入札公告

次のとおり一般競争入札に付します。

令和６年１月31日

支出負担行為担当官

横浜植物防疫所長　森田　富幸

◎調達機関番号　018　◎所在地番号　14

１　調達内容

(1)　品目分類番号　71、27

(2)　購入等件名及び数量　植物防疫所業務システム更改業務　一式（電子入札方式対象案件）

(3)　調達案件の仕様等　入札説明書による。

(4)　履行期間　令和６年４月１日から令和７年３月31日まで。

(5)　履行場所　支出負担行為担当官が指定する場所。

(6)　入札方法　落札者の決定は総合評価落札方式をもって行うので、提案に係る性能、機能、技術等に関する書類（以下「総合評価の

ための書類」という。）を提出すること。なお、落札決定に当たっては、入札書に記載された金額に当該金額の10パーセントに相当する額を加算した金額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てるものとする。）をもって落札価格とするので、入札者は消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の110分の100に相当する金額を入札書に記載すること。

２　競争参加資格

(1)　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。

(2)　予算決算及び会計令第71条の規定に該当しない者であること。

(3)　令和４・５・６年度農林水産省競争参加資格（全省庁統一資格）「役務の提供等」にお

いて、「Ａ」又は「Ｂ」の等級に格付けされている者であること。

(4)　予算決算及び会計令第73条の規定に基づき、支出負担行為担当官が定める資格を有する者であること。

(5)　契約担当官等から物品の製造契約、物品の購入契約及び役務等契約指名停止等措置要領（平成27年４月１日付け26横植第1521号）に基づく指名停止を受けている期間中の者でないこと。

３　電子調達システム（ＧＥＰＳ）の利用

本案件は、入札等を電子調達システムで行う対象案件である。なお、電子調達システムによりがたい者は、発注者に書面により申出のうえ、紙入札によることができる。

４　入札書の提出方法及び場所等

(1)　入札書の提出方法　電子調達システムによるが、電子調達システムに停電等の不具合、システム障害等やむを得ない事情によるトラブルが発生した場合は、紙入札に移行す

ることがある。

(2)　入札書の提出場所、契約条項を示す場所、入札説明書の交付場所及び問い合わせ先

〒231－0003　神奈川県横浜市中区北仲通５－57　横浜植物防疫所総務部会計課調達係　小林　孝之　電話045－211－7151

(3)　入札説明書の交付方法　本公告日から調達ポータル上にてダウンロード可能。

https://www.p-portal.go.jp/pps-web-biz/UAA01/OAA0101

(4)　入札説明会の開催　開催しない。

(5)　入札書の受領期限　令和６年３月21日午後５時

(6)　開札の日時及び場所　令和６年３月26日午後２時　横浜植物防疫所会議室

４　その他

(1)　入札及び契約手続において使用する言語及び通貨　日本語及び日本国通貨。

(2)　入札保証金及び契約保証金　免除。

(3)　入札者に要求される事項　この一般競争に

参加を希望する者は、封印した入札書に総合評価のための書類を添付して入札書に添付して入札書の受領期限までに提出しなければならない。入札者は開札日の前日までの間において、支出負担行為担当官から当該書類に関し説明を求められた場合は、それに応じなければならない。当該書類に関し説明の義務を履行しない者は落札決定の対象としない。

(4)　入札の無効　本公告に示した競争参加資格のない者の入札、総合評価のための書類に虚偽の記載をした者の入札及び入札に関する条件に違反した者の入札は無効とする。

(5)　契約書作成の要否　要。

(6)　落札者の決定方法　本公告に示した調達案件を履行できると支出負担行為担当官が判断した総合評価のための書類を添付して入札書を提出した入札者であって、予算決算及び会計令第79条の規定に基づいて作成された予定価格の制限の範囲内で支出負担行為担当官が入札説明書で説明する、性能、機能、技術等

（以下「性能等」という。）のうち、最低限の要求要件をすべて満たしている性能等を提案した入札者の中から、支出負担行為担当官が入札説明書で定める総合評価の方法をもって落札者とする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって入札した他の者のうち他の評価の最も高い者を落札者とすることがある。

(7)　手続きにおける交渉の有無　無。

(8)　その他　詳細は入札説明書による。

5　Summary

(1)　Official in charge of disbursement of the procuring entity : MORITA Tomiyuki, Director General, Yokohama Plant Protec-

tion Station

(2) Classification of the services to be procured : 71, 27

(3) Nature and quantity of the services to be required : Operation upgrade work in Plant Protection Stations service system 1 set

(4) Fulfillment period : From 1 April, 2024 through 31 March, 2025

(5) Fulfillment place : The place specified by Official in charge of disbursement of the procuring entity

(6) Qualification for participating in the tendering procedures : Suppliers eligible for participating in the proposed tender are those who shall :

① not come under Article 70 of the Cabinet Order concerning the Budget, Auditing and Accounting. Furthermore, minors, Person under Conservatorship or

Person under Assistance that obtained the consent necessary for concluding a contract may be applicable under cases of special reasons within the said clause.

② not come under Article 71 of the Cabinet Order concerning the Budget, Auditing and Accounting.

③ have the Grade "A" or "B" in terms of the qualification "provision of services" for participating in tenders by Ministry of Agriculture, Forestry and Fisheries (Single qualification for every ministry and agency) in the fiscal year, 2022, 2023 and 2024.

④ meet the qualification requirements which the Obligating Officer may specify in accordance with Article 73 of the Cabinet Order.

⑤ Prove not to be a period of receivi-

ng nomination stop from the contracting officer etc.

(7) Time limit for tender : 5:00 P.M., 21 March, 2024

(8) Contact point for the notice: KOBAYASHI Takayuki, Procurement Section, General Affairs Department, Yokohama Plant Protection Station, Kitanakadori 5－57 Naka-ku Yokohama city Kanagawa prefecture 231－0003 Japan. TEL 045－211－7151

植物防疫所業務システム

更改業務

調達仕様書

農林水産省

横浜植物防疫所

目次

1　調達案件の概要 4
（1）調達件名 4
（2）調達の背景 4
（3）調達目的及び調達の期待する効果 4
（4）業務・情報システムの概要 5
（5）契約期間 8
（6）作業スケジュール 8
2　調達案件及び関連調達案件 9
（1）調達範囲 9
（2）調達案件の一覧 10
3　情報システムに求める要件 11
4　作業の実施内容 12
（1）対象４サーバの MAFF クラウド移行及び各種ソフトウェアの更新等 12
（2）通信機器等デバイス類の更新等 13
（3）設計・開発実施計画書等の作成 14
（4）設計 14
（5）開発・テスト 15
（6）受入テスト支援 16
（7）情報システムの移行 16
（8）クラウドサービスを運用保守する場合の前提 17
（9）定常時対応 17
（１０）障害発生時対応 18
（１１）引継ぎ 19
（１２）定例会等の実施 19
（１３）契約金額内訳及び情報資産管理標準シートの提出 19
（１４）植物防疫所業務システム（PPS-System）のセキュリティ要件の点検支援 20
（１５）成果物 21
5　作業の実施体制・方法 23
（1）作業実施体制 23
（2）作業要員に求める資格等の要件 24
（3）作業場所 25
（4）作業の管理に関する要領 26
6　作業の実施に当たっての遵守事項 26
（1）機密保持、資料の取扱い 26
（2）個人情報の取扱い 26
（3）法令等の遵守 27
（4）標準ガイドラインの遵守 27
（5）その他文書、標準への準拠 28
（6）情報システム監査 29
（7）セキュリティ要件 29
7　成果物の取扱いに関する事項 30
（1）知的財産権の帰属 30
（2）契約不適合責任 31
（3）検収 32
8　入札参加資格に関する事項 32

（1）競争参加資格 32
（2）公的な資格や認証等の取得..... 32
（3）受注実績..... 33
（4）複数事業者による共同入札..... 33
（5）入札制限..... 33
9　再委託に関する事項..... 33
（1）再委託の制限及び再委託を認める場合の条件 33
（2）承認手続..... 34
（3）再委託先の契約違反等..... 34
１０その他特記事項..... 34
（1）前提条件等..... 34
（2）入札公告期間中の資料閲覧等..... 34
（3）その他 36
１１附属文書..... 36
（1）別紙１　情報セキュリティの確保に関する共通基本仕様 36
（2）別紙２　AWS 設定確認リスト 36
（3）別紙３　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... 36
（4）別紙４　資料閲覧申請書 36
（5）別紙５　守秘義務に関する誓約書..... 36
（6）別紙６　質問書..... 36

1　調達案件の概要

（1）調達件名

植物防疫所業務システム更改業務

（2）調達の背景

植物防疫所では、植物防疫法に基づき、植物に被害をもたらす病害虫の侵入を未然に防ぐため、全国の海港や空港で輸入される植物の検査を行う輸入植物検疫を行っている。

また、国内で重要な病害虫のまん延を防ぐため、特定の植物の移動規制や種苗類の検査などを行う国内植物検疫業務及び日本産の植物を輸出する際、輸出先国の要求に応じた検査や検定を行う輸出植物検疫業務を行っており、我が国の農業生産の安全及び助長を図っている。これらの業務を遂行するため、横浜、名古屋、神戸、門司及び那覇に本所を置き、全国に 16 支所、35 出張所に、植物防疫官を約 1,000 名配置して、年間、輸入貨物約 57.3 万件、輸出貨物約 12.4 万件の検査を行っている。その他、携帯品（輸入約 16.4 万件、輸出約 0.2 万件）、郵便物（輸入約 20.2 万件、輸出約 1.1 万件）の検査も行っている。（いずれも 2022 年実績）

上記の業務を円滑かつ適切に行うため、貨物の輸出入検査の手続は輸出入・港湾関連情報処理センター株式会社が運営する「輸出入・港湾関連情報処理システム」（以下、「NACCS」という。）を利用して処理している。

さらに、植物防疫官の検査を迅速かつ的確に行うため、検査に必要な病害虫等の情報や輸出入検疫の条件等を提供する個別システム群を総称した「植物防疫所業務システム（PPS-System）」を民間のクラウドサービス（IaaS）と農林水産省クラウド（以下、「MAFF クラウド」という。）を利用して運用している。

2018 年 6 月には、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」が決定（最終改定は、2023 年 9 月 29 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。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、2020 年 3 月に「農林水産省デジタル・ガバメント中長期計画」を改定し、情報システムのクラウド化の推進に当たっては、共通基盤となる MAFF クラウドを利用することを前提としたパブリッククラウドへの移行を進めることとしている。

（3）調達目的及び調達の期待する効果

本調達は、「植物防疫所業務システム更改業務（以下、「本案件業務」という。）」の調達に必要とされる基本的な要件を記載し、対象4サーバ（ホームページサーバ、成田 Web サーバ、成田バーコード中継サーバ、Cotipa Web サーバ）を現行クラウドサービスから MAFF クラウド（AWS）へ移行するための更改作業、成田検疫情報提供システムを構成する通信機器等デバイス類の更新作業、等を目的とする。

なお、本案件業務の調達要件等の具体的内容については、次項以降で詳述する。

（4） 業務・情報システムの概要

植物防疫所業務システム（PPS-System）、成田検疫情報提供システム及び MAFF クラウドの概要は次のとおりである。

ア 概要

（ア）植物防疫所業務システム（PPS-System）

植物防疫所業務システム（PPS-System）は、一般国民向けの外部公開システム、当所職員向けのシステム、各種データベース等からなる。

外部公開しているシステムとしては、植物検疫に係る手続きを電子化した「電子申請システム」、植物の輸出入検査の実績等を調べることが可能な「植物検疫統計」、植物を輸入する際の輸入条件の有無等を調べることが可能な「輸入条件に関するデータベース」等がある。当所職員向けのシステム、各種データベースとしては、研究目的等のための輸入禁止品の輸入許可状況を管理する「輸入禁止品管理システム」、横浜植物防疫所成田支所で利用しているサブシステムの「成田検疫情報提供システム」、検疫業務を支援するための「各種対応事例データベース」、「各種検査指標」等がある。

なお、これらの機能は基本的には Web 形式で提供されている。

また、植物検疫業務に係る業務処理の効率化を図るため、NACCS との連携機能が構築されており、職員端末から Web ブラウザでアクセス・利用する仕様となっている。

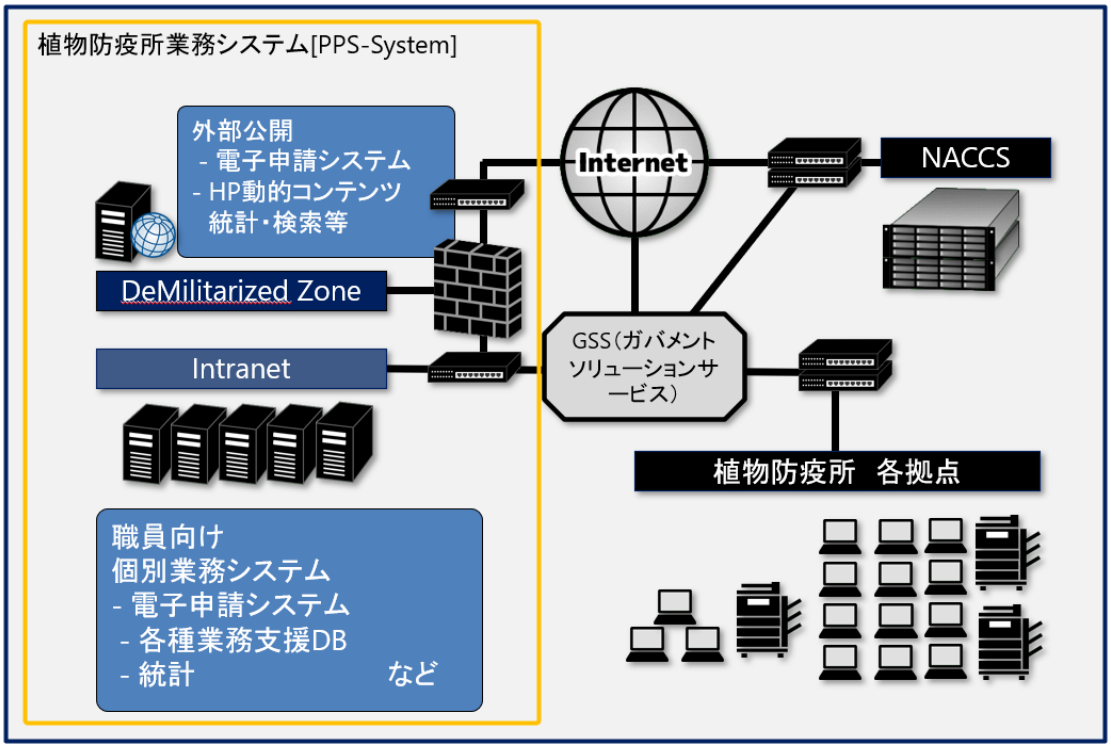

図 1　植物防疫所業務システム（PPS-System）の概要

※図中の GSS（ガバメントソリューションサービス）については、令和5年度に農林水産省統合 NW からの移行が完了したものである。

（イ）成田検疫情報提供システム

成田検疫情報提供システムは、横浜植物防疫所成田支所において利用している植物防疫所業務システム（PPS-System）内の一業務システムである。

同システムは、植物防疫所業務システム（PPS-System）を構成するサーバ群の中の成田 WEB サーバ及び成田バーコード中継サーバの2サーバで構成・稼働しており、輸入検査の申請者が申請情報を受付端末に登録することにより、NACCS と連携して当該輸入検査の進捗状況等をモニタに表示する機能、植物防疫所職員が検査する貨物を抽出するための機能、植物防疫所業務システム（PPS-System）の統計 DB サーバと連携して規制対象の植物であることを表示する機能等がある。また、検査する貨物を抽出する機能については、携帯電話からホームページサーバの画面にアクセスして利用している。

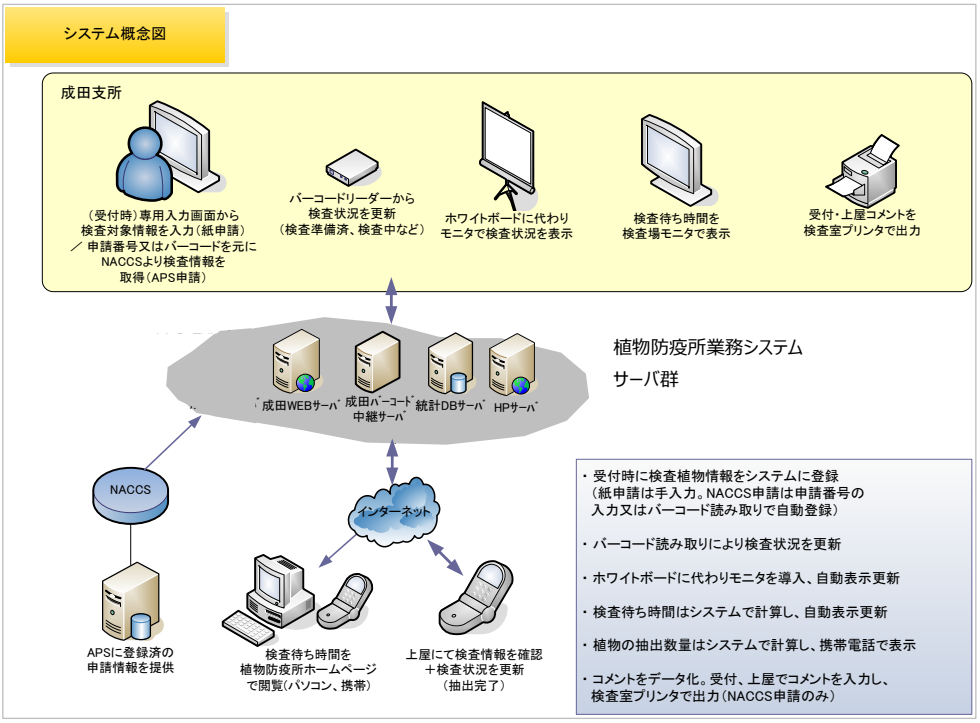

図 2　成田検疫情報提供システムの概要

（ウ）MAFF クラウド

MAFF クラウドでは、クラウド運用に必要最小限な共通機能を提供するとともに、クラウド運用等の一連の工程における、PMO による PJMO への総合的な支援活動を実施する（総合的な支援活動を行う組織を「MAFF クラウド CoE」という。）。サービス詳細は、

入札公告期間中の閲覧資料の「農林水産省クラウド利用ガイドライン及び関係資料」を参照すること。引き続き、本システムでは MAFF クラウドを利用することを前提とする。

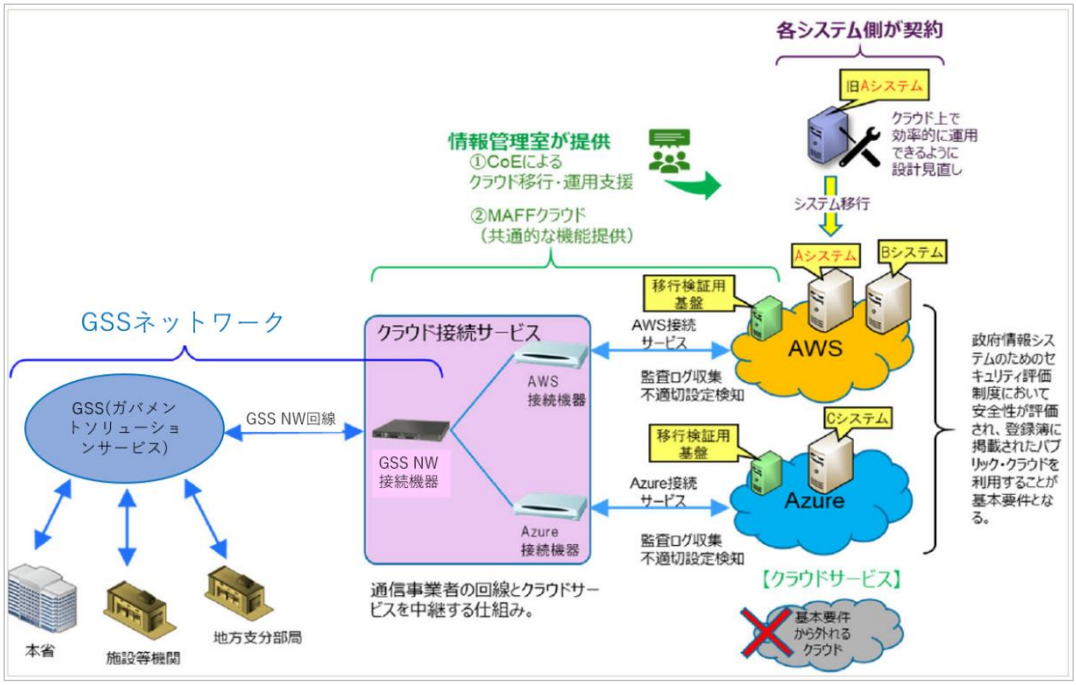

図 3　MAFF クラウドの概要

※図中の GSS（ガバメントソリューションサービス）については、令和5年度に農林水産省統合 NW からの移行が完了したものである。

イ　利用形態

植物防疫所業務システム（PPS-System）は海港・空港に設置された事務所以外に、国際郵便局や隔離ほ場の事務室等を加えた約 100 拠点から約 1,000 名が利用している。

また、各拠点及び植物防疫所業務システム（PPS-System）のクラウドを繋ぐネットワーク網は、デジタル庁が提供する GSS（ガバメントソリューションサービス）を利用している（令和5年度に農林水産省統合 NW からの移行が完了済み）。

植物防疫所外へのメール送受信に当たっては、農林水産省本省のメールサーバを経由することとなっており、また、職員がインターネット接続を行う際は、農林水産省共有のプロキシサーバを経由することになっている。

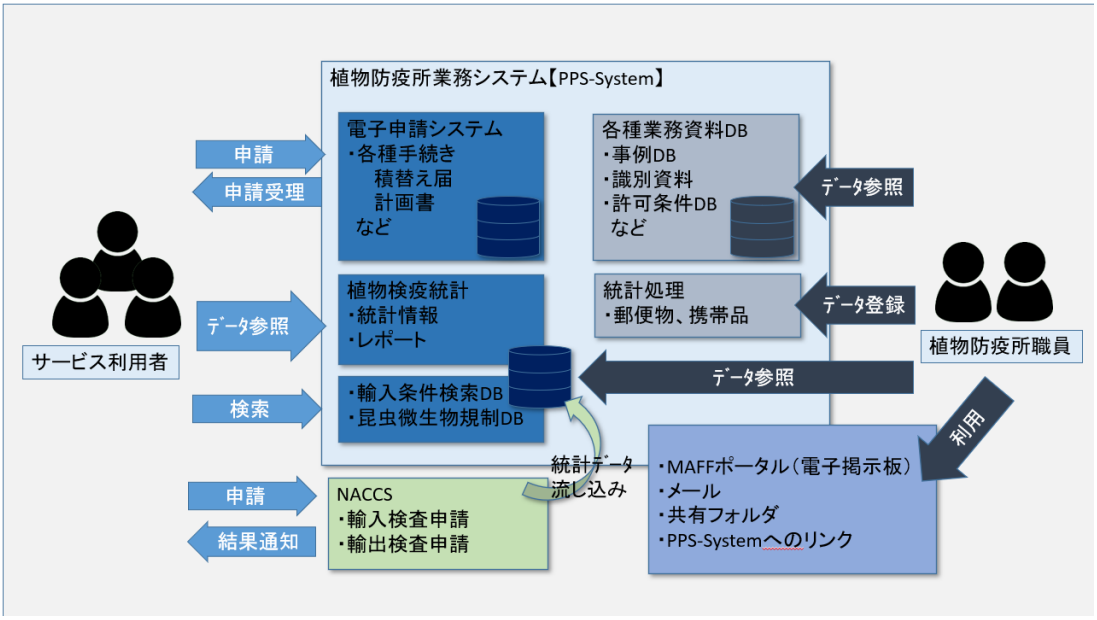

図 4　植物防疫所の業務概要

ウ　システム運用概要

（ア）運転日

植物防疫所は国際空港を中心に 24 時間 365 日開庁して植物検疫業務を行っていることから、植物防疫所業務システム（PPS-System）は原則 24 時間 365 日稼働している。

（イ）保守日

上述のとおり植物防疫所業務システム（PPS-System）は原則 24 時間 365 日稼働しているため、バックアップ取得はオンラインのまま行っている。なお、パッチの適用や緊急の障害対応等を要する場合は、植物防疫所システム管理者（以下、「PJMO」という。）及び本案件業務の受注者間で協議の上、緊急保守日を設けることとし、保守時間については、システムが頻繁に利用される時間帯（6:00～24:00）を可能な限り避けて作業を行っている。

（5）契約期間

契約締結日から令和7年3月 31 日まで

（6）作業スケジュール

作業スケジュールは次のとおり想定しているが、具体的なスケジュールについては、PJMO と協議の上決定すること。

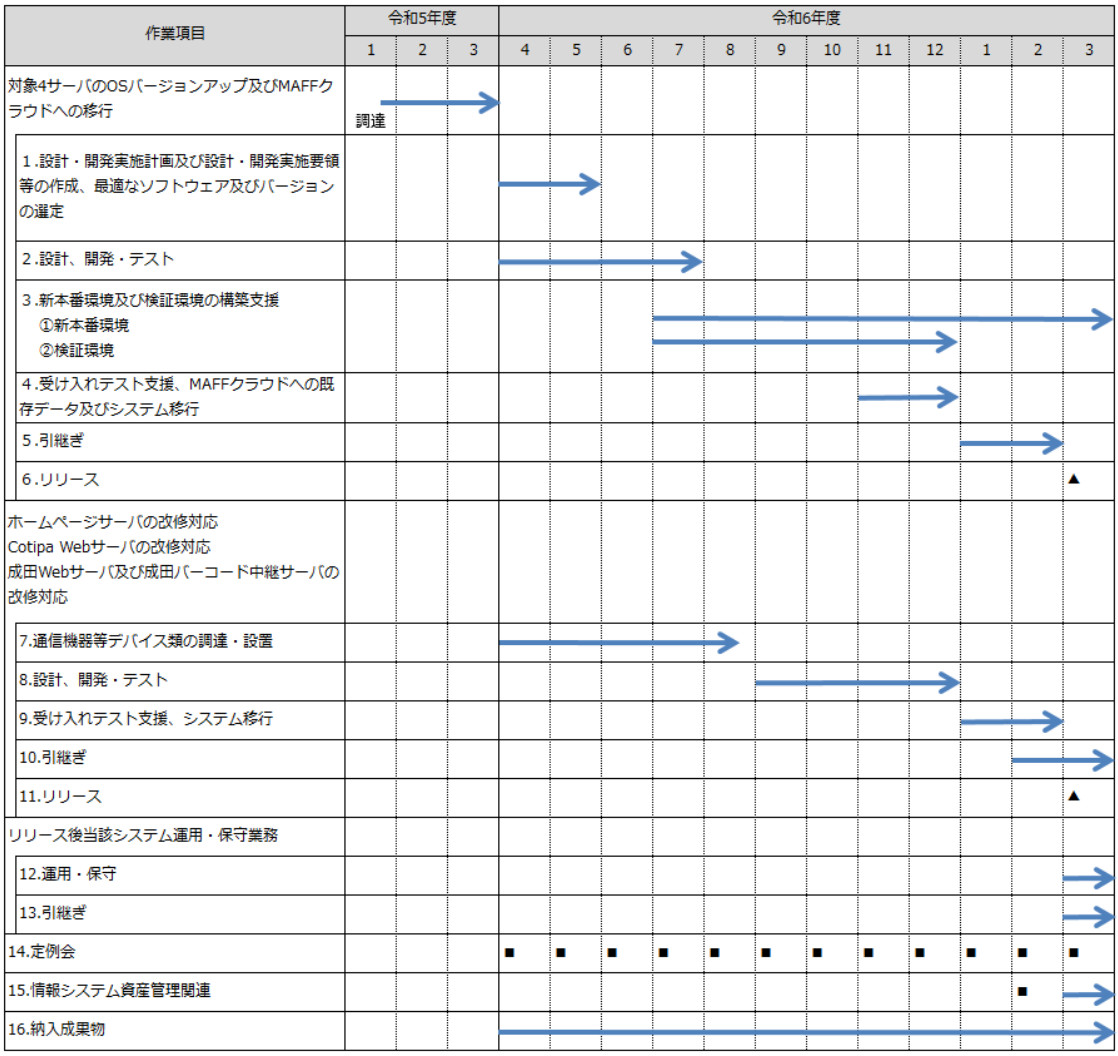

図 5 作業スケジュール

2 調達案件及び関連調達案件

(1) 調達範囲

本調達業務では、現行クラウドで稼働している植物防疫所業務システム（PPS-System）を構成するサーバ群の中の対象4サーバ（ホームページサーバ、成田 Web サーバ、成田バーコード中継サーバ、Cotipa Web サーバ）を MAFF クラウドへ移行し、併せて、当該サーバの OS 等ソフトウェアを更新する作業及び通信機器等デバイス類の更新等並びに契約期間終了までの対象サーバ及びシステムの運用・保守業務をその範囲とする。なお、本調達においては、MAFF クラウドを利用する上で必要な金額及び同システムのリリース後から契約期間終了までの運用・保守費用を入札金額に含めることとする。

また、本調達の契約期間終了後については、別途植物防疫所が契約する次年度の「植物防疫所業務システム等運用支援及び保守業務」において同様のライセンスや外部サービスを継続利用していくことを想定しているため、次年度以降の植物防疫所業務システムの運

用・保守費用については本調達の対象範囲外であるが、ライセンス等は確実に次年度の「植物防疫所業務システム等運用支援及び保守業務」の受注者（以下、「支援業者」という。）へ引き継ぐこと。

表１ 調達内容

No	調達内容	本資料参照先	その他
1	植物防疫所業務システム更改業務	４ 業務の実施内容 植物防疫所業務システム更改業務に係る要件	ー
2	植物防疫所業務システム更改業務リリース後当該システム運用・保守業務	４ 業務の実施内容 植物防疫所業務システム更改業務の移行完了後、契約期間中における当該システムの運用及び保守に係る要件	ー
3	システム運用・保守引継ぎ業務	４ 業務の実施内容 当該システムの運用及び保守の引継ぎに係る要件	ー

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、植物防疫所と協議の上、決定するものとする。

（2） 調達案件の一覧

調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等は次の図のとおりであり、植物防疫所業務システム（PPS-System）の MAFF クラウドへの移行は令和5年度から実施している。

表 2 本調達案件及び関連する調達案件の一覧

No	調達案件名	調達の方式	契約締結日	意見招請 入札公告 落札者決定	契約期間
1	植物防疫所業務システム更改業務	一般競争入札（総合評価落札方式）	令和 6 年 4 月 1 日	令和 5 年 12 月頃 令和 6 年 1 月頃 令和 6 年 3 月頃	令和 6 年 4 月から 令和 7 年 3 月まで
2	植物防疫所業務システム運用支援及び保守業務	最低価格落札方式	令和 6 年 4 月 1 日	ー 令和 5 年 12 月頃 令和 6 年 2 月頃	令和 6 年 4 月から 令和 7 年 3 月まで
3	植物防疫所業務システムハードウェア等保守及びパソコン等管理運用業務	最低価格落札方式	令和 6 年 4 月 1 日	ー 令和 5 年 12 月頃 令和 6 年 2 月頃	令和 6 年 4 月から 令和 7 年 3 月まで
4	植物防疫所業務システムクラウドサービス提供業務	随意契約	令和 6 年 4 月 1 日	ー ー ー	令和 6 年 4 月から 令和 7 年 3 月まで

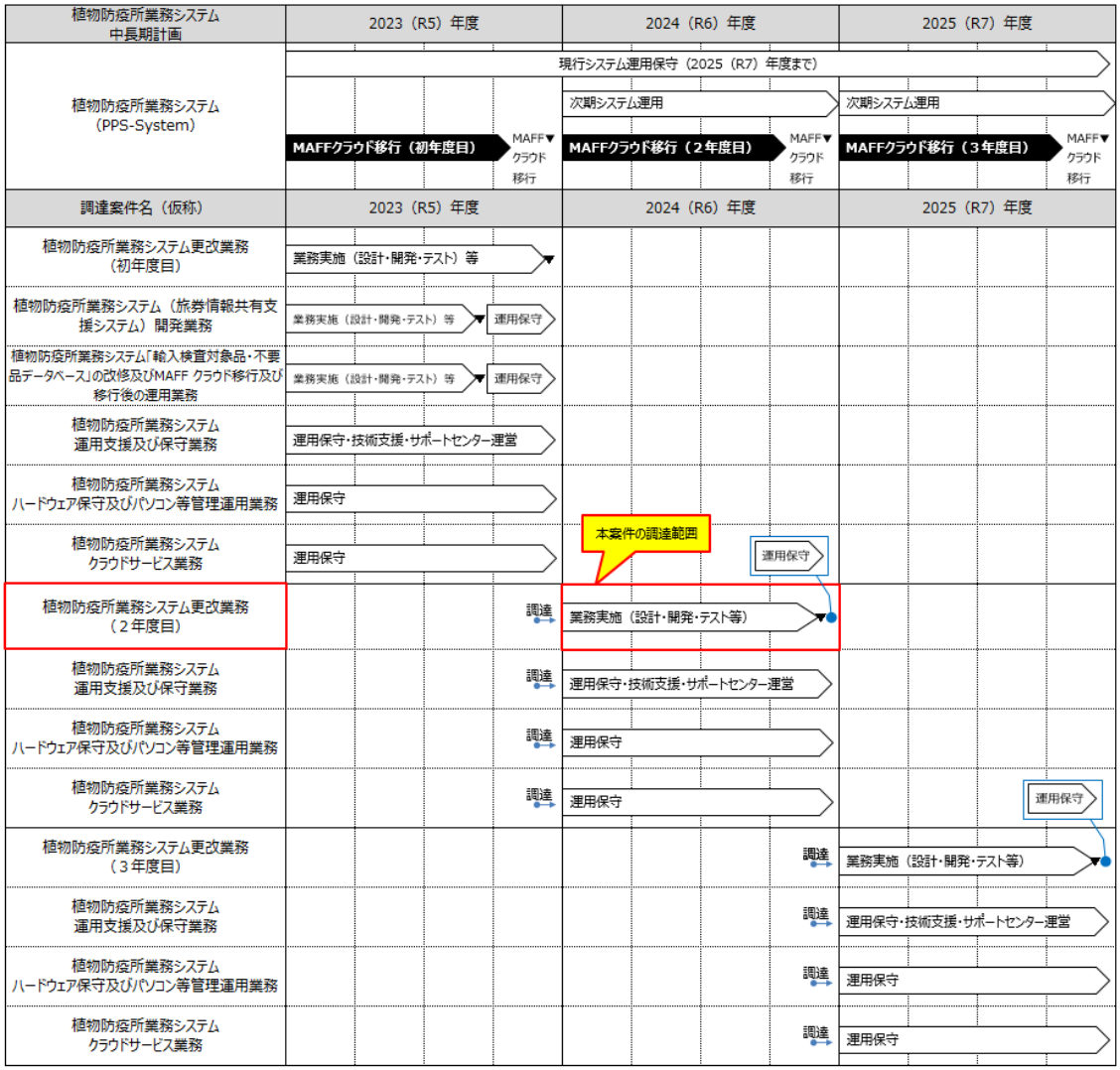

図 6 本調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等

3 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、以下を満たすこと。

また、本業務の対象であるシステムに係る開発について、受注者は以下に基づき設計に必要な要件を確認すること。

（1）パブリック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。

（2）パブリック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等、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。

（3）将来クラウドサービスプロバイダー（CSP）が変わっても、新たなクラウドサービスプロバイダー（CSP）が提供するクラウドへのデータ移行が容易に可能であること。

（4）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。

ア　運用管理

イ　死活監視

ウ　稼働状況監視

エ　セキュリティ監視

オ　ジョブ管理

カ　バックアップ管理

キ　ログ管理（送受信ログ等の保存）

ク　ウィルスパターン更新管理

ケ　セキュリティパッチ更新管理

コ　依頼作業対応

サ　構成管理

シ　文書管理

ス　アカウント管理

セ　データ管理

ソ　障害対応

タ　定例報告

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

ア　令和5年度の更改業務にて、植物防疫所業務システム（PPS-System）の一部サーバを MAFF クラウドへ移行している。その際に選定した、クラウドサービスプロバイダー（AWS）を利用すること。

イ　MAFF クラウド共通機能については利用を前提とし、詳細については MAFF クラウドの関係者と協議の上決定すること。

ウ　MAFF クラウドを利用する情報システム構築においては、クラウドサービスプロバイダー（CSP）が提供するサービスを活用することを基本とするが、提供サービス以外に必要な機能に関しては、MAFF クラウドにて選定しているクラウドサービスプロバイダー（CSP）が提供するクラウドサービス上に独自にシステム構築を行う。

4　作業の実施内容

（1）対象4サーバの MAFF クラウド移行及び各種ソフトウェアの更新等

ア　対象とするサーバは、植物防疫所業務システム（PPS-System）を構成するサーバ群の中のホームページサーバ、成田 Web サーバ、成田バーコード中継サーバ、Cotipa Web サーバの4サーバである。

イ　対象4サーバで利用している OS、ミドルウェア及びソフトウェア等については、最新

バージョンに更新を行い、それに伴い、正常に動作しないアプリケーションの改修を行うこと。また、OS 標準の機能で可能な機能については、フリーソフト等を使用しないこと。

ウ　対象４サーバで現在利用しているソフトウェアについては、「ソフトウェア情報」、MAFF クラウドのサーバ要件については、「新クラウドサーバスペック」に記載する。また、ソフトウェア名、バージョン及びサーバスペック等の開示については、応札希望者に対して機密保持契約を結んだ上で開示することとする。

エ　対象4サーバのうち成田 Web サーバについては、NACCS とオンライン連携しているため、当該サーバの MAFF クラウド移行及び各種ソフトウェアの更新については、NACCS との接続試験等を本調達の対象範囲として十分に考慮し対応すること。また、入札公告期間中の閲覧資料である参考1から5までを必読すること。

オ　NACCS の次期大規模更改を令和7年 10 月に控えた中で、次期 NACCS と植物防疫所業務システムの接続試験等が令和6年 10 月以降に予定されており、次期 NACCS と MAFF クラウド移行後の成田 Web サーバとの接続試験等についても、本調達の対象範囲として十分に考慮し対応すること。

カ　作業に際しては、デバイス類の更新作業及び成田検疫情報提供システムの改修により、従来の成田バーコード中継サーバが担っていた機能を新成田 Web サーバに包含することで対象2サーバを統合する等、成田検疫情報提供システムの構成等に関するベストプラクティスを提案・追及すること。

（2）通信機器等デバイス類の更新等

ア 対象とするデバイス類は、成田検疫提供システムを構成する通信機器等デバイス類である。

イ　入札公告期間中の閲覧資料である参考１：成田検疫提供システム通信機器等デバイス類一覧を基に、必要台数を調達すること。

ウ　調達後、所要のセットアップ作業を行い、成田検疫情報提供システムでの利用が可能な状態とすること。

エ　調達したデバイス類の搬入、設置、接続試験等に際して、横浜植物防疫所成田支所への配送又はオンサイト対応が生じた場合の費用については、全て本調達の範囲とすること。

オ　前項（1）カと同様に、当該作業に際しても、成田検疫情報提供システムの構成等に関するベストプラクティスを提案・追及すること。

カ　納入候補となる機器について、提案書、証明書等の提出期限までに、担当部署へ機器等リスト（区分（ノート PC 等）、製造業者名、製造業者の法人番号、製品名及び型番を記載したリスト）を提出することとし、農林水産省においてサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、速やかに担当部署に確認した上で、代替品の選定等、納入候補となる機器を見直すこと。

（3） 設計・開発実施計画書等の作成

受注者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、PJMO の指示に基づき、支援業者と調整の上、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、PJMO の承認を受けること。

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：2023 年 3 月 31 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。

（4） 設計

受注者は、現行の設計書及び入札公告期間中の閲覧資料の「MAFF クラウド利用ガイドライン」を参照して要件を確認した上で実施し、内容及び成果物について、PJMO の承認を得ること。

ア　受注者は、現行システムの稼働環境の調査・分析を行い、基本設計、詳細設計等既存の設計に基づき作業を行うこと。なお、当該調査・分析の結果、既存の設計に変更が生じる場合は既存の設計を修正した上で作業を行うこと。

イ　受注者は、プロジェクト開始後、速やかに MAFF クラウド CoE にシステム構成図案を提出し、レビューを受けること。また、レビュー結果の指摘内容をインフラの運用設計及び保守設計に反映させること。

ウ　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運用計画及び保守作業計画書兼実施要領（以下、「運用保守実施要領」という。）の案を作成し、PJMO の確認を受けること。

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

オ　受注者は、インフラの運用設計及び保守設計した結果を踏まえ、別途、設定につい

てのパラメータシートを作成し、PJMO に提出すること。

カ　受注者は、MAFF クラウド利用ガイドライン別紙 1_共通機能_利用申請書を作成し、担当部署と MAFF クラウド CoE の承認を受けること。プロジェクト期間中に利用申請書の内容が変更になった場合は、更新内容について、PJMO と MAFF クラウド CoE へ説明し、承認を受けること。

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

ク　受注者は、MAFF クラウドでサーバを利用するにあたり、ネットワーク設計、バックアップ設計、監視設計及び保守で使用するマニュアル等の作成を行うこと。

ケ　受注者は、設計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を変更すること。なお、選定理由書及び機能証明書に変更がある場合は修正すること。

コ　受注者は特にインフラの運用設計及び保守設計において、Shared 型の MSP(マネージドサービスプロバイダ)サービス等を活用した設計とすることで運用コストの低減に努めること。なお、Shared 型の MSP サービスの利用とは、以下の定義のいずれかとする。

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

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

③受注者が自社で Shared 型の MSP サービスを提供できない企業において外部企業が提供する MSP サービスの利用ではなく、複数の運用案件を受注することで自社内で運用サービスの改善共通化（サービスデスク、監視サービス等）に取組んでいること。

サ　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ー、支援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。

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

（5）開発・テスト

受注者は、OS 等ソフトウェアの更改等に伴い、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。

ア　受注者は、OS 等ソフトウェアの更改等に伴い、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。

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、移行後の環境において、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、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標準（標準コーディング規約、セキュアコーディング規約等）を定め、PJMO 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、PJMO 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、PJMO の承認を受けること。

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実施した各テストの実施状況及びテスト結果について、テスト計画時に作成した合否判定基準に基づく評価結果を PJMO に報告し、承認を受けること。

ク　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。

（6）受入テスト支援

ア　受注者は、PJMO が受入テストを実施するにあたり、受入テストケースを作成し PJMO の確認を受けること。

イ　受注者は、PJMO 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、PJMO 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、テスト計画書作成の支援を行うこと。

（7）情報システムの移行

ア　受注者は、現行環境から新本番環境へのシステムの移行を行うにあたり、移行計画書を作成し PJMO の承認を受けること。なお、移行は、AWS の仕様に準拠したデータ移行方式で行うものとする。

イ　受注者は、PJMO の移行判定を受けて、移行計画書に基づく移行作業を行うこと。

ウ　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、PJMO の承認を受けること。

エ　受注者は、上記ウの手順書に従い、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。

オ　移行計画書には、新本番環境への移行が失敗した場合を想定し、切り戻しを行う場合の手順も含めること。

カ　受注者は、移行した新本番環境に切り替え後、遅滞なくPJMO の承認を受けること。

キ　検証作業等でパブリッククラウド上に保管されたデータについては、ISMAP で規定された方法でデータが消去されていること、それが正しく運用されているか第三者による監査（PJMO による確認行為を含む。）により証明されていること。

（8）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ーのサービス（AWS の場合、AWS Systems Manager Session Manager 、AWS Systems Manager Fleet Manager）を利用すること。

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。

（9）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、農林水産省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、PJMO 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、担当部署と MAFF クラウド CoE 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、PJMO 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、PJMO 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。

（10）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 PJMO 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。なお、災害等の発生に備え、最低年１回は事前訓練を実施すること。

（11）引継ぎ

ア　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、現行及び次期の支援業者に対して確実な引継ぎを行うこと。

イ　受注者は、植物防疫所が別途、植物防疫所業務システムの更改を行う際には、当該更改業務の要件定義支援事業者、設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供、質疑応答等の協力を行うこと。

ウ　受注者は、次期の支援業者にパブリッククラウド上に構築された情報システムの引継ぎを行い、アカウントの契約を移管すること。

（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要領に基づき報告すること。

イ　PJMO 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（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、担当部署の承認を受けること。

（13）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。

イ　受注者は、植物防疫所が定める時期に、情報資産管理標準シートを提出すること。

ウ　受注者は、標準ガイドライン「別紙3　調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業」に基づき PJMO 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、PJMO が定める時期に、提出すること。

（ア）ハードウェアの管理

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

（イ）ソフトウェアの管理

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

（ウ）回線の管理

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

（エ）外部サービスの管理

情報システムを構成するクラウドコンピューティングサービス等の外部サービスの外部サービス利用形態、使用期間等

（オ）施設の管理

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

（カ）公開ドメインの管理

情報システムが利用する公開ドメインの名称、DNS名、有効期限等

（キ）取扱情報の管理

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

（ク）情報セキュリティ要件の管理

情報システムの情報セキュリティ要件

（ケ）指標の管理

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

（コ）各データの変更管理

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

（サ）作業実績等の管理

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

（シ）スケジュールや工数の管理

スケジュールや工数等の計画値及び実績値

（14）植物防疫所業務システム（PPS-System）のセキュリティ要件の点検支援

受注者は、植物防疫所が行う内閣サイバーセキュリティセンター（NISC）が提供する「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」の「同　マニュアル活用ワークシート」による点検を行う場合は、ワークシート作成等に対する支援を行うこと。

(15)成果物

ア　成果物名

本業務の成果物を以下に示す。

表 3 成果物一覧

No.	成果物名	内容及び 納品数量	納品期日 （原則）
1	設計・開発実施計画書	標準ガイドライン実務手引書第3編「第7章 設計・開発」の設計・開発実施計画書の記載内容等を踏まえ作成する。	契約締結後20日以内
2	設計・開発実施要領		
3	情報セキュリティ管理計画書		契約締結後20日以内
4	選定理由書及び機能証明書	現行システムのソフトウェア及び選定したソフトウェアについて、バージョン、選定した理由等を記載したもの。	契約締結後20日以内
5	影響調査書	更改に伴う影響範囲の調査結果を記載したもの。	契約締結後20日以内
6	MAFFクラウド利用ガイドライン別紙1_利用申請書	新本番環境及び検証環境を構築するためのIPアドレスや連携システムを記載したもの。	MAFFクラウドCoEに環境構築を依頼する2週間前まで
7	標準コーディング規約		開発段階の1週間前まで
8	脆弱性検査結果報告書		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）
9	テスト計画書及びテストケース		各テスト開始の2週間前まで
10	テスト結果報告書		各テスト終了後2週間以内
11	移行計画書及び移行手順書	システムの移行の方法、環境、ツール、段取り及び移行が失敗した場合の切り戻し手順等を記載したもの。	移行の2週間前まで
12	移行結果報告書		移行終了後2週間以内
13	運用保守実施要領		時期についてはPJMOと協議するものとする
14	運用保守作業報告書		時期についてはPJMOと協議するものとする
15	各種設計書類 新規：ネットワーク設計 新規：バックアップ設計 新規：監視設計	本案件業務に関連する全ての設計書について、既存の資料を差し替えるところ。差分のみの提出は不可とする。	MAFFクラウドでの環境構築の2週間前まで
16	各種マニュアル等 新規：保守マニュアル	本案件業務に関連する全てのマニュアルについて、変更がない場合でも既存の資料と差し替えること。差分のみの提出は不可とする。	次期の運用支援保守業者に引き渡す2週間前まで
17	プログラム及びプログラムソース一式	新本番環境の稼働機器上の記録媒体に、システムが正常に稼働する状	時期についてはPJMOと協議するものとする

		態で格納及び電磁的記録媒体に格納し納品すること。	
18	引継書	標準ガイドライン実務手引書「第3編 第7章 設計・開発」の引継ぎに示されているもの。	次期の運用支援保守業者に引き渡す2週間前まで
19	契約金額内訳		契約後遅滞なく
20	情報資産管理標準シート		更新が必要な都度PJMOと協議の上決定するものとする
21	外部サービスを利用する場合、当該サービスに係る設定情報その他の必要な情報一式		サービス利用開始予定の1週間前まで

イ　成果物の納品方法

- 成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
- 用字・用語・記述符号の表記については、「「公用文作成の考え方」の周知について（令和 4 年 1 月 11 日内閣文第 1 号内閣官房長官通知）」を参考にすること。
- 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。
- 成果物は紙媒体又は電磁的記録媒体により作成し、植物防疫所から特別に示す場合を除き、原則紙媒体は1部、電磁的記録媒体は2部を納品すること。
- 紙媒体による納品について、用紙のサイズは、原則として日本産業規格 A 列4番とするが、必要に応じて日本産業規格 A 列3番を使用すること。
- 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。
- 納品後、植物防疫所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。
- 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、PJMO の承認を得ること。
- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 電磁的記録媒体により納品する場合は、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、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

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、植物防疫所が納

品場所を別途指示する場合はこの限りではない。

〒231-0003

横浜市中区北仲通 5-57　横浜第2合同庁舎内

横浜植物防疫所　総務部会計課調達係

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 PJMO と協議することができるものとする。

5　作業の実施体制・方法

（1）作業実施体制

本業務の推進体制及び本業務受注者に求める作業実施体制は次の図及び表のとおりである。

なお、受注者内の人員構成については想定であり、受注者決定後に PJMO と協議の上、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。

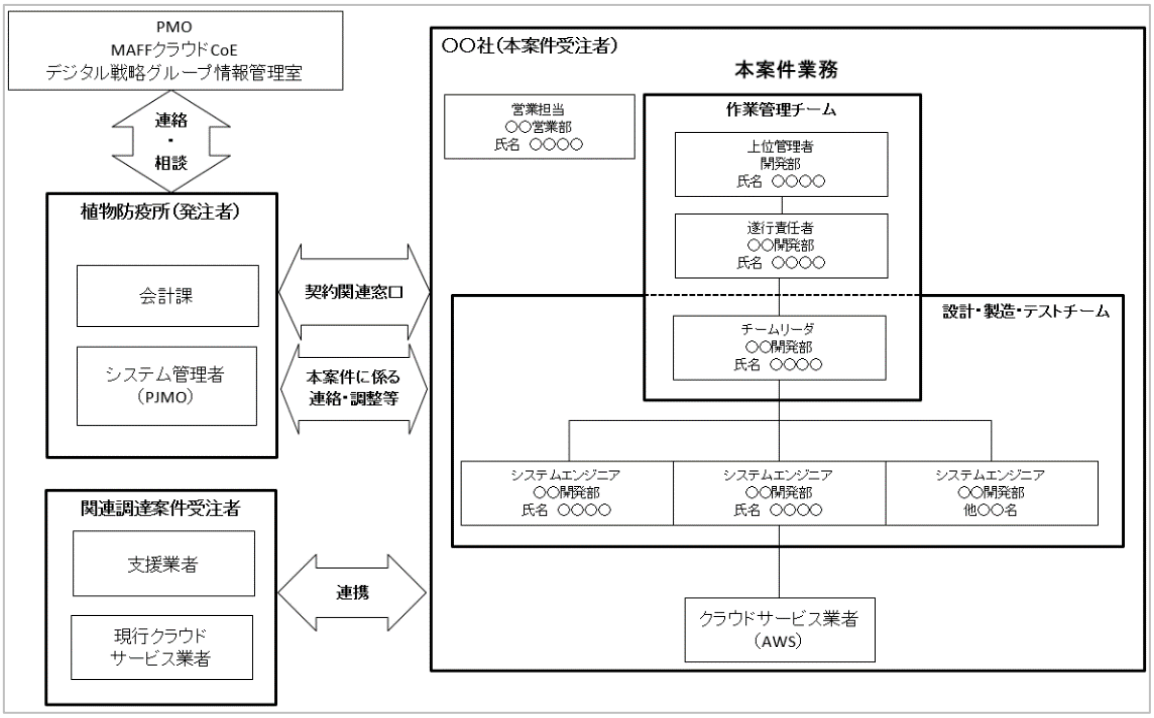

図 7 本案件業務の推進体制及び本案件業務受注者に求める作業実施体制

表 4 本案件業務における組織等の役割

組織等	本案件業務における役割
植物防疫所 会計課	本契約関係の事務を担当する。
植物防疫所 PJMO	植物防疫所業務システム（PPS-System）の管理組織として、本案件

組織等	本案件業務における役割
	業務の進捗等を管理する。
本案件業務受注者	本案件業務を実施する。
PMO	農林水産省の全体管理組織。クラウド利用を含む情報システムに関する担当部署からの問い合わせを受け、対応、助言・指導等を行う。
MAFFクラウドCoE	PJMO・受注者に対して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。
MAFFクラウド事業者	MAFFクラウドの運用及び移行業務への支援を行う。
支援業者	植物防疫所業務システム運用支援及び保守業務の受注者。PJMOを通じて、現行及び次期植物防疫所業務システム（PPS-System）の工程管理、情報提供等に係る支援・保守を行う。
クラウドサービス業者	植物防疫所と契約し、植物防疫所業務システム（PPS-System）が稼働する現行クラウドの運用を行う。

表 5 本案件業務受注者に求める作業実施体制の役割

組織等	本案件業務における役割
遂行責任者	• 本案件業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。 • 原則として全ての進捗会議及び品質評価会議に出席する。
チームリーダ	本案件業務及びサブシステムに関する設計・開発において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
設計・開発担当者	本案件業務及びサブシステムに関する設計・開発を担う。
テスト担当者	本案件業務及びサブシステムに関するテストを担う。
品質管理者	本案件業務全体において所定の品質を確保するため、監視・管理を担う。
情報管理責任者	本案件業務の情報取扱い全てに関する監督を担う。

（2） 作業要員に求める資格等の要件

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

イ 受注者における遂行責任者は、情報処理技術者試験のうちプロジェクトマネージャ試験の合格者又は技術士（情報工学部門又は総合技術監理部門（情報工学を選択科目とする者））の資格を有すること。

ウ チームリーダは、情報システムの設計・開発又はシステム基盤導入の経験年数を3年以上有すること。また、その中でリーダクラスとしての経験を3件以上有すること。

エ 設計・開発に関わるメンバのうち、情報システムの設計・開発等の情報処理業務の

経験年数が5年以上の者又は同等の実績を有する者を3分の1以上配置すること。
また、以下の経験を有するメンバを参画させること。

（ア） Windows 系 Web システムに関する開発又は運用経験があること。

（イ） Linux 系 Web システムに関する開発又は運用経験があること。

（ウ） Oracle データベースに関する開発又は運用経験があること。

（エ） PostgreSQL データベースに関する運用経験があること。

オ　設計・開発を行う担当者には、情報処理技術者試験のうち、次に掲げる試験区分の合格者を1名以上必要な人数含むこと。なお、同一人が全ての試験区分に合格していることを求めるものではない。

（ア） システムアーキテクト試験

（イ） データベーススペシャリスト試験

（ウ） ネットワークスペシャリスト試験

カ　設計・開発を行う担当者には、情報処理安全確保支援士の登録を受けている者又は同等の資格を有する者を含むこと。
パブリッククラウドを利用する情報システムの要件定義、設計開発等を担当するチームのチームリーダ及び担当メンバは以下の資格を有するものを含めること。

（ア） チームリーダは、パブリッククラウドに係る全ての技術領域において当該クラウドサービスプロバイダーの認定技術者として上級資格（例：AWS Certified Solutions Architect – Professional）を有する者を 1 名以上配置すること。なお、チームリーダの資格は全体リーダまたはパブリッククラウド上での情報システム構築期間中に専任でチームリーダを支援する要員が保有していることでも可とする。または、クラウドサービスプロバイダーが提供するサポートサービス（AWS プロフェッショナルサービス）の利用での対応も可とする。

（イ） 担当メンバは、パブリッククラウドに係る全ての技術領域において当該クラウドサービスプロバイダーの認定技術者としての中級資格（例：AWS Certified Solutions Architect – Associate）以上を有する者を 1 名以上配置すること。

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

（ア） 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

（イ） 課題・改善点を識別し、改善する能力

（ウ） 本業務を履行するうえで適当な AWS のスキル

（3） 作業場所

本案件業務の作業場所及び作業に当たり必要となる設備（クラウドサービスを含む）、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、必要に応じて植物防疫所担当職員による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

受注者は、PJMO 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。

6　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　PJMO 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、本案件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、本案件業務に関する影響分析を行うこと。

イ　本案件業務に係る情報セキュリティ要件は次の通りである。

（ア） 委託した業務以外の目的で利用しないこと。

（イ） 業務上知り得た情報について第三者への開示や漏えいをしないこと。

（ウ） 持出しを禁止すること。

（エ） 受注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、必要に応じて植物防疫所による実地調査が実施できること。

ウ　上記以外に、「別紙1　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植物防疫所と協議の上

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　本案件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、PJMO 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、本案件業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当職員に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。

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

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

（3）法令等の遵守

本案件業務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）、関連する環境関係法令（労働安全衛生法（昭和 47 年法律第 57 号））等）、等を遵守し履行すること。

（4）標準ガイドラインの遵守

本案件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エに基づくこと。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-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン
エ DS-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

（5） その他文書、標準への準拠

ア プロジェクト計画書等

本案件業務の遂行に当たっては、担当部署が定めるプロジェクト計画書及びプロジェクト管理要領との整合を確保して行うこと。

イ プロジェクト標準

開発に当たっては、植物防疫所業務システム（PPS-System）の現行のコーディング規約に準拠して作業を行うこと。

ウ アプリケーション・コンテンツの作成規程

（ア） 提供するアプリケーション・コンテンツに不正プログラムを含めないこと。
（イ） 提供するアプリケーションにぜい弱性を含めないこと。
（ウ） 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
（エ） 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。
（オ） 提供するアプリケーション・コンテンツの利用時に、ぜい弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。
（カ） サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。
（キ） 「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。なお、ドメインを新規に導入する場合又はドメインを変更等する場合は、担当部署から農林水産省ドメイン管理マニュアルの説明を受けるとともに、それに基づき必要な作業を行うこと。
（ク） 詳細については、担当部署から「アプリケーション・コンテンツの作成及び提供に

関する規程」の説明を受けるとともに、それに基づきアプリケーション・コンテンツの作成及び提供を行うこと。

（6） 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。

（7） 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を提出し、PJMO と協議の上、PJMO の承認を受けること。対応方針については、設計・開発実施計画書及び設計・開発実施要領に記載することも可能とする。

なお、既存のシステムについては、アクセスする情報等を検討し、PJMO と協議の上、可能な範囲で対応するものとする。

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 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。

ウ 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。

エ 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。

オ 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。

カ 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「5.5. 本案件業務における管理運営」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。

キ SC-1-1 委託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、受託者は情報セキュリティ監査を受け入れること。

また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。

ク クラウドアーキテクトのベストプラクティス（AWS Well-Architected Framework）及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 別冊クラウド設計・開発編」に準拠すること。

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すること。

・別紙2 AWS 設定確認リスト

・別紙3 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

7 成果物の取扱いに関する事項

（1） 知的財産権の帰属

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

イ 植物防疫所は、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、複製等により植物防疫所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。

ウ 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植物防疫所の承認を得ることとし、植物防疫所は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら植物防疫所の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、植物防疫所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。

エ　本調達に係るプログラムに関する権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、植物防疫所から受注者に対価が完済されたとき受注者から植物防疫所に移転するものとする。

オ　受注者は植物防疫所に対し、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。

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

（2）契約不適合責任

ア　植物防疫所は検収完了後、成果物についてシステム仕様書との不一致（バグも含む。以下「契約不適合」という。）が発見された場合、受注者に対して当該契約不適合の修正等の履行の追完（以下「追完」という。）を請求することができ、受注者は、当該追完を行うものとすること。ただし、植物防疫所が追完の方法についても請求した場合であって、植物防疫所に不相当な負担を課するものでないときは、受注者は植物防疫所が請求した方法と異なる方法による追完を行うことができること。

イ　前記アにかかわらず、当該契約不適合によっても本契約の目的を達することができる場合であって、追完に過分の費用を要する場合、受注者は前記アに規定された追完に係る義務を負わないものとすること。

ウ　植物防疫所は、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こと。

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

オ　受注者が本項に定める責任その他の契約不適合責任を負うのは、検収完了後１年以内に植物防疫所から当該契約不適合を通知された場合に限るものとすること。ただし、検収完了時において受注者が当該契約不適合を知り若しくは重過失により知

らなかったとき、又は当該契約不適合が受注者の故意若しくは重過失に起因するときにはこの限りでない。

カ　前記アからオまでの規定は、契約不適合が植物防疫所の提供した資料等又は植物防疫所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、納品期日までに植物防疫所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、変更点について植物防疫所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。

8　入札参加資格に関する事項

（1）競争参加資格

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

イ　公告日において令和4・5・6年度全省庁統一資格の「役務の提供等」の「A」又は「B」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。

ウ　上記「5(2)作業要員に求める資格等の要件」を満たすこと。

（2）公的な資格や認証等の取得

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

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

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

イ　応札者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。

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

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

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

（3）受注実績

ア　応札者は、拠点数 10 以上のネットワークを構築した実績を過去3年以内に有すること。

イ　応札者は、100 名以上の職員が利用するデータベース登録・検索機能を有する情報システムの設計・開発を行った実績を過去3年以内に有すること。

（4）複数事業者による共同入札

ア　複数の事業者が共同入札する場合、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入札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　共同入札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　共同入札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入札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。

（5）入札制限

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

9　再委託に関する事項

（1）再委託の制限及び再委託を認める場合の条件

ア　本案件業務の受注者は、業務を一括して又は主たる部分を再委託してはならない。

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

ウ　受注者は再委託先の行為について一切の責任を負うものとする。

エ　再委託先における情報セキュリティの確保については受注者の責任とする。

オ　再委託を行う場合、再委託先が「８（５）入札制限」に示す要件を満たすこと。

（2）承認手続

ア　本案件業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を植物防疫所に提出し、あらかじめ承認を受けること。

イ　前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を植物防疫所に提出し、承認を受けること。

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

（3）再委託先の契約違反等

再委託先において、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、植物防疫所は、当該再委託先への再委託の中止を請求することができる。

10 その他特記事項

（1）前提条件等

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

イ　令和6年 10 月から令和7年3月の期間は、担当部署の繁忙期に当たるため、担当職員のプロジェクトへの関与が十分にできなくなる恐れがあることに留意すること。

ウ　本案件業務受注後に調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって植物防疫所に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が確認することによって変更を確定する。

エ　本仕様書について疑義等がある場合は、「別紙6　質問書」により質問すること。なお、質問書に対する回答は適宜行うこととする。

（2）入札公告期間中の資料閲覧等

本案件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、

植物防疫所内にて閲覧可能とする。なお、本案件業務の入札参加希望者は応札前までに必ずこれらの資料を閲覧し、植物防疫所業務システム及び本案件業務について、その内容をよく理解しておくこと。また、資料の閲覧に当たっては、必ず事前に当所会計課まで連絡の上、閲覧日時を調整すること。

ア　資料閲覧場所

〒231-0003

神奈川県横浜市中区北仲通 5-57 横浜第 2 合同庁舎内

イ　閲覧期間及び時間

（ア）令和6年2月5日から令和6年3月14日まで

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

ウ　閲覧手続

最大3名まで。応札希望者の商号、連絡先、閲覧希望者氏名を「別紙4　資料閲覧申請書」に記載の上、閲覧希望日の3日前までに提出すること。また、閲覧日当日までに「別紙5　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。なお、MAFF クラウドを利用する場合は、資料閲覧時に守秘義務に関する誓約書を提出した事業者に、次のカの（サ）の資料についてデータで提供することは可能である。必要に応じて申し出ること。

オ　連絡先

横浜植物防疫所総務部会計課　　電話 045-211-7151

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）参考1から5の資料

（イ）過去の監査結果

（ウ）ソフトウェア情報

（エ）新クラウドサーバスペック

（オ）植物防疫所業務システム（PPS-System）運用・保守計画及び運用・保守実施要領

（カ）現行のコーディング規則等

（キ）遵守すべき各府省独自の規定類

・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

・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

（ク）現行の情報システムの情報システム設計書、操作マニュアル

（ケ）関連する他の情報システムの操作マニュアル、設計書、各種プロジェクト標準

（コ）過去の検討資料等

（サ）農林水産省クラウド利用ガイドライン及び関係資料

（3）その他

本仕様書について疑義等がある場合は、「別紙6　質問書」により質問すること。なお、質問書に対する回答は適宜行うこととする。

11　附属文書

（1）別紙1　情報セキュリティの確保に関する共通基本仕様

（2）別紙2　AWS 設定確認リスト

（3）別紙3　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

（4）別紙4　資料閲覧申請書

（5）別紙5　守秘義務に関する誓約書

（6）別紙6　質問書

以　上

（別紙１）

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

（4）MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績

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

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

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

（6）本業務における情報セキュリティ対策の履行状況を定期的に報告すること。

（7）農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、農林水産省又は農林水産省が選定した事業者による立入調査等の情報セキュリティ監査（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 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。

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

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

（10）情報セキュリティ対策の履行が不十分な場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。

２　受託者は、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。

３　受託者は、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。

４　受託者は、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、本業務上不要

となったとき若しくは本業務の終了までに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。

Ⅳ　情報システムの各工程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、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）農林水産省内通信回線への端末の接続を監視する機能

（エ）端末への外部電磁的記録媒体の挿入を監視する機能

（オ）サーバ装置等の機器の動作を監視する機能

（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。

２　受託者は、本業務において情報システムの設計・開発を行う場合には、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　ソフトウェアに関する脆（ぜい）弱性等対策
ケ　不正プログラム対策
コ　サービス不能攻撃対策
サ　標的型攻撃対策
シ　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
ス　政府ドメイン名（go.jp）の使用
セ　不正なウェブサイトへの誘導防止
ソ　農林水産省外のアプリケーション・コンテンツの告知

（２）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分離して実施すること。
イ　試験項目及び試験方法を定め、これに基づいて試験を実施すること。
ウ　試験の実施記録を作成し保存すること。

（３）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　ソースコードが不正に変更されることを防止するため、ソースコードの変更管理、アクセス制御及びバックアップの取得について適切に管理すること。
イ　調達仕様書等に規定されたセキュリティ実装方針に従うこと。
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に、情報システムの設計及びソースコードを精査する範囲及び方法を定め実施すること。
エ　オフショア開発を実施する場合、試験データとして実データを使用しないこと。

３　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。

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、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。

（１）情報システムの運用環境に課せられるべき条件の整備
（２）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
（３）情報システムの保守における情報セキュリティ対策
（４）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
（５）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
（６）「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：2023 年 3 月 31 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。

（7）情報システム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、サポート継続中の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情報システムの改修等

5　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、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。

（1）情報セキュリティに関わる運用保守体制の整備

（2）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

（3）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

6　受託者は、本業務において情報システムのセキュリティ監視を行う場合には、以下の内容を含む監視手順を定め、適切に監視運用すること。

（1）監視するイベントの種類

（2）監視体制

（3）監視状況の報告手順

（4）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

（5）監視運用における情報の取扱い（機密性の確保）

7　受託者は、本業務において運用中の情報システムに脆（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。

8　受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する府省庁等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体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　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、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すること。

10　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　クラウドサービス等外部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、クラウドサービス等外部サービスを活用する場合には、外部サービス毎に以下の措置を講じること。また、当該外部サービスの活用が本業務の再委託に該当する場合は、当該外部サービスに対して、Ⅸの措置を講じること。

１　外部サービス条件

（１）外部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）外部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）クラウドサービスの場合、ペネトレーションテストや脆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。

２　ISMAP 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であること。

３　ISMAP 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。

４　クラウドサービス以外の外部サービスの場合は、以下の措置を講じること。

（１）外部サービスの利用を通じて農林水産省が取り扱う情報の外部サービス提供者における目的外利用の禁止。

（２）外部サービスの提供に当たり、外部サービス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）。

（３）外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部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。

（４）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。

（５）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。

（６）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。

（７）外部サービス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外部サービス提供者と合意し、定められた手順により情報を取り扱うこと。

Ⅵ　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。

Ⅶ　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、以下の措置を講じること。

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）

Ⅷ　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。

Ⅸ　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及びⅢ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。

Ⅹ　資料等の提出

上記Ⅱの1、Ⅱの2、Ⅲの1、Ⅴの4（2）、4（3）、Ⅶの1及びⅦ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、総合評価落札方式にあっては提案書等の総合評価のための書類に添付して提出すること。

Ⅺ　変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ、Ⅶ及びⅨ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。

AWS設定確認リスト

凡例：〇：責任者、△：サポート

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

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４

農林水産省横浜植物防疫所　宛

資料閲覧申請書

「植物防疫所業務システム更改業務」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５

農林水産省横浜植物防疫所　宛

守秘義務に関する誓約書

「植物防疫所業務システム更改業務」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

別紙６

植物防疫所業務システム更改業務　質問表

事業者名：
日付：　　令和　　年　　月　　日

No.	資料名	頁	仕様書の該当記載内容	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					

植物防疫所業務システム更改業務の応札資料作成要領

本書は、植物防疫所業務システム更改業務の調達に係る応札資料（評価項目一覧及び提案書）の作成要領を取りまとめたものである。

１　応札者が提出すべき資料

この要領に基づき、応札者は、下表に示す資料を作成し提出する。

資料名称	資　料　内　容
誓約書	仕様書に記載されている要件を遵守する旨の誓約書
評価項目一覧（総合評価項目表）	発注者が提示する評価項目一覧の提案書頁番号欄に該当する提案書の頁番号を記載したもの
提案書（設計･開発実施計画書案及び設計･開発実施要領案）	仕様書に記載されている要件をどのように実現するかを提案書にて説明したもの。主な項目は以下のとおり ○　応札者が提案する要件確認、設計・開発、テスト、運用・保守の内容、体制、波及効果等 ○　実施計画 ○　応札者の資格 ○　業務従事者リスト ○　当該業務従事者に係る履歴資料 ○　保護すべき情報の取扱いに関する資料 ○　補足資料（応札者の実績の詳細）等

（注）応札者は、上記以外に、通常の一般競争入札と同様、入札書、参加資格を満たしていることを証明する資格審査結果通知書（全省庁統一資格）の写し等を提出しなければならない。

２　誓約書の作成

仕様書に記載されている要件を遵守する旨の誓約書を作成し、発注者に提出すること（様式自由）。

３　評価項目一覧の作成

(1) 評価項目一覧の構成

評価項目一覧の構成は、下表のとおり。

事　項	概　要　説　明
提案要求事項	提案を要求する事項。これらの事項については、応札者が提出した提案書について、各提案要求項目の必須項目及び任意項目を区分し、得点配分の定義に従いその内容を評価する。 例：業務の内容、実施計画等
添付資料	応札者が作成した提案の詳細を説明するための資料。これら自体は、直接評価されて点数を付与されることはない。

	例：実施体制及び担当者略歴、会社としての実績

(2) 提案要求事項

評価項目一覧中の提案要求事項における各項目の説明は下表のとおり発注者が作成し提示する「評価項目一覧（提案要求事項）」における「提案書頁番号」欄に該当頁を記載すること。

項目名	項目説明・記載要領	記載者
評価項目	事業内容に応じて定める評価項目	発注者
評価基準	事業内容に応じて定める評価基準	発注者
評価区分	必須項目と任意項目の別の区分	発注者
得点配分	各項目に対する最大得点	発注者
提案書頁番号	応札者が作成する提案書における該当頁番号を記載する。	応札者

(3) 添付資料

評価項目一覧中の添付資料における各項目の説明は下表のとおり

項目名	項目説明・記載要領	記載者
資料項目	事業内容に応じて定める資料項目	発注者
資料内容	応札者に提案を要求する資料の内容	発注者
提案の要否	必ず提案すべき項目（必須）又は必ずしも提案する必要のない項目（任意）の区分が設定されているもの。評価基準とは異なり、採点対象とはしない。	発注者
提案書頁番号	応札者が作成する提案書における該当頁番号を記載する。	応札者

4 提案書の作成

(1) 提案書様式

ア　提案書は、提案書雛型を参考にして、10部作成する。

イ　提案書は、Ａ４版カラーとし、特別に大きな図面等が必要な場合には、原則としてＡ３版カラーとする。

ウ　提出物は、紙資料とともに電子メール、大容量ファイル転送システム等により電子媒体でも提出する。その際のファイル形式は、Ms-Word、Ms-PowerPoint、MS-Excel又はPDF形式とする（これにより難い場合は、発注者まで申し出ること）。

なお、電子媒体についてはウイルス対策を施して、使用したソフトウェア情報及び実施日時をラベル面に記載して提出すること。

(2) プレゼンテーション

ア　応札者はプレゼンテーション形式による提案書の説明を行うこと。プレゼンテーションの時間は説明15分、質疑応答15分、計30分とする。

イ　実施日時等の詳細は、提出期限以降に連絡する。

(3) 提案書作成に当たっての留意事項

ア　提案書を評価する者が特段の専門的知識、商品に関する一切の知識を有しなくても評価が可能な提案書を作成すること。

　なお、必要に応じて用語解説などを添付すること。

イ　提案に当たって、特定の製品を採用する場合は、当該製品を採用する理由を提案書に記載するとともに、記載内容を証明又は補足するものとしてパンフレット、比較表等を添付すること。

ウ　応札者は、提案内容をより具体的・客観的に説明するための資料として添付資料を提案書に含めて提出すること。

　なお、添付資料は、提案書本文と区分できるようにすること。

エ　発注者から連絡が取れるように、提案書には担当者の氏名及び連絡先（電話番号、メールアドレス）を明記すること。

オ　提案書を作成するに当たり発注者に対し質問等がある場合には、別紙の質問状に必要事項を記載の上、令和６年３月14日（木）午後５時までに横浜植物防疫所総務部会計課に提出すること。

　横浜植物防疫所総務部会計課調達係

　担当：小林、牧野

　電話：045-211-7151

カ　提案書の様式及び留意事項に従った提案書ではないと発注者が判断した場合には、提案書の評価を行わないことがあるので留意すること。

　なお、補足資料の提出、補足説明等を発注者が求める場合があるので、併せて留意すること。

キ　提案書等の提出書類の作成及び提出に係る費用は、応札者の負担とする。

ク　提出された提案書等の返却はしない。

別紙

質　　問　　状

社　名	
住　所	
ＴＥＬ	
質問者	
質問に関連する文書名及び頁	
質問内容	

評　価　手　順　書

本書は、植物防疫所業務システム更改業務の調達に係る評価手順を取りまとめたものである。落札方式及び評価の手続は以下のとおり

１　落札方式及び得点配分

(1) 落札方式

次の要件を全て満たしている者のうち数値の最も高い者を落札者とする。

○　入札価格が予定価格の範囲内であること。

○　「評価項目一覧」に記載される要件のうち必須とされた項目を全て満たしていること。

(2) 総合評価点の計算

総合評価点　＝　技術点　＋　価格点

技術点＝基礎点＋加点

価格点＝（１－入札価格／予定価格）×価格点の配分

(3) 得点配分

技術点に関し、必須項目及び任意項目の配分を７点及び４５３点とし、価格点の配分を２３０点とする。

技術点（必須項目）	７点
技術点（任意項目）	４５３点
価格点	２３０点

２　技術点の加点方法

(1) 技術点の構成

技術点は、基礎点と加点に分かれており、基礎点は評価項目のうちの必須項目、加点は評価項目のうちの任意項目となっている。

(2) 基礎点

基礎点は、評価項目のうちの必須項目にのみ設定されている。

基礎点は、要件を満たしているか否かを判断するため、満たしていれば満点、満たしていなければ０点のいずれかとなる。

なお、満たしていない項目が一つでもあれば、不合格となる。

(3) 加点

加点は、評価項目のうちの任意項目に設定されている。

加点は、評価基準に照らしその充足度に応じて点数が付されるため、基礎点と異なり様々な点数となる。

３　評価の手続

(1) 一次評価

まず、以下の事項について評価を行う。

○　誓約書が提出されているか。

○　「評価項目一覧（提案要求事項）」で評価区分欄が必須とされている項目に対して提案書頁番号欄に頁番号が記載されているか。

○　「評価項目一覧（添付資料）」で提案の要否欄が必須とされている項目に対して提案書頁番号欄に頁番号が記載されているか。

(2) 二次評価

一次評価で合格した提案書に対し、「評価項目一覧（提案要求事項）」に記載している評価基準に基づき採点を行う。

なお、複数の評価者のうち１人でも「評価項目一覧」に記載される要件のうち必須とされた項目を満たしていないと判断した場合には、不合格とする。

また、複数の評価者がいる場合の技術点の算出方法は、各評価者の評価結果（点数）を合計し、それを平均して技術点を算出する。

(3) 総合評価点の算出

上記（２）により算出した技術点と上記１（２）により計算した価格点を合計して、総合評価点を算出する。

様式５号

誓　約　書

支出負担行為担当官
横浜植物防疫所長　殿

「植物防疫所業務システム更改業務」の一般競争入札に参加するにあたり、入札説明書、仕様書及び入札心得に記載されている要件を遵守することを誓約します。

令和　　年　　月　　日

住　　所
商号又は名称
代 表 者 氏 名

提　案　書　雛　形

事業名　植物防疫所業務システム更改業務

本調達案件の概要
調達の背景や目的についての理解
本案件と関連調達案件等に関する理解
システムへの理解
業務の実施内容に関する提案
業務の実施内容（要件確認）
作業実施計画（実施スケジュールの作業分解構成図（WBS）（概要）を入れ、プレゼンテーション時に簡潔に説明のこと）
設計
開発・テスト
運用・保守
作業の実施体制・方法
作業実施体制等（作業実施体制図は担当者名（予定）を入れ、プレゼンテーション時に簡潔に説明のこと）
作業要員に求める資格等の要件
作業場所
作業の管理に関する要領
その他
全体を通じての有益な提案（仕様書の不足点や追加対応内容等。プレゼンテーション時に簡潔に説明のこと）
ワーク・ライフ・バランス等の推進(総合評価項目表に記載のこと)

マイナンバーカードの利活用等(総合評価項目表に記載のこと)
賃上げの実施を表明した企業等(総合評価項目表に記載のこと)
デジタルスタートアップ(総合評価項目表に記載のこと)

社　　名　　等	
担 当 者 氏 名	
電　話　番　号	
メールアドレス	

令和６年度植物防疫所業務システム更改業務　総合評価項目表

	評価内容
＜必須項目＞ 「必須」	「仕様を満たしている」　：「合格（○）」（配点15点） 「仕様を満たしていない」：「不合格（×）」
＜加点項目＞ 「重要度」 （大、中、小）	相対的評価 / 評価区分（重要度）：大 / 中 / 小 A　相対的に優れている（３倍）：４５点 / ３０点 / １５点 B　相対的に平均である（２倍）：３０点 / ２０点 / １０点 C　相対的に劣っている（１倍）：１５点 / １０点 / ５点 D　提案自体がないもの（０倍）：０点 / ０点 / ０点

No	仕様書該当箇所	評価項目	評価基準	提案内容・ポイント	提案書における記述場所	評価区分	配点配分 合計（最大）	加点基準点	加重（倍）
	1　調達案件の概要、2　調達案件及び関連調達案件、3　情報システムに求める要件								
1	1（2） 1（3）	本調達案件の背景や目的についての理解度	本調達の背景として、政府全体の動きとそれを踏まえた農林水産省（植物防疫所）の目的や狙い、取組の状況について正しく理解した上で、提案に臨んでいるか[必須]			必須	-	-	-
2	1（6） 2（1） 2（2）	本案件と関連調達案件等に関する理解度	本案件及び各関連調達案件との関係性を正しく理解した上で、本案件の位置付けを正しくとらえているか［加点］			大	45	15	0～3
3	1（4） 3	システムへの理解度	本システムへの理解が十分であることが分かるか、あるいは理解を深めようとするための具体的な提案が確認できるか［加点］			大	45	15	0～3
	4　業務の実施内容								
4	4（1） 4（2）	業務の実施内容についての理解度	当省（当所）の求める業務内容が漏れなく提案されているか。［必須］			必須	-	-	-
5	4（3）	具体的な作業実施計画の策定	設計・開発実施計画書に記載すべき事項を正しく理解した上で、個々の改修の期日を踏まえた計画の策定について具体的な案を提示しているか。［加点］			中	30	10	0～3
6	4（4）	設計	現行システムの現状と設計書等との不整合がある可能性を踏まえ、システムの現状把握をした上で設計をすることが示されているか［加点］ 改修した内容を確実にドキュメントに反映させる手順について提案されているか［加点］			大	45	15	0～3
7	4（5）	開発・テスト	改修要件ごとの実装期限を理解した上で計画的に開発していく提案があるか［必須］			必須	-	-	-
8	4（8） 4（9） 4（10）	運用・保守	本調達案件では、MAFFクラウドへの移行が完了した後の当該年度末までの運用・保守を含むため、運用・保守に関する提案がなされているか［必須］			必須	-	-	-
9	4（11）	引継ぎ	定めた時期までに引継ぎ書面を作成する必要があることを認識したスケジュールになっていることが提案されているか［加点］			小	15	5	0～3
10	4（12）	定例会等の実施	定例会での報告内容や開催のタイミング等、効率的かつ効果的な定例会の開催について具体的な提案が示されているか［加点］			小	15	5	0～3
11	4（15）	成果物	提出が必要な成果物について、期限を含めて認識していることが分かるようなスケジュールが提示されているか［加点］			小	15	5	0～3
	5　作業の実施体制・方法								
12	5（1） ～（4）	作業実施体制等	5（1）から5（4）までの作業の実施体制、方法等について、当省（当所）の求める業務内容が漏れなく提案されているか。［必須］			必須	-	-	-
13	5（1）	作業実施体制（追加提案）	作業の実施体制について、円滑に実施するための具体的な提案があるか。また、緊急時の連絡体制や作業要員のバックアップ体制など、着実に作業を実施するためのに、仕様書に記載された条件以外の提案があるか。［加点］			中	30	10	0～3
14	5（2）	作業要員に求める資格等の要件	作業要員について、5（2）ア～キの要件を満たす者がいるか［加点］			大	45	15	0～3
15	5（3）	作業場所	円滑に業務を行うための作業場所の設備の整備について記載されているか。また、リモート接続を行うことについて提案があり、かつ、リモートの接続についてセキュリティを確保しつつ、効率的に運用を行うための提案について記載されているか。［加点］			中	30	10	0～3
16	5（4）	作業の管理に関する要領	作業の管理について、仕様書に記載された内容以外に、適切な管理を行うための具体的な提案があるか［加点］			中	30	10	0～3
	8　入札参加資格に関する事項								
17	8（2） 8（3）	公的な資格や認証等の取得	調達仕様書の8（2）、（3）の要件に係る証明書類が提示されているか。[必須]			必須	-	-	-
18	入札公告期間中の閲覧資料	システム構成等	MAFFクラウドを前提としたシステム構成を正しく理解していることが示されているか。			必須	-	-	-

	その他								
19		ワーク・ライフ・バランス等の推進	ワーク・ライフ・バランスを推進する企業として、以下（(1)～(3)）の法令に基づく認定を受けているか。[加点] (1) 女性の職業生活における活躍の推進に関する法律（以下「女性活躍推進法」という。）に基づく認定（えるぼし認定企業・プラチナえるぼし認定企業）等 ① プラチナえるぼし 30点 ※１ ② えるぼし３段階目 24点 ※２ ③ えるぼし２段階目 21点 ※２ ④ えるぼし１段階目 12点 ※２ ⑤ 行動計画 6点 ※３ ※１ 女性活躍推進法第12条の規定に基づく認定。 ※２ 女性活躍推進法第９条の規定に基づく認定。なお、労働時間等の働き方に係る基準は満たすこと。 ※３ 常時雇用する労働者の数が100人以下の事業者に限る（計画期間が満了していない行動計画を策定している場合のみ）。 (2) 次世代育成支援対策推進法に基づく認定 ・プラチナくるみん認定企業 30点 ※４ ・くるみん認定企業（令和４年４月１日以降の基準） 21点 ※５ ・くるみん認定企業（平成２９年４月１日～令和４年３月３１日までの基準） 18点 ※６ ・トライくるみん認定企業 15点 ※７ ・くるみん認定企業（平成２９年３月３１日までの基準） 12点 ※８ ※４ 次世代法第１５条の２の規定に基づく認定 ※５ 次世代法第１３条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令（令和３年厚生労働省令第１８５号。以下「令和３年改正省令」という。）による改正後の次世代育成支援対策推進法施行規則（以下「新施行規則」という。）第４条第１項第１号及び第２号の規定に基づく認定 ※６ 次世代法第１３条の規定に基づく認定のうち、令和３年改正省令による改正前の次世代育成支援対策推進法施行規則第４条又は令和３年改正省令附則第２条第２項の規定に基づく認定（ただし、※８の認定を除く。） ※７ 次世代法第１３条の規定に基づく認定のうち、新施行規則第４条第１項第３号及び第４号の規定に基づく認定 ※８ 次世代法第１３条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則等の一部を改正する省令（平成２９年厚生労働省令第３１号。以下「平成２９年改正省令」という。）による改正前の次世代育成支援対策推進法施行規則第４条又は平成２ (3) 青少年の雇用の促進等に関する法律に基づく認定 ・ユースエール認定 24点 ※９ (1)～(3)のうち複数の認定等に該当する場合は、最も配点の高い区分により加点を行う。			加点（加重しない）	30		-
20		マイナンバーカードの利活用等に関する指標	(1)電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（公的個人認証法）第17条第1項第4号、5号若しくは6号に該当する事業者であって、同条第4項に規定する取決めを地方公共団体情報システム機構と締結した者又は同法第29条第１項に規定する総務大臣の認定を受けたものとみなされた事業者 認定事業者 6点 ※１ 上記のうち、複数の規定に該当する場合も、6点とすること。 (2)官民データ活用推進基本法第10条第2項に規定する電子情報処理組織を使用して入札に参加する事業者であって、公的個人認証法第3条第1項に定める署名用電子証明書又は第22条に定める利用者証明用電子証明書を用いて入札に参加する事業者 電子入札事業者 12点 (3)上記(1)及び(2)のいずれも該当する事業者 18点			加点（加重しない）	18		
21		賃上げ企業に対する加点	賃上げを実施する企業として、以下の（１）又は（２）の表明をしているか。 (1)大企業に該当する場合は、事業年度（又は暦年）において、対前年度（又は対前年）比で給与等受給者一人当たりの平均受給額を３％以上増加させる旨を従業員に表明していること (2)中小企業等に該当する場合は、事業年度（又は暦年）において、対前年度（又は対前年）比で給与総額を1.5%以上増加させる旨を従業員に表明していること			加点（加重しない）	30		
22		デジタル・スタートアップ	次の要件を全て満たす事業者であるか。 (1)中小企業基本法（昭和38年法律第154号）第２条第１項に規定する中小企業者（みなし大企業を除く）であること (2)設立から10年未満であること（調達する案件の内容・性質等を踏まえ、設立から15年未満とすることも可能） (3)情報システムに関連した先進技術やアイデアをもって当該事業に主体的に取り組み、今回の調達を実績として今後事業拡大することが期待できる事業者であること			加点（加重しない）	30		
					加点(最大時)		453		
					基礎点		7		
					加点(最大時)＋基礎点		460		

（別添）

賃上げの実施を表明した企業等に対する加点措置について

１　趣旨

「コロナ克服・新時代開拓のための経済対策」（令和３年 11 月 19 日閣議決定）及び「緊急提言～未来を切り拓く「新しい資本主義」とその起動に向けて～」（令和３年 11 月８日新しい資本主義実現会議）を受けて、政府において賃上げを行う企業から優先的に調達を行うため、令和４年４月１日以降に契約するものから、総合評価落札方式の評価項目に賃上げに関する項目を設け、賃上げの実施を表明した企業等に対して加点措置を行います。

なお、本措置は、以下の通知等に基づき、全省的に取り組むものです。

○「総合評価落札方式における賃上げを実施する企業に対する加点措置について」（令和３年 12 月 17 日付け財計第 4803 号財務大臣通知）

○「「総合評価落札方式における賃上げを実施する企業に対する加点措置について」（令和３年 12 月 17 日付け財計第 4803 号）第２（１）及び（２）に定める率について」（令和３年 12 月 17 日付け財計第 4804 号財務大臣通知）

２　措置の内容

（１）国の調達において、応札者が給与等受給者一人当たりの平均受給額を対前年度（又は対前年）（※）に比べ一定の増加率（大企業の場合３％、中小企業等の場合 1.5％）以上とする旨を「従業員への賃金引上げ計画の表明書」（様式１の１又は１の２）により表明した場合に加点します。

（２）発注者は、契約の相手方の事業年度等終了後に、契約の相手方が（１）により表明した賃上げが実行されているか確認します。

このため、契約の相手方になった場合には、発注者の指示に従い、「従業員への賃金引上げ実績整理表」（様式２の１又は２の２）及び「法人事業概況説明書」等の提出が必要になります。

（３）（２）の確認の結果、（１）により表明した賃上げが実行されていない場合、本制度の趣旨を意図的に逸脱していると認められる場合又は発注者が指示する資料の提出がない場合は、当該事実判明後、全省庁における総合評価落札方式による調達において、１年間、所定の点数を減点します。

※　企業の決算期（事業年度又は暦年）により、対前年度又は対前年を判断してください。

（様式１の１）　　【大企業用】

従業員への賃金引上げ計画の表明書

当社は、〇年度（令和〇年〇月〇日から令和〇年〇月〇日までの当社事業年度）（又は〇年（令和〇年１月１日から令和〇年 12 月 31 日））において、給与等受給者一人当たりの平均受給額を対前年度（又は対前年）増加率３％以上とすることを表明いたします。

年　　月　　日
株式会社 〇〇〇〇
（住所を記載）
代表者氏名　〇〇　〇〇

上記の内容について、我々従業員は、〇 年 〇 月 〇 日に、〇〇〇 という方法によって、代表者から説明を受けました。

年　　月　　日
株式会社 〇〇〇〇
従業員代表　　氏名　〇〇　〇〇　　印
給与又は経理担当者　　氏名　〇〇　〇〇　　印

（留意事項）

1　この「従業員への賃金引上げ計画の表明書」は大企業用（様式１の１）と中小企業等用（様式１の２）で異なります。

貴社がどちらに該当するかは、以下により御判断いただき、いずれかの用紙をご利用ください。

大 企 業：中小企業等以外の者をいう。

中小企業：法人税法第 66 条第２項又は第３項に該当する者をいう。

ただし、同条第６項に該当する者は除く。

2　貴社の事業年度により賃上げを表明し、契約の相手方となった場合には、貴社が作成する「法人事業概況説明書」を用いて賃上げ実績を確認させていただきますので、発注者の指示に従い、当該書類の写しをご提出いただくことを予めご承知ください。

なお、法人事業概況説明書を作成しない事業者の場合は、税務申告のために作成する類似の書類（事業活動収支計算書）等の賃金支払額を確認できる書類を提出していただきます。

3　暦年により賃上げを表明し、契約の相手方となった場合には、貴社が作成する「給与所得の源泉徴収票等の法定調書合計表」を用いて賃上げ実績を確認させていただきますので、発注者の指示に従い、当該資料の写しをご提出いただくことを予めご承知ください。

4　発注者において上記２若しくは３の提出を確認し、貴社が表明書に記載した賃上げを実行していないと認められる場合、本制度の趣旨を意図的に逸脱していると認められる場合又は上記２若しくは３の提出がない場合は、当該事実が判明した以降の総合評価落札方式による入札に参加する場合、技術点又は評価点を減点するものとします。

5　上記４による減点措置は、減点措置開始日から１年間、総合評価落札方式による入札に参加する場合に実施します。なお、減点措置の開始時期は、減点事由の判明の時期により異なるため、減点事由を確認した発注者から適宜の方法で通知します。

（様式１の２）　　【中小企業等用】

従業員への賃金引上げ計画の表明書

当社は、〇年度（令和〇年〇月〇日から令和〇年〇月〇日までの当社事業年度）（又は〇年（令和〇年 1 月 1 日から令和〇年 12 月 31 日））において、給与総額を対前年度（又は対前年）増加率 1.5 %以上とすることを表明いたします。

年　　月　　日
株式会社 〇〇〇〇
（住所を記載）
代表者氏名　〇〇　〇〇

上記の内容について、我々従業員は、〇 年 〇 月 〇 日に、〇〇〇 という方法によって、代表者から説明を受けました。

年　　月　　日
株式会社 〇〇〇〇
従業員代表　　氏名　〇〇　〇〇　　印
給与又は経理担当者　　氏名　〇〇　〇〇　　印

（留意事項）

1　この「従業員への賃金引上げ計画の表明書」は大企業用（様式１の１）と中小企業等用（様式１の２）で異なります。

貴社がどちらに該当するかは、以下により御判断いただき、いずれかの用紙をご利用ください。

大 企 業：中小企業等以外の者をいう。

中小企業：法人税法第 66 条第２項又は第３項に該当する者をいう。

ただし、同条第６項に該当する者は除く。

2　貴社の事業年度により賃上げを表明し、契約の相手方となった場合には、貴社が作成する「法人事業概況説明書」を用いて賃上げ実績を確認させていただきますので、発注者の指示に従い、当該資料の写しをご提出いただくことを予めご承知ください。

なお、法人事業概況説明書を作成しない事業者の場合は、税務申告のために作成する類似の書類（事業活動収支計算書）等の賃金支払額を確認できる書類を提出していただきます。

3　暦年により賃上げを表明し、契約の相手方となった場合には、貴社が作成する「給与所得の源泉徴収票等の法定調書合計表」を用いて賃上げ実績を確認させていただきますので、発注者の指示に従い、当該資料の写しをご提出いただくことを予めご承知ください。

4　発注者において上記２若しくは３の提出を確認し、貴社が表明書に記載した賃上げを実行していないと認められる場合、本制度の趣旨を意図的に逸脱していると認められる場合又は上記２若しくは３の提出がない場合は、当該事実が判明した以降の総合評価落札方式による入札に参加する場合、技術点又は評価点を減点するものとします。

5　上記４による減点措置は、減点措置開始日から１年間、総合評価落札方式による入札に参加する場合に実施します。なお、減点措置の開始時期は、減点事由の判明の時期により異なるため、減点事由を確認した発注者から適宜の方法で通知します。

（様式２の１）　　【大企業用】

従業員への賃金引上げ実績整理表

１　賃上げ実績

前年(度)の給与等平均受給額 ①	当年(度)の給与等平均受給額 ②	賃上げ率 （②／①－１） ×100	賃上げ基準	達成状況
		%	%	達成／未達成

２　使用した書類

□	法人事業概況説明書
【算出方法】「「10主要科目」の（労務費＋役員報酬＋従業員給料)」÷「「４期末従業員等の状況」の計欄」で算出した金額を前年度と比較する	

□	給与所得の源泉徴収票等の法定調書の合計表
【算出方法】「「１給与所得の源泉徴収票合計表」の「支払金額」」÷「人員」で算出した金額を前年と比較する	

（注）使用した書類の左欄の□に「✓」を付してください。

年　月　日
株式会社○○○○
（住所を記載）
代表者氏名　○○　○○

（留意事項）
前年(度)分と当年(度)分の「法人事業概況説明書」又は「給与所得の源泉徴収票等の法定調書合計表」の写しを添付してください。

（様式２の２）　　【中小企業等用】

従業員への賃金引上げ実績整理表

１　賃上げ実績

前年(度)の給与総額　①	当年(度)の給与総額　②	賃上げ率 （②／①－１） ×100	賃上げ基準	達成状況
		%	%	達成／未達成

２　使用した書類

□	法人事業概況説明書
【算出方法】「「10主要科目」の（労務費＋役員報酬＋従業員給料)」で算出した給与総額を前年度と比較する	

□	給与所得の源泉徴収票等の法定調書の合計表
【算出方法】「「１給与所得の源泉徴収票合計表」の「支払金額」」で算出した給与総額を前年と比較する	

（注）使用した書類の左欄の□に「✓」を付してください。

年　月　日
株式会社○○○○
（住所を記載）
代表者氏名　○○　○○

（留意事項）
前年(度)分と当年(度)分の「法人事業概況説明書」又は「給与所得の源泉徴収票等の法定調書合計表」の写しを添付してください。