情報セキュリティ共通仕様

情報セキュリティの確保

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。

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すること。

４　本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策について、提案書に記載すること。（または、証明書等を提出すること。）

（１）受託者に提供される情報の目的外利用の禁止

（２）情報セキュリティ対策の実施内容及び管理体制

（３）業務の実施に当たり、受託者又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

（４）受託者の資本関係・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提供

（５）情報セキュリティインシデントへの対処方法

（６）情報セキュリティ対策その他の契約の履行状況の確認方法

（７）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

５　担当部署が必要と認めた場合、情報セキュリティ監査の受入れ及び業務内容、品質等のサービス水準（サービスレベル）の保証を行うこと（農林水産省が別途選定した事業者による監査を含む。）。

６　本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を受託後速やかに提出すること。また、変更があった場合は、速やかに再提出すること。

（１）本業務に携わる者の特定

（２）本業務に携わる者が実施する具体的な情報セキュリティ対策の内容

７　情報の受渡し方法や本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実施計画に記載し、担当部署の承認を得ること。また、定められた手順により情報を取り扱うこと。

８　本業務の遂行に当たり、役務内容を一部再委託する場合は、再委託することにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記４から７までの措置の実施を委託先に担保させること。

９　受託者は、自己の情報セキュリティ水準について、以下を証明する資料を提案書に

記載すること。（または、証明書等を提出すること。）

（１）ISO/IEC27001 等の国際規格とそれに基づく認証制度の活用

（２）IPA が公開する自己診断ツール（情報セキュリティ対策ベンチマーク）等、情報セキュリティガバナンスの確立促進のために開発された自己評価の結果

（３）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

10　担当部署から情報セキュリティ対策の履行状況の確認を求められた場合、速やかに報告すること。

11　本業務に係る情報セキュリティインシデントの発生若しくは情報の目的外利用等の認知に際して、担当部署の指示に従い必要な措置を講じること。

12　本業務の遂行に当たっては、知り得た全ての事項について、契約期間中はもとより、契約終了後においても外部に漏らしてはならない。秘密保全に関することは、担当部署の指示に従うこと。

13　本業務の遂行に当たっては、従事する全ての者と個別に退職後も有効な守秘義務契約を締結すること。

14　本業務において知り得た情報の漏えい等の事案が発生した際には、担当部署に電話、口頭等による報告を行うとともに、書面にて提出すること。なお、事案の発生後は事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。また、受託者以外の者の作業も含め、対処に係る費用は全て受託者が負担すること。

15　本業務の終了時に、受託者において取り扱われた情報は確実に返却又は抹消し、結果を書面にて報告すること。

16　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することとし、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。

17　情報システムを構成するソフトウェアについては、既知のセキュリティホールに対するセキュリティ対策を行うこと。

18　情報システムの運用期間中、当該情報システムで利用するソフトウェアのサポート期限等を情報収集し、定期的に報告すること。【保守業務の場合】

19　「政府情報システムの整備及び管理に関する標準ガイドライン」（平成 26 年 12 月３日各府省情報化統括責任者（CIO）連絡会議決定。）「別紙３　調達仕様書に盛り込むべき ODB 登録用シートの提出に関する作業内容」に基づき、政府情報システム管理データベース（ODB）に情報を登録（又は更新）するために必要な ODB 登録用シートを提出すること。【ODB 登録/更新対象の場合】

機器等に対するセキュリティ要件

機器等に対するセキュリティ要件は以下のとおり。【取り扱う情報の格付、取扱制限、機器等を利用する組織の特性、利用環境等に応じて、想定されるリスクを考慮した上で検討すること】

１　機器等の開発工程における品質保証体制を証明する資料を提出すること。
２　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。
３　利用マニュアル・ガイダンスが整備された機器等を採用すること。
４　ソフトウェアの利用期間を踏まえ、サポート期間が十分に確保されたものを採用すること。また、サポート期限が公表されていない場合には、ソフトウェアを導入する情報システム等のライフサイクルを踏まえ、発売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すること。
５　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。

外部委託等における情報セキュリティ上のサプライチェーン・リスク対応

１　外部委託

（１）外部委託に係る契約事項

ア　情報システムの【設計・構築／運用・保守／廃棄 等の各工程のうち、調達内容に応じて必要な場面を選択】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。

イ　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ための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。

ウ　情報システムに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、追跡調査や立入検査等、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、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注先から要求された場合には提出させるようにするなど）を整備していること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。

エ　農林水産省の許可無く、作業の一部又は全部を第三者（再委託先）に請け負

わせてはならない。ただし、農林水産省が許可した場合には、受託者は、農林水産省との契約上受託者に求められる水準と同等の情報セキュリティ水準を、再委託先においても確保すること。また、受託者は、再委託先が実施する情報セキュリティ対策及びその実施状況について、農林水産省に報告すること。

オ　委託事業において取り扱う情報について、再委託先が閲覧することがないように、受託者は情報を厳重に管理すること。止むを得ず、再委託先において委託事業に係る情報を閲覧する必要がある場合には、受託者は、事前に農林水産省の担当者と調整し、農林水産省の担当者の指示に従うこと。（再委託先における情報の取扱いを含む包括的な秘密保持契約を締結する、作業の都度情報の取扱いについて調整するなどの手続き方法について合意すること。

（２）委託先の資本関係・役員の情報等に関する事項

ア　受託者は、資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・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提示すること。

イ　委託事業の運用に係る要員を限定すること。また、全ての要員の所属、専門性（資格等）、実績及び国籍について掲示すること。委託事業の実施期間中に要員を変更する場合は、事前に農林水産省の担当者へ連絡し、許可（又は確認）を得ること。

ウ　運用に係る者の所属（契約社員、派遣社員等の雇用形態は問わず、委託事業に従事する全ての要員）、実績（経験年数、資格等）及び国籍について、農林水産省の担当者にあらかじめ提出し、許可（又は確認）を得ること。

エ　再委託を行う場合には、受託者は、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について、委託元である府省庁の担当者へ提示し、許可（又は確認）を得ること。

オ　前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（資格等）、実績及び国籍についての情報を委託元である府省庁の担当者へ提示すること。

（３）監査に関する事項

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、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）に基づく情報セキュリティ監査を受託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）。

２　機器等の調達

（１）当該機器等の製造工程において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）当該機器等の製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。また、当該管理体制を証明する資料を提出すること。

（３）機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。また、それらを証明する資料を提出すること。

（４）機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更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。機器に不正が見つかったときに、追跡調査や立入検査等、農林水産省と迅速かつ密接に連携して原因を調査し、排除できる体制を整備している生産工程による製品であること。

（５）情報システムを構成する要素（ソフトウェア、ハードウェア）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が確立していること。また、当該構成管理体制が書類等で確認できること。

（６）受託者が情報システムを構成する要素（ソフトウェア、ハードウェア）として採用した機器等について、不正な変更が加えられていないことを検査する体制が受託者において確立していること。また、当該検査体制が書類等で確認できること。