家畜疾病サーベイランス報告システム拡充等業務（飼養衛生管理等支援システム）調達仕様書

（案）

令和７年 10 月

農林水産省消費・安全局

食品安全政策課・畜水産安全管理課・動物衛生課

目次

調達案件の概要

1.1 調達件名

家畜疾病サーベイランス報告システム拡充等業務（飼養衛生管理等支援システム）

1.2 調達の背景

日本国内の畜産生産現場では、不十分な飼養衛生管理に起因する家畜の越境性疾病、常在病原体による疾病等が、生産性を押下げる主因の一つとなっている。

疾病の発生予防は、感染源対策、感染経路対策及び感受性動物対策が基本であるが、生産現場では、飼養衛生管理の意義や取組内容の普及が必ずしも十分にできておらず、さらには、生産現場には、飼養衛生管理に関連した病性鑑定、生産資材の使用状況、と畜検査結果等の貴重な情報が、十分に連携・分析されないまま眠っている状況である。

一方で、家畜保健衛生所や自治体は、家畜伝染病予防法（昭和 26 年法律第 166 号）に基づく事務等の作業に追われ、本来果たすべき生産者支援の業務に大きな制約が存在している現状にある。

こうした課題の解決に向けて、農林水産省消費・安全局食品安全政策課、畜水産安全管理課及び動物衛生課（以下、「担当者」という。）は、令和３年度に「飼養衛生管理支援システム構築プロジェクトチーム」を立ち上げ、デジタル技術を活用して、家畜保健衛生所等の事務作業を省力化しつつ、疾病予防に向けた情報を迅速かつ効果的に利活用する「飼養衛生管理等支援システム」構築に向けた検討を開始した。

このような中、令和４年６月 27 日に閣議決定された「デジタル田園都市国家構想基本計画」において、デジタル技術を活用して畜産業の生産基盤強化を図るため、飼養衛生管理等に関する情報をタイムリーに共有・活用する飼養衛生管理等支援システム（以下、「本システム」という。）を、令和５年度より第１期開発を開始、令和６年度から順次運用を開始している。また、令和７年度は家畜疾病サーベイランス報告システムをリビルドによるシステム更改を実施し、令和８年４月より運用を開始するところである。

農林水産省では、「農林水産省デジタル・ガバメント中長期計画」（令和２年３月 27 日農林水産省決定）に基づき、行政手続等のオンライン化に向けた共通的な申請システムのプラットフォームとして「農林水産省共通申請サービス（eMAFF)」（以下、「共通申請サービス」という。）の運用が開始されている。また、農林水産省では、政府全体の動向や利用者視点に立った、あるべき農林水産行政の姿を踏まえ、令和４年６月７日に閣議決定された「デジタル社会の実現に向けた重点計画」を受けて、「デジタル社会の形成に向けた農林水産省中長期計画」（令和４年 10 月５日に農林水産省行政情報化推進委員会決定）を策定した。同計画では、品質・低コスト・スピードを兼ね備えた行政サービスに向けて、 ガバメントクラウド、ガバメントソリューショ ンサービス（GSS)、ベースレジストリ等の共通機能について、農林水産省の各情報システムの状況を踏まえ、活用できるものについてはその活用を徹底するとしている。その上で、農林水産省では、クラウドの共通基盤を整備し、パブリッククラウドへの移行・運用に必要な最小限の共通機能を提供するとともに、情報システムの状況に応じて適切なクラウドへの移行方式を選択した上で円滑にクラウド移行できるよう支援を行っている。なお、当該共通機能を利用するパブリッククラウドを MAFF クラウドと言い、総合的な支援活動を行う組織を MAFF クラウド CoE と言う。

本システムは MAFF クラウドを利用しており、本調達期間においても引き続き MAFF クラウドを利用することを前提とする。

令和５年度の第１期開発で蓄積された共通申請サービスデータを最大限に活用しつつ、各システムと連携強化、現行の家畜疾病サーベイランス報告システムからのデータ移行等及び情報セキュリティの対策の徹底を図り、令和８年度の業務を行うものである。

プログラム資源、ドキュメント等の借受けについては、２章関連調達案件記載の受注事業者と連携の上実施することとし、バージョン不整合等が発生しないよう留意すること。

(1) 家畜疾病サーベイランス報告システム更改の状況

PCで利用するWEBシステムとして、令和８年４月よりMAFFクラウド上で以下のとおり運用する予定（別紙１システム稼働環境、クラウドサービス一覧を参照のこと。）。WEBシステムは主に家畜保健衛生所（全都道府県に241カ所（独立した病性鑑定施設、支所等を含む。）以下同じ。）の職員、国立研究開発法人農業・食品産業技術総合研究機構動物衛生研究部門（以下、「農研機構」という。）及び農林水産省が使用しており、共通申請サービスとAPI連携している。

（補足）
・農林水産省本省からは、ガバメントネットワーク経由及びインターネット経由で接続している。
・都道府県庁及び家畜保健衛生所は、インターネット経由または総合行政ネットワーク（以下、「LGWAN」という。）経由で接続している。
・農研機構及び農林水産省は、インターネット経由で接続している。
本業務でも引き続き、上記経由での接続を維持する必要がある。

（留意事項等）
ア　本システムの基本構造は、別紙１「システム稼働環境、クラウドサービス一覧」を参照すること。最新の情報は、第９章9.1入札参加要件(4)に記載の資料閲覧において確認すること。
イ　本システムは、本番環境の他、ステージング環境及び開発環境があるため、本業務は全ての環境を対象として実施すること。
ウ　受注者は、契約期間中の本業務の実施に必要となる作業場所、資材、社内環境、更改前の家畜疾病サーベイランス報告システム並びに共通申請サービスからのデータ移行に係る各環境への接続するための費用は全て受注者の負担により用意すること。なお、本システムではAWS CodeCommitを利用したソース管理を行っており、受注者側で準備する社内環境においても利用できるように準備すること。本件の利用が難しい場合は、担当者に状況を申し出ること。本章 (1)～(3)のライセンス料（サービス利用料）等は、本業務に含めるものとし、受注者が負担すること。ユーザアカウントの引継ぎについては、営業担当者を紹介するため、確認の上、引継ぎに必要な対応を行うこと。
　なお、受注者は仕様書に詳細な記載のない事項であっても、サービスの提供に必要な問合せ等の事項は実施するとともに、その費用を負担すること。臨時的バージョンアップ等も含むものとする。

(2) 共通申請サービスの状況

農林水産省における補助金・交付金等の手続きを電子的に行うシステムとして、令和元年度に共通申請サービスを構築し、令和２年度から試行運用、令和３年度から運用を開始している。本制度では飼養衛生管理基準に係る手続きを、共通申請サービス上で行っている。

令和７年度から次期オンライン申請システム（以下、「eMAFF申請2.0」という。）の開発を行っており、現行の共通申請サービスは、令和８年度中に終了する予定のため、影響を受ける範囲は本システムで対応する必要がある。

(3) MAFF クラウドの状況

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。農林水産省では、政府

全体の動向や利用者視点に立った、あるべき農林水産行政の姿を踏まえ、令和２年３月に「農林水産省デジタル・ガバメント中長期計画」を改定し、情報システムのクラウド化の推進に当たっては、MAFF クラウドを中心としたクラウドへの移行を進めることとしている。

MAFF クラウドでは、クラウド移行・運用に必要な最小限の共通機能を提供するとともに、クラウド移行・運用等の一連の工程における、PMO による担当者への総合的な支援活動を実施する。なお、総合的な技術支援を行う組織を MAFF クラウド CoE と言う。

これらの状況を踏まえ、第４期開発等業務でも MAFF クラウドを利用する。

1.3 本業務の概要

受注者は、本調達仕様書の内容に基づき、消費・安全局食品安全政策課・畜水産安全管理課・動物衛生課の担当者（以下、「担当者」という。）と十分協議の上、以下の対応を行い、家畜疾病サーベイランス報告システム拡充等を行うこと。

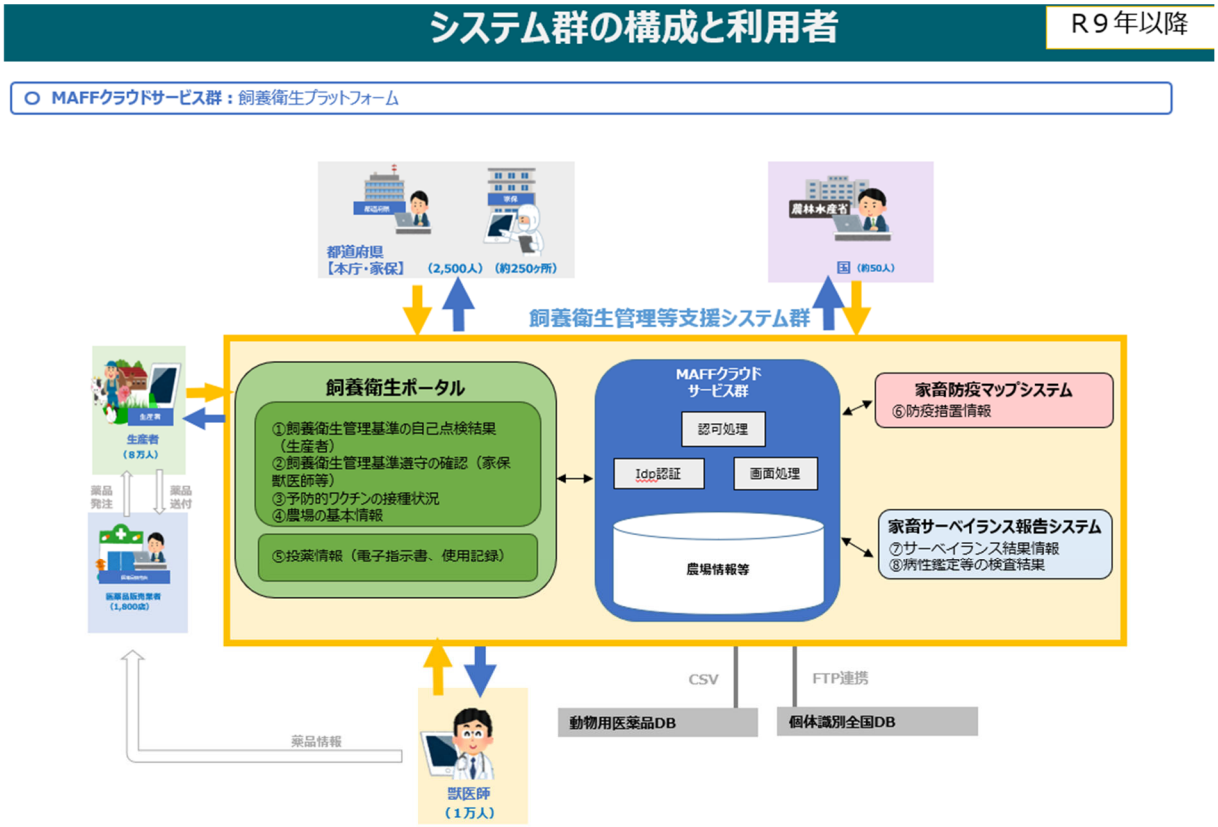
２章関連調達案件に記載の飼養衛生管理等支援システム第４期開発及び運用・支援保守等業務（以下、「第４期開発等業務」という。）において、令和６年度から運用しているシステムを改修する予定。更改後の家畜疾病サーベイランス報告システムは、第４期開発等業務で改修するシステムのサブシステムの位置づけで開発する必要があり、第４期開発等業務で管理している農場台帳等管理ファイルサーバを引き続き利用する必要があるため、第４期開発等業務の事業者と協議を行いながら業務を進めること。

本業務において、AWSアカウントを取得し、クラウドサービス提供業務も含めることとするため、クラウドサービス提供に係る費用及び利用料は受注者の負担とする。

また、共通申請サービスは、令和７年度からeMAFF申請2.0の開発を開始、令和８年度に現行の共通申請サービスの運用を終了する予定。第４期開発等業務において令和８年度にIdP認証機能等を開発する方針のため、本業務でも切替対応をする必要があるため、それぞれの対応する事業者と協議を行いながら業務を進めること。

令和７年度時点

令和９年度以降（予定）



図：本プロジェクトに係る概要

1.4 目的及び期待する効果

慢性疾病の発生をコントロール、急性感染症の増加により、自治体の事務量の負担が大きくなっており、迅速な防疫措置が実施できていない現状がある。

以上のような状況を踏まえ、本業務では、令和７年度から開発、運用している本システムの効率的な運用を行うための機能追加及び事務処理機能の向上を目的とし、関係者間で効率的に活用する情報システムを設計・開発する。

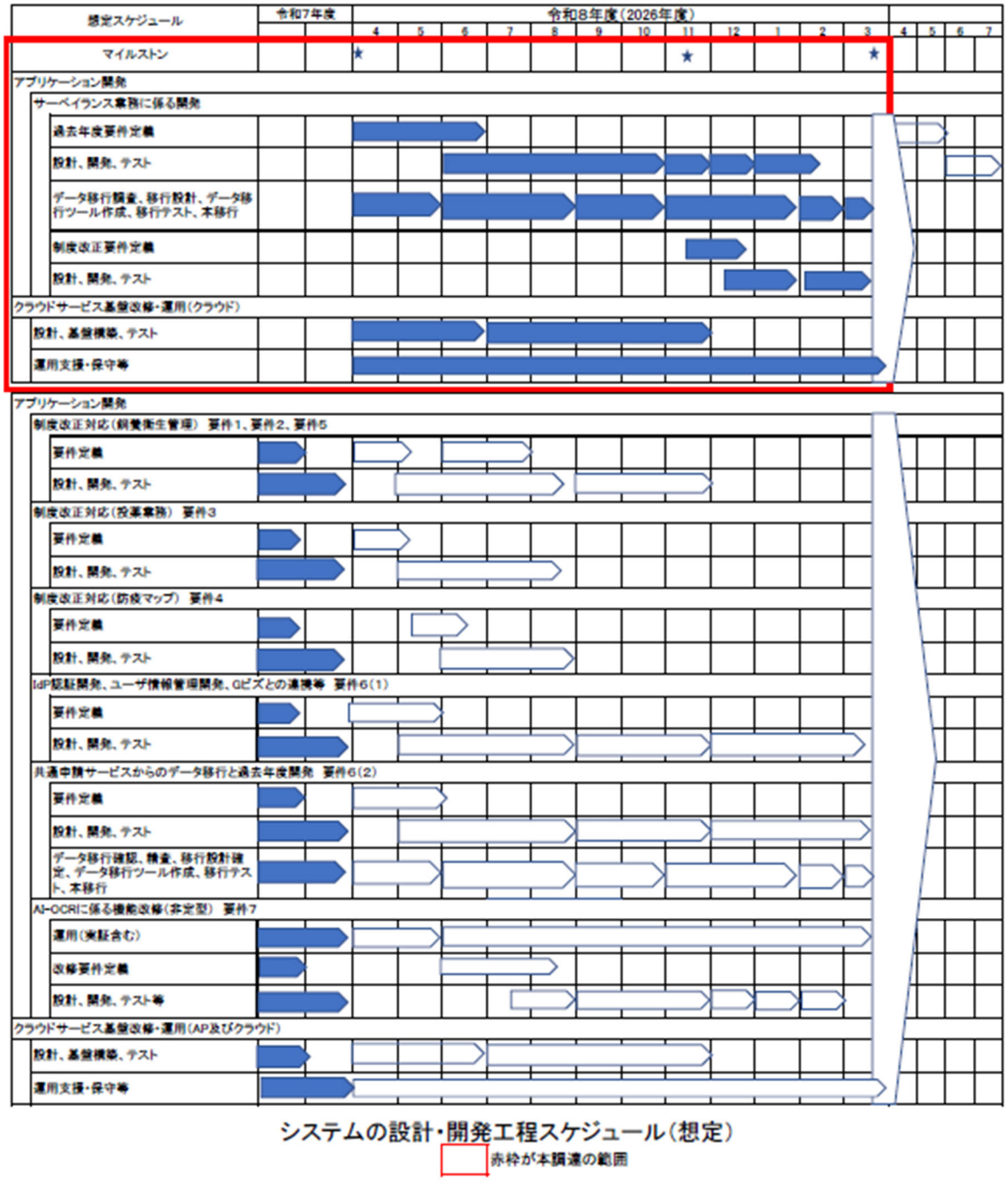
また、本制度を的確に運用する観点から、家畜保健衛生所等の事務作業時間を削減し、情報の効率的・即時的な把握・共有が円滑に実施できるよう、令和８年度の本システムの運用保守等の業務を行うものとする。

1.5 契約期間

契約締結日から令和９年３月 31 日まで

1.6 作業スケジュール

作業スケジュールは次のとおり想定している。



システムの設計・開発工程スケジュール（想定）

赤枠が本調達の範囲

2 関連調達案件

関連する調達単位、調達の方式、調達実施時期については、以下を想定している。

調達案件名	調達方式	主な業務内容	契約期間
令和８年度 eMAFF 運用保守等業務（仮称）	一般競争（総合評価落札方式）	基盤運用、システム保守業務	未定
eMAFF 第８度 eMAFF 運用支援業務（仮称）	一般競争（総合評価落札方式）	コールセンタ運用、支援業務	未定

調達案件名	調達方式	主な業務内容	契約期間
飼養衛生管理等支援システム第４期開発及び運用・支援保守等業務	一般競争入札 （総合評価落札方式）	システム開発に係るプログラム設計、テスト、リリース、基盤運用等業務	令和８年４月１日から令和９年３月 31 日まで（予定）
令和７、８年度飼養衛生管理支援システムコールセンター運用業務	一般競争入札 （最低価格落札方式）	生産者等からの問合せ対応、システム状況確認等業務	令和７年６月３日から令和８年７月３１日まで
令和８、９年度飼養衛生管理支援システムコールセンター運営業務	一般競争入札 （最低価格落札方式）	生産者等からの問合せ対応、システム状況確認等業務	令和８年５月頃から令和９年７月 31 日まで（予定）

3 作業の実施内容に関する事項

3.1 本業務における作業の構成

本業務は、以下の作業により構成する。本業務の遂行に当たっては、「デジタル・ガバメント推進標準ガイドライン」（2025 年（令和７年） ５月 27 日最終改訂（以下、「標準ガイドライン」という。））に基づき、作業を行うこと。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（以下、「解説書」という。）」を参考とすること。なお、「標準ガイドライン」及び「解説書」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。

表 本業務における作業の構成

作業	本調達仕様書の項番
作業実施計画の策定	3.2
要件確認及び要件定義	3.4
設計	3.5
開発	3.6
基盤構築	3.7
テスト	3.8
データ移行及びテスト	3.9
情報システムの移行	3.10
運用保守	3.11
教育	3.10
次期事業者への引継ぎ	3.13
情報資産管理標準シートの提出	3.14

3.2 作業実施計画の策定

受注者は、本制度の内容、本調達仕様書に基づき、契約締結後５日以内に設計・開発実施計画書及び設計・開発実施要領、運用保守実施計画書兼実施要領(以下、「運用保守実施要領」という。)を契約締結後５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。以下同じ。）を除く。）に作成の上、電子ファイルで担当者にメールで提出し、関係者を集め、作業実施計画書の説明（キックオフ）を行った上で担当者に内容の承認を得ること。

設計・開発実施計画書及び設計・開発実施要領の記載内容は、標準ガイドライン「第７章 設計・開発」で定義されている事項及び以下を踏まえたものとすること。運用保守実施要領の記載内容は、標準ガイドライン第３編「第９章　運用及び保守」で定義されている事項を踏ま

えたものとすること。

(1) 各種計画・実施要領等の策定支援

受注者は、以下により、担当者が行う運用作業計画・実施要領等の作成支援を行うこと。

- 担当者が、２章関連調達案件に記載の関連する調達案件の全て含むプロジェクトの運用作業計画及び運用実施要領を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。運用作業計画及び運用実施要領の記載内容は、標準ガイドライン第３編「第９章　運用及び保守」で定義されている事項を踏まえたものとする。

(2) 開発管理

受注者は、以下により適切な開発管理を行うこと。

- 上記 3.2 で担当者が承認した設計・開発実施計画書に従い、記載された成果物を作成すること。その際、設計・開発業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、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。
- やむを得ず開発スケジュール等を変更する場合は、事前に担当者と協議し、指示に従うこと。
- スケジュール管理は、WBS 等により定量的な計測に基づく進捗状況を報告すること。
- 省内での作業においては、担当者の指示に従うこと。
- 貸与された物件は、厳重な管理を行い、本業務の完了時に返却すること。データは復元できないよう消去を行い、消去証明書を速やかに提出すること。
- 作業を進める中で発生する問題、課題等が検討事項から漏れないように、原因・解決策等を課題一覧表に整理し、進捗状況と併せて報告すること。
- 本業務遂行に当たっては、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。
- 本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。
- システムの設計・開発工程スケジュール（想定）に記載のタスク単位で各工程毎に担当者によるレビューを受けること。なお、レビュー期間については、担当者と打合せの上、十分な期間を設けるスケジュールにすること。なお、担当者レビューは次期工程の進捗を妨げるものではない。

3.3 会議体等

(1) キックオフ

受注者は、本業務の本調達仕様書に基づき、作業実施計画書、設計・開発実施計画書及び設計・開発実施要領、運用保守実施要領を作成の上、関係者を集め、作業実施計画書の説明（キックオフ）を行った上で担当者の承認を得ること。キックオフ会議は契約締結後、14 日以内に開催する予定である。

(2) 進捗報告

受注者は、本業務の進捗状況（作業内容、作業予及び実績、作業上の課題、課題に対する対応方針、直近の作業内容、リスク・リスクに対する対応方針等）、品質管理情報等について、作業実施計画に基づき、定期的に報告し（原則、月に２回程度）、担当者の承認を得ること。

ただし、進捗状況によっては開催頻度を毎週に変更することを要請することがある。状況により、次回の開催を待たず、臨時で会議を開催の上報告し、担当者の確認を得ること。

また、全ての作業終了後に、本業務における作業実績工数を報告すること。

(3) 個別検討会議

受注者は、担当者と対面で移行設計に係る認識合せの打合せを行うこと。上記、(2)と同日開催も可とするが、個別検討会議は対面での実施を原則とし、打合せ場所は農林水産省本省内を原則とするが、会議室の確保が困難な場合等、受注事業者のオフィス会議室等で実施する場合があるため、対応すること。

(4) 月次報告・年次報告

運用保守の月次報告会は月１回、固定した曜日の第２回目での開催を予定している（金曜日開催であれば、第２回目の金曜日）。年次報告会は、令和９年３月の第３週目に予定している。このため、令和９年３月については、月次報告会と年次報告会を同時開催することとし、担当者に報告の上、承認を得ること。

担当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、上記会議体とは別に会議を開催すること。

また、全ての作業終了後に、本業務における作業実績工数を報告すること。作業実績工数は、開発は契約期間中をまとめた工数とし、運用・保守は契約期間中、月単位でまとめた工数とする。

(5) 議事録の作成

受注者は、担当者を含めた会議等を開催した際には、会議終了後、５日以内に議事録を作成し、担当者に提出し承認を得ること。

3.4 要件確認及び要件定義

受注者は、設計・開発の実施に先立ち、本調達仕様書、担当者が提示する資料等に基づき、設計に必要な要件の確認を行うこと。別紙２「家畜疾病サーベイランス報告システム拡充等業務に係る要件資料」を更に詳細化し、不足、齟齬がないか確認の上、担当者及び各制度の政策担当者と打合せを実施し、要件定義書を作成（資料作成の粒度は、第３期開発業務の成果物と同等を必須とする。）、内容の承認を得ること。その際、内容について調整すべき事項があれば、担当者及び制度担当者等関係者と調整の上、結果に基づき要件定義書の修正を行うこと。要件の調整内容は、担当者及び関係するステークホルダーに提示し、合意形成を図りつつ進めること。

データ項目は新規情報システムのデータ構造を明示し、保有・管理するデータの変換、例外データ等の処理方法等も考慮し、記載すること。システム操作性及び機能について疑義が発した場合は、想定されるシステム利用者にヒアリング等を実施し、反映させること。ヒアリング等は書面アンケート方式及びWEB会議方式でも可能とする。

なお、要件の確認は、以下のドキュメントも考慮すること。特に、病性鑑定は令和５年度に共通申請サービス飼養衛生アドオン開発において共通申請サービスに実装しているが、更改後の家畜疾病サーベイランス報告システムにおいて開発する必要があるため、留意（※）が必要。

（※）病性鑑定は現行の家畜疾病サーベイランス報告システムには実装されていない。

- 令和６年度飼養衛生管理等支援システム開発に係る調査及び動物用医薬品に係る調査等業務の納入・成果物、打合せ資料及びドキュメント等
- 令和５年度、令和６年度及び令和７年度調達の納入・成果物
- 共通申請サービスの設計資料等ドキュメント
- 現行家畜疾病サーベイランス報告システム納入・成果物等
- 監視伝染病のサーベイランス対策指針

・担当者から提供されるドキュメント（病性鑑定含む）
・本制度に係る実施要綱等

(1) 共通申請サービスの対応

現行の共通申請サービスは、令和８年度中に運用を終了する予定のため、共通申請サービスに登録されているデータを令和８年度中に移行する必要がある。これに対応するため、共通申請サービスの受注業者と十分協議し、必要なデータ移行を行うこと。

なお、病性鑑定は、令和５年度に共通申請サービス飼養衛生アドオン開発にて実装しており、実運用は令和７年度となることを踏まえ作業負荷を見積もること。

(2) 第４期開発システムの対応

令和８年４月（予定）より第４期開発等業務のシステム開発が行われる。家畜疾病サーベイランス報告システムは第４期開発等業務において改修するシステムのサブシステムとして、同じ MAFF クラウド上の飼養衛生管理群に構築している。

令和８年度の第４期開発では、現行の共通申請サービスの運用終了に合わせ、現行の共通申請サービスが行っている IdP 認証機能、ユーザ管理等の開発を行う予定。これに対応するため、第４期開発等業務の事業者と十分協議し、必要な通信要件等を定めること。

また、第４期開発等業務において制度改正対応による改修を行う予定のため、農場台帳等の変更に合わせた対応を行うこと。

(3) GSS の DNS、FW 利用の対応

農林水産省は、デジタル庁が整備する「ガバメントソリューションサービス」（以下、「GSS」という。）を利用している。設計、構築にあたり、GSS や農林水産省に申請が必要な場合は、定められた様式で申請書等を作成し提出すること。

なお、GSS の DNS に設定を行う場合は、デジタル庁 GSS 担当が定めた DNS 設定規則、を担当者から受領して、その内容に基づいて申請書を作成し、担当者を通じて申請すること。

3.5 設計

受注者は、本調達仕様書、上記 3.4 でまとめた各要件定義書を踏まえ、別紙２「家畜疾病サーベイランス報告システム拡充等業務に係る要件資料」の機能要件及び非機能要件を満たすための基本設計及び詳細設計を行い、担当者の承認を得ること。

制度改正対応は、担当者及び関係者と合意形成し、基本設計書、詳細設計書、運用設計書に取りまとめ、担当者の承認を得ること。

更改後の家畜疾病サーベイランス報告システムでも継続して MAFF クラウドを利用するため、事前に MAFF クラウドが提供する共通サービス以外の必要なリソースやインスタンスの種類、クラウドが提供するサービス利用等について担当者、MAFF クラウド CoE 及び関係者に報告し、合意形成すること。合意に基づき、基本設計書、詳細設計書、運用設計書に取りまとめ、担当者及び MAFF クラウド CoE の承認を得ること。既存の追加部分については各種設計書を新規で作成せず、第３期開発の納入・成果物を修正、追記等の必要な作業を行うこと。

データ移行及び紐づけする場合は、データ移行に係る必要な設計を行い、移行設計書にとりまとめ、担当者の承認を得ること。なお、基本設計にはリリース方式設計（IaC、インフラテストの自動化、CI/CD パイプライン化等）を必ず含めること。

設計書の記載内容は、標準ガイドライン第３編第７章を参照の上、資料作成の粒度は、第３期開発業務の成果物と同等を必須とする。

(1) MAFF クラウドの対応

飼養衛生管理支援システム（仮称）第１期開発業務で開発した飼養衛生管理等支援システムを第４期開発等業務において拡張する予定であり、本業務はサブシステムとして開発すること。

LGWAN 接続は、G-Net 経由を必須とする。

本調達仕様及び要件定義書の要件を満たす必要なリソースやインスタンスの種類、クラウドが提供するサービス等を元に、契約期間終了後の次年度以降を含め課題等をまとめたものを担当者に報告し、承認を得ること。承認されたドキュメントは第４期開発等業務でドキュメントを一元管理するため、第４期開発等業務の受注者へ適宜提供すること。

受注者は、「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」の 1.6 クラウドサービスのスマートな利用によるメリット（マネージドサービス活用によるコスト削減、サーバレスによるセキュリティ向上とセキュリティ対策コストの削減、IaC による構築の 3 項目）に適合する設計を行い、クラウドサービスの構成変更を効率的に実施できるよう配慮すること。適合しない設計を行う場合は、合理的な理由の詳細を農林水産省 PMO 及び担当者に説明し、承認を得た上で適合しない設計を採用すること。また、設計書等に検討の過程を記載すること。合理的な理由とは、例えば「IaC による構築（ACloudFormation）が対応していないサービスを使用するために、IaC による構築を行わない」等、真にやむを得ない場合を指す。なお、IaC で構築しても運用役務において、マネージメントコンソールなどを用いた手動変更を行うと IaC にて管理をしていない変更（ドリフト）が発生するため、IaC を用いた運用ができる運用設計並びに運用体制ついて、検討し導入すること。

受注者は特にインフラの運用設計及び保守設計において、MSP(マネージドサービスプロバイダ)サービス等を活用した設計とすることで運用コストの低減に努めること。

なお、MSP サービスの利用とは、以下の定義のいずれかを指す。

①受注者が自社で MSP サービスを提供している企業の場合はそれを利用すること。

②受注者が自社で MSP サービスを提供できない企業は、運用品質の均一化と不要なコストを削減するために外部企業が提供する MSP サービスを利用すること。

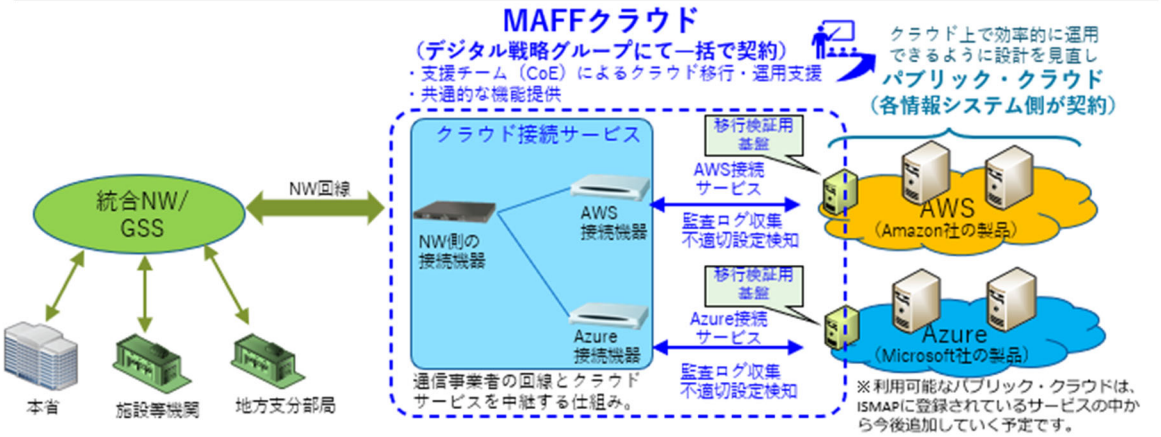
受注者は、運用設計及び保守設計においてクラウドサービスの責任共有モデルを理解し、クラウドサービスプロバイダー、運用保守事業者の責任範囲に重複がないように役割分担を定義すること。

受注者は、プロジェクト開始後、速やかに MAFF クラウド CoE にシステム構成案を提出し、レビューを受けること。レビューを受けた結果、インフラの運用設計及び保守設計に指摘内容を反映すること。

受注者は、インフラの運用設計及び保守設計した結果を踏まえ、設定についてはパラメータシートを作成し、担当者に提出すること。

本システムの管理者及び関係者が速やかに状況を把握できるよう、クラウドの機能を用いて定量的に計測すること。また、ダッシュボードにより、可視化された仕組みが自動で提供される仕組みを構築すること。

MAFFクラウド構成イメージ



(2) 情報システム運用継続計画書の作成支援

受注者は、運用設計時において、情報システム運用継続計画書の更新を行うこと。飼養衛生管理支援等システムの問題発生時に求められる必要最低限の機能、目標復旧時間等に関する内容をまとめ、情報システム運用継続計画書（変更案）を作成、支援を行うこと。また、担当者が情報システム運用継続計画書を更新する際は、更新案を作成、支援を行うこと。

作成支援を行う際は、政府機関等における情報システム運用継続計画ガイドライン（内閣官房国家サイバー統括室（NCO）（2025 年（令和 7 年） 7 月最終更新））を参照とすること。

3.6 開発

上記 3.5 で作成した設計書を踏まえ、以下により、機能開発を行うこと。開発は、現行の家畜疾病サーベイランス報告システムのソースコード等の資産は使用しないこと。機能開発に必要な環境は、受注者の負担で準備すること。

- アプリケーションプログラムの開発又は保守を効率的に実施するため、プログラミング　等のルールを定めた開発標準（標準コーディング規約、セキュアコーディング規約、データやデータ項目の命名規約等）を定め、担当者の確認を受けること。
- 情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、標準コーディング規約遵守の確認、ソースコードの検査、現場での抜き打ち調査等についての実施主体、手順、方法等）を定め、担当者の確認を受けること。
- 現行の家畜疾病サーベイランス報告システムで保持しているデータの移行及び業務移行は、別紙２「家畜疾病サーベイランス報告システム拡充等業務に係る要件資料」のサーベイランス業務-データ移行方針定義書及びサーベイランス業務-開発・運用スケジュールを参照とすること。病性鑑定やマスタ等は、システムが問題なく稼働するように本業務内で移行等、必要な対応を行うこと。
- 現行の家畜疾病サーベイランス報告システムから移行する過去年度のデータは、現行の家畜疾病サーベイランス報告システムと同値結果となるため、テスト工程で検証作業を実施すること。病性鑑定は、共通申請サービス飼養衛生アドオン開発と同値結果となるため、テスト工程で検証作業を実施すること。
- 受注者は、本調達にて開発したプログラム一式を成果物として提出すること。
- 脆弱性検査については、「デジタル庁　政府情報システムにおける脆弱性診断ガイドライン」の実施基準を満たすように脆弱性診断実施事業者の選定、脆弱性診断の実施、検出された脆弱性への対応を行うこと。

3.7 基盤構築

上記 3.5 で作成した設計書を踏まえ、機能が正常に動作するための必要な基盤構築を行うこと。クラウドは MAFF クラウドが提供する共通サービス以外に係る費用について受注者の責任の範囲で調達し、負担すること。

なお、本システムはインターネット経由、ガバメントネットワーク及び LGWAN 経由での利用が必須となるため、接続に係る必要な対応を行うこと。また、ガバメントネットワーク等の作業による影響が判明した場合は、それぞれ必要な対応を行うこと。

また、上記 3.6 で開発した機能を MAFF クラウド基盤上に構築し、正常に動作するようにすること。クラウドサービスの運用は、オンプレミスのように人を張り付けるのではなく、シェアード型の運用サービスを使うこと。

（留意事項）

- 受注者は、インフラの設定変更があった場合は設計書等の更新版（パラメータシート含む）を、担当者に提出すること。
- 受注者は、農林水産省クラウド利用ガイドライン別紙 1_共通機能_利用申請書の内容（システム構成を含む）に変更がある場合、資料を更新し、担当者と MAFF クラウド CoE の確認を受けること。
- G-Net 経由での LGWAN 接続が必須要件となる。

3.8 テスト

上記 3.6 で開発した機能の動作、一連の機能としての動作に係るテストを実施すること。テストにあたっては、事前に以下の内容を含めたテスト実施計画書を作成し、担当者の承認を得た上で実施すること。テスト実施計画書には、実施状況の報告（定例、随時）についても記載すること。また、以下のテストを実施した結果を取りまとめ、テスト結果報告書を作成し、担当者の承認を得ること。

(1) テスト実施計画書の作成

テスト計画を立案した上でテストを実施すること。開発テスト計画には、テスト体制と役割、詳細な作業とスケジュール、テスト環境、テストツール合否判定基準等に関する記述を含むこと。立案した計画はテスト実施前に担当者に説明し、内容について承認を得ること。

(2) テスト実施体制と役割

テスト実施においては、関係者の負荷に配慮し、できるだけ早い段階で計画を立案し、理解・協力を得ること。

(3) テスト環境、テストデータ

本システムが正常稼動することを確認できるテスト環境で構築し、テスト環境を受注者側（社内）に設置の上で、システム動作の確認試験を実施すること。なお、本作業期間中における必要な機器、テストデータの準備については、受注者が手配すること。

(4) テストの実施

受注者は、設計工程の成果物及びテスト計画書に基づき、アプリケーションプログラムの開発、テストを行うこと。単体、結合、総合テストは社内環境で行うこと。総合テストのうち、以下の性能テストは MAFF クラウド上の開発環境で改めて行うこと。

（主な内容）

- 各テスト工程（単体テスト、結合テスト、総合テスト、運用テスト、受入テスト）のテ

スト方針及びテスト観点
- テスト項目（正常系テストに加え、例外テスト、境界テスト、限界値テスト、性能テスト等を行うこと。）
- 合否判定基準
- テストスケジュール（再試験も想定し、スケジュールを決定すること。）
- テスト実施体制（品質管理体制を含む。品質管理体制は、第三者による確認等、客観的な品質管理体制とすること。）
- テスト環境
- 第４期開発業務との連携テスト・品質管理指標項目と目標値・完了基準（管理ドキュメントとして、バグ管理図（信頼度成長曲線）や品質管理表等を作成すること。）
- テスト結果報告内容（試験密度と不良率などが確認できること。機能別/サブシステム別の試験項目数、不良数による目標値や自社の経験に基づく指標範囲内であるか等が確認できること。品質状況分析）
- 不具合の原因を分類整理し、類似の潜在不具合を潰すための横展開や品質強化のための追加試験実施等、品質強化の対応
- 繰り返しテストが出来るように自動化の対応

単体、結合テストは社内環境で行うこと。以下の性能テストは MAFF クラウド上の開発環境で行うこと。

・本番運用時と同程度の件数のテスト。
・業務上ピークを想定した負荷試験。
・農林水産省本省の会議室からレスポンスタイム確認。
・LGWAN 接続の疎通確認結果含む、接続テスト。

MAFF クラウド上でしか確認できない確認及び２章関連調達案件に記載の事業者との連携が必要なテストを行う場合は、それぞれに応じた環境を利用し、テストを行うこと。

試験成績書及び操作結果をテスト実施後速やかに担当者に提出すること。また、テスト結果について報告書を作成し、受注者は、テスト計画書に基づき、各テストの実施状況を担当者に報告すること。報告書にはテスト実施項目数や不具合検出率、検出した不具合の分析結果等を記載し、不具合が十分に検出されたことが分かる内容とすること。テストを実施する際は、システム利用者の環境とできる限り同じくするため、低スペックの端末を用いること。

検出した不具合を分析した結果又は担当者が報告書を確認した結果、ソフトウェアの品質を保つために十分なテストが実施されていないと判断した場合は、担当者と協議の上、対策を講じること。

総合テスト完了後、全テスト結果をとりまとめ品質報告書を作成し、担当者に説明し、承認を得ること。

ア　単体テスト

テスト実施計画書に基づき、開発した機能単体が設計書に基づいて動作することのテストを実施すること。また、テスト実施結果を担当者に報告し、担当者にテスト完了の判断を得ること。

イ　結合テスト

テスト実施計画書に基づき、開発した機能を組み上げてテストを実施すること。既存クラウドサービスを使用する場合は、必要な設定を行った上でテストを実施すること。テストを実施するに当たっては、正常系のテストに加え、異常系（誤ったデータの登録等）のテストを実施すること。また、テスト実施結果を担当者に報告し、担当者にテスト完了の判断を得ること。

ウ　総合テスト

テスト実施計画書に基づき、機能要件、非機能要件を満たすことをテストで確認するこ

と。開発した機能を組み上げてテストを実施すること。また、テスト実施結果を担当者に報告し、担当者にテスト完了の判断を得ること。

エ　運用テスト及び受入テスト

総合テスト完了後、担当者が動作確認のための運用テスト及び受入テストを実できるよう、システムデータ、テスト計画書、テストシナリオ、テスト仕様書兼報告書（案）を作成すること。担当者がテストを実施するに当たり、環境整備、運用等の支援を行うこと。テストはステージング環境で行う想定。質疑応答時間を設け、質疑があれば対応すること。日程は担当者の指示に従うこと。

(5) 第４期開発等業務との連携テスト

上記(4)のテストと並行して、第４期開発等業務との連携テストを実施すること。当該連携テストの実施にあたっては、第４期開発等業務の受注者と必要な調整を行いながら実施すること。疎通試験等のテストは平日時間外対応も想定されるため留意すること。

3.9 データ移行及びテスト

受注者は、3.5 に基づき、本システムにデータ移行を行うこと。なお、関連調達のシステムは令和８年度も運用を行うため、移行対象のデータも随時更新がされている。利用者含め協力してもらう範囲等を明確にし、関係者と合意形成の上、影響が出ないようデータ移行計画を作成すること。データ移行は利用者等に影響を出さないよう、留意すること。

また、移行データには個人情報が含まれている点にも留意すること。

3.10情報システムの移行

受注者は、担当者の移行判定を受けて、移行計画書に基づく移行作業を行うこと。

マスタ等データ移行の必要がある場合は、受注者はデータ移行に当たり、新規情報システムのデータ構造を明示し、保有・管理するデータの変換、移行要領の策定、例外データ等の処理方法等に関する手順書を作成し、担当者の承認を得ること。

受注者は、上記手順書に従い、データを変換・移行した後は、移行後のデータだけでなく、例外データ等についても確認を行い、データの信頼性の確保を図ること。

3.11運用保守

本システムは、令和８年４月より本稼働を開始する予定。MAFF クラウド環境で運用を行っている。本業務では、前年度の家畜疾病サーベイランス報告システム更改等業務（飼養衛生管理等支援システム）の受注事業者から MAFF クラウド上に構築された本システムの引継ぎを受け、アカウントの契約移管を行い、契約締結から契約期間満了まで環境を維持し、以下の業務を行うこと。

① MAFF クラウドの運用・保守（別紙１システム稼働環境、クラウドサービス一覧のクラウドサービスを含む。）

② 本システム及びサブシステムのアプリケーション保守

また、上記 3.5 で作成した設計書も踏まえ、開発したプログラム一式を利用するための役務を提供すること。なお、ここでいう役務とは、開発したプログラムを含めてシステムを適正に運用するための保守を含む。また、システムを運用するために必要となる運用保守マニュアル等を修正することとし、修正した運用保守マニュアル等は、運用期間中、適宜見直しを行い、今後の適切な運用保守に資するものにすること。

なお、契約締結までにアカウント譲渡が完了していない場合でも、契約締結日からの MAFF クラウド利用料は受注者が負担すること。

(1) 適正なシステムの運用

受注者は、以下の作業を飼養衛生管理支援システム（仮称）第１期開発業務及び飼養衛生管理等支援システム第３期開発及び運用等業務の納入・成果物、農林水産省クラウド利用ガイドラインを参照して要件確認の上実施し、内容及び成果物について、担当者の承認を得ること。

① 本システムを稼働するために必要な環境整備の準備及び方式の検証をすること。検証結果について、担当者の承認を得ること。
② 本システムを稼働させるために必要なアプリケーションが適正か確認すること。必要に応じて、既存の基本設計書、詳細設計書を修正し、担当者の承認を得ること。なお、導入するソフトウェアは十分なサポート期間があるものを選定し、MAFF クラウド CoE 及び MAFF クラウド事業者と調整を行った上で、導入を実施すること。
③ 本システムを稼働させる運用・保守は、運用設計書等に記載の内容を基に実施すること。
④ 本システムの稼働状況の監視、ソフトウェアの障害発生時対応、ソフトウェアの脆弱(ぜい)対応、２章関連調達案件に記載の受注事業者からの基盤に関する問合せ対応の受付・回答及びその他本システムの安定運用維持に関する業務を行うこと。
⑤ 定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用・保守実施計画書及び保守・保守実施要領を作成し、担当者の承認を得ること。承認されたドキュメントは第４期開発等業務でドキュメントをマージするため、第４期開発等業務へ適宜提供すること。

なお、運用・保守計画書及び運用・保守実施要領の記載内容は、標準ガイドライン「第９章　運用及び保守」で定義されている事項を踏まえたものとする。また、運用設計及び保守設計において MSP 等を活用とした設計とすることで運用コスト低減に努めること。

(2) 運用の実施

ア　受注者は、クラウドサービスの利用実績について、利用明細書の写し並びに月額の運用サービスの費用実績（Shared 型の MSP サービスを利用した場合）を含め、それらを一覧表にとりまとめ、担当者に提出すること。利用明細書の発行から５日以内に担当者へ提出することが望ましい。また、担当者の求めに応じ、クラウドサービスを含めた情報システムの構成を適切に見直すための資料（AWS Cost Explorer、AWS Trusted Advisor、AWS CUR 等の出力結果）を提出すること。

なお、Shared 型の MSP サービスの利用とは、以下の定義のいずれかとする。

受注者が自社で Shared 型の MSP サービスを提供している企業の場合はそれを利用すること。

・受注者が自社で Shared 型の MSP サービスを提供できない企業は、運用品質の均一化と不要なコストを削減するために外部企業が提供する MSP サービスを利用すること。
・受注者が自社で Shared 型の MSP サービスを提供できない企業において外部企業が提供する MSP サービスの利用ではなく、複数の運用案件を受注することで自社内の運用サービスの改善共通化（サービスデスク、監視サービス等）に取組んでいること。

イ　受注者は、ソフトウェアの情報をクラウドサービスの機能 SSM（AWS Systems Manager）を利用して取得し、出力結果を提出すること。

ウ　受注者は、構成管理及びパッチの適用について自動化すること。なお、自動化とは、対象を選定し、タイミングをコントロールして適用することをいう。

エ　受注者は、原則、メンテナンスの際に踏み台サーバを独自で構築せず、クラウドサービスプロバイダーのサービス AWS Systems Manager Session Manager ・AWS Systems Manager Fleet Manager を利用して運用すること。

オ　受注者は、基盤の設定変更があった場合はパラメータシートを更新し、担当者に提出すること。担当者の求めに応じ、クラウド構成を適切に見直すための資料（AWS Cost Explorer、AWS Trusted Advisor、AWS CUR 等の出力結果）を提出すること。

カ　ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、担当者にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること（本要件は、既存クラウドサービスに係るソフトウェア等に対して求めるものではなく、本システム向けに新たな環境を構築する場合に、これに係るソフトウェア製品に対して求めるものである）。

キ　受注者は、農林水産省クラウド利用ガイドライン別紙 1 共通機能_利用申請書を作成し、担当者と MAFF クラウド CoE の承認を得ること。プロジェクト期間中に利用申請書の内容が変更になった場合は、更新内容について、担当者と MAFF クラウド CoE へ説明し、承認を得ること。

ク　受注者は、インベントリ情報を収集するため、設定作業 Systems Manager Inventory と EC2 の設定を実施すること。

ケ　ソフトウェアにセキュリティの脆弱性が見つかった場合は、対応策について計画し、担当者の承認を得た上で対応すること。

コ　農林水産省をエンドカスタマー（エンドユーザー）として登録していることを証明する書面を提出すること。

①　環境整備等

受注者は MAFF クラウド環境で運用している本システムの稼働状況の監視及び必要な操作を原則、運用テスト計画を立案した上でテストを実施すること。開発テスト計画には、テスト体制と役割、詳細な作業とスケジュール、テスト環境、テストツール合否判定基準等に関する記述を含むこと。立案した計画はテスト実施前に担当者に説明し、内容について承認を得ること。

(3) 障害発生時の対応

受注者は、障害発生時（又は発生が見込まれる時）には、直ちに担当者に報告するとともに、その緊急度及び影響度を判断の上、運用要件に示す障害発生時運用業務（障害検知、障害発生箇所の切り分け、保守事業者への連絡、復旧確認、報告等）を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は運用作業計画及び運用実施要領に基づいて行うこと。

なお、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案すること。

また、大規模災害等の発生時には、担当者の指示を受けて、情報システム運用継続計画に基づく運用業務を実施すること。

情報システム運用継続計画は適宜更新（担当者の求めに応じた更新を含む。）を行い、そ

の都度担当者の承認を得ること。

(4) 運用支援・保守等作業

ア　受注者は、担当者が運用・保守計画書及び運用・保守実施要領を検討するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する情報提供をするとともに、運用・保守計画書及び運用・保守実施要領の案を作成し、担当者に提案すること（運用・保守計画書及び運用・保守実施要領の記載内容は、標準ガイドライン「第９章　運用及び保守」で定義されている事項を踏まえたものとする。）。

イ　アプリケーションの稼働が不測のシステムメンテナンスによって、毀損されないこと。

ウ　業務データ（紙媒体、電子媒体、MAFF クラウド環境内等）や、ログ等の証跡は、履行期間中は保存し、契約終了時までに適切に破棄し、担当者に報告すること。廃棄対象、方法、時期等は担当者に提案し、承認を得ること。担当者から業務データの提供依頼があれば対応すること。

エ　受注者は担当者の指示に従い、必要な調整を行うこと。保守案件の対応状況は、受注者が責任を持って管理すること。

オ　クラウドサービスに係るアップデート前後の動作試験

クラウドサービスに係るアップデート作業の適用後は、以下の表のシステム動作試験を行い、アップデート適用による不具合が発生していないことを確認すること。ただし、緊急性が高い内容は、即時対応を可能とすること。

アップデートの適用後のシステム動作試験の確認項目

確認事項	確認内容
Web アプリケーションの動作確認	Web アプリケーションにログインできることを確認する（ログイン画面に接続できることを確認する。）。

カ　運用保守等作業の改善提案

受注者は、担当者に対して各会議等を通じて当業務推進上で得られた知見を積極的に提供するとともに、改善案を提案し、担当者の承認を得た上で実施すること。また、年度末までに本業務で実施した運用保守等実績を取りまとめるとともに、必要に応じて運用計画や運用・保守作業手順書に対する改善提案を行い、担当者の承認を得ること。その際、運用・保守作業手順書も改訂すること。

なお、上記の改善提案に当たっては、パブリッククラウドの運用体制において、マネージドサービスプロバイダーが提供している共有型のクラウド運用・保守サービスの活用についても検討し整理することとする。検討した結果、MSP サービスの活用を運用・保守計画に組み込めた場合は、実際にサービス等の活用を開始すること。また、上記の改善提案に当たっては、クラウドサービスプロバイダーが提供する ベストプラクティス準拠状況を定期的に調査 Trusted Advisor し、検出項目の対応可否を検討し、担当者の承認の上、対応すること。クラウド構成のベストプラクティス（AWS Well-Architected フレームワークの全ての柱を活用し、年に 1 度システムが適切に運用されているかチェックし、次年度の改善点を整理すること。改善提案を作成したら担当者並びに PMO／MAFF クラウド CoE に報告すること。

キ　利用全般

担当者が本システムを利用する上で必要な運用保守（担当者からのシステム操作・仕様の

問合せ対応、マニュアル修正等）を行うこと。

3.12 教育

受注者は、本調達で構築したシステムの操作等に係るユーザ用マニュアルを作成すること。ユーザマニュアルは、設定されたユーザ種別毎に作成し、担当者の承認を得ること。

3.13次期事業者への引継ぎ

受注者は、設計・開発の設計書、作業経緯、残存課題等を文書化し、令和９年４月からシステムが円滑に運用できるよう、必要となるプログラム、データ、ドキュメント等を整理し、提出すること。

また、次年度の受注事業者に対し、以下の予定内容について対面で引継ぎを行い、受注事業者からの質問等に対しては、誠意をもって回答すること。

なお、下記の受注事業者は予定であり、実際に更改後のシステムを引継ぐ受注事業者に対し、引継ぎを行う必要があるため、留意すること。

① 令和９年度家畜疾病サーベイランス報告システム改修等業務(仮称)への引継ぎ

（予定内容）

・作業経緯、残存課題等を文書化し、構築内容等について説明を行うこと。

② 飼養衛生管理等支援システム第５期開発及び運用・支援保守等業務（仮称）への引継ぎ

・クラウド運用・保守を行うことを想定しているため、MAFF クラウド上に構築された情報システムの引継ぎを行い、システムの運用等を行うクラウド環境を原則としてそのまま引継ぐこと。そのため、引継ぎに際しては、必要に応じて次年度の事業者との間で書面による契約等を行い、管理者権限の引き渡し等、クラウド環境の引継ぎを適切に行うこと。なお、利用するクラウドサービスによっては、クラウドサービスプロバイダーとの契約についても、あらかじめ、第三者にクラウド環境を引き継ぐことが可能な形としておく必要があるため、利用するクラウドサービスを選定する際には、クラウド環境の引継ぎに遺漏がないよう、クラウドサービスプロバイダーとの契約内容や引継ぎ手順等を引継書として纏めておくこと。

・AWS アカウントの契約を移管すること。支払代行については、契約締結日分からを対象とすること。

・アプリケーションのシステム保守を行うことを想定しているため、ライセンス等の引継ぎがある場合は、引継ぎが可能なように準備し、引継ぐこと。

・作業経緯、残存課題等を文書化し、構築内容等について説明を行うこと。

引継ぎは令和９年３月中を予定している。令和９年３月中に次年度の受注事業者が決定しなかった場合は、担当者に引継ぐこと。

3.14 情報資産管理標準シートの提出

受注者は、次に掲げられた標準ガイドライン「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。なお、担当者から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した情報資産管理標準シートを提出すること。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。

(1) 契約締結後

・標準ガイドライン「別紙３ 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を記載

(2) 設計・開発実施要領において定める時期

・開発規模の管理 情報システムの開発規模（工数、ファンクションポイント等）の計画値及び実績値

・ハードウェアの管理：情報システムを構成するハードウェアの製品名、型番、ハードウェア分類、契約形態、保守期限等
・ソフトウェアの管理：情報システムを構成するソフトウェア製品の名称（エディションを含む。）、バージョン、ソフトウェア分類、契約形態、ライセンス形態、サポート期限等
・回線の管理 情報システムを構成する回線の回線種別、回線サービス名、事業者名、使用期間、ネットワーク帯域等
・外部サービスの管理：情報システムを構成するクラウドコンピューティングサービス等の外部サービスの外部サービス利用形態、使用期間等
・施設の管理：情報システムを構成するハードウェア等が設置され、又は情報システムの運用業務等に用いる区域を有する施設の施設形態、所在地、耐久性、ラック数、各区域に関する情報等
・公開ドメインの管理：情報システムが利用する公開ドメインの名称、DNS 名、有効期限等
・取扱情報の管理：情報システムが取り扱う情報について、データ・マスタ名、個人情報の有無、格付等
・情報セキュリティ要件の管理：情報システムの情報セキュリティ要件
・指標の管理：情報システムの運用及び保守の間、把握すべき KPI（Key Performance Indicator の略称で、「重要業績評価指数」を指す。）名、KPI の分類、計画値等の案
・各データの変更管理：情報システムの運用において、開発規模の管理、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目
・作業実績等の管理：情報システムの運用中に取りまとめた作業実績、リスク、課題及び障害事由

(3)　運用実施要領及び保守実施要領において定める時期

・各データの変更管理：情報システムの運用、保守において、開発規模の管理、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目
・作業実績等の管理：情報システムの運用、保守中に取りまとめた作業実績、リスク、課題及び障害事由

また、年１回、農林水産省の指示に基づき、情報システム資産管理データと情報システムの現況との突合・確認（以下、「現況確認」という。）を支援すること。

・受注者は、現況確認の結果、情報資産管理データと情報システムの現況との間の差異がみられる場合は、運用実施要領に定める変更管理方法に従い、差異を解消すること。
・受注者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上、担当者に報告すること。
・受注者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査の上、担当者に報告すること。

4 機能要件、非機能要件等に関する事項

本業務で開発するシステムに係る機能要件、非機能要件等に関する事項は別紙２「家畜疾病サーベイランス報告システム更改等業務に係る要件資料」のとおり。なお、本要件は、調達時の想定であることから、上記 3.4 により必要な要件を確認し、設計を確定すること。

5 成果物、納品方法等に関する事項

(1) 納入・成果物と納品方法

本業務の成果物を次の表に示す。

成果物と納品期日

こ項番	成果物名	納品期日
1	・設計・開発実施計画書及び設計・開発実施要領 ・運用作業計画及び運用実施要領 ・設計・開発実施要領に基づく管理資料（該当があれば）	○設計・開発実施計画書及び設計・開発実施要領…契約締結後５日以内 ○運用作業計画及び運用実施要領…運用開始２か月前を目途 ○他…キックオフ開催まで （最終：令和９年３月 31 日）
2	議事録	会議終了後５日以内 （最終：令和９年３月 31 日）
3	要件定義書	設計開始時迄 （最終：令和９年３月 31 日）
4	設計書（パラメータシート含む）	機能開発、基盤開発開始時まで （最終：令和９年３月 31 日）
5	テスト計画書	テスト開始時まで （最終：令和９年３月 31 日）
6	テスト仕様書兼報告書、受入テストのテスト仕様書兼報告書（案）	テスト開始時まで （最終：令和９年３月 31 日）
7	各テスト結果報告書	各テスト終了後、速やかに （最終：令和９年３月 31 日）
8	・品質報告書（脆弱性検査結果報告を含む） ・テストエビデンス等（操作結果の画面キャプチャ等のエビデンスを含む） ・各テストデータ	○品質報告書…テスト終了後、速やかに ○テストエビデンス等、各テストデータ…テスト終了後 10 日以内メド ※項番 6 の報告書も含めること。 ※各テストデータは受注者社内テストで使用したデータも含めること。 （最終：令和９年３月 31 日）
9	・移行計画書 ・移行手順書	移行開始時まで （最終：令和９年３月 31 日）
10	移行結果報告書	移行終了後、速やかに （最終：令和９年３月 31 日）
11	各マニュアル及びリリースノート	○開発環境リリース前まで ○リリースノートは各リリース日の１週間前まで （最終：令和９年３月 31 日）
12	進捗報告書	契約期間中、本番環境リリース前まで月２回程度開催（開催前日 12 時まで） （最終：令和９年３月 31 日）
13	月次運用作業報告書	運用期間中、毎月１回（固定曜日の第２回目前日 12 時まで） （最終：令和９年３月 31 日）
14	引継資料	引継開催２日前 10 時まで （最終：令和９年３月 31 日）

こ項番	成果物名	納品期日
15	情報資産管理標準シート	○契約締結後 ○設計・開発実施要領に定める時期 ○運用実施要領、保守実施要領に定める時期 （最終：令和９年３月 31 日）
16	ソースコード、実行プログラム、オブジェクト等一式 ※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使用する場合、設計書やソースコード一式の生成等に使用される設定情報その他の必要な情報一式	各リリース後速やかに （最終：令和９年３月 31 日）
17	関係事業者への対応状況をまとめた資料	（最終：令和９年３月 31 日）
18	本業務における作業実績工数（作業実施計画書で作成した内容の実績）	（最終：令和９年３月 31 日）
19	コーディング規約及びセキュアコーディング規約	機能開発、基盤開発開始時まで （最終：令和９年３月 31 日）
20	外部サービスを利用する場合、当該サービスに係る設定情報その他の必要な情報一式	（最終：令和９年３月 31 日）
21	障害報告書	障害発生時、速やかに （最終：令和９年３月 31 日）
22	農林水産省クラウド利用ガイドライン別紙１共通機能_利用申請書 ・システム構成図 ・IaC で構築した際に作成された定義ファイル（CloudFormation） ・EC2…パッチ適用設定ファイル(SSM patch manager ・それ以外…クラウドのセキュリティ実施対応状況（例　ECR スキャンの結果、Fargete のプラットフォームバージョン等システム構成に合わせて必要なファイルを納品すること。）	最終：令和９年３月 31 日 ※CloudFormation が対応していないサービスを使用するなどの理由で、CloudFormation 等を使用せずにシステムを構築する場合は、納品不可理由を記載すること。
23	クラウド環境一式（管理者権限等のアカウント情報を含むこと。なお、アカウント情報については、必要な情報を記載した「アカウント情報一覧」を準備した上で、担当者が指定する方法で納品すること。）	最終：令和９年３月 31 日
24	その他（本業務において対応した資料等）	適宜 （最終：令和９年３月 31 日）

(2) 納品方法

令和９年３月 31 日の最終納品の納入部数及び体裁については以下に基づくこと。以下の体裁に従うことが困難である場合は、事前に担当者に申告し、その指示に従うこと。

- 紙媒体：一式（ファイルに保存し、背表紙にファイルされているドキュメント名を記載すること。
- 電子媒体：３部（原則として、Microsoft Office 形式及び PDF 形式の両方）
- PMO 保存用電子媒体:２部（原則として、Microsoft Office 形式及び PDF 形式の両方。）
- 納入・成果物は全て日本語で作成すること。
- 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」の周知について（令和４年１月 11 日内閣文第１号内閣官房長官通知)」を参考にすること。
- 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。
- 納品後、担当者において改変が可能となるよう、図表等の元データも合せて納品すること。
- 納入・成果物の作成に当たって特別なツールを使用しないこと。
- 納入・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、納入・成果物の情報セキュリティの確保に留意すること。
- 資料を閉じるファイルの背表紙に「機密性２情報」、「省内限り」の文字を印字すること。
- 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。

なお、最終令和９年３月 31 日以外の納品時は電子媒体で担当者にメールで提出（容量の大きいデータは大容量転送システム等を利用すること。）すること。

電子データを格納する媒体の種類及びデータ形式は、担当者と協議して決定すること。また、納品媒体及びデータについては、ウイルス等悪意を持ったソフトウェアを混入させないように、提出までに受注者側で責任をもってチェックし、電子媒体で納品する際にはウイルス対策に関する情報（ウイルス対策ソフト名、ウイルス定義、チェック年月日）を記載したラベルを貼り付けること。

紙媒体でしか提出できないもの（手書き図面等）の提出方法については、担当者と協議して決定すること。

(3) 納品場所

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

〒100－8950
東京都千代田区霞が関 1-2-1
農林水産省消費・安全局動物衛生課（北別館６階ドア No.北 606）

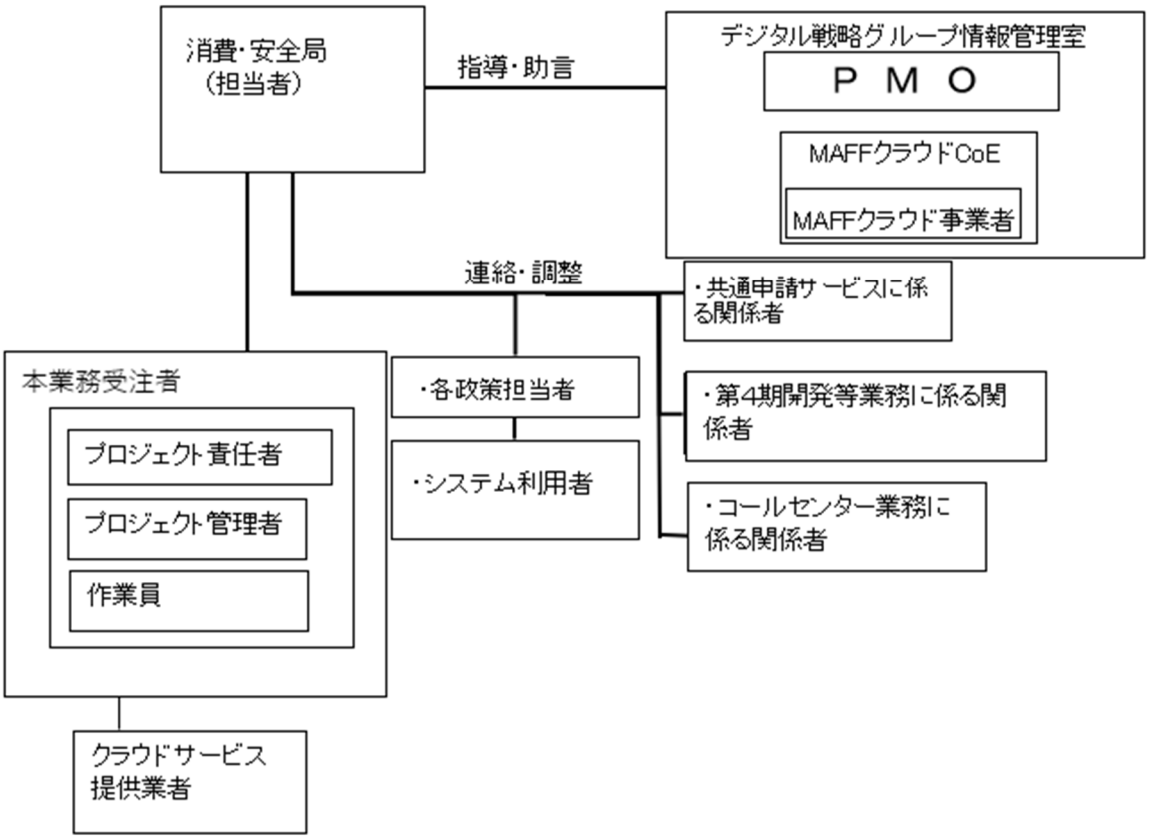
6 作業の実施体制・方法に関する事項

6.1 作業実施体制

プロジェクトの推進体制については、次のとおりである。

また、受注者内の体制については、想定により作成した体制図である。受注者は、業務内容と要件を踏まえ、必要な体制を提案すること。

なお、本業務においては、２章関連調達案件に記載している別途調達と業務的及びシステム的にも関係が密になると想定される。受注者においては、担当者のみならず、各事業者とも連携を密にし、作業を実施できる体制を準備すること。



本業務推進体制（想定）

役割分担

No	構成メンバ	役割・責任	受注者
1	プロジェクト責任者	本プロジェクトにおける統括責任者。作業実施計画、要員等プロジェクト遂行に必要な資源を確保することに責任をもつ。	○
2	プロジェクト全体管理者	本プロジェクトにおける管理者（PM）。マネジメント窓口。作業の進捗、リスク、課題管理に責任をもつ。	○
3	プロジェクト管理者	本プロジェクトにおける管理者（PL）。作業の進捗、課題管理に責任をもつ。	○
4	作業員	本調達における各業務を担当する。プロジェクト管理者が兼務しても良い。	○
5	担当者	管理組織として、本業務の進捗等を管理する。また、各種ドキュメントに対する承認を行う。	－
6	PMO	担当者からのシステム構築に関する相談対応を行う。また、進捗報告会等に出席し、本業務の実施に関する指導、助言を行う。農林水産省ITテクニカルアドバイザー（旧農林水産省CIO補佐官に相当）及びPMO支援スタッフが主に担当する。	－
7	MAFF クラウド CoE	担当者・受注者に対してクラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。	－
8	各政策担当者	農林水産省の本制度の制度設計をしている担当者。制度に係る要件、ロジック等を決定しており、要件定義時に現状の説明等を行う。担当者と連携し、担当者とともに要件確認、承認を行う。システム操作等を行う。	－

No	構成メンバ	役割・責任	受注者
9	システム利用者	都道府県及び家畜保健衛生所の職員、販売店、獣医師、生産者。システムの操作等を行う。	-
10	共通申請サービスに係る関係者	「農林水産省共通申請サービス（eMAFF）運用・保守業務」及び「農林水産省共通申請サービス（eMAFF）開発業務（仮称）」に係る担当者、事業者。本システムと共通申請サービスの連携に関する協議を行う。	-
11	コールセンター業務に係る関係者	現在、稼働している飼養衛生管理等支援システムの利用者である生産者からの問合せに回答等を行う。	-
12	第４期開発等業務に係る関係者	現在、稼働している飼養衛生管理等支援システムの基盤運用等及び第４期開発等業務を行う。	-

6.2 作業要員に求める資格等の要件

受注者は、本業務の遂行にあたり、本制度に関する知識・知見のあるもの、並びに業務ヒアリング・分析及び業務改善に関する知識・知見のあるものを確保すると共に、適切な作業体制を確保すること。業務遂行において、専門的かつ高度な知識に基づきながら、当省職員や関係先と、日本語により円滑かつ適切なコミュニケーションが図れること。

作業実施計画の作成、要員等プロジェクト遂行に必要な資源を確保するとともに、プロジェクト責任者として、プロジェクト体制の確立及び納期・品質などの管理を行うものを１名従事させること。プロジェクト責任者として、次の要件を全て満たすものの参画を必須とする。

- プロジェクトマネジメントの経験を５年以上有すること。
- 「情報処理の促進に関する法律」(昭和 45 年５月 22 日法律第 90 号)に基づく情報処理技術者試験の「プロジェクトマネージャ」又はプロジェクトマネジメント協会（PMI）が認定する「プロジェクトマネジメントプロフェッショナル（PMP)」の資格を有すること。

上記に加え、プロジェクト責任者の指揮・総括の下で実務を担い、作業状況を管理、監視するプロジェクト全体管理者として、以下の全要件を満たすものの参画を必須とする。

- 標準ガイドラインに基づくプロジェクト管理が実施できること。
- 情報処理業務の経験年数及びプロジェクトマネジメント経験を３年以上有すること。契約締結日において３年以上になることが望ましい。
- 複数のシステムとの連携を有する同等規模の情報システムの経験を有すること。
- コストメリットを追求できること。
- 十分なコミュニケーション能力を有すること。
- 高い業務品質を持ち、指摘された問題を改善する能力を有すること。
- 進捗報告会だけではなく、担当者との打合せに参加すること。

また、プロジェクト全体管理者の下で実務を担い、作業状況の管理、課題管理等をするプロジェクト管理者として、以下の全要件を満たすものの参画を必須とする。

- 標準ガイドラインに基づくプロジェクト管理が実施できること。
- 情報処理業務の経験年数及びプロジェクト管理経験を３年以上有すること。
- 複数のシステムとの連携を有する同等規模の情報システムの経験を有すること。
- コストメリットを追求できること。
- 十分なコミュニケーション能力を有すること（担当者からの連絡及び指示に迅速な対応ができるコミュニケーション能力を含む。)。
- 高い業務品質を持ち、指摘された問題を改善する能力を有すること。
- 幅広い技術知識を有すること。

加えて、作業員として、次の要件を満たすものの参画を必須とする。

- システム設計、プログラム開発、テストまでの一連のプロセスについて知識と経験を持ち、中核担当者としてシステム開発プロジェクトの遂行に携わった経験を有すること。
- 情報セキュリティ管理に関する以下又は相当する資格を有すること。

情報処理技術者試験　情報処理安全確保支援士（経済産業省)。

・十分なコミュニケーション能力を有すること。
・高い業務品質を持ち、指摘された問題を改善する能力を有すること。
・システム利用者の利便性、操作性の向上を常に追求できること。
・システム実現方式に係る適用技術や連携方式、データベース操作など、幅広い解決策の提案を行う能力を有すること。
・G-Net 経由の LGWAN 経由接続のシステムに関する知識と経験を有すること。
・共通申請サービス IdP 認証、アカウント管理等の知識を有すること。
・クラウド基盤の要件定義、設計開発等を担当するチームのチームリーダー及び担当メンバは以下の資格を有するものを含めること。（チームリーダーの資格は全体リーダーまたはクラウド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。）
チームリーダーは AWS の Professional、設計開発担当メンバは AWS の Associate。

なお、体制に前記の資格保有者を準備できない場合、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）を利用することで、クラウドの知見を有するものを配置する体制とすること。・運用・保守を行う担当者には、以下の資格のいずれかを有する者を１名以上配置すること。

AWS solutions architect associate もしくは AWS solutions architect professional
資格を有する人材を配置できない場合は、クラウド事業者の Solutions Architect（プリセールス SE）やクラウド事業者の Professional Services などの外部人材の支援を仰ぎ、その助言を真摯に受け止め実施すること。

・Salesforth の制約等、仕様を理解していること。

担当者と随時協議して、その指示に従い、誠実かつ確実に作業を遂行する体制を設けること。なお、担当者の指示以外では、原則として体制変更や提案書の傾注率を変更することは認めず、業務完了まで継続して続けられる者を本業務の作業従事者とすること。万が一交代する場合は担当者の事前承認を得た上で、同等以上の人物を確保すること。

受注者は、必要な資格要件を満たしている場合においても、要員の選定にあたって、以下の観点から、本業務の遂行に支障を生じさせないようにしなければならない。受注者側の体制について、本業務の実施に当たり、適切な遂行が期待できないと担当者が判断した場合は、受注者側の体制について、改善を要請するので対応すること。

・担当者と円滑な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
・担当者からの問合せ・指示等に適切な回答、対応をする能力
・本業務の実施にあたり、適切な執行を行う能力
・提案時の傾注率が守る能力（農林水産省の利益になる場合は除く）
・業務品質を保ち、受注者が指摘した問題を改善する能力
・担当する業務に応じた技術力（AWS のスキルを含む）

制度、運用の実施の都合上、スケジュール変更を要請する場合があるので対応すること。

ア　受注者の体制（要員の指名、役割、保有資格、業務履歴等を記載）
イ　受注者側の責任者
ウ　連絡体制（受注者側の対応窓口）

6.3 作業場所

本業務の遂行に必要な作業場所、備品、消耗品等の一切については、全て受注者の責任において用意すること。また、必要に応じて担当者が現地確認を実施することができるものとする。

なお、担当者との会議については、原則として農林水産省本省で実施する予定だが、会議室の確保が困難等の理由により、受注者のオフィス等で行うこともある。また、オンライン会議を依頼することも想定されるため、オンライン会議を実施する場合は、Microsoft Teams 会議の利用を基本とする。Cisco Webex 等の場合は、無償提供版は不可とし、法人サービス利用を原則とす

る。導入、接続に係る手続き等は一切を受注者が行うこととし、費用についても一切を負担すること。実施時に脆弱性が見つかった場合等の理由により、農林水産省として利用が不可となることも想定されるため、代替案も検討しておくこと。

6.4 作業の管理

受注者は、以下のとおり作業管理を実施すること。

- 担当者が承認した設計・開発実施計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、設計・開発実施要領に従い、コミュニケーション管理、体制管理、工程管理、品質管理、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。
- 農林水産省が定める運用実施要領に基づき、運用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。
- 進捗状況について、担当者からの照会があった場合は、速やかに回答すること。
- 本業務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、対応案を担当者と協議し、指示された期間までに是正を図ること。
- 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。

6.5 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

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受注者及び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。

農林水産省をエンドカスタマーとしてクラウドサービスの再販を行うこと。

また、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。

7 作業の実施に当たっての遵守事項

7.1 機密保持、資料の取扱い

(1) 機密保持、資料の取扱い

受注者は、以下のとおり機密保持、資料の取扱いを実施すること。

- 担当者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３月 31 日農林水産省訓令第４号。以下、「セキュリティ規則」という。）、「農林水産省における個人情報の適正な取扱いのための措置に関する訓令」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、「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。
- 本業務に係る情報セキュリティ要件は次のとおりである。

ア 受注した業務以外の目的で利用しないこと
イ 業務上知り得た情報について第三者への開示や漏えいをしないこと
ウ 持出しを禁止すること
エ 受注者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと
オ 業務の履行中に受け取った情報の管理、業務終了後の返却又は抹消等を行い復元不可能な状態にすること
カ 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

・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。

(2) 個人情報の取扱い

ア 個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の取扱いに係る事項について担当者と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。
(ｱ) 個人情報取扱責任者が情報管理責任者と異なる場合には、個人情報取扱責任者等の管理体制
(ｲ) 個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等）

イ 本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。なお、受注者はその旨を証明する書類（農林水産省宛の派遣労働者の誓約を含む。）を提出し、担当者の了承を得たうえで実施すること。

ウ 個人情報を複製する際には、事前に担当職員の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。なお、受注者は廃棄作業が適切に行われた事を確認し、その保証をすること。

エ 受注者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当職員に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。
また、当該情報等を本業務以外の目的に使用又は第三者に開示してはならない。請負者（法人である場合にあっては、その役員並びにその職員その他の本業務に従事している者及び従事していた者）は、業務上知り得た秘密を漏らし、又は盗用してはならない。これらの者が秘密を漏らし、又は盗用した場合には、行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 57 号）第 171 条及び第 175 条により罰則の適用がある。

オ 個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする

カ 受注者は、農林水産省からの指示に基づき、個人情報の取扱いに関して原則として年１回以上の実地検査を受け入れること。なお、やむを得ない理由により実地検査の受入れが困難である場合は、書面検査を受け入れること。また、個人情報の取扱いに係る業務を再請負する場合は、受注者（必要に応じ農林水産省）は、原則として年１回以上の再請負先への実地検査を行うこととし、やむを得ない理由により実地検査の実施が困難である場合は、書面検

査を行うこと。

キ　個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

(3) その他文書、標準への準拠

受注者は、以下のとおり、取扱いを実施すること。

- 本業務の遂行に当たっては、担当者が定めるプロジェクト計画書及びプロジェクト管理要領との整合を確保して行うこと。
- 開発に当たっては、「飼養衛生管理等支援システムコーディング規約」に準拠して作業を行うこと。
- 提供するアプリケーション・コンテンツに不正プログラムを含めないこと。
- 提供するアプリケーションに脆弱性を含めないこと。
- 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
- 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。
- 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。
- サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。
- 「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。なお、ドメインを新規に導入する場合又はドメインを変更等する場合は、担当者から農林水産省ドメイン管理マニュアルの説明を受けるとともに、それに基づき必要な作業を行うこと。
- 詳細については、担当者から「アプリケーション・コンテンツの作成及び提供に関する規程」の説明を受けるとともに、それに基づきアプリケーション・コンテンツの作成及び提供を行うこと。

(4) セキュリティ要件

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に基づき、以下の内容について対応すること。

- ①不正アクセス等の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを、ファイアウォールにより DMZ を構築するなどして分離すること。
- ②不正アクセス等の通信回線を介した不正を防止するため、ファイアウォール等による通信制御、サーバ装置の不要な通信プロトコルを停止するなどして、外部とサーバ装置との通信及びサーバ装置間の通信を必要な通信のみに制限すること。
- ③不正行為の検知、発生原因の特定に用いるために、ウェブサイトの利用記録、例外的事象の発生に関するログを蓄積し、過去 12 か月分のログを保管すること
- ④ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること
- ⑤情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析

等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
- ⑥不正行為に迅速に対処するため、通信回線を介して所属する農林水産省外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。
- ⑦特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。
- ⑧情報の漏えいを防止するため、入退室管理、施錠可能なサーバラックの採用、通信ケーブル及び通信回線装置の物理的保護（床下への埋設等）等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。
- ⑨物理的な手段によるセキュリティ侵害に対抗するため、ウェブサイトの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。
- ⑩情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、ハードウェア、ソフトウェア及びサービス構成に関する詳細情報が記載された文書を提出するとともに、文書どおりの構成とすること。
- ⑪農林水産省が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。当該品質保証体制を証明する書類（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）を提出すること。
- ⑫アクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。
- クラウドアーキテクトのベストプラクティス（AWS の場合 AWS Well-Architected Framework、Azure の場合 Azure Well-Architected Framework）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。

7.2 遵守する法令等

受注者は、本業務の実施に当たっては、以下の法令等を確認、履行すること。実績等の証明提出及び報告は不要。

(1) 受注者は、著作権法（昭和 45 年 5 月 6 日法律第 48 号)、不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）等の関係法規を遵守すること。

(2)本業務の遂行に当たっては、標準ガイドラインに該当する以下のアからカに基づくこと。また、具体的な作業内容及び手順等については、解説書参考とすること。なお、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。

ア　DS-100 デジタル・ガバメント推進標準ガイドライン
イ　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
ウ　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
エ　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
オ　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
カ　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

(3)関係法令の遵守

受注者は、役務の提供に当たり、関連する環境関係法令を遵守するものとする。
- 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）
- 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）
- 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） 等

(4) 受注者は、役務の提供に当たり、新たな環境負荷を与えることにならないよう、業務の最終報告時に別紙５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～ウの各項目について、一つ以上「実施した／努めた」にチェックを入れること。

ア　環境負荷低減に配慮したものを調達するよう努める。

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。

ウ　みどりの食料システム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。

(5)本業務の遂行に当たっては、「農林水産省クラウド利用ガイドライン」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、「農林水産省クラウド利用ガイドラインの関係資料」を参考とすること。なお、農林水産省クラウド利用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。

(6)本業務の遂行に当たっては、「農林水産省データマネジメント・データ活用基本方針書（令和５年 10 月）」に基づくこと。

8 成果物の取扱いに関する事項

8.1 知的財産権の帰属

(1)本業務における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にて権利譲渡不可能と示されたもの以外は、全て農林水産省に帰属するものとする。

(2)受注者又は第三者に帰属する知的財産権を用いて成果物を作成（情報システムの構築等を含む。）する場合、当該知的財産権の利用における制約等を担当者に説明するとともに、WEB サイトのコンテンツ利用規約にその内容を記載する等によりシステム利用者が意図せず知的財産権を侵害することがないよう、必要な措置を講じること。

(3)農林水産省は、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、複製等により農林水産省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。

(4)本調達に係る成果物の権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、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農林水産省に移転するものとする。

(5)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農林水産省の承認を得ることとし、農林水産省は、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農林水産省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、農林水産省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。

(6)受注者は農林水産省に対し、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。

(7)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。

8.2 契約不適合責任の条件

契約不適合責任の条件は、以下のとおり。

・農林水産省は検収（「検査」と同義。以下同じ。）完了後、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。
・前号の場合において、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。
・前号の規程にかかわらず、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。
・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。
・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。
・前各号までの規定にかかわらず、成果物の種類又は品質に関して契約不適合責任がある場合であって、農林水産省が検収完了後１年以内に農林水産省から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、検収完了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はこの限りでない。
・検収によって農林水産省が当該契約不適合を発見することがその性質上合理的に期待できない場合、前各号までの規程を適用しない。ただし、この場合にあっても受注者が本条に定める責任その他の契約不適合責任を負うのは、検収完了後、２年以内に農林水産省から当該不

適合を通知された場合に限るものとする。
・前各号までの規定にかかわらず、契約不適合が農林水産省の提供した資料等又は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。

8.3 検収

本業務の受注者は、納入・成果物等について、納品期日までに担当者へ内容の説明を実施し、検収を受けること。なお、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、直ちに必要な修正等を行い、変更点について担当者への説明を行った上で、指定された日時までに再度納品すること。

9 入札参加資格に関する事項

本業務に対する応札希望者は、提案書を作成すること。詳細は、入札説明書及び提案書作成要領に定める。

9.1 入札参加要件

以下の要件を満たしていることの証明書を提出すること（提出期限は、入札説明書を参照すること。）。なお、(4)の証明は除くものとする。

(1) 公的な資格や認証等の取得

当案件を確実に遂行するため、応札者は次の条件を満たしていることを証明すること。再請負先も同様とする。

- 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。または、これ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、品質管理手順規程等を提出すること。）。
- 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保証する者として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。
- 業務遂行において、専門的かつ高度な知識に基づきながら、担当者や関係先と、日本語により円滑かつ適切なコミュニケーションが図られること。数字は算用数字、単位は原則としてメートル法とすること。
- 応札者は以下のア又はイのいずれかの条件を満たすこと。
  ア　クラウドサービスプロバイダーから代理店の認定を受け、かつ AWS Solution Provider Program（SPP）の登録を受けていること。加えて、本案件の関係者が、日本国内のクラウドサービスプロバイダーから日本語で契約や技術に関するサポートを受けられる商流であること。
  イ　国内企業のディストリビュータ経由でクラウドサービスの再販が可能であること。

(2) 受注実績

当案件を確実に遂行するため、応札者は中央省庁または民間企業等において、次の条件を満た

していることを、具体的な事例を挙げ、契約書の写し等（一部、マスキング可）を提出し、証明すること。ただし、情報システムの受注者から請負、委任、代理又は下請けされたものである場合は、実績には含まない。

- 複数のシステムとの連携を有する同等規模の情報システムにおいて、構築業務（改修含む）を履行した実績を過去３年以内に有すること。
- 拠点数２以上の接続を利用した web システムの要件定義から基本設計、詳細設計、プログラムの開発、テストまでの作業の全体を一括して行った実績（改修含む）を、過去３年以内に少なくとも１年以上有していること。
- 応札者は、本システムで利用中のパブリッククラウドにおいて、運用・保守を行った実績を過去３年以内に有すること。

(3) 複数事業者による共同入札

単独で対象業務を行えない場合は、適正な業務を遂行できる共同事業体（対象業務を共同して行うことを目的として複数の民間事業者により構成される組織をいう。以下同じ。）として参加することができる。

その場合、証明書等の提出時までに共同事業体を構成し、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とし、他の者は構成員として参加するものとする。ただし、共同事業体として参加する者については、他の共同事業体又は単独で本入札に参加することはできない。

共同事業体として本入札に参加する場合は、以下の要件を満たすこと。

- 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。
- 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。
- 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。
- 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。

(4) 資料閲覧

11.2に記載する資料閲覧をした上で、本制度に関する機能、リスク等を十分理解すること。なお、ドキュメント量が多いため、資料閲覧の時間及び体制に留意すること。

9.2 入札制限

(1) 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。

(2) 6.4 で示した監査対応のため、本業務の履行は全て日本国内作業で完結すること。共同事業体及び再請負先も同様とする。

10 再請負に関する事項

本業務の難易度、品質確保の観点から再請負は禁止とする。

11 その他特記事項

11.1 前提条件等

本業務受注後に調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって農林水産省に申し入れを行うこと。

11.2 入札公告期間中の資料閲覧等

入札公告期間中（行政機関の休日を含まない）に、資料閲覧を希望する場合は担当者に連絡すること。担当者が指示する日時及び場所において、閲覧することができる。閲覧時間及び連絡時間は 10:00～17:00（12:00～13:00 を除く）とする。また、閲覧申請書等を担当者へ閲覧日に提出すること。なお、担当者が必要な調整を行うことがある。

(1) 資料閲覧場所
東京都千代田区霞が関 1-2-1　農林水産省内

(2) 閲覧手続
応札希望者の商号、連絡先、閲覧希望者氏名を別紙６「閲覧申請書」に希望予定者を記載の上、閲覧希望日の２日前までに提出すること。また、閲覧日当日までに別紙７「機密保持誓約書」に記載の上、提出すること。

(3) 閲覧時の注意
閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

(4) 連絡先：農林水産省消費・安全局動物衛生課
担　当：中越、後藤
電　話：03-6744-7144

(5) 閲覧資料
閲覧に供する資料の例を次に示す。

ア　飼養衛生管理支援システム（仮称）第１期開発業務納入・成果物
イ　令和５年度飼養衛生管理支援システム要件定義書作成等業務納入・成果物
ウ　飼養衛生管理等支援システム第２期開発及び運用等業務納入・成果物
エ　家畜疾病サーベイランス報告システム更改等業務（飼養衛生管理等支援システム）
オ　プロジェクト計画書、プロジェクト管理要領
カ　遵守すべき各府省独自の規定類
(ア)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
(イ)農林水産省における個人情報の適正な取扱いのための措置に関する訓令
(ウ)農林水産省クラウド利用ガイドライン及び関係資料
キ　共通申請サービスにおける飼養衛生管理等機能に係るドキュメント一式等（設計書、操作説明書等）
ク　本制度に係る要綱、事務処理マニュアル
ケ　本制度に係る各種調査結果資料
(ア)令和３年度飼養衛生管理情報通信整備委託事業納入・成果物
(イ)令和４年度飼養衛生管理情報通信整備委託事業（畜産衛生情報のデジタル化に向けた畜産衛生業務の最適化調査及び飼養衛生管理支援システム（仮称）要件定義書作成等事業）納入・成果物
(ウ)令和６年度飼養衛生管理等支援システム開発に係る調査及び動物用医薬品に係る調

査等業務納入・成果物

11.3 その他

(1)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。
(2)本調達仕様書について疑義等がある場合は、質問書により質問すること。なお、質問書に対する回答は適宜行うこととする。
(3) MAFF クラウドについて不明点等がある場合は、担当者及びMAFF クラウドCoE と協議の上、作業を進めること。
(4) MAFF クラウドCoE からクラウドのシステム構成について、改善点の指摘を受けた場合に協議の上、対応を行うこと。また、MAFF クラウドCoE が監査・指導の観点でクラウド環境の確認が必要と判断した際には、要請に基づき、リードオンリーの IAM ユーザーを払い出すこと。

12　付属文書

付属文書は下記のとおり。
・別紙１　システム稼働環境、クラウドサービス一覧
・別紙２　家畜疾病サーベイランス報告システム拡充等業務に係る要件資料
・別紙３　情報システムの経費区分
・別４　情報セキュリティの確保に関する共通基本仕様
　別添１　情報セキュリティ対応状況・確認書
　別添２　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
・別紙５　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
・別紙６　閲覧申請書
・別紙７　機密保持誓約書
・別紙８　品質管理要件

飼養衛生管理等支援システムで利用されるネットワークの図を以下に示す。

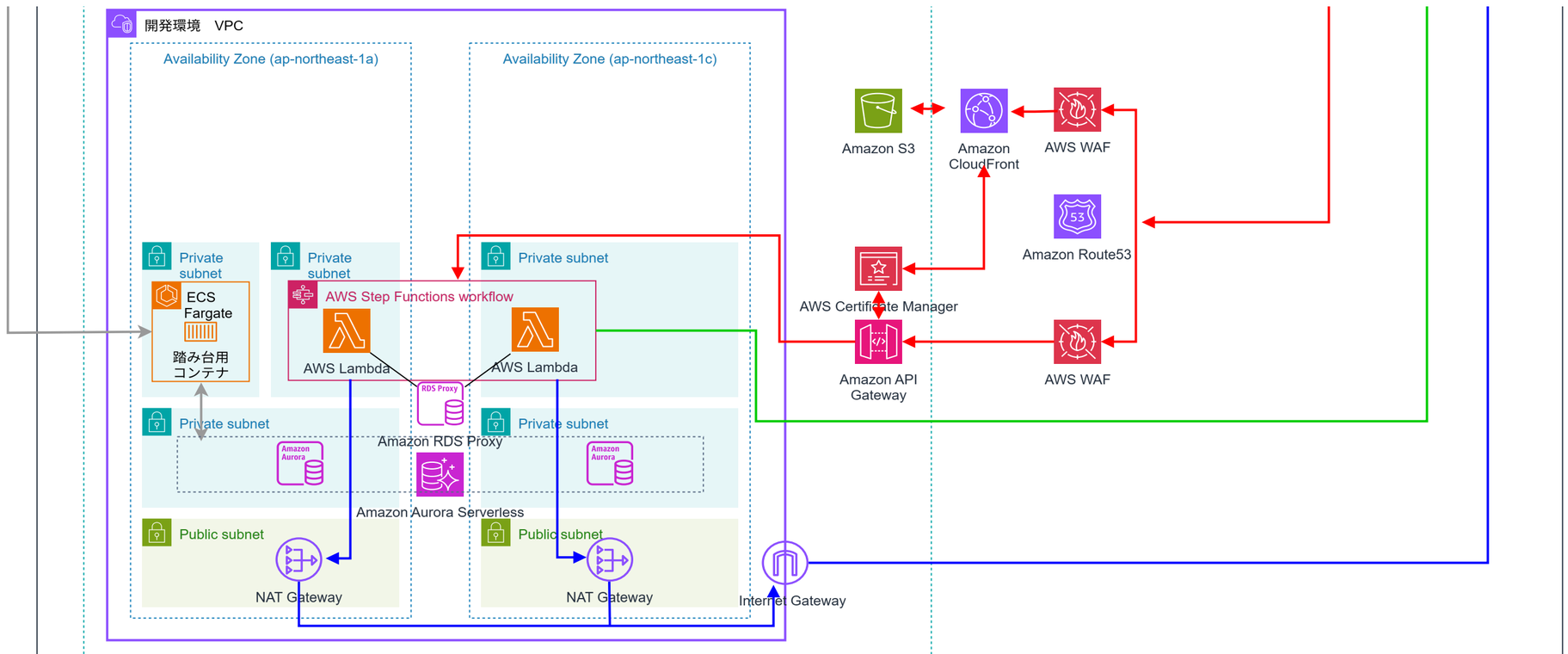
新家畜疾病サーベイランス報告システム

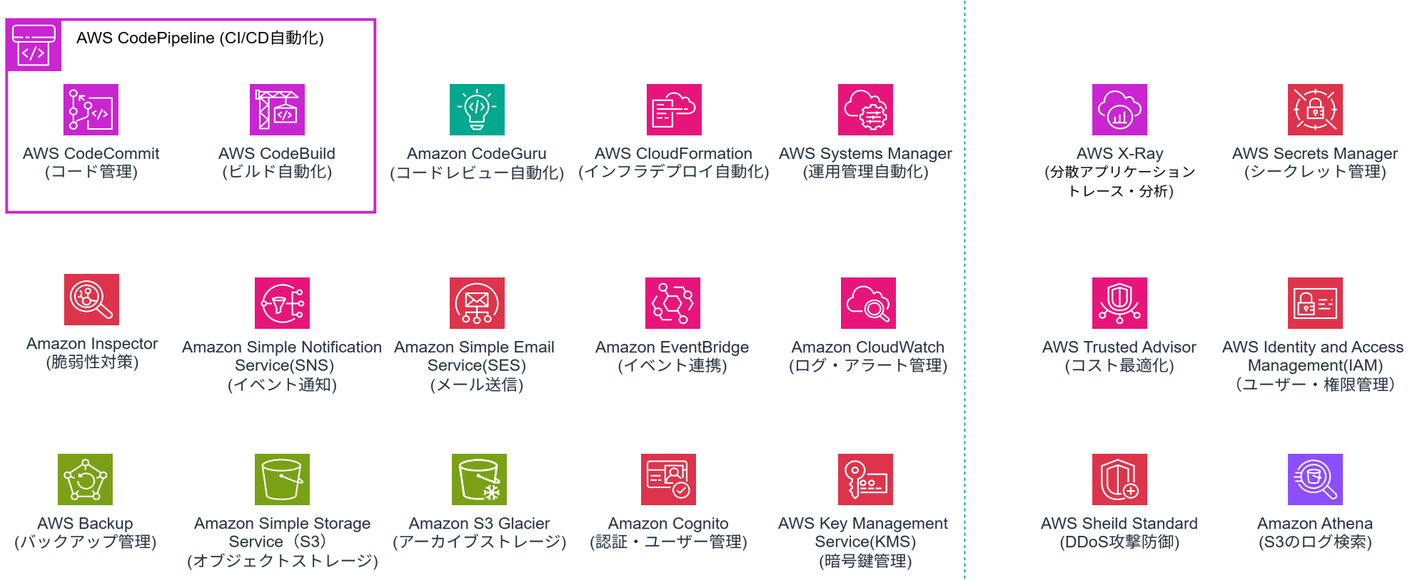
別紙1

凡例
- LGWAN経由のアクセス
- インターネット経由のアクセス
- 両方からのアクセス
- アウトバウンド通信
- 第３期開発システムとの連携経路
- 監査ログ機能
- 構成管理

※連携対象のDBのみ記載し他リソースは省略しています。

家畜保健衛生所職員
都道府県職員
農林水産省職員
農研機構
家畜保健衛生所職員
都道府県職員
LGWAN
GSS
インターネット
Direct Connect
第３期開発システムアカウント
東京リージョン
VPC
Amazon Aurora
管理者アカウント
東京リージョン
AWS Security Hub
Amazon GuardDuty
AWS Config
Amazon S3
Transit Gateway
GSSアカウント
Direct Connect Gateway
家畜疾病サーベイランス報告システムアカウント
東京リージョン
AWS Security Hub
Amazon GuardDuty
AWS Config
VPC Flow Logs
AWS CloudTrail
本番環境　VPC
Availability Zone (ap-northeast-1a)
Availability Zone (ap-northeast-1c)
Private subnet
NLB
LGWANユーザー用
ALB
LGWANユーザー用
VPC Endpoint
Amazon S3
Amazon CloudFront
AWS WAF
VPC Endpoint
Amazon API Gateway
Amazon Route53
AWS Certificate Manager
Amazon API Gateway
AWS WAF
運用保守事業者
Session Manager
ECS Fargate
踏み台用コンテナ
AWS Step Functions workflow
AWS Lambda
AWS Lambda
RDS Proxy
Amazon RDS Proxy
Amazon Aurora Serverless
Internet Gateway
Public subnet
NAT Gateway
NAT Gateway
ステージング環境　VPC
Availability Zone (ap-northeast-1a)
Availability Zone (ap-northeast-1c)
NLB
LGWANユーザー用
ALB
LGWANユーザー用
VPC Endpoint
Amazon S3
Amazon CloudFront
AWS WAF
VPC Endpoint
Amazon API Gateway
Amazon Route53
AWS Certificate Manager
Amazon API Gateway
AWS WAF
ECS Fargate
踏み台用コンテナ
AWS Step Functions workflow
AWS Lambda
AWS Lambda
RDS Proxy
Amazon RDS Proxy
Amazon Aurora Serverless
Internet Gateway
NAT Gateway
NAT Gateway
インターネット
eMAFF
共通申請サービス


開発環境　VPC
Availability Zone (ap-northeast-1a)
Availability Zone (ap-northeast-1c)
Private subnet
ECS Fargate
踏み台用コンテナ
Private subnet
AWS Step Functions workflow
AWS Lambda
Private subnet
AWS Lambda
RDS Proxy
Amazon RDS Proxy
Private subnet
Amazon Aurora
Private subnet
Amazon Aurora
Amazon Aurora Serverless
Public subnet
NAT Gateway
Public subnet
NAT Gateway
Internet Gateway
Amazon S3
Amazon CloudFront
AWS WAF
Amazon Route53
AWS Certificate Manager
Amazon API Gateway
AWS WAF


AWS CodePipeline (CI/CD自動化)
AWS CodeCommit (コード管理)
AWS CodeBuild (ビルド自動化)
Amazon CodeGuru (コードレビュー自動化)
AWS CloudFormation (インフラデプロイ自動化)
AWS Systems Manager (運用管理自動化)
AWS X-Ray (分散アプリケーショントレース・分析)
AWS Secrets Manager (シークレット管理)
Amazon Inspector (脆弱性対策)
Amazon Simple Notification Service(SNS) (イベント通知)
Amazon Simple Email Service(SES) (メール送信)
Amazon EventBridge (イベント連携)
Amazon CloudWatch (ログ・アラート管理)
AWS Trusted Advisor (コスト最適化)
AWS Identity and Access Management(IAM) (ユーザー・権限管理)
AWS Backup (バックアップ管理)
Amazon Simple Storage Service（S3） (オブジェクトストレージ)
Amazon S3 Glacier (アーカイブストレージ)
Amazon Cognito (認証・ユーザー管理)
AWS Key Management Service(KMS) (暗号鍵管理)
AWS Sheild Standard (DDoS攻撃防御)
Amazon Athena (S3のログ検索)

サーベイランス業務クラウドサービス一覧（令和7年8月時点）

No.	区分	サービス名称	利用目的	備考
1	権限管理	AWS Identity and Access Management (IAM)	正当なアクセスのみが許可されるよう、最小特権の原則に基づいた制御を実装するために使用	
2	仮想ネットワーク	Amazon Virtual Private Cloud (VPC)	仮想ネットワーク環境を構築し、可用性と拡張性に優れたシステムを実現するために使用	
3		VPC Flow Logs	VPC 内のネットワークトラフィックを記録し、セキュリティ監査、通信トラブルの調査、アクセス制御の検証に活用するために使用	
4		VPC Endpoint	VPC 内からS3 やAPI Gateway などのAWS サービスに対して、インターネットを経由せずにセキュアにアクセスするために使用	
5	ロードバランサー	Network Load Balancer (NLB)	IPアドレスを固定化し、外部システムとの通信を安定化させるために使用	NLBはElastic Load Balancing (ELB) の一部
6		Application Load Balancer (ALB)	アプリケーションサービスへのルーティングを行うために使用	ALBはElastic Load Balancing (ELB) の一部
7	DNS	Amazon Route 53	可用性と拡張性に優れたドメインネームシステム (DNS) ウェブサービスを実現するために使用	
8	API 管理	Amazon API Gateway	API の作成及び管理を行うために使用	
9	Web サーバ／キャッシュサーバ	Amazon CloudFront	Web ページを公開するために使用	
10	アプリケーション保存／業務ログ管理	Amazon Simple Storage Service (S3)	アプリケーションの静的アセット（HTML、CSS、JavaScript ファイルなど）を保存するため、取得したログを保管するために使用	
11	プログラム実行環境	AWS Lambda	業務コードを実行するために使用	
12	バックアップ	AWS Backup	Amazon Aurora や S3 のデータの自動バックアップを管理するために使用	
13	クラウド証跡管理	AWS CloudTrail	クラウドサービスに対する操作ログを取得・保管を行うことで不正アクセスや内部犯行を追跡するために使用	
14	リソース変更管理	AWS Config	リソースのインベントリ、構成履歴、構成変更通知を行うために使用	
15	DDos 対策／不正アクセス対策	AWS Web Application Firewall (WAF)	アプリケーション層での攻撃の特定と、不正アクセスを遮断するために使用	

No.	区分	サービス名称	利用目的	備考
16	リモートメンテナンス／パッチ適用	AWS Systems Manager	Session Manager 機能を用いて、IAM 認証が行われたアカウントからサーバへの接続を行うために使用 Parameter Store 機能を用いて、アプリケーションやインフラ構成で使用するパラメータを安全かつ一元的に管理するために使用	
17	証明書管理	AWS Certificate Manager	SSL/TLS証明書の発行や更新を行うために使用	
18	監視	Amazon CloudWatch	リソース監視、ログ監視等のシステム監視を行うために使用	
19	通知	Amazon Simple Notification Service (SNS)	システム管理者への通知メールを送信するために使用	
20	開発ツール	AWS CodeCommit	ソースコードや構成ファイルなどを安全にバージョン管理するための Git ベースのリポジトリサービスとして使用	
21		AWS CodeBuild	ソースコードのビルド、テスト、パッケージ化を自動化するために使用	
22		Amazon CodeGuru Security	アプリケーションコードに対して静的解析を行い、脆弱性を検出し、修正方法の提案を通じてセキュリティ品質を向上させるために使用	
23		AWS CodePipeline	ソースコードの変更をトリガーにして、ビルド・テスト・デプロイの各ステップを自動化する CI/CD パイプラインを構築するために使用	
24	データベース	Amazon Aurora PostgreSQL-Compatible DB (Aurora Serverless v2)	データベース「PostgreSQL」を利用するために使用	
25		Amazon RDS Proxy	アプリケーションと Aurora 間の接続を中継し、接続プールによる効率化と、瞬間的な接続数の増加に対する耐性を向上させるために使用	
26	認証情報の管理	AWS Secrets Manager	データベースの接続情報などの認証情報を管理するために使用	
27	暗号化キー管理	AWS Key Management Service (KMS)	暗号化キーを一元管理するために使用	
28	通知	Amazon EventBridge	定期的なバッチ処理を実行するために、Lambda や Step Functions などの処理をスケジュールに基づいて自動的にトリガーする目的で使用	
29	プログラム実行環境	Amazon Step Functions	複数の AWS サービス（Lambda、Aurora など）を組み合わせた処理をステップ単位で定義し、順序制御・分岐・エラー処理などを含むバッチ処理や業務フローを自動化するために使用	
30	不正挙動監視／改ざん検知	Amazon GuardDuty	AWS アカウント内の脅威を継続的にモニタリングし、異常な API 呼び出しや不審なネットワークアクティビティを検出することで、セキュリティインシデントの早期発見と対応を支援するために使用	
31	セキュリティ管理	AWS Security Hub	AWS のセキュリティチェックの自動化とセキュリティアラートの一元化を行うために使用	

No.	区分	サービス名称	利用目的	備考
32	環境管理	AWS CloudFormation	アプリケーションのリソースをテンプレート化して管理するために使用	
33	通信	AWS Direct Connect	AWS とオンプレミス環境とのプライベート接続（専用接続）を実現するために使用	
34	DDos 対策	AWS Shield Standard	アプリケーションを DDoS 攻撃から保護するために使用	
35	認証	Amazon Cognito	ユーザのサインアップ及びサインイン機能を追加するために使用	
36	コンテナ	Amazon ECS (Fargate)	データベースへのアクセスを行うための踏み台としてセキュアなアクセスを実現するために使用	
37	E メール送信	Amazon Simple Email Service (SES)	ユーザへの通知メールを送信するために使用	
38	ネットワーキング	Transit Gateway	本システムの VPC を eMAFF・LGWAN 等の環境と相互接続させるのに使用	
39		Network Address Translation (NAT) Gateway	VPC 内のプライベートサブネット内に配置されたリソースをインターネットに接続する際に外部からの直接アクセスは遮断し、セキュアなアウトバウンド通信を実現するために使用	
40		Internet Gateway	パブリックサブネット内のリソースがインターネットと通信できるようにするために使用	
41	運用支援	AWS Trusted Advisor	AWS 環境のコスト、セキュリティ、パフォーマンス、耐障害性、サービス制限などを自動チェックし、ベストプラクティスに基づいた改善提案を得るために使用	
42	アナリティクス	Amazon Athena	S3 に保存されたログデータに対して SQL を用いた検索・分析を行うために使用	
43		AWS X-Ray	アプリケーションの分散トレーシングを行い、リクエストの流れや処理時間を可視化することで、パフォーマンスのボトルネックやエラーの原因を特定するために使用	
44	脆弱性対策	Amazon Inspector	Lambda に対して自動的に脆弱性スキャンを実行し、セキュリティリスクを早期に検出・可視化するために使用	
45	コスト管理	AWS Cost Explorer	AWS リソースの利用状況とコストを可視化し、サービス別・期間別の費用分析を行うことで、コスト最適化や予算管理に活用するために使用	
46		AWS Cost Anomaly Detection	AWS 利用料金における異常な増加や予期しないコスト変動を自動的に検出し、通知することで、早期に対応しコストの無駄を防止するために使用	

別紙２

家畜疾病サーベイランス報告システム拡充等業務（飼養衛生管理等支援システム）に係る要件資料

第 1.0 版

目次

1. リリース時期及び開発（改修）概要

1.1. リリース時期

本番環境のリリース時期は以下のとおり。機能ごとに実装期限が異なる。
ステージンク環境及び開発環境は、本番環境リリースに影響が出ない時期とすること。

本番環境リリース　令和9年3月中旬頃

・上記実装期限までにリリースが困難な一部機能は、担当部者と協議の上、実装日を変更することは可能とするが、利用者の業務へ影響が出ないことを条件とする。
・上記に関連する内容は、当該システム及び関連機能も業務が問題なく運用できるよう調査し、併せて改修すること。ただし、当該システムへの影響が最小限となるように実装する要件の調整を優先とする。
・開発（改修）目的を把握した上で、開発（改修）目的に沿った形で開発（改修）仕様を実現すること。

1.2. 開発（改修）概要

	内容
要件1 過去年度対応	旧システムから過去年度のデータ移行に伴う、集計機能等の開発等、以下の対応を行うこと。 （1）過去年度機能の開発 ・旧家畜疾病サーベイランス報告システム及び共通申請サービスから過去年度分のデータ移行を行った際に、CSV 出力や集計等、過去年度の運用に必要な操作ができるように開発すること。 ・過去年度の制度ロジックを踏襲する必要があるため、旧家畜疾病サーベイランス報告システムと同値結果になるよう、対応すること。 （2）過去年度のデータ移行 ・旧家畜疾病サーベイランス報告システムでは、更改後の家畜疾病サーベイランス報告システムと異なるデータ管理を行っているため、更改後の家畜疾病サーベイランス報告システムでも運用に必要な情報のシステム管理が行えるよう、データクレンジングを行うこと。 ・共通申請サービスでは、更改後の家畜疾病サーベイランス報告システムとロジックが異なるため、更改後の家畜疾病サーベイランス報告システムでも運用に必要な情報のシステム管理が行えるよう、デー

	タクレンジングを行うこと。 ・システム管理する情報項目については、更改後の家畜疾病サーベイランス報告システムで必要となる運用と整合性を考慮した上で、データ移行設計を行うこと。
要件2 制度改正対応	2026 年（2027 年運用分）の制度改正に合せて、以下の対応を行うこと。 （1）2026 年に登録された情報を活用した帳票出力ができるように、帳票出力機能の開発をすること。 ・制度改正に伴うシステム管理データの追加、変更に合わせ、制度改正に対応した印刷内容になるようにすること。 （2）2026 年様式に対応したデータ登録 ・2026 年の様式に合せ運用に必要な情報のシステム管理が行えるよう、データの登録、修正、削除、CSV 出力等の改修すること。 ・システム管理する情報項目については、本制度で必要となる運用と整合性を考慮した上で、項目設計を行うこと。 ・関連する台帳群の改修も行うこと。 （3）2026 年度様式に対応した集計機能 ・登録されたデータが適切に集計できるよう改修すること。 （4）外部インタフェースの改訂 ・2026 年様式に合わせた外部インタフェースの改訂を行うこと。

2. 機能要件（詳細は別途記載）

2.1. 機能に関する事項

2.1.1. 機能一覧

本システムにおいて備える各機能は、後続の設計において具体化されるものとする。

2.1.2. 機能設計ポリシー

本システムの機能設計に関する要件は、下記のとおり。

- 設計を進める上で、必要に応じて機能の統廃合や共通化を検討するともに、メニュー、お知らせ機能、各種設定の管理機能、ログや修正履歴機能及びマスタメンテナンス機能等、アプリケーションの実装に伴って必要となるシステム機能に関しても併せて検討を行い、業務要件に示す業務を実現するために必要なシステム機能を開発すること。
- システム稼働後に追加開発及び改修が発生することを考慮し、変更する可能性の高い箇所のメンテナンスの容易さや改修時の影響箇所が最小限となるよう、機能設計を行うこと。
- 入力時にデータを保存せずに画面を遷移しようとした場合は、データが保存されていないことをメッセージ等で通知し、注意喚起を行うこと。

2.2. 画面に関する事項

2.2.1. 画面一覧

本システムに備える画面構成等については、後続の設計において具体化されるものとする。

2.2.2. 画面設計ポリシー

本システムの画面設計に関する要件は、下記のとおり。

- 本システム全体の画面遷移、画面表示及び画面構成に統一性を持たせること。
- 画面を一度閉じたり、メニュー画面に遡ったりすることなく、連続的な操作を可能とすること。
- 一連の処理において、画面が遷移しても一度入力した情報が引き継がれるようにし、再入力を不要とすること。
- 画面の複数起動を可能とすること。
- 各画面の上部もしくは左側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。

2.3. 帳票に関する事項

本システムから出力する帳票の出力レイアウト等については、後続の設計において具体化されるものとする。

2.4. 情報・データに関する事項

2.4.1. 情報・データ一覧

本システムで取り扱う情報・データとして想定されるものについては、後続の設計において具体化されるものとする。

2.4.2. 情報・データ設計ポリシー

本システムの情報・データ設計に関する要件は、下記のとおり。

- データの構造化を行い再利用しやすいデータとすること。
- データベースは正規化し、項目間の整合性を保つため冗長性は可能な限り排除すること。
- インタフェースになるデータに関しては、データの意味や記述方法を定義したインタフェース仕様書を作成すること
- データ設計にあたっては、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(2021 年(令和3年)3月 30 日最終改定)(以下、「実践ガイドブック」という。)を参照すること
- コードを使う必要がある場合には、できるだけ既存のコードを活用すること。コードの設計にあたっては、実践ガイドブックを参照すること
- 他システムとの連携や過去データの参照等が必要な場合には、そのデータのコンバージョンを実施すること
- 氏名や法人名等の特段の指示がない場合には、文字は以下の条件を想定して整備すること。ただし、開発に問題が発生する場合は、変更も可とする。
  - 取り扱う日本語文字集合の範囲:JIS X 0213:2012
  - 符号 JIS X 0221:2014(ISO/IEC 10646(UCS))の USC-2 の範囲を符号化
  - 文字の符号化方式:UTF-8

3. 非機能要件（詳細は別途記載）

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

3.1.1. 情報システムの利用者の種類、特性

情報システムの利用者の種類と特性は、下記のとおり（システム管理者、関連調達事業者を除く。）。システム利用者が幅広いため、ユニバーサルデザインを採用すること。

No.	利用者区分	利用者の種類	特性
1	農林水産省本省	制度設計、システムでのデータ集計等、管理業務を行う。 テストで AI-OCR を利用する。	・PC スキル：パソコン上で基礎的な Excel 操作等をほぼ問題なく完遂できるが、データベースの操作まではできない。 ・利用機器：パソコン ・機器の用途：各種情報参照・集計等 ・機器の設置場所：執務室内、外勤先、テレワーク環境内（自宅もしくは実家）
2	都道府県、家畜保健衛生所	システムでの利用者登録、入力、データ集計等を行う。 AI-OCR を利用する。	・PC スキル：パソコン上で基礎的な Excel 操作等をほぼ問題なく完遂できるユーザからパソコンの基礎的な操作も厳しいユーザまで多様。 ・利用機器：パソコン、タブレット ・機器の用途：各種情報参照・集計、登録、入力等 ・機器の設置場所：執務室内、外勤先、テレワーク環境内（自宅もしくは実家）
3	農研機構	データ集計等を行う。	・PC スキル：パソコン上で基礎的な Excel 操作等をほぼ問題なく完遂できるユーザからパソコンの基礎的な操作も厳しいユーザまで多様。 ・利用機器：パソコン ・機器の用途：システムの利用者登録、入力等 ・機器の設置場所：執務室内、自宅もしくは農場等、多種多様

3.1.2. ユーザビリティ要件

本システムのユーザビリティ要件は、下記のとおり。

No.	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成	・ ユーザが想定する流れに沿った手順（画面遷移・タブの移動順等）にすること。 ・ ユーザが必要な操作を想起しやすい画面構成とすること。 ・ 出来る限り、最小限の操作となる画面構成とすること。 ・ 無駄な情報、デザイン及び機能を排し、簡潔で分かりやすい画面であること。 ・ 基本的なデザインには一貫性を持たせること。 ・ システム利用者の年齢層が幅広いことを考慮した上で、十分な視認性の高い表示とすること。 ・ ユーザ操作履歴、変更履歴、処理履歴等が確認できること。
2	操作方法の分かりやすさ	· 無駄な手順を省き、最小限の操作、入力等でユーザが作業できるようにすること。 · 画面上で入出力項目のコピー及び貼り付けができること。 · 同時に複数画面の起動ができ、画面サイズの変更（画面最大化を含む）ができること。 · ブラウザのズーム等により、文字切れ等が起きないよう、文字の自動折り返し等がされること。 · 業務の実施状況によっては、ショートカットや代替入力方法が用意されること。 · TAB キーによる項目遷移ができることがのぞましい。 · 日付入力の際にはカレンダーからの選択が出来る等、入力の簡易化がされていることがのぞましい。 · 保留機能等を設け、事務処理の失念防止機能が設けられていること。
3	指示や状態の分かりやすさ	· 操作の指示、説明、メニュー等には、ユーザが正確にその内容を理解できる用語を使用すること。 · 基本的な用語には一貫性を持たせること。 · 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ユーザが認識できるようにすること。 · システムが処理を行っている間、その処理内容をユーザが直ちに分かるようにすること。 · 操作する内容がすぐに分かるように、画面内に適度な説明を記載し、ユーザが分かりやすく操作で

		きること。
4	エラーの防止と処理	・ ユーザが操作、入力等を間違えないようなデザインやガイド(案内)を提供すること。 ・ 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、ユーザ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こと。 ・ 必要に応じて確認画面等を設け、ユーザが行った操作または入力の取消し、修正等が容易に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表示を行い、ユーザの確認を促すこと。 ・ エラーが発生したときは、ユーザが容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすい情報提供をすること。 ・ エラーではないが、入力内容による相関関係等により確認を促す機能(warning 機能)を提供すること。
5	ヘルプ	・ ユーザが必要とする際に、ヘルプ情報やマニュアル等を利用できるようにすること。 ・ マニュアルはカテゴリ単位で作成、メニューを細分化することで確認しやすいようにすること。 ・ FAQ はシステムから確認が安易にできるよう工夫をすること。キーとなる情報に各種リンクを張ることで、利用者が目的に到達しやすいよう、考慮すること。

3.1.3. アクセシビリティ要件

本システムのアクセシビリティ要件は、下記のとおり。

No.	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	・ JIS X 8341-3:2016 等に準拠していること。
2	指示や状態の分かりやすさ	・ 入力内容の形式に問題がある項目の強調表示やエラーメッセージ等については、色の違いを識別しにくいユーザ(視覚障害者の方等)を考慮し、可能な限り色のみで判別するようなものは用いないこと。
3	操作画面や操作手順の分かりやすさ	・ 情報端末の操作に不慣れな方や情報システムの仕組みに詳しくない方が存在すると想定されるため、操作画面や操作手順の分かりやすさに配慮すること。

3.2. システム方式に関する事項

3.2.1. 情報システムの構成に関する全体の方針

情報システムの構成に関する全体の方針は、下記のとおり。

No.	全体方針の分類	全体方針
1	汎用ソフトウェアの活用	・ 可能な限り汎用ソフトウェアの活用を図り、低コストでかつ効率的にシステム化を行うこと。 ・ LGWAN 接続でも利用できる製品とすること。
3	Web 対応のアプリケーション	・ 本システムの実現方式は Web 対応のアプリケーションとし、端末に対して実行環境のインストールを必要とする仕組みは原則として使用しないものとする。
4	開発容易性の実現	・ 令和7年度以降に追加開発及び改修を予定しているため、追加開発及び変更となった場合においても、改修がしやすいよう、可能な限り複雑な開発を行わないこと。
5	開発生産性及び保守性向上	・ 開発生産性及び保守性向上のため、画面、業務ロジック、データアクセスを極力疎結合な構造とし、各々の変更における影響範囲を最小化すること。

3.2.2. 本システムの利用環境

本システムは、複数の種類のユーザが複数の環境から利用することを前提とする。そのため、利用する端末やブラウザについては Windows OS における Edge 、Chrome の農林水産省内で採用するバージョンに対応するものとし、一般的にサポートされているバージョンは動作保証対象とする。

スマホ及びタブレットは飼養衛生管理支援システム（仮称）第1期開発業務に準ずるものとし、一般的にサポートされているバージョンは動作保証対象とする。

3.3. 拡張性に関する事項

3.3.1. 性能の拡張性

本システムの性能の拡張性として求める要件については、下記のとおり。

- 処理能力やデータ保存領域を拡張するための CPU、メモリ等、導入後の拡張性を有すること。
- システムユーザ数、データボリューム等の増大、ユーザ別業務システムの追加にも容易に対応可能な拡張性を有すること。
- サーバ負荷軽減の為、分散処理可能な構成であること。

3.3.2. 機能の拡張性

本システムの機能の拡張性として求める要件については、下記のとおり。

- 令和9年度以降の追加開発及び改修を予定しているため、変更となる可能性の高い数値項目等は変数やマスタで持ち、改修を行わずに変更可能とする等、柔軟性を持たせること。
- 複数の機能において、共通の処理ロジックを使用する場合には、共通モジュール化し、汎用的に利用可能となるよう設計すること。

3.4. 上位互換性に関する事項

本システムの上位互換性として求める要件については、下記のとおり。

- クライアント OS のバージョンアップに備え、OS の特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。

3.5. システムの稼働環境に関する事項

3.5.1. システム稼働環境に関する事項

本システムの稼働環境は下記に示す環境とし、本システムの開発・テスト等を実施すること。本番環境以外は必要な時のみの稼働を想定している。なお、下記に加えて、その他環境を追加する場合は、担当者と協議の上、追加すること。

No.	環境	定義
1	本番環境	本稼働環境。
3	ステージング環境	システム利用者がシステム操作演習、受入テスト等を行う環境。通常時は、担当者が動作検証等を行う環境として使用する。
4	開発環境	リリース前のアプリケーションを導入し、受注者が性能テスト等を行う環境。必要に応じて担当者がリリース前のアプリケーションに関するテスト環境として用いる。
5	社内環境	受注者社内の開発環境

3.6. 引継ぎに関する事項

他事業者への円滑な引継ぎとして求める要件については、下記のとおり。

- 特定の事業者に依存することなく、他事業者による保守、追加開発が可能なシステム構成であること。
- 特定のベンダーのみが保有するソフトウェア及びライセンスを前提としないこと。

・ 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知が適切な方法・期限で実施されること。また、サービス終了又は変更に伴うデータ移行が適切な方法で実施できること。

・

3.6.1. 教材の作成

教材の作成に関する要件は、下記のとおり。

No.	教育の方法	教育の方法
1	システム操作マニュアル	・ 職員向けの基本操作をマニュアルにすること。 ・ 誰が見てもわかりやすい記載とすること。 – マニュアルの章立ては、システム対象ユーザの業務の流れに沿って組み立てる。カテゴリ別に作成すること。 – 基本操作や基本機能の流れをわかりやすく図解する。 – 画面貼付等の図示により、該当箇所を明確にする。 – よくある質問やよくある操作ミス等に対する事例や回答を記載する。 – 専門用語は使用しない。 – エラーチェック等の仕様についても記載する。

別紙３　情報システムの経費区分

経費区分		摘要
1）整備経費		情報システムの整備（新規開発、機能改修・追加、更改及びこれらに付随する環境の整備をいう。）に要する一時的な経費
	ア　調査研究等経費	情報システムの整備に当たり、業務の設計、要件定義を行う目的で行う現状分析、プロトタイプ作成、ドキュメント作成支援、調査研究等に要する経費（最適化計画の策定に要する経費を含む。）
	イ　設計経費	情報システムの整備に際し、その開発に関する設計書の作成に要する経費
	ウ　開発経費	情報システムの整備に際し、情報システムのプログラミング、パラメータ設定等による情報システムの開発（単体テストを含む。）に要する経費
	エ　据付調整経費	ハードウェアやラックの搬入・据付け、ネットワークケーブルの敷設等、情報システムの物理的な稼働環境の整備に要する経費
	オ　テスト経費	開発する情報システムの結合テスト、総合テスト及び受入テストに要する経費
	カ　移行経費	情報システムのシステム移行及びデータ移行に要する経費
	キ　廃棄経費	情報システムの廃止及び更改に伴う、ハードウェアやラック、ネットワークケーブル等の撤去及び廃棄に要する経費
	ク　プロジェクト管理支援経費	情報システムの整備に伴うプロジェクト管理支援事業者に要する経費
	ケ　施設整備等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用・保守等を行うために駐在する施設の整備、改修等に要する経費
	コ　ハードウェア買取経費	情報システムを構成するハードウェアの買取りに要する経費
	サ　ソフトウェア買取経費	情報システムを構成するソフトウェア製品のライセンスの買取り又は更新に要する経費
	シ　その他整備経費	アからサまでのいずれにも該当しない情報システムの整備に要する経費
2）運用等経費		情報システムの運用、保守等に要する経常的な経費
	ア　システム運用経費	情報システムの正常な稼働を保持するために行うハードウェアの状態ファイルの管理、アプリケーションの設定等の管理、障害に対する予防等の措置など、仕様変更や構成変更を伴わない情報システムの技術的及び管理的業務の実施に要する経費
	イ　業務運用支援経費	情報システムの稼働に当たって、業務実施部門が行う業務（データ作成（Web サイトや e ラーニングのコンテンツ作成等）、データ受付・登録等）の運用支援に要する経費
	ウ　操作研修等経費	情報システムの利用に当たって、当該情報システム部門の担当者又は情報システムの利用者に対する操作研修等（教材作成・更新を含む。）に要する経費
	エ　ヘルプデスク経費	職員等の情報システム利用者からの問合せに対応するために行う業務に要する経費
	オ　コールセンター経費	国民や事業者等の情報システム利用者からの問合せに対応するために行う業務に要する経費

経費区分		摘要
	カ　アプリケーション保守経費	開発した情報システムについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行うアプリケーションプログラムの改修、設定変更等に要する経費
	キ　ハードウェア保守経費	情報システムを構成するハードウェアについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費
	ク　ソフトウェア保守経費	情報システムを構成するソフトウェア製品について、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費
	ケ　監査経費	情報システムについて、システム監査又は情報セキュリティ監査の実施に要する経費
	コ　情報セキュリティ検査経費	情報システムについて、ペネトレーションテスト、脆弱性診断等の情報セキュリティ検査・診断の実施に要する経費
	サ　ハードウェア借料	情報システムを構成するハードウェアについて、その使用に要する借料
	シ　ソフトウェア借料	情報システムを構成するソフトウェア製品について、その使用に要する借料
	ス　サービス利用料	情報システムの稼働又は利用に当たって、ASP、SaaS、PaaS、ホスティングサービスなど、国の行政機関以外の者が提供するサービスの利用に要する経費
	セ　通信回線料	情報システムを構成するネットワークにおいて必要となる通信回線の利用に要する経費
	ソ　施設利用等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用・保守等を行うために駐在する施設の利用等に要する経費
	タ　その他運用等経費	アからソまでのいずれにも該当しない情報システムの運用等に要する経費
3）その他経費		国の行政機関以外の情報システムに関係する経費及びデジタル・ガバメントの推進のための体制整備に要する経費
	(1) 情報システム振興等経費	地方公共団体、独立行政法人等に対する情報システムの整備・運用に関する助成金、補助金、交付金等の経費
	ア　地方公共団体情報システム関係経費	地方公共団体に対する情報システムの整備・運用に関する補助金、交付金等の経費
	イ　独立行政法人等情報システム関係経費	独立行政法人、国立大学法人（大学共同利用機関法人を含む。）、特殊法人、公益法人等に対する情報システムの整備・運用に関する助成金、補助金、交付金（法人の運営に関する経費は除く。）等の経費
	(2) デジタル・ガバメントの推進のための体制整備関係経費	高度デジタル人材の登用に要する経費、ＰＭＯの支援スタッフ等に要する経費、内部職員の育成に要する経費等、デジタル・ガバメントの推進のための体制整備に要する経費

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に関する作業内容

調達を行うときは、調達内容に応じ、少なくとも次の１．から４．までに定める作業内容を調達仕様書に盛り込むものとする。

１．契約金額内訳

「別紙３　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を記載した情報資産管理標準シートを契約締結後速やかに提出すること。

２．設計・開発

次の 1）から 10）までに掲げる事項について記載した情報資産管理標準シートを、設計・開発実施要領において定める時期に、提出すること。

1）　開発規模の管理

情報システムの開発規模（工数、ファンクションポイント（「第３編第３章３．経費の見積り」参照）等）の計画値及び実績値

2）　ハードウェアの管理

情報システムを構成するハードウェアの製品名、型番、ハードウェア分類、契約形態、保守期限等

3）　ソフトウェアの管理

情報システムを構成するソフトウェア製品の名称（エディションを含む。）、バージョン、ソフトウェア分類、契約形態、ライセンス形態、サポート期限等

4）　回線の管理

情報システムを構成する回線の回線種別、回線サービス名、事業者名、使用期間、ネットワーク帯域等

5）　外部サービスの管理

情報システムを構成するクラウドサービス等の外部サービスの外部サービス利用形態、使用期間等

6）　施設の管理

情報システムを構成するハードウェア等が設置され、又は情報システムの運用業務等に用いる区域を有する施設の施設形態、所在地、耐久性、ラック数、各区域に関する情報等

7）　公開ドメインの管理

情報システムが利用する公開ドメインの名称、ＤＮＳ名、有効期限等

8）　取扱情報の管理

情報システムが取り扱う情報について、データ・マスタ名、個人情報の有無、格付等

9）　情報セキュリティ要件の管理

情報システムの情報セキュリティ要件

10)　指標の管理

情報システムの運用及び保守の間、把握すべきＫＰＩ[注記)]名、ＫＰＩ分類、計画値等の案

注記）ＫＰＩ（Key Performance Indicator）とは、目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なものをいう。

３．運用及び保守

次の 1）及び 2）に掲げる事項について記載した情報資産管理標準シートを、運用実施要領（「第３編第９章１．3)ア コミュニケーション管理」参照）及び保守実施要領（「第３編第９章１．5)ア コミュニケーション管理」参照）において定める時期に、提出すること。

1)　各データの変更管理

情報システムの運用及び保守において、上記２．の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目

2)　作業実績等の管理

情報システムの運用及び保守中に取りまとめた作業実績、リスク、課題及び障害事由

４．その他

上記２．及び３．以外においても、役務を伴う調達案件については、ＰＪＭＯの求めに応じ、スケジュールや工数等の計画値及び実績値について記載した情報資産管理標準シートを提出すること。

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４別添１

令和×年×月×日

農林水産省
消費・安全局動物衛生課　殿

住所　○○○○○○○○○
株式会社○○○○○○○○○
情報セキュリティ管理責任者　○○○○

情報セキュリティ対応状況・確認書

下記調達に関して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、当社の情報セキュリティ対応状況について以下のとおり回答させていただきます。

調達件名：家畜疾病サーベイランス報告システム拡充等業務（飼養衛生管理等支援システム）

１．受託者及び業務実施体制に関する情報の提供について

No	情報提供依頼事項	情報の提供に応じる		備考
1	受託者は、受託者の資本関係・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（○○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。	はい □	いいえ □	提出資料有
2	受託者は、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。 （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）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 （４）MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績	はい □	いいえ □	提出資料有

２．情報セキュリティの確保について

No	チェック事項	チェック事項の措置を講じる		備考
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及び本業務以外の目的で利用しないこと。	はい □	いいえ □	
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。	はい □	いいえ □	
3	本業務の各工程において、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。）。	はい □	いいえ □	提出資料有
4	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。	はい □	いいえ □	
5	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。	はい □	いいえ □	
6	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。	はい □	いいえ □	
7	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 25 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。	はい □	いいえ □	
8	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。	はい □	いいえ □	
9	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。	はい □	いいえ □	
10	情報セキュリティ対策の履行が不十分な場合、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。	はい □	いいえ □	

２．情報セキュリティの確保について（続き）

No	チェック事項	チェック事項の措置を講じる		備考
11	本業務においてクラウドサービスを活用する場合（※）には、ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、当該認証の証明書等の写しを提出すること。	はい □	いいえ □	提出資料有
		該当なし □		
12	本業務においてクラウドサービスを活用する場合（※）には、クラウドサービス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。 （１）ISO/IEC 27017 又は ISMS クラウドセキュリティ認証制度に基づく認証 （２）セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report）） （３）情報セキュリティ監査により対策の有効性が適切であることを証明する報告書（クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 言明書等）	はい □	いいえ □	提出資料有
		該当なし □		
13	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、ソフトウェア等を納品、賃貸借等をする場合には、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。	はい □	いいえ □	提出資料有
		該当なし □		
14	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、ソフトウェア等を納品、賃貸借等をする場合には、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。	はい □	いいえ □	提出資料有
		該当なし □		

※発注業務の要件でクラウドサービス利用を指定している場合のみ該当。（発注業務の要件でクラウドサービス利用を指定していないが、受託者側の選択で利用する場合（受注者の開発環境をクラウド環境で構築するなど）や、発注業務の要件に関係なく、受託者側の都合でメール、ファイル管理等の機能にクラウドサービスを利用している場合等については該当しないものとする。）

３．個人情報保護について

No	チェック事項	チェック事項の措置を講じる		備考
1	本業務の各工程において、農林水産省の意図としない個人情報漏えい等が行われないことを保証する管理が一貫した保証管理体制の下でなされていること（例えば、個人情報等の取扱いに関する責任者及び業務従事者の管理及び実施体制、個人情報等の管理状況の検査に関する事項等を証明する書類等を提出すること。）。	はい □	いいえ □	提出資料有
2	本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、担当部署の承認を得た上で実施すること。また、作業実施前に教育を実施し、認識を徹底させること。	はい □	いいえ □	
		該当なし □		
3	個人情報を複製する際には、事前に担当部署の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去すること。	はい □	いいえ □	
4	受託者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大防止等のため必要な措置を講ずるとともに、担当部署に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。	はい □	いいえ □	

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５】

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～ウの取組について、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　みどりの食料システム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
（　　）

別紙６

閲覧申請書

申込日：　令和　　年　　月　　日

１　会 社 名：

２　住　　所：

３　担当者名：

４　電話番号：

５　E-mail アドレス：

６　閲覧希望日時：　令和　　年　　月　　日　　時
令和　　年　　月　　日　　時
令和　　年　　月　　日　　時

７　閲覧者氏名：
：
：
：

別紙７

農林水産省
消費・安全局動物衛生課　宛

機密保持誓約書

「家畜疾病サーベイランス報告システム拡充等業務（飼養衛生管理等支援システム）」に係る資料閲覧に当たり、下記の事項を厳守することを誓約します。

記

１　農林水産省の情報セキュリティに関する規程等を遵守し、農林水産省が開示した情報（公知の情報等を除く。）を本調達の目的以外に使用又は第三者に開示若しくは漏えいすることのないよう、必要な措置を講じます。

２　閲覧資料については、複製及び撮影を行いません。

３　本業務に係る調達の期間中及び終了後にかかわらず、守秘義務を負います。

４　上記１～３に反して、情報を本調達の目的以外に使用又は第三者に開示若しくは漏えいした場合、法的な責任を負うものであることを確認し、これにより農林水産省が被った一切の損害を賠償します。また、その際には秘密保持に関する農林水産省の監査を受けることとし、誠実に対応します。

令和　　年　　月　　日

住　　所

会 社 名

代表者名

別紙８

品質管理要件

１．作業実施計画書の作成段階において、以下の事項を記載すること。

〇品質管理体制

〇品質管理の手法

・品質管理として各工程において、どのような活動を行うのか、全体フレームワークを示すこと。なお、内容が不十分と判断した場合には必要な修正を行うこと。

・各工程においては社内レビューのみならず、発注者へのレビュー実施事項を含むこと。

・品質管理を一元的に管理するためのツール又は標準ドキュメントがあれば、それを示すこと。

なお、様式等は任意とするが、情報項目として不足等があると判断した場合には、追加修正対応すること。

〇課題管理表により、検討課題を管理すること。

〇問題管理表により、課題事項を管理すること。

〇リスク管理表によりプロジェクトリスクを管理すること。なお、作業計画時のリスク想定事項をあらかじめ反映すること。

〇その他、品質管理に係わる取組事項があれば明示すること。

２．品質管理事項として、少なくとも以下に示す取組みを実施すること。

〇設計・開発段階

・設計書案についてレビュー実施すること。

・その際に、レビュー目的、レビューポイントを明確にすること。

・実施時期については、スケジュール表に反映すること。

・レビュー実施の方法、体制について明示すること。

〇テスト段階

・各リリース段階において、試験前にテスト計画書を作成し、レビューすること。

・テスト計画書に基づき、各テスト実施前にテスト内容の詳細についてレビューを行うこと。

・テスト計画書には試験方針を示すこと。また、試験方針として、テストの目的と範囲、テスト方法、テスト体制、テスト期間、テスト環境など明示すること。

・テスト実施体制においては、第三者による確認など、客観的な品質管理体

制とすること。
・また、テスト段階に用いる品質管理指標項目と目標値・完了基準を設定し、その説明をすること。
・テスト実施においては、機能テストとして、正常系テスト、例外テスト、境界テスト、限界値テスト等を行うものとする。また、必要に応じて性能試験を行うこと。
・操作性など、ユーザーの視点に立ったテスト項目を設定すること。
・上記試験項目一覧（チェックリスト）等を含むテスト計画書を各テスト実施前に提示すること。
・設定した品質管理指標項目と目標値・完了基準に基づき、試験結果を報告すること。
・テスト実施においては、管理ドキュメントとして、バグ管理図（信頼度成長曲線）や品質管理表などを作成・管理すること。
・実際の運用を想定したテスト内容を設定すること。登録系のテストは登録後、修正、削除、再登録も行うこと。
・本番環境の登録データ、マスタ等も調査、考慮の上、テスト内容を設定すること。
・改修に関連する機能も含めてテストを行うこと。
〇テスト結果報告
・テスト結果報告書及び品質管理表による報告を行うこと。
・摘出不良目標値；試験密度と不良率などが確認できる資料を提示すること。
・機能別／サブシステム別の試験項目数（予定・実績・密度）、不良数（予定／実績・不良率）による目標値や自社の経験に基づく指標値範囲内であるか等の報告を行うこと。
・品質状況分析（障害・不良原因分析）に基づく報告を行うこと。
・不具合の原因を分類整理し、類似の潜在不具合を潰すための横展開や品質強化ための追加試験実施など、品質強化のための対応策を示し、速やかに実施すること。