流通木材の合法性確認システム

非機能要件定義書

第 1.2 版

2023 年 12 月 13 日

林野庁

改訂履歴

版数	発行日	改訂履歴
0.8 版	2023 年 2 月 28 日	ドラフト版を作成。
0.8 版	2023 年 3 月 7 日	2.システム方式に関する事項 2.1.情報システムの構成に関する全体の方針 システムアーキテクチャとして、MAFF クラウドを含めたパブリッククラウドを前提とすると明記。
0.8 版	2023 年 3 月 7 日	2.3.開発方式及び開発手法 開発手法を修正。
0.8 版	2023 年 3 月 7 日	3.規模に関する事項 3.2.データ量 イメージデータ容量の見積を見直し、修正。
0.8 版	2023 年 3 月 7 日	10.8.クラウドサービスの利用 誤記を修正。
0.9 版	2023 年 3 月 7 日	版数を 0.9 版に変更。
0.9 版	2023 年 3 月 9 日	.3.開発方式及び開発手法 開発手法を修正。
1.0 版	2023 年 3 月 9 日	版数を 1.0 版に変更。
1.0 版	2023 年 3 月 13 日	.3.開発方式及び開発手法 開発手法を修正。
1.1 版	2023 年 10 月 10 日	MAFF クラウド前提に修正。
1.2 版	2023 年 12 月 13 日	付属書、1.2、5.3、9.1、10、11.1、16.1(2)イについて、一部修正。

目次

付属書一覧

付属書１：AWS・Azure 設定確認リスト

付属書２：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

1. ユーザビリティ及びアクセシビリティに関する事項

1.1. 情報システムのユーザの種類、特性

本システムにおけるユーザの種類及び特性を以下に記載する。

表 1：ユーザの種類及び特性

No	ユーザの種類	利用する機能			利用する端末	利用するネットワーク
		利用者向け	事業管理者向け	システム管理者向け		
1	一般利用者	○			PC、タブレット、スマートフォン、等	インターネット
2	事業管理者		○		PC、タブレット、等	インターネット
3	システム運用担当者			○	PC、タブレット、等	インターネット
4	監督府省庁担当職員			○	PC、タブレット、等	インターネット

1.2. ユーザビリティ要件

本システムに求めるユーザビリティ要件を以下に記載する。
システム UI（特に、一般利用者画面 UI）の言語仕様については日英対応とする。

表 2：ユーザビリティ要件

No	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成	● 何をすればよいかが見て直ちに分かるような画面構成にすること。フォームの種類や用途が簡潔に理解できる見出しを付けること。PC では、目線がジグザグに動かなくて済むレイアウトにすること。 ● 本文テキストの色と、本文テキストが配置されている箇所の背景色において、少なくとも 4.5：1 のコントラストとすること（例：背景色が白（#FFFFFF）で本文テキストが黒の場合、黒は#76767E 以上の濃さ） ● 無駄な情報、デザイン及び機能を廃し、簡潔で分かりやすい画面にすること。 ● 十分な視認性のあるフォント及び文字サイズ（本文テキストにおいて 16px 以上）を用い、文字サイズについては、ユーザ側の環境の設定で拡大等が可能なものとすること。合法性を証明する書類名などが確実に読めること。 ● ユーザ側の環境の設定で画面の大きさや位置の変更ができること。 ● PC だけでなく、スマートフォンやタブレット端末よりインターネット回線を介してアクセスすることも考慮し、それぞれの画面サイズに応じた表示（レスポンシブデザイン）を実現すること。なお、スマートフォンでは、タップのターゲットエリアを 44px 以上確保すること。 ● 紛らわしい項目は、その違いが利用者にも明確に理解できるよう工夫すること。 ● モーダルダイアログ、ポップアップメニュー、トースト、スナックバー等の画面内で小窓等が開く UI がある場合、以下の配慮を実装すること。 ・キーボード操作だけで利用しているときに、一度フォーカスしたら抜け出せないコンテンツを作らない。

No	ユーザビリティ分類	ユーザビリティ要件
		・アクションを要求する UI を時間経過で自動的に閉じない。 ・当該 UI を開いた場合、中身の要素にフォーカスを移す。 ・当該 UI を閉じて戻る場合、閉じて戻るという挙動が、読み上げたときに自然と理解できるようにする。また、元のコンテンツの位置にフォーカスが戻る。 ・時間経過で消える UI も読み上げを行う（「入力内容を送信しました」など）。また、フォーカスされている場合は自動的に UI を閉じない。
2	操作方法のしやすさ、分かりやすさ	● 無駄な手順を省き、最小限の操作、入力等でユーザが作業できるようにすること。頻繁に選択される項目は、デフォルトに設定すること。繰り返し入力する項目がプリセットとして保存できること。 ● 画面上で入出力項目のコピー及び貼付けができること。 ● 業務の実施状況によっては、ショートカットや代替入力方法が用意されること（例えば、片手だけで主要な操作が完了することが求められたり、マウスを利用することが困難であったりする場合が考えられる） ● タブ送りなど、キーボード操作だけで行えるようにすること。 ● テキストエリアは、入力内容（文字数）に応じた幅とすること。 ● 日付の入力が必要な場合に、セレクト方式またはカレンダー方式で選択入力できるようにすること。ただし、例えば生年月日のように、何十回もクリックしないと目的の入力値に辿り着けないことが想定される場合、直接入力ができる等の入力の効率性を高めるための仕組みや、複数の入力手段を用意すること。 ● 都道府県コードや機関コード、または電話番号の国番号のように、プリセットを用意できる項目に対しては、コード表を参照することなくリストあるいはセレクターを用いて選択できること（選択肢が非常に多い場合、直接入力して選択候補を絞り込める仕組みとすること。） ● 住所の入力において、都道府県から町名の途中まで郵便番

No	ユーザビリティ分類	ユーザビリティ要件
		号で自動入力できるようにすること。また、郵便番号が分からない場合の救済策（一覧から選択できる等）を用意すること。 ● 法人情報の入力において、「法人番号」、「商号または名称」、「商号または名称（カナ）」、「連絡先情報」の項目を用意すること。 ● ファイルアップロードでは、複数のファイルを一度にアップできるようにすること。 ● ドラッグアンドドロップでファイルをアップできるようにしている場合、ドラッグアンドドロップ以外の方法（システムダイアログによるファイルの直接選択）でもファイルをアップできるようにすること。 ● 検索などの操作結果の画面をブックマークできるようにすること。
3	指示や状態の分かりやすさ	● 操作の指示、説明、メニュー等には、ユーザが正確にその内容を理解できる用語を使用すること。 ● 必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度をユーザが認識できるようにすること。 ● システムが処理を行っている間、その処理内容をユーザが直ちに分かるようにすること。 ● 入力が必要な文字数が何文字なのか、あるいは入力可能な文字数が何文字までなのかを入力前に判断できるように、入力項目に半/全角での具体的な最大文字数を表示すること。また、最大文字数が決まっている場合に、入力中の文字数がテキストエリアの枠外や下部に表示されていて、あとどれくらいの文字を入力できるかが把握できるようにすること。 ● 入力前に、あらかじめ入力内容やフォーマットの制約を判断できるように、入力フォーマット（書式）を表示すること（例：電話番号の入力項目に対して「半角数字のみ。ハイフンなし」等と入力の制約を具体的に表示する。）。 ● 氏名の入力を要求する場合に、「氏」と「名」に入力項目を分割すること。 ● タイムアウトが必要な場合、時間を延長する仕組みを用意

No	ユーザビリティ分類	ユーザビリティ要件
		すること。 ● 利用者によって行うべきことが違う場合、Yes/No フローチャートのように、不必要な情報を減らして、利用者の理解を支援するための工夫をすること。
4	エラーの防止と処理	● ユーザが操作、入力等を間違えないようなデザインや案内を提供すること。 ● ありえないデータを入力できないようにすること。(例：生年で明治１年が選択できないようにする) ● 入力内容の形式に問題がある項目については、それを強調表示する等、ユーザがその都度その該当項目を容易に見つけられるようにすること。 ● ファイルの登録等については、確認画面等を設け、ユーザが行った操作又は入力の取消し、修正等が容易にできるようにすること。 ● 重要な処理については事前に注意表示を行い、ユーザの確認を促すこと。 ● エラーが発生したときは、ユーザが容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすい情報提供をすること。ページ上部にエラーサマリーを表示しつつ、各エラー箇所それぞれに具体的なエラー内容を表示すること。 ● 選択肢の回答によって入力項目を出し分ける仕組みを用意すること。 ● 入力の際に判断に迷いそうな項目についての記入例や必要な書式などをサポートテキストで用意すること。 ● 全角ダッシュ「ー」と全角ハイフン「 - 」など、目視でエラー回避が難しい記号などの入力を避ける仕組みを用意すること。 ● 以下のように入力のブレをエラーとせず、UI 上で補正・吸収するか、送信・保存時に整形すること。電話番号のハイフン未入力は保存時整形、英数字・カナの全角入力は半角に置き換える。 ● 入力を一時中断・保存できる仕組みを用意すること。

No	ユーザビリティ分類	ユーザビリティ要件
		● リロード、ブラウザバックしてもエラーにしないこと。 ● メールアドレスの確認が必要な場合、メールアドレスを 2 回入力させるのではなく、疎通確認メールを送る仕組みを用意すること。
5	ヘルプ	● ユーザが必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること。 ● 必要となるハードウェアやソフトウェア環境を、利用者が確実に読めるかたちで表示すること。 ● ホーム画面に、利用できない曜日や時間帯を、利用者が確実に読めるかたちで表示すること。

1.3. アクセシビリティ要件

本システムに求めるアクセシビリティ要件を以下に記載する。

表 3：アクセシビリティ要件

No	アクセシビリティ分類	アクセシビリティ要件
1	基準等への準拠	● 本システムにおいてはアクセシビリティを確保し、ユーザが操作しやすく誤操作の生じないシステムとなるよう設計するため、日本工業規格 JIS X 8341 シリーズ等に従い、アクセシビリティを確保した設計・開発を行うこと。
2	指示や状態の分かりやすさ	● データの更新が行われた箇所、異常値が検出された箇所等については、色等を使って分かり易く表示すること。 ● 色の違いを識別しにくいユーザ（視覚障害のかた等）を考慮し、ユーザへの情報伝達や操作指示を促す手段はメッセージを表示する等とし、可能な限り色のみで判断するようなものは用いないこと。

2. システム方式に関する事項

2.1. 情報システムの構成に関する全体の方針

本システムの構築に当たり、システム構成に関する全体の方針を以下に記載する。その他、具体的な個別事項については本定義書の各章を参照すること。

表 4：情報システムの構成に係る全体方針

No	全体方針の分類	全体方針
1	システムアーキテクチャ	● 本システムは、IaaS/PaaS（MAFF クラウド及びパブリック・クラウド）を利用して Web サービスを提供することを前提とする。
2	アプリケーションプログラムの設計方針	● 本システムを構成する API 間の依存関係を無くすとともに、再利用性および運用・保守性を確保すること。API の構築に当たっては、API テクニカルガイドブック[注 1]で推奨される技術を採用すること。 ● 開発の生産性や保守性向上を目的とし、画面、業務ロジック、データアクセス方法を極力疎結合な構造とし、変更等における影響範囲を極小化するように考慮すること。
3	ソフトウェア製品の活用方針	● 広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 ● アプリケーションプログラムの動作及び性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらの OSS 製品のサポートが確実に継続されていることを確認しなければならない。
4	システム基盤の方針	● IaaS/PaaS（パブリック・クラウド）を利用するクラウド型とすること。

[注 1]「API テクニカルガイドブック」（内閣官房情報通信技術(IT)総合戦略室、2019 年 3 月、https://cio.go.jp/sites/default/files/uploads/documents/1020_api_tecnical_guidebook.pdf）

2.2. 情報システムの全体構成

本システムの全体構成図を以下に記載する。

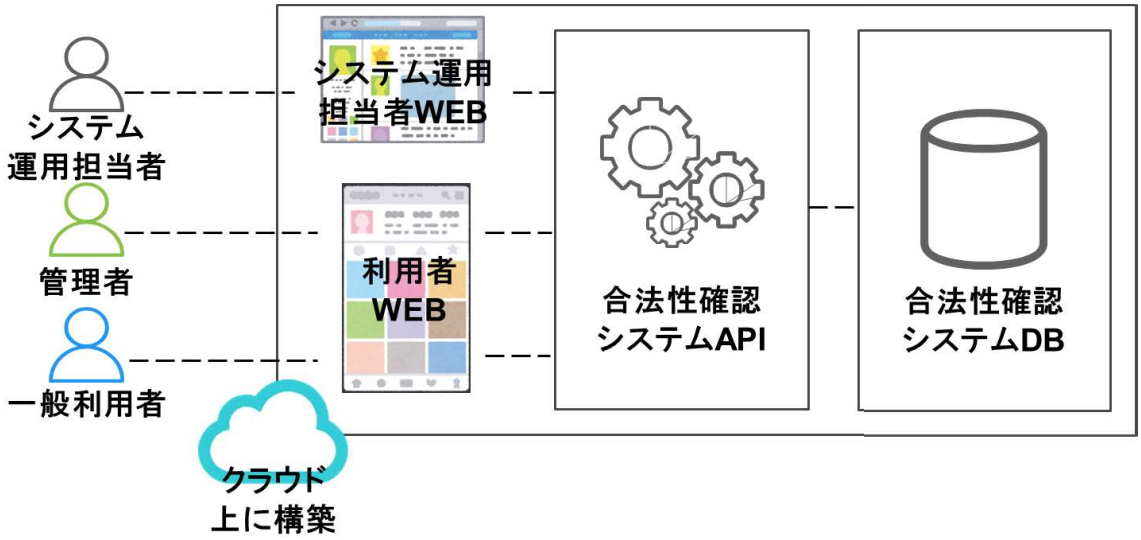


図 1：システム構成図

2.3. 開発方式及び開発手法

本システムの開発方式及び開発手法を以下に記載する。

表 5：開発方式及び開発手法

No	項目	要件
1	開発方式	● 本システムの開発方式は、スクラッチ開発／アプリケーションプログラムの移植／ソフトウェア製品のカスタマイズのいずれかを前提とする。
2	開発手法	● 本システムの開発手法は、ウォーターフォール型・アジャイル型のどちらを採用してもよい。受注者が過去の情報システム開発（設計・開発）案件において、豊富な成功実績を有する設計・開発プロセスを採用すること。 ● ただし、開発開始から運用開始までの期間は 1 年程度と想定しているので、採用する開発手法に合わせ、以下のことに留意すること。 ● ウォーターフォール型は、採用率の高い手法である分、経験者も多く、開発を計画通りに進めやすいが、デメリットは、設計工程での作業ミスが発生した場合の手間が大きいこと、仕様変更・要件変更など手戻りに柔軟に対応できないなどである。よって、ウォーターフォール型を採用する場合はレビュー頻度を通常よりも多く設定し、手戻りをなるべく発生させないこと。 ● アジャイル型は、リリースまでに優先順位の高いシステムから開発ができるため、短納期でサービスを届けられるが、反面、開発の方向性がずれやすいという欠点がある。この欠点を解消させるため、適切なスプリント期間（プランニングからレビューまで）を設定し、開発の方向性を補正しながら進めていくこと。

3. 規模に関する事項

3.1. 機器数及び設置場所

- 本システムを構成するクラウドサービスについては、他の機能要件、非機能要件を満たすものであれば特段の制約を設けず、提案に基づき発注者との調整により決定する。設置場所についても他の機能要件、非機能要件を満たす日本国内であれば特段の制約を設けず、提案に基づき発注者との調整により決定する。
- 管理者端末については、他の機能要件、非機能要件を満たすものであれば特段の制約を設けず、提案により決定する。
- 利用者端末や、利用者がシステムへ接続するためのアクセス通信網については各利用者が準備するものであるが、本システムを利用するためにハードウェアや OS を含むソフトウェア等に関して何らかの制約や条件がある場合は明らかにすること。ただし、利用者端末は既存の端末を流用することが前提であり、利用者端末環境（ハードウェア、OS を含むソフトウェア等）は統一されていないことを想定する。

3.2. データ量

- データ量については、合法性情報 1 レコードあたりのテキストデータ容量は 10Kbyte（100byte×100 項目）を想定すること。また、合法性情報 1 レコードあたりのイメージデータ容量は 10Mbyte（5Mbyte[注 2]×2 帳票）を想定する。
- 通信時には処理対象データはペイロードに相当し、データ送受信時にはサイズに応じて複数のパケットに分割の上、伝送処理のための管理情報（プロトコル対応の制御情報、ヘッダやトレーラ）が付加されるため、通信量はデータ量よりも大きくなることに留意する。
- データについては、電子帳簿保存法に基づくデータ保存は本システムでは行わない。ただし、年報作成等の統計業務の目的としたデータ保存期間は原則 5 年間とする。なお、サービスの利用状況等を踏まえ最大 10 年間保存できるよう設計検討を行うこととし、詳細は設計・開発フェーズ以降にて調整・協議のうえ、発注者の決定に従うこと。
- 管理者（国、等のシステム運営主体）は業務要件で記載の以下の業務を実施するための各種管理データを利用する。当該データ量に関しては、設計・開発フェーズ以降にて調整・協議し、発注者の決定に従うこと。
  - マスタデータのメンテナンス：コード等のマスタ情報など。
  - システムの保守・運用：本システムの障害情報など。

[注 2] 合法性確認に用いられた書類の PDF は、複数取引をまとめたり、認証材付きのものでも 1 MB 程度。現場で発生する納品書等をカメラで撮影する場合はこれよりも増えることは想定されるが、500Kbyte の写真でも十分に情報伝達が可能。図面などを取り扱うとサイズが飛躍的に上昇するが、出現頻度は多くない。これを踏まえ、イメージデータ容量を 10Mbyte としている。

3.3. 処理件数

本システムに係る利用者が実施する業務処理件数に関しては、業務要件で記載の通りとなる。(業務要件定義書「3. 規模に関する事項 - 3.2. 処理件数」を参照。)

3.4. 利用者数

本システムの利用者数(見込み)に関しては、業務要件で記載の通りとなる。(業務要件定義書「3. 規模に関する事項 - 3.1. サービスの利用者数」を参照。)

4. 性能に関する事項

4.1. 応答時間（レスポンスタイム、ターンアラウンドタイム、サーバ処理時間）

- 本システムの利用に関しては、利用者の通信環境の条件が多種多様であることが想定されるため、通信時間（伝送時間）を含めたオンライン処理におけるターンアラウンドタイムについての目標を設定することは適切ではない。そのため通信時間（伝送時間）を除いた、システム内におけるクラウドサービスの応答時間（レスポンスタイム)、つまりシステム内における処理時間とシステム内の通信時間として、以下の目標を設定する。
  - 応答時間（レスポンスタイム）
    - 管理機能以外：平常時 3 秒以内（順守率 90%[注 3]）、ピーク時 5 秒以内（順守率 80%[注 4]）
    - 管理機能：平常時 8 秒以内（順守率 90%[注 3]）、ピーク時 14 秒以内（順守率 80%[注 4]）
    - 採用するクラウドサービスの SLA（Service Level Agreement、サービス品質保証）に照らして上記の目標値を達成することが困難な場合などには、採用するクラウド環境で実現可能な応答時間（レスポンスタイム）の目安を明示すること。

[注 3]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「B.2.1.1 オンラインレスポンス/通常時レスポンス順守率」レベル 3 の推奨値「90%」を採用

[注 4]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「B.2.1.2 オンラインレスポンス/ピーク時レスポンス順守率」レベル 2 の推奨値「80%」を採用

4.2. スループット

- 本システムのサービス提供時間（利用者が使用可能な時間）に関しては、業務要件で記載の通り、通常は 9 時～17 時であるが、本システムのサービス提供時間は極力 365 日 24 時間としている。そのため、バッチ処理時間については以下の目標を設定する。
  - 365 日 24 時間のサービス提供となることを見据えて、本システムでの処理件数の少ない時間帯にオンラインでのバッチ処理を行うなど、サービス・業務への影響を少なくするよう検討すること。
  - バッチ処理においてサービス停止がやむをえない場合は、サービス・業務への影響が少なくなるよう検討し、その時間（再実行の余裕を確保すること）[注 5]や頻度を発注者と調整すること。

[注 5]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「B.2.2.1 バッチレスポンス（ターンアラウンドタイム）/通常時レスポンス順守度合い」及び「B.2.2.2 バッチレスポンス（ターンアラウンドタイム）/ピーク時レスポンス順守度合い」レベル 2 の推奨値「再実行の余裕が確保できる」を採用

5. 信頼性に関する事項

5.1. 可用性要件

- 以下の算式により算出する稼働率について 99.9%[注 6]を満たすこと。

  稼働率（%）＝ 1 ヶ月の実稼働時間 ÷ 1 ヶ月の予定稼働時間 × 100

  ＝(1 −（1 ヶ月の停止時間）÷ 1 ヶ月の予定稼働時間）× 100

  - 予定稼働時間とは、稼働すべき時間を指し、計画停電及び定期保守等の事前に計画した停止時間を除く。
  - 停止時間とは、計画外で本システムが停止していた時間、あるいは多数の利用者が使用できない状態にあった時間を指し、待機系システム等への切り替えのために発生した停止時間、障害発生から復旧のために必要となった停止時間及び人為的なミスにより発生した停止時間を含む。

- 採用するクラウドサービスの SLA に照らして、上記の 99.9%を達成することが困難な場合、あるいは冗長化を行えば達成は可能であるがコスト対効果の観点で課題が残ると考えられる場合などには、その旨を示した上で、業務要件に照らして最もコスト対効果が高いと考えられるように検討すること。その他、採用するクラウドサービスにおいてアップデート対応のために計画停止等の時間が必要となることが予め判明している場合には、当該期間がどの程度事前に把握できるのか、変更等の調整は可能なのか等についても提案書で明示すること。

[注 6]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「A.1.5.1 稼働率/稼働率」レベル 4 の推奨値「99.99%」に次ぐ値を採用

5.2. 可用性に係る対策

- 前項の目標値について採用するクラウドサービスの SLA 等により評価するとともに、クラウドサービス事業者に公開可能な範囲について基盤構成を確認し、下記の負荷分散、縮退運転、冗長化、障害調査について検討し、必要に応じて適宜契約内容に含めること。
  - 通常時の負荷分散は可能か。
  - 障害発生時や基盤アクセス集中時（輻輳時）の縮退運転は可能か。
  - 障害発生時の運用として組織的かつ計画的・予防的に行えるように準備し、通信経路やサーバ構成（ホットスタンバイ、コールドスタンバイなど）は冗長化されているか。
  - クラウドサービスを構成するハードウェア、ソフトウェア（OS、ミドルウェア、各種プログラム、DBMS、プロトコル等）の障害発生時に障害内容の調査は容易に行うことができるか。

5.3. 完全性要件

- 下記の内容について採用するクラウドサービスの SLA 等により評価するとともに、クラウドサービス事業者に公開可能な範囲で確認し、必要に応じて適宜契約内容に含めること。達成することが困難な場合、あるいは達成は可能であるがコスト対効果の観点で課題が残ると考えられる場合などには、その旨を示した上で、業務要件に照らして最もコスト対効果が高いと考えられるように検討すること。
  - 障害時や誤操作等により重要なデータが安易に消去されることのないよう、必要な措置を行うこと。
  - 業務に用いるデータの信頼性を確保し、データの正確性・保全性を維持するため、データについては二重化などの冗長構成をとるなど必要な措置を行うこと。
  - データの整合性を確保するため、更新処理においては十分なデータチェックを行うこと。エラー等により処理が中断された場合には、データを処理実行前の状態に戻すこと。
  - データの保全性を確保するため、業務に用いるデータのバックアップ処理は、業務への影響を排除した設計とすること。
  - 異常な入力や処理を検出し、データの滅失や改変を防止する対策を講ずること。
  - 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
  - データの複製や移動を行う際に、データが毀損しないよう、保護すること。
  - データの複製や移動を行う際にその内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定するための措置を行うこと。

6. 拡張性に関する事項

6.1. 性能の拡張性

- 本システムの利用者数については、業務要件で記載の通り、第 1 次稼働リリース時（2025 年 4 月）に対して 5 年目には約 2 倍を想定しているが、オンライン処理、バッチ処理とも性能が劣化することのないよう、処理能力の向上やデータ保存領域の拡張等のため、クラウドサービスにおけるスケールアップ／スケールダウン（動作環境の変更）などが容易に可能なこと。
- 本システムを拡張する必要が生じた場合、クラウドサービスの契約料については、原則として初期構築時の単価と同程度で提供すること。
- 本システムのサービス導入は段階式移行を行うため、その段階導入のタイミングと併せて、ネットワークや接続機器の最適な拡張が可能な構成とすること。

6.2. 機能の拡張性

- 利用者ニーズ及び業務環境の変化等に最小コストで対応可能とするため、本システムを構成する各機能の再利用性を確保する。
- 将来の制度変更や対象業務の追加等に伴い、本システムで扱うデータ項目や外部インタフェースに追加等が生じることが想定されるため、データ設計にあたっては項目変更（追加、削除、統合、分割、属性変更など）にあたっては改修規模・費用を最小限に抑えるよう対策を講ずること。

7. 上位互換性に関する事項

- 本システムを構成するクラウドサービスの動作環境等が限定されている場合には、その制約の具体的な内容について明らかにすること。特定の OS、ミドルウェア、ソフトウェア、DBMS（Database Management System、データベース管理システム）、プロトコル等のバージョンに依存することが判明している場合は、その利用を最低限とすること。
- 本システムを構成するクラウドサービスの OS、ミドルウェア、ソフトウェア、DBMS、プロトコル等のバージョンアップの際、必要な調査及び作業を実施することで、バージョンアップに対応可能な基盤とすること。
- ユーザ端末の OS 等のバージョンアップに備え、OS 等の特定バージョンに依存する機能が判明している場合は、その利用を最低限とすること。
- 契約期間中に本システムの稼働環境として導入しているソフトウェアのバージョンアップが発生した場合は、原則として追加費用なくバージョンアップ後の環境を前提として構築を行うこと。

8. 中立性に関する事項

8.1. オープンな標準的技術又は製品に関する事項

- 本システムで利用するクラウドサービスについて、採用するクラウドサービスの SLA 等により下記の内容を評価するとともに、クラウドサービス事業者に公開可能な範囲で確認し、必要に応じて適宜契約内容に含めること。内部仕様が公開されていなくても供給するクラウドサービス事業者において競争性が確保され中立性の趣旨において問題とならない場合は、その旨を記載すること。
  - 採用されているハードウェア、ソフトウェア等は、原則として特定ベンダーの技術に依存しない、オープンな技術仕様に基づいているか。
  - 採用されているハードウェア、ソフトウェア等は、原則としてオープンなインタフェースを利用して接続又はデータの入出力が可能であるか。
  - 採用されているハードウェア、ソフトウェア等の構成要素は、原則として標準化団体(ISO、IETF、ITU、JISC 等）が規定又は推奨する各種業界標準に準拠しているか。

8.2. 他事業者への円滑な引き継ぎに関する事項

- 採用する SLA やクラウドサービス事業者との契約内容、公開されている情報(ハードウェア、ソフトウェア等）をとりまとめ、他事業者への引き継ぎを可能とすること。
- 運用・保守や追加開発等の役務を調達する必要が生じた場合に特定のクラウドサービス事業者に依存することなく十分な競争性が働くものとすること。
- 本システム更改の際に、移行の妨げや特定の装置やプログラム等に依存することを防止するため、原則として基盤内のデータを標準的な形式で取り出すことができるものとすること。

9. 継続性に関する事項

9.1. 継続性に係る目標値

- 本システムでは、障害や大規模災害等として以下のような場合を想定する。
  - 地震、火災、風水害等、攻撃等による直接的な基盤の損壊。
  - 基盤周辺のライフライン（電力、通信等）の機能不全のよる基盤の長時間停止
  - マルウェア感染や不正侵入等のネットワークを介した攻撃による長時間停止
- 本システムは、復旧時間の目標値として以下を満たすこと。ただし、基盤と利用者間のネットワーク部分に障害の原因がある場合は除外してよい。

  障害発生時：24 時間[注 7]

  業務停止時：24 時間[注 8]

  大規模災害時：1 週間[注 9]
  - 大規模災害時については必ずしも完全復旧ではなく、管理機能よりも情報連携機能を優先させ、業務実施に必要となるデータ入出力のための API や GUI を利用できるようそれらを優先して復旧し、機能を限定した縮退運用により業務を継続することができればよい。
  - 採用するクラウドサービスの SLA に照らして、上記の目標値を達成することが困難な場合、あるいは冗長化を行えば達成は可能であるがコスト対効果の観点で課題が残ると考えられる場合などには、その旨を示した上で、業務要件に照らして最もコスト対効果が高いと考えられるように検討すること。

[注 7]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「A.1.2.2 業務継続性/サービス切替時間」レベル 1 の推奨値「1 営業日以内」を採用

[注 8]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「A.1.3.2 目標復旧水準(業務停止時)/RTO(目標復旧時間)」レベル 1 の推奨値「1 営業日以内」を採用

[注 9]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「A.1.4.1 目標復旧水準(大規模災害時)/システム再開目標」レベル 3 の推奨値「1 週間以内に再開」を採用

9.2. 継続性に係る対策

- バックアップの取得は日次[注 10]、バックアップの保存は 3 年間[注 11]とし、対象ことにバックアップの取得方法や保存先等を考慮し適切なバックアップ処理が可能な基盤とすること。
- バックアップの取得は自動化し、成否について運用管理者へ通知する機能を具備すること。なお、自動化されたバックアップ処理についても運用管理者による手動バックアップの取得が可能であること。
- クラウドサービス事業者から提供されるバックアップサービスを利用して差し支えない。ただし、利用するサービスの種類、同時被災しないことを前提としたバックアップサイトの場所、バックアップデータの取得時期及び保持期間（世代管理を含む）、自動化の程度等については、対象とするデータの性質等に応じて、業務へ影響を与えず、かつコスト対効果が高いものを適宜選定すること。

[注 10]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「C.1.2.5 バックアップ/バックアップ取得間隔」レベル 4 の推奨値「日次で取得」を採用

[注 11]「非機能要求グレード 2018」（独立行政法人情報処理推進機構、2018 年 4 月、https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html）において「社会的影響が限定されるシステム」における指標値「C.1.2.6 バックアップ/バックアップ保存期間」レベル 2 の推奨値「3 年」を採用

10. 情報セキュリティに関する事項

本事項については、以下に準拠する。

- 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
（内閣官房内閣サイバーセキュリティセンター、2022 年 7 月、
https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html）
- 「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」
（内閣官房内閣サイバーセキュリティセンター、2021 年 7 月、
https://www.nisc.go.jp/policy/group/general/kijun.html）
- 「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」
- クラウドアーキテクト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）

「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」に関する本システムの要件の詳細は以下のとおりである。

なお、セキュリティ対策については、ＭＡＦＦクラウドで定める規定がある場合は、それに従い対応すること。

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

表 6：情報システムに係る政府調達における情報セキュリティ要件

大項目	小項目	記載内容
情報システムに求める要件	信頼性	＜システムの可用性確保＞ サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として【24 時間】を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。
	情報セキュリティ	＜通信経路の分離＞ 不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。

		＜不正通信の遮断＞ 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。
		＜通信のなりすまし防止＞ 情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。
		＜サービス不能化の防止＞ サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。
		＜不正プログラムの感染防止＞ 不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。
		＜ログの蓄積・管理＞ 情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、１年保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。
		＜ログの保護＞ ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。
		＜時刻の正確性確保＞ 情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
		＜侵入検知＞ 不正行為に迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。

		＜主体認証＞ 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち【ユーザーID】の認証を行う機能として、【ユーザーID とパスワードによる認証】の方式を採用すること。
		＜ライフサイクル管理＞ 主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。
		＜アクセス権管理＞ 情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。
		＜管理者権限の保護＞ 特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。
		＜通信経路上の盗聴防止＞ 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。
		＜保存情報の機密性確保＞ 情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、外部との接続のある情報システムにおいて保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。
		＜保存情報の完全性確保＞ 情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。
		＜システムの構成管理＞ 情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出する

		とともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
		＜調達する機器等に不正プログラム等が組み込まれることへの対策＞ 機器等の製造工程において、府省庁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。
		＜情報セキュリティ水準低下の防止＞ 情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。
		＜プライバシー保護＞ 情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。
	情報システム稼働環境	仕様書　1調達案件の概要（4）業務・情報システムの概要　を参照
	テスト	＜構築時の脆弱性対策＞ 情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
	運用	＜情報の物理的保護＞ 情報の漏えいを防止するため、【メールアドレスの設定時の検証】等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。
		＜侵入の物理的対策＞ 物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

	保守	＜運用時の脆弱性対策＞ 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。
作業の実施体制・方法	作業実施体制	＜委託先において不正プログラム等が組み込まれることへの対策＞ 情報システムの構築において、府省庁が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。当該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。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁が情報セキュリティ監査の実施を必要と判断した場合は、受託者は情報セキュリティ監査を受け入れること。 また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。

11. 情報システム稼働環境に関する事項

11.1. クラウドサービス要件

本システムは、「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」（高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略本部）において示されている「クラウド・バイ・デフォルト」の考え方に即して、クラウドサービスを利用して構築する。具体的には、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年（平成 30 年）6 月 7 日各府省 CIO 連絡会議決定。最終改定は、2023 年 9 月 29 日）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。これらの状況を踏まえ、本システムはパブリッククラウド利用を前提とし、MAFF クラウドの利用を指定する。

パブリッククラウドの利用にあたっては、「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」の 1.6 クラウドサービスのスマートな利用によるメリット（マネージドサービス活用によるコスト削減、サーバレスによるセキュリティ向上とセキュリティ対策コストの削減、IaC による構築の 3 項目）に適合すること。

稼働環境については、以下を満たすこと。なお、詳細については資料閲覧にて「農林水産省クラウド利用ガイドライン及び関係資料」を参照すること。本業務の実施において、農林水産省クラウド利用ガイドラインの改定があった場合は最新版を参照すること。

（ア）MAFF クラウドにて選定しているクラウドサービスプロバイダーを利用すること。

なお、2023 年度利用しているクラウドサービスプロバイダーは：Amazon Web Services、Microsoft Azure である。

MAFF クラウドで利用するクラウドサービスは、政府情報システムのためのセキュリティ評価制度（ISMAP)の ISMAP クラウドサービスリストに登録されている。

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

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

（エ）Azure を採用する場合は、サブスクリプションの紐づけ先に MAFF クラウドが用意した AzureAD テナントを設定すること。また、契約種別は原則として CSP 契約とすること。

（オ）パブリッククラウド上に構成するサーバ・サービスは自動スケーリング機能の利用やスペック調整を容易にできるような構成にし、性能を容易に改善できること。

（カ）パブリッククラウド上で稼働するサーバやサービスに対しては冗長化などの構成を行うなど、可用性を高めた構成とすること。可能であればクラウドサービスのベストプラクテ

ィスが自動で適用されるよう、SaaS 形態のサービスを利用すること。

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

（ク）以下の各管理については、クラウドサービスで可能な限り実現することとし、自動化を図ること。

運用管理、死活監視、稼働状況監視、セキュリティ監視、ジョブ管理、バックアップ管理、ログ管理（送受信ログ等の保存）、ウィルスパターン更新管理、セキュリティパッチ更新管理、依頼作業対応、構成管理、文書管理、アカウント管理、データ管理、障害対応、定例報告

（ケ）クラウドのアカウント／サブスクリプションについて、AWS ならびに Azure のアカウントは、納品物の一部であり、引継ぎの対象である。アカウントの契約者は、農林水産省の PJMO とすることが必須とする。なお、業者がクラウドのアカウントを契約し、農林水産省の PJMO にサービスとして提供することは、原則認めない。

AWS アカウントの契約は、下記のいずれかとすること。

・日本に本社を置く AWS パートナーネットワークに参加する AWS の代理店

・AWS Distribution Program に登録されている日本企業

Azure サブスクリプションの契約は、下記のいずれかとすること。

・日本に本社を置くマイクロソフト クラウド パートナー プログラムに参加する Microsoft の代理店

・インダイレクトソリューションプロバイダーに登録されている日本企業

11.2. ハードウェア要件

本システムで利用するクラウドサービスについては、SLA やクラウドサービス事業者との契約内容、公開されている情報（ハードウェア、ソフトウェア等）により、以下の要件を満たしていることを確認すること。

- 本要件定義書記載の要件を満たす最適、且つ合理的で費用対効果の優れたハードウェア構成（搭載するソフトウェア及びネットワーク構成を含む）であること。
- 前記の「情報セキュリティに関する事項」を満たす構成であること。
- システム使用容量の増加への対応及び運用作業を容易に行えるハードウェア構成となっていること。
- 環境に配慮し、省スペース、電源容量、発熱量等について考慮されていること。

11.3. ソフトウェア要件

本システムで利用するクラウドサービスについては、SLA やクラウドサービス事業者との契約内容、公開されている情報（ハードウェア、ソフトウェア等）により、以下の要件を満たしていることを確認すること。

- 汎用的な複数の製品（サーバ、OS 等）でソフトウェアが動作できること。なお、以下のブラウザにおいては、公示時点の最新バージョンのブラウザでの動作を保証するよう構築されていること。
  - Microsoft(R) Edge
  - Mozilla Firefox
  - Apple(R) Safari
  - Google Chrome
- ユーザ数、業務量が同程度の民間企業又は行政機関等で同規模以上のシステムに導入され、十分な稼動実績を有するソフトウェアが選定されていること。
- ユーザの利便性に配慮したソフトウェア構成であること。
- 安定性及び安全性の確保のため、導入されているソフトウェアは調達段階での最新のバージョンが使用されていること。
- 本要件定義書に定めた要件、費用対効果及びソフトウェア製品の組み合わせを総合的に検討したうえで、本システムで利用するクラウドサービスを決定すること。

11.4. ネットワーク要件

前記の「情報セキュリティに関する事項」を満たし、且つインターネットへ接続できるよう構築すること。

11.5. 施設・設備要件

本システムで利用する施設・設備は各事業者がそれぞれ持っているものを使用する。

12. テストに関する事項

12.1. 基本方針

設計・開発事業者は、テスト手法及び品質検証の手法として、過去の情報システム構築案件において、豊富な成功実績を有する手法を利用すること。なお、設計・開発事業者固有のテスト手法及び品質検証手法を利用する場合は、ISO/IEC12207、共通フレーム SLCPJCF2013 等の標準的なテスト手法、ISO/IEC25040 等の標準的な品質評価規格との対応関係について監督府省庁に説明すること。

本業務において行うテストの方針を以下に記載する。

表 6：テストの基本方針

No	テストの名称	テストの方針
1	単体テスト	● プログラム及びモジュールが個別単体において正しく機能することを確認するためのテストを実施する。
2	結合テスト	● 本システムで想定される機能全体において、段階的にプログラム及びモジュールを結合した状態でテストを行い、アプリケーションプログラムの結合が完全であること、詳細設計の内容を実現していることを確認するためのテストを実施する。
3	総合テスト	● 本システム全体の欠陥除去及びシステムの要件の充足を目的とし、システム全体として妥当であることを機能性、使用性、運用性、性能、信頼性及びセキュリティ等の観点から確認するためのテストを本番環境と同様の環境にて実施する。
4	連携テスト	● 本システムと、利用者側の他システム及びプラットフォームとの接続が、適切に実施できることを確認するためのテストを実施する。
5	受入テスト	● 機能及び運用手順の確認を目的として、一部の利用者（木材関連事業者）及び監督府省庁が受入テストを実施する。設計・開発事業者は、受入テストの実施要件に従って、監督府省庁が受入テストを実施する上で必要な支援を行う。

各テストを行うため、単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載した「テスト計画書」を作成し、監督府省庁と協議の上、承認を得ること。

各テスト実施時に「テスト計画書」に基づきテストケース、テスト項目、テスト手順、テスト条件、想定するテスト結果等を含む「テスト仕様書」を作成の上、テスト実施期間中には監督府省庁に適宜進捗報告を行い、テスト終了時には、実施内容、品質評価結果及び次工程への申し送り事項等について、テストごとに「結果報告書」を作成し、監督府省庁と協議の上、承認を得ること。

必要に応じてテストツール、テスト管理ツールを活用し、効率良くテストを実施すること。

12.2. テストの種類及び目的、内容

各テストの目的、内容を以下に記載する。

表 7：テストの内容

No	テストの名称	テストの内容
1	単体テスト	【新規作成する機能】 ● 設計・開発事業者は、以下のとおり、本システムを構成する機能別にテストを実施すること。 ● プログラムソースコードを網羅するホワイトボックステスト（命令網羅、分岐網羅、条件網羅）、関数又は機能の入出力を網羅するブラックボックステストの双方を行うこと。 【パッケージ化されている機能】 ● ソフトウェアパッケージ製品を利用した新規作成機能を対象とし、動作検証テストを実施すること。
2	結合テスト	● テスト対象機能について、同値分析、境界値分析、原因結果分析を行い、その結果を踏まえてテストケース、テスト項目を設定すること。 ● 本システムに備えるユーザインタフェースについて、仕様どおりに操作できるか、誤った操作をしても適切なエラーメッセージが表示されるか等の操作確認を行うこと。 ● テスト対象に対して異常データを含む様々なバリエーションのデータを投入し、動作及び処理結果を確認すること。 ● 結合したプログラム及びモジュールが正常に問題なく動作することを確認すること。

No	テストの名称	テストの内容
3	総合テスト	● 機能テスト、操作マニュアルテストは実運用を想定した環境下でテストを実施し、障害時対応を含めて、各業務シナリオの実運用で定められた手順・体制等により問題なく運用できることを検証すること。 ● 性能テスト、負荷テストにおいて、充分な性能を満たせない場合は、監督府省庁と協議の上、速やかに性能改善に取り組むこと。
4	連携テスト	● 機能テスト、操作マニュアルテストは実運用を想定した環境下でテストを実施し、障害時対応を含めて、複数の他システム及びプラットフォームとの連携が問題なく運用できることを検証すること。 ● 性能テスト、負荷テストにおいて、充分な性能を満たせない場合は、監督府省庁と協議の上、速やかに性能改善に取り組むこと。 ● 外部連携テストにおいて、「機能要件定義書」に示した外部の連携情報システムと正常に連携可能であること等のテストを行うこと。また、テストを実施するに当たり、連携先システムとの調整を行うこと。 ● テストを実施するに当たり、連携先システムとの調整を行うこと。
5	受入テスト	● 監督府省庁は、本調達の設計・開発事業者が作成する、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載した「受入テスト計画書」の案の内容を確認し、適宜修正の上、内容を確定させる。 ● 設計・開発事業者は、可能な限り本番環境に近いテスト環境を用意すること。 ● 設計・開発事業者は、可能な限り本番運用に近いテストシナリオを準備すること。 ● 設計・開発事業者は、監督府省庁が実施する受入テストに必要に応じて立ち合いを行うこと。立ち合いを行う対象・期間はテスト計画書において協議し・決定する。また、立ち合いを行う受入テストについては、設計・開発事業者がその結果を整理すること。 ● 監督府省庁は、受入テストの結果を踏まえ、設計・開発事業者

No	テストの名称	テストの内容
		に対し、必要に応じ、課題等の指摘を行うので、設計・開発事業者は監督府省庁からの受入テスト結果報告内容を取りまとめ、必要に応じ指摘事項への対応を行うこと。

12.3. テスト環境

設計・開発事業者にて準備したテスト環境にて単体テスト及び結合テストを実施すること。

また、連携テスト、総合テスト及び受入テストは、実際に導入する機器をシステム運用する環境に移設した環境にて実施すること。また、既設の機器等を使用する必要がある場合には、使用する機器等、その理由、作業日時、作業担当者等をあらかじめ取りまとめ、監督府省庁、関係部局等と調整・協議のうえ、監督府省庁の承認を得ること。なお、不足する機器等がある場合には、設計・開発事業者にて準備すること。

また、「機能要件定義書」に記載されたサービスのテストを実施可能な環境を準備すること。

設計・開発事業者は、本システム稼働開始後は運用・保守業務において、アプリケーションプログラム保守等の対応が発生した際のテスト環境を構築すること。なお、「機能要件定義書」に記載されたサービスのテストを想定するが、テスト用に縮退を前提とする最小構成にて構築すること。

12.4. テストデータ

各テストデータは、原則として設計・開発事業者が擬似データを作成して用いること。ただし、外部の連携情報システムとの総合テストについては、設計・開発事業者が調整を行いテストデータの作成分担を決定し、監督府省庁の承認を得ること。

各テストで使用したテストシナリオ、テストスクリプト、テストデータ等については、受入テスト、運用業務期間における動作確認等において、それらを一部改変して再利用できるようにしておくこと。

13. システム使用に関する事項

13.1. ユーザ登録

クリーンウッド法に基づく木材関連事業者の登録やバイオマス関連の認定事業者情報などのマスタデータについては、初期登録の必要がある。具体的には、システム利用者として登録する事業者及び個人事業主ならびに各部署・グループとその所属する利用者を登録する。

13.2. システム利用関連資料

本システムを、利用するにあたって必要となるユーザーズマニュアル、教育資料、ユーザ登録資料等、一連のシステム利用ガイドについては、監督府省庁の提供する情報提供サイトに掲載する。

14. 移行に関する事項

14.1. データ移行

本システムは、今回新規に構築されるものであり、原則としてシステム移行(データ移行)は発生しない。また、本システムの連携対象システムからの過去トランザクションデータ等のデータ移行も求めない。

15. 引継ぎに関する事項

設計・開発事業者は、設計・開発の設計書、作業経緯、及び監督府省庁の承認のもと本システムの運用・保守業務として解決すべきとした残存課題等を文書化し、監督府省庁及び次期運用・保守事業者に対して確実な引継ぎを行うこと。

なお、特に監督府省庁の担当者は必ずしも情報システムに関する専門的知見を有していない可能性があることに留意し、情報システムに関する専門的知見のない担当者でも円滑な業務継続が可能となるよう、引継資料には、要点を簡潔かつ分かりやすく整理したものを付属させること。

16. 教育に関する事項

16.1. 教育対象者の範囲、教育の方法

(1) 教育対象者の範囲

本システムの教育実施対象者は、下表の「情報システムのユーザの種類、特性」に記載した各ユーザ、及び監督府省庁担当職員とする。なお、各ユーザへの教育研修については実施内容やスケジュールを受託者が検討し、「教育研修計画」を作成して予め監督府省庁の承認を得て研修を実施すること。

表８：情報システムのユーザの種類及び特性

No	ユーザの種類	利用する機能			利用する端末	利用するネットワーク
		利用者向け	事業管理者向け	システム管理者向け		
1	一般利用者	○			PC、タブレット、スマートフォン、等	インターネット
2	事業管理者		○		PC、タブレット、等	インターネット
3	システム運用担当者			○	PC、タブレット、等	インターネット
4	監督府省庁担当職員			○	PC、タブレット、等	インターネット

ア. システム管理者、運用担当者に対する教育

本システムのユーザのうち、メンテナンスや管理の主体となるシステム管理ならびに運用に関する担当者に対して、必要に応じてシステムの管理操作マニュアルを作成すること。

イ. 一般ユーザに対する教育

本システムを利用するシステム管理者・運用担当者以外の一般ユーザについて、ロール・サブシステムごとの機能概要、操作方法に関するマニュアルを作成すること。

ウ. 監督府省庁担当職員に対する教育

本システムに係る監督府省庁担当職員について、上記ア及びイでそれぞれ作成したマニュアルを用いること。

(2) 教育の方法

本システムの教育実施方法としては以下のとおりとする。

ア. 資料配布

設計・開発事業者はシステムを利用する際に参照する操作マニュアル等の資料を配布し、ユーザが配布された操作マニュアルを通読することにより教育を行う。なお、端末にインストールし、利用される日本語ワープロソフトウェア、統合ビジネスアプリケーションプログラム及び PDF ファイル作成・編集ソフトウェア等については、設計・開発事業者自身が用意するマニュアルの代替として、市販等のマニュアル及び独習用テキストにより教育することも可とする。

イ. 研修の実施

設計・開発事業者は上記教育対象者に対して作成・配布した資料並びに当システムの動作を確認した PC を使用し、システムの使用方法についての研修を実施する。

本業務における研修の規模は、オンライン又は対面にて 3 ～ 5 回程度（受講生 20 人程度/回）とし、実施時期は統合テスト終了後とする。実施にあたっては、日程、教育内容、開催場所、配布資料、関連機器の手配と合わせ、出席者への事前通達を行い、万全の準備をしたうえで実施する。

なお、研修参加者の一部に対して受入テストに参画してもらう。

ウ. FAQ

設計・開発事業者が頻度の高い問合せとその回答やマニュアルに記載しきれない細かなシステム利用上のテクニック等を、操作マニュアルに付属、ならびにインターネット上に公開し、ユーザが問題の自己解決やシステムのより便利な使い方を知ることができるようにすることで教育を行う。

16.2. 教材の作成

設計・開発事業者は、教育に必要となる「教材（各種操作マニュアル、FAQ 等を含む）」の作成を実施すること。教材の詳細な種類、内容、提供方法等は、監督府省庁と協議し、「教育実施計画書」として取りまとめたうえで決定すること。加えて、以下に記載する要件を遵守する教材とすること。

- IT リテラシが高くないユーザであっても理解できるように、平易な表現を用いること。
- 操作マニュアルや FAQ については、運用中に発生するシステムに係る疑問をユーザ自身で解

決できるようにすることを目的に、業務の流れに則した構成や検索性を確保するなどの工夫を行うこと。

17. 運用に関する事項

本システムの運用について、実施する範囲は、採用するクラウドサービスにおけるクラウドサービス事業者との責任分界等に左右されるものと考えられる。かかる観点から、設計・開発事業者は、設計・開発に関する作業の中で、下記の要素を含んだ運用設計を、採用するクラウドサービスの性質等に応じて実施すること。

17.1. 運転管理・監視等

(1) 運転管理・監視

人が行う処理と情報システム側で行う処理の切り分け、情報システムの運用を行う時間、内容、手法、連絡等について記載する。記載に当たっては、ステークホルダー間・プロセス間の責任分界を考慮し、作業の抜け漏れ、重複等がないように定義すること。特に、情報システムの障害発生箇所の切り分け、発生原因の追究と解消について、関係する事業者との連携のあり方、監視、切り分け、復旧等に係るオペレーションなどが、新規の運用・保守事業者にも把握できるものとすること。

代表的な作業項目の例としては、次のようなものが考えられる。

- 運転管理・監視
  - 死活監視
  - 性能監視
  - 稼働状況監視
  - セキュリティ監視（不正侵入・不正アクセス等の監視）
  - 障害の一次対応（障害検知又は受付、保守事業者への連絡等）

なお、上記の運転管理・監視の内容に応じて、必要となるログ等の情報の取得（取得対象、取得内容等）、保管（保管媒体、保管期間等）等の要件を別途、定義しておくこと。

- システム操作
  - バックアップ管理（バックアップの実施、及びバックアップデータからの復旧の実施等）
  - 情報システムの設定変更（ユーザの追加・削除、アカウントロック解除、パスワードの変更・初期化等）
  - 修正プログラム又はアップデートファイルの適用

(2) 運用サポート業務

業務の実施に必要な体制以外に、ユーザからの問い合わせ対応や操作研修等の運用サポート体制が必要となる場合は、その内容を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- ヘルプデスク業務（ユーザからの問い合わせに対し、解決策を講ずるために行う業務）
- コールセンタ業務（ユーザからの問い合わせに対し、予め決められた事項を案内又は回答する業務であり、主に大量の問い合わせがある場合）
- 操作研修（各ユーザに対する操作研修等）

17.2. 業務運用支援

本システムの稼働に当たり、管理者以外の関係課室が行う業務の運用支援作業について記載する。また、本システムの運用期間中に更改や改修業務等が予定されている場合、これに伴い本システムに対して実施することが想定される作業があれば、必要な作業内容を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 本システム内のデータ抽出作業

17.3. 運用の実績の評価と改善

本システムの安定的な運用の維持と継続的な改善のために必要となる運用実績の評価、改善活動について記載する。前記の「性能に関する事項」、「信頼性に関する事項」及び「継続性に関する事項」で定義した各指標のほか、計画的なクラウドサービス利用の判断材料とするための監視項目についても定義する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 運用実績（サービスレベルの達成状況、情報システムの構成と運転状況（リソース使用量等含む。）等）の値の取得、評価及び管理。
- 運用実績が目標に満たない場合の要因分析、改善措置の検討。

18. 保守に関する事項

本システムの保守について、実施する範囲は、前記の「運用に関する事項」と同様、採用するクラウドサービスにおけるクラウドサービス事業者との責任分界等に左右されるものと考えられる。かかる観点から、受注者は、設計・開発に関する作業の中で、下記の要素を含んだ保守設計を、採用するクラウドサービスの性質等に応じて実施すること。

18.1. アプリケーションプログラムの保守

情報セキュリティに関する脆弱性の修正や不具合等の確認及び修正、小規模な改修等の対応範囲や条件を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 不具合の受付と修正サービスの提供期間
- 不具合の確認や修正プログラムの作成及びテストのための環境（誰が用意するか等）
- 不具合修正に係る作業の実施期間

18.2. ハードウェアの保守

不具合の修理等の対応範囲や条件を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 製品の保守継続可能期間
- 契約形態（故障発生時のみ対応、年間契約による対応）
- 修理のための対応方法（障害機の送付・作業員のオンサイト作業）
- 保守受付時間（平日のみ・休日込み、日中営業時間帯、24 時間）
- 保守対応時間（平日のみ・休日込み、日中営業時間帯、24 時間）
- 保守応動時間（オンサイト作業の場合、障害の連絡を受け付けてから機器設置場所までの応動時間）

18.3. ソフトウェア製品の保守

情報セキュリティに関する脆弱性の修正としての最新のセキュリティパッチの適用、不具合への対応としてのパッチの適用、小規模な改善等を目的とするリビジョンアップや大幅な改修を伴うバージョンアップ等の対応範囲や条件を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 脆弱性情報の報告とセキュリティパッチ適用サービス等の提供期間
- システム稼働時間を踏まえたセキュリティパッチ適用方針
- 不具合の受付とパッチ適用サービス等の提供期間
- リビジョンアップやバージョンアップにおける使用権の提供有無
- サポート対応

18.4. データの保守

本システムの設定データやマスタデータの更新作業等に関する要件を記載する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 設定データに異常が生じた場合の復旧作業
- マスタデータに異常が生じた場合の復旧作業及びアップデート時の更新作業

18.5. 保守実績の評価と改善

安定的な運用の維持と継続的な改善のために必要となる保守実績の評価、改善活動について記載する。前記の「性能に関する事項」、「信頼性に関する事項」及び「拡張性に関する事項」で定義した指標のほか、計画的なクラウドサービス利用の判断材料とするための監視項目についても定義する。

代表的な作業項目の例としては、次のようなものが考えられる。

- 保守実績（サービスレベルの達成状況等）の値の取得、評価及び管理
- 保守実績が目標に満たない場合の要因分析、改善措置の検討

AWS/Azure設定確認リスト　　凡例：〇：責任者、△：サポート

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

項目		見出し		要件		備考	必須可否
1	認証・認可	1.1	ユーザー認証	1.1.1	特定のユーザーや管理者のみに表示・実行を許可すべき画面や機能、APIでは、ユーザー認証を実施すること	特定のユーザーや管理者のみにアクセスを許可したいWebシステムでは、ユーザー認証を行う必要があります。また、ユーザー認証が成功した後にはアクセス権限を確認する必要があります。そのため、認証済みユーザーのみがアクセス可能な箇所を明示しておくことが望ましいでしょう。 リスクベース認証や二要素認証など認証をより強固にする仕組みもあります。不特定多数がアクセスする必要がない場合には、IPアドレスなどによるアクセス制限も効果があります。 OpenIDなどIdP(ID Provider)を利用する場合には信頼できるプロバイダであるかを確認する必要があります。IdPを使った認証・認可を行う場合も他の認証・認可に関する要件を満たすものを利用することが望ましいです。	必須
				1.1.2	上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ（非公開にすべきデータは直接URLで指定できる公開ディレクトリに配置しない）では、ユーザー認証を実施すること		必須
				1.1.3	多要素認証を実施すること	多要素認証（Multi Factor Authentication: MFA）とは、例えばパスワードによる認証に加え、TOTP（Time-Based One-Time Password：時間ベースのワンタイムパスワード）やデジタル証明書など二つ以上の要素を利用した認証方式です。手法については NIST Special Publication 800-63B などを参照してください。	推奨
		1.2	ユーザーの再認証	1.2.1	個人情報や機微情報を表示するページに遷移する際には、再認証を実施すること	ユーザー認証はセッションにおいて最初の一度だけ実施するのではなく、重要な情報や機能へアクセスする際には再認証を行うことが望ましいでしょう。	推奨
				1.2.2	パスワード変更や決済処理などの重要な機能を実行する際には、再認証を実施すること		推奨
		1.3	パスワード	1.3.1	ユーザー自身が設定するパスワード文字列は最低 8文字以上であること	認証を必要とするWebシステムの多くは、パスワードを本人確認の手段として認証処理を行います。そのためパスワードを盗聴や盗難などから守ることが重要になります。	必須
				1.3.2	登録可能なパスワード文字列の最大文字数は64文字以上であること	パスワードを処理する関数の中には最大文字数が少ないものもあるので注意する必要があります。	必須
				1.3.3	パスワード文字列として使用可能な文字種は制限しないこと	任意の大小英字、数字、記号、空白、Unicode文字など任意の文字が利用可能である必要があります。	必須
				1.3.4	パスワード文字列の入力フォームはinput type="password"で指定すること	基本的にinputタグのtype属性には「password」を指定しますが、パスワードを一時的に表示する可視化機能を実装する場合にはこの限りではありません。	必須
				1.3.5	ユーザーが入力したパスワード文字列を次画面以降で表示しないこと（hiddenフィールドなどのHTMLソース内やメールも含む）		必須

項目	見出し		要件		備考	必須可否
			1.3.6	パスワードを保存する際には、平文で保存せず、Webアプリケーションフレームワークなどが提供するハッシュ化とsaltを使用して保存する関数を使用すること	関数が存在しない場合にはパスワードは「パスワード文字列＋salt（ユーザー毎に異なるランダムな文字列）」をハッシュ化したものとsaltのみを保存する必要があります。（saltは20文字以上であることが望ましい） パスワード文字列のハッシュ化をさらに安全にする手法としてストレッチングがあります。	必須
			1.3.7	ユーザー自身がパスワードを変更できる機能を用意すること		必須
			1.3.8	パスワードはユーザー自身に設定させること システムが仮パスワードを発行する場合はランダムな文字列を設定し、安全な経路でユーザーに通知すること		推奨
			1.3.9	パスワードの入力欄でペースト機能を禁止しないこと	長いパスワードをユーザーが利用出来るようにするためにペースト機能を禁止しないようにする必要があります。	推奨
			1.3.10	パスワード強度チェッカーを実装すること	使用する文字種や文字数を確認し、ユーザー自身にパスワードの強度を示せるようにします。またユーザーIDと同じ文字列や漏洩したパスワードなどのリストとの突合を行う必要があります。手法については NIST Special Publication 800-63B などを参照してください。	推奨
	1.4	アカウントロック機能について	1.4.1	認証時に無効なパスワードで10回試行があった場合、最低30分間はユーザーがロックアウトされた状態にすること	パスワードに対する総当たり攻撃や辞書攻撃などから守るためには、試行速度を遅らせるアカウントロック機能の実装が有効な手段になります。アカウントロックの試行回数、ロックアウト時間については、サービスの内容に応じて調整することが必要になります。	必須
			1.4.2	ロックアウトは自動解除を基本とし、手動での解除は管理者のみ実施可能とすること		推奨
	1.5	パスワードリセット機能について	1.5.1	パスワードリセットを実行する際にはユーザー本人しか受け取れない連絡先（あらかじめ登録しているメールアドレス、電話番号など）にワンタイムトークンを含むURLなどの再設定方法を通知すること	連絡先については、事前に受け取り確認をしておくことでより安全性を高めることができます。 使用されたワンタイムトークンは破棄し、有効期限を12時間以内とし必要最低限に設定してください。	必須
			1.5.2	パスワードはユーザー自身に再設定させること		必須
	1.6	アクセス制御について	1.6.1	Web ページや機能、データをアクセス制御（認可制御）する際には認証情報・状態を元に権限があるかどうかを判別すること	認証により何らかの制限を行う場合には、利用しようとしている情報や機能へのアクセス（読み込み・書き込み・実行など）権限を確認することでアクセス制御を行うことが必要になります。 画像やファイルなどのコンテンツ、APIなどの機能に対しても、全て個別にアクセス権限を設定、確認する必要があります。 これらはアクセス権限の一覧表に基づいて行います。 CDNなどを利用してコンテンツを配置するなどアクセス制御を行うことが困難な場合、予測が困難なURLを利用することでアクセスされにくくする方法もあります。	必須

項目		見出し		要件		備考	必須可否
				1.6.2	公開ディレクトリには公開を前提としたファイルのみ配置すること	公開ディレクトリに配置したファイルは、URLを直接指定することでアクセスされる可能性があります。そのため、機微情報や設定ファイルなどの公開する必要がないファイルは、公開ディレクトリ以外に配置する必要があります。	必須
		1.7	アカウントの無効化機能について	1.7.1	管理者がアカウントの有効・無効を設定できること	不正にアカウントを利用されていた場合に、アカウントを無効化することで被害を軽減することができます。	推奨
2	セッション管理	2.1	セッションの破棄について	2.1.1	認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側のセッションを破棄しログアウトすること	認証を必要とするWebシステムの多くは、認証状態の管理にセッションIDを使ったセッション管理を行います。認証済みの状態にあるセッションを不正に利用されないためには、使われなくなったセッションを破棄する必要があります。セッションタイムアウトの時間については、サービスの内容やユーザー利便性に応じて設定することが必要になります。また、NIST Special Publication 800-63B などを参照してください。	必須
				2.1.2	ログアウト機能を用意し、ログアウト実行時にはサーバー側のセッションを破棄すること	ログアウト機能の実行後にその成否をユーザーが確認できることが望ましい。	必須
		2.2	セッションIDについて	2.2.1	Webアプリケーションフレームワークなどが提供するセッション管理機能を使用すること	セッションIDを用いて認証状態を管理する場合、セッションIDの盗聴や推測、攻撃者が指定したセッションIDを使用させられる攻撃などから守る必要があります。 また、セッションIDは原則としてcookieにのみ格納すべきです。	必須
				2.2.2	セッションIDは認証成功後に発行すること 認証前にセッションIDを発行する場合は、認証成功直後に新たなセッションIDを発行すること		必須
				2.2.3	ログイン前に機微情報をセッションに格納する時点でセッションIDを発行または再生成すること		必須
				2.2.4	認証済みユーザーの特定はセッションに格納した情報を元に行うこと		必須
		2.3	CSRF（クロスサイトリクエストフォージェリー）対策の実施について	2.3.1	ユーザーにとって重要な処理を行う箇所では、ユーザー本人の意図したリクエストであることを確認できるようにすること	正規ユーザー以外の意図により操作されては困る処理を行う箇所では、フォーム生成の際に他者が推測困難なランダムな値（トークン）をhiddenフィールドやcookie以外のヘッダーフィールド（X-CSRF-TOKENなど）に埋め込み、リクエストをPOSTメソッドで送信します。フォームデータを処理する際にトークンが正しいことを確認することで、正規ユーザーの意図したリクエストであることを確認することができます。 また、別の方法としてパスワード再入力による再認証を求める方法もあります。 cookieのSameSite属性を適切に使うことによって、CSRFのリスクを低減する効果があります。SameSite属性は一部の状況においては効果がないこともあるため、トークンによる確認が推奨されます。	必須
3	入力処理	3.1	パラメーターについて	3.1.1	URLにユーザーID やパスワードなどの機微情報を格納しないこと	URLは、リファラー情報などにより外部に漏えいする可能性があります。そのため URLには秘密にすべき情報は格納しないようにする必要があります。	必須

項目		見出し		要件		備考	必須可否
				3.1.2	パラメーター（クエリーストリング、エンティティボディ、cookieなどクライアントから受け渡される値）にパス名を含めないこと	ファイル操作を行う機能などにおいて、URL パラメーターやフォームで指定した値でパス名を指定できるようにした場合、想定していないファイルにアクセスされてしまうなどの不正な操作を実行されてし まう可能性があります。	必須
				3.1.3	パラメーター要件に基づいて、入力値の文字種や文字列長の検証を行うこと	各パラメーターは、機能要件に基づいて文字種・文字列長・形式を定義する必要があります。入力値に想定している文字種や文字列長以外の値の入力を許してしまう場合、不正な操作を実行されてしまう可能性があります。サーバー側でパラメーターを受け取る場合、クライアント側での入力値検証の有無に関わらず、入力値の検証はサーバー側で実施する必要があります。	必須
		3.2	ファイルアップロードについて	3.2.1	入力値としてファイルを受け付ける場合には、拡張子やファイルフォーマットなどの検証を行うこと	ファイルのアップロード機能を利用した不正な実行を防ぐ必要があります。画像ファイルを扱う場合には、ヘッダー領域を不正に加工したファイルにも注意が必要です。	必須
				3.2.2	アップロード可能なファイルサイズを制限すること	圧縮ファイルを展開する場合には、解凍後のファイルサイズや、ファイルパスやシンボリックリンクを含む場合のファイルの上書きにも注意が必要です。	必須
		3.3	XMLを使用する際の処理について	3.3.1	XMLを読み込む際は、外部参照を無効にすること	手法についてはXML External Entity Prevention Cheat Sheetなどを参照してください。 https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html	必須
		3.4	デシリアライズについて	3.4.1	信頼できないデータ供給元からのシリアライズされたオブジェクトを受け入れないこと	デシリアライズする場合は、シリアライズしたオブジェクトにデジタル署名などを付与し、信頼できる供給元が発行したデータであるかを検証してください。	必須
		3.5	外部リソースへのリクエスト送信について	3.5.1	他システムに接続や通信を行う場合は、外部からの入力によって接続先を動的に決定しないこと	外部から不正なURLやIPアドレスなどが挿入されると、SSRF(Server-Side Request Forgery)の脆弱性になる可能性があります。外部からの入力によって接続先を指定せざるを得ない場合は、ホワイトリストを基に入力値の検証を実施するとともに、アプリケーションレイヤーだけではなくネットワークレイヤーでのアクセス制御も併用する必要があります。	推奨
4	出力処理	4.1	HTMLを生成する際の処理について	4.1.1	HTMLとして特殊な意味を持つ文字（< > " ' &）を文字参照によりエスケープすること	外部からの入力により不正なHTMLタグなどが挿入されてしまう可能性があります。「<」→「<」や「&」→「&」、「"」→「"」のようにエスケープを行う必要があります。スクリプトによりクライアント側でHTMLを生成する場合も、同等の処理が必要です。実装の際にはこれらを自動的に実行するフレームワークやライブラリを使用することが望ましいでしょう。また、その他にもスクリプトの埋め込みの原因となるものを作らないようにする必要があります。 XMLを生成する場合も同様にエスケープが必要です。	必須
				4.1.2	外部から入力したURLを出力するときは「http://」または「https://」で始まるもののみを許可すること		必須

項目	見出し		要件		備考	必須可否
			4.1.3	<script>...</script>要素の内容やイベントハンドラ（onmouseover=""など）を動的に生成しないようにすること	<script>...</script>要素の内容やイベントハンドラは原則として動的に生成しないようにすべきですが、jQueryなどのAjaxライブラリを使用する際はその限りではありません。ライブラリについては、アップデート状況などを調べて信頼できるものを選択するようにしましょう。	必須
			4.1.4	任意のスタイルシートを外部サイトから取り込めないようにすること		必須
			4.1.5	HTMLタグの属性値を「"」で囲うこと	HTMLタグ中のname="value"で記される値(value)にユーザーの入力値を使う場合、「"」で囲わない場合、不正な属性値を追加されてしまう可能性があります。	必須
			4.1.6	CSSを動的に生成しないこと	外部からの入力により不正なCSSが挿入されると、ブラウザに表示される画面が変更されたり、スクリプトが埋め込まれる可能性があります。	必須
	4.2	JSONを生成する際の処理について	4.2.1	文字列連結でJSON文字列を生成せず、適切なライブラリを用いてオブジェクトをJSONに変換すること	適切なライブラリがない場合は、JSONとして特殊な意味を持つ文字（"￥,:{}[]）をUnicodeエスケープする必要があります。	必須
	4.3	HTTPレスポンスヘッダーについて	4.3.1	HTTPレスポンスヘッダーのContent-Typeを適切に指定すること	一部のブラウザではコンテンツの文字コードやメディアタイプを誤認識させることで不正な操作が行える可能性があります。これを防ぐためには、HTTPレスポンスヘッダーを「Content-Type: text/html; charset=utf-8」のように、コンテンツの内容に応じたメディアタイプと文字コードを指定する必要があります。	必須
			4.3.2	HTTPレスポンスヘッダーフィールドの生成時に改行コードが入らないようにすること	HTTPヘッダーフィールドの生成時にユーザーが指定した値を挿入できる場合、改行コードを入力することで不正なHTTPヘッダーやコンテンツを挿入されてしまう可能性があります。これを防ぐためには、HTTPヘッダーフィールドを生成する専用のライブラリなどを使うようにすることが望ましいでしょう。	必須
	4.4	その他の出力処理について	4.4.1	SQL文を組み立てる際に静的プレースホルダを使用すること	SQL文の組み立て時に不正なSQL文を挿入されることで、SQLインジェクションを実行されてしまう可能性があります。これを防ぐためにはSQL文を動的に生成せず、プレースホルダを使用してSQL文を組み立てるようにする必要があります。 静的プレースホルダとは、JIS/ISOの規格で「準備された文(Prepared Statement)」と規定されているものです。	必須
			4.4.2	プログラム上でOSコマンドやアプリケーションなどのコマンド、シェル、eval()などによるコマンドの実行を呼び出して使用しないこと	コマンド実行時にユーザーが指定した値を挿入できる場合、外部から任意のコマンドを実行されてしまう可能性があります。コマンドを呼び出して使用しないことが望ましいでしょう。	必須
			4.4.3	リダイレクタを使用する場合には特定のURLのみに遷移できるようにすること	リダイレクタのパラメーターに任意のURLを指定できる場合（オープンリダイレクタ）、攻撃者が指定した悪意のあるURLなどに遷移させられる可能性があります。	必須
			4.4.4	メールヘッダーフィールドの生成時に改行コードが入らないようにすること	メールの送信処理にユーザーが指定した値を挿入できる場合、不正なコマンドなどを挿入されてしまう可能性があります。これを防ぐためには、不正な改行コードを使用できないメール送信専用のライブラリなどを使うようにすることが望ましいでしょう。	必須

項目		見出し		要件		備考	必須可否
				4.4.5	サーバ側のテンプレートエンジンを使用する際に、テンプレートの変更や作成に外部から受け渡される値を使用しないこと	サーバ側のテンプレートエンジンを使用してテンプレートを組み立てる際に不正なテンプレートの構文を挿入されることで、任意のコードを実行される可能性があります。 外部から渡される値をテンプレートの組み立てに使用せず、レンダリングを行う際のデータとして使用する必要があります。 また、レンダリング時にはクロスサイトスクリプティングの脆弱性が存在しないか確認してください。	必須
5	HTTPS	5.1	HTTPSについて	5.1.1	Webサイトを全てHTTPSで保護すること	適切にHTTPSを使うことで通信の盗聴・改ざん・なりすましから情報を守ることができます。次のような重要な情報を扱う画面や機能ではHTTPSで通信を行う必要があります。 ・入力フォームのある画面 ・入力フォームデータの送信先 ・重要情報が記載されている画面 ・セッションIDを送受信する画面 HTTPSの画面内で読み込む画像やスクリプトなどのコンテンツについてもHTTPSで保護する必要があります。	必須
				5.1.2	サーバー証明書はアクセス時に警告が出ないものを使用すること	HTTPSで提供されているWebサイトにアクセスした場合、Webブラウザから何らかの警告がでるということは、適切にHTTPSが運用されておらず盗聴・改ざん・なりすましから守られていません。適切なサーバー証明書を使用する必要があります。	必須
				5.1.3	TLS1.2以上のみを使用すること	SSL2.0／3.0、TLS1.0／1.1には脆弱性があるため、無効化する必要があります。使用する暗号スイートは、7.2.1を参照してください。	必須
				5.1.4	レスポンスヘッダーにStrict-Transport-Securityを指定すること	Hypertext Strict Transport Security(HSTS)を指定すると、ブラウザがHTTPSでアクセスするよう強制できます。	必須
6	cookie	6.1	cookieの属性について	6.1.1	Secure属性を付けること	Secure属性を付けることで、http://でのアクセスの際にはcookieを送出しないようにできます。特に認証状態に紐付けられたセッションIDを格納する場合には、Secure属性を付けることが必要です。	必須
				6.1.2	HttpOnly属性を付けること	HttpOnly属性を付けることで、クライアント側のスクリプトからcookieへのアクセスを制限することができます。	必須
				6.1.3	Domain属性を指定しないこと	セッションフィクセイションなどの攻撃に悪用されることがあるため、Domain属性は特に必要がない限り指定しないことが望ましいでしょう。	推奨
7	その他	7.1	エラーメッセージについて	7.1.1	エラーメッセージに詳細な内容を表示しないこと	ミドルウェアやデータベースのシステムが出力するエラーには、攻撃のヒントになる情報が含まれているため、エラーメッセージの詳細な内容はエラーログなどに出力するべきです。	必須

項目	見出し		要件		備考	必須可否
	7.2	暗号アルゴリズムについて	7.2.1	ハッシュ関数、暗号アルゴリズムは『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』に記載のものを使用すること	広く使われているハッシュ関数、疑似乱数生成系、暗号アルゴリズムの中には安全でないものもあります。安全なものを使用するためには、『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』や『TLS暗号設定ガイドライン』に記載されたものを使用する必要があります。	必須
	7.3	乱数について	7.3.1	鍵や秘密情報などに使用する乱数的性質を持つ値を必要とする場合には、暗号学的な強度を持った疑似乱数生成系を使用すること	鍵や秘密情報に予測可能な乱数を用いると、過去に生成した乱数値から生成する乱数値が予測される可能性があるため、ハッシュ関数などを用いて生成された暗号学的な強度を持った疑似乱数生成系を使用する必要があります。	必須
	7.4	基盤ソフトウェアについて	7.4.1	基盤ソフトウェアはアプリケーションの稼働年限以上のものを選定すること	脆弱性が発見された場合、修正プログラムを適用しないと悪用される可能性があります。そのため、言語やミドルウェア、ソフトウェアの部品などの基盤ソフトウェアは稼働期間またはサポート期間がアプリケーションの稼働期間以上のものを利用する必要があります。もしアプリケーションの稼働期間中に基盤ソフトウェアの保守期間が終了した場合、危険な脆弱性が残されたままになる可能性があります。	必須
			7.4.2	既知の脆弱性のないOSやミドルウェア、ライブラリやフレームワーク、パッケージなどのコンポーネントを使用すること	利用コンポーネントにOSSが含まれる場合は、SCA（ソフトウェアコンポジション解析）ツールを導入し、依存関係を包括的かつ正確に把握して対策が行えることが望ましいでしょう。	必須
	7.5	ログの記録について	7.5.1	重要な処理が行われたらログを記録すること	ログは、情報漏えいや不正アクセスなどが発生した際の検知や調査に役立つ可能性があります。認証やアカウント情報の変更などの重要な処理が実行された場合には、その処理の内容やクライアントのIPアドレスなどをログとして記録することが望ましいでしょう。ログに機微情報が含まれる場合にはログ自体の取り扱いにも注意が必要になります。	必須
	7.6	ユーザーへの通知について	7.6.1	重要な処理が行われたらユーザーに通知すること	重要な処理（パスワードの変更など、ユーザーにとって重要で取り消しが困難な処理）が行われたことをユーザーに通知することによって異常を早期に発見できる可能性があります。	推奨
	7.7	Access-Control-Allow-Originヘッダーについて	7.7.1	Access-Control-Allow-Originヘッダーを指定する場合は、動的に生成せず固定値を使用すること	クロスオリジンでXMLHttpRequest (XHR)を使う場合のみこのヘッダーが必要です。不要な場合は指定する必要はありませんし、指定する場合も特定のオリジンのみを指定する事が望ましいです。	必須
	7.8	クリックジャッキング対策について	7.8.1	レスポンスヘッダーにX-Frame-OptionsとContent-Security-Policyヘッダーのframe-ancestors ディレクティブを指定すること	クリックジャッキング攻撃に悪用されることがあるため、X-Frame-Optionsヘッダーフィールドに DENY または SAMEORIGIN を指定する必要があります。 Content-Security-Policyヘッダーフィールドに frame-ancestors 'none' または 'self' を指定する必要があります。 X-Frame-Options ヘッダーは主要ブラウザーでサポートされていますが標準化されていません。CSP レベル 2 仕様で frame-ancestors ディレクティブが策定され、X-Frame-Options は非推奨とされました。	必須

項目		見出し		要件		備考	必須可否
		7.9	キャッシュ制御について	7.9.1	個人情報や機微情報を表示するページがキャッシュされないよう Cache-Control: no-store を指定すること	個人情報や機密情報が含まれたページはCDNやロードバランサー、ブラウザなどのキャッシュに残ってしまうことで、権限のないユーザーが閲覧してしまう可能性があるためキャッシュ制御を適切に行う必要があります。	必須
		7.10	ブラウザのセキュリティ設定について	7.10.1	ユーザーに対して、ブラウザのセキュリティ設定の変更をさせるような指示をしないこと	ユーザーのWebブラウザのセキュリティ設定などを変更した場合や、認証局の証明書をインストールさせる操作は、他のサイトにも影響します。	必須
		7.11	ブラウザのセキュリティ警告について	7.11.1	ユーザーに対して、ブラウザの出すセキュリティ警告を無視させるような指示をしないこと	ブラウザの出す警告を通常利用においても無視させるよう指示をしていると、悪意のあるサイトで同様の指示をされた場合もそのような操作をしてしまう可能性が高まります。	必須
		7.12	WebSocketについて	7.12.1	Originヘッダーの値が正しいリクエスト送信元であることが確認できた場合にのみ処理を実施すること	WebSocketにはSOP (Same Origin Policy)という仕組みが存在しないため、Cross-Site WebSocket Hijacking(CSWSH)対策のためにOriginヘッダーを確認する必要があります。	必須
		7.13	HTMLについて	7.13.1	html開始タグの前に<!DOCTYPE html>を宣言すること	DOCTYPEで文書タイプをHTMLと明示的に宣言することでCSSなど別フォーマットとして解釈されることを防ぎます。	必須
				7.13.2	CSSファイルやJavaScriptファイルをlinkタグで指定する場合は、絶対パスを使用すること	linkタグを使用してCSSファイルやJavaScriptファイルを相対パス指定した場合にRPO (Relative Path Overwrite) が起きる可能性があります。	必須
8	提出物	8.1	提出物について	8.1.1	サイトマップを用意すること	認証や再認証、CSRF対策が必要な箇所、アクセス制御が必要なデータを明確にするためには、Webサイト全体の構成を把握し、扱うデータを把握する必要があります。そのためには上記の資料を用意することが望ましいでしょう。	必須
				8.1.2	画面遷移図を用意すること		必須
				8.1.3	アクセス権限一覧表を用意すること	誰にどの機能の利用を許可するかまとめた一覧表を作成することが望ましいでしょう。	必須
				8.1.4	コンポーネント一覧を用意すること	依存しているライブラリやフレームワーク、パッケージなどのコンポーネントに脆弱性が存在する場合がありますので、依存しているコンポーネントを把握しておく必要があります。	推奨
				8.1.5	上記のセキュリティ要件についてテストした結果報告書を用意すること	自社で脆弱性診断を実施する場合には「脆弱性診断士スキルマッププロジェクト」が公開している「Webアプリケーション脆弱性診断ガイドライン」などを参照してください。	推奨

（別紙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

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

Ⅲ　業務の実施における情報セキュリティの確保

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

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

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

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

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

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

（６）本業務における情報セキュリティ対策の履行状況を定期的に報告すること。

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

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

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

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

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

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

４　受託者は、本業務において取り扱われた情報を、担当部署の指示に従い、本業務上不要

となったとき若しくは本業務の終了までに返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

Ⅳ　情報システムの各工程における情報セキュリティの確保

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

（１）情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

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

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

（ア）農林水産省外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能

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

（ウ）農林水産省内通信回線への端末の接続を監視する機能

（エ）端末への外部電磁的記録媒体の挿入を監視する機能

（オ）サーバ装置等の機器の動作を監視する機能

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

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

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

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

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

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

（１）情報システムのセキュリティ要件の適切な実装

ア　主体認証機能

イ　アクセス制御機能

ウ　権限管理機能

エ　識別コード・主体認証情報の付与管理

オ　ログの取得・管理

カ　暗号化機能・電子署名機能
キ　暗号化・電子署名に係る管理
ク　ソフトウェアに関する脆（ぜい）弱性等対策
ケ　不正プログラム対策
コ　サービス不能攻撃対策
サ　標的型攻撃対策
シ　アプリケーション・コンテンツのセキュリティ要件の策定
ス　政府ドメイン名（go.jp）の使用
セ　不正なウェブサイトへの誘導防止
ソ　農林水産省外のアプリケーション・コンテンツの告知

（２）情報セキュリティの観点に基づく試験の実施

ア　ソフトウェアの開発及び試験を行う場合は、運用中の情報システムと分離して実施すること。
イ　試験項目及び試験方法を定め、これに基づいて試験を実施すること。
ウ　試験の実施記録を作成し保存すること。

（３）情報システムの開発環境及び開発工程における情報セキュリティ対策

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

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

４　受託者は、本業務において情報システムの運用・保守を行う場合には、情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。

（１）情報システムの運用環境に課せられるべき条件の整備
（２）情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
（３）情報システムの保守における情報セキュリティ対策
（４）運用中の情報システムに脆（ぜい）弱性が存在することが判明した場合の情報セキュリティ対策
（５）利用するソフトウェアのサポート期限等の定期的な情報収集及び報告
（６）「デジタル・ガバメント推進標準ガイドライン」(デジタル社会推進会議幹事会決定。最終改定：2023 年 3 月 31 日)の「別紙3　調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」に基づく情報資産管理を行うために必要な事項を記載した情

報資産管理標準シートの提出。

（7）情報システムの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポート継続中のバージョンでの動作検証及び当該バージョンで正常に動作させるための情報システムの改修等

5　受託者は、本業務において情報システムの運用・保守を行う場合には、運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。

（1）情報セキュリティに関わる運用保守体制の整備

（2）運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

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

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

（1）監視するイベントの種類

（2）監視体制

（3）監視状況の報告手順

（4）情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順

（5）監視運用における情報の取扱い（機密性の確保）

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

8　受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する府省庁等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

9　受託者は、本業務において情報システムの運用・保守を行う場合には、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

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

（1）情報システム更改時の情報の移行作業における情報セキュリティ対策

（2）情報システム廃棄時の不要な情報の抹消

Ⅴ　クラウドサービス等外部サービスに関する情報セキュリティの確保

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

１　外部サービス条件

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

（２）外部サービスの契約に定める準拠法が国内法のみであること。

（３）クラウドサービスの場合、ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

２　ISMAP クラウドサービスリストに登録されているクラウドサービスであること。

３　ISMAP クラウドサービスリストに登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（３桁の番号で表現される項目）及び末尾にBが付された詳細管理策（４桁の番号で表現される項目）を原則として全て満たしていること。

４　クラウドサービス以外の外部サービスの場合は、以下の措置を講じること。

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

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

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

（４）情報セキュリティインシデントへの対処方法を確立していること。

（５）情報セキュリティ対策その他の契約の履行状況を確認できること。

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

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

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

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

Ⅶ　機器等に関する情報セキュリティの確保

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

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

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

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

４　利用マニュアル・ガイダンスが適切に整備された機器等を採用すること。

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

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

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

８　機器等の納品時に、以下の事項を書面で報告すること。

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

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

Ⅷ　管轄裁判所及び準拠法

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

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

Ⅸ　業務の再委託における情報セキュリティの確保

１　受託者は、本業務の一部を再委託（再委託先の事業者が受託した事業の一部を別の事業

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

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

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

Ⅹ　資料等の提出

上記Ⅱの１、Ⅱの２、Ⅲの１、Ⅴの４（２）、４（３）、Ⅶの１及びⅦの６において提出することとしている資料等については、最低価格落札方式にあっては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式にあっては提案書等の総合評価のための書類に添付して提出すること。

Ⅺ　変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ、Ⅶ及びⅨに関して、農林水産省に提示した内容を変更しようとする場合には、変更する事項、理由等を記載した申請書を提出し、農林水産省の許可を得ること。

【別紙３】

合法伐採木材等の流通及び利用の促進に関する法律の一部を改正する法律の概要

令和５年5月8日
公布

１．背景

○ 違法伐採及び違法伐採に係る木材の流通は、**森林の有する多面的機能に影響を及ぼすおそれ**があるとともに、**木材市場における公正な取引を害するおそれ。**

○ 現行制度は、①事業者に**合法伐採木材等の利用の努力義務**を課すとともに、②**合法性の確認等を確実に行う木材関連事業者を第三者機関が登録**すること等により、合法伐採木材等の流通及び利用を促進。

○ しかしながら、登録木材関連事業者により合法性が確認された木材量は、我が国の木材総需要量の約４割等の状況。

○ G7関連会合やAPEC林業担当大臣会合等で違法伐採の根絶に向けた取組が課題として取り上げられるなど、**更なる取組の強化**が必要。

２．法律の概要

（1）川上・水際の木材関連事業者による合法性の確認等の義務付け

○ 国内市場における木材流通の最初の段階での対応が重要であることから、**川上・水際の木材関連事業者に対し、**素材生産販売事業者又は外国の木材輸出事業者から木材等の譲受け等をする場合に、**①原材料情報の収集、合法性の確認**、**②記録の作成・保存**、**③情報の伝達**を**義務付け**（第６条～第８条）。

（2）素材生産販売事業者による情報提供の義務付け

○ （１）で義務付けられる合法性の確認等が円滑に行われるよう、**素材生産販売事業者に対し**、当該木材関連事業者からの求めに応じ、**伐採届等の情報提供を行う**ことを**義務付け**（第９条）。

（3）小売事業者の木材関連事業者への追加

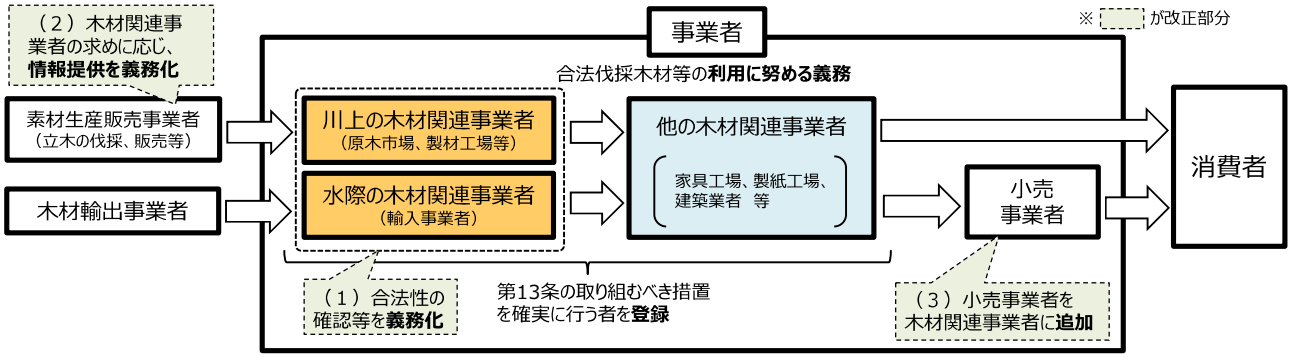
○ 合法性の確認等の情報が消費者まで伝わるよう、**小売事業者を木材関連事業者に追加**し、登録を受けることができるよう措置（第２条第４項）。

（4）その他の措置

○ （１）及び（２）に関し、主務大臣による**指導・助言、勧告、公表、命令、命令違反の場合の罰則**等を措置（第10条、第11条、第45条等）。

○ 木材関連事業者が（１）のほか、**合法伐採木材等の利用を確保するために取り組むべき措置**として、**違法伐採に係る木材等を利用しないようにするための措置**等を明確化（第13条）。

○ 一定規模以上の川上・水際の木材関連事業者に対する**定期報告の義務付け**、**関係行政機関の長等に対する協力要請**を措置（第12条、第41条）。



３．施行期日

令和７年４月１日

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				