

令和 8 年度

農業農村整備情報機器購入

仕様書

中国四国農政局土地改良技術事務所

第1章 基本要件

1 目的

中国四国農政局における農業農村整備事業の円滑な実施とセキュリティの向上に資するため、土地改良技術事務所に設置している集約管理サーバーの更新機器の調達を目的とする。

2 調達の範囲

本調達の範囲は、以下のとおりである。購入する機器等の詳細は、第2章に示す。

(1) 機器等の購入

(2) 集約管理サーバーの設置・調整

サーバーラックへの搭載、配線接続、ソフトウェアの導入・設定、現行の Active Directory 移行作業、動作確認を含む。

(3) 成果物の作成及び提出

3 履行期限

令和9年3月19日（金）

4 履行場所

〒700-0984 岡山市北区桑田町1-36
中国四国農政局土地改良技術事務所

5 作業体制

受注者は、契約締結後、実施体制、納品日等を記載した「履行スケジュール」を作成のうえ、中国四国農政局土地改良技術事務所企画情報課の担当職員（以下「担当職員」という。）へ提出し承諾を得るものとする。

6 前提条件

本調達に当たっての前提条件は、次に示すとおりである。

(1) 本調達は、担当職員と緊密な連携及び調整を図り行うものとする。なお、購入機器等の搬入、設置に当たっては、事前に担当職員と打合せのうえ行うものとする。また、機器間の接続ケーブル等については、受注者が用意し設置するものとする。

(2) 現行の集約管理サーバーは、Microsoft Windows Server 2019 で稼働している。ドメインの機能レベルは、Windows Server 2016 である。

(3) 納入候補となる機器等について、納入前に担当職員へ機器等リスト（区分（サーバー等）、製造業者・役務実施業者名、業者の法人番号、製品名・役務実施場所、型番等を記載したリスト）を提出することとし、農林水産省においてサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、速やかに担当職員に確

認した上で、代替品の選定等、納入候補となる機器等を見直すこと。なお、機器等リストの様式は、担当職員より受注者に提供する。

- (4) 納入する集約管理サーバーについては、事前にハードウェア及びソフトウェアの仕様、設定項目等を記述した資料（機器構成一覧表）を担当職員に提出し、承諾を得るものとする。
- (5) 集約管理サーバーは、拡張性を有するとともに、業務の変化やレイアウトの変化に柔軟に対応できるものとする。
- (6) 機器等を構成するハードウェア、ソフトウェアは、過去に出荷・稼働実績及び十分に高い信頼性を有する標準的な既製品で、かつ、最新のものとする。「標準的な既製品」とは、メーカーが一般市場において販売するために主要な製品系列の一環として製造する物品で、稼働実績を有するものをいう。なお、証明書（機器等一覧表及びカタログ）等提出時において市販化されていない機器等を含める場合には、次の条件を厳守するものとする。
- ・市販化されていない部分の存在及びその範囲を明確にするものとする。
 - ・上記に関し、要件を満たす機器等を納品時までに出荷する旨の意志表明を行い、提供可能である根拠を十分説明できる資料を付すものとする。

(7) 集約管理サーバーの設置場所等

設置場所	設置階数等
中国四国農政局 土地改良技術事務所	・ 1 階（5 階建） ・ 空調設備有り。空調の温度設定は、24 時間 25℃設定である。 ・ 既設電源コンセントは、100V 15A×2 個有り。 ・ 既設の無停電電源装置有り。

- (8) 原則として、現行システムの運用を停止することなく設置・調整作業を実施するものとするが、やむを得ず停止を行う必要がある場合は担当職員と調整を行うものとする。
- (9) 集約管理サーバーの設置・調整作業は、原則として、日曜日、土曜日及び祝日（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）に現行システムの運用を停止し作業を実施するものとするが、やむを得ず平日に作業を行う必要がある場合は担当職員と調整を行うものとする。

第 2 章 購入機器等の仕様等

1 購入機器等の名称及び数量

番号	名称等	仕様等	数量
1	集約管理サーバー	詳細仕様及び要件定義は、第 2 章 2 のとおり。	2 台

2	Windows Server Standard 16 Core License Pack	バージョン：Windows Server 2025	1 式（サーバー 2 台分）
3	Windows Server User CAL	バージョン：Windows Server 2025	1 式（350 人分）

※ 対象機器等は、上表に指定する製品又は同等品以上とする。

（注）「同等品以上」とは、メーカーが一般市場において販売するために主要な製品系列の一環として製造する物品で、稼働実績を有するものをいう。

2 詳細仕様及び要件定義

（1）共通事項

購入機器等において、「国等による環境物品等の調達の推進等に関する法律」に基づく「環境物品等の調達の推進に関する基本方針（2012 年 2 月 7 日変更閣議決定）」で定める特定調達品目については、その判断の基準に適合しているものとする。

（2）ハードウェア及びソフトウェアの詳細仕様

ハードウェア及びソフトウェアの詳細仕様については、以下に示すものと同等以上のものとする。

ア ハードウェア及びソフトウェアについては、原則として日本語表示による操作ができることし、日本語表示によらない場合は日本語マニュアル等が付属しているものとする。

イ 集約管理サーバーの形状は、ラックマウント専用型とし、取付器具等によりタワー型等をラックマウント形状にしたものは不可とする。

ウ ソフトウェア及びハードウェアのファームウェア等について、導入時点において最新の修正プログラム及びセキュリティパッチ（以下「パッチ」という。）を適用すること。ただし、安全性等の観点からメーカー等から提供されたパッチを即適用することが好ましくないと判断される場合は、担当職員に報告を行うものとする。

（3）集約管理サーバーの要件定義

ア ハードウェア

項目	仕様
CPU	インテル Xeon プロセッサー E-2136 相当以上の性能を有するものとする。
主記憶装置	32GB（DDR4）以上を有するものとする。（データ転送レート 2133 MT/s 以上）
RAID コントローラ	RAID1+HotSpare 機能を有するものとする。SATA 6Gbps 以上の転送速度を有するものとする。
磁気ディスク装置	ハードウェア RAID にて RAID1+HotSpare を実現した後、240GByte 以上の SSD ディスクを有するものとする。

ネットワークインターフェイス	1000Base-T のインターフェイスを 1 ポート以上、10GBase-T のインターフェイスを 1 ポート以上有するものとする。
標準インターフェイス	・ディスプレイのポートを 1 ポート以上有するものとする。 ・キーボード、マウスを設置した後に USB3.0 以上のポートを 1 ポート以上有するものとする。
電源	・ AC100V 60Hz ・ 冗長構成を有するものとする。

イ パーティション構成

ドライブ名	論理容量	RAID	備考
C	全て	RAID1+HotSpare	OS

ウ ソフトウェア

項目	仕様	備考
OS	Microsoft® Windows® Server 2025 64bit Standard Edition を導入し、現行 AD を移行するものとする（1 台をプライマリーAD、もう 1 台をセカンダリ AD としレプリケーションを設定する）。	現行 AD をサブ AD に降格する。また、Server に必要な User CAL（350 人分）を有するものとする。
UPS	集約管理サーバー 2 台に Power Chute を導入し、停電が一定時間（300 秒）続いたら OS が自動的にシャットダウンするよう設定するものとする。	Power Chute のソフトウェアは、受注者が用意するものとする。

※上表の「AD」は、「Active Directory」を示す。

（４）現行の集約管理サーバーとの共有機器

項目	仕様	備考
モニタ、キーボード、マウス	・ 切替機 PY-KVFA08 ・ コンソール PY-R1DP1	・ 既存の機器を使用する。 ・ 切替機と集約管理サーバーの接続ケーブルは、受注者が用意し設置するものとする。なお、KVM ケーブル（PY-CBKCU01）は、発注者が 2 本用意する。
無停電電源装置	SMT1500RMJ2U、LAN 接続	無停電電源装置（HUB 経由）と集約管理サーバーの接続ケーブルは、受注者が用意し設置するものとする。
HUB	AT-SH230-28GT	

第 3 章 設定作業

1 ソフトウェア及び機器設定

受注者は、以下に示す本仕様に係るソフトウェア及び機器の設定を行うものとする。

番号	設定内容
1	第2章2（3）に示す OS のインストール
2	Microsoft® Windows® Server 2025 64bit Standard Edition（ドメイン機能レベル 2019、AD・DNS・NTP サーバー）を設定し、現行 AD を移行する（1 台をプライマリーAD、もう 1 台をセカンダリ AD としレプリケーションを設定する）。
3	第2章2（3）に示す UPS 管理コンソールの設定
4	第2章2（3）に示す UPS 管理エージェントの設定

※上表の「AD」は、「Active Directory」を示す。

2 動作確認試験

受注者は、本仕様に係る機能確認のための動作確認試験を行うものとする。

動作確認試験の実施に当たっては、内容、スケジュール等を含めた「動作確認計画書」を作成し、事前に担当職員の承諾を得るものとする。また、動作確認試験の結果については、「動作確認結果報告書」にとりまとめて担当職員に報告を行うものとする。

なお、動作確認試験に係る費用については受注者の負担とするものとする。

第4章 取扱説明

本調達の購入機器等の引渡しまでに担当職員に取扱説明を実施するものとする。なお、説明内容、説明日時等については、担当職員と調整を行うものとする。

第5章 成果物

1 成果物

以下に示す資料を完成図書としてとりまとめ、紙媒体 1 部（分冊及び市販のファイル綴じで可）、電子媒体（CD-R）1 部を提出するものとする。なお、取扱説明書及び各種保証書は、電子媒体への格納は求めない。

- ・購入機器一覧（機器名称、機器型番、数量等について記載）
- ・環境設定一覧
- ・動作確認計画書及び動作確認結果報告書
- ・サーバー障害対応一覧表
- ・取扱説明書（機器、ソフトウェア等）
- ・各種保証書（該当するものがある場合）
- ・ソフトウェアのライセンス証書
- ・消耗品一覧（名称、型名、単価、使用目安等について記載）
- ・その他担当職員が指示する資料

2 成果物取扱いに関する事項

- （1）本調達における成果物の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書面にて権利譲渡不可能と示されたものの以外は、全て農林水産省に帰属するものとする。

- (2) 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調達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。
- (3) 本調達に係る成果物の所有権は、農林水産省から受注者に対価が完済されたとき受注者から農林水産省に移転するものとする。
- (4) 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、本調達の受注者は、当該既存著作物の内容について事前に農林水産省の承認を得ることとし、農林水産省は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら農林水産省の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、農林水産省は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。
- (5) 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。
- (6) 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。

3 成果物における契約不適合責任

- (1) 農林水産省は検査完了後、成果物について仕様書との不一致（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。ただし、農林水産省が追完の方法についても請求した場合であって、農林水産省に不相当な負担を課するものでないときは、受注者は農林水産省が請求した方法と異なる方法による追完を行うことができること。
- (2) 前記（１）にかかわらず、当該契約不適合によっても個別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（１）に規定された追完に係る義務を負わないものとする。

- (3) 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こと。
- (4) 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個別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及び個別契約の全部又は一部を解除することができること。
- (5) 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、検査完了後1年以内に農林水産省から当該契約不適合を通知された場合に限るものとする。ただし、検査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。
- (6) 前記(1)から(5)までの規定は、契約不適合が農林水産省の提供した資料等又は農林水産省の与えた指示によって生じたときは適用しないこと。ただし、受注者がその資料等又は指示が不相当であることを知りながら告げなかったときはこの限りでない。

4 成果物の提出先

〒700-0984 岡山県岡山市北区桑田町1-36
中国四国農政局土地改良技術事務所

第6章 その他

1 情報セキュリティの確保

受注者は、別途貸与する「農林水産省における情報セキュリティの確保に関する規則」（平成27年3月31日農林水産省訓令第4号）に定められている事項について遵守することとし、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。なお、上記規則等が改定された場合は、本業務に関する影響分析を行うこと。

本調達の実施において知り得た全ての事実については、契約期間中はもとより、契約終了後においても第三者に漏らしてはならない。なお、本調達の一部を再委託等する場合は、再委託等を受ける者も同様とする。また、秘密保全に関する事項は、担当職員の指示に従うこと。

2 クロスコンプライアンスについて

(1) 主な環境関係法令の遵守

受注者は、物品の提供に当たり、関連する環境関係法令を遵守するものとする。

ア エネルギーの節減

- ・エネルギーの使用の合理化及び非化石エネルギーへの転換等に関する法律（昭和 54 年法律第 49 号） 等
- イ 廃棄物の発生抑制、適正な循環的な利用及び適正な処分
 - ・廃棄物の処理及び清掃に関する法律（昭和 45 年法律第 137 号）
 - ・国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）
 - ・プラスチックに係る資源循環の促進等に関する法律（令和 3 年法律第 60 号）
- ウ 環境関係法令の遵守等
 - ・労働安全衛生法（昭和 47 年法律第 57 号）
 - ・環境影響評価法（平成 9 年法律第 81 号）
 - ・地球温暖化対策の推進に関する法律（平成 10 年法律第 117 号）
 - ・国等における温室効果ガス等の排出の削減に配慮した契約の推進に関する法律（平成 19 年法律第 56 号）

（２）環境関係法令の遵守以外の事項

受注者は、物品の提供に当たり、新たな環境負荷を与えることにならないよう、以下の取組に努めるものとする。

- 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 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。
- エ 廃棄物の発生抑制、適正で循環的な利用及び適正な処分に努める。
- 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。
- 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。

３ その他留意事項

作業に際して発生した不明な点等については、担当職員と調整又は指示に従うものとする。

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弱（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 既知の脆弱（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弱（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弱（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可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可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弱（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（G S S）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弱（ぜい）弱性対策の状況を確認すること。
 - (6) 情報システムに脆弱（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弱（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弱（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弱（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

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へ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へ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。
- 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つ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つ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。