

応募要領

農林水産省大臣官房統計部（以下「統計部」という。）が実施する水稻収穫量調査については、全国約 8,000 の調査ほ場において、ほ場内で実際に刈取りを行い、10a 当たり収量を算出しています。

統計部では、水稻収穫量調査の精度向上に向け、これまで実施している標本調査に加え、人工衛星データ等のデジタル技術を活用した水稻収穫量予測の今後の導入に向け検討を進めることとしています。

この取組の一環として、今般、人工衛星データ等を活用した水稻収穫量予測の精度向上に向けた統計的研究に無償でご協力いただける事業者を募集いたします。

ご協力いただける事業者には、統計部と本業務に関する業務契約を締結いただき、当該研究の検証に必要とされる水稻収穫量調査で実施している調査対象ほ場ごとの水稻収穫量データ等について提供する予定です。

1 統計的研究の業務仕様

人工衛星データ等のデジタル技術を活用し、水稻の収穫量を精度高くかつ効率的に把握する手法が導入できるよう、民間事業者の協力を得て各種知見の収集に取り組みます。

具体的には、統計部から提供するほ場ごとの水稻収穫量データ等と人工衛星データ等を組み合わせ、民間事業者の持つ AI 技術を活用して水稻収穫量予測に取り組んでいただき、その結果等について報告を頂きます。

2 応募条件

- 人工衛星データや AI 等を活用して、現行の水稻収穫量調査の精度向上に貢献する水稻収穫量予測手法の具体的なプランが提示可能であること。
- 過去 3 年間に於いて、人工衛星データや AI 等を活用して農業分野における生育予測や収量予測等に取り組んだ実績を有すること。また、そのことが分かる資料の提出が可能であること。
- 水稻収穫量予測の結果を報告することについて承諾し、統計部との間で業務契約を締結することに合意できること。

- 統計法(平成19年5月23日法律第53号)に基づく調査票情報(水稻収穫量調査で実施している調査対象ほ場ごとの水稻収穫量データ)の適正な管理及び守秘義務を遵守する体制を整備できること。
- 日本国内に所在する事業者であって、日本国の法令に準拠し、日本語での対応が可能であること。
- 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を有していること。また、そのことが分かる証明書等の写しの提出が可能であること。
 - (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

3 提供予定データ

全国約1,000ほ場程度の水稻標本調査データ(令和4~6年の3か年分)

ほ場ごとの10a当たり収量、面積、位置情報(緯度・経度情報)等

4 募集期間

令和7年7月15日(火)から7月31日(木)まで

5 応募方法

別添の応募様式に必要事項を入力いただき、登記事項証明書に加え、募集条件に記載している提出資料と併せて以下の提出先メールアドレスにご提出ください。応募いただいた事業者の方に対して、個別にご連絡をさせていただき、面談を実施させていただきます。

面談の際に、人工衛星データ等のデジタル技術を活用した水稻収穫量予測手法の具体的なプランが分かる資料をご用意いただき、説明をお願いします。

説明内容を踏まえ、統計部と事業者の双方において統計的研究の実施及びデータ提供について合意に至った場合は、両者連名で業務契約

を締結させていただきます。

【提出先メールアドレス】 fude_polygon@maff.go.jp

6 本研究の実施期間

本研究の実施期間は、原則として業務契約締結日から令和7年12月26日（金）までとします。

なお、実施期間終了日前に研究が完了した場合は、その時点で7の報告をしていただいても構いません。

7 報告事項

提供したほ場ごとの水稻収穫量データを活用し、人工衛星データ等を用いて水稻収穫量予測を実施した結果及びその精度の水準、実証を行って判明した課題、考えられる改善点、実運用を想定した場合の費用感等について報告をいただきます。

8 留意事項

本研究の実施に当たっては、以下の点について留意願います。

- ① 応募様式に入力し提出いただいた氏名、事業者名等の個人情報等は、統計部において応募いただいた事業者との連絡などの事務手続のみに利用します。
- ② 統計部から提供する調査票情報（調査対象ほ場ごとの水稻収穫量データ）については、業務契約を締結した事業者に対しても統計法第39条に基づく調査票情報等の適正な管理及び第41条に基づく守秘義務が生じ、これに違反すれば第57条に基づき、罰則が課される場合もあります。このため、契約期間中は、同法に基づく統計部からの指導・監督に従っていただきます。
- ③ 本研究の実施に当たり、業務契約締結後に第三者に再委託することはできません。第三者に再委託する場合は、業務契約を締結する時点で予めその者を明示していただくこととなります。
- ④ 本研究の実施に当たっては、統計部担当者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）の説明を受けるとともに、情報セキュリティ対策を講じていた

だきます。具体的には、「情報セキュリティの確保に関する事項」(別紙)に基づいて作業を行うとともに、以下の点について遵守いただきます。

ア 情報漏えい防止をはじめとする情報セキュリティを確保するための体制を整備し、情報セキュリティ責任者を設置すること。

イ 情報セキュリティ責任者は、本研究において使用する情報システム、通信ネットワーク等の運用管理の徹底に努めるとともに、ウイルス対策ソフト等の活用や電子ファイルへのパスワード設定等、セキュリティ確保に向けた対応を実施すること。

ウ 本研究で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。また、作業過程で作成し不要となった資料等については、細断、粉碎等により確実に廃棄すること。

エ 統計部から提供する調査票情報は、日本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、国外からのアクセスは行わないこと。

オ 本研究において情報セキュリティに関する事故等が発生した場合は速やかに統計部担当者に報告するとともに、事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。また、対処に係る費用は全て負担すること。

- ⑤ 本研究において作成した資料、成果物等に関する著作権に関する権利は、統計部に無償で譲渡するものとし、統計部の行為について著作権人格権を行使しないこととします。
- ⑥ 本研究において、調査票情報を利用したことにより、事業者は何らかの不利益や損失を被る事態が発生した場合、統計部は一切の責任を負いません。
- ⑦ 本研究において個人情報を取扱う場合は、個人情報保護法に関する法令の趣旨に従うこととし、善良な管理者の注意をもって厳重に管理することとします。

9 問合せ先

農林水産省 大臣官房統計部 生産流通消費統計課 山下、松永
電話 03-3502-8111 (代表) 内線 3683
03-3502-5670 (直通)

情報セキュリティの確保に関する事項

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 応募者に関する情報の提供

- 1 応募者は、応募者の資本関係・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 応募者は、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、応募者は、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、個人情報又は統計部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) 統計部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、統計部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、統計部の指示に従い、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。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 クラウドサービスに関する情報セキュリティの確保

応募者は、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、VI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弱(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、統計部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。

V 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。

VI 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、統計部の許可を得ること。
- 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、統計部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。
- 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。

VII 変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅳ、及びⅥに関して、統計部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、統計部の許可を得ること。