令和８年度動物用医薬品等データベース
運用保守及び基盤提供業務
調達仕様書

農林水産省動物医薬品検査所

目次

1　調達案件の概要

（1）調達件名

令和8年度動物用医薬品等データベース運用・保守及び基盤提供業務

（2）調達の背景

動物医薬品検査所では、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に基づき、動物用医薬品、動物用医薬部外品、動物用医療機器、動物用体外診断用医薬品及び動物用再生医療等製品（以下、「動物用医薬品等」とする。）の審査、検定業務等を行っている。

動物用医薬品等に関する情報やその副作用に関する情報を収集し、国民に公開することを目的とする「動物用医薬品等データベース」はオンプレミスで稼働していたが、2018 年6月に決定した「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」（最終決定：2025 年5月 27 日）において政府方針として示された「クラウド・バイ・デフォルトの原則」を踏まえ、令和元年度（2019 年度）にクラウドサービス（NECCI）に移行した。

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 クラウドといい、総合的な支援活動を行う組織を MAFF クラウド CoE という。

本システムは令和7年度（2025 年度）から 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。

本調達では、当該政府方針に従い、MAFF クラウド（AWS）上に構築された動物用医薬品等データベースの運用業務及び MAFF クラウドにおけるクラウドサービスの提供業務を調達するものとし、クラウドサービスの提供に係る費用及び利用料は受注者の負担とする。

（3）調達目的及び調達の期待する効果

本業務は、受注者が R8年度（2026 年度）の「動物用医薬品等データベース」の運用保守及び基盤提供業務を行う。また、「動物用医薬品等データベース」の維持・改善に関し、担当部署に助言・提言を行い、システムが円滑かつ効率的に運用されることを目的とする。

（4） 業務・情報システムの概要

「動物用医薬品等データベース」と関連するシステム及び業務の概要は図１のとおり。別に運用する「飼養衛生管理支援（投薬指示）システム」、「畜産クラウド」及び「有害事象報告システム」と情報を連携している。システム構成図は図2のとおりである。

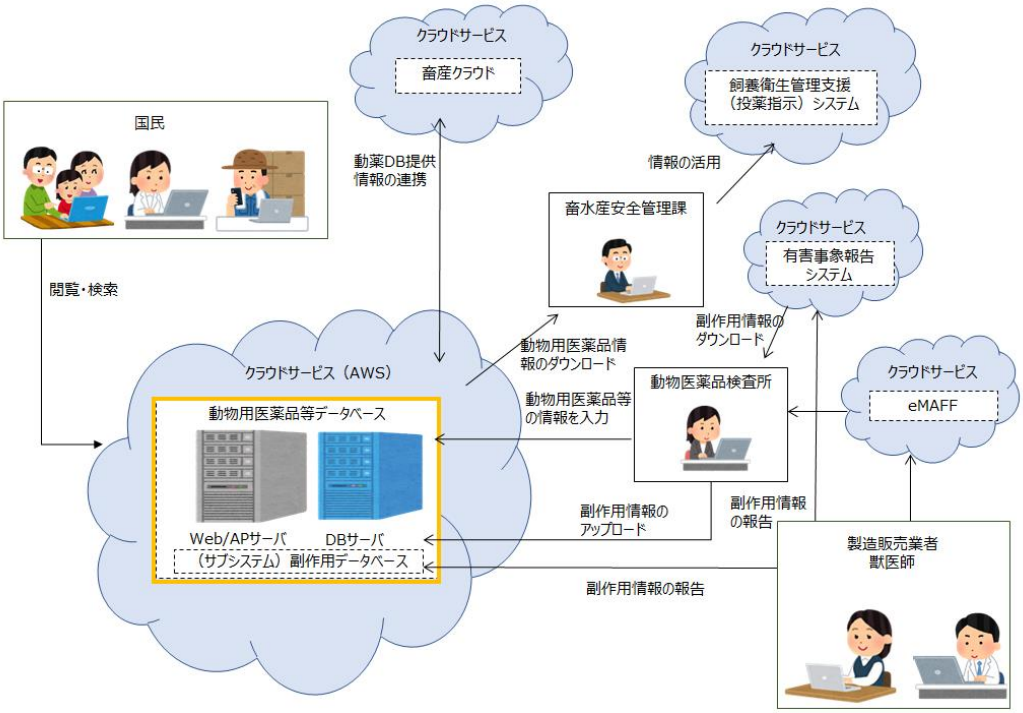

図 1 「動物用医薬品等データベース」の概要

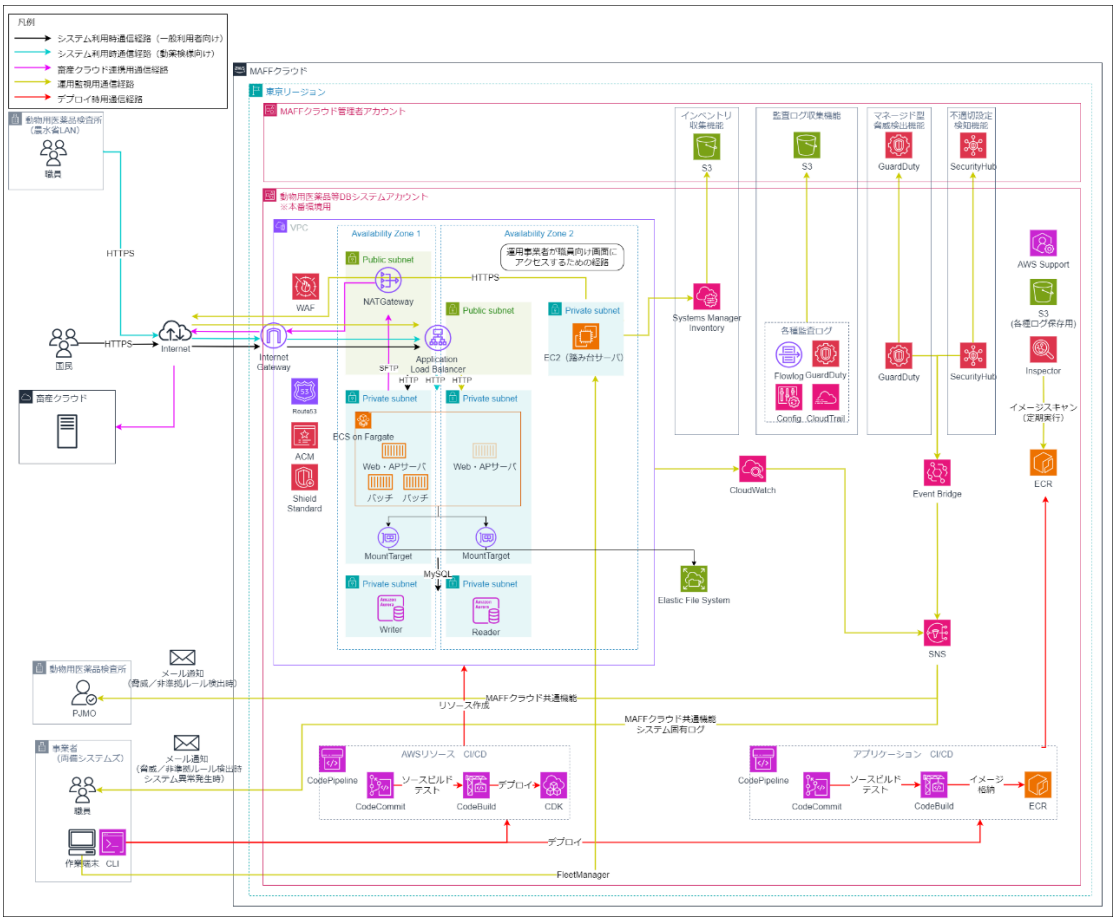

図 2 「動物用医薬品等データベース」のシステム構成図

（5） 契約期間

令和8年4月1日から令和9年3月 31 日まで

（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が、具体的なスケジュールについては、担当部署と本案件業務の受注者間で協議の上、決定すること。

作業項目		2025年度（R7年度）												2026年度（R8年度）												2027年度（R9年度）											
		4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
システム運用保守	運用保守＋基盤提供																	今回の調達の範囲																			
システム改修	改修																																				

図 3 作業スケジュール

2 調達案件及び関連調達案件

（1） 調達範囲

本調達では、「動物用医薬品等データベース」に係る運用保守及び基盤提供を行うものと

とする。

なお、上記は責任分界の基本方針であり、責任範囲の調整が必要となった場合には、担当部署と協議の上、決定するものとする。

（2） 調達案件の一覧

調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等は次の表のとおり。

表 1 関連する調達案件の一覧

No	調達案件名	調達の方式	契約締結日	入札公告 落札者決定	契約期間
1	運用保守及び基盤提供	一般競争入札（総合評価）	令和8年4月1日	－ －	令和8年4月から 令和9年3月まで
2	改修業務（副作用報告機能追加）	一般競争入札（総合評価）	令和8年4月（予定）	令和8年2月（予定） 令和8年3月（予定）	令和8年4月から 令和8年 10 月まで（予定）

図 4 調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等

（3） 調達案件間の入札制限

調達する業務について、他の調達案件と入札制限の対象となる案件はない。

3 情報システムに求める要件

以下を満たすこと。なお、詳細については別途農林水産省が提示する最新の「農林水産省クラウド利用ガイドライン及び関係資料」を参照すること。また、本案件業務の実施において、農林水産省クラウド利用ガイドラインの改定があった場合は最新版を参照すること。

令和6年度の MAFF クラウド移行業務にて、「動物用医薬品等データベース」のサーバが MAFF クラウドへ移行している。その際に選定した、クラウドサービスプロバイダー（AWS）を利用すること。

4　運用保守及び基盤提供作業の実施内容

（1） 運用保守計画書、運用保守実施要領の作成

受注者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、担当部署の指示に基づき、運用保守計画書及び運用保守実施要領の案を作成し、担当部署の承認を得ること。

なお、運用保守計画書と運用保守実施要領の記載内容は「デジタル・ガバメント推進標準ガイドライン」(デジタル社会推進会議幹事会決定。最終改定：2025 年 5 月 27 日以下「標準ガイドライン」という。)「第9章　運用及び保守」で定義されているものとする。

（2） 情報セキュリティ対策

ア　クラウドアーキテクトのベストプラクティス（AWS 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。

イ　以下のセキュリティ対策要件を参照し、動物用医薬品等データベースのセキュリティ対策要件を点検すること。

（ア） AWS/Azure 設定確認リスト（別紙1）

（イ） web システム/web アプリケーションセキュリティ要件書（別紙2）

（3） クラウドサービスを運用保守する場合の前提

ア　受注者は、前年度の動物用医薬品等データベースの運用保守及び基盤提供業務の事業者からパブリッククラウド上に構築された情報システムの引継ぎを受け、アカウントの契約の移管を行い、環境を維持すること。アカウント契約の移管にあたり、前年度の事業者からの引継ぎが4月1日に完了できない場合は、システムの運用に支障がでないよう、前年度の事業者との間で書面による契約等を行い、クラウド環境の引継ぎを適切に行うこと。

イ　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。

ウ　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 の場合、AWS Systems Manager Session Manager ・AWS Systems Manager Fleet Manager）を利用すること。

エ　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（AWS の場合、SSM（AWS Systems Manager））を利用して自動取得すること。

オ　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。

（4） 定常時対応

ア　受注者は、定常時対応（システム操作説明、問合せ窓口の提供)を行うこと。具体的な実施内容及び手順については、担当部署が定める運用保守計画に基づいて行うこと。問合せ窓口は、メールでの受付にあっては、24 時間、電話での受付にあっては、9:30 から 18:00(行政機関の休日は含まない。)の間、対応できるよう、窓口を提供すること。ただし、緊急性が高いと担当部署が判断した場合は、通常対応時間外であっても対応すること。なお、問い合わせの頻度については、週に2～3回程度、担当部署からの回答期限までに回答することとし、目安としては、問い合わせの翌日までに回答もしくは回答見込みを担当部署まで回答すること。また、以下の作業は受注者にて実施すること。

（ア） OS、ミドルウェアのセキュリティパッチの適用とシステムの動作確認（緊急・重要な更新は月1回程度）

（イ） サーバ監視に必要な諸設定の調整作業（監視項目の追加・変更、アラームのしきい値の調整等）

（ウ） サーバの監視にてアラームが発報した際の調査、対応

（エ） OS（インスタンス）のバックアップが日々、正常に取得されていることの確認

（オ） ログが日々、正常に取得・保管されていることを確認し、異常があれば、PJMO へ報告、原因確認、及び、異常解消に向けた諸対応の実施

（カ） 発注者側のシステム研修などに利用するユーザーの追加・削除やデータの追加削除に係る依頼された作業

（キ） 事故や問題の発生や機能改善が必要な事案が生じた際に、これらの原因を調査し、特定すること。調査の結果、基盤サービスやアプリケーションに原因があった場合、基盤サービスの設定やアプリケーションプログラムの不具合を修正すること。修正作業を行う際は、検証用サーバにおいて、テストを行った上で、本番環境に移行すること。

令和7年度の改修内容については、閲覧資料にて確認すること。

イ　連携する「飼養衛生管理支援（投薬指示）システム」「畜産クラウド」及び「有害事象報告システム」の運用保守業務受注者から問い合わせや支援依頼があった場合、これに対応すること。また、連携機能が正常に稼働しているか監視を行い、問題が生じた際には速やかに担当部署に報告すること。

ウ　受注者は、担当部署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、打合せ等を開催すること。

エ　受注者は、担当部署との協議内容は受注者の責任において議事録に整理し、農林

水産省の確認を得ること。議事録は打合せ等の実施後、原則として 5 日以内（行政機関の休日を除く。）に電子ファイルを電子メールで担当部署に提出すること。

オ　受注者は、担当部署が承認した運用保守及び基盤提供実施計画及び実施要領に基づき、運用保守業務の内容や工数などの作業実績状況、サービスレベルの達成状況、「動物用医薬品等データベース」のシステムの構成と運転状況（セキュリティ監視状況、情報システムの脆弱性への対応状況を含む。）、システムの定期点検状況、システム利用者のサポート、教育・訓練状況、リスク・課題の把握・対応状況について月次で運用作業報告書を取りまとめること。

カ　セキュリティ管理として、（AWS の場合 SecurityHub）が発報したセキュリティアラートについて、対応ならびに無効化／抑制を検討するものとする。なお、新たなルールの追加について、迅速に対応するものとする。

キ　受注者は、月間の運用・保守実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。

ク　受注者は、月次の運用・保守作業報告書の内容について、その内容を報告すること。

ケ　受注者は、担当部署が、情報システム運用継続計画を作成又は更新するにあたり、情報提供等の支援を行うこと。

コ　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、担当部署に提出すること。

サ　受注者は、担当部署が承認した運用保守計画書及び実施要領に基づいて、システム及びクラウドサービスの日常的な状態監視を行うこと。

シ　受注者は、「動物用医薬品等データベース」に導入されているソフトウェアのバージョンに関して、脆弱性の有無を毎月確認し、確認した内容を月次の報告書に記載し、担当部署に報告すること。脆弱性が確認された場合、緊急性が高いものに関しては、至急報告すること。受注者は、ソフトウェアの保守の実施において、ソフトウェアの構成またはバージョンに変更が生じる場合には、担当部署にその旨を報告し、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。

ス　ソフトウェアにセキュリティのぜい弱性が見つかった場合は、対応策について計画し、承認を得た上で対応すること。使用しているソフトウェアのサポート期限についても適切に管理し、必要に応じてバージョンアップの計画を行い、承認を得たうえで対応すること。

セ　受注者は、ぜい弱性及びソフトウェアのバージョンアップ作業に対応する際は、保有するテスト環境でバージョンアップ後の動作確認を行い、担当部署から承認を得た上で、本番環境への適用を行うこと。動作確認の内容は、事前に担当部署の許可を得ること。受注者は、バージョンアップ前の環境に戻せるようにバックアップを取得すること。使用しているソフトウェアは下表のとおり。その他のソフトウェア及びバージョン等詳細情報は、閲覧資料にて確認すること。

表2　導入ソフトウェア一覧

機能	導入ソフトウェア
リレーショナルデータベース	Amazon　Aurora MySQL
Web サーバソフト	Apache
開発プラットフォーム	.NET
プログラミング言語	PHP
ライブラリ	jQuery
フレームワーク	CakePHP、AWS CDK
TLS プロトコル	OpenSSL

ソ　受注者は、保守作業でプログラムの修正を行った場合、設計書等の更新を行い、テストを行った上で本番環境へ適用すること。改修の際に作成、更新した資料は、担当部署へ提出すること。

タ　受注者は、パッチの自動適用を用いて、検証環境や品質保証環境などを用いてパッチベースラインを検証し、その後に本番環境にパッチを適用するなど、パッチのリリース管理を行うこと。なお、パッチ適用に起因する不具合が出た際に行う切り戻しやアプリケーション修正などの対応を予め計画すること。

チ　受注者は、年度末までに年間の運用実績を取りまとめるとともに、使用するソフトウェア、ミドルウェア等のサポート期限などをもとに、必要に応じて、次期運用保守計画、運用保守実施要領に対する改善提案を行うこと。

ツ　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、担当部署と MAFF クラウド CoE の確認を受けること。

テ　受注者は、インベントリ情報を収集するため、設定作業（AWS の場合、Systems Manager Inventory と EC2 の設定）を実施すること。
なお、インベントリ収集機能はコンテナの構成管理に対応していないため、コンテナを利用しているシステムは、MAFF クラウド利用ガイドラインの記載を参考に、脆弱性対策を実施すること。

ト　「動物用医薬品等データベース」のサブシステムである「副作用情報データベース」について、「副作用情報データベース」上に表示される項目にあわせ、「有害事象報告システム」、「eMAFF」及び「副作用報告システム」から報告されたデータを調整し、担当部署が「副作用情報データベース」に移行する作業をサポートすること（移行件数は、年間約 32,400 件程度を想定）。

ナ　さらに、「副作用情報データベース」で使用するマスタについて、関連する国際的な用語集（VICH、Veddra 及び WHO）（注）の改訂等にあわせ、追加、変更、更新作業と

して、旧バージョンファイルを担当部署が提供する新バージョンファイルに差替えること（作業頻度はVeddra及びWHOは年に1回、VICHは改訂が発生した場合を想定）。

（注）VICH：https://vichsec.org/en/guidelines/pharmacovigilance/vich-gl30.html
Veddra：https://www.ema.europa.eu/en/veterinary-regulatory-overview/post-authorisation-veterinary-medicines/pharmacovigilance-veterinary-medicines/eudravigilance-veterinary
WHO：https://www.whocc.no/atcvet/atcvet_index/

（5） 障害発生時対応

ア　受注者は、「動物用医薬品等データベース」のシステムについて、障害発生時（又は発生が見込まれる時）には、障害を感知してから3時間以内（業務ができないなどシステム停止により緊急の対応を要する場合は、1時間以内）、問い合わせ対応時間外にあっては、翌開始日の開始時間から1時間以内に担当部署に報告するとともに、その緊急度及び影響度を判断の上、障害発生時運用業務（障害検知、障害発生箇所の切り分け、関係する事業者への連絡、復旧確認、障害報告書による報告等）及び障害発生時保守作業（原因調査、応急措置、報告等）を行うこと。なお、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し、具体的な実施内容・手順は担当部署が承認した運用保守計画及び運用保守実施要領に基づいて行うこと。

イ　受注者は、「動物用医薬品等データベース」の不具合、システム障害に関して、その原因を調査し、特定する。不具合復旧に当たっては、事前に担当部署へ十分な説明を行うと共に作業計画書を提出し、担当部署の承認を得てから実施すること。なお、復旧までに時間を要する場合は、担当部署と協議すること。不具合の復旧は、「動物用医薬品等データベース」を利用した業務に支障が無いことを確認出来た時点とし、復旧の完了後に、作業内容（原因、対応及び対応結果等）を記載した報告書を提出し、担当部署に不具合の原因とその対策について詳細な説明をし、承認を得ること。また、当該不具合に関する分析（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は、恒久的な対応策を提案すること。

ウ　受注者は、災害等の発生時には、担当部署の指示を受けて、「動物用医薬品等データベース」運用継続計画に基づく業務を実施すること。なお、災害時の発生に備え、最低年1回は、事前訓練を実施すること。

エ　障害対応における作業及び関係者との役割を以下に示す。

表3 システム障害対応における作業及び関係者との役割分担

（〇＝作業責任 （ ）内は責任者の作業実施内容に関連する側の行為）

作業項目	役割分担	
	受注者	PJMO
日常的な状態監視	〇	〇
担当職員からの「動物用医薬品等データベース」のシステム障害連絡を受ける。	〇 （受付）	〇 （連絡）
障害の原因切り分けを行い、原因がアプリケーション、基盤、ソフトウェア、その他かどうか調査を行う。	〇	
原因がアプリケーション障害の場合、対応作業を行う。	〇	
原因が基盤またはソフトウェアの場合、基盤提供及び基盤運用保守業者へ作業依頼を行う。関係者は依頼内容に基づき作業を行う。	〇	
関係者の作業報告内容を確認し、正しく対応されていることを確認後、担当職員へ報告する。	〇	

（6） 引継ぎ

ア 受注者は、担当部署が動物用医薬品等データベースの更改を行う際には、次期の当該システムにおける事業者等に対し、作業経緯、残存課題等に関する情報提供、質疑応答等の協力を行うこと。

イ 受注者は、本契約の終了後に他の業者が動物用医薬品等データベースの運用保守及び基盤提供業務を受注する場合には、次年度の受注者に対し、契約期間内に作業経緯、残存課題等についての引継ぎを行うこと。

ウ 受注者は、次年度の運用保守及び基盤提供業務受注者に対し、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運用保守及び基盤提供業務受注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。

（7） 定例会等の実施

エ 受注者は、定例会を四半期に1回開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。

オ 担当部署から要請があった場合、又は、受注者が必要と判断した場合、必要資料を

作成の上、定例会とは別に会議を開催すること。

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

（8）情報システムの現状確認支援

ア　受注者は、年１回、担当部署の指示に基づき、情報資産管理データと動物用医薬品等データベースの現状との突合・確認（以下、「現状確認」という。）を支援すること。

イ　受注者は、現状確認の結果、情報資産管理データと動物用医薬品等データベースの現状との間の差異がみられる場合は、その差異を解消すること。

ウ　受注者は、現状確認の結果、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部署に報告すること。

エ　受注者は、現状確認の結果、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、担当部署に報告すること。

（9）運用保守及び基盤提供業務の改善提案

ア　受注者は、年度末までに年間の運用保守実績を取りまとめること。必要に応じて、定例会の際に運用保守計画、運用保守実施要領に対する改善提案を行うこと。

イ　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（AWS の場合、Trusted Advisor）し、検出項目の対応可否を検討し、担当部署の承認の上、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 フレームワークのすべての柱を活用し、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。

ウ　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（MSP サービスを利用した場合）を一覧表にとりまとめ、半年分と 1 年分を年に 2 回担当部署に提出すること。また、MSP サービスを利用した場合等の運用サービスの共通化の効果を定量で説明すること。受注者は、担当部署の求めに応じ、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。

エ　運用サービスの共通化とは、以下の取り組みとする。

（ア）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。

（イ）受注者が自社で MSP サービスを提供していない企業は、運用品質の均一化と不要なコストを削減するために

a　外部企業が提供する MSP サービスを利用すること、又は

b　複数の運用案件を受注することで、自社内で運用サービス（サービスデスク、監視サービス等）の Shared service（シェアードサービス）に取り組み、費用を逓減すること。

（ウ）クラウド利用料について、提出した実績を踏まえ、当該年度の９月末までに次年度の利用内容及び契約予定額を担当部署と協議する。また、クラウド利用料等の実績より、クラウドサービスの稼働状況やコストの遷移から、見積の作成、不要リソースの削除検討を行うものとする。

（エ）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で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。

オ　改善提案を作成したら担当部署ならびに PMO／MAFF クラウド CoE に報告すること。

（10）契約金額内訳及び情報資産管理標準シートの提出

ア　受注者は、「標準ガイドライン別紙2 情報システムの経費区分」（別紙3）に基づき区分等した契約金額の内訳が記載されたエクセルの電子データを契約締結後速やかに提出すること。なお、人件費については人件費単価ごとに工数を提示すること。最大何次請負、再委託総額、累計契約額(前年度まで)、年度契約金額を提示すること。

イ　受注者は、担当部署が定める時期に、情報資産管理標準シートを提出すること。

ウ　受注者は、「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」（別紙4）に基づき担当部署から情報資産管理標準シートの作成を依頼された場合、次に掲げる事項について記載した様式について、担当部署が定める時期に、提出すること。

（ア）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

（イ）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

（ウ）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

（エ）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

（オ）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

（カ）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

（キ）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

（ク）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

（ケ）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名、KPIの分類、計画値等の案

（コ）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

（サ）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

（シ）スケジュールや工数の管理

スケジュールや工数等の計画値及び実績値

（11）成果物の作成

ア　成果物名

本業務の成果物を以下に示す。

表4　成果物一覧

成果物名	記載内容	提出期限
運用保守計画書	標準ガイドライン実務手引書第3編「第9章　運用及び保守」の運用保守計画の案の作成・記載内容・確定に示されているもの	契約締結後 10 日以内（行政機関の休日を除く。）
運用保守実施要領	標準ガイドライン実務手引書第3編「第9章　運用及び保守」の運用保守実施要領	契約締結後 10 日以内（行政機関の休日を除く。）

成果物名	記載内容	提出期限
情報資産管理標準シート	契約金額内訳記載	契約締結後 10 日以内 （行政機関の休日を除く。）
	システム要件の変更管理及び作業実績等の管理について記載	運用保守実施要領において定める時期
	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	運用保守実施要領において定める時期
月次運用保守作業報告書	運用保守計画書及び運用保守実施要領に基づき、運用保守業務の内容や工数などの作業実績状況、サービスレベルの達成状況、動物用医薬品等データベースのシステム構成と運転状況（情報セキュリティ監視状況を含む。）、定期点検状況、利用者サポート、教育・訓練状況、リスク・課題の把握・対応状況について記載	前月の報告書を月初10日までに提出すること。ただし、2027 年３月分の報告書は、2027 年3月31日までに提出すること。
議事録	担当部署との協議内容を記載	打合せを実施した場合、５日以内 （行政機関の休日を除く。）
障害報告書	アプリケーションの不具合の内容と、その対応について記載	原則、運用保守作業報告書に含める なお、緊急・重大なインシデントの場合は、発生後速やかに提出する
クラウドサービスの利用実績	クラウドサービスの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を含め、一覧表にまとめたもの。	半年分をまとめたもの 2026 年 10 月 30 日 1年分をまとめたもの 2027 年3月 24 日まで
クラウドサービスの機能を利用したソフトウェア情報等の出力結果	クラウドサービスの機能を利用したソフトウェア情報等の出力結果	2027 年3月 24 日まで
農林水産省がエンドユーザーであることを証明する書面	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もの	2027 年3月 24 日まで

イ　成果物の納品方法

- 成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
- 用字・用語・記述符号の表記については、「公用文作成の考え方（令和 4 年 1 月 11 日内閣官房長官通知）」を参考にすること。
- 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。
- 作成した成果物は担当部署が指定したサーバへ納品（PrimeDrive 等）すること。なお、納品の際は、検収が終了したファイル一式を時点がわかるような形式（例：zip 等）で提出すること。
- サーバ納品について、Microsoft Office 又は PDF のファイル形式で作成すること。
- 納品後、担当部署において改変が可能となるよう、図表等の元データも併せて納品すること。
- 各ファイルについて、原則として日本産業規格 A 列4番または日本産業規格 A 列3番紙媒体に、収まりよく印刷ができるように適切な印刷設定を行うこと。
- 成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。
- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。
- 上記に加えて紙媒体についても作成し、担当部署から特別に示す場合を除き、原則紙媒体は1部を納品すること。
- 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。

ウ　成果物の納品場所

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

〒305-8535
茨城県つくば市観音台2丁目1－22
農林水産省　動物医薬品検査所　企画連絡室

5　満たすべき要件

運用保守及び基盤提供業務の実施に当たっては、担当部署が承認した「動物用医薬品等データベース」の運用保守計画及び運用保守実施要領の各要件を満たすこと。

本システムの性能目標として、web ページのパフォーマンスを評価するツールを用い、原則月に1回、アクセス頻度が高いページについて、業務時間帯に以下の指標項目を測定し、合格となるよう対応すること。

・Largest Contentful Paint (LCP)

・First Input Delay (FID)

・Cumulative Layout Shift (CLS)

（1） 可用性について

ア 「動物用医薬品等データベース」の可用性にかかる目標値は表4のとおり。サービスの継続性を確保するため、「動物用医薬品等データベース」の各業務の停止時間が復旧目標時間として以下の表で示す目標値を下回ることのない運用を可能とし、障害時には迅速な復旧を行う方法または機能を備えること。

表5 可用性に係る目標値

設定対象	目標稼働率値	補足
動物用医薬品等データベース	99.48%	計画的に停止する場合は除く。 業務アプリケーションを利用するために必要な全体の稼働率から算出する。

イ 可用性に係る対策は以下の通り

（ア） 障害復旧時間を 24 時間以内とすること。（クラウドサービスのユーザーとして対処可能な範囲とする。）

※障害検知：保守員がアラート等で認知した後で、かつ障害と判断する前

（イ） バックアップの世代は、データバックアップ3世代（日次）、システムバックアップ2世代（システム更新毎）とする。ただし、クラウドサービスの機能を使用することにより、同等の時点への復旧が可能な場合はこの限りではない。また、データの保存はシステムを稼働する拠点とは異なる拠点に保存が可能となる拡張性を有する。

（2） 完全性について

ア 機器の故障に起因するデータの滅失や改変を防止する対策を講ずること。

イ 異常な入力や処理を検出し、データの滅失や改変を防止する対策を講ずること。

ウ 処理の結果を検証可能とするため、ログ等の証跡を残すこと。

エ データの複製や移動を行う際に、データが毀損しないよう、保護すること。

オ　データの複製や移動を行う際に、その内容が毀損した場合でも、毀損したデータおよび毀損していないデータを特定するための措置を行うこと。

カ　利用する基盤サービスは、AWS とする。

（3）システム稼働環境について

動物用医薬品等データベースの構成（コンテナ、サーバ、DB、ストレージ）は以下の通り。

表6　コンテナー覧

区分	種別	OS	タスク数	vCPU	メモリ（GB）	実行時間	ディスク（GB）	設置場所
公開 web・APサーバ	ECS	Linux	1	4	8	24 時間 365 日	20	AWS
バッチ処理	ECS	Windows	1	2	4	都度	20	AWS
バッチ処理	ECS	Linux	1	2	4	都度	20	AWS

表7　サーバー覧

区分	種別	OS	インスタンスタイプ	vCPU	メモリ（GB）	実行時間	ディスク（GB）	設置場所
踏み台サーバ	EC2	Windows	m6a.large	2	8	都度	100	AWS

表8　DB 一覧

区分	種別	インスタンスタイプ	vCPU	メモリ（GB）	ディスク（GB）	設置場所
DB サーバ（Writer）	Aurora（MySQL）	db.r6g.xlarge	4	32	－ ※自動拡張	AWS
DB サーバ（Reader）	Aurora（MySQL）	db.r6g.xlarge	4	32	－ ※自動拡張	AWS

表9　ストレージー覧

区分	種別	用途	ストレージクラス	容量（GB）	設置場所	備考
各種ログ保存用	S3	本システムへのアクセスやサーバログを保存する。	スタンダード	無制限	AWS	
AWS 監査ログ保存用	S3	監査ログを保存する。	スタンダード	無制限	AWS	MAFF クラウド管理者アカウントに存在
一時ファイル保存用	EFS	Web・AP サーバが出力する一時ファイルを保存する。	スタンダード	無制限	AWS	Web・AP サーバからマウントして使用

（4） ネットワーク構成について

ア　ネットワーク全体構成

イ　新たに回線を導入する場合は、以下に記載した仕様とすること。

表 10 回線の要件

回線種別	ネットワーク要件	備考
インターネット	インターネット接続、100Mbps（ベストエフォート）	

（5） クラウドサービスの要件について

ア 基盤提供について

内容は、以下に記載した仕様とすること。なお、その際は「政府機関の情報セキュリティ対策のための統一基準（最終改定令和7年6月 27 日サイバーセキュリティ戦略本部決定）」に準拠したクラウドサービスにより情報システム基盤を提供するものとする。

表 11 クラウドサービス要件

項目	要件
サーバホスティング	・ システムが動作する環境をクラウドとして提供可能なこと。 ・ サーバ用途（コスト、性能、信頼性）に応じて複数のサービスメニューを用意し、バランスよく配置が可能なこと。 ・ ポータルを利用し、監視設定や仮想サーバの作成、インシデント問合せ、リソース利用状況の確認が可能であること。

項目	要件
ネットワークサービスの提供	・ ネットワーク設備の提供を可能とすること。 ・ ファイアウォール（仮想、物理共有、物理占有のいずれか）の提供を可能とすること。 ・ SSL 暗号化/復号機能の提供を可能とすること。 ・ 特定の回線事業者に限ることなく、外部回線と安全かつ柔軟に接続が可能なこと。
死活監視サービスの提供	・ 仮想サーバに対する死活監視（Ping、Port 監視、Web、サーバからのメール送信等）の実施が可能なこと。 ・ リソース監視（CPU、メモリ、ディスク）が可能なこと。 ・ プロセス監視が可能なこと。 ・ ログ監視（Syslog、イベントログ、指定されたログ）が可能なこと。 ・ ジョブ実施状況監視が可能なこと。 ・ 各サーバの監視項目及び閾値については、以下のとおり。 ◆ サーバの CPU 使用率 5 分平均が 75%を超えた場合アラート ◆ サーバのメモリ使用率 5 分平均が 75%を超えた場合アラート ◆ サーバの死活監視 1 分以内に 1 回検知でアラート ◆ サーバの HTTP 応答のうち、5xx と 4xx のレスポンスコードの場合（エラーコード） アラート
セキュリティ監視	・ 情報セキュリティ監視、不正アクセスの検知等を行い、調査に必要な対応をすること。
バックアップ管理	・ 上記可用性の要件を満たすこと。なお、バックアップ管理はクラウドサービスの利用も可とする。
冗長化の提供	・ 仮想サーバ冗長化構成の提供が可能なこと。 ・ 仮想サーバ利用ストレージ内のディスク冗長化の提供が可能なこと。
施設・設備	・ 利用するデータセンターは国内にあること。 ・ 国内の単一拠点内において、独立した電源、冷却手段、ネットワークをもつ複数のデータセンターを組み合わせた、高可用性サービスを利用できること。 ・ 国内に複数の拠点を持つこと。
その他	・ 対応時間は 24 時間 365 日であること。

イ 運用要件について

動物用医薬品等データベースの運用要件は以下のとおり。

表 12 システム運用要件

作業名	作業概要	監視項目例
可用性管理	・ 利用するクラウドサービスについて、上記可用性で定める目標値が満たされていることを監視すること。	・ サービスレベル等
セキュリティ監視	・ 情報セキュリティに関する事象の発生状況を監視すること。	・ 不正アクセス件数 ・ ウイルス検知数 ・ 不正侵入検知数 等
バックアップ管理	・ 上記可用性に記載した内容を満たすようにデータ及びシステム構成情報、OS、ミドルウェア等のソフトウェア、アプリケーション等について、バックアップを行うこと。 ・ 障害発生時に、直近のバックアップ採取時点のシステム状態に速やかに復旧可能となるように、バックアップを取得すること。	・ 定時バックアップ率 ・ バックアップ実施回数 ・ バックアップデータからの復旧回数 等
障害復旧対応	・ 障害発生時に影響度等の分析を行った上で、障害による影響を最小限にとどめ、情報システムの復旧作業を行うこと。	・ 障害復旧時間 等
セキュリティパッチ運用等業務	・ 事前検証を実施の上、セキュリティパッチの適用やアップデートを実施すること。 ・ 緊急の対応が必要な場合は担当部署と協議の上、実施すること。	・ セキュリティパッチ適用件数 ・ アップデート実施件数 等
ログ管理	・ 情報システムのログを管理すること。	・ Windows イベントログ
構成管理	・ ハードウェアやソフトウェア製品、ネットワーク等の情報システムを構成する資産の管理を行うこと。	・ 構成変更件数 等

作業名	作業概要	監視項目例
基盤運用に関する問合せ対応	・ 担当部署からの基盤の運用に関する問合せに対応すること。なお、受付時間は、電子メールの場合 24 時間、電話の場合平日 9:30 から 18:00(行政機関の休日は含まない。)までとすること。	

ウ　保守要件について

動物用医薬品等データベースの保守要件は以下のとおり。

表 13 システム保守要件

作業項目	作業概要
クラウドサービスの保守	・ 上記可用性に示す目標値を下回らないようにすること。 ・ 基盤が健全であるか、定期点検を行う。 ・ システム運用に資するため、クラウドサービスに関する担当部署からの問い合わせに対応する。 ・ クラウドサービス事業者から提供されたメンテナンス、事故発生などの情報について、担当部署に遅滞なく伝達する。 ・ 本システムが利用するクラウドサービスに不具合等が発生した場合は、担当部署に速やかに報告するとともに迅速に復旧させること。 ・ ロードバランサーに適用している SSL 証明書の有効期限を確認し、期限が近い場合は AWS Certificate Manager で期限更新を確認すること。

エ　セキュリティ要件について

動物用医薬品等データベースのセキュリティ要件は以下のとおり。

表 14 情報システムのセキュリティ要件

No.	情報セキュリティ対策	対策に係る要件	システム	クラウドサービス
1	通信経路の分離	不正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通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。		○
2	不正通信の遮断	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。	○	○
3	通信のなりすまし防止	情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備える。	○	
4	サービス不能化の防止	サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。	○	○
5	不正プログラムの感染防止	不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。		○
6	不正プログラム対策の管理	システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。		○

No.	情報セキュリティ対策	対策に係る要件	システム	クラウドサービス
7	ログの蓄積・管理	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、1年間保管できるようにするとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。	○	○
8	ログの保護	ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。	○	○
9	時刻の正確性確保	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。	○	○
10	侵入検知	不正行為に迅速に対処するため、府省庁内外で送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、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。		○
11	サービス不能化の検知	サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。		○
12	ライフサイクル管理	主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。	○	○

No.	情報セキュリティ対策	対策に係る要件	システム	クラウドサービス
13	アクセス権管理	情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。	○	○
14	管理者権限の保護	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。	○	○
15	通信経路上の盗聴防止	通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	○	○
16	保存情報の機密性確保	情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	○	○
17	保存情報の完全性の確保	情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。	○	・

No.	情報セキュリティ対策	対策に係る要件	システム	クラウドサービス
18	システムの構成管理	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、構築時の情報システムの構成（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し、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。	○	○
19	調達する機器等に不正プログラム等が組み込まれることへの対策	機器等の製造工程において、府省庁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。	○	○
20	情報セキュリティ水準低下の防止	情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。	○	○
21	プライバシー保護	情報システムに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。	○	○
22	主体認証	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、認証コード（ID）とパスワードによる主体認証の方式を採用すること。主体認証情報の推測や盗難等のリスクの軽減を行う機能として、2段階認証の機能を付けること。		○

No.	情報セキュリティ対策	対策に係る要件	システム	クラウドサービス
23	システムの可用性確保	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として 24 時間を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。		○
24	構築時の脆弱性対策	情報システムを構成するソフトウェアおよびハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な億弱制は修正の上で納入すること。	○	○
25	運用時の脆弱性対策	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。	○	○
26	委託先において不正プログラム等が組込まれることへの対策	情報システムの構築において、府省庁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。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁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、受託者は情報セキュリティ監査を受入れること。 また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。	○	○

６　作業の実施体制・方法

（1） 作業実施体制

本業務の推進体制及び本業務受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者内の人員構成については想定であり、受注者決定後に協議の上、見直しを行う。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

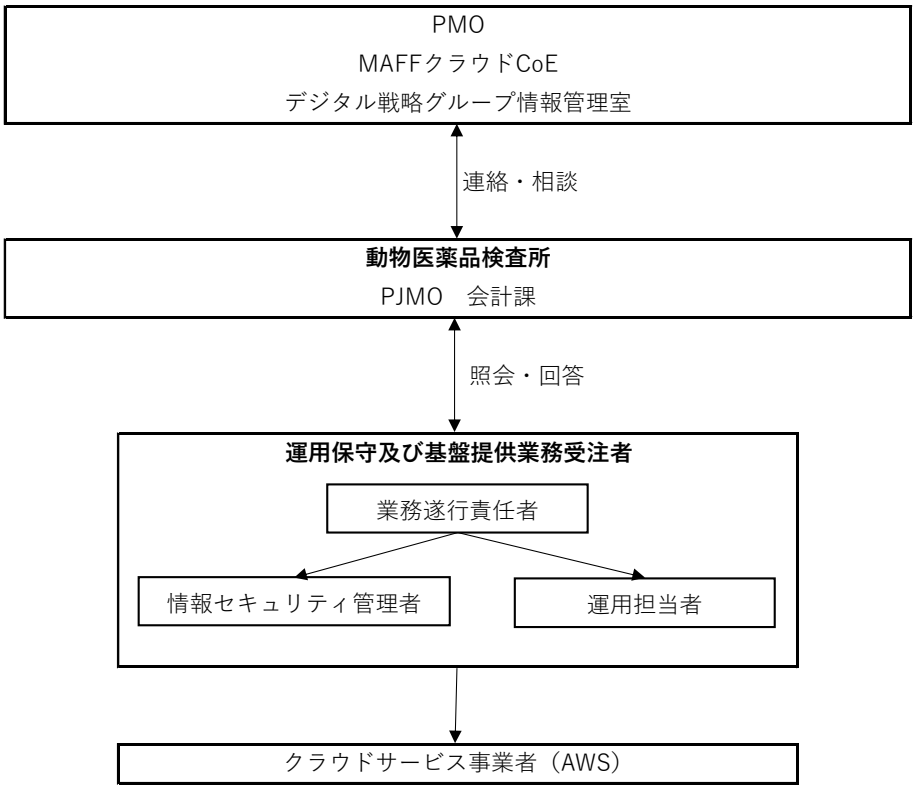

図 ５ 本業務の推進体制及び本業務受注者に求める作業実施体制

表 15 本業務における組織等の役割

組織等	本業務における役割
PMO／デジタル戦略グループ情報管理室	農林水産省の全体管理組織。クラウド利用を含む情報システムに関する担当部署からの問い合わせを受け、対応、助言・指導等を行う。
MAFFクラウドCoE	PJMO・受注者に対してMAFFクラウド利用に係る技術的な支援を行う。
動物医薬品検査所 PJMO	動物用医薬品等データベースの管理組織として、本業務の進捗等を管理する。 ・責任者: 農林水産省動物医薬品検査所企画連絡室長 ・プロジェクト責任者: 農林水産省動物医薬品検査所企画連絡室企画調整課長 （サブシステム）企画連絡室技術指導課長
運用保守業務及び基盤提供業務受注者	本業務の受注者 動物用医薬品等データベースの運用保守業務の実施 動物用医薬品等データベースの基盤の提供

表 16 本業務受注者に求める作業実施体制の役割

組織等	本業務における役割
遂行責任者	• 本業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。 • 原則として全ての進捗会議に出席する。
運用担当者	受注した業務を実施する。
情報セキュリティ管理者	本業務の情報取扱い全てに関する監督を担う。

（2） 作業要員に求める資格等の要件

受注者は、本業務の遂行責任者及び担当者等の役割に応じて次に示すスキル・経験を持つ人員を充て、プロジェクト全体として全ての要件を満たす作業実施体制とすること。

ア 受注者における遂行責任者は、日本語で円滑なコミュニケーションが可能で、「標準ガイドライン」の内容を理解し、本業務を円滑に運営する能力を有すること。

イ 受注者における遂行責任者は、システム（利用者 100 名以上）の運用又は保守の遂行責任者としての経験を3年以上有すること。

ウ 受注者における遂行責任者は、独立行政法人情報処理推進機構の IT スキル標準、IT サービスマネジメントの各スキル項目について、スキル熟達度レベル4以上に相当すること。

エ 動物用医薬品等データベースの運用保守に関わるメンバーのうち、少なくとも 1 名はクラウドサービスを用いた情報システムの構築又は構築を支援する業務のいずれかの経験を有する者を配置すること。

オ 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 ／ AWS solutions architect professional

カ　応札者は、本システムで利用中のパブリッククラウド（AWS）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。

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

（ウ）　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

（エ）　課題・改善点を識別し、改善する能力

（オ）　本業務を履行するうえで適当な AWS のスキル

（3）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

ア　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、発注者から受注者に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。

イ　農林水産省の情報システムにおけるクラウドサービスの契約は、農林水産省を契約者として契約すること。本業務の契約とクラウドサービスの契約は別に契約することが必要であることを理解して対応すること。

ウ　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。

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

オ　農林水産省の情報システムにおけるクラウドサービスの契約は、AWS の場合、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。

（4）作業場所

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

（5）作業の管理に関する要領

受注者は、担当部署が承認した運用保守計画書及び運用保守実施要領に従い、記載された成果物を作成すること。その際、運用保守計画書及び運用保守実施要領に従い、コミュニケーション管理、体制管理、作業管理、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。

7　作業の実施に当たっての遵守事項

（1） 機密保持、資料の取扱い

ア　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３月 31 日農林水産省訓令第４号。以下「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。

イ　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） 委託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） 受注事業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。

（キ） 生成 AI システム特有のリスクケース等が発生した場合、受注者は関係するデータの提供や調査等に協力すること。

（ク） 本業務の開発・運用において、ソースコード解析やソースコード生成、ソースコードの管理を行う際には、セキュリティ・バイ・デザイン（DS-200）を元に、情報セキュリティ対策の責任者を定め、開発環境や開発工程等も含めたすべてのライフサイクルに対してぬけ漏れなく情報セキュリティ対策を実行すること。

ウ　上記以外に、別紙5「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部署と協議の上決

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）個人情報の取扱いに関する責任者が情報管理責任者と異なる場合には、個人情報の取扱いに関する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を提出し、担当部署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。

オ　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委託する場合は、受注者（必要に応じ農林水産省）は、原則として年１回以上の再委託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。

カ　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）法令等の遵守

ア　関係法令の遵守

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

（ア）エネルギーの節減

a　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）

（イ）廃棄物の発生抑制、適正な循環的な利用及び適正な処分

a　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）

b　国等による環境物品等の調達の推進等に関する法律 （平成 12 年法律第

100 号）

c　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）

d　労働安全衛生法（昭和 47 年法律第 57 号）

e　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）

（4） 環境負荷低減に係る遵守事項

受注者は、物品・役務（委託事業を含む）の提供に当たり、新たな環境負荷を与えることにならないよう、事業の最終報告時に様式（別紙6）を用いて、以下の取組に努めたことを、みどりチェック実施状況報告書として提出すること。なお、全ての事項について「実施した/努めた」又は「左記非該当」のどちらかにチェックを入れるとともに、ア～エの各項目について、一つ以上「実施した/努めた」にチェックを入れること。

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　廃棄物の発生抑制、適切な循環的な利用及び適正な処分に努める。

エ　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） 標準ガイドラインの遵守

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

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-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン

エ　DS-670.1 ユーザビリティガイドライン

オ　DS-680.1 ウェブサイトガイドライン

カ　DS-680.2 ウェブコンテンツガイドライン

キ　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

ク　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

ケ　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

（6） その他文書、標準への準拠

ア　プロジェクト計画書等

本業務の遂行に当たっては、担当部署が定めるプロジェクト計画書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。

イ　アプリケーション・コンテンツの作成規程

（ア） 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。

（イ） 提供するアプリケーションにぜい弱性を含めないこと。

（ウ） 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。

（エ） 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。

（オ） 提供するアプリケーション・コンテンツの利用時に、ぜい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。

（カ） 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。

（キ）「.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、担当部署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。

（ク） 詳細については、担当部署から「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。

（7） 情報システム監査

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

イ 情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担

当部署と協議し、指示された期間までに是正を図ること。

（8） データマネジメント・データ活用要件

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。

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

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

8 成果物の取扱いに関する事項

（1） 知的財産権の帰属

ア 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等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。

イ 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部署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。

ウ 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。

エ 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。

オ　本調達に係る成果物の関する権利（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。

カ　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。

キ　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。

（2）契約不適合責任

ア　農林水産省は検収（「検査」と同義。以下同じ。）完了後、成果物についてシステム仕様書との不一致（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、受注者は、当該追完を行うものとすること。ただし、農林水産省が追完の方法についても請求した場合であって、農林水産省に不相当な負担を課するものでないときは、受注者は農林水産省が請求した方法と異なる方法による追完を行うことができること。

イ　前記アの場合において、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。

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

（ア）追完が不能であるとき。

（イ）受注者が追完を拒絶する意思を明確に表示したとき。

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

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

エ　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。

オ　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、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こと。

カ　受注者が本項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１年以内に農林水産省から当該契約不適合を通知された場合に限るものとすること。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きにはこの限りでない。

キ　前記アからカまでの規定は、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。

（3）検収

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

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

９　競争参加資格に関する事項

（1）競争参加資格

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

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

（2）公的な資格や認証等の取得

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

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

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

イ　応札者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。

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

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

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

（3）受注実績等

ア　100 名以上の職員が利用する情報システムの運用又は保守業務を行った実績を、直近5年以内に有すること。

イ　受注者は、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。

ウ　クラウドサービスについて

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。

（4）入札制限

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委託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。

10 その他特記事項

（1）前提条件等

ア　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。

イ　本業務に関する契約の締結は、令和8年度の予算成立を条件とする。令和8年4月1日以前に令和8年度予算が成立していない場合には契約締結の中止等を行う可

能性があり、この場合、農林水産省は、契約締結の中止等に伴ういかなる責任も負担しない。

ウ　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担当部署に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が確認することによって変更を確定する。

エ　本業務に使用する言語（会話によるコミュニケーションを含む。）は日本語、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。

オ　MAFF クラウドについて不明点等がある場合は、担当部署及び MAFF クラウド CoE と協議の上、作業を進めること。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。

（2）入札公告期間中の資料閲覧等

本業務の実施に参考となる過去の類似業務の報告書等に関する資料については、農林水産省動物医薬品検査所内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に担当部署まで連絡の上、閲覧日時を調整すること。

ア　資料閲覧場所

茨城県つくば市観音台2丁目1－22

農林水産省動物医薬品検査所企画連絡室

イ　閲覧期間及び時間

（ア）公告日から入札日前日まで

（イ）行政機関の休日を除く日の 10 時から 17 時まで。（12 時から 13 時を除く。）

ウ　閲覧手続

最大3名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別記様式1「閲覧申込書」に記載の上、閲覧希望日の3日前までに提出すること。また、閲覧日当日までに別記様式2「守秘義務に関する誓約書」に記載の上、提出すること。

エ　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。

オ　連絡先

農林水産省　動物医薬品検査所　企画連絡室

電話 029-811-6964

Email：nval_kikakuchouseika@maff.go.jp

カ　事業者が閲覧できる資料

閲覧に供する資料の例を次に示す。

（ア）遵守すべき各府省独自の規定類

a　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

b　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

（イ）「動物用医薬品等データベース」の設計書

（3）その他

本仕様書について疑義等がある場合は、応札希望者は別記様式3「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。

11　附属文書

（1）別紙1　AWS/Azure 設定確認リスト

（2）別紙2　web システム/web アプリケーションセキュリティ要件書

（3）別紙3　情報システムの経費区分

（4）別紙4　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

（5）別紙5　情報セキュリティの確保に関する共通基本仕様

（6）別紙6　みどりチェック実施状況報告書

（7）別記様式1　閲覧申込書

（8）別記様式2　守秘義務に関する誓約書

（9）別記様式3　質問書

以　上

AWS・Azureセキュリティ設定確認リスト　　凡例：〇：責任者、△：サポート

※各リソースの詳細な設定についてご不明な点等ございましたら別途お問合せください。

セキュリティ設定確認リスト（AWS/Azure）	担当		役割分担に関する補足
	MAFFクラウド管理者(PMO)	PJMO	
IDおよびアクセス管理			
組織が許可したアカウントの管理		〇	
管理者アカウントに対する多要素認証の利用		〇	PJMOに一任
管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し		〇	年度初めに実施
必要最低限の管理者権限の割当て		〇	PJMOに一任
グループを利用した権限の設定		〇	
管理者アカウントに関する復旧手段の確保		〇	
すべてのアカウントへのパスワードポリシーの適用		〇	
アクセスキー、サービスアカウントキー等の適切な管理		〇	
管理者アカウントと日常的に使用するアカウントの分離		〇	ユーザーの払い出しはPJMO管理
アカウント・権限・認証情報の定期的な見直し		〇	年度初めに実施
AWSにおいて考慮すべき設定			
AWS サポートセンターへのアクセス設定		〇	PJMOに一任
IAM Access analyzerの有効化		〇	PJMOに一任
Azureにおいて考慮すべき設定			
Microsoft Azure サポートセンターへのアクセス設定		〇	PJMOに一任
事業者への権限付与		〇	PJMOに一任
ログ（アクセスログ）の記録と監視			
ログの有効化及び取得	△	〇	MAFFクラウド共通機能「監査ログ収集機能」で下記のログは収集。 その他のログについてはPJMOに一任。 AWS：Configの「Configsnapshot」「Confighistory」・CloudTrailの証跡ログ・VPCフローログ・GuardDutyの検出結果 Azure：Microsoft Defender for Cloudの評価結果・Activity Log・VNetフローログ・Azure Policyの評価結果
ログの一元管理	△	〇	同上
ログの保護	△	〇	同上
ログの監視/通知の設定		〇	PJMOに一任
ネットワーク			
ロードバランサの接続設定		〇	PJMOに一任
DDoS対策		〇	PJMOに一任
SSL/TLS証明書の設定・管理		〇	PJMOに一任
AWSにおいて考慮すべき設定			
セキュリティグループの設定		〇	PJMOに一任
Azureにおいて考慮すべき設定			
ネットワークセキュリティグループ（NSG）の設定		〇	PJMOに一任
他セキュリティ全般			
不適切な設定を検知するサービスの導入	〇	△	MAFFクラウド共通機能「不適切設定検知機能」により設定 AWS：Config・Security Hub Azure：Azure Policy
クラウド環境内の脅威を検知するサービスの導入	〇	△	MAFFクラウド共通機能「マネージド型脅威検出機能」により設定 AWS：GuardDuty Azure：Microsoft Defender for Cloud
攻撃対象となるネットワークポートへのアクセス制限		〇	PJMOに一任
各サービスにおける不要な匿名/公開アクセスのブロック		〇	PJMOに一任
各サービスにおけるデータ・通信の暗号化		〇	PJMOに一任
不正プログラム対策ソフトウェアの導入		〇	IDS/IPS対策（※要否については応相談）
脆弱性管理			
最新のOSパッチの適用確認		〇	
インベントリ収集機能の有効化	〇	△	MAFFクラウド共通機能「インベントリ収集機能」を有効化し、管理者アカウントで監視
AWSにおいて考慮すべき設定			
Amazon Inspectorの有効化		〇	PJMOに一任
コンテナにおける脆弱性対策		〇	ECR（基本スキャン）またはInspector（拡張スキャン）を利用
Azureにおいて考慮すべき設定			
コンテナにおける脆弱性対策		〇	Defender CSPMまたはDefender for Containersを利用 ※基本的にはDefender for Containersを利用（脆弱性診断の性能に差はほとんどない一方、Defender CSPMはサブスクリプション内のリソース毎に料金が発生するため、 Defender for Containersに比べコストが高くなりやすい）
バックアップ			
各サービスのバックアップ設定		〇	PJMOに一任

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２　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 目的により、投資的整備と維持的整備のものに分けられる。 ・　投資的整備 国民・利用者の利便性向上・負担軽減や業務効率化、経済効果の創出、システムのスリム化などの面で積極的に効果を得ることを目的として行うもの（注１） ・　維持的整備 外部環境の変更等により生じる障害の回避を目的として、義務的に行うもの（仕様変更を伴うが積極的に効果を得ることを目的としないもの）（注２）
	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　サービス利用料	情報システムの整備に当たって、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及び国の行政機関以外の者が提供するサービスの利用開始に要する経費
	ス　その他整備経費	アからシ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

経費区分		摘要
	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
	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

経費区分			摘要
		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

（注１）以下の例による。

- 紙による行政手続のオンライン化による国民の利便性向上に有効なもの
- ワンストップ化による国民の来訪回数の低減など国民の負担軽減に有効なもの
- 行政事務の自動化又は時間短縮などに有効なもの
- 運用等経費など将来の経費削減に有効なもの

（注２）以下の例による。

- 法令改正等により現行の仕様のままでは法令等に違反する状態になることを避けるために行うもの
- 災害発生等の情報収集及び人々の避難等の行動につなげるなど国民の身体への悪影響又は経済的損失を回避するためのもの
- サイバー攻撃による基盤となる情報システムの停止などを回避するためのもの
- 重要インフラの停止など社会混乱を回避するためのもの
- パソコンやネットワークの更新など行政事務の停止を回避するためのもの

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

調達を行うときは、調達内容に応じ、少なくとも次の１．及び２．に定める作業内容を調達仕様書に盛り込むものとする。また、３．に掲げる項目については、必要に応じて、適宜様式を定めた上で適時に内容を記載することを調達仕様書に盛り込むものとする。

■ 契約金額内訳

「別紙２　情報システムの経費区分」に基づき区分等した契約金額の内訳を、デジタル庁から作業依頼のある時期（原則毎年度末）に提出すること。

■ 情報資産管理標準シートの提出

情報資産管理標準シートを、デジタル庁から作業依頼のある時期（原則毎年度末）に提出すること。

■ その他

1)　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

2)　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

3)　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

4)　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

5)　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

6)　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

7)　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

8)　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

9) **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。

10) **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

11) **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

12) **スケジュールや工数等の管理**

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

（別紙５）

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６】

様式

みどりチェック実施状況報告書

事業名	
事業者名	
担当者・連絡先	

以下のア～カの取組について、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。	□	□
・夏期のクールビズや冬期のウォームビズの実施に努めている。	□	□
・その他（　　）		

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

ウ　廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

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

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

エ　みどり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
・「環境配慮のチェック・要件化（みどりチェック）チェックシート解説書 －民間事業者・自治体等編－」にある記載内容を了知し、関係する事項について取り組むよう努める。	□	□
・事業者として独自の環境方針やビジョンなどの策定している、もしくは、策定を検討する。	□	□
・従業員等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
（　　）

（別記様式1）

閲覧申込書

「動物用医薬品等データベース運用保守及び基盤提供業務」に係る資料を閲覧したいので、下記日程で資料閲覧を申し込みます。

	希望日	時間
第一希望	月　日（ ）	
第二希望	月　日（ ）	
第三希望	月　日（ ）	

【記入方法】

・第1希望から第3希望まで記入してください。

・閲覧を希望する最も早い日の3営業日前までに動物医薬品検査所　企画連絡室　担当宛にメールで提出してください。

提出先：動物医薬品検査所　企画連絡室

e-mail：　nval_kikakuchouseika@maff.go.jp

・動物医薬品検査所から、最も早い閲覧希望日の前日の 12 時までに閲覧日時をご連絡いたします。

・閲覧希望時間は下表の①～③の中から選択して記入してください。

	時間
①	10 時～12 時
②	13 時 15 分～15 時 15 分
③	15 時 30 分～17 時 30 分

連絡先

会社名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

部署名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

氏名：＿＿＿＿＿＿＿＿＿＿＿＿

TEL：＿＿＿＿＿＿＿＿＿＿＿＿

E-MAIL：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（別記様式2）

守秘義務に関する誓約書

動物医薬品検査所長　殿

＿＿＿＿＿＿＿＿＿＿＿＿（以下「弊社」という。）は、このたび、農林水産省動物医薬品検査所（以下「貴所」という。）の行う「動物用医薬品等データベース運用保守及び基盤提供業務」の入札等（以下「本入札等」という。）に関する資料を閲覧に関し、以下の事項を誓約します。

第1条（守秘義務の誓約）
弊社は、貴所の許可なくして、社外はもちろん貴所職員で本件に直接関与していない者に対しても、本入札等に関し弊社が知り得たすべての事項・情報を開示、漏洩し、若しくは自ら使用しないことを約束します。

第2条（資料複写の禁止等）
弊社は、守秘義務を厳守するため、貴所より本入札等に関し、開示された資料一切の複写をしないことを約束し、貴所より返還要求された場合、これらの資料及びコピー並びにそれらに関する資料の一切を直ちに返還することを約束します。

第3条（入札等後の守秘義務について）
弊社は、貴所において本入札等が行われた後といえども、第1条記載の事項・情報を開示、漏洩若しくは使用しないことを約束します。

第4条（守秘義務違反後の処置）
弊社は、貴所と約束した守秘義務に反した場合は、貴所が行う合法的処置を受けることを約束します。

令和　　年　　月　　日

住　所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
会社名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
代表者＿＿＿＿＿＿＿＿＿＿＿＿＿＿

機密性2情報

（別記様式3）

質問書

質問者会社名、所属:

質問者氏名:

質問者（連絡先）電話:

電子メール:

No	質問者記入欄			動物医薬品検査所記入欄		備　　考
	質問日	目次	質問事項	回答日	回答内容	
1						
2						