

資料招請説明書

下記委託事業の別添仕様書案にかかる資料提供及び意見の招請にあたっては、以下のとおりとします。

1 件名

令和8年度グローバル産地づくり推進委託事業（「GFP」WEBコンテンツ運用・保守・機能向上業務事業）

2 仕様書案の説明会

- (1)開催日時 令和8年1月6日(火) 15時00分
- (2)開催場所 農林水産省輸出・国際局第5会議室(本館7階、ドアNo.本735)(オンライン参加も可能とする。)
※説明会への参加を希望する場合は下記3(3)提出先記載のメール宛に令和8年1月5日(火)15時00分までに連絡すること。

3 意見の提出方法

- (1)招請する資料等
- ア 仕様書案に対する意見及び参考資料
(意見提出は別添の様式を使用すること。)
 - イ 仕様書案及び意見に基づく参考見積
(参考見積の内訳は、任意の様式に仕様書(案)の「3. 作業の実施内容」に基づく、「(4)機能向上内容」の各項目の見積もりについて、人件費、数量、単価、金額、消費税等が分かるように記載すること。)
- (2)意見の提出期限 令和8年1月13日(火) 17時00分
(郵送の場合は必着のこと。)
- (3)提出先 〒100-8950 東京都千代田区霞が関1-2-1
農林水産省輸出・国際局輸出支援課輸出産地形成室
(本館4階 ドアNo.本459)
電話:03-6738-7897(直通)
メールの場合:gfp_1/atmark/maff.go.jp
(注)スパムメール対策のため、「@」を「/atmark/」と表示しているので、送信の際は「@」に変更してください。
- (4)提出様式 意見提出は別添様式、参考見積は任意様式とする。

意見提出様式

令和 年 月 日

件名：令和８年度グローバル産地づくり推進委託事業（「GFP」WEBコンテンツ運用・保守・機能向上業務事業）

（事業所）
住所
商号又は名称
代表者等責任者

（担当者）
所属
役職
氏名
電話番号
メールアドレス

No	資料名	頁	仕様書の該当記載内容	分類 (意見/質問)	意見/質問内容	意見/質問の理由
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

令和8年度グローバル産地づくり推進委託事業
(「GFP」WEB コンテンツ運用・保守・機能向上業務事業)
仕様書案

農林水産省輸出・国際局輸出支援課輸出産地形成室

目次

1	事業の概要	4
	(1) 業務名	4
	(2) 業務の背景と目的	4
	(3) 現行 WEB コンテンツの概要	5
	(4) 関連する調達案件	8
	(5) 契約期間	9
	(6) 作業スケジュール	10
2	業務範囲	10
3	作業の実施内容	11
	(1) 本サイトの前提条件	11
	(2) 設計・開発実施計画書等の作成	12
	(3) 運用・保守作業計画及び運用・保守実施要領の作成	13
	(4) 機能向上内容	13
	(5) 設計	15
	(6) 開発・テスト	15
	(7) 受入テスト支援	16
	(8) 引継ぎ	16
	(9) 定例会等の実施	16
	(10) 定常時対応	17
	(11) 障害時発生対応	18
	(12) 情報システムの現況支援	19
	(13) 改善提案	19
	(14) 成果物	20
4	作業の実施体制・方法	22
	(1) 作業実施体制	22
	(2) 作業要員に求める資格等の要件	24
	(3) 作業場所	24
	(4) 作業の管理に関する要領	25
5	作業の実施に当たっての遵守事項	25
	(1) 機密保持、資料の取扱い	25
	(2) 個人情報の取扱い	26
	(3) その他文書、標準への準拠	27
	(4) 情報システム監査	28
	(5) 情報セキュリティの確保	28
	(6) ドメイン名の登録・維持に関する要件	31
	(7) 情報システムの保護に関する事項	31
6	成果物の取扱いに関する事項	31
	(1) 知的財産権の帰属	31
	(2) 契約不適合責任	32
	(3) 検収	33
7	入札参加資格に関する事項	34

(1) 複数事業者による共同入札	34
(2) 入札制限.....	34
(3) その他の入札要件	35
8 再委託に関する事項.....	35
(1) 再委託の制限及び再委託を認める場合の条件	35
(2) 承認手続.....	35
(3) 再委託先の契約違反等.....	36
9 その他特記事項	36
(1) 前提条件等	36
(2) 入札公告期間中の資料閲覧等.....	36
(3) 事業効果の調査分析	37
(4) その他	38
10 ウェブサイト構築等に係る情報セキュリティの確保のための基本仕様	38
11 環境への配慮（環境負荷低減のクロスコンプライアンス）	38

1 事業の概要

(1) 業務名

令和 8 年度グローバル産地づくり推進委託事業（「GFP」WEB コンテンツ運用・保守・機能向上業務事業）（以下「本業務」という。）

(2) 業務の背景と目的

農林水産省においては、2018 年 8 月に GFP（農林水産物・食品輸出プロジェクト）を立ち上げ、輸出に意欲を持った農林水産・食品事業者等のコミュニティを形成し各種支援を行っている。

中でも GFP コミュニティサイト（URL：<https://www.gfp1.maff.go.jp/>、以下、WEB コンテンツという。）においては、コミュニティメンバー間のマッチングや輸出関連情報の発信等の機能を搭載することで、日本の農林水産物・食品の輸出促進に向けた環境づくりを推進してきた。

令和 7 年度の調達では、これまで GFP コミュニティで実施してきた輸出診断・訪問診断を改良した新たな機能として、WEB コンテンツ上に輸出診断機能を実装した。また、輸出診断機能に関するデータを関係者間で編集・共有可能な管理システムの改良を実施した。既存の輸出診断・訪問診断では、診断を受けた会員への情報提供が最適化されていなかったほか、実施までに多くの工数と煩雑なプロセスを要していた。新輸出診断では、その内容を改良・省力化しており、GFP ユーザーが繰り返し輸出診断を行うことが可能になると共に、これまで輸出診断でメンターとなっていた GFP 事務局や農政局、各種専門家の省力化に貢献するものである。

本業務は上記の背景を踏まえ、輸出診断機能が実装された WEB コンテンツ及び管理システムについて、その趣旨を理解した上で、GFP ユーザーや GFP 事務局からの要望を反映したデザインや機能の向上や、WEB コンテンツの運用・保守に関する事務作業を行うとともに、日本の農林水産物や食品を世界各国に広めることを意図とした GFP 登録者のコミュニティ化や、各種輸出サポートを効果的に行う上で必要とされる WEB コンテンツの改修等を行うものであり、国民に効果的かつ効率的に普及啓発する発信力・訴求力・影響力を備えた WEB コンテンツに充実させることを目的とする。

また、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。情報システムのクラウド化の推進に当たっては、共通基盤となる農林水産省クラウド（以下「MAFF クラウド」という。）を利用することを前提としたパブリッククラウドへの移行を進めることとしている。

本システムでは MAFF クラウドを利用しており、MAFF クラウドでは、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、パブリッククラウドへの移

行・運用等の一連の工程における、PMO による PJMO への総合的な支援活動を実施する。
 なお、総合的な技術支援を行う組織を MAFF クラウド CoE と言う。引き続き、本システムでは MAFF クラウドを利用することを前提とする。

(3) 現行 WEB コンテンツの概要

本業務の現行のシステム構成は次のとおりである。

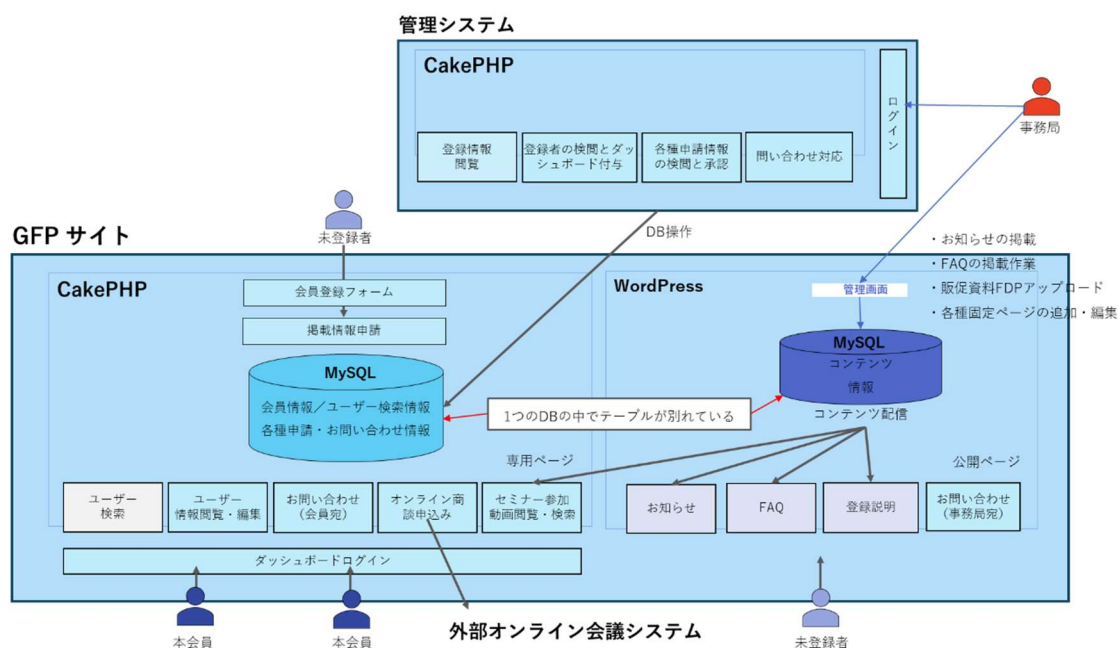


図1：本業務のシステム構成

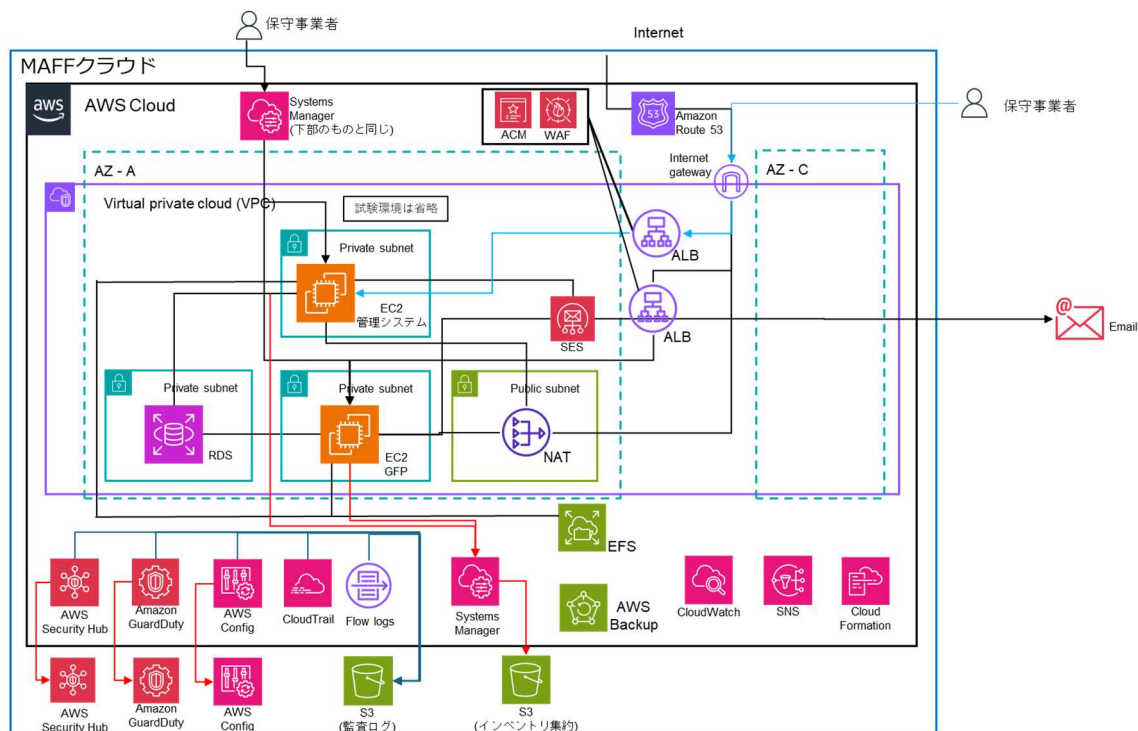


図 2 : 本業務のシステム構成

MAFFクラウド構成イメージ

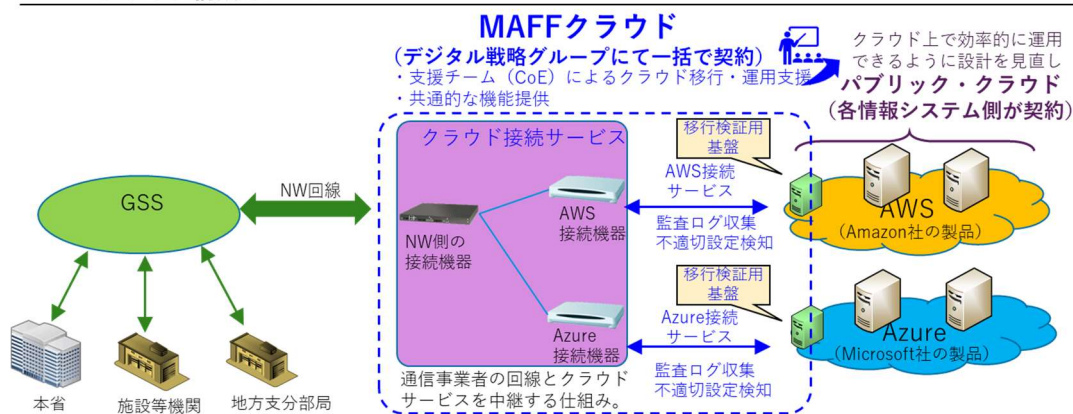


図 3 : MAFF クラウド構成イメージ

※GSS 経由での閉域網接続と、利用システムに対する監査ログ取得等の共通機能を提供する。

TOPページ

メニュー			
GFPとは			
サービスについて			
生産品検索 一覧		生産品 詳細	
		生産者 詳細	
		オンライン商談の申し込み	
		非ログイン時：(GFP登録説明へリンク)	
		ログイン時：オンライン商談の申し込み(完了)	
		事業者へのお問合せ(入力)	
		事業者へのお問合せ(確認)	
		事業者へのお問合せ(完了)	
イベント/セミナー 一覧			
		イベント/セミナー(絞り込み検索)	
		イベント/セミナー 詳細	
		イベント/セミナー お問合せ(入力)・事務局へのお問合せ	
		イベント/セミナー お問合せ(確認)・事務局へのお問合せ	
ニュース 一覧			
		ニュース 詳細	
実績インタビュー 一覧			
		実績インタビュー 詳細	
よくある質問			
事務局へのお問合せ(入力)			
		事務局へのお問合せ(確認)	
		事務局へのお問合せ(完了)	
サイト利用規約			
プライバシーポリシー			
サイトマップ			
サイト内検索			
機種依存文字について			
GFP登録説明			
		生産者・加工食品製造事業者の登録フォーム(入力)	
		生産者・加工食品製造事業者の登録フォーム(確認)	
		流通事業者・その他の登録フォーム(入力)	
		流通事業者・その他の登録フォーム(確認)	

TOPページ(EN)

GFP登録説明			
		登録フォーム	
お問合せ			
サイト利用規約			
プライバシーポリシー			
ログイン後メニュー			

TOPページ(CH)

図4：GFP サイト TOP ページの画面構成（赤字部分のみログイン時）

ログイン後メニュー	
プロフィールを充実させたい 一覧	プロフィールを充実させたい 詳細
ログイン後ニュース 一覧 → ニュース 一覧	ログイン後ニュース 詳細 → ニュース 詳細
オンライン商談がしたい(全体) → 生産品/生産者検索 一覧	オンライン商談がしたい(絞り込み検索) → 生産品/生産者検索 一覧
	オンライン商談がしたい(生産者) → 生産品/生産者検索 詳細
	オンライン商談がしたい 詳細(生産者) → オンライン商談の申し込み
	オンライン商談がしたい(流通事業者)
	オンライン商談がしたい 詳細(流通事業者)
ビジネスパートナーへ相談したい(全体)	ビジネスパートナーへ相談したい(絞り込み検索)
	ビジネスパートナーへ相談したい(生産者)
	ビジネスパートナーへ相談したい 詳細(生産者)
	ビジネスパートナーへ相談したい(流通事業者)
輸出を勉強したい	輸出を勉強したい(絞り込み検索)
	輸出を勉強したい詳細
売りたい・買いたい(全体)	売りたい・買いたい(買いたい)
	売りたい・買いたい 詳細(買いたい)
	売りたい・買いたい(売りたい)
	売りたい・買いたい 詳細(売りたい)
	売りたい・買いたい(その他)
	売りたい・買いたい 詳細(その他)
	売りたい・買いたい 募集を掲載する(入力)
	売りたい・買いたい 募集を掲載する(確認)
登録者を探す(全体)	売りたい・買いたい 募集を掲載する(完了)
登録者を探す(絞り込み検索)	登録者を探す(生産者)
	登録者を探す 詳細(生産者)
	登録者を探す(流通事業者)
	登録者を探す 詳細(流通事業者)
GFP会員カタログ(日本語版)	
GFP Member Catalog (English)	
輸出関連リンク集	輸出関連リンク集「貿易について知りたい」
	輸出関連リンク集「相談したい(農林水産省)」
	輸出関連リンク集「JETRO」
	輸出関連リンク集「規制を知る(国・地域で一括して知りたい)」
	輸出関連リンク集「規制を知る(放射性物質規制)」
	輸出関連リンク集「規制を知る(動植物検疫)」
	輸出関連リンク集「規制を知る(残留農薬)」
	輸出関連リンク集「規制を知る(輸出に関する手続き・制度)」
	輸出関連リンク集「補助金・補助事業を知る」
	輸出関連リンク集「海外でプロモーションをしたい」
	輸出関連リンク集「展示会・商談会に参加しよう」
	輸出関連リンク集「金融支援措置について知りたい」
マイページ	マイページ(編集)
	基本情報編集(編集)
	基本情報編集(確認)
	メールマガジン設定(切り替え)
	オンライン商談設定(切り替え)
一般公開設定(切り替え)	

図5：GFP サイトログイン後マイページの画面構成

(4) 関連する調達案件

関連する調達案件については以下を予定しており、以降はこれらの事業を GFP 関連事業、これら事業の受託者は GFP 関連事業受託者という。

ア 令和8年度グローバル産地づくり推進事業(GFPコミュニティ形成委託事業のうち伴走支援等(全国版))(仮称)

- ① 契約方式:未定
 - ② 契約締結日:令和8年3月頃
 - ③ 入札公告:令和8年1月頃
入札落札者決定:令和8年3月頃
 - ④ 契約期間:契約締結日～令和9年3月31日
 - ⑤ 主な事業内容:事業者へのきめ細やかな伴走支援、効果的な情報発信とコミュニティの活性化、GFPの円滑な実施に向けた体制づくり等
- イ 令和7年度グローバル産地生産流通基盤強化緊急対策事業(GFPコミュニティ構築支援加速化委託事業(全国版))(仮称)
- ① 契約方式:未定
 - ② 契約締結日:令和8年3月頃
 - ③ 入札公告:令和8年1月頃
入札落札者決定:令和8年3月頃
 - ④ 契約期間:契約締結日～令和9年3月31日
 - ⑤ 主な事業内容:全体的なGFP事業方針の策定、輸出産地等向けのセミナー・交流会等の実施、人づくりによる輸出のすそ野拡大と支援、GFPの円滑な実施に向けた体制づくり等
- ウ 令和7年度グローバル産地生産流通基盤強化緊急対策事業(GFPコミュニティ構築支援加速化委託事業(地方版))(仮称)
- ① 契約方式:未定
 - ② 契約締結日:令和8年3月頃
 - ③ 入札公告:令和8年1月頃
入札落札者決定:令和8年3月頃
 - ④ 契約期間:契約締結日～令和9年3月31日
 - ⑤ 主な事業内容:地方農政局等で実施する地方GFP事業に係る活動を実施・サポートする。
- エ 令和7年度グローバル産地生産流通基盤強化緊急対策事業(GFPコミュニティ構築支援加速化委託事業(異業種連携を通じた輸出促進))(仮称)
- ① 契約方式:未定
 - ② 契約締結日:令和8年3月頃
 - ③ 入札公告:令和8年1月頃
入札落札者決定:令和8年3月頃
 - ④ 契約期間:契約締結日～令和9年3月31日
 - ⑤ 主な事業内容:未定

(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。

作業項目	令和 8 年												令和 9 年		
	4	5	6	7	8	9	10	11	12	1	2	3			
1. 契約締結	4月1日														
2. 設計・開発実施計画書															
3. 運用・保守作業計画及び運用・保守実施要領															
4. 基本設計・詳細設計															
5. 開発															
6. 受入テスト支援									下旬						
7. 受入テスト										上旬					
8. WEBサイト本番公開										中旬					
9. 状況確認会議	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
10. WEBサイト運用・保守															
11. 作業完了報告書など成果物提出													3月31日まで		
12. 引継ぎ															

図6 作業スケジュール

2 業務範囲

本業務における主な作業内容は表 1 に記載の通りである。なお、必要に応じて農林水産省(以下「発注者」という。)の輸出・国際局輸出支援課(以下「担当部署」という。)の担当職員(以下「監督職員」という。)の承認を得ること。

表 1 主な作業内容

主な作業項目	作業内容
設計・開発実施計画書の作成と計画書に基づく作業実施状況報告	本業務遂行に当たっては、本仕様書に基づき、作業の目的、成果、実施体制、作業管理方法、スケジュール等、プロジェクト全体を計画し実行するための設計・開発実施計画書を作成すること。作業内容、作業スケジュール、プロジェクト管理ルール、報告ルール、ドキュメント等について取りまとめた計画書を作成し、監督職員の承認を得ること。
WEB コンテンツの運用、保守、機能向上	設計・開発実施計画書等に基づき WEB コンテンツの運用、保守、機能向上を行うこと。
会議の開催及び報告	進捗状況確認会議（定例）及び個別検討会議を主催すること。また議事録を作成し 2 週間以内に監督職員の承認を得て提出すること。
次期事業者への引継ぎの実施	要すれば次期事業者と十分なコミュニケーション

主な作業項目	作業内容
	ンを取りながら、過不足のない引き継ぎを行うこと。

WEB コンテンツ改修について、関係者から必要な情報を得る必要がある場合は、受託者の責任において調整すること。また、公開用ウェブサーバの設定に変更が生じる場合は、受託者の責任において調整すること。

また、本業務にパブリッククラウドにおけるクラウドサービスの提供業務も含めることとする。なお、クラウドサービスの提供に係る費用及び利用料は受託者の負担とする。

3 作業の実施内容

(1) 本サイトの前提条件

- ア 令和7年度グローバル産地づくり推進委託事業(「GFP」WEB コンテンツ機能向上・運用・保守業務事業)(以下「前事業」)を受託する GFP-WEB 機能向上推進コンソーシアム(代表者:株式会社博報堂)(以下「前受託者」という。)より各種情報(WEB コンテンツのデータ一式、デザインデータ(ai、psd 等)、WEB コンテンツ更新マニュアル、WEB 解析アカウントの譲渡)の提供を受け、本業務を遂行するものとする。
- イ 現行の WEB コンテンツデータは、MAFF クラウド上の AWS サーバーに格納されている。受託者は、WEB コンテンツの管理・運用に関する業務について MAFF クラウド上のサーバーで以後の作業を実施すること。
- ウ サーバー運用に関し、WAF(Web Application Firewall)が入っていること。
- エ 現在運用を行っている WEB コンテンツ(URL: <https://www.gfp1.maff.go.jp/>)をベースとすること。
- オ WEB コンテンツにおいて利用するサブドメインは現行の「gfp1.maff.go.jp」とすること。切替等の作業でサブドメインの DNS 情報を書き換える際は、監督職員と協議のうえで実施すること。
- カ https による暗号化通信を必須とする。そのために必要となるサーバー証明書の提供も本業務の範囲に含む。TLS1.0、TLS1.1 は使用できないよう、無効化すること。
- キ 登録済みのGFP会員に限らず、会員登録していない一般の方も使用する。
- ク 年間想定アクセス数約 30 万。GFP会員の増加に伴い、アクセス数は増える見込み。
- ケ 本システムは、OS として Amazon Linux2023、ミドルウェアとして Apache、PHP、アプリケーションとして cakePHP を使用している。
- コ 本 WEB サイトはオープンソフトウェアである、Word Press の標準機能を利用して構築されている。
- サ 端末側の動作環境は、ブラウザとして Google Chrome、Microsoft Edge、Safari の最

新バージョン、PC の OS は Windows と Mac の最新バージョン、またスマートフォン OS (Android、iOS) やタブレット OS へ対応すること。

- シ WEB サイトはレスポンシブデザインにすること。
- ス 現行の WEB サイトは、グローバルで利用されることを想定しているため、部分的に英語、中国語に対応している。
- セ 本 WEB サイトの特権アカウントは、多要素認証を採用すること。
- ソ 本業務に用い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こと。また、本業務でデータ消去を行う場合、クラウド上に保管されたデータについて、ISMAP で規定された方法でデータが消去されていること、それが正しく運用されているか第三者による監査により証明されていること。
- タ 本業務に関わる電子データの提供に関しては、以下の仕様とすること。
 - (ア) Microsoft 社 Windows11 上で表示可能なものとする。
 - (イ) 使用するアプリケーションソフトについては、以下のとおりとする。
 - ・ 文書 : Microsoft 社 Word
 - ・ 計算表 : Microsoft 社 Excel
 - (ウ) 使用する画像ファイルについては、以下のとおりとする。
BMP 形式又は JPEG 形式
 - (エ) (イ)、(ウ) による成果物に加え、「PDF ファイル形式」による成果物を作成すること
- チ 受託者は、前受託者からパブリッククラウド上に構築された情報システムの引継ぎを受け、アカウントの契約の移管を行い、環境を維持すること。
- ツ 受託者は、構成管理及びパッチの適用について可能な限り自動化すること。なお、自動化とは、対象を選定し、タイミングをコントロールして適用することをいう。
- テ 受託者は、原則、メンテナンスの際に踏み台サーバを独自で構築せず、クラウドサービスプロバイダーのサービス (AWS Systems Manager Session Manager ・AWS Systems Manager Fleet Manager) を利用すること。
- ト 受託者は、ソフトウェアの情報をクラウドサービスの機能 (AWS の場合、SSM (AWS Systems Manager)) を利用して自動取得すること。

(2) 設計・開発実施計画書等の作成

受託者は、監督職員の指示に基づき、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、監督職員の承認を受けること。

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、別添の「デジタル・ガバメント推進標準ガイドライン」の「第3編第7章 設計・開発」で定義されている事項を踏まえたものとする。

(3) 運用・保守作業計画及び運用・保守実施要領の作成

受託者は、監督職員が定める運用・保守作業計画及び運用・保守実施要領（以下、運用・保守計画等という）について、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。なお、運用・保守作業計画等の記載内容は、デジタル・ガバメント推進標準ガイドライン「第3編第9章 運用及び保守」で定義されている事項を踏まえたものとする。

(4) 機能向上内容

本業務では、WEBコンテンツの積極的な活用、GFP登録者間のコミュニケーションの活性化、事務作業の効率化を目的とした機能向上を行う。下記機能向上内容についての基本設計及び詳細設計を行い、成果物について監督職員の承認を受けること。なお、例示内容については、代替案・改良案により要件を満たすことができる場合は、必ずしも例示どおりに実装する必要はない。

ア 機能向上に当たっての前提仕様

機能向上に当たり、本業務では次の事項に留意すること。

- ① 監督職員と実施内容を協議のうえ、委託費の範囲内で実施すること。
- ② 効率的かつ効果的なウェブサイト運営を継続して行うため、ユーザー及び GFP事務局が扱いやすいサイト構成を目指すこと。ユーザー及びGFP事務局については、以下の 1.及び 2.の定義を参照すること。
 1. ユーザー
ユーザーとは、GFP サイトで会員登録済の事業者のみに留まらず、日本の農林水産物・食品の輸出に関わる全ての事業者・団体・行政関連機関等を想定している。
 2. GFP 事務局
GFP 事務局とは、担当部署の職員、各地方農政局等の職員及び GFP 関連事業受託者等を想定している。
- ③ GFPは輸出に関わる事業者間でのコミュニティ形成の促進を目的としており、生産から加工、流通、販売の各段階で輸出に関わるあらゆる事業者が対象である。GFP 会員等のニーズを踏まえて次年度以降も継続した機能向上を想定しているため、次期事業受託者が改修・構築しやすいよう、一定の拡張性を考慮した設計を行うこと。
- ④ 機能向上に当たっては、監督職員の指示の下、GFP 関連事業受託者とも積極的に連携すること。

イ 具体的な機能向上内容

① 輸出診断機能の改善

令和7年度に実装した輸出診断機能について、実際に運用していく上で可視化された不具合（当該機能を実装した受託事業者の契約不適合による不具合は除く）や、ユーザー及び GFP 事務局からの要望を基に可能な限り対応すること。また、本機能の趣旨を理解した上で、改善点があれば提案し、対応すること。

② 会員管理システムの更新

本業務や GFP 関連事業及びこれまでの事業で取得された会員情報や関連データを GFP 事務局内で共有し、そのデータを分析・活用することを念頭に、会員管理システムで管理可能なデータを追加・修正すること。

追加・修正する内容は、例えば、会員情報としては GFP イベント参加履歴や輸出に関する取組等を、関連データとしては GFP 事務局で管理した項目等を想定している。また、追加・修正するデータは csv 形式でエクスポート可能にするなど、データの分析・活用がしやすいように設計すること。

③ 会員マイページのアップデート

ログイン後の会員マイページについて、より使いやすい形でアップデートすること。例えば、マイページの UI/UX の改善（デザインや導線の整理等）や、英訳対応（ブラウザの標準機能としての翻訳機能による英訳ではなく、海外のユーザーが使用しやすいようネイティブチェックを前提とした英訳）等を想定している。

④ その他

1. ソフトウェアバージョンアップについて

本業務の運営に必要なソフトウェアは、契約期間中にサポート期限が切れることの無いよう、サポート期限が切れる前にバージョンアップを実施すると共に、それに伴う影響を調査し、必要に応じて改修等行うこと。

2. 脆弱性診断について

5(5)トを参照の上、改修後、公開日までに WEB コンテンツの全ページの脆弱性診断を行い、脆弱性が発見された場合は対応すること。

3. マニュアル作成について

本業務で機能向上を実施したページも含め、ユーザー向け、GFP 事務局向けの操作マニュアルをそれぞれ更新し、監督職員の承認を受けること。ユーザー向けマニュアルについては、サイト上のわかりやすい位置（上部等）に掲載し、随時更新できるような形式で構築すること。

4. ニーズを踏まえた検討について

ユーザー及び GFP 事務局のニーズを踏まえ、継続的に WEB コンテンツ充実に向けた検討を実施すること。

5. 設備、備品購入について

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等の購入・貸借は、本業務の契約金額外で受託者の責任において用意すること。

6. 設計について

受託者は、詳細設計を行い、その内容を詳細設計書として作成し、監督職員の承認を受けること。

(5) 設計

- ア 受託者は、(4)機能向上内容を満たすための基本設計及び詳細設計を行い、その内容を設計書として作成して監督職員の承認を得ること。
- イ 受託者は、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、監督職員に提出すること。
- ウ 受託者は、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、監督職員と MAFF クラウド CoE の確認を受けること。

(6) 開発・テスト

- ア 受託者は、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標準(標準コーディング規約、セキュリティコーディング規約等)を定め、監督職員の確認を受けること。
- イ 受託者は、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、監督職員の確認を受けること。
- ウ テスト手順を策定し、開発したアプリケーションが正常に動作するかシステムテストを行うこと。
- エ テスト体制、テスト項目(画面遷移、カテゴライズ、リンクチェックを含むコンテンツ確認テスト等)、スケジュール、合否判定基準等を記載したテスト要領書を作成し、監督職員の承認を得ること。
- オ 受託者は、設計工程の成果物及びテスト要領書に基づき、アプリケーションプログラムの開発、テストを行うこと。
- カ 受託者は、本業務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。
- キ ブラウザテストは、スマートフォン、タブレット、PC での使用を意識したブラウザソフト(最低3種類)での確認を行うこと。
- ク 受託者は、テスト要領書に基づき、各テストの実施状況を監督職員に報告すること。テストの実施において対応不十分な事項や改善が望ましい事項があった場合は、

速やかに修正対応すること。なお、テスト結果は、「テスト結果報告書」にまとめて、監督職員に提出すること。

(7) 受入テスト支援

- ア 受託者は、監督職員が受入テストのテスト要領書を作成するに当たり、情報提供等の支援を行うこと。
- イ 受託者は、監督職員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 受託者は、監督職員の指示に基づき、WEB コンテンツ利用者のテスト実施も含めて、テスト要領書作成の支援を行うこと。

(8) 引継ぎ

- ア 受託者は、設計・開発の設計書、システム環境やソースコードなどの詳細な内部仕様書、作業経緯、残存課題等を文書化して引継ぎ書にまとめること。また、次期事業者が円滑に次期事業を開始できるように、次期事業者に対して確実な引継ぎを行うこととし、次期事業者の契約締結日から1か月以内に引継ぎ書に関する質問事項があった場合、契約期間外であっても対応すること。また、以上の内容に関する覚書を作成し、監督職員の承認を得ること。
- イ 受託者は、次期事業者に対し、システムの運用等を行うクラウド環境を原則としてそのまま引継ぐこと。そのため、引継ぎに際しては、必要に応じて引継ぎ先事業者との間で書面による契約等を行い、管理者権限の引き渡し等、クラウド環境の引継ぎを適切に行うこと。
- ウ 受託者は、次期事業者への引継ぎを完了した際、管理者権限やクラウド環境へのアクセス等に係る自らのアカウント情報を破棄し、監督職員に書面で報告すること。
- エ 受託者は、監督職員が WEB コンテンツの更改を行う際には、次期の情報システムにおける要件定義支援事業者及び設計・開発事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

(9) 定例会等の実施

- ア 受託者は、定例会を原則1ヶ月に1回開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。なお、開催日時については、監督職員の承認を得て実施すること。
- イ 監督職員から要請があった場合、又は、受託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 定例会等の会議においては、監督職員の指示の下で GFP 関連事業受託者も参画するものとし、より効率的な GFP 事務局運営及び、より効果的な GFP サービス提

供に資するため、監督職員のみならず、GFP 関連事業受託者とも積極的に討議を行うこと。

- エ 進捗状況確認会議及び各個別検討会議の議事録は受託者が作成し、2 週間以内に監督職員の承認を得て電子メール等を用いて提出すること。また、各種会議、監督職員との協議においては、協議の内容を受託者の責任において議事録に整理し、発生した問題点等についても記録するとともに、それを適切に管理し、監督職員に報告、承認を得ること。
- オ 監督職員との協議（電話又は電子メールによる報告を含む。）、各種議事録等、本作業において作成した文書等は、適切な手法によって監督職員が適宜参照できるようにし、履行期間終了時にそれらを全て納入すること。

(10) 定常時対応

- ア 受託者は、定常時対応の計画書を作成の上、定常時対応運用業務（アクセス数、WEB コンテンツ操作、運転管理・監視、稼働状況監視、サービスデスク提供定期点検、不具合受付等）を行うこと。
- イ 受託者は、運用計画に基づき、運用業務の内容や工数などの作業実績状況、サービスレベルの達成状況、情報システムの構成と運転状況（情報セキュリティ監視状況を含む。）、情報システムの利用者サポート、リスク・課題の把握・対応状況について月次で運用作業報告書を取りまとめること。また、自動取得したソフトウェアの情報を把握し、発注者の求めに応じて最新の構成情報の出力結果を提出すること。
- ウ 受託者は、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、達成状況の改善に向けた対応策を提案すること。
- エ 受託者は、運用作業報告書の内容について、月例の定期運用会議に出席し、その内容を報告すること。
- オ 受託者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、監督職員にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること。また、自動取得したソフトウェアの情報を把握し、監督職員の求めに応じて最新の構成情報の出力結果を提出すること。
- カ ソフトウェアにセキュリティの脆弱性が見つかった場合は、対応策について計画し、監督職員の承認を得た上で対応すること。
- キ 受託者は、パッチの自動適用を用いて、検証環境や品質保証環境などを用いてパッチベースラインを検証し、その後に本番環境にパッチを適用するなど、パッチのリリース管理を行うこと。

なお、パッチ適用に起因する不具合が出た際に行う切り戻しやアプリケーション修正などの対応を予め計画すること。

- ク 受託者は、保守作業でプログラムの修正を行った場合、設計書等の更新を行い、テストを行った上で本番環境へ適用すること。改修の際に作成、更新した資料は、監督職員へ提出すること。
- ケ 受託者は、監督職員が情報システム運用継続計画を作成又は更新するにあたり、情報提供等の支援を行うこと。
- コ 受託者は、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、監督職員に提出すること。
- サ 受託者は、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、監督職員と MAFF クラウド CoE の確認を受けること。
- シ 受託者は、インベントリ情報を収集するため、設定作業(AWS の場合、Systems Manager Inventory と EC2 の設定)を実施すること。なお、インベントリ収集機能はコンテナの構成管理に対応していないため、コンテナを利用しているシステムは、MAFF クラウド利用ガイドラインの記載を参考に、脆弱性対策を実施すること。
- ス 受託者は、クラウドサービスの利用実績について、利用明細書の写し及びそれらを一覧表にとりまとめ、半年分と1年分を年に2回担当部署に提出すること。また、監督職員の求めに応じ、クラウドサービスを含めた情報システムの構成を適切に見直すための資料を提出すること。
- セ 運用・保守業務の対応時間は原則として開庁日(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 号第 1 項各号に掲げる日をいう。))を除く。))の9時から 18 時とするが、緊急時は監督職員と調整のうえ、時間外(行政機関の休日を含む。))も対応すること。
- ソ セキュリティ管理として、(AWS の場合 SecurityHub)が発報したセキュリティアラートについて、対応ならびに無効化／抑制を検討するものとする。なお、新たなルールの追加について、迅速に対応するものとする。

(11) 障害時発生対応

- ア 受託者は、WEB コンテンツの障害発生時(又は発生が見込まれる時)には、速やかに監督職員に報告するとともに、その緊急度及び影響度を判断の上、運用・保守作業計画の運用要件に示す障害発生時運用業務(障害検知、障害発生箇所の切り分け、保守事業者への連絡、復旧確認、報告等)又は保守要件に示す障害発生時保守作業(原因調査、応急措置、報告等)を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は監督職員が定める運用計画に基づいて行うこと。
- イ 受託者は、WEB コンテンツの障害に関して事象の分析(発生原因、影響度、過去の発生実績、再発可能性等)を行い、同様の事象が将来にわたって発生する可能性が

ある場合には、恒久的な対応策を提案すること。

受託者は、災害等の発生時には、監督職員の指示を受けて、情報システム運用継続計画に基づく運用・保守業務を実施すること。なお、災害等の発生に備え、最低年1回は事前訓練を実施すること。

(12) 情報システムの現況支援

ア 受託者は、年1回、監督職員の指示に基づき、情報資産管理データと情報システムの現況との突合・確認(以下「現況確認」という。)を支援すること。

なお、MAFF クラウドを利用している場合、MAFF クラウドから提供されるインベントリ情報を活用することで、現況確認は省略することも可とするが、インベントリ情報から収集できない製品が含まれる場合は、当該製品の構成情報の取得を行うこと。

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

ウ 受託者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査の上監督職員に報告すること。

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

(13) 改善提案

ア 受託者は、令和9年3月 17 日までに年間の運用・保守実績を取りまとめるとともに、必要に応じて運用・保守計画、運用・保守実施要領に対する改善提案を行うこと。なお、上記の改善提案に当たっては、パブリッククラウドの運用体制において、マネージドサービスプロバイダーが提供している共有型のクラウド運用・保守サービスの活用についても検討し整理することとする。検討した結果、MSP サービスの活用を運用・保守計画に組み込んだ場合は、実際にサービス等の活用を開始すること。

イ 前記アの改善提案に当たっては、クラウドサービスプロバイダーが提供する ベストプラクティス準拠状況(AWS の場合、Trusted Advisor)を定期的に調査し、検出項目の対応可否を検討し、担当部署の承認の上、対応すること。クラウド構成のベストプラクティス(AWS の場合、AWS Well-Architected フレームワーク(信頼性・運用上の優秀性))を活用し、年に1度システムが適切に運用されているかチェックし、次年度の改善点を整理すること。

ウ 受託者は、クラウドサービスの利用実績について、利用明細書の写し及び月額の利用サービスの費用実績(MSP サービスを利用した場合)を一覧表にとりまとめ、半年分と1年分を年に2回担当部署に提出すること。また、MSP サービスを利用した場合

等の運用サービスの共通化の効果を定量で説明すること。

エ 受託者は、監督職員の求めに応じ、クラウドサービスを含めた情報システムの構成を適切に見直すための資料(AWS Cost Explorer、AWS Trusted Advisor、AWS CUR、Azure Cost Management 等の出力結果)を提出すること。運用サービスの共通化とは、以下の取組とする。

(ア) 受託者が自社で MSP サービスを提供している場合はそれを利用すること。

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

i)外部企業が提供する MSP サービスを利用すること、又は

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

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

オ 改善提案を作成したら監督職員ならびに PMO/MAFF クラウド CoE に報告すること

(14) 成果物

ア 成果物名

本業務の成果物を表2に示す。

表 2 成果物一覧

No.	成果物名	内容及び納品数量	納品期日
1	事前引継完了確認書	1 式	契約締結後1か月以内
2	設計・開発実施計画書	1 式	契約締結後1か月以内
3	設計・開発実施要領	1 式	契約締結後1か月以内
4	設計・開発実施要領に基づく管理資料	1 式	令和9年3月17日
5	標準コーディング規約	1 式	令和9年3月17日
6	設計書(基本設計書、詳細設計書)	1 式	令和9年3月17日
7	ソースコード一式	1 式	令和9年3月31日
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	1 式	令和9年3月31日

	成等に使用される設定情報その他の必要な情報一式		
9	実行プログラム一式	1 式	令和9年3月31日
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 式	令和9年3月17日
11	テスト要領書	1 式	テスト前
12	テスト結果報告書 (脆弱性検査結果も含む)	1 式	テスト終了後速やかに
13	運用計画(案)	1 式	契約締結後1か月以内
14	保守作業計画(案)	1 式	契約締結後1か月以内
15	WEBコンテンツ	1 式	令和9年3月31日
16	業務完了報告書	1 式	令和9年3月31日
17	WEBコンテンツ操作マニュアル(本業務での機能向上実施内容を反映させたもの)	1 式	令和9年3月17日
18	運用・保守報告書	1 式	令和9年3月17日
19	障害報告書	1 式	令和9年3月17日
20	クラウドサービスの利用実績	1 式	令和9年3月17日
21	クラウド環境一式 (管理者権限等のアカウント情報を含むこと。なお、アカウント情報については、必要な情報を記載した「アカウント情報一覧」を準備した上で、監督職員が指定する方法で納品すること。)	1 式	令和9年3月31日
22	(システム構成に変更があった場合) ・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 ・システム構成図 ・IaCで構築した際に作成された定義ファイル(CloudFormation) ・パッチ適用設定ファイル(SSM patch manager)	1 式	令和9年3月17日
23	個人情報破棄報告書	1 式	令和9年3月31日
24	引継ぎ書	1 式	令和9年3月17日
25	事後引継ぎに関する覚書	1 式	令和9年3月17日

機能向上業務の成果物については、設計・開発実施計画書に各成果物の提出時期を記載し、監督職員が必要な時期に内容確認できるように提出すること。

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。
- ・ 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」の周知について(令和4年1月11日内閣文第1号内閣官房長官通知)」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。
- ・ 成果物は監督職員から特別に示す場合を除き、原則電子データをサーバー納入すること。
- ・ 受託者は、納品データをサーバーに設置するため、コーディングデータを監督職員が指定するサーバーにアップすること。
- ・ 電子データの納品について、Microsoft Office 又は PDF のファイル形式で作成し、監督職員が指定するサーバーに格納して納品すること。
- ・ 納品後、発注者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、監督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。

納品にあたっては、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報(対策ソフトウェア名称、定義パターンバージョン、確認年月日)についても、監督職員が指定する方法で提出すること。

ウ 成果物の納品場所

原則として、監督職員が指定する先のサーバーに成果物一式を納入すること。なお、指定先のサーバーとしては、発注者が用意する PrimeDrive や、監督職員と受託者を含む Teams に割り当てられる SharePoint 等を想定している。

4 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託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、受託者内の人員構成については、落札後に協議を行い、決定する。また、受託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し、書面で提出すること。

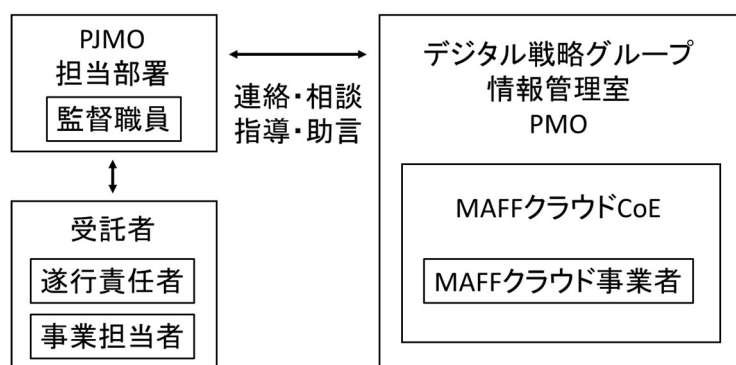


図7 本業務の推進体制及び本業務受託者に求める作業実施体制

表 3 本業務における組織等の役割

組織等	本業務における役割
PMO	農林水産省の全体管理組織。クラウド利用を含む情報システムに関する各PJMOからの問い合わせを受け、対応、助言・指導等を行う。
MAFFクラウドCoE	監督職員・受託者に対してパブリッククラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。
PJMO	WEBコンテンツの管理組織として、本業務の進捗等を管理する。
本業務受託者	本業務を実施する。

受託者は、以下の実施体制を確保すること。

- ア 日本語での対応ができること。
- イ 本業務を遂行させるために十分な業務実施体制を確保したうえ、業務ごとの連絡窓口を明示するとともに、責任体制を明確にし、全社的対応を図ることとし、作業体制表を提出すること。業務ごとに、必要な知識及び経験、資格を有するものを担当させること。
- ウ 本業務の円滑な運営を図るため、受託者は監督職員との連絡を密にして本業務を行うこと。
- エ 本業務は GFP コミュニティを形成することを目的としているため、GFP 関連事業受託者とも、監督職員の指示の下、必要に応じて連携を取ること。
- オ 作業の経過、進捗状況等について遅延が認められた場合は、速やかに監督職員に報告するとともに、対応策を提示すること。
- カ 体制を変更する必要がある場合には、事前に変更内容を記載した別に定める計画変更承認申請書をもって監督職員に報告し、監督職員の承認を得ること。

なお、担当者の異動が発生する場合には、後任の担当者に対して、本業務に支障をきたさないように十分な訓練を実施した後に業務の引継ぎを行い、引継ぎ結果を報告すること。

- キ 担当者の病気等により欠務が生じる場合は、その旨、代行する受託者側担当者の名前及び経歴・保有資格等担当者として十分な資格を有している旨を、速やかに監督職員へ書面にて報告し、承認を得ること。なお、代行する担当者は業務に支障をきたさないようにすることができる者を担当させること。
- ク 本業務を行う担当者は、業務を効率的、効果的に推進するために求められる業務遂行能力を有すること。
- (ア) 情報や意見を的確に交換できるコミュニケーション能力
- (イ) 課題・改善点を識別し、改善する能力
- (ウ) 担当する職務に応じた技術力(クラウド業務を実施する場合は、AWS のスキル)

表4 本業務受託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	<ul style="list-style-type: none"> 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。
遂行責任者(副)	遂行責任者の補佐を行う。
事業担当者	本業務に関する設計・開発、テスト、運用、保守等を担う。
事業担当者(副)	事業担当者の補佐を行う。

(2) 作業要員に求める資格等の要件

- ア 受託者における遂行責任者は、本業務と類似のシステムの設計・開発の遂行責任者としての経験を5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3年以上の者又は同等の実績を有する者を1人以上配置すること。
- ウ 運用・保守を行う担当者には、以下の資格のいずれかを有する者を1名以上配置すること。

AWS solutions architect associate / AWS solutions architect professional

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

(3) 作業場所

本業務の作業場所は事前に登録した場所とする。また、作業に当たり必要となる設備、備

品の購入は認めない。消耗品等については、受託者の責任において用意すること。また、必要に応じて監督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

受託者は、監督職員が承認した設計・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、運用業務、保守業務に係るコミュニケーション管理、体制管理、作業管理、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。

5 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 受託者は農林水産省における情報セキュリティの確保に関する規則（平成 27 年3月 31 日農林水産省訓令第4号。以下「規則」という。）、「農林水産省における個人情報の適正な取扱いのための措置に関する訓令」等の内容を理解するとともに、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、政府機関等の情報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。

イ 本業務に係る情報セキュリティ要件は次の通りである。

- (ア) 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) 受託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。

ウ 受託者は、発注者から要機密情報を提供された場合には、当該情報の機密性の格付けに応じて適切に取り扱うための措置を講ずること。また、委託業務において受託者が作成する情報については、監督職員からの指示に応じて適切に取り扱うこと。

エ 受託者は、農林水産省情報セキュリティ共通仕様に準拠した情報セキュリティ対策の履行が不十分と見なされるとき又は受託者において委託業務に係る

情報セキュリティ事故が発生したときは、必要に応じて監督職員の行う情報セキュリティ対策に関する監査を受け入れること。

- オ 受託者は、監督職員から提供された要機密情報が業務終了等により不要になった場合には、確実に返却し又は廃棄すること。また、委託業務において受託者が作成した情報についても、監督職員からの指示に応じて適切に廃棄すること。
- カ 上記以外に、仕様書別紙「ウェブサイト構築等に係る情報セキュリティの確保のための基本仕様」に基づき、作業を行うこと。

(2) 個人情報の取扱い

- ア 個人情報の取扱いに係る事項について監督職員と協議の上決定し、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) 個人情報取扱責任者が情報管理責任者と異なる場合には、個人情報取扱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、受託者はその旨を証明する書類を提出し、監督職員の下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、事前に監督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、受託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 受託者は、本業務を履行する上で個人情報(生存する個人に関する情報であつて、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、監督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 受託者は、監督職員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、受託者(必要に応じ監督職員)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 発注者が本業務で構築したシステムを用いて本契約終了後も事業を実施する場合、受託者は当該システムから個人情報を抹消せず、次期事業者と十分なコミュニケーションを取りつつ、取り扱い方法も含みシステムを引継ぐものとする。
- キ 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) その他文書、標準への準拠

ア 農林水産省クラウド利用ガイドライン

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。

イ 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とともに、認められた場合は削除すること。
- (イ) 提供するアプリケーションにぜい弱性を含めないとともに、認められた場合は削除すること。
- (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、監督職員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、監督職員から「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。

(4) 情報システム監査

- ア 本業務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、監督職員が情報システム監査の実施を必要と判断した場合は、監督職員が定めた実施内容(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託者は受け入れること。(監督職員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、対応案を監督職員と協議し、指示された期間までに是正を図ること。

(5) 情報セキュリティの確保

受託者は下記の点に留意して情報セキュリティを確保するものとする

- ア 通信経路の分離
不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。
- イ 不正通信の遮断
通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。
- ウ 通信のなりすまし防止
WEB コンテンツ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。
- エ サービス不能化の防止
サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して WEB コンテンツを構築すること。
- オ 不正プログラムの感染防止
不正プログラム(ウイルス、ワーム、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。
- カ ログの蓄積・管理
WEB コンテンツ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、WEB コンテンツの利用記録、例外的事象の発生に関するログを蓄積し、契約締結の日から1年間保管するとともに、不正の検知、原因特定に有効な管理機能(ログの検索機能、ログの蓄積不能時の対処機能等)を備えること。

キ ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。

ク 時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

ケ 侵入検知

不正行為に迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。

コ 主体認証

WEB コンテンツによるサービスを許可された者のみに提供するため、WEB コンテンツにアクセスする主体のうちメンバー専用ページの認証を行う機能として、識別コード（ID）とパスワードの方式を採用すること。

サ ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

シ 管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

ス 通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。

セ 保存情報の機密性確保

WEB コンテンツに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、外部との接続のある WEB コンテンツにおいて保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。

ソ WEB コンテンツの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の WEB コンテンツの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて WEB コンテンツに関す

る運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

タ 調達する機器等に不正プログラム等が組み込まれることへの対策

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

チ 情報セキュリティ水準低下の防止

WEB コンテンツ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。

ツ プライバシー保護

WEB コンテンツ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。

テ システムの可用性確保

サービスの継続性を確保するため、WEB コンテンツの各業務の異常停止時間が復旧目標時間として 24 時間を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

ト 構築時の脆弱性対策

WEB コンテンツ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。

ナ 情報の物理的保護

情報の漏えいを防止するため、端末の離席対策等（自動スクリーンロック等）によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

ニ 侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、WEB コンテンツの構成装置（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。

ヌ 運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、WEB コンテンツ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、WEB コンテンツ全体の更新漏れを防止する機能を備えること。

ネ 委託先において不正プログラム等が組み込まれることへの対策

WEB コンテンツの構築において、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。本業務の遂行における情報セキュリティ対策の履行状況を確認するために、府省庁が情報セキュリティ監査の実施を必要と判断した場合は、受託者は情報セキュリティ監査を受け入れること。

ノ クラウドサービスに関する事項

クラウドアーキテクトのベストプラクティス(AWS Well-Architected Framework)及び「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル別冊クラウド設計・開発編」に準拠すること。以下のセキュリティ対策要件を参照し、本システムのセキュリティ対策要件を点検すること。

・ Web システム／Web アプリケーションセキュリティ要件書

(6) ドメイン名の登録・維持に関する要件

ア 受託者は、属性型、汎用 JP、都道府県型 JP ドメイン名の登録及び維持を行い、その費用負担を行うこと。なお、登録及び維持の対象となるドメイン数は3つである。

イ 前記アに加えて、これまでに使用していたドメインで、廃止にあたってセキュリティ確保のために保持していた旧ドメインが存在する。それらの旧ドメインを保持し、廃止日になったら廃止すること。なお、保持及び廃止の対象となるドメイン数は2つである。

(7) 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、監督職員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、農林水産省を契約者として契約すること。

ウ 本業務の契約とクラウドサービスの契約は別に契約することが必要であることを理解して対応すること。クラウドサービスの利用にあたり、情報資産が漏えいすることがないよう、必要な措置を講じること。

エ 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。

6 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著作権及び二次的著作物の著作権(著作権法第21条

から第 28 条に定める全ての権利を含む。)は、受託者が本業務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にて権利譲渡不可能と示されたもの以外は、全て発注者に帰属するものとする。

- イ 受託者に帰属する知的財産権を利用して本業務を行う場合、発注者及びシステム利用者に受託者の知的財産権の利用を許諾する範囲及び制約を受託者が周知すること。
- ウ 発注者は、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、受託者は、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、複製等により発注者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は通知したときは、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、受託者は、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、本業務の受託者は、当該既存著作物の内容について事前に発注者の承認を得ることとし、発注者は、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発注者の責めに帰す場合を除き、受託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、発注者は係る紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。
- オ 本業務に係る成果物の権利(著作権法第 21 条から第 28 条に定める全ての権利を含む。)及び所有権は、検収に合格した成果物の引渡しを受けたとき受託者から発注者に移転するものとする。
- カ 受託者は発注者に対し、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 受託者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

(2) 契約不適合責任

- ア 監督職員は検収(「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、受託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、受託者は、当該追完を行うものとする。ただし、監督職員が追完の方法を指定して請求した場合であって、監督職員に不相当な負担を課するものでないときは、受託者は監督職員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こと。

- 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、監督職員は、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、発注者は、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) 受託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、受託者が追完をしないでその時期を経過したとき。
 - (エ) 前記(ア)から(ウ)までに掲げる場合のほか、監督職員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 監督職員は、当該契約不適合(受託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、受託者に対して損害賠償を請求することができること。
- 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、当該契約不適合により個別契約の目的を達することができないときは、監督職員は本契約及び個別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責任がある場合であって、監督職員が検収完了後1年以内に当該契約不適合について通知しないときは、発注者は、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託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託者の故意若しくは重過失に起因するときにはこの限りでない。
- キ 前記アからオまでの規定にかかわらず、契約不適合が監督職員の提供した資料等又は監督職員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、受託者がその資料等又は指示が不相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 本業務の受託者は、成果物等について、履行期限までに監督職員に内容の説明

を実施して WEB コンテンツの完成をもって検査を受けること。また、検査の結果、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、変更点について監督職員及び検査職員に説明を行った上で、指定された日時までに再度提出すること。

- イ 作成方針について事前に監督職員と協議や確認を行う機会を十分に設け、求める内容を反映すること。
- ウ 監督職員に提出する以前に、内容及び品質について受託者において十分に確認を行ったうえで提出すること。
- エ 提出時に、受託者内での確認者名、確認日、確認内容を明示した確認書を添付すること。
- オ 提出された成果物について、監督職員による確認を行う期間、確認結果を伝達する機会、確認結果を反映する期間を十分に設けること。
- カ 監督職員による確認を経て承認を得ること。
- キ 専門用語や業界用語の使用を避け、監督職員が理解できる資料等を作成すること。
- ク 本業務の受託者は、成果物等について、納品期日までに監督職員に内容の説明を実施して検収を受けること。
- ケ 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、変更点について監督職員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。

7 入札参加資格に関する事項

(1) 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、本代表者が本業務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。

(2) 入札制限

- ア 本業務を直接担当する農林水産省 IT テクニカルアドバイザー(旧農林水産省 CIO 補

佐官に相当)、農林水産省全体管理組織(PMO)支援スタッフ及び農林水産省最高情報セキュリティアドバイザーが、その現に属する事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」(昭和38年大蔵省令第59号)第8条に規定する親会社及び子会社、同一の親会社を持つ会社並びに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。

(3) その他の入札要件

ア 受託者は以下の(ア)又は(イ)のいずれかの条件を満たすこと。

(ア) クラウドサービスプロバイダーから代理店の認定を受け、かつ AWS Solution Provider Program(SPP)の登録を受けていること。加えて、本案件の関係者が、日本国内のクラウドサービスプロバイダーから日本語で契約や技術に関するサポートを受けられる商流であること。

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

イ 受託者は、本システムで利用中のパブリッククラウドにおいて構築又は改修又は運用・保守を行った実績を過去3年以内に有すること。

8 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 本業務の受託者は、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。なお、主たる部分とは、業務における総合的企画、業務遂行管理、手法の決定及び技術的判断等をいうものとする。受託者は、この委託事業達成のため、委託事業の一部を第三者に委任し、又は請け負わせること(以下「再委託」という。)を必要とするときは、監督職員と協議のうえ、別に定める再委託承認申請書を提出し、あらかじめ監督職員の承認を得なければならない。ただし、再委託が出来る事業は、原則として委託費の限度額に占める再委託の金額の割合が50パーセント以内の業務とする。

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

ウ 受託者は再委託先の行為について一切の責任を負うものとする。

エ 再委託先における情報セキュリティの確保については受託者の責任とする。

オ 再委託を行う場合、再委託先が「7.(2)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監督職員に提出し、あらかじめ承認を受けること。

- イ 前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を監督職員に提出し、承認を受けること。
- 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、本業務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、受託者が一切の責任を負うとともに、監督職員は、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。

9 その他特記事項

(1) 前提条件等

- ア 本業務仕様書と契約書の内容に齟齬が生じた場合には、本業務仕様書の内容が優先する。
- イ 本業務受託後に仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって監督職員に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が確認することによって変更を確定する。
- ウ 本仕様書について疑義等がある場合は、質問書により質問すること。なお、質問書に対する回答は適宜行うこととする。
- エ MAFF クラウドについて不明点等がある場合は、監督職員及び MAFF クラウド CoE と協議の上、作業を進めること。
- オ MAFF クラウド CoE や PMO 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は、監督職員及び MAFF クラウド CoE、PMO と協議の上、対応を行うこと。

(2) 入札公告期間中の資料閲覧等

現行の WEB コンテンツについては、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、必ず事前に監督職員まで連絡の上、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 農林水産省輸出・国際局輸出支援課輸出産地形成室(4階ドア番号 459)

イ 閲覧期間及び時間

(ア) 公告期間中

(イ) 行政機関の休日を除く日の 10 時から 17 時まで。(12 時から 13 時を除く。)

ウ 閲覧手続

最大2名まで。応札希望者の商号、連絡先、閲覧希望者氏名を別記様式「資料閲覧申請書」に記載の上、閲覧希望日の1日前までに提出すること。また、閲覧日当日までに別記様式「機密保持誓約書」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、本業務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は、次の力の(ウ)の資料についてデータで提供することは可能である。必要に応じて申し出ること。

オ 連絡先

農林水産省輸出・国際局輸出支援課輸出産地形成室 電話 03-6738-7897

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) 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

(イ) 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、ソフトウェアバージョン情報

(ウ) 農林水産省クラウド利用ガイドライン及び関係資料

(3) 事業効果の調査分析

ア 農林水産省は、本業務の効果(ユーザーのアクセス数、サイト上でのマッチング数等)について調査分析を行うため、受託者に対し、本業務の実施に関し必要な報告を求めることができるものとする。その際、受託者は、正当な理由がある場合を除き、当該調査分析に協力するものとする。

イ 農林水産省は、本業務の効果の調査分析に必要がある場合には、関係行政機関又は当該調査分析業務の一部を受託した第三者に対し、本業務の実施に係る情報を提供することができるものとする。

ウ 農林水産省は、イの規定により情報を提供する場合には、当該情報の漏えい、滅失又は毀損の防止その他の当該情報の適切な管理のために必要な措置を講ずるものとする。

(4) その他

- ア 受託者は、提案書のとおり事業を実施すること。
- イ 本業務における人件費の算定に当たっては、別添の「委託事業における人件費の算定等の適正化について」に従うこと。
- ウ 受託者は、本仕様書に疑義が生じたとき、あるいは本仕様書に記載のない細部事項については、監督職員と速やかに協議しその指示に従うこと。
- エ MAFF クラウドについて不明点等がある場合は、監督職員及び MAFF クラウド CoE と協議の上、作業を進めること。

10 ウェブサイト構築等に係る情報セキュリティの確保のための基本仕様

仕様書別紙「ウェブサイト構築等に係る情報セキュリティの確保のための基本仕様」を参照のこと。

11 環境への配慮（環境負荷低減のクロスコンプライアンス）

受託者は、委託事業の提供に当たり、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仕様書案別紙「環境負荷低減のクロスコンプライアンス実施状況報告書」の様式を用いて、以下の取組に努めたことを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～カの各項目について、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 臭気や害虫の発生源となるものについて適正な管理や処分に努める。
- エ 廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。
- オ 工事等を実施する場合は、生物多様性に配慮した事業実施に努める。
- カ みどりの食料システム戦略の理解に努めるとともに、機械等を扱う場合は、機械の適切な整備及び管理並びに作業安全に努める。

以 上

(別記様式)

資料閲覧申請書

申込日： 令和 年 月 日

1 会 社 名：

2 住 所：

3 担当者名：

4 電話番号：

5 E-mail アドレス：

6 閲覧日時： 令和 年 月 日 時

7 閲覧者氏名：

：
：
：

農林水産省輸出・国際局輸出支援課長 宛

機密保持誓約書

当社は、「令和8年度グローバル産地づくり推進委託事業（「G F P」WEBコンテンツ運用・保守・機能向上業務事業）」（以下「本件業務」という）に係る資料閲覧に当たり、下記の事項を厳守することを誓約します。

記

1 農林水産省の情報セキュリティに関する規程等を遵守し、次の情報を除き農林水産省が開示した情報（以下「閲覧情報」という）を、本件業務を調達する目的以外に使用又は第三者に開示若しくは漏洩しません。

- ① 開示の時点ですでに公知のもの、又は、当社の責めによらずして公知となったもの
- ② 正当な第三者から機密保持義務を負うことなく適法に入手したもの
- ③ 開示の時点ですでに保有しているもの

2 当社は、閲覧情報を第三者に開示若しくは漏洩することのないように必要な措置を講じます。

3 閲覧資料については、一切複製、複写、撮影、記録、又は閲覧場所からの持ち出しを行いません。

4 本件業務に係る調達の期間中及び終了後にかかわらず、本誓約を遵守いたします。

5 当社が本誓約に違反し、閲覧情報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えい等した場合、当社は、一切の責任を負担し、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

(別記様式)

会 社 名

氏 名

委託事業における人件費の算定等の適正化について

1. 委託事業に係る人件費の基本的な考え方

- (1) 人件費とは委託事業に直接従事する者（以下「事業従事者」という。）の直接作業時間に対する給料その他手当をいい、その算定に当たっては、原則として以下の計算式により構成要素ごとに計算する必要がある。

また、委託事業計画書及び実績報告書の担当者の欄に事業従事者の役職及び氏名を記載すること。

$\text{人件費} = \text{時間単価}^{\ast 1} \times \text{直接作業時間数}^{\ast 2}$
--

※1 時間単価

時間単価については、契約締結時に後述する算定方法により、事業従事者一人一人について算出し、原則として額の確定時に時間単価の変更はできない。

ただし、以下に掲げる場合は、額の確定時に時間単価を変更しなければならない。

- ・事業従事者に変更があった場合
- ・事業従事者の雇用形態に変更があった場合（正職員が嘱託職員として雇用された等）
- ・委託先における出向者の給与の負担割合に変更があった場合
- ・超過勤務の概念がない管理職や研究職等職員（以下、「管理者等」という。）が当該委託事業に従事した時間外労働の実績があった場合

※2 直接作業時間数

① 正職員、出向者及び嘱託職員

直接作業時間数については、当該委託事業に従事した実績時間についてのみ計上すること。

② 管理者等

原則、管理者等については、直接作業時間数の算定に当該委託事業に従事した時間外労働時間（残業・休日出勤等）を含めることはできない。ただし、当

該委託事業の遂行上やむを得ず当該委託事業のために従事した時間外労働にあつては、直接作業時間数に当該委託事業に従事した時間外労働時間（残業・休日出勤等）を含めることができることとする。

- （２）一の委託事業だけに従事することが、雇用契約書等により明らかな場合は、上記によらず次の計算式により算定することができる

$$\text{人件費} = \text{日額単価} \times \text{勤務日数}$$

$$\text{人件費} = \text{給与月額} \times \text{勤務月数（１月に満たない場合は、日割り計算による。）}$$

２．受託単価による算定方法

委託先（地方公共団体を除く。以下同じ。）において、受託単価規程等が存在する場合には、同規程等における単価（以下「受託単価」という。）の構成要素等の精査を委託契約締結時に行った上で、受託単価による算定を認める。

○ 受託単価の構成要素を精査する際の留意点

- ア 事業従事者の職階（課長級、係長級などに対応した単価）に対応しているか。
- イ 受託単価に人件費の他に技術経費、一般管理費、その他経費が含まれている場合は、各単価及びその根拠を確認すること。
- ウ 受託単価に技術経費、一般管理費等が含まれている場合は、委託事業計画書及び委託事業実績報告書の経費の区分欄に計上する技術経費、一般管理費に重複計上されていないか確認すること。

<受託単価による算定方法>

○正職員及び管理者等の時間単価は、受託単価規定等に基づく時間単価を使用すること。

○出向者、嘱託職員の受託単価計算

事業従事者が出向者、嘱託職員である場合は、受託単価規程等により出向者受託単

価、嘱託職員受託単価が規定されている場合は、それぞれの受託単価を使用することができる。ただし、出向者及び嘱託職員に係る給与については、委託先が全額を負担、一部のみ負担、諸手当が支給されていない等多様であるため、適用する受託単価の構成要素のうち人件費分について精査し、後述する実績単価により算出された人件費単価を超えることはできない。

3. 実績単価による算定方法

委託先に受託単価規程等が存在しない場合には、時間単価は以下の計算方法（以下「時間単価計算」という。）により算定する。（円未満は切捨て）

＜実績単価の算定方法＞

○正職員、出向者（給与等を全額委託先で負担している者に限る。）及び嘱託職員の
人件費時間単価の算定方法

原則として下記により算定する。

$$\text{人件費時間単価} = (\text{年間総支給額} + \text{年間法定福利費等}) \div \text{年間理論総労働時間}$$

- ・年間総支給額及び年間法定福利費の算定根拠は、「前年支給実績」を用いるものとする。ただし、中途採用など前年支給実績による算定が困難な場合は、別途委託先と協議の上定めるものとする（以下同じ。）。
- ・年間総支給額は、基本給、管理職手当、都市手当、住宅手当、家族手当、通勤手当等の諸手当及び賞与の年間合計額とし、時間外手当、食事手当などの福利厚生面で支給されているものは除外する（以下同じ。）。
- ・年間法定福利費等は、健康保険料、厚生年金保険料（厚生年金基金の掛金部分を含む。）、労働保険料、児童手当拠出金、身体障害者雇用納付金、労働基準法の休業補償及び退職手当引当金の年間事業者負担分とする（以下同じ。）。
- ・年間理論総労働時間は、営業カレンダー等から年間所定営業日数を算出し、就業規則等から1日当たりの所定労働時間を算出し、これらを乗じて得た時間とする（以下同じ。）。

○出向者（給与等の一部を委託先で負担している者）の時間単価の算定方法

出向者（給与等の一部を委託先で負担している者）の時間単価は、原則として下記により算定する。

$$\text{人件費時間単価} = \text{委託先が負担する（した）（年間総支給額＋年間法定福利費等）} \div \text{年間理論総労働時間}$$

- ・事業従事者が出向者である場合の人件費の精算に当たっては、当該事業従事者に対する給与等が委託先以外（出向元等）から支給されているかどうか確認するとともに、上記計算式の年間総支給額及び年間法定福利費は、委託先が負担した額しか計上できないことに注意すること。

○管理者等の時間単価の算定方法

原則として管理者等の時間単価は、下記の（１）により算定する。ただし、やむを得ず時間外に当該委託事業に従事した場合は、（２）により算定した時間単価を額の確定時に適用する。

（１）原則

$$\text{人件費時間単価} = \text{（年間総支給額＋年間法定福利費等）} \div \text{年間理論総労働時間}$$

（２）時間外に従事した場合

$$\text{人件費時間単価} = \text{（年間総支給額＋年間法定福利費等）} \div \text{年間実総労働時間}$$

- ・時間外の従事実績の計上は、業務日誌以外にタイムカード等により年間実総労働時間を立証できる場合に限る。
- ・年間実総労働時間＝年間理論総労働時間＋当該委託事業及び自主事業等における時間外の従事時間数の合計

４．一般競争入札により委託契約を締結する場合の例外について

一般競争入札により委託契約を締結する場合、受託規程で定める単価よりも低い受託単価又は本来の実績単価よりも低い実績単価を定めている場合は、精算時においても同単価により人件費を算定すること。

５．直接作業時間数を把握するための書類整備について

直接作業時間数の算定を行うためには、実際に事業に従事した事を証する業務日誌が必要となる。また、当該業務日誌において事業に従事した時間のほか、他の業務との重複がないことについて確認できるよう作成する必要がある。

【業務日誌の記載例】

(4月)		所属 ○○○部 ××課				役職 ○○○○				氏名 ○○ ○○				時間外手当支給対象者か否か										業務時間及び業務内容
時 日	0	...	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24					
1				A				B													A(3h)○○検討会資料準備 B(5.25h)○○調査打ち合わせ			
2				A				A			C									A(6h)○○検討会資料準備、 検討会 C(2h)○○開発打ち合わせ				
3				D				B		A										D(3h)自主事業 B(2h)○○調査打ち合わせ A(4h)現地調査事前準備				
4				A																	A(9.5h)○○調査現地調査			
5				A				D													A(3h)○○検討会資料準備 D(5h)自主事業			
.																								
.																								
.																								
.																								
30																								
31																								
勤務時間管理者 所属：○○部長 氏名：○○○○												A:○○○○委託事業(○○農政局) B:○○○○委託事業(○○農政局) C:○○○○補助事業(○○局) D:自主事業										合計		A(○○h) B(○○h) C(○○h) D(○○h)

- ① 人件費の対象となっている事業従事者ごとの業務日誌を整備すること（当該委託事業の従事時間と他の事業及び自主事業等に係る従事時間・内容との重複記載は認められないことに留意する。）。
- ② 業務日誌の記載は、事業に従事した者本人が原則毎日記載すること（数週間分まとめて記載することや、他の者が記載すること等、事実と異なる記載がなされることがないように適切に管理すること。）。
- ③ 当該委託事業に従事した実績時間を記載すること。なお、従事した時間に所定時間外労働（残業・休日出勤等）時間を含める場合は、以下の事由による場合とする。
- ・委託事業の内容から、平日に所定時間外労働が不可欠な場合
 - ・委託事業の内容から、休日出勤（例：土日にシンポジウムを開催等）が必要である場合で、委託先が休日手当を支給している場合。ただし、支給していない場合でも委託先において代休など振替措置を手当している場合は同様とする。
- ④ 昼休みや休憩時間など勤務を要しない時間は、除外すること。
- ⑤ 当該委託事業における具体的な従事内容が分かるように記載すること。なお、出張

等における移動時間についても当該委託事業のために従事した時間として計上することができるが、出張行程に自主事業等他の事業が含まれる場合は、按分計上を行う必要がある。

- ⑥ 当該委託事業以外の業務を兼務している場合には、他の事業と当該委託事業の従事状況を確認できるように区分して記載すること。
- ⑦ 委託先における勤務時間管理者は、タイムカード（タイムカードがない場合は出勤簿）等帳票類と矛盾がないか、他の事業と重複して記載していないかを確認の上、記名する。

附 則

（施行期日）

- 1 この通知は、平成２２年９月２７日以降に制定する委託事業仕様書等に基づく委託事業から適用する。

（経過措置）

- 2 この通知の施行日現在、既に制定されている委託事業仕様書等に基づき実施されている平成２２年度の委託事業における人件費の算定等について、当該委託事業に係る委託元又は委託先において本通知の趣旨を踏まえた対応が可能な事項がある場合には、当該事項については、本通知により取り扱うものとする。
- 3 前項の委託事業仕様書等に基づく委託事業を平成２３年度以降も実施する場合には、本通知を適用する。

附 則

この通知は、令和３年１月１日から施行する。

別紙_ウェブサイト構築等に係る情報セキュリティの確保のための基本仕様

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3に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書
 - （4）MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績

III 業務の実施における情報セキュリティの確保

- 1 受託者は、本業務の実施に当たって、以下の措置を講じること。なお、応札者は、以下の措置を講じることを証明する資料を提出すること。
 - （1）本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても第三者に開示及び本業務以外の目的で利用しないこと。

- (2) 本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。
 - (3) 本業務の各工程において、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者を示した管理体制図を提出すること）。
 - (4) 本業務において、農林水産省の意図しない変更が行われるなどの不正が見つかったときに、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を整備していること。
 - (5) 本業務において、個人情報又は農林水産省における要機密情報を取り扱う場合は、当該情報（複製を含む。以下同じ。）を国内において取り扱うものとし、当該情報の国外への送信・保存や当該情報への国外からのアクセスを行わないこと。
 - (6) 本業務における情報セキュリティ対策の履行状況を定期的に報告すること。
 - (7) 情報セキュリティインシデントが発生した場合は、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。）を受け入れ可能であること。
 - (8) 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。
 - (9) 情報セキュリティ対策の履行が不十分な場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。
- 2 受託者は、私物（本業務の従事者個人の所有物等、受託者管理外のものをいう。）の機器等を本業務に用いないこと。
- 3 受託者は、成果物等を電磁的記録媒体により納品する場合には、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処するとともに、確認結果（確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等）を成果物等に記載又は添付すること。
- 4 受託者は、本業務において取り扱われた情報を、担当部署の指示に従い、本業務上不要となったとき若しくは本業務の終了までに返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

IV 情報システムの各工程における情報セキュリティの確保

- 1 受託者は、本業務において情報システムの運用管理機能設定に係る企画・要件定義を行う場合には、以下の措置を実施すること。
- (1) 情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。
 - ア 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

- イ 情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。
 - (ア) 農林水産省外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
 - (イ) 不正プログラム感染や踏み台に利用されること等による農林水産省外への不正な通信を監視する機能
 - (ウ) 農林水産省内通信回線への端末の接続を監視する機能
 - (エ) 端末への外部電磁的記録媒体の挿入を監視する機能
 - (オ) サーバ装置等の機器の動作を監視する機能
- 2 受託者は、本業務において情報システムの設定を行う場合には、以下の事項を含む措置を適切に実施すること。
 - (1) 情報システムのセキュリティ要件の適切な実装
 - ア 主体認証機能
 - イ アクセス制御機能
 - ウ 権限管理機能
 - エ 識別コード・主体認証情報の付与管理
 - オ ログの取得・管理
 - カ 暗号化機能・電子署名機能
 - キ 暗号化・電子署名に係る管理
 - ク ソフトウェアに関する脆弱(ぜい)弱性等対策
 - ケ 不正プログラム対策
 - コ サービス不能攻撃対策
 - サ 標的型攻撃対策
 - シ アプリケーション・コンテンツのセキュリティ要件の策定
 - ス 政府ドメイン名(gojp)の使用
 - セ 不正なウェブサイトへの誘導防止
 - ソ 農林水産省外のアプリケーション・コンテンツの告知
 - (2) 情報セキュリティの観点に基づく試験の実施
 - ア ソフトウェアの開発及び試験を行う場合は、運用中の情報システムと分離して実施すること。
 - イ 試験項目及び試験方法を定め、これに基づいて試験を実施すること。
 - ウ 試験の実施記録を作成し保存すること。
- 3 受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、担当部署に報告し、協議の上、対策を講ずること。
- 4 受託者は、本業務において情報システムの運用・保守を行う場合には、情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。
 - (1) 情報システムの運用環境に課せられるべき条件の整備
 - (2) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

- (3) 情報システムの保守における情報セキュリティ対策
- (4) 運用中の情報システムに脆弱（ぜい）弱性が存在することが判明した場合の情報セキュリティ対策
- (5) 利用するソフトウェアのサポート期限等の定期的な情報収集及び報告
- (6) 情報システムの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポート継続中のバージョンでの動作検証及び当該バージョンで正常に動作させるための情報システムの改修等
- 5 受託者は、本業務において情報システムの運用・保守を行う場合には、運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。
 - (1) 情報セキュリティに関わる運用保守体制の整備
 - (2) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
 - (3) 情報セキュリティインシデント（可能性がある事象を含む。以下同じ。）を認知した際の対処方法の確立
- 6 受託者は、本業務において情報システムのセキュリティ監視を行う場合には、以下の内容を含む監視手順を定め、適切に監視運用すること。
 - (1) 監視するイベントの種類
 - (2) 監視体制
 - (3) 監視状況の報告手順
 - (4) 情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順
 - (5) 監視運用における情報の取扱い（機密性の確保）
- 7 受託者は、本業務において運用中の情報システムに脆弱（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弱（ぜい）弱性の対策を行うこと。
- 8 受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する府省庁等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。
- 9 受託者は、本業務において情報システムの運用・保守を行う場合には、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。
- 10 受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。
 - (1) 情報システム更改時の情報の移行作業における情報セキュリティ対策
 - (2) 情報システム廃棄時の不要な情報の抹消

V クラウドサービス等外部サービスに関する情報セキュリティの確保

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

1 外部サービス条件

- (1) 外部サービスを提供する情報処理設備が収容されているデータセンターについて、設置されている独立した地域（リージョン）が国内であること。
- (2) 外部サービスの契約に定める準拠法が国内法のみであること。
- (3) クラウドサービスの場合、ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。
- 2 ISMAP クラウドサービスリストに登録されているクラウドサービスであること。
- 3 ISMAP クラウドサービスリストに登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標(3桁の番号で表現される項目)及び末尾にBが付された詳細管理策(4桁の番号で表現される項目)を原則として全て満たしていること。
- 4 クラウドサービス以外の外部サービスの場合は、以下の措置を講じること。
 - (1) 外部サービスの利用を通じて農林水産省が取り扱う情報の外部サービス提供者における目的外利用の禁止。
 - (2) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること）。
 - (3) 外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を記載した資料を提出すること。
 - (4) 情報セキュリティインシデントへの対処方法を確立していること。
 - (5) 情報セキュリティ対策その他の契約の履行状況を確認できること。
 - (6) 情報セキュリティ対策の履行が不十分な場合の対処方法を確立していること。
 - (7) 外部サービス提供者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について外部サービス提供者と合意し、定められた手順により情報を取り扱うこと。

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

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

VII 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。

Ⅷ 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へ委託する再々委託等、多段階の委託を含む。以下同じ。）する場合には、受託者が上記Ⅱの１、Ⅱの２及びⅢの１において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、農林水産省の許可を得ること。
- 2 受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、農林水産省又は農林水産省が選定した事業者による再委託先への立入調査等の監査を受け入れ可能であること。
- 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。

Ⅸ 資料等の提出

上記Ⅱの１、Ⅱの２、Ⅲの１、Ⅴの４(２)、４(３)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つては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式にあつては提案書等の総合評価のための書類に添付して提出すること。

Ⅹ 変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ及びⅦ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。

様式

環境負荷低減のクロスコンプライアンス実施状況報告書

以下のア～カの取組について、実施状況を報告します。

ア 環境負荷低減に配慮したものを調達するよう努める。

具体的な事項	実施した／努めた	左記非該当
・対象となる物品の輸送に当たり、燃料消費を少なくするよう検討する（もしくはそのような工夫を行っている配送業者と連携する）。	<input type="checkbox"/>	<input type="checkbox"/>
・対象となる物品の輸送に当たり、燃費効率の向上や温室効果ガスの過度な排出を防ぐ観点から、輸送車両の保守点検を適切に実施している。	<input type="checkbox"/>	<input type="checkbox"/>
・農林水産物や加工食品を使用する場合には、農薬等を適正に使用して（農薬の使用基準等を遵守して）作られたものを調達することに努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・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。	<input type="checkbox"/>	<input type="checkbox"/>
・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。	<input type="checkbox"/>	<input type="checkbox"/>

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

ウ 臭気や害虫の発生源となるものについて適正な管理や処分に努める。

具体的な事項	実施した／努めた	左記非該当
・臭気が発生する可能性がある機械・設備（食品残さの処理や堆肥製造等）を使用する場合、周辺環境に影響を与えないよう定期的に点検を行う。	<input type="checkbox"/>	<input type="checkbox"/>
・臭気や害虫発生の原因となる生ごみの削減や、適切な廃棄などに努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・食品保管を行う等の場合、清潔な環境を維持するため、定期的に清掃を行うことに努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・その他（ ）		
・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、 その他の取組も行っていない場合は、その理由 （ ）		

エ 廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に使用する資材について、プラスチック資材から紙などの環境負荷が少ない資材に変更することを検討する。	<input type="checkbox"/>	<input type="checkbox"/>

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

オ 工事等を実施する場合は、生物多様性に配慮した事業実施に努める。

具体的な事項	実施した／努めた	左記非該当
・近隣の生物種に影響を与えるような、水質汚濁が発生しないよう努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・近隣の生物種に影響を与えるような、大気汚染が発生しないよう努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・施工にあたり使用する機械や車両について、排気ガスの規制に関連する法令等に適合したものを使用する。	<input type="checkbox"/>	<input type="checkbox"/>
・その他（ ）	<input type="checkbox"/>	<input type="checkbox"/>
・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由（ ）		

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

具体的な事項	実施した／努めた	左記非該当
・「環境負荷低減のクロスコンプライアンスチェックシート解説書 一民間事業者・自治体等編一」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。	<input type="checkbox"/>	<input type="checkbox"/>

・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。	<input type="checkbox"/>	<input type="checkbox"/>
・従業員等の向けの環境や持続性確保に係る研修などを行っている、もしくは、実施を検討する。	<input type="checkbox"/>	<input type="checkbox"/>
・作業現場における、作業安全のためのルールや手順などをマニュアル等に整理する。また、定期的な研修などを実施するように努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・資機材や作業機械・設備が異常な動作などを起こさないよう、定期的な点検や補修などに努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・作業現場における作業空間内の工具や資材の整理などを行い、安全に作業を行えるスペースを確保する。	<input type="checkbox"/>	<input type="checkbox"/>
・労災保険等の補償措置を備えるよう努めている。	<input type="checkbox"/>	<input type="checkbox"/>
・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（ ）

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

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

項目		見出し		要件		備考	必須可否
				1.6.2	公開ディレクトリには公開を前提としたファイルのみ配置すること	公開ディレクトリに配置したファイルは、URLを直接指定することでアクセスされる可能性があります。そのため、機微情報や設定ファイルなどの公開する必要がないファイルは、公開ディレクトリ以外に配置する必要があります。	必須
		1.7	アカウントの無効化機能について	1.7.1	管理者がアカウントの有効・無効を設定できること	不正にアカウントを利用されていた場合に、アカウントを無効化することで被害を軽減することができます。	推奨
2	セッション管理	2.1	セッションの破棄について	2.1.1	認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側のセッションを破棄しログアウトすること	認証を必要とするWebシステムの多くは、認証状態の管理にセッションIDを使ったセッション管理を行います。認証済みの状態にあるセッションを不正に利用されないためには、使われなくなったセッションを破棄する必要があります。セッションタイムアウトの時間については、サービスの内容やユーザー利便性に応じて設定することが必要になります。また、NIST Special Publication 800-63Bなどを参照してください。	必須
				2.1.2	ログアウト機能を用意し、ログアウト実行時にはサーバー側のセッションを破棄すること	ログアウト機能の実行後にその成否をユーザーが確認できることが望ましい。	必須
		2.2	セッションIDについて	2.2.1	Webアプリケーションフレームワークなどが提供するセッション管理機能を使用すること	セッションIDを用いて認証状態を管理する場合、セッションIDの盗聴や推測、攻撃者が指定したセッションIDを使用させられる攻撃などから守る必要があります。また、セッションIDは原則としてcookieにのみ格納すべきです。	必須
				2.2.2	セッションIDは認証成功後に発行すること 認証前にセッションIDを発行する場合は、認証成功直後に新たなセッションIDを発行すること		必須
				2.2.3	ログイン前に機微情報をセッションに格納する時点でセッションIDを発行または再生成すること		必須
				2.2.4	認証済みユーザーの特定はセッションに格納した情報を行うこと		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tring、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	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	必須
		4.1.6	CSSを動的に生成しないこと	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	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	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	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	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	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	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	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ー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