仕　様　書

1. 件名

財務会計システム用サーバ等設定業務

2. 納品場所

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

3. 履行期間

契約締結日から令和５年１月２７日まで
ただし、具体的なスケジュールは「6.業務内容及びスケジュール」を参照。

4. 目的と調達の概要

財務会計システムは、国際農林水産業研究センター（以下「国際農研」という。）における予算の執行から契約決議、支出決議に至る予算執行管理及び独立行政法人会計基準に基づく会計管理、出納管理、決算管理並びに取得、償却、移動を管理する資産管理を行う基幹となるシステムであり、国際農研業務の推進上、重要な役割を担っている。

現行財務会計システムは 2016 年より運用しており、サーバ等のハードウェアが保守期限を迎えたため、リプレイスに伴う環境設定が必要な状態にある。そのため、本契約により、同システムのデータ移行のための環境設定を実施し、安定稼働を担保する。

なお、データ移行は本契約には含まない。

5. 国際農研提供機器

別紙物品リストの通り。

6. 業務内容及びスケジュール

受注者は、「５.国際農研提供機器」に対し、以下のスケジュールに従い、財務会計システムデータ移行に必要な環境設定を実施する。

万が一、以下のスケジュールでの作業が困難な場合には、国際農研担当者に申し出を行い、日程の再調整を行うこと。

＊6.1-6.3 に記載した業務の全体的な予備日は令和４年１２月２５日とする。

6.1　サーバ環境構築完了：令和４年１２月１５日（木）

OVF取得候補日：令和４年１２月１０日・１１日

「8. サーバ環境の構築」参照。

6.2　財務会計システムデータ移行作業立ち会い

作業候補日：令和４年１２月１８日

（予備日）：令和４年１２月１９日

「9. 財務会計システムデータ移行作業立ち会い」参照。

6.3　周辺機器（L4スイッチ、外付けUSBハードディスクドライブ、UPS等）接続、設定変更ならびに各種動作検証の実施

：財務会計システムデータ移行完了次第

「10. 周辺機器（L4スイッチ、外付けUSBハードディスクドライブ、UPS等）接続、設定変更ならびに各種動作検証」の実施

6.4　各種設定書・完成図書の作成・確認・納品

：令和５年1月２７日（金）

「13. 各種設定書・完成図書」参照。

7. システム構成等

国際農研提供機器の所外への持ち出しは許可しない。国際農研コンピュータ室での作業を原則とする。

ネットワークプロトコルは、TCP／IPの利用を前提とする。

7.1　本調達により購入を必要とするもの

・外付けUSBハードディスクドライブ（USB3.1以上、2TB以上）１個

「10.2.1参照」

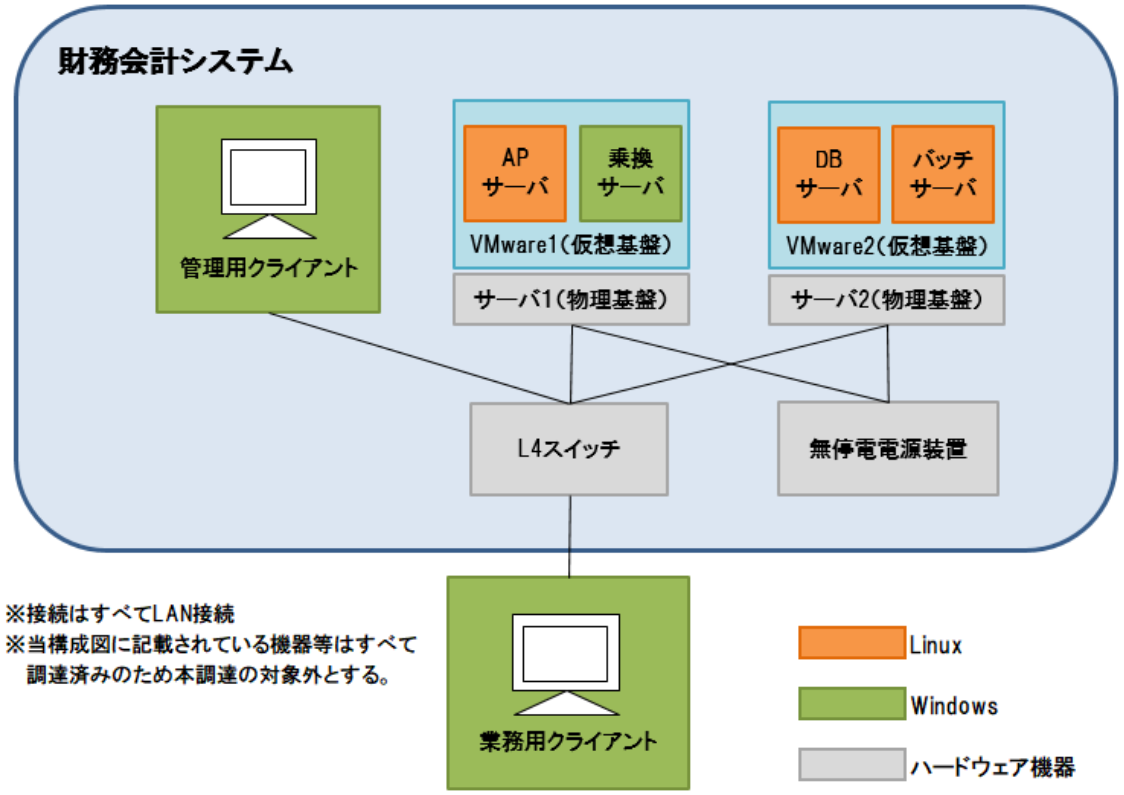
・無停電電源装置に対応する電源管理ソフトウェア

（PowerChute Network Shutdown　1 Node Virtualization）　2式

「10.3.1 参照」

7.2　「システム構成図」

財務会計システム構成図（案）を以下に示す。



8. サーバ環境構築

8.1 員数検査・外観検査の実施

8.2 財務会計システム用サーバ２台（物理基盤）の上に、物理サーバ用OS（VMware vSphere 7 Essentials for 3 hosts（ライセンス5年付））を利用し、仮想基盤を構築（インストール）すること。

8.3 現行財務会計システムの仮想サーバ４台（APサーバ、乗換案内サーバ、DBサーバ、バッチサーバ）のOVF(※1)を取得する。

（※1）OVF とは：仮想マシンの構成や状態を丸ごとデータとしてファイルに写し取ることができるデータ形式の一つ。仮想化ソフトの種類を問わず仮想マシンの複製等が可能

8.4 8.3で取得した各サーバのOVFファイルを利用し、8.2で構成した仮想基盤に複製する。サーバの構成は7.2「システム構成図」参照。

9. 財務会計システムデータ移行作業立ち会い

「8.サーバ環境構築」において構築した環境に、現行財務会計システムサーバよりデータ移行を行う。データ移行は別契約により他受注者が実施する予定。データ移行時のトラブル等への即時対応のため、立ち会い、設定修正等に対応し、記録する。

10. 周辺機器（外付けUSBハードディスクドライブ、UPS、L4スイッチ等）接続、設定変更

10.1 設定情報の変更

9.財務会計システムデータ移行後のサーバにおいて、IPアドレス（接続先）変更が伴う場合は、設定情報の変更を行うこと。なお、本作業を実施するにあたり、必要な情報については国際農研より提供する。

10.2 外付けUSBハードディスクドライブへのフルバックアップ設定（手動）

10.2.1 復元ポイント管理用の外付けUSBハードディスクドライブ（USB3.1以上、4TB以上）を購入

10.2.2 財務計システムのシステム全体に対するシステムバックアップ（フルバックアップ）をVMwareのイメージバックアップ機能などを利用して取得できるようにする設定すること。なお、取得したデータは、管理用クライアントを介して、ＵＳＢハードディスクドライブに手動でバックアップできること。

10.2.3 原則として現行サーバの設定を継承すること。

10.3 会計でのバックアップ設定（自動タスク）

10.3.1 財務会計システムのデータベースのバックアップを、DBサーバのディレクトリ上に自動生成する設定を行うこと。
自動生成したバックアップの世代管理は、10世代保管とする。

10.3.2 10.3.1で作成したバックアップデータは、定期的に財務会計システムのアプリケーションサーバ（APサーバ）上に保存し、２重化を図ること。

10.3.3 DBサーバドライブ故障等緊急時対策として、財務会計システムのアプリケーションサーバ（APサーバ）から財務会計システム用データベースサーバ（DBサーバ）にバックアップファイルを戻すための手順書を作成すること。

10.4 10.2ならびに10.3で取得したバックアップデータからのリストア手順書の作成

「10.2の復元ポイント用フルバックアップ」ならびに「10.3の会計システムデータベースの世代管理バックアッル」を利用したリストア手順書を作成すること。

10.5 無停電源装置（UPS）の設定

10.5.1 「5.国際農研提供機器」中の無停電電源装置に対応する電源管理ソ

フトウェア(PowerChute Network Shutdown　1 Node Virtualization　2式)を購入する。

10.5.2 各サーバに無停電電源装置を接続し、インストール後、必要な以下の設定を行うこと。

・停電などによる障害が発生時を想定し、各物理サーバ２式及び仮想サーバ４式が安全に停止を担保するため、一定時間の電源供給と自動シャットダウン等タスクの設定

10.5.3 電源（分電盤）は国際農研で指定されたものを使用すること

10.6 L4スイッチの接続

すべての設定が完了後、L4 スイッチの指定ポートに接続する。

11. 新財務会計システム動作検証と結果の共有

11.1 検証内容

・UPS設定検証（自動シャットダウン　等）

・バックアップ検証（手動実行、タスク自動実行）

・サーバ機器のアップデート等の正常動作確認

・上記の他、検証が必要と思われる事項

（国際農研担当者と打ち合わせの上、実施を検討する）

なお、動作検証の実施にあたっては、随時国際農研担当者へ報告の上、結果の共有を図ること。

万が一、トラブル等が発生した場合には、具体的な対応策の提案等を行うこと。

11.2 動作検証完了後

すべての動作検証が完了後、復元ポイント管理用の外付けUSBハードディスクドライブに手動でフルバックアップを実施すること。取得するタイミングについては国際農研担当者と協議の上、決定すること。

12. 各種設定書・完成図書

12.1 本業務により実施した各機器の設定書、システム構成図、メンテナンス手順書、リストア手順書等を完成図書（冊子体　1部）提出すること。併せてPDF形式の完成図書をCD-ROMに保存して1部提出すること。

12.2 提出する資料は、事前に国際農研担当者と協議・確認の上、決定すること。

12.3 調達した機器及びソフトウェアにメーカマニュアルが付属する場合には、

メーカマニュアルも提供すること。

13. 検収要件

以下に示す事項の合格をもって検収とする。

13.1 「11.新財務会計システム動作検証」において、正常な確認がとれていること。

13.2 「12.各種設定書・完成図書」に示す完成図書等の提出

14. 資格要件

当該業務に関する情報セキュリティ管理、品質管理、対象システムのサービス管理及びリスク評価等について実務レベルの高い能力を有すること。その証左として

・ISO9001

・ISO27001

を取得していることを示すため、入札時に認定証の写しを提出すること。

15. 免責事項

・財務会計システムの動作及びデータ移行

・財務会計システムクライアントのセットアップ

・国際農研の都合により受注者に無断で機能を変更し、当初設定した機能を失った場合

・国際農研の管理上の原因による故障等が発生した場合

16. 業務遂行上の条件

16.1 作業計画書の作成について

国際農研にて作業を行う際は、以下の情報を作業予定日の3日前までに提示し、許可を得ること。

・作業日時

・所要時間

・作業場所

・作業者

・作業対象及び作業内容

・当該作業による業務等への影響とその範囲調達プログラム

16.2 受注者は、本契約の履行に当たり、必要な事項について事前に国際農研と協議すること。

16.3 本仕様書の記載内容及び解釈に疑義が生じた場合は、速やかに国際農研と協議すること。本仕様書に記載の無い事項については、国際農研と協議の上で対応を決めることとする。

16.4 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。

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。

別紙物品リスト

No.	用途	品名	メーカ名	型番	数量
1	財務会計システム用サーバ①	PowerEdge T550 サーバー	デル・テクノロジーズ株式会社	T550	1
2	財務会計システム用サーバ②	PowerEdge T550 サーバー	デル・テクノロジーズ株式会社	T550	1
3	無停電電源装置	APC Smart-UPS 1500 LCD Tower 100V オンサイト4年保障	シュナイダーエレクトリック	SMT1500J-H4	1
		Network Management Card 3	シュナイダーエレクトリック	AP9640J-H4	1
4	管理用PC	OptiPlex 3000 Small Form Factor	デル・テクノロジーズ株式会社	-	1
	モニタ	Dell モニタ（4年延長 ベーシック交換サービス）	デル・テクノロジーズ株式会社	SE2222H	1
5	KVMスイッチ	CS1794 -4-Port USB HDMI KVMP Switch W/JP ADP	ATEN	CS1794	1
6	物理サーバ用OS	VMware vSphere 7 Essentials for 3 hosts（ライセンス5年付）	vmware	528-CKIF	1