# 仕 様 書

1. 件名
   オンライン会議システム（CISCO Webex）ライセンス更新

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)

3. 納入期限　：　令和４年８月31日
   ※ライセンス利用期間は令和４年 ９月１日～令和５年８月31日

4. ライセンス種別と数量
   種別：「Cisco Webex Active User」
   ライセンス数は、現在の利用実績に基づき算出するとともに、ライセンス数を算出した根拠となる資料を見積書ほか提出書類と併せて提出すること。
   ※現在の利用ライセンス数は42であり、令和４年 ８月１日に上記更新期間分のライセンス数が確定する。数量は直接 Cisco へ問い合わせること。

5. 調達の概要
   - ライセンス数の算出と１年間の期間の延長にあたり、現在利用中のサイト情報はCiscoテイクオーバー制度を利用し継承すること。
   - 国際農研担当者からの問い合わせ対応・支援

   注）受注者の変更を要因とする設定の変更やシステム利用不可等が生じないよう、調達を行うこと。

6. 国際農研提供情報
   ・サイト情報（Webexサブスクリプション ID）や管理者情報　等

7. 業務遂行上の条件
   - 現在利用中のサイト情報と各種設定を継承すること。
   - 受注者の変更に伴う設定変更等が生じないように注意すること。
   - 現行ライセンス期間との利用期間の欠損や重複が生じないように、契約更新を行うこと。
   - 国際農研担当者からの問い合わせ（主にメール）用の窓口を整備し、問い合わせに対応すること。

8. 情報セキュリティに関する遵守事項
   - 受注者に提供する情報は、本業務を遂行するためのものである。業務の遂行以外の目的で情報を利用しないこと。
   - 受注者は、「調達における情報セキュリティ基準」に則り、情報の取扱い、情報セキュリティインシデント等への対処体制等に関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。
   - 本業務の実施にあたり、受託者は国際農研の意図しない変更が行われな

いことを保証するための品質保証体制を定め、国際農研に提出すること。国際農研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、追跡調査や立入調査等国際農研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すること。

- 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情報を提出すること。
- 本業務において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに国際農研に報告しなければならない。
- 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、国際農研は、本仕様書において求める情報セキュリティ対策の実績について、随時報告を求めることができる。
- 上記の報告に基づき、情報セキュリティ対策の履行が不十分である可能性を国際農研が認めた場合は、両者による協議を行い、合意した対応を採ること。
- 本仕様書において国際農研が求めるセキュリティ要件及び受注者が本業務の遂行のために整備したセキュリティ対策を、本業務に従事する全ての者に周知徹底すること。
- 国際農研内で業務を遂行する際、受注者が持ち込んだ機器の国際農研内通信回線への接続は禁止とする。
- 本業務で取り扱う各種情報のうち、要保護情報として取り扱う情報の範囲及びその格付け・取扱制限、パスワード生成ルール等については、初回ミーティング等で共有するなど、必要となる対策を検討し、実施すること。
- 本業務で取り扱う要保護情報が不要になった場合は、確実に返却または抹消すること。
- 国際農研が保有する情報について、本業務実施のために提供され又は許可を受けたもの以外の情報にアクセスしてはならない。

9. 関連規程

- 本業務の遂行にあたっては、「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」の最新版、「国際農林水産業研究センター情報セキュリティポリシー関係規程」等を参照し、必要に応じて国際農研の説明を受け、定められている事項を遵守すること。
- 「個人情報の保護に関する法律」（平成 15 年法律第 57 号）の内容を遵守遂行すること。

10. 提出物

受注者は、各業務完了後、速やかに、当システム開発ベンダーCisco とのライセンス更新完了が確認できる書類を国際農研担当者に提出すること。

11. 応札者の条件

下記書類を提出できること。

- 本業務において、適切に業務を実施できることの証明として、以下の証明書類等を提出すること。開発ベンダー（Cisco）から法人契約のパートナー指定を有していることが証明可能な書類（写し可）
- 情報セキュリティ管理
  適切な情報セキュリティ管理を実施できることの証明として、情報セキュリティマネジメントシステム(ISMS)認証の写し
- 実施体制図
  連絡窓口（担当者）を明記した本契約を実施するための体制図

12. 再委託
- 受注者は、受注業務の全部又は主要部分を第三者に再委託することはできない。受注業務の一部を再委託する場合は、事前に再委託する業務、再委託先等を国際農研に申請し、承認を得ること。
- 本仕様書等が定める受注者の責務は、再委託先も負う。なお、再委託された業務に係る最終的な責任は受注者が負う。

13. 国際農研体制
- 担当者
  ・企画連携部研究基盤室デジタル科
  連絡先　TEL：029-838-6340
- 契約関係
  ・総務部財務課調達第２係
  連絡先　TEL：029-838-6327

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

# 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又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。