襲する。一部業務は業務効率化の観点から機能自体の見直しを想定している。本システムでは XXX 機能が新たに業務範囲として追加されるため、留意すること。

現行の本システムが対象とする業務及び情報システム化の範囲を下表に示す。

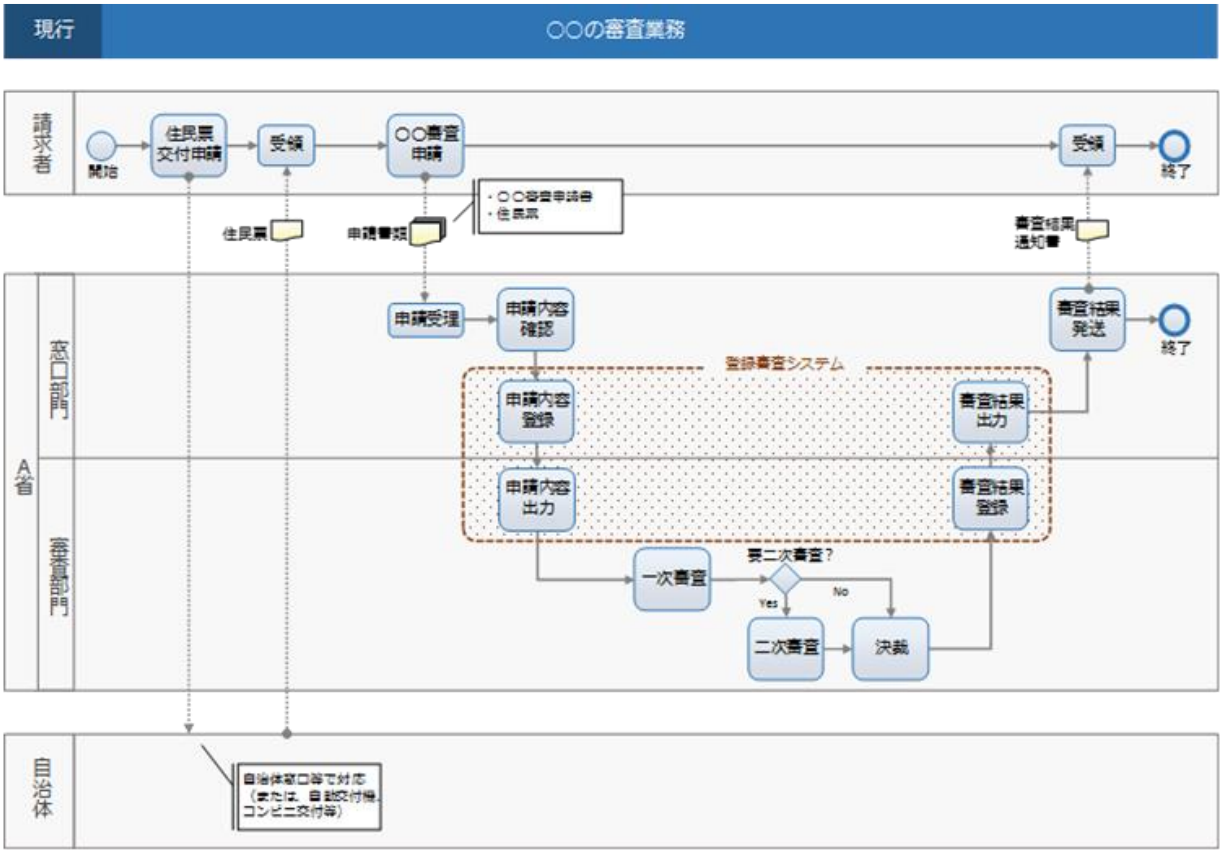
表 1 業務の範囲（業務機能とその階層）

階層 0		階層 1		階層 2			新情報システム適用対象候補
項番	名称	項番	名称	項番	業務 ID	名称	
1	図書貸出業務	1-1	貸出申請	1-1-1	A0001	申請作成	○
				1-1-2	A0002	申請提出	
		1-2	貸出申請受理	1-2-1	A0003	申請受理	○
				1-2-2	A0004	申請内容確認	
		1-3	貸出申請承認	1-3-1	A0005	貸出承認	○
…	…	…	…	…	…	…	…

(2) 業務フロー

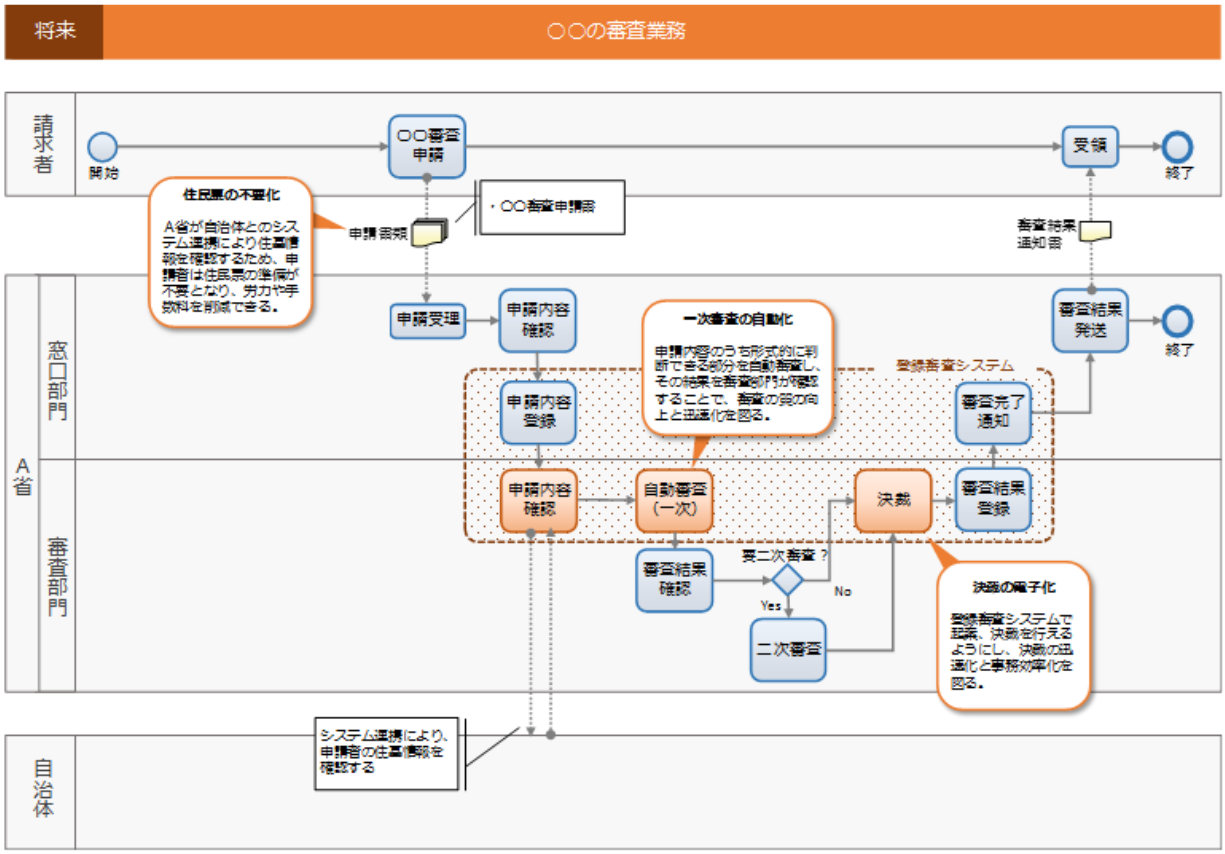
現行システムが対象とする業務及び情報システム化の範囲を下表に示す。

図 1 業務フロー（現行）の定義例



また、次期システムが対象とする業務及び情報システム化の範囲を下表に示す。なお、本システムで変更予定の業務フローについては該当箇所を明示している。

図 2 業務フロー（将来）の定義例



(3) 業務の実施に必要な体制

本システム関連業務の実施に現段階で想定する体制について、下表に示す。

表 2 業務の実施体制

項番	実施体制	業務概要	補足
1	サービス課（窓口担当者）	窓口における各種手続の受付及び審査、督促等を行う。	XXX
2	サービス課（貸出承認者）	貸出等の最終承認を行う。	XXX
3	管理課	蔵書に関する管理業務を行う。	XXX
…	…	…	…

(4) 入出力情報項目及び取扱量

本サービス運用開始後 1 年間程度の入出力情報及び取扱量に関する現段階における見通しを下表に示す。なお、本システム並びに関連するシステムの利用範囲の拡大に伴い、データの範囲と種類、容量が拡大する可能性もあることを、あらかじめ留意すること。

表 3 入出力情報項目及び取扱量

項番	業務処理	入出力情報名	入出力情報概要	入出力の区分	主な入出力情報項目	取扱量	用途	取得元/提供元	補足
1	貸出申請	貸出申請書	貸出手続の	入力	申請年月	年間約	貸出申請	申請者	XXX

			申請書		日、氏名、住所、貸出希望書籍名	20,000 件			
2	貸出申請承認	貸出承認書	貸出手続の審査結果通知	出力	受理年月日、氏名、住所、審査結果等	年間約 20,000 件	貸出申請結果通知	申請者/サービス課	XXX
3	蔵書更新	蔵書更新情報	蔵書の更新を記した帳票	入力	年月、書籍名、著者名、格納場所等	毎月 50 件	蔵書管理	管理課	XXX
4	…	…	…	…	…	…	…	…	…

(5) 管理対象情報一覧

対象業務で管理すべき情報（管理対象情報）を下表に示す。

表 4 管理対象情報一覧

項番	管理対象情報名	管理単位	主たる用途	主な属性	補足
1	書籍情報	書籍情報番号	ある書籍のタイトルに紐づく情報を持つ	書籍名、ISBN、著者、出版社名、版数、出版年月日、絶版の有無	書籍初回購入時に付番
2	書籍	書籍番号（書籍情報番号＋枝番）	ある書籍（物理的な印刷物など）個体に関する情報を持つ	購入年月日、貸出回数、廃棄予定日	書籍購入時ごとに付番
3	貸出申請	貸出番号（日付＋連番）	利用者が提出した申請書に関する情報を持つ	申請年月日、利用者氏名、貸出希望書籍名	申請受理時に付番
4	利用者	利用者番号	利用者に関する情報を持つ	氏名、住所、連絡先、利用回数	利用者登録時に付番
5	…	…	…	…	…

1.2. 業務の規模

本システムで実現する業務で想定される規模について、以下に示す。なお、本システムで実現する業務は、システム構築と合わせて令和 XX 年度以降に新しく開始される予定である。以下の内容についても、過去の業務実績等に基づく値ではなく、本調達時点の想定に基づく値である点に留意すること。

(1) サービスの利用者数及び情報システムの利用者数

本サービス及び情報システムの利用者について、下表に示す。

表 5 サービスの利用者数及び情報システムの利用者数（想定）

項番	利用者	利用者の種類		主な利用拠点	サービス提供時間帯	利用者数	補足
		サービス利用者	情報システム利用者				
1	市民	○	○	全国	9:00～17:00	約 100,000 人	XXX
2	図書館サービス窓口担当者	–	○	本省	24 時間	約 10 人	XXX
3	図書館管理課担当者	–	○	本省	24 時間	約 5 人	XXX

項番	利用者	利用者の種類		主な利用拠点	サービス提供時間帯	利用者数	補足
		サービス利用者	情報システム利用者				
4	…	…	…	…	…	…	…

(2) 処理件数

現行システムを用いた主な業務の処理件数は下表のとおりである。

表 6 主な業務の処理件数

項番	項目	処理件数		補足
		定常時	ピークの特性	
1	貸出申請件数（令和 XX 年度）	約 100 件/日	約 300 件/日 午前中と夕方に集中	XXX
2	・・・	・・・	・・・	・・・

1.3. 業務実施の時期・時間

(1) 業務実施時期・期間及び繁忙期

本サービスに係る業務実施時期・期間は、原則として開庁日（土日及び祝日、年末年始を除く）とする。本サービスに係る業務の通常時と繁忙期を下表に示す。なお、繁忙期においてもレスポンスの低下等を招かないよう、十分な処理性能を確保すること。

表 7 業務の通常期、繁忙期

項番	実施時期・期間		補足
1	通常期	下記以外	XXX
2	繁忙期	3 月～4 月、6 月～7 月	XXX

(2) 業務の実施・提供時間

本システムについては、主管課の責任のもとで運用・保守事業者が運用作業を実施する。なお、本システムのサービス提供時間、運用時間、システム障害時の対応については以下のとおりである。

ア サービス提供時間

本サービスは計画停止を除き、24 時間 365 日サービスを提供できること。利用者ごとのサービス提供時間帯は「表 5 サービスの利用者数及び情報システムの利用者数（想定）」に記載の通り。

イ 運用時間

運用・保守業者の運用時間は平日（土日及び祝日、年末年始を除く）の 9 時から 17 時までとする。ただし、システムの監視は 24 時間 365 日行うこと。

夜間や休日におけるシステム障害時の連絡体制については、運用時間と同等の体制を維持することは求めないが、障害の重要性に応じた機動的な体制を提案すること。

ウ システム障害時の対応

システム障害時は復旧を優先し、一次対応を速やかに実施すること。障害の原因究明・恒久的対策は、原則としてシステム復旧後、翌開庁日の運用時間内にシステム保守として実施すること。

【プロジェクトの特性上ミッションクリティカルである場合】
システム障害時は復旧を優先し、一次対応を速やかに実施すること。障害の原因究明・恒久的対策についても速やかに実施し、結果を主管課に報告すること。

(3) ヘルプデスク業務

ヘルプデスク業務における問合せ対応の受付時間を下表に示す。

表 8 ヘルプデスク業務の問合せ対応時間

項番	問い合わせ方法	受付時間	回答時間	補足
1	電話	開庁日 9:00~17:00	開庁日 9:00~17:00	XXX
2	メール	24 時間 365 日	同上	XXX
3	Web フォーム	同上	同上	回答はメールにて実施する。回答メールの内容は主管課と協議して定める。
4	…	…	…	…

1.4. 業務の実施等

本システムにおける業務の実施場所に関する要件について、以下に示す。

表 9 利用者の業務の実施場所

項番	場所名	実施体制	実施業務	所在地
1	XXX 図書館	管理課	蔵書に関する管理業務を行う。	XXX 県 XXX 市 XXX 町 XXX 番地
2		サービス課	情報システムを利用した貸出申請に対する受付、審査、督促等を行う。	
3	・・・	・・・	・・・	・・・

1.5. 業務観点で管理すべき指標

本サービスに係る達成度評価指標（KPI：Key Performance Indicator）を下表に示す。なお、本サービスの利用動向を踏まえ、必要に応じて更に KPI を追加または変更する場合がある。KPI の追加または変更により「2.4.（8） モニタリング対象データ一覧」および「3.16.（5） 主な運用作業一覧」に変更があった場合は、対応範囲を主管課と協議の上で決定、対応すること。

表 10 達成度評価指標（KPI：Key Performance Indicator）

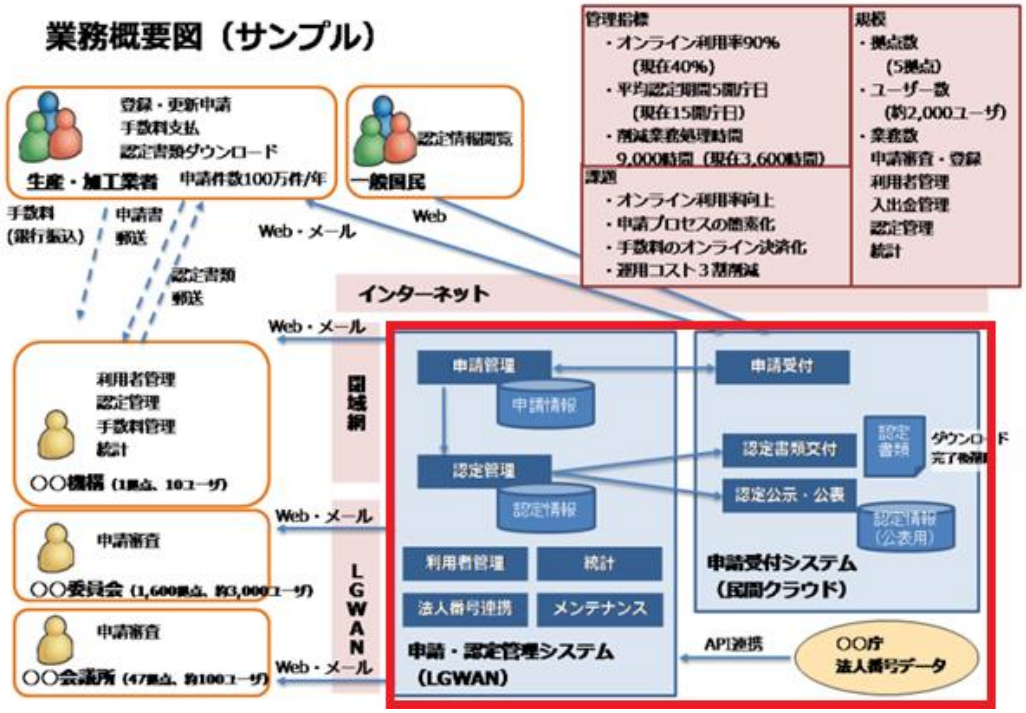
項番	指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
1	業務（サービス）効果指標	平均審査期間	対象案件における以下の平均値（結果通知日）－（申請受付日）	日	7 日（開庁日・閉庁日を含める） 現状:平均 20 日	本システムの統計機能から取得する	月次
2	業務処理時間の削減	XXX 業務処理 1 件あたりの削減時間	「現行業務処理時間」－「業務・サービス改革実施後の業務処理時間」	時間	2 時間 現状:5 時間	業務ログから 1 件当たりの処理時間を取得する。	四半期に 1 度
3	…	…	…	…	…	…	…

1.6. 情報システム化の範囲

(1) 情報システム化の範囲

本調達の範囲は、下図の赤枠部分に示す範囲である。

図 3 業務概要図（サンプル）



1.7. 業務の継続の方針等

システムの継続に関しては「3.9 継続性に関する事項」に記載する対策を講じること。

【障害によるシステム停止時にも最低限継続すべき業務がない場合】

本システムでは障害によるシステム停止時にも最低限継続すべき業務はないため、本章は特に定めない。

【障害によるシステム停止時にも最低限継続すべき業務がある場合】

本項目では業務の継続に関する要件を記載する。

(1) システム停止時を想定した業務

本システムが全面的に利用できなくなった場合でも、業務を継続するために最低限必要となる情報については、主管課の指示に従い、電子媒体もしくは紙資料に別途保存すること。保存の頻度は１か月に一回を想定する。

1.8. 情報セキュリティ対策の方針等

本システムの情報セキュリティ対策に係る具体的な要件は、「3.10 情報セキュリティに関する事項」を参照すること。

(1) 情報セキュリティ対策の基本的な考え方

表 11 システムで扱う情報の特徴

項番	主な情報	情報の機密性		その他（情報の完全性、可用性等）		情報の取扱いで考慮すべき関連法令	補足
		特徴	格付の区分	特徴	格付の区分		
1	貸出申請書	個人情報が含まれる。情報漏えい等が発生した場合、利用者に財産上の被害を与えるおそれがある。当該業務において最も機密性の高い情報。	機密性２情報	－	－	XXX 法	XXX
2	貸出承認書	個人情報が含まれる。情報漏えい等が発生した場合、一定程度の社会的批判を受けるおそれがある。	機密性２情報	情報の改竄により業務に一定の影響を受けるおそれがある。（電子署名の付与等の対策が必要）	完全性２情報	XXX 法	XXX
3	…	…	…	…	…	…	…

2. 機能要件定義

2.1. 機能に関する事項

(1) 機能一覧

本調達で要求する主要な機能を下表に示す。詳細な機能構成は、要件定義工程にて主管課と協議の上決定すること。

表 12 機能一覧

項番	機能 ID	機能分類	機能名	機能概要			処理方式	利用者区分	現状の機能との差異	該当業務	補足
				入力	処理	出力					
1	BP1110	XXX	利用者登録	XXX	XXX	XXX	オンライン	XXX	XXX	業務 ID：Z0001	XXX
2	BP1121	XXX	貸出申請	XXX	XXX	XXX	オンライン	XXX	XXX	XXX	XXX
3	BP1122	XXX	申請書確認	XXX	XXX	XXX	オンライン	XXX	XXX	XXX	XXX
4	BP1123	XXX	申請書承認	XXX	XXX	XXX	オンライン	XXX	XXX	XXX	XXX
5	BP1130	XXX	返却	XXX	XXX	XXX	オンライン	XXX	XXX	XXX	XXX
6	BP1140	XXX	申請情報連携	XXX	XXX	XXX	バッチ	XXX	XXX	XXX	XXX
…	…	…	…	…	…	…	…	…	…	…	…

【受託者から提案を受ける場合】

受託者は、「表 12 機能一覧」を踏まえ、具体的な機能及びその実装の方法（機能の単位、画面構成・遷移等を含む。）等について、提案するシステム方式等に応じて適切なものを提案すること。その際には、現行システムの実装方法（機能の単位、画面構成・遷移等を含む。）を単純に踏襲するのではなく、現時点で広く使われている技術を前提として、ユーザビリティや開発効率性の観点から優れた方法を選択するよう留意すること。

より適切な他の手段により実質的に想定機能の一部又は全部を代替可能な場合（外部サービスの利用、ノンプログラミングによる画面生成等プロトタイピング用のツール等を採用する場合など、既存の機能・サービスで置き換えることが可能な場合を含む。）には、当該代替可能な機能と当該手段を示すこと。また、想定機能は、受託者が提案する方法で実質的に代替可能であることを客観的かつ具体的に確認できる提案となっていること。

(2) 技術検証

現在、実現性、性能、セキュリティ、利便性、運用性等の観点から技術検証を行っている。当該技術検証の結果を踏まえ、本システムを設計・開発すること。なお、技術検証の状況については、本調達時点の技術検証状況を閲覧資料として提供する予定である。

(3) 機能の主な追加・変更点

本システムでは下表の観点での機能見直しを行う予定である。

表 13 機能の主な追加・変更点

項番	変更区分	主な観点	説明	メリット
1	新規追加	スマートフォンによる利用者登録機能の実装	現行システムにおいては PC からのみ利用者登録が可能だったが、次期システムではスマートフォンからも利用者登録を可能とする。	利用者の利便性が向上する。
2	変更	本システム及び外部連携システム間の連携項目の追加	法制度の変更に伴い、XXX 情報を追加で取得する必要があるため、連携項目を追加する。	法制度に準拠した対応ができる。
3	…	…	…	…

(4) 今後の機能追加を踏まえた構成

本調達で要求する機能ではないが、将来追加が必要となる機能を下表に示す。これらの機能追加を想定した構成とすること。なお、拡張性については、「3.6 拡張性に関する事項」も参照すること。

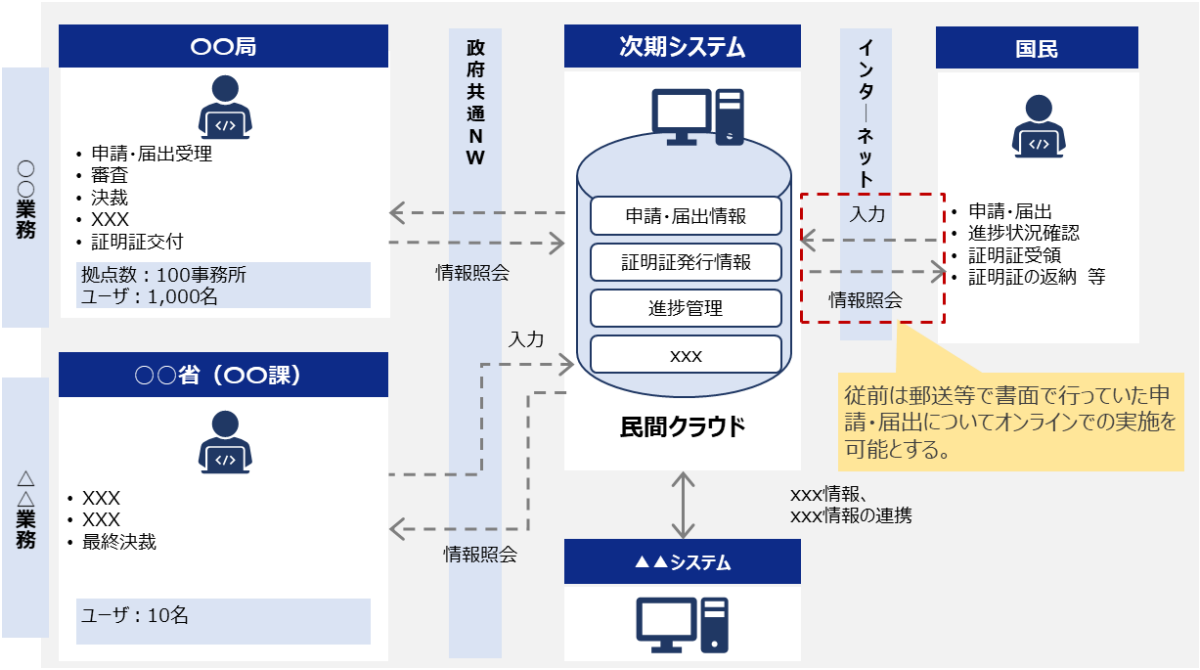
表 14 将来追加する必要のある機能一覧

項番	機能分類	機能名	概要
1	XXX	督促	返却期限が迫る貸出本を借りている利用者をシステムで洗い出し、登録されているメールアドレス宛に自動で督促に係るメールを送信する機能を搭載する。
2	…	…	…

(5) 機能構成概念図

本サービスの機能構成概念図を以下に示す。なお、図の記載内容が過度に複雑化することを避けるため、下図では機能分類に着目し、各機能の位置関係と情報フローに焦点を当てて表現することとしている。

図 4 機能構成概念図例



2.2. 画面に関する事項

前述の「2.1 機能に関する事項」を実現するために必要な画面については、本システムの受託者の提案を踏まえ、設計時点で決定する。

画面レイアウト等の設計に当たっては、予めワイヤーフレーム（画面の完成イメージを線や枠で表現したもの）などを作成し、主管課の了承を得た上で設計を行うこと。なお、主管課ではワイヤーフレーム作成環境として Figma を採用しているため、受託者側でも Figma を使用できる環境を準備すること。

(1) 画面一覧

本サービスの画面一覧を下表に示す。なお、個別具体のユーザーインタフェースとして実装する際の画面構成、画面レイアウト、画面タイトル等のラベル、画面遷移等の詳細は基本設計工程で定める。本要件定義書では画面設計に当たっての基本的な方針を定めている。

表 15 画面一覧（想定）

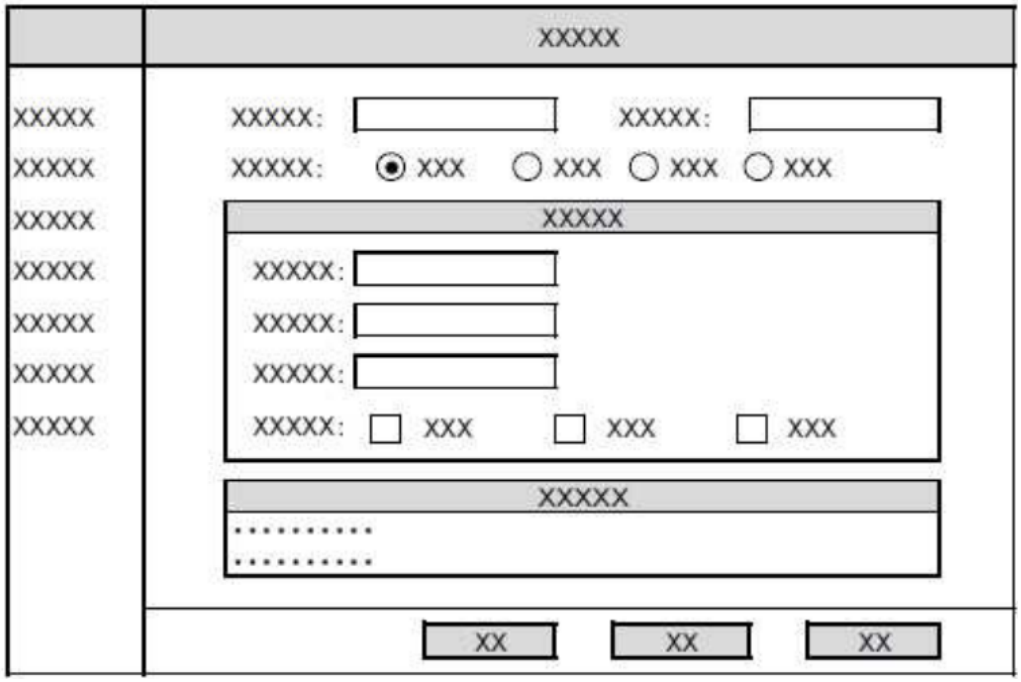
項番	画面 ID	画面名	画面概要	該当機能	補足
1	XXX	XXX 申請書作成	XXX 申請者が利用する XXX 申請書の作成画面	機能 ID:XXX	XXX
2	XXX	XXX 申請書確認	XXX 申請者が利用する XXX 申請書の作成確認画面	機能 ID:XXX	XXX
3	…	…	…	…	…

(2) 画面イメージ

本サービスの基本的・代表的な画面イメージを下図に示す。紙面スペースの制約上、一部を抜粋したものとしているが、全体像については、調達仕様書に基づく資料閲覧を行う際に確認することが可能である。なお、以下に示す表示イメージは、デザインプロトタイプとして作成したものである。個別具体のユーザーインタフェースとして実装する際の画面構成、画面レイアウト、画面タイトル等のラベル等については、本サービスの設計・開発段

階で行う UX 開発において改めて設計を行う。また、画面表示イメージに表現されている内容は、デザインを明確にする観点から便宜的に当てはめたものである。

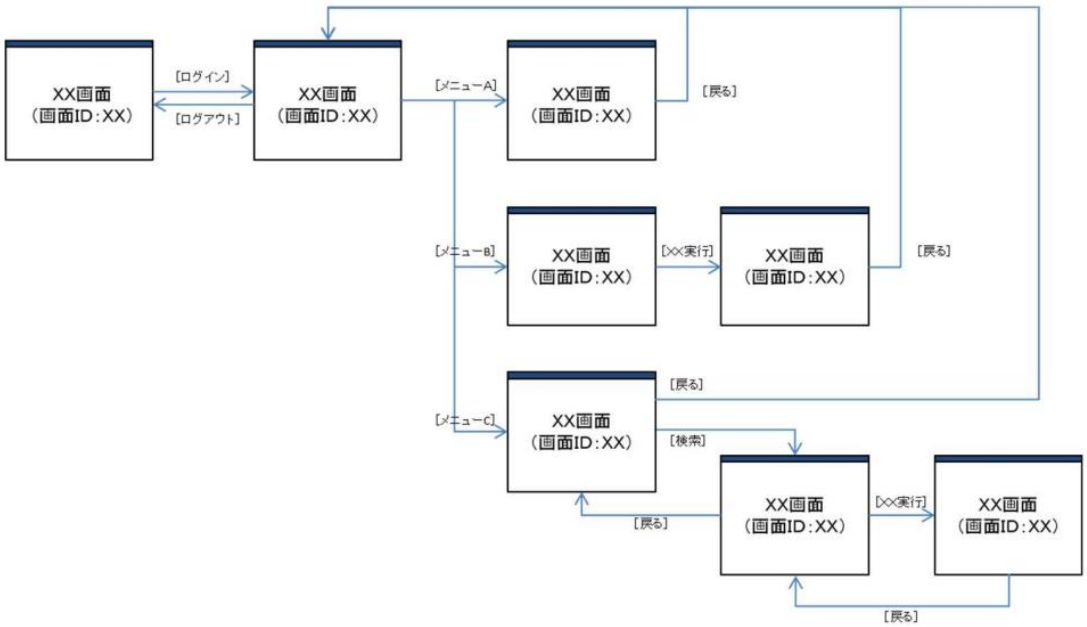
図 5 画面イメージ



(3) 画面遷移の基本的考え方

基本的・代表的な画面遷移として、トップ画面遷移図を以下に記載する。

図 6 画面遷移図



(4) 画面設計ポリシー

画面設計における要件を以下に示す。

ア　UX デザイン

UX デザインについては、以下の要件を満たすこと。加えて「3.1 ユーザビリティ及びアクセシビリティに関する事項」の要件も考慮すること。

- 本サービス想定利用者の目的を満足する観点から、本サービスを構成する機能、コンテンツの設計に当たっては、適切なユーザー調査によって利用者の要件を把握すること。
- 本サービスに係る UX デザインは、UX に影響を及ぼす要素を 5 階層によって把握する UX5 階層モデルの考え方を導入する。本サービスの Web サイト及び Web アプリケーションについて、本サービスの目的を基底として、体系的かつ一貫性のある UX を確保できるようにすること。

イ　画面の表示

画面の表示に関して、利用者に正しく内容を伝達するために、以下の要件を満たすこと。

- 画面の表示には HTML を利用し、Web ブラウザ上で正常に表示されることを確認すること。また、JavaScript を無効にした状態でも最低限のコンテンツ情報を閲覧可能とすること。
- 画面の表示で使用する Web ブラウザには追加でプラグイン等のインストールを必要としないこと。
- Web ブラウザのバージョンの更新があった際は、基本的には更新前のバージョンへの対応を保ちつつ、更新後のバージョンに対応させること。やむを得ず、双方のバージョンへの対応が困難な場合は、対応を優先するバージョンは主管課が判断を行うものとする。
- 利用者が他に起動している Web ブラウザの動作に干渉しないように配慮すること。
- Web ブラウザや利用端末の要件については、「3.11.情報システム稼働環境に関する事項」の「(7) 利用端末の要件」を参照すること。

ウ　入力負荷の軽減

画面での入力操作は以下の要件を満たすこと。

- 画面での入力操作は、業務特性に応じて、入力負荷の軽減及び誤操作防止等に配慮すること。
- 日付を入力する項目については可能な限りカレンダーから日付を選択できること。

エ　誤操作の防止

利用者認証情報を取り扱う重要性を考慮し、誤操作によるデータの消失や誤った情報の登録等を防止する為、以下の要件を満たすこと。

- Web ブラウザ自体が備えている「戻る」、「更新」等のボタンを押下しても、二重登録などの不具合が発生しないこと。
- Web ブラウザで表示する画面内のボタンを連続で押下しても、二重登録などの不具合が発生しないこと。
- 検索処理中に再度の検索実行が行われないこと。（検索処理中は検索実行ボタンを非活性化する等）

オ　メニュー

メニューについては、以下の要件を満たすこと。

- 各画面の上部に統一的な操作メニューを表示し、他の画面への遷移を可能とすること。
- 現在の画面のメニュー体系における位置を階層的に表示し、他の画面への遷移を可能とすること。
- 利用用途（一般利用、システム管理等）、利用者（承認者、担当者等）により操作可能な画面が異なるため、権限設定に応じたメニュー表示を可能とすること。

2.3. 帳票に関する事項

【帳票を作成する機能がないシステムの場合】

本システムでは、帳票（紙帳票、PDF 等の電子帳票の双方を指す）を作成する想定はない。ただし、利用登録の初期発行、失効等の各種処理完了時には、利用者に対して、画面やメール等で通知を行う仕組みを設けること。

【帳票を作成する機能を持つシステムの場合】

本システムの帳票に関する要件を「表 16 帳票一覧」「図 7 帳票イメージ」に示す。なお、法定帳票以外の帳票については、代替手段を積極的に提案して帳票の削減を提案すること。

(1) 帳票一覧

原則として、各帳票間で基本レイアウトの統一を図ること。なお、帳票の実装方式については、現時点で広く使われている技術を前提として、ユーザビリティや開発効率性の観点から優れた方法を選択するよう特に留意すること。

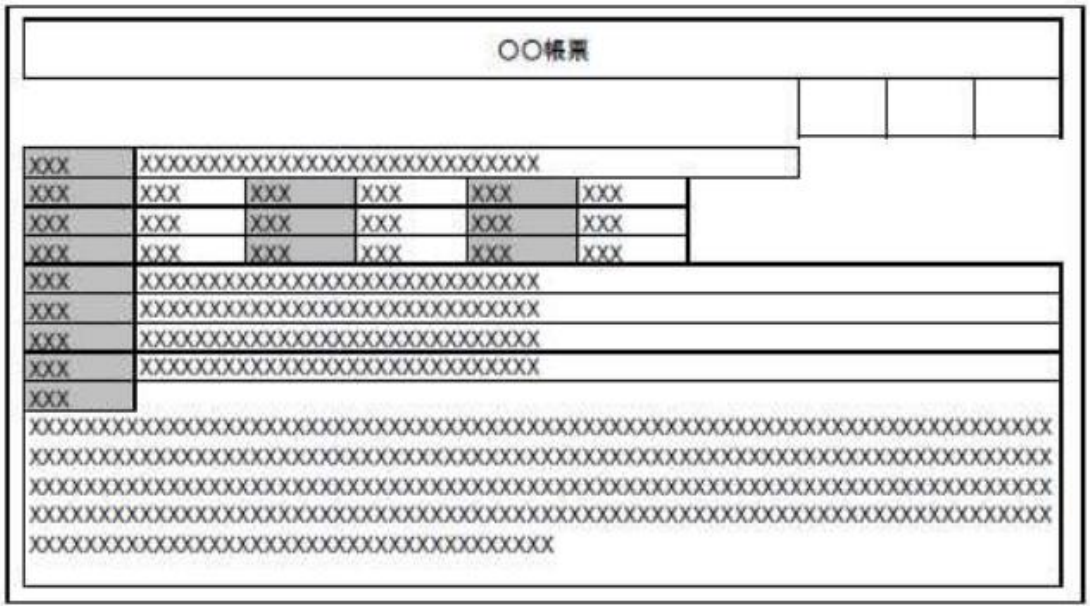
表 16 帳票一覧

項番	帳票 ID	帳票概要	入出力形式	該当機能	補足
1	XXX	XXX 申請用	紙（A4）	機能 ID:XXX	XXX
2	XXX	XXX 申請用	PDF	機能 ID:XXX	XXX
3	…	…	…	…	…

(2) 帳票イメージ

本サービスの基本的・代表的な帳票イメージを下図に示す。

図 7 帳票イメージ



2.4. データに関する事項

本システムで管理する各種情報については、以下に示す情報・データを概念レベルでの基本とする。なお、情報・データの修正が必要になる場合や、関係する組織やシステム等とのデータ授受方法の詳細については、設計工程で主管課と協議の上で対応すること。

(1) データモデル

本システムのデータモデルを下図に示す。

図 8 データモデル

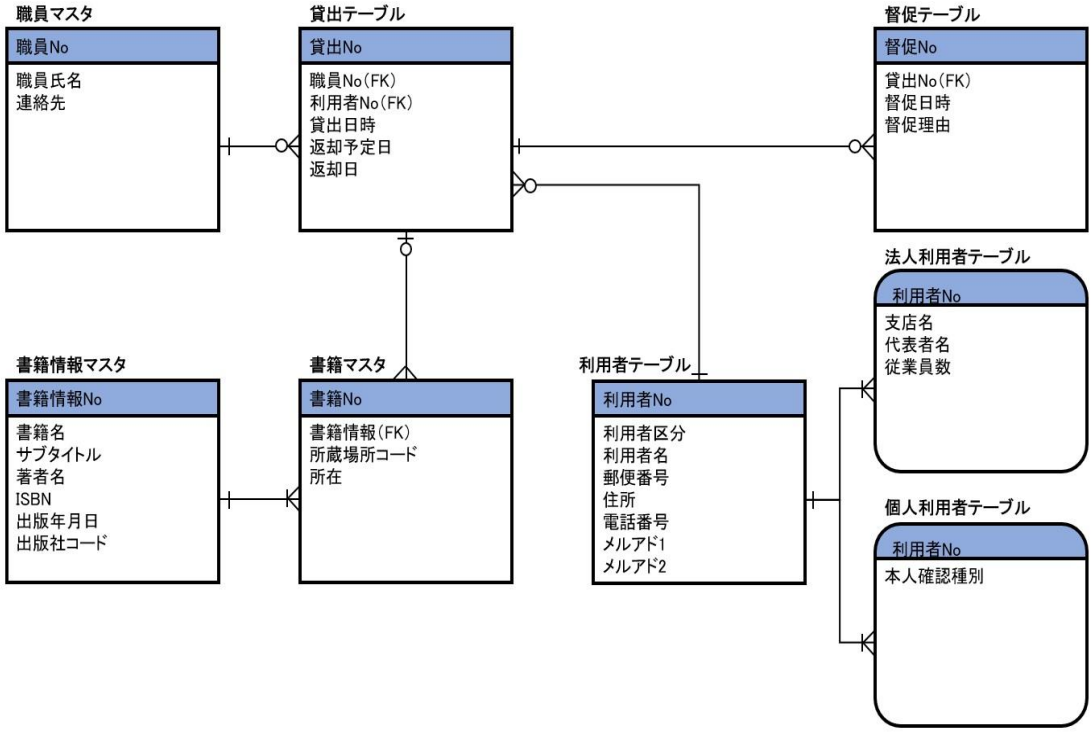
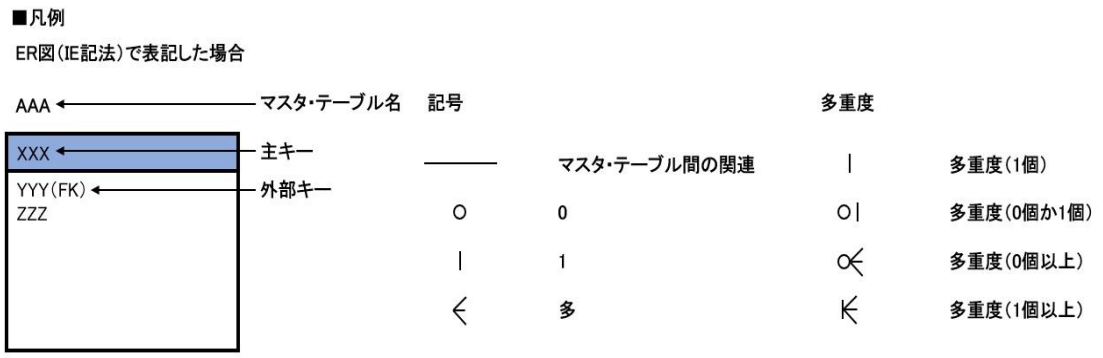


図 9 データモデルの凡例



(2) データ一覧

本システムのデータ一覧を下表に示す。なお、下表のデータ一覧については、主管課が定める DS-400 政府相互運用性フレームワーク（GIF）を参照して作成している。受託者も同フレームワークを十分に理解し、作

業を進めること。

ア　マスターデータ

表 17 マスターデータ一覧

No.	データID	データ名	概要・用途	主管部門	保存期間	規模情報（概算）				状態遷移の確認対象	マスターデータ分類	分類選択理由	標準化レベル	個人情報／特定個人情報の有無	格付・取扱・アクセス制限	公開可否	公開範囲	公開不可の理由	運用管理レベル	保管方法	備考
						初期件数	増加件数	最大件数	レコード長												
1	EN-003	利用者	すべての利用者情報を一元的に管理する。	サービス課	永久保存	7,000	1,000/年	20,000	200B	×	4	個人情報		個人情報	機密性２ ・下のアクセス権を複数に応じて付与する ・データベースへのアクセスに対し認証を求め付ける	×	管理者のみ	個人情報	レベル３	・利用者が直接アクセス可能な機器に保存しない ・複製できるデータベースを制限する	
2	EN-004	年次	すべての年次データを一元的に管理する。	管理課	永久保存	40,000	1,000/年	200,000	100B	×	3	他の業務システムでの利用を見込んでいるため。	省内標準	無	データの変更権限は担当者1名のみとする。	○	制限なし		レベル２	管理するデータベースと、利用者がアクセスできるデータベースとを別にしてデータを保管する。	
3	EN-005	書籍検索	すべての書籍検索を一元的に管理する。	管理課	永久保存	15,000	500/年	75,000	400B	×	3	他の他システムでの利用を見込んでいるため。	省内標準	無	データの変更権限は担当者1名のみとする。	○	制限なし		レベル２	管理するデータベースと、利用者がアクセスできるデータベースとを別にしてデータを保管する。	
4	EN-006	職員	すべての職員情報を一元的に管理する。	管理課	永久保存	20	1～2/年	25	400B	×	4	個人情報		個人情報	機密性２ ・下のアクセス権を複数に応じて付与する ・データベースへのアクセスに対し認証を求め付ける	×	管理者のみ	個人情報	レベル３	・利用者が直接アクセス可能な機器に保存しない ・複製できるデータベースを制限する	
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

イ　マスターデータ以外（トランザクションデータ、入出力ファイル等）

表 18 マスターデータ以外のデータ一覧

No.	データID	データ名	概要・用途	主管部門	保存期間	規模情報（概算）				状態遷移の確認対象	個人情報／特定個人情報の有無	格付・取扱・アクセス制限	公開可否	公開範囲	公開不可の理由	運用管理レベル	保管方法	備考
						初期件数	増加件数	最大件数	レコード長									
1	EN-001	貸出	すべての貸出情報を一元的に管理する。	サービス課	2年	15,000	2,000/年	30,000	400B	○	無	本業務に関わる省内職員のみアクセス可能とする	○	管理者のみ		レベル２	利用者が直接アクセス可能な機器に保存しない	
2	EN-002	延保	貸出情報に基づいた該当利用者への催促情報を一元的に管理する。	管理課	2年	15,000	2,000/年	300,000	300B	○	無	本業務に関わる省内職員のみアクセス可能とする	○	管理者のみ		レベル２	利用者が直接アクセス可能な機器に保存しない	
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

(3) データ定義

本システムのデータ定義を下表に示す。

表 19 データ定義

データID	EN-001	データ名	貸出	データ分類	E	上位概念						
用途	すべての貸出情報を一元的に管理する。											
データの単位	利用者に書籍の貸し出しを行う際、貸出票ごとに1件の「貸出」を作成する。											
No.	データ項目名	データタイプ	データ概要	主キー	参照キー	データ型	桁数	標準化レベル	機密性レベル	暗号化有無	履歴管理	備考
1	貸出No.	貸出No.	貸出をユニーク識別するナンバー。	○			8	省内標準	機密性1情報	有	原則変更不可とし、変更する場合は変更履歴において変更者と変更日時を明示する。	
2	貸出日時	年月日時分秒	当該貸出の時刻（年月日時分秒まで）				14	省内標準	機密性1情報	無	原則変更不可とする。	
3	返却予定日	年月日	当該貸出の書籍返却期限				8	省内標準	機密性1情報	無	原則変更不可とし、変更する場合は変更履歴において変更者と変更日時を明示する。	
4	返却日	年月日	実際の返却日				8	省内標準	機密性1情報	無	原則変更不可とする。	
…	…	…	…	…	…	…	…	…	…	…	…	…

(4) CRUD マトリクス

本システムの CRUD マトリクスを下表に示す。

表 20 CRUD マトリクス

機能ID	機能名	概念データ（EN-xxx）					
		001	002	003	004	005	006
		貸出	催促	利用者	書籍	書籍情報	職員
BP1110	利用者登録			C			
BP1121	貸出申請	C		R	U	R	R
BP1122	申請書確認	R		R	R	R	R
BP1123	申請書承認	U		R	U	R	R
BP1130	返却	U		R	U	R	R
BP1140	催促	R	C	R	R	R	R

(5) コード一覧

本システムで使用するデータのコード一覧を下図に示す。

表 21 コード一覧

No.	コード名	用途	主管部門	コード内容定義の有無	コード構成				コード標準化分類	分類選択理由	標準化レベル	公開可否	公開範囲	公開不可の理由	備考
					データ型	桁数	項目名	構成項目説明							
1	利用者区分	利用者を識別する区分	サービス課	有	数字	1	法人個人区分	法人か個人かの区分	3	他システムでも利用可能であるため	省内標準	○	制限なし		
2	本人確認種別	本人確認方法の種別	サービス課	有	数字	2	本人確認種別	2桁の本人確認種別	3	他システムでも利用可能であるため	省内標準	○	一般市民		
3	催促理由	催促理由の種別	サービス課	有	数字	1	催促理由	1桁の催促理由	3	他システムでも利用可能であるため	省内標準	○	一般市民		
4	出版社コード	書籍の出版社を識別するコード	管理課	無	数字	13	法人番号	国税庁の法人番号13桁	1	既に公開されているため	国内標準	○	一般市民		
5	所在	書籍の所在の有無	管理課	無	数字	1	所在	0:貸出中、1:所蔵中	3	他システムでも利用可能であるため	省内標準	○	一般市民		
6	所蔵場所コード	書籍の所蔵場所を特定するコード	管理課	無	英数字	2	書架コード	2桁の書架コード	3	他システムでも利用可能であるため	省内標準	○	一般市民		
					数字	2	棚番号	2桁連番の棚番号	3	他システムでも利用可能であるため	省内標準	○	一般市民		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

(6) コード内容定義

本システムで使用するデータのコード内容定義を下表に示す。

表 22 コード内容定義

No.	コード名	値	値の内容	備考
1	利用者区分	1	個人利用者	
		2	法人利用者	
2	本人確認種別	01	マイナンバーカード	
		02	免許証	
		03	住民票	
		04	健康保険証	
		05	パスポート	
		06	身分証明書	
		99	その他	
3	催促理由	1	返却期限後1週間経過	
		2	返却期限後2週間経過	
		9	その他	「返却期限後3週間以上経過」も含む

(7) オープンデータ一覧

本システムのオープンデータを下表に示す。

表 23 オープンデータ一覧

No.	データID	データ名	概要	利用者	公開範囲	利用目的	利用頻度・特徴	実装方式	処理方式	備考
1	EN-004	書籍	すべての書籍を一元的に管理する	職員・一般市民	制限なし	書籍の所蔵場所や所在を確認する	アクセス数100件／日 ピーク時はアクセス数200件／日 ピークは3～4月及び7～8月を想定している	API	バッチ型	
2	EN-005	書籍情報	すべての書籍情報を一元的に管理する	職員・一般市民	制限なし	書籍情報（書籍名や著者名等）を確認する	アクセス数80件／日 ピーク時はアクセス数160件／日 ピークは3～4月及び7～8月を想定している	API	バッチ型	
3	EN-009	所蔵場所	すべての所蔵場所の情報を一元的に管理する	職員・一般市民	制限なし	書籍の所蔵場所の住所や書架を確認する	アクセス数80件／日 ピーク時はアクセス数160件／日 ピークは3～4月及び7～8月を想定している	API	リアルタイム型	
…	…	…	…	…	…	…	…	…	…	…

(8) モニタリング対象データ一覧

「1.5.業務観点で管理すべき指標」に記載したプロジェクトの目標について、実績値を適時に確認するデータとして、現時点の案を示す。

表 24 モニタリング対象データ一覧（想定）

No.	データ名	分析軸となる項目	目的
1	サービスに関する登録者のユニークな数	性別、年代、アカウント種別など	サービスの利用意向者の数およびその特徴が把握できること
2	サービスサイトへアクセスしたユーザーのユニークな数	性別、年代、アカウント種別など	サービスの利用意向者の数およびその特徴が把握できること
3	サービスに関する申請の数	申請種別、申請の受付種別など	サービスの利用件数およびその詳細が把握できること
4	Web ページや特定コンテンツの閲覧数、ダウンロード数	コンテンツ種別など	サービスのアクセス件数およびその詳細が把握できること
5	API のリクエスト数	API 種別など	システムからの利用件数およびその詳細が把握できること
6	…	…	…

2.5. 外部インタフェースに関する事項

本システムの外部インタフェースに関する要件を以下に示す。なお、一部のインタフェースは機能要件の変更に合わせて修正が必要になることが想定される。新たに追加となった機能への対応を含め、外部インタフェースの修正が必要になる場合については、設計工程で主管課と協議の上で対応すること。なお、インタフェースについては API 連携を原則とし、旧来型のインタフェースについては API 化を積極的に提案すること。

(1) 外部インタフェース一覧

本サービスは、下表に示す他の情報システム等と連携する。なお、外部インタフェース一覧における記載内容は現在の想定である。設計工程において、連携先システム担当と調整の上、決定すること。

表 25 外部インタフェース一覧（想定）

項番	外部インタフェースID	外部インタフェース名	外部インタフェース概要	相手先システム	送受信区分	送受信データ種別	送受信タイミング	送受信の条件		補足
								プロトコル	文字コード	
1	XXX	申請者情報連携	申請の審査に関わる申請者の情報を取得	XXXシステム	受信	API（REST）	リアルタイム	HTTPS	UTF-8	XXX
2	XXX	申請結果一括連携	審査において承認された申請情報を提供	XXXシステム	送信	ファイル（CSVファイル形式）	日次	FTPS	UTF-8	XXX
3	…	…	…	…	…	…	…	…	…	…

3. 非機能要件定義

3.1. ユーザビリティ及びアクセシビリティに関する事項

(1) 情報システムの利用者の種類、特性

本システムの利用者の種類、特性について、下表に示す。

表 26 情報システムの利用者の種類、特性

項番	利用者区分	利用者の種類	利用イメージ	特性
1	利用者	利用者（マイナンバーカードの有効な署名用電子証明書を保有しており、スマートフォン用電子証明書の発行を希望する国民）	本システムで開発するスマートフォンのアプリケーションを用いて、スマートフォン用電子証明書の発行申請等を行う。	スマートフォンの操作に不慣れな利用者も想定されるため、分かりやすいユーザーインタフェースを考慮する必要がある
2	行政担当者	本システムの運用管理担当者	本システムの運用管理に当たり、必要に応じて本システムの操作を行う。	パソコンの操作について、事務作業等に係る一定の知識・スキルはあるが、情報システムの運用管理に関する専門的、技術的な知識・スキルは多くはないため、ユーザビリティ上留意する必要がある。
3	事業者	本システムと連携する行政・民間業務アプリのサービス提供者	本システムが提供する連携方法（アプリ間連携及びブラウザ連携を想定）を利用して、自組織が提供するアプリにおいて、公的個人認証サービスを利用する。（具体的な連携方法等は技術検証、検討会等で今後検討）	本システムを介して、自組織が提供しているアプリにおいて公的個人認証サービスを利用する。
4	…	…	…	…

(2) ユーザビリティ要件

「表 26 情報システムの利用者の種類、特性」に示す役割・業務内容に基づき、各利用者の特性を十分に留意する。また、利用者が想定する流れに沿った操作手順、画面遷移、画面レイアウト、帳票レイアウト等とする。

表 27 ユーザビリティ要件

項番	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成（直感・シンプル）	・ 利用者が何をすればよいか直感的に理解できるデザインにすること。 ・ 無駄な情報、デザイン、機能を排したシンプルでわかりやすい画面にすること。
2	画面の構成（フォント及び文字サイズ）	・ 十分な視認性のあるフォント及び文字サイズを使用すること。 ・ 画面サイズや位置を変更できること。 ・ 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成（マルチデバイス対応）	・ スマートフォン、タブレット端末により本サービスを利用する利用者を想定し、これら端末の特性を考慮した画面にすること。 ・ レスポンシブデザインにより、PC、タブレット端末、スマートフォン等の利用環境を問わず、同一の情報をグリッドレイアウト等の適切なレイアウトにより表示できるようにすること。
4	画面の構成（表示/非表示）	・ 情報の優先順位をつけ、重要度の低い情報、特定の利用者層に対して提示する情報は、利用者が必要に応じて表示/非表示を切替え可能とする等の工夫をすること。
5	画面の構成（クリックやチェックができる箇所）	・ 画面上でクリックやチェックができる箇所とできない箇所の区別を明確にすること。 ・ タップ操作が可能なタブレット端末やスマートフォンの場合は、タップ操作の結果（どの部分をタップしたのか）を適切にレスポンスできること。
6	画面遷移	・ 利用者が次の処理を想像しやすい画面遷移とすること。 ・ 無駄な画面遷移を排除し、シンプルな操作とすること。
7	画面表示・操作の一貫性（統一）	・ 機能、用語、レイアウト、操作方法は統一すること。
8	画面表示・操作の一貫性（視認性）	・ 必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること。 ・ 見やすさを考慮し、画面のフォントサイズを決定すること。 ・ 画面ごとに異なるフォントを使わないこと。
9	操作方法のわかりやす	・ 無駄な手順を省き、使いやすく、利用者が効率的に作業できるようにすること。

項番	ユーザビリティ分類	ユーザビリティ要件
	さ	・ 利用者が操作しやすい手順にするため、画面上の情報項目を上から下へ、左から右へ流れる順番に配置すること。 ・ 利用者の操作を軽減できるよう、画面の初期表示時、入力項目、選択項目等に適切な既定値を設定すること
10	操作方法のわかりやすさ（操作説明）	・ 原則としてマニュアルを参照しなくても操作できるようにすること。
11	操作方法のわかりやすさ（Tab キー）	・ Tab キー等による画面上のフォーカスの移動順序について、利用者が操作しやすい順序となるようにすること。
12	操作方法のわかりやすさ（画面遷移）	・ 利用者が同じ情報の入力や操作を何度も行う必要がないよう、画面が遷移しても情報がその後の手順に反映されるようにすること。 ・ 利用者の手間を軽減するため、利用者の手順に即した画面遷移に留意し、可能な限り不要な画面遷移を行わないようにすること。
13	操作方法のわかりやすさ（マルチデバイス対応）	・ スマートフォン、タブレット端末等の狭い表示領域、タッチインタフェースでも効率的に作業できる操作性を実現すること。
14	指示や状態のわかりやすさ	・ ユーザーインタフェース及び UX に関する一般的に使われているデザイントレンドを取り入れ、アイコン・図表のグラフィック表現を適切に適用すること。 ・ 本サービスが処理している内容や状況を、利用者が把握できるようにすること。
15	指示や状態のわかりやすさ（外部ドメインへの遷移）	・ ドメインを異にする他の Web サイトへの遷移を行う際は、離脱メッセージを表示する等、利用者が認識できるようにすること。
16	メッセージ出力	・ 利用者に分かりやすいメッセージとすること。 ・ 必要に応じて、登録・変更・削除等の操作を行う場合には、確認画面等で表示し、利用者の注意を促すこと。 ・ 処理時間がかかる操作では、処理中であることが分かるようにすること。
17	メッセージ出力（次の操作）	・ 指示メッセージは、次操作が具体的にイメージできるようなメッセージ出力を行うこと。
18	エラーの防止と処理	・ 利用者が操作や入力を間違えないデザインや案内を提供すること。
19	エラーの防止と処理（エラー防止）	・ 利用者の誤操作を想定し、入力チェック機能によりエラーを防止すること。 ・ 入力値が選択できる場合には、プルダウンメニュー等を活用し、極力キーボード入力操作をなくすこと。
20	エラーの防止と処理（エラーメッセージ）	・ エラーメッセージは、その内容が分かりやすく表示されるとともに、利用者が何をすればよいかを示すこと。
21	エラーの防止と処理（エラー表示と解決策）	・ 入力内容の形式に問題がある項目については、利用者がその都度該当項目を容易に見つけることができるようにすること。 ・ エラーが発生した時は、利用者が迷わずに問題解決できるよう、操作の続行に必要な選択肢を利用者が適切に理解できるようわかりやすく提示すること。 ・ 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにする。
22	エラーの防止と処理（確認画面）	・ 必要に応じて、登録、更新、削除等の処理の前に確認画面を用意し、利用者が行った操作や入力のやり直し、取り消しがその都度できるようにすること。 ・ 重要な処理については、事前に注意喚起し、利用者の確認を促すこと。
23	エラーの防止と処理（画面遷移）	・ 入出力の過誤があった場合、次の画面へ遷移しないこと。
24	エラーの防止と処理（情報保持）	・ タブレット端末等、屋外での使用を考慮し、電波受信状況の悪い場所においても操作不能とならないよう工夫すること。
25	ヘルプ	・ 利用者が必要とする際に、ヘルプ情報やマニュアル等を容易に参照できるようにする。 ・ ヘルプ情報やマニュアル等についても、利用者が必要な情報を容易に検索できるようにする。
26	既存のシステムとの統合	・ 本システムで開発するシステム（またはアプリ）は、既存の XXX システムと統合を行う。そのため、既存の XXX システム（もしくはアプリ）の UI/UX との統一感を意識したデザインとすること。 ・ 必要に応じて、既存の XXX システムに係る担当部局及び関連事業者からの要望対応の

項番	ユーザビリティ分類	ユーザビリティ要件
		検討、連携を行うこと。 ・ 技術検証の結果を反映して、統合後の機能構成を示すこと。
27	デザイナーによる UI/UX 検討	・ 本システムで開発するスマホアプリの UI/UX 検討に当たっては、利用者の利用動機に着目し、サービスデザイン思考の観点から検討を行うこと。 ・ UI/UX 検討に当たっては、民間スマホアプリ等の経験を有する専門の UI/UX デザイナーを体制に組み入れること。
28	画面遷移、操作ログ等の分析	・ 運用・保守工程において継続的に UI/UX の改善を検討できるよう、利用者の画面遷移、操作ログ等を分析できる仕組みを整備すること。
29	言語対応	・ 本情報システムでは、日本語のほか、XXX 語で記述されたコンテンツに対応すること

(3) アクセシビリティ要件

アクセシビリティに関する要件を下表に示す。

表 28 アクセシビリティ要件

項番	アクセシビリティ分類	アクセシビリティ要件
1	基準等への準拠	・ 広く国民に利用され公益性の高い情報システムであるため、日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用モデル」（総務省）に準拠し、以下を前提とすること。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html ・ JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－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：Web コンテンツ」の適合レベル AA に準拠することを目標とする。また、レベル AAA のうち、以下の達成基準についても可能な範囲で適用すること。 ➢ 2.1.3 キーボード（例外なし）の達成基準 ➢ 2.3.2 3 回のせん（閃）光の達成基準 ➢ 2.4.8 現在位置の達成基準 ➢ 3.2.5 要求による状況の変化の達成基準 ・ 注記：本仕様書における「準拠」という表記は、情報通信アクセス協議会 Web アクセシビリティ基盤委員会「Web コンテンツの JIS X 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 ・ また、スマートフォン等での操作を行うユーザーが増えていることを踏まえ「Web Content Accessibility Guidelines （WCAG） 2.1」で追加された達成基準についても、可能な範囲で適用すること。 ➢ 1.3.4 表示の向き（レベル AA） ➢ 2.5.1 ポインタのジェスチャ（レベル A） ➢ 2.5.2 ポインタのキャンセル（レベル A） ➢ 2.5.4 動きによる起動（レベル A） ➢ 4.1.3 ステータスメッセージ（レベル AA） ・ デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
2	指示や状態の分かりやすさ	・ 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。ただし、業務の利用用途から、画面色での振り分けを行うことを予定していることから、適用範囲及び配色については主管課及び関係省庁と協議し、決定すること。 ・ Web ブラウザ等の音声読み上げ機能を活用し、視覚障がいの方でも問題なく利用可能な UI とすること。
3	マルチデバイス対応	・ 解像度の低い機種、画面サイズの小さい機種でも、業務継続が可能な UI とすること。 ・ OS の設定でフォントサイズ・表示サイズをそれぞれ最大とした場合でも、業務継続が可能な UI とすること。 ・ スタイルシートを利用しないユーザーと利用するユーザーにおいて得られる情報に差

		（表示されない文字や画像がある等）がないこと。レイアウトにおいても大きな差がないことが望ましい。

3.2. システム方式に関する事項

(1) システム方式についての全体方針

システム方式についての全体方針を下表に示す。本システムはクラウドネイティブの構成として、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（以下、「クラウド方針」という。）」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。

使用する IaaS/PaaS はガバメントクラウドを原則とし、SaaS についても積極的に活用すること。

表 29 システム方式についての全体方針

項番	観点	全体方針
1	システムアーキテクチャ	・本システムのシステムアーキテクチャはクラウドサービス上に用意される Web アプリケーションから構成される。Web アプリケーションは利用者の端末に追加的なソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとする。 ・本システムや業務機能等の特性を十分に検討し、クラウドサービスプロバイダが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、システムを構築する。 ・クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションプログラムの作り込みを削減できる設計とする。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 ・クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を行い、安全かつ効率的にシステムを構築する。 ・予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。管理者アカウントについては、多要素認証を必須とすること。多要素認証はハードウェア方式を原則とするが、ソフトウェア方式も許容する。ハードウェア方式の場合は対応するワンタイムパスワード用のデバイスを利用システム側で調達すること。 ・リソース使用量の変動等に柔軟に対応するとともに、コスト削減を図るため、民間クラウドサービスの利用を原則とする。 ・全体構成及び利用するクラウドサービスについては、受託者において移行、引き継ぎ、確実なサービス提供等について問題が生じないことをクラウドサービスプロバイダに応札前に確認し、本調達の要件を踏まえ、確認結果と合わせて適切なものを提案する。
2	アプリケーションプログラムの設計方針	・マイクロサービスアーキテクチャ、API、クラウドネイティブ、クラウドサービスのマネージドサービスのみによる構成等、モダン技術を前提として構築する。 ・クライアントサーバ方式、専用端末のシンクライアント（VDI）等の旧来技術は、高コスト化の要因となるため採用しないこと。 ・原則としてバッチ処理を採用せず、リアルタイム処理を基本とすること。バッチ処理が必要となる場合は、その理由について主管課の承認を得た上で採用すること。 ・情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする。

		・システムが取り扱うデータの保管・管理に際して、データの容量、更新頻度、保存期間等を考慮し最適なストレージサービスを選定の上、利用する。またデータの保管・管理方針が変更となった際に、ストレージサービス間でのデータの移行が容易となるよう設計上考慮する。
3	ソフトウェア製品の活用方針	・SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 ・ソフトウェア製品については、広く市場に流通し、利用実績を十分に有するものを活用する。広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 ・アプリケーションプログラムの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認しなければならない。 ・ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討する。

(2) クラウドサービスの選定、利用に関する要件

ア　セキュリティ確保のため、本システムで用いるクラウドサービスは、原則として ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録されているクラウドサービスを選定すること。なお、例外的に ISMAP クラウドサービスリスト、または ISMAP-LIU クラウドサービスリストに登録されていないクラウドサービスを選定する場合は、受託者の責任において、当該クラウドサービスが「ISMAP 管理基準」の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）と同等以上のセキュリティ水準を確保していることものを選定すること。

イ　要機密情報を取り扱うクラウドサービスの選定、利用に関しては、「政府機関等のサイバーセキュリティ対策のための統一基準　（令和 5 年度版）」の「4.2.1　クラウドサービスの選定（要機密情報を取り扱う場合）」「4.2.2　クラウドサービスの利用（要機密情報を取り扱う場合）」の内容を遵守すること。

ウ　情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。

エ　契約の解釈が日本法に基づくものであること。

オ　クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

カ　主管課の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。

キ　障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。

ク　情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、主管課が要求する任意の時点で情報資産を他の環境に移管させることができること。

ケ　SaaS サービスの選定に関する参考事項

- SaaS ベースで構築することを前提に検討し、SaaS では要件を満たさない場足は、PaaS、IaaS などを選択すること。なお、本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。
- 今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。

コ　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。

サ　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

シ　クラウドサービスに係るアクセスログ等の証跡を保存し、主管課からの要求があった場合は提供すること。

ス　インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線とクラウド基盤との接続点の通信を監視すること。

セ　クラウドサービスの提供に関する次のいずれかの認証を取得していること。

- ISO/IEC 27017:2015
- CS マーク（特定非営利活動法人日本セキュリティ監査協会（JASA）のクラウドセキュリティ推進協議会が定めるもの）

(3) 開発方式

ア　開発に当たっては、継続的インテグレーション・継続的デリバリー（以下、「CI/CD」という。）を可能とし、必要な要素（開発環境、検証環境等）一式を用意すること。

イ　統合開発環境（エディタ、コンパイラ、デバッガなどプログラミング支援機能を含む）等は、受託者が用意すること。また、リポジトリ管理・プロジェクト管理の効率化やソースコード品質向上を目的としたプロジェクト関係者間のコラボレーション促進機能等の提案も許容する。

ウ　これらの開発環境については運用・保守事業者に引き継ぐことを想定し、可能な限りクラウド提供の CI/CD パイプラインもしくはマネージドサービス等と連携してクラウド環境に構築すること。なお、開発ツール等の組合せで実現した場合には、運用・保守事業者が該当ライセンス等を用意した上でそれらを引き継ぐことが可能であること。

エ　UI 設計は UI 設計専用のアプリケーションを利用し随時共有すること。

オ　API 設計には Open API 設計用のツールを利用すること。

(4) 機器等の設置方針

本システムはクラウドサービスを前提としているため、設置場所についてはクラウドサービスプロバイダの提供す

る場所となるが、その際は日本国内のリージョンを選択すること。

(5) その他

システム方式に係るその他の要件を以下に示す。

ア 「2.1 機能に関する事項 （2） 技術検証」の結果を踏まえ、本システムを設計・開発すること。なお、技術検証の結果については、本調達時点の検討状況を閲覧資料として提供する予定である。

イ 本システムは短期間での機能追加・改善を行うことが想定されており、できるだけ簡潔なアーキテクトかつ簡易な構成とすること。なお、IaaS/PaaS については単一クラウドサービスでの構築を想定している。

3.3. システム規模に関する事項

本サービスの規模要件を以下に示す。また、本サービスの規模に関する業務要件は、「1.2 業務の規模」を参照のこと。

(1) 規模に関する前提条件

本システムはクラウドサービスを利用して運用されるため、以下の取り組みを行うこと。

ア 運用期間中において利用予定範囲を超過することがないよう、システムの縮退を検討するために必要となる情報収集等の仕組み（クラウドサービスの課金状況やリソースの利用量の監視、一定の閾値を超えた場合のアラート処理等）を設けること。定量的に計測したデータについては、ダッシュボード等による状況の可視化を行うこと。また、リソース利用状況に基づいたリソース見直しを行う点に留意し、情報収集の仕組みについても修正可能とすること。

イ クラウドサービスのマネージドサービスを効果的に活用し、コスト削減を継続的に図ること。原則としてサーバレスの構成を取ることとするが、インスタンスを利用してサーバを立てる場合は、サーバのスペック等を適切な範囲に調整してコスト削減を継続的に図ること。（オートスケールを利用する場合の変更条件・上下限値等を含む。）

ウ リソース確保の方式（リザーブドインスタンス、スポットインスタンス等）についても検討すること。

(2) データ量

本システムで想定されるデータ量を下表に示す。なお、年間データ増加量は仮定をおいた上での試算結果を記載しているため、設計等を考慮の上、必要なデータ量のサイジングを行うこと。

表 30 データ量

項番	項目	データ種類	データ量	年間データ増加率（%）	補足
1	XXX 業務データ	データベース	XXX	5%	XXX
2	添付書類	画像	XXX	3%	XXX
3	操作ログ	テキスト	XXX	1%	XXX
4	…	…	…	…	…

(3) 処理件数

本システムで想定される処理件数を下表に示す。なお、本システムの運用期間を踏まえ予想される増加率（年間で 5%～10%程度の増加率）を考慮する必要がある点について留意すること。

表 31 処理件数

項番	項目	処理件数	補足
1	業務処理件数（ピーク時）	300（件／分）	4 月 1 日から 4 月 5 日頃まで、XXX 業務を実施するために業務処理が集中する
2	業務処理件数（通常時）	120（件／分）	XXX
3	…	…	…

(4) 利用者数

本システムで想定される利用者数を下表に示す。

表 32 利用者数

項番	利用者区分	利用者数	補足
1	想定利用者（アクティブユーザー）	500,000（人）	XXX
2	…	…	…

本システムの想定利用者数及び「3.4 性能に関する事項」で求める性能目標を考慮の上、必要スペックのサイジングを行うこと。

【日本全国民が利用者の対象となる場合】

本機能の対象とする利用者は、個人番号を付番された利用を希望する者が対象となるが、現時点では、「住民基本台帳に基づく人口、人口動態及び世帯数（令和 5 年 1 月 1 日現在）」により、利用者数を日本人及び常住の外国人を含めた最大約 1 億 3 千万人と想定する。なお、本機能としての利用者数の最大値は基本設計の段階で、業務要件や業務量、マイナンバーカードの交付状況等を踏まえ決定し、主管課の承認を得ること。また、利用者及び業務量については、現状以下の条件も想定している。

ア 本機能はマイナンバーカードを保有するほとんどの者が利用すると想定する。

イ 利用者は年 1 回、還付申告等の手続において利用するものと想定する。利用者数は、マイナンバーカードの交付枚数等の状況により、大きく変動することが想定されるため、設計に当たっては、柔軟性のある設計とすることが求められる。

(5) 保管データ量・保管期間

本サービスに保管するデータ量やデータの保管期間については、要件の整理の中で調査を行い、主管課と協議の上、決定すること。

3.4. 性能に関する事項

本サービスの性能要件を以下に示す。下記の性能要件を踏まえて、本サービスの業務処理の特徴を考慮し、業務処理のピーク時においてもレスポンスの低下等を招かないように、十分な処理性能を確保すること。

(1) 性能を考慮する対象

以下のサブシステム・機能についての性能要件を満たすことを、本システムの性能要件とする。

・ XXX サブシステム
・ XXX サブシステム
・ データセット提供、コミュニケーション、メタデータ管理、コミュニケーション管理に関連する機能

ア 性能目標の設定対象

性能目標の設定対象は本システムの Web サーバにリクエストが到着した時点からレスポンスを返す時点までとする。ブラウザ、ネットワーク部分での処理時間に関しては、性能目標の設定対象外とする。

イ 性能見積もり

本サービスのアプリケーション処理時間に係る性能見積りは、以下を考慮する。

・ アプリケーション又はコードの起動に要する時間、アプリケーション又はコードの実行時間、データベースアクセスに要する時間に要素分解を行った上で実施すること。
・ 各画面・機能等の利用者体験を踏まえた余裕を見込むこと。

(2) 応答時間

目標時間を満たすトランザクションの割合を「遵守率」とし、その目標値を設定すること。ピーク時の遵守率は80%とする（80%以上のトランザクションがレスポンスタイム処理目標時間を満足する性能であること。なお、障害等による縮退運転時並びにネットワーク遅延等の受託者の責によらない遅延は除外する。）

レスポンスタイムは、画面を表示するための要求を行った時（ボタン等を押下した時）から画面が全て表示されるまでの時間を指す。

表 33 目標レスポンスタイム

項番	指標名	目標値	補足
1	参照系処理	3 秒	画面の読み込み、情報の表示に関する処理
2	更新系処理	5 秒	情報の登録、更新、削除に関する処理
…	…	…	…

【新規システムの場合】

本処理の目標値は、XXX の実績に基づき、「3.3 システム規模に関する事項」にて予想される最大負荷に対して 50%の余裕を考慮して算定したものである。処理の目標値は、連携するシステムやデータベース等の状況に影響を受けることを踏まえ、必要に応じて目標値の見直しを主管課へ提案すること。

(3) スループット

本システムにおいて、令和 XX 年度に処理件数がピークとなった日の処理件数を下表に示す。設計に当たっては業務処理件数の実績値及び想定値を踏まえ、さらに安全率を加味し、主管課の承認を得ること。

表 34 処理件数（実績）

項番	対象業務	対象サーバ	ピーク日（令和 XX 年度）	処理件数（件/日）
1	XXX 業務	内部 Web サーバ	令和 XX 年 XX 月 XX 日	XXX
		外部 Web サーバ	令和 XX 年 XX 月 XX 日	XXX
2	XXX 業務	内部 Web サーバ	令和 XX 年 XX 月 XX 日	XXX
		外部 Web サーバ	令和 XX 年 XX 月 XX 日	XXX
3	…	…	…	…

上記は XXX システムにおける Web サーバのアクセスログ情報より、各業務に対応するシステム機能のアクセス件数を日単位で集計し、ピーク日の処理件数を算定している。

3.5. 信頼性に関する事項

本サービスに備える機能の停止等による業務への影響を最低限にとどめるため、クラウドサービスの利用を前提として、以下に示す要件を踏まえ本サービスの信頼性を確保すること。

(1) 可用性要件

単一障害点（SPOF）を極力排除するとともに、サーキットブレーカーパターンなども検討し、一律ではなく機能又はセグメントの特性に応じた合理的な提案を示すこと。また、SPOF の発生が避けられない場合においてそれら稼働状況を管理する仕組みを準備すること。

ア　可用性に係る目標値

可用性に係る目標値を下表に示す。

表 35 可用性に係る目標値

項番	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ・ 接続回線の計画停止時間 ・ 大規模災害等の天災地変に起因する停止時間 ・ 連携するサービス又はクラウドサービスまたはスマートフォン端末の通信キャリアの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・ 本サービスのメンテナンスによる計画停止時間
2	稼働率	99.9%以上	本サービスにおける稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x 100 当該計算式において、年間実稼働時間は「利用者がサービスを利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。
3	…	…	…

イ　可用性に係る対策

本サービスの可用性を確保し、前述に示した稼働率を遵守するため、以下に示す要件に基づく対策を行うこと。

- クラウドサービスの利用を前提として、本サービスを構成するサーバ、ネットワーク機器及びネットワーク経路を冗長化し、単一障害点（SPOF）を回避すること。
- クラウドサービスの利用を前提として、フェールソフトの観点から、障害が発生したコンポーネントを切り離すことによりサービス全体を停止せずに運用可能とすることを考慮する。そのために各種障害発生時の影響を回避又は局所化し、原則として自動縮退運用に対応すること。
- 本サービスに係る運用・保守上の人的ミスに起因する障害が本サービスの可用性に影響を与える事態を未然に防止するため、「3.16 運用に関する事項」及び「3.17 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

(2) 完全性要件

以下に示す要件を踏まえ、本サービスの完全性を確保するための対策を行うこと。

ア　クラウドサービスの利用を前提とし、以下の対策を講ずること。

- コンポーネントの故障に起因するデータの減失や改変を防止する。
- 異常な入力や処理を検出しデータの減失や改変を防止する。

イ　システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。ログの出力に当たっては、システム稼働環境（本番環境、検証環境等）別に出力するログのレベル（ERROR、WARNING、INFO、DEBUG 等）の設定を可能とすること。
なお、ログの保管期間は 1 年間とする。

3.6. 拡張性に関する事項

(1) 性能及び機能の拡張性

ア　基本方針
本システムの利用率の増加、データ量の増加等により、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正等により機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

イ　マネージドサービスなどの活用
本サービスはクラウドサービスを利用する想定としている。本サービスの構築に当たっては、当該クラウドサービスをマネージドサービスなど可能な限り活用することにより、処理能力等の動的調整を実現することとし、業務量及び処理能力の拡張性については特段の拡張性要件を定義しない。

ウ　機能の追加
機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。
本サービスは、連携業務アプリケーションとの一層の連携など、拡張性を備えたシステム・サービスであることが求められる。連携機能等の拡張が必要になった際に拡張が容易となるような構成をとること。

エ　コンポーネントの再利用性・拡張性
アプリケーションやインフラの設計に当たっては、将来の拡張時に効率良く対応ができるように、設定情報の外部化や一元化、機能の共通化等に努めること。特にスマホアプリについては、様々な利用者が広く利用することが想定されるため、特定のスマートフォン端末、OS のバージョン、ミドルウェア等に可能な限り依存しない設計とすること。

オ　モニタリングと定期的な報告
本システムの運用に当たっては、定期的な運用報告において定期的にサーバコア数やディスク、メモリ、ネットワークの帯域などの使用状況等を確認すること。またリソースの増加の必要性が見込まれる場合は、リソースの増強の必要性の有無を判断できるような形で主管課に報告を行うこと。

カ　割り当て変更
業務量の増加減に伴い、これらリソースの割り当てを動的に行えるようにし、主管課の指示に基づきリソースの割り当てを変更すること。

3.7. 上位互換性に関する事項

(1) 上位互換性

クラウドサービスの活用を踏まえ、OS、サーバソフトウェアのバージョンアップ又は変更に備え、本サービスを構成する。

ア　クラウドサービスのバージョンアップ
　システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

イ　OS 等への依存
　原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェア等の特定バージョンに依存する場合は、その利用を最低限とすること。

ウ　クライアント端末の更新
　クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

(2) 業務分担
　本システムを構成する機器・ソフトウェアの更新、バージョンアップの必要性が生じた場合は、各事業者がそれぞれの担当範囲において影響調査、対応策の検討を実施することとしている。

ア　アプリケーション保守事業者は、業務アプリケーションへの影響調査、対応策の検討を実施する。

イ　運用事業者は、システム基盤の影響調査、対応策の検討を実施する。

ウ　機器・ソフトウェアの更新、バージョンアップの対象が持ち込みソフトウェアの場合は、運用事業者が実施する影響調査、対応策の検討を機器・ソフトウェア賃貸借・保守事業者が支援する。

3.8. 中立性に関する事項

(1) オープンな標準的技術又は製品の採用
　本サービスを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準サービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。

ア　データの可搬性の担保
　データの可搬性の担保に当たっては、以下の要件を満たすこと。
- 情報システム内のデータについては、原則として XML や CSV 等の標準的な形式で取り出すことができるものとすること。
- パッケージ製品から抽出されたデータであっても、移行データフォーマットや移行データの権利は主管課に所属すること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）を文書化すること。文書については、情報システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当文書の内容に変更が生じる場合は継続して

改定を行い最新化できること。

・ 移行データに関する文字コード等は以下に従うこと。

- 取り扱う日本語文字集合の範囲： JIS X 0213
- 文字コード： ISO/IEC 10646
- 文字の符号化形式： UTF-8

イ オープンソースソフトウェア（OSS）活用

ソフトウェア又はアプリケーションについてフレームワークを活用する場合は、可能な限りオープンソースソフトウェアとして提供されているフレームワークを選定すること。

ウ オープンなインタフェースの活用

本サービスを構成するサーバ、ソフトウェア等は、原則として仕様が公開された API 等のインタフェースを選定すること。

3.9. 継続性に関する事項

本サービスの停止等に際しても必要最低限の業務を継続（又は回復）するため、以下に示す要件を踏まえ、本サービスの継続性を確保すること。

(1) 継続性に係る目標値

以下に、機能停止等の原因となる事象の規模に応じて継続性に係る目標値を示す。なお、連携する XXX サービスの障害・計画停止時は、本サービスの継続も困難になることから、XXX 関連業務も停止する。この場合は、連携する XXX サービスの復旧後、XXX 関連業務も速やかに復旧を行うこととする。

ア 予測可能な障害発生時

予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。また、単一障害発生時は業務停止せずに処理継続可能であること。

イ 業務停止を伴う障害発生時

予測困難な事象により業務停止を伴う障害が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を下表に示す。

表 36 継続性に係る目標値（業務停止を伴う障害発生時）

項番	設定対象	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	XXX サービス	2 時間以内	通常どおりのサービスレベルに復旧	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）
2	…	…	…	…

ウ 大規模災害発生時

インターネット等通信インフラが被災しておらず、発災前と同様の通信環境が確保されていることを前提として、大規模災害による業務停止が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を下表に示す。

表 37 継続性に係る目標値（大規模災害発生時）

項番	設定	目標復旧時間	目標復旧レベル（RLO）	目標復旧時点（RPO）

	対象	（RTO）		
1	XXX サービス	3 日以内	通常どおりのサービスレベルに復旧（機能面は通常レベル、性能面では通常の半分のレベルの復旧とする）	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）
2	…	…	…	…

(2) 継続性に係る対策

本システムの継続性要件を実現するために、以下の対策を講じること。

ア　冗長化

各構成要素について、故障等を検知した際、クラウドサービスの利用を前提として自動的に予備の環境へ切替える等、適切に冗長化を行い、特定の部分の障害によりシステム全体が停止してしまうようなSPOF（単一障害点）を極力排除するよう、設計時に配慮すること。

イ　災害対策

災害対策環境の事前準備等によるシステム上の対策及び非常時の運用体制や切替え手順の整備等による運用上の対策を行うことで、業務継続を可能とすること。

災害発生後に本番環境が正常に稼働できる場合は、災害対策環境から切り戻しができるよう連携先システムと調整しておくこと。

ウ　アベイラビリティゾーン

アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とする。しかし頻繁に AZ 間の通信が発生するアプリケーションについては、AZ 間のレイテンシが増幅し性能に影響を与える可能性がある。これらの性能面の影響を評価できるよう、設計・開発期間中の早い段階で性能面の影響を評価し、必要に応じてアプリケーション改修等の手段で性能改善への対応方針を確立すること。

エ　データバックアップ

・　バックアップ対象

データバックアップに当たっては、本サービスの稼働に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグ等に起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

・　バックアップ頻度

バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR：Point In Time Recovery/Restore を保存する等の対応を行うこと。

・　保存期間

万一の障害発生に備え本サービスの稼働に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

・　アクセス権限

バックアップしたデータの保管場所にはアクセス権限を付与し、管理者以外がアクセスできないようにすること。

・ データの隔地保管

「3-2-1 ルール」（2012 年に米国土安全保障省サイバーセキュリティ・インフラストラクチャー・セキュリティ庁の US-CERT が提唱）に示されている「データはコピーして 3 つ保有（プライマリー1 つ、バックアップ 2 つ）、2 種類の異なる記録媒体に保管、コピーのうち 1 つは遠隔地に保存」という方針を十分に理解した上で、データのバックアップについて万全を期した対応を行うこと。クラウドサービス上のスナップショットやレプリカだけではこの要件に十分対応できないので、バックアップとして永久増分と重複排除を積極的に活用し、ISMAP 管理基準が求める暗号化を行った上で、別リージョンのオフサイトに隔地保管すること。

・ バックアップツール

バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスをできるだけ利用すること。なお、個別データの復旧にはデータベース等の PITR：Point In Time Recovery/Restore を実現できることが望ましい。

オ システムバックアップ

クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。なお、インスタンスを利用してサーバを立てる場合のバックアップ方式は、バックアップ＆リストア、コールドスタンバイ、ウォームスタンバイ、マルチサイトの 4 つのディザスタリカバリ方式のうち、目標復旧時間から考えて、コールドスタンバイ以上の構成を想定している。

「表 36 継続性に係る目標値（業務停止を伴う障害発生時）」及び「表 37 継続性に係る目標値（大規模災害発生時）」に示す RTO、RLO、RPO を満たすようにすること。

カ システム障害時の業務継続

システム障害時も一部業務は継続出来るよう対策を検討すること。

【継続すべき業務（例）】

参照業務

入力業務

【対策（例）】

データベースのバックアップを別環境に保存し、クライアント PC 等から参照、ダウンロード等が出来るようにする。

入力作業を、Excel 等のファイルに入力、システム復旧後にファイルをインポートすることで、一括入力を可能とする。

3.10. 情報セキュリティに関する事項

(1) セキュリティ対応方針

セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を下表に示す。

表 38 当該システムにおけるセキュリティ対応方針

項番	分類	概要
1	原則	・ 「政府機関等のサイバーセキュリティ対策のための統一基準」、「農林水産省における情報セキュリティの確保に関する規則」に準拠した情報セキュリティ対策を講ずること。なお、「農林水産省における情報セキュリティの確保に関する規則」は非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準」に準拠しているので、必要に応じ参照すること。「農林水産省における情報セキュリティの確保に関する規則」の開示については、契約締結後、受託者が農林水産省に守秘義務の誓約書を提出した際に開示する。 ・ セキュリティ対策については、高度化/大規模化するサイバー攻撃等に対応するため、多層防御やサイバーレジリエンス強化といった原則に基づいて要件を定義する。
2	システム特性（概要）	【システムの利用者】 ・ 当該システムは国民向けサービスであり、一日に XXX 人程度の利用者が想定される 【システムで取り扱う情報】 ・ 個人情報は取り扱われ、利用者の収入に関わる要配慮情報に相当する情報も取扱われる ・ 特定個人情報は取扱われない 【使用環境・ネットワーク構成】 ・ 利用者はブラウザ、スマホアプリからンターネットを介して当該 web システムにアクセスし、ログインして各種機能を使用する ・ システム管理者はインターネット VPN を介して当該システムにアクセスし、システム管理を実施する ・ 外部システムとの接続はなし 【その他】 ・ 当該サービスは国民の XXX 申請に関わるシステムであり、システム停止により国民の XXX 申請が受付けられなくなり、甚大な影響が発生することから可用性に関しても機密性、完全性と同等に高いレベルで担保する必要がある
3	優先的に対処すべきセキュリティリスク	【優先的に対処すべきセキュリティリスク】 ・ 外部からの不正アクセスにより、システムの個人情報が漏洩する。 ・ サービス妨害を目的とした攻撃等によりシステムが長時間停止する。
4	セキュリティ対応方針	【セキュリティ要件のベースライン】 ・ 本システムにおいては、セキュリティ要件を過不足なく導出するため、NISC の提供する SBD マニュアルをセキュリティベースラインとして利用する 【優先的に対処すべきセキュリティリスクへの対応方針】 ・ 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 ・ 外部からの不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 ・ サービス妨害を目的とした攻撃対策については、L3～L7 層で対策可能な仕組みを導入する。 【その他セキュリティリスクへの対応方針】 ・ ・上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

(2) セキュリティ要件

上記のセキュリティ対応方針に基づき、「別紙 情報セキュリティに関する事項」に当該システムにおけるセキュリティ要件を記載する。

受諾者は、開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。

開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみ

に縛られず、必要に応じて追加のセキュリティ対策を講じること。また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（政府情報システムにおける セキュリティ・バイ・デザインガイドライン（digital.go.jp）） 」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考にシステムの脆弱性が作りこまれないように留意すること。

3.11. 情報システム稼働環境に関する事項

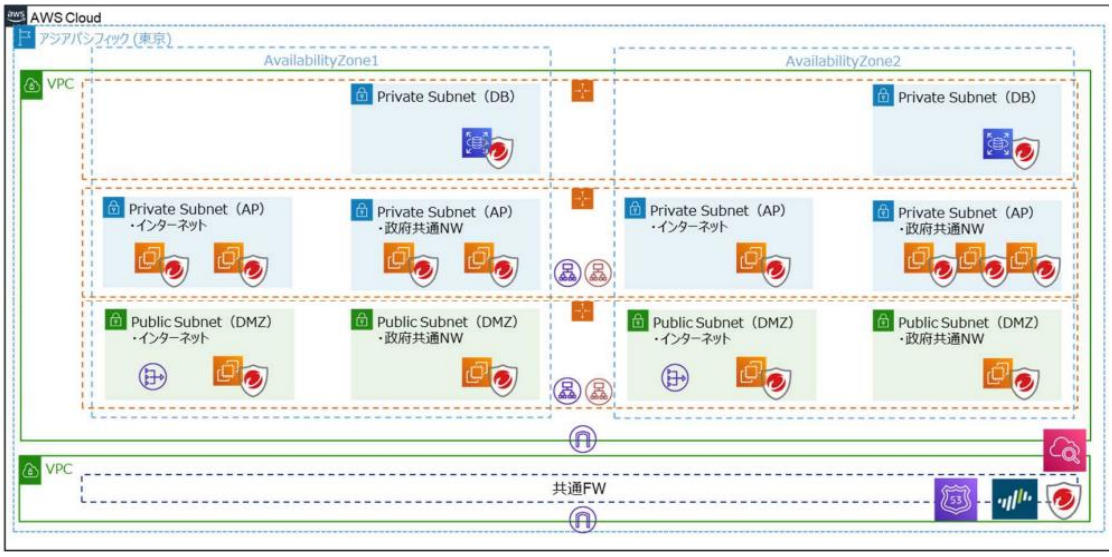
クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。

(1) システム構成

ア 本番環境

現段階で想定する本サービス本番環境の構成図を下図に示す。

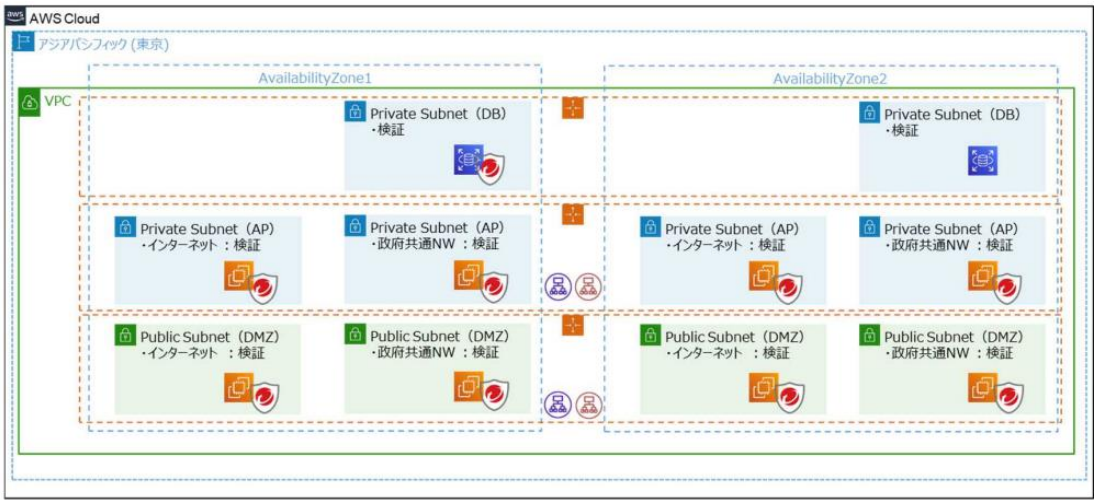
図 10 本番環境システム構成（想定）



イ 検証環境

現段階で想定する本サービス検証環境の構成図を下図に示す。原則として本番環境同様とするが、検証用途に最低限必要な要素を踏まえ、縮退した構成とし、性能、信頼性については本番環境と同等にする必要はない。

図 11 検証環境システム構成（想定）



(2) クラウドサービス構成

ア クラウドサービスの要件

クラウドサービスの要件については、「3.2.システム方式に関する事項」の「(1)システム方式についての全体方針」、「(2)クラウドサービスの選定、利用に関する要件」を参照すること。

イ クラウドサービス構成

本システムのクラウドサービス構成を下表に示す。なお、速やかに本番同等の環境を構築できるように、インフラの設定は Infrastructure as Code にて構成し、環境変更時にはその変更をメンテナンスできるようにすること。

表 39 クラウドサービス構成

項番	クラウドサービス	補足
1	Amazon EC2	コンピューティングプラットフォーム
2	Elastic Load Balancing	負荷分散装置
3	…	…

(3) ハードウェア構成

クラウドサービス外に準備するハードウェアを下表に示す。なお、特定の装置への依存により、将来的なシステムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。

表 40 ハードウェア構成

項番	ハードウェア分類	ハードウェア名	ハードウェア要件	補足
1	コンピュータ本体：サーバ機器	連携サーバ	XXX	XXX
2	記憶装置:ストレージ・ＮＡＳ等	XXX	データ量：XXX ディスクの回転数：XXX	XXX
3	ネットワーク機器:ＨＵＢ・ルータ・スイッチ等	XXX	XXX	XXX

4	…	…	…	…

ア　検証環境のサーバについては、業務で利用しない場合はサーバを停止する運用を実施し、コスト適正化を図ること。

イ　災害対策の方針として、 異なるリージョンにシステム及びデータベースのバックアップを実施しておき、災害発災時にはそのバックアップから本番同等の環境を構築できること。

(4) ソフトウェア構成

本サービスの構築に当たっては、可能な限りクラウドサービス提供のサービスを活用すること。また、いずれのソフトウェアについても、原則として最新バージョンを適用する。クラウドサービス外に準備するソフトウェアを下表に示す。

表 41 ソフトウェア一覧

項番	ソフトウェア分類	ソフトウェア名	ソフトウェア要件	補足
1	ＯＳ：連携サーバ用	連携ソフトウェア	機能：XXX バージョン：XXX 必要ライセンス数：XXX 保有済のライセンス内容：XXX	XXX
2	ＯＳ：クライアント用	アプリケーションサーバソフトウェア	XXX	XXX
3	…	…	…	…

ソフトウェアの持ち込みが必要な場合においては、特定のソフトウェアへの依存により将来的なシステムの拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。

(5) ネットワーク構成

ネットワーク構成は「（1）システム構成」を参照すること。

【ネットワーク構成を設計・開発時に決定する場合】

本システムのネットワーク構成については本システムの設計・開発時に決定する。以下の点に留意すること。

ア　連携先システムとのネットワークについては、閉域網（専用線、広域イーサネット、IP-VPN 等）で接続し、外部からの侵入を物理的に防ぐこと。

イ　敷設する回線で本システムに固有のグローバル IP を要する場合、適切なグローバル IP アドレス数を同時に用意すること。

ウ　クラウド上に論理的に隔離された仮想閉域ネットワークを構築すること。

表 42 ネットワーク構成

項番	回線種別	ネットワーク要件	補足
1	高速デジタル専用線	・ ネットワーク帯域：XXX ・ 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：XXX	XXX
2	広域イーサネット網	XXX	XXX
3	パケット通信網	XXX	XXX

4	…	…	…

(6) 施設・設備要件

本システムの施設・設備要件を下表に示す。

表 43 施設・設備要件

項番	施設名	施設形態	施設・設備要件	補足
1	XXX 施設	国有施設	・制震／耐震／免震：有/無 ・非常用電源：有/無 ・非常用電源の稼働時間：XXX ・ラック数：XXX ・使用可能な電源の容量：XXX ・位相及び系統：XXX ・許容する発熱量：XXX ・耐荷重：XXX	XXX
2	…	…	…	…

(7) 利用端末の要件

本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS・ブラウザの考え方について、以下に示す。

ア 本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS の機種やバージョンを下表に示す。

表 44 動作保証対象とする利用端末

項番	端末	OS	バージョン
1	PC	Windows	10/11
2	…	…	…

イ 本システムの運用開始時点で動作保証の対象とするブラウザは以下とする。

- PC（Mac OS/Windows） の場合：Microsoft Edge/Mozilla Firefox/Google Chrome/Safari の最新バージョン
- Android の場合：Google Chrome の最新バージョン
- iOS の場合：Safari の最新バージョン

3.12. テストに関する事項

本システムのテストに関する要件を下表に示す。なお、品質管理の観点から必要に応じて主管課が指定する専門チームがテストに参加することもあるため、受け入れること。また、テストデータやテストに関連する情報の提供にも協力すること。

表 45 テスト要件

項番	分類	要件
1	テスト工程の定義	・ 本システムでは調達仕様書に記載の通り、以下のテストを実施する。 (1) 単体テスト (2) 結合テスト

		(3) 総合テスト (4) 受入テスト
2	テスト環境	・ 本番環境に加え、テストを実施するための環境（開発環境・検証環境等）を整備すること。 ・ テスト環境については、連携先機関と接続して行う外部連動テストが実施可能な環境として整備するほか、同時並行的な開発に対応できるように複数のテスト環境を整備すること。 ・ 開発スケジュールを踏まえ、効率化を考え、各環境を流用するなど検討すること。
3	テスト 計画書	・ 各テスト工程の開始時に、以下の内容を定義したテスト計画書を作成し、主管課の承認を得ること。 ➢ テスト体制 ➢ テスト環境 ➢ 作業内容 ➢ 作業スケジュール ➢ テストシナリオの概要 ➢ テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等） ➢ 合否判定基準 ・ 受託者は、本業務を実施する各過程においてテスト計画書の内容に変更が生じる場合、変更箇所及び内容について主管課の承認を得ることを条件として、テスト計画書を適切に更新すること。 ・ 情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。 ・ 受託者は、テストに係る管理要領を共通化し、各テスト工程において、原則として同一の管理要領を適用するようにすること。各テスト工程に応じて部分的に異なる管理要領の適用を必要とする場合は、その適用差分のみ「テスト計画書」に記載すること。 ・ 機能一覧を基準として欠陥の相対的な発生確率と欠陥顕在化時の相対的な影響度について、それぞれ高・中・低の 3 段階で評価することにより、本サービスの品質リスクを分析し、その結果を踏まえてテストケースの数や質に変化をつけるリスク・ベース・テストを適用すること。
4	テスト 仕様書	・ 本システムの各テスト工程の開始前に、テストシナリオ、テスト項目等を記載したテスト仕様書を作成すること。 ・ 各テスト工程のテスト項目は、設計書等の記述内容を網羅的に確認できるよう作成すること。 ・ 各テスト工程に応じたテスト技法を適用すること。 ・ テスト項目は、品質を確保するために十分なテスト項目を定義すること。また、テスト計画の策定時に定めた定性・定量評価方法を満たすよう作成すること。 ・ 受託者においてレビューを徹底し、上記要件を満たしたテスト仕様書となっているかを確認すること。
5	テストの実施	・ 作成したテスト項目に基づきテストを実施すること。 ・ テストを実施する際は証跡を取得すること。証跡の納品対象については別途主管課と協議の上決定すること。 ・ 受託者は証跡等に代表されるテストの成果物のレビューを徹底し、テスト項目に基づきテストを実施しているか確認する。想定外のテスト結果となった場合は、システムの欠陥であるか、想定結果が誤りであるか等、原因を明らかにした上で必要な対応を行うこと。 ・ 欠陥を検知した場合は、その原因を明らかにした上で、原因を解消すること。 ・ 検知した欠陥について修正を行った場合は、修正対象機能について回帰テストを実施すること。 ・ 主管課において、再テストが必要と判断した場合、受託者は再テストの計画を作成し、主管課の承認を得た上で、定められた期限内に再テストを実施すること。また、類似バグを抽出するため、必要に応じて強化テストを実施すること。
6	テストデータ	・ 総合テスト及び受入テストにおいて実データを使用する必要がある場合は、実データの取得申請を条件として、実データの使用を許可する。なお、疑似データの作成に当たり、実データの匿名化、符号化等を行う場合は受託者の作業とする。 ・ 取得した実データは、適切に保管・管理すること。 ・ 受入テストにおいて作成したテストデータは、システム切替え実施前までに、検証環境等のデータも含め削除すること。 ・ 機密性の高いデータ項目や個人情報に係るデータ項目は、マスキングした上で使用すること。
7	対応状況の	・ テストの進捗としては、テスト実施済項目数や信頼度成長曲線等の定量的なメトリクスの推移を示すことにより、テスト進捗状況、不具合検出状況及び不具合対応状況を報告すること。

	報告	・ 受託者は、主管課からのテストの進捗状況や品質等に対する指摘に対し確実に修正すること。 ・ 結合テスト・総合テストでの報告書には、ソースコードメトリクスを取得し、テスト結果及び品質指標とともに、主管課に報告すること。 ・ 受託者は、各テスト工程に応じたテスト計画内容について主管課に説明し、各テスト工程における最初のテスト開始予定日の遅くとも 1 週間前までに主管課の承認を得ること。
8	テスト完了報告書	・ 各テスト工程の完了に当たっては、テスト完了報告書を作成し、主管課の承認を得ること。また、完了に当たっては以下をすべて満たすこと。 ➢ すべてのテスト項目が完了していること。 ➢ テスト結果について、定性評価及び定量評価（テスト密度、バグ検出密度等）により評価を行うこと。 ➢ テストで発生したすべての障害が、当該テスト工程内で解消されていること。 ➢ 外的要因等により次工程への申し送り事項が発生した場合は、対応方針、対応時期等を明確にした上で、主管課の承認を得ること。
9	テストの自動化	・ 各テスト項目のうち、反復的にテストを実施するものについては、自動化することを原則とする。そのために、必要となるテストツールについては、新規に作成するか、既存のツールを活用すること。 ・ UI のテスト、受入テスト等、テストの自動化に馴染まないものについては、自動化対象外とする。ただし、自動化対象外とすることについて、主管課の承認を得ること。
10	将来時点の仕様変更	・ OSS を適用する部分を除き、将来時点の仕様変更への対応を柔軟にする観点から、テスト駆動開発、ソースコードに対する静的解析及びリファクタリングにより、クラスや関数構造をシンプルに保つこと。
11	構築時の脆弱性対策	・ ネガティブテスト、ファジング、フォルト・インジェクション等の障害注入テスト手法を活用し、エラー処理や例外処理に係る脆弱性に対処すること。 ・ 品質保証、フォレンジック及びインシデント・レスポンスの観点から、問題原因を把握するために必要な例外情報をログに出力するようにすること。 ・ 設計・開発段階の早期からセキュリティを検証すること。

(1) 単体テスト

単体テストは、本サービスにおける最小の実装構成要素（関数、メソッド等）に着目し、ソースコードの確からしさを確認することを目的とするコードベースの単体テストと、UI を含む単機能のテストにより構成する。現時点で想定する単体テストの要件を以下に示す。

ア 本サービスにおける最小の実装構成要素の動作を検証するために必要となるテストコードを作成し、コードベースの単体テストを実行すること。また、テストコードは、テスト対象とする実装構成要素に関するソースコードを記述する前に記述するようにすること。

イ 単体テストの結果は、必要に応じて数値的指標等（ステップ数あたりの試験項目数、試験消化率等）をもって報告すること。以下に示す事項については、あらかじめ主管課に提示すること。

- 単体テストのスケジュール
- テスト環境（テストを実施するハードウェア、ソフトウェアの構成、テストツール等）の概要
- 合否判定基準 等

ウ 単体テスト実施時は、テスト結果を検証するための証跡を採取すること。

エ 単体テストは、原則として開発環境において実施すること。

(2) 結合テスト

結合テストは、本サービスの構成要素（アプリケーション機能、ソフトウェア、ハードウェア等）に着目し、各要素の連動又は協調動作に関する設計の欠陥を検出することを目的として行う。現時点で想定する結合テストの要件を以下に示す。

ア　結合テストの観点として以下を想定する。

表 46 結合テストの主なテスト観点

項番	テスト種別	概要
1	システム基盤テスト	構築した本番環境及び検証環境の確認を行う。現時点で想定するシステム基盤テストの要件を以下に示す。 ・ 環境設計において作成したリソース定義コードを実行し、サービスのインフラストラクチャを構成する環境及び仮想資源を構築すること。 ・ 構築した環境及び仮想資源が正しく動作するか、動作確認テストを実施すること。 ・ クラウドサービスが提供するツールによって実行可能なテストコードを作成すること。 ・ 動作確認テストの結果、何らかの異常またはエラーを確認した場合、実行したリソース定義コードに原因が作り込まれていないか、必要な見直しを行うこと。 ・ 問題修正後、該当する環境または仮想資源について、再構築と動作テストを再度実施すること。
2	外部連携テスト	外部システムとの連携部分の確認を行うため、以下を実施する。 ・ 疎通テスト：本システムと外部連携システム間で必要な通信の疎通が通ることを確認する。 ・ 異常系テスト：想定しうるエラーを発生させ、エラーメッセージ等の確認をする。また必要な対処を行うように修正する。 ・ バリエーションテスト：インタフェースによる動作と必要なバリエーションの確認を行う。 ・ 運用観点テスト：正常時、異常時の運用に関する動作を確認する。異常時の対応として、エラーメッセージやログ等を基に、運用事業者が運用業務を行えることを確認すること。

イ　テスト対象機能について同値分析、境界値分析、原因結果分析を行い、その結果を踏まえてテストケース、テスト項目を設定し、アプリケーション機能相互間の接合に不具合が無いことを検証すること。

ウ　状態遷移マトリクスを踏まえ、本サービスに備えるユーザーインタフェースについて、仕様どおりに操作可能か、誤った操作をした場合も適切なエラーメッセージが表示されるか等の操作確認を行うこと。

エ　状態遷移マトリクスを踏まえ、アプリケーションコンポーネントが備える API に対して境界値テストを行い、境界及び状態遷移を網羅すること。

オ　結合テストに用いるテストデータには、テストケース、テスト項目を踏まえた疑似データを作成して使用すること。

カ　結合テスト実施時は、テスト結果を検証するための証跡を採取すること。

キ　結合テストは、原則として開発環境または検証環境において実施すること。

(3) 総合テスト

総合テストは、機能仕様及びアーキテクチャに由来する欠陥を検出することを目的として行う。現時点で想定する総合テストの要件を以下に示す。

ア　総合テストの観点として下表を想定する。

表 47 総合テストの主なテスト観点

項番	テスト種別	概要
1	業務運用テスト	・ 業務の実施手順や業務で取り扱うデータを基に様々なシナリオ・データのバリエーションを作成し、情報システムを用いて業務、機能を確認する。 ・ シナリオ・データには、日常的に実施する業務や日常的に取り扱うデータだけではなく、月次や年次等の特定のタイミングでしか発生しない業務やイレギュラデータも含めること。

		・ ユーザーの誤操作や予期しない現象を契機としたシステム障害が発生しないことを確認することを目的として異常系のテストケースも含めること。
2	ユーザビリティ/アクセシビリティテスト	利用者にとっての主観的な利用品質を計測する。現時点で想定するユーザビリティ/アクセシビリティテストの要件を以下に示す。 ・ ユーザビリティ/アクセシビリティテストの計画に当たっては、以下の内容を総合テスト計画書に記載すること。 ➢ テスト目標 ➢ 実施場所及び実施時期 ➢ 具体的なテスト内容 ➢ UX メトリクス ➢ タスクシナリオの開始基準・終了基準 ➢ ユーザビリティ/アクセシビリティテスト実施報告書の構成 ・ 本サービスを対象としたユーザビリティ/アクセシビリティテストに必要となる実施施設や実施環境は、原則として受託者が手配すること。当該施設を利用するに当たって利用料金が発生する場合、受託者は、当該施設の利用料を本業務に伴う設計・開発に係る経費に含めること。 ・ ユーザビリティ/アクセシビリティテストの実施担当者を受託者において選定することとして差し支えないが、当該実施担当者は、調達仕様書「5.2.作業要員に求める資格等の要件」に示す要件を満たす者であること ・ ユーザビリティ/アクセシビリティテストの被験者、人数及び選定方法は、主管課との協議により定めること。ユーザビリティ/アクセシビリティテストの被験者は、最終ユーザーだけでなく、管理者である職員もテスト対象とすること。 ・ ユーザビリティ/アクセシビリティテストにおいてどのようなユーザー補助手段（マニュアル、ヘルプ等）を用意できるか整理すること。 ・ 受託者は、本業務において実施する各ユーザビリティ/アクセシビリティテストについて、客観的な評価を行うため、必要に応じて簡易な映像記録を制作することが望ましい。
3	性能・拡張性テスト	ユーザー数、データ量、リクエスト数、レスポンス等の性能要件を情報システムが満たしているか検証する。検証に当たっては、現在の想定だけではなく、今後の予想される増加量も含めて確認する。 短時間で情報システムに重い負荷をかけ、情報システムが処理量や長時間稼働等のシステム限界に関する性能や拡張の要件を満たしているか確認する。
4	可用性（障害）テスト	疑似的に障害を発生させる等の方法により、本サービスのコンポーネントに障害が発生した場合に、どの程度許容して安定動作するか検証する。また、システム障害及びエラー発生時の回復機能等が適切に動作することを確認する。
5	完全性テスト	疑似的に障害を発生させる等の方法により、本サービスのコンポーネントに障害が発生した場合に、データの減失や改変がないことを検証する。また、操作ログやアクセスログ等のシステムログが出力されることを検証すること。
6	互換性検証テスト	更改開発の前後で、同様の手順で業務が実施できるよう、現行システム・次期システムが提供する業務についてメインの機能・動作及び、入出力の同値を保証できているか確認する。現時点で想定する互換性検証テストの要件を以下に示す。 ・ 互換性検証テストは以下 2 点の環境を構築・準備の上、実施すること。 ➢ 本調達開始時点における環境を再現した環境 ➢ 本調達における必要な改修等を実施後の環境 ・ 互換性検証テストの例として以下を想定している。また、職員によるテストが必要な場合はその旨、申し出ること。 ➢ ソフトウェアのバージョンアップに伴う互換性 ➢ 旧システムから新システム移行にともない、関連部分（外部ツール等）の互換性 ➢ 機能改修に伴う影響の確認（デグレードの有無の確認） ・ 使用するテストデータは、本番環境から取得したマスク済みのデータを使用すること。なお、マスク済みデータは、主管課及び各事業者と調整の上、取得すること。

7	セキュリティテスト	不正侵入や Web 特有の攻撃への対策、データベースへの不正アクセスなどに対する対策、データの持ち出しに対する対策、マルウェア（ウィルス）対策等のセキュリティ要件を満たしているか脆弱性検査、インシデントレスポンステスト等を実施し確認する。
8	運用・保守テスト	運用・保守作業全般を通して、運用・保守事業者が円滑に日々の業務を実施できることを確認する。 また、運用・保守における正常時、異常時の運用に関する動作を確認し、特に異常時の対応として、エラーメッセージやログ等を基に、運用・保守事業者が業務を行えることを確認すること。

イ　総合テストに用いるテストデータには、本番運用を想定した疑似データを作成して使用すること。

ウ　キーワード駆動テストの適用により、総合テストの効率化を図ること。

エ　システム停止に伴うシステムバックアップやシステム停止、リストア、システム起動等については、受託者が主体的に実施すること。

オ　総合テスト実施時は、テスト結果を検証するための証跡を採取すること。

カ　総合テストは、原則として検証環境または本番環境において実施すること。

(4) 受入テスト

受入テストは、要件に対するアプリケーションの充足性確認を目的として行い、主管課は構築された情報システムが要件定義書に記載した事項を適切に実現しているか、構築された情報システムを用いて実際のサービス・業務を正しく実施できるかといった観点でテストを実施する。受入テストに用いるテストデータには、本サービスが原則として公開情報を取扱うことを踏まえ、可能な限り本番環境に近い複製データを使用する。ただし、受入テストの目的を担保可能であることを条件に、疑似データを使用することも可能とする。

受託者は調達仕様書にある通り以下の支援を行うこと。

ア　受託者は、主管課が実施する受入テスト計画書作成作業を支援するために、受入テスト計画書（案）を作成すること。主管課は受入テスト計画書（案）を基にして受入テスト計画書を作成する。なお、受入テストの実施期間は十分に確保したスケジュールとすること。

イ　受託者は、主管課が実施する受入テスト仕様書作成作業を支援するために、テスト項目、使用するテストデータ、合格判定基準等を示した受入テスト仕様書（案）を作成すること。主管課は受入テスト仕様書（案）を基にして受入テスト仕様書を作成する。

ウ　受託者は、主管課及びプロジェクト関係者が受入テスト計画書及び受入テスト仕様書に基づき実施する受入テストの実施支援を行う。

エ　受入テストは、原則として検証環境または本番環境において実施すること。受入テストの実施に当たり、必要に応じて本システムの運転スケジュール、環境設定、テストデータ等の変更を行うこと。

オ　受入テストの実施に当たり、主管課からの質問に対する問合せ対応を行うこと。

カ　受入テストで発生したすべての障害が解消されている、または問題を特定した上で対応策について主管課の承認を得ていること。

3.13. 移行に関する事項

本サービスに関する現段階での移行要件を以下に示す。

(1) 移行に関する前提条件

移行における前提条件を下表に示す。

ア　データの移行漏れを防止するため、データ移行時には現行システムを停止する必要がある。業務停止に当たっては、主管課に対して移行に係る時間や制約条件等を報告し、事前に十分な調整を行うこと。

イ　新システムの要件等に伴い、移行対象データの作成や加工が必要な場合においては、移行元システムの運用・保守事業者と協力し、調整の上で、確実に実施すること。なお、移行実施体制と役割分担については下表を参照の上、移行作業が円滑に進むよう適宜調整すること。

表 48 移行に向けた作業手順及び役割分担

項番	作業名	主管課	工程管理支援事業者	現行システム運用・保守事業者	次期システム設計・開発事業者（受託者）	…
1	移行計画の作成	■	●	△	◎	…
2	移行データ準備・提供	◎、■	●	◎	△	…
3	移行データ分析	■	●	△	◎	…
4	移行設計	■	●		◎	…
5	データ移行サーバ・ツールの開発	■	●		◎	…
6	移行リハーサル	■	●	△	◎	…
7	移行判定	◎、■	●		◎	…
8	本番移行	■	●	△	◎	…
9	稼働判定	◎、■	●		◎	…

◎：主体者、●：確認者、■：承認者、△：支援者

ウ　移行時期については、令和 XX 年 XX 月を想定する。具体的な移行時期については、本サービスの設計・開発着手後に別途定める。

エ　本番環境への移行作業は、システム停止を伴うことから、システム運用時間外の土日祝日に実施する予定である。移行作業中に障害が発生する場合も想定し、連絡体制・現場対応体制を確保すること。

(2) 移行計画の作成

移行等に関しての計画をまとめた「移行計画書」を作成し、主管課の承認を得ること。「移行計画書」には、下記を含めること。なお、移行計画は本プロジェクト関係者以外の第三者にも容易に理解可能でかつ継承可能な形式で作成すること。

表 49 移行計画書の記載内容

項番	項目	補足

1	主管課及び各事業者の移行実施体制と役割	・ 移行作業は、受託者が主体となり実施するものとする。
2	移行に係る詳細な作業及びスケジュール	・ 受託者は、主管課に最終的な移行スケジュールを提示し、確定した内容を移行計画に反映させること。
3	移行対象	・ データ名称、保管環境、容量、など
4	移行環境／移行方法／移行ツール	・ 移行可能期間の制約も踏まえた上で、一括移行、差分連携等の手法を組み合わせて、円滑に移行が行えるように留意すること。 ・ 業務停止に当たっては、主管課に対して移行に係る時間や制約条件等を報告し、事前に十分な調整を行うこと。 ・ 移行方式は、原則として一括移行（or 複数回の分割移行）とする。
5	移行作業、移行に伴い発生する各種設定を行うための各種手順書・マニュアル	・ 移行する際の移行手順及び、機能改修のリリースに係る移行手順を作成し、主管課の承認を得ること。具体的な移行方法や手順は、主管課との協議の上で確定し、必要に応じて手順やツールの操作方法等に関するマニュアル等を受託者が作成すること。 ・ 移行手順は、本システムと連携する XXX システムにも影響があることを踏まえ、主管課経由で調整等を実施した上で作成すること。
6	切り戻し基準、切り戻し手順書	・ 令和 XX 年 1 月～3 月（3 か月間）は、現行システムをバックアップシステムとして並行稼動させる。 ・ 本システムの不具合等により現行システムへの切り戻しが必要となった場合に対応できるよう、切り戻し基準や切り戻し手順書をあらかじめ定めること。 ・ 切り戻し手順書には、切り戻した後の両システムの運用方法、データの整合性を確保する方法、再度本システムに切替える際の移行手順等も含めること。
7	移行判定基準	・ 移行開始時に満たすべき移行判定基準を定めること。なお、移行判定基準には以下を含め詳細は主管課と協議の上決定すること。 ➢ 計画した全てのテストケースを消化し、摘出された全ての障害（バグ、不具合等を含む）が除去されていること。仮に除去されていない障害がある場合は、その対処方針が明確となっていること。 ➢ 移行計画書及び移行リハーサルの結果が適正であること。 ➢ 切り戻し基準や切り戻し手順書を定めており、主管課の承認を得ていること。 ➢ 稼働後の運用準備が整っていること。
8	連携先の外部システム	・ システム移行に当たっては、XXX システム関係者と連携すること。その際、システム連携の現状を把握し、新システム移行に伴うテスト計画を作成し、テストに向けた事前合意形成を行い、テストフェーズでも進捗管理、課題管理を行って、テスト結果の取りまとめを行うこと。その際に、必要な資料等の作成を行うこと。また、システム停止を伴うことから、XXX システム関係者と連携し、利用者に対する通知方法、通知内容の検討等について、受託者が主体的に実施すること。
9	移行リハーサルの実施場所（システム環境）	・ 移行リハーサルについては、必要に応じて、XXX システム関係者と調整の上、検証環境及び本番環境で実施すること。 なお、移行リハーサルにおいて本番環境を利用しない場合は、可能な限り本番環境に近い環境を準備した上で移行リハーサルを実施すること。

移行計画書に加えて下表の計画も作成すること。

表 50 計画の種類

項番	計画の種類	概要
1	移行リハーサル計画	移行の設計内容、データ移行用サーバ及び移行用インポートサーバの設計内容、連携業務 AP の接続切替え方法、移行リハーサルにおける方針、スケジュール、実施体制、実施手順、検証方法等を定めたもの

2	移行（本番）計画	本番移行時の方針、スケジュール、実施体制、実施手順、作業結果判定方法、移行作 業時のセキュリティ対策等を定めたもの
3	並行稼動計画	並行稼働における方針、スケジュール、実施体制、実施手順、検証方法、切戻しを行う際のコンティンジェンシープラン等を定めたもの

(3) 移行データ準備・提供

主管課は、現行システム運用・保守事業者の支援を受けつつ移行対象となるデータを整理し受託者に提供する。

受託者は、移行対象データを受領し内容を確認すること。

(4) 移行データ分析

受託者は、移行対象データを分析し、データ・クレンジング等の加工作業が必要であるか確認の上、結果について主管課に報告すること。

(5) 移行設計

受託者は、「移行計画書」を踏まえ、以下の点に留意して移行設計書を作成の上、主管課の承認を得ること。また、業務実施部門が本システムを利用するために必要となる準備事項について、提案や支援を行うこと。

ア　システム移行、データ移行、稼働の方式を設計すること。

イ　本番移行等、各移行作業に関しての見込み時間を記載すること。その際は、部分的なデータを送信して所要時間を計測するなど、必ず事前に計測を行い、本番移行の見込み時間の妥当性を証明すること。

ウ　現行サービスから次期サービスへ接続切替えを実施する方法に関する設計を行うこと。なお、接続切替えを実施するために、他のシステム等に設定変更等を依頼する場合には、依頼内容を整理した上で、主管課を通じて、担当事業者、担当府省との調整を行うこと。

エ　データ移行を含む移行に係る作業を抽出し、システム移行フローを組み立て、タイムスケジュール化等を行うこと。

(6) データ移行サーバ・ツールの開発

「移行設計書」の内容に基づき、データ移行ツールの開発及びテストを実施すること。なお、既製のソフトウェア製品の機能をそのまま利用してデータ移行を実施する場合は不要であるが、利用には主管課に報告の上、承認を得ること。

なお、移行対象データに対し、データ・クレンジング等の加工作業が必要な場合は当該作業を実施すること。

(7) 移行リハーサル

システム移行、データ移行のリハーサルでは以下の点に留意すること。

ア　移行リハーサル設計書及び移行リハーサル手順書の内容を最終確認し、XXX システムの担当府省と最終的な意識合わせを行うこと。

イ　XXX システム側に設定変更等を依頼する場合は、依頼書を準備し、期間的な余裕を持って、主管課経由で依頼すること。

ウ　受託者は、移行リハーサルの実施後、移行に係る作業手順、作業時間見積もり等を評価し、「移行リハーサル結果報告書」を作成すること。また、その内容について主管課に説明し、承認を得ること。

エ　移行計画書及び移行手順書に問題がないことを検証するため、最低 1 回以上移行リハーサルを実施すること。
なお、移行リハーサル実施後における使用データの扱い（移行リハーサル後に使用データを削除等）についても検討すること。

オ　受託者は、移行リハーサルの結果として移行リハーサルの結果を分析し、本番移行に向けた課題などを明確にすること。

カ　作業品質に改善及び再検証を要する問題点を確認した場合、必要に応じて移行リハーサルの再実行を検討すること。

キ　受託者は、主管課の指示がある場合、修正した移行リハーサル計画書及び移行リハーサル手順書を基準として移行リハーサルを再実行すること。

ク　受託者は、移行リハーサル評価結果に基づき、本番移行までに解決を要する課題について整理すること。

(8) 移行判定

主管課は、移行開始判定を目的とした会議を招集し、「（2） 移行計画の作成」にて定めた移行判定基準を満たしているか確認した上で、移行判定を行う。

受託者は、主管課が移行判定を適切に実施できるよう、報告には「（2） 移行計画の作成」に記載した移行判定基準を満たしているか分かるような情報を含めること。

(9) 本番移行

本番移行では以下の点に留意すること。

ア　本番移行に向けて、移行リハーサルの実施結果を元に移行計画書及び移行手順書を修正すること。また、その内容について主管課に説明し、承認を得ること。

イ　移行計画書には、チェックポイントを設定し、作業の進捗度と経過時間などを元に、切り戻しの判断基準を設けること。

ウ　受託者は、本番移行及び稼働に係る作業過程において作成する提出物及び成果物の内容について、主管課に説明を行い、承認を得ること。

エ　受託者は、本番移行に伴う作業状況について、事前にチェックポイントを設定し、適切なタイミングで主管課に報告すること。万一、作業の実施中に不具合等を生じた場合は、速やかに主管課に報告するとともに、必要な対応を行うこと。

オ　受託者は、本番移行開始判断を受け、稼働のための作業を実施し、本番稼働を開始すること。

カ　受託者は、稼働関連作業の完了後、本サービスの稼働状況を確認すること。また、稼働以降安定運用までの X か月程度の期間、QA 対応を主体とした運用支援を行うこと。特に、本番稼働後 X 週間は、問合せ対応、インシデント対応等に手厚い対応体制をとること。

キ　令和 XX 年 XX 月 XX 月～XX 月 XX 日（X か月間）は、次期サービスの不具合等により、 現行サービスへの切り戻しが必要となった場合には、移行設計書内の並行稼働実施計画に記載する対応方針に基づき、次期サービスから現行サービスへの切替え処理を行うこと。

ク　移行リハーサル、本番移行の実施結果を「移行結果報告書」として取りまとめ、主管課の承認を得ること。

(10)　稼働判定

主管課は、サービスインを判断（稼働判定）する。
その際、受託者は、本番環境への移行の実施結果が適正であり、新しい情報システムへ切り替えても業務に支障が生じないことを主管課が判断するための資料を提出すること。

(11)　移行対象データ

【新規システムの場合】
本システムは新規開発するシステムであるため、旧システムからのデータ移行は発生しない。

【更改システムの場合】
移行対象データを下表に示す。

表 51 移行対象データ

項番	移行元	移行対象データ	件数	提供方法	補足
1	XXX 申請システム	XXX テーブル	XXX	CSV 形式での提供	XXX
2		XXX 申請ファイル	XXX	CSV 形式での提供	XXX
3		XXX 申請情報	XXX	CSV 形式での提供	XXX
…	…	…	…	…	…

(12)　移行対象業務

移行対象業務は、XXX から XXX までの範囲に該当する全ての業務とする。

3.14. 引継ぎに関する事項

本システムの運用は、別途調達する本システムの運用・保守事業者が実施する予定である。現時点で想定する引継ぎ要件を以下に示す。

(1) 引継ぎ計画書の作成

本システムの関連事業者に対する引継ぎの開始前に、本システムの引継ぎに係る引継ぎ対象、引継ぎ体制、引継ぎ内容、引継ぎ方法、引継ぎスケジュール、理解度確認方法、完了条件等を記載した「引継ぎ計画書」を作成し、主管課の承認を得ること。

(2) 引継ぎ方法

ア　受託者は、「引継ぎ計画書」に従い、十分な時間的余裕を持って、必要な運用引継ぎを行うこと。その際は、引継ぎ対象者の理解度を確認し、必要な場合には、「引継ぎ計画書」に記載したスケジュール等の変更を行うこと。

イ　本サービスは、その保守や将来の拡張等の業務を他事業者に引き継ぐことが可能であること（引き継ぎのために必要となる各種ドキュメントを整備する等）。第三者による保守性を向上させるため、成果物等は標準的に利用されているドキュメント作成ソフトウェアを用い、編集可能な形式で納品すること。

ウ　ドキュメントには設計結果のみを記載するのではなく、設計根拠等も明示し、検討経緯を可視化すること。

エ　並行稼働期間中（引継ぎ期間中）における当該システムの運用・保守事業者からの問合わせにも対応すること。

オ　期間内に引継ぎが完了しない場合は、原則として受託者の責任と負担において引継ぎを完了すること。

カ　連携先システムである、XXX のアプリケーション保守事業者に対しては、必要となる知識等について引継ぎを行うこと。引継ぎは約 X 時間/回を X 回程度実施することを想定している。

(3) 引継ぎ対象

本システムの引継ぎ対象を下表に示す。なお、引継ぎに際しては主管課の指示に基づき書面又は電子媒体で行うこと。

表 52 本システムの引継ぎ対象

項番	引継ぎ期間	引継ぎ先	引継ぎ内容	引継ぎ手順	補足
1	令和 XX 年 XX 月 XX 日 ～ 令和 XX 年 XX 月 XX 日	本システムの運用・保守事業者（令和 XX 年度後半に調達予定）	・ ソースコード（テスト・構成管理・環境構築等に利用するコード含む） ・ 開発環境に必要となる各種ツール ・ 各種設計書・ドキュメント類 ・ 運用課題（管理簿） ・ 仕様課題（管理簿） ・ インシデント状況（管理簿） ・ 連携業務アプリケーション対応状況（管理簿） ・ ヘルプデスク作業 ・ 各種運用・保守作業 ・ その他成果物一式 （クラウドサービスの管理に必要なアカウントや鍵情報、また IaC（Infrastructure as Code）に基づくシステム構築・管理等に係る構成管理ファイル等情報を漏れなく含む）	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	XXX
2	令和 XX 年 XX 月 XX 日 ～ 令和 XX 年 XX 月 XX 日	連携先システムである XXX システムのアプリケーション保守事業者	必要となる知識等	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	XXX
3	…	…	…	…	…

(4) クラウドサービスを利用する場合の引継ぎ

本システムでは、本調達の契約期間終了後も、クラウドサービスの契約期間終了前に契約の延長又は他の引継ぎ先事業者（運用・保守事業者を想定）への引継ぎ等を行うことで、クラウドサービスをそのまま継続利用することを想定している。引継ぎに際しては、必要に応じて引継ぎ先事業者及びクラウドサービスプロバイダとの間で書面による契約等を行い、しかるべく管理者権限の引渡し等を行うこと。

(5) 引継ぎ結果報告書の作成

引継ぎ作業の完了時に、本システムの、他事業者等への引継作業の実施結果について記載した「引継ぎ結果報告書」を作成し、主管課へ報告を行うこと。

【前任事業者から既存システムの運用を引き継ぐ場合】

(6) 前任事業者からの引継作業

受託者は、本業務を実施するために必要な情報について、引継元である前任の運用・保守事業者からの引継ぎを受けること。引継ぎ完了後は、受託者が引継ぎ完了報告書（確認者、確認日時、完了条件の適合性等を記載）を作成し、主管課の承認を得ること。

3.15. 教育に関する事項

(1) 教育計画の策定

教育訓練の対象者、スケジュール、実施内容、実施方法（集合研修、テキスト配布等）、教材等に関する教育訓練実施計画書を作成し、主管課からの承認を得ること。

(2) 教育対象者

本システムの教育対象者を下表に示す。詳細は本システムの開発時点で決定する。

表 53 教育対象者

項番	教育対象者	教育内容	教育対象者数
1	システム部門職員	運用業務の全体概要、システム部門職員の業務手順等	XXX
2	業務部門職員	職員の業務に関する本システムの操作手順、画面遷移、UI 表示仕様、エラー発生時の対応等	XXX
3	運用・保守事業者	運用・保守業務の全体概要、運用・保守事業者の業務手順等 運用・保守要員の業務内容等	XXX
4	…	…	…

(3) 教育の実施時期

教育訓練の実施スケジュールについては、主管課を介した調整により、受講対象者と事前に調整した上で確定すること。ただし、遅くとも本サービス運用開始の 4 週間前までに教育を完了し、本サービスを利用した業務開始前までに十分な習熟期間を確保できるようにすること。

(4) 教育の方法

教育訓練の実施方法は、主に講義形式又はマニュアル配布を想定している。以下に、各教育訓練方法についての要件を示す。

ア 講義における講師は、受託者が実施すること。

イ 講義に必要な教材については、受託者が準備すること。必要な機材（プロジェクタ等）は、主管課と協議の上、必要に応じて受託者が準備すること。

ウ 講義会場及び Web 会議環境は、主管課側で準備するものとする。詳細については主管課と協議の上、決定とする。

エ 講義は録画を行い、必要に応じて、掲載等を行うこと。また、録画データは納品の上、主管課が再利用することを妨げないこと。

オ 講義開催日数は、2 回（2 日×1 回）を想定している。講義開催時間は、概ね 2 時間とすること。

カ 講義参加予定人数分の教育教材を用意すること。なお、必ずしも紙媒体で教材を準備する必要はなく、受講者が確認しやすい形態であれば電子データを配布する形でも構わない。

キ 講義終了後、15 分程度の質疑応答の時間を設けること。

ク　講義では受講者がシステム操作を実体験できるようにすること。ただし、本番環境以外に研修用の環境を構築するなどし、本番稼動に影響を与えずに研修を実施できるよう主管課と調整すること。

ケ　講義、マニュアルに関するアンケート用紙を作成の上、講義後に受講者に回答を依頼すること。なお、アンケート内容は事前に主管課と調整すること。

(5) 教材の作成

上記の教育対象者に対して、操作マニュアル、運用・保守手順書、教育資料（システムの概要資料、操作動画、FAQ 等を想定）を作成すること。詳細は教育実施計画書の策定時に、主管課と協議の上決定する。教育資料の概要を下表に示す。

表 54 教育資料の概要

項番	教材	教材の概要	対象者	補足
1	システムの概要資料	情報システムや関連業務の概要を取りまとめた資料	システム部門職員 業務部門職員 運用・保守事業者	対象者毎に教材を作成
2	操作動画	情報システムの操作方法について動画に取りまとめたもの	業務部門職員	XXX
3	FAQ	よくある質問や回答を取りまとめた資料	システム部門職員 業務部門職員 運用・保守事業者	対象者毎に教材を作成
4	…	…	…	…

ア　教育資料の作成に当たっては、情報システムやスマートフォンの操作に不慣れな者でも分かりやすいような構成、内容とすること。

イ　利用者（国民）向けの操作マニュアル等については、サービスデザイン思考、UI/UX 等の観点から、民間スマートフォンアプリ等の経験を有する専門の UI/UX デザイナーを体制に組み入れること。

ウ　教育資料については、主管課のレビューを経て承認を得ること。

(6) 教育訓練実施結果報告

教育訓練の実施結果を教育訓練実施結果報告書にて主管課に報告し、承認を得ること。

3.16. 運用に関する事項

現時点で想定する運用要件を以下に示す。

(1) 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件が含まれる形で運用・保守計画書及び運用・保守実施要領の確定版を作成すること。

表 55 運用・保守計画書の記載内容

項番	項目	補足
1	作業概要	・ 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載する。
2	作業体制に関する事項	・ 運用・保守業務を実施するための体制について、管理体制図、本件受託者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。
3	スケジュールに関する事項	・ プロジェクト計画書及び調達仕様書に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。 ・ 日次、週次、月次等の定型的な業務について、作業内容を記載すること。 また複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。 ・ 年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、その改善（例えば自動化等）の提案を行う作業、情報システム運用継続計画の見直し作業、運用・保守計画書の見直し作業を含めること。
4	成果物に関する事項	・ 運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。
5	運用・保守形態、運用・保守環境等	・ 運用において採用する運用形態（オンサイト、リモート等）、運用環境（本番環境、検証環境、研修環境等の有無）等を記載する。こと。
6	管理対象	・ 受託者は本業務で開発する XXX システム及びドキュメントについて保守を行うこと。
7	クラウドサービスの利用	・ 運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。 ・ 利用しているクラウドサービスの機能や性能等に変更が発生した場合、受託者側でクラウドサービスの変更に伴う開発中システムへの影響を確認し、システムの改修が必要な場合は、原則対応すること。ただし、改修規模が大きい又は影響範囲が広い場合は主管課と協議の上対応を検討・実施すること。
8	サービスレベル	・ 運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを主管課が協議の上、決定すること。 ・ 運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、サービスレベル達成状況の改善に向けた対応策を提案すること。
9	その他	・ 上記に掲げる事項のほか、運用・保守を行う上での前提条件、時間、予算、品質等の制約条件等について記載する。

表 56 運用・保守実施要領の記載内容

項番	項目	補足
1	コミュニケーション管理	・ 運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体 名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時 の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	・ 運用・保守に携わる事業者における作業体制の管理手法等について記載する。
3	作業管理	・ 運用・保守作業及びその品質の管理手法等について記載する。
4	リスク管理	・ 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	・ 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	・ 運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーションプログラム、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	・ 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	・ 運用・保守における情報漏えい対策等について記載すること。

(2) 運用・保守準備

運用・保守に当たって、以下の準備作業の実施等を行うこと。

ア 監視設定

運用業務を効率的に実施するため、監視、アラートについて、システムの特性、各種アラート発生時の重要度に応じたチューニング（マッチング文字列、閾値、アラート検知結果の重要度など）を行い、定量的な計測に基づいて監視を行うこと。また、アラートの通知先、通知手段等は主管課と協議の上、決定すること。

イ バックアップサービス

サービスの故障復旧に必要なデータのバックアップを定期的に取得すること。また、故障復旧時における必要なデータのリストア作業の手順、役割分担等を事前に決定し、故障発生時には実施すること。

ウ 運用・保守手順書

運用・保守実施要領及び運用・保守計画書に基づき、運用・保守手順書を作成すること。

(3) 共通的な要件

ア 運用・保守期間

稼働後、令和 XX 年 XX 月 XX 日まで運用・保守を行うこと。

イ 運用・保守報告書の作成

運用・保守業務の実施結果を運用・保守報告書として取りまとめ、主管課が指定した日時までに納品すること。

ウ 情報セキュリティ対策の実施

「3.10.情報セキュリティに関する事項」を踏まえて実施した情報セキュリティ対策の対応結果を情報セキュリティ対策実施報告書に取りまとめ、主管課が指定した日時までに納品すること。

(4) システム稼働要件

本システムの本番稼動に係る要件は「1.3 業務実施の時期・時間」を参照すること

(5) 主な運用作業一覧

現時点で想定する主な運用作業の一覧について、以下に示す。以下の内容を基に、本システムの設計及び開発時に、運用・保守計画書、運用・保守設計書及び運用・保守マニュアルの案を作成すること。

表 57 主な運用作業一覧

項番	運用作業の分類	主な運用作業の内容
1	パッチ適用	・ 保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼働確認を行う。
2	ログ管理業務	・ 操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログを取得すること。 ・ ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ・ 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。
3	ジョブ管理業務	・ ジョブの登録・更新、ジョブの起動スケジュール（カレンダー）を登録し、ジョブの実施結果を確認、報告する。 ・ 主管課が必要性を認めた際は、主管課の指示に従い、ジョブの手動実行を行う。
4	システム監視	・ サービスの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性等で分類した上で、メールなどにより自動で通知する仕組みを構築すること。監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）、外形監視（当該システムを利用するユーザーと同じ方法でアクセスし正常に動作しているか監視する方式）等 ・ 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、主管課の承認を得た上でこれに係る設計を行い、対応を実施すること。※システムサイジングについても定期的に分析を行い、主管課の承認を得た上で見直すこと。
5	問題管理	・ 本サービスに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。
6	変更管理	・ 課題管理機能の活用を前提として、適切な変更管理を実施すること。 ・ 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。
7	リリース管理	・ 主管課とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。 ・ リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。 ・ 「リリース管理台帳」には以下の項目を管理し、履歴を確認することとし、その管理が必要な項目についても管理する仕組みとすること。 ➢ 実施計画の内容 ➢ リリーステストの実施有無及び結果 ➢ リリース時期 ➢ 各種レビューの実施有無及び結果 ➢ リリース内容 ・ リリース計画書については、リリース予定日より十分な期間を確保の上、前もって主管課の承認をもって提出すること。なお、緊急なリリースを要する場合は主管課と協議すること。
8	システム構成管理	・ 本システムに係る全ての構成品目について、適切な構成管理を実施すること。 ・ システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本システムを構成するクラウドサービス、ソフトウェア製品、ソフトウェアのバージョン、アプリケーションプログラム、通信回線、公開ドメインのほか、本システムの運用・保守に係る全ての文書及

項番	運用作業の分類	主な運用作業の内容
		びデータとすること。ただし、本システムの外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。 ・ システム構成管理対象の変更について、変更履歴を追跡可能であること。 ・ 本番環境・検証環境の維持管理を行うこと。 ・ 本システムのアプリケーションは CI ツールで管理すること。
9	バックアップ	・ システムバックアップ、データバックアップを取得すること。 ・ 必要に応じてシステムリストア、データリストアを実施すること。
10	業務支援	・ 主管課の指示に基づき、利用者の利用状況のデータを集計し、主管課に定期的に報告すること。 ・ 必要に応じて、データベースやディレクトリ等に施されるアクセス制御の設定変更を実施すること。 ・ 運用に必要な端末は受託者が用意すること。 ・ ヘルプデスク担当者からの問合せ、またはサービスデスクからの問合せに対する FAQ を作成すること。
11	障害対応	・ 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因アプリケーションの再設計・製造・試験、再発防止・品質向上作業、報告書作成・報告実施、アプリケーション保守環境反映）を行うこと。 ・ 本システムの連携先システムにおいて障害が発生し、業務影響が発生した場合においても、連携先システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。 ・ システム障害と想定される連絡を受け付けた際、別途、主管課より指示する担当者へ速やかにエスカレーションすること。 ・ 府省内担当者との応答内容の記録を残すこと。
12	ヘルプデスク業務	・ 本サービスの利用方法に関する問合せの受付からクローズまでを一元管理するヘルプデスクを設け、本サービス利用者からの問合せを受け付けること。 ・ 問い合わせの要件は以下に示す。 ➢ 受付時間・方法：「1.3 業務実施の時期・時間」に記載 ➢ 平均処理時間：XXX ➢ 平均応答速度：XXX ➢ 一日の問い合わせ想定量：XXX ・ ヘルプデスク担当者のスケジューリング等の運営を適切に行うこと。 ・ ヘルプデスク担当者による対応手順、サービスレベル等を統一するため、ヘルプデスク運用マニュアルを作成し、主管課の承認を得ること。 ・ ヘルプデスク運営の中で FAQ は適宜追加、更新等、メンテナンスを行うこと。 ・ 受け付けた問合せは、質問、インシデント、サービス要求、作業依頼等に分類した上で、対応日時、問合せ元、内容、回答状況等とともに記録すること。なお、具体的な運用方法については、本サービスの設計開始以降に改めて検討する。 ・ 問い合わせ記録は受付件数、問い合わせ者情報、問い合わせ内容、回率、回答に要した期間、回答内容等を適切な粒度で整理した上で、定期的に問題発生状況を分析し、必要な対応を行うこと。 ・ 運用・保守の計画及び実施状況について、主管課の定める報告様式に従って取りまとめ、主管課に報告を行うこと。（原則、月次での報告）
13	設計・開発事業者による報告・問合せ対応	・ 問合せに関する調査完了後、ヘルプデスクへの回答を行うこと。 ・ その他、適宜、主管課と必要に応じて密に連携を図り、ヘルプデスクの円滑な運営に資すること。
14	インシデント管理	・ 情報セキュリティインシデントが発生した場合は、「運用・保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、主管課、関係事業者と適宜調整の上で対応を行うこと。
15	バージョンアップ対応	・ 保守におけるバージョンアップ対応要否の判断結果に基づき、バージョンアップ対応を実施し、稼働後の動作確認を行うこと。
16	大規模災害	・ 大規模災害等への対応訓練を行うこと。

項番	運用作業の分類	主な運用作業の内容
	等対応訓練	➢ 大規模災害対応訓練シナリオ見直し 本番運用・保守の計画で定義されている訓練シナリオ・手順書を適宜見直し、必要に応じて、設計・開発事業者に確認を依頼すること。訓練シナリオ・手順書を変更した場合は、主管課の承認を得ること。 ➢ 大規模災害対応訓練の実施 受託者は、大規模災害発生時から復旧に係る作業について、主管課及び関係する事業者が迅速かつ適切に作業を実施できるよう、年に 1 回、訓練シナリオ・手順書に基づき、訓練を実施すること。実施に当たっては、主に連絡ルートの確認を実施し、結果を「大規模災害等対応訓練完了報告書（本番運用開始後）」に記載し、主管課に報告すること。なお、訓練への参加は、受託者と主管課のみとし、他事業者や外部連携システムは対象外とする。 ・ 情報漏洩への対応訓練を行うこと。 ➢ 情報漏洩対応訓練の実施 受託者は、情報漏洩等に係る情報セキュリティインシデント対応について、主管課及び関係する事業者が迅速かつ適切に作業を実施できるよう、年に 1 回、訓練シナリオ・手順書に基づき、訓練を実施すること。実施に当たっては、主に連絡ルートの確認を実施し、結果を「情報漏洩等対応訓練完了報告書（本番運用開始後）」に記載し、主管課に報告すること。なお、訓練への参加は、受託者と主管課のみとし、他事業者や外部連携システムは対象外とする。
17	運用改善	・ 受託者は、システムの状況を主管課が定期的に把握できるように仕組みを整えること。 ➢ プロジェクトの目標とする指標、システムの利用者の利用状況 ➢ クラウドのリソース等、システムの利用状況・コストの発生状況 ・ システムの利用状況については、少なくとも以下の項目および「2.4.（8） モニタリング対象データ一覧」に記載した項目を実施し、利用状況の分析とその後の改善策に資する項目を含めること。 ➢ 運用管理・保守業務の作業別の所要時間 ➢ 自動化や効率化が可能と思われる作業の洗い出し ➢ システム及び運用・保守業務の改善提案 ・ アイドリングなどの無駄／過剰なリソースを発見し、コスト削減につながる仕組みを整え、アドバイスも指摘すること ・ 受託者は、システムの利用拡大や利便性向上のため、実績に基づいた定量的なデータや利用者からの問合せ内容等を分析し、多くの利用者が操作方法に迷う部分や誤操作を誘発する部分を把握した上でシステムの改善策を検討すること。また主管課と協議の上、システムの改善を実施すること。
18	サービスオペレーション支援	・ 本サービスが動作するに当たり、必要となるデータベースの各種マスタ情報を維持管理すること。また、マスタ情報管理のための GUI を具備しないマスタ情報の場合、変更依頼を前提として情報の登録、検索、更新、削除のための SQL を作成し、これを実行すること。 ・ 計画停止、保守作業、障害対応等により利用者への影響が生じる場合、本サービスの Web サイトにお知らせを掲載するなどの方法により周知連絡を行うこと。 ・ 作業影響を生じる範囲について、不測の運用障害を回避する観点から、メンテナンス機能を利用してサービス閉塞・閉塞解除運用を実施すること。 ・ アプリケーションの障害を防ぐため、システムメンテナンスの一環として、サーバを定期的に再起動する。再起動後はサービスの動作確認等を行い、問題が無いことを確認すること。再起動のタイミングは主管課と協議の上、決定すること。
19	情報セキュリティ監査	・ 主管課が情報セキュリティ監査を実施する場合がある。その際はセキュリティ監査事業者との調整・ヒアリングへの協力を行うこと。
20	アカウント管理	・ 受託者は、主管課からの指示に基づき、ユーザーID（特権 ID 含む）の払い出し、削除、パスワード再発行を実施すること。 ・ アカウントの利用状況の棚卸を実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については主管課と協議の上、決定すること。
21	その他業務	・ サーバ証明書の更新、ドメインの管理等を行うこと。

3.17. 保守に関する事項

受託者は、運用・保守計画書及び運用・保守実施要領に基づき以下の作業を適切に実施すること。

(1) 保守業務の実施

保守業務として以下を実施すること。

ア　問合せの受付時間は、「1.3 業務実施の時期・時間」に記載の通りとする。ただし、主管課が緊急かつ業務に支障を来すと判断した場合はこの限りではない。

イ　受け付けた問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。

ウ　障害について対応したときは、障害報告書を作成し、主管課に報告すること。

(2) 保守設計

保守設計として以下を実施すること。

ア　役割分担の整理

役割分担を行う際に以下の点に留意すること。

- 保守業務の設計に際し、受託者の責任範囲及びクラウドサービスを含めた関連事業者間の役割分担を整理すること。
- 新システムがクラウドサービス上で稼働することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。

イ　クラウドサービスの利用

クラウドサービスを利用する際に以下の点に留意すること。

- 保守設計を実施する上で、クラウドサービスの標準機能を可能な限り活用すること。
- クラウドサービスによる自動化等により、省力化を実施すること。
- 運用・保守実施要領、運用・保守計画書及び運用・保守手順書については、クラウドサービスが提供する各サービスを活用することにより、作業のみならずドキュメント類についても効率的に作成すること。
- 利用するクラウドサービスにおいて、提供サービスの仕様上必要となるアップデートパッチの適用やメンテナンス等の対応に際して、システムへの影響度に鑑み、主管課と協議の上対応を行うこと。または、自動適用を行う等の対応が可能となるよう、必要な仕組み（検知、適用、等）を準備すること。

(3) アプリケーションの保守

アプリケーションの保守として以下を実施すること。

ア　インシデント管理

運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

イ　是正保守

アプリケーションに起因した障害発生時、監査指摘事項への対応時等、アプリケーションの是正が必要な場合に、是正保守を行うこと。

ウ　適応保守

OS、ブラウザ、ミドルウェア等のバージョンアップ対応等、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。

エ　予防保守

本サービスのアプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合又はアプリケーションコンポーネントについて新たに脆弱性が報告された場合に、予防保守を行うこと。

オ　改善措置

上記イ～エに伴う改善措置を実施する際には以下の点に留意すること。

- 国民等の利用者に影響がある保守作業を実施する場合は、アプリケーション保守の実施効果、現在及び将来の利用者に対する影響の分析を行うこと。
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性等の改善が必要な場合に、対処を行うこと。
- Web 解析結果に基づき、本サービスのユーザーインタフェースについて、ユーザビリティ又は UX に関する課題を識別した場合、課題解決に資する是正保守、予防保守を行うこと。
- Web サーバ、データベース等について、「表 57 主な運用作業一覧 17 運用改善」の結果を踏まえ、必要に応じて稼働環境の改善等に伴う設定変更を実施すること。

カ　根本原因の分析

根本原因を分析する際に以下の点に留意すること。

- 是正保守及び予防保守の実施に当たり、障害、監査指摘、潜在する問題等に係る根本原因の分析を行うこと。

キ　検証

修正したアプリケーションを本番環境へ展開（デプロイ）する前に、修正が適切に実施されているか否かについて検証環境において検証すること。

ク　文章の修正

アプリケーション保守に伴い、ドキュメント（設計書、マニュアル等）の修正を要する場合は、速やかに修正を行うこと。なお、改修等に伴い画面等に発生する変更が軽微な場合は、ドキュメントの更新方針等について別途主管課と協議すること。

(4) クラウドサービスの保守

クラウドサービスの保守として以下を実施すること。

ア　利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応について主管課と協議し、パッチ適用要否を判断すること。

イ　クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、主管課と協議し、適用等の可否を決定すること。なお、実施することとなったバージョンアップに伴う機器・サービス等の停止は計画停止に準ずるものとして扱う。また、バージョンアップに起因して改修が必要な場合には、対応について別途主管課と協議すること。

ウ　クラウドサービスで利用している環境の最新化や更新は、原則として IaC（Infrastructure as Code）を活用しコードを変更し、変更後のコードを実行することにより実施すること。

エ　修正パッチ適用やバージョンアップ等を行う場合には、事前に検証環境において本サービスの運用に影響が生じないことを十分に検証し、環境更新の事前評価を実施すること。

(5) ソフトウェア保守

ソフトウェアの保守として以下を実施すること。

ア　ソフトウェア最新化

本サービスを構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、主管課と協議の上、ソフトウェア実行環境の形態に応じてソフトウェアを最新化すること。

イ　修正プログラム

修正プログラム適用の際は以下の点に留意すること。

- 情報セキュリティや安定稼働の観点から緊急性が高いと考えられる修正プログラムについては、緊急適用を計画すること。緊急性が低い修正プログラムについては、定期保守作業の中での適用を計画すること。
- 使用しているクラウドサービスの内容に変更が発生する際には、クラウドサービスより提供する情報を元にシステムへの影響範囲を調査の上、修正プログラムの適用可否を主管課へ報告すること。適用が必要と判断された場合、クラウドサービスより提供されるソフトウェアに対する修正プログラムの適用作業を実施すること。

ウ　検証・デプロイ

検証・デプロイを行う際は以下の点に留意すること。

- ソフトウェア保守に当たっては、事前に検証環境において本サービスの運用に影響が生じないことを十分に検証すること。
- ソフトウェア保守に伴い、本サービスの安定稼働に影響が生じる事態が予測される場合、主管課の指示に基づいてデプロイ実施の是非を判断すること。

エ　設計書への反映

ソフトウェア保守によりソフトウェア構成に変更が生じた場合、設計書等へ変更内容を反映すること。

オ　保守条件

保守条件は、「製品の導入や使用方法」、「製品の互換性や相互操作性」、「製品資料の解釈」、「構成サンプルの提供」、「修正策の情報提供」、「製品プログラム、製品コードに起因する障害」等の保守が提供されることを想定しているが、最終的な保守条件は、主管課と調整の上、保守設計において決定すること。

(6) 保守実績の評価及び改善

保守実績の評価及び改善として以下を実施すること。

ア　本サービスの運営に関わる関係者間で本サービスの保守に係る情報や問題認識を共有し、保守業務の品質を継続的に維持・向上させること。

イ　本システムが使用するアプリケーション、クラウドサービス、ソフトウェア等の保守実施状況について、日々の保守業務の中で収集する定量的な管理指標を定め、主管課と合意すること。

ウ　ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。

エ　管理指標の達成状況を評価し、未達の場合は原因分析を行い、改善措置を検討すること。また、これらの実績、評価、改善措置について、定期報告すること。

オ　ログ解析機能、Web 解析機能の活用を前提として、モニタリング及び運用過程を通じて得られた利用状況を分析することにより、ライフサイクルコスト低減の観点から、利用するクラウドサービスの所要量及びソフトウェアライセンスの削減可能性を検討すること。また、利用状況の実績、評価、コスト削減可能性について、定期報告すること。

(7) ドキュメントの保守

設計・開発関連ドキュメント及び運用・保守関連ドキュメントが、受託者の契約期間において、最新の状態であるよう維持・更新等を行う。

(8) 軽微な改修

運用・保守の期間中に必要となる軽微な改修として以下を実施すること。

ア　運用・保守の期間中に、利用者からの要望対応、不具合の改善、環境変化への対応等の目的で軽微な改修を行うことを想定している。改修への対応工数（必要に応じて教育訓練等を含む）として、合計 X 人月の作業を見込むこと。

イ　個々の改修に当たっては、改修範囲、影響範囲等を分析して必要工数を事前に見積もった上で、主管課の承認を得た上で作業を実施すること。

ウ　月次の定期報告において、個々の改修の実施状況（工数の消化状況等）について報告すること。また、改修が必要と考えられる事項が受託者においてある場合は積極的な提案を行うこと。

エ　個々の改修が完了した後に、工数実績を提示すること。また、計画工数と実績工数の差異を分析した上で、その後の改修案件のおける見積精度向上と改修生産性向上に努めること。

別紙８

様式

環境負荷低減のクロスコンプライアンス実施状況報告書

以下のア～エの取組について、実施状況を報告します。

ア　環境負荷低減に配慮したものを調達するよう努める。

具体的な事項	実施した／努めた	左記非該当
・対象となる物品の輸送に当たり、燃料消費を少なくするよう検討する（もしくはそのような工夫を行っている配送業者と連携する）。	□	□
・対象となる物品の輸送に当たり、燃費効率の向上や温室効果ガスの過度な排出を防ぐ観点から、輸送車両の保守点検を適切に実施している。	□	□
・農林水産物や加工食品を使用する場合には、農薬等を適正に使用して（農薬の使用基準等を遵守して）作られたものを調達することに努めている。	□	□
・事務用品を使用する場合には、詰め替えや再利用可能なものを調達することに努めている。	□	□
・その他（　　）	／	／

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

イ　エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に消費する電気・ガス・ガソリン等のエネルギーについて、帳簿への記載や伝票の保存等により、使用量・使用料金の記録に努めている。	□	□

・事業実施時に使用するオフィスや車両・機械等について、不要な照明の消灯やエンジン停止に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、基準となる室温を決めたり、必要以上の冷暖房、保温を行わない等、適切な温度管理に努めている。	□	□
・事業実施時に使用する車両・機械等が効果的に機能を発揮できるよう、定期的な点検や破損があった場合は補修等に努めている。	□	□
・夏期のクールビズや冬期のウォームビズの実施に努めている。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

ウ　廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に使用する資材について、プラスチック資材から紙などの環境負荷が少ない資材に変更することを検討する。	□	□
・資源のリサイクルに努めている（リサイクル事業者に委託することも可）。	□	□
・事業実施時に使用するプラスチック資材を処分する場合に法令に従って適切に実施している。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

エ　みどり戦略の理解に努めるとともに、機械等を扱う場合は、機械の適切な整備及び管理並びに作業安全に努める。

具体的な事項	実施した／努めた	左記非該当

・「環境負荷低減のクロスコンプライアンスチェックシート解説書 －民間事業者・自治体等編－」にある記載内容を了知し、関係する事項について取り組むよう努める。	□	□
・事業者として独自の環境方針やビジョンなどの策定している、もしくは、策定を検討する。	□	□
・従業員等の向けの環境や持続性確保に係る研修などを行っている、もしくは、実施を検討する。	□	□
・作業現場における、作業安全のためのルールや手順などをマニュアル等に整理する。また、定期的な研修などを実施するように努めている。	□	□
・資機材や作業機械・設備が異常な動作などを起こさないよう、定期的な点検や補修などに努めている。	□	□
・作業現場における作業空間内の工具や資材の整理などを行い、安全に作業を行えるスペースを確保する。	□	□
・労災保険等の補償措置を備えるよう努めている。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）