違法輸入動植物等流通監視システム
整備業務

調達仕様書
（案）

農林水産省
消費・安全局植物防疫課
令和8年 11 月

目次

１　調達案件の概要 3

（１）　調達件名 3

（２）　調達の背景 3

（３）　調達目的及び調達の期待する効果 3

（４）　業務・情報システムの概要 4

（５）　契約期間 5

（６）　作業スケジュール 5

２　調達案件及び関連調達案件 6

（１）　調達範囲 6

（２）　調達案件の一覧 6

（３）　調達案件間の入札制限 6

３　情報システムに求める要件 6

４　作業の実施内容 7

（１）　設計・開発実施計画書等の作成 7

（２）　要件定義内容の調整・確定 7

（３）　設計 7

（４）　開発・テスト 10

（５）　受入テスト支援 10

（６）　システムのリリース（本番稼働） 11

（７）　教育（マニュアル作成・研修） 11

（８）　運用・保守実施要領の作成 11

（９）　クラウドサービスを運用保守する場合の前提 12

（１０）　定常時対応 12

（１１）　障害発生時対応 13

（１２）　定例会等の実施 14

（１３）　情報システムの現況確認支援 14

（１４）　契約金額内訳及び情報資産管理標準シートの提出 14

（１５）　プロジェクト計画書の更新支援 15

（１６）　引継ぎ 15

（１７）　成果物の作成 16

５　機能要件、非機能要件等に関する事項 18

６　業務の実施体制・方法 18

（１）　業務実施体制 18

（２）　作業要員に求める資格等の要件 20

（３）　作業場所 20

（４）　作業の管理に関する要領 20

（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 21

７　作業の実施に当たっての遵守事項 **21**
（１）　機密保持、資料の取扱い 21
（２）　個人情報の取扱い 22
（３）　法令等の遵守 22
（４）　環境負荷低減に係る遵守事項 23
（５）　標準ガイドラインの遵守 23
（６）　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 23
（７）　その他文書、標準への準拠 24
（８）　情報システム監査 25
（９）　セキュリティ要件 25
（１０）　データマネジメント・データ活用要件 26
（１１）　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 26
８　成果物の取扱いに関する事項 **26**
（１）　知的財産権の帰属 26
（２）　契約不適合責任 27
（３）　検収 28
９　入札参加資格に関する事項 **28**
（１）　競争参加資格 28
（２）　公的な資格や認証等の取得 28
（３）　入札実績等 29
（４）　入札制限 29
（５）　複数事業者による共同入札 30
１０　再請負に関する事項 **30**
（１）　再請負の制限及び再請負を認める場合の条件 30
（２）　承認手続 30
（３）　再請負先の契約違反等 31
１１　その他特記事項 **31**
（１）　前提条件 31
（２）　入札公告期間中の資料閲覧等 31
１２　附属文書 **32**
１３　本業務に関する問い合わせ先 **32**

1　調達案件の概要

（1）調達件名

違法輸入動植物等流通監視システム整備業務

（2）調達の背景

近年、訪日・在留外国人の増加や e コマース（EC）の拡大等、国際的なヒトやモノの流れの増加により、我が国への病害虫の侵入リスクが増大しており、実際に海外から持ち込まれる植物等から、我が国が侵入を警戒している病害虫等が多数発見されている。また、令和6（2024）年度は、手荷物や国際郵便による違法な動植物等の持ち込み件数が過去最多を記録し、空港・港湾周辺等では果樹の大害虫であるミバエ類が発見される事例も増加してきている。さらに、輸入される海空港での適切な植物検疫／動物検疫を受けることなく、国内の EC サイトやフリマサイト等で動植物等の販売・譲渡等がなされていると疑われる事例を多数確認しており、その事例を確認する都度、農林水産省植物防疫所／動物検疫所の検査官が電話・メール等による協力依頼及び販売店等への立会い調査等を実施している状況にある。

このような状況を踏まえ、国内の EC サイトやフリマサイト等での流通実態を詳細に捕捉するための「違法輸入動植物等流通監視システム」を構築することで、植物防疫所／動物検疫所の検査官による Web サイトの循環及び情報収集の手間を自動化・省力化するとともに、従来は捕捉が困難であった外国語でのやり取りによる対象品の販売・譲渡等をも捕捉することで出品者及び当該 Web サイト等への更なる抑止効果が期待されている。

なお、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。

また、「情報通信技術を活用した行政の推進等に関する法律の一部を改正する法律」（令和７年法律第４号）が令和７年３月８日に施行されたことから、整備（新規構築又は更改）を行おうとする際には、農林水産省はガバメントクラウドを利用することについての検討を行う必要がある。

これらの状況を踏まえて、本業務においては、ガバメントクラウド上に「違法輸入動植物等流通監視システム」を整備（新規構築）する。

（3）調達目的及び調達の期待する効果

本業務は、「違法輸入動植物等流通監視システム」の整備（新規構築）を目的としている。その結果、従来職員が手作業で担っている一連の作業の自動化により、運用段階での省力化及び即応化

が期待される。

（4） 業務・情報システムの概要

ア 「違法輸入動植物等流通監視システム」の運用段階でのユーザ数の想定は表１のとおりである。詳細は別紙１要件定義書（違法輸入動植物等流通監視システム整備業務）を参照のこと。

表1「違法輸入動植物等流通監視システム」の利用対象組織等

対象組織	利用者数
農林水産省消費・安全局植物防疫課	50 人
農林水産省消費・安全局動物衛生課	50 人
植物防疫所	1,000 人
動物検疫所	700 人

イ クラウドサービスについて

平成 30 年６月に「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：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と等を踏まえ、本システムはガバメントクラウドを利用する。

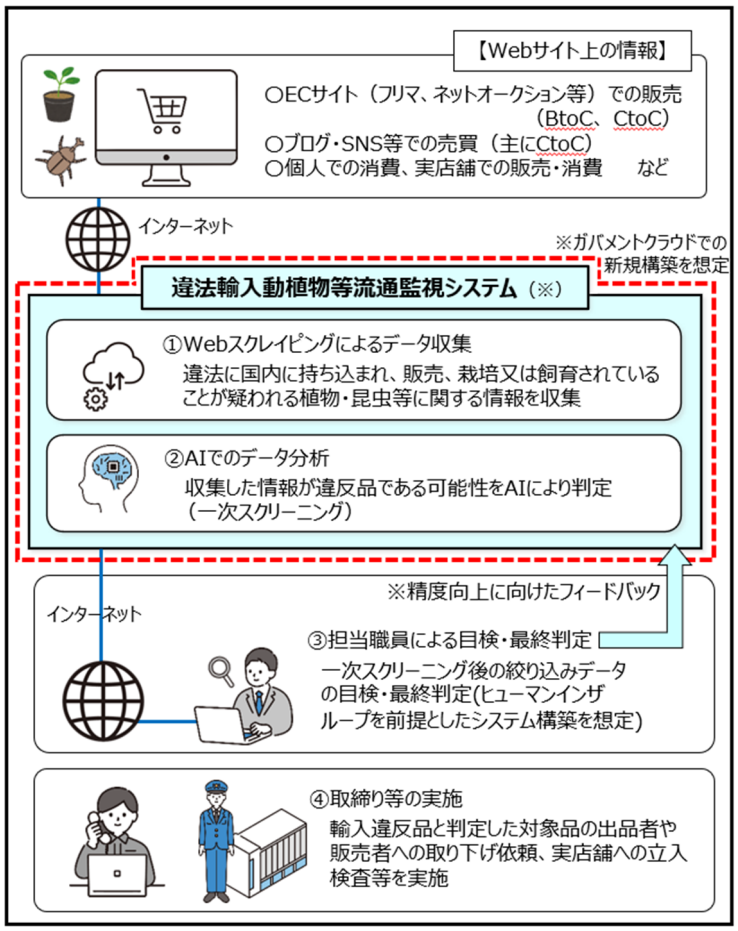
ウ ガバメントクラウドの概要

本調達では、本システムのクラウド化に係る設計・開発業務及び開発後のシステムの運用保守業務を行うものとする。なお、ガバメントクラウド上のクラウド基盤へのログインの際に必要となるFIDO 規格準拠のハードウェアトークンを農林水産省消費・安全局植物防疫課（以下「担当部署」という）向けに５つ調達し、納品すること。なお、受注者にて使用するハードウェアトークンについては受注者の負担にて必要数量を準備すること。また、サービス利用料、ライセンス費用、物品購入等、その費用は受注者の負担とする。開発・検証用の環境については、受注者の負担として、本調達の費用に含めるものとする。ガバメントクラウドの詳細については、「https://guide.gcas.cloud.go.jp」を参照すること。

エ 全体構想

ガバメントクラウド上に、図１の環境を構築することを想定している。

図1　違法輸入動植物等流通監視システムの全体構想図



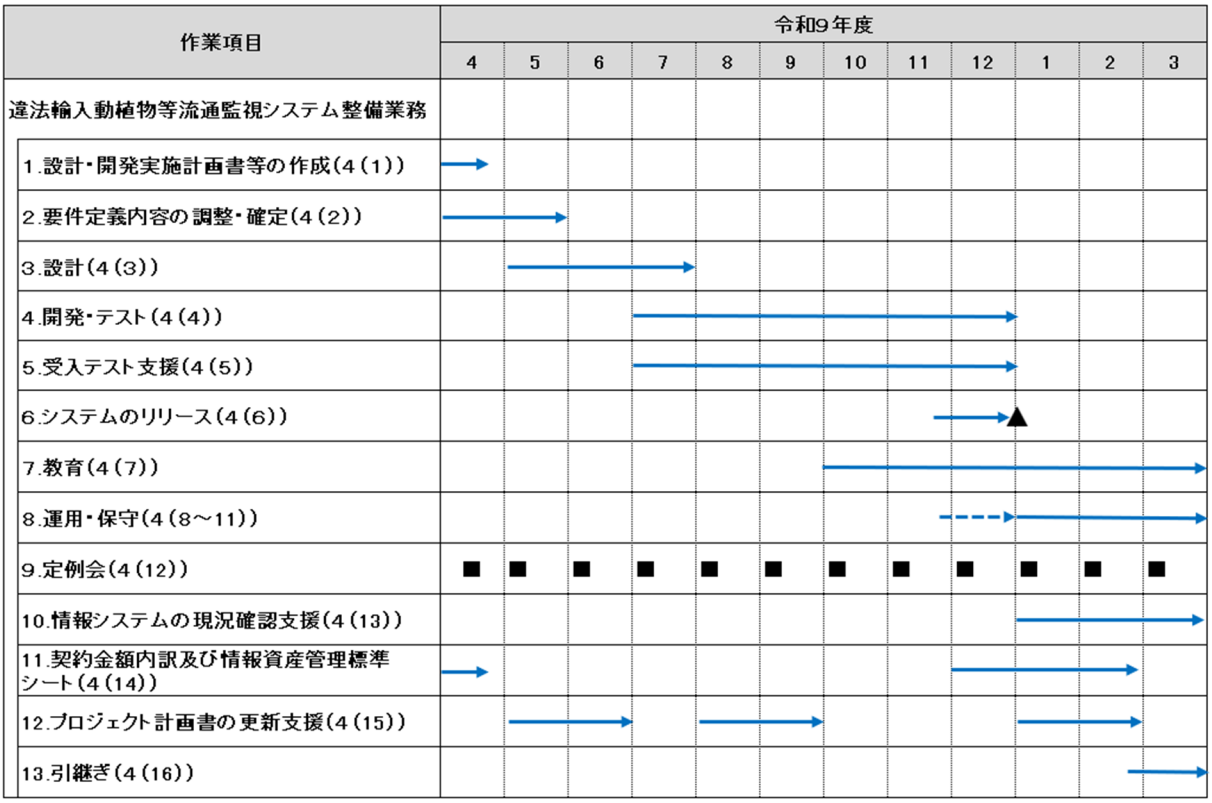
（5）契約期間

契約締結日から令和 10 年 3 月 31 日まで

（6）作業スケジュール

作業スケジュールの想定は図2のとおりである。

図2　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、ガバメントクラウド上での「違法輸入動植物等流通監視システム」の整備（新規構築）及び契約期間終了まで（令和9年度末まで）のシステム運用・保守をその範囲とする。

なお、本調達の実施にあたり必要となる、開発環境の構築費用ならびに当該環境で利用する各種ライセンス等に係る費用を入札金額に含めることとする。また、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開発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、担当部署に状況を申し出ること。

さらに、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

関連する調達案件の調達単位、調達の方式、実施時期等はない（本業務のみ）。

（3）　調達案件間の入札制限

特になし。

3　情報システムに求める要件

設計・開発の実施に当たっては、「別紙1要件定義書（違法輸入動植物等流通監視システム整備業務）」の各要件を満たすこと。

4　作業の実施内容

（1） 設計・開発実施計画書等の作成

受注者は、担当部署が定めるプロジェクト計画書と整合をとりつつ、担当部署の指示に基づき、設計・開発実施計画書及び設計・開発実施要領の案を作成し、担当部署の承認を得ること。

なお、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「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：2026 年 6 月 12 日以下「標準ガイドライン」という。)「第7章　設計・開発」で定義されているものとする。

加えて、ガバメントクラウド利用には、デジタル庁による技術審査を受け、承認を得ること。また、必要に応じて担当部署及び MAFF クラウド CoE と事前協議すること。

設計・開発実施計画書及び設計・開発実施要領は各工程での検討結果等を踏まえて必要に応じて詳細化・更新し、担当部署の承認を得ること。なお、設計・開発実施計画書及び設計・開発実施要領の詳細化・更新にあたり、システム構成の変更・ガバメントクラウド利用額の変動等が生じる場合は、デジタル庁の承認を得ること。また、必要に応じて MAFF クラウド CoE と事前協議すること。

設計・開発・テスト等に際しては、関連する事業者等への依頼・連携が必要であるため、その内容や役割分担を記載すること。

（2） 要件定義内容の調整・確定

ア　受注者は、設計・開発の実施に先立ち、「別紙1要件定義書（違法輸入動植物等流通監視システム整備業務）」（リファレンスアーキテクチャ及びシステム構成図案を含む）の内容を確認すること。その際、内容について調整すべき事項又は構成の最適化が必要な事項があれば、担当部署と調整の上、結果に基づき要件定義書の修正や GCAS 上のシステム情報更新を行うこと。要件の調整内容は、担当部署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。加えて、必要に応じて MAFF クラウド CoE と事前協議すること。

イ　受注者は、「要件定義書（確定版）」に基づき、システム要件及び運用・保守要件を整理すること。その際、利用するクラウドサービスのクラウドサービスプロバイダが提供する上級資格の保有者等、モダンな技術・運用に明るい者が整理を行うこと。

ウ　運用・保守要件の作成にあたり、旧来技術・運用を極力排除するとともに、クラウドサービスに適したリリース方式・セキュリティ対策・運用監視手段 を整理すること。加えて、担当部署の作業の軽減等、効率的なシステム運用・保守に資する内容を反映させること。また、システムリリース後に障害に起因するインシデント及びアプリケーションに関連する問合せ数が削減される等、効率的なシステム運用・保守に資するシステム改修案があれば提案すること。

（3） 設計

ア　受注者は、別紙1要件定義書（違法輸入動植物等流通監視システム整備業務）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（運用設計を含む。）を行い、成果物について担当部署の承認を得ること。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。また、必要に応じて MAFF クラウド CoE と事前協議すること。その際、利用するクラウドサービスのクラウドサービスプロバイダが提供する上級資格の保有者等、モダンな技術・運用に明るい者が流用可能資産の調査及び評価、

設計を行うこと。加えて、各ブロックを単純に組み合わせるだけでなく、リファレンスアーキテクチャに記載された構成を参考に本システムに最適化された構成での提案を行うこと。なお、当該提案内容は、各府省におけるシステム品質向上のため、ベストプラクティスとして共有されうる旨留意すること。担当部署の他にも、システム関係事業者が継続して本システムを運用・保守していくことが想定されることから、第三者が理解できるように、特に用語の定義や表記ゆれに注意した上で、各種資料及び成果物は分かりやすく作成すること。

イ　クラウドサービスの機能により自動生成可能なドキュメントが存在する場合、積極的に自動生成を行うこと。

ウ　受注者は、整備する違法輸入動植物等流通監視システムの稼働環境の調査・分析予測を行った上で、基本設計書、詳細設計書等既存の設計書に基づき作業を行うこと。なお、当該調査・分析予測の結果、既存の設計書に変更が生じる場合は既存の設計書を修正した上で作業を行うこと。

エ　受注者は、プロジェクト期間中にシステム構成図に変更が生じた場合は、変更内容について、担当部署の承認を得ること。

オ　設計、構築にあたり、デジタル庁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 設定規則を担当部署から受領して、その内容に基づいて申請書を作成し、担当部署を通じて申請すること。

カ　受注者は、情報システムのリリースの方法、環境、ツール、段取り等を記載した移行計画書を作成し担当部署の承認を得ること。

キ　受注者は、運用設計及び保守設計を行い、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作業計画書及び作業実施要領の案を作成し、担当部署の確認を受けること。なお、運用設計及び保守設計には、「マネージドサービス等のアップデート に係る作業内容」を含めることとし、定常業務としてコストをかけず管理に組み込むこと。

ク　受注者は、自動化、セルフサービス化等による効率的なシステム運用・保守に資するシステム改修案があれば提案すること。

ケ　受注者は、別紙1要件定義書（違法輸入動植物等流通監視システム整備業務）のリファレンスアーキテクチャの内容を参照し、システム方式に関する基本設計結果を記載したものとして基本設計書（システム方式）を作成し、担当部署の承認を得ること。また、必要に応じて MAFF クラウド CoE と事前協議すること。基本設計書（システム方式）には必ず以下の内容を含むこと。

（ア）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）

（イ）セキュリティ設計（クラウドサービスプロバイダが推奨するリファレンスアーキテクチャへの準拠、各レイヤにおけるセキュリティ対策、必須適用テンプレート等の展開）

（ウ）運用自動化設計（オートスケーリング、自動リカバリー、検知・通知自動化等）

コ　受注者は、生成 AI を活用したシステム構築を行う場合、インプットの定義、インプットの利用条件等について、基本設計で検討し、担当部署の承認を得ること。

サ　受注者は、詳細設計において、基本設計書（システム方式）を踏まえ、クラウドサービスにおける環境定義を実施し、システム方式に関する詳細設計結果を記載した IaC 設定ファイル及び

パラメータシートを作成し、担当部署の確認を受けること。また、必要に応じて MAFF クラウド CoE と事前協議すること。

シ　受注者は、設計書類とプログラムソースに差異がある場合はプログラムソースを優先し、その上で、要修正箇所等を明確にして設計書を修正すること。なお、選定理由書、機能証明書及び影響調査書に変更がある場合は修正すること。

ス　受注者は、本調達に関連する全ての設計書及びマニュアル等の資料について、改修部分に関する既存の資料を更新し、改修部分以外の既存の資料と一式で納品すること。差分のみの納品は不可とする。

セ　受注者は、インフラの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、令和 10 年度本システム運用保守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。

ソ　ガバメントクラウドについて不明点等がある場合は、担当部署及びデジタル庁ガバメントクラウド担当と協議の上、作業を進めること。

タ　作業実施に当たり、「デジタル・ガバメント推進標準ガイドライン」（令和 6 年 5 月 31 日デジタル社会推進会議幹事会決定。以下「標準ガイドライン」という。）、「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」（令和5年9月 29 日デジタル社会推進会議幹事会決定。以下「クラウド方針」という。）及び GCAS（Government Cloud Assistant Service：https://guide.gcas.cloud.go.jp/）上に公開されたガバメントクラウド関連文書の内容を遵守すること。契約期間中に上記文書が改定された場合は最新の版を参照し、担当部署と協議の上、対応について決定すること。

チ　以下に記載された観点に基づき、各種マニュアル、設計書等及びアーキテクチャイメージについて、システム観点での見直しを実施すること。その際、ガバメントクラウドが用意するリファレンスアーキテクチャ（https://guide.gcas.cloud.go.jp/general/quotation-request-procurement/）を積極的に活用すること。また、リファレンスアーキテクチャに記載された構成を参考に各ブロックを単純に組み合わせたり、アーキテクチャイメージを単純に踏襲したりするだけでなく、本システムに最適化された構成での提案を行うこと。なお、当該提案内容は、各府省におけるシステム品質向上のため、ベストプラクティスとして共有されうる旨留意すること。

ツ　ガバメントクラウドの各環境における業務遂行のため、担当部署に対し管理ユーザ等の払い出しを依頼すること。

テ　受注者は、クラウドサービス上に構築する「本番環境」及び「検証環境」並びに「開発環境」の3種類を利用すること。ただし、設計・開発に用いる環境は、原則として「検証環境」及び「開発環境」とする。本番環境及び検証環境では、アプリケーションプログラムのリリース、リリース後の動作確認等を行う。開発環境では、アプリケーションプログラムの開発、業務結合テスト（アプリケーションプログラムの結合テスト）等を行うこと。なお、リリース後も継続的改善を実施できるよう、「リファレンスアーキテクチャ」の内容を参考に、継続的インテグレーション・継続的デリバリー（CI/CD）パイプラインを構築すること。

ト　受注者は、ガバメントクラウド AWS 利用ガイド（https://guide.gcas.cloud.go.jp/aws/）に従い、システム構築及び運用を行うこと。

（4） 開発・テスト

ア　受注者は、開発に当たり、追加で使用するソフトウェアがある場合は、当該ソフトウェアに関する選定理由書、機能証明書及び影響調査書を作成し、担当部署の承認を受けること。また、作成した選定理由書、機能証明書及び影響調査書を踏まえて、ソフトウェアを選定し、各種アプリケーションが正常に動作するための設定変更、プログラムの改修等を行うこと。なお、本システムのソフトウェア情報については、「別紙１要件定義書（違法輸入動植物等流通監視システム整備業務）」を参照すること。

イ　受注者は、本システムに影響を与える脆弱性が混入されていないことを確認するため、開発環境において、脆弱性検査ツールなどを用いたソースコードへのチェックを行い、脆弱性検査結果報告書を作成の上、検査結果を報告し、問題がないように対応すること。

ウ　受注者は、開発に当たり、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、担当部署の確認を受けること。

エ　受注者は、開発に当たり、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、担当部署の確認を受けること。

オ　受注者は、単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、担当部署の承認を得ること。

カ　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。

キ　受注者は、テスト計画書に基づき、各テストの実施状況と実施結果について担当部署に報告すること。その際、セキュリティ関連のテストの実施結果が確認できるようにすること。

ク　脆弱性検査については、原則として「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」に沿って担当部署との協議により実施内容を決定し、脆弱性診断の実施及び検出された脆弱性への対応を行うこと。

ケ　受注者は、生成 AI を活用したシステム構築を行う場合、導入予定の生成 AI システムが期待する品質を満たしているか確認し、担当部署の承認を得ること。なお、担当部署が品質が満たされていないと判断した場合（生成 AI の出力精度やハルシネーションの発生頻度等の生成 AI モデル自体に起因した”品質”を除く）、その原因を特定し、改善措置を講じること。

コ　AI データ分析サブシステムにおける AI による分析手法及び分析機能並びに基本構成については、令和８年度に実施した「違法輸入植物等流通監視システムの整備に係る調査等業務」の成果を継承するものとし、要件、分析精度、データ利用・連携対象サイトその他の仕様については、原則として同業務において整理・構築した内容と同等以上の水準を確保すること。なお、LLM モデルによる判定結果等アウトプットの精度向上は、モデル選定と利用コストのバランス等に依存するため、必ずしもこの限りではない（都度、担当部署と協議すること）。

サ　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。

（5） 受入テスト支援

ア　受注者は、受入テスト計画書及びテスト項目、使用するテストデータ、合格判定基準等を示した受入テスト仕様書を作成し、担当部署の承認を得ること。

イ　受注者は、担当部署が受入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。

ウ　受注者は、担当部署の指示に基づき、担当部署以外の情報システム利用者のテスト実施も含めて、受入テストの実施支援を行うこと。

（6）　システムのリリース（本番稼働）

ア　受注者は、ガバメントクラウドでのシステムリリース（本番稼働）を行うにあたり、リリース計画書を作成し、担当部署の承認を得ること。なお、リリース計画書にはリハーサル計画及び本番リリース計画を含めること。

イ　受注者は、リリース計画書を踏まえ、リリース（本番稼働）設計書を作成し、担当部署の承認を得ること。また、職員が本システムを利用するために必要となる準備事項について、提案や支援を行うこと。

ウ　受注者は、担当部署の移行判定を受けて、リリース計画書に基づく移行作業を行うこと。

エ　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、担当部署の承認を得ること。

オ　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。

カ　検証作業等で開発環境等に保管されたデータについては、ISMAP で規定された方法でデータが消去されていることが第三者による監査（担当部署による確認行為を含む。）により証明されていること。

キ　受注者は、リリース計画書に基づく事前リハーサルを行うこと。事前リハーサルの実施後、本番リリースに係る作業手順、作業時間見積もり等を評価し、「事前リハーサル結果報告書」を作成し、担当部署の承認を得ること。

ク　受注者は、担当部署のリリース判定を受けて、リリース計画書に基づく本番リリース作業を行うこと。本番リリースの実施結果を「リリース結果報告書」として取りまとめ、担当部署の承認を得ること。

（7）　教育（マニュアル作成・研修）

受注者は、本システムの機能について操作や画面の趣旨、操作に必要な項目（入力項目やボタン等）の意味を記載した利用者向けの操作マニュアルを作成すること。

また、当該マニュアル及び別紙1要件定義書（違法輸入動植物等流通監視システム整備業務）を踏まえ、消費・安全局植物防疫課、同動物衛生課、植物防疫所、動物検疫所の職員のそれぞれを対象とした研修を行うこと。研修の実施にあたっては、事前に担当部署と日程調整、内容の調整を行うこと。

（8）　運用・保守実施要領の作成

受注者は、プロジェクト計画書、プロジェクト管理要領、プロジェクト運用計画、プロジェクト保守作

業計画と整合をとりつつ、「運用実施要領、保守実施要領」の案を作成し、担当部署の承認を受けること。

なお、運用実施要領、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。

（9） 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、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。

イ 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。

ウ 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。

エ 受注者は、各サブシステムのクラウドサービスの利用状況を注視するとともに、PJMO がインスタンスのサイズ（AWS の場合、インスタンスタイプ）変更が必要と判断した場合、インスタンスのサイズ変更を行うこと。

オ 受注者は、AWS の Security Hub の各ベンチマークの「セキュリティスコア」の値（以降、準拠率という）について、90%以上の状態を維持し、「準拠率」が、100%に近づくように継続的な改善に取り組むこと。

（10）定常時対応

ア 受注者は、運用保守実施要領の運用要件に示す定常時運用業務（システム操作、運転管理・監視、稼動状況監視、等）及び保守要件に示す定常時保守作業（定期点検、不具合受付等）を行うこと。具体的な実施内容・手順は運用保守実施要領に基づいて行うこと。

イ 受注者は、運用保守実施要領に基づき、運用及び保守作業業務の内容や回数、工数などの作業実績状況、サービスレベルの達成状況、情報管理システムの構成と運転状況（情報セキュリティ監視状況を含む。）、情報管理システムの利用者サポート、教育・訓練状況、リスク・課題の把握・対応状況について運用保守作業報告書を取りまとめること。

ウ 受注者は、全期間の運用及び保守作業実績を評価し、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。

エ 受注者は、運用保守作業報告書の内容について、定期運用及び保守作業会議に出席し、その内容を報告すること。

オ 受注者は、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。また、自動取得したソフトウェアの情報を把握し、担当部署の求めに応じて最新の構成情報の出力結果を提出すること。

カ 受注者は、ソフトウェアの脆弱性の対応が行えるようサポート期限内のバージョンを使用し、セキュリティパッチ適用を定期的に実施するとともに、バージョンアップが必要な場合は実施すること。

キ　受注者は、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、担当部署の承認を得た上で対応すること。

ク　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。

ケ　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、担当部署の確認を受けること。

コ　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。

サ　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。

シ　受注者は、クラウドサービスの利用実績について、利用明細書の写し及びそれらを一覧表にとりまとめ、クラウドサービスの利用が開始した月より毎月、担当部署に提出すること。また、担当部署の求めに応じ、クラウドサービスを含めた情報管理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。

ス　受注者は、担当部署が情報管理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。

セ　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。

ソ　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とともに、必要に応じて運用・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。

（11）障害発生時対応

ア　受注者は、情報管理システムの障害発生時（又は発生が見込まれる時）には、速やか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、運用保守実施要領の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）又は保守要件に示す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。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・手順は運用保守実施要領等に基づいて行うこと。

イ　受注者は、情報管理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。

ウ　受注者は、災害等の発災時には、担当部署の指示を受けて、緊急時対応マニュアルに基づく運用及び保守作業業務を実施すること。

エ　受注者は、生成 AI を活用しているシステムにおいて、生成 AI システムのバージョンアップ等の要因でアウトプットが期待する品質を満たさなくなった場合、そこから生じる被害を最小限に食い止め、原因を特定し、改善措置を講じること。

（12）定例会等の実施

ア　受注者は、定例会を隔週開催するとともに、業務の進捗状況を作業実施計画書及び作業実施要領に基づき報告すること。進捗報告書については定例会の前日（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。）までに提出すること。

イ　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。

ウ　受注者は、会議終了後、3日以内に議事録を作成し、担当部署の承認を得ること。

（13）情報システムの現況確認支援

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。

イ　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。

ウ　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部署に報告すること。

エ　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部署に報告すること。

（14）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」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。

イ　再請負先がある場合は、再請負先の法人番号と再請負金額を提示すること。最大何次請負、再請負総額、累計契約額（前年度まで）、年度契約金額を提示すること。

ウ　受注者は、農林水産省が定める時期に、情報資産管理標準シートを提出すること。

エ　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」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

（イ）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

（ウ）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

（エ）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

（オ）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

（カ）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

（キ）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

（ク）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

（ケ）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

（コ）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

（サ）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

（シ）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

（ス）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

（15）プロジェクト計画書の更新支援

受注者は、担当部署が本業務における検討結果をプロジェクト計画書に適宜反映させる作業に関して、プロジェクト計画書を段階的詳細化し、内容変更の支援をすること。

（16）引継ぎ

ア　受注者は、令和10年度本システム運用保守業者に対する引継ぎの開始前に、本システムの引継ぎに係る引継ぎ対象、引継ぎ体制、引継ぎ内容、引継ぎ方法、引継ぎスケジュール、理解度確認方法、完了条件等を記載した「引継ぎ計画書」を作成し、担当部署の承認を得ること。

イ　受注者は、システム整備（新規構築）で行った開発環境への設定変更等の環境に関する情報及びデプロイ方法等に更新があった場合にその情報を引継ぐこと。

ウ　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た引継ぎ資料を作成し、令和 10 年度本システム運用保守業者に対して確実な引継ぎを行うこと。引継ぎ作業の完了時に、実施結果について記載した「引継ぎ結果報告書」を作成し、担当部署へ報告を行うこと。

エ　受注者は、関連調達の受注者に対し、必要に応じて作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと（令和9年度は関連調達はなし）。

オ　契約完了に伴い運用・保守事業者が変更される場合、本システムは、本契約の終了後も引き続き同一の環境を継続して利用することを想定していることから、受注者は、本システムのシステ

ム運用・保守事業者が円滑に業務を実施できるよう必ず以下の引継ぎ資産を整理し、担当部署へ提出すること。また、ガバメントクラウドにおける本システムに係る各種環境上の不要な資産及び権限は、担当部署確認の上削除すること。

（ア）本システムに係るガバメントクラウドの管理者権限

（イ）ガバメントクラウドとの接続回線

（17）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2　成果物一覧

No.	成果物名	調達仕様書等の記載箇	記載内容、留意事項等	納品期日（原則）
1	設計・開発実施計画書（案）	4（1）設計・開発実施計画書等の作成	標準ガイドライン実務手引書第3編「第7章　設計・開発」の内容等を踏まえ作成する。 No.1、2のとおり事前に案を作成し、担当部署の承認を受けること。	契約締結後5日以内
2	設計・開発実施要領（案）	4（1）設計・開発実施計画書等の作成		
3	設計・開発実施計画書	4（1）設計・開発実施計画書等の作成		契約締結後20日以内
4	設計・開発実施要領	4（1）設計・開発実施計画書等の作成		
5	要件定義書の修正案	4(2)要件定義内容の調整・確定		担当部署が指示する
6	システム構成図	4（3）設計	担当部署から提供されたシステム構成図（案）をもとに作成。	担当部署が指示する
7	各種申請書	4（3）設計	DNS設定やSSL証明書発行に係る申請書等	担当部署が指示する
8	選定理由書及び機能証明書	4（4）開発・テスト	使用するソフトウェアがある場合に作成。当該ソフトウェアについて、機能、バージョン、選定理由等を記載。	契約締結後20日以内
9	影響調査書	4（4）開発・テスト	使用するソフトウェアがある場合に作成。当該ソフトウェアについて、影響範囲の調査結果を記載。	
10	開発標準（標準コーディング規約等）	4（4）開発・テスト		開発着手の1週間前
11	脆弱性検査結果報告書	4（4）開発・テスト		検査終了後2週間以内（特に問題が認められた場合速やかに）
12	テスト計画書、テスト仕様書（テストケース）	4（4）開発・テスト	作成対象：単体テスト、結合テスト、総合テスト	テスト開始の2週間前
13	テスト結果報告書	4（4）開発・テスト	作成対象：単体テスト、結合テスト、総合テスト	各テスト終了後2週間以内
14	受入テスト仕様書	4（5）受入テスト支援		テスト開始の2週間前

No.	成果物名	調達仕様書等の記載箇	記載内容、留意事項等	納品期日（原則）
15	リリース計画書及びリリース手順書	4（6）システムのリリース（本番稼働）	リリース手順書の内容をリリース計画書に含めることで差し支えない。	事前リハーサル実施の2週間前
16	リリース設計書	4（6）システムのリリース		
17	事前リハーサル結果報告書	4（6）システムのリリース		事前リハーサル終了後2週間以内
18	リリース結果報告書	4（6）システムのリリース		本番リリース完了後2週間以内
19	引継ぎ計画書	4（16）引継ぎ		令和10年度運用・保守業者に引き渡す2週間前まで
20	引継書	4（16）引継ぎ	標準ガイドライン「第3編 第7章 設計・開発」の「引継ぎ」に定義されているもの。	
21	運用実施要領（案）	4（8）運用・保守実施要領の作成	標準ガイドライン「第3編 第9章 運用及び保守」に定義されているもの。	担当部署が指示する
22	保守実施要領（案）	4（8）運用・保守実施要領の作成		担当部署が指示する
23	運用実施要領	4（8）運用・保守実施要領の作成	標準ガイドライン「第3編 第9章 運用及び保守」に定義されているもの。	本番リリースの2週間前まで
24	保守実施要領	4（8）運用・保守実施要領の作成		本番リリースの2週間前まで
25	基本設計書一式	4（3）設計		担当部署が指示する
26	詳細設計書一式	4（3）設計		担当部署が指示する
27	パラメータシート	4（3）設計		担当部署が指示する
28	IaC設定ファイル	4（3）設計		担当部署が指示する
29	実行プログラム及びソースコード一式	4（4）開発・テスト	実行プログラム及びソースコードと一式で納品すること。	担当部署が指示する
30	作業計画書（案）	4（3）設計		担当部署が指示する
31	作業実施要領（案）			
32	引継ぎ結果報告書	4（16）引継ぎ		引継ぎ完了後2週間以内
33	契約金額内訳	4（8）契約金額内訳及び情報資産管理標準シートの提出		契約締結後5日以内
34	情報資産管理標準シート			担当部署が指示する
35	進捗報告書及び議事録	4（7）定例会等の実施		進捗報告書は定例会前日、議事録は定例会後3日以内
36	外部サービスに係る設定情報その他の必要な情報一式		外部サービスを利用する場合、利用前に担当部署の承認を受けること。	サービス利用開始予定の1週間前まで
37	情報セキュリティ管理計画書	7（9）セキュリティ要件		契約締結後20日以内
38	情報セキュリティ対策実施報告書	7（9）セキュリティ要件		担当部署が指示する

イ 成果物の納品方法

（ア） 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。

（イ） 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。

（ウ） 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。

（エ） 作成した成果物は担当部署が指定したサーバへ納品（例：PrimeDrive 又は SharePoint 等）するとともに、電磁的記録媒体でも納品すること。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。

（オ） 担当部署から特別に示す場合を除き、原則電磁的記録媒体は2部を納品すること。

（カ） サーバ及び電磁的記録媒体の納品について、Microsoft Office 又は PDF のファイル形式で作成すること。

（キ） 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。

（ク） 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。

（ケ） 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、担当部署の承認を得ること。

（コ） 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。

（サ） 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。

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。

〒100－8950
東京都千代田区霞が関１－２－１
農林水産省消費・安全局植物防疫課
電話番号：03-6744-2035

エ 留意事項

成果物の提出方法、期限等については、必要に応じてその都度、担当部署と協議することができるものとする。

５　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1「要件定義書（違法輸入動植物等流通監視システム整備業務）」のとおり。なお、本要件定義書は調達時の想定であることから、上記4（3）により必要な要件を確認し、設計を確定すること。

６　業務の実施体制・方法

（1） 業務実施体制

プロジェクトの推進体制及び本件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、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行う。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 3 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

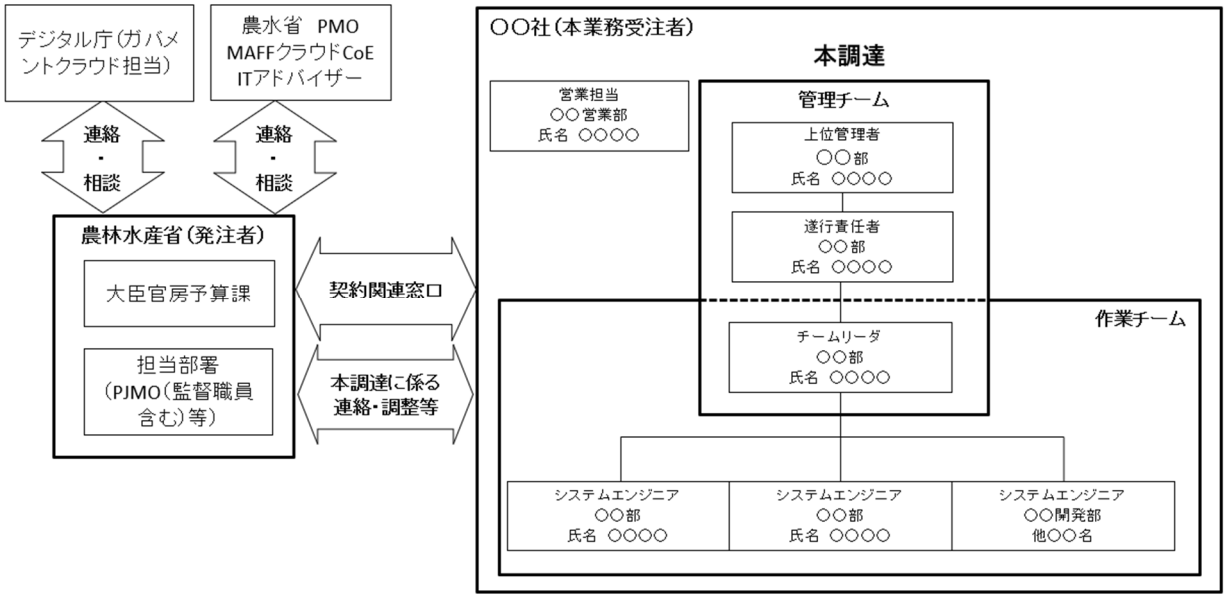


表3 本業務における組織等の役割

組織等	本業務における役割
大臣官房予算課	本業務の契約関係事務を担当する。
担当部署	本業務の管理組織として、本業務の進捗等を管理する。
本業務受注者(遂行責任者・担当者)	本業務を実施する。
PMO、ITアドバイザー	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	担当部署・受注者に対してパブリッククラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。利用システムに対して、全体クラウドCoEから提示された方針や基準を実施できるように支援を行う。
運用・保守事業者	令和10年度の本システム運用・保守業務を実施する。
デジタル庁ガバメントクラウド担当	デジタル庁:ガバメントクラウドの所管組織。全体クラウドCoEとして、以下の3つの役割を担う。 ・ガバメントクラウドの方針や基準等の戦略を立案し、各府省PMOに提示を行う。 ・政策優先度の高いプロジェクトに対して、ガバメントクラウドの方針や基準を実施できるように支援を行う。 ・各府省クラウドCoE体制不足時の支援を行う。

表4 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

組織等	本業務における役割
	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。
担当者	1名以上を従事させること。

（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 遂行責任者

（ア） 情報処理技術者試験のうちプロジェクトマネージャ試験の合格者、又は米国 PMI が認定する PMP（Project Management Professional）の資格を有すること。もしくは、これらに相当するプロジェクトマネジメント業務の経験（10 名以上のプロジェクトマネジメントの経験年数が、直近5年間で複数回又は複数年に及ぶ等）でも可とする。

（イ） パブリッククラウドに係る全ての技術領域において、以下のいずれかのクラウドサービスプロバイダの認定技術者としての上級資格[*1]を有する者を配置すること。なお、遂行責任者の資格は本業務期間中に専任で遂行責任者を支援する要員が保有していることでも可とする。または、クラウドサービスプロバイダ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）の利用での対応も可とする。

*1 AWS Certified Solutions Architect – Professional

イ 担当者

パブリッククラウドに係る全ての技術領域において、以下のいずれかのクラウドサービスプロバイダの認定技術者としての中級資格[*2]以上を有する者を1名以上配置すること。

*2 AWS Certified Solutions Architect – Associate

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

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

（3） 作業場所

本業務の実施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。

（4） 作業の管理に関する要領

ア 受注者は、担当部署が承認した設計・開発計画書の作業体制、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、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。

イ　受注者は、担当部署が承認した運用・保守実施要領に基づき、運用・保守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。

（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

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に移転されるものでないこと。

イ　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。

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。

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）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2「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農林水産省と協議の上決定し、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、農林水産省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。

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

本調達の遂行に当たっては、民法（明治 29 年 4 月 27 日法律第 89 号）、刑法（明治 40 年 4 月 24 日法律第 45 号）、私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年 4 月 14 日法律第 54 号）、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 128 号）等を遵守し履行すること。

イ　環境関係法令の遵守

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。

（ア）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）

（イ）労働安全衛生法（昭和 47 年法律第 57 号）

（4） 環境負荷低減に係る遵守事項

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、事業の最終報告時に様式を用いて、以下の取組に努めたことを、「別紙3 環境負荷低減の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原則として「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、該当するものの実施しなかった／努めなかった場合には空欄とし、アからエまでの各項目について、一つ以上「実施した／努めた」にチェックを入れること。アからエまでの各項目について、各項目内の事項について、1つもチェックが入らなかった場合は、その理由を記載すること。

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、適正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。

（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） 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。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 クラウドサービスの解約等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。

（7） その他文書、標準への準拠

ア プロジェクト計画書等

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

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） 農林水産省ドメイン（maff.go.jp）のサブドメインについては、農林水産省のドメイン管理ルールに従い命名等を行うこととし、農林水産省の指示に従うこと。

（ケ） 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。

（8） 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。

（9） 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、以下の各項目から対応が必要となる項目についての対応方針（情報セキュリティ管理計画書）を提出し、担当部署と協議の上、その承認を受けること。

また、情報セキュリティ管理計画書に基づき実施した情報セキュリティ対策の対応結果を情報セキュリティ対策実施報告書に取りまとめ、担当部署の承認を受けること。

ア　AT-1-1　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こと。

イ　AT-1-3　通信のなりすまし防止

電子メールのなりすましの防止策を講ずること。その際、DMARC による対策は必須とし、送信側の対策は SPF 及び DKIM のいずれか又は両方により実施し、受信側の対策は SPF 及び DKIM の両方により実施すること。

ウ　AU-1-1　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、可能な限り１年の期間保管すること。

エ　AU-1-3　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。

オ　PR-1-2　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、外部との接続のある情報システムにおいて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。

カ　UP-2-1　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。

キ　DA-2-1　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「別紙１要件定義書（違法輸入動植物等流通監視システム整備業務）」で定めるサービスレベル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に努めること。

ク　SC-1-1　請負先において不正プログラム等が組み込まれることへの対策

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、受注者は情報セキュリティ監査を受け入れること。

また、役務内容を一部再請負する場合は、再請負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。

ケ　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」への準拠すること。

また、以下のセキュリティ対策要件を参照し、本システムのセキュリティ対策要件を点検し、「別紙5　Web システム／Web アプリケーションセキュリティ要件書　Ver.4.0」については必須項目を全て満たすこと。なお、本資料における MAFF クラウド管理者と担当部署の役割を理解し、不要な作業見積をしないよう注意の上、担当部署に必要な支援を行うこと。

（ア）別紙4　AWS 設定確認リスト

（イ）別紙5　Web システム／Web アプリケーションセキュリティ要件書　Ver.4.0

（10）データマネジメント・データ活用要件

本調達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。

（11）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

本調達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。本調達においては、国民等による農林水産省外利用の場合、個人情報、プライバシー、知的財産を取り扱う場合の要件についても対応すること。行政の進化と革新のための生成 AI の調達・利活用に係るガイドラインが改定された場合は、最新のものを参照し、その内容に従うこと。

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が生じた場合には、そ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当該紛争を一切処理すること。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。

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

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

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。

カ　前記アからオ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きはこの限りでない。

キ　前記アからオ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。

（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　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別途定める。

（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　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。

ウ　その他、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。

（3）　入札実績等

当案件を確実に遂行するため、応札者は、以下の条件をすべて満たしていることを具体的な事例を挙げて証明すること。ただし、実績があったとしても、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、ここでいう実績には含まれない。

（ア）入札参加者は、ガバメントクラウド対象クラウドサービス上にシステムを構築した実績を過去3年以内2件以上有すること。

（イ）入札参加者は、レガシーシステムをモダンなアプリケーションへ刷新した実績を過去3年以内に有すること。

（ウ）入札参加者は、レガシーシステムをガバメントクラウド対象クラウドサービスへ移行した実績を過去3年以内に有すること。

（エ）入札参加者は、本システムと同等の規模を有する情報システムの運用実績を過去3年以内に有すること。

（オ）ガバメントクラウド上で稼働中のシステムの運用保守の実績を過去3年以内に有すること。

（カ）生成 AI を利用したシステムの開発業務又は運用保守業務の実績を過去3年以内に1件以上有していること。

（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。

（5） 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。

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

イ 共同提案を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

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

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

10 再請負に関する事項

（1） 再請負の制限及び再請負を認める場合の条件

ア 本業務の受注者は、業務を一括して又は主たる部分を再請負してはならない。

イ 再請負ができる業務は、原則として契約金額に占める再請負金額の割合（以下「再請負比率」という。）が 50 パーセント以内の業務とする。

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

エ 受注者は再請負先の行為について一切の責任を負うものとする。

オ 再請負先における情報セキュリティの確保については受注者の責任とする。

カ 再請負を行う場合、再請負先が「8（4）入札制限」に示す要件を満たすこと。

（2） 承認手続

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

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

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

（3） 再請負先の契約違反等

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

11 その他特記事項

（1） 前提条件

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を優先する。

イ　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は、変更契約の手続きを行うこと。

ウ　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。

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

（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

東京都千代田区霞が関1-2-1　農林水産省

具体的には担当部署が指定する。

イ　閲覧期間及び時間

（ア）未定

（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4名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別紙6「資料閲覧申請書」に記載の上、閲覧希望日の前日までに提出すること。また、閲覧日当日までに別紙7「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

下記 113 による。

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）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）令和8年度に実施した「違法輸入動植物等流通監視システムの整備に係る調査等業務」の関係資料一式

（エ）プロジェクト計画書

※ガバメントクラウドについては、以下の GCAS サイトにアクセスし情報を確認すること。

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

12 附属文書

別紙1 要件定義書（違法輸入動植物等流通監視システム整備業務）

別紙2 情報セキュリティの確保に関する共通基本仕様

別紙3 環境負荷低減のみどりチェック実施状況報告書

別紙4 AWS 設定確認リスト

別紙5 Web システム／Web アプリケーションセキュリティ要件書 Ver.4.0

別紙6 資料閲覧申請書

別紙7 守秘義務に関する誓約書

別紙8 質問表

13 本業務に関する問い合わせ先

農林水産省 消費・安全局 植物防疫課

担当：小森、湯山

電話：03-6744-2035

メールアドレス： kazuya_komori690/atmark/maff.go.jp

hironari_yuyama170/atmark/maff.go.jp

※ /atmark/を@に変更して送信すること。

以上

令和９年度

違法輸入動植物等流通監視システム

別紙１　要件定義書

令和８年 11 月

農林水産省　消費･安全局植物防疫課

1. 業務要件定義 2
1.1. 業務実施手順 2
1.2. 業務の規模 5
1.3. 業務実施の時期・時間 7
1.4. 業務の実施等 7
1.5. 業務観点で管理すべき指標 8
1.6. 情報システム化の範囲 9
1.7. 業務の継続の方針等 10
1.8. 情報セキュリティ対策の方針等 10
2. 機能要件定義 11
2.1. 機能に関する事項 11
2.2. 画面に関する事項 12
2.3. 帳票に関する事項 14
2.4. データに関する事項 14
2.5. 外部インタフェースに関する事項 17
3. 非機能要件定義 19
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 19
3.2. システム方式に関する事項 21
3.3. システム規模に関する事項 23
3.4. 性能に関する事項 25
3.5. 信頼性に関する事項 26
3.6. 拡張性に関する事項 27
3.7. 上位互換性に関する事項 27
3.8. 中立性に関する事項 28
3.9. 継続性に関する事項 29
3.10. 情報セキュリティに関する事項 30
3.11. 情報システム稼働環境に関する事項 31
3.12. データマネジメントに関する事項 34
3.13. テストに関する事項 35
3.14. 移行に関する事項 39
3.15. 引継ぎに関する事項 39
3.16. 教育に関する事項 40
3.17. 運用に関する事項 41
3.18. 保守に関する事項 47

1. 業務要件定義

1.1. 業務実施手順

(1) 業務範囲

本調達で実装が必要となる対象業務及び情報システム化の範囲を「図 1 システム全体像における業務の範囲」及び「表 1 業務の範囲」に示す。

図 1 システム全体像における業務の範囲（赤枠）

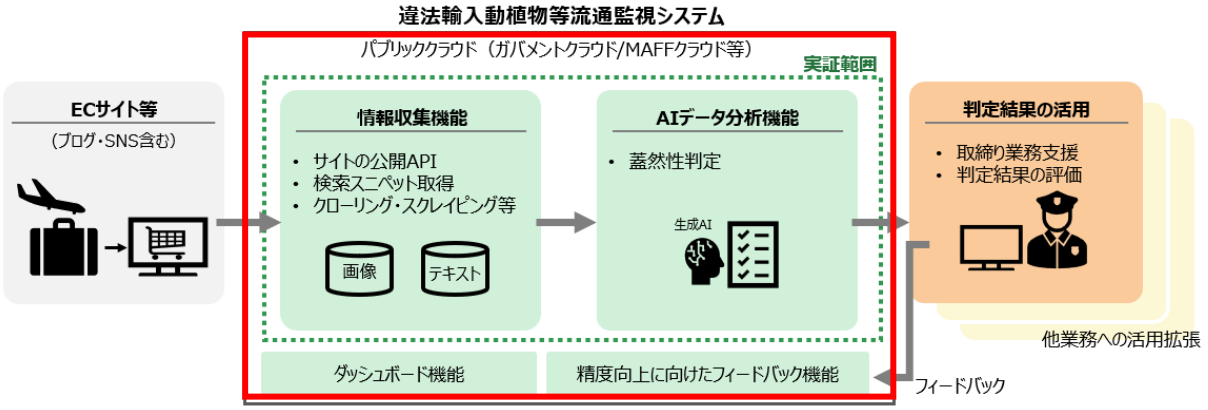


表 1 業務の範囲（業務機能とその階層）

階層 0		階層 1		階層 2	本システム適用対象候補
項番	名称	項番	名称	詳細	
1	違法性商品の監視	1-1	常時監視	情報収集	○
				AI データ分析	○
		1-2	定期監視	ダッシュボード確認	○
2	違法性商品の発見・評価	2-1	違法性判断	違法性商品一覧確認	○
				違法性商品及び出品者確認	○
				違法性判断	○
				違法性商品情報更新	○
3	違法性商品の出品者に対する対応判断	3-1	対応判断	違法性商品及び出品者確認	○
				対応判断	○
				違法性商品情報更新	○
4	違法性商品の出品者に対する対応の実行	4-1	対応の実施	出品者に対する対応実施記録作成	○
				違法性商品に対する対応実施記録作成	○
5	マスタ管理	5-1	監視条件変更	変更判断	○
				設定	○
6	システム運用	6-1	職員の権限管理	職員の権限管理	○

(2) 業務フロー

本システムが対象とする違法出品の収集・対応における業務及び管理機能の範囲を「別添資料 1-1.システム化業務フロー」に示す。

(3) 業務の実施に必要な体制

本システム関連業務の実施に現段階で想定する体制について、「表 2 業務の実施体制」に示す。

表２　業務の実施体制

項番	対象	業務概要	補足
1	農林水産省消費・安全局 植物防疫課／ 動物衛生課 システム管理者	● 出品状況のダッシュボードを確認して、違法品の流通実態を把握する。 ● 違法出品の取り締まり状況やコストを鑑みて、検索する Web サイト・検索に用いる検索ワード・ 検索頻度（監視条件）の設定を行う。	
2	農林水産省消費・安全局 植物防疫課／ 動物衛生課	● 出品状況のダッシュボードを確認して、違法品の流通実態を把握する。 ● 違法出品の取り締まり状況、コスト、商品の検索ヒット数や検知数を鑑みて、検索する Web サイト・検索に用いる検索ワード・検索頻度等の監視条件の設定変更を判断する。 ● 違法出品の取り締まり状況やコストを鑑みて、検索する Web サイト・検索に用いる検索ワード・ 検索頻度（監視条件）の設定を行う。	
3	植物防疫所／ 動物検疫所 出品監視担当者	● 本システムにおいて、違法性リスクが高いと判断した出品を、商品情報や出品者情報等も考慮して、違法性の最終判断を行う。 ● 違法性のある商品を出品していた出品者に対する対応を最終的に判断する。 ● （違法な出品の情報を規制当局等のステークホルダーに連携する。） ● 国民に対する対応を実施する（聞き取りや立会検査などの具体的なアクション） ● 対応実施結果を対応実施履歴として登録する。 ● 継続的な監視対象を設定する。（経過観察）	
4	システム運用担当者 (事業者含む)	● 本システム機能に関わる以下運用業務を行う。 • 本システムのサーバーメンテナンス等の運用作業 • 問い合わせ対応業務 • 暗号化通信用等電子証明書管理機能の管理等 • 認証連携ゲートウェイのサーバーメンテナンス等の運用作業 • 連携先システムが認証連携ゲートウェイを介して属性連携、データ連携を実施するために認証連携ゲートウェイ側で必要なデータ登録や設定作業	

(4) 入出力情報項目及び取扱量

本サービス運用開始後 1 年間程度の入出力情報及び取扱量に関する現段階における見通しを「表 3 入出力情報項目及び取扱量」に示す。なお、本システム並びに関連する情報システムの利用範囲の拡大に伴い、データの範囲と種類、容量が拡大する可能性もあることを、あらかじめ留意すること。

表３　入出力情報項目及び取扱量

項番	業務処理	入出力情報名	入出力情報概要	入出力の区分	主な入出力情報項目	取扱量	用途	取得元/提供元	補足
1	ダッシュボード確認	違法性判定状況	違法性商品に対する判定	出力	高リスク判定数、高リスク数先月比率、高リスク増加傾向の項目数、高リスク出品数	1 日に 60 件	定期監視	システム	

2	違法性商品一覧確認	違法性商品	違法性商品に対する情報	出力	商品名、商品 URL、出品日時、リスク判定結果	1 日に 10 件	違法性商品情報の確認	システム	
3	違法性商品及び出品者確認	違法性商品詳細及び出品者詳細	違法性商品及び出品者情報	出力	商品名、商品 URL、出品日時、リスク判定結果出品者名、出品者情報	1 日に 10 件	違法性商品情報詳細の確認	システム	
4	対応実施記録	対応実施履歴	対応実施内容	入力	対応実施情報、更新日時	1 日に 10 件	対応実施の記録	植物防疫所／動物検疫所 出品監視担当者	
5	監視条件確認	監視条件	現状の監視条件の内容	出力	検索ワード、検索カテゴリ、検索サブカテゴリ、サイト検索種別、検査日時、監視頻度	1 カ月に 1 件	監視条件の確認	システム	
6	監視条件変更	監視条件	変更する監視条件	入力	検索ワード、検索カテゴリ、検索サブカテゴリ、サイト、検索種別	1 カ月に 1 件	監視条件の変更	農林水産省 消費・安全局 植物防疫課／ 動物衛生課 システム管理者	

(5) 管理対象情報一覧

対象業務で管理すべき情報（管理対象情報）を「表 4　管理対象情報一覧」に示す。

表 4　管理対象情報一覧

項番	管理対象情報名	管理単位	主たる用途	主な属性	補足
1	商品情報	商品情報 ID	収集した商品情報を持つ	監視条件 ID、商品名、商品 URL、出品者 ID、出品日時、商品情報格納先、商品画像格納先、登録状況ステータス	
2	確認結果	確認結果 ID	違法性が高い商品に対する確認の可否の情報を持つ	商品 ID、確認者、確認日時、リスク確認結果、リスク確認ステータス、確認メモ	
3	違法性判定結果	判定結果 ID	商品に対する違法性判定の結果を持つ	商品 ID、調査対象格納先、リスク判定結果、判定メモ	
4	出品者情報	出品者情報 ID	商品の出品者情報を持つ	出品者 ID、出品者名、出品者 URL	
5	対応実施履歴	対応実施履歴 ID	対応実施の内容をもつ	出品者情報 ID、対応実施内容、更新日時	
6	監視条件	監視条件 ID	商品情報収集のための、Web サイトや SNS の監視条件を持つ	検索ワード、検索カテゴリ ID、検索サブカテゴリ ID、サイト ID、検索種別 ID、検索日時、検索結果格納先、監視頻度	
7	ユーザー情報	ユーザーID	システムを利用するユーザーの情報を持つ	ユーザー名、所属、役職	

1.2. **業務の規模**

本システムで実現する業務で想定される規模について、以下に示す。

(1) サービスの利用者数及び管理機能の利用者数

本サービス及び管理機能の利用者について、「表 5 サービスの利用者の種類及び利用者数（想定）」に示す。

表 5 サービスの利用者の種類及び利用者数（想定）

項番	利用者	利用者の種類		主な利用拠点	サービス提供時間帯	利用者数	補足
		サービス利用者	管理機能利用者				
1	農林水産省 消費・安全局 植物防疫課 システム管理者		○	本省	8:00～20:00	約 3 人	
2	農林水産省 消費・安全局 植物防疫課 すべての職員	○		本省	8:00～20:00	約 50 人	
3	植物防疫所 出品監視 担当者	○		全国	8:00～20:00	約 30 人	
4	植物防疫所 すべての職員	○		全国	8:00～20:00	約 1,000 人	
5	動物衛生課 システム管理者		○	本省	8:00～20:00	約 3 人	
6	動物衛生課 すべての職員	○		本省	8:00～20:00	約 50 人	
7	動物検疫所 出品監視担当者	○		全国	8:00～20:00	約 30 人	
8	動物検疫所 すべての職員	○		全国	8:00～20:00	約 700 人	

(2) 処理件数

本システムを用いた主な業務の処理件数は「表 6 主な業務の処理件数（想定）」のとおりである。

想定される処理件数について、自動出品監視・情報収集の対象として植物防疫法施行規則の別表 1 の 2 及び 2 の 2 に記載のものを含むか否かによって異なるが、詳細は要件定義における検討事項とする。

表 6 主な業務の処理件数（想定）

項番	業務	項目	処理件数		補足
			定常時	ピークの特性	
1	違法性商品の常時監視	情報収集	約 1,500 件/日 (別表 1-2 及び 2-2 を対象外とする)		● 検索結果一覧を表示する回数を 1 件と定義 ● 3,000 個の検索ワードを 10 サイトで検索し、1 ワード当たり平均 5 ページ分検索結果一覧を取得する想定で概算

2		AI データ分析	約 20,000 件/日 (別表 1-2 及び 2-2 を対象外とする)		● 生成 AI にリクエストを送る回数を 1 件と定義 ● 1 検索あたり 10 個の商品ページを取得し、平均 2 回ほど生成 AI による違法性判定を行う想定で概算
3	違法性商品の定期監視	ダッシュボード確認		約 2000 件/時間	● ログインページにアクセスする回数（詳細な画面へのアクセス回数を含まない）を 1 件と定義 ● 全現場検疫担当者が月 1 回のダッシュボード更新時に集中的にアクセスすると仮定
4	違法性商品の違法性判断	違法性商品等情報確認	約 60 件/日		● ログインページにアクセスする回数（詳細な画面へのアクセス回数を含まない）を 1 件と定義 ● 全ユーザーが 1 月に 1 回アクセスする想定で概算
5		違法性商品情報更新			● 経過観察、対応不要
6	違法性商品の対応判断	出品情報等確認			
7		違法性商品情報更新			● 経過観察
8	違法性商品の出品者に対する対応の実行における記録	対応実施記録作成			
9	マスタ管理	監視条件変更			

1.3. 業務実施の時期・時間

(1) 業務実施時期・期間及び繁忙期

本サービスに係る業務実施時期・期間は、原則として開庁日（土日及び祝日、年末年始を除く）とする。

本サービスに係る業務に繁忙期は存在しないが、常にレスポンスの低下等を招かないよう、十分な処理性能を確保すること。

(2) 業務の実施・提供時間

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

ア　サービス提供時間

本システムは計画停止を除き、24 時間 365 日サービスを提供できること。利用者ごとのサービス提供時間帯は「表 5 サービスの利用者の種類及び利用者数（想定）」に記載の通り。

イ　運用時間

運用・保守業者の運用時間は平日（土日及び祝日、年末年始を除く）の 9 時から 18 時までとする。ただし、情報システムの監視は 24 時間 365 日行うこと。

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

ウ　システム障害時の対応

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

(3) ヘルプデスク業務

ヘルプデスク業務における問合せ対応の受付時間を「表 7　ヘルプデスク業務の問合せ対応時間」に示す。

表 7　ヘルプデスク業務の問合せ対応時間

項番	問い合わせ方法	受付時間	回答時間	補足
1	電話	開庁日 9:00~18:00	開庁日 9:00~18:00	
2	メール	24 時間 365 日	同上	

1.4. 業務の実施等

本システムによる業務は、植物防疫所及び動物検疫所内の各部署スペースから、インターネット／GSS ネットワークを経由したアクセスで実施する。

1.5. 業務観点で管理すべき指標

本調達に係る管理すべき指標を「表 8　管理すべき指標」に示す。受注者は、本指標を達成することが可能なシステムを構築すること。

ただし、目標値は仮の値とし、要件定義にあたって PJMO と協議の上、改めて定めるものとする。

表 8　管理すべき指標

項番	指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
1	業務効果指標	違法出品発見数	月ごとの違法出品発見数の合計	件 / 月	3 件/月	システムの DB から取得する。	月次
2		月間アクティブユーザー数	月ごとのログインしたユーザー数の合計	ユーザー数 / 月	100 人/月	業務ログから直近 1 カ月のアクセスユーザー数を取得する。	月次
3	情報システム効果指標（バックエンド バッチ処理）	システム稼働率	「年間実稼働時間」/「年間予定稼働時間」×100	%	99%	サーバーの監視ログを用いて算出する。	年次
4		目標復旧時間	障害による停止時間の平均	時間	24 時間以内	障害発生から復旧までの時間を計測する。	障害発生時
5	情報システム効果指標（フロントエンドによるサービス提供）	システム稼働率	「年間実稼働時間」/「年間予定稼働時間」×100	%	99%	サーバーの監視ログを用いて算出する。	年次
6		目標復旧時間	障害による停止時間の平均	時間	24 時間以内	障害発生から復旧までの時間を計測する。	障害発生時

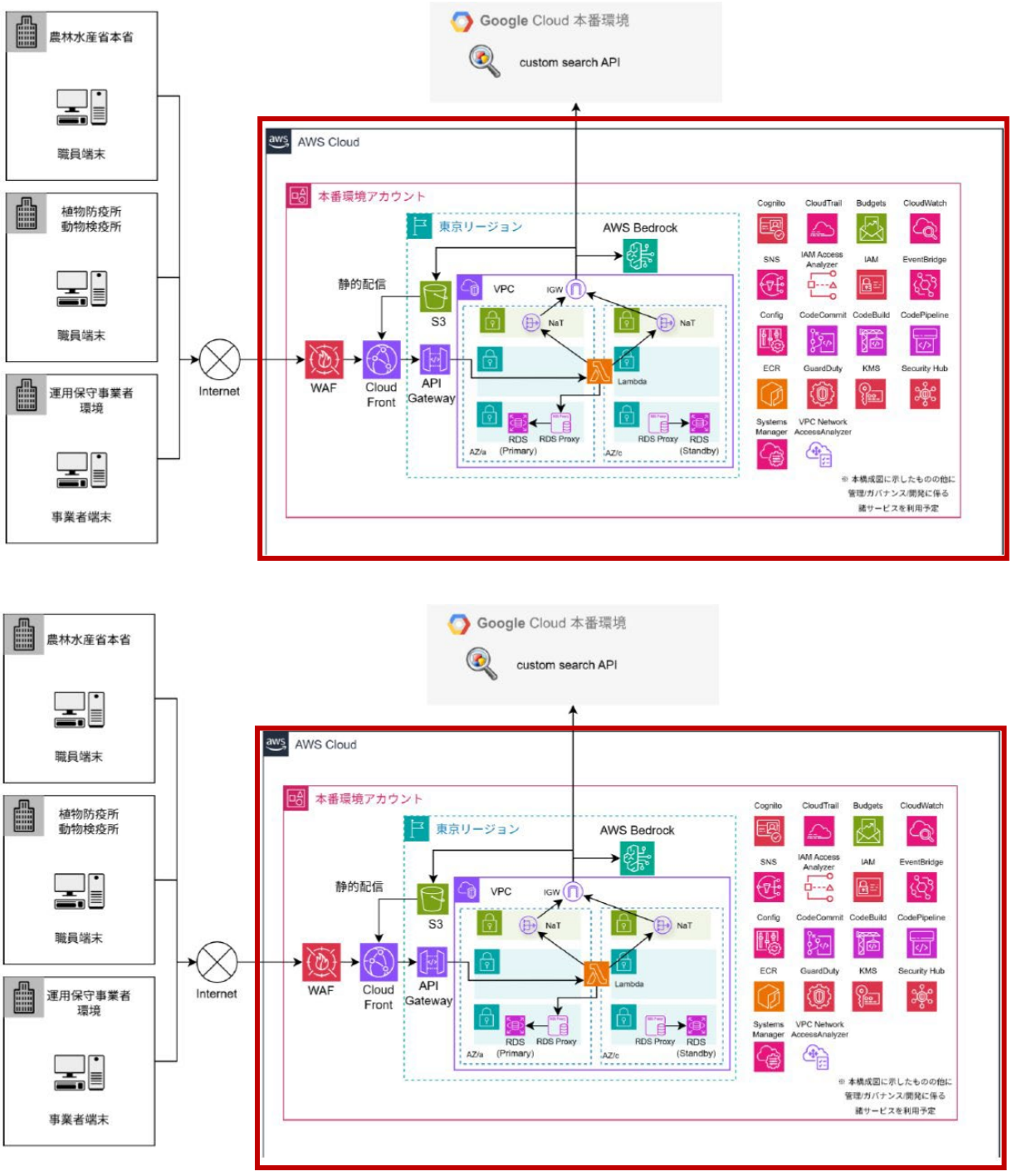
1.6. 情報システム化の範囲

本システムの現時点の想定における情報システム化の範囲、及び簡易的なアーキテクチャ図を「図 2　情報システム化の範囲（上：本番、下：検証）」に示す。

本システムはガバメントクラウド又は MAFF クラウド上に構築する。

本システムでは後述するように個人情報等の機微情報を扱わないため、十分なセキュリティを担保（ホワイトリスト IP の設定など）した上でインターネット/GSS ネットワーク経由での接続を検討する。

図 2　情報システム化の範囲（上：本番、下：検証）



1.7. 業務の継続の方針等

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

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

1.8. 情報セキュリティ対策の方針等

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

2. 機能要件定義

2.1. 機能に関する事項

(1) 機能一覧

本調達で要求する主要な機能を「別添資料 2-1.システム機能一覧」に示す。詳細な機能構成は、要件定義工程にて PJMO と協議の上決定すること。

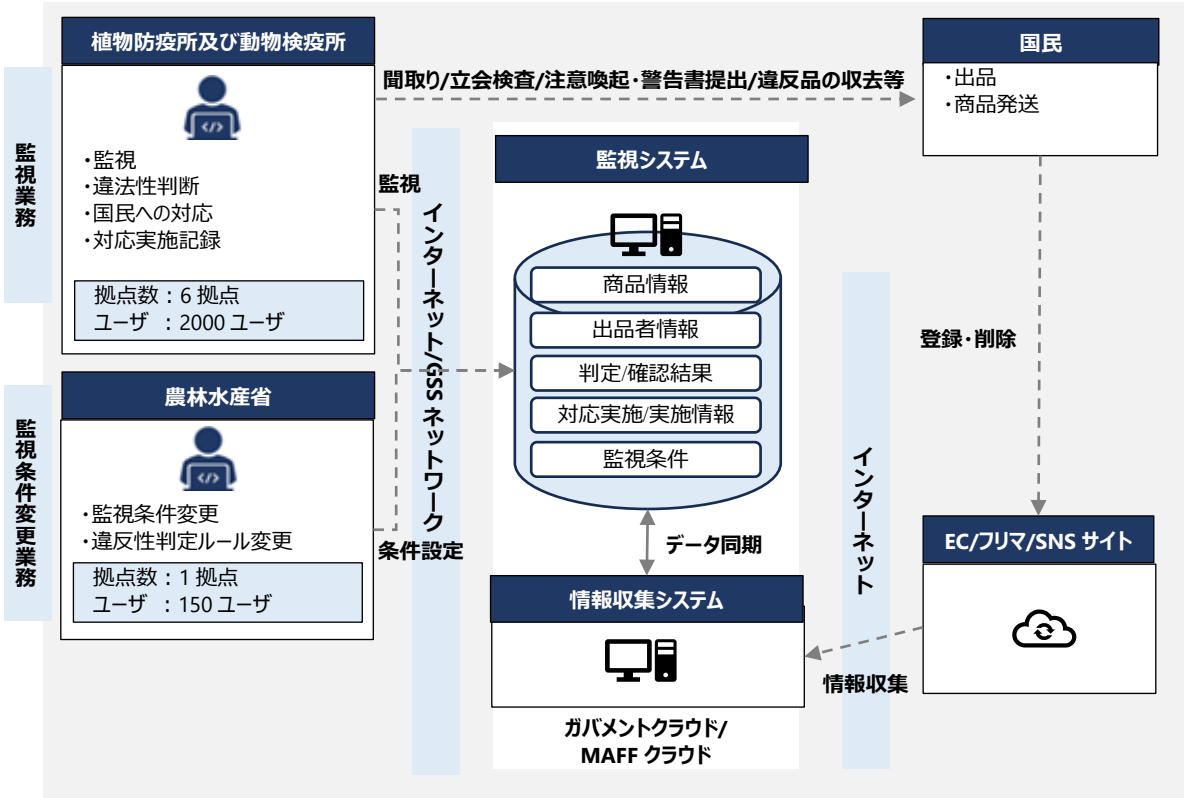
(2) 技術検証

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

(3) 機能構成概念図

本サービスの機能構成概念図を「図 3　機能構成概念図例」に示す。なお、図の記載内容が過度に複雑化することを避けるため、下図では機能分類に着目し、各機能の位置関係と情報フローに焦点を当てて表現することとしている。

図 3　機能構成概念図例



2.2. **画面に関する事項**

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

画面レイアウト等の設計に当たっては、予めワイヤーフレーム（画面の完成イメージを線や枠で表現したもの）などを作成し、PJMO の了承を得た上で設計を行うこと。

(1) 画面一覧

本システムの画面一覧を「表９　画面一覧（想定）」に示す。なお、個別具体のユーザーインタフェースとして実装する際の画面構成、画面レイアウト、画面タイトル等のラベル、画面遷移等の詳細は基本設計工程で定める。本要件定義書では画面設計に当たっての基本的な方針を定めている。

表９　画面一覧（想定）

項番	画面 ID	画面名	画面概要	該当機能	補足
1	S01	ダッシュボード画面	最新の商品情報に基づく違法性判定を実施された高リスク商品の集計値などをダッシュボードに表示する	F-1-1 ダッシュボード機能	
2	S02	違法性商品一覧画面	違法性の高い可能性のある商品(高リスク商品)情報の一覧を表示する	F-2-1 違法性商品一覧確認機能	
3	S03	違法性商品詳細画面	商品情報の詳細情報を表示する。経過観察などの状態を更新可能とする	F-2-2 違法性商品詳細確認機能	
4	S04	出品者一覧画面	システムが自動で収集した商品の出品者情報を表示する	F-2-3 出品者一覧確認機能	
5	S05	出品者詳細画面	出品者情報の詳細情報を表示する。対応実施内容の登録、履歴を表示する	F-2-4 出品者情報確認機能	
6	S06	監視条件管理画面	システムによる自動収集に係る監視条件を表示、修正する	F-3-1 監視条件確認機能 F-3-2 監視条件変更機能	
7	S07	違法性判定ルール管理画面	違法性判定に係るルールを表示、修正する	F-3-3 違法性判定ルール確認機能 F-3-4 違法性判定ルール変更機能	
8	—	ログイン画面	クラウドログインサービスを用いてシステムにログインする	F-4-1 ログイン機能 F-4-2 ユーザ管理機能	

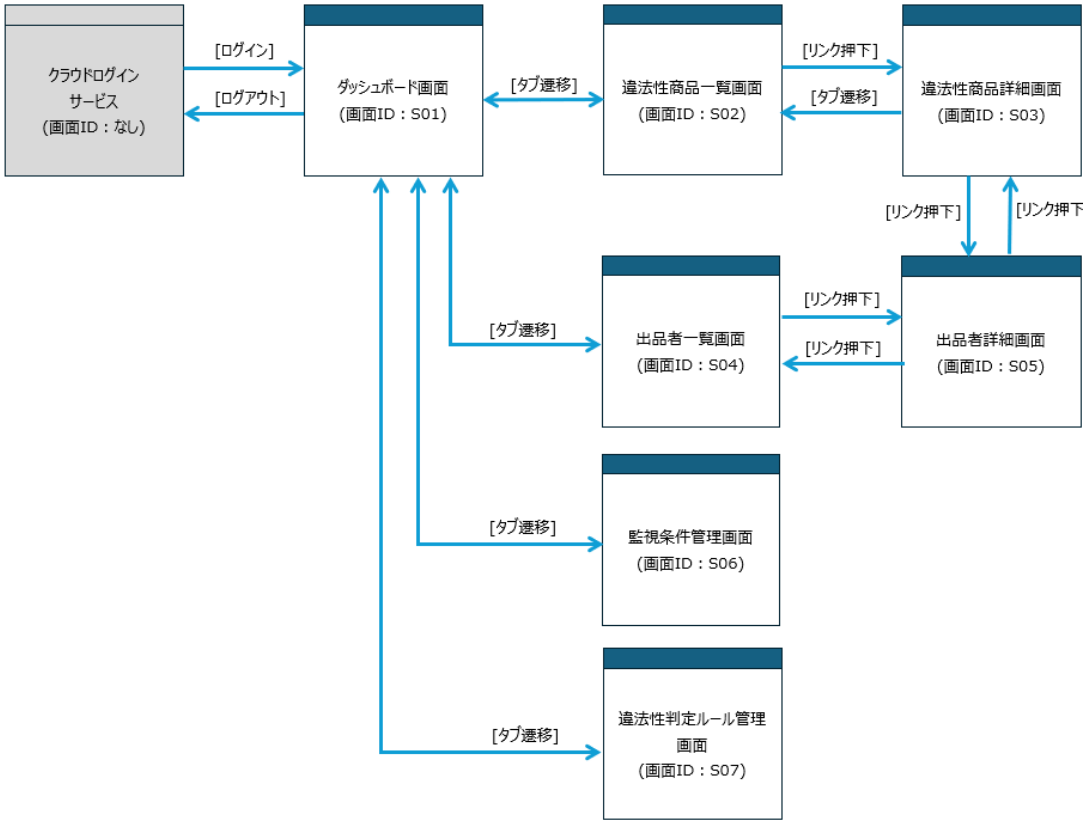
(2) 画面イメージ

本システムの基本的・代表的な画面イメージを「別添資料 2-2.画面イメージ一覧」に示す。紙面スペースの制約上、一部を抜粋したものとしているが、全体像については、調達仕様書に基づく資料閲覧を行う際に確認することが可能である。なお、表示イメージは、デザインプロトタイプとして作成したものである。個別具体のユーザーインタフェースとして実装する際の画面構成、画面レイアウト、画面タイトル等のラベル等については、本システムの設計・開発段階で行う UX 開発において改めて設計を行う。また、画面表示イメージに表現されている内容は、デザインを明確にする観点から便宜的に当てはめたものである。

(3) 画面遷移の基本的考え方

基本的・代表的な画面遷移として、トップ画面遷移図を「図４　画面遷移図」に示す。

図４　画面遷移図



(4) 画面設計ポリシー

画面設計における要件を以下に示す。

ア　UX デザイン

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

・　本サービス想定利用者の目的を満足する観点から、本サービスを構成する機能、コンテンツの設計に当たっては、適切なユーザ調査によって利用者の要件を把握すること。

・　本サービスに係る UX デザインは、UX に影響を及ぼす要素を 5 階層によって把握する UX5 階層モデルの考え方を導入する。本サービスの Web サイト及び Web アプリケーションについて、本サービスの目的を基底として、体系的かつ一貫性のある UX を確保できるようにすること。

イ　画面の表示

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

・　画面の表示には HTML を利用し、Web ブラウザ上で正常に表示されることを確認すること。また、JavaScript を無効にした状態でも最低限のコンテンツ情報を閲覧可能とすること。

・　画面の表示で使用する Web ブラウザには追加でプラグイン等のインストールを必要としないこと。

・　Web ブラウザのバージョンの更新があった際は、基本的には更新前のバージョンへの対応を保ちつつ、更新後のバージョンに対応させること。やむを得ず、双方のバージョンへの対応が困難な場合は、対応を優先するバージョンは担当部署が判断を行うものとする。

・　利用者が他に起動している Web ブラウザの動作に干渉しないように配慮すること。

・ Web ブラウザや利用端末の要件については、「3.11.情報システム稼働環境に関する事項」の「(7) 利用端末の要件」を参照すること。

ウ 入力負荷の軽減

画面での入力操作は以下の要件を満たすこと。

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

エ 誤操作の防止

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

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

オ メニュー

メニューについては、以下の要件を満たすこと。

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

2.3. **帳票に関する事項**

【帳票を作成する機能がない情報システムの場合】

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

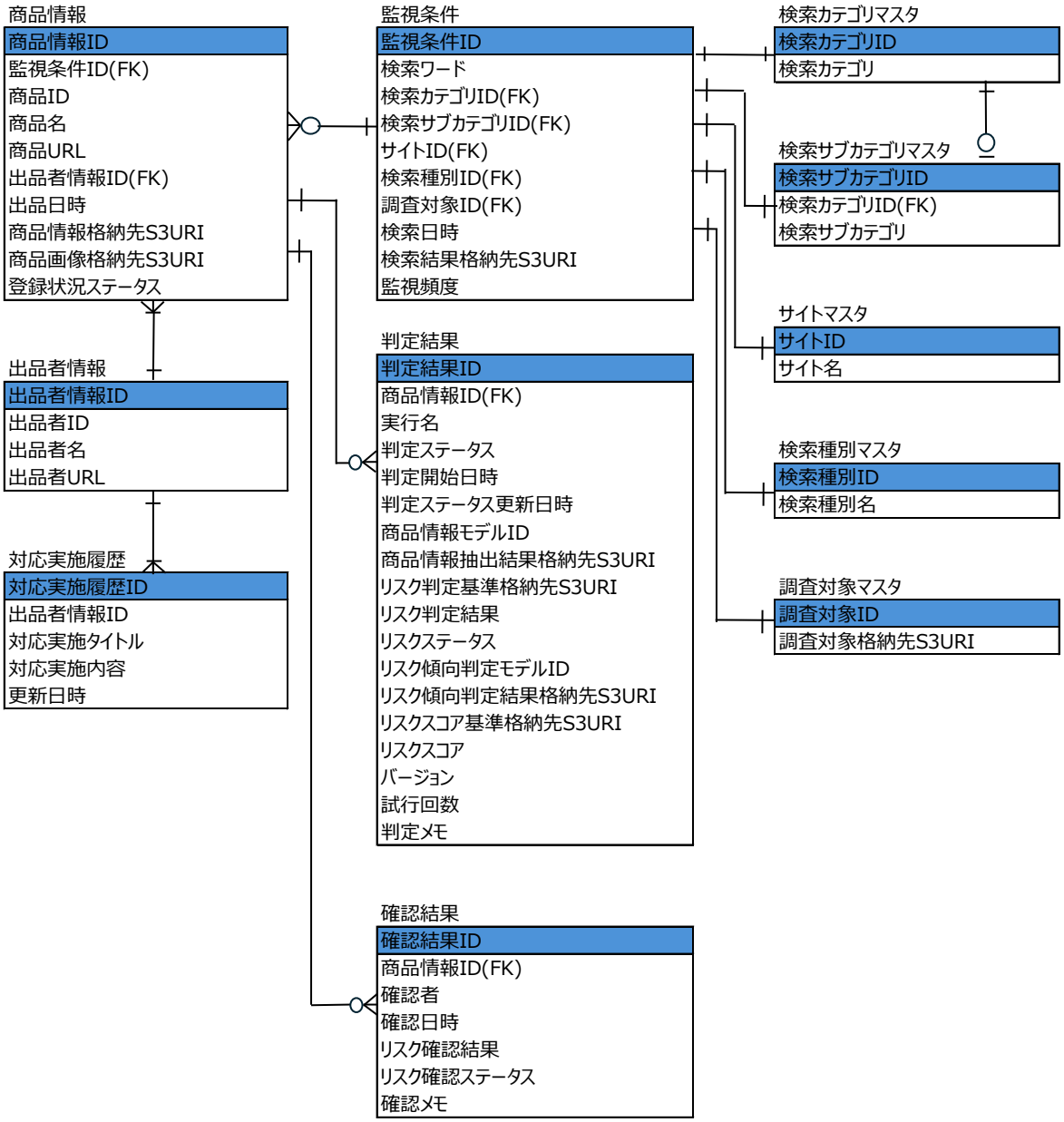
2.4. **データに関する事項**

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

(1) データモデル

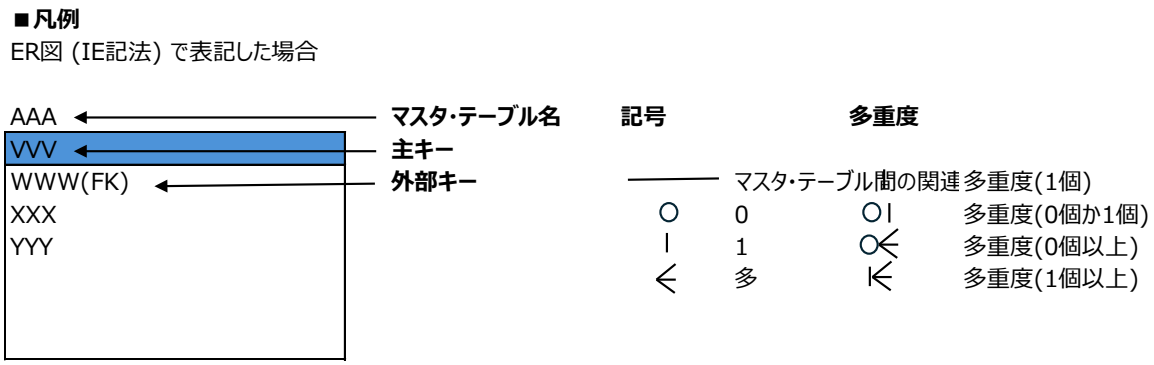
本システムのデータモデルを「図 5　データモデル」に示す。

図５　データモデル



また、データモデルの判例を「図６　データモデルの凡例」に示す。

図６　データモデルの凡例



(2) データ一覧

本システムのデータ一覧を「別添　2-3.データ一覧」に示す。

(3) データ定義

本システムのデータ定義は「別添資料　2-4.データ定義」に示す。

(4) CRUD マトリクス

本システムの CRUD マトリクスを「表 10　CRUD マトリクス」に示す。

表 10　CRUD マトリクス

機能 ID	機能名	概念データ (EN-xxx)										
		001	002	003	004	005	006	007	008	009	010	011
		監視条件	商品情報	判定結果	確認結果	出品者情報	対応実施履歴	サイトマスタ	検索種別マスタ	検索カテゴリマスタ	検索サブカテゴリマスタ	調査対象マスタ
F-1-1	ダッシュボード		R	R	R	R						
F-2-1	違法性商品一覧確認		R	R	R	R		R	R	R	R	R
F-2-2	違法性商品詳細確認	R	R	R	R	R		R	R	R	R	R
F-2-3	出品者一覧確認		R	R	R	R						
F-2-4	出品者詳細確認		R	R	R	R	R					
F-3-1	監視条件確認	R	R	R								
F-3-2	監視条件変更	RU										

F-3-3	違法性判定ルール確認											
F-3-4	違法性判定ルール変更											
F-4-1	ログイン											
F-4-2	ユーザ管理											
F-5-1	情報収集	R	C					R	R	R	R	R
F-5-2	AI データ分析	R	R	C		C						
F-5-3	データ削除		D	D	D	U						

※CRUD は、Create（作成）、Read（参照）、Update（更新）、Delete（削除）の各頭文字を指す。

(5) モニタリング対象データ一覧

「1.5.業務観点で管理すべき指標」に記載したプロジェクトの目標について、実績値を適時に確認するデータとして、現時点の案を「表 11　モニタリング対象データ一覧（想定）」に示す。

表 2　モニタリング対象データ一覧（想定）

No.	データ名（指標名）	分析軸となる項目	目的
1	違法出品発見数	違法出品発見数	月ごとの違法出品発見数を把握することで本システムの有用性を把握すること
2	月間アクティブユーザ数	ログインしたユーザ数	月ごとのログインユーザ数を把握することで本システムの業務への適用を把握すること
3	システム稼働率	年間実績稼働時間、 年間予定稼働時間	年間のシステム稼働率を算出することで、システムの課題を洗い出すこと
4	目標復旧時間	障害による停止時間	復旧時間が運用目標内にあるかを把握し、運用上の課題を洗い出すこと
5	システム稼働率 （フロントエンド）	年間実稼働時間、 年間予定稼働時間	実際にユーザが利用できる稼働率を算出することで運用上の課題を洗い出すこと
6	目標復旧時間 （フロントエンド）	障害による停止時間	障害発生時の停止時間を把握し、システムの課題を洗い出すこと

2.5. **外部インタフェースに関する事項**

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

(1) 外部インタフェース一覧

本システムは、「表 12　外部インタフェース一覧（想定）に示す他の情報システム等と連携する。なお、外部インタフェース一覧における記載内容は現在の想定である。設計工程において、連携先システム担当と調整の上、決定すること。

表 3 外部インタフェース一覧（想定）

項番	外部インタフェース ID	外部インタフェース名	外部インタフェース概要	相手先システム	送受信区分	送受信データ種別	送受信タイミング	送受信の条件		補足
								プロトコル	文字コード	
1	IF-001	商品情報取得(検索スニペット)	EC/フリマ/SNS サイトから商品情報を取得	検索サービス	受信	API（REST）	週次	HTTPS	UTF-8	
2	IF-002	商品情報取得(スクレイピング)	フリマサイト(スクレイピング許諾済)から商品情報を取得	各サイト	受信	HTML	週次	HTTPS	UTF-8	
3	IF-003	商品情報取得(API)	EC サイトから商品情報を取得	商品検索 API	受信	API（REST）	週次	HTTPS	UTF-8	

3. 非機能要件定義

3.1. ユーザビリティ及びアクセシビリティに関する事項

(1) 本システムの利用者の種類、特性

本システムの利用者の種類について、「表 13　本システムの利用者の種類」に示す。

表 4　本システムの利用者の種類

項番	利用者区分	利用者の種類	利用イメージ
1	農林水産省消費・安全局　植物防疫課／動物衛生課　システム管理者	本システム利用者（状況把握） 本システムの設定管理担当者 本システムのユーザ管理担当者	本システムの出品状況のダッシュボードを確認し、違法品の流通実態を把握する。 対象サイト、検索ワード等の監視条件の設定を行う。 本システムのユーザ管理の設定を行う。
2	農林水産省消費・安全局　植物防疫課／動物衛生課	本システム利用者（状況把握） 本システムの設定管理担当者	本システムの出品状況のダッシュボードを確認し、違法品の流通実態を把握する。 対象サイト、検索ワード等の監視条件の設定を行う。
3	植物防疫所／動物検疫所 出品監視担当者	本システム利用者（業務遂行）	本システムを用いて、出品に対する違法性の最終判断を行う。 対応を実施した場合は対応結果を記録として登録する。 経過観察など状況を更新する。
4	システム運用担当者 (事業者含む)	本システムの運用管理担当者	本システムのメンテナンス等の運用作業、認証サービス（アクセス管理）のメンテナンスを行う。

(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について、「表　14　ユーザビリティ要件」に示す。利用者が想定する流れに沿った操作手順、画面遷移、画面レイアウト、帳票レイアウト等とする。

表 54　ユーザビリティ要件

項番	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成 （直感・シンプル）	・　利用者が何をすればよいか直感的に理解できるデザインにすること。 ・　無駄な情報、デザイン、機能を排したシンプルでわかりやすい画面にすること。
2	画面の構成（フォント及び文字サイズ）	・　十分な視認性のあるフォント及び文字サイズを使用すること。 ・　画面サイズや位置を変更できること。 ・　一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成 （表示/非表示）	・　情報の優先順位をつけ、重要度の低い情報、特定の利用者層に対して提示する情報は、利用者が必要に応じて表示/非表示を切替え可能とする等の工夫をすること。
4	画面の構成 （クリックやチェックができる箇所）	・　画面上でクリックやチェックができる箇所とできない箇所の区別を明確にすること。 ・　タップ操作が可能なタブレット端末やスマホの場合は、タップ操作の結果（どの部分をタップしたのか）を適切にレスポンスできること。
5	画面遷移	・　利用者が次の処理を想像しやすい画面遷移とすること。 ・　無駄な画面遷移を排除し、シンプルな操作とすること。
6	画面表示・操作の一貫性（統一）	・　機能、用語、レイアウト、操作方法は統一すること。
7	画面表示・操作の一貫性（視認性）	・　必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること。 ・　見やすさを考慮し、画面のフォントサイズを決定すること。 ・　画面ごとに異なるフォントを使わないこと。
8	操作方法のわかりやすさ	・　無駄な手順を省き、使いやすく、利用者が効率的に作業できるようにすること。 ・　利用者が操作しやすい手順にするため、画面上の情報項目を上から下へ、左から右へ流れる順番に配置すること。 ・　利用者の操作を軽減できるよう、画面の初期表示時、入力項目、選択項目等に適切な既定値を設定すること。

項番	ユーザビリティ分類	ユーザビリティ要件
9	操作方法のわかりやすさ（操作説明）	・ 原則としてマニュアルを参照しなくても操作できるようにすること。
10	操作方法のわかりやすさ（Tab キー）	・ Tab キー等による画面上のフォーカスの移動順序について、利用者が操作しやすい順序となるようにすること。
11	操作方法のわかりやすさ（画面遷移）	・ 利用者が同じ情報の入力や操作を何度も行う必要がないよう、画面が遷移しても情報がその後の手順に反映されるようにすること。 ・ 利用者の手間を軽減するため、利用者の手順に即した画面遷移に留意し、可能な限り不要な画面遷移を行わないようにすること。
12	指示や状態のわかりやすさ	・ ユーザインタフェース及び UX に関する一般的に使われているデザイントレンドを取り入れ、アイコン・図表のグラフィック表現を適切に適用すること。 ・ 本システムが処理している内容や状況を、利用者が把握できるようにすること。
13	指示や状態のわかりやすさ（外部ドメインへの遷移）	・ ドメインを異にする他の Web サイトへの遷移を行う際は、離脱メッセージを表示する等、利用者が認識できるようにすること。
14	メッセージ出力	・ 利用者に分かりやすいメッセージとすること。 ・ 必要に応じて、登録・変更・削除等の操作を行う場合には、確認画面等で表示し、利用者の注意を促すこと。 ・ 処理時間がかかる操作では、処理中であることが分かるようにすること。
15	メッセージ出力（次の操作）	・ 指示メッセージは、次操作が具体的にイメージできるようなメッセージ出力を行うこと。
16	エラーの防止と処理	・ 利用者が操作や入力を間違えないデザインや案内を提供すること。
17	エラーの防止と処理（エラー防止）	・ 利用者の誤操作を想定し、入力チェック機能によりエラーを防止すること。 ・ 入力値が選択できる場合には、プルダウンメニュー等を活用し、極力キーボード入力操作をなくすこと。
18	エラーの防止と処理（エラーメッセージ）	・ エラーメッセージは、その内容が分かりやすく表示されるとともに、利用者が何をすればよいかを示すこと。
19	エラーの防止と処理（エラー表示と解決策）	・ 入力内容の形式に問題がある項目については、利用者がその都度該当項目を容易に見つけることができるようにすること。 ・ エラーが発生した時は、利用者が迷わずに問題解決できるよう、操作の続行に必要な選択肢を利用者が適切に理解できるようわかりやすく提示すること。 ・ 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにする。
20	エラーの防止と処理（確認画面）	・ 必要に応じて、登録、更新、削除等の処理の前に確認画面を用意し、利用者が行った操作や入力のやり直し、取り消しがその都度できるようにすること。 ・ 重要な処理については、事前に注意喚起し、利用者の確認を促すこと。
21	エラーの防止と処理（画面遷移）	・ 入出力の過誤があった場合、次の画面へ遷移しないこと。
22	ヘルプ	・ 利用者が必要とする際に、ヘルプ情報やマニュアル等を容易に参照できるようにする。 ・ ヘルプ情報やマニュアル等についても、利用者が必要な情報を容易に検索できるようにする。
23	画面遷移、操作ログ等の分析	・ 運用・保守工程において継続的に UI/UX の改善を検討できるよう、利用者の画面遷移、操作ログ等を分析できる仕組みを整備すること。
24	言語対応	・ 本システムでは、日本語のみのコンテンツとする。

(3) アクセシビリティ要件

アクセシビリティに関する要件を「表 15　アクセシビリティ要件」に示す。

表 6 アクセシビリティ要件

項番	アクセシビリティ分類	アクセシビリティ要件
1	基準等への準拠	・ 日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用ガイドライン」（総務省）に準拠し、以下を前提とすること。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html ・ JIS X 8341-3:2016「高齢者・障害者等配慮設計指針 – 情報通信における機器，ソフトウェア及びサービス – 第 3 部 : Web コンテンツ」の適合レベル AA に準拠することを目標とする。 ・ 注記 : 本仕様書における「準拠」という表記は、情報通信アクセス協議会 Web アクセシビリティ基盤委員会「Web コンテンツの JIS X 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 ・ デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
2	指示や状態の分かりやすさ	・ 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者への情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。ただし、業務の利用用途から、画面色での振り分けを行うことを予定していることから、適用範囲及び配色については担当部署及び関係省庁と協議し、決定すること。 ・ Web ブラウザ等の音声読み上げ機能を活用し、視覚障がいの方でも問題なく利用可能な UI とすること。

3.2. **システム方式に関する事項**

(1) システム方式についての全体方針

システム方式についての全体方針を「表 16 システム方式についての全体方針」に示す。本システムはクラウドネイティブの構成として、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（以下、「クラウド方針」という。）」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。本システムは、ガバメントクラウド又は MAFF クラウド上に構築し、AWS、Azure、GCP、OCI で同等のシステムを構築可能であるが、特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。

表 7 システム方式についての全体方針

項番	観点	全体方針
1	システムアーキテクチャ	・ 本システムのシステムアーキテクチャはクラウドサービス上に用意される Web アプリケーションから構成される。Web アプリケーションは利用者の端末に追加的なソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとする。 ・ 本システムや業務機能等の特性を十分に検討し、クラウドサービスプロバイダが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、情報システムを構築する。 ・ クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションの作り込みを削減できる設計とする。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 ・ クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を行い、安全かつ効率的に情報システムを構築する。 ・ 予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。管理者アカウントについては、多要素認証を必須とすること。
2	アプリケーションの設計方針	・ サーバレス実行 ・ マイクロサービスアーキテクチャ、API、クラウドネイティブ、クラウドサービスのマネージドサービスによる構成等、モダン技術を前提として構築する。

		・ クライアントサーバ方式、専用端末のシンクライアント（VDI）等の旧来技術は、高コスト化の要因となるため採用しないこと。 ・ 情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする。 ・ 本システムが取り扱うデータの保管・管理に際して、データの容量、更新頻度、保存期間等を考慮し最適なストレージサービスを選定の上、利用する。またデータの保管・管理方針が変更となった際に、ストレージサービス間でのデータの移行が容易となるよう設計上考慮する。
3	ソフトウェア製品の活用方針	・ SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 ・ 広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 ・ アプリケーションの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認しなければならない。

(2) クラウドサービスの選定、利用に関する要件

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

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

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

エ　契約の解釈が日本法に基づくものであること。

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

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

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

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

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

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

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

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

ス　クラウドサービスの提供に関する次のいずれかの認証を取得していること。
- ISO/IEC 27017:2015
- CS マーク（特定非営利活動法人日本セキュリティ監査協会（JASA）のクラウドセキュリティ推進協議会が定めるもの）

セ　ガバメントクラウドにおける開発に際し、特定の機能群を代替する優れた SaaS が存在する場合、当該 SaaS の導入も検討すること。

(3) 開発方式

ア　開発に当たっては、開発環境等を用意すること。各環境の詳細については「3.11.情報システム稼働環境に関する事項」を参照すること。

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

ウ　ソースコード管理（バージョン管理）については、発注者/PJMO と協議の上、受注者にてサービスを構築して整備すること。また、運用・保守事業者が該当ライセンス等を用意した上でそれらを引き継ぐことが可能であること。

(4) 機器等の設置方針

本システムはクラウドサービスを前提としているため、設置場所についてはクラウドサービスプロバイダの提供する場所となるが、その際は日本国内のリージョンを選択すること。

(5) その他

システム方式に係るその他の要件を以下に示す。

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

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

3.3. システム規模に関する事項

本システムの規模要件を以下に示す。また、本システムの規模に関する業務要件は、「1.2 業務の規模」を参照のこと。

(1) 規模に関する前提条件

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

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

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

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

(2) データ量

本システムで想定されるデータ量を「表 17　データ量」に示す。なお、年間データ増加量は仮定をおいた上での試算結果を記載しているため、設計等を考慮の上、必要なデータ量のサイジングを行うこと。

表 8　データ量

項番	項目	データ種類	データ量	補足
1	業務データ	データベース	12GB	データベースのオーバーヘッド、 バックアップ、BCP 除く
2	収集ファイル	テキスト・画像	525GB	テキストファイル　25GB/年 画像ファイル　500GB/年
3	操作ログ	テキスト	22GB	

(3) 処理件数

本システムで想定される処理件数を「表 18　処理件数」に示す。なお、本システムの運用期間を踏まえ予想される増加率（年間で 5%～10%程度の増加率）を考慮する必要がある点について留意すること。

表 9　処理件数

項番	項目	処理件数	補足
1	業務処理件数（ピーク時）	125（件／分）	通常時の 5 倍程度を想定。
2	業務処理件数（通常時）	25（件／分）	1 日 6000 アクセスと想定。 業務時間（8 時間）。
3	バッチ処理	24 万（件／月）	情報収集：18 万件/月 AI データ分析：6 万件/月

(4) 利用者数

本システムで想定される利用者数を「表 19　利用者数」に示す。

表 10　利用者数

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

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

(5) 保管データ量・保管期間

本システムに保管するデータ量やデータの保管期間について「表 20 データ保持期間（案）」に示す。要件の整理の中で調査を行い、PJMO と協議の上、決定すること。

表 11 データ保持期間（案）

項番	項目	データ種類	保管期間
1	業務データ（商品/出品情報など）	データベース	5 年間
2	業務データ（報告情報など）	データベース	5 年間
3	収集ファイル	テキスト・画像	3 年間
4	操作ログ	テキスト	1 年間

3.4. 性能に関する事項

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

また、クラウド上に構成するサーバ・サービスは自動スケーリング機能の利用やスペック調整を容易にできるような構成にし、性能を容易に改善できること。

(1) 性能を考慮する対象

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

- ダッシュボード/違法性商品一覧・確認/出品者情報/監視条件確認・変更/違法性判定ルール確認・変更/ログインの画面表示機能

ア 性能目標の設定対象

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

イ 性能見積もり

本システムのアプリケーション処理時間に係る性能見積りは、以下を考慮する。

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

(2) 応答時間

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

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

表 12 目標レスポンスタイム

項番	指標名	目標値	補足
1	参照系処理	3 秒	画面の読み込み、情報の表示に関する処理
2	更新系処理	5 秒	情報の登録、更新、削除に関する処理
3	読込系処理	120 秒	検索キーワードファイルなどの読込に関する処理

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

3.5. 信頼性に関する事項

本システムに備える機能の停止等による業務への影響を最低限にとどめるため、クラウドサービスの利用を前提とし、その中でもマネージドサービスを主体として構築する。クラウド上で稼働するサーバやサービスに対しては冗長化などの構成を行うなど、可用性を高めた構成とすること。可能であればクラウドサービスのベストプラクティスが自動で適用されるよう、SaaS 形態のサービスを利用すること。また、サーバで構築する場合、以下に示す要件を踏まえ本システムの信頼性を確保すること。

(1) 可用性要件

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

ア　可用性に係る目標値

可用性に係る目標値を「表 22 可用性に係る目標値」に示す。

表 13　可用性に係る目標値

項番	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ・　接続回線の計画停止時間 ・　大規模災害等の天災地変に起因する停止時間 ・　連携する情報システムやクラウドサービス又は通信ネットワークの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・　本システムのメンテナンスによる計画停止時間
2	稼働率	99.9% 以上	本システムにおける稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x 100 当該計算式において、年間実稼働時間は「利用者が本システムを利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。

イ　可用性に係る対策

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

・　クラウドサービスの利用を前提として、本システムを構成するサーバ、ネットワーク機器及びネットワーク経路を冗長化し、単一障害点（SPOF）を回避すること。
・　本システムに係る運用・保守上の人的ミスに起因する障害が本システムの可用性に影響を与える事態を未然に防止するため、「3.17 運用に関する事項」及び「3.18 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

(2) 完全性要件

以下に示す要件を踏まえ、本システムの完全性を確保するための対策を行うこと。

ア　クラウドサービスの利用を前提とし、以下の対策を講ずること。
・　コンポーネントの故障に起因するデータの減失や改変を防止する。
・　異常な入力や処理を検出しデータの減失や改変を防止する。

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

3.6. 拡張性に関する事項

(1) 性能及び機能の拡張性

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

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

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

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

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

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

3.7. 上位互換性に関する事項

(1) 上位互換性
クラウドサービスのマネージドサービスの活用を前提とするが、サーバを使用する場合は、OS、サーバソフトウェアのバージョンアップ又は変更に備え、本システムを構成する。

ア　クラウドサービスのバージョンアップ

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

イ　OS 等への依存

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

ウ　クライアント端末の更新

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

3.8. 中立性に関する事項

(1) オープンな標準的技術又は製品の採用

本システムを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準的なサービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。将来クラウドサービスプロバイダーが変わっても、新たなクラウドサービスプロバイダーが提供するクラウドへのデータ移行を容易に可能とすること。

ア　データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

- 本システム内のデータについては、原則として XML や CSV 等の標準的な形式で取り出すことができるものとすること。
- パッケージ製品から抽出されたデータであっても、移行データフォーマットや移行データの権利は PJMO に所属すること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）をドキュメントに取りまとめること。ドキュメントについては、本システムの業務要件を理解しているユーザであれば理解できるように記述すること。なお、システム運用期間中に該当ドキュメントの内容に変更が生じる場合は継続して改定を行い最新化できること。
- 移行データに関する文字コード等は以下に従うこと。

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

イ　オープンソースソフトウェア（OSS）の活用

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

ウ　オープンなインタフェースの活用

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

3.9. 継続性に関する事項

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

(1) 継続性に係る目標値

以下に、機能停止等の原因となる事象の規模に応じて継続性に係る目標値を示す。

ア　予測可能な障害発生時

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

イ　業務停止を伴う障害発生時

予測困難な事象により業務停止を伴う障害が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を「表 23 継続性に係る目標値（業務停止を伴う障害発生時）」に示す。

表 14 継続性に係る目標値（業務停止を伴う障害発生時）

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

ウ　大規模災害発生時

インターネット等通信インフラが被災しておらず、発災前と同様の通信環境が確保されていることを前提として、大規模災害による業務停止が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を「表 24 継続性に係る目標値（大規模災害発生時）」に示す。

表 15 継続性に係る目標値（大規模災害発生時）

項番	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	5 日以内	通常どおりのサービスレベルに復旧（機能面は通常レベル、性能面では通常の半分のレベルの復旧とする）	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）

(2) 継続性に係る対策

本システムの継続性要件を実現するために、以下の対策を講じること。

ア　冗長化

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

イ　アベイラビリティゾーン

マネージドサービス以外では、アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とする。しかし頻繁に AZ 間の通信が発生するアプリケーションについては、AZ 間のレイテンシが増幅し性能に影響を与える可能性がある。これらの性能面の影響を評価できるよう、設計・開発期間中の早い段階で性能面の影響を評価

し、必要に応じてアプリケーション改修等の手段で性能改善への対応方針を確立すること。

ウ　データバックアップ

・　バックアップ対象

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

・　バックアップ頻度

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

・　保存期間

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

・　アクセス権限

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

・　バックアップツール

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

エ　システムバックアップ

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

　「表 23　継続性に係る目標値（業務停止を伴う障害発生時）」及び「表 24　継続性に係る目標値（大規模災害発生時）」に示す RTO、RLO、RPO を満たすようにすること。

3.10.　情報セキュリティに関する事項

(1) セキュリティ対応方針

　セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を「表 25　本システムにおけるセキュリティ対応方針」に示す。

表 16　本システムにおけるセキュリティ対応方針

項番	分類	概要
1	原則	・　「政府機関等のサイバーセキュリティ対策のための統一基準」、「農林水産省における情報セキュリティ確保に関する規則」に準拠した情報セキュリティ対策を講ずること。なお、「農林水産省における情報セキュリティの確保に関する規則」は非公表であるが、「政府機関等

		のサイバーセキュリティ対策のための統一基準」に準拠しているので、必要に応じ参照すること。「農林水産省における情報セキュリティの確保に関する規則」の開示については、契約締結後、受注者が農林水産省に守秘義務の誓約書を提出した際に開示する。 ・ セキュリティ対策については、高度化/大規模化するサイバー攻撃等に対応するため、多層防御やサイバーレジリエンス強化といった原則に基づいて要件を定義する。
2	システム特性 （概要）	【システムの利用者】 ・ 本システムは政府系職員向けサービスであり、一日に 10 人程度の利用者が想定される 【システムで取り扱う情報】 ・ 特定個人情報は取扱われない ・ EC・フリマ・SNS サイトで扱われる情報が取扱われる 【利用環境・ネットワーク構成】 ・ 利用者はブラウザからンターネット、または GASS ネットワークを介して当該 Web システムにアクセスし、ログインして各種機能を使用する ・ システム管理者はインターネット VPN を介して本システムにアクセスし、システム管理を実施する ・ 外部システムとの接続はなし
3	優先的に 対処すべき セキュリティリスク	【優先的に対処すべきセキュリティリスク】 ・ 外部からの不正アクセスにより、本システムの個人情報が漏洩する。 ・ サービス妨害を目的とした攻撃等により本システムが長時間停止する。
4	セキュリティ対応 方針	【セキュリティ要件のベースライン】 ・ 本システムにおいては、セキュリティ要件を過不足なく導出するため、NISC の提供する SBD マニュアルをセキュリティベースラインとして利用する 【優先的に対処すべきセキュリティリスクへの対応方針】 ・ 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 ・ 外部からの不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 ・ サービス妨害を目的とした攻撃対策については、L3～L7 層で対策可能な仕組みを導入する。 【その他セキュリティリスクへの対応方針】 ・ ・上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

(2) セキュリティ要件

上記のセキュリティ対応方針に基づき、「別添資料 3-1.情報セキュリティに関する事項」に本システムにおけるセキュリティ要件を記載する。

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

開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみに縛られず、必要に応じて追加のセキュリティ対策を講じること。また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考に情報システムの脆弱性が作りこまれないように留意すること。

3.11. 情報システム稼働環境に関する事項

クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。稼働環境については、ガバメントクラウドを利用することを前提とする。詳細については、

「 https://guide.gcas.cloud.go.jp」を参照すること。

(1) システム構成

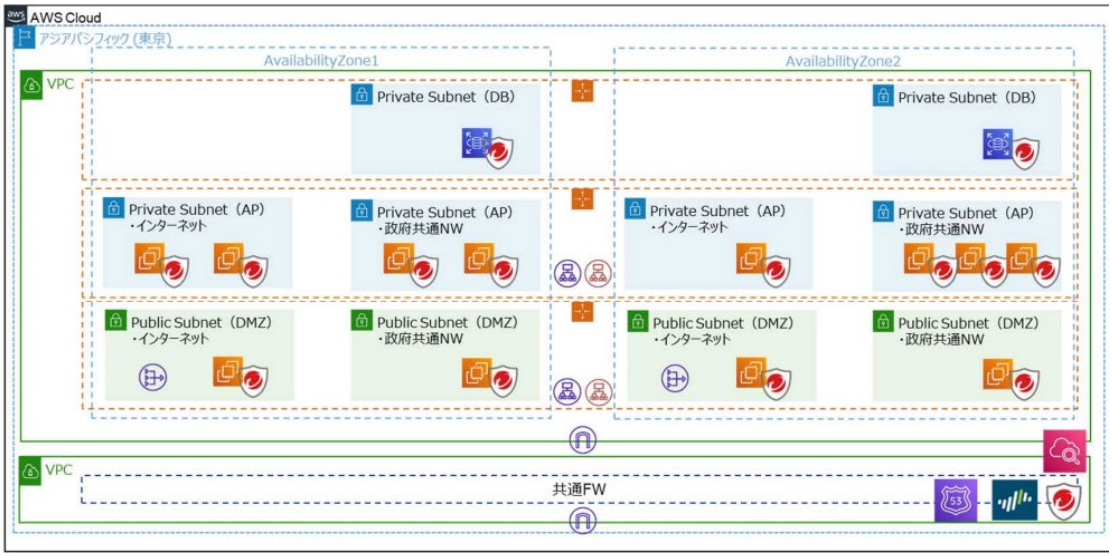
受注者は、設計・開発及び運用・保守に用いる環境としてクラウドサービス上に構築する「本番環境」、「検証環境」及び「開発環境」の 3 種類を利用すること。

設計・開発及び保守作業は、原則として「検証環境」及び「開発環境」で行った上で、「本番環境」にリリースし、運用作業を行うこと。環境の構成や利用方法の詳細は、PJMO と協議の上決定すること。

ア 本番環境

現段階で想定する本システム本番環境の構成図を「図 7 本番環境システム構成（想定）」に示す。本構成では、AWS を想定として記載している。

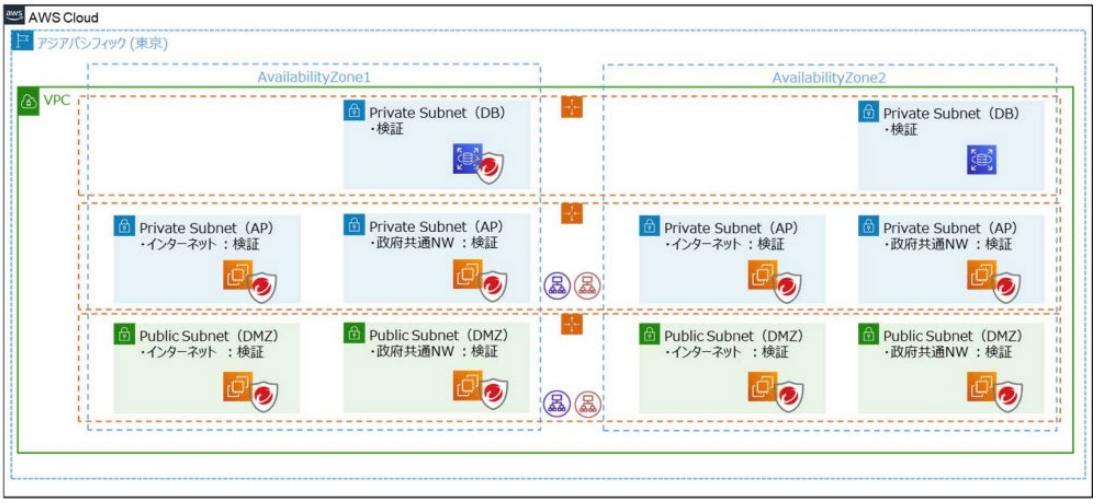
図 7 本番環境システム構成（想定）



イ 検証環境

現段階で想定する本システム検証環境の構成図を「図 8 検証環境システム構成（想定）」に示す。原則として本番環境同様とするが、検証用途に最低限必要な要素を踏まえ、縮退した構成とし、性能、信頼性については本番環境と同等にする必要はない。

図 8 検証環境システム構成（想定）



ウ　開発環境

継続的インテグレーション・継続的デリバリー（以下、「CI/CD」）を実現するための開発環境を整備すること。

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

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

(2) クラウドサービス構成

ア　クラウドサービスの要件

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

イ　クラウドサービス構成

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

(3) ソフトウェア構成

本システムの構築に当たっては、可能な限りクラウドサービス提供のマネージドサービスを活用すること。また、いずれのソフトウェアについても、原則として最新バージョンを適用する。

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

(4) ネットワーク構成

ネットワーク構成は「（1）システム構成」を参照すること。

【ネットワーク構成を設計・開発時に決定する場合】

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

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

イ　クラウド上に論理的に隔離された仮想閉域ネットワークを構築すること。

表 17　ネットワーク構成

項番	回線種別	ネットワーク要件	補足
1	インターネット/GSS ネットワーク	・ ネットワーク帯域：1Gbps 程度(理論値) ・ 冗長構成：有 ・ 通信回線装置におけるアクセス制御の設定：有 ・ 暗号化：有 ・ 通信プロトコル：HTTPS	

(5) 利用端末の要件

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

ア　本システムの運用開始時点で動作保証の対象とする PC・OS の機種やバージョンを「表 27 動作保証対象とする利用端末」に示す。

表 18 動作保証対象とする利用端末

項番	端末	OS	バージョン
1	PC	Windows	11
2	PC	Mac	26

イ　本システムの運用開始時点で動作保証の対象とするブラウザは以下とする。

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

3.12. データマネジメントに関する事項

本システムのライフサイクル全般を通じて、保有するデータ品質の維持・向上やデータの適正な利活用等を実現するため、以下に示す要件を踏まえ本システムのデータマネジメントを実施すること。

(1) データ管理体制の明確化

システムで扱うデータの種別ごとに管理主体（管理する組織、担当者等）や役割の設定を PJMO と共に行い、データ毎の管理責任を明確化すること。

(2) データの標準化

データの相互運用性を高めるため、以下の点に留意すること。

ア　マスターデータは、広範囲に共通利用できるデータから選定すること。マスターデータを独自に作成する場合は、関連する分野でも共通利用できるように設計上の配慮を行うこと。

イ　コード値については、国際標準、業界標準など、広範囲に共通利用されているものを採用すること。コード値の標準化については、「コード（分類体系）導入実践ガイドブック」（デジタル社会推進標準ガイドライン DS-463-1）を参考とすること。

ウ　本システムだけでなく、関連分野全体でのデータ流通を促進するという大局的な視点も踏まえて、ステークホルダーとの連携、調整を PJMO と共に行うこと。

(3) データに関するドキュメントの一元的管理

本システムの運用・保守にあたってデータに関する一元的管理が行えるように、データに関する各種設計書等のドキュメントを内容的に独立した構成とすること。

(4) オープンデータ化を容易にする設計

本システムが扱うデータのうち、オープンデータとして対外的に公開することが有意義と考えられるものについては、公開要否を PJMO が検討することを支援する。また、オープンデータとして公開するデータについては、オープンデータ・バイ・デザインの考え方に基づき、機械判読性の高いデータにする、Web-API により処理できるようにする、データを抽出しやすいデータベース構造にする等の対応を設計段階から十分に検討し、実装すること。

(5) データに関する運用情報の管理

システム障害等が発生した際に迅速な原因分析が行えるように、データに関するログ機能を充実させること。

また、サービス・業務の運営状況に関する指標や本システムの利用状況等のデータを適時に把握できる機能を組み込み、取得したデータに基づいて本システムの継続的な改善を行うとともに、サービス・業務改革（BPR）が行えるようにすること。

(6) データの機密性定義に応じた設計

データの機密性に応じたセキュリティを確保するため、データ配置やアクセス管理方法について設計段階から十分に検討し、実装すること。

(7) データ品質の継続的改善

データ品質に起因するシステム障害や不具合を防止し、データの利活用を推進するため、データ品質の定期的な棚卸と不備・不具合の改善を行うこと。

3.13. テストに関する事項

本システムのテストに関する要件を「表 28 テスト要件」に示す。なお、品質管理の観点から必要に応じてPJMO が指定する専門チームがテストに参加することもあるため、受け入れること。また、テストデータやテストに関連する情報の提供にも協力すること。

表 19 テスト要件

項番	分類	要件
1	テスト工程の定義	・ 本システムでは調達仕様書に記載の通り、以下のテストを実施する。 (1) 単体テスト (2) 結合テスト (3) 総合テスト (4) 受入テスト
2	テスト環境	・ 本番環境に加え、テストを実施するための環境（開発環境・検証環境等）を整備すること。 ・ テスト環境については、連携先機関と接続して行う外部連動テストが実施可能な環境として整備するほか、同時並行的な開発に対応できるように複数のテスト環境を整備すること。 ・ 開発スケジュールを踏まえ、効率化を考え、各環境を流用するなど検討すること。
3	テスト計画書	・ 各テスト工程の開始時に、以下の内容を定義したテスト計画書を作成し、PJMO の承認を得ること。 ➢ テスト計画書の目的と位置付け ➢ テストの目的、概要 ➢ 対象範囲 ➢ テストスケジュール ➢ テストの観点 ➢ テスト実施体制、役割分担 ➢ テスト実施手順 ➢ テスト環境 ➢ テストシナリオの概要 ➢ 工程開始条件、工程終了条件 ➢ 使用するテスト自動化ツール ➢ 成果物一覧 ➢ テスト結果に係る定性・定量評価の方法（テスト密度、バグ検出密度等） ➢ 進捗管理 ➢ 品質管理 ➢ 不具合管理 ・ 受注者は、本業務を実施する各過程においてテスト計画書の内容に変更が生じる場合、変更箇所及び内容について PJMO の承認を得ることを条件として、テスト計画書を適切に更新すること。 ・ 情報セキュリティの観点から必要なテストがある場合には、テスト項目及びテスト方法を定め、これに基づいてテストを実施し、その実施記録を保存すること。

		・ 受注者は、テストに係る管理要領を共通化し、各テスト工程において、原則として同一の管理要領を適用するようにすること。各テスト工程に応じて部分的に異なる管理要領の適用を必要とする場合は、その適用差分のみ「テスト計画書」に記載すること。
4	テスト 仕様書	・ 本システムの各テスト工程の開始前に、テストシナリオ、テスト項目等を記載したテスト仕様書を作成すること。 ・ 各テスト工程のテスト項目は、設計書等の記述内容を網羅的に確認できるよう作成すること。 ・ 各テスト工程に応じたテスト技法を適用すること。 ・ テスト項目は、品質を確保するために十分なテスト項目を定義すること。また、テスト計画の策定時に定めた定性・定量評価方法を満たすよう作成すること。 ・ 受注者においてレビューを徹底し、上記要件を満たしたテスト仕様書となっているかを確認すること。
5	テストの 実施	・ 作成したテスト項目に基づきテストを実施すること。 ・ テストを実施する際は証跡を取得すること。証跡の納品対象については別途 PJMO と協議の上決定すること。 ・ 受注者は証跡等に代表されるテストの成果物のレビューを徹底し、テスト項目に基づきテストを実施しているか確認する。想定外のテスト結果となった場合は、本システムの欠陥であるか、想定結果が誤りであるか等、原因を明らかにした上で必要な対応を行うこと。 ・ 欠陥を検知した場合は、その原因を明らかにした上で、原因を解消すること。 ・ 検知した欠陥について修正を行った場合は、修正対象機能について回帰テストを実施すること。 ・ PJMO において、再テストが必要と判断した場合、受注者は再テストの計画を作成し、PJMO の承認を得た上で、定められた期限内に再テストを実施すること。また、類似バグを抽出するため、必要に応じて強化テストを実施すること。
6	テストデータ	・ 総合テスト及び受入テストにおいて実データを使用する必要がある場合は、実データの取得申請を条件として、実データの使用を許可する。なお、疑似データの作成に当たり、実データの匿名化、符号化等を行う場合は受注者の作業とする。 ・ 取得した実データは、適切に保管・管理すること。 ・ 受入テストにおいて作成したテストデータは、システム切替え実施前までに、検証環境等のデータも含め削除すること。 ・ 機密性の高いデータ項目や個人情報に係るデータ項目は、マスキングした上で使用すること。
7	対応状況の 報告	・ テストの進捗としては、テスト実施済項目数や信頼度成長曲線等の定量的なメトリクスの推移を示すことにより、テスト進捗状況、不具合検出状況及び不具合対応状況を報告すること。 ・ 受注者は、PJMO からのテストの進捗状況や品質等に対する指摘に対し確実に修正すること。 ・ 結合テスト・総合テストでの報告書には、ソースコードメトリクスを取得し、テスト結果及び品質指標とともに、PJMO に報告すること。 ・ 受注者は、各テスト工程に応じたテスト計画内容について PJMO に説明し、各テスト工程における最初のテスト開始予定日の遅くとも 1 週間前までに PJMO の承認を得ること。
8	テスト 完了報告書	・ 各テスト工程の完了に当たっては、テスト完了報告書を作成し、PJMO の承認を得ること。また、完了に当たっては以下をすべて満たすこと。 ➢ すべてのテスト項目が完了していること。 ➢ テスト結果について、定性評価及び定量評価（テスト密度、バグ検出密度等）により評価を行うこと。 ➢ テストで発生したすべての障害が、当該テスト工程内で解消されていること。 ➢ 外的要因等により次工程への申し送り事項が発生した場合は、対応方針、対応時期等を明確にした上で、PJMO の承認を得ること。
9	テストの 自動化	・ 各テスト項目のうち、反復的にテストを実施するものについては、自動化することを原則とする。そのために、必要となるテストツールについては、新規に作成するか、既存のツールを活用すること。 ・ UI のテスト、受入テスト等、テストの自動化に馴染まないものについては、自動化対象外とする。ただし、自動化対象外とすることについて、PJMO の承認を得ること。
10	将来時点の 仕様変更	・ OSS を適用する部分を除き、将来時点の仕様変更への対応を柔軟にする観点から、ソースコードに対する静的解析及びリファクタリングにより、クラスや関数構造をシンプルに保つこと。
11	構築時の 脆弱性対策	・ 品質保証、フォレンジック及びインシデント・レスポンスの観点から、問題原因を把握するために必要な例外情報をログに出力するようにすること。 ・ 設計・開発段階の早期からセキュリティを検証すること。

(1) 単体テスト

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

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

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

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

ウ　単体テスト実施時は、テスト結果を検証するための証跡を採取すること。

エ　単体テストは、原則として開発環境において実施すること。

(2) 結合テスト

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

ア　結合テストの観点として「表 29 結合テストの主なテスト観点」を想定する。

表 20 結合テストの主なテスト観点

項番	テスト種別	概要
1	システム基盤テスト	構築した本番環境及び検証環境の確認を行う。現時点で想定するシステム基盤テストの要件を以下に示す。 ・ 環境設計において作成したリソース定義コードを実行し、本システムのインフラストラクチャを構成する環境及び仮想資源を構築すること。 ・ 構築した環境及び仮想資源が正しく動作するか、動作確認テストを実施すること。 ・ クラウドサービスが提供するツールによって実行可能なテストコードを作成すること。 ・ 動作確認テストの結果、何らかの異常またはエラーを確認した場合、実行したリソース定義コードに原因が作り込まれていないか、必要な見直しを行うこと。 ・ 問題修正後、該当する環境または仮想資源について、再構築と動作テストを再度実施すること。

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

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

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

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

カ　結合テスト実施時は、テスト結果を検証するための証跡を採取すること。

キ　結合テストは、原則として開発環境または検証環境において実施すること。

(3) 総合テスト

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

ア　総合テストの観点として「表 30 総合テストの主なテスト観点」を想定する。

表 21 総合テストの主なテスト観点

項番	テスト種別	概要
1	業務運用テスト	・ 業務の実施手順や業務で取り扱うデータを基に様々なシナリオ・データのバリエーションを作成し、本システムを用いて業務、機能を確認する。 ・ シナリオ・データには、日常的に実施する業務や日常的に取り扱うデータだけではなく、月次や年次等の特定のタイミングでしか発生しない業務やイレギュラーデータも含めること。 ・ ユーザの誤操作や予期しない現象を契機としたシステム障害が発生しないことを確認することを目的として異常系のテストケースも含めること。
2	性能・拡張性テスト	ユーザ数、データ量、リクエスト数、レスポンス等の性能要件を本システムが満たしているか検証する。検証に当たっては、現在の想定だけではなく、今後の予想される増加量も含めて確認する。 短時間で本システムに重い負荷をかけ、本システムが処理量や長時間稼働等のシステム限界に関する性能や拡張の要件を満たしているか確認する。
3	可用性（障害）テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、どの程度許容して安定動作するか検証する。また、システム障害及びエラー発生時の回復機能等が適切に動作することを確認する。
4	完全性テスト	疑似的に障害を発生させる等の方法により、本システムのコンポーネントに障害が発生した場合に、データの減失や改変がないことを検証する。また、操作ログやアクセスログ等のシステムログが出力されることを検証すること。
5	セキュリティテスト	不正侵入や Web 特有の攻撃への対策、データベースへの不正アクセスなどに対する対策、データの持ち出しに対する対策、マルウェア（ウィルス）対策等のセキュリティ要件を満たしているか脆弱性検査、インシデントレスポンステスト等を実施し確認する。
6	運用・保守テスト	運用・保守作業全般を通して、運用・保守事業者が円滑に日々の業務を実施できることを確認する。 また、運用・保守における正常時、異常時の運用に関する動作を確認し、特に異常時の対応として、エラーメッセージやログ等を基に、運用・保守事業者が業務を行えることを確認すること。

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

ウ　キーワード駆動テストの適用により、総合テストの効率化を図ること。

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

オ　総合テスト実施時は、テスト結果を検証するための証跡を採取すること。

カ　総合テストは、原則として検証環境または本番環境において実施すること。

(4) 受入テスト

受入テストは、要件に対するアプリケーションの充足性確認を目的として行い、PJMO は構築された情報システムが要件定義書に記載した事項を適切に実現しているか、本システムを用いて実際のサービス・業務を正しく実施できるかといった観点でテストを実施する。受入テストに用いるテストデータには、本サービスが原則として公

開情報を取扱うことを踏まえ、可能な限り本番環境に近い複製データを使用する。ただし、受入テストの目的を担保可能であることを条件に、疑似データを使用することも可能とする。

受注者は調達仕様書にある通り以下の支援を行うこと。

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

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

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

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

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

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

3.14. 移行に関する事項

本システムは新規システムであり、データ移行作業はない。ただし、新たに業務を開始するための作業としての移行計画、コンティンジェンシープラン、稼働判定基準等を作成すること。

また、チェックリスト等の所定フォーマットは必ず取込み、出力可能な状態であること。

3.15. 引継ぎに関する事項

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

(1) 引継ぎ計画書の作成

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

(2) 引継ぎ方法

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

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

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

エ　引継ぎ期間中における本システムの次期運用・保守事業者からの問合わせにも対応すること。

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

(3) クラウドサービスを利用する場合の引継ぎ

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

(4) 引継ぎ結果報告書の作成

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

3.16. 教育に関する事項

(1) 教育計画の策定

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

(2) 教育対象者

本システムの教育対象者を「表 31 教育対象者」に示す。詳細は本システムの開発時点で決定する。

表 22 教育対象者

項番	教育対象者	教育内容	教育対象者数
1	農林水産省 植物防疫課・動物衛生課 システム管理者	運用業務の全体概要、システム管理者の業務手順等	約 6 人
2	農林水産省 植物防疫課・動物衛生課	職員の業務に関する本システムの操作手順、画面遷移、UI 表示仕様、エラー発生時の対応等	約 100 人
3	植物防疫所／動物検疫所 出品監視担当者	職員の業務に関する本システムの操作手順、画面遷移、UI 表示仕様、エラー発生時の対応等	約 6 人
4	システム運用担当者（事業者含む）	運用・保守業務の全体概要、運用・保守事業者の業務手順等 運用・保守要員の業務内容等	約 5 人

(3) 教育の実施時期

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

(4) 教育の方法

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

ア　講義における講師は、受注者が実施すること。

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

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

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

オ　講義開催日数は、2 回を想定している。講義開催時間は、概ね 2 時間とすること。

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

キ　講義終了後、15 分程度の質疑応答の時間を設けること。

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

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

(5) 教材の作成

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

(6) 教育訓練実施結果報告

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

3.17. 運用に関する事項

現時点で想定する運用要件を以下に示す。

(1) 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、「表 32 運用・保守計画書の記載内容」「表 33 運用・保守実施要領の記載内容」の要件が含まれる形で運用・保守計画書及び運用・保守実施要領の確定版を作成すること。

表 23 運用・保守計画書の記載内容

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

表 24　運用・保守実施要領の記載内容

項番	項目	補足
1	コミュニケーション管理	・　運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体　名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時　の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	・　運用・保守に携わる事業者における作業体制の管理手法等について記載する。
3	作業管理	・　運用・保守作業及びその品質の管理手法等について記載する。
4	リスク管理	・　運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	・　運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	・　運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーション、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	・　運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	・　平常時のセキュリティ運用として、継続的な脆弱性管理、構成管理及び変更管理を行い、不正アクセス等のセキュリティ脅威に対する監視運用を行うための具体的な方法を記載すること。 また、セキュリティインシデント発生に備えた体制や手順、発生時の被害極小化、速やかなサービス復旧を行うための具体的な方法を記載すること。

(2) 運用・保守準備

運用・保守に当たって、以下の準備作業の実施等を行うこと。

ア　監視設定

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

イ　バックアップサービス

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

ウ　運用・保守手順書

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

(3) 共通的な要件

ア　運用・保守期間

稼働後、契約期間まで運用・保守を行うこと。

イ　運用・保守報告書の作成

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

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

エ　以下の各管理については、クラウドサービスで可能な限り実現することとし、自動化を図ること。
運用管理、死活監視、稼働状況監視、セキュリティ監視、ジョブ管理、バックアップ管理、ログ管理（送受信ログ等の保存）、ウィルスパターン更新管理、セキュリティパッチ更新管理、依頼作業対応、構成管理、文書管理、アカウント管理、データ管理、障害対応、定例報告

(4) システム稼働要件
本システムの本番稼働に係る要件は「1.3 業務実施の時期・時間」を参照すること

(5) 主な運用作業一覧
現時点で想定する主な運用作業の一覧について、「表 34 主な運用作業一覧」に示す。以下の内容を基に、本システムの設計及び開発時に、運用・保守計画書、運用・保守設計書及び運用・保守マニュアルの案を作成すること。

表 25 主な運用作業一覧

項番	運用作業の分類	主な運用作業の内容
1	パッチ適用	・ 保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼働確認を行う。
2	ログ管理業務	・ 操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログを取得すること。 ・ ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ・ 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。 ・ ログの正確性を担保するため、適切なアクセス制御を行い、ログの改ざんを防止すること。
3	ジョブ管理業務	・ ジョブの登録・更新、ジョブの起動スケジュール（カレンダー）を登録し、ジョブの実施結果を確認、報告する。 ・ PJMO が必要性を認めた際は、PJMO の指示に従い、ジョブの手動実行を行う。
4	システム監視	・ 本システムの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性等で分類した上で、メールなどにより自動で通知する仕組みを構築すること。 監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）等 なお、セキュリティ監視に当たっては、取得ログやセキュリティ製品のアラート等を用いて、不正アクセスやマルウェア感染等のセキュリティ脅威により引き起こされる異常な状態の監視等を行い、セキュリティインシデントやその兆候を早期に検知すること。 ・ 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、PJMO の承認を得た上でこれに係る設計を行い、対応を実施すること。※システムサイジングについても定期的に分析を行い、PJMO の承認を得た上で見直すこと。
5	問題管理	・ 本システムに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。
6	変更管理	・ 課題管理機能の活用を前提として、適切な変更管理を実施すること。 ・ 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。 ・ 機密情報の不要な公開等の意図しないセキュリティインシデントを防止するため、本システムの設定変更等に当たっては、情報セキュリティ関連の設定に影響しないことを確認すること。
7	リリース管理	・ PJMO とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。

項番	運用作業の分類	主な運用作業の内容
		・ リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。 ・ 「リリース管理台帳」には以下の項目を管理し、履歴を確認することとし、その管理が必要な項目についても管理する仕組みとすること。 ➢ 実施計画の内容 ➢ リリーステストの実施有無及び結果 ➢ リリース時期 ➢ 各種レビューの実施有無及び結果 ➢ リリース内容 ・ リリース計画書については、リリース予定日より十分な期間を確保の上、前もって PJMO の承認をもって提出すること。なお、緊急なリリースを要する場合は PJMO と協議すること。
8	システム構成管理	・ 本システムに係る全ての構成品目について、適切な構成管理を実施すること。 ・ システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本システムを構成するクラウドサービス、ソフトウェア（製品名、開発元、バージョン、ライセンス、依存関係等）、アプリケーション、通信回線、公開ドメインのほか、本システムの運用・保守に係る全てのドキュメント及びデータとすること。ただし、本システムの外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。 ・ システム構成管理対象の変更について、変更履歴を追跡可能であること。 ・ 本番環境・検証環境の維持管理を行うこと。 ・ 本システムのアプリケーションは CI ツールで管理すること。
9	バックアップ	・ システムバックアップ、データバックアップを取得すること。 ・ 必要に応じてシステムリストア、データリストアを実施すること。
10	業務支援	・ PJMO の指示に基づき、利用者の利用状況のデータを集計し、PJMO に定期的に報告すること。 ・ 必要に応じて、データベースやディレクトリ等に施されるアクセス制御の設定変更を実施すること。 ・ 運用に必要な端末は受注者が用意すること。 ・ ヘルプデスク担当者からの問合せ、またはサービスデスクからの問合せに対する FAQ を作成すること。
11	障害対応	・ 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因アプリケーションの再設計・製造・試験、再発防止・品質向上作業、報告書作成・報告実施、環境（本番環境・検証環境等）反映）を行うこと。 ・ 本システムの連携先システムにおいて障害が発生し、業務影響が発生した場合においても、連携先システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。 ・ システム障害と想定される連絡を受け付けた際、別途、PJMO より指示する担当者へ速やかにエスカレーションすること。 ・ 府省内担当者との応答内容の記録を残すこと。
12	ヘルプデスク業務	・ 本システムの利用方法に関する問合せの受付からクローズまでを一元管理するヘルプデスクを設け、本システム利用者からの問合せを受け付けること。 ・ 問い合わせの要件は以下に示す。 ➢ 受付時間・方法：「1.3 業務実施の時期・時間」に記載 ・ ヘルプデスク担当者のスケジューリング等の運営を適切に行うこと。 ・ ヘルプデスク担当者による対応手順、サービスレベル等を統一するため、ヘルプデスク運用マニュアルを作成し、PJMO の承認を得ること。 ・ ヘルプデスク運営の中で FAQ は適宜追加、更新等、メンテナンスを行うこと。 ・ 受け付けた問合せは、質問、インシデント、サービス要求、作業依頼等に分類した上で、対応日時、問合せ元、内容、回答状況等とともに記録すること。なお、具体的な運用方法については、本システムの設計開始以降に改めて検討する。 ・ 問い合わせ記録は受付件数、問い合わせ者情報、問い合わせ内容、回答率、回答に要した期間、回答内容等を適切な粒度で整理した上で、定期的に問題発生状況を分析すること。分析結果を踏まえ、回答時間の短縮や回答内容の分かりやすさ向上等、必要な対策を検討し、PJMO と協議の上、実施すること。 ・ 問い合わせで把握した問題については、運用改善を実施する際の参考情報となるよう整理すること。 ・ 運用・保守の計画及び実施状況について、PJMO の定める報告様式に従って取りまとめ、

項番	運用作業の分類	主な運用作業の内容
		PJMO に報告を行うこと。（原則、月次での報告）
13	設計・開発事業者による報告・問合せ対応	・ 問合せに関する調査完了後、ヘルプデスクへの回答を行うこと。 ・ その他、適宜、PJMO と必要に応じて密に連携を図り、ヘルプデスクの円滑な運営に資すること。
14	インシデント管理	・ 情報セキュリティインシデントが発生した場合は、「運用・保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、PJMO、関係事業者と適宜調整の上で対応を行うこと。 ・ インシデント対応手順の実効性を担保するため、定期的にインシデント対応手順の見直しやインシデント対応訓練を実施すること。
15	バージョンアップ対応	・ 保守におけるバージョンアップ対応要否の判断結果に基づき、バージョンアップ対応を実施し、稼働後の動作確認を行うこと。
16	大規模災害等対応訓練	・ 大規模災害等への対応訓練を行うこと。 ➢ 大規模災害対応訓練シナリオ見直し 本番運用・保守の計画で定義されている訓練シナリオ・手順書を適宜見直し、必要に応じて、設計・開発事業者に確認を依頼すること。訓練シナリオ・手順書を変更した場合は、PJMO の承認を得ること。 ➢ 大規模災害対応訓練の実施 受注者は、大規模災害発生時から復旧に係る作業について、PJMO 及び関係する事業者が迅速かつ適切に作業を実施できるよう、年に 1 回、訓練シナリオ・手順書に基づき、訓練を実施すること。実施に当たっては、主に連絡ルートの確認を実施し、結果を「大規模災害等対応訓練完了報告書（本番運用開始後）」に記載し、PJMO に報告すること。なお、訓練への参加は、受注者と PJMO のみとし、他事業者や外部連携システムは対象外とする。
17	運用改善	・ 受注者は、本システムの状況を PJMO が定期的に把握できるように仕組みを整えること。 ➢ プロジェクトの目標とする指標、本システムの利用者の利用状況 ➢ クラウドのリソース等、本システムの利用状況・コストの発生状況 ・ 本システムの利用状況については、少なくとも以下の項目および「2.4.（5） モニタリング対象データ一覧」に記載した項目を実施し、利用状況の分析とその後の改善策に資する項目を含めること。 ➢ 運用管理・保守業務の作業別の所要時間 ➢ 自動化や効率化が可能と思われる作業の洗い出し ➢ 本システム及び運用・保守業務の改善提案 ・ アイドリングなどの無駄／過剰なリソースを発見し、コスト削減につながる仕組みを整え、アドバイスも指摘すること。 ・ 受注者は、本システムの利用拡大や利便性向上のため、実績に基づいた定量的なデータや利用者からの問合せ内容等を分析し、多くの利用者が操作方法に迷う部分や誤操作を誘発する部分を把握した上で本システムの改善策を検討すること。また PJMO と協議の上、本システムの改善を実施すること。
18	サービスオペレーション支援	・ 本システムが動作するに当たり、必要となるデータベースの各種マスタ情報を維持管理すること。また、マスタ情報管理のための GUI を具備しないマスタ情報の場合、変更依頼を前提として情報の登録、検索、更新、削除のための SQL を作成し、これを実行すること。 ・ 計画停止、保守作業、障害対応等により利用者への影響が生じる場合、本システムの Web サイトにお知らせを掲載するなどの方法により周知連絡を行うこと。 ・ 作業影響を生じる範囲について、不測の運用障害を回避する観点から、メンテナンス機能を利用してサービス閉塞・閉塞解除運用を実施すること。
19	情報セキュリティ監査	・ PJMO が情報セキュリティ監査を実施する場合がある。その際はセキュリティ監査事業者との調整・ヒアリングへの協力を行うこと。
20	アカウント管理	・ 受注者は、PJMO からの指示に基づき、ユーザ ID（特権 ID 含む）の払い出し、削除、パスワード再発行を実施すること。 ・ アカウントの利用状況の棚卸を実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については PJMO と協議の上、決定すること。
21	その他業務	・ サーバ証明書の更新、ドメインの管理等を行うこと。

3.18. **保守に関する事項**

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

(1) 保守業務の実施

保守業務として以下を実施すること。

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

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

ウ　障害について対応したときは、障害報告書を作成し、PJMO に報告すること。

(2) 保守設計

保守設計として以下を実施すること。

ア　役割分担の整理

役割分担を行う際に以下の点に留意すること。

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

イ　クラウドサービスの利用

クラウドサービスを利用する際に以下の点に留意すること。

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

(3) アプリケーションの保守

アプリケーションの保守として以下を実施すること。

ア　インシデント管理

運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

イ　是正保守

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

ウ　適応保守

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

エ　予防保守

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

オ　改善措置

上記イ～エに伴う改善措置を実施する際には以下の点に留意すること。

- 国民等の利用者に影響がある保守作業を実施する場合は、アプリケーション保守の実施効果、現在及び将来の利用者に対する影響の分析を行うこと。
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性等の改善が必要な場合に、対処を行うこと。
- Web 解析結果に基づき、本サービスのユーザインタフェースについて、ユーザビリティ又は UX に関する課題を識別した場合、課題解決に資する是正保守、予防保守を行うこと。
- Web サーバ、データベース等について、「表 34　主な運用作業一覧 項 17 運用改善」の結果を踏まえ、必要に応じて稼働環境の改善等に伴う設定変更を実施すること。

カ　根本原因の分析

根本原因を分析する際に以下の点に留意すること。

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

キ　検証

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

ク　ドキュメントの修正

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

(4) クラウドサービスの保守

クラウドサービスの保守として以下を実施すること。

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

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

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

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

(5) ソフトウェア保守

ソフトウェアの保守として以下を実施すること。

ア　ソフトウェア最新化

本システムを構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、PJMO と協議の上、ソフトウェアを最新化すること。なお、ソフトウェアの最新化に当たっては、本システムのシステム構成等に考慮すること。

イ　修正プログラムの適用

修正プログラム適用の際は以下の点に留意すること。

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

ウ　検証・デプロイ

検証・デプロイを行う際は以下の点に留意すること。

- ソフトウェア保守に当たっては、事前に検証環境で本システムの運用に影響が生じないことを十分に検証すること。
- ソフトウェア保守に伴い、本システムの安定稼働に影響が生じる事態が予測される場合、PJMO の指示に基づいてデプロイ実施の是非を判断すること。

エ　設計書への反映

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

オ　保守条件の決定

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

カ　脆弱性管理

ソフトウェアに関する脆弱性に対処するために、以下の対応を行うこと。

- 脆弱性管理基準の作成と運用

  脆弱性管理の方針を定めた脆弱性管理基準を、保守設計において PJMO と調整の上で作成し、運用すること。

  脆弱性管理基準には、以下の項目を含めること。

  - 個別対応の要否判断の基準

    情報システムの「脅威」、「脆弱性」、「重要度」からの観点からのリスクの評価基準と対応優先度、個別対応または定期保守でのどちらで対応するかの方針、目標とする脆弱性対処の対応期限を取り決めたもの。
  - 定期アップデート規則

    ソフトウェアの定期アップデートを実施する頻度、実施条件、回帰テストの範囲を取り決めたもの。
  - ソフトウェア採用判断の基準

提供元の信頼性やサポート条件、脆弱性の情報開示やパッチ提供など、脆弱性対応を円滑に行うための基準を取り決めたもの。

- 脆弱性管理の対象と管理方式
  クラウドの責任共有モデルを含む情報システムの脆弱性管理の対象と、ソフトウェア構成や脆弱性を管理するツールやサービスなどの管理方式を取り決めたもの。

・ 脆弱性管理手順の作成と運用
脆弱性に対処する手順を定めた脆弱性管理手順を、保守設計において PJMO と調整の上で作成し、運用すること。
脆弱性管理手順には以下の項目を含めること。

- ソフトウェア構成の管理
  情報システムで使用するソフトウェアの製品名、開発元、バージョン、ライセンス、依存関係などを容易に参照できるよう構成管理及び変更管理を行うこと。
- 脅威情報の収集、自システムへの影響分析
  日々出現するセキュリティ脅威や脆弱性に対処するため、定常的に脅威情報や脆弱性情報を収集し、情報システムへの影響含めてリスク分析を行うこと。
- リスクに応じた脆弱性対応及び定期アップデート
  情報セキュリティや安定稼働の観点からリスク評価を行い、即時もしくは優先的な対応が望ましいと判断される脆弱性については、緊急対応を計画すること。即時対応が不要もしくは対応の必要性が低い脆弱性については、定期保守作業の中での対応を計画すること。

(6) 保守実績の評価及び改善
保守実績の評価及び改善として以下を実施すること。

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

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

ウ ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。

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

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

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

(8) 軽微な改修
運用・保守の期間中に必要となる軽微な改修として以下を実施すること。

ア　運用・保守の期間中に、利用者からの要望対応、不具合の改善、環境変化への対応等の目的で軽微な改修を行うことを想定している。改修への対応工数（必要に応じて教育訓練等を含む）として、合計 1 人月の作業を見込むこと。

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

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

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

業務一覧

- 国内ECサイト等を対象とした流通監視システム導入後の業務の一覧（想定）を整理します。 この業務一覧に基づき、各段階における業務内容を次頁以降フローの形で整理しております。

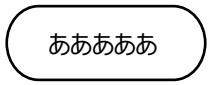
段階	業務内容
監視	対象となるECサイトやフリマサイト等を継続的に確認し、違法性が疑われる商品の出品状況を把握する。
発見・評価	把握した出品情報について、商品内容や説明、画像、原産地情報等を確認し、規制対象に該当する可能性を一次判定する。 違法性が疑われる場合には、詳細情報やソースを確認するとともに、類似事例や過去対応と照合しながら、違法性の程度やリスクを評価する。
判断	違法性の疑いが高い案件について、出品者情報や過去の対応履歴等を確認し、対応の要否および対応方針を決定する。 経過観察とするか、関係機関と連携するか、出品者等への対応を行うか等を判断し、優先度や対応区分を整理する。
実行	決定した対応方針に基づき、出品者や関係事業者への照会、注意喚起、必要に応じた立入検査や回収等の対応を実施する。 また、対応内容や結果を記録・報告し、関係機関との情報共有を行うとともに、今後の監視や判断に活用する。
マスタ管理	監視対象のサイト、対象品目、検索条件、巡回頻度等を定期的に見直し、監視方針を調整するとともに、過去の違法性の高い商品に対する対応結果も踏まえて重点的に監視すべき領域を把握する。
共通	システムとして共通の処理を実施する。

システム化業務フロー一覧

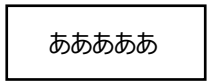
業務	項目名	フロー名	アクション
監視	違法性商品等の監視	A	システムの常時監視（クローリングやスクレイピングによる情報収集とAIデータ分析）
		B	人による定期監視による状況確認
発見・評価	出品情報の違法性判断	C	商品情報と出品者情報を用いた詳細調査及び人による違法性判断
判断	違法性の高い出品を行う出品者への対応判断	D	違法性の高い出品を行う出品者への対応判断
実行	国民への対応の実施	E	国民への対応（聞き取り/立会検査/注意喚起・警告書発出/違反品の収去等）の実施及び対応実施記録
マスタ管理	監視条件変更の判断	F	監視条件の確認及び変更判断
	監視条件変更	G	システムの監視条件の設定確認・変更
共通	ログイン	H	通常ログイン時
	ログアウト	I	通常ログアウト時

システム化業務フロー

凡例定義



アクターによる業務プロセスの開始を示します。
（例：「ログイン」なら、「ログインという業務を開始する」意味を示します。）



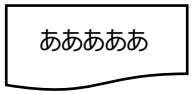
アクターの、システムとの関連動作を示します。
（例：「ID/パスワード入力」なら、「ID/パスワードをシステムに入力する」というアクターの動きを示します。）



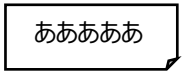
フローの分岐を示します。

アクターの業務フローの流れを示します。

システムと関連するフロー（入出力操作、データの流れ、システム処理の流れ）を示します。



システムに入出力されるファイル形式のデータ（画像、帳票等）を示します。



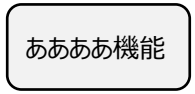
紙媒体（帳票等）を示します。



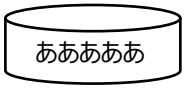
システムから利用者への通知（メール等）を示します。



入出力のシステム画面を示します。



システムの機能を示します。



システムのデータ格納領域（テーブル等）を示します。



フローの差し戻しや、別のフローへの遷移を示します。
※NNNは業務番号（N）＋連番（NN）で表現
　業務番号・・・1:監視、2:発見・評価、3:判断、4:実行、
　　5:マスタ管理、0:共通



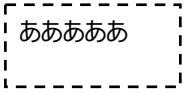
フローの開始を示します。



フローの終了を示します。



フローの次頁への継続/前頁からの継続を示します。



備考欄を示します。図示では表現できないシステムの挙動、留意点等を記載します。

システム化業務フロー

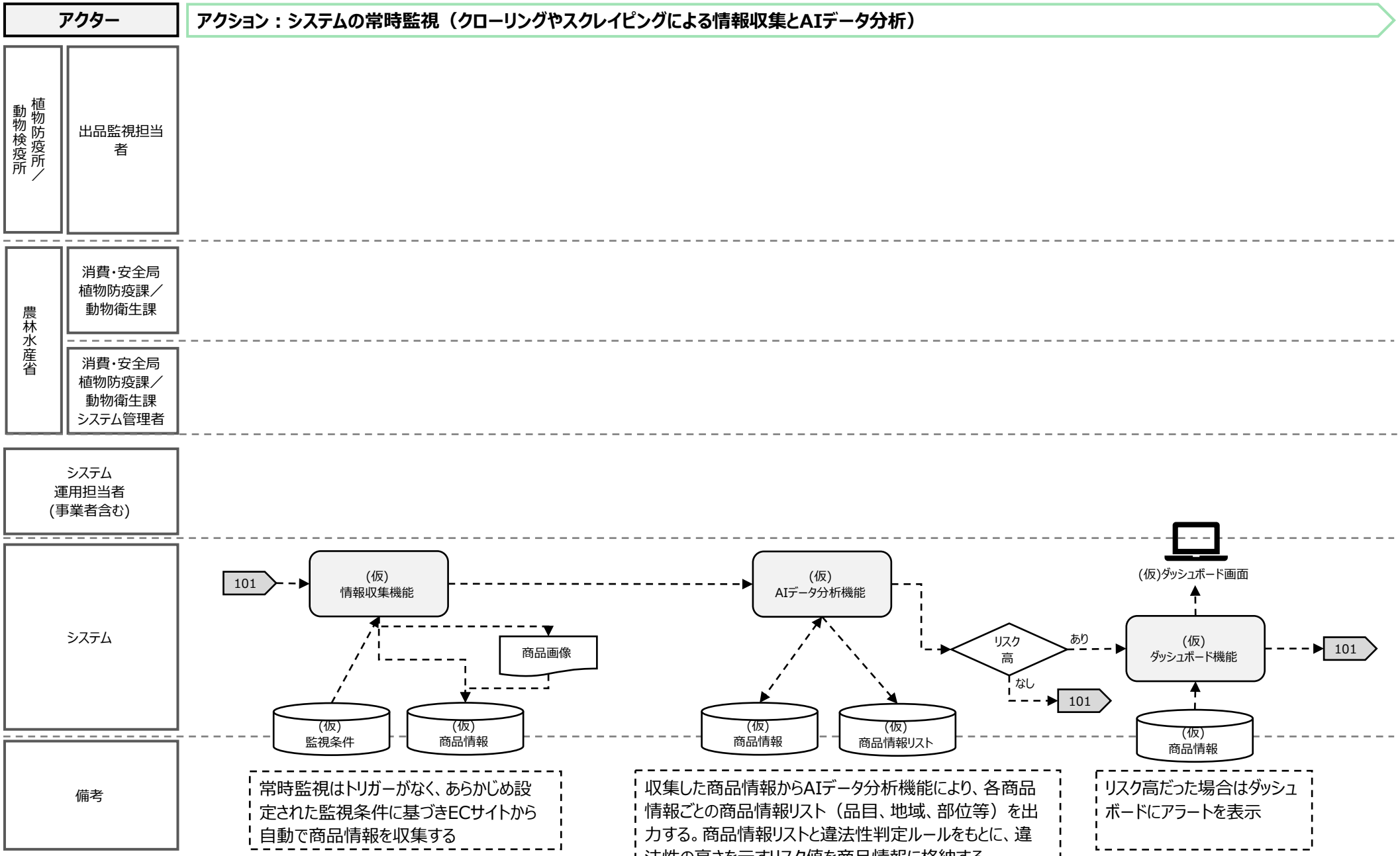
アクター定義

- 本資料におけるアクター定義は、要件定義書「１．業務要件定義」内、「（３）業務の実施に必要な体制」を参照すること。

システム化業務フロー　監視業務

違法性商品等の監視

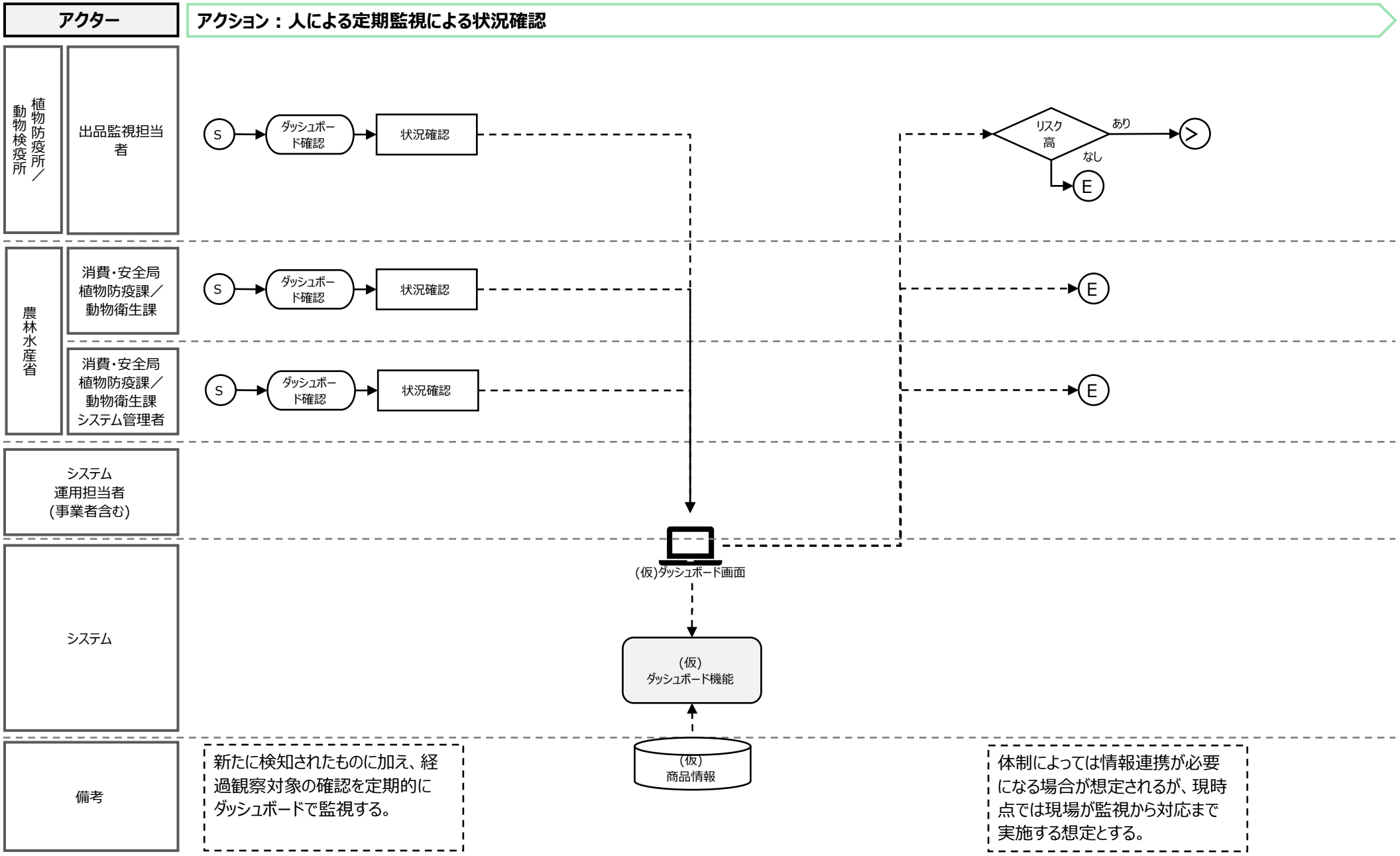
フロー名：A



システム化業務フロー　監視業務

違法性商品等の監視

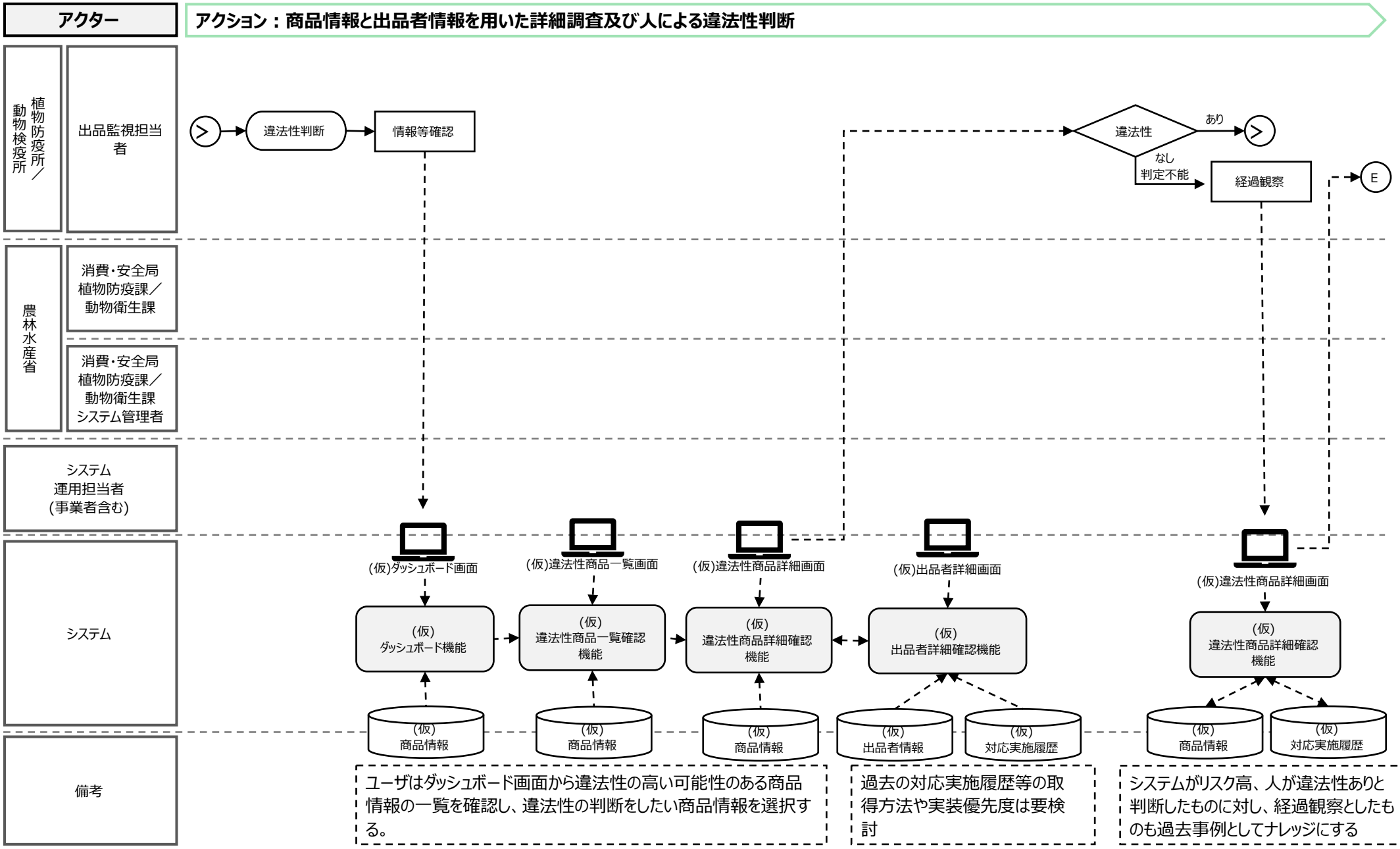
フロー名：B



システム化業務フロー　発見・評価業務

出品情報の違法性判断

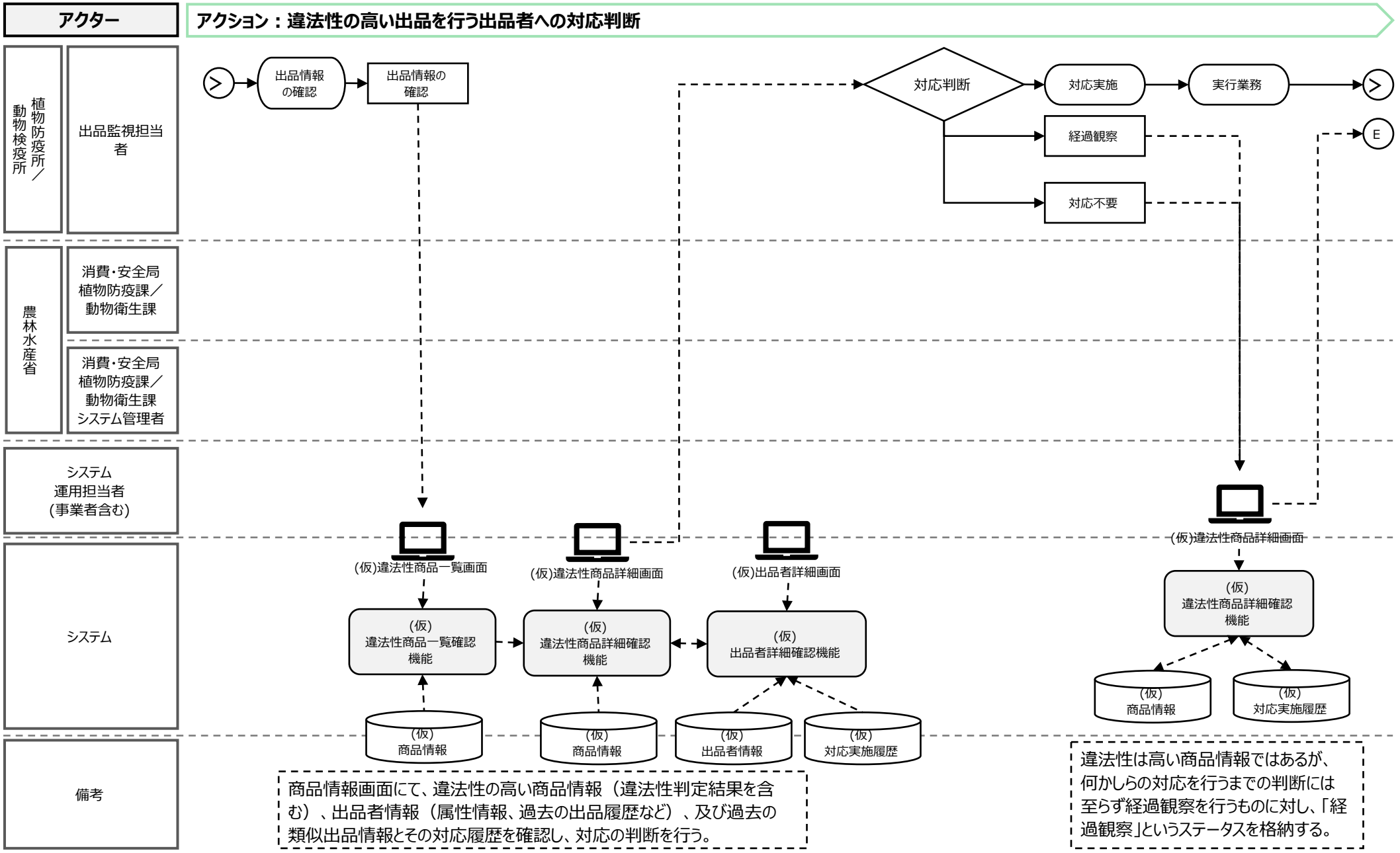
フロー名：C



システム化業務フロー　判断業務

違法性の高い出品を行う出品者への対応判断

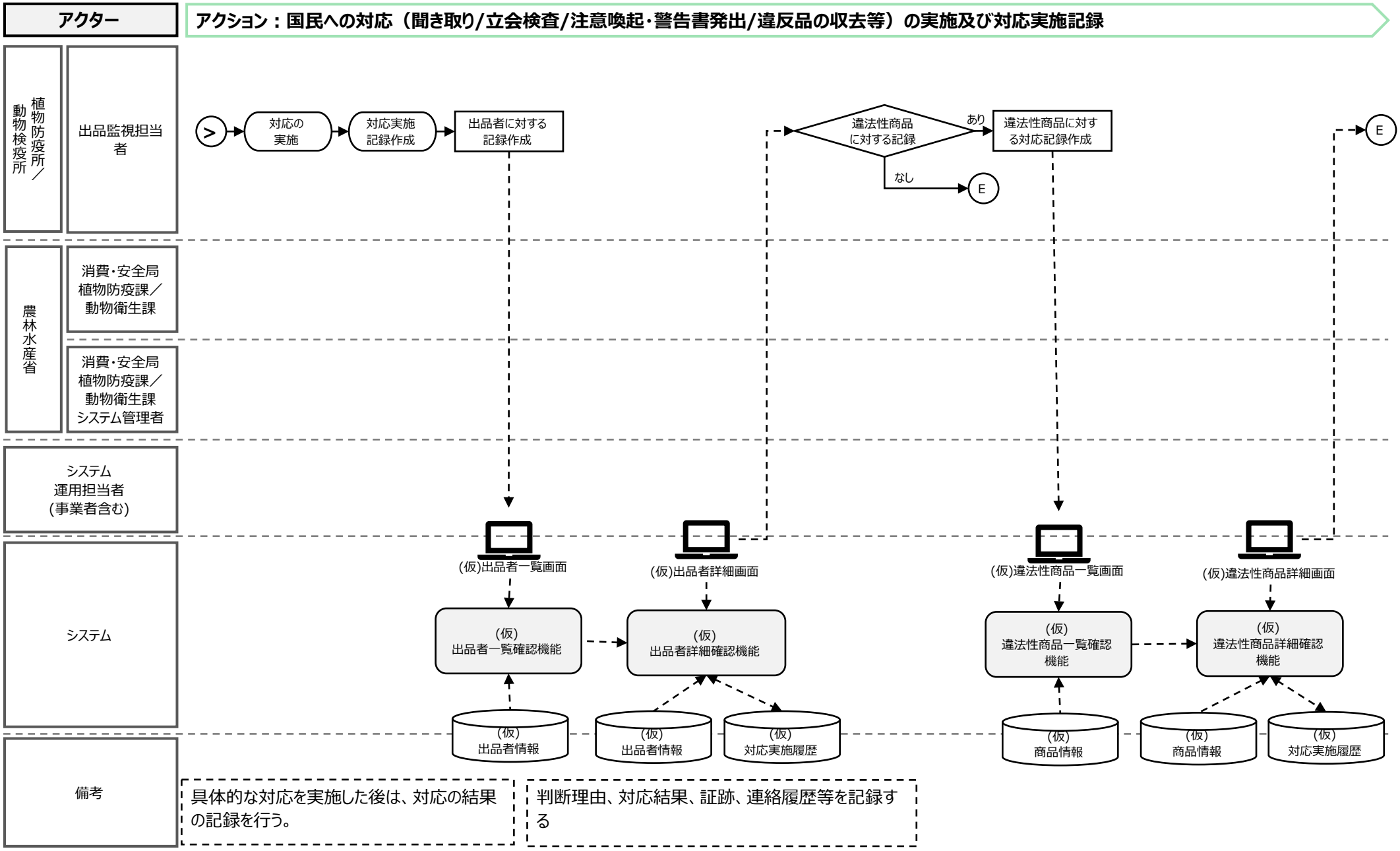
フロー名：D



システム化業務フロー　実行業務

国民への対応の実施

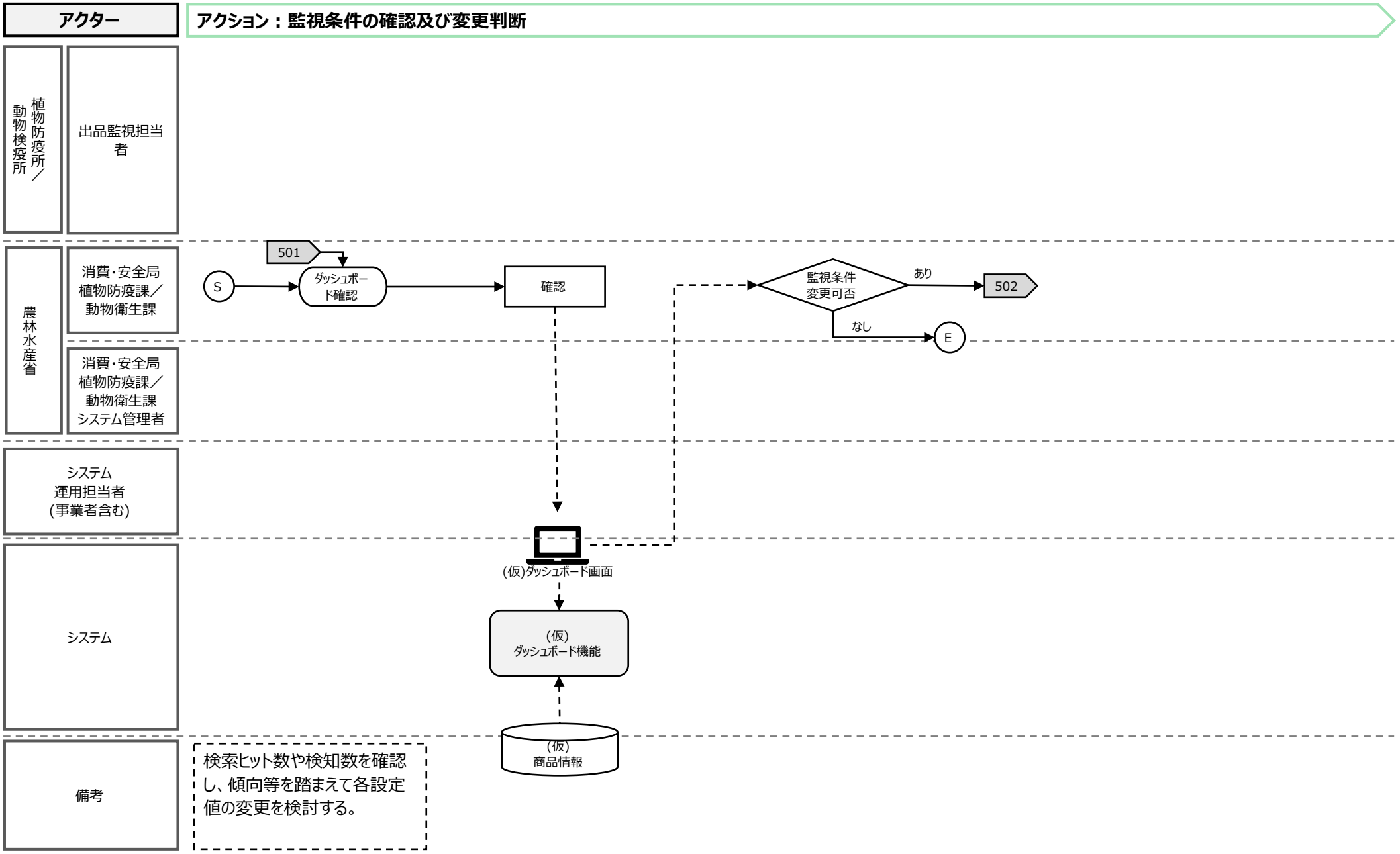
フロー名：E



システム化業務フロー　マスタ管理業務

監視条件変更の判断

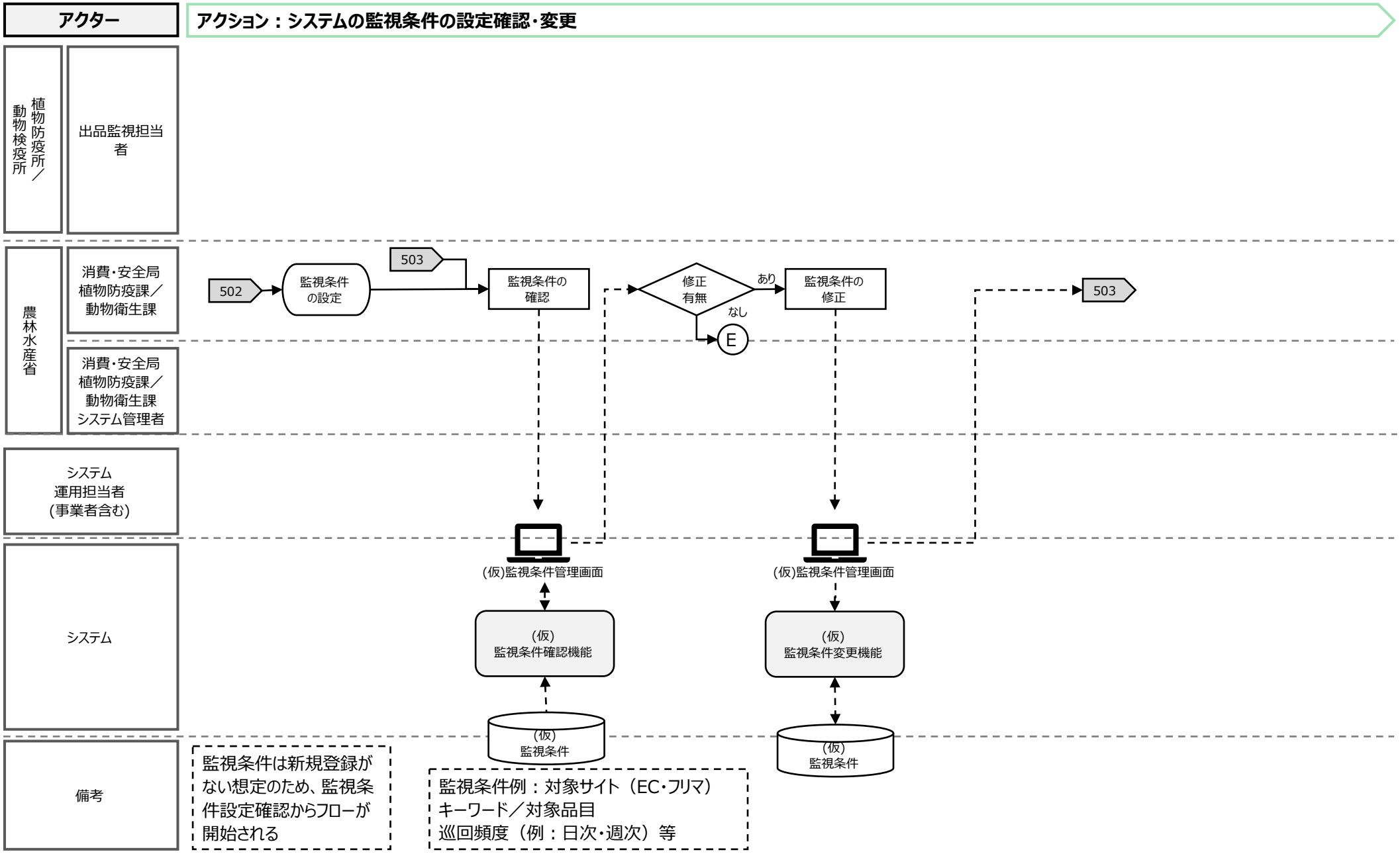
フロー名：F



システム化業務フロー　マスタ管理業務

監視条件変更

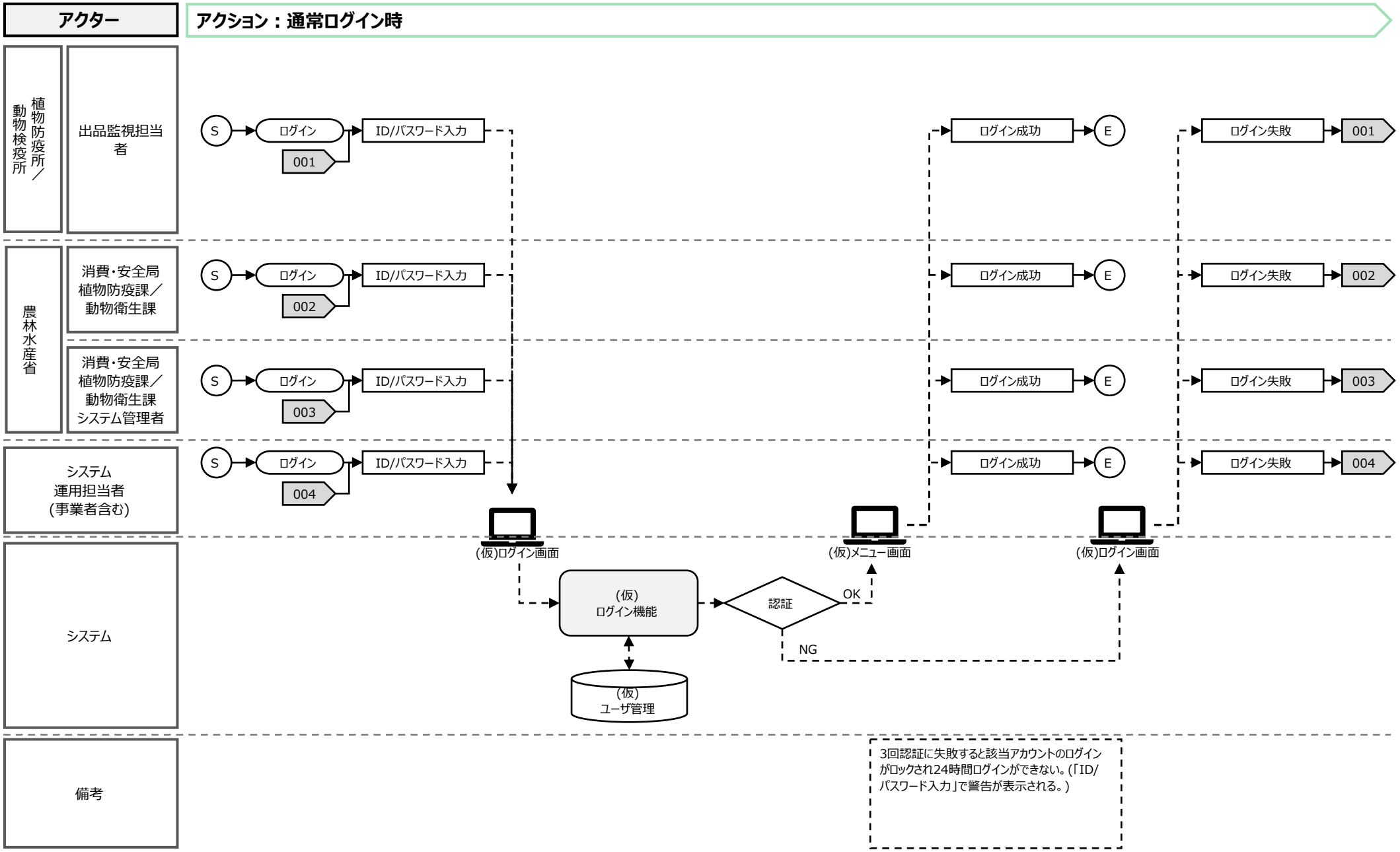
フロー名：G



システム化業務フロー　共通業務

ログイン

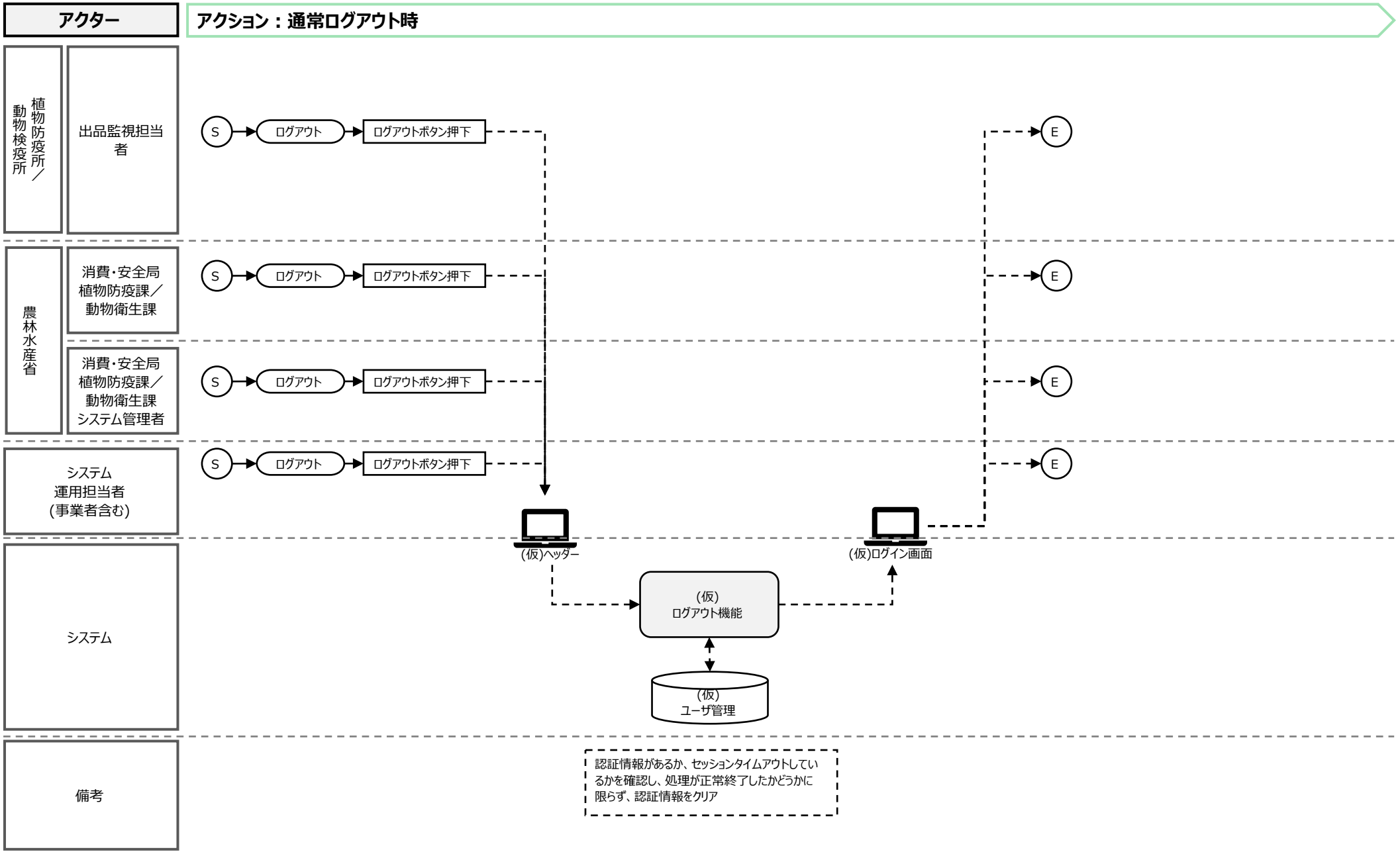
フロー名：H



システム化業務フロー　共通業務

ログアウト

フロー名：I



別添資料2-1. システム機能一覧

項番	機能ID	機能分類	機能名	機能概要			処理方式	利用者区分	現状の機能との差異	該当業務	補足	R9年度要件
				入力	処理	出力						
1	F-1-1	ダッシュボード	ダッシュボード機能	【DB】商品情報 【DB】判定結果 【DB】確認結果	新規検知および経過観察対応の情報を元にダッシュボードを作成し、表示する。	【画面】ダッシュボードの情報	アプリケーション	全ユーザ	新規	1-2定期監視		○
2	F-2-1	出品情報の閲覧	違法性商品一覧確認機能	【DB】商品情報 【DB】判定結果 【DB】確認結果	高リスクと判定された商品情報の一覧を表示する。 絞り込み条件を指定することで一覧の表示条件およびソート順を変更することを可能とする。 結果が１ページ内に収まらない場合はページ分割し、ページ送りを可能とすること。	【画面】商品情報の一覧	アプリケーション	植物防疫所・動物検疫所の出品監視担当者	新規	2-1違法性判断		○
3	F-2-2	出品情報の閲覧	違法性商品詳細確認機能	【DB】商品情報 【DB】判定結果 【DB】確認結果 【DB】出品者情報	対象商品の詳細情報、画像を表示する。 商品情報の対応状況（ステータス）を変更することを可能とする。 ユーザによる対象商品に対するコメントやフィードバック入力を可能とし、入力履歴を表示する。	【画面】商品情報の詳細 【DB】出品者情報 【DB】判定結果 【DB】確認結果	アプリケーション	植物防疫所・動物検疫所の出品監視担当者	新規	2-1違法性判断	出品者間、サイト間で同じと思われる商品の突合はシステムでは実施しない。（別商品として扱う）	○
4	F-2-3	出品情報の閲覧	出品者一覧確認機能	【DB】出品者情報 【DB】商品情報 【DB】判定結果 【DB】確認結果	出品者の一覧情報を表示する。 該当商品を出品している出品者の一覧を確認することができる。	【画面】出品者情報の一覧 【画面】商品の情報 【画面】対応状況	アプリケーション	植物防疫所・動物検疫所の出品監視担当者	新規	3-1対応判断	サイト間で同じと思われる出品者の突合はシステムでは実施しない。（別出品者として扱う）	○
5	F-2-4	出品情報の閲覧	出品者詳細確認機能	【DB】出品者情報 【DB】商品情報 【DB】判定結果 【DB】確認結果 【DB】対応実施履歴	出品者の詳細情報を表示する。 対象出品者が出品する商品を確認することができ、また、対応実施結果を対応実施記録として登録、履歴確認できる。	【画面】出品者情報の情報 【画面】商品の情報 【画面】対応状況	アプリケーション	植物防疫所・動物検疫所の出品監視担当者	新規	3-1対応判断	サイト間で同じと思われる出品者の突合はシステムでは実施しない。（別出品者として扱う）	○
6	F-3-1	システム管理	監視条件確認機能	【DB】監視条件	監視条件を取得し、表示する。	【画面】監視条件の情報	アプリケーション	農林水産省の全ユーザ システム運用担当者	新規	5-1監視条件設定		○
7	F-3-2	システム管理	監視条件変更機能	【DB】監視条件	監視条件を変更する。	【画面】監視条件の情報 【DB】監視条件	アプリケーション	農林水産省の全ユーザ	新規	5-1監視条件設定		○
8	F-3-3	システム管理	違法性判定ルール確認機能	【DB】違法性判定ルール	違法性判定ルール内で植物の違法性判定に使用する特定条件である、「植物」×「地域」×「部位」を表示する。	【画面】違法性判定ルールの情報	アプリケーション	農林水産省の全ユーザ システム運用担当者	新規	5-1監視条件設定		○
9	F-3-4	システム管理	違法性判定ルール変更機能	【ファイル】違法性判定ルール	植物の判定で使用するルール「植物」×「地域」×「部位」の組み合わせを更新する。 組み合わせは膨大となるため、CSV形式等での一括更新を可能とする。	【DB】違法性判定ルール	アプリケーション	農林水産省の全ユーザ	新規	5-1監視条件設定		○
10	F-4-1	ログイン	ログイン機能	【クラウドログインサービス】 ・ユーザID ・パスワード ・MFA	クラウドログインサービスを利用して、認証し、ユーザ情報および権限情報を取得する。 ユーザ情報は基本的にクラウドログインサービスのみに保持し、アプリケーション内にユーザ情報は保持しない。 (各情報に関連するユーザID等、最低限の情報のみアプリケーション内に保持している想定)	なし	クラウドログインサービス	全ユーザ	新規	なし	アプリケーションでの機能、画面の実装なしを想定する	○

別添資料2-1. システム機能一覧

項番	機能ID	機能分類	機能名	機能概要			処理方式	利用者区分	現状の機能との差異	該当業務	補足	R9年度要件
				入力	処理	出力						
11	F-4-2	メンテナンス	ユーザ管理機能	【クラウドログインサービス】 ・ユーザ情報 ・権限	クラウドログインサービス上でユーザ情報を管理する。 所属や役職等の情報はカスタム属性で定義する想定。 異動に係るメンテナンス業務(ユーザ登録、削除、所属・役職変更)はクラウドログインサービスで提供される画面、機能で実施する。	なし	クラウドログインサービス	システム運用担当者	新規	6-1職員の権限管理	アプリケーションでの機能、画面の実装なしを想定する	○
12	F-5-1	出品情報の検索・収集	情報収集機能	【DB】監視条件	予め設定された監視条件に基づき、インターネット上の情報収集対象サイトから定期的に自動で商品情報を収集する。 ・監視条件案 URL、監視頻度、スケジュール など ・情報収集対象サイト案 ECサイトおよびSNSサイトから 選定された複数サイト ・収集方式案 対象サイトの利用許諾に応じた 方式(公開API、検索スニペットAPI など)を使い分ける 対象サイトのポリシーに準拠する こと ・収集する商品情報案 テキストベースの商品情報と 商品画像、出品者情報	【ファイル】商品画像 【ファイル】商品情報	バッチ	システム	新規	1-1常時監視	監視条件はシステムリリース時に初期設定され、監視条件変更機能でメンテナンスされる	○
13	F-6-1	出品情報の違法性判定	AIデータ分析機能	【ファイル】商品画像 【ファイル】商品情報 【DB】違法性判定ルール	収集された商品データを入力として、AIにより高リスク(違法性の高い)商品を選別し、リスト化する。 そのリストに対して設定された違法性判定ルールを適用し、リスクを判定する。判定は商品情報からAIが抽出した項目（カテゴリ、地名、品名、部位など）を用いる。 判定結果を商品情報に格納する。 商品情報から出品者情報を抽出する。	【DB】判定結果 【DB】商品情報 【DB】出品者情報	バッチ	システム	新規	1-1常時監視	違法性判定ルールはシステムリリース時に初期設定され、違法性判定ルール変更機能でメンテナンスされる	○
14	F-7-1	データ削除	データ削除機能	【ファイル】商品画像 【ファイル】商品情報 【DB】商品情報 【DB】出品者情報 【DB】確認結果	システムにより自動収集された商品情報のうち、削除条件に合致したものを定期的に削除する。	なし	バッチ	システム	新規	6-3サーバメンテナンス等の運用業務		○

ダッシュボード

違法輸入動植物等流通監視ツールの概要と分析結果を確認できます。

▣ 2025年12月

今月の高リスク総数
137
⚠

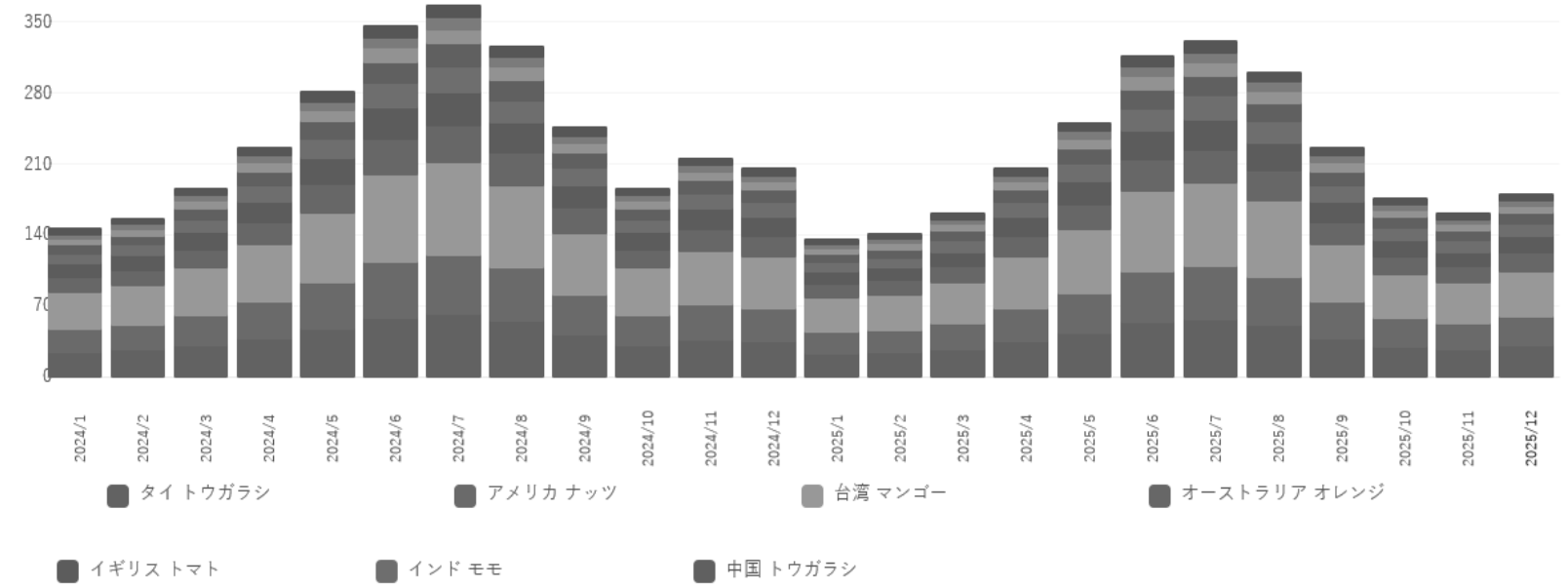
高リスク数先月比
+6.1%
↑ 増加
↗

高リスク増加の国×品目数
4
増加傾向の項目数
⊙

高リスク出品数変化

過去24ヶ月間の推移

積み上げ棒　折れ線　表示: 国×品目別 ∨



違法性商品一覧

検索結果の一覧を確認できます。ソート・フィルタ機能で絞り込みが可能です。

検索カテゴリ: すべて
検索サブカテゴリ: すべて
検索サイト: すべて
顕在違法性リスク: すべて
ステータス: すべて
作成日（From）: 年/月/日
作成日（To）: 年/月/日
違法性判定ラベル: 入力で候補表示
検索実行
フィルターリセット

検索結果

全694,849件中 1〜20件を表示（1/34,743ページ）

‹ 1 2 3 4 ... 34,743 ›

画像	カテゴリ ▽△	サブカテゴ リ ▽△	サイト ▽△	違法性判定ラベル ▽△	ステータス ▽△	作成日時 ▽△	操作
	植物	生果実	メルカリ	中	経過観察	2026/01/18	詳細
	植物	生果実	メルカリ	低	問題なし	2026/01/18	詳細
	植物	生果実	メルカリ	低	経過観察	2026/01/18	詳細
	植物	生果実	メルカリ	中	経過観察	2026/01/18	詳細
	植物	種子	YAHOO	低	判定不能	2026/01/18	詳細
	植物	幼苗	YAHOO	高	経過観察	2026/01/18	詳細

違法性商品詳細

検索結果の詳細情報を確認できます

登録　修正　戻る

この商品の出品者　：　株式会社　あああああ商事

違法性商品情報

商品画像





出品サイト名　：Yahoo!ショッピング

商品URL
https://store.shopping.yahoo.co.jp/sample/navel17kg

検索ワード　：“オーストラリア” “みかん”

検索カテゴリ　：植物

検索サブカテゴリ　：果実

違法性判定ラベル　：　中

取得日時
2026-07-16 00:15:00.000000

ステータス：　経過観察

ステータス変更事由/：

ステータス履歴

この商品の出品者に係るコメント

※各段階のコメントやメンションをすべて表示

出品者一覧

該当商品の出品者を一覧表示します。

該当商品名：　オーストラリア　アメリカ　ネーブルオレンジ　大きさおまかせ　∨

全23件中 1～6 件を表示（1/4ページ）

‹ 1 2 3 4 ›

出品者名	所在地	登録メールアドレス	サイト	出品日時 ↓	出品者詳細
株式会社　あああああ商事	花	ABCDE@yahoo.co.jp	メルカリ	2026/01/18	詳細画面
株式会社　いいいい	花	FGHIJK@yahoo.co.jp	メルカリ	2026/01/18	詳細画面
株式会社　ううううう	花	LMNOP@yahoo.co.jp	メルカリ	2026/01/18	詳細画面
（有）えええ	花	ABCDE@ocn.ne.jp	メルカリ	2026/01/18	詳細画面
おおおお　株式会社	種子	ABCDE@plala.or.jp	YAHOO	2026/01/18	詳細画面
かかか（株）	幼苗	ABCDE@gmail.com	YAHOO	2026/01/18	詳細画面

出品者詳細

該当商品の出品者に対しての記録を登録する画面です

登録　修正　戻る

出品者情報

出品者　：　株式会社　@@@@@@物産

該当商品名：　オーストラリア　アメリカ　ネーブルオレンジ　大きさおまかせ

記録タイトル

記録内容

記録履歴

2026/08/26 15:00 出品者問合実施

記録内容

※選択した記録内容を表示

監視条件管理

検索スケジュールの確認や検索頻度・カバレッジの確認ができます。

検索スケジュール

毎日 9:00実行

検索設定

検索頻度

毎日

本権限では設定変更できません。

検索カテゴリ

全カテゴリ

検索サブカテゴリ

全サブカテゴリ

検索キーワード

検索キーワードを入力してください…

検索キーワード移入　：　CSVファイルを添付

設定を保存　検索を実行

違法性判定ルール管理

監視条件における違法性判定基準を設定します

植物判定ルール

	植物	地域	部位
☐	野菜	アメリカ	果実
☐	生果実	インド	茎葉
☐	栽培用	ベトナム	根、地下部
☑	野菜	香港	植物
☑	栽培用植物	タイ	果実

削除　設定を保存

No.	データID	スキーマ /Schema	テーブルID /Table ID	テーブル名 /Table name	種別 /Type of table	保存期間 /Saving period	初期件数 /Initial count	増加件数 /Increasing count		最大想定件数 /Max record count	レコード長 /Record length	説明 /Description
								件数 /Count	単位 /Unit			
1	EN-001	SCM01	MONITORING_CONDITIONS	監視条件テーブル	トラン/Transaction	永久	0	-	-	-	-	検索方法や取得した情報全般を管理する
2	EN-002	SCM01	PRODUCT_INFORMATION	商品情報テーブル	トラン/Transaction	永久	0	-	-	-	-	取得した商品情報やその格納先を管理する
3	EN-003	SCM01	JUDGMENT_RESULT	判定結果テーブル	トラン/Transaction	永久	0	-	-	-	-	商品の違法性判定に使用するAIモデルや結果を管理する
4	EN-004	SCM01	VERIFICATION_RESULT	確認結果テーブル	トラン/Transaction	永久	0	-	-	-	-	防疫官が確認した結果を管理する
5	EN-005	SCM01	SELLER_INFORMATION	出品者情報テーブル	トラン/Transaction	永久	0	-	-	-	-	商品の出店者情報を管理する
6	EN-006	SCM01	IMPLEMENTATION_HISTORY	対応実施履歴テーブル	トラン/Transaction	永久	0	-	-	-	-	出品者への対応履歴を管理する
7	EN-007	SCM01	SITE_MASTER	サイトマスタ	マスタ/Master	永久	10	-	-	-	-	検索対象サイトのマスタデータを管理する
8	EN-008	SCM01	SEARCH_TYPE_MASTER	検索種別マスタ	マスタ/Master	永久	3	-	-	-	-	検索種別のマスタデータを管理する
9	EN-009	SCM01	SEARCH_CATEGORY_MASTER	検索カテゴリマスタ	マスタ/Master	永久	4	-	-	-	-	検索カテゴリのマスタデータを管理する
10	EN-010	SCM01	SEARCH_SUB_CATEGORY_MASTER	検索サブカテゴリマスタ	マスタ/Master	永久	3	-	-	-	-	検索サブカテゴリのマスタデータを管理する
11	EN-011	SCM01	SEARCH_TARGET_MASTER	調査対象マスタ	マスタ/Master	永久	-	-	-	-	-	調査対象JSON格納先のマスタデータを管理する。レコード数は未定。

No.	データID	スキーマ /Schema	テーブルID /Table ID	テーブル名 /Table name	種別 /Type of table	保存期間 /Saving period	初期件数 /Initial count	増加件数 /Increasing count		最大想定件数 /Max record count	レコード長 /Record length	説明 /Description
								件数 /Count	単位 /Unit			
1	EN-008	SCM01	SEARCH_CATEGORY_MASTER	検索カテゴリマスタ	マスタ/Master	永久	4	-	-	-	-	検索カテゴリのマスタデータを管理する
2	EN-009	SCM01	SEARCH_SUB_CATEGORY_MASTER	検索サブカテゴリマスタ	マスタ/Master	永久	3	-	-	-	-	検索サブカテゴリのマスタデータを管理する
3	EN-010	SCM01	SITE_MASTER	サイトマスタ	マスタ/Master	永久	10	-	-	-	-	検索対象サイトのマスタデータを管理する
4	EN-011	SCM01	SEARCH_TYPE_MASTER	検索種別マスタ	マスタ/Master	永久	3	-	-	-	-	検索種別のマスタデータを管理する
5	EN-012	SCM01	SEARCH_TARGET_MASTER	調査対象マスタ	マスタ/Master	永久	-	-	-	-	-	調査対象JSON格納先のマスタデータを管理する。レコード数は未定。

No.	データID	スキーマ /Schema	テーブルID /Table ID	テーブル名 /Table name	種別 /Type of table	保存期間 /Saving period	初期件数 /Initial count	増加件数 /Increasing count		最大想定件数 /Max record count	レコード長 /Record length	説明 /Description
								件数 /Count	単位 /Unit			
1	EN-001	SCM01	MONITORING_CONDITIONS	監視条件テーブル	トラン/Transaction	永久	0	-	-	-	-	検索方法や取得した情報全般を管理する
2	EN-002	SCM01	PRODUCT_INFORMATION	商品情報テーブル	トラン/Transaction	永久	0	-	-	-	-	取得した商品情報やその格納先を管理する
3	EN-003	SCM01	JUDGMENT_RESULT	判定結果テーブル	トラン/Transaction	永久	0	-	-	-	-	商品の違法性判定に使用するAIモデルや結果を管理する
4	EN-004	SCM01	VERIFICATION_RESULT	確認結果テーブル	トラン/Transaction	永久	0	-	-	-	-	防疫官が確認した結果を管理する
5	EN-005	SCM01	SELLER_INFORMATION	出品者情報テーブル	トラン/Transaction	永久	0	-	-	-	-	商品の出店者情報を管理する
6	EN-006	SCM01	IMPLEMENTATION_HISTORY	対応実施履歴テーブル	トラン/Transaction	永久	0	-	-	-	-	出品者への対応履歴を管理する

| テーブルID /Table ID | | SEARCH_CATEGORY_MASTER | | | | | テーブル名 Table name | | | 検索カテゴリマスタ | | | | |

テーブルID /Table ID		SEARCH_SUB_CATEGORY_MASTER					テーブル名 Table name			検索サブカテゴリマスタ																										
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																				説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1	SEARCH_SUB_CATEGORY_ID	検索サブカテゴリID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○																								
2	SEARCH_CATEGORY_ID	検索カテゴリID	半角数字/Single byte numeric character	INTERGER	-	-	-	-	○	-	-	SEARCH_CATEGORY_MASTER	SEARCH_CATEGORY_ID																							
3	SEARCH_SUB_CATEGORY	検索サブカテゴリ	半角英数字/Single byte Alphanumeric character	VERCHAR	16	-	-	-	○	-	-																								植物の場合であれば下記3つのいずれか。 別表2、別表1の2、別表2の2 昆虫と土の場合はなし。肉の場合は現状ないが、今後追加される可能性あり。

テーブルID /Table ID		SITE_MASTER					テーブル名 Table name				サイトマスタ																								
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																		説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1	SITE_ID	サイトID	半角英数字/Single byte Alphanumeric character	INTERGER	-	-	1	-	○	-	○																								
2	SITE_NAME	サイト名	全角文字/Double byte charactor	VERCHER	32	-	-	○	○	-	-																								検索サイト（Amazon、メルカリ等）を格納

テーブルID /Table ID		SEARCH_TYPE_MASTER					テーブル名 Table name				検索種別マスタ																								
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																				説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1	SEARCH_TYPE_ID	検索種別ID	半角英数字/Single byte Alphanumeric character	INTEGER	-	-	1	-	○	-	○																								
2	SEARCH_TYPE_NAME	検索種別名	全角文字/Double byte charactor	VERCHER	32	-	-	○	○	-	-																								API、検索スニペット取得API、スクレイピング・クローリングのいずれか

テーブルID /Table ID		SEARCH_TARGET_MASTER					テーブル名 Table name				調査対象マスタ			
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID	
1	SEARCH_TARGET_ID	調査対象ID	半角英数字/Single byte Alphanumeric character	INTEGER	-	-	1	-	○	-	○			
2	SEARCH_TARGET_STORAGE_S3_URI	調査対象格納先S3URI	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	-	○	-	-			調査対象データを格納したS3URI。検索キーワードの元情報を保持するために使用する。 例：植物を対象とする場合 植物名、学名、植物コードなどを含むJSONを作成、そのJSONが

テーブルID /Table ID		MONITORING_CONDITIONS					テーブル名 Table name			監視条件テーブル				
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	ﾁｪｯｸ /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID	
1	MONITORING_CONDITIONS_ID	監視条件ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○			
2	SEARCH_WORD	検索ワード	全角文字/Double byte charactor	VERCHAR	1024	-	-	-	○	-	-			
3	SEARCH_CATEGORY_ID	検索カテゴリID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	SEARCH_CATEGORY_MASTER	SEARCH_CATEGORY_ID	
4	SEARCH_SUB_CATEGORY_ID	検索サブカテゴリID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	-	-	-	SEARCH_SUB_CATEGORY_MASTER	SEARCH_SUB_CATEGORY_ID	
5	SITE_NAME	サイトID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	SITE_MASTER	SITE_ID	
6	SEARCH_TYPE	検索種別ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	SEARCH_TYPE_MASTER	SEARCH_TYPE_ID	
7	SEARCH_TARGET_ID	調査対象ID	半角英数字/Single byte Alphanumeric character	INTEGER	-	-	-	-	-	-	-	SEARCH_TARGET_MASTER	SEARCH_TARGET_ID	
8	SEARCH_DATETIME	検索日時	ﾀｲﾑｿﾞｰﾝ付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	○	-	-			
9	SEARCH_RESULT_STORAGE_S3_URI	検索結果格納先S3URI	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	-	○	-	-			
10	MONITORING_FREQUENCY	監視頻度	全角文字/Double byte charactor	VERCHAR	8	-	-	-	-	-	-			年、月、日のような値を想定している。

テーブルID /Table ID		PRODUCT_INFORMATION					テーブル名 Table name				商品情報テーブル			
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID	
1	PRODUCT_INFORMATION_ID	商品情報ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○			
2	MONITORING_CONDITIONS_ID	監視条件ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	SEARCH	SEARCH_ID	
3	PRODUCT_ID	商品ID	半角英数字/Single byte Alphanumeric character	VERCHAR	64	-	-	-	-	-	-			Yahoo!ショッピングと楽天市場の商品検索APIで取得可能。商品の重複を防ぐために取得する。
4	PRODUCT_NAME	商品名	全角文字/Double byte charactor	VERCHAR	128	-	-	-	-	-	-			
5	PRODUCT_URL	商品URL	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	-	-	-	-			braveでは商品IDを取得できないため、商品URLで商品の重複を判断する
6	SELLER_INFORMATION_ID	出品者情報ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	-	-	-	SELLER_INFORMATION	SELLER_INFORMATION_ID	
7	LISTED_AT	出品日時	タイムゾーン付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	-	-	-			
8	PRODUCT_INFORMATION_STORAGE_S3_URI	商品情報格納先S3URI	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	-	○	-	-			
9	PRODUCT_IMAGE_STORAGE_S3_URI	商品画像格納先S3URI	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	-	○	-	-			
10	REGISTRATION_STATUS	登録状況ステータス	フラグ/BOOLEAN	BOOLEAN	-	-	-	-	-	-	-			解析可能な状態かどうか判断する TRUE:解析可、FALSE:解析不可

テーブルID /Table ID		JUDGMENT_RESULT					テーブル名 Table name				判定結果テーブル																												
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																								説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18							
1	JUDGMENT_RESULT_ID	判定結果ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○																												
2	PRODUCT_INFORMATION_ID	商品情報ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	PRODUCT_INFORMATION	PRODUCT_INFORMATION_ID																												
3	EXECUTION_NAME	実行名	全角文字/Double byte charactor	VERCHAR	128	-	-	-	○	-	-																												
4	JUDGMENT_STATUS	判定ステータス	半角英数字/Single byte Alphanumeric charact	VERCHAR	16	-	-	-	-	-	-																												AIによる判定の進行状況。 STEP1_DONE、STEP2_DONE、COMPLETED、FAILEDのいずれか
5	JUDGMENT_START_DATETIME	判定開始日時	タイムゾーン付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	○	-	-																												
6	JUDGMENT_STATUS_UPDATED_AT	判定ステータス更新日時	タイムゾーン付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	-	-	-																												
7	PRODUCT_INFORMATION_MODEL_ID	商品情報モデルID	半角英数字/Single byte Alphanumeric charact	VERCHAR	128	-	-	-	-	-	-																												例.jp.anthropic.claude-haiku-4-5-20251001-v1:0
8	PRODUCT_INFORMATION_EXTRACTION_RESULT_STORAGE_S3_URI	商品情報抽出結果格納先S3URI	半角英数字/Single byte Alphanumeric charact	VERCHAR	1024	-	-	-	-	-	-																												LLMが抽出した結果をjsonで格納
9	RISK_JUDGMENT_CRITERIA_STORAGE_S3_URI	リスク判定基準格納先S3URI	半角英数字/Single byte Alphanumeric charact	VERCHAR	1024	-	-	-	-	-	-																												高/中/低リスク判定のパラメータをjsonで格納
10	RISK_JUDGMENT_RESULT	リスク判定結果	全角文字/Double byte charactor	VERCHAR	10	-	-	-	-	-	-																												高、中、低のいずれかだが、今後の拡張性も加味し、桁数を長めに確保しておく
11	RISK_JUDGMENT_STATUS	リスク判定ステータス	全角文字/Double byte charactor	VERCHAR	10	-	-	-	-	-	-																												違法、判定不能、違法疑いのような値を想定している。詳細は未定だが、不要になる可能性もあり。
12	RISK_TREND_JUDGMENT_MODEL_ID	リスク傾向判定モデルID	半角英数字/Single byte Alphanumeric charact	VERCHAR	128	-	-	-	-	-	-																												例.jp.anthropic.claude-haiku-4-5-20251001-v1:0
13	RISK_TREND_JUDGMENT_RESULT_STORAGE_S3_URI	リスク傾向判定結果格納先S3URI	半角英数字/Single byte Alphanumeric charact	VERCHAR	1024	-	-	-	-	-	-																												LLMが判定した結果をjsonで格納
14	RISK_SCORE_CRITERIA_STORAGE_S3_URI	リスクスコア基準格納先S3URI	半角英数字/Single byte Alphanumeric charact	VERCHAR	1024	-	-	-	-	-	-																												リスクスコア算出のパラメータをjsonで格納
15	RISK_SCORE	リスクスコア	半角数字/Single byte numeric character	INTEGER	-	-	-	-	-	-	-																												点数範囲は決定し てない。
16	VERSION	バージョン	半角英数字/Single byte Alphanumeric charact	VERCHAR	128	-	-	-	-	-	-																												文字列、内部的にプロンプトやロジック修正時にバージョンの違いを識別するため
17	RETRY_COUNT	試行回数	半角数字/Single byte numeric character	INTEGER	-	-	-	-	-	-	-																												
18	JUDGMENT_MEMO	判定メモ	全角文字/Double byte charactor	TEXT	-	-	-	-	-	-	-																												

テーブルID /Table ID		VERIFICATION_RESULT					テーブル名 Table name		確認結果テーブル																										
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																				説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1	VERIFICATION_RESULT_ID	確認結果ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○																								
2	PRODUCT_INFORMATION_ID	商品情報ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	PRODUCT_INFORMATION	PRODUCT_INFORMATION_ID																							
3	Verifier	確認者	全角文字/Double byte charactor	VERCHAR	64	-	-	-	○	-	-																								
4	VERIFICATION_DATETIME	確認日時	タイムゾーン付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	○	-	-																								
5	RISK_VERIFICATION_RESULT	リスク確認結果	全角文字/Double byte charactor	VERCHAR	10	-	-	-	○	-	-																								高、中、低のいずれかだが、今後の拡張性も加味し、桁数を長めに確保しておく
6	RISK_VERIFICATION_STATUS	リスク確認ステータス	全角文字/Double byte charactor	VERCHAR	10	-	-	-	○	-	-																								違法、判定不能、違法疑いのような値を想定している。詳細は未定だが、不要になる可能性もあり。
7	VERIFICATION_MEMO	確認メモ	全角文字/Double byte charactor	TEXT	-	-	-	-	-	-	-																								

テーブルID /Table ID		SELLER_INFORMATION			テーブル名 Table name		出品者情報テーブル																													
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																					説明 /Description
							主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18		
					全体 /Integer	小数 /Decimal						テーブルID /Table ID	項目ID /Item ID																								
1	SELLER_INFORMATION_ID	出品者情報ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○																									
2	SELLER_ID	出品者ID	半角英数字/Single byte Alphanumeric character	VERCHAR	64	-	-	-	-	-	-																									Yahoo!ショッピングと楽天市場の商品検索APIで取得可能。出品者の重複を防ぐために取得する。
3	SELLER_NAME	出品者名	全角文字/Double byte charactor	VERCHAR	64	-	-	-	-	-	-																									
4	SELLER_URL	出品者URL	半角英数字/Single byte Alphanumeric character	VERCHAR	1024	-	-	○	-	-	-																									

テーブルID /Table ID		IMPLEMENTATION_REPORT					テーブル名 Table name				対応実施報告テーブル																											
No.	項目ID Item ID	項目名 /Item name	型 /Format	型 /Type	桁数 /No. of Digits		制約（DDL） /Restriction(DDL)							初期値 /Initial value	INDEX																						説明 /Description
					全体 /Integer	小数 /Decimal	主キー /Primary key	Unique	NotNull	チェック /Check	オートインクリメント/Auto increment	外部キー /Foreign Key テーブルID /Table ID	外部キー /Foreign Key 項目ID /Item ID		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18				
1	IMPLEMENTATION_HISTORY_ID	対応実施履歴ID	半角数字/Single byte numeric character	INTEGER	-	-	1	-	○	-	○																											
2	SELLER_INFORMATION_ID	出品者情報ID	半角数字/Single byte numeric character	INTEGER	-	-	-	-	○	-	-	SELLER_INFORMATION	SELLER_INFORMATION_ID																											
3	IMPLEMENTATION_TITLE	対応実施タイトル	全角文字/Double byte charactor	INTEGER	64	-	-	-	○	-	-	IMPLEMENTATION_REQUEST	IMPLEMENTATION_REQUEST_ID																											
4	IMPLEMENTATION_TEXT	対応実施内容	全角文字/Double byte charactor	VERCHAR	1024	-	-	-	○	-	-																											
5	UPDATE_DATE_TIME	更新日時	タイムゾーン付日時/DateTime with Time Zone	TIMESTAMPTZ	-	-	-	-	-	-	-																											

別添資料 3-1.情報セキュリティに関する事項

1　情報セキュリティ対策要件

（１）情報システムのセキュリティ機能

ア　主体認証

（ア）本システムの主体認証は、パスワードを使った知識による認証を導入すること。

（イ）管理者権限を有するユーザの主体認証を行う場合、ネットワーク接続元の制限を行うなどして知識による認証以外の手段を併用すること。

（ウ）パスワードを使用する認証については、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる以下の機能を設けること。

A パスワード長は「13～64 文字」の範囲で設定できること。

B パスワード履歴は「3 回」以上記録することができ、パスワード履歴として記録されているパスワードを設定することができないこと。なお、機器の制限により、自動保存ができない場合については、管理台帳等を利用することも可とする。

C 文字種は「英大文字、英小文字、数字、記号」の 4 種類中 3 種類」以上を含むこと。

D 重複チェックは「認証コード又は氏名(ローマ字)と 3 文字以上重複」したパスワードを設定することができないこと。なお、機器の制限により、自動チェックができない場合については、管理台帳等を利用することも可とする。

（エ）主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。

A 原則として、機器等において初期値として設定されている認証コードを使用しない。

B 不要な認証コードを無効にする。

（オ）利用者に主体認証情報の定期的な変更を求める設定をすること。その場合には、利用者に対して定期的な変更を促す機能のほか、以下のいずれかの機能を設けること。

A 利用者が定期的に変更しているか否かを確認する機能

B 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能

C 利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能

（カ）主体認証情報が第三者に対して明らかにならないよう、以下を全て含む方法を用いて適切に管理すること。

A 主体認証情報を送信又は保存する場合には、その内容を暗号化する。

B 主体認証情報に対するアクセス制限を設ける。

C 主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認する。

（キ）主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下のいずれかの機能を設けること。

A 当該主体認証情報及び対応する識別コードの利用を停止する機能

B 主体認証情報の再設定を利用者に要求する機能

（ク） 本システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下（ケ）～（ス）において同じ。）すること。

（ケ） 識別コードの付与に当たっては、以下のいずれかの措置を講ずること。

A 本システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

B 主体への識別コードの付与に関する記録を消去する場合の監督職員からの事前の許可

（コ） 主体以外の者が識別コード又は主体認証情報を設定する場合、主体以外の者が設定する主体認証情報は強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を設定し、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

（サ） 識別コード及び知識による主体認証情報を付与された主体に対し、主体以外の者が設定した主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促す措置を講ずること。主体認証情報変更日時を確認し変更がなされない（使用していない）識別コードについては無効にする措置を講ずること。

（シ） 他の情報システムで利用している主体認証情報を設定しないよう主体に対し、利用者操作マニュアル等で注意喚起を行うこと。

（ス） 情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する実施手順を整備し、その実施手順に従って利用者に付与すること。

（セ） 主体が本システムを利用する必要がなくなった場合、以下の措置を講ずること。

A 当該主体の識別コードを無効にする。

B 無効化した識別コードを他の主体に新たに発行することを禁止する。

C 識別コードを追加又は削除する時に、不要な識別コードの有無を点検する。

（ソ） 導入する機器は、必要最低限の識別コードのみを登録すること。

（タ） その他、識別コードの付与に当たっては、以下のいずれかの措置を講ずること。ただし、他システムによって付与されるものは対象外とする。

A 識別コードの付与に関する記録及び当該記録を消去する場合の承認ルール等の規定

B ある主体に付与した識別コードを別の主体に対して付与することの禁止

C 主体以外の者が識別コード又は主体認証情報を設定する場合、主体への安全な配布方法

イ　アクセス制御

（ア） アクセス制御の導入

A 情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

B 情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、以下を例とするアクセス制御機能を適切に運用すること。

(A) 利用時間や利用時間帯によるアクセス制御

(B) 同一主体による複数アクセスの制限

(C) IP アドレスによる端末の制限

(D) ネットワークセグメントの分割によるアクセス制御

(E) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲内でアクセス可能となる制御

(F) 前各号に掲げるもののほか、以下を例とするアクセス制御機能を用いることを検討すること。

C 認証・認可の統合管理基盤を用いたアクセス制御

D アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御

（イ） 主体の属性、アクセス対象の属性に基づくアクセス制御の要件の定期的な確認による見直しをすること。

ウ　権限の管理

（ア） 権限管理機能の導入

A 主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、以下を例とする措置を講ずること。

(A) 管理作業をするときに限定してその管理者権限を利用することを可能とする方式

B 情報システムに権限管理機能を導入するに当たり、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって、不正に窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置として、以下を例とする措置を講ずること。

(A) 業務上必要な主体のみに限定する。

(B) 必要最小限の権限のみ付与する。

(C) デュアルロック機能を導入する。

(D) 管理者権限を行使できる端末をシステム管理者等の専用端末とする。

C 主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認すること。

（イ） 識別コード・主体認証情報の付与管理

A 情報システムを利用する主体に対して、全ての識別コード及び主体認証情報を適切に付与し、適切に管理するための措置を講ずること。

B 情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下本条において同じ。）すること。

C 識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。

D 識別コードは、情報システムを利用する主体ごとに個別に付与すること。ただし、システム管理者の判断の下、やむを得ず、複数の主体で共用する識別コード（以下「共用識別コード」という。）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。

E 管理者権限を持つ識別コードを付与する場合は、以下の措置を講ずること。

(A) 業務上必要な場合に限定する。

(B) 初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更する。

(C) 初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更する。

(D) ネットワーク経由のログインを制限する。

(E) 管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させないこと。

F 主体が情報システムを利用する必要がなくなった場合には、以下の措置を講ずること。

(A) 当該主体の識別コードを無効にする。

(B) 識別コードを追加又は削除する時に、不要な識別コードの有無を点検する。

(C) 主体認証情報の不正な利用を防止するために、当該主体に交付した主体認証情報格納装置を返還させる。

(D) 無効化した識別コードを他の主体に新たに発行することを禁止する。

G 業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス権を与えるようにアクセス制御を設定すること。また、人事異動等により、識別コードを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。

H 識別コードの付与に当たっては、以下を例とする措置を講ずること。

(A) 単一の情報システムにおいては、職員等 1 人に対する単一の識別コードのみの付与

(B) 職員等への識別コードの付与に関する記録及び当該記録を消去する場合の情報セキュリティ責任者からの事前の許可

(C) ある主体に付与した識別コードを別の主体に対して付与することの禁止

(D) 他の情報システムで利用している主体認証情報を設定しないようにするための主体に対する注意喚起

(E) 主体以外の者が識別コード又は主体認証情報を設定する場合、主体への安全な配付方法

エ ログの取得・管理

（ア）ログの取得・管理

A 情報システムにおいて、情報システム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を取得すること。

B 情報システムに含まれる構成要素 （サーバ装置・端末等）のうち、時刻設定が可能なものについては、可能な限り政府情報システムにおいて基準となる政府共通ネットワークが提供する時刻同期サービスの時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

C 情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法等について定め、適切にログを管理すること。

D 所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。

(A) 事象の主体（人物又は機器等）を示す識別コード

(B) 識別コードの発行等の管理記録

(C) 利用者による情報システムの操作記録

(D) 事象の種類

(E) 事象の対象

(F) 正確な日付及び時刻

(G) 試みられたアクセスに関わる情報

(H) 電子メールのヘッダ情報及び送信内容

(I) 通信パケットの内容

(J) 操作する者、監視する者、保守する者等への通知の内容

E 取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。

F ログが取得できなくなった場合の対処方法を定めること。

G 情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

H 取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、 必要に応じて、 以下の(A)の基本セキュリティ対策、及び、(B)の追加セキュリティ対策を例とする、当該作業を支援する機能を導入すること。

(A) ログ情報をソフトウェア等により集計し、 時系列で表示し、報告書を生成する等の作業の自動化

(B) リアルタイムでのログの調査・分析を行うための機能

オ　暗号・電子署名

（ア） 情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

A　要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、 必要があると認めたときは、 当該機能を設けること。

B 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

（イ） 暗号化又は電子署名を行う情報システムにおいて、可能な限り以下の措置を講ずること。

A 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

B 複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とする。

C 選択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。

D 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

E 安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

（ウ） 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

（エ） 職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、情報システムで使用するアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを、「電子政府推奨暗号リスト」に基づき定めること。

（オ） 前項で定めた事項の運用方法について、以下を全て含めて実施手順として定めること。

A 暗号化及び電子署名に使用するアルゴリズム又は鍵長が危殆化した

B 場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

C 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

（カ） 当省における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用するように定めること。

（２） 情報セキュリティの脅威への対策

ア　ソフトウェアの脆弱性対策

（ア） サーバ装置、端末及び通信回線装置の設置又は運用開始時に以下の対策を実施すること。

A インターネット向けにサービスを公開しているサーバ装置や直接インターネットから到達可能なサーバ装置、端末及び通信回線装置に対し脆弱性診断を実施すること。また、その他のサーバ装置、端末及び通信回線装置については、 情報システムの分類や保有する情報、 システム特性等を踏まえ、脆弱性診断の実施を検討すること。

B サーバ装置、端末及び通信回線装置に対し脆弱性診断の実施を検討すること。 また、 脆弱性診断の実施に当たっては、ペネトレーションテスト、TLPT （脅威ベースのペネトレーションテスト） 等の高度な脆弱性診断の実施を検討すること。

（イ） 対象となるソフトウェアの脆弱性に関して、以下を全て含む情報を適宜入手すること。

A 脆弱性の原因

B 影響範囲

C 対策方法

D 脆弱性を悪用する不正プログラムの流通状況

（ウ） 利用するソフトウェアはサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

（エ） 構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認すること。

（オ） 情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計を行うこと。

（カ） システム管理者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合には、当該対策を実施すること。

（キ） システム管理者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的及び適時に確認すること。

（ク） サーバ装置、端末及び通信回線装置の運用時に、定期的な脆弱性診断（ペネトレーションテスト、TLPT 等の高度な脆弱性診断を含む。）を実施すること。

（ケ） 脆弱性対策の状況を確認する間隔を、可能な範囲で短くすること。

（コ） ネットワーク境界にある通信回線装置や認証サーバ、要機密情報を保有するサーバ等のサイバーセキュリティリスクが高い機器等に対しては、原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずること。リスク評価結果を踏まえ措置を講じないと判断した場合には、リスク評価結果の記録を残すこと。

（サ） ソフトウェアに関する脆弱性対策計画を策定する際、以下の全ての事項について判断すること。

A 対策の必要性

B 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入する等により、効率的に脆弱性対策を実施する手法をあらかじめ決定すること

C 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法

D 対策方法又は回避方法が情報システムに与える影響

E 対策の実施予定時期

F 対策試験の必要性

G 対策試験の方法

H 対策試験の実施予定時期

（シ） 脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認すること。

（ス） 脆弱性対策を実施する際、少なくとも以下の全ての事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

A 実施日

B 実施内容

C 実施者

（セ） セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手し、完全性を検証すること。

（ソ） 脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。

（タ） セキュリティパッチの適用やソフトウェアのバージョンアップ等、脆弱性を解決するための早急な措置を講じることが困難な場合、解決策を適用するまでの期間においてログの監視を強化する等、脆弱性を悪用した攻撃を受けたことを迅速に察知するための対策を実施すること。

イ　不正プログラム対策

（ア） サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。

（イ） 不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

（ウ） 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

（エ） 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。

（オ） 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

（カ） 不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

（キ） 想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。

（ク） EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能を導入すること。

（ケ） 不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。

A 不正プログラム対策ソフトウェア等の導入状況

B 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

ウ　高度サイバー攻撃対策

（ア） システム管理端末とユーザ端末のネットワーク分離設計

A ユーザセグメント等の他セグメントとシステム管理端末の設置されたネットワーク上の専用セグメント（以下「運用管理セグメント」という。）を、他セグメントからアクセスできないよう、以下のいずれかの方法によりネットワークを分離設計すること。

(A) 各サーバのサーバ（業務）セグメントとは別に運用管理用セグメントの LAN ポートから LAN を構築する方法

(B) 当該 LAN ポートに直接管理端末を接続する方法等

B システム管理用の専用端末を準備すること。

C 他セグメントとネットワーク分離した運用管理セグメントを構築し、当該セグメントにシステム管理端末を接続すること。

D 認証サーバにて、認証サーバに管理者権限でログインできる端末を当該システム管理端末のみに制限すること。

E 当該サーバはサーバ（業務）セグメントからサーバの運用管理用セグメントの LAN ポートにアクセスできないようにすること

F 運用管理セグメントは、システム管理者のみが使用できる専用ネットワーク構成とすること。

G 運用管理セグメントの端末について、セキュリティパッチの適用やウイルス対策ソフトウェアのパターンファイル更新等を適宜実施すること。

（イ） 適切なネットワークセグメント分離及びアクセス制御設計

A 運用管理セグメント等に適切なネットワークの分離設計を行い、各セグメント間で行う通信を必要最小限のものに制限するように、適切なアクセス制御を行うこと。

B 組織内ネットワーク（内部ネットワーク）を VLAN やサブネットにより、サーバセグメント、ユーザセグメント等に適切に分離する設計を行うこと。

C 各セグメント間の通信に係るアクセス制御（IP アドレス及びポート番号の許可又は拒否）を設計し、ネットワーク上の基幹スイッチ等でアクセス制御リストを設定すること。

D 組織や業務の見直し等に合わせて、アクセス制御の設計見直しを実施すること。

（ウ） 高い管理者権限を有する認証コードのキャッシュ禁止

A ユーザ端末を利用するためのユーザアカウントとシステム管理端末を利用するための管理者用アカウントを分離すること。

B ユーザ、管理者、監査者等の役割ごとにアカウントを割り当てるよう設計すること。

C 管理者用アカウントの権限を最小化すること。

D 管理者に割り当てるアカウントは、必要最小限の権限となるよう設計すること。

E 高い管理者権限については、ActiveDirectory 等を管理する管理者のみに割り当てる。

F 管理する内容に応じて、ドメイン管理者よりも低い権限を割り当てること。

G 各端末のシステム管理に割り当てるアカウントは、ローカル管理者権限等の必要最小限の権限となるように設計すること。

H サービスやスケジュールされたタスクについて、ユーザ端末においてドメイン管理者権限等の高い権限のアカウントで実行しないように設計すること。

I ユーザ端末の利用者に対して、ユーザ権限ではなく、ローカル管理者権限等が付与されていないか確認すること。

J リモートデスクトップ接続でローカル管理者権限によるログインを禁止すること。

K 端末のローカル管理者のパスワードを他の端末とは異なるものに設定すること。

L ユーザ端末には、ドメイン管理者等の高い管理者権限を持つアカウントでログインしないこと。

M ドメイン管理者等の高い管理者権限を持つアカウントでログインしていないか、定期的に確認すること。

（エ）トラップアカウントによる認証ログの監視と分析

A 管理者権限アカウントに似せたトラップアカウントをユーザ端末に仕込み、当該トラップアカウントを用いた攻撃者のログイン行為を検知すること。

B トラップアカウントによる不正な操作を防止すること。

C トラップアカウントを利用して不正な操作が行われないよう、アカウントをキャッシュした後に認証サーバ側でパスワードを変更すること、

D 認証に成功したら直ちにログアウトするよう設計する等の対策を行うこと。

E トラップアカウントが利用されたことを検出するため、認証サーバのセキュリティイベントにおいてトラップアカウントの認証ログを監視すること。

F トラップアカウントの認証結果が残っていた場合は、アクセス元の端末を調査する等の対応を行うこと。

2 情報システムの構成要素に関する要件

（1）端末

ア 端末

（ア）要保護情報を取り扱う物理的な端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

（イ）モバイル端末を除く物理的な端末について、原則としてクラス 2 以上の要管理対策区域に設置すること。

（ウ）物理的な端末の盗難及び不正な持ち出しを防止するために、以下の対策を講ずること。

A モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定すること。

B モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意すること。

（エ）第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずること。

A 一定時間操作が無いと自動的にスクリーンロックするよう設定すること。

B 不特定多数の人が出入りする場所で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付けること。

（オ）以下の全てを考慮した上で、端末で利用を認めるソフトウェアをバージョンも含め定め、それ以外のソフトウェアは利用させないこと。

A ソフトウェアベンダ等のサポート状況

B ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む）、使用するポート、暗号化の有無

C インストール時に同時にインストールされる他のソフトウェアその他、ソフトウェアの利用に伴う情報セキュリティリスク（管理者権限使用時におけるパスワード入力の必要性、サーバソフトウェアとしての稼働有無等）

（カ） 端末に対して、利用を認めるソフトウェア以外のソフトウェアを利用者が自由にインストールできない技術的な措置を講じること。

（キ） 利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。

（ク） 利用を認めるソフトウェアの定期的な確認においては、引き続き利用を認めるか否かを判断し、利用を認めない場合は利用を認めるソフトウェアから削除すること。

（ケ） 利用を認めるソフトウェア以外のソフトウェアについて職員等から利用申請があった場合には、当該ソフトウェアの利用を認める否かを判断し、利用を認める場合は利用を認めるソフトウェアに追加すること。

（コ） 所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

（サ） 端末の運用を終了する際に、以下を例とする措置を講じて、端末の電磁的記録媒体の全ての情報を復元できないように抹消すること。

A 媒体の物理的破壊

B データ消去ソフトウェアによる情報の抹消

C 暗号化保存している場合、暗号鍵の削除

D HDD 等の磁気記録媒体の場合、消磁装置による情報の抹消

（２）サーバ装置

ア　サーバ装置の導入時の対策

（ア） 要保護情報を取り扱う物理的なサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

（イ） 要保護情報を取り扱う物理的なサーバ装置については、クラス 2 以上の要管理対策区域に設置すること。

（ウ） 物理的なサーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。

A 施錠可能なサーバラックに設置して施錠する。

B 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

（エ） 第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。

A 一定時間操作がないと自動的にスクリーンロックするよう設定する。

（**オ**） 障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、以下を例とする対策を講じ、可用性を確保すること。

A 複数のサーバ装置の設置による負荷分散

B 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

C 同一システムを 2 系統で構成することによる冗長化

（**カ**） 多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、以下を全て考慮した上で、サーバ装置で利用を認めるソフトウェアを定め、それ以外のソフトウェアは利用させないこと。

A ソフトウェアベンダ等のサポート状況

B ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む。） 、使用するポート、暗号化の有無

C インストール時に同時にインストールされる他のソフトウェア

D その他、ソフトウェアの利用に伴う情報セキュリティリスク

（**キ**） サーバ装置で利用を認めるソフトウェア以外のソフトウェアを利用する場合は申請を求め、前項 A から D までの全てを考慮した上で承認すること。

（**ク**） サーバ装置に接続を認めた機器等を定め、接続を認めた機器等以外は接続させないこと。

（**ケ**） 情報システムのセキュリティ要件として策定した内容に従い、サーバ装置に対して適切なセキュリティ対策を実施すること。

（**コ**） サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。

（**サ**） 要安定情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得すること。

イ　サーバ装置の運用時の対策

（**ア**） 所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

（**イ**） 所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、改善を図る場合は、作業日、作業を行ったサーバ装置名、具体的な作業内容（サーバ装置の構成等の変更、脆弱性管理、ソフトウェアのインストール等） 及び作業者、正常動作を確認した者などを含む変更事項等を記録し、管理すること。

（**ウ**） サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための以下を例とする措置を講ずること。

A アクセスログ等を定期的に確認する。

B 不正プログラム対策ソフトウェアを利用する。

C ファイル完全性チェックツールを利用する。

D CPU、メモリ、ディスク I/O 等のシステム状態を確認する。

E ホスト型の IDS/IPS を利用する。

F ユーザ、グループ、システム管理者の追加、変更の有無を確認する。

G 管理者、ユーザのパスワード漏洩の有無、大量のログオン失敗や、通常とは異なる時間帯やアクセス元 IP アドレスからのログインがないか確認する。

（エ） 要安定情報を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行えるよう、以下を全て含む運用をすること。

A サーバ装置の構成やソフトウェア等の設定の変更が行われた際及び定期的に、サーバ装置が停止した際の復旧手順の確認による見直し

B 以下の点を考慮してサーバ装置全体の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

・バックアップの対象（対象とするシステム、データ、ソフトウェアその他）

・バックアップの範囲（フルバックアップ、差分バックアップ等）

・バックアップを保存する電磁的記録媒体等の種類

・バックアップの周期、世代管理の方法

・使用するバックアップツール

・バックアップデータの秘匿性確保、改ざん防止の方法

・保管場所

・緊急時のバックアップデータの配送手段、配送時間

ウ　電子メール

（ア） 電子メールサーバが電子メールの不正な中継を行わないように設定すること。

（イ） 電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下の主体認証を行う機能を備えること。

A 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入すること。

（ウ） 以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

A DMARCによる送信側の対策を行うこと。DMARCによる送信側の対策を行うためには、SPF、DKIMのいずれか又は両方による対策を行う必要がある。

B DMARCによる受信側の対策を行うこと。DMARCによる受信側の対策を行うためには、SPF、DKIMの両方による対策を行う必要がある。

（エ） 職員等が機関等外の者と電子メールを送受信する場合には、政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能を備えること。

（オ） インターネットを介して通信する電子メールの盗聴及び改ざんを防止するため、以下を例とする電子メールのサーバ間通信の暗号化の対策を講ずること。

A SMTP によるサーバ間通信を TLS により保護する。

B S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。

エ　ウェブ

（**ア**）ウェブサーバが備える機能のうち、必要な機能のみを利用するために、以下を全て含むウェブサーバの管理や設定を行うこと。

A CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とすること。

B ディレクトリインデックスの表示を禁止すること。

C ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限すること。

D ウェブサーバ上で動作するソフトウェアは、最新のものを利用する等、既知の脆弱性が解消された状態を維持すること。

（**イ**）ウェブサーバからの不用意な情報漏えいを防止するための措置を講ずること。

（**ウ**）ウェブサーバからの不用意な情報漏えいを防止するため、以下を全て含むウェブサーバの管理や設定を行うこと。

A 公開を想定していないファイルをウェブ公開用ディレクトリに置かないこと。

B 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除すること。

C ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

（**エ**）ウェブコンテンツの編集作業を担当するアカウントの限定として、以下を全て含むウェブサーバの管理や設定を行うこと。

A ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えないこと。

B OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除すること。

（**オ**）ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下のとおりウェブサーバの管理や設定を行うこと。

A ウェブコンテンツの更新の際は、専用の端末を使用して行う。

B ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限すること。

C ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行うこと。

（**カ**）通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を全て含むウェブサーバの実装を行うこと。

A TLS 機能を適切に用いること。

B TLS 機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

C 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定すること。

（キ） ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

オ データベース

（ア） データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。

（イ） データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

（ウ） データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

（エ） データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

（オ） データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。

（３） ソフトウェア

ア 情報システムの基盤を管理又は制御するソフトウェア

（ア） 情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講ずること。

（イ） 利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備すること。

A 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

B 情報システムの基盤を管理又は制御するソフトウェアで発生した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

（ウ） 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するため、権限設定やアクセス制御、セキュリティ設定が適切であるか定期的な確認をすること。

（エ） 情報システムの基盤を管理又は制御するソフトウェアにおいて、脅威や情報セキュリティインシデントを迅速に検知し、対応するため、以下の全ての対策を実施すること。

A 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順に基づく教育の実施

B 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基づく訓練

（４） アプリケーション・コンテンツ

ア アプリケーション・コンテンツのセキュリティ要件の策定

（ア） 当省外の情報システム利用者の情報セキュリティ水準の低下を招かないよう、アプリケーション・コンテンツについて、以下を全て含む対策をセキュリティ要件として仕様に含めること。

A アプリケーション・コンテンツを提供する前に、 不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

B 業務委託により作成したアプリケーションプログラムを提供する場合には、 委託先事業者に、 当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。

（イ） 提供するアプリケーション・コンテンツが脆弱性を含まないように開発することをセキュリティ要件として仕様に含めること。

（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場合を除き、実行プログラムの形式でコンテンツを提供しないことをセキュリティ要件として仕様に含めること。

（エ） 電子証明書を用いた署名等、 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をアプリケーション・コンテンツの提供先に与えることをセキュリティ要件として仕様に含めること。

（オ） 提供するアプリケーション・コンテンツの利用時に、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をセキュリティ要件として仕様に含めること。

（カ） 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、サービス利用に当たって必須ではない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、以下を全て含む開発をすることをセキュリティ要件として仕様に含めること。

A 当省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当省外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

B 本来のサービス提供に必要のない当省外へのアクセスを自動的に発生させる機能を含めないこと。

イ アプリケーション・コンテンツの開発時の対策

（ア） ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。

（イ） ウェブアプリケーションの開発において、以下を含む既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れがないか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

A SQL インジェクション脆弱性

B OS コマンドインジェクション脆弱性

C ディレクトリトラバーサル脆弱性

D セッション管理の脆弱性

E アクセス制御欠如と認可処理欠如の脆弱性

F クロスサイトスクリプティング脆弱性

G クロスサイトリクエストフォージェリ脆弱性

H クリックジャッキング脆弱性

Ｉ メールヘッダインジェクション脆弱性

Ｊ HTTP ヘッダインジェクション脆弱性

Ｋ eval インジェクション脆弱性

Ｌ レースコンディション脆弱性

Ｍ バッファオーバーフロー及び整数オーバーフロー脆弱性

ウ　アプリケーション・コンテンツの運用時の対策

（**ア**） 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

（**イ**） 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずること。

（**ウ**） ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずること。

エ　アプリケーション・コンテンツ提供時の対策

（**ア**） 提供するウェブサイト等が実際の当省提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。

別紙２

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３】

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。	□	□
・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　臭気や害虫の発生源となるものについて適正な管理や処分に努める。

具体的な事項	実施した／努めた	左記非該当
・臭気が発生する可能性がある機械・設備（食品残さの処理や堆肥製造等）を使用する場合、周辺環境に影響を与えないよう定期的に点検を行う。	□	□
・臭気や害虫発生の原因となる生ごみの削減や、適切な廃棄などに努めている。	□	□
・食品保管を行う等の場合、清潔な環境を維持するため、定期的に清掃を行うことに努めている。	□	□
・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
（　　）

エ　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
（　　）

オ　工事等を実施する場合は、生物多様性に配慮した事業実施に努める。

具体的な事項	実施した／努めた	左記非該当
・近隣の生物種に影響を与えるような、水質汚濁が発生しないよう努めている。	□	□
・近隣の生物種に影響を与えるような、大気汚染が発生しないよう努めている。	□	□
・施工にあたり使用する機械や車両について、排気ガスの規制に関連する法令等に適合したものを使用する。	□	□
・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
（　　）

カ　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
（　　）

別紙４

AWS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）	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
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
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
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
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
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
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６

農林水産省　宛

資料閲覧申請書

「違法輸入動植物等流通監視システム整備業務」に係る資料閲覧を申請します。

申込日：　令和　　年　　月　　日

１　会 社 名：

２　住　　所：

３　部署名・担当者名：

４　電話番号：

５　E-mail アドレス：

６　閲覧日時：第１候補日　令和　年　　月　　日　　時　　分～　　時　　分
　　第２候補日　令和　年　　月　　日　　時　　分～　　時　　分
　　第３候補日　令和　年　　月　　日　　時　　分～　　時　　分

７　閲覧者氏名：
　　：
　　：

別紙７

農林水産省　宛

守秘義務に関する誓約書

「違法輸入動植物等流通監視システム整備業務」に係る資料閲覧に当たり、下記の事項を遵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、若しくは漏洩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関わらず、守秘義務を負います。

４　上記１～３に反して、情報の開示、漏えい若しくは使用した場合、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

違法輸入動植物等流通監視システム整備業務　質問表

別紙８

事業者名：

日付：　　令和　　年　　月　　日

No.	資料名	頁	資料の該当記載内容	分類 (意見/質問)	意見/質問内容
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					