令和7年度（補正予算）

山地災害調査アプリケーション

改修等業務

調達仕様書

林野庁

目次

1　調達案件の概要

（1） 調達件名

令和7年度（補正予算）山地災害調査アプリケーション改修等業務

（2） 調達の背景

林野庁では、農林水産省防災業務計画に基づく「被害状況把握・報告」並びに「被害状況の把握と二次災害の未然防止」に迅速に対応するため、ArcGIS をプラットフォームとした山地災害調査アプリケーションを構築し、令和 4 年度から運用を開始している。

当該システムは、豪雨や地震等大規模な自然災害の発生時における迅速な山地災害の概況把握や治山・林道施設の緊急点検に不可欠なものであり、気候変動に伴い激甚化・頻発化する気象災害や切迫する南海トラフ地震、首都直下地震、日本海溝・千島海溝周辺海溝型地震等の大規模地震から国民の安心・安全を確保するため必要あり、継続的に運用する必要がある。

本業務においては、治山台帳情報の GIS データ化及び ArcGIS for Excel 等を活用した台帳作成機能の検討、ArcGIS 3D analyst を活用した復旧数量の算出手法の検討、山地災害危険地区やなだれ危険地区の GIS データ整備を実施し、山地災害調査アプリケーションを用いた更なる業務の効率化を実現することを目的とする。

2018 年6月には、「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」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。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を利用する。

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 クラウドといい、総合的な支援活動を行う組織を MAFF クラウド CoE という。

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。

（3） 調達目的及び調達の期待する効果

本業務は、治山台帳データの GIS データ整備や機能追加等の山地災害調査アプリケーションの改修により、農林水産省防災業務計画に基づく「被害状況把握・報告」並びに「被害状況の把握と二次災害の未然防止」に迅速に対応することを目的とする。

（4） 業務・情報システムの概要

山地災害調査アプリケーション及び令和7年度（補正予算）山地災害調査アプリケーションの概要は次のとおりである。

図 1 システム概要図

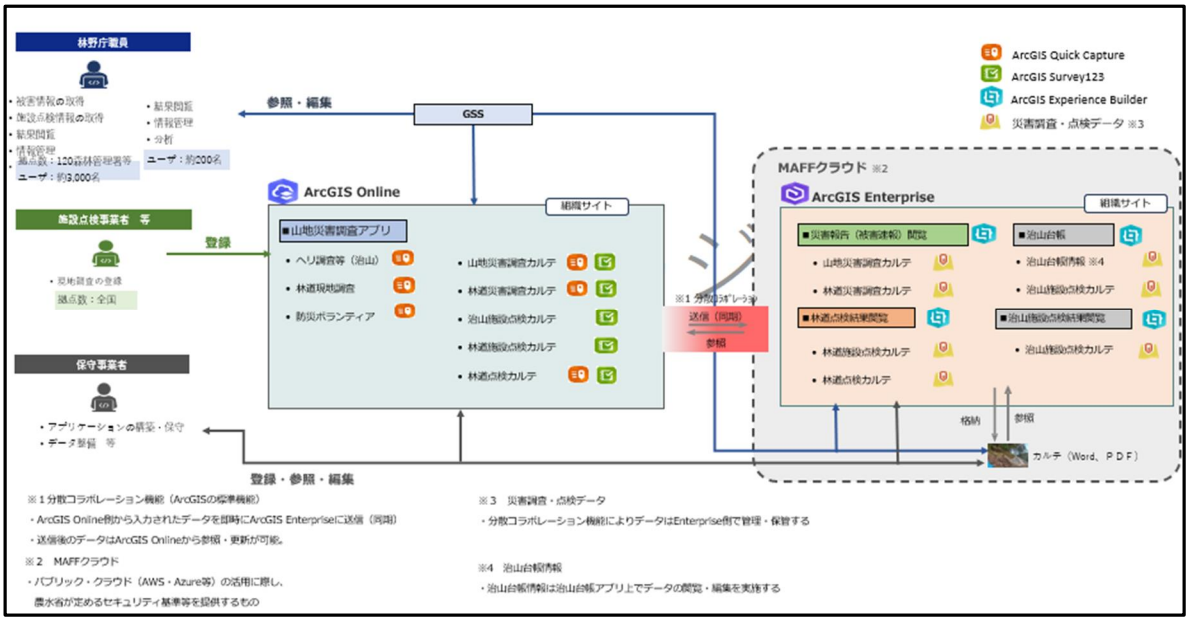


図2 システム構成図

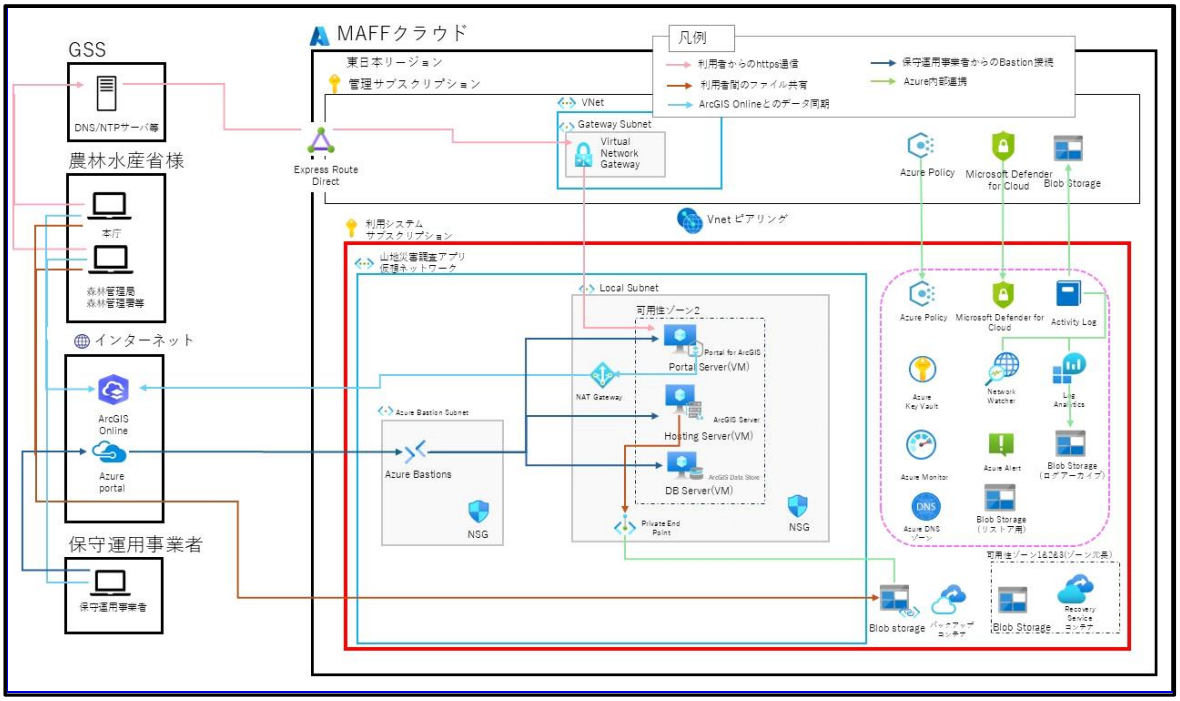
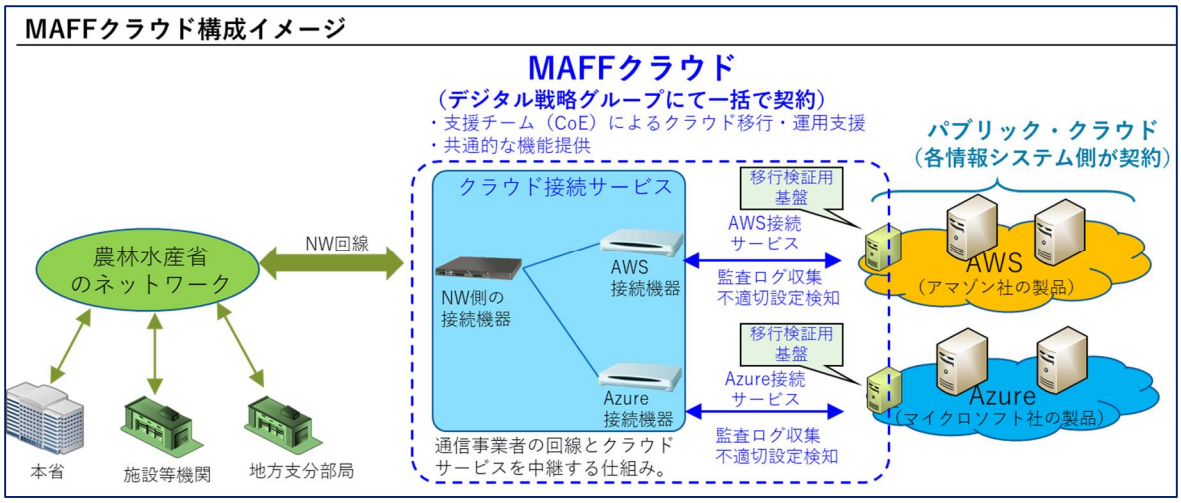


図３　MAFF クラウドの構成イメージ



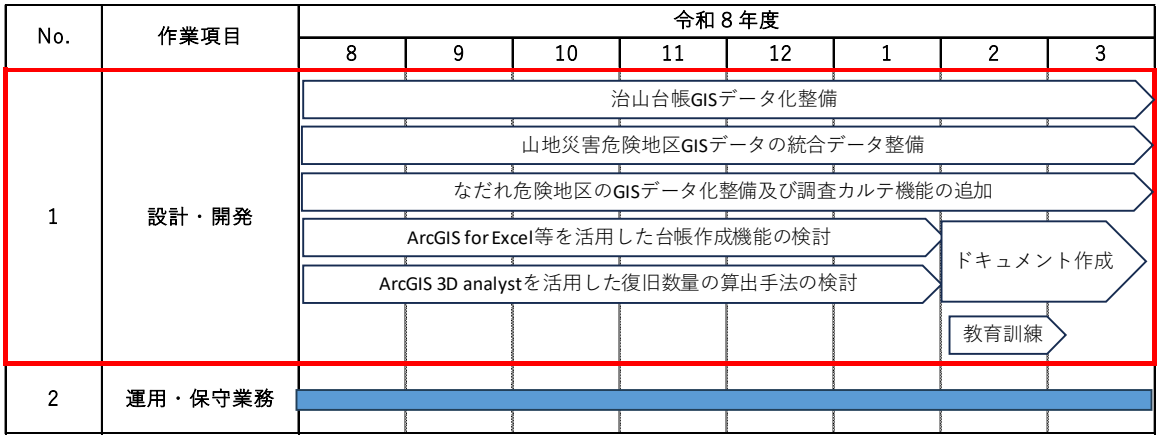
（5） 契約期間

契約締結日から令和9年3月 31 日まで

（6） 作業スケジュール

作業スケジュールは次のとおり想定している。

表1 作業スケジュール



2 調達案件及び関連調達案件

（1） 調達範囲

本調達では、山地災害調査アプリケーションをより効率的に活用するための以下①～⑥の業務を行うものとする。

① 治山台帳情報の GIS データ化整備（治山台帳2万件分）

② ArcGIS for Excel 等を活用した治山台帳作成機能の検討

③ ArcGIS 3D analyst を活用した復旧数量の算出手法の検討

④ 山地災害危険地区 GIS データの統合データ整備

⑤ なだれ危険地区の GIS データ化整備（533 箇所分）及び調査カルテ機能の追加

⑥ 教育訓練の実施

また、以下ア、イについては、受注者の負担として本調達の費用に含めるものとする。

ア ArcGIS 3D analyst 数量：1（1年分）

イ 本システムの開発・検証用の環境及びライセンス費用

なお、責任範囲の調整が必要となった場合には、農林水産省と協議の上、決定するものとする。

（2） 調達案件の一覧

調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期等は次の表のとおり。

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	入札公告 落札者決定	契約期間
1	令和6年度（補正予算）山地災害調査プリケーションのクラウド移行及び改修業務	一般競争入札（総合評価）	令和7年9月 16 日		令和7年9月から令和8年3月まで
2	令和8年度山地災害調査アプリケーション運用・保守業務	一般競争入札（総合評価）	令和8年4月1日		令和8年4月から令和9年3月まで
3	令和7年度（補正予算）山地災害調査アプリケーション改修等業務	一般競争入札（総合評価）	令和8年8月頃	令和8年5月頃 令和8年7月頃	令和8年8月頃から令和9年3月まで

（3） 調達案件間の入札制限

本業務と関連する業務で、入札制限の対象とするものはない。

3 情報システムに求める要件

設計・開発の実施に当たっては、「別紙1 要件定義書」の各要件を満たすこと。

4 作業の実施内容

本業務においては、（1）システム改修業務と（2）システム実証業務に分類される。（1）システム改修業務においては、（3）～（7）について実施すること。

（1） システム改修業務

ア 治山台帳情報の GIS データ化整備

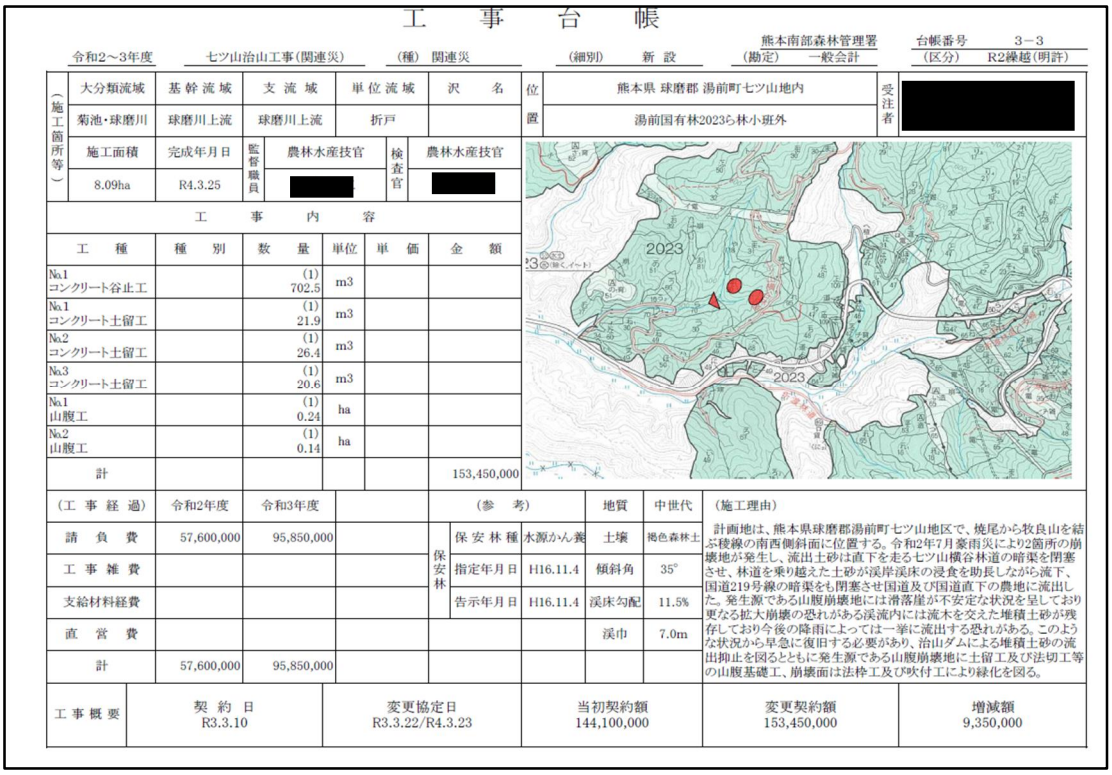
当該システムの Azure Blob Storage 内に格納された7森林管理局分の治山台帳情報を治山台帳アプリ上に GIS データ化整備を行うこととし、本業務における事業量（治山台帳件数）は、2万件とする。

治山台帳を基に施設の位置情報及び表3の項目についての属性を登録する。具体の、登録方法については、「治山台帳アプリ手順書」によること。

表3 治山台帳アプリに登録する属性情報（点構造物の例）

番号	項目名	フィールド名	データタイプ	備考
1	Kanrikyoku	森林管理局	整数型	
2	Kanrisyo	森林管理署等	整数型	
3	KokuminKubun	国直民直別	文字型	
4	KanseiNendo	完成年度	整数型	
5	GIS_DaityouNo	GIS 台帳番号	文字型	
6	DaityouNo	台帳番号	文字型	
7	KoujiName	工事名	文字型	
8	UkeoiKoujihi	請負工事費	整数型	
9	KousyuName	工種名	文字型	
10	Note	備考	文字型	
11	TikuName	地区名	文字型	
12	KokuyurinName	国有林名	文字型	
13	Rinpan	林班	文字型	
14	Jigyousyo	事業所	文字型	
15	Attachment	添付ファイル	文字型	
16	Kaitenkakudo	回転角度	整数型	
17	created_user	登録者	文字型	
18	created_date	登録年月日	日付型	
19	last_edited_user	編集者	文字型	
20	last_edited_date	編集年月日	日付型	
21	HensyuNaiyou	編集内容	文字型	

図４　治山台帳（参考）



工　事　台　帳

令和2～3年度　七ツ山治山工事(関連災)　(種)　関連災　(細別)　新　設　熊本南部森林管理署　(勘定)　一般会計　台帳番号　3－3　(区分)　R2繰越(明許)

(施工箇所等)	大分類流域	基幹流域	支流域	単位流域	沢名	位置	熊本県 球磨郡 湯前町七ツ山地内	受注者	[redacted]
	菊池・球磨川	球磨川上流	球磨川上流	折戸			湯前国有林2023ら林小班外		
	施工面積	完成年月日	監督職員	農林水産技官	検査官	農林水産技官			
	8.09ha	R4.3.25	[redacted]		[redacted]				

工　事　内　容

工種	種別	数量	単位	単価	金額
No.1 コンクリート谷止工		(1) 702.5	m3		
No.1 コンクリート土留工		(1) 21.9	m3		
No.2 コンクリート土留工		(1) 26.4	m3		
No.3 コンクリート土留工		(1) 20.6	m3		
No.1 山腹工		(1) 0.24	ha		
No.2 山腹工		(1) 0.14	ha		
計					153,450,000

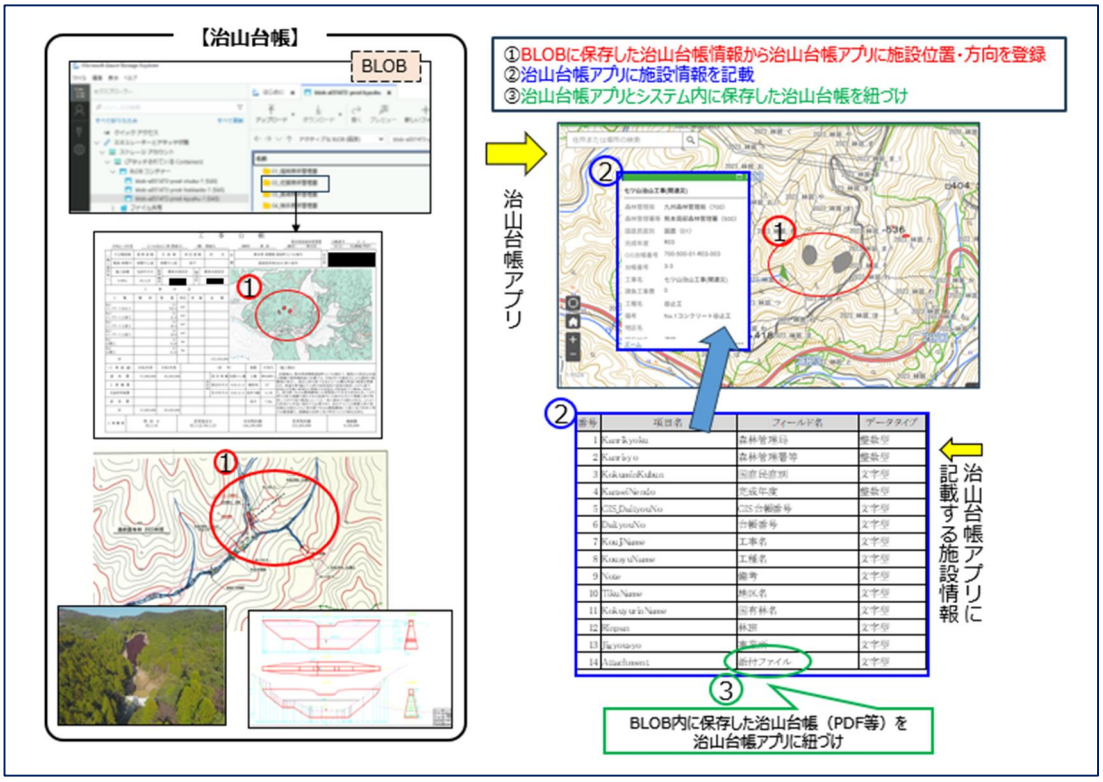
(工事経過)	令和2年度	令和3年度		(参考)		地質	中世代
請負費	57,600,000	95,850,000	保安林	保安林種	水源かん養	土壌	褐色森林土
工事雑費				指定年月日	H16.11.4	傾斜角	35°
支給材料経費				告示年月日	H16.11.4	渓床勾配	11.5%
直営費						渓巾	7.0m
計	57,600,000	95,850,000					

(施工理由)

計画地は、熊本県球磨郡湯前町七ツ山地区で、焼尾から牧良山を結ぶ稜線の南西側斜面に位置する。令和2年7月豪雨災により2箇所の崩壊地が発生し、流出土砂は直下を走る七ツ山横谷林道の暗渠を閉塞させ、林道を乗り越えた土砂が渓岸渓床の浸食を助長しながら流下、国道219号線の暗渠をも閉塞させ国道及び国道直下の農地に流出した。発生源である山腹崩壊地には滑落崖が不安定な状況を呈しており更なる拡大崩壊の恐れがある渓流内には流木を交えた堆積土砂が残存しており今後の降雨によっては一挙に流出する恐れがある。このような状況から早急に復旧する必要があり、治山ダムによる堆積土砂の流出抑止を図るとともに発生源である山腹崩壊地に土留工及び法切工等の山腹基礎工、崩壊面は法枠工及び吹付工により緑化を図る。

工事概要	契約日	変更協定日	当初契約額	変更契約額	増減額
	R3.3.10	R3.3.22/R4.3.23	144,100,000	153,450,000	9,350,000

図５　治山台帳情報の GIS データ化整備　事業概要



イ　山地災害危険地区の GIS データの統合データ整備

山地災害危険地区については、令和7年度までに全国的に再点検を実施したところ。当システムで活用している、各森林管理局が管轄する山地災害危険地区の GIS データについて、整備主体によって再点検後のデータ形式（シェープファイル等）や作成単位（都道府県毎、森林管理署等毎 等）、属性情報の格納方法などが一律でないことから、当システムへの危険地区情報の反映及び令和9年度に予定されている山地災害危険地区のオープンデータ化の事前準備として、以下の仕様のとおり、統合データを整備する。

なお、令和9年度に林野庁が別途整備する都道府県単位の民有林の山地災害危険地区の GIS データと統合することを念頭に整備するほか、整備した GIS データは ArcGIS 及び QGIS において動作確認を行うこと。

(a)　形式及び単位

都道府県単位のジオパッケージ形式（ジオメトリ;ポリゴン）とする。

(b)　座標参照系

JGD2011 の地理座標系（EPSG:6668）とする。

(c)　属性定義

表5のとおり

表4　森林管理局別の GIS データの状況

森林管理局名	データ形式	作成単位
北海道森林管理局	シェープファイル	都道府県毎
東北森林管理局	シェープファイル	都道府県毎
関東森林管理局	シェープファイル	森林管理局毎
中部森林管理局	シェープファイル	森林管理署毎
近畿中国森林管理局	シェープファイル	都道府県毎
四国森林管理局	ジオパッケージ	森林管理署毎
九州森林管理局	ジオパッケージ	森林管理署毎

表5　山地災害危険地区統合データの属性定義

No.	属性名	説明	属性の型	長さ（桁数）
1	fid	地物ごとの固有の識別子、ジオパッケージの自動附番	整数	0
2	森林管理局名称	林野庁の地方支部部局	文字列	50
3	森林管理署等名称	森林管理局の下部組織	文字列	50

4	危険地区種別	山腹崩壊危険地区、地すべり危険地区、崩壊土砂流出危険地区の別	文字列	50
5	国民別	国、民、国民、民直の別	文字列	50
6	危険地区番号	［3桁の市町村コード- 連番］で構成される番号	文字列	3
7	危険度	A、B、C の別	文字列	50
8	危険地区名称	地区名称	文字列	50
9	留意事項	データに関する留意事項等	文字列	50

ウ　なだれ危険地区の GIS データ化整備及び調査カルテ機能の追加

現在、紙・PDF データで管理されている各森林管理局で所管しているなだれ危険地区 533 個所について、以下の使用のとおり GIS データ化整備を行う。

(d)　形式及び単位

都道府県単位のジオパッケージ形式（ジオメトリ：ポリゴン）とする。

(e)　座標参照系

JGD2011 の地理座標系（EPSG：6668）とする。

(f)　属性定義

表6のとおり。

属性定義に必要な資料については、発注者より提供する。

また、ArcGIS Survey123 を活用し図8に示す点検カルテを作成する。システム内の仕様については、治山施設点検カルテを踏襲することとし、ダッシュボートは ArcGIS Enterprise 内に別途作成する。

表6　なだれ危険個所データの属性定義

No.	属性名	説明	属性の型
1	fid	地物ごとの固有の識別子、ジオパッケージの自動附番	整数
2	森林管理局名称	林野庁の地方部局	文字列
3	森林管理署等名称	森林管理局の下部組織	文字列
4	都道府県名称	都道府県の名称	文字列
5	市町村名称	市町村の名称	文字列
6	市町村番号	JISX0402 で定められている市区町村コード 3 桁	文字列
7	調査番号	市町村毎の連番	文字列
8	発生危険度	A、B、C の別	文字列
9	留意事項	データに関する留意事項等	文字列

図６　なだれ危険個所点検表

なだれ危険箇所点検調査表

〇〇森林管理署

危険箇所	市町村名	
	調査番号	
	所在地	
	過去のなだれの発生の有無	有 ・ 無
	保全対象	〇道 〇m　人家 〇戸　公共施設 〇〇 〇棟　鉄道 〇m その他〇〇
	なだれ防止施設	有 ・ 無　（施設:〇〇〇〇 〇基）（〇年度完成）
	実施事由	緊急点検　　通常点検
	日時・時間	平成〇〇年〇〇月〇〇日
	実施者	〇〇課　〇〇職　氏名 〇〇〇〇 〇〇課　〇〇職　氏名 〇〇〇〇
	天候	吹雪　雪　みぞれ　曇　雨　晴
	警報等	大雪警報（発令　月　日　:　解除　月　日） 注意報　大雪・雪崩・風雪・強風・低温・着雪・融雪・濃霧・霜
	積雪深	〇〇cm　目測　実測
	新雪深	〇〇cm　目測　実測

点検項目		有無	コメント
斜面状況	①なだれ発生の有無	有 ・ 無	
	②雪庇	有 ・ 無	
	③吹き溜まりによる雪庇（巻きだれ）	有 ・ 無	
	④クラック（雪割れ）	有 ・ 無	
	⑤雪しわ	有 ・ 無	
	⑥積雪表面のフラット化	有 ・ 無	
	⑦スノーボール	有 ・ 無	
	⑧地すべり・崩落等の地形変状	有 ・ 無	
	⑨その他の異常	有 ・ 無	
植生状況	①植生密度（密・中・疎）	密 ・ 中 ・ 疎	
	②立木高（高・中・低）	高 ・ 中 ・ 低	
	③なだれ抑止効果	有 ・ 無	
	④積雪深に対する雪上木高	有 ・ 無	
	⑤植生の折れ、たわみ、位置の変化	有 ・ 無	
	⑥その他、樹木の着冠雪など	有 ・ 無	
施設状況	①施設の埋没	有 ・ 無	
	②施設天端からの巻きだれ	有 ・ 無	
	③施設の破損等の変状	有 ・ 無	
	④施設間からの崩落雪	有 ・ 無	
	⑤防護擁壁等のポケット部の堆雪	有 ・ 無	
	⑥その他の異常	有 ・ 無	

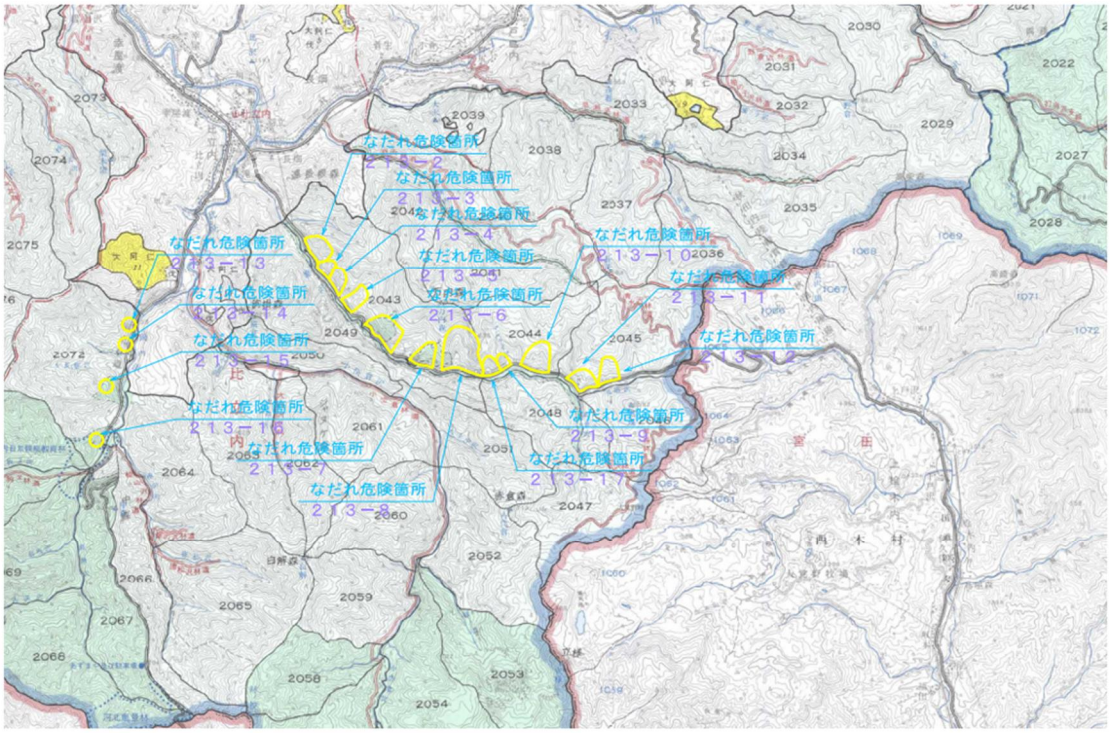
評　価	A:対策が必要　B:監視観測が必要　C:通常点検を継続

写真添付	写真は必ず添付のこと。（全体写真、雪庇・クラック等の写真、異常箇所の位置関係など）

摘要	必要により記載	コメント
	①今後講じようとする措置	例:専用道を国有林入り口で交通止めとした。 例:今後、注意報の出ている期間や融雪期に週1回程度巡視する。 例:直下に民家があり、雪崩防止柵高さ2m長さ50m1基の設置が必要である。
	②関係機関への連絡	例:〇〇市に、位置図と写真を提供し、現況を説明した。（危険度や将来の対策工は除く）
その他		

注:該当に〇印を付し、必要事項を記載する。

図７　なだれ危険個所（参考）



北秋田市のなだれ危険個所位置図
https://www.rinya.maff.go.jp/tohoku/policy/business/tisan/attach/pdf/28nadare-56.pdf

（2）システム実証業務

受注者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、担当部署の指示に基づき、以下の項目を記載したシステム実証業務計画書の案を作成し、担当部署の承認を得ること。

・作業概要

システム実証業務の対象範囲、作業概要等について記載する。

・作業体制に関する事項

システム実証業務に関連する全ての関係者について、その体制、関係者間の関係性、役割分担・責務等について記載する。

・スケジュールに関する事項

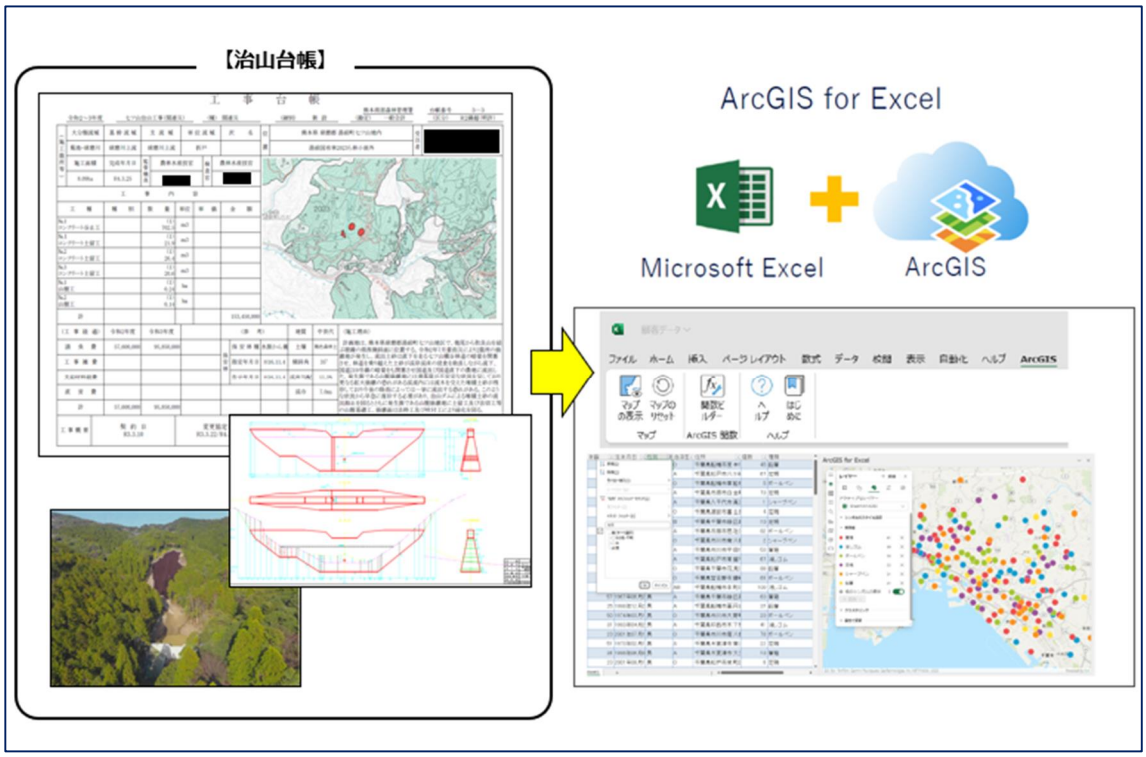
プロジェクト計画書及び調達仕様書に基づき、作業内容、スケジュール、マイルストーン等について記載する。

ア　ArcGIS for Excel 等を活用した治山台帳作成機能の検討

現行においては、Excel 等により作成した治山台帳を PDF 化したものを、Azure Blob Storage に格納し、格納された治山台帳情報を基に、治山台帳アプリに GIS データ化整備を行っているところ。

将来的には、治山台帳アプリ内で位置情報と紐づいた治山台帳の作成を目指すこととし、当該業務においては、ArcGIS for Excel 等を活用した治山台帳作成のデジタル完結の手法を検討し、検討結果について取りまとめること。

図８　ArcGIS for Excel 等を活用した治山台帳帳作成機能の検討　事業概要



イ　ArcGIS 3D analyst を活用した復旧数量の算出手法の検討

災害箇所の復旧計画策定の効率化を目指し、現地で LiDER 等により取得した点群データと ArcGIS 3D analyst を活用した被災箇所の復旧数量の算定手法を検討し、検討結果について取りまとめること。

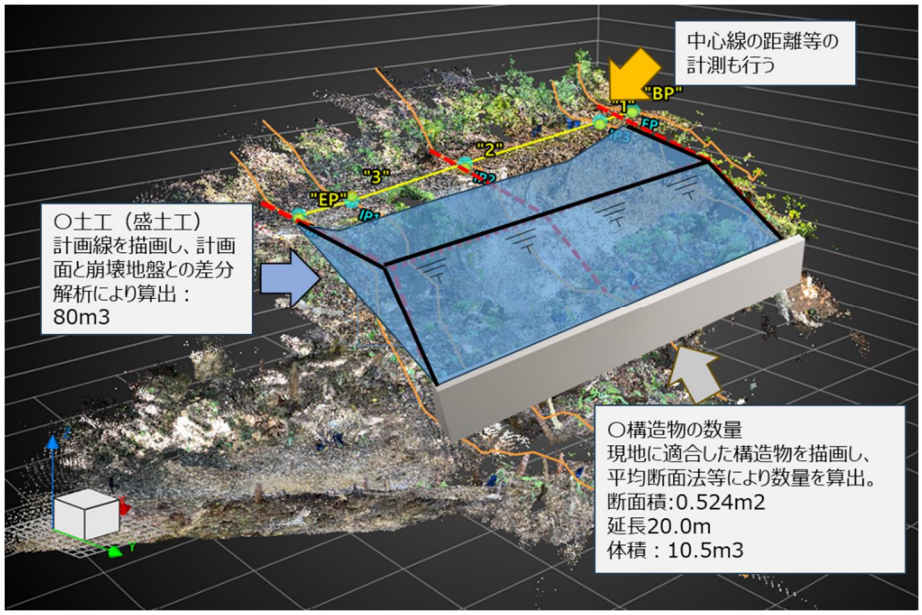
林道被災箇所における、復旧に要する土工（盛土工）と構造物の数量を概略的に把握する手法を検討し、具体的には以下の実現を想定している。

(g)　計画線を描画し、計画面と崩壊地盤との差分解析により算出

(h)　現地に適合した構造物を描画し、平均断面法等により数量を算出

なお、業務に使用する点群データについては林野庁から提供する。

図９　ArcGIS 3D analyst を活用した復旧数量の算出手法の検討（イメージ図）



（3） 設計・開発実施計画書等の作成

受注者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、担当部署の指示に基づき、設計・開発実施計画書及び設計・開発実施要領の案を作成し、担当部署の承認を得ること。

なお、設計・開発実施計画書及び設計・開発実施要領の記載内容は「デジタル・ガバメント推進標準ガイドライン」(デジタル社会推進会議幹事会決定。最終改定：2025 年 5 月 27 日以下「標準ガイドライン」という。)「第7章　設計・開発」で定義されているものとする。

（4） 要件定義内容の調整・確定

受注者は、設計・開発の実施に先立ち、「別紙1　要件定義書」の内容を確認すること。その際、内容について調整すべき事項があれば、担当部署、令和 8 年度山地災害調査アプリケーション運用・保守業務の受注者と調整の上、結果に基づき要件定義書の修正を行うこと。要件の調整内容は、担当部署及び関係するステークホルダーに提示し、合意形成を図りつつ進めること。

（5） 設計

ア　受注者は、「別紙1　要件定義書」の機能要件及び非機能要件を満たすための基本設計及び詳細設計を行い、成果物について担当部署の承認を得ること。

イ　受注者は、運用設計及び保守設計を行い、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用計画及び保守作業計画の案を作成し、担当部署の確認を受けること。

ウ　受注者は、生成 AI を活用したシステム構築を行う場合、インプットの定義、インプットの利用条件等について、基本設計で検討し、担当部署の承認を得ること。

エ　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。

オ　受注者は、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。

（6） 開発・テスト

ア　受注者は、開発に当たり、アプリケーションプログラムの開発又は保守を効率的に実施するため、プログラミング等のルールを定めた開発標準（標準コーディング規約、セキュアコーディング規約、データやデータ項目の命名規約等）を定め、担当部署の確認を受けること。

イ　受注者は、開発に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、標準コーディング規約遵守の確認、ソースコードの検査、現場での抜き打ち調査等についての実施主体、手順、方法等）を定め、担当部署の確認を受けること。

ウ　受注者は、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、担当部署の承認を得ること。

エ　受注者は、設計工程の成果物及びテスト計画書に基づき、アプリケーションプログラムの開発、テストを行うこと。

オ　受注者は、テスト計画書に基づき、各テストの実施状況と実施結果について担当部署に報告すること。その際、セキュリティ関連のテストの実施結果が確認できるようにすること。

カ　受注者は、生成 AI を活用したシステム構築を行う場合、導入予定の生成 AI システムが期待する品質を満たしているか確認し、担当部署の承認を得ること。なお、担当部署は品質が満たされていないと判断した場合、原因を特定し、改善措置を講じること。

キ　受注者は、本調達にて開発したプログラム一式を成果物として提出すること。

（7） 受入テスト支援

ア　受注者は、担当部署が受入テストのテスト計画書を作成するに当たり、情報提供等の支援を行うこと。

イ　受注者は、担当部署が受入テストを実施するに当たり、環境整備、運用等の支援を行うこと。

ウ　受注者は、担当部署の指示に基づき、担当部署以外の情報システム利用者のテスト実施も含めて、テスト計画書作成の支援を行うこと。

（8）引継ぎ

ア　受注者は、設計・開発の設計書、作業経緯、残存課題等を文書化し、運用事業者及び保守事業者に対して確実な引継ぎを行うこと。

イ　受注者は、他の運用事業者が本情報システムの運用を受注した場合には、次期運用事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

ウ　受注者は、運用・保守事業者に対し、システム改修で行った開発環境への設定変更等の環境に関する情報及びデプロイ方法等に更新があった場合にその情報を引継ぐこと。

（9）教育訓練の実施

山地災害調査アプリケーション全体に共通する使用方法について教育訓練を実施することとし、教育対象者は林野庁職員のうち 500 人程度を想定している。また、教育訓練の実施方法は、Web による講義形式を想定している。

以下に、各教育訓練方法についての要件を示す。

ア 講義における講師は、受注者が実施すること。

イ 講義に必要な教材については、受注者が準備すること。必要な機材（プロジェクタ等）は、林野庁と協議の上、必要に応じて受注者が準備すること。

ウ 講義会は Web 形式により実施するものとする。

エ 講義は録画を行い、必要に応じて、掲載等を行うこと。また、録画データは納品の上、林野庁が再利用することを妨げないこと。

オ 講義開催日数は、森林管理局毎に各１回（１日×７回）の合計7回とし、令和９年２月頃を想定している。講義開催時間は、おおむね2時間とすること。

カ 教育教材については、電子データにて配布する形とする。

キ 講義終了後、15 分程度の質疑応答の時間を設けること。

ク 講義では受講者がシステム操作を実体験できるようにすること。ただし、本番環境以外に研修用の環境を構築するなどし、本番稼動に影響を与えずに研修を実施できるよう林野庁と調整すること。

ケ 講義、マニュアルに関するアンケート用紙を作成の上、講義後に受講者に回答を依頼すること。なお、アンケート内容は事前に林野庁と調整すること。

コ 上記の教育対象者に対して、操作マニュアル、教育資料（システムの概要資料、操作動画、FAQ 等を想定）を作成すること。詳細は、林野庁と協議の上決定する。

サ 教育資料の作成に当たっては、情報システムやスマートフォンの操作に不慣れな者でも分かりやすいような構成、内容とすること。

シ　教育資料については、林野庁のレビューを経て承認を得ること。

ス　教育訓練の実施結果を教育訓練実施結果報告書にて林野庁に報告し、承認を得ること。

（10）定例会等の実施

ア　受注者は、定例会を月１回程度開催するとともに、業務の進捗状況を報告すること。

イ　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。

ウ　受注者は、会議終了後、3 日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、担当部署の承認を得ること。

（11）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、農林水産省が定める時期に、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内容」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

(12)成果物の作成

ア　成果物名

本業務の成果物を以下に示す。

表 1 成果物一覧

No.	成果物名	内容及び納品数量	納品期日
1	設計・開発実施計画書	1	契約締結後2週間以内
2	設計・開発実施要領	1	契約締結後2週間以内
3	設計・開発実施要領に基づく管理資料	1	契約締結後2週間以内
4	システム実証業務計画書	1	契約締結後2週間以内

5	開発標準（標準コーディング規約等）	1	事業完了時
6	設計書	1	事業完了時
7	ソースコード一式	1	事業完了時
8	ノンプログラミングによる画面生成等プロトタイピング用のツール等を使用する場合、設計書やソースコード一式の生成等に使用される設定情報その他の必要な情報一式	1	事業完了時
9	実行プログラム一式	1	事業完了時
10	外部サービスを利用する場合、当該サービスに係る設定情報その他の必要な情報一式	1	事業完了時
11	テスト計画書	1	テスト前
12	テスト仕様書	1	テスト前
13	単体テスト結果報告書	1	単体テスト後
14	結合テスト結果報告書	1	結合テスト後
15	総合テスト結果報告書	1	総合テスト後
16	各種申請書（あれば）	1	申請時
17	テストデータ	1	テスト終了時
18	操作手順書（追加機能分）	1	事業完了時
19	研修用資料	1	研修前
20	要件定義書の改定案	1	事業完了時
21	契約金額内訳	1	契約後速やかに
22	情報資産管理標準シート	1	担当部署の支持する時期
23	引継ぎ資料	1	事業完了時
24	ArcGIS for Excel等を活用した治山台帳作成機能の検討結果報告書	1	事業完了時
25	ArcGIS 3D analystを活用した復旧数量の算出手法の検討結果報告書	1	事業完了時

イ　成果物の納品方法

・　成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

・　用字・用語・記述符号の表記については、「公用文作成の考え方」（令和 4 年 1 月 11 日内閣官房長官通知）を参考にすること。

- 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。
- 作成した成果物は担当部署が指定したサーバへ納品（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。
- サーバ納品について、Microsoft Office 又は PDF のファイル形式で作成すること。
- 納品後、農林水産省において改変が可能となるよう、図表等の元データも併せて納品すること。
- 成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。
- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

ウ　成果物の納品場所

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

〒100－8950
東京都千代田区霞が関 1-2-1
林野庁国有林野部業務課

５　作業の実施体制・方法

（1）作業実施体制

本業務の推進体制及び本業務受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者内の人員構成については想定であり、受注者決定後に協議の上、見直しを行う。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

図 10 本業務の推進体制及び本業務受注者に求める作業実施体制

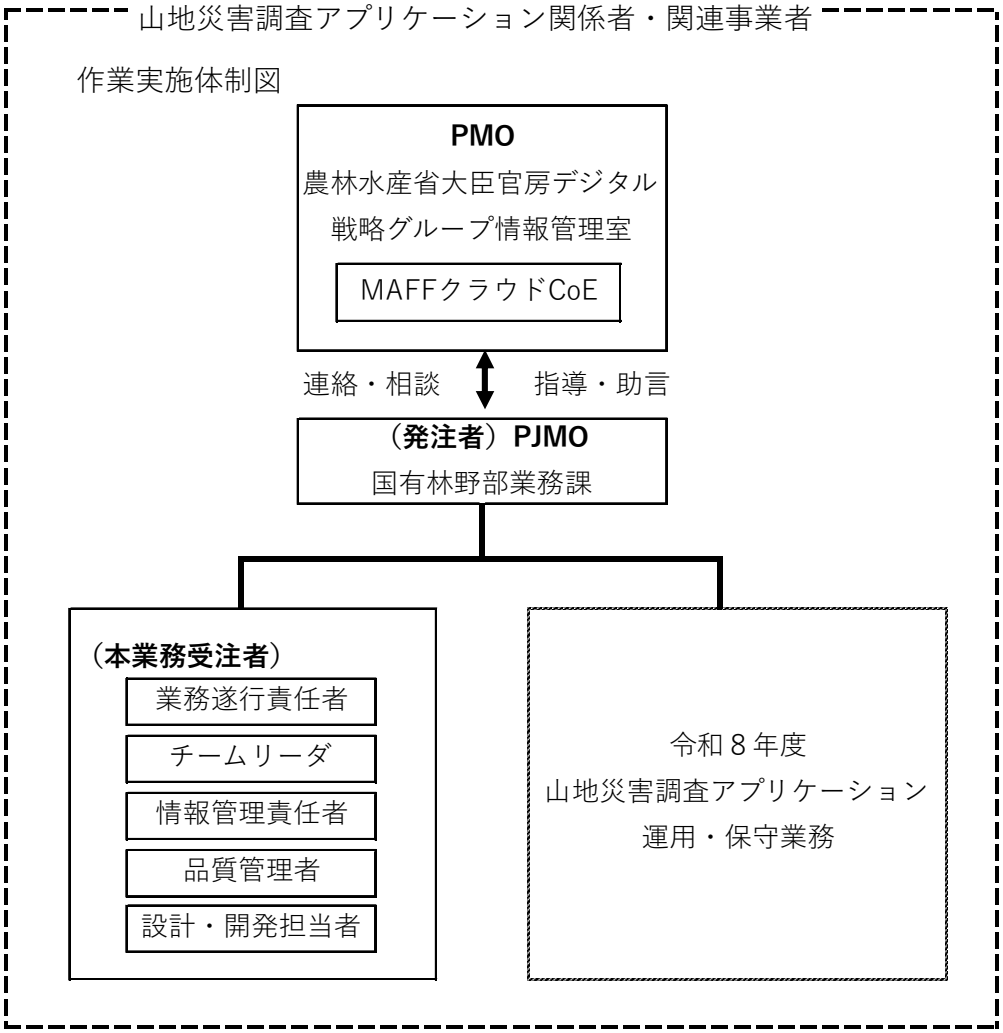


表 2 本業務における組織等の役割

組織等	本業務における役割
PJMO（担当部署）	山地災害調査アプリケーションの管理組織として、本業務の進捗等を管理する。
本業務受注者	本業務を実施する。
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担当部署からの問い合わせを受け、対応、助言・指導等を行う。
MAFFクラウドCoE	担当部署・受注者に対してパブリッククラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。
令和8年度山地災害調査アプリケーション	本業務受注者と情報共有を図りながら山地災害調査アプリケーションの運用・保守を実施する。

組織等	本業務における役割
運用・保守業務の受注者	

表 3 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
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。
チームリーダー	山地災害調査アプリケーション改修等業務に関する設計・開発において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
設計・開発担当者	山地災害調査アプリケーション改修等業務に関する設計・開発を担う。
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

受注者は、本業務の遂行責任者及び担当者等の役割に応じて次に示すスキル・経験を持つ人員を充て、プロジェクト全体として全ての要件を満たす作業実施体制とすること。

ア 遂行責任者及びチームリーダーは、情報システムの設計・開発又はシステム基盤導入の経験年数を5年以上有すること。また、その中でリーダクラスとしての経験を1件以上有すること。

イ 設計・開発に関わるメンバーのうち、情報システムの設計・開発等の情報処理業務の経験年数が5年以上の者又は同等の実績を有する者を 1 名以上配置すること。

ウ 設計・開発に関わるメンバーのうち、ArcGIS の設計・開発の経験を有する者を1名以上配置すること。

エ 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

オ 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。

カ 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。

キ　パブリッククラウドを利用する情報システムの要件定義、設計開発等を担当するチームのチームリーダー及び担当メンバーは以下の資格を有するものを含めること。

① チームリーダーは、パブリッククラウドに係る全ての技術領域において当該のクラウドサービスプロバイダーの認定技術者としての上級資格[*1]を有する者を 1 名以上配置すること。

なお、チームリーダーの資格は全体リーダーまたはパブリッククラウド上での情報システム構築期間中に専任でチームリーダーを支援する要員が保有していることでも可とする。なお、体制に前記の資格保有者を準備できない場合、クラウドサービスプロバイダーが提供するサポートサービス（Azure 有償サポート（プロアクティブサービス））を利用することで、クラウドの知見を有するものを配置する体制とすること。

② 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[*2]以上を有する者を 1 名以上配置すること。

例として、以下のような資格が挙げられる。

*1 Microsoft Certified: Azure Solutions Architect Expert

*2 Microsoft Certified:Azure Administrator Associate

（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、Azure のスキル）

（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、必要に応じて担当職員が現地確認を実施することができるものとする。

（4） 作業の管理に関する要領

受注者は、担当部署が承認した設計・開発計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、設計・開発実施要領に従い、コミュニケーション管理、体制管理、作業管理、品質管理、リスク管理、課題管理、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。

6　作業の実施に当たっての遵守事項

（1） 機密保持、資料の取扱い

ア　担当部署から農林水産省における情報セキュリティの確保に関する規則（平成 27 年3

月 31 日農林水産省訓令第4号。以下「規則」という。）、農林水産省における個人情報の適正な取扱いのための措置に関する訓令（平成 17 年 3 月 18 日農林水産省、林野庁、水産庁訓令第1号）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）受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

（オ）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、必要に応じて発注者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。

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農林水産省と協議の上決定し、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、農林水産省の了承を得たうえで実施すること。

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事を確認し、その保証をすること。

エ　受注者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当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、農林水産省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（必要に応じ農林水産省）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　関係法令の遵守

本業務の遂行に当たっては、民法（明治 29 年法律第 89 号）、刑法（明治 40 年法律第 45 号）、著作権法（昭和 45 年法律第 48 号）、不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）等の関係法令を遵守し履行すること。

イ　環境関係法令の遵守

受注者は、役務（委託事業を含む。）の提供に当たり、関連する環境関係法令を遵守するものとする。

・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）

・労働安全衛生法 （昭和 47 年法律第 57 号）

（4）環境負荷低減に係る遵守事項

受注者は、役務の提供に当たり、新たな環境負荷を与えることにならないよう、事業の

最終報告時に様式を用いて、以下の取組に努めたことを、環境負荷低減のみどりのチェック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。

（5）標準ガイドラインの遵守

本業務の遂行に当たっては、「デジタル社会推進標準ガイドライン群」のうち標準ガイドライン（政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント）に該当する以下の①から⑨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。

① DS-100 デジタル・ガバメント推進標準ガイドライン
② DS-310 政府情報システムにおけるクラウドサービスの適切な 利用に係る基本方針
③ DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン
④ DS-670.1 ユーザビリティガイドライン
⑤ DS-680.1 ウェブサイトガイドライン
⑥ DS-680.2 ウェブコンテンツガイドライン
⑦ 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
⑧ 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
⑨ 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

（6）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

開発に当たっては、「山地災害調査アプリケーション　コーディング規約」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　農林水産省は、デジタル庁が整備する「ガバメントソリューションサービス」（以下「GSS」という。）を利用している。設計、構築に当たり、GSS や農林水産省に申請が必要な場合は、定められた様式で申請書等を作成し提出すること。なお、GSS の DNS に設定を行う場合は、デジタル庁 GSS 担当が定めた DNS 設定規則を担当部署から受領して、その内容に基づいて申請書を作成し、担当部署を通じて申請すること。

オ　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。

（7）クラウドサービス利用時の情報システムの保護に関する事項

ア　情報システム、情報システムで取り扱うデータ等の情報資産の所有権その他の権利

がクラウドサービスプロバイダーに帰属せず、また、発注者からクラウドサービスプロバイダーに移転されるものでないこと。

イ　農林水産省の情報システムにおけるクラウドサービスの契約は、農林水産省とカスタマー向け契約及びマイクロソフトクラウド契約（MCA）を締結すること。

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

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

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

（8）情報システム監査

ア　本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために、農林水産省が情報システム監査の実施を必要と判断した場合は、農林水産省が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を受注者は受け入れること （農林水産省が別途選定した事業者による監査を含む。）。

イ　情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担当部署と協議し、指示された期間までに是正を図ること。

（9）セキュリティ要件

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基づき、以下の内容について対応すること。

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改修すること。

カ　利用に当たって必須ではない、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改修すること。

キ　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。

（10）データマネジメント・データ活用要件

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。

（11）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への対応

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」の項目もそれぞれ満たすこと。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。

7　成果物の取扱いに関する事項

（1）知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条まで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 条まで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、納品期日までに農林水産省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、変更点について農林水産省に説明を行った上で、指定された日時までに再度納品すること。

8　入札参加資格に関する事項

（1）競争参加資格

ア　予算決算及び会計令第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

イ　令和7・8・9年度全省庁統一資格の「役務の提供等」の「A」又は「B」の等級に格付され、競争参加資格を有する者であること。

（2） 公的な資格や認証等の取得

ア　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、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。）

（ア） ISO/IEC27001 等の国際規格とそれに基づく認証の証明書等

（イ） プライバシーマーク又はそれと同等の認証の証明書等

（ウ） 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

（3） 受注実績等

ア　入札参加者は、本システムで利用中のパブリッククラウド（Azure）への移行又は構築又は改修を行った実績を過去5年以内に有すること。

イ　入札参加者は、システムで使用しているGISソフトウェア（ArcGIS）製品を有する情報システムの設計・開発業務を行った実績を過去5年以内に有すること。

（4） 複数事業者による共同入札

ア　複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同入札の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

イ　共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

ウ　共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札へ

の参加を行っていないこと。

エ　共同事業体の代表者は、品質マネジメントシステム及び情報セキュリティに係る要件について満たすこと。その他の入札参加要件については、共同事業体を構成する事業者のいずれかにおいて満たすこと。

（5）入札制限

本業務を直接担当する農林水産省 IT アドバイザー（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　再委託ができる業務は、原則として契約金額に占める再委託金額の割合（以下「再委託比率」という。）が 50 パーセント以内の業務とする。

ウ　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。

エ　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。

オ　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。

カ　再委託を行う場合、再委託先が「7（6）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添の再委託承認申請書を農林水産省に提出し、あらかじめ承認を得ること。

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農林水産省に提出し、承認を得ること。

ウ　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を書面で報告すること。

（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、農林水産省は、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 本業務受注後に調達仕様書（別添要件定義書を含む。）の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって農林水産省に申し入れを行うこと。

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

エ 本仕様書に対する質問がある場合においては、次に従い、書面（様式は任意）により提出すること。質問に対する回答は、林野庁ホームページ及び電子調達システムに掲載し公表することがある。

（ア）受領期間 令和8年7月6日から令和8年8月 26 日まで

（イ）提出場所 林野庁国有林野部業務課治山班（農林水産省北別館8階 ドア No. 北 814）

（ウ）その他 書面は持参又は郵送により提出するものとする。

オ 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。

カ 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。

（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、農林水産省内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に担当部署まで連絡の上、閲覧日時を調整すること。

ア 資料閲覧場所

東京都千代田区霞が関 1-2-1 林野庁 国有林野部 業務課 治山班（北別館8階 ドア番号北 814）

イ 閲覧期間及び時間

令和8年7月6日から令和8年8月 26 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3名まで。入札希望者の商号、連絡先、閲覧希望者氏名を別紙4「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、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。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、以下のカの（ウ）の資料についてデータで提供することは可能であるため、必要に応じて申し出ること。

オ　連絡先

林野庁　国有林野部　業務課　治山班　電話　03-3502-8349

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）プロジェクト計画書

（イ）遵守すべき各府省独自の規定類

a　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

b　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

（ウ）現行の情報システムの情報システム設計書、操作マニュアル

（エ）農林水産省クラウド利用ガイドライン及び関係資料

11　附属文書

（1）別紙1　要件定義書

（2）別紙2　情報セキュリティの確保に関する共通基本仕様

（3）別紙3　みどりチェック実施状況報告書様式

（4）別紙4　閲覧申込書

（5）別紙5　守秘義務に関する誓約書

以　上

令和７年度（補正予算）

山地災害調査アプリケーション改修等業務

別紙１　要件定義書

令和８年４月

林野庁

1. 本書の位置付け

本書は、「山地災害調査アプリケーション」（以下「本システム」という。）のシステム要件（システム用途、対象ユーザ、ソフトウェア要件、機能要件、性能要件等）及び運用・保守に関する要件等を定義したものである。

2. 業務要件

本システムは、農林水産省防災業務計画に基づく「被害状況把握・報告」並びに「被害状況の把握と二次災害の未然防止」に迅速に対応するため、現地で取得した山地災害等の被害情報、治山・林道施設の点検情報等を地図データ上で情報共有・管理するための GIS である。

ArcGIS Online 及び ArcGIS Enterprise の2つのプラットフォーム型 GIS を活用し、各種機能により、山地災害への対応の効率化を図るシステムである。

また、本システムは、特に予備知識のない職員においても支障なく利用できるような操作性と業務での利用に支障のない処理速度を備えるものとする。

2.1. 事業の規模

本システムで実現する業務で想定される規模について、以下に示す。以下の内容については、過去の業務実績等に基づく値ではなく、本調達時点の想定に基づく値である点に留意すること

表１　サービスの利用者数及び情報システムの利用者数（想定）

項番	利用者	利用者の種類		主な利用拠点	主な利用時間帯	利用者数	補足
		サービス利用者	情報システム利用者				
1	林野庁職員	－	○	全国	10時間 （8時15分～18時15分） ※通常、土日祝日は休日のため利用しない	約 4,300 人	
2	委託契約 （施設点検） 事業者等	－	○	全国	10時間 （8時15分～18時15分） ※通常、土日祝日は休日のため利用しない	約 14 人	

2.2. 業務実施の時期・時間

(1) 業務実施時期・期間及び繁忙期

本サービスに係る業務実施時期・期間は、原則として開庁日（土日及び祝日、年末年始を除く）とする。本サービスに係る定期的な繁忙期はないが、大規模な山地災害等の発生時は利用者数が急増する可能性がある。

(2) 業務の実施・提供時間

本システムについては、林野庁の責任のもとで運用・保守事業者が運用作業を実施する。なお、本システム

のサービス提供時間、運用時間、システム障害時の対応については以下のとおりである。

ア　サービス提供時間

本サービスは計画停止を除き、24 時間 365 日サービスを提供できること。利用者ごとのサービス提供時間帯は「表 1　サービスの利用者数及び情報システムの利用者数（想定）」に記載の通り。

イ　運用時間

運用・保守業者の運用時間は平日（土日及び祝日、年末年始を除く）の 9 時から 17 時までとする。ただし、システムの監視は 24 時間 365 日行うこと。

夜間や休日におけるシステム障害時の連絡体制については、運用時間と同等の体制を維持することは求めないが、障害の重要性に応じた機動的な体制を提案すること。

ウ　システム障害時の対応

システム障害時は復旧を優先し、一次対応を速やかに実施すること。障害の原因究明・恒久的対策は、原則としてシステム復旧後、翌開庁日の運用時間内にシステム保守として実施すること。

2.3. **場所等**

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。

2.4. **管理すべき指標**

本サービスに係る達成度評価指標（KPI：Key Performance Indicator）を下表に示す。なお、本サービスの利用動向を踏まえ、必要に応じて更に KPI を追加または変更する場合がある。KPI の追加または変更により「2.4.（8）　モニタリング対象データ一覧」および「3.16.（5）　主な運用作業一覧」に変更があった場合は、対応範囲を林野庁と協議の上で決定、対応すること。

表　2　達成度評価指標（KPI：Key Performance Indicator）

項番	指標の種類	指標名	計算式等	単位	目標値	計測方法	計測周期
1	情報システム効果指標	ユーザ満足度	システム利用者の利便性に関する満足度	%	R８：50%	職員を対象としたアンケートを実施する	年１回
2	業務効果指標	職員の山地災害調査アプリの利用割合	利用実績のあるアカウント（ArcGIS Online ライセンス）の割合	%	R８：40%	システムのログにより確認する。	年１回
3	業務処理時間の削減	災害速報において、山地災害調査アプリを活用した件数の割合	災害速報のうち、山地災害調査アプリを活用した件数の割合	%	R８：20%	災害速報より集計	年１回

2.5. 業務の継続の方針等

「第４非機能要件（可用性・継続性）」に記載のある要件を満たすこと。

2.6. 情報セキュリティ

本要件定義書、調達仕様書を満たすこと。

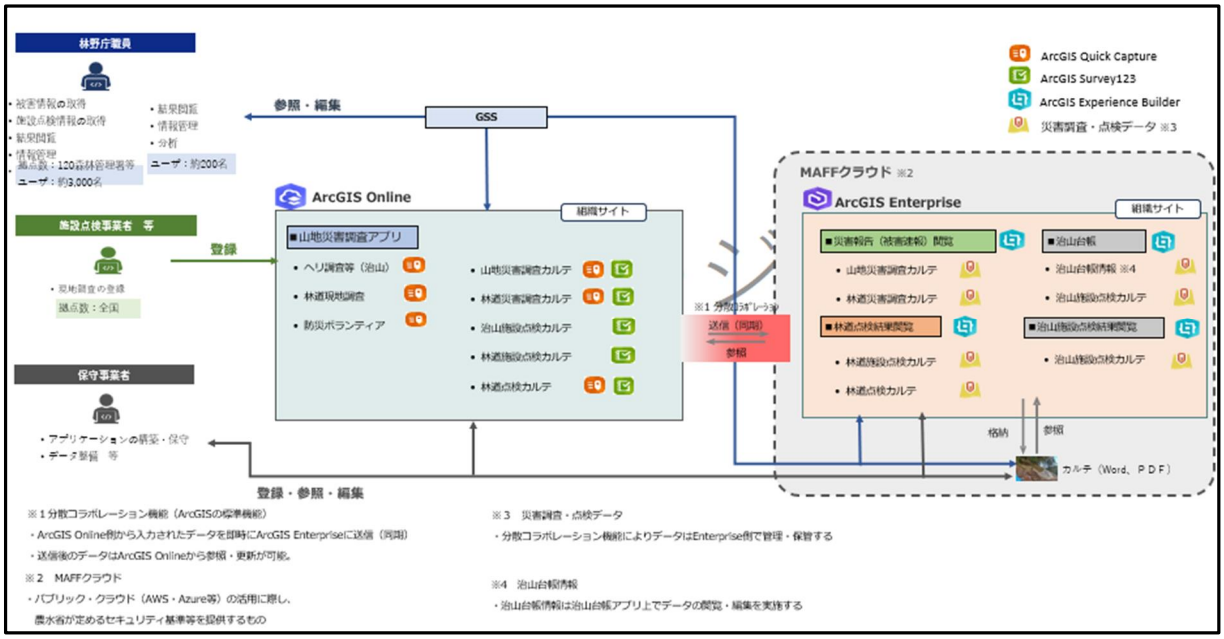
あわせて、情報システムの構築において、府省庁が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁が情報セキュリティ監査の実施を必要と判断した場合は、受注者は情報セキュリティ監査を受け入れること。

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。

2.7. 情報システムの稼働環境に関する事項

クラウドサービスの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件等について記載する。

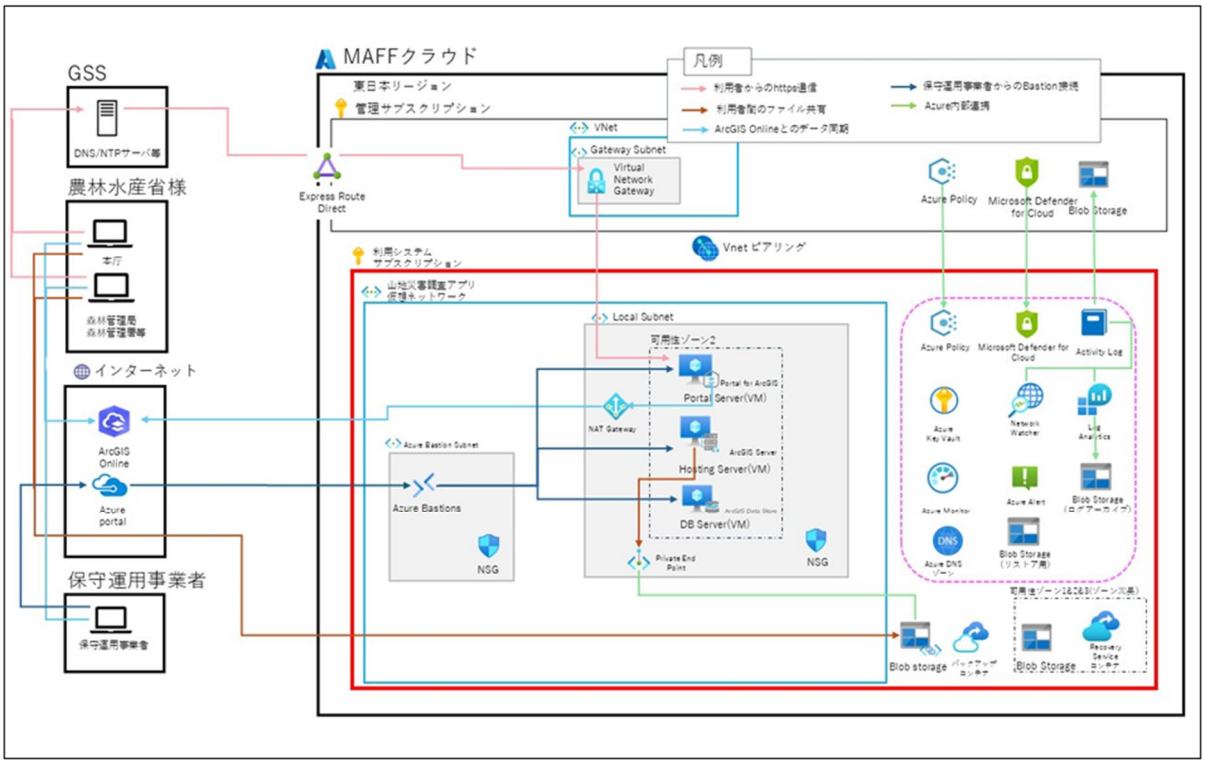
図 1 システム概要図



(1) システム構成

本システムの本番環境の構成図を以下に示す。

図２　システム構成図



(2) クラウドサービス構成

本システムのクラウドサービス構成を下表に示す。なお、速やかに本番同等の環境を構築できるように、インフラの設定は Infrastructure as Code にて構成し、環境変更時にはその変更をメンテナンスできるようにすること。

表２　クラウドサービス構成

項番	クラウドサービス	補足
1	Activity Log	アクティビティログ（Azure Monitor）
2	Azure Alert	アラート（Azure Monitor）
3	Azure Application Gateway	アプリケーションゲートウェイ
4	Azure Automation	オートメーション
5	Azure Backup	バックアップ
6	Azure Bastions	VM へのリモート接続用サービス
7	Azure Blob Storage	オブジェクトストレージ
8	Azure Files	ファイルストレージ
9	Azure Key Vault	暗号化キーの保管・管理サービス
10	Azure Monitor	ログ監視・分析、アラート
11	Azure Policy	ポリシー定義
12	Azure Private DNS Zone	プライベート DNS
13	Azure WAF	WAF
14	Log Analytics	ログ分析（Azure Monitor）
15	Microsoft Defender for cloud	クラウド セキュリティツール
16	NAT Gateway	NAT サービス
17	Network Wacher	リソース監視
18	NSG	NSG
19	Private Endpoint	プライベート IP エンドポイント
20	Recovery Service コンテナー	バックアップ用ストレージコンテナー
21	Subnet	サブネット
22	Virtual Machines	仮想マシン
23	Virtual Network	仮想ネットワーク
24	Azure Storage Explore	ストレージ管理

・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、2024 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。

(3) ソフトウェア構成

本サービスの構築に当たっては、可能な限りクラウドサービス提供のサービスを活用すること。また、いずれのソフトウェアについても、原則として最新バージョンを適用する。クラウドサービス外に準備するソフトウェアを下表に示す。

表３　ソフトウェア一覧

項番	ソフトウェア分類	ソフトウェア名	ソフトウェア要件
1	ミドルウェア：Web サーバー	Portal for ArcGIS	プロセッサ：4 コア メモリ/RAM：8GB 以上 ディスク容量：2TB 以上
2	ミドルウェア：アプリケーションサーバー	ArcGIS Server	メモリ/RAM：8GB 以上
3	ミドルウェア：DB サーバー	ArcGIS Data Store	メモリ/RAM：8GB 以上
4	ミドルウェア：DB サーバー	PostgreSQL	プロセッサ：4 コア メモリ/RAM：GB 以上 ディスク容量：20GB 以上
5	アプリケーション	ArcGIS Pro	プロセッサ：2 コア メモリ/RAM：32GB 以上 ディスク容量：32GB 以上
	アプリケーション	ArcGIS License Manager	メモリ/RAM：2GB 以上 ディスク容量：119GB 以上
	アプリケーション	ArcGIS Web Adaptor (Java Platform)	Apache Tomcat 9.0.x /10.1.x
	アプリケーション	Apache Tomcat	プロセッサ：2 コア メモリ/RAM：4GB 以上 ディスク容量：500 MB 以上 Java 8 以上

拡張及び更新や事業者間での引継ぎが妨げられることがないよう十分に配慮すること。

(4) 利用端末の要件

本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS・ブラウザの考え方について、以下に示す。

ア　本システムの運用開始時点で動作保証の対象とする PC・スマートフォン・OS の機種やバージョンを下表に示す。

表４　動作保証対象とする利用端末

項番	端末	OS	バージョン
1	PC	Windows	10/11

イ　本システムの運用開始時点で動作保証の対象とするブラウザは以下とする。

・　PC（Mac OS/Windows） の場合：Microsoft Edge/Mozilla Firefox/Google Chrome/Safari の最新バージョン

3. 機能要件定義

本システムの機能、業務フロー図、画面に関する事項、データに関する事項は、別紙1に示す

4. 非機能要件定義

4.1. ユーザビリティ及びアクセシビリティに関する事項

(1) 情報システムの利用者の種類、特性

本システムの利用者の種類、特性について、下表に示す。

表 1 情報システムの利用者の種類、特性

項番	利用者区分	利用者の種類	利用イメージ	特性
1	林野庁職員	内部利用者	本システムのアプリケーションを用いて、山地災害や施設点検調査を実施、管理等を行う。	利用者については、毎年一定数入替わることから、分かりやすいユーザーインタフェースを考慮する必要がある
2	委託契約（施設点検）事業者等	外部利用者	本システムのアプリケーションを用いて、山地災害や施設点検調査を実施、管理等を行う。	利用者については、毎年一定数入替わることから、分かりやすいユーザーインタフェースを考慮する必要がある

(2) ユーザビリティ要件

「表５ 情報システムの利用者の種類、特性」に示す役割・業務内容に基づき、各利用者の特性を十分に留意する。また、利用者が想定する流れに沿った操作手順、画面遷移、画面レイアウト、帳票レイアウト等とする。

表６ ユーザビリティ要件

項番	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成（直感・シンプル）	・ 利用者が何をすればよいか直感的に理解できるデザインにすること。 ・ 無駄な情報、デザイン、機能を排したシンプルでわかりやすい画面にすること。
2	画面の構成（フォント及び文字サイズ）	・ 十分な視認性のあるフォント及び文字サイズを使用すること。 ・ 画面サイズや位置を変更できること。 ・ 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成（マルチデバイス対応）	・ スマートフォン、タブレット端末により本サービスを利用する利用者を想定し、これら端末の特性を考慮した画面にすること。 ・ レスポンシブデザインにより、PC、タブレット端末、スマートフォン等の利用環境を問わず、同一の情報をグリッドレイアウト等の適切なレイアウトにより表示できるようにすること。
4	画面の構成（表示/非表示）	・ 情報の優先順位をつけ、重要度の低い情報、特定の利用者層に対して提示する情報は、利用者が必要に応じて表示/非表示を切替え可能とする等の工夫をすること。
5	画面の構成（クリックやチェックができる箇所）	・ 画面上でクリックやチェックができる箇所とできない箇所の区別を明確にすること。 ・ タップ操作が可能なタブレット端末やスマートフォンの場合は、タップ操作の結果（どの部分をタップしたのか）を適切にレスポンスできること。
6	画面遷移	・ 利用者が次の処理を想像しやすい画面遷移とすること。 ・ 無駄な画面遷移を排除し、シンプルな操作とすること。

項番	ユーザビリティ分類	ユーザビリティ要件
7	画面表示・操作の一貫性（統一）	・ 機能、用語、レイアウト、操作方法は統一すること。
8	画面表示・操作の一貫性（視認性）	・ 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利用者が認識できるようにすること。 ・ 見やすさを考慮し、画面のフォントサイズを決定すること。 ・ 画面ごとに異なるフォントを使わないこと。
9	操作方法のわかりやすさ	・ 無駄な手順を省き、使いやすく、利用者が効率的に作業できるようにすること。 ・ 利用者が操作しやすい手順にするため、画面上の情報項目を上から下へ、左から右へ流れる順番に配置すること。 ・ 利用者の操作を軽減できるよう、画面の初期表示時、入力項目、選択項目等に適切な既定値を設定すること
10	操作方法のわかりやすさ（操作説明）	・ 原則としてマニュアルを参照しなくても操作できるようにすること。
11	操作方法のわかりやすさ（Tab キー）	・ Tab キー等による画面上のフォーカスの移動順序について、利用者が操作しやすい順序となるようにすること。
12	操作方法のわかりやすさ（画面遷移）	・ 利用者が同じ情報の入力や操作を何度も行う必要がないよう、画面が遷移しても情報がその後の手順に反映されるようにすること。 ・ 利用者の手間を軽減するため、利用者の手順に即した画面遷移に留意し、可能な限り不要な画面遷移を行わないようにすること。
13	操作方法のわかりやすさ（マルチデバイス対応）	・ スマートフォン、タブレット端末等の狭い表示領域、タッチインタフェースでも効率的に作業できる操作性を実現すること。
14	指示や状態のわかりやすさ	・ ユーザーインタフェース及び UX に関する一般的に使われているデザイントレンドを取り入れ、アイコン・図表のグラフィック表現を適切に適用すること。 ・ 本サービスが処理している内容や状況を、利用者が把握できるようにすること。
15	指示や状態のわかりやすさ（外部ドメインへの遷移）	・ ドメインを異にする他の Web サイトへの遷移を行う際は、離脱メッセージを表示する等、利用者が認識できるようにすること。
16	メッセージ出力	・ 利用者に分かりやすいメッセージとすること。 ・ 必要に応じて、登録・変更・削除等の操作を行う場合には、確認画面等で表示し、利用者の注意を促すこと。 ・ 処理時間がかかる操作では、処理中であることが分かるようにすること。
17	メッセージ出力（次の操作）	・ 指示メッセージは、次操作が具体的にイメージできるようなメッセージ出力を行うこと。
18	エラーの防止と処理	・ 利用者が操作や入力を間違えないデザインや案内を提供すること。
19	エラーの防止と処理（エラー防止）	・ 利用者の誤操作を想定し、入力チェック機能によりエラーを防止すること。 ・ 入力値が選択できる場合には、プルダウンメニュー等を活用し、極力キーボード入力操作をなくすこと。
20	エラーの防止と処理（エラーメッセージ）	・ エラーメッセージは、その内容が分かりやすく表示されるとともに、利用者が何をすればよいかを示すこと。
21	エラーの防止と処理（エラー表示と解決策）	・ 入力内容の形式に問題がある項目については、利用者がその都度該当項目を容易に見つけることができるようにすること。 ・ エラーが発生した時は、利用者が迷わずに問題解決できるよう、操作の続行に必要な選択肢を利用者が適切に理解できるようわかりやすく提示すること。 ・ 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、利用者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。
22	エラーの防止と処理（確認画面）	・ 必要に応じて、登録、更新、削除等の処理の前に確認画面を用意し、利用者が行った操作や入力のやり直し、取り消しがその都度できるようにすること。 ・ 重要な処理については、事前に注意喚起し、利用者の確認を促すこと。
23	エラーの防止と処理（画面遷移）	・ 入出力の過誤があった場合、次の画面へ遷移しないこと。
24	エラーの防止と処理（情報保持）	・ タブレット端末等、屋外での使用を考慮し、電波受信状況の悪い場所においても操作不能とならないよう工夫すること。

項番	ユーザビリティ分類	ユーザビリティ要件
25	ヘルプ	・ 利用者が必要とする際に、ヘルプ情報やマニュアル等を容易に参照できるようにする。 ・ ヘルプ情報やマニュアル等についても、利用者が必要な情報を容易に検索できるようにする。
26	デザイナーによる UI/UX 検討	・ 本システムで開発するスマホアプリの UI/UX 検討に当たっては、利用者の利用動機に着目し、サービスデザイン思考の観点から検討を行うこと。 ・ UI/UX 検討に当たっては、民間スマホアプリ等の経験を有する専門の UI/UX デザイナーを体制に組み入れること。
27	画面遷移、操作ログ等の分析	・ 運用・保守工程において継続的に UI/UX の改善を検討できるよう、利用者の画面遷移、操作ログ等を分析できる仕組みを整備すること。

(3) アクセシビリティ要件

アクセシビリティに関する要件を下表に示す。

表 7　アクセシビリティ要件

項番	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	・ 広く国民に利用され公益性の高い情報システムであるため、日本産業規格 JIS X8341 シリーズ、「みんなの公共サイト運用モデル」（総務省）に準拠し、以下を前提とすること。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html ・ JIS X 8341-3:2016「高齢者・障害者等配慮設計指針 – 情報通信における機器，ソフトウェア及びサービス – 第 3 部：Web コンテンツ」の適合レベル AA に準拠することを目標とする。また、レベル AAA のうち、以下の達成基準についても可能な範囲で適用すること。 ➢ 2.1.3 キーボード（例外なし）の達成基準 ➢ 2.3.2 3 回のせん（閃）光の達成基準 ➢ 2.4.8 現在位置の達成基準 ➢ 3.2.5 要求による状況の変化の達成基準 ・ 注記：本仕様書における「準拠」という表記は、情報通信アクセス協議会 Web アクセシビリティ基盤委員会「Web コンテンツの JIS X 8341-3:2016 対応度表記ガイドライン（令和 3 年 4 月版）」で定められた表記による。 ・ また、スマートフォン等での操作を行うユーザーが増えていることを踏まえ「Web Content Accessibility Guidelines （WCAG） 2.1」で追加された達成基準についても、可能な範囲で適用すること。 ➢ 1.3.4 表示の向き（レベル AA） ➢ 2.5.1 ポインタのジェスチャ（レベル A） ➢ 2.5.2 ポインタのキャンセル（レベル A） ➢ 2.5.4 動きによる起動（レベル A） ➢ 4.1.3 ステータスメッセージ（レベル AA） ・ デジタル庁が整備する「ウェブアクセシビリティ導入ガイドブック」を参考にすること。
2	指示や状態の分かりやすさ	・ 色の違いを識別しにくい利用者（視覚障がいのかた等）を考慮し、利用者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。ただし、業務の利用用途から、画面色での振り分けを行うことを予定していることから、適用範囲及び配色については林野庁及び関係省庁と協議し、決定すること。 ・ Web ブラウザ等の音声読み上げ機能を活用し、視覚障がいの方でも問題なく利用可能な UI とすること。
3	マルチデバイス対応	・ 解像度の低い機種、画面サイズの小さい機種でも、業務継続が可能な UI とすること。 ・ OS の設定でフォントサイズ・表示サイズをそれぞれ最大とした場合でも、業務継続が可能な UI とすること。 ・ スタイルシートを利用しないユーザーと利用するユーザーにおいて得られる情報に差

		（表示されない文字や画像がある等）がないこと。レイアウトにおいても大きな差がないことが望ましい。

4.2. **システム方式に関する事項**

(1) システム方式についての全体方針

システム方式についての全体方針を下表に示す。本システムはクラウドネイティブの構成として、「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（以下、「クラウド方針」という。）」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。特に、信頼性、拡張性（スケーラビリティ）、継続性等の向上に寄与するクラウドサービスと構成を選定すること。
使用する IaaS/PaaS はガバメントクラウドを原則とし、SaaS についても積極的に活用すること。

表 8　システム方式についての全体方針

項番	観点	全体方針
1	システムアーキテクチャ	・ 本システムのシステムアーキテクチャはクラウドサービス上に用意される Web アプリケーションから構成される。Web アプリケーションは利用者の端末に追加的なソフトウェアのインストール等を行うことなく、一般に利用されている Web ブラウザで処理を行うものとする。 ・ 本システムや業務機能等の特性を十分に検討し、クラウドサービスプロバイダが提供するリファレンスアーキテクチャに準拠した形で PaaS、SaaS、IaaS 等の最適なサービスを採用し、システムを構築する。 ・ クラウドサービスプロバイダが提供するマネージドサービスを最大限活用することを基本とし、アプリケーションプログラムの作り込みを削減できる設計とする。特にデータベース、認証、セキュリティ機能や運用管理機能はクラウドサービスが提供する機能を最大限活用すること。 ・ クラウドサービスが責任共有モデルとして提供されている前提を踏まえ、クラウドサービスを利用するに当たって必要となる考慮事項について検討を行い、安全かつ効率的にシステムを構築する。 ・ 予防的統制と発見的統制を実施すること。また、クラウドサービスを利用するために作成する各種アカウントについては、ガバナンスやセキュリティに係るポリシーを設定の上で、権限管理を確実に行うこと。管理者アカウントについては、多要素認証を必須とすること。多要素認証はハードウェア方式を原則とするが、ソフトウェア方式も許容する。ハードウェア方式の場合は対応するワンタイムパスワード用のデバイスを利用システム側で調達すること。 ・ リソース使用量の変動等に柔軟に対応するとともに、コスト削減を図るため、民間クラウドサービスの利用を原則とする。 ・ 全体構成及び利用するクラウドサービスについては、受注者において移行、引き継ぎ、確実なサービス提供等について問題が生じないことをクラウドサービスプロバイダに応札前に確認し、本調達の要件を踏まえ、確認結果と合わせて適切なものを提案する。
2	アプリケーションプログラムの設計方針	・ マイクロサービスアーキテクチャ、API、クラウドネイティブ、クラウドサービスのマネージドサービスのみによる構成等、モダン技術を前提として構築する。 ・ クライアントサーバ方式、専用端末のシンクライアント（VDI）等の旧来技術は、高コスト化の要因となるため採用しないこと。 ・ 原則としてバッチ処理を採用せず、リアルタイム処理を基本とすること。バッチ処理が必要となる場合は、その理由について林野庁の承認を得た上で採用すること。 ・ 情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする。

		・システムが取り扱うデータの保管・管理に際して、データの容量、更新頻度、保存期間等を考慮し最適なストレージサービスを選定の上、利用する。またデータの保管・管理方針が変更となった際に、ストレージサービス間でのデータの移行が容易となるよう設計上考慮する。
3	ソフトウェア製品の活用方針	・SaaS については、開発量削減の観点から幅広く優先的に、その利用を検討すること。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。 ・ソフトウェア製品については、広く市場に流通し、利用実績を十分に有するものを活用する。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、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。 ・ノンプログラミングによる画面生成等プロトタイピング用のツール等を利用することにより、システムライフサイクルコストの削減等が見込める場合には、積極的に採用を検討する。

(2) クラウドサービスの選定、利用に関する要件

ア　本システムで用いるクラウドサービスは、MS Azure（東京リージョン）とすること。

イ　要機密情報を取り扱うクラウドサービスの選定、利用に関しては、「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　（令和 5 年度版）」の「4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）」「4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）」の内容を遵守すること。

ウ　情報資産を管理するデータセンタの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。

エ　契約の解釈が日本法に基づくものであること。

オ　クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

カ　林野庁の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方についてはクラウド方針を参照すること。なお、利用者がアクセス可能な部分を除き、国外から情報資産へアクセスする場合も日本国外への持ち出しに該当する。

キ　障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。

ク　情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、林野庁が要求する任意の時点で情報資産を他の環境に移管させることができること。

ケ　SaaS サービスの選定に関する参考事項

・　SaaS ベースで構築することを前提に検討し、SaaS では要件を満たさない場足は、PaaS、IaaS などを選択すること。なお、本調達で構築するシステムでは、比較的短期間での機能の追加が求められることが想定されることから、簡易な操作で機能の追加が可能であること。

・　今後、利用者の拡大が見込まれることから、今後の発行アカウント数の拡大時の安定稼働や運用費用の抑制等の観点から、本調達の趣旨に適したクラウドサービスを利用すること。

コ　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。

サ　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

シ　クラウドサービスに係るアクセスログ等の証跡を保存し、林野庁からの要求があった場合は提供すること。

ス　インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線とクラウド基盤との接続点の通信を監視すること。

セ　クラウドサービスの提供に関する次のいずれかの認証を取得していること。
・　ISO/IEC 27017:2015

4.3. **システム規模に関する事項**

本サービスの規模要件を以下に示す。また、本サービスの規模に関する業務要件は、「２.１業務の規模」を参照のこと。

(1) 規模に関する前提条件

本システムはクラウドサービスを利用して運用されるため、以下の取り組みを行うこと。

ア　運用期間中において利用予定範囲を超過することがないよう、システムの縮退を検討するために必要となる情報収集等の仕組み（クラウドサービスの課金状況やリソースの利用量の監視、一定の閾値を超えた場合のアラート処理等）を設けること。定量的に計測したデータについては、ダッシュボード等による状況の可視化を行うこと。また、リソース利用状況に基づいたリソース見直しを行う点に留意し、情報収集の仕組みについても修正可能とすること。

イ　クラウドサービスのマネージドサービスを効果的に活用し、コスト削減を継続的に図ること。原則としてサーバレスの構成を取ることとするが、インスタンスを利用してサーバを立てる場合は、サーバのスペック等を適切な範囲に調整してコスト削減を継続的に図ること。（オートスケールを利用する場合の変更条件・上下限値等を含む。）

ウ　リソース確保の方式（リザーブドインスタンス、スポットインスタンス等）についても検討すること。

(2) データ量

本システムで想定されるデータ量を下表に示す。なお、年間データ増加量は仮定をおいた上での試算結果を記載しているため、設計等を考慮の上、必要なデータ量のサイジングを行うこと。

表９　データ容量（想定）

No	種類	登録先（想定）	データ容量（GB）	備考
1	フィーチャレイヤー	ArcGIS Enterprise	1.4	治山施設、林道の位置情報及び属性情報等

2	タイルレイヤー	ArcGIS Enterprise	0.4	全国林小班タイル
3	画像	Azure	4,640	治山台帳、施設点検情報のデータ

(3) 利用者数

本システムで想定される利用者数を下表に示す。

表 10 利用者数

項番	利用者区分	利用者数	補足
1	林野庁職員	・利用者総数：約 4,300 人 ・同時アクセス可能人数約 120 人 ・利用時間帯 8 時 15 分～18 時 15 分 ※通常、土日祝日は休日のため利用しない	
2	委託契約（施設点検）事業者	・利用者総数：約 14 人 ・同時アクセス可能人数約 7 人 ・利用時間帯 8 時 15 分～18 時 15 分 ※通常、土日祝日は休日のため利用しない	

本システムの想定利用者数及び「４.4 性能に関する事項」で求める性能目標を考慮の上、必要スペックのサイジングを行うこと。

(4) 保管データ量・保管期間

本サービスに保管するデータ量やデータの保管期間については、要件の整理の中で調査を行い、林野庁と協議の上、決定すること。

4.4. 性能に関する事項

本サービスの性能要件を以下に示す。下記の性能要件を踏まえて、本サービスの業務処理の特徴を考慮し、業務処理のピーク時においてもレスポンスの低下等を招かないように、十分な処理性能を確保すること。

なお、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。

(1) 性能を考慮する対象

ア 性能目標の設定対象

性能目標の設定対象は本システムの Web サーバにリクエストが到着した時点からレスポンスを返す時点までとする。ブラウザ、ネットワーク部分での処理時間に関しては、性能目標の設定対象外とする。

イ 性能見積もり

本サービスのアプリケーション処理時間に係る性能見積りは、以下を考慮する。

- アプリケーション又はコードの起動に要する時間、アプリケーション又はコードの実行時間、データベースアクセスに要する時間に要素分解を行った上で実施すること。
- 各画面・機能等の利用者体験を踏まえた余裕を見込むこと。

(2) 応答時間

目標時間を満たすトランザクションの割合を「遵守率」とし、その目標値を設定すること。ピーク時の遵守率は80%とする（80%以上のトランザクションがレスポンスタイム処理目標時間を満足する性能であること。なお、障害等による縮退運転時並びにネットワーク遅延等の受注者の責によらない遅延は除外する。）

レスポンスタイムは、画面を表示するための要求を行った時（ボタン等を押下した時）から画面が全て表示されるまでの時間を指す。

表 11 目標レスポンスタイム

項番	指標名	目標値	補足
1	参照系処理	10 秒	画面の読み込み、情報の表示に関する処理
2	更新系処理	10 秒	情報の登録、更新、削除に関する処理

4.5. **信頼性に関する事項**

本サービスに備える機能の停止等による業務への影響を最低限にとどめるため、クラウドサービスの利用を前提として、以下に示す要件を踏まえ本サービスの信頼性を確保すること。

(1) 可用性要件

単一障害点（SPOF）を極力排除するとともに、サーキットブレーカーパターンなども検討し、一律ではなく機能又はセグメントの特性に応じた合理的な提案を示すこと。また、SPOF の発生が避けられない場合においてそれら稼働状況を管理する仕組みを準備すること。

ア 可用性に係る目標値

可用性に係る目標値を下表に示す。

表 2 可用性に係る目標値

項番	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ・ 接続回線の計画停止時間 ・ 大規模災害等の天災地変に起因する停止時間 ・ 連携するサービス又はクラウドサービスまたはスマートフォン端末の通信キャリアの障害・計画停止・緊急メンテナンス等に起因する停止時間 ・ 本サービスのメンテナンスによる計画停止時間
2	稼働率	99.9%以上	本サービスにおける稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x 100 当該計算式において、年間実稼働時間は「利用者がサービスを利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間及び大規模災害による停止・縮退時間を除いた時間の合計」とする。

イ 可用性に係る対策

本サービスの可用性を確保し、前述に示した稼働率を遵守するため、以下に示す要件に基づく対策を行うこと。

・ クラウドサービスの利用を前提として、本サービスを構成するサーバ、ネットワーク機器及びネットワーク

経路を冗長化し、単一障害点（SPOF）を回避すること。

- クラウドサービスの利用を前提として、フェールソフトの観点から、障害が発生したコンポーネントを切り離すことによりサービス全体を停止せずに運用可能とすることを考慮する。そのために各種障害発生時の影響を回避又は局所化し、原則として自動縮退運用に対応すること。
- 本サービスに係る運用・保守上の人的ミスに起因する障害が本サービスの可用性に影響を与える事態を未然に防止するため、「3.16 運用に関する事項」及び「3.17 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。
- 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。
- 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 3 日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。

(2) 完全性要件

以下に示す要件を踏まえ、本サービスの完全性を確保するための対策を行うこと。

ア　クラウドサービスの利用を前提とし、以下の対策を講ずること。

- コンポーネントの故障に起因するデータの減失や改変を防止する。
- 異常な入力や処理を検出しデータの減失や改変を防止する。

イ　システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。ログの出力に当たっては、システム稼働環境（本番環境、検証環境等）別に出力するログのレベル（ERROR、WARNING、INFO、DEBUG 等）の設定を可能とすること。
なお、ログの保管期間は 1 年間とする。

4.6. **拡張性に関する事項**

(1) 性能及び機能の拡張性

ア　基本方針

本システムの利用率の増加、データ量の増加等により、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正等により機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

イ　マネージドサービスなどの活用

本サービスはクラウドサービスを利用する想定としている。本サービスの構築に当たっては、当該クラウドサービスをマネージドサービスなど可能な限り活用することにより、処理能力等の動的調整を実現することとし、業務量及び処理能力の拡張性については特段の拡張性要件を定義しない。

ウ　機能の追加

機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。

本サービスは、連携業務アプリケーションとの一層の連携など、拡張性を備えたシステム・サービスであ

ることが求められる。連携機能等の拡張が必要になった際に拡張が容易となるような構成をとること。

エ　コンポーネントの再利用性・拡張性

アプリケーションやインフラの設計に当たっては、将来の拡張時に効率良く対応ができるように、設定情報の外部化や一元化、機能の共通化等に努めること。特にスマホアプリについては、様々な利用者が広く利用することが想定されるため、特定のスマートフォン端末、OS のバージョン、ミドルウェア等に可能な限り依存しない設計とすること。

オ　モニタリングと定期的な報告

本システムの運用に当たっては、定期的な運用報告において定期的にサーバコア数やディスク、メモリ、ネットワークの帯域などの使用状況等を確認すること。またリソースの増加の必要性が見込まれる場合は、リソースの増強の必要性の有無を判断できるような形で林野庁に報告を行うこと。

カ　割り当て変更

業務量の増加減に伴い、これらリソースの割り当てを動的に行えるようにし、林野庁の指示に基づきリソースの割り当てを変更すること。

4.7. 上位互換性に関する事項

(1) 上位互換性

クラウドサービスの活用を踏まえ、OS、サーバソフトウェアのバージョンアップ又は変更に備え、本サービスを構成する。

ア　クラウドサービスのバージョンアップ

システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

イ　OS 等への依存

原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェア等の特定バージョンに依存する場合は、その利用を最低限とすること。

ウ　クライアント端末の更新

クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

(2) 業務分担

本システムを構成する機器・ソフトウェアの更新、バージョンアップの必要性が生じた場合は、各事業者がそれぞれの担当範囲において影響調査、対応策の検討を実施することとしている。

ア　アプリケーション保守事業者は、業務アプリケーションへの影響調査、対応策の検討を実施する。

イ　運用事業者は、システム基盤の影響調査、対応策の検討を実施する。

ウ　機器・ソフトウェアの更新、バージョンアップの対象が持ち込みソフトウェアの場合は、運用事業者が実施する影響調査、対応策の検討を機器・ソフトウェア賃貸借・保守事業者が支援する。

4.8. **中立性に関する事項**

(1) オープンな標準的技術又は製品の採用

本サービスを構成するサーバ、ソフトウェア、アプリケーションとして、市場で広く利用されている製品群及びクラウドサービスが提供する標準サービスを除き、原則として特定事業者の技術に依存しないオープンな技術仕様に基づくものを選択すること。

ア　データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

- 情報システム内のデータについては、原則として XML や CSV 等の標準的な形式で取り出すことができるものとすること。
- パッケージ製品から抽出されたデータであっても、移行データフォーマットや移行データの権利は林野庁に所属すること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）を文書化すること。文書については、情報システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当文書の内容に変更が生じる場合は継続して改定を行い最新化できること。
- 移行データに関する文字コード等は以下に従うこと。

  - 取り扱う日本語文字集合の範囲： JIS X 0213
  - 文字コード： ISO/IEC 10646
  - 文字の符号化形式： UTF-8

- 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。

イ　オープンソースソフトウェア（OSS）活用

ソフトウェア又はアプリケーションについてフレームワークを活用する場合は、可能な限りオープンソースソフトウェアとして提供されているフレームワークを選定すること。

ウ　オープンなインタフェースの活用

本サービスを構成するサーバ、ソフトウェア等は、原則として仕様が公開された API 等のインタフェースを選定すること。

4.9. **継続性に関する事項**

本サービスの停止等に際しても必要最低限の業務を継続（又は回復）するため、以下に示す要件を踏まえ、本サービスの継続性を確保すること。

(1) 継続性に係る目標値

以下に、機能停止等の原因となる事象の規模に応じて継続性に係る目標値を示す。

ア　予測可能な障害発生時

予測できる障害（一時的な過負荷等）については、あらかじめ業務停止を回避するための対策を講ずること。また、単一障害発生時は業務停止せずに処理継続可能であること。

イ　業務停止を伴う障害発生時

予測困難な事象により業務停止を伴う障害が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を下表に示す。

表 13　継続性に係る目標値（業務停止を伴う障害発生時）

項番	設定対象	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	山地災害調査アプリケーション	24 時間以内	通常どおりのサービスレベルに復旧	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）

ウ　大規模災害発生時

インターネット等通信インフラが被災しておらず、発災前と同様の通信環境が確保されていることを前提として、大規模災害による業務停止が発生した場合の目標復旧時間（RTO）、目標復旧レベル（RLO）及び目標復旧時点（RPO）を下表に示す。

表 14　継続性に係る目標値（大規模災害発生時）

項番	設定対象	目標復旧時間（RTO）	目標復旧レベル（RLO）	目標復旧時点（RPO）
1	山地災害調査アプリケーション	2 週間以内	通常どおりのサービスレベルに復旧（機能面は通常レベル、性能面では通常の半分のレベルの復旧とする）	停止前の最新バックアップ状態へ復旧（ただし、アーカイブログを取得しているデータは障害発生時点への復旧を可能とする。）

(2) 継続性に係る対策

本システムの継続性要件を実現するために、以下の対策を講じること。

ア　冗長化

各構成要素について、故障等を検知した際、クラウドサービスの利用を前提として自動的に予備の環境へ切替える等、適切に冗長化を行い、特定の部分の障害によりシステム全体が停止してしまうようなSPOF（単一障害点）を極力排除するよう、設計時に配慮すること。

イ　災害対策

災害対策環境の事前準備等によるシステム上の対策及び非常時の運用体制や切替え手順の整備等による運用上の対策を行うことで、業務継続を可能とすること。

災害発生後に本番環境が正常に稼働できる場合は、災害対策環境から切り戻しができるよう連携先システムと調整しておくこと。

ウ　アベイラビリティゾーン

アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とする。しかし頻繁に AZ 間の通信が発生するアプリケーションについては、AZ 間のレイテンシが増幅し性能に影響を与える可能性がある。これらの性能面の影響を評価できるよう、設計・開発期間中の早い段階で性能面の影響を評価し、必要に応じてアプリケーション改修等の手段で性能改善への対応方針を確立すること。

エ　データバックアップ

・　バックアップ対象

　データバックアップに当たっては、本サービスの稼働に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグ等に起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

・　バックアップ頻度

　バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR：Point In Time Recovery/Restore を保存する等の対応を行うこと。

・　保存期間

　万一の障害発生に備え本サービスの稼働に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

・　アクセス権限

　バックアップしたデータの保管場所にはアクセス権限を付与し、管理者以外がアクセスできないようにすること。

・　データの隔地保管

　「3-2-1 ルール」（2012 年に米国土安全保障省サイバーセキュリティ・インフラストラクチャー・セキュリティ庁の US-CERT が提唱）に示されている「データはコピーして 3 つ保有（プライマリー1 つ、バックアップ 2 つ）、2 種類の異なる記録媒体に保管、コピーのうち 1 つは遠隔地に保存」という方針を十分に理解した上で、データのバックアップについて万全を期した対応を行うこと。クラウドサービス上のスナップショットやレプリカだけではこの要件に十分対応できないので、バックアップとして永久増分と重複排除を積極的に活用し、ISMAP 管理基準が求める暗号化を行った上で、別リージョンのオフサイトに隔地保管すること。

・　バックアップツール

　バックアップ対象、頻度、バックアップデータへのアクセス権限及び保存期間といったバックアップポリシーを一元的に管理できる機能を持った、クラウドサービスプロバイダが提供するバックアップサービスをできるだけ利用すること。なお、個別データの復旧にはデータベース等の PITR：Point In Time Recovery/Restore を実現できることが望ましい。

オ　システムバックアップ

　クラウドサービスのマネージドサービスにおけるバックアップ機能を有効に活用すること。なお、インスタンスを利用してサーバを立てる場合のバックアップ方式は、バックアップ＆リストア、コールドスタンバイ、ウォームスタンバイ、マルチサイトの 4 つのディザスタリカバリ方式のうち、目標復旧時間から考えて、コールドスタンバイ以上の構成を想定している。

　「表 36　継続性に係る目標値（業務停止を伴う障害発生時）」及び「表 37　継続性に係る目標値（大規模災害発生時）」に示す RTO、RLO、RPO を満たすようにすること。

カ　システム障害時の業務継続

システム障害時も一部業務は継続出来るよう対策を検討すること。
【継続すべき業務】
データ参照業務
【対策】
データベースのバックアップを別環境に保存し、クライアント PC 等から参照、ダウンロード等が出来るようにする。

4.10. 情報セキュリティに関する事項

(1) セキュリティ対応方針
セキュリティ要件を決定するためのシステム特性や特に対処すべきセキュリティリスク、セキュリティ対応方針を下表に示す。

表 3 当該システムにおけるセキュリティ対応方針

項番	分類	概要
1	原則	・ 「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」、「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」に準拠した情報セキュリティ対策を講ずること。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」は非公表であるが、「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」に準拠しているので、必要に応じ参照すること。「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」の開示については、契約締結後、受注者が農林水産省に守秘義務の誓約書を提出した際に開示する。 ・ セキュリティ対策については、高度化/大規模化するサイバー攻撃等に対応するため、多層防御やサイバーレジリエンス強化といった原則に基づいて要件を定義する。
2	システム特性（概要）	【システムの利用者】 ・ 当該システムは林野庁職員、委託契約（施設点検）事業者が活用する。一日に数人程度の利用者が想定される 【システムで取り扱う情報】 ・ 個人情報、利用者の収入に関わる要配慮情報に相当する情報は取扱われない ・ 特定個人情報は取扱われない 【使用環境・ネットワーク構成】 ・ 林野庁職員、委託契約（施設点検）事業者は PC、スマートフォンからンターネットを介して ArcGIS Online にアクセスし、ログインして各種機能を使用する ・ 林野庁職員は PC から内部ネットワークを介して ArcGIS Enterprise にアクセスし、ログインして各種機能を使用する ・ システム管理者は管理用 LAN を介して当該システムにアクセスし、システム管理を実施する ・ 外部システムとの接続はなし
3	優先的に対処すべきセキュリティリスク	【優先的に対処すべきセキュリティリスク】 ・ サービス妨害を目的とした攻撃等によりシステムが長時間停止する。
4	セキュリティ対応方針	【セキュリティ要件のベースライン】 ・ 本システムにおいては、セキュリティ要件を過不足なく導出するため、NISC の提供する SBD マニュアルをセキュリティベースラインとして利用する 【優先的に対処すべきセキュリティリスクへの対応方針】 ・ 上記の優先的に対処すべきセキュリティリスクについては、多層防御の観点で発生確率を抑えるとともに、発生時の範囲を極小化するような対策を実施する。 ・ 外部からの不正アクセス対策として不正ログイン対策、脆弱性対策を徹底するとともに、攻撃やインシデントの兆候を早期検知できるような仕組みを導入する。 ・ サービス妨害を目的とした攻撃対策については、L3～L7 層で対策可能な仕組みを導入

		する。 【その他セキュリティリスクへの対応方針】 ・　・上記以外のセキュリティリスク（内部不正や人為的ミス等に起因するもの、サプライチェーンに起因するもの等）についても発生時影響は看過できないことから、予防的な対策だけでなく早期検知するための対策を実施し、リスクを低減する。

(2) セキュリティ要件

ア　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 3 日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。

ウ　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やアプリケーションの通信を通信回線上にて遮断する機能を備えること。

エ　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。

オ　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。

カ　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や感染拡大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。

キ　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 年の期間保管すること。

ク　ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。

ケ　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。

コ　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林野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

サ　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林野庁職員及び委託契約（施設点検）事業者の認証を行う機能として、個人を特定できる方式を採用すること。

シ　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。

ス　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。

セ　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すること。

ソ　機器等の製造工程において、林野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。

タ　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。

チ　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。

ツ　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。

テ　情報の漏えいを防止するため、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。

ト　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。

ナ　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。

ニ　情報システムの構築において、林野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、林野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。

ヌ　クラウドアーキテクトのベストプラクティス（Azure の場合 Azure Well-Architected Framework）及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 別冊クラウド設計・開発編」に準拠すること。

ネ　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。
・別表２　AWS/Azure 設定確認リスト

ノ　農林水産省ドメイン（maff.go.jp）のサブドメインについては、農林水産省のドメイン管理ルールに従い命名等を行うこととし、農林水産省の指示に従うこと。

ハ　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。
・別表３　Web システム／Web アプリケーションセキュリティ要件書

ヒ　受注者は、別紙「山地災害調査アプリケーション 開発標準」を元に、本システムを設計・開発すること。

受諾者は、開発の各工程において、本セキュリティ要件に則ってセキュリティ対策がもれなく実装されていることを検証する方法を定め、要件のトレーサビリティを確保することが求められる。

開発工程以降、セキュリティ対策を具体化する過程でセキュリティ上の懸念が発生した場合は、本要件のみに縛られず、必要に応じて追加のセキュリティ対策を講じること。また、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（政府情報システムにおける セキュリティ・バイ・デザインガイドライン（digital.go.jp）） 」の記載内容（要求事項、実施内容、重要なセキュリティ対策の考え方）に従い、各工程でのセキュリティ対応状況について抜け漏れを確認して是正すること。加えて、デジタル庁「政府情報システムにおける脆弱性診断導入ガイドライン」の 4 付録 A を参考にシステムの脆弱性が作りこまれないように留意すること。

4.11. 引継ぎに関する事項

受注者は、他の事業者が本システムの次期の運用等を受注した場合には、次期運用事業者に対し、引継を行うこと。現時点で想定する引継ぎ要件を以下に示す。

(1) 引継ぎ計画書の作成

本システムの関連事業者に対する引継ぎの開始前に、本システムの引継ぎに係る引継ぎ対象、引継ぎ体制、引継ぎ内容、引継ぎ方法、引継ぎスケジュール、理解度確認方法、完了条件等を記載した「引継ぎ計画書」

を作成し、林野庁の承認を得ること。

(2) 引継ぎ方法

ア　受注者は、「引継ぎ計画書」に従い、十分な時間的余裕を持って、必要な運用引継ぎを行うこと。その際は、引継ぎ対象者の理解度を確認し、必要な場合には、「引継ぎ計画書」に記載したスケジュール等の変更を行うこと。

イ　本サービスは、その保守や将来の拡張等の業務を他事業者に引き継ぐことが可能であること（引き継ぎのために必要となる各種ドキュメントを整備する等）。第三者による保守性を向上させるため、成果物等は標準的に利用されているドキュメント作成ソフトウェアを用い、編集可能な形式で納品すること。

ウ　ドキュメントには設計結果のみを記載するのではなく、設計根拠等も明示し、検討経緯を可視化すること。

エ　並行稼働期間中（引継ぎ期間中）における当該システムの運用・保守事業者からの問合わせにも対応すること。

オ　期間内に引継ぎが完了しない場合は、原則として受注者の責任と負担において引継ぎを完了すること。

(3) 引継ぎ対象

本システムの引継ぎ対象を下表に示す。なお、引継ぎに際しては林野庁の指示に基づき書面又は電子媒体で行うこと。

表 16 本システムの引継ぎ対象

項番	引継ぎ先	引継ぎ内容	引継ぎ手順	補足
1	次年度山地災害調査アプリケーション運用・保守事業者	・ ソースコード（テスト・構成管理・環境構築等に利用するコード含む） ・ 開発環境に必要となる各種ツール ・ 各種設計書・ドキュメント類 ・ 運用課題（管理簿） ・ 仕様課題（管理簿） ・ インシデント状況（管理簿） ・ 連携業務アプリケーション対応状況（管理簿） ・ ヘルプデスク作業 ・ 各種運用・保守作業 ・ その他成果物一式 （クラウドサービスの管理に必要なアカウントや鍵情報、また IaC（Infrastructure as Code）に基づくシステム構築・管理等に係る構成管理ファイル等情報を漏れなく含む）	受注者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。	

(4) クラウドサービスを利用する場合の引継ぎ

本システムでは、本調達の契約期間終了後も、クラウドサービスの契約期間終了前に契約の延長又は他の引継ぎ先事業者（運用・保守事業者を想定）への引継ぎ等を行うことで、クラウドサービスをそのまま継続利用することを想定している。引継ぎに際しては、必要に応じて引継ぎ先事業者及びクラウドサービスプロバイダとの

間で書面による契約等を行い、しかるべく管理者権限の引渡し等を行うこと。

(5) 引継ぎ結果報告書の作成

引継ぎ作業の完了時に、本システムの、他事業者等への引継作業の実施結果について記載した「引継ぎ結果報告書」を作成し、林野庁へ報告を行うこと。

(6) 前任事業者からの引継作業

受注者は、本業務を実施するために必要な情報について、引継元である前任の運用・保守事業者からの引継ぎを受けること。引継ぎ完了後は、受注者が引継ぎ完了報告書（確認者、確認日時、完了条件の適合性等を記載）を作成し、林野庁の承認を得ること。

4.12. 運用に関する事項

現時点で想定する運用要件を以下に示す。

(1) 運用・保守計画

運用・保守の設計で検討した内容を踏まえて、以下の要件が含まれる形で運用・保守計画書及び運用・保守実施要領の確定版を作成すること。

表 17 運用・保守計画書の記載内容

項番	項目	補足
1	作業概要	・ 監視、運用・保守作業の対象範囲、管理対象、作業概要等を記載する。
2	作業体制に関する事項	・ 運用・保守業務を実施するための体制について、管理体制図、本件受注者の要員（責任者、作業者、役割分担）、連絡手段等について記載し、全体的な運用管理体制を明確にすること。
3	スケジュールに関する事項	・ プロジェクト計画書及び調達仕様書に基づき、運用・保守を行う上で基本とする作業内容、関係するほかの作業工程、そのスケジュール等について記載すること。 ・ 日次、週次、月次等の定型的な業務について、作業内容を記載すること。 また複数回発生した非定型業務の報告及びその定形業務化（手順書の作成等）の提案を含めること。 ・ 年次の作業内容には、運用業務の中で発生した運用上の課題、作業量の多い作業等について整理報告し、その改善（例えば自動化等）の提案を行う作業、情報システム運用継続計画の見直し作業、運用・保守計画書の見直し作業を含めること。
4	成果物に関する事項	・ 運用・保守業務にて納品する成果物の内容、担当者、納品期限、納品方法、納品部数等について記載する。
5	運用・保守形態、運用・保守環境等	・ 運用において採用する運用形態（オンサイト、リモート等）、運用環境（本番環境、検証環境、研修環境等の有無）等を記載する。こと。
6	管理対象	・ 受注者は本業務で開発する山地災害調査アプリケーション及びドキュメントについて保守を行うこと。
7	クラウドサービスの利用	・ 運用作業、運用手順及び運用管理用のソフトウェアも含め、可能な限り統一化を図るとともに、自動化された機能及びクラウドサービスが提供する機能等を利用し、運用に係る役務を可能な限り効率化すること。 ・ 利用しているクラウドサービスの機能や性能等に変更が発生した場合、受注者側でクラウドサービスの変更に伴う開発中システムへの影響を確認し、システムの改修が必要な場合は、原則対応すること。ただし、改修規模が大きい又は影響範囲が広い場合は林野庁と協議の上対応を検討・実施すること。
8	サービスレベル	・ 運用・保守業務で達成目標とするサービスレベル項目及びサービスレベルを林野庁が協議の上、決定すること。 ・ 運用におけるリソース使用状況に基づき、毎年のリソース計画を策定する。月間の運用実績を評価し、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、サービスレベル達成状況の改善に向けた対応策を提案すること。
9	その他	・ 上記に掲げる事項のほか、運用・保守を行う上での前提条件、時間、予算、品質等の制約条件等について記載する。

表 4 運用・保守実施要領の記載内容

項番	項目	補足
1	コミュニケーション管理	・ 運用・保守業務を実施する上で必要となるコミュニケーション手段について、会議体（会議体 名称、開催目的、開催スケジュール、出席者、報告内容等）、インシデント発生時 の報告ルート等について記載し、効率的かつ円滑なコミュニケーションを実現すること。
2	体制管理	・ 運用・保守に携わる事業者における作業体制の管理手法等について記載する。
3	作業管理	・ 運用・保守作業及びその品質の管理手法等について記載する。
4	リスク管理	・ 運用・保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載すること。
5	課題管理	・ 運用・保守において解決すべき問題について、発生時の対応手順、管理手法等について記載すること。
6	システム構成管理	・ 運用・保守における情報システムの構成（ハードウェア、ソフトウェア製品、アプリケーションプログラム、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の管理手法等について記載すること。
7	変更管理	・ 運用・保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載すること。
8	情報セキュリティ対策	・ 運用・保守における情報漏えい対策等について記載すること。

(2) 運用・保守準備

運用・保守に当たって、以下の準備作業の実施等を行うこと。

ア 監視設定

運用業務を効率的に実施するため、監視、アラートについて、システムの特性、各種アラート発生時の重要度に応じたチューニング（マッチング文字列、閾値、アラート検知結果の重要度など）を行い、定量的な計測に基づいて監視を行うこと。また、アラートの通知先、通知手段等は林野庁と協議の上、決定すること。

イ バックアップサービス

サービスの故障復旧に必要なデータのバックアップを定期的に取得すること。また、故障復旧時における必要なデータのリストア作業の手順、役割分担等を事前に決定し、故障発生時には実施すること。

ウ 運用・保守手順書

運用・保守実施要領及び運用・保守計画書に基づき、運用・保守手順書を作成すること。

(3) システム稼働要件

本システムの本番稼動に係る要件は「2.2 業務実施の時期・時間」を参照すること

(4) 主な運用作業一覧

現時点で想定する主な運用作業の一覧について、以下に示す。以下の内容を基に、本システムの設計及び開発時に、運用・保守計画書、運用・保守設計書及び運用・保守マニュアルの案を作成すること。

表 19 主な運用作業一覧

項番	運用作業の分類	主な運用作業の内容
1	パッチ適用	・ 保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼働確認を

項番	運用作業の分類	主な運用作業の内容
		行う。
2	ログ管理業務	・ 操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログを取得すること。 ・ ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ・ 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。
3	ジョブ管理業務	・ ジョブの登録・更新、ジョブの起動スケジュール（カレンダー）を登録し、ジョブの実施結果を確認、報告する。 ・ 林野庁が必要性を認めた際は、林野庁の指示に従い、ジョブの手動実行を行う。
4	システム監視	・ サービスの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性等で分類した上で、メールなどにより自動で通知する仕組みを構築すること。監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）、外形監視（当該システムを利用するユーザーと同じ方法でアクセスし正常に動作しているか監視する方式）等 ・ 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直し等が必要な場合は、林野庁の承認を得た上でこれに係る設計を行い、対応を実施すること。※システムサイジングについても定期的に分析を行い、林野庁の承認を得た上で見直すこと。
5	問題管理	・ 本サービスに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度及び優先度を定め、根本原因の調査及び解決策の立案を行うこと。
6	変更管理	・ 課題管理機能の活用を前提として、適切な変更管理を実施すること。 ・ 構成要素を追加、変更又は廃棄する場合は、変更依頼書を起票すること。
7	リリース管理	・ 林野庁とリリース作業の日程、作業内容、依頼事項等の調整を行い、実施の計画をリリース計画書に記載すること。 ・ リリースを実施した際、リリースに関する情報を「リリース管理台帳」にて管理すること。 ・ 「リリース管理台帳」には以下の項目を管理し、履歴を確認することとし、その管理が必要な項目についても管理する仕組みとすること。 ➢ 実施計画の内容 ➢ リリーステストの実施有無及び結果 ➢ リリース時期 ➢ 各種レビューの実施有無及び結果 ➢ リリース内容 ・ リリース計画書については、リリース予定日より十分な期間を確保の上、前もって林野庁の承認をもって提出すること。なお、緊急なリリースを要する場合は林野庁と協議すること。
8	システム構成管理	・ 本システムに係る全ての構成品目について、適切な構成管理を実施すること。 ・ システム構成管理対象を特定し、管理レベルを定めること。なお、システム構成管理対象は、本システムを構成するクラウドサービス、ソフトウェア製品、ソフトウェアのバージョン、アプリケーションプログラム、通信回線、公開ドメインのほか、本システムの運用・保守に係る全ての文書及びデータとすること。ただし、本システムの外部から提供を受けるものであり、運用・保守において変更を行わないものは、システム構成管理の対象外とする。 ・ システム構成管理対象の変更について、変更履歴を追跡可能であること。 ・ 本番環境・検証環境の維持管理を行うこと。 ・ 本システムのアプリケーションは CI ツールで管理すること。
9	バックアップ	・ システムバックアップ、データバックアップを取得すること。 ・ 必要に応じてシステムリストア、データリストアを実施すること。
10	業務支援	・ 林野庁の指示に基づき、利用者の利用状況のデータを集計し、林野庁に定期的に報告すること。 ・ 必要に応じて、データベースやディレクトリ等に施されるアクセス制御の設定変更を実施すること。 ・ 運用に必要な端末は受注者が用意すること。

項番	運用作業の分類	主な運用作業の内容
		・ ヘルプデスク担当者からの問合せ、またはサービスデスクからの問合せに対する FAQ を作成すること。
11	障害対応	・ 障害発生時は、発生から解決までの一連の作業（受付、問題判別、業者間調整、調査解析、修復方法の検討、障害原因アプリケーションの再設計・製造・試験、再発防止・品質向上作業、報告書作成・報告実施、アプリケーション保守環境反映）を行うこと。 ・ 本システムの連携先システムにおいて障害が発生し、業務影響が発生した場合においても、連携先システム担当が実施する原因調査、代替策、解決策の検討及び処置を必要に応じて支援すること。 ・ システム障害と想定される連絡を受け付けた際、別途、林野庁より指示する担当者へ速やかにエスカレーションすること。 ・ 府省内担当者との応答内容の記録を残すこと。
12	ヘルプデスク業務	・ 本サービスの利用方法に関する問合せの受付からクローズまでを一元管理するヘルプデスクを設け、本サービス利用者からの問合せを受け付けること。 ・ 問い合わせの要件は以下に示す。 ➢ 受付時間・方法：「２.２業務実施の時期・時間」に記載 ➢ 平均処理時間：1 時間/件 ➢ 平均応答速度： 3 営業日/件 ➢ 一年の問い合わせ想定量：20 件 ・ ヘルプデスク担当者のスケジューリング等の運営を適切に行うこと。 ・ ヘルプデスク担当者による対応手順、サービスレベル等を統一するため、ヘルプデスク運用マニュアルを作成し、林野庁の承認を得ること。 ・ ヘルプデスク運営の中で FAQ は適宜追加、更新等、メンテナンスを行うこと。 ・ 受け付けた問合せは、質問、インシデント、サービス要求、作業依頼等に分類した上で、対応日時、問合せ元、内容、回答状況等とともに記録すること。なお、具体的な運用方法については、本サービスの設計開始以降に改めて検討する。 ・ 問い合わせ記録は受付件数、問い合わせ者情報、問い合わせ内容、回率、回答に要した期間、回答内容等を適切な粒度で整理した上で、定期的に問題発生状況を分析し、必要な対応を行うこと。 ・ 運用・保守の計画及び実施状況について、林野庁の定める報告様式に従って取りまとめ、林野庁に報告を行うこと。（原則、月次での報告）
13	設計・開発事業者による報告・問合せ対応	・ 問合せに関する調査完了後、ヘルプデスクへの回答を行うこと。 ・ その他、適宜、林野庁と必要に応じて密に連携を図り、ヘルプデスクの円滑な運営に資すること。
14	インシデント管理	・ 情報セキュリティインシデントが発生した場合は、「運用・保守実施要領」等に定めた手順に従ってインシデント対応を行うこと。対応に当たっては、林野庁、関係事業者と適宜調整の上で対応を行うこと。
15	バージョンアップ対応	・ 保守におけるバージョンアップ対応要否の判断結果に基づき、バージョンアップ対応を実施し、稼働後の動作確認を行うこと。
16	大規模災害等対応訓練	・ 大規模災害等への対応訓練を行うこと。 ➢ 大規模災害対応訓練シナリオ見直し 本番運用・保守の計画で定義されている訓練シナリオ・手順書を適宜見直し、必要に応じて、設計・開発事業者に確認を依頼すること。訓練シナリオ・手順書を変更した場合は、林野庁の承認を得ること。 ➢ 大規模災害対応訓練の実施 受注者は、大規模災害発生時から復旧に係る作業について、林野庁及び関係する事業者が迅速かつ適切に作業を実施できるよう、年に 1 回、訓練シナリオ・手順書に基づき、訓練を実施すること。実施に当たっては、主に連絡ルートの確認を実施し、結果を「大規模災害等対応訓練完了報告書（本番運用開始後）」に記載し、林野庁に報告すること。なお、訓練への参加は、受注者と林野庁のみとし、他事業者や外部連携システムは対象外とする。 ・ 情報漏洩への対応訓練を行うこと。

項番	運用作業の分類	主な運用作業の内容
		➢ 情報漏洩対応訓練の実施 受注者は、情報漏洩等に係る情報セキュリティインシデント対応について、林野庁及び関係する事業者が迅速かつ適切に作業を実施できるよう、年に 1 回、訓練シナリオ・手順書に基づき、訓練を実施すること。実施に当たっては、主に連絡ルートの確認を実施し、結果を「情報漏洩等対応訓練完了報告書（本番運用開始後）」に記載し、林野庁に報告すること。なお、訓練への参加は、受注者と林野庁のみとし、他事業者や外部連携システムは対象外とする。
17	運用改善	・ 受注者は、システムの状況を林野庁が定期的に把握できるように仕組みを整えること。 ➢ プロジェクトの目標とする指標、システムの利用者の利用状況 ➢ クラウドのリソース等、システムの利用状況・コストの発生状況 ・ システムの利用状況については、少なくとも以下の項目および「2.4.（8） モニタリング対象データ一覧」に記載した項目を実施し、利用状況の分析とその後の改善策に資する項目を含めること。 ➢ 運用管理・保守業務の作業別の所要時間 ➢ 自動化や効率化が可能と思われる作業の洗い出し ➢ システム及び運用・保守業務の改善提案 ・ アイドリングなどの無駄／過剰なリソースを発見し、コスト削減につながる仕組みを整え、アドバイスも指摘すること ・ 受注者は、システムの利用拡大や利便性向上のため、実績に基づいた定量的なデータや利用者からの問合せ内容等を分析し、多くの利用者が操作方法に迷う部分や誤操作を誘発する部分を把握した上でシステムの改善策を検討すること。また林野庁と協議の上、システムの改善を実施すること。
18	サービスオペレーション支援	・ 本サービスが動作するに当たり、必要となるデータベースの各種マスタ情報を維持管理すること。また、マスタ情報管理のための GUI を具備しないマスタ情報の場合、変更依頼を前提として情報の登録、検索、更新、削除のための SQL を作成し、これを実行すること。 ・ 計画停止、保守作業、障害対応等により利用者への影響が生じる場合、本サービスの Web サイトにお知らせを掲載するなどの方法により周知連絡を行うこと。 ・ 作業影響を生じる範囲について、不測の運用障害を回避する観点から、メンテナンス機能を利用してサービス閉塞・閉塞解除運用を実施すること。 ・ アプリケーションの障害を防ぐため、システムメンテナンスの一環として、サーバを定期的に再起動する。再起動後はサービスの動作確認等を行い、問題が無いことを確認すること。再起動のタイミングは林野庁と協議の上、決定すること。
19	情報セキュリティ監査	・ 林野庁が情報セキュリティ監査を実施する場合がある。その際はセキュリティ監査事業者との調整・ヒアリングへの協力を行うこと。
20	アカウント管理	・ アカウントの利用状況の棚卸を実施すること。実施するタイミングは、年 1 回程度を想定しているが、具体的な時期については林野庁と協議の上、決定すること。
21	その他業務	・ サーバ証明書の更新、ドメインの管理等を行うこと。

なお、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

4.13. 保守に関する事項

受注者は、運用・保守計画書及び運用・保守実施要領に基づき以下の作業を適切に実施すること。

(1) 保守業務の実施

保守業務として以下を実施すること。

ア　問合せの受付時間は、「２.２業務実施の時期・時間」に記載の通りとする。ただし、林野庁が緊急かつ業務に支障を来すと判断した場合はこの限りではない。

イ　受け付けた問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。

ウ　障害について対応したときは、障害報告書を作成し、林野庁に報告すること。

(2) 保守設計

保守設計として以下を実施すること。

ア　役割分担の整理

役割分担を行う際に以下の点に留意すること。

- 保守業務の設計に際し、受注者の責任範囲及びクラウドサービスを含めた関連事業者間の役割分担を整理すること。
- 新システムがクラウドサービス上で稼働することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。

イ　クラウドサービスの利用

クラウドサービスを利用する際に以下の点に留意すること。

- 保守設計を実施する上で、クラウドサービスの標準機能を可能な限り活用すること。
- クラウドサービスによる自動化等により、省力化を実施すること。
- 運用・保守実施要領、運用・保守計画書及び運用・保守手順書については、クラウドサービスが提供する各サービスを活用することにより、作業のみならずドキュメント類についても効率的に作成すること。
- 利用するクラウドサービスにおいて、提供サービスの仕様上必要となるアップデートパッチの適用やメンテナンス等の対応に際して、システムへの影響度に鑑み、林野庁と協議の上対応を行うこと。または、自動適用を行う等の対応が可能となるよう、必要な仕組み（検知、適用、等）を準備すること。

(3) アプリケーションの保守

アプリケーションの保守として以下を実施すること。

ア　インシデント管理

運用管理・監視等作業におけるインシデント管理と適切な連携を図ること。

イ　是正保守

アプリケーションに起因した障害発生時、監査指摘事項への対応時等、アプリケーションの是正が必要な場合に、是正保守を行うこと。

ウ　適応保守

OS、ブラウザ、ミドルウェア等のバージョンアップ対応等、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。

エ　予防保守

本サービスのアプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合又はアプリケーションコンポーネントについて新たに脆弱性が報告された場合に、予防保守を行うこと。

オ　改善措置

上記イ～エに伴う改善措置を実施する際には以下の点に留意すること。

- 国民等の利用者に影響がある保守作業を実施する場合は、アプリケーション保守の実施効果、現在及び将来の利用者に対する影響の分析を行うこと。
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性等の改善が必要な場合に、対処を行うこと。
- Web 解析結果に基づき、本サービスのユーザーインタフェースについて、ユーザビリティ又は UX に関する課題を識別した場合、課題解決に資する是正保守、予防保守を行うこと。
- Web サーバ、データベース等について、「表 57 主な運用作業一覧 17 運用改善」の結果を踏まえ、必要に応じて稼働環境の改善等に伴う設定変更を実施すること。

カ　根本原因の分析

根本原因を分析する際に以下の点に留意すること。

- 是正保守及び予防保守の実施に当たり、障害、監査指摘、潜在する問題等に係る根本原因の分析を行うこと。

キ　検証

修正したアプリケーションを本番環境へ展開（デプロイ）する前に、修正が適切に実施されているか否かについて検証環境において検証すること。

ク　文章の修正

アプリケーション保守に伴い、ドキュメント（設計書、マニュアル等）の修正を要する場合は、速やかに修正を行うこと。なお、改修等に伴い画面等に発生する変更が軽微な場合は、ドキュメントの更新方針等について別途林野庁と協議すること。

(4) クラウドサービスの保守

クラウドサービスの保守として以下を実施すること。

ア　利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応について林野庁と協議し、パッチ適用要否を判断すること。

イ　クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、林野庁と協議し、適用等の可否を決定すること。なお、実施することとなったバージョンアップに伴う機器・サービス等の停止は計画停止に準ずるものとして扱う。また、バージョンアップに起因して改修が必要な場合には、対応について別途林野庁と協議すること。

ウ　クラウドサービスで利用している環境の最新化や更新は、原則として IaC（Infrastructure as Code）を活用しコードを変更し、変更後のコードを実行することにより実施すること。

エ　修正パッチ適用やバージョンアップ等を行う場合には、事前に検証環境において本サービスの運用に影響が生じないことを十分に検証し、環境更新の事前評価を実施すること。

(5) ソフトウェア保守

ソフトウェアの保守として以下を実施すること。

ア　ソフトウェア最新化

本サービスを構成する全てのソフトウェアについて、製品不具合や情報セキュリティに関する脆弱性を修正するため、林野庁と協議の上、ソフトウェア実行環境の形態に応じてソフトウェアを最新化すること。

イ　修正プログラム

修正プログラム適用の際は以下の点に留意すること。

・　情報セキュリティや安定稼働の観点から緊急性が高いと考えられる修正プログラムについては、緊急適用を計画すること。緊急性が低い修正プログラムについては、定期保守作業の中での適用を計画すること。

・　使用しているクラウドサービスの内容に変更が発生する際には、クラウドサービスより提供する情報を元にシステムへの影響範囲を調査の上、修正プログラムの適用可否を林野庁へ報告すること。適用が必要と判断された場合、クラウドサービスより提供されるソフトウェアに対する修正プログラムの適用作業を実施すること。

ウ　検証・デプロイ

検証・デプロイを行う際は以下の点に留意すること。

・　ソフトウェア保守に当たっては、事前に検証環境において本サービスの運用に影響が生じないことを十分に検証すること。

・　ソフトウェア保守に伴い、本サービスの安定稼働に影響が生じる事態が予測される場合、林野庁の指示に基づいてデプロイ実施の是非を判断すること。

エ　設計書への反映

ソフトウェア保守によりソフトウェア構成に変更が生じた場合、設計書等へ変更内容を反映すること。

オ　保守条件

保守条件は、「製品の導入や使用方法」、「製品の互換性や相互操作性」、「製品資料の解釈」、「構成サンプルの提供」、「修正策の情報提供」、「製品プログラム、製品コードに起因する障害」等の保守が提供されることを想定しているが、最終的な保守条件は、林野庁と調整の上、保守設計において決定すること。

(6) 保守実績の評価及び改善

保守実績の評価及び改善として以下を実施すること。

ア　本サービスの運営に関わる関係者間で本サービスの保守に係る情報や問題認識を共有し、保守業務の品質を継続的に維持・向上させること。

イ　本システムが使用するアプリケーション、クラウドサービス、ソフトウェア等の保守実施状況について、日々の保守業務の中で収集する定量的な管理指標を定め、林野庁と合意すること。

ウ　ログ解析機能等を活用し、指標値の収集、評価及び管理を効率的に行うこと。

エ　管理指標の達成状況を評価し、未達の場合は原因分析を行い、改善措置を検討すること。また、これらの実績、評価、改善措置について、定期報告すること。

オ　ログ解析機能、Web 解析機能の活用を前提として、モニタリング及び運用過程を通じて得られた利用状況を分析することにより、ライフサイクルコスト低減の観点から、利用するクラウドサービスの所要量及びソフトウェアライセンスの削減可能性を検討すること。また、利用状況の実績、評価、コスト削減可能性について、定期報告すること。

(7) ドキュメントの保守

設計・開発関連ドキュメント及び運用・保守関連ドキュメントが、受注者の契約期間において、最新の状態であるよう維持・更新等を行う。

（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

みどりチェック実施状況報告書

事業名	令和７年度（補正予算）山地災害調査アプリケーション改修等業務
事業者名	
担当者・連絡先	

以下のア～エの取組について、実施状況を報告します。

ア　環境負荷低減に配慮したものを調達するよう努める。

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

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

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

具体的な事項	実施した／努めた	左記非該当
・事業実施時に消費する電気・ガス・ガソリン等のエネルギーについて、帳簿への記載や伝票の保存等により、使用量・使用料金の記録に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、不要な照明の消灯やエンジン停止に努めている。	□	□

・事業実施時に使用するオフィスや車両・機械等について、基準となる室温を決めたり、必要以上の冷暖房、保温を行わない等、適切な温度管理に努めている。	□	□
・事業実施時に使用する車両・機械等が効果的に機能を発揮できるよう、定期的な点検や破損があった場合は補修等に努めている。	□	□
・夏期のクールビズや冬期のウォームビズの実施に努めている。	□	□
・その他（　　）		

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

ウ　廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

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

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

エ　みどりの食料システム戦略の理解に努める。

具体的な事項	実施した／努めた	左記非該当
・「環境配慮のチェック・要件化（みどりチェック）チェックシート解説書 －民間事業者・自治体等編－」にある記載内容を了知し、関係する事項について取り組むよう努める。	□	□

・事業者として独自の環境方針やビジョンなどの策定している、もしくは、策定を検討する。	□	□
・従業員等向けの環境や持続性確保に係る研修などを行っている、もしくは、実施を検討する。	□	□
・その他（　　）		

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

【別紙４】閲覧申込書

林野庁国有林野部業務課
　治山班　宛

閲覧申込書

「令和７年度（補正予算）山地災害調査アプリケーション改修等業務」に係る資料閲覧を申請します。

申込日：　令和　　年　　月　　日

１　　会 社 名：

２　　住　　所：

３　　部署名・担当者名：

４　　電話番号：

５　　E-mail アドレス：

６　　閲覧日時：第１候補日　令和　年　　月　　日　　時　　分～　　時　　分
　　第２候補日　令和　年　　月　　日　　時　　分～　　時　　分
　　第３候補日　令和　年　　月　　日　　時　　分～　　時　　分

７　　閲覧者氏名：
　　：
　　：
　　：
　　：

【別紙５】守秘義務に関する誓約書

林野庁国有林野部業務課
　治山班　宛

守秘義務に関する誓約書

「令和７年度（補正予算）山地災害調査アプリケーション改修等業務 」に係る資料閲覧に当たり、下記の事項を遵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。）を本調達の目的以外に使用、又は第三者に開示、若しくは漏洩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　本業務に係る調達の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、情報の開示、漏えい若しくは使用した場合、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

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

（別表２）

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

（別表３）

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