淀川水系土地改良調査管理事務所NAS外購入
仕 様 書

近畿農政局淀川水系土地改良調査管理事務所

１．適用範囲

本調達は、この仕様書によるものとする。

２．購入の対象

本調達の品目及び数量は、以下のとおりであり、詳細は別紙1のとおりとする。

（1）NAS 及び関連機器 1式

３．納入先

〒612－0855

京都府京都市伏見区桃山町永井久太郎56

近畿農政局淀川水系土地改良調査管理事務所

４．納入候補となる機器

納入候補となる機器リスト（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）を様式1により作成し、令和7年7月11日（金）までに発注者へ提出すること。

提出された納入候補機器リストを農林水産省で審査し、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、代替品の選定等、納入候補となる機器の見直しを図ること。

なお、納入候補となる機器の承認が得られず見直しをする場合においても機器リストの提出期限は延長しないので、機器リストについてはなるべく早期の提出を行うこと。

また、納入候補となる機種については、複数機種（3機種程度まで）記載することも可とする。

５．納入期限

納入期限は、令和7年9月19日（金）とする。

６．支払期限

支払は、納品確認後に適法な請求書を受理した日から30日以内とする。

７．入札参加資格に関する事項

（1） 別紙2「情報セキュリティの確保に関する共通基本仕様」（以下「共通基本仕様」という。）記載事項を遵守すること。

なお、本調達においては、共通基本仕様において求められている資料等の提出は不要とする。

（2） 本調達を直接担当する農林水産省CIO 補佐官、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。

８．情報セキュリティに関する事項

（1） 受注者は、物品の搬入を行う場合は、発注者の立会の下に行うと共に、搬入する物品の内容の確認を受けること。

（2） 本調達により知り得た情報については厳重に管理し、第三者に漏らさないこと。
（3） 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。）
（4） その他、秘密保全に関することは、発注者の指示に従うこと。

9. 環境負荷低減のクロスコンプライアンス
（1） 環境関係法令の遵守
受注者（受託者）は、物品・役務の提供に当たり、関連する環境関係法令を遵守するものとする。
①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
②環境関係法令の遵守等
・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
・グリーン購入法（平成12年法律第100号）
（2） 環境関係法令の遵守以外の取組
受注者は、物品・役務の提供に当たり、新たな環境負荷を与えることにならないよう、以下の取組に努めるものとする。
① みどりの食料システム戦略の理解に努める、もしくは、環境配慮の取組方針の策定や研修の実施に努めること。
② 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）の実施に努めること。
③ 物品調達に当たっては、エネルギーの節減及び生物多様性への悪影響の防止等の観点から、環境負荷低減に配慮したものの調達に努めること。

10. その他
（1） 受注者は、機器の取扱いについて担当職員に説明するとともに、マニュアル、保証書等の資料を提出するものとする。
（2） 本仕様書に明記されていない事項及び疑義等については、担当職員と協議するものとする。
（3） 搬入した製品に係る箱等の梱包材は、受注者の責任において搬出・処分すること。

別紙1

各機器の詳細仕様等

1．品目及び数量

① NAS　1台
② NASバックアップ用外付けHDD　1台
③ 無停電電源装置（UPS）　1台
④ ウィルス対策ソフト　　1式（2．仕様等の①NASに記載）

2．仕様等

①NAS

項目	仕様内容
OS	Linux
ハードディスク	・データ容量2TB以上であること 　データ実効保存容量1TB以上想定 ・NAS専用ハードディスクであること ・ホットスワップ対応であること
RAID構成	RAID1以上もしくは拡張ボリューム対応であること
バックアップ	下記②の外付けハードディスクに接続し、定期的にスケジュールバックアップが可能なこと（フル＋差分（2TB程度））
対応OS	Windows10，Windows11に対応していること
最大同時接続数	30台程度
LANポート	1000BASE-Tに対応していること
USBポート	USB3．0×2以上（外付けハードディスクでのバックアップ用として利用できること）
電源	AC100V（50Hz／60Hz）
ウイルスチェック機能	ウィルス対策ソフト（5年間保守付き）をインストールするものとする
製品保証	デリバリー保守（ハードディスク返却不要）サービスパックを付属するものとする（5年間）
アクセス制限	Windowsからアクセスした場合に、共有フォルダー、サブフォルダー、ファイルに対しアクセス制限をおこなえること。

②NASバックアップ用外付けハードディスク

項目	仕様内容
対応機種	上記①のNASのバックアップ用として対応可能な機種であること
データ容量	定期的にスケジュールバックアップが可能なこと（フル＋差分（2TB程度））

対応OS	Windows10、Windows11に対応していること
インターフェース	
その他	接続ケーブル（USB）を付属すること

③無停電電源装置（UPS）

項目	仕様内容
対応機種	・常時商用、正弦波出力 ・バックアップ時間（最大不可時）5分以上（250W） ・上記①NAS及び②NASバックアップ用外付けハードディスクに対応可能な機種であること

3．設置作業

（1） 機器等の選定にあたっては、「2.仕様等」を満たしている物、またはそれ以上のものとする。

（2） 機器の搬入及び初期設定(設置、接続、動作確認)を含む。

（3） 現在発注者が使用しているファイルサーバからのデータ移行は、発注者で行うものとする。

（4） 物品の納入、設置等にあたっては発注担当者の指示に従うこと。

4．その他

（1）送料等、調達にかかる一切の費用については受注者が負担すること。

（2）作業（納品時）において、施設及び既存機器等を毀損しないこと。
また、危険、火災、盗難等の事故防止には万全の注意を払い、事故回避のため必要な安全対策をとること。万一、事故が発生した場合は、全て受注者の負担において原状回復及び修理を行うものとする。

（3）受注者は、物品を納入しようとする場合は、発注者に対し納入する旨を通知し、発注者が命じた検査のための職員（ 以下「検査職員」という。） の検査を受けなければならない。

（4）代金の支払いについては、受注者が提出する適法な支払請求書を受理した日より起算して30日以内の日に支払うものとする。

（5）本仕様に定めのない事項については、必要に応じ担当職員と打ち合わせを行うこと。

別紙2

情報セキュリティの確保に関する共通基本仕様

Ⅰ 情報セキュリティポリシーの遵守

1 受託者は、担当部署から農林水産省における情報セキュリティの確保に関する規則（平成27年農林水産省訓令第4号。以下「規則」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。

なお、規則は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、規則が改正された場合には、受託者は改定内容を踏まえて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、様式2により提出すること。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。（様式は自由とする。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（様式は自由とする。）。

（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（様式は自由とする）。

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、その結果を担部署に書面で報告すること（様式は自由とする）。

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。

（ｉ）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

（ii）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

（iii）農林水産省内通信回線への端末の接続を監視する機能

（iv）端末への外部電磁的記録媒体の挿入を監視する機能

（ｖ）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、様式3により提出すること。

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（様式は自由とする）。
（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。