令和７年度

国有林野情報管理システム

－市町村交付金算定サブシステム

の構築に係る要件定義書作成等業務

調達仕様書

林野庁

目次

1　調達案件の概要

（１）調達件名

令和７年度　国有林野情報管理システム－市町村交付金算定サブシステムの構築に係る要件定義書作成等業務

（２）調達の背景

林野庁　国有林野部　経営企画課　（以下「PJMO」という。）では、「国有林野情報管理システム」を国有林野事業に係る基幹システムとして、平成19年度から運用を開始し、現在約4,000人の職員及び指定調査機関が利用している。しかしながら、森林整備の推進による国有林における木材供給や造林業務の増加が見込まれることや、システム構築時から相当の年月が経過していることで、構築当初の業務要件との齟齬が出ているところもあり、業務に係る作業の負担が増加していることから、下記システムの設計・構築を発注している。

① R6～8 次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務（工程１）

② R6 次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務(工程２)

これらのシステム設計・構築を進めるに当たり、現行の国有林野情報管理システムの補助機能として提供している「市町村交付金算定プログラム」(以下、「当プログラム」という。）について、当プログラムを見直し、要件を確定した上で上記②のサブシステムとして設計・構築することで、より効率的な業務とすることを想定している。

当プログラムをシステム化するための要件定義を確定させること及び当プロセスに必要となる紙ベースの閲覧資料を電子化に向けて、その対象範囲（総量）、工数、経費及び電子化する際の課題の調査結果を当調達の対象とする。

（３）調達目的及び調達の期待する効果

現行の市町村交付金算定に当たっては、Microsoft Accessを使用し、コード変換、データの取り込み、入力等に基づき控除対象などを計算、必要な書類の印刷が可能となる機能が提供されているが、ほとんどが手作業で行われており、係る労力、所要時間が問題となっている。

当調達においては、現行プログラムを見直し、システム化(「市町村交付金算定サブシステム」を念頭において、現行プロセスで課題となっている作業やシステムを活用したい業務の要件を担当部署とともに整理し、担当部署と協議の上、優先順位をつけてシステム要件に落とし込んだ上で、１（２）②のシステムの機能の一部(サブシステムとしての位置づけ)として、この業務がより効率的、効果的なプログラムとなるようなシステムの設計・構築につなげることを目指す。

また、市町村交付金の算定において参照する資料、例えば貸付契約書やその申請書は、作成時点が非常に古く紙ベースの資料として保管されており、算定時の確認において、簿冊から探すといった手間が発生している。このため、これらの資料を電子化し、算定時にシステム上で確認ができるようにする。当調達ではこの電子化に向けた作業量や経費を調査し、その調査結果を当

該要件定義に反映させた上で、要件定義の実装に併せて、全国的な電子化を行う際の基礎となる資料とすることを目指す。

これらの対応により機能が追加、改善された基幹システムとして「次期国有林野情報管理システム」が国有林野事業に係る業務の効率化、情報の信頼性・透明性の向上につながることを目標とする。

(４)業務・情報システムの概要

ア. 対象業務

(ア) 本プログラムの概要は次のとおりである。

市町村交付金は、地方税法第 348 条第 1 項において固定資産税を課することができないとされている国及び地方公共団体等が所有する固定資産のうち、当該固定資産を所有する国又は地方公共団体以外の者が使用している固定資産又は国有林野に係る土地等につき、当該固定資産所在の市町村に対して交付するものである。

現行業務の処理フロー概要を図１に示す。

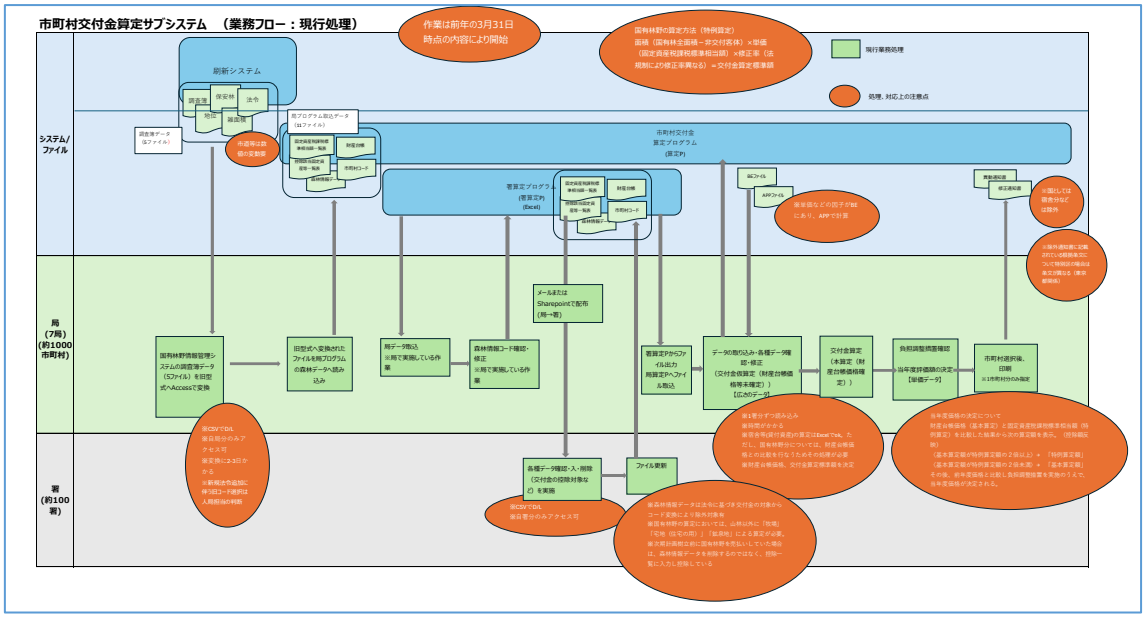


図　1　市町村交付金算定プログラム処理フロー概要

(イ) 本プログラムに係る資料電子化調査については次のとおりである。

市町村交付金の算定に当たって、控除の対象となる市町村等への貸付地の確認を、貸付契約書などによって把握し、進めているところである。土地の貸付は、長期の契約が結ばれているものが一定量あり、貸付決定当時の紙の状態で原本として保管されている実態がある。

このように、算定に当たり参照すべき情報のうち、どのような資料が、どの程度紙ベースで参照されているかを特定し、それらをどのようなデータ形式で電子化すると業務の効率化、精緻化をつながるかをサンプル調査し、それらに係る作業量、データ量を調査した上で、同様の電子化を全国的に行った場合、どの程度の規模感となるかを把握し、その課題と対応策をまとめた資料電子化調査結果報告書を作成する。

イ．本プログラムにおいて利用する情報システム

(ア) 関連システム(次期国有林野情報管理システム)

本プロセスに関連するシステムとして現在構築を進めている「次期国有林野情報管理システム」がある。その概要は下図のとおり。

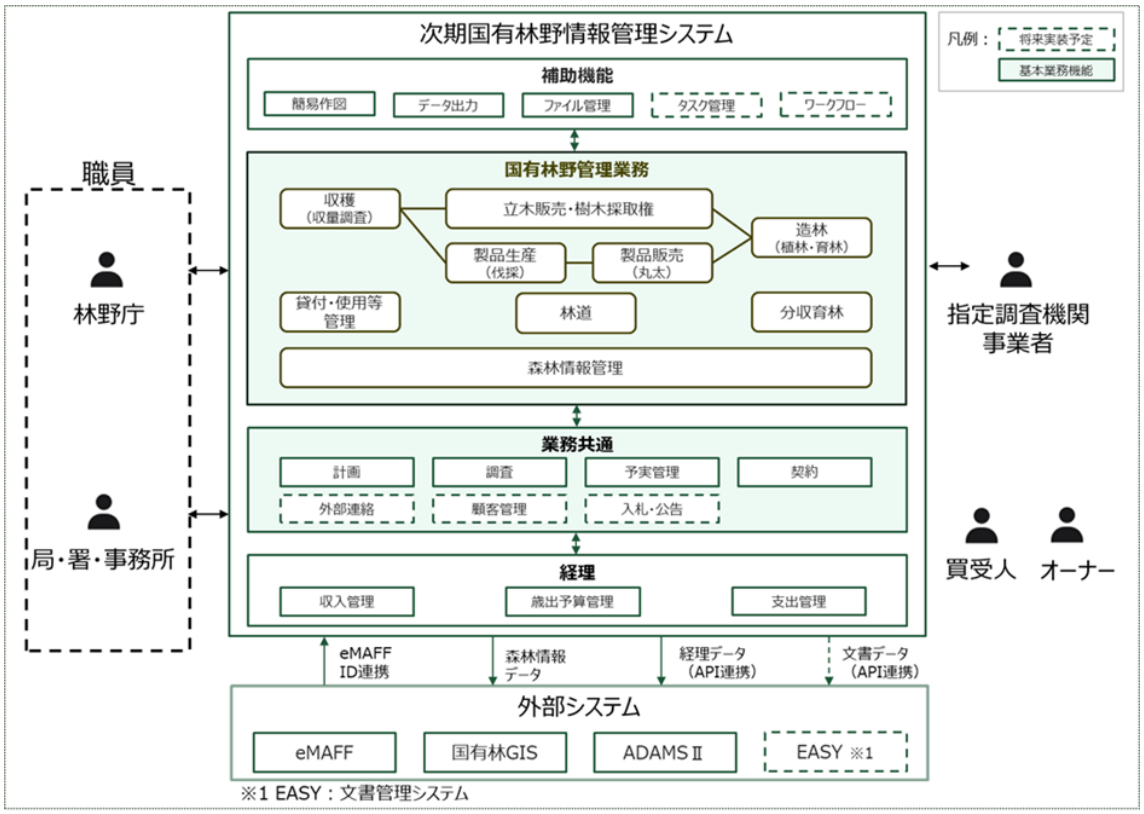


図　2　次期国有林情報管理システムの概要

(イ) MAFF クラウド

2018年６月に、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018年６月７日各府省情報化統括責任者（CIO）連絡会議決定。以下「クラウド利用方針」という。）が決定（最終改定は、2025年5月27日）された。この中で、「クラウド・バイ・デフォルトの原則」が政府方針として出されている。農林水産省では、政府全体の動向や利用者視点に立った、あるべき農林水産行政の姿を踏まえ、令和4年6月7日に閣議決定された「デジタル社会の実現に向けた)重点計画」を受けて、「デジタ

ル社会の形成に向けた農林水産省中長期計画」（令和4年10月５日に農林水産省行政情報化推進委員会決定）を策定した。
同計画では、品質・低コスト・スピードを兼ね備えた行政サービスに向けて、 ガバメントクラウド、ガバメントソリューショ ンサービス（GSS）、ベースレジストリ等の共通機能について、農林水産省の各情報システムの状況を踏まえ、活用できるものについてはその活用を徹底するとしている。その上で、農林水産省では、クラウドの共通基盤を整備し、パブリッククラウドへの移行・運用に必要な最小限の共通機能を提供するとともに、情報システムの状況に応じて適切なクラウドへの移行方式を選択した上で円滑にクラウド移行できるよう支援を行っている。なお、当該共通機能を利用するパブリッククラウドをMAFFクラウドと言い、総合的な支援活動を行う組織をMAFFクラウドCoEと言う。
本システムはMAFFクラウドを利用しており、本調達期間においても引き続きMAFFクラウドを利用することを前提とする。
MAFFクラウドについて不明点等がある場合は、担当部署及びMAFFクラウドCoEと協議の上、作業を進めること。また、クラウドサービスの提供に係る費用及び利用料は受注者の負担とする。
　本業務の遂行に当たっては、「農林水産省クラウド利用ガイドライン」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、「農林水産省クラウド利用ガイドラインの関係資料」を参考とすること。なお、農林水産省クラウド利用ガイドラインが改定された場合は、最新のものを参照し、その内容に従うこと。

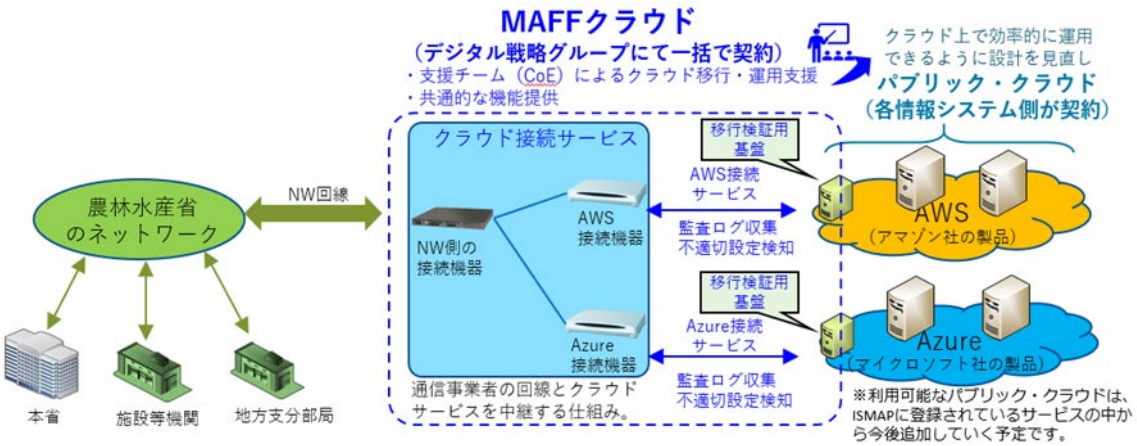


図３　MAFFクラウドの概要

（５）契約期間

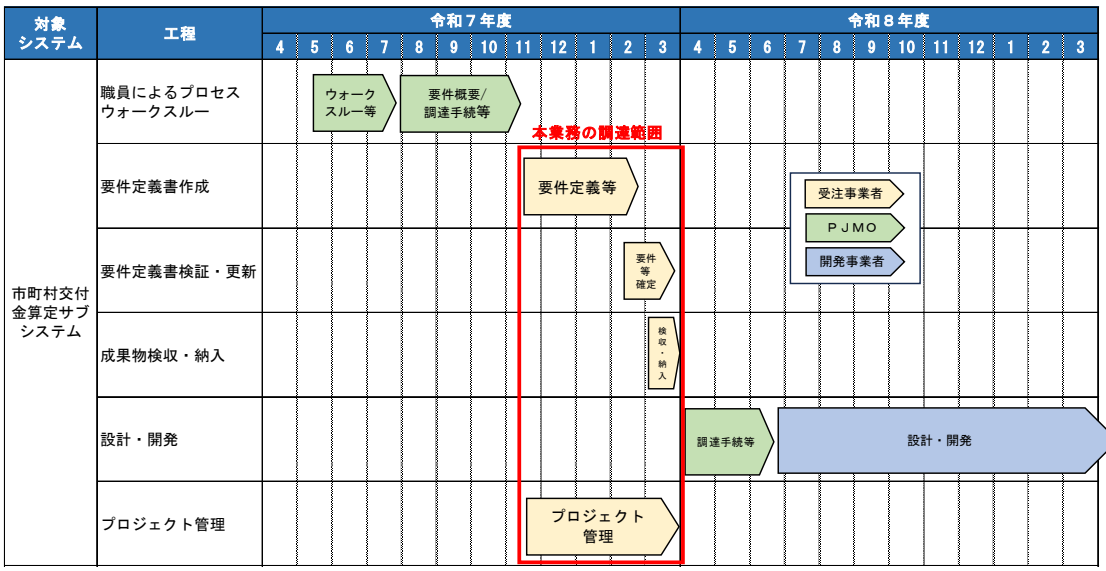
契約締結日から令和８年３月 13 日まで

（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。なお、本調達による要件定義結果に基づき、R6

次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務(工程２)のサブシステムとして設計・構築することを想定している。

図４　作業スケジュール



２　調達案件及び関連調達案件

（１）　調達範囲

本調達では、本プロセスに係る次期国有林野情報管理システムのサブシステムとしての位置づけで設計・開発業務を行うベースとなる要件定義を確定する業務を行うものとし、受注者の責任範囲は、本プロセスの業務分析から要件定義書作成までとする。

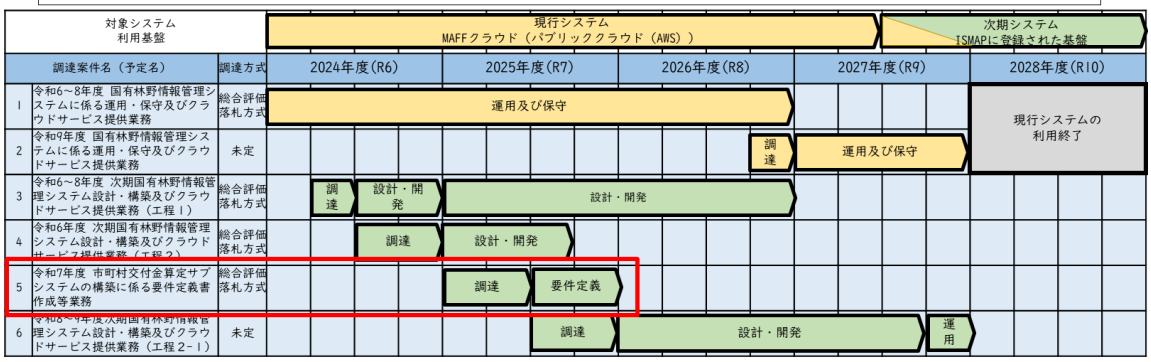
（２）　調達案件の一覧

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、実施時期等は次の表及び図のとおりである。

表　１　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	令和６～８年度国有林野情報管理システムに係る運用・保守及びクラウドサービス提供業務	一般競争入札 （総合評価）	令和6年 4月1日	令和5年10月 令和5年12月 令和6年3月	令和6年4月から 令和9年3月まで
2	令和９年度　次期国有林野情報管理システムに係る運用・保守及びクラウドサービス提供業務	一般競争入札 （総合評価）	令和10年 4月1日予定	令和7年10月頃 令和8年2月頃 令和8年3月頃	令和8年4月から 令和10年3月まで
3	令和６～８年度　次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務（工程１）	一般競争入札 （総合評価）	令和6年 11月14日	令和6年9月 令和6年10月 令和6年10月	令和6年10月から 令和9年3月まで
4	令和６年度　次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務（工程２）	一般競争入札 （総合評価）	令和7年 3月14日	令和6年10月 令和6年12月 令和7年3月	令和7年3月から 令和8年3月まで
5	令和７年度市町村交付金算定サブシステムの構築に係る要件定義書作成等業務	一般競争入札 （総合評価）	令和7年 11月頃予定	－ 令和7年9月頃予定 令和7年11月頃予定	令和7年11月から 令和8年3月まで
6	令和8～9年度次期国有林野情報管理システム設計・構築及びクラウドサービス提供業務	未定	令和7年 12月頃予定	未定	令和8年4月から 令和9年3月まで

整備スケジュール



※当初予算の状況により図5 No6が変更になる可能性があり、調達件名は仮とする。

図５　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）　調達案件間の入札制限

本業務において相互に入札制限の対象となる調達案件はないが、相互入札制限以外の制限については、「８（５）入札制限」を参照すること。

３　情報システムに求める要件

当業務の実施に当たっては、「別紙１要件概要」の各要件を満たすこと。

４　作業の実施内容

（１）　作業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、担当部署の指示に基づき、作業実施計画書及び作業実施要領の案を作成し、担当部署の承認を得ること。また、本業務における検討結果をプロジェクト計画書に適宜反映するとともに、プロジェクト計画書を段階的詳細化し、内容変更の支援をすること。

なお、作業実施計画書及び作業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：2025年5月27日以下「標準ガイ

ドライン」という。）で定義されているものとする。 なお、作業実施計画書には、以下の内容を記述し、作業実施計画書の内容に変更の必要が生じた場合は、変更の理由及び変更内容とともに修正された作業実施計画書を担当部署に書面にて届け出て承認を得ること。

①全体スケジュール（作業工程名、各作業工程の実施内容、実施期間、作業担当、各作業工程の完了条件を含む。）

②WBS及び詳細スケジュール（作成したWBSを元に、各作業の関連性（作業間の依存関係が明確になるようにスケジュールをガントチャートとして記述し、明確にすること。）、作業担当、開始・完了日等の制約、各作業項目の作業内容と成果物の関係を踏まえ整理するもの。）

③プロジェクト体制図（要員数、要員の経験・スキル、連絡先、作業計画と要員配置との対応関係も含む。）

④会議体ルール

⑤コミュニケーション管理（手段、様式を含む。）

⑥本業務の成果物を詳細に定義したドキュメント体系

⑦ドキュメント管理（採番ルール、版数管理を含む。）

⑧情報セキュリティ管理（請負先等を含む。）

⑨作業体制の管理手法

⑩品質管理、品質基準の設定

⑪リスク管理

⑫課題管理

⑬変更管理

（２） 要件定義内容の調整・確定

受注者は、担当部署と本調達案件の業務要件内容を確認・検討し、市町村交付金算サブシステムの要件定義書並びに工数・費用積算を含めた資料電子化調査結果報告書を作成・更新、担当部署の承認を受けるものとする。なお、調達支援については本業務の対象外とする。

その際、内容について調整すべき事項があれば、担当部署、関係部署、次期国有林野情報管理システム関係者と調整の上、結果に基づき要件定義書の修正・更新を行うこと。要件の調整内容は、担当部署及び関係するステークホルダーに提示し、合意形成を図りつつ進めること。

受注者は、要件定義書等を作成する際には、下記の項目を主眼として別紙1に記載している要件概要を基に検討・作成すること。また、サブシステム化の要件として下記の１） ～３）で整理した簡素化、効率化案について、各段階で行われている作業の所要時間や求められる書類の量などの業務実態を整理し、次期システム等の入力、申請を行いやすくする観点で、既存の業務フローに追記。その際、新様式の導入による効果が分かるように整理すること。

１）事務の負担軽減策の検討

２）申請及び報告の各種様式の見直し

３）様式の簡素化の検討

４）簡素化、効率化案についての議論、検討

５）業務フローの整理

受注者は、アーキテクチャ実装方式を検討する際は、CI/CD を原則とする開発・運用方式を検討すること、及び、合理的な調達単位の検討において、CI/CD実施による開発と運用保守の一体化等、担当部署による調達単位の整理を技術的観点から支援すること。

受注者は、「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（ 2024年10月８ 日内閣サイバーセキュリティセンター）」の点検を行い、要件定義書に反映すること。

（３） 資料電子化調査結果報告書の作成

ア．資料電子化調査の内容は以下のとおり。

(ア) 現在電子化が必要と想定される資料の例

① 貸付申請書

② 貸付契約書（図面等付属する資料を含む）

③ 固定資産税課税標準相当額一覧（市町村からの通知）等

イ．調査の範囲（抽出調査）

(ア) 代表的な１森林管理局における電子化

(イ) 代表的な３森林管理署における電子化（異なる局に所属する署を選定）

ウ．調査項目

(ア) 電子化により効率化が図れると判断する対象資料、資料名（以下、「対象資料」という。）

(イ) 抽出調査の拠点において対象資料の量（用紙サイズ、枚数等、データ量）

最適な電子化方法の調査

- PDF、Web 等による電子化、OCR の適用可否
- 国有林野情報管理システムのデータベースへの登録可否
- 電子化に当たり機密保持のため持ち出しが禁止されるかどうか
- その他最適な電子化の手法・保管方法

(ウ) 対象資料を特定のための作業量、最適な電子化方法を選定するため作業量及び電子化する作業量

(エ) 電子化したデータの活用方法及び市町村交付金算定サブシステムの構築に係る要件定義への反映

(オ) 全国的に電子化を行う際の総作業量、経費の試算、最適な手順及び課題

（４）引継ぎ

受注者は、ＰＪＭＯが本サブシステムの構築を行う際には、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及び質疑応答等の協力を行うこと。また、受注者は、

要件定義の作業経緯、残存課題等を文書化し、担当部署並びに開発時期に則し設計・開発業者に対して確実な引継ぎを行うこと。

（５）定例会等の実施

受注者は、担当部署と定例会を隔週（暫定）開催するとともに、業務の課題並びに進捗状況を作業実施要領に基づき報告すること。

受注者は、担当部署から要請があった場合、又は、受注者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

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、担当部署の承認を得ること。

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。

（６）契約金額内訳及び情報資産管理標準シートの提出

受注者は、標準ガイドライン「別紙２　情報システムの経費区分」に基づき区分等した契約金額の内訳が記載されたエクセルの電子データを契約締結後速やかに提出すること。なお、人件費については人件費単価ごとに工数を提示すること。再請負先がある場合は再請負先の法人番号と再請負金額を提示すること。

最大何次請負、再請負総額、累計契約額(前年度まで)、年度契約金額を提示すること。

受注者は、担当部署が定める時期に、情報資産管理標準シートを提出すること。

受注者は、標準ガイドライン「別紙３　調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業」に基づき担当部署から情報資産管理標準シートの作成を依頼された場合、次に掲げる事項について記載した様式について、担当部署が定める時期に、提出すること。

ア．ハードウェアの管理（MAFF クラウドの仕様に依存する。）

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外部サービスの管理

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(MAFF クラウド)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（MAFF クラウドの仕様に依存する。）

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

(７)成果物の作成

ア．成果物名

本業務の成果物を以下に示す。本業務の各成果物の納品期限は下表 No.1～No.4 を除き、最終納品の期日であり、各資料のレビューにおいての期日は、作業実施計画書に定めたスケジュールに合わせて提出時期を記載し、担当部署が必要な時期に内容確認できるように対応すること。

表 2 成果物一覧

No.	成果物名	納品期日
1	作業実施計画書	契約締結後10日以内
2	作業実施要領	契約締結後10日以内
3	作業実施要領に基づく管理資料	契約締結後10日以内

4	契約金額内訳及び情報資産管理標準シート	契約締結後10日以内
5	要件定義書(業務要件、機能要件、非機能要件)	契約の終了時
6	資料電子化調査結果報告書	契約の終了時
7	情報セキュリティ管理計画書	契約の終了時
8	引継計画書	契約の終了時
9	引継書	契約の終了時
10	業務実施結果報告書	契約の終了時

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（令和４年１月 11 日内閣官房長官通知）」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。

・ 作成した成果物は担当部署が指定したサーバへ納品（PrimeDrive 等）すること。
成果物は、Microsoft Office 又は PDF のファイル形式で作成すること。
納品後、担当部署において改変が可能となるよう、図表等の元データも併せて納品すること。

・ 成果物の作成に当たって、特別なツールを使用する場合は、担当部署の承認を得ること。

・ 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。

・ 不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

ウ．成果物の納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、担当部署が納品場所を別途指示する場合はこの限りではない。

〒100－8950
東京都千代田区霞が関 1-2-1
農林水産省　林野庁　国有林野部　経営企画課

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。

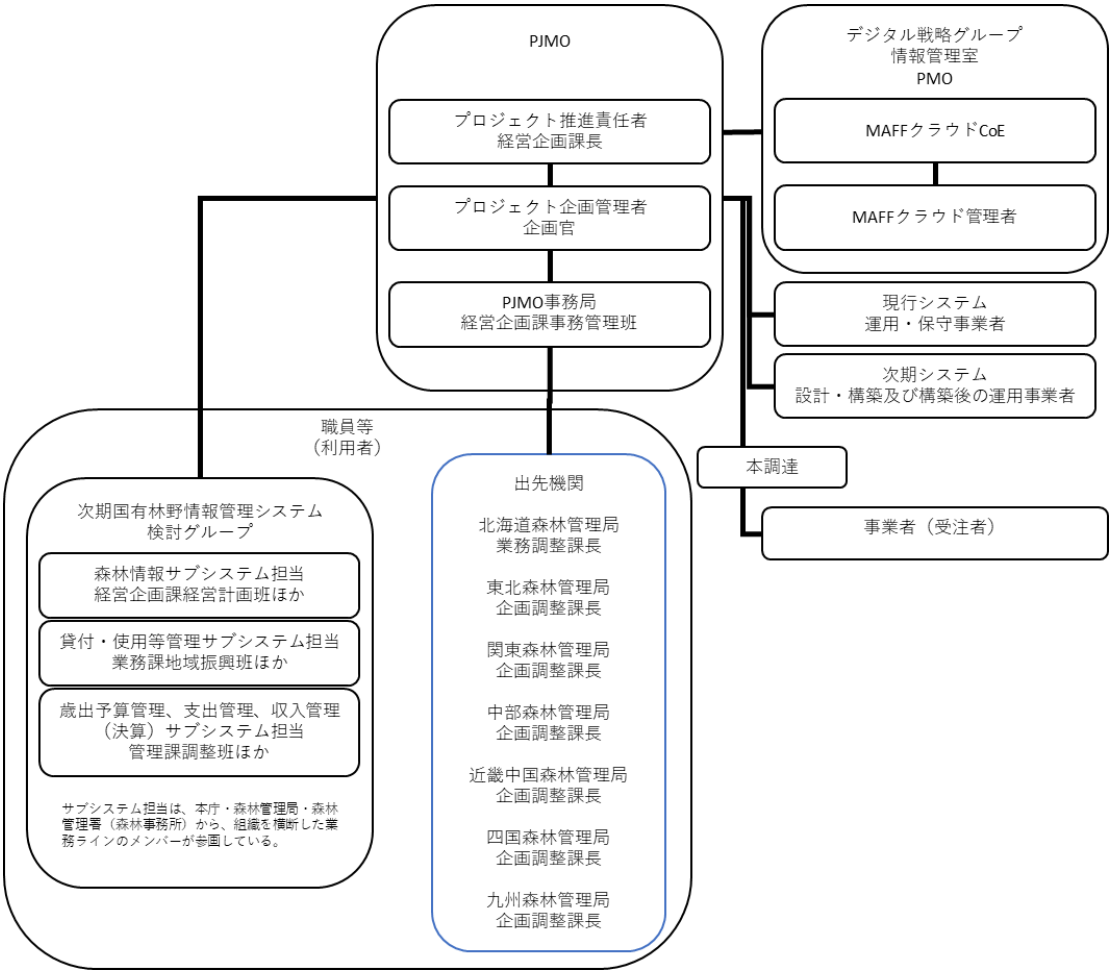


図６　本業務の推進体制及び本業務受注者に求める作業実施体制

表３　本業務における組織等の役割

組織等	本業務における役割
デジタル戦略グループ 情報管理室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合せを受け、対応、助言・指導等を行う。
MAFFクラウドCoE	担当部署・受注者に対してパブリッククラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。
PJMO(担当部署)	本システムの管理組織として、本業務の進捗等を管理する。
事業者(本業務の受注者)	本業務を実施する。
現行システム　運用・保守事業者	現行システムの運用・保守業務を行う。
次期システム　設計・	次期システムの設計・開発・構築並びに運用・保守事業を実施する。

組織等	本業務における役割
構築及び構築後の運用事業者	
職員等	国有林野情報管理システムの利用者

表４　本業務受注者における作業実施体制の役割

組織等	本業務における役割
業務遂行責任者	本業務全体を統括し、必要な意思決定を行う。また、関連する各組織・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。
チームリーダー	業務遂行責任者により任命された本業務を遂行するためのチームのリーダー
担当者	チームを構成するメンバー
品質管理者	本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。

（２）作業要員に求める資格等の要件

受注者は、本業務の業務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。

受注者における業務遂行責任者は、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。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当部署の了承を得ること。）。

チームリーダーは、情報システムの要件定義並びに設計・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。

ア．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) 担当する職務に応じた技術力（クラウド業務を実施する場合は、AWS、Azure のスキル）

イ．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を担当するチームのチームリーダーは以下の資格を有するものを含めること。

・ チームリーダーは、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上級資格[*1]を有する者を１名以上配置すること。なお、チームリーダーの資格は全体リーダー又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ーを支援する要員が保有していることでも可とする。又は、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、Azure 有償サポート）の利用での対応も可とする。なお、Azure の有償サポートとは、マイクロソフト社のプレミアサポートやユニファイドサポート等の“プロアクティブサービス“を指す。

（３）作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受注者の責任において用意すること。また、必要に応じて担当部署が現地確認を実施することができるものとする。

（４）作業の管理に関する要領

受注者は、担当部署が承認した作業計画書の作業体制、スケジュール等に従い、記載された成果物を作成すること。その際、作業実施要領に従い、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、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．担当部署から農林水産省における情報セキュリティの確保に関する規則（平成 27 年 3月 31 日農林水産省訓令第４号。以下「規則」という。）、「農林水産省における個人情報の適正な取扱いのための措置に関する訓令」等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。なお、「農林水産省における情報セキュリティの確保に関する規則」は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受注者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

イ．本業務に係る情報セキュリティ要件は次の通りである。

(ア) 請負した業務以外の目的で利用しないこと。

(イ) 業務上知り得た情報について第三者への開示や漏えいをしないこと。

(ウ) 持出しを禁止すること。

(エ) 受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

(オ) 受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

(カ) 受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の

事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

(キ) 受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

(ク) 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。

(ケ) 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 PJMO による実地調査が実施できること。

(コ) 上記以外に、別紙２「情報セキュリティの確保に関する共通基本仕様」に基づき、作業を行うこと。

(２)個人情報の取扱い

ア．個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の取扱いに係る事項について担当部署と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。

(ア) 個人情報の取扱いに関する責任者が情報管理責任者と異なる場合には、個人情報の取扱いに関する責任者等の管理体制

(イ) 個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等

イ．本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。なお、受注者はその旨を証明する書類を提出し、担当部署の了承を得た上で実施すること。

ウ．個人情報を複製する際には、事前に担当部署の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。なお、受注者は廃棄作業が適切に行われた事を確認し、その保証をすること。

エ．受注者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当部署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、担当部署からの指示に基づき、個人情報の取扱いに関して原則として年１回以上の実地検査を受け入れること。なお、やむを得ない理由により実地検査の受入れ

が困難である場合は、書面検査を受け入れること。また、個人情報の取扱いに係る業務を再請負する場合は、受注者（必要に応じ担当部署）は、原則として年１回以上の再請負先への実地検査を行うこととし、やむを得ない理由により実地検査の実施が困難である場合は、書面検査を行うこと。

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

（３）法令等の遵守

ア．関係法令の遵守

本業務の遂行に当たっては、日本国内法を適用すること。

イ．環境関係法令の遵守

受注者は、物品・役務（請負事業を含む）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 49 号）

(イ) 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）

(ウ) 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）

(エ) 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）

(オ) 労働安全衛生法（昭和 47 年法律第 57 号）

(カ) 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）

ウ．環境負荷低減に係る遵守事項

受注者は、役務の提供に当たり、新たな環境負荷を与えることにならないよう、事業の最終報告時に様式を用いて、以下の取組に努めたことを、環境負荷低減のクロスコンプライアンス実施状況報告書として提出すること。(別紙 3 参照) なお、全ての事項について「実施した／努めた」又は「左記非該当」のどちらかにチェックを入れるとともに、ア～エの各項目について、一つ以上「実施した／努めた」にチェックを入れること。

(ア) 環境負荷低減に配慮したものを調達するよう努める。

(イ) エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

(ウ) 廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

(エ) みどりの食料システム戦略の理解に努める。

（４）標準ガイドラインの遵守

本業務の遂行に当たっては、「デジタル社会推進標準ガイドライン群」のうち標準ガイドライン

（政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント）に該当する以下の①から⑥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。要件の策定に当たっては、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記載の留意事項等を参考に、クラウドサービスの利用に適した刷新に向け、適切に作業を進めること。

① DS-100 デジタル・ガバメント推進標準ガイドライン
② 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
③ 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
④ DS-900 Web サイト等の整備及び廃止に係るドメイン管理ガイドライン
⑤ 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
⑥ DS-920 行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン

（５）その他文書、標準への準拠

ア．プロジェクト計画書等

本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

対象外とする。

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

クラウドアーキテクチャーのベストプラクティス（AWS の場合 AWS Well-Architected Framework、Azure の場合 Azure 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。

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。

・AWS/Azure 設定確認リスト

・Web システム／Web アプリケーションセキュリティ要件書 (別紙２-１)

(８)クラウドサービス利用時の情報システムの保護に関する事項

情報システム、情報システムで取り扱うデータ等の情報資産の所有権その他の権利がクラウドサービスプロバイダーに帰属せず、また、発注者からクラウドサービスプロバイダーに移転されるものでないこと。

農林水産省の情報システムにおけるクラウドサービスの契約は、農林水産省をエンドカスタマーとしてクラウドサービスの再販を行うこと。

ガバメントクラウドでも MAFF クラウドでもないクラウドを使用する場合は、情報システムで取り扱うデータ等の情報資産の所有権その他の権利がクラウドサービスプロバイダーに移転されないクラウドサービスプロバイダーのみを使用すること。なお、ISMAP を取得したクラウドサービス（SaaS）を利用する場合は当たらない。

クラウドサービスの利用に当たり、情報資産が漏えいすることがないよう、必要な措置を講じること。

現在利用しているクラウドサービスの解約に伴うデータの削除については、クラウドサービスプロバイダーが定めるデータ消去の方法で、データ削除し、削除したことを証明する資料を提出すること。なお、クラウドサービスの契約を移管する場合は当たらない。

7　成果物の取扱いに関する事項

（１）知的財産権の帰属

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

イ．受注者に帰属する知的財産権を利用して本業務を行う場合、担当部署及びシステム利用者に受注者の知的財産権の利用を許諾する範囲及び制約を受注者が周知すること。

ウ．農林水産省は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、受注者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により農林水産省がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

エ．納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受注者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前に農林水産省の承認を得ることとし、農林水産省は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争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。

オ．本調達に係る成果物の権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び所有権は、検収に合格した成果物の引渡しを受けたとき受注者から農林水産省に移転するものとする。

カ．受注者は農林水産省に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

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

(２)契約不適合責任

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

イ．前記アの場合において、追完の請求にも関わらず相当の期間内に追完がなされないときは、農林水産省は、その不適合の程度に応じて支払うべき金額の減額を請求することができる。

ウ．前記イの規定にかかわらず、次に掲げる場合には、農林水産省は、相当の期間の経過を待つことなく、直ちに支払うべき金額の減額を請求することができる。

（ア）　追完が不能であるとき。

（イ）　受注者が追完を拒絶する意思を明確に表示したとき。

（ウ）　特定の日時又は一定の期間内に履行をしなければ本調達の目的を達することができない場合において、受注者が追完をしないでその時期を経過したとき。

（エ）　（ア）から（ウ）までに掲げる場合のほか、農林水産省が追完の請求をしても追完を受ける見込みがないことが明らかであるとき。

エ．農林水産省は、当該契約不適合（受注者の責めに帰すべき事由により生じたものに限る。）により損害を被った場合、受注者に対して損害賠償を請求することができる。

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

カ．前記アからオまでの規定にかかわらず、成果物の種類又は品質に関して契約不適合がある場合であって農林水産省が検収完了後１年以内に当該契約不適合について通知しないときは、農林水産省は、本仕様書に定める契約不適合責任に係る請求をすることができない。ただし、検収完了時において受注者が当該契約不適合を知り、若しくは重過失により知らなかったとき、又は当該契約不適合が受注者の故意若しくは重過失に起因するときはこの限りでない。

キ．前記アからオまでの規定にかかわらず、契約不適合が農林水産省の提供した資料等又は農林水産省の与えた指示によって生じたときは適用しないこと。ただし、受注者がその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りでない。

(３)検収

ア．本業務の受注者は、成果物等について、納品期日までに担当部署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、変更点について担当部署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．令和 7・8・9 年度全省庁統一資格の「役務の提供等」の「A」の等級に格付けされ、競争参加資格を有する者であること。

（2）公的な資格や認証等の取得

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

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

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

イ．応札者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。

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

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

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

（3）受注実績

ア．応札者は、本業務と類似する事業の受注実績を過去 3 年以内に有すること。

イ．応札者は、本システムで有する可能性のある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 5 年以内に有すること。

ウ．応札者は、本システムで導入予定（又は提案予定）のパブリッククラウドへの要件定義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

本業務を直接担当する農林水産省 IT 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請負先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。

９　再請負に関する事項

（１）　再請負の制限及び再請負を認める場合の条件

ア．本業務の受注者は、業務を一括して又は主たる部分を再請負してはならない。

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

ウ．受注者は再請負先の行為について一切の責任を負うものとする。

エ．再請負先における情報セキュリティの確保については受注者の責任とする。

オ．再請負を行う場合、「８．（５）入札制限」に示す要件を再請負の制限要件として読み替えること。

（２）承認手続

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

イ．前項による再請負の相手方の変更等を行う必要が生じた場合も、前項と同様に再請負に

関する書面を担当部署に提出し、承認を受けること。

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

（３）再請負先の契約違反等

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

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．本業務受注後に調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって農林水産省に申入れを行うこと。双方の協議において、その変更内容が軽微（請負料、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。

ウ．本業務に使用する言語（会話によるコミュニケーションを含む。）は日本語、数字は算用数字、単位は原則としてメートル法とすること。

エ．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。

オ．本仕様書について疑義等がある場合は、別紙４　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、担当部署内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に担当部署まで連絡の上、閲覧日時を調整すること。

ア．資料閲覧場所

東京都千代田区霞が関 1-2-1　林野庁国有林野部経営企画課（北別館８階ドア番号北 812）

イ．閲覧期間及び時間

(ア) 公告の日から入札終了の前日まで

(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

(エ) 最大５名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別添様式１「閲覧申込書」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添様式２「守秘義務に関する誓約書」に記載の上、提出すること。

ウ．閲覧時の注意

(ア) 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。

(イ) 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、下記オ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。

エ．連絡先

林野庁国有林野部経営企画課

電話 03－3502－6008

オ．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。

・プロジェクト計画書、プロジェクト管理要領
・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
・現行の業務分析結果
・農林水産省クラウド利用ガイドライン及び関係資料
・過去の検討資料等

１１　付属文書

(１)別紙１　要件概要
(２)別紙２　情報セキュリティの確保に関する共通基本仕様
(３)別紙３　環境負荷低減のクロスコンプライアンス実施状況報告書
(４)別紙４　質問書

以　上

(別紙 1)

国有林野情報管理システム-市町村交付金算定サブシステム要件概要

1 市町村交付金制度とは

・市町村交付金は、地方税法第 348 条第 1 項において固定資産税を課することができないと されている国及び地方公共団体等が所有する固定資産のうち、当該固定資産を所有する国又 は地方公共団体以外の者が使用している固定資産又は国有林野に係る土地等につき、当該固 定資産所在の市町村に対して交付するもの

・地方自主財源の増強に資することを目的とするものであって、固定資産税に代わるべきものとして設けられた制度

・市町村交付金の客体たる固定資産は、固定資産税の課税客体たる固定資産と同意義であること、その算定率は固定資産税の標準税率である 100 分の 1.4 を採用していること等から、実質的には地方税制度の固定資産税と同様に観念されるべき性格を有している。反面、現行地方税制とは別個の制度とされているため、地方税一般に適用される通則的規定に相当するような規定は設けられていないので、交付金制度の運用については、必ずしも固定資産税と同一に取り扱うことができない

・交付金算定にあたっては、関係法令及び長官通知に基づき適正に算定する必要がある
・国有資産等所在市町村交付金法（以下、「法」という。）第２条第１項各号による交付客体で森林管理局署に関連する固定資産については以下のとおり。
ただし、「５ 交付客体としない固定資産（非交付客体）」のとおり、非交付客体となる場合があるので留意。
（１）国有林野の管理経営に関する法律（昭和 26 年法律第 246 号。以下「管理経営法」という。）第２条第１項に規定する国有林野に係る土地。（以下、「国有林野」という。）
（２）国以外の者に使用させている国有林野以外の固定資産※１。（以下、「貸付資産」という。

５ 交付客体としない固定資産

次に掲げる固定資産は、法第２条第２項の規定に基づき交付客体としない。

主な固定資産	根　拠 （法第２条第２項）	プログラムでの控除方法
(1)国家公務員宿舎法（昭和 24 年法律第 117 号）第 12 条の無料宿舎の用に供する固定資産 **非交付客体**となるのは、へき地にある官署に勤務する職員等が貸与されている**無料宿舎**。行政専門員等が**有償**で貸与されている場合は**交付客体**となる。	第２号	台帳入力 ※台帳入力時に当該固定資産を入力しない。
(2)当該国有林野所在の市町村（隣接する市町村含む）又は当該市町村を包括する都道府県が分収造林契約の造林者又は分収育林契約の費用負担者である国有林野 分収育林は、当該市町村等の持分割合に相当する面積のみが交付の客体とならない。	第５号	控除該当
(3)日米間の地位協定の実施に伴い使用させている固定資産　**【例】同協定に基づく訓練場、通信施設等**	第６号	控除該当（※１）
(4)付属地（林道、苗畑、貯木場等）に係る国有林野 国有財産台帳に登載されている付属地が該当。作業道、国以外の者に貸し付け又は使用させている場合を除く。	第７号	森林情報の面積区コード（※２）
(5)河川敷（沢敷）に係る国有林野	第７号	森林情報の面積区コード
(6)レクリエーションの森のうち、森林レクリエーション施設の用に供している国有林野（国が実施主体）	第７号	森林情報の面積区コード（※２）
(7)宗教法人法第３条に規定する境内地の用に供するため、貸し付け又は使用させている国有林野 **【例】境内建物では、本殿、社務所等。境内地では、境内建物が存する一画の土地、参道、庭園、山林等**	第７号	控除該当
(8)墓地の用に供するため、貸し付け又は使用させている国有林野 **【例】地方公共団体が所有する斎場、墓地、霊園地等**	第７号	控除該当
(9)公共の用に供する道路、運河用地及び水道用地のため、貸し付け又は使用させている国有林野又は貸付資産 **【例】道路法の適用を受ける道路敷（道路法第 32 条第１項の規定の工作物等を継続して使用を許可された特定部分、広く不特定多数の人の利用に供されている林道、農道等を含む）** **市町村住民の給水を目的とした水道の水源地、貯水池、沪水場、ポンプ場及び水道線路敷**	第７号	控除該当 台帳入力
(10)公共の用に供する用悪水路、ため池、堤とう及び井溝のため、貸し付け又は使用させている国有林野又は貸付資産 **【例】農耕用のかんがい用水路、悪水排泄用水路、耕地かんがい用の用水貯水池、防水堤防、田畝又は村落間の通水路**	第７号	控除該当 台帳入力
(11)文化財保護法の規定により、史蹟、名勝又は天然記念物として指定されている国有林野	第７号	森林情報の面積区コード（※２）
(12)学校教育法第１条に規定する学校の施設の用に供するため、貸し付け又は使用させている国有林野又は貸付資産	第７号	控除該当 台帳入力
(13)生活保護法等に規定する包括的支援事業の用に供す	第７号	控除該当

る施設及び社会福祉事業の用に供するため、社会福祉法人に貸し付け又は使用させている国有林野又は貸付資産 **【例】救護施設、児童養護施設、養護老人ホーム等**		台帳入力
(14)国家公務員共済組合法第 12 条第２項又は同法第 36 条において準用する同法第 12 条第２項の規定により、無償で国家公務員共済組合又は国家公務共済組合連合会の利用に供するため、貸し付けている貸付資産 **【例】食堂等**	第８号	台帳入力
(15)管理経営法第７条の規定により地方公共団体に貸し付け又は使用させている国有林野	第８号	控除該当
(16)管理経営法第８条の２第１項又は第８条の３の規定により、その対価を無償又は時価よりも低く定めて貸し付け又は使用させている国有林野 **【例】採草放牧地等**	第８号	控除該当
(17)旧沖縄県地方費をもって経営した国有林に関する件（明治 42 年勅令第 32 号）に基づく契約により沖縄県に貸し付けている国有林野 **【例】勅令貸付国有林**	第８号（※３）	控除該当
(18)その他（前各号に該当しない）公用又は公共の用に供するため、国並びに都道府県、市町村、特別区、これらの組合又は財産区に貸し付け又は使用させている国有林野又は貸付資産 ※国有財産法の規定に基づき、貸し付け又は使用させているもの。 **【例】公用では、試験場、警察消防関係施設、社会事業児童福祉施設等。公共の用では、公園、運動場等**	第７号	控除該当 台帳入力

2　機能概要

1）マスタ更新(市町村コードなど各種コード、局、署、係数(率)、伐採方法、算定年度など)
2）データファイルの保存
3）保存データの取り込み、ファイル出力
4）データ、ファイル等の検索機能
5）期間(年度別等)による保存と取り出し
6）データ、ファイル、一覧表等の伝達機能(メール形式)
7）印刷機能
8）帳票のD/Lと更新、更新後データの取り込み
9）入力時、データ不整合時等のエラー機能

国有林野情報管理システム－市町村交付金算定サブシステム　（業務

作業は前年の3月31日
時点の内容により開始

国有林野の算定方法（特例算定）
面積（国有林全面積－非交付客体）×単価
（固定資産税課税標準相当額）×修正率（法規制により修正率異なる）＝交付金算定標準額

現行業務処理

処理、対応上の注意点

システム/ファイル

刷新システム
調査簿
保安林
法令
地位
雑面積

調査簿データ（5ファイル）

市道等は数値の変動要

局プログラム取込データ（11ファイル）
固定資産税課税標準相当額一覧表
財産台帳
控除該当固定資産等一覧表
市町村コード
森林情報データ

市町村交付金
算定プログラム
(算定P)

署算定プログラム
(署算定P)
(Excel)
固定資産税課税標準相当額一覧表
財産台帳
控除該当固定資産等一覧表
市町村コード
森林情報データ

BEファイル
APPファイル

※単価などの因子がBEにあり、APPで計算

異動通知書
修正通知書

※国としては宿舎分などは除外

※除外通知書に記載されている根拠条文について特別区の場合は条文が異なる（東京都関係）

局（7局）（約1000市町村）

国有林野情報管理システムの調査簿データ（5ファイル）を旧型式へAccessで変換

※CSVでD/L
※自局分のみアクセス可
※変換に2-3日かかる
※新規法令追加に伴う旧コード選択は人局担当の判断

旧型式へ変換されたファイルを局プログラムの森林データへ読み込み

局データ取込
※局で実施している作業

森林情報コード確認・修正
※局で実施している作業

メールまたはSharepointで配布(局→署)

署算定Pからファイル出力
局算定Pへファイル取込

データの取り込み・各種データ確認・修正
（交付金仮算定（財産台帳価格等未確定））
【広さのデータ】

※1署分ずつ読み込み
※時間がかかる
※宿舎等(貸付資産)の算定はExcelでok。ただし、国有林野分については、財産台帳価格との比較を行なうためその処理が必要
※財産台帳価格、交付金算定標準額を決定

交付金算定
（本算定（財産台帳価格確定））

負担調整措置確認
当年度評価額の決定
【単価データ】

当年度価格の決定について
財産台帳価格（基本算定）と固定資産税課税標準相当額（特例算定）を比較した結果から次の算定額を表示。（控除額反映）
〈基本算定額が特例算定額の２倍以上〉→　「特例算定額」
〈基本算定額が特例算定額の２倍未満〉→　「基本算定額」
その後、前年度価格と比較し負担調整措置を実施のうえで、当年度価格が決定される。

市町村選択後、印刷
※1市町村分のみ指定

署（約100署）

各種データ確認・入・削除（交付金の控除対象など）を実施

※CSVでD/L
※自署分のみアクセス可

ファイル更新

※森林情報データは法令に基づき交付金の対象からコード変換により除外対象有
※国有林野の算定においては、山林以外に「牧場」「宅地（住宅の用）」「鉱泉地」による算定が必要。
※次期計画樹立前に国有林野を売払いしていた場合は、森林情報データを削除するのではなく、控除一覧に入力し控除している

国有林野情報管理システム－市町村交付金算定サブシステム　（業務フロー：システム化対象(案)）

作業は前年の3月31日時点の内容により開始

国有林野の算定方法（特例算定）
面積（国有林全面積－非交付客体）×単価
（固定資産税課税標準相当額）×修正率（法規制により修正率異なる）＝交付金算定標準額

現行業務処理
新システムでの対応対象と考えられる要件
処理、対応上の注意点

システム/ファイル

刷新システム
調査簿
保安林
法令
地位
雑面積

調査簿データ（5ファイル）

市道等は数値の変動要

局プログラム取込データ（11ファイル）
固定資産税課税標準相当額一覧表
財産台帳
控除該当固定資産等一覧表
市町村コード
森林情報データ

市町村交付金算定プログラム（算定P）

署算定プログラム（署算定P）（Excel）
固定資産税課税標準相当額一覧表
財産台帳
控除該当固定資産等一覧表
市町村コード
森林情報データ

BEファイル
APPファイル

※単価などの因子がBEにあり、APPで計算

異動通知書
修正通知書

※国としては宿舎分などは除外

※除外通知書に記載されている根拠条文について特別区の場合は条文が異なる（東京都関係）

局（7局）（約1000市町村）

新システムでの対応対象として検討
※Accessのロジック(主にコード変換)分析要
・コード変換対象はマニュアルに記載
※調査簿をコード変換後提供
※次期刷新システムに内に取り込まれると、コード変換（本機能）は不要になるが、その代わりデータ連携（データモデリング）を新たに行う必要がある

国有林野情報管理システムの調査簿データ（5ファイル）を旧型式へAccessで変換

※CSVでD/L
※自局分のみアクセス可
※変換に2-3日かかる
※新規法令追加に伴う旧コード選択は人局担当の判断

次期システムでは取込不要

旧型式へ変換されたファイルを局プログラムの森林データへ読み込み

次期システムでは取込不要（データ連携は新たに構築必要）

局データ取込
※局で実施している作業

新システムでの対応対象

森林情報コード確認・修正
※局で実施している作業

新システムでの対応対象として検討（貸付資産（宿舎等）の入力を除く）

メールまたはSharepointで配布(局→署)

各種データ確認・入・削除（交付金の控除対象など）を実施

※CSVでD/L
※自署分のみアクセス可

ファイル更新

署算定Pからファイル出力
局算定Pへファイル取込

※森林情報データは法令に基づき交付金の対象からコード変換により除外対象有
※国有林野の算定においては、山林以外に「牧場」「宅地（住宅の用）」「鉱泉地」による算定が必要。
※次期計画樹立前に国有林野を売払いしていた場合は、森林情報データを削除するのではなく、控除一覧に入力し控除している

・現行システムでは、山林以外の地目により算定する場合は、当該地目による算定を行なう際に対象の山林面積について手動で控除しなければならなかったが、次期システムでは山林控除を手動で行なわなくても対応する
・次期システムでは、森林計画の樹立に係わらず森林調査簿が更新されれば、その時点で売払い面積の控除を行なわなくても済むようにする

データの取り込み・各種データ確認・修正（交付金仮算定（財産台帳価格等未確定））【広さのデータ】

新システムでの対応対象として検討

※※1署分ずつ読み込み
※時間がかかる
※宿舎等(貸付資産)の算定はExcelでok。ただし、国有林野分については、財産台帳価格との比較を行なうためその処理が必要
※財産台帳価格、交付金算定標準額を決定

新システムでの対応対象として検討

交付金算定（本算定（財産台帳価格確定））

新システムでの対応対象として検討
基本算定（財産台帳価格）と特例算定（固定資産税）の比較計算の実施

負担調整措置確認
当年度評価額の決定
【単価データ】

当年度価格の決定について
財産台帳価格（基本算定）と固定資産税課税標準相当額（特例算定）を比較した結果から次の算定額を表示。（控除額反映）
〈基本算定額が特例算定額の２倍以上〉→　「特例算定額」
〈基本算定額が特例算定額の２倍未満〉→　「基本算定額」
その後、前年度価格と比較し負担調整措置を実施のうえで、当年度価格が決定される。

新システムでの対応対象として検討
・複数選択可能
・署単位/局単位も可とする
次期システムで算定を行なう国有林野ではない貸付資産の情報について通知書への追記方法について検討

市町村選択後、印刷
※1市町村分のみ指定

・移行時にイニシャライズとして【前年度末の】貸し付け台帳、調査簿(?)を整理、登録し、それを基に更新する流れを想定

・次年度や年途中の計算結果のシミュレーション機能付加

・控除対象や財産台帳の計算のもととなる表、市町村コード表等の刷新システムとの共有、取り込み(マスター管理)
・現行算定プログラムで出力できた様式帳票について対応可能か検討

・刷新システムのサブシステムとしての位置づけ(メニュー追加、マスター管理)

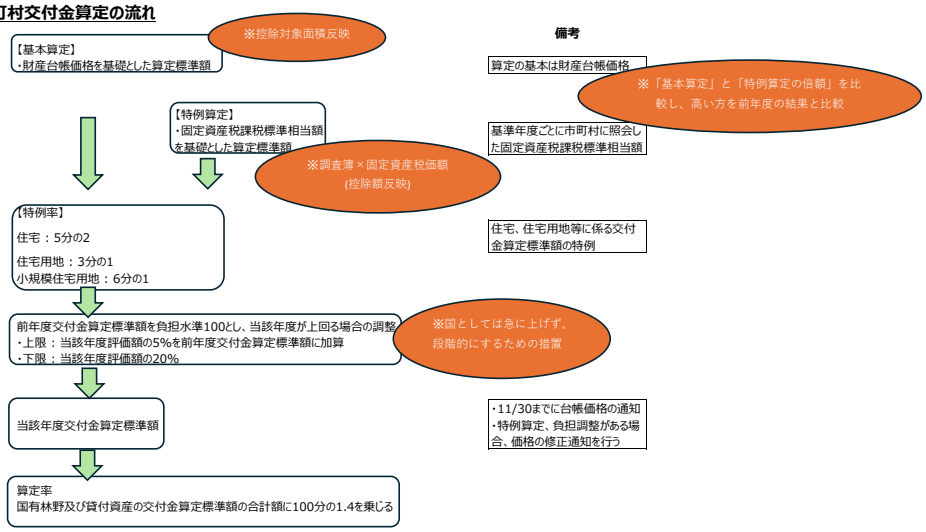
署（約100署）

国有林野情報管理システム－市町村交付金算定サブシステム　システム化要件(案)

現行処理・業務					システム化要件(案)	
現行業務実施時期	署	局	市町村	林野庁	システム機能(案)	備考/要検討事項
4月	⑥情報、データ、コードなどの更新・修正 ⑦財産台帳入力 ⑧入力確認後、局へ報告	③情報、データ、コードなどの取り込みと更新・修正(国有林野情報管理システムの調査簿データ（5ファイル）を旧型式へAccessで変換 ④署へ作業依頼 ⑤市町村からの請求額の妥当性確認	②固定資産価格(修正)通知に基づく交付金の請求	①局への算定作業依頼	⓪作業は前年の3月31日時点の内容により開始 ①林野庁から各局への算定作業依頼メール発信機能 ②固定資産価格のファイルでの検証と更新、更新後の局への請求申請処理 ③自局担当データの閲覧、データの取り込み(D/L)、更新後のU/Lとそれによるシステムデータ更新と確定 ※次期刷新システムでAccessのコード変換、データ取込の代わりにデータ連携（データモデリング）を行う ④③に基づいた、局から担当署の選択後、データ連携機能(含む、作業依頼メール発信機能等)による伝達 ⑤②に基づいた請求額の確認のためのデータ取得と必要に応じた修正依頼処理とその連携機能 ⑥各署担当データの閲覧、データの取り込み(D/L)、更新後のU/Lとそれによるシステムデータ更新と確定処理 ※控除対象（貸付資産（宿舎等））の入力の除外処理 ⑦⑥に基づいた財産台帳作成・更新と保存 ⑧⑦の結果を署内の検証、承認後、局にデータ連携で伝達	・現在使用しているAccessのロジック(主にコード変換)の分析が必要(コード変換対象はマニュアルに記載) ・ベースの機能と特殊処理 ・必要に応じ各署、局で異なる処理への対応 ・確定、申請・承認、差戻のワークフロー ・過去分との差分の表示の要否 ・このシステムの位置づけ(サブシステム?) ・データの保管先(MAFFクラウド?)とその期間 ・次処理への通知・伝達方法(データ連携方法) ・各署、局、市町村の地域別区分を設けて複数選択、処理可能(含む、印刷対象など) ・各処理の進捗トラッキング、必要に応じリマインド機能 ・交付客体としない固定資産（非交付客体）」のとおり、非交付客体となる場合がある ・アクセス可能対象データの絞り込み
5月		⑨請求額に基づく交付金額の確定 ⑩情報・データの取り込み、チェック ⑪算定・報告			⑨⑧に基づいた請求額の確定(データ連携による情報伝達(確認依頼メール、ステータスチェックなど)とファイル内容の確認と修正機能) ⑩各署担当データの閲覧、データの取り込み(D/L)、更新後のU/Lとそれによるシステムデータ更新と確定（交付金仮算定（財産台帳価格等未確定）） ⑪⑩の結果を局内の検証、承認交付金算定（本算定（財産台帳価格確定）） ※当年度評価額の決定時には基本算定（財産台帳価格）と特例算定（固定資産税）の比較計算の実施サポート機能	・各処理の進捗トラッキング、必要に応じリマインド機能 ・確定、申請・承認、差戻のワークフロー ・各署、局、市町村の地域別区分を設けて複数選択、処理可能(含む、印刷対象など) ・算定を行なう国有林野ではない貸付資産の情報について通知書への追記方法について要検討 ・山林以外の地目により算定する場合は、当該地目による算定を行なう際に対象の山林面積について手動で控除しているのをマスター、コード、テーブルなどにより自動計算対応検討 ・森林計画の樹立に拘わらず森林調査簿が更新されれば、その時点で売払い面積の控除を行なわなくても済むように検討
6月		⑫交付金の交付			⑫交付金の確定後、交付金の交付	・当システムの対象とするか検討要
8月				⑬予算概算要求	⑬⑫に基づいた林野庁での概算要求を行うための集計結果一覧のファイルの提供	・各地域別、局、署別に区分できる一覧表の提供
11月		⑭台帳価格改定 ⑮林野庁に報告 ⑯次年度分固定資産価格通知			⑭⑫の結果に基づいた台帳の検証と確定と結果の保存(年度別) ⑮⑫の結果をワークフローを使用し林野庁に報告 ⑯次年度分固定資産価格を各市町村にワークフローを使い伝達	

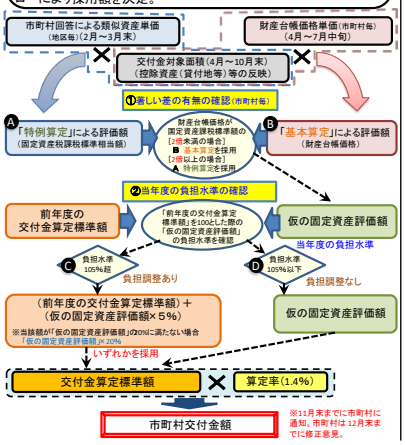
12月			⑰価格修正の申し出	⑱予算概算決定	⑰⑯の結果を確認し、差異があった場合は当該局にワークフローを介して伝達。局は、その結果の妥当性を確認後、必要に応じ更新し、結果を保存 ⑱⑰に基づいた林野庁での概算要求を行うための集計結果一覧のファイルの提供	・変更箇所の明示
その他のシステム機能					・移行時にイニシャライズとして【前年度末の】貸し付け台帳、調査簿を整理、登録し、それを基に更新する流れを想定 ・控除対象や財産台帳の計算のもととなる表、市町村コード表等の刷新システムとの共有、取り込み(マスター管理) ・次年度や年途中の計算結果のシミュレーション機能 ・刷新システムのサブシステムとしての位置づけ(メニュー追加、マスター管理)	・現行算定プログラムで出力できた様式帳票について対応可能か検討 ・期間(年度別等)による保存と取り出し(閲覧、D/L、印刷)、期間外(特に過去分)の更新については要検討
					・資料電子化調査結果報告書の作成 現在電子化が必要と想定される資料の例 ①貸付申請書 ②貸付契約書（図面等付属する資料を含む） ③固定資産税課税標準相当額一覧（市町村からの通知）等 ・調査項目 (ア)電子化により効率化が図れると判断する対象資料、資料名（以下、「対象資料」 (イ)抽出調査の拠点において対象資料の量（用紙サイズ、枚数等、データ量） ・最適な電子化方法の調査 (ア)PDF、Web等による電子化、OCRの適用可否 (イ)国有林野情報管理システムのデータベースへの登録可否 (ウ)対象資料を特定のための作業量、最適な電子化方法を選定するため作業量及び電子化する作業量 (エ)電子化したデータの活用方法及び市町村交付金算定サブシステムの構築に係る要件定義への反映	・ 電子化にあたり機密保持のため持ち出しが禁止されるかどうか ・ その他最適な電子化の手法・保管方法 ・ PDF、Web等による電子化、OCRの適用可否 ・ 国有林野情報管理システムのデータベースへの登録可否 ・ 電子化にあたり機密保持のため持ち出しが禁止されるかどうか ・ 全国的に電子化を行う際の総作業量、経費の試算、最適な手順及び課題

市町村交付金算定の流れ

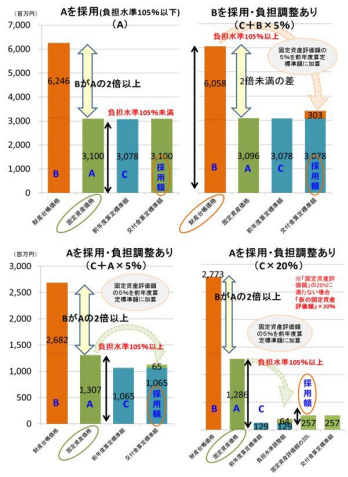


市町村交付金算定の流れ

○基本算定額と特例算定額が著しく異なっていなかった場合は、負担調整措置等を講じることなく、基本算定額を採用。この際の著しく異なっているかの判断は、財産台帳価格と固定資産税課税標準相当額の基の価格の評価方法が異なることから、基本的には著しく異なる価格として対応。
○基本算定額と特例算定額が著しく異なっている場合は、以下のフローにより採用額を決定。



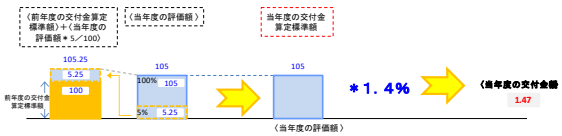
算定例



林野庁長官通知第３－７に基づく負担調整措置の概要

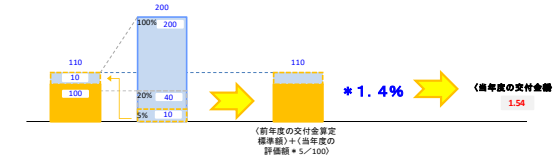
◆関係法令：地方税法　附則第18条

【負担調整なし】当年度の評価額が、前年度の交付金算定標準額に当年度の評価額の5%を加算した額に満たない場合。

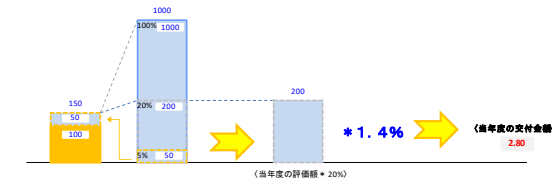


※例示した数値の単位は「万円」とする。

【負担調整5%】当年度の評価額が、前年度の交付金算定標準額に当年度の評価額の5%を加算した額を上回り、前年度の交付金算定標準額に当年度の評価額の5%を加算した額が当年度の評価額の20%以上となる場合。



【負担調整20%】当年度の評価額が、前年度の交付金算定標準額に当年度の評価額の5%を加算した額を上回り、前年度の交付金算定額に当年度の評価額の5%を加算した額が今年度の評価額の20%に満たない場合。



（注）交付金法第4条に基づく住宅等の特例率は、算定の過程で乗じているものとして仮定。

市町村交付金に係わる森林調査簿データとの関係性について

国有林野の算定方法

山林の交付金算定標準額は状況類似地区（林産物の搬出の便等のおおむねその状況が類似していると認められる単位の区域。）を市町村ごとに設定し、当該山林に係る固定資産税の課税標準の基礎となるべき価格に相当する額の単価に状況類似地区内に所在する山林面積（非交付客体を除く。）を乗じて算定している。

森林調査簿データとの関係性イメージ

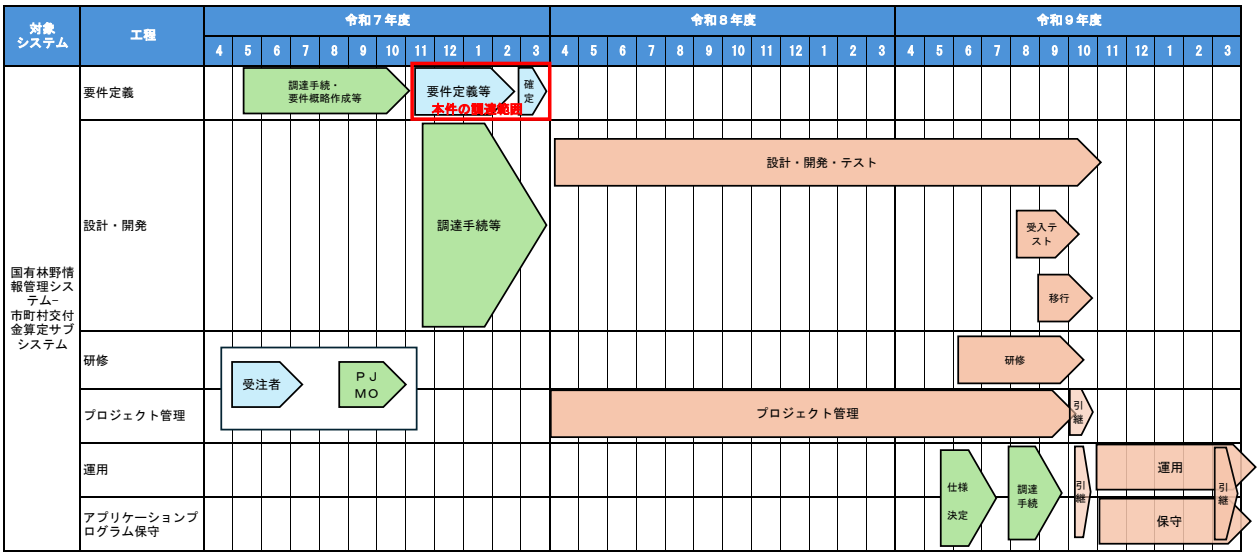
市町村名	林班	小班
○○市	10	い
○○市	11	ろ
○○市	12	は
○○町	100	に
○○町	110	ほ
○○町	120	へ
○○村	150	と
○○村	160	い
○○村	170	ろ

森林調査簿データを状況類似地区を整理番号で分類

市町村名	林班	小班	状況類似地区
○○市	10	い	1
○○市	11	ろ	1
○○市	12	は	2
○○町	100	に	3
○○町	110	ほ	4
○○町	120	へ	4
○○村	150	と	5
○○村	160	い	6
○○村	170	ろ	7

状況類似地区毎の法的規制等毎の修正率により分類。
※法的規制が重複している場合は、大きい法的規制の修正率を採用

市町村名	林班	小班	状況類似地区	修正率区分
○○市	10	い	1	0.7
○○市	11	ろ	1	0.2
○○市	12	は	2	0.5
○○町	100	に	3	0.2
○○町	110	ほ	4	0.5
○○町	120	へ	4	0.2
○○村	150	と	5	0.7
○○村	160	い	6	0.2
○○村	170	ろ	7	0.5


対象システム
工程
令和７年度
令和８年度
令和９年度
4 5 6 7 8 9 10 11 12 1 2 3
4 5 6 7 8 9 10 11 12 1 2 3
4 5 6 7 8 9 10 11 12 1 2 3
国有林野情報管理システム－市町村交付金算定サブシステム
要件定義
設計・開発
研修
プロジェクト管理
運用
アプリケーションプログラム保守
調達手続・要件概略作成等
要件定義等
本件の調達範囲
確定
調達手続等
設計・開発・テスト
受入テスト
移行
受注者
ＰＪＭＯ
研修
プロジェクト管理
引継
仕様決定
調達手続
引継
運用
保守
引継

（別紙　2）

情報セキュリティの確保に関する共通基本仕様

Ⅰ　情報セキュリティポリシーの遵守

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

なお、規則は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

2　受託者は、規則と同等の情報セキュリティ管理体制を整備していること。

3　受託者は、本業務の従事者に対して、規則と同等の情報セキュリティ対策の教育を実施していること。

Ⅱ　応札者に関する情報の提供

1　応札者は、応札者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を提出すること。

なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（〇〇国籍の者が△名（又は□%）等）を記載すること。また、この場合であっても、担当部署からの要求に応じて、可能な限り要員に関する情報を提供すること。

2　応札者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

（1）ISO/IEC27001 等の国際規格とそれに基づく認証の証明書等

（2）プライバシーマーク又はそれと同等の認証の証明書等

（3）独立行政法人情報処理推進機構（IPA）が公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が4に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書

Ⅲ　業務の実施における情報セキュリティの確保

1　受託者は、本業務の実施に当たって、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。

（1）本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても、第三者に開示し、又は本業務以外の目的で利用しないこと。

（2）本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結す

ること。

（3）本業務に係る情報を適切に取り扱うことが可能となるよう、情報セキュリティ対策の実施内容及び管理体制を整備すること。なお、本業務実施中及び実施後において検証が可能となるよう、必要なログの取得や作業履歴の記録等を行う実施内容及び管理体制とすること。

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

（5）農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、農林水産省又は農林水産省が選定した事業者による立入調査等の情報セキュリティ監査（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 26 条第1項第2号に基づく監査等を含む。以下同じ。）を受け入れること。また、担当部署からの要求があった場合は、受託者が自ら実施した内部監査及び外部監査の結果を報告すること。

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

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

2　受託者は、委託期間を通じて以下の措置を講ずること。

（1）情報の適正な取扱いのため、取り扱う情報の格付等に応じ、以下に掲げる措置を全て含む情報セキュリティ対策を実施すること。また、実施が不十分の場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。

ア　情報セキュリティインシデント等への対処能力の確立・維持

イ　情報へアクセスする主体の識別とアクセスの制御

ウ　ログの取得・監視

エ　情報を取り扱う機器等の物理的保護

オ　情報を取り扱う要員への周知と統制

カ　セキュリティ脅威に対処するための資産管理・リスク評価

キ　取り扱う情報及び当該情報を取り扱うシステムの完全性の保護

ク　セキュリティ対策の検証・評価・見直し

（2）本業務における情報セキュリティ対策の履行状況を定期的に報告すること。

（3）本業務において情報セキュリティインシデントの発生、情報の目的外使用等を認知した場合、直ちに委託事業の一時中断等、必要な措置を含む対処を実施すること。

（4）私物（本業務の従事者個人の所有物等、受託者管理外のものをいう。）の機器等を本業務に用いないこと。

（5）本業務において取り扱う情報が本業務上不要となった場合、担当部署の指示に従い返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

3　受託者は、委託期間の終了に際して以下の措置を講ずること。

（1）本業務の実施期間を通じてセキュリティ対策が適切に実施されたことを書面等により報告すること。

（2）成果物等を電磁的記録媒体により納品する場合には、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処するとともに、確認結果（確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等）を成果物等に記載又は添付すること。

（3）本業務において取り扱われた情報を、担当部署の指示に従い返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

4　受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、担当部署に報告し、協議の上、対策を講ずること。

Ⅳ　情報システムにおける情報セキュリティの確保

1　受託者は、本業務において情報システムに関する業務を行う場合には、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。

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

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

2　受託者は、本業務において情報システムの運用管理機能又は設計・開発に係る企画・要件定義を行う場合には、以下の措置を実施すること。

（1）情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、情報システム運用時に情報セキュリティ確保のために必要となる管理機能や監視のために必要な機能を本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

ア　情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

イ　情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

（ア）農林水産省外と通信回線で接続している箇所における外部からの不正アクセスやサービス不能攻撃を監視する機能

（イ）不正プログラム感染や踏み台に利用されること等による農林水産省外への不正な通信を監視する機能

（ウ）端末等の農林水産省内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能

（エ）農林水産省内通信回線への端末の接続を監視する機能

（オ）端末への外部電磁的記録媒体の挿入を監視する機能

（カ）サーバ装置等の機器の動作を監視する機能

（キ）ネットワークセグメント間の通信を監視する機能

（2）開発する情報システムに関連する脆（ぜい）弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

ア　既知の脆（ぜい）弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

イ　開発時に情報システムに脆（ぜい）弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

ウ　セキュリティ侵害につながる脆（ぜい）弱性が情報システムに存在することが発覚した場合に修正が施されること。

エ　ソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を提供すること。

（3）開発する情報システムに意図しない不正なプログラム等が組み込まれないよう、以下を全て含む対策を本業務の成果物に明記すること。

ア　情報システムで利用する機器等を調達する場合は、意図しない不正なプログラム等が組み込まれていないことを確認すること。

イ　アプリケーション・コンテンツの開発時に意図しない不正なプログラム等が混入されることを防ぐための対策を講ずること。

ウ　情報システムの構築を委託する場合は、委託先において農林水産省が意図しない変更が加えられないための管理体制を求めること。

（4）要安定情報を取り扱う情報システムを構築する場合は、許容される停止時間を踏まえて、情報システムを構成する要素ごとに、以下を全て含むセキュリティ要件を定め、本業務の成果物に明記すること。

ア　端末、サーバ装置及び通信回線装置等の冗長化に関する要件

イ　端末、サーバ装置及び通信回線装置並びに取り扱われる情報に関するバックアップの要件

ウ　情報システムを中断することのできる時間を含めた復旧に関する要件

（5）開発する情報システムのネットワーク構成について、以下を全て含む要件を定め、本業務の成果物に明記すること。

ア　インターネットやインターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否の判断及びインターネットから分離するとした場合に、分離を確実にするための要件

イ　端末、サーバ装置及び通信回線装置上で利用するソフトウェアを実行するために必要な通信要件

ウ　インターネット上のクラウドサービス等のサービスを利用する場合の通信経路全般のネットワーク構成に関する要件

エ　農林水産省外通信回線を経由して機器等に対してリモートメンテナンスすることの要

否の判断とリモートメンテナンスすることとした場合の要件

3　受託者は、本業務において情報システムの構築を行う場合には、以下の事項を含む措置を適切に実施すること。

（1）情報システムのセキュリティ要件の適切な実装

ア　主体認証機能

イ　アクセス制御機能

ウ　権限管理機能

エ　識別コード・主体認証情報の付与管理

オ　ログの取得・管理

カ　暗号化機能・電子署名機能

キ　暗号化・電子署名に係る管理

ク　監視機能

ケ　ソフトウェアに関する脆（ぜい）弱性等対策

コ　不正プログラム対策

サ　サービス不能攻撃対策

シ　標的型攻撃対策

ス　動的なアクセス制御

セ　アプリケーション・コンテンツのセキュリティ

ソ　政府ドメイン名（go.jp）の使用

タ　不正なウェブサイトへの誘導防止

チ　農林水産省外のアプリケーション・コンテンツの告知

（2）監視機能及び監視のための復号・再暗号化

監視のために必要な機能について、2（1）イの各項目を例として必要な機能を設けること。また、必要に応じ、監視のために暗号化された通信データの復号化や、復号されたデータの再暗号化のための機能を設けること。

（3）情報セキュリティの観点に基づくソフトウェアの選定

情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう可能な限り最新版を選定し、利用するソフトウェアの種類、バージョン及びサポート期限に係る情報を農林水産省に提供すること。

ただし、サポート期限が公表されていないソフトウェアについては、情報システムのライフサイクルを踏まえ、ソフトウェアの発売等からの経過年数や後継となるソフトウェアの有無等を考慮して選定すること。

（4）情報セキュリティの観点に基づく試験の実施

ア　ソフトウェアの開発及び試験を行う場合は、運用中の情報システムとの分離

イ　試験項目及び試験方法の決定並びにこれに基づいた試験の実施

ウ　試験の実施記録の作成・保存

（5）情報システムの開発環境及び開発工程における情報セキュリティ対策

ア　変更管理、アクセス制御、バックアップの取得等、ソースコードの不正な変更・消去を

防止するための管理

イ　調達仕様書等に規定されたセキュリティ実装方針の適切な実施

ウ　セキュリティ機能の適切な実装、セキュリティ実装方針に従った実装が行われていることを確認するための設計レビュー及びソースコードレビューの範囲及び方法の決定並びにこれに基づいたレビューの実施

エ　オフショア開発を実施する場合の試験データに実データを使用することの禁止

（6）政府共通利用型システムの利用における情報セキュリティ対策

ガバメントソリューションサービス（GSS）等、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程等に基づき、政府共通利用型システムの情報セキュリティ水準を低下させることがないように、適切なセキュリティ要件を実装すること。

4　受託者は、本業務において情報システムの運用・保守を行う場合には、以下の事項を含む措置を適切に実施すること。

（1）情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。

ア　情報システムの運用環境に課せられるべき条件の整備

イ　情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

ウ　情報システムの保守における情報セキュリティ対策

エ　運用中の情報システムに脆（ぜい）弱性が存在することが判明した場合の情報セキュリティ対策

オ　利用するソフトウェアのサポート期限等の定期的な情報収集及び報告

カ　「デジタル・ガバメント推進標準ガイドライン」（デジタル社会推進会議幹事会決定。最終改定：2025 年 5 月 27 日）の「別紙3　調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」に基づく情報資産管理を行うために必要な事項を記載した情報資産管理標準シートの提出

キ　アプリケーション・コンテンツの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポートを継続しているバージョンでの動作検証及び当該バージョンで正常に動作させるためのアプリケーション・コンテンツ等の修正

（2）情報システムの運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。

ア　情報セキュリティに関わる運用保守体制の整備

イ　運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

ウ　情報セキュリティインシデント（可能性がある事象を含む。以下同じ。）を認知した際の対処方法の確立

（3）情報システムのセキュリティ監視を行う場合には、以下の内容を全て含む監視手順を定め、適切に監視運用すること。

ア　監視するイベントの種類や重要度

イ　監視体制

ウ　監視状況の報告手順や重要度に応じた報告手段

エ　情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順

オ　監視運用における情報の取扱い（機密性の確保）

（4） 情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか定期的に見直しを行うこと。

（5） 情報システムにおいて定期的に脆（ぜい）弱性対策の状況を確認すること。

（6）情報システムに脆（ぜい）弱性が存在することを発見した場合には、速やかに担当部署に報告し、本業務における運用・保守要件に従って脆（ぜい）弱性の対策を行うこと。

（7）要安定情報を取り扱う情報システムについて、以下の内容を全て含む運用を行うこと。

ア　情報システムの各構成要素及び取り扱われる情報に関する適切なバックアップの取得及びバックアップ要件の確認による見直し

イ　情報システムの構成や設定の変更等が行われた際及び少なくとも年１回の頻度で定期的に、情報システムが停止した際の復旧手順の確認による見直し

（8）ガバメントソリューションサービス（GSS）等、本業務の調達範囲外の政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを運用する場合は、政府共通利用型システム管理機関との責任分界に応じた運用管理体制の下、政府共通利用型システム管理機関が定める運用管理規程等に従い、政府共通利用型システムの情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

（9）不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

５　受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。

（1）情報システム更改時の情報の移行作業における情報セキュリティ対策

（2）情報システム廃棄時の不要な情報の抹消

Ⅴ　情報システムの一部の機能を提供するサービスに関する情報セキュリティの確保

応札者は、要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除くものとし、以下「業務委託サービス」という。）に関する業務を実施する場合は、業務委託サービス毎に以下の措置を講ずること。

１　業務委託サービスの中断時や終了時に円滑に業務を移行できるよう、取り扱う情報の可用性に応じ、以下を例としたセキュリティ対策を実施すること。

（1）業務委託サービス中断時の復旧要件

（2）業務委託サービス終了または変更の際の事前告知の方法・期限及びデータ移行方法

２　業務委託サービスを提供する情報処理設備が収容されているデータセンターが設置されている独立した地域（リージョン）が国内であること。

３　業務委託サービスの契約に定める準拠法が国内法のみであること。

4　ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

5　業務委託サービスの利用を通じて農林水産省が取り扱う情報について、目的外利用を禁止すること。

6　業務委託サービスの提供に当たり、業務委託サービスの提供者若しくはその従業員、再委託先又はその他の者によって、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること）。

7　業務委託サービスの提供者の資本関係、役員等の情報、業務委託サービスの提供が行われる施設等の場所、業務委託サービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

8　業務委託サービスの提供者の情報セキュリティ水準を証明する、Ⅱの2で掲げる証明書等または同等以上の国際規格等の証明書の写しを提出すること。

9　情報セキュリティインシデントへの対処方法を確立していること。

10　情報セキュリティ対策その他の契約の履行状況を確認できること。

11　情報セキュリティ対策の履行が不十分な場合の対処方法を確立していること。

12　業務委託サービスの提供者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について業務委託サービスの提供者と合意し、定められた手順により情報を取り扱うこと。

Ⅵ　クラウドサービスに関する情報セキュリティの確保

応札者は、本業務において、クラウドサービス上で要機密情報を取り扱う場合は、当該クラウドサービスごとに以下の措置を講ずること。また、当該クラウドサービスの活用が本業務の再委託に該当する場合は、当該クラウドサービスに対して、Ｘの措置を講ずること。

1　サービス条件

（1）クラウドサービスを提供する情報処理設備が収容されているデータセンターについて、設置されている独立した地域（リージョン）が国内であること。

（2）クラウドサービスの契約に定める準拠法が国内法のみであること。

（3）クラウドサービス終了時に情報を確実に抹消することが可能であること。

（4）本業務において要求されるサービス品質を満たすクラウドサービスであること。

（5）クラウドサービス提供者の資本関係、役員等の情報、クラウドサービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）のうち農林水産省の情報又は農林水産省が利用するクラウドサービスの環境に影響を及ぼす可能性のある者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

（6）ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に

関する情報が開示されていること。

（7）原則として、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP クラウドサービスリスト等」という。）に登録されているクラウドサービスであること。

（8）ISMAP クラウドサービスリスト等に登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（3桁の番号で表現される項目）及び末尾にBが付された詳細管理策（4桁の番号で表現される項目）を原則として全て満たしていることを証明する資料を提出し、農林水産省の承認を得ること。

2 クラウドサービスのセキュリティ要件

（1）クラウドサービスについて、以下の要件を満たしていること。

ア クラウドサービス提供者が提供する主体認証情報の管理機能が農林水産省の要求事項を満たすこと。

イ クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること。

ウ クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作が特定されていること。

エ クラウドサービス内及び通信経路全般における暗号化が行われていること。

オ クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合、ソフトウェアのクラウドサービス上におけるライセンス規定に違反していないこと。

カ クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合、その機能を確認していること。

キ 暗号鍵管理機能をクラウドサービス提供者が提供する場合、鍵管理手順、鍵の種類の情報及び鍵の生成から廃棄に至るまでのライフサイクルにおける情報をクラウドサービス提供者から入手し、またリスク評価を実施していること。

ク 利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていること。

ケ クラウドサービス提供者が提供するバックアップ機能を利用する場合、農林水産省の要求事項を満たすこと。

（2）クラウドサービスで利用するアカウント管理に関して、以下のセキュリティ機能要件を満たしていること。

ア クラウドサービス提供者が付与し、又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

イ クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者に対する、強固な認証技術による認証

ウ クラウドサービス提供者が提供する主体認証情報の管理機能について、農林水産省の要求事項を満たすための措置の実施

（3）クラウドサービスで利用するアクセス制御に関して、以下のセキュリティ機能要件を満たしていること。

ア クラウドサービス上に保存する情報やクラウドサービスの機能に対する適切なアクセ

ス制御

イ　インターネット等の農林水産省外通信回線から農林水産省内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合の適切なセキュリティ対策

（4）クラウドサービスで利用する権限管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス利用者によるクラウドサービスに多大な影響を与える誤操作の抑制

イ　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（5）クラウドサービスで利用するログの管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの管理

（6）クラウドサービスで利用する暗号化に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス内及び通信経路全般における暗号化の適切な実施

イ　情報システムで利用する暗号化方式の遵守度合いに係る法令や農林水産省訓令等の関連する規則の確認

ウ　暗号化に用いる鍵の保管場所等の管理に関する要件

エ　クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理

（7）クラウドサービスを利用する際の設計・設定時の誤り防止に関して、以下のセキュリティ要件を満たしていること。

ア　クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策

イ　クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

ウ　クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用

エ　クラウドサービスの設定の誤りを見いだすための対策

（8）クラウドサービス運用時の監視等に関して、以下の運用管理機能要件を満たしていること。

ア　クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

イ　利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

ウ　クラウドサービス内における時刻同期の方法

エ　利用するクラウドサービスの不正利用の監視

（9）クラウドサービス上で要安定情報を取り扱う場合は、その可用性を考慮した設計となっていること。

（10）クラウドサービスにおいて、不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施を含む、情報セキュリティインシデントが発生した際の復旧に関する対策要件が策定されていること。

3　クラウドサービスを利用した情報システム

クラウドサービスを利用した情報システムについて、以下の措置を講ずること。

（1）導入・構築時の対策

ア　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス利用のための責任分界点を意識した利用手順

（イ）クラウドサービス利用者が行う可能性がある重要操作の手順

イ　情報システムの運用・監視中に発生したクラウドサービスの利用に係る情報セキュリティインシデントを認知した際の対処手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス提供者との責任分界点を意識した責任範囲の整理

（イ）クラウドサービスのサービスごとの情報セキュリティインシデント対処に関する事項

（ウ）クラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

ウ　クラウドサービスが停止し、又は利用できなくなった際の復旧手順を実施手順として整備すること。なお、要安定情報を取り扱う場合は十分な可用性を担保した手順とすること。

（2）運用・保守時の対策

ア　クラウドサービスの利用に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービス提供者に対する定期的なサービスの提供状態の確認

（イ）クラウドサービス上で利用するIT資産の適切な管理

イ　クラウドサービスで利用するアカウントの管理、アクセス制御、管理権限に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

（イ）クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

ウ　クラウドサービスで利用する機能に対する脆（ぜい）弱性対策を実施すること。

エ　クラウドサービスを運用する際の設定変更に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（イ）クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

（ウ）クラウドサービス利用者が行う可能性のある重要操作に対する監督者の指導の下での実施

オ　クラウドサービスを運用する際の監視に関して、以下の内容を全て含む対策を実施すること。

（ア）クラウドサービスの不正利用の監視

（イ）クラウドサービスで利用しているデータ容量、性能等の監視

カ　クラウドサービスを運用する際の可用性に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）不測の事態に際してサービスの復旧を行うために必要なバックアップの確実な実施

（イ）要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る定期的な訓練の実施

（ウ）クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

キ　クラウドサービスで利用する暗号鍵に関して、暗号鍵の生成から廃棄に至るまでのライフサイクルにおける適切な管理の実施を含む情報セキュリティ対策の実施

（3）更改・廃棄時の対策

ア　クラウドサービスの利用終了に際して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービスで取り扱った情報の廃棄

（イ）暗号化消去が行えない場合の基盤となる物理機器の廃棄

（ウ）作成されたクラウドサービス利用者アカウントの削除

（エ）利用したクラウドサービスにおける管理者アカウントの削除又は返却

（オ）クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

Ⅶ　Web システム／Web アプリケーションに関する情報セキュリティの確保

受託者は、本業務において、Web システム／Web アプリケーションを開発、利用または運用等を行う場合、別紙「Web システム／Web アプリケーションセキュリティ要件書 Ver.4.0」の各項目について、対応可、対応不可あるいは対象外等の対応方針を記載した資料を提出すること。

Ⅷ　機器等に関する情報セキュリティの確保

受託者は、本業務において、農林水産省にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等（以下「機器等」という。）を納品、賃貸借等をする場合には、以下の措置を講ずること。

1　納入する機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

2　機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、農林水産省と受託者が連携して原因を調査・排除できる体制を整備していること。

3　機器等の設置時や保守時に、情報セキュリティの確保に必要なサポートを行うこと。

4　利用マニュアル・ガイダンスが適切に整備された機器等を採用すること。

5　脆（ぜい）弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。

6　ISO/IEC 15408 に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

7　情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新版を採用するとともに、ソフトウェアの種類、バージョン及びサポート期限について報告すること。なお、サポート期限が事前に公表されていない場合は、情報システムのライフサイクルを踏まえ、販売からの経過年数や後継ソフトウェアの有無等を考慮して選定すること。

8　機器等の納品時に、以下の事項を書面で報告すること。

（1）調達仕様書に指定されているセキュリティ要件の実装状況（セキュリティ要件に係る試験の実施手順及び結果）

（2）機器等に不正プログラムが混入していないこと（最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等）

Ⅸ　管轄裁判所及び準拠法

1　本業務に係る全ての契約（クラウドサービスを含む。以下同じ。）に関して訴訟の必要が生じた場合の専属的な合意管轄裁判所は、国内の裁判所とすること。

2　本業務に係る全ての契約の成立、効力、履行及び解釈に関する準拠法は、日本法とすること。

Ⅹ　業務の再委託における情報セキュリティの確保

1　受託者は、本業務の一部を再委託（再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託を含む。以下同じ。）する場合には、受託者が上記Ⅱの1、Ⅱの2、Ⅲの1及びⅣの1において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、農林水産省の許可を得ること。

2　受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、農林水産省又は農林水産省が選定した事業者による再委託先への立入調査等の監査を受け入れるものとすること。

3　受託者は、担当部署からの要求があった場合は、再委託先における情報セキュリティ対策の履行状況を報告すること。

XI 資料等の提出

上記Ⅱの1、Ⅱの2、Ⅲの1、Ⅳの1、Ⅴの6、Ⅴの7、Ⅴの8、Ⅵの1（5）、Ⅵの1（6）、Ⅵの1（8）、Ⅷの1及びⅧの6において提出することとしている資料等については、最低価格落札方式にあっては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式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。

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。

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３）

環境負荷低減のクロスコンプライアンス実施状況報告書

以下のア～エの取組について、実施状況を報告します。

ア　環境負荷低減に配慮したものを調達するよう努める。

具体的な事項	実施した／努めた	左記非該当
・事務用品を使用する場合には、詰め替えや再利用可能なものを調達することに努めている。	□	□
・その他（　　）	／	／

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

イ　エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に消費する電気・ガス・ガソリン等のエネルギーについて、帳簿への記載や伝票の保存等により、使用量・使用料金の記録に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、不要な照明の消灯やエンジン停止に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、基準となる室温を決めたり、必要以上の冷暖房、保温を行わない等、適切な温度管理に努めている。	□	□
・事業実施時に使用する車両・機械等が効果的に機能を発揮できるよう、定期的な点検や破損があった場合は補修等に努めている。	□	□
・夏期のクールビズや冬期のウォームビズの実施に努めている。	□	□

・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

ウ　廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に使用する資材について、プラスチック資材から紙などの環境負荷が少ない資材に変更することを検討する。	□	□
・資源のリサイクルに努めている（リサイクル事業者に委託することも可）。	□	□
・事業実施時に使用するプラスチック資材を処分する場合に法令に従って適切に実施している。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

エ　みどり戦略の理解に努める。

具体的な事項	実施した／努めた	左記非該当
・「環境負荷低減のクロスコンプライアンスチェックシート解説書 －民間事業者・自治体等編－」にある記載内容を了知し、関係する事項について取り組むよう努める。	□	□
・事業者として独自の環境方針やビジョンなどの策定している、もしくは、策定を検討する。	□	□
・従業員等向けの環境や持続性確保に係る研修などを行っている、もしくは、実施を検討する。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

（別紙４）

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	質問内容
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

（別添様式１）

令和７年度
国有林野情報管理システム-市町村交付金算定サブシステム
の構築に係る要件定義書作成等業務

閲覧申込書

申込日：　令和　　年　　月　　日

１　会 社 名：

２　住　　所：

３　担当者名：

４　電話番号：

５　E-mail アドレス：

６　閲覧日時：　令和　　年　　月　　日　　時

７　閲覧者氏名　１：
（５名まで）　２：
３：
４：
５：

（別添様式２）

林野庁経営企画課
課長　　宛

守秘義務に関する誓約書

「令和７年度国有林野情報管理システムー市町村交付金算定サブシステムの構築に係る要件定義書作成等業務」に係る資料閲覧に当たり、下記の事項を厳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。）を見積書作成の目的以外に使用又は第三者に開示若しくは漏えい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　本件に係る作業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、情報を本件の目的以外に使用又は第三者に開示若しくは漏えいした場合、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