仕様書

1. 件名

財務会計システムサーバ等機器保守及び運用支援業務

2. 作業場所

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. 保守期間

令和 7 年 4 月 1 日から令和 8 年 3 月 31 日まで（12 ヶ月）

4. 目的

国際農研の財務会計システムサーバ等機器の運用に対し、国際農研担当者を支援し、安定稼働を担保する。

5. 対象機器等

財務会計システム用サーバ 2 台（仮想マシン 4 台)、管理用 PC、周辺機器及び無停電電源装置、財務会計システム用 L4 スイッチ（内訳は別紙 1 のとおり）

6. 定期点検 の実施

6.1）-4）記載した各対象機器に対する定期点検を期間内に２回実施すること。実施日等は、事前に書面等で国際農研担当者と調整の上決定すること。

定期点検時に使用する各コマンドはキックオフ打ち合わせ時に国際農研担当者より指定する。

定期点検の実施により、万が一、異常を発見した場合には、国際農研担当者へ報告を行うとともに、速やかに適切な策を提案し、講ずること。

1） 財務会計サーバ（2 台 VMware vSphere を利用）

(1) 健全性ステータスの確認

異常がないことを確認すること。

・ CPU

・ メモリ

・ ストレージ・RAID コントローラ

・ 電源・ファン

(2) DVD-ROM 装置：正常に読み込みできることを確認すること。

(3) クリーニング

筐体外部・DVD ドライブ・コネクタ部に塵埃が認められた場合は、クリーニングを実施すること。

2) 仮想サーバ（Linux：AP サーバ、DB サーバ、バッチサーバ）

(1) セキュリティパッチの適用

適用するセキュリティパッチは、アプリケーションソフトウェアの開発元（株式会社 NTT データアイ）の検証が取れたパッチのみを適用すること。具体的な検証結果は国際農研担当者より提供する。 なお、セキュリティパッチの適用は、必ず各仮想マシンのシステムバックアップ取得後に実施すること。あわせて、セキュリティパッチ正常適用後も各仮想マシンのシステムバックアップを取得し、適用前後の 2 世代を国際農研の指定する場所に保存すること。

セキュリティパッチの適用手順は、国際農研が提供する手順書に従って作業を行うこと。

万が一、セキュリティパッチ適用時にトラブルが発生した場合には、速やかに適用前の状態に戻すなど、業務に影響が生じないようにすること。

(2) OS・CPU・メモリ

国際農研が指定するコマンドを使用し、システムログに問題となるエラーが出力されず、正常に起動していることを確認すること。

(3) ディスク

オペレーティングシステム上から、正常に書き込み、読み込みがで きることを確認すること。さらに、国際農研が指定するコマンドを使用し、システムから正常に認識されていることを確認すること。

(4) ネットワークインタフェース

国際農研が指定するコマンドを使用し、ネットワークインタフェースが機能していることを確認すること。

(5) 動作ログ等の確認・保存・待避

国際農研が指定するコマンドを使用し、下記の項目についての情報を収集し、サーバ上に保存すること。

・ 動作ログ

・ 設定ファイル

・ パッケージ情報

・ 稼働状態

(6) ウイルス対策ソフト（別紙 1 参照）の各種メンテナンス等

インストールされたウイルス対策のメンテナンスとして以下を実施すること。

・ パターンファイルの更新

・ ウイルス等検知状況の確認

・ セキュリティパッチの適用（必要に応じて）

・ ウイルス対策ソフトのバージョンアップ（必要に応じて）

3) 仮想サーバ（Windows：乗換案内サーバ）

(1) OS・CPU・メモリ

イベントビューアー中の Windows ログの「システム」に問題となるエラーが出力されておらず、正常に起動していることを確認すること。

(2) ディスク

オペレーティングシステム上から、正常に書き込み、読み込みでき ることを確認すること。

(3) ネットワークインタフェース

国際農研が指定するコマンドを使用し、ネットワークインタフェースが機能していることを確認すること。

(4) 動作ログの確認・保存・待避

国際農研が指定するコマンドを使用し、下記の項目についての情報を収集し、サーバ上に保存すること。

・ Windows ログの「システム」、「セキュリティ」、「Application」

(5) ウイルス対策ソフト（別紙 1 参照）の各種メンテナンス等

インストールされたウイルス対策のメンテナンスとして以下を実施すること。

・ パターンファイルの更新

・ ウイルス等検知状況の確認

・ セキュリティパッチの適用 （必要に応じて）

・ ウイルス対策ソフトのバージョンアップ（必要に応じて）

4) 周辺機器

(1) KVM スイッチ

コンソール切替が正常に行われることを確認する。また、筐体外部・コネクタ部に塵埃が認められる場合は、クリーニングを実施すること。

(2) 無停電電源装置

① 本体・出力容量

Web 管理画面にログインし問題となるエラー表示等がなく、接続機器に電源が供給されていることを確認すること。また、筐体外部・コネクタ部に塵埃が認められる場合は、クリーニングを実施すること。

② 動作確認

無停電電源装置の電源供給を遮断し、正常に各機器のシャットダウンが行われるかを確認すること。

5) 管理用端末（Windows 10 Pro）

管理端末は、本年度中に OS のサポート期限を迎えるため、8.4）に記載した Windows 11 Pro へのアップグレードを実施し、保守対象を継続すること。

(1) OS・CPU・メモリ

イベントビューアー中の Windows ログの「システム」に問題となるエラーが出力されず、正常に起動していることを確認すること。

(2) ディスク

正常に書き込み、読み込みできることを確認すること。

(3) DVD-ROM 装置

正常に読み込みできることを確認すること。

(4) モニタ

正常に画面表示されることを確認すること。

(5) ネットワークインタフェース

国際農研が指定するコマンドを使用し、ネットワークインタフェースが機能していることを確認すること。

(6) クリーニング

筐体外部・DVD ドライブ・コネクタ部に塵埃が認められた場合は、クリーニングを実施すること。

7. サーバの設定情報及び動作ログの確認と待避・保存（6. 定期点検時に実施）

サーバの設定情報および動作状態（ログ）の収集を行い、国際農研が指定する場所に保存すること。

保存したログを確認し、情報セキュリティ上の問題点や、システムの改善につながる、あるいは将来的な障害につながる事案が発見された場合は、作業報告書により国際農研に報告すること。

なお、作業の結果、設定内容など、構築・導入時の設計書の記載に変更が生じた場合は、変更履歴を含めて適宜これを修正し国際農研に提出すること。

8. 運用支援の実施

1) 5.に明記した 対象機器の運用に関する国際農研担当者からの問い合わせに対応するこ と。問い合わせは、メール、電話または FAX で対応すること。

2) 対象機器の製品開発元ならびに JPCERT/CC 等から最新の脆弱性情報を入手すること。入手した脆弱性の中に本システムに該当する緊急かつ重大な事項を発見した場合は、対処の要否、可否を適切に判断するとともに、速やかに国際農研担当者に報告し、国際農研の判断に従って必要な対処を行うこと。実施した対処結果は実施結果（対処方法)、ならびに対処の可否（否の理由、代替措置およびその影響）をまとめ記録するとともに、国際農研担当者に報告し承認を得ること。後日、対処を行う事案は対処予定日等の提示を行うこと。

3) 財務会計システム用サーバ上で稼働する仮想マシン（Windows Server 1 台)並びに管理用端末（Windows 10 Pro）に対して、セキュリティパッチの適用作業を履行期間中に毎月実施すること。各作業日は国際農研と調整の上、決定すること。

4) 管理用端末のサポート終了（2025. 10）に伴い、当該機器を Windows 11 Pro へアップグレードすること。アップグレードは国際農研担当者と事前に日程調整の上、サポート終了前に実施すること。また、アップグレード後も実施前と同様の作業（各種サーバへのアクセス等）が可能であることを確認し、作業報告書として提出すること。

5) 財務会計システム用サーバ上で稼働する仮想マシン 4 台並びに財務会計システム用サーバ 2 台のハードディスク使用率の確認を月 1 回行うこと。

6) 財務会計システム用 L4 スイッチに関する情報を入手し、重大なセキュリティホールが発見された場合は、国際農研担当者に相談の上、速やかにメーカー提供の新たなファームウェアの更新を適用すること。

また、原則として契約期間中 1 回、国際農研の要請によりアクセスフィルタリング設定の変更を行うとともに、設定情報の履歴管理を実施すること。

なお、設定変更を行う場合には事前に十分な検証を実施し、業務や所内ネットワークに影響を及ぼすことがないよう、注意すること。

7) トラブル・障害等への対応（財務会計システム構成機器、管理用端末と仮想サーバ等のインターネット接続を含む）

(1) 対象機器に障害が発生した場合には、問題が対象機器にあるか、他の原因であるかの切り分け作業を行うこと。

(2) 対象機器に障害が発生した場合には、速やかにベンダーへの連絡、修理または交換作業およびベンダー作業の完了確認を行うこと。

なお、機器のベンダーが提供する保守については、国際農研が別途契約済みである。

(3) 対象機器に含まれるソフトウェアに対し、製品の動作不具合に関する問い合わせへの対応、対策ソフトウェアの提供、適用を行うこと。

(4) Windows サーバや管理用端末のアップデートが正常に行われない等、仮想サーバや管理用端末のインターネット接続に障害が発生した場合には、問題が対象機器にあるか、他の原因であるかの切り分け作業を行うこと。対象機器が原因である場合には、正常な状態となるよう復旧作業を行うこと。

8) ソフトウェアの更新

更新対象となっているソフトウェア（別紙 1 参照）については、1 年分の使用権を提供すること。

9) 研修の実施

管理方法についての研修を年 1 回行うこと。実施時期については担当者と協議の上定めること。

9. 業務遂行上の条件

1) 運用支援業務実施日等

3. 保守期間に明示した原則月～金曜日の午前 9 時から午後 5 時 15 分内とし、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）を除くとする。ただし、定期点検等運用支援以外の業務ならびに、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求める場合がある。

2) 打ち合わせ議事録の提出

本業務の実施に関して国際農研と打ち合わせ・協議等の際には、5 営業日以内に議事録を提出し国際農研の承認を受けること。この議事録については、受注者と国際農研の双方で保管する。

3) 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 7 営業日前までに提示し、許可を得ること。障害対応など、緊急の場合は国際農研と調整すること。

・ 作業日時

・ 作業者

・ 所用時間

・ 作業場所

・ 作業対象及び内容（設定変更やバージョンアップと行う場合には変更内容）

4) 作業報告書の作成と提出

9.3)に示す作業の実施後は、以下の内容を記載された作業報告書を 5 営業日以内に議事録を提出し国際農研の承認を受けること。

・ 作業日時

・ 作業者

・ 所用時間

・ 作業場所

・ 作業内容及び結果（作業結果を詳細に）

万が一、予定していた作業が未完の場合でも、その旨がわかるように記載し提出すること。

5）トラブル・障害時対応計画ならびに報告書の作成と提出

8..6）に明記したトラブル・障害等への対応については、速やかに事象確認の上、対応計画書を国際農研管理者に提出すること。また、対応実施後は、月次報告書として、以下の内容を含む月次報告書を作成し、翌月 20 日までに国際農研管理者に提出すること。

・ 障害対応

・ トラブル・障害対応後の定期点検

・ 仮想サーバ４機のハードウェアディスク使用率

・ 問い合わせ対応

・ 情報セキュリティ対策作業

・ 上記各業務の実施状況

10. その他

1）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。

2）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。

3）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。

別紙１：財務会計システム 構成機器及び保守対象一覧

No	機器名	品名	数量	保守契約*	更新**
財務会計システム用サーバ					
1	財務会計システム用サーバ	Dell PowerEdge T550	2	o	—
2	仮想化基盤ソフトウェア	VMware vSphere 7 Essentials K it for 3 hosts(Max 2 CPUs per host)	1	o	—

3	AP サーバ/DB サーバ/バッチサーバ用オペレーティングシステム	Red Hat Enterprise Linux Serv er release 8.8 (2 ソケット or 2 ゲスト)	2	o	—
4	乗換案内サーバ用オペレーティングシステム	Microsoft Windows Server 2019 St andard(1809) ビルド 17763.5329	1	—	—
5	乗換案内サーバ接続用 Windows CAL	CSP WINDOWS SERVER 2022-1 USE R CAL	3	—	—
6	ウィルス対策ソフトウェア（AP サーバ/DB サーバ/バッチサーバ)	ServerProtect for Linux Ver3.0 PKG	3	o	o
7	ウィルス対策ソフトウェア（乗換案内サーバ/管理用 PC）	TrendMicro ApexOne	2	o	o
周辺機器					
8	KVM スイッチ	ATEN CS1794 -4-Port USB HDMI KVMP Switch W/JP ADP	1	o	—
無停電電源装置					
9	無停電電源装置	APC Smart-UPS 1500 LCD Tower 100V	1	o	—
10	無停電電源装置用ネットワークカード	Network Management Card 3	1	o	—
11	電源管理ソフトウェア	PowerChute Network Shutdown 1 Node Virtualization	2	—	—
管理用 PC					
12	管理用 PC	Dell OptiPlex 3000 ｽﾓｰﾙﾌｫｰﾑﾌｧｸﾀ	1	o	—
13	モニタ	Dell モニタ	1	o	—
L4 スイッチ					
14	L4 スイッチ	C9300L-24T-4G-A	1	o	—

* 保守契約：当センターがベンダーの保守を契約済みであるものはo

** 更新：本仕様に従い、受注者が調達を要するものはo

別紙２

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５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、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の確保に関する特約条項

第１条　受注者は、契約締結後、別添の「調達における情報セキュリティ基準」（以下「基準」という。）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、発注者に提出し、確認を受けなければならない。

２　情報セキュリティ実施手順の作成は、基準に従い作成しなければならない。

３　発注者は、受注者に対して情報セキュリティ実施手順及びそれらが引用している文書の提出、貸出し、閲覧、又は説明を求めることができる。

第２条　受注者は、前条において発注者の確認を受けた情報セキュリティ実施手順に基づき、この契約に関する要保護情報を取り扱わなければならない。

第３条　受注者は、契約の履行に係る作業に従事する全ての者（再委託先等を含む）の故意又は過失により要保護情報の漏えい、紛失、破壊等の事故があったときであっても、契約上の責任を免れることはできない。

第４条　受注者は、やむを得ず要保護情報を第三者に開示する場合には、あらかじめ、開示先において情報セキュリティが担保されることを確認した上で、発注者に申し出を行い、手続きの上発注者の許可を得なければならない。

２　受注者は、第三者との契約において受注者の保有し、又は知り得た情報を伝達、交換、共有その他提供する約定があるときは、要保護情報をその対象から除く措置を講じなければならない。

第５条　発注者は、基準等に定める情報セキュリティ対策に関する調査を行うことができる。

２　発注者は、前項に規定する調査を行うため、発注者の指名する者を受注者の事業所、工場その他の関係場所に派遣することができる。

３　発注者は、第１項に規定する調査の結果、受注者の情報セキュリティ対策が情報セキュリティ実施手順を満たしていないと認められる場合は、その是正のため必要な措置を講じるよう求めることができる。

４　受注者は、前項の規定による発注者の求めがあったときは、速やかにその是正措置を講じなければならない。

５　受注者は、発注者が受注者の再委託先等に対し調査を行うときは、発注者の求めに応じ、必要な協力を行わなければならない。また、受注者は、受注者の再委託先が是正措置を求められた場合、講じられた措置について発注者に報告しなければならない。

第６条　受注者は、要保護情報の漏えい、紛失、破壊等の情報セキュリティインシデントが発生したときは、あらかじめ作成し、発注者の確認を受けた情

報セキュリティ実施手順に従い、発注者に報告しなければならない。

２　受注者は、第１項に規定する情報セキュリティインシデントが当該契約及び関連する物品の運用等に与える影響等について調査し、その措置について発注者と協議しなければならない。

３　第１項に規定する情報セキュリティインシデントが受注者の責めに帰すべき事由によるものである場合には、前項に規定する協議の結果取られる措置に必要な経費は、受注者の負担とする。

４　前項の規定は、発注者の損害賠償請求権を制限するものではない。

第７条　発注者は、受注者の責めに帰すべき事由により前条第１項に規定する情報セキュリティインシデントが発生し、この当該契約の目的を達することができなくなった場合は、この当該契約の全部又は一部を解除することができる。

２　前項の場合においては、主たる契約条項の契約の解除に関する規定を準用する。

第８条　第２条、第３条、第５条及び第６条の規定は、契約履行後においても準用する。ただし、当該情報が要保護情報でなくなった場合は、この限りではない。

２　発注者は、業務に支障が生じるおそれがない場合は、受注者に要保護情報の返却、提出、破棄又は抹消を求めることができる。

３　受注者は、前項の求めがあった場合において、要保護情報を引き続き保有する必要があるときは、その理由を添えて発注者に協議を求めることができる。

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。