仕様書

１．件名

情報機器等運用支援業務

２．履行場所

国立研究開発法人国際農林水産業研究センター（国際農研）
（茨城県つくば市大わし 1－1）

３．履行期間

令和 5 年 4 月 1 日～令和 6 年 3 月 31 日　8 時 30 分～17 時 15 分

ただし、土曜日、日曜日、国民の祝日に関する法律（昭和 23 年法律第 178 号）に規定する休日及び年末年始(12/29～1/3）を除く。

また、緊急時及び早急な対応が必要な場合には、上記時間外の業務を行うことがある。

４．目的

国際農研は日本国内の研究拠点（茨城県つくば市、沖縄県石垣市）における業務に加え、開発途上地域における農林水産業研究を実施しており、業務用の情報機器等を海外に持参する機会が多い。本業務は、セキュリティ等に関する情報を入手し、適切な対策を実施することによって、国際農研が保有する情報関連機器のセキュリティ対策の徹底と安定稼働のための環境確保を目的とする。

５．業務の内容

1) 受注者は、以下の業務（具体的な業務は「国際農研において行う業務の詳細」を参照）を遂行するため、「６．技術者の要件」を満たす２名（共有システム担当・イントラネット担当）の技術者を本業務作業者として国際農研（茨城県つくば市）に常駐させる。

①情報関連機器のセキュリティチェック
②グループウェア（リンコムネクスト 6.1sp3）用サーバの運用管理
③国際農研職員等に対するヘルプデスク業務

2) 本業務による管理対象機器等は以下のとおりとする。

① 国際農研本所（茨城県つくば市）の職員等（300 名程度）が使用する PC（業務用持ち出し機器を含む：480 台程度）とその周辺機器（プリンタ、ハブ、NAS、スキャナ等を含む）

Windows OS ： 10 以降製品
Mac OS ： Ver.10.15 以降製品

② グループウェア（リンコムネクスト）用サーバ
OS：Windows Server Standard 2016
③ Kaspersky Security Center 運用端末
④ 国際農研本所本館設置無線 LAN

６．国際農研に常駐する業務作業者の要件
業務作業者のうち、共有システム担当は次の 1)～5)を満たす者、イントラネット担当は 1)～2)を満たす者、とする。

1) Windows PC（10 以降製品）及び Mac PC（10.15 以降製品）に関するユーザサポート経験を有し、OS のインストール、ネットワーク、メール等に関する初期設定、トラブル対応等が可能なこと。
2) ウイルス対策、ネットワークに関するユーザサポート及びトラブルシューティング対応経験を有すること。
3) Windows サーバの運用管理経験を有し、日常的なメンテナンス、トラブル等への適切な対応が可能なこと。
4) ワークフロー（電子決裁システム）を導入したグループウェア(※)の運用管理経験（１年以上)を有すること。
※管理経験を有するグループウェア名及びバージョン、ワークフローのバージョン、担当年数、顧客名等を具体的に業務経歴書に記載すること。
5) Kaspersky Security Center の運用に関する知識を有すること。

７．契約条件等
1) 業務体制の構築
受注者は、国際農研に常駐する業務作業者及び常駐する業務作業者では十分に対応できない場合に後方支援（電話・メール等）にあたる業務毎の体制を構築するとともに、各担当者及び総括する者の氏名、連絡先等を記載した業務体制表を受注後、速やかに発注者に提出すること。体制に変更がある場合は、２週間前までに国際農研担当職員に申し出ること。受注者が配置した業務作業者について、発注者が不適当と認めた場合、受注者は早急に交代要員を配置すること。
2) 技術者が業務を履行できない場合の対応
業務実施日（または時間内）において、本業務作業者両名が業務を履行できない場合、受注者は 1 時間以内に共有システム担当と同等以上の技能を有する者を派遣すること。
3) 作業報告書の提出
業務作業者は、1 週間ごとに作業内容について時系列で記載した作業報告書を作成し、国際農研情報セキュリティ担当部門（企画連携部研究基盤室デジタル科）に提出すること。

4) 国際農研が保有する機器等の使用

本業務遂行に必要となる国際農研の機器、資料、施設、設備、電力は国際農研担当職員等の許可を得て、無償で利用できるものとする。ただし、本業務中に故意または過失により、国際農研の施設、設備及び機器等に汚損、破損等が生じた場合は、受注者の責任において速やかに原状回復すること。

8. その他

1) 業務遂行上の疑義が発生した場合は、速やかに国際農研担当職員に申し出ること。発生した疑義は協議の上、対応を決定する。
2) 本業務の実施にあたっては、当センターの定める諸規程を遵守するとともに、本業務に従事したことにより知り得た情報を本業務以外の目的のために使用してはならない。また、その情報の取り扱いについては、本契約期間にかかわらず、契約終了後も第三者へ漏洩してはならない。
3) 履行期間満了に伴い受注者が変更となる場合は、変更する受注者に対して所要の情報開示等を行い、業務の遂行に支障が生じないようにすること。特に、５．2)②に記載されたサーバ運用については、その手順を明記すること。
4) 別紙の情報セキュリティに関する共通事項を遵守すること。

国際農研において行う業務の詳細

受注者から配置される業務作業者は、国際農研職員の指示に従い、以下の作業を実施する。

（1）情報関連機器のセキュリティチェック

職員等が海外出張、国内出張等で所外へ持ち出し、外部ネットワーク等への接続を行った業務用持ち出し機器及び関係者が国際農研本所（つくば）へ持ち込み、ネットワーク等へ接続する全ての業務用機器(PC、強制暗号化 USB メモリ、外付け HD 等)に対し、以下のセキュリティチェックを行う。また、不具合を生じた機器については、解決に必要な措置（OS のリカバリ等も含む）を講じる。

① OS 及びアプリケーションの各種 Update 確認
② ウイルス定義ファイルの更新状況の確認及び更新作業
③ ウイルス感染状況チェックと機器トラブルの解決等

（2）グループウェア（リンコムネクスト 6.1sp3）用サーバの運用管理

グループウェアの安定運用のため、日常的なサーバメンテナンス業務（動作確認・バックアップログ等各種ログの掌握）の他、トラブル解決に向けた対応を行う。併せて、運用に伴うユーザ登録・削除・アクセス権の変更、ワークフロー承認ルート等の新規作成・変更等の業務を行う。

グループウェアにおける主な稼働アプリケーションは、以下のとおり。

・スケジューラ（職員のスケジュールの登録等）
・ファイルライブラリ（各種様式ならびに情報提供等）
・掲示板（所内（沖縄含む）への連絡等）
・施設予約（会議室・公用車、大型プリンタ等の予約）
・ワークフロー（出張申請、IP アドレス申請、パソコン等持ち出し申請、セミナー参加申請等に利用）

（3）国際農研職員等に対するヘルプデスク業務

① 業務用 PC 等の障害対応

発生したトラブルに対し、要因を特定し、リカバリの実施など、必要な対策を講じる。ただし、障害要因のうち、ハードウェアに起因する場合は、別途修理手配（ユーザより別途発注）とする。また、必要に応じ修理に関するメーカー連絡等のユーザ支援を行う。ソフトウェアに起因する場合の障害については、仕様書 5　2）および「業務の詳細」(3) ②に掲げるサポート対象アプリケーションのみ対応する。

② 国際農研本所（つくば）PC の購入・更新・リカバリ等に伴う以下の設定

・サポート対象 OS のインストール及び初期設定
・ネットワーク及びグループウェアへの接続設定
・メール等・データ移行サポート作業
・国際農研使用禁止ソフト等のアンインストール
・周辺機器（プリンタ、HUB、NAS、スキャナ）等の設定
・Microsoft Office 関連プロダクトキー等の管理
・IP アドレス管理台帳等の管理
・以下のアプリケーションのインストール・設定

Microsoft Office
Adobe Acrobat　／　Reader 含む
メールソフト：Thunderbird、Becky、AFFRIT Portal 提供の WEB-MAIL
（https://nss.sys.affrc.go.jp/sso/login より利用）
ブラウザ：Microsoft Edge 、Mozilla Firefox、Safari
ウイルス対策ソフト：カスペルスキー社製品　等
Java
Soliton Key Manager（MAFFIN 多要素認証使用ユーザのみ）

作業は原則として、販売元のサポート期間に準ずるものとし、販売元のサポートがないバージョンについては業務の対象外とする。
リカバリに伴うインストール及び初期設定の実施にあたっては、ライセンス侵害がないことを確認して実施することとし、ライセンス侵害等が判明した場合はユーザへ通知して是正を図る。

③ ウイルス対策ソフトの運用

ウイルス対策ソフト（Kaspersky Endpoint Security）の状況確認ツール（Kaspersky Security Center、Kaspersky Vulnerability and Patch Management）を運用する。また、OS の更新等に応じて提供される新バージョンの動作検証、バージョンアップツール作成、日常的な Kaspersky Security Center 等のログ監視、ユーザへの注意喚起、メーカーへの問い合わせ対応等を実施する。

④ Microsoft365 E3（付帯機能を含む）の運用支援

⑤ 強制暗号化 USB メモリ管理システムの管理及び運用

情報持ち出しの際の紛失・盗難による情報漏洩対策のための強制暗号化 USB メモリの運用に際し、管理台帳による貸出・返却の管理、ユーザへの使用法等の教示、返却に伴う USB メモリの初期化等を行う。

⑥ 国際農研本所（つくば）本館設置無線 LAN の管理

国際農研本所（つくば）本館 1F に設置した無線 LAN のアクセスパスワード変更等の定期的なメンテナンス

⑦ セキュリティ対策情報の提供

農林水産研究情報総合センター等より提供されるウイルス感染防止、不正アクセス等防止に係る情報（OS の Update、定義ファイルの更新等）を入手し、監督職員等へ随時提供する。

また、セキュリティ対策に関する職員等からの問い合わせに速やかに対応する。

⑧ 所内（本所及び拠点）ネットワーク、システム運用、海外出張に伴う情報機器等のトラブルに関する解決支援

関連する情報の収集、監督職員に対するコンサルティング、技術支援等を行う。

情報セキュリティに関する共通事項

1. 受注者は「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（令和３年度版)」及び国際農研情報セキュリティ関係規程を遵守すること。
2. 受注者は、別添「調達における情報セキュリティの確保に関する特約条項」を遵守するとともに、本特約条項第１条に従い、契約締結後、別添「調達における情報セキュリティ基準」第２項第８号に規定する「情報セキュリティ実施手順」を作成し、国際農研の確認を受けること。
3. 受注者は、受注者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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国際農研への情報提供を行うこと。
4. 受注者は、本業務の実施のために国際農研から提供され又は許可を受けたものを除き、国際農研が保有する情報にアクセスしてはならない。

調達における情報セキュリティ基準

1. 趣旨

調達における情報セキュリティ基準（以下「本基準」という。）は、国際農林水産業研究センター（以下「国際農研」という。）が行う調達を受注した者（以下「受注者」という。）において当該調達に係る要保護情報の管理を徹底するため、国際農研として求める情報の取扱い手順を定めるものであり、受注者は、契約締結後速やかに、本基準に則り情報セキュリティ実施手順を作成し、適切に管理するものとする。

2. 用語の定義

(1)「要保護情報」とは、紙媒体・電子媒体の形式を問わず、国際農研が所掌する事務・事業に係る情報であって公になっていない情報のうち、当該調達の履行のために国際農研から提供された情報であって、「機密性」「完全性」「可用性」の対応が必要な情報であり、受注者においても情報管理の徹底を図ることが必要となる情報をいう。

(2)「機密性」とは、限られた人だけが情報に接触できるように制限をかける必要性をいう。

(3)「完全性」とは、不正な改ざんなどから保護する必要性をいう。

(4)「可用性」とは、利用者が必要な時に安全にアクセスできる環境確保の必要性をいう。

(5)「情報セキュリティインシデント」とは、要保護情報の漏えい、紛失、破壊等のトラブルをいう。

(6)「取扱者」とは、当該調達の履行に関連し、要保護情報の取扱いを許可された者をいう。取扱者は、取扱者名簿への登録を必須とし、国際農研との共有を図ること。

(7)「取扱施設」とは、要保護情報の取扱い及び保管を行う施設をいう。

(8)「情報セキュリティ実施手順」とは、当該調達の契約締結後、本基準に基づき、受注者が情報の取扱い手順について定めるものである。詳細については、本基準３．情報セキュリティ実施手順の作成を参照のこと。

3. 情報セキュリティ実施手順の作成

受注者は、４．及び５．に示す各項目についての対応を検討し、「情報セキュリティ実施手順」として作成し、国際農研の確認を受けなければならない。国際農研の確認後、変更が必要な場合には、あらかじめ変更箇所が国際農研の定める本基準に適合していることを確認のうえ、国際農研の再確認を受けなければならない。

4. 受注者における情報の取扱い対策

(1)情報を取り扱う者の特定（取扱者の範囲）

・要保護情報の取扱者（再委託を行う場合の取扱者も含む）の範囲は、履行に係る必

要最小限の範囲とするとともに、適切と認める者を充てること。

・取扱者以外の利用は禁止する。

・情報の取扱いに際し、国際農研が不適切と指摘した場合には、できるだけ速やかに取扱者を交代させること。

(2)取扱者名簿の提出

受注者は、(1)で特定した取扱者の名簿を作成し、国際農研に提出すること。名簿には、以下の情報を盛り込むこと。また、情報の管理責任者を定め、国際農研に提出すること。

取扱者に変更が必要と判断した場合には、遅延なく国際農研に名簿の更新を申し出、確認を得ること。

・氏名

・所属する部署

・役職

・国籍等

・資格等を証明する書類（調達仕様書に定めがある場合のみ）

(3)取扱い施設等の対策

受注者は、要保護情報を取り扱う施設を明確にすること。

取扱施設に対する条件は以下のとおりとする。

・日本国内（バックアップ等を含め）に設置されていること。

・物理的なセキュリティ対策として、適切なアクセス制限の適用が可能なこと。

・(1)で特定した者以外（第三者）への情報漏洩対策並びに取扱施設での盗み見対策等を適切に講ずることが可能なこと。

(4)要保護情報の適切な保管対策の徹底

・受注者は、要保護情報を保管する場合、施錠および暗号化等の対策を適切に講じなければならない。

・要保護情報の電子データを端末・外部電子媒体等で管理する場合には、不要な持出し等が行われないための対策を行うこと。

・受注者は、要保護情報を取扱施設以外で取り扱う場合における対策を定め、適切に持出し等の記録を行うこと。

・情報セキュリティインシデントの疑い又は事故につながるおそれのある場合は、適切な措置を講じるなど、常にリスクの未然防止に努めること。

(5)情報セキュリティ実施手順の周知

受注者は、(1)で特定した要保護情報を取り扱う可能性のある全ての者に作成した情報セキュリティ実施手順を周知徹底のうえ、適切な管理体制を構築すること。また、再委託等により要保護情報を取り扱う作業に従事する全ての者（国際農研と直接契約関係にある者を除く。）に対しても周知徹底のうえ、受注者と同等の管理を行うこと。

(6)取扱者の遵守義務

・取扱者は、国際農研から提供を受けた要保護情報に対し、提示された格付けおよび取扱い制限を厳守し、利用すること。
・取扱者の要保護情報の複製および貸出しを禁止する。複製及び貸出しが必要な場合には国際農研の事前許可を得ること。
・守秘義務及び目的外利用の禁止
受注者は、取扱者に対し、履行開始前に守秘義務及び目的外利用の禁止を定めた契約は合意を行わなければならない。合意事項には、取扱者の在職中及び離職後において、知り得た国際農研の要保護情報を第三者に漏洩禁止の旨を含むこと。
・要保護情報の返却・破棄及び抹消
受注者は、接受、作成、製作した要保護情報を国際農研に返却、または復元できないように細断等確実な方法により破棄又は抹消すること。

(7)要保護情報の管理台帳の整備ならびに取扱いの記録、保存

① 台帳の管理
受注者は、履行期間中の要保護情報の管理に対し、接受、作成、製作、返却、破棄、抹消等の各プロセスにおいて、接受（作成）日、情報名、作成者、保管場所、取扱者、保存期限、抹消日等を明記した台帳を整備し、記録・管理を行い、履行期間満了時に国際農研に提出すること。

② 作成、製作した情報の取扱い
受注者は、作成、製作された全ての情報は、要保護情報として取り扱う。要保護情報としての取扱いを不要とする場合は、理由を添えて国際農研に確認を行うこと。

③ 要保護情報の保有
受注者は、返却、破棄、抹消の指示を受けた当該情報を引き続き保有する必要がある場合には、その理由を添えて、国際農研に協議を求めることができる。

(8)情報の取扱い状況の調査

・受注者は、情報の取扱い状況について、定期的及び情報セキュリティの実施に係る重大な変化が発生した場合には、調査を実施し、その結果を国際農研に報告しなければならない。また、必要に応じて是正措置を取らなければならない。
・受注者は、管理責任者の責任の範囲において、情報セキュリティ実施手順の遵守状況を確認しなければならない。

(9)情報セキュリティ実施手順の見直し

受注者は、情報セキュリティ実施手順を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティインシデントが発生した場合は、その都度、見直しを実施し、必要に応じて情報セキュリティ実施手順を変更し、国際農研の確認を得なければならない。

5. 情報セキュリティインシデント等に伴う受注者の責務

(1)情報セキュリティインシデント等の報告

受注者は、情報セキュリティインシデントが発生（可能性の認知を含む）した時は、初動対応を実施後、速やかに発生した情報セキュリティインシデントの概要を国際農研に報告しなければならない。

概要報告後、情報セキュリティインシデントの詳細な内容（発生事案、被害状況、国際農研要保護情報への影響の有無、適用した対策、再発防止策　等）をとりまとめの上、国際農研に提出すること。

情報セキュリティインシデントの発生に伴い、当該契約の履行が困難な場合には、国際農研担当者との打ち合わせの上、決定することとする。

報告が必要な情報セキュリティインシデントの例は以下のとおり。次に掲げる場合において、受注者は、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を報告しなければならない。また、その後速やかに詳細を国際農研に報告しなければならない。

・要保護情報が保存されたサーバ等の不正プログラムへの感染又は不正アクセスが認められた場合
・要保護情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に不正プログラムへの感染又は不正アクセスが認められ、要保護情報が保存されたサーバ等に不正プログラムへの感染又は不正アクセスのおそれがある場合
・要保護情報の漏えい、紛失、破壊等のトラブルが発生した場合

(2)情報セキュリティインシデント等の対処等

①　対処体制及び手順

受注者は、情報セキュリティインシデント、その疑いのある場合及び情報セキュリティリスクに適切に対処するための体制、責任者及び手順を定め、国際農研に提出しなければならない。

②　証拠の収集・保存と解決

受注者は、情報セキュリティインシデントが発生した場合、その疑いのある場合には、発生したインシデントの種類に応じた要因特定が可能となる証拠等の収集・保存に努めなければならない。また、速やかに対処策・改善策を検討し、適用すること。

③　情報セキュリティインシデント発生に伴う報告

受注者は、発生した情報セキュリティインシデントの経緯及び対応結果（リスク未対応の有無を含む）を国際農研に報告し、概要について国際農研との共有を図ること。また、必要に応じて、情報セキュリティ実施手順の見直しも検討すること。

6.　その他

(1)国際農研による調査の受入れと協力

受注者は、国際農研による情報セキュリティ対策に関する調査の要求があった場

合には、これを受入れなければならない。また、国際農研が調査を実施する場合、国際農研の求めに応じ必要な協力（職員又は国際農研の指名する者の取扱施設への立入り、書類の閲覧等への協力）をしなければならない。

(2)業務遂行上疑義が発生した場合は、速やかに国際農研に申し出ること。発生した疑義は協議の上、対応を決定するものとする。

(3)本基準に定めのない事項については、国際農研情報セキュリティポリシーを参照し、適切に実施すること。