令和8年度

流通木材の合法性確認システムに係る

運用・保守及びクラウドサービス提供業務

調達仕様書

林野庁　林政部　木材利用課

目次

Ⅰ．調達案件の概要

（Ⅰ）調達件名

令和８年度　流通木材の合法性確認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

（２）調達の背景

林野庁 林政部 木材利用課（以下「担当部署」という。）では、「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」（令和５年５月８日 公布、令和７年４月１日施行）（以下「改正 CW 法」という。）に基づき、流通木材の合法性確認に係る業務の効率化と改正法施行後の新たな事業者負担の低減に資することを目的として、合法性確認のデジタル化に向けた「流通木材の合法性確認システム」（以下「本システム」という。）を令和６年度に構築し、改正 CW 法の施行とあわせ令和７年４月に稼働を開始した。本システムは、合法性確認に係る大規模企業から小規模・零細企業まで多様な事業者が多層的に関わることになり、改正 CW 法に基づく木材流通過程における共通基盤となるシステムに位置づけられている。

本システムの稼働後、システム利用者に対し安定したシステムの運用稼働を提供するべく令和８年度における本システムの運用・保守作業及び付帯する業務を調達するものである。

（３）調達目的及び調達の期待する効果

本調達は、令和８年度における本システムの円滑な運用の確保及び利用者への支援を行うことを目的とする。

（４）業務・情報システムの概要

本システムの概要は次のとおりである。

ア．本システム

（ア）対象業務（参考：別紙Ⅰ「改正CW法概要」及び林野庁HP「クリーンウッド・ナビ」[1]）

①改正 CW 法に基づく木材等の原材料情報の収集、合法性の確認、記録の作成・保存、情報の伝達、定期・年度報告に係る業務。

対象となる利用者：国内の素材生産販売事業者、木材関連事業者

②提出された報告書の閲覧、ダウンロード

対象となる利用者：登録実施機関、経済産業省、林野庁

---

[1] 林野庁HP「クリーンウッド・ナビ」
https://www.rinya.maff.go.jp/j/riyou/goho/index.html
https://www.rinya.maff.go.jp/j/riyou/goho/brochure/pdf/brochure-r7-09.pdf

（イ）システムの概要

本システムの利用者は、木材等の流通と併行し、合法性の確認に係る情報や書類をシステムに登録し、記録を作成、必要な情報を納品先へ伝達する。本システムの利用は任意であることから、サプライチェーンにおいて最初にシステムを利用する者が情報を登録し、以降の利用者は、その確認と納品先への情報伝達を繰り返す。

また、合法性確認のために収集・登録した情報に加え、取引情報（製品の納品情報）や関連書類等も本システムに登録できる。さらに本システムに登録したデータをもとに自動集計機能で国や登録実施機関への定期・年度報告の事務簡略化を図る。

本システムの業務範囲およびシステムの概要は図 1，2 のとおりである。

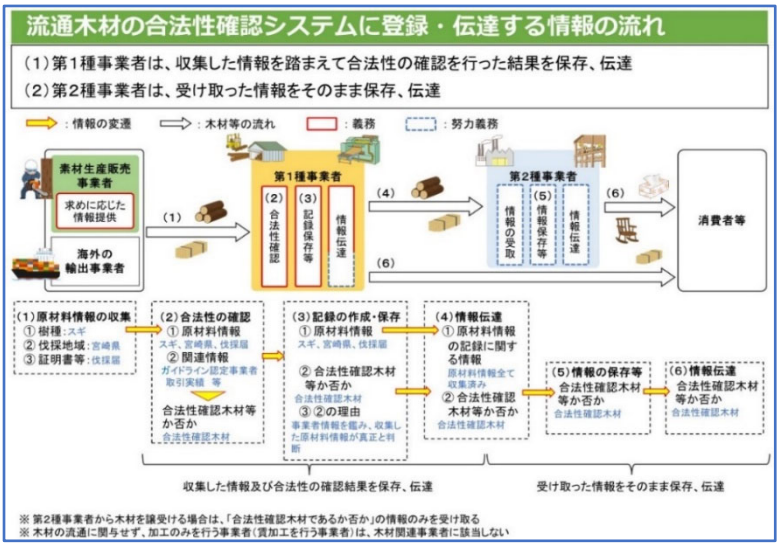


図 1　流通木材の合法性確認システムの業務範囲

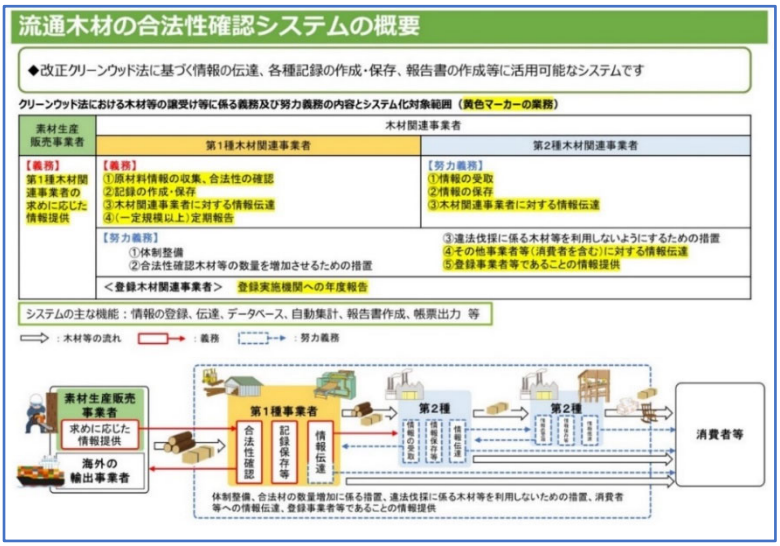


図 2　流通木材の合法性確認システムの概要

イ．本システムにおいて利用する情報システム

（ア）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。

プラットフォームとなる MAFF クラウドの取組及び構成については図 3 のとおりである。

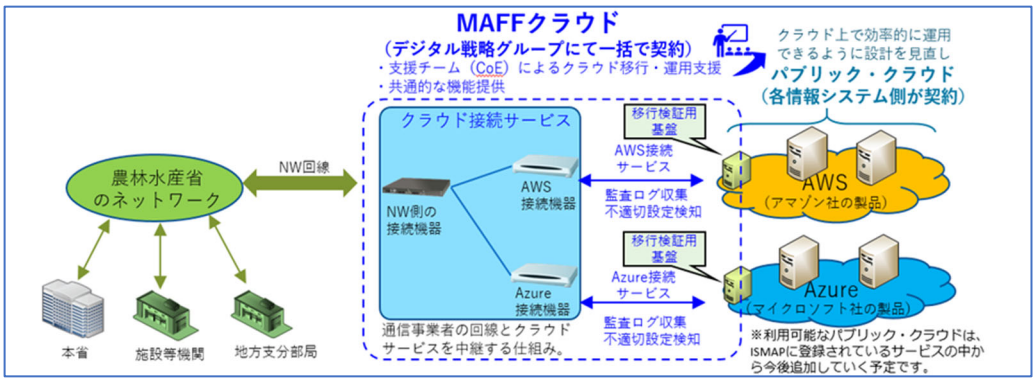
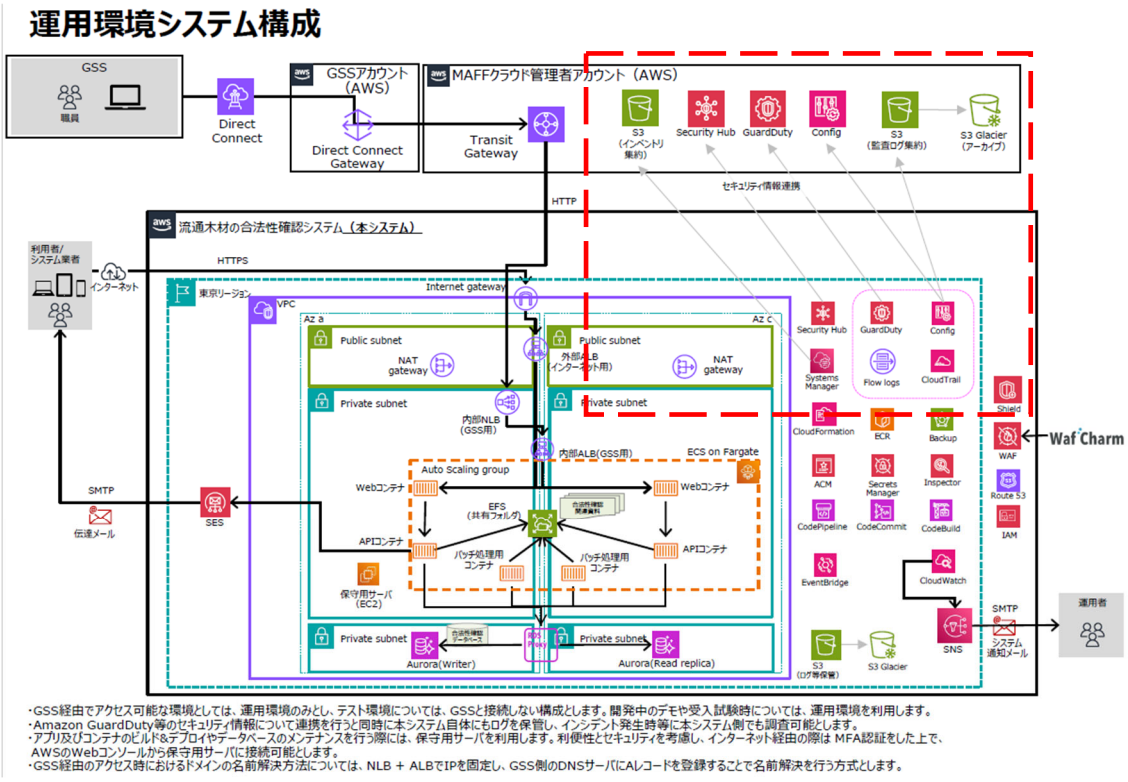


図3　MAFF クラウドの概要

（イ）MAFF クラウド連携に関わるシステム構成図



：MAFF クラウド連携に関わるサービス

図4　運用環境システム構成図

テスト環境システム構成

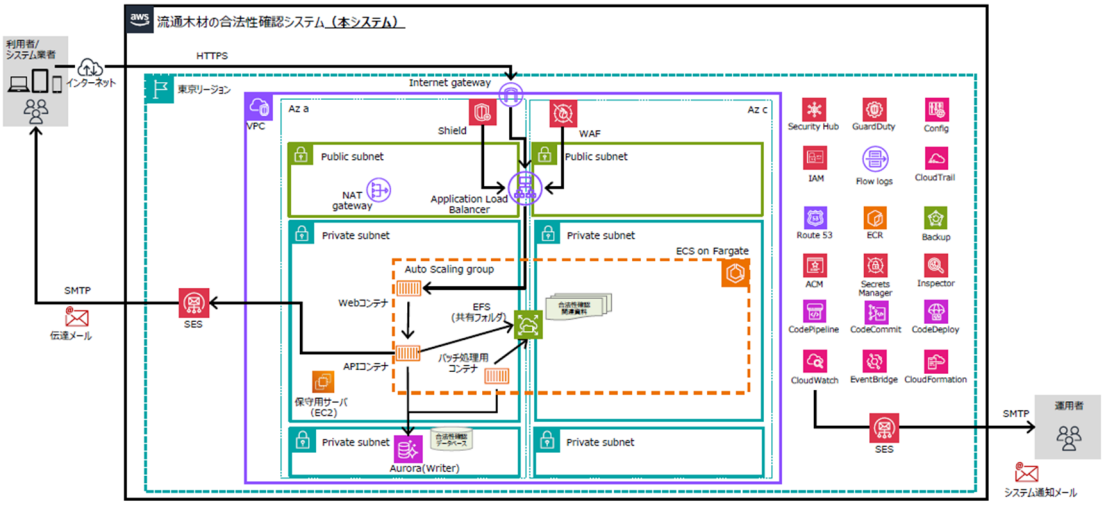


図5　テスト環境システム構成図

ウ．その他システム関連情報

（ア）使用サービス名一覧

① ACM
② Aurora
③ Backup
④ CloudFormation
⑤ CloudTrail
⑥ CloudWatch
⑦ CodeBuild
⑧ CodeCommit
⑨ CodePipeline
⑩ Config
⑪ EC2
⑫ ECR
⑬ ECS on Fargate
⑭ EFS
⑮ EventBridge
⑯ Flow logs

⑰ GuardDuty
⑱ Inspector
⑲ Internet gateway
⑳ NAT gateway
㉑ RDS Proxy
㉒ Route 53
㉓ S3
㉔ S3 Glacier
㉕ Secrets Manager
㉖ Security Hub
㉗ SES
㉘ Shield
㉙ SNS
㉚ Systems Manager
㉛ VPC
㉜ WAF
㉝ 外部 ALB
㉞ 内部 NLB
㉟ IAM

（イ）フレームワーク名称、ソースコード行数

①フロントエンド

開発言語：TypeScript

フレームワーク名称：Angular

想定ステップ数：37.1kstep

②バックエンド

開発言語：PHP

フレームワーク名称：Laravel

想定ステップ数：12.8kstep

※想定総ステップ数（フロントエンド＋バックエンド）：49.9kstep

（５）契約期間

令和８年４月１日から令和９年３月31日まで

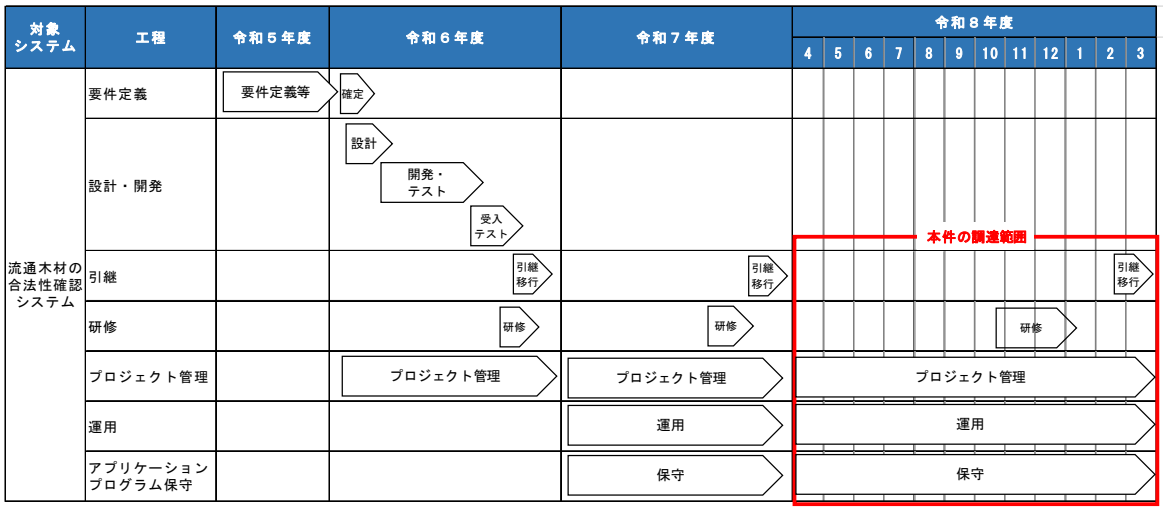


図6　対象契約期間

（６）作業スケジュール

受注者は、後述「４　作業の実施内容」に基づいて作業を実施する。当内容については、別途、担当部署と協議、確定することとする。

■作業項目

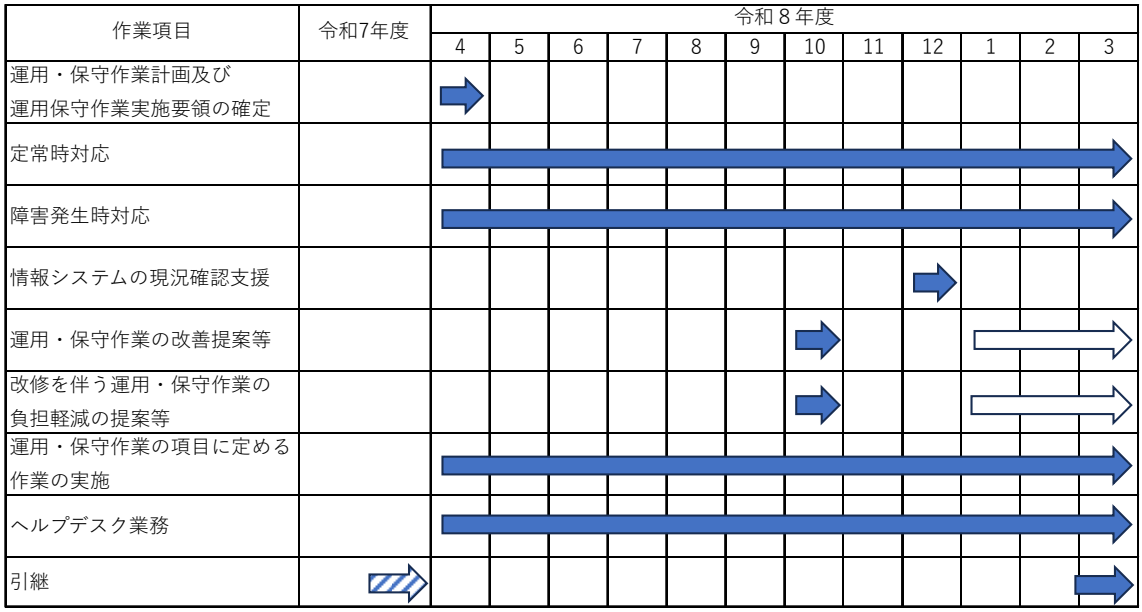


図7　作業スケジュール

表 1 作業スケジュール

実施時期	作業内容	「4 作業の実施内容」の項番
定常時対応		(3)
日次	定常時運用業務（システム操作、運転管理・監視、稼動状況監視、ヘルプデスク提供、定期点検、不具合受付等）	ア
月次	運用・保守作業報告書の取りまとめ	イ
適宜	ソフトウェア保守におけるソフトウェア製品の構成変更時対応	ウ
適宜	ソフトウェアのセキュリティぜい弱性対応	エ
適宜	パッチのリリース管理	オ
適宜	運用・保守作業におけるシステム改善対応	カ
適宜	運用・保守作業におけるプログラム修正時対応	キ
適宜	運用・保守実績の未達部分結果分析	ク
月次	定期運用・保守会議を開催	ケ
適宜	情報システム運用継続計画の作成又は更新支援	コ
適宜	設計書等の更新版の提出	サ
適宜	リモートアクセス時のマネージドサービスの利用	シ
適宜	農林水産省クラウド利用ガイドライン別紙 I_共通機能_利用申請書の内容変更時対応	ス
適宜	インベントリ情報収集のための設定作業	セ
適宜	利用者への研修教育の実施	ソ
適宜	セキュリティ管理	タ

障害発生対応		(4)
発生時	障害発生時運用業務（障害検知、障害発生箇所の切り分け、関係する事業者への連絡、復旧確認、報告等）及び障害発生時保守作業（原因調査、応急措置、報告等）	ア、イ、ウ
年１回	事前訓練	エ
情報システムの現況確認支援		(5)
年１回	情報資産管理データと情報システムの現況との突合・確認の支援	ア、イ、ウ、エ
適宜	本システムで利用しているソフトウェア情報の提供	オ
適宜	クラウドサービスを含めた情報システムの構成を適切に見直すための資料提供	カ
運用・保守作業の改善提案		(6)
年１回	改善提案、年間の運用・保守実績の取りまとめ	ア
適宜	運用・保守作業計画、運用・保守作業実施要領に対する報告及び改善提案	ア、イ、ウ、エ、オ、キ
月次	クラウドサービス利用実績提供	カ
改修を伴う運用・保守作業の負担低減提案		(7)
適宜	システム改修により運用・保守作業の負担軽減が見込める提案	
運用・保守作業項目に定める作業の実施		(8)
適宜	「運用・保守作業計画」、「運用・保守作業実施要領」に定める作業	
サーバー証明書の調達・更新		(9)
適宜	サーバー証明書の調達・更新の実施	
ヘルプデスク業務		(10)
日次	システム利用者である木材関連事業者等及び林野庁職員からの問い合わせに対応するヘルプデスク業務	

引継		（I1）
契約開始前	前年度の運用・保守業者からの引継	ア
契約終了時	（他の事業者が本システムの運用・保守を受注した場合）他の事業者（次期システム運用・保守事業者）への引継	イ、ウ
業務の完了		（I2）
すべての業務完了時	業務の完了報告	
定例会等の実施		（I3）
契約後10日以内	キックオフ会議の開催と議事録作成	ア
月1回	業務の進捗状況報告の定例会と議事録作成	イ、エ
適宜	定例会以外の会議開催と議事録作成	ウ、エ
契約金額内訳及び情報資産管理標準シートの提出		（I4）
契約締結後	契約金額内訳を記載したエクセル電子データの提出	ア
適宜	情報資産管理標準シートの提出	イ

定常作業含め作業内容の年間のスケジュールについても、担当部署と協議、確定することとする。

２．調達案件及び関連調達案件

（１）調達範囲

本調達では、MAFF クラウドでの本システムの運用・保守業務及び利用者への支援を行うものとする。契約締結から速やかに、令和７年度の本システム運用・保守事業者と調整の上、引継業務を行うものとする。

本調達にパブリッククラウドにおけるクラウドサービスの提供業務も含めることとする。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。また、本システムの調達対象としては、本番運用環境だけでなく、テスト環境を含むものとする。なお、このテスト環境は MAFF クラウドと連携するものではない。CI/CD については、テスト環境で確認したのち、本番環境にリリースする運用を想定している。

（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、実施時期等は表２のとおりである。

表 2 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	「クリーンウッド」利用推進事業のうち流通木材の合法性確認システム構築事業（要件定義書案の作成）	随意契約 （企画競争）	令和４年３月18日 変更契約： 令和４年３月30日	契約済み	令和４年３月から 令和５年３月まで
2	「クリーンウッド」利用推進事業のうち木材流通における情報伝達状況調査	随意契約 （企画競争）	令和５年５月24日	契約済み	令和５年５月から 令和５年12月まで
3	流通木材の合法性確認システム整備の設計・開発	一般競争入札 （総合評価）	令和６年４月16日	契約済み	令和６年４月から 令和７年３月まで
4	流通木材の合法性確認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 （最低価格）	令和７年４月１日	契約済み	令和７年４月から 令和８年３月まで
5	【本調達】流通木材の合法性確認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 （最低価格）	令和８年４月１日 ※１	意見招請なし 令和７年12月頃 令和８年２月頃	令和８年4月から 令和９年3月まで

※1：仮日程

（３）調達案件間の入札制限

現時点で本調達と、前項記載の調達案件間の入札制限はない。その他、詳細については「8（5）入札制限」も参照すること。

３．情報システムに求める要件

本業務の実施に当たっては、担当部署と協議、確定の上作成する「運用・保守作業計画」及び「運用・保守作業実施要領」の各要件を満たすこと。

４．作業の実施内容

作業の実施内容は、次の各号のとおりである。また、現行システムの構成等については、令和７年度の本システム運用・保守事業者から引き継がれた資料を基に「運用・保守作業計画」、「運用・保守作業実施要領」および「インフラ基盤設計書、システム構成図、ソフトウェア」を含めた「システム構成図」として作成する。

（１）運用・保守の前提

ア．受注者は、令和７年度の本システム運用・保守事業者からパブリッククラウド上に構築された情報システムの引継を受け、アカウントの契約の移管を行い、環境を維持すること。

イ．受注者は、構成管理及びパッチの適用について自動化すること。なお、自動化とは、対象を選定し、タイミングをコントロールして適用することをいう。

ウ．受注者は、原則、メンテナンスの際にクラウドサービスプロバイダーのサービス（AWS の場合、AWS Systems Manager Session Manager・AWS Systems Manager Fleet Manager）を利用すること。

エ．受注者は、ソフトウェアの情報をクラウドサービスの機能（AWS の場合、ASM（AWS Systems Manager））を利用して自動取得すること。

オ．農林水産省をエンドカスタマー（エンドユーザー）として登録していることを証明する書面を提出すること。

カ．運用時間帯の前提・制約については以下のとおりとする。

（ア）システム稼働時間：24 時間、365 日

（障害対応を行う時間帯：平日（農林水産省開庁日）8:30～18:30）

（イ）ヘルプデスク運営時間：平日（農林水産省開庁日）9:00～18:00

キ．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

（ア）地震、火災、風水害等、攻撃等による直接的な基盤の損壊

（イ）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

（ウ）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

ク．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。

（ア）障害発生時：24 時間[注 1]

（イ）業務停止時：24 時間[注 2]

（ウ）大規模災害時：1 週間[注 3]

[注 1]「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 2]「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 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「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

（２）運用・保守作業計画及び運用・保守作業実施要領の確定作業支援

受注者は、「運用・保守作業計画（案） 及び運用・保守作業実施要領（案)」を作成する。それに基づき、担当部署が運用・保守作業計画及び運用・保守作業実施要領を確定するために要する支援を行うこと。支援に当たり、担当部署と具体的な作業内容や実施時間、実施サイクル等に関し確認を行うこと。運用・保守作業計画及び運用・保守作業実施要領を必要に応じ更新し、契約締結後 10 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 担当部署に提出、承認を受けること。

なお、運用・保守作業計画及び運用・保守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」（令和６年５月 31 日デジタル社会推進会議幹事会決定。以下「標準ガイドライン」という。)「第９章　運用及び保守」で定義されている事項を踏まえたものとする。

（３）定常時対応

ア．受注者は、定常時運用業務（システム操作、運転管理・監視、稼動状況監視、ヘルプデスク提供、定期点検、不具合受付等）を行うこと。具体的な実施内容・手順は担当部署が定める運用・保守作業計画に基づいて行うこと。主な監視対象としては、CPU 使用率と CPU queue とプロセス情報、Apache のログを用いたレスポンス

タイムの監視を行う。これらを同一の時間軸でログ管理を行うことでリソース不足が発生した際に、深堀して分析ができるようにすること。

イ．受注者は、運用業務の内容や工数などの作業実績、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（情報セキュリティ監視状況、情報システムのぜい弱性への対応状況を含む。）、情報システムの利用者への研修を含めたサポート、受注者内教育・訓練状況、リスク・課題の把握・対応状況について月次で運用・保守作業報告書を取りまとめ、担当部署に報告、承認を得ること。

ウ．受注者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、担当部署にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること。また、自動取得したソフトウェアの情報を把握し、担当部署の求めに応じて最新の構成情報の出力結果を提出すること。

エ．ソフトウェアにセキュリティのぜい弱性が見つかった場合は、受注者は対応策について計画し、担当部署の承認を得た上で対応すること。

オ．受注者は、パッチの自動適用を用いて、検証環境や品質保証環境などを用いてパッチベースラインを検証し、その後に本番環境にパッチを適用するなど、パッチのリリース管理を行うこと。なお、パッチ適用に起因する不具合が出た際に行う切り戻しやアプリケーション修正などの対応を予め計画すること。

カ．受注者は、画面の操作性や分かり易さ等の改善の要望が生じた際、担当部署と検討を行い、軽微なプログラム修正で改善可能と判断された場合、対応を行うものとする。

キ．受注者は、保守作業でプログラムの修正を行った場合、設計書等の更新を行い、テストを行った上で本番環境へ適用すること。改修の際に作成、更新した資料は、担当部署へ提出すること。

ク．受注者は、月間の運用・保守実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。

ケ．受注者は、別途定めたSLAに基づいた運用・保守作業報告書の内容について、月例の定期運用・保守会議を開催し、その内容を報告すること。なお、SLAの内容と乖離がある場合は、その原因分析と対応策、解決予定日を報告すること。

コ．受注者は、担当部署が、情報システム運用継続計画を作成又は更新するにあたり、情報提供等の支援を行うこと。

サ．受注者は、インフラの設定変更があった場合は設計書等の更新版（パラメータシート含む）を、担当部署に提出すること。

シ．受注者は、本システムへのリモートアクセスを行う際、原則として安全にリモートアクセスを行うことができるマネージドサービス（AWSの場合、AWS Systems Manager Session Manager・AWS Systems Manager Fleet Manager）を利用するこ

と。

ス.受注者は、「農林水産省クラウド利用ガイドライン別紙 I_共通機能_利用申請書」の内容（システム構成を含む）に変更がある場合、資料を更新し、担当部署と MAFF クラウド CoE の確認を受けること。

セ．受注者は、インベントリ情報を収集するため、設定作業（AWS の場合、Systems Manager Inventory と EC2 の設定）を実施すること。なお、インベントリ収集機能はコンテナの構成管理に対応していないため、コンテナを利用しているシステムは、MAFF クラウド利用ガイドラインの記載を参考に、脆弱性対策を実施すること。

ソ．受注者は年に一回程度、利用者への教育研修を実施する。実施内容やスケジュールを受注者が検討し、「教育研修計画」を作成して予め担当部署の承認を得て研修を実施すること。

タ．受注者はセキュリティ管理として、（AWS の場合 SecurityHub）が発報したセキュリティアラートについて、対応ならびに無効化／抑制を検討するものとする。なお、新たなルールの追加について、迅速に対応するものとする。

（４）障害発生時対応

ア．受注者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに担当部署に報告するとともに、その緊急度及び影響度を判断の上、担当部署と別途検討・確定のうえ作成する「運用・保守作業計画」および「運用・保守作業実施要領」に盛り込む障害発生時運用業務（障害検知、障害発生箇所の切り分け、関係する事業者への連絡、復旧確認、報告等）の保守要件として障害発生時保守作業（原因調査、応急措置、報告等）を行うこと。

イ．障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は担当部署と別途検討・確定のうえ作成する「運用・保守作業計画」および「運用・保守作業実施要領」に基づいて行うこと。

ウ．受注者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案すること。

エ．受注者は、災害等の発生時には、担当部署の指示を受けて、情報システム運用継続計画に基づく運用業務を実施すること。なお、災害等の発生に備え、最低年 I 回（II 月を予定）は事前訓練を実施すること。

オ．受注者は、生成 AI を活用しているシステムにおいて、生成 AI システムのアウトプットが期待する品質を満たさなくなった場合、そこから生じる被害を最小限に食い止め、原因を特定し、改善措置を講じること。

（５）情報システムの現況確認支援

ア．受注者は、年１回（年度下期中を予定）、担当部署の指示に基づき、情報資産管理データと情報システムの現況との突合・確認（以下「現況確認」という。）を支援すること。なお、MAFF クラウドを利用している場合、MAFF クラウドから提供されるインベントリ情報を活用することで、現況との突合確認は省略することも可とするが、インベントリ情報から収集できない製品が含まれる場合は、当該製品の構成情報の取得を行うこと。

イ．受注者は、現況確認の結果、情報資産管理データと情報システムの現況との間の差異がみられる場合は、運用・保守作業実施要領に定める変更管理方法に従い、差異を解消すること。

ウ．受注者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上、担当部署に報告すること。

エ．受注者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査の上、担当部署に報告すること。

オ．受注者は、担当部署の求めに応じ、本システムで利用しているソフトウェアの情報を提供すること。情報の取得に際しては、クラウドサービスの機能(AWS の場合、SSM（AWS Systems Manager)）を利用して取得し、その出力結果を提供すること。

カ．受注者は、担当部署の求めに応じクラウドサービスを含めた情報システムの構成を適切に見直すための資料（AWS Cost Explorer、AWS Trusted Advisor、AWS CUR 等の出力結果）を提出すること。

（６）運用・保守作業の改善提案

ア．受注者は、年度末までに年間の運用・保守実績を取りまとめること。また、担当部署の求めに応じ、年１回程度（10 月頃を予定）運用・保守作業計画、運用・保守作業実施要領に対する報告及び改善提案を行い、担当部署の承認を得ること。

イ．担当部署は、受注者から受けた報告及び改善提案を PMO、MAFF クラウド CoE へ報告し、必要な助言、指導等を受ける。この際、受注者は担当部署の求めに応じ、PMO、MAFF クラウド CoE への報告に参加すること。

ウ．改善提案のうち、パブリッククラウドの運用体制については、自社による運用・保守の改善の他、MSP サービスの活用についても検討し提案すること。改善提案に当たっては、パブリッククラウドの運用体制において、マネージドサービスプロバイダーが提供している共有型のクラウド運用・保守サービスの活用についても検討し整理することとする。

検討した結果、MSP サービスの活用を運用・保守作業計画に組み込めた場合は、実際にサービス等の活用を開始すること。

エ．改善提案には、クラウドサービスプロバイダーが提供するベストプラクティス準

拠状況(AWS：Trusted Advisor)及び、検出項目の対応可否を含めること。

オ．改善提案には、システムが適切に運用されているか確認した結果及び改善点を含めること。確認にはクラウド構成のベストプラクティス（AWS：AWS Well-Architected フレームワークの全ての柱）を活用し、年に一度システムが適切に運用されているかチェックし、次年度の改善点を整理すること。

カ．受注者はクラウドサービス利用明細書の写し及び月額の運用サービスの費用実績（MSP サービスを利用した場合）を一覧表にとりまとめ、月次の運用・保守作業報告書の取りまとめに合わせて担当部署に提出すること。また、担当部署の求めに応じ、クラウドサービスを含めた情報システムの構成を適切に見直すための資料（AWS Cost Explorer、AWS Trusted Advisor、AWS CUR 等の出力結果）を提出すること。なお、運用サービスの共通化とは、以下の取り組みとする。

（ア）受注者が自社で MSP サービスを提供している企業の場合はそれを利用すること。

（イ）受注者が自社で MSP サービスを提供していない企業は、運用品質の均一化と不要なコストを削減するために

①外部企業が提供する MSP サービスを利用すること

又は

②複数の運用案件を受注することで、自社内で運用サービス（サービスデスク、監視サービス等）の Shared service（シェアードサービス）に取り組み、費用を逓減すること。

クラウド利用料について、提出した実績を踏まえ、当該年度の９月末までに次年度の利用内容及び契約予定額を担当部署と協議する。また、クラウド利用料等の実績より、クラウドサービスの稼働状況やコストの遷移から、見積の作成、不要リソースの削除検討を行うものとする。

改善提案を作成したら担当部署ならびに PMO/MAFF クラウド CoE に報告すること。

キ．担当部署は改善提案を受けて、本業務の実施内容を変更しようとする場合は「１０（Ⅰ）ウ」の協議を行うものとする。

（７）改修を伴う運用・保守作業の負担低減提案

受注者は、前項以外に、本システムを一部改修することにより運用・保守作業低減が見込まれる場合、その改修に係る工数と低減が見込める工数を明らかにして改修の提案を「４．（６）」の改善提案と合わせて行うこと。

（８）運用・保守作業項目に定める作業の実施

受注者は、令和７年度の本システム運用・保守事業者から引き継がれた資料・情報を基に作成し担当部署と確認した「運用・保守作業計画」、「運用・保守作業実施要領」に

定める作業を行うこと。

（９）サーバー証明書の調達及び更新

受注者は本システムの運用に必要なサーバー証明書を調達し、必要に応じて更新の手続きを行うこと。なお、これらに要する費用は受注者の負担とする。

（10）ヘルプデスク業務

受注者は、運用手順書に定めるユーザー(一部職員を含む木材関連事業者)からの問い合わせに対応するヘルプデスク業務を行うこと。ヘルプデスク業務では電話受付（平日(農林水産省開庁日) 9:00～18:00、緊急対応が必要な場合は適宜対応）及びメールでの対応を可能とすること。IP 電話の利用を認める。ただし、当該電話は利用者が契約している電話料金で通話が可能なプランを利用して開設することとし、いわゆるナビダイヤルは認めない。受け付けた問い合せと回答については Q&A としてまとめること。また、問い合わせ結果については件数と主な内容について月別に一覧表としてまとめ、定期報告としてまとめること。

表３　月別ヘルプデスク受付件数　（サンプル）

	年度計	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
R5年度	228	18	28	24	12	22	14	19	30	9	19	21	12
R6年度	247	21	4	29	31	14	28	11	32	12	20	23	22
R7年度	186	5	26	14	17	23	16	9	8	6	25	20	17
計	661	44	58	67	60	59	58	39	70	27	64	64	51

（11）引継

ア．受注者は、令和７年度の本システム運用・保守事業者から運用・保守に必要な引継を受けること。なお、「４．（1）ア」に係る契約の移管には１か月程度要することがあるため、前年度の運用・保守事業者への支払いが発生する場合がある。この費用については受注者が前年度の運用・保守事業者へ支払うこと。

また、令和８年４月の契約開始直後から円滑に運用・保守作業を実施するため、契約開始までの引き継ぎ期間及び契約終了後概ね２か月程度は真摯に対応すること。

イ．受注者は、本契約の終了後に他の事業者が本システムの運用・保守を受注した場合には、他の事業者（次期システム運用・保守事業者）に対し、作業経緯、残存課題等についての引継を行うとともに、質疑応答等の協力を行うこと。

ウ．受注者は、次年度の運用・保守事業者に対し、システムの運用等を行うクラウド環境を原則としてそのまま引継ぐこと。そのため、引継に際しては、必要に応じて次年度の運用・保守事業者との間で書面による契約等を行い、管理者権限の引き渡し等、クラウド環境の引継を適切に行うこと。

（12）業務の完了

受注者はすべての業務が完了したときに、担当部署に業務の完了を報告すること。

（13）定例会等の実施

ア．受注者は、契約後 10 日（行政機関の休日を含まない。）以内に、作業実施計画書等の案について、担当部署及びステークホルダー等に説明し、認識共有を図ること等を目的とするキックオフ会議を開催すること。

イ．受注者は、定例会を原則、月次開催(月一回)（前述（3）ケの「定期運用・保守会議」を含む）するとともに、業務の進捗状況を運用・保守作業実施要領に基づき報告すること。

ウ．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。

エ．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。

（14）契約金額内訳及び情報資産管理標準シートの提出

ア．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。再委託（業務の一部を第三者に委任し、又は請け負わせること。以下同じ）先がある場合は再委託先の法人番号と再委託金額を提示すること。

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

イ．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。

ウ．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

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

（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

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

（I5）その他

運用・保守作業によって操作手順書等のドキュメントに変更が生じた場合は、修正後のドキュメントを成果物とすること。

（I6）成果物

ア．成果物名

本業務の成果物を表 4 に示す。

表４　成果物一覧

No.	記載箇所	成果物名	納品期日
1	4(13)ア	作業実施計画書	契約締結後 10 日以内
2	4(11)ア,イ	引継結果報告書	引継完了後５日以内
3	4(11)イ,ウ	引継書	令和９年３月 20 日
4	4(3)イ,ケ (6)カ	月次運用・保守作業報告書（含む、クラウドサービス利用実績、SLA）	定例会開催の２日前
5	4(12)	業務完了報告書	令和９年３月 31 日
6	4(13)エ	議事録及び会議資料一式	会議終了後３日以内
7	-	本業務における作成データ	作成・修正時適宜
8	4(5)オ	クラウドサービスの機能を利用したソフトウェア情報等の出力結果	担当部署の求めに応じ適宜
9	4(2)	「運用・保守作業計画」「運用・保守作業実施要領」の改定案	修正時適宜
10	4(14)	契約金額内訳	契約締結後５日以内
11		情報セキュリティ管理計画書	策定時
12	4(3)	パラメータシート（運用・保守の場合はシステム構成変更時のみ提出）	更新時適宜
13		農林水産省クラウド利用ガイドライン別紙 1_共通機能_利用申請書（更新時のみ提出） ・システム構成図 ・IaC で構築した際に作成された定義ファイル（AWS の場合は、CloudFormation） 「クラウドのセキュリティ実施対応状況（例 AWS の場合、ECR スキャンの結果、Fargete のプラットフォームバージョン等によるコンテナスキャン結果等、システム構成に合わせて必要なファイルを納品すること。）」	
14		ソースコード一式（更新時のみ）	
15		実行プログラム一式（更新時のみ）	
16		設計書一式（更新時のみ）	
17	4(3)、(15)	保守作業に係るドキュメント（改修等の記録	保守作業時

		等）	
18		操作手順書（一般利用者向け及び情報システム管理者向け）	
19	4(4)	障害報告書	障害発生時 担当部署の求めに応じ適宜
20	4(6)、(7)	運用・保守改善提案書	担当部署の求めに応じ年１回程度 （令和８年 10 月頃）
21	4(3)ソ	研修資料（含む研修計画）	作成時適宜
22	4(1)、(11)	クラウド環境一式（管理者権限等のアカウント情報を含むこと。なお、アカウント情報については、必要な情報を記載した「アカウント情報一覧」を準備した上で、担当部署が指定する方法で納品すること。）	引継前適宜
23	4(6)カ	クラウドサービスの利用実績	定例会開催の２日前
24	4(14)イ	情報資産管理標準シート	担当部署の求めに応じ適宜
25	４(1)オ	農林水産省をエンドカスタマー（エンドユーザー）として登録していることを証明する書面	契約締結後速やかに

イ．成果物の説明

（ア）作業実施計画書

受注者は、本調達仕様書、デジタル・ガバメント推進標準ガイドライン、解説書から、本業務の作業内容を把握した上で、契約日の翌日から 10 日（行政機関の休日を含まない。）以内に作業実施計画書を作成して提出すること。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。また、受注者は、承認を得た作業実施計画書に基づき、本業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

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（委託先等を含む。）

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

（イ）本業務における作成データ

担当部署の求めに応じて作成した全てのデータを提出すること。例えば会議資料を作成するために利用した元の生データや、本業務に関連して作成した資料を想定している。

（ウ）運用・保守作業計画および運用・保守作業実施要領の改定案

運用・保守作業計画及び運用・保守作業実施要領を必要に応じ更新し、担当部署に提出、承認を受けること。

（エ）情報セキュリティ管理計画書

本業務を遂行する上での情報セキュリティの管理方法等について記述したものを作成して提出すること。

ウ．成果物の納品方法

（ア）成果物は、すべ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。

（イ）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。

（ウ）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。

（エ）作成した成果物は担当部署が指定したサーバへ納品（例：PrimeDrive 又は SharePoint 等）すること。なお、納品の際は、検収が終了したファイル一式を時点がわかるような形式（例：zip 等）で提出すること。

（オ）電磁的記録媒体の納品について、Microsoft Office 又は PDF のファイル形

式で作成すること。

（カ）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。

（キ）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、担当職員の承認を得ること。

（ク）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。

（ケ）電磁的記録媒体により納品する場合は、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、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

エ．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。

〒100-8952

東京都千代田区霞が関 1-2-1

林野庁 林政部 木材利用課

オ．その他

本事業で作成した資料等について、納品前であっても担当部署の求めに応じ、担当部署の業務に必要な範囲で利用可能とすること。ただし、特別の事情がある場合はこの限りではない。

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の役割は図８、表５及び表６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。

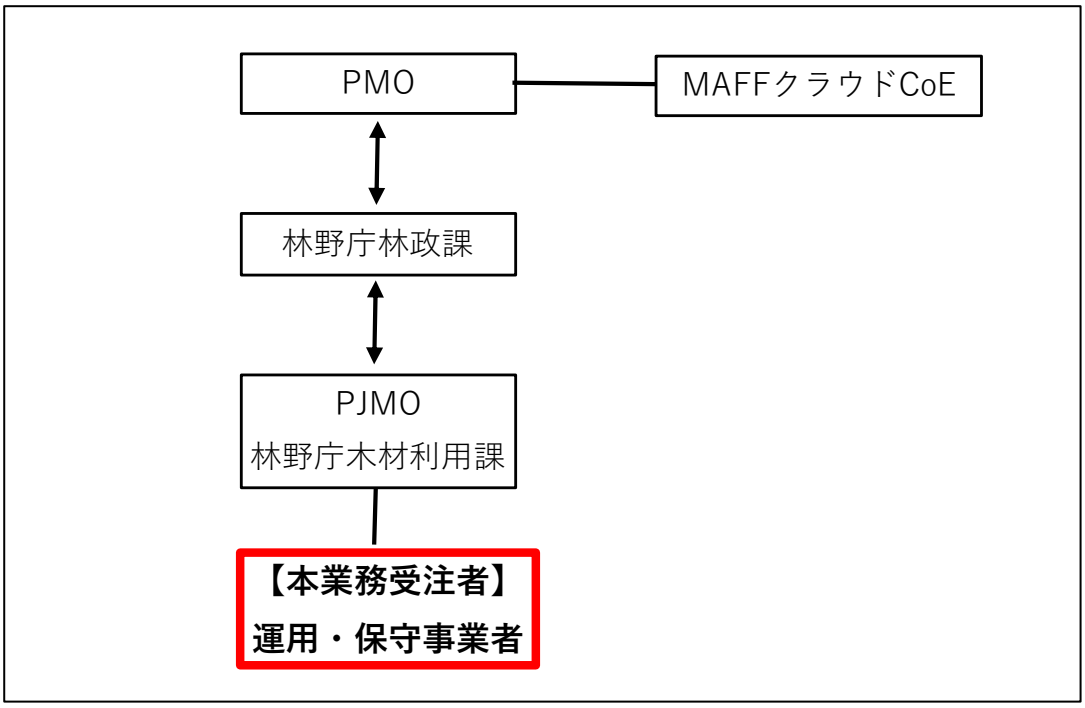


図8　業務の推進体制

表 5　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
ＰＪＭＯ（担当部署）	林野庁 林政部 木材利用課 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。
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各ＰＪＭＯからの問い合わせを受け、対応、助言・指導等を行う。中でも MAFF クラウド CoE は、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。
運用・保守事業者	本業務を実施する受注者。

表 6 本業務受注者に求め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、各関連する組織・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。 本業務の委託期間中は専任でこれに当たるものとする。
業務担当者	流通木材の合法性確認に係る業務内容、本システムの構成及び運用要件について把握し、本業務に当たる。 業務・ヘルプデスクチーム 業務アプリに関する運用及び保守作業を実施する。 各ユーザーからの問い合せを受け付ける。 インフラチーム インフラ基盤に関する運用及び保守作業を実施する。
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。
情報管理責任者	本業務の情報取扱い全てに関する監督を担う。

（2）作業要員に求める資格等の要件

ア．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資格・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を構築すること。また、担当する職務に応じて業務を効率的・効果的に推進する業務遂行能力を有すること。加えて、作業要員に求める資格試験のシラバス等に示される内容に即した技術・知識・実務能力を有すること。

イ．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、担当部署の理解を得ること。）。

ウ．運用・保守期間に改修などにより設計・開発を行う担当者には、情報処理技術者試験のうち、次に掲げる試験区分の合格者を１名以上必要な人数含むこと。なお、同一人が全ての試験区分に合格していることを求めるものではない。

（ア）システムアーキテクト試験

（イ）データベーススペシャリスト試験

（ウ）ネットワークスペシャリスト試験

エ．運用・保守期間に改修などにより設計・開発を行う担当者には、情報処理安全確保支援士の登録を受けている者又は同等の資格を有する者を含むこと。

オ．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のスキル）

カ. 担当メンバーは、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中級資格[*1] 以上を有する者を1名以上配置すること。

*1　例として、以下のような資格が挙げられる。

AWS Certified Solutions Architect – Associate

資格を有する人材を配置できない場合は、クラウド事業者のSolutions Architect（プリセールスSE）やクラウド事業者のProfessional Servicesなどの外部人材の支援を仰ぎ、その助言を真摯に受け止め実施すること。

（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、担当部署が定める運用・保守作業実施要領に基づき、運用・保守業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

（５）使用する言語

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。

（６）会議の体制

担当部署が参加する会議は原則として農林水産省本省内で開催することとし、事前に日程等を担当部署と協議して会場の確保に努めること。なお、効率的な業務実施のために、事前に担当部署の承認を得た上でウェブ会議等を実施することを可能とする。

（７）貸与条件

本業務の遂行に必要な貸与物品がある場合は、事前に担当部署と協議の上、貸与申請を行うこと。貸与された物品は、厳重な管理を行い、貸与期間終了後は速やかに返却すること。また、貸与期間終了前であっても、必要がなくなった場合には速やかに返却すること。

６.作業の実施に当たっての遵守事項

（ｌ）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とおりである。

（ア）委託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）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。

（カ）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、必要に応じて担当部署による実地調査が実施できること。

（キ）生成 AI システム特有のリスクケース等が発生した場合、受注者は関係するデータの提供や調査等に協力すること。

（ク）本業務の開発・運用において、ソースコード解析やソースコード生成、ソースコードの管理を行う際には、セキュリティ・バイ・デザイン（DS-200）を元に、情報セキュリティ対策の責任者を定め、開発環境や開発工程等も含めたすべてのライフサイクルに対してぬけ漏れなく情報セキュリティ対策を実行すること。

（ケ）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受注者及びクラウドサービスプロバイダーに帰属しないこと。

（コ）クラウドサービスの利用にあたり、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。

（サ）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において、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。

ウ. 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、事前に担当職員の許可を得ること。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ことを確認し、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、直ちに被害拡大防止等のため必要な措置を講ずるとともに、担当職員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委託する場合は、受注者（必要に応じ担当部署）は、原則として年１回以上の再委託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．本業務の遂行に当たっては、不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号)、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号)、行政手続における特定の個人を識別するための番号の利用に関する法律（平成 25 年 5 月 31 日法律第 27 号）等、適用される法令等を遵守し履行すること。

イ．受託者は、本業務の遂行に当たり、以下の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．環境負荷軽減に係る遵守事項

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、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」として提出すること。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）に該当する以下のアからカに基づくこと。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。

ア．DS-100 デジタル・ガバメント推進標準ガイドライン

イ．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

ウ．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

エ．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

オ．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

カ．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

開発（保守）に当たっては、「コーディング規約（Java 編）」「コーディング規約（JSP、JavaScript 編）」に準拠して作業を行うこと。

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。

エ．流通木材の合法性確認に関する法律及びそれらに基づく規程・通知

本システムを利用する業務は、改正 CW 法及びそれらに基づく規程・通知に沿って行われている。本システムのあるべき姿については現状有姿の他これらの文書による。本システムへ変更を加える際は関連する規程・通知等から逸脱しないよう担当部署と協議を行うこと。

オ．MAFF クラウドで要件定義、新規開発、移行、改修又は運用・保守する場合

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。

カ．本業務の遂行に当たっては、「農林水産省データマネジメント・データ活用基本方針書（令和５年 10 月）」に基づくこと。

キ．本業務の遂行に当たっては、生成 AI を活用する場合、「デジタル社会推進標準ガイドライン　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 別紙３調達チェックシート」の基本項目を満たすこと。本業務においては、国民等による農林水産省外利用の場合、個人情報、プライバシー、知的財産を取り扱う場合の要件についても対応すること。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。

（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、担当部署が情報システム監査の実施を必要と判断した場合は、担当部署が定めた実施内容（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。（担当部署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トのベストプラクティス（AWS の場合 AWS 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（SBD マニュアル)」及び同「別冊クラウド設計・開発編」に準拠すること。AWS の Security Hub の各ベンチマークの「セキュリティスコア」の値（準拠率という）について、90%以上の状態を維持し、運用保守役務において「準拠率」が、100%に近づくように継続的な改善に取り組むこと。(括弧内は SBD マニュアルにおける項番)

ア．システムの可用性確保(DA-2-1)

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運用継続計画書に記載の復旧目標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。

イ．不正プログラムの感染防止(AT-2-1)

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。

ウ．ログの蓄積・管理(AU-1-1)

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、本事業の期間保管するとともに、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。

エ．ログの保護(AU-1-2)

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。

オ．時刻の正確性確保(AU-1-3)

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。

カ．主体認証(AC-1-1)

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記憶の認証を行う機能として、パスワードの方式を採用すること。

キ．ライフサイクル管理(AC-2-1)

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。

ク．管理者権限の保護(AC-2-3)

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。

ケ．通信経路上の盗聴防止(PR-I-I)

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。

コ．保存情報の機密性確保(PR-I-2)

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。

サ．システムの構成管理(DA-I-I)

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。

シ．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(SC-2-I)

機器等の製造工程において、担当部署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。

ス．構築時のぜい弱性対策(AT-3-I)

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ぜい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ぜい弱性の有無を確認の上、運用上対処が必要なぜい弱性は修正の上で納入すること。

セ．運用時のぜい弱性対策(AT-3-2)

運用開始後、新たに発見されるぜい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行う方法（手順等）を備えること。

ソ．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(SC-I-I)

情報システムの構築において、担当部署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、担当部署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、受注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。

（８）情報システムの稼働環境

システムの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。

資料閲覧の際には別紙４「守秘義務に関する誓約書」の提出が必要となる。

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、2025 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 である。

イ. 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。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 CoE 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。

７.成果物の取扱いに関する事項

（Ｉ）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. 受注者又は第三者に帰属する知的財産権を用いて成果物を作成（情報システムの構築等を含む。）する場合、当該知的財産権の利用における制約等を担当部署に説明するとともに、WEB サイトのコンテンツ利用規約にその内容を記載する等によりシステム利用者が意図せず知的財産権を侵害することがないよう、必要な措置を講じること。

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。

ク．生成 AI を活用したシステムを構築・運用する場合、生成 AI で作成したアウトプットや本業務で作成した生成 AI 向けの指示文については、農林水産省に権利が帰属するものとする。

（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．公告日において令和７・８・９年度全省庁統一資格の「役務の提供等」の「A」又は「B」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。

ウ．入札資料の提出期限の日から、開札の時までの間において林野庁長官から物品の製造契約、物品の購入契約及び役務等契約指名停止措置要領に基づく指名停止を受けている期間中でないこと。

（２）公的な資格や認証等の取得

ア．入札参加者は、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．入札参加者は、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）受注実績等

ア．入札参加者は、本システムで具備する機能を有する情報システムの運用・保守を行った実績を過去３年以内に有すること。

イ．入札参加者は、パブリッククラウドへの移行又は構築を行った実績を過去３年以内に有すること。

ウ．入札参加者は、パブリッククラウドにおいて運用・保守を行った実績を過去３年以内に有すること。

エ．入札参加者は以下の①又は②のいずれかの条件を満たすこと。

（ア）クラウドサービスプロバイダーから代理店の認定を受け、かつ AWS Solution Provider Program（SPP）の登録を受けていること。

加えて、本案件の関係者が、日本国内のクラウドサービスプロバイダーから日本語で契約や技術に関するサポートを受けられる商流であること。

（イ）国内企業のディストリビュータ経由でクラウドサービスの再販が可能であること。

（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（デジタル統括アドバイザーに相当）、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委託先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。

９．再委託に関する事項

（１）再委託の制限及び再委託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委託してはならない。

イ．受注者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。

ウ．受注者は再委託先の行為について一切の責任を負うものとする。

エ．再委託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．再委託を行う場合、再委託先が「８．（５）入札制限」に示す要件を満たすこと。

（２）承認手続

ア．本業務の実施の一部を効率的な履行を図るため、合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに

再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別紙４の「再委託承認申請書」を担当部署に提出し、あらかじめ承認を受けること。

イ．前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を担当部署に提出し、承認を受けること。

ウ．効率的な履行を図るため、再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲、再々委託の必要性等を書面で届け出ること。

（３）再委託先の契約違反等

再委託先において、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、当該再委託先への再委託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．本業務に関する契約の締結は、令和８年度の予算成立を条件とする。令和８年３月 31 日以前に令和８年度予算が成立していない場合には契約締結の中止等を行う可能性があり、この場合、農林水産省は、契約締結の中止等に伴ういかなる責任も負担しない。

ウ．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担当部署に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、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。

エ．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。

オ．MAFF クラウド CoE からクラウドのシステム構成について、改善点の指摘を受けた場合に協議の上、対応を行うこと。また、MAFF クラウド CoE が監査・指導の観点でクラウド環境の確認が必要と判断した際には、要請に基づき、リードオンリーの IAM ユーザーを払い出すこと。

（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 林政部 木材利用課（本館７階ドア番号本 720）

イ．閲覧期間及び時間

令和７年 12 月 26 日から令和８年２月 18 日まで

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

最大２名まで。入札希望者の商号、連絡先、閲覧希望者氏名を別紙６「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紙５「守秘義務に関する誓約書」に記載の上、提出すること。

エ．閲覧時の注意

閲覧にて知り得た内容については、入札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。

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、次のカ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。

オ．連絡先

林野庁 林政部 木材利用課

電話 03-6744-2496

メール ： cleanwood@maff.go.jp

カ．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。

（ア）プロジェクト管理要領

（イ）プロジェクト標準（標準コーディング規約）

（ウ）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

（エ）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

（オ）現行の情報システムの情報システム設計書

（カ）農林水産省クラウド利用ガイドライン及び関係資料

（３）その他

本仕様書について疑義等がある場合は、別紙７「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。

11.附属文書

別紙Ⅰ　改正 CW 法概要
別紙２　情報セキュリティの確保に関する共通基本仕様
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
別紙４　再委託承認申請書
別紙５　守秘義務に関する誓約書
別紙６　閲覧申込書
別紙７　質問書

別添　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

以　上

【別紙１】

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７年４月１日施行

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

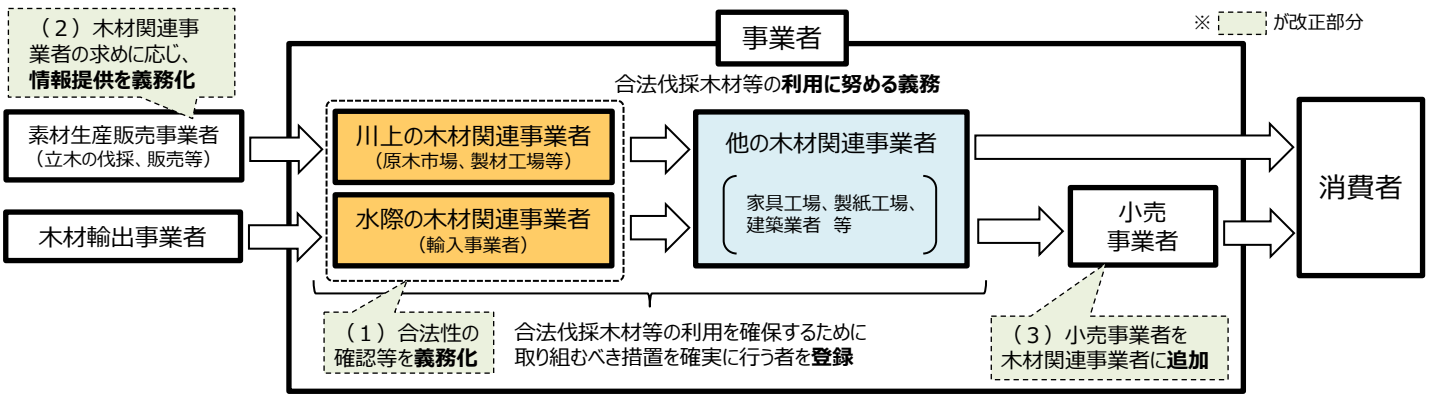
○ 合法性の確認等の情報が消費者まで伝わるよう、**小売事業者を木材関連事業者に追加**し、登録を受けることができるよう措置（第２条第４項）。

（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）。



（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、総合評価落札方式及び企画競争方式にあっては提案書等の評価のための書類に添付して提出すること。

Ⅻ 変更手続

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

【別紙３】

様式

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～カの取組について、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
・対象となる物品の輸送に当たり、燃料消費を少なくするよう検討する（もしくはそのような工夫を行っている配送業者と連携する）。	□	□
・対象となる物品の輸送に当たり、燃費効率の向上や温室効果ガスの過度な排出を防ぐ観点から、輸送車両の保守点検を適切に実施している。	□	□
・農林水産物や加工食品を使用する場合には、農薬等を適正に使用して（農薬の使用基準等を遵守して）作られたものを調達することに努めている。	□	□
・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　臭気や害虫の発生源となるものについて適正な管理や処分に努める。

具体的な事項	実施した／努めた	左記非該当
・臭気が発生する可能性がある機械・設備（食品残さの処理や堆肥製造等）を使用する場合、周辺環境に影響を与えないよう定期的に点検を行う。	□	□
・臭気や害虫発生の原因となる生ごみの削減や、適切な廃棄などに努めている。	□	□
・食品保管を行う等の場合、清潔な環境を維持するため、定期的に清掃を行うことに努めている。	□	□
・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
（　　）

エ　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
（　　）

オ　工事等を実施する場合は、生物多様性に配慮した事業実施に努める。

具体的な事項	実施した／努めた	左記非該当
・近隣の生物種に影響を与えるような、水質汚濁が発生しないよう努めている。	□	□
・近隣の生物種に影響を与えるような、大気汚染が発生しないよう努めている。	□	□
・施工にあたり使用する機械や車両について、排気ガスの規制に関連する法令等に適合したものを使用する。	□	□
・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
（　　）

カ　みどり戦略の理解に努めるとともに、機械等を扱う場合は、機械の適切な整備及び管理並びに作業安全に努める。

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。	□	□
・従業員等の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。	□	□
・作業現場における、作業安全のためのルールや手順などをマニュアル等に整理する。また、定期的な研修などを実施するように努めている。	□	□
・資機材や作業機械・設備が異常な動作などを起こさないよう、定期的な点検や補修などに努めている。	□	□
・作業現場における作業空間内の工具や資材の整理などを行い、安全に作業を行えるスペースを確保する。	□	□
・労災保険等の補償措置を備えるよう努めている。	□	□
・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
（　　）

別紙４

令和８年度流通木材の合法性確認システムに係る
運用・保守及びクラウドサービス提供業務再委託承認申請書

番　　号
年　　月　　日

支出負担行為担当官
林　野　庁　長　官　　殿

（請負者）
住　　所
氏　　名

令和　年　　月　　日付け契約の令和８年度流通木材の合法性確認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に係る請負事業について、下記のとおり再委託したいので、請負契約書第３条の規定により承認されたく申請します。

記

１　再委託先の相手方の住所及び氏名

２　再委託の業務範囲

３　再委託の必要性

４　再委託の金額

５　その他必要な事項

（注）１．申請時に再委託先及び再委託の契約金額（限度額を含む。）を特定できない事情がある場合には、その理由を記載すること。
なお、再委託の承認後に再委託先及び再委託の金額が決定した場合には、当該事項をこの書式に準じて、その旨報告すること。
２．再委託の承認後に再委託の相手方、業務の範囲又は契約金額（限度額を含む。）を変更する場合には、あらかじめ甲の承認を受けなければならない。
３．契約の性質に応じて、適宜、様式を変更して使用すること。

調達仕様書（別紙５）

林野庁木材利用課
課長　　宛

守秘義務に関する誓約書

「令和８年度流通木材の合法性確認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」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

調達仕様書（別紙６）

令和８年度　流通木材の合法性確認システムに係る
運用・保守及びクラウドサービス提供業務
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：
（２名まで）
２：

（別紙７）

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】

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