

企画競争説明書

業務名称： インドネシア国サイバーセキュリティ人材育成プロジェクト（オープンソースソフト開発／サイバーセキュリティ技術）

調達管理番号： 22a00075

【内容構成】

第1章 企画競争の手続き

第2章 特記仕様書案

第3章 プロポーザル作成に係る留意事項

本説明書は、「独立行政法人国際協力機構（以下、JICA という）」が、民間コンサルタント等に実施を委託しようとする業務について、当該業務の内容及び委託先を選定する方法（企画競争）について説明したものです。

企画競争とは、競争参加者が提出する技術提案書（以下「プロポーザル」という。）に基づき、その企画、技術の提案、競争参加者の能力等を総合的に評価することにより、JICA にとって最も有利な契約相手方を選定する方法です。競争参加者には、この説明書及び貸与された資料に基づき、本件業務に係るプロポーザル及び見積書の提出を求めます。

なお、本説明書の第2章「特記仕様書案」、第3章2. 「業務実施上の条件」は、プロポーザルを作成するにあたっての基本的な内容を示したものですので、競争参加者がその一部を補足、改善又は修補し、プロポーザルを提出することを妨げるものではありません。プロポーザルの提案内容については、最終的に契約交渉権者を行う契約交渉において、協議するものとしています。

2022年4月27日

独立行政法人国際協力機構
調達・派遣業務部

第1章 企画競争の手続き

1. 公示

公示日 2022年4月27日

2. 契約担当役

理事 植嶋 卓巳

3. 競争に付する事項

- (1) 業務名称：インドネシア国サイバーセキュリティ人材育成プロジェクト（オープンソースソフト開発／サイバーセキュリティ技術）
- (2) 業務内容：「第2章 特記仕様書案」のとおり
- (3) 適用される契約約款：
 - () 「調査業務用」契約約款を適用します。これに伴い、消費税課税取引と整理しますので、最終見積書において、消費税を加算して積算してください。（全費目課税）
 - (○) 「事業実施・支援業務用」契約約款を適用します。これに伴い、契約で規定される業務（役務）が国外で提供される契約、すなわち国外取引として整理し、消費税不課税取引としますので、最終見積書においても、消費税は加算せずに積算してください。（全費目不課税）
- (4) 契約履行期間（予定）：2022年7月 ～ 2023年4月

新型コロナウイルス感染拡大等による影響により、本企画競争説明書に記載の現地業務時期、契約履行期間、業務内容が変更となる場合も考えられます。これらにつきましては契約交渉時に協議のうえ決定致します。

4. 担当部署・日程等

- (1) 選定手続き窓口
調達・派遣業務部 契約第一課
電子メール宛先：outm1@jica.go.jp、担当者メールアドレス：Keiji.Kawaguchi@jica.go.jp

- (2) 事業実施担当部
ガバナンス・平和構築部 STI・DX室

- (3) 日程
本案件の日程は以下の通りです。

No.	項目	期限日時
1	企画競争説明書に対する質問	2022年 5 月 11日 12時
2	競争参加資格確認申請書	2022年 5 月 13日 12時

3	質問への回答	2022年 5 月 16日
4	競争参加資格要件の確認結果の通知日	2022年 5 月 20日
5	プロポーザル等の提出用フォルダ作成依頼	プロポーザル等の提出期限日の 4営業日前から1営業日前の正午まで
6	本見積書及び別見積書、プロポーザル等の提出期限日	2022年 5 月 27日 12時
7	プレゼンテーション	行いません。
8	評価結果の通知日	2022年 6 月 7日
9	技術評価説明の申込日（順位が第1位の者を除く）	評価結果の通知メールの送付日の翌日から起算して7営業日以内

5. 競争参加資格

(1) 各種資格の確認

以下についてはコンサルタント等契約におけるプロポーザル作成ガイドライン（2022年4月）」を参照してください。

(URL:https://www.jica.go.jp/announce/information/20220330_01.html)

- 1) 消極的資格制限
- 2) 積極的資格要件
- 3) 競争参加資格要件の確認
- 4) 全省庁統一資格の経過措置

令和4年度は全省庁統一資格の更新時期にあたりますが、更新にかかる期間も考慮し、2022年4月1日～2022年6月30日までの期間を経過措置期間と位置づけ、当該期間中の公告・公示案件では、令和元・02・03年の全省庁統一資格にて代替することを認めます。

(URL : <https://www.jica.go.jp/announce/information/20211216.html>)

(2) 利益相反の排除

具体的には、以下に掲げる者については、競争への参加を認めません。

特定の排除者はありません。

(3) 共同企業体の結成の可否

共同企業体の結成を認めます。ただし、業務主任者は、共同企業体の代表者の者とします。

共同企業体を結成する場合は、共同企業体結成届（様式はありません。）を作成し、プロポーザルに添付してください。結成届には、代表者及び構成員の全ての社の代表者印又は社印は省略可とします。また、共同企業体構成員との再委託契約は認めません。

(4) 競争参加資格要件の確認

競争参加資格要件を確認するため、以下の要領で競争参加資格確認申請書の提出を求めます。プロポーザル作成ガイドラインP. 49-50「【「競争参加資格確認申請書」の提出を求められた場合】」に記載の各種書類を提出ください。

なお、本資格確認審査プロセスを追加するため、同ガイドラインにおける「消極的資格制限」の3)に規定している「競争参加日」は、プロポーザル等の提出締切日ではなく、資格確認申請書の提出締切日に読み替えます。

- 1) 提出期限： 上記4. (3) 日程参照
- 2) 提出方法： 下記「8. プロポーザル等の提出」参照し、上記1)の提出期限日の4営業日前から1営業日前の正午までに、競争参加資格提出用フォルダ作成依頼メールを e-koji@jica.go.jp へ送付願います。(件名：「競争参加資格確認申請書提出用フォルダ作成依頼_ (調達管理番号)_ (法人名)」)

※依頼が1営業日前の正午までになされない場合は、競争参加資格申請書の提出ができなくなりますので、ご注意ください。

- 3) 確認結果の通知：上記4. (3) 日程の期日までにメールにて通知します。

6. 資料の配付依頼

資料の配付について希望される方は、JICA ウェブサイトの手順に則り依頼ください。

(URL: <https://www.jica.go.jp/announce/notice/distribution.html>)

- ・ 第3章2. 業務実施上の条件に記載の配付資料
- ・ 「独立行政法人国際協力機構 サイバーセキュリティ対策に関する規程(2022年4月1日版)」及び「サイバーセキュリティ対策実施細則(2022年4月1日版)」

「独立行政法人国際協力機構 サイバーセキュリティ対策に関する規程(2022年4月1日版)」及び「サイバーセキュリティ対策実施細則(2022年4月1日版)」については、プロポーザル提出辞退後もしくは失注後、受注した場合は履行期間終了時に速やかに廃棄することを指示します。

7. 企画競争説明書に対する質問

(1) 質問提出期限

- 1) 提出期限：上記4. (3) 日程参照
- 2) 提出先：上記4. (1) 選定手続き窓口
(outm1@jica.go.jp 宛、CC: 担当メールアドレス)
- 3) 提出方法：電子メール
 - ① 件名：「【質問】調達管理番号_案件名」
 - ② 添付データ：「質問書フォーマット」(JICA 指定様式)

注1) 質問は「質問書フォーマット」の様式に記入し電子メールに添付して送付し

てください。本様式を使用されない場合は、回答を掲載しない可能性があります。JICA 指定様式は下記（２）の URL の「公示共通資料」を参照してください。

注２）公正性・公平性確保の観点から、電話及び口頭でのご質問は、お断りしています。

（２）質問への回答

上記４．（３）日程の期日までに以下の JICA ウェブサイト上に掲示します。

（URL: <https://www2.jica.go.jp/ja/announce/index.php?contract=1>）

8. プロポーザル等の提出

（１）提出期限：上記４．（３）日程参照

（２）提出方法

具体的な提出方法は、JICAウェブサイト「業務実施契約の公示にかかる説明書等の受領方法及び競争参加資格確認申請書・プロポーザル・見積書等の電子提出方法（2021年10月13日版）」をご参照ください

（URL: <https://www2.jica.go.jp/ja/announce/index.php?contract=1>）

１）プロポーザル・見積書

- ① 電子データ（PDF）での提出とします。
- ② 上記４．（３）日程を参照し提出期限日の４営業日前から１営業日前の正午までに、プロポーザル提出用フォルダ作成依頼メールを e-koji@jica.go.jp へ送付願います。
- ③ 依頼メール件名：「提出用フォルダ作成依頼_（調達管理番号）_（法人名）」
- ④ 依頼メールが１営業日前の正午までに送付されない場合は技術提案書の提出ができなくなりますので、ご注意ください。
- ⑤ プロポーザル等は パスワードを付けずにGIGAPOD内のフォルダに格納 ください。
- ⑥ 本見積書と別見積書は GIGAPOD内のフォルダに格納せず、PDFにパスワードを設定し、別途メールでe-koji@jica.go.jpへ送付 ください。なお、パスワードは、JICA調達・派遣業務部からの連絡を受けてから送付願います。

（３）提出先

１）プロポーザル

「JICA 調達・派遣業務部より送付された格納先 URL」

２）見積書（本見積書及び別見積書）

- ① 宛先：e-koji@jica.go.jp
- ② 件名：（調達管理番号）_（法人名）_見積書
〔例：22a00075_〇〇株式会社_見積書〕
- ③ 本文：特段の指定なし
- ④ 添付ファイル：「22a00075_〇〇株式会社_見積書」
- ⑤ 見積書のPDFにパスワードを設定してください。なお、パスワードは、

JICA調達・派遣業務部からの連絡を受けてから送付願います。

- ⑥ 評価点の差が僅少で価格点を計算する場合、もしくは評価結果順位が第一位になる見込みの場合のみ、パスワード送付を依頼します。

(4) 提出書類

- 1) プロポーザル・見積書

9. 契約交渉権者決定の方法

提出されたプロポーザルは、別紙2の「プロポーザル評価配点表」に示す評価項目及びその配点に基づき評価（技術評価）を行います。評価の具体的な基準や評価に当たっての視点については、「コンサルタント等契約におけるプロポーザル作成ガイドライン（2022年4月）」より以下と参照してください。

- ① 別添資料1「プロポーザル評価の基準」
- ② 別添資料2「コンサルタント等契約におけるプロポーザル評価の視点」
- ③ 別添資料3「業務管理グループ制度と若手育成加点」

技術評価点が基準点（100点満点中60点）を下回る場合には不合格となります。

(URL: https://www.jica.go.jp/announce/information/20220330_01.html)

(1) 評価配点表以外の加点について

評価で60点以上の評価を得たプロポーザルを対象に、以下の2点について、加点・斟酌されます。

1) 業務管理体制及び若手育成加点

本案件においては、業務管理グループ（副業務主任者1名の配置）としてシニア（46歳以上）と若手（35～45歳）が組んで応募する場合（どちらが業務主任者でも可）、一律2点の加点（若手育成加点）を行います。

2) 価格点

若手育成加点の結果、各プロポーザル提出者の評価点について第1位と第2位以下との差が僅少である場合に限り、提出された見積価格を加味して契約交渉権者を決定します。

10. 評価結果の通知と公表

評価結果（順位）及び契約交渉権者を上記4.（3）日程の期日までにプロポーザルに記載されている電子メールアドレス宛にて各競争参加者に通知します。

第2章 特記仕様書案

本特記仕様書案に記述されている「脚注」及び別紙1「プロポーザルにて提案を求める事項」については、競争参加者がプロポーザルを作成する際に提案いただきたい箇所や参考情報を注意書きしたものであり、契約に当たって、契約書附属書Ⅱとして添付される特記仕様書からは削除されます。

また、契約締結に際しては、契約交渉相手方のプロポーザルの内容を適切に反映するため、契約交渉に基づき、必要な修正等が施された上で、最終的な「特記仕様書」となります。

第1条 総則

この仕様書は、独立行政法人国際協力機構（以下「発注者」という）と受注者名（以下「受注者」という）との業務実施契約により実施する「インドネシア国サイバーセキュリティ人材育成プロジェクト（オープンソースソフト開発／サイバーセキュリティ技術）」に係る業務の仕様を示すものである。

第2条 プロジェクトの背景

情報通信技術（Information and Communication Technology。以下、「ICT」という。）の重要性増加に比例し、サイバー攻撃や情報漏えいのリスクも甚大化している。インドネシアにおいては、サイバーセキュリティ（以下、「CS」という。）に関する中央政府の担当部門設立やルールの策定は概ね了しているが、民間機関や政府におけるCS人材の量・質の不足が行政及び経済団体から指摘されている。研修機会の絶対量が不足していること及びCS人材における各役割の定義が曖昧であることがその背景にある。

情報通信省が2016年に策定したインドネシアCS戦略における柱の一つとして、CSに関する意識改革及び産業界のニーズを踏まえた人材を高等教育機関を通じて輩出することが計画されている。また、電力、交通、金融をはじめとする8分野を重要情報インフラ（Critical Information Infrastructure。以下、「CII」という。）に指定し、CS対策の重点としている。

このような状況の中で、インドネシア国「サイバーセキュリティ人材育成プロジェクト」（以下「プロジェクト」という。）が2019年5月に開始され、2024年5月までの5年間の予定で実施中である。プロジェクトでは、インドネシア最高峰の大学の一つであるインドネシア大学においてプロフェッショナル（実務者）向けCS教育システムを立上げることで、CII分野を中心とする民間機関や政府に対してCS人材を持続的に供給する。さらに、アジア各国政府のCS人材に対し、プロジェクトで開発した科目、教材、オープンソース・セキュリティツール等を提供し、CS人材の相互交流、及びスキル向上を行うこととしている。

また、モンゴルにおいては、サイバーセキュリティ国家戦略や国家CSIRTの設立を進めている段階にあり、サイバーセキュリティの段階として初期的な段階にある。特に今後モンゴル国内のサイバーセキュリティ技術者を育成することが優先課題として検討されており、2021年度にモンゴル国より「サイバーセキュリティ及びICT分野人材育成プロジェクト」の要請がなされ、採択された。2022年度中に

プロジェクトの詳細計画が確定し、2022年12月より事業を開始する予定となっている。同プロジェクトにおいては、インドネシア国「サイバーセキュリティ人材育成プロジェクト」にて開発された教材及びツールをモンゴルの大学においても活用・展開する方針についてJICAより提案しており、モンゴル側関係者よりこの方針について口頭にて合意を受けている。

本契約の業務（以下「本業務」という。）においては、インドネシアのプロジェクトにおける、既にJICA長期専門家及び契約済の業務実施契約を通じて実施されている事業において、特に成果1「インドネシア大学において世界水準のプロフェッショナル向けCS教育が提供される」、成果2「産業界のニーズを踏まえたオープンソースサイバーセキュリティツールが開発される」、及び成果4「中・長期的なカリキュラムへの参加者・協力者拡大を目的に、諸外国との間でサイバーセキュリティに関するネットワークが強化される」に関連する一部の業務を実施するものとなる。また、今後開始が予定されるモンゴル国「サイバーセキュリティ及びICT分野人材育成プロジェクト」における一部の活動も、詳細計画確定後に本業務に追加することを予定している。

第3条 プロジェクトの概要

（インドネシア国「サイバーセキュリティ人材育成プロジェクト」）

（1）上位目標

インドネシアの政府や民間機関におけるサイバーセキュリティ対応能力が強化される。

（2）プロジェクト目標

インドネシア大学において産業界のニーズを踏まえたプロフェッショナル向けサイバーセキュリティ教育システムが強化される。

（3）プロジェクトにおいて期待される成果

成果1: インドネシア大学において世界水準のプロフェッショナル向けサイバーセキュリティ教育が提供される。

成果2: 産業界のニーズを踏まえたオープンソース（以下「OSS」という。）サイバーセキュリティツールが開発される。

成果3: オープンコースウェアが開発され、公開される

成果4: 中・長期的なカリキュラムへの参加者・協力者拡大を目的に、諸外国との間でサイバーセキュリティに関するネットワークが強化される。

（4）プロジェクトの活動の概要

成果1に関する活動

1-1. NICE¹ , SecBoK² 等、他国における ICT スキル標準に関する事例が研究される。

¹ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

² <https://www.jnsa.org/result/2018/skillmap/>

- 1-2. 包括的で最新のサイバーセキュリティに関するカリキュラムが設計される。
- 1-3. 上記カリキュラムに基づきシラバスが設計される。
- 1-4. 教員への必要なトレーニングが行われる（民間企業のゲスト教員を含む）。
- 1-5. 長期科目のコンポーネントとなる短期のサイバーセキュリティ科目が設立される。
- 1-6. 必要なタイミングで科目に関係する活動が見直される。

成果2に関する活動

- 2-1. 既存オープンソースサイバーセキュリティツールに関し、調査する。
- 2-2. インドネシアにおけるサイバーセキュリティツールへのニーズについて調査する。
- 2-3. 上記調査を踏まえ、最適なツールをローカライズする、あるいは開発する。
- 2-4. 上記ツールの導入を支援する。

成果3に関する活動

- 3-1. カリキュラムのうちオープン科目に適した科目を選別する。
- 3-2. 該当科目のオープンコースウェアを開発する。
- 3-3. 開発されたオープンコースウェアをリリースする。
- 3-4. 必要なタイミングでユーザーからフィードバックを集め、コースウェアを改善する。

成果4に関する活動

- 4-1. 他国（ASEAN 加盟国等）を対象とした研修を戦略的に実施する。
- 4-2. 国内外の機関を通して成果を発信する。

(5) プロジェクトの対象地域
インドネシア国ジャカルタ、バリ

(6) プロジェクトの実施機関
インドネシア国立大学

(7) プロジェクトの実施期間
2019年5月から2024年5月

(8) 本業務の実施期間
2022年7月から2023年4月を予定。なお、モンゴル国プロジェクトに関する活動追加により期間延長の可能性あり。

(モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」)

なお、以下内容は先方政府からの要請書に記載の事項であり、今後の詳細計画策定により大幅に変更となる可能性があります。

(1) 上位目標

モンゴルの安全なデジタル経済の推進を実現させる。

(2) プロジェクト目標

サイバーセキュリティ分野を含むデジタル人材が育成され、組織間の連携が強化される。

(3) プロジェクトにおいて期待される成果

成果1：学生・社会人・公務員向けサイバーセキュリティ（CS）教育プログラムを策定・実施する。

成果2：学生・社会人・公務員向け ICT 教育プログラムを策定・実施する。

成果3：重要インフラセキュリティ向上のための産学官連携ネットワークを構築する。

(4) プロジェクトの対象地域

モンゴル国ウランバートル

(5) プロジェクトの実施機関

通信情報技術庁及び高等教育機関

(6) プロジェクトの実施期間

2022年12月から2025年12月を予定（3年間の見込み）

(7) 本業務の実施期間

2022年12月から2023年4月を予定。なお、モンゴル国プロジェクトに関する活動追加により期間延長の可能性あり。

第4条 業務の目的

（インドネシア国「サイバーセキュリティ人材育成プロジェクト」）

(1) 第3条(4)プロジェクトの成果1に関する活動のうち、1-3及び1-4に関連し、複数の科目で重複する内容や、いずれの科目にも含まれていないが、サイバーセキュリティ（以下、CS）に従事するエンジニアに必須と考えられる内容を、共通事前学習教材として開発し、かつ、影響を受ける各科目のシラバスに修正を加える。さらに、フォレンジック科目で活用するマルウェアラボを安全に運用するためのポリシー作成、及びCSの最新トピックを扱ったCSトレンドセミナーを実施する。

(2) 第3条(4)プロジェクトの成果2に関する活動のうち、2-3に関連し、プロジェクトで開発を推進しているオープンソース CS ツールの開発体制を確立させ、安定版をリリースする。

(3) 第3条(4)プロジェクトの成果4に関する活動のうち、4-1、4-2に関連し、成果1で開発したカリキュラム、教材、さらに、これらを開発する際の考え方をまとめたカリキュラム開発マニュアルを紹介する CS カリキュラム開発セミナーを

実施する。

(モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」)

(4) インドネシアプロジェクト成果で開発したカリキュラム、教材、ツールを活用し、技術移転を行う。

(5) 技術移転を通じ、インドネシアプロジェクト成果品の改善、修正等を検討し、インドネシアプロジェクトへのフィードバックを行う。

第5条 業務の範囲

「第4条 業務の目的」を達成するため、「第6条 実施方針及び留意事項」を踏まえつつ、「第7条 業務の内容」に示す事項の業務を行い、「第8条 報告書等」に示す報告書等を作成する。

第6条 実施方針及び留意事項

(1) プロジェクト実施体制について

(インドネシア国「サイバーセキュリティ人材育成プロジェクト」)

➤ 日本側

当機構の国際協力専門員（ICT 分野）が、短期専門家としての渡航を繰り返す形でチーフアドバイザーを務めており、かつ、長期専門家（情報技術／業務調整）が派遣されている。業務の実施に当たっては、両専門家と十分な情報共有を行うものとする。なお、本プロジェクトでは、複数の活動が同時並行で行われていることから、現地での活動日程の調整については、両専門家と密な連携が必要とされる。

➤ インドネシア側

インドネシア大学工学部長がプロジェクトダイレクターを、また同学部のシニア教員がプロジェクトマネージャーを務めている。主たるプロジェクトメンバーは、同学部の ICT 系教員十数名であり、各科目の主任教員は、全て同学部所属である。それに加えて、客員教員として、他大学の ICT 系教員や、官・民の CS 技術者が参加しており、教員訓練の際は、これら客員教員も対象となる。

(モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」)

詳細未定であるが、当機構の国際協力専門員（ICT 分野）が、助言を行う予定である。業務の実施に当たっては、国際協力専門員及び、他の専門家が既にいる場合にはその専門家との密な連携が必要とされる。

(2) プロジェクトで独自開発した科目について

これまで、下の表に示す9科目をプロジェクトが独自に設計・開発を完了している（以下、「カスタム科目」と呼ぶ）。これらは、将来は国内外の教育機関に対して、無償で提供する予定である。また、これらの科目は別々の専門家により開発されたものであるため、一部科目に重複している内容があるため、本業務にて共通事前学習教材として取りまとめを行う。なお、受注者はこれら科目のシラバスや教材に改善を加える際、インドネシア大学に情報共有すると共に、無償提供を行うこと

を前提として、著作権の扱いや侵害等に十分配慮すること。

科目名	概要
How to make top managements aware of CS	Develop IT engineers who can convince their boss the importance of CS.
How to make general employees aware of CS	Develop IT engineers who can convince general employees the importance of CS.
Malware analysis	Process flow, Static & Dynamic analysis
Cybersecurity law and regulation	International norm, Ethics, Indonesian CS laws, example of company (IT &) CS policy
Supply-chain risk	Incidents caused by supply chain, Procurement, Basics of secure-coding, Sample contract etc.
How to make IT system forensic-enabled	Logging strategy in designing IT infrastructure, Case study by using network log files, Exercise: Scenario based analysis using network and host logs etc.
Comprehensive exercise: CSIRT	Exercise to understand all the activities of CSIRT
Computer Forensic	Hands-on training for PC (Windows/Mac) forensic
Mobile device forensic	Hands-on training for Mobile (Android) forensic

(3) カリキュラムについて

インドネシア大学 CS カリキュラムは、上記(2)で挙げたカスタム科目と、以下の商用科目から構成されている。なお、インドネシア大学は、EC-Council 社、CompTIA 社のアカデミック・パートナーとなっており、これら商用科目も、インドネシア大学教員によって提供される予定である。

- EC-Council 社 : CEH, CPENT, CTIA, ECIH, CHFI, CCISO
- CompTIA 社 : CySA+, Pentest+, CASP+

なお、カリキュラムに含まれるカスタム科目、商用科目とも、インドネシア大学の CS 修士科目と単位互換性を持つ。

(4) 共通事前学習教材について

第4条(1)に記載のある共通事前学習教材の項目は以下を想定している。受注者は、カスタム科目内容、商用科目内容を精査の上、必要があればこれ以外の教材を提案することも可能。なお、教材は英語で作成すること。自習が前提の教材となるため、内容量、表現方法、理解度確認方法、提供形態について十分検討すること。

教材名	含むべきトピック	影響する既存科目数
Common cyberattacks	● Types of Cyberattacks	7科目

and Malwares	<ul style="list-style-type: none"> ● Types of Malwares ● Common cyber-attack situation ● Trends of cyber-attacks 	
Basis of Information security	<ul style="list-style-type: none"> ● CIA concept ● Information Assets ● ISO27001 (ISMS) 	2科目
Introduction of NIST Frameworks (CSF, RMF, SP 800 Series, SP8100 Series)	<ul style="list-style-type: none"> ● Introduction of NIST documents ● Cyber Security Framework ● Risk Management Framework 	既存科目への影響なし。前提知識
NICE Framework/ SecBoK	<ul style="list-style-type: none"> ● Introduction of NICE Framework ● Introduction of SecBoK ● Usage of SecBoK in curriculum of this project 	既存科目への影響なし。前提知識

(5) マルウェアラボ・ポリシーについて

プロジェクトでは教育・研究に供するため、マルウェア解析を行うために必要な機材を一式供与している。本業務では、これら機材を用いて、安全にマルウェア解析を行える環境を構築・維持する指針となるマルウェア解析にかかるポリシーを策定する。ポリシーの策定に当たっては、物理的なラボへのアクセス、ネットワーク環境を介したアクセスの両面から検討し、マルウェア流出防止と、万一流出した際に、カウンターパートが対策を取れるよう考慮すること。

(6) CSトレンドセミナーについて

主な目的は、カウンターパート・教員の最新知識取得とするが、裨益効果を高めるため、公開セミナーとし、以下のような内容で実施する。各々半日から1日間程度を想定。

- 第一回目：2022年10月頃にインドネシア国内向けに開催を想定。インドネシア固有のトレンド（想定されるトピック：制定が検討されている個人情報保護法）を扱い、インドネシア国内のCS関係者も参加可能とする。英語・インドネシア語併用で、英語部分はインドネシア語への通訳を付ける。Covid-19による社会規制が無ければ、オフラインとオンラインを併用した開催とするが、その場合、プロジェクトがオフライン会場提供と、オフライン参加者選定を行う。
- 第二回目：2023年2月頃にインドネシア国内外問わずの開催を想定。国際的なトレンド（想定されるトピック：IoT・Cloud Security、Secure Coding、SecDevOps）を扱い、域内のCS関係者も参加可能とする。英語のみ。オンラインで開催。

なお、これらセミナーで利用する発表資料は、カウンターパート教員が補助教材として利用できることが望ましい。よって、受注者は発表資料に関し、できるだけ補助教材利用を可能とすべく講演者と交渉した上、利用可能部分や利用時の条件について明確にすること。

なお、第二回セミナーにはモンゴル関係者も招待をする想定となる。

(7) OSS ツール・Mata-elang について

現在、プロジェクトが開発を推進しているのは、Mata-elang³（インドネシア語で「鷹の眼」の意味）という OSS ツールである。これは、既存の複数のオープンソースを組み合わせ、現地のニーズに合わせてダッシュボードなどいくつかの機能を追加したネットワーク・モニタリングシステムで、インドネシア大学と密接な関係にあるスラバヤ電子工学大学（Politeknik Elektronika Negeri Surabaya：PENS）が開発を行っている。ただし、次のような問題があり、広く普及するには至っていない。

- 多数の仮想センサー管理と、大容量のログ管理を目指していることから、実験的な側面が強い
- 限られたグループ内で開発していることから、技術仕様やスケジュールが流動的で、外部の技術者が開発に参加することが難しい

プロジェクトでは、2021年度の活動として、小規模ユーザー向けの要件に絞って安定版の開発に着手したが、実際の現場での実稼働には至っていない。今後の追加開発要件が既に十数件挙がっており、IPV6対応や、オフラインインストーラー（Internet 接続が無い環境でのインストール）機能の追加等がある。なお、Mata-elang の開発方針を決めるための Mata-elang 開発委員会（以下、委員会）が、インドネシア国立大学の教員を中心として設置されており、体制確立や開発機能の優先度等については、この委員会と密にコミュニケーションをとる必要がある。

(8) カリキュラム開発セミナーについて

2022年11月頃開催で、5日間程度を想定。カスタム科目のシラバス、教材、及び、商用科目のシラバス、共通事前学習教材の紹介と共に、カリキュラム開発マニュアルを用いて CS カリキュラムを疑似的に開発する Workshop を行うこととする

このカリキュラム開発マニュアルは、プロジェクトが包括的で最新の CS カリキュラムを開発した際、NICE、SecBoK 等を利用したプロセスをまとめたものである。なお、参加者選定及び実施会場手配はプロジェクトが行う。参加者は、モンゴル、ラオス、東チモール等の高等 IT 教育機関スタッフ、実施場所はバリ島を想定している

(9) COVID-19の影響で現地渡航出来ない場合の措置

COVID-19の影響により業務の進捗に遅れが生じる際など、受注者は発注者に報告し、必要があれば変更契約等で対応すること。

(10) 相手国関係機関等とのアポイントメント

本業務の実施に際し、相手国関係機関や C/P とのアポイントメントの取り付けは、原則受注者が行うことを前提とするが、それが困難な場合（例：初回のアポイントメント取り付け）は、適宜プロジェクトの長期専門家に協力を依頼すること。

³ <https://github.com/mata-elang-pens> より入手可能

(11) モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」における業務（契約変更にて以下の業務の追加を予定）（モンゴル）

同プロジェクトは、2022 年度後半に開始される見込みであり、詳細計画確定後、JICA は、受注者に対して、以下の業務を追加した契約変更を打診することを想定しており、受注者は契約変更にて以下を追加業務として対応することが期待されている。

なお、これら業務は、現時点の想定となるため、詳細な活動については、契約締結後に受注者と JICA との間で確認するものとする。

- 第 6 条（2）に挙げたカスタム科目のうち、3 科目の教員トレーニングの実施（実施科目は、モンゴル側の優先度に従って契約変更前に決定）
- インドネシア国立大学で開発した成果物（例：カリキュラム、教材、オープンソースソフトウェア）のうち、モンゴルでの利用が適するもの、さらに、利用する際にローカライズが必要な部分を特定することを目的とした、現地ニーズ調査、そのまま利用可能なものがある場合には、その利用にかかる指導
- モンゴルへの展開検討を踏まえた、インドネシアプロジェクトへの成果品改善にかかるフィードバックの実施

第 7 条 業務の内容

(1) 業務計画書（和文）及びワーク・プラン（英文）の作成

1) チーフアドバイザー及び長期専門家から情報を入手し、プロジェクトの全体像及びこれまでのプロジェクト成果物（例：シラバス、教材、カリキュラム開発マニュアル、Mata-elang 関連資料）の内容を精査する。

2) 業務計画書を和文、ワークプランを英文で取りまとめ、業務計画書についてはチーフアドバイザーの、また、ワークプランについてはプロジェクトマネージャー及びチーフアドバイザーの合意を得る。

(2) 共通事前学習教材の開発とシラバス修正

1) 共通事前学習教材の概要及び修正が必要な関連科目を明示した開発計画案を作成し、プロジェクトマネージャー、各科目主任教員及びチーフアドバイザーの合意を得る。

2) 共通事前学習教材の開発とシラバス修正を行い、プロジェクトマネージャー、各科目主任教員及びチーフアドバイザーのレビューを受け最終化する。

3) 開発した共通事前学習教材と修正済みシラバスを教員（例：各科目主任教員、客員教員）に説明する。

本業務 2) 及び 3) については現地再委託を可とする。

なお、本業務 2) 及び 3) については JICA の長期専門家と共同実施する部分であり、現地再委託する場合においても長期専門家と協議しつつ指示・監督

を行うこと。

(3) マルウェアラボ・ポリシーの開発

1) プロジェクトの現有機材及び想定しているシステム構成図やネットワークポロジ図を確認する。また、ポリシー作成に参考となる公開資料やラボ利用者や解析対象となるマルウェアについて、プロジェクトマネージャー、チーフアドバイザー等にヒアリングする。

2) ポリシーの目次や各章の概要を明確にした中間成果物を作成し、プロジェクトマネージャー、フォレンジック担当主任教員及びチーフアドバイザーの承認を得る。

3) ポリシーの開発を行い、プロジェクトマネージャー、フォレンジック担当主任教員及びチーフアドバイザーのレビューを受け最終化する。

4) 開発したポリシーを、ラボを利用する可能性のある関係者（例：各科目主任教員、客員教員、外部セキュリティ団体メンバー）に説明する。

本業務2)、3)、及び4)については、現地再委託を可とする。

なお、本業務2)、3)、4)についてはJICAの長期専門家と共同実施する部分であり、現地再委託する場合においても長期専門家と協議しつつ指示・監督を行うこと。

(4) カリキュラム開発及びCSトレンドに関するセミナー実施

1) プロジェクトマネージャー、各科目主任教員と意見交換し、セミナーで扱うトピック及び日時を確定する

2) 日本、インドネシア、第三国から適切な講師を確保し、講義を依頼する。また、当日の通訳が必要な場合は併せて確保する。

3) セミナーの広報資料（電子ファイル）を作成しプロジェクトに提供するとともに、各種メディアを通じ広報を行う。

4) セミナー準備を行い、実施する。オフライン開催の場合は、茶菓・昼食の提供を行うこと。また、オフライン、オンラインに関わらず、参加者リスト、参加者アンケートを取りまとめ、後日提出すること。

5) セミナーで利用した資料（例：スライド）をカウンターパート教員が利用できる部分や利用条件を明示の上、プロジェクトに提供する。

本業務2)については現地再委託も可能とする。

(5) OSS ツール（Mata-elang）開発体制確立と安定版リリース

1) プロジェクトで作成した OSS 開発マニュアル（開発体制と各関係者の役割、リリース予定、開発ドキュメント書式等を含む）、Mata-elang 安定版の開発ドキュメント、さらにコード等を確認し、現在の開発状況を理解する。

2) 想定対象ユーザー、追加開発機能の優先度、リリース・スケジュール等について委員会と協議し、必要があれば、OSS 開発マニュアルを更新の上、委員会の承認を得る。

3) 役割分担に応じて開発を実施する。受注者は開発全体の管理を行う。なお、コーディングやテストは現地 IT ベンダーへの再委託を想定しているが、開発機能の要件定義、RFP 作成といった上流工程は、委員会の関与を最大限にするよう配慮すること。

4) 、開発した安定版を委員会とともに検収する。検収の際は、実環境（インドネシア国立大学構内のネットワークを想定）の上で導入・稼働させ、ユーザー（インドネシア国立大学のネットワーク担当者等、委員会から指定された者）とともに、アクセプタンステストを行うこと。

5) GitHub 上に開発物を公開する。

本業務 3) における、開発業務については現地再委託も可能とする。

(6) インドネシア成果物のローカライズ対象の特定

1) インドネシア国立大学で開発した成果物（例：カリキュラム、教材、オープンソースソフトウェア）のうち、モンゴルでの利用が適する部分及び利用する際にローカライズが必要な部分を特定することを目的とした現地ニーズの調査を行う。

本業務については現地再委託も可能とする。

2) 上記 1) の調査結果を分析し、インドネシア国立大学で開発した成果物（例：カリキュラム、教材、オープンソースソフトウェア）のうち、モンゴルでの利用が適する部分及び利用する際にローカライズが必要な部分を特定する

(7) インドネシア成果物による教員訓練

インドネシア国立大学で開発した科目（第 6 条（2）に挙げられているもの）のうち、3科目の教員訓練を行う。対象科目は、モンゴル側の優先度に従って契約変更前に決定することとする。なお、この教員訓練に関し、インドネシアで開発した共通事前学習教材の併用が有効と考えられる場合は、自習教材としてモンゴル側に事前に提供すること。

本業務についてはインドネシアからのオンライン講義も可とし、その業務につ

いて現地再委託も可能とする。

(8) インドネシアプロジェクトへのフィードバック

モンゴル国における活動の結果、インドネシア国立大学で開発した成果物（例：カリキュラム、教材、オープンソースソフトウェア）における改善につながる事項があれば取りまとめた上で、インドネシア国プロジェクト専門家に共有する。

(9) 業務完了報告書の作成

活動結果を業務完了報告書に取りまとめる。

以下は、想定される業務の流れの一例である。ただし、必ずしもこの流れに沿う必要はなく、渡航回数や滞在期間も含め、また、COVID-19の影響も鑑みながら、受注者が最適と考える業務計画を立てて良いこととする。

インドネシア国における予定業務は、現時点で以下のとおりを想定。

1) 第一回派遣前国内作業（2022年7月上旬頃を想定）

- プロジェクトの状況把握
- プロジェクト既存成果物の詳細確認
- 業務計画書、ワークプランの作成
- 現地再委託業者との契約準備
- 共通事前学習教材の開発案作成
- マルウェアラボ・ポリシーの目次・概要案作成

2) 第一回現地作業（2022年8月上旬頃を想定）

- 現地再委託業者との契約
- カウンターパートへのワークプランの説明
- 委員会と共に開発要件を確定。OSS 開発マニュアル修正、RFP 作成
- 共通事前学習教材の開発案合意と開発
- マルウェアラボ・ポリシーの目次・概要案合意
- 第一回 CS トレンドセミナーの準備
- カリキュラム開発セミナーの準備
- 現地再委託業者への作業指示とモニタリング

3) 第二回派遣前国内作業

- 現地再委託業者による作業のモニタリング
- （受注者が共通事前学習教材、マルウェアラボ・ポリシー、Mata-elang の開発に直接関与する場合は、それら作業）

4) 第二回現地作業（2022年10月下旬頃からを想定）

- 第一回 CS トレンドセミナーの実施
- カリキュラム開発セミナーの実施

- 事前学習共通教材のレビュー、関連シラバス変更、最終化
 - マルウェアラボ・ポリシーのレビュー、最終化
 - 第二回 CS トrendセミナーの準備
- 5) 第三回派遣前国内作業
- 現地再委託業者による作業のモニタリング
 - (受注者が Mata-elang の開発に直接関与する場合は、それら作業)
- 6) 第三回現地作業 (2023年1月下旬頃を想定)
- 第二回 CS トrendセミナーの実施
 - Mata-elang 検収
- 7) 帰国後整理作業 (2023年2月下旬頃を想定)
- カウンターパートへの最終成果物説明 (遠隔会議)
 - 業務完了報告書のとりまとめ

モンゴル国における予定業務は、現時点で以下のとおりを想定。

- 8) 第一回追加派遣前国内作業 (2022年12月頃を想定)
- プロジェクトの状況把握
 - 業務計画書、ワークプランの修正
 - 現地再委託業者との契約準備
- 9) 第一回追加現地作業 (2023年1月頃を想定)
- 現地再委託業者との契約
 - カウンターパートへのワークプランの説明
 - 指導対象共通事前学習教材の選定及び指導
 - CS トrendセミナーの実施
- 10) 帰国後整理作業 (2023年3月頃を想定)
- カウンターパートへの最終成果物説明 (遠隔会議)
 - インドネシア国プロジェクトへのフィードバック
 - 業務完了報告書のとりまとめ

第8条 報告書等

(1) 報告書

業務の各段階において作成・提出する報告書は以下のとおり。最終成果品は業務完了報告書とし、提出期限は契約履行期間の末日とする。

報告書名	提出時期	部数
業務計画書	契約締結後10営業日以内	和文: 電子ファイル
ワークプラン	第1回現地作業開始後5営業日以内	英文: 電子ファイル

業務完了報告書	契約履行期間の末日 2023年4月下旬を予定	英文:電子ファイル
---------	---------------------------	-----------

注1. 「業務計画書」は、共通仕様書第6条に規定する業務計画書を意味しており、同条に規定する事項を記載するものとする。

注2. 報告書の印刷（簡易製本を含む）、電子化（CD-R）にあたっては、「コンサルタント等契約における報告書の印刷・電子媒体に関するマニュアル」を参照する。

注3. 報告書等全体を通じて、固有名詞、用語、単位、記号等の統一性と整合性を確保すること。また、英文報告書の作成にあたっては、その表現ぶりに十分注意を払い、必ず当該分野の経験・知識とともに豊富なネイティブスピーカーの校閲を受けること。

各報告書等の記載項目（案）は以下のとおりとする。最終的な記載項目の確定にあたっては、JICAとコンサルタントで協議、確認する。

- 1) ワーク・プランの記載項目（案）
最低限、以下の項目を含むこと。
 - 業務の概要、方針、方法
 - スケジュール（マイルストーンとして、技術協力作成資料の中間成果物の提供予定を含むこと）
 - カウンターパート、または長期専門家に求める作業
- 2) 業務完了報告書の記載項目（案）
含むべき内容は、受注者が提案することとするが、最低限、以下を含むこと
 - 活動内容
 - 技術移転実施上の工夫・教訓（業務実施方法、運営体制等、OSSコミュニティ形成方法）

なお、業務完了報告書は公開資料となるため、セキュリティ上の機微な情報や、カウンターパートの個人情報が含まれる場合等は、必要に応じて当該部分は別のレポートとしてまとめ、かつ、カウンターパート及びチーフアドバイザーの承認を得たのち、JICAに提出すること。

（2）技術協力作成資料

業務の各段階において作成・提出する作成資料（ソースコード含む）は以下の通り。

資料名	提出時期	部数
共通事前学習資料、修正済み関連科目シラバス	ワークプラン作成時に決定（2022年12月末頃を想定）	英文：電子ファイル。編集可能な形式のファイルであること。
安定版Mata-elangと、関連技術資料	ワークプラン作成時に決定	英文:技術ドキュメント、ソースコード

	(2023年2月末頃を想定)	ド、実行ファイル、インストーラーなどはJICAにはHDDにて提出した上で、GitHubにて公開し、URLをJICAに通知
OSS開発マニュアル（変更を加えた場合）	ワークプラン作成時に決定 (2023年2月末頃を想定)	英文：電子ファイル
CSトレンドセミナー、およびカリキュラム開発セミナーで利用したスライド類、	セミナー終了後、20営業日以内	英文：電子ファイル
マルウェアラボ・ポリシー	ワークプラン作成時に決定（2022年12月末頃を想定）	英文：電子ファイル

- 1) 共通事前学習資料、修正済み関連科目シラバス
第6条（4）を参照し、適切な内容で作成すること。
 - 2) 安定版Mata-elangと、関連技術資料
含むべき内容は、受注者が提案することとするが、最低限、以下を含むこと。
 - テスト済みMatal-elang安定版のコード、実行ファイル
 - 技術ドキュメント一式
 - 3) OSS開発マニュアル
改変を加えた場合のみ。含むべき内容は、受注者が提案することとするが、可能な範囲で、元の形式を踏襲すること。
 - 4) CSトレンドセミナー、およびカリキュラム開発セミナーで利用したスライド類
形式は特に指定しないが、インドネシア国立大学講師が、副教材として使える範囲に制限がある場合、その範囲、条件を明示すること。
 - 5) マルウェアラボ・ポリシー
第6条（5）を参照し、適切な内容で作成すること
- (3) コンサルタント業務従事月報
 コンサルタントは、国内・海外における業務従事期間中の業務に関し、以下の内容を含む月次の業務報告を作成し、共通仕様書第7条に規定されているコンサルタント業務従事月報に添付して、当機構に提出する。
 - 今月の実績（投入、活動）
 - 来月の計画（投入、活動）
 - ワークプランで設定したマイルストーンとの差異

- 当面の課題
- 活動に関する写真

第3章 プロポーザル作成に係る留意事項

1. プロポーザルに記載されるべき事項

プロポーザルの作成に当たっては、「コンサルタント等契約におけるプロポーザル作成ガイドライン（2022年4月）」の内容を十分確認の上、指定された様式を用いて作成して下さい。

(URL: https://www.jica.go.jp/announce/information/20220330_01.html)

(1) コンサルタント等の法人としての経験、能力

1) 類似業務の経験

類似業務：サイバーセキュリティ分野に係る各種業務

2) 業務実施上のバックアップ体制等

3) その他参考となる情報

(2) 業務の実施方針等

1) 業務実施の基本方針

プロポーザル及び見積書は本説明書の記載内容に基づき作成いただきます。一方で、コロナ禍の影響が長引き現地渡航できない状況が継続する可能性もあります。現地調査について、本説明書あるいはプロポーザルの計画から延期せざるを得ない場合を想定し、現地調査開始前に実施できる国内業務について提案があればプロポーザルに追加で記載してください。こちらの提案につきましては、制限ページ数外、見積不要とします。

2) 業務実施の方法

1) 及び2) を併せた記載分量は、20 ページ以下としてください。

3) 作業計画

4) 要員計画

5) 業務従事予定者ごとの分担業務内容

6) 現地業務に必要な資機材

7) その他

第2章に記載した通り、本件業務については、モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」の実施内容が確定（RD 締結）後に当該技術協力プロジェクトの一部業務を追加発注する可能性があります。このため上記1)～7)においては、第2章に記載の想定仕様に基づいて、モンゴル国「サイバーセキュリティ及び ICT 分野人材育成プロジェクト」の業務についても提案を行ってください。また、各記述、提案についてはそれぞれインドネシア分とモンゴル分を分けて分かるように記載ください。

(3) 業務従事予定者の経験、能力

1) 評価対象業務従事者の経歴及び業務従事者の予定人月数

別紙2「プロポーザル評価配点表」の「3. 業務従事予定者の経験・能力」において評価対象となる業務従事者の担当専門分野及び想定される業務従事人月数は以下のとおりです。評価対象業務従事者にかかる履歴書と類似業務の経験を記載願います。

- ① 評価対象とする業務従事者の担当専門分野
 - 業務主任者／サイバーセキュリティ技術
 - ソフトウェア開発技術
- ② 評価対象とする業務従事者の予定人月数
約 4.67 人月

(上記予定人月は、インドネシアにかかる業務のみを計上)

2) 業務経験分野等

各評価対象業務従事者を評価するに当たっての類似業務経験分野、業務経験地域、及び語学の種類は以下のとおりです。

【業務主任者（業務主任者／サイバーセキュリティ技術）】

- ① 類似業務経験の分野：
 - 実業務で使用するソフトウェアの開発にかかる各工程（企画、要件定義、設計、開発、テスト）にエンジニアとして関わった経験
 - ソフトウェア開発におけるプロジェクトマネージャーの経験
- ② 対象国及び類似地域：インドネシア国及びASEAN地域
- ③ 語学能力：英語
- ④ 業務主任者等としての経験

【業務従事者：担当分野 ソフトウェア開発技術】

- ① 類似業務経験の分野：
 - CSエンジニア、システムエンジニア、インフラエンジニア、いずれかの実務経験
 - 現役CSエンジニア向けの研修コースを設計した経験
- ② 対象国及び類似地域：インドネシア国及びASEAN地域
- ③ 語学能力：英語

2. 業務実施上の条件

(1) 業務工程

本件に係る業務工程は、2022年7月に開始し、2023年3月に業務完了報告書ドラフトを作成・提出し、2023年4月に終了するものとする。

(2) 業務量目途と業務従事者構成案

1) 業務量の目途

約 6.17人月（現地：4.67人月、国内1.50人月）
（上記予定人月は、インドネシアにかかる業務のみを計上）

2) 業務従事者の構成案

業務従事者の構成（及び格付案）は以下を想定していますが、競争参加者は、業務内容等を考慮の上、最適だと考える業務従事者の構成（及び格付）を提案してください。

- ① 業務主任者/サイバーセキュリティ技術（3号）
- ② ソフトウェア開発技術（3号）
- ③ 技術セミナー設計

3) 渡航回数を目途 全3回

上記渡航回数は、インドネシアにかかる業務のみを計上しております。なお、上記回数は目途であり、回数を超える提案を妨げるものではありません。

第2章に記載した通り、本件業務については、モンゴル国「サイバーセキュリティ及びICT分野人材育成プロジェクト」の実施内容が確定（RD締結）後に当該技術協力プロジェクトの一部業務を追加発注する可能性があります。

当該追加業務に係る追加の業務量目途と業務従事者構成案については、以下のとおり想定しています。ただし、本業務量目途と業務従事者構成案は、発注者側の現時点での想定であるため、具体的業務量及び従事者構成は、変更契約の契約交渉において、発注者・受注者で協議するものとします。

1) 追加業務量を目途

約4.00人月（現地：3.00人月、国内1.00人月）

2) 追加の業務従事者構成案

構成は上記から変更なし

3) 追加渡航回数目途

全1回

(3) 現地再委託

以下の業務については、業務対象国・地域の現地法人（ローカルコンサルタント等）への再委託を認めます。

- 第2章 第7条（2）共通事前学習教材の開発とシラバス修正
における共通事前学習教材の開発及び修正済みシラバスの教員説明
- 第2章 第7条（3）マルウェアラボ・ポリシーの開発
におけるマルウェア運用ポリシー作成、開発及び説明
- 第2章 第7条（4）カリキュラム開発・CSトレンドセミナー実施
における、セミナー準備と実施（例：内容詳細設計、現地講師）
- 第2章 第7条（5）OSS ツール（Mata-elang）開発体制確立と安定版リリース
におけるOSS ツール（Mata-elang）開発
- 第2章 第7条（6）インドネシア成果物のローカライズ対象の特定
- 第2章 第7条（7）インドネシア成果物による教員訓練

また、可能な範囲で再委託する業務内容、業務の実施方法、選定方針、契約手続き（見積書による価格比較、入札等）、価格競争に参加を想定している現地及び第三国の業者の候補者名並びに再委託業務の監督・成果品の検査方法等について、プロポーザルにて具体的な提案を行うこと。

現地再委託費等にあたっては「コンサルタント等契約における現地再委託契約ガイドライン（2017年4月版）」に則り選定及び契約を行うこととし、委託業務者の業務遂行に関しては現地において適切な監督、指示を行う。

（４）配付資料／公開資料等

１）配付資料

- 既存教材の閲覧、Mata-elang 開発ドキュメントを希望する方はガバナンス・平和構築室 STI・DX 室 (Kamitani.Yoshimi@jica.go.jp)にご連絡ください。

２）公開資料

- インドネシア「サイバーセキュリティ人材育成プロジェクト」事業事前評価表
https://www2.jica.go.jp/ja/evaluation/pdf/2018_1701288_1_s.pdf
- Key Findings from the Global State of Information Security Survey™ 2017 - Indonesian Insights
<https://www.pwc.com/id/en/publications/assets/assurance/Risk%20Assurance/gsiss-indonesian-report-2017.pdf>

（５）対象国の便宜供与

概要は、以下のとおりです。なお、詳細については、R/Dを参照願います。

	便宜供与内容	
1	カウンターパートの配置	有
2	通訳の配置（*語⇔*語）	無
3	執務スペース（インドネシア国立大学内にあるプロジェクト室を、派遣中の長期専門家と共用する）	有
4	家具（机・椅子・棚等）	有
5	事務機器（コピー機等）	有
6	Wifi	有

（６）安全管理

JICAインドネシア事務所にて以下の行動規範を定めているため、下記に従った行動をお願いいたします。

- ・「JICA 安全対策マニュアル（JICA インドネシア事務所作成）」を遵守する。 ・安

全対策の 3 原則「目立たない、行動を予知されない、用心を怠らない。」を徹底する。

- ・イスラム教の習慣に配慮し、露出の多い服装、飲酒、宗教的な発言は慎む。
- ・渡航者は携帯電話を所持し、事務所他関係者に電話番号を伝達し、常時連絡が取れるようにする。
- ・空港出発／到着ロビーは相対的に脆弱なエリアであるため、滞在時間を最小限とする。
- ・事件・事故・災害等に遭遇した場合は、直ちに JICA 事務所の担当者に連絡する。
- ・パスポートもしくはパスポートの写しを常に携行する。
- ・ひったくりが多いため、徒歩移動は最小限とする。
- ・夜間における不要・不急の外出は避ける。
- ・自動二輪車の運転及び乗車を絶対に行わない。
- ・Lion Air 等の LCC の利用は避ける。
- ・外国人の多い場所、不特定多数が集まる場所での行事、テロの標的となりやすい場所（公的機関、軍・警察等の治安当局施設、駅・バスターミナル、宗教関連施設、宗教行事開催場所、欧米関連施設、レストラン、カフェ、バー、ショッピングセンター、大型スーパーマーケット、観光スポット、市場等）にやむを得ず訪問する場合は、滞在時間を最小限とする。
- ・デモ行進や政治集会等には近づかない。
- ・欧米資本・欧米ブランドのホテルの利用を極力避ける。
- ・事務所から宿泊先、渡航日程等変更の指示がある場合には、これに従う。

3. プレゼンテーションの実施

本案件については、プレゼンテーションを実施しません。

4.見積書作成にかかる留意事項

本件業務を実施するのに必要な経費の見積書（内訳書を含む。）の作成に当たっては、「コンサルタント等契約における経理処理ガイドライン」（2022年4月）を参照してください。

（URL: <https://www.jica.go.jp/announce/manual/guideline/consultant/quotation.html>）

（1）契約期間の分割について

第1章「3 競争に付する事項」において、契約全体が複数の契約期間に分割されることが想定されている場合は、各期間分及び全体分の見積りをそれぞれに作成して下さい。

見積もりにおいては、インドネシア分の業務のみを計上ください。モンゴル分は別見積もりとします。

（2）別見積もりについて

以下の費目については、見積書とは別に見積もり金額を提示してください。なお、新型コロナウイルス感染対策に関連する経費（PCR検査代及び隔離期間中の待機費用等）は見積金額に含めないでください。契約交渉の段階で確認致します。

- 1) 旅費（航空賃）
- 2) 旅費（その他：戦争特約保険料）
- 3) 一般業務費のうち安全対策経費に分類されるもの
- 4) 直接経費のうち障害のある業務従事者に係る経費に分類されるもの
- 5) モンゴル国「サイバーセキュリティ及びICT分野人材育成プロジェクト」分の業務に係る全経費

（3）定額計上について

以下の費目については、以下に示す定額を見積もってください。

- 1) 現地再委託に係る経費（現地再委託費）： 9,000千円
- 2) 資料等翻訳料

なお、セミナーで、講演者に必要と想定される謝金については、一般業務費に計上して下さい。

（4）外貨交換レートについて

- 1) JICAウェブサイトより公示月の各国レートを使用して見積もってください。

（URL: https://www.jica.go.jp/announce/manual/form/consul_g/rate.html）

5. その他留意事項

- 1) 特になし

以上

別紙1：プロポーザルにて提案を求める事項

別紙2：プロポーザル評価配点表

プロポーザルにて提案を求める事項

プロポーザルの作成に当たっては、特に以下の事項について、コンサルタントの知見と経験に基づき、第3章1.(2)「2)業務実施の方法」にて指定した記載分量の範囲で具体的な提案を行うこと。詳細については特記仕様書を参照すること。なお、プロポーザルにおいては、特記仕様書の内容と異なる内容の提案については、これを認めています。プロポーザルにおいて代替案として提案することを明記し、併せてその優位性／メリット及び費用／コストについての説明を必ず記述してください。見積書については、同代替案に要する経費を本見積に含めて提出することとします。代替案の採否については契約交渉時に協議を行うこととします。

No.	提案を求める項目	特記仕様書案への該当条項及び記載ページ
1	マルウェアラボ・ポリシーの策定方針	第2章第6条 実施方針及び留意事項 (5) P. 12
2	CSトレンドセミナー（第一回、第二回）の想定している内容について	第2章第6条 実施方針及び留意事項 (6) P. 12
3	現地再委託する業務の業者選定方針、契約手続き、実施方法業者候補者名、成果本検査方法等	第3章2. (3) P. 24

プロポーザル評価配点表

評価項目	配点	
1. コンサルタント等の法人としての経験・能力	(10)	
(1) 類似業務の経験	6	
(2) 業務実施上のバックアップ体制等	4	
2. 業務の実施方針等	(40)	
(1) 業務実施の基本方針の的確性	18	
(2) 業務実施の方法の具体性、現実性等	18	
(3) 要員計画等の妥当性	4	
(4) その他（実施設計・施工監理体制）	—	
3. 業務従事予定者の経験・能力	(50)	
	(34)	
(1) 業務主任者の経験・能力／業務管理グループの評価	業務主任者のみ	業務管理グループ
① 業務主任者の経験・能力： <u>業務主任者／サイバーセキュリティ技術</u>	(34)	(13)
ア) 類似業務の経験	20	7
イ) 対象国・地域での業務経験	3	1
ウ) 語学力	4	2
エ) 業務主任者等としての経験	2	1
オ) その他学位、資格等	5	2
② 副業務主任者の経験・能力： <u>副業務主任者／〇〇〇〇</u>	(—)	(13)
ア) 類似業務の経験	—	7
イ) 対象国・地域での業務経験	—	1
ウ) 語学力	—	2
エ) 業務主任者等としての経験	—	1
オ) その他学位、資格等	—	2
③ 業務管理体制、プレゼンテーション	(—)	(8)
ア) 業務主任者等によるプレゼンテーション	—	—
イ) 業務管理体制	—	8
(2) 業務従事者の経験・能力：<u>ソフトウェア開発技術</u>	(16)	
ア) 類似業務の経験	10	
イ) 対象国・地域での業務経験	2	
ウ) 語学力	2	
エ) その他学位、資格等	2	