意見招請

対象国名：東南アジア（インドネシア、カンボジア、フィリピン）
業務名称:サイバーセキュリティ人材育成プロジェクト(サイバー攻撃防護演習設計・実施者育成)

表記案件につき、別添の特記仕様書（案）に対するご意見・コメントを募集いたします。
頂いたご意見・コメントにつきましては、個別に回答は致しませんが、企画競争説明書へ適宜反映させていただきます。また、ご意見・コメントにつきまして確認させていただきたい点などある場合には、ご連絡差し上げる場合がございます。

コメント締切：	2024年7月2日（火）　15:00（JST）
事業担当部署：	TO:ガバナンス・平和構築部STI・DX室 gpgsd@jica.go.jp CC：Hirayama.Anju@jica.go.jp
調達・派遣業務部担当：	契約第一課 Morita.Akane@jica.go.jp

別添：企画競争説明書のうち、第２章　特記仕様書（案）

別添

第２章　特記仕様書案

（契約交渉相手方のプロポーザル内容を踏まえて、契約交渉に基づき、最終的な「特記仕様書」を作成します。）

第１条　業務の目的

「第２条　業務の背景」に記載する技術協力事業について、「第３条　実施方針及び留意事項」を踏まえ、「第４条　業務の内容」に記載される活動の実施により、相手国政府関係機関等と協働して、期待される成果を発現し、プロジェクト目標達成に資することを目的とする。

第２条　業務の背景

現在、以下3件のサイバーセキュリティ人材育成協力が進行中である（各案件の概要は、別紙参照）。フィリピンは個別専門家案件であるが、本仕様書では便宜上すべて「JICAプロジェクト」と表現する。

- サイバーセキュリティ人材育成プロジェクト（インドネシア）
- サイバーセキュリティ能力向上プロジェクト（カンボジア）
- サイバーセキュリティ能力開発（フィリピン）

いずれの協力でも、カウンターパート（以下、「C/P」）組織内外のComputer Security Incident Response Team（以下、「CSIRT」）要員育成ないし、育成教材の開発が活動に含まれており、C/P機関の担当スタッフが、最新のサイバー攻撃手法を含んだサイバー攻撃防御演習を継続的に企画・実施できる能力を持つことが求められている。

第３条　実施方針及び留意事項

１．共通留意事項

別紙「共通留意事項」のとおり。

２．本業務に係る実施方針及び留意事項

（１）サイバー攻撃防御演習環境の構築に係る留意事項

一般的に商用のサイバー攻撃防御演習環境[1]（以下、「Cyber Range」）の利用には高額な使用料がかかることから、本業務では、C/Pが用意しうる一般的なIT機器やソフトウェア（例：PC、ネットワーク機材、Windows、オープンソース・ソフトウェア）

[1] サイバー攻撃に対する防御の演習を行うため、コンピュータ上に構築する仮想環境

のみを用いたCyber Range構築が求められる。

本事業においては、具体的に以下の要件を満たすことを前提とする。

- オープンソースと商用基本ソフト（OS）のみを利用し、商用基本ソフトのライセンス料以外の運用維持費が発生しないこと
- カウンターパートによる演習環境構築と自由な改変と再利用が可能なこと
- 提案された演習環境は、継続的な利用実績があること

（２）サイバー攻撃防御演習運営者（以下、「Red Team」）の育成

Red Teamは、各国において、サイバー攻撃シナリオの開発、シナリオに沿ったCyber Range構築、演習の準備・実施および評価といった一連の活動を行うことを目的としたTeamである。このRed Teamメンバーの育成は、3か国のC/P機関を通じて参加者を集め、インドネシア（ジャカルタを想定）で実施する。参加者数は20～24名程度、4チーム（4名から6名/チーム）。参加者選定は以下２．（５）に述べるように、受注者主体で行うものとするが、参加候補者のリスト化は各国の直営専門家及びC/P機関が担当し、参加者の渡航・宿泊・研修会場確保などのロジ作業はインドネシアプロジェクトの直営専門家が担当する。

（３）想定されるRed Team育成研修のスケジュール[2]

インドネシアでのRed Team育成研修は、実働7日間（休日含まず）とし、実施は2025年1月を想定している。想定される研修内容例は以下のとおり。なおプロポーザルにて内容の追加や、日程調整を提案すること可能。

日程	内容
1-2日目	参加者によるCyber Rangeの構築
3-4日目	受注者がRed Team役、研修参加者がサイバー攻撃防御人材役（以下、「Blue Team」）を務めるサイバー攻撃防御演習の実施、及び、この演習で用いたシナリオの解説と各Blue Teamの評価
5日目	演習シナリオの詳細、新規演習シナリオ設計、Blue Team育成演習設計などに関する講義
6-7日目	参加者主体のサイバー攻撃防御演習の試行（例：参加者の一部がRed Teamを務め、残りがBlue Teamを務める）

[2] 上記、想定される研修内容例を参考に受注者が提案するCyber Rangeの提供方法、構成図、予想維持費用等を踏まえ、最も効率的かつ効果的にCyber Rangeを実施するための研修内容、スケジュールを提案してください。

（４）各国におけるサイバー攻撃防御人材（Blue Team）の育成支援

２．（１）の終了後、育成された各国のRed Teamは、インドネシア、フィリピン、カンボジアの各国でBlue Team育成研修を企画し、実施する。受注者は企画段階から各国Red Teamに対し助言を行うとともに、Blue Team演習期間中は現地に滞在し、Red Teamによる研修実施を支援すること。なお、Red Teamのメンバーは技術者が中心となるが、Blue Teamには、技術者と共に、管理者等もメンバーとして加わる可能性が高い。Blue Teamは意思決定者である管理者Sub Team（例：経営者、CIO、CISO、ICTセクション長）と、現場技術者Sub Team（例：CSIRTスタッフ、ICTセクションスタッフ）の2種類のサブチームから構成されることを想定している。

受注者は、各国Red Teamが希望する場合、技術者向けのシナリオと親和性のある管理者Sub Team向けの演習シナリオを事前に準備し、各国Red Teamが演習に取り込めるよう支援すること。

Blue Teamの募集・選定、及び研修会場確保などのロジ作業は、各国のRed Teamと各国の直営専門家またはC/P機関が行う。ただし、Red Teamの準備において技術的な支援が必要な場合は、受注者がオンラインで支援する。なお、Blue Team育成研修は、実働2日、実施は各国において1回、2025年2月から4月の間を想定している。

（５）演習シナリオとCyber Range[3]

演習シナリオは可能な限り、実際に発生したサイバー攻撃（以下、「インシデント」）をもとに作成し、かつ、Red Team育成研修では、直近で発生したインシデント情報を収集し、それに基づいた新シナリオの作成方法も含むことする。

また、Cyber Rangeには、Firewallと、DeMlitarized Zone（以下、「DMZ」）[4]で守られたDomain Name System（以下、「DNS」）[5]、Webサーバー、メールサーバー、Proxyサーバー、及び内部公開用のファイルサーバー（Windows server）とクライアントPC

---

[3] 第3条　2. (1)記載の通り、本業務におけるCyber Rangeは、運用維持管理費を抑え、自由な改変と再利用ができるように、オープンソースと商用基本ソフト（OS）のみを利用することが求められている。また、直近で発生した実際のサイバー攻撃をもとにした演習シナリオの作成方法も本業務において提供される。これらの条件のもとで、Cyber Rangeの提供方法、Cyber Rangeの構成図、予想維持費用についてプロポーザルで提案してください。

[4] コンピュータネットワークにおいて、インターネット等の外部ネットワークと内部ネットワーク（プライベートネットワーク）の中間に設けられたネットワーク。各ネットワーク間の通信を必要に応じて制限し、外部ネットワークと接続する必要があるサーバー等を設置することで内部ネットワークのセキュリティを保護しながら外部ネットワークと接続できる。

[5]コンピュータネットワーク上のホスト名や電子メールアドレスに使われるドメイン名とIPアドレスとの対応付けを管理するために使用されるシステム。

を構成要素に含み、かつ、既に受注者が実際の研修で利用した実績のある環境をベースとすること。なお、プロポーザルには、Cyber Rangeの構成図と、本業務終了後、C/P機関が負担する必要のある予想維持費用を記載すること。

（６）Red Team研修参加者に求めるクライテリアの提案と参加者選定[6]

Red Teamメンバーは、Cyber Range構築を行うことから、各種スキル（例：ネットワーク構築、サーバー構築、仮想環境構築）が必要となる。受注者は、（２）のRed Team育成研修の内容や日程を念頭に、参加する人材に事前に求める知識・経験（クライテリア）をプロポーザルで提案すること。各国JICA直営専門家ないし、プロジェクト関係者は、このクライテリアに基づき、C/Pとともに参加候補者リストを作成する。また、受注者は、参加候補者リストから、JICAガバナンス・平和構築部、JICAプロジェクト関係者と確認の上、実際に参加するメンバーを選定するものとする。

（７）Red Team向け事前学習教材の開発と提供

受注者は、（５）で設定したクライテリアに基づき、事前に学んでおくべき資料・教材（英語）を準備し、Red Team育成研修の3か月前までに各国Red Teamに提供すること。また、各国Red Teamに対しては、インドネシアのRed Team育成研修実施前に、Cyber Range構築を自主的に試み、Teamとしてのスキルの確認をしてもらうことを想定している。よって、受注者は、Red Team育成研修の1か月前までに、Cyber Rangeの仕様（例：ネットワーク構成、ソフトウェア構成、設定情報）、及び、それを実装した仮想環境を構築し、答え合わせ用として、各国のRed Teamに提供すること。

（８）Cyber Range用機材の仕様[7]

Red Team育成研修に必要な機材（ハードウェア、ソフトウェア）は、発注者で準備するため、プロポーザルに必要機材の仕様を記載すること。（６）に記載されているCyber Range構築の事前学習に必要な機材は、各国のC/PあるいはJICAプロジェクト直営専門家が準備する。

インドネシア、及びカンボジアのBlue Team育成研修に必要な機材は、JICAプロジェクトが準備する。Red Team育成研修と異なる必要機材がある場合はRed Team育成研

---

[6] Red TeamはITに関する高度なスキルを保有することが前提となっていることから、受注者は、サイバー攻撃防御演習のRed Team育成研修に参加するための前提スキルについてプロポーザルで提案してください。

[7] 発注者は、インドネシアではRed Team育成研修用機材を、各国ではCyber Range構築の事前学習に必要な機材をそれぞれRed Team育成研修前に準備する。そのため、受注者は、Cyber Rangeに必要な機材仕様についてプロポーザルで提案してください。

修用機材仕様を提出する際、同時に情報提供すること。

（９）フィリピン向けCyber Range用機材の調達

受注者は、フィリピン国内で実施するサイバー攻撃防御演習におけるBlue Team 2チーム分の必要機材（C/Pと調整の上必要なものを特定する）を本邦調達し、必要な設定を国内で行った上で現地に携行する。また、研修終了後は、C/Pに機材の受け渡しを行ったうえで、受領書を取得すること。本機材については、定額計上とする。

第４条　業務の内容

１．共通業務

別紙「共通業務内容」のとおり。

２．本業務にかかる事項

（１）プロジェクトの活動に関する業務

本業務にかかる各協力活動との対応は以下の通り

協力	該当する活動	備考
サイバーセキュリティ人材育成プロジェクト(インドネシア)	PDMの活動4－1、及び活動1-4	インドネシア大学では、Blue Team育成研修を正規科目化する予定
サイバーセキュリティ能力向上プロジェクト(カンボジア)	PDMの活動1－5、1－8	
サイバーセキュリティ能力開発（フィリピン）	個別専門家Workplanの活動1－2、1－3	

（２）本邦研修・招へい

本業務では、本邦研修・招へいを想定していない。

（３）その他

① 収集情報・データの提供

- 業務のなかで収集・作成された調査データ（一次データ）、数値データ等について、発注者の要望に応じて、発注者が指定する方法（Webへのデータアップロード・直接入力・編集可能なファイル形式での提出等）で、適時提出する。
- 調査データの取得に当たっては、文献や実施機関への照会等を通じて、対象国の法令におけるデータの所有権及び利用権を調査する。調査の結果、発注

者が当該データを所有あるいは利用することができるものについてのみ提出する。

② ベースライン調査

本業務では当該項目は適用しない。

③ インパクト評価の実施

本業務では当該項目は適用しない。

④ C/Pのキャパシティアセスメント

本業務では当該項目は適用しない。

⑤ エンドライン調査

本業務では当該項目は適用しない。

⑥ 環境社会配慮に係る調査

本業務では当該項目は適用しない。

⑦ ジェンダー主流化に資する活動

本業務では当該項目は適用しない。

第５条　報告書等

１．報告書等

本業務で作成・提出する報告書等及び数量

報告書名	提出時期	言語	形態	部数
業務計画書	契約締結後10営業日以内	日本語	電子データ	1
業務完了報告書	契約履行期限末日	日本語	電子データ	1

- 業務完了報告書は、履行期限１ヶ月前を目途にドラフトを作成し、発注者の確認・修正を経て、最終化する。
- 本業務を通じて収集した資料およびデータは項目毎に整理し、収集資料リストを添付して、発注者に提出する。
- 受注者もしくはC/P等第三者が従来から著作権を有する等、著作権が発注者に譲渡されない著作物は、利用許諾の範囲を明確にする。

記載内容は以下のとおり。

（１）業務計画書

共通仕様書第６条に記された内容、及び以下の項目を含む内容で作成する。

① サイバー攻撃防御演習の概要（背景・目的）
② サイバー攻撃シナリオ案
③ Cyber Range構成案
④ 研修スケジュール
⑤ 要員計画
⑥ JICAプロジェクト側負担事項（例：機材、便宜供与）

（２）業務完了報告書

① サイバー攻撃防御研修の実施概要
② Red Team育成研修参加者リスト、及び参加者評価
③ 各国Blue Team育成研修参加者数、及びRed Team研修実施能力評価
④ 研修実施上の課題・工夫・教訓（業務実施方法、運営体制等）

２．技術協力作成資料

本業務を通じて作成する以下の資料については、事前に相手国実施機関及び発注者に確認し、そのコメントを踏まえたうえで最終化し、当該資料完成時期に発注者に共有する。また、これら資料は、業務完了報告書にも添付する。

（１）Cyber Range構築マニュアル、及びシナリオ構築マニュアル（Red Team育成研修で用いた教材をベースに、参加者からのコメント等を入れたもの：英文）

３．コンサルタント業務従事月報

業務従事期間中の業務に関し、以下の内容を含む月次の報告を作成し、発注者に提出する。なお、先方と文書にて合意したものについても、適宜添付の上、発注者に報告する。

（１）今月の進捗、来月の計画、当面の課題
（２）業務従事者の従事計画／実績表
（３）活動に関する写真

第６条　再委託

本業務では、再委託を想定していない[8]。

[8] ただし、再委託による業務の遂行が不可欠と考える業務がある場合には、当該業務の内容・方法及び再委託によることが必要な理由を詳述し、協議する。

第７条　機材調達

受注者は、業務の実施に必要と判断される以下の機材を「コンサルタント等契約における物品・機材の調達・管理ガイドライン」に沿って調達する。受注者は、C/Pと確認し、発注者・受注者協議の上で機材名/数量/仕様を最終的に確定する。

調達機材の想定規模は以下のとおり。

	機材名	内容	数量	機材の別	見積の取扱
1	演習機材一式	フィリピンBlue Team演習用機材	2セット	事業用物品	定額計上

第８条　「相談窓口」の設置

発注者、受注者との間で本特記仕様書に記載された業務内容や経費負担の範囲等について理解の相違があり発注者と受注者との協議では結論を得ることができない場合、発注者か受注者のいずれか一方、もしくは両者から、定められた方法により「相談窓口」に事態を通知し、助言を求めることができる。

案件概要表

１．案件名

国　名：インドネシア共和国
案件名：和名　サイバーセキュリティ人材育成プロジェクト
　　英名　Project for Human Resources Development for Cyber Security Professionals

２．事業の背景と必要性

（1）当該国におけるサイバーセキュリティセクターの開発実績（現状）と課題

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。バングラデシュ中央銀行が被害を受けた 8100 万ドルの不正送金等、重要インフラへのサイバー攻撃が世界各国で確認されており、国家の重要リスクとして認識されている。

インドネシアにおいては、サイバーセキュリティ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サイバーセキュリティ人材の量・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サイバーセキュリティ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。

（2）当該国におけるサイバーセキュリティセクターの開発政策と本事業の位置づけ

情報通信省が 2016 年に策定したインドネシアサイバーセキュリティ戦略における柱の一つとして、サイバーセキュリティに関する意識改革及び産業界のニーズを踏まえた人材の育成を、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、サイバーセキュリティ対策の重点としている。

本協力は、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）向けサイバーセキュリティ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サイバーセキュリティ人材を持続的に供給するものである。

（3）サイバーセキュリティセクターに対する我が国及び JICA の援助方針と実績

我が国の援助方針として、開発協力大綱で、サイバー空間に関わる開発途上国の能力強化が挙げられている。また、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2016 年）においても、ASEAN 諸国を中心に能力構築支援を行う方針が示されている。

また本事業は、CII のサイバーセキュリティ対策強化を通じて、SDGs における「目標９．レジリアントなインフラ構築、包括的かつ持続可能な産業化の促進及びイノベーションの推進」に貢献する。

国際協力機構（JICA）は、「インドネシア国情報セキュリティ能力向上プロジェクト」（2014 年 7 月～2017 年 1 月）を通じ、インドネシア政府機関のサイバーセキュリティ対策強化のための仕組み作りや、インドネシア及び近隣諸国（カンボジア、ラオス、ミャンマー、ベトナム及び、東ティモール、ブルネイ）の政府セキュリティ人材の育成を支援してきた。課題別研修（「ASEAN 地域のサイバーセキュリティ対策強化のた

めの政策能力向上」、「サイバー攻撃防御演習」及び「サイバー犯罪対処能力向上に関する研修」）を通じて、人材育成を継続しており、本協力はそれらアセットの活用と発展に資するものである。

（4）他の援助機関の対応
韓国国際協力団（KOICA）による「国立 ICT 人材育成（National Information and Communication Technology-Human Resource Development：NICT-HRD）センター」の設立（2010 年～2019 年）

３．事業概要

（1）事業目的（協力プログラムにおける位置づけを含む）
本事業は、インドネシア国において、セキュリティ知識分野（SecBoK）人材スキルマップに準拠するプロフェッショナル人材育成のためのサイバーセキュリティプログラムをインドネシア大学内に立上げ、諸外国のサイバーセキュリティ人材も巻込みながら、オープンソースのセキュリティツール[9]やオープンコースウェア[10]を開発することにより、同大学におけるサイバーセキュリティ人材の育成システム強化を図り、もって重要インフラをはじめとするインドネシアの民間機関・政府のサイバーセキュリティ対応能力強化に寄与するものである。

（2）プロジェクトサイト/対象地域名
インドネシア国ジャカルタ市インドネシア大学
（3）本事業の受益者（ターゲットグループ）
直接受益者：インドネシア大学職員・学生等、インドネシア政府機関職員、CII 防御の対象となるインフラ機関職員及び諸外国の政府関係機関や IT 系高等教育機関の職員
最終受益者：インドネシア国民、並びに諸外国及び周辺国の国民

（4）事業スケジュール（協力期間）
2019 年 5 月～2025 年 5 月を予定（計 72 ヶ月）

（5）総事業費（日本側）
5.03 億円（概算額）

（6）相手国側実施機関
インドネシア大学（責任機関は情報通信省）

（7）投入（インプット）
1）日本側
【専門家】（計 149M/M を想定）チーフアドバイザー、業務調整／サイバーセキュリティ、カリキュラム策定、科目策定広報計画

[9] ソースコードを無償で公開し、誰でも自由に改良・再配布ができるようにしたもの
[10] 高等教育機関で正規に提供された講義とその関連情報を、インターネットを通じて無償で公開するもの

【機材供与】ラボ用機材
【研修】カリキュラム策定
【プロジェクト活動に係る業務費】
　2）インドネシア国側
【カウンターパートの配置】プロジェクトダイレクター、副プロジェクトダイレクター、プロジェクトマネージャー及びカウンターパート人員
【プロジェクト事務所スペース】事務所スペース、事務機器（机、椅子等）、
【予算】下記事項の実施に関する予算：
プロジェクト活動に関するカウンターパート（C/P）の給与・交通費、その他日本側が負担しない業務費
【外部関係者との連携に関するアレンジ】

（8）環境社会配慮・貧困削減・社会開発
　1）環境に対する影響/用地取得・住民移転
　　① カテゴリ分類（A,B,C を記載）C
　　② カテゴリ分類の根拠：　本事業は、「国際協力機構環境社会配慮ガイドライン」（2010 年 4 月公布）上、環境への望ましくない影響は最小限であると判断されるため。
　2）ジェンダー平等推進・平和構築・貧困削減「ジェンダー対象外」
　3）その他 特に無し

（9）関連する援助活動
　1）我が国の援助活動
「情報セキュリティ能力向上プロジェクト」（2014 年 7 月～2017 年 1 月）
　2）他ドナー等の援助活動
KOICA が「国立 ICT 人材育成（National Information and Communication Technology-Human Resource Development：NICT-HRD）センター」の設立を支援（2010 年～2019 年）しており、政府職員に対する ICT に関する幅広い分野で基礎的な教育を行っているが、本協力では大学を通じてより高度な人材育成を行うことにより、効果を補完することができる。

４．協力の枠組み

（1）協力概要
　1）上位目標と指標
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。
指標：水準を満たすサイバーセキュリティ教育を受けた ICT エンジニアの割合（CII オペレーターのみ場合に分けた評価）、水準を満たすインシデントハンドリングツールを備えた機関の割合（CII オペレーターのみ場合に分けた評価）
※ベースラインサーベイにより指標及び水準を具体化する
　2）プロジェクト目標と指標
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。
指標：インドネシア大学におけるセキュリティ知識分野（SecBoK）人材スキルマップ

に準拠するプロフェッショナル向けサイバーセキュリティ教育の受講可能人数、プログラム修了者の所属機関等の満足度

3）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サイバーセキュリティツールが開発される。

成果 3：サイバーセキュリティに関するオープンコースウェアが開発され公開されるとともに、専門的に開発された教材についても要望があれば提供する。

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）活動

成果 1）

1-1　NICE, SecBoK 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。

1-2　包括的で最新のサイバーセキュリティ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　講師への必要なトレーニングが行われる。（民間企業のゲスト講師を含む）

1-5　長期コースのコンポーネントとなる短期のサイバーセキュリティコースが設立される。

1-6　必要なタイミングでコースに関係する活動が見直される。

成果 2）

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）

3-1　他教育機関の要請に基づき、インドネシア大学にて開発された一部の教材共有にかかる協定をインドネシア大学と該当教育機関で締結する。

3-2　教育機関に対して、教材の提供及び講師向け研修を実施する。

3-3　授業ビデオや生徒用の教材等をオープンコースウェアにて提供する。

3-4　教育機関及びオープンコースウェア利用者からフィードバックを集め、科目の改善を行う。

成果 4）

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．前提条件・外部条件

（1）前提条件

特になし。

（2）外部条件（リスクコントロール）

１）成果達成のための外部条件

（設定なし）

２）プロジェクト目標達成のための外部条件

（設定なし）

３）上位目標達成のための外部条件

参加機関において予算措置含む必要なセキュリティ対策が準備される。

インドネシア大学がインドネシア国のサイバーセキュリティ専門人材育成機関の中枢として位置付けられ続ける。

４）上位目標達成後さらなる発展を得るための外部条件

（設定なし）

６．評価結果

本事業は、インドネシア国の開発政策、開発ニーズ、日本の援助政策と十分に合致しており、また計画の適切性が認められることから、実施の意義は高い。

７．過去の類似案件の教訓と本事業への活用

（1）類似案件の評価結果

インドネシア国情報セキュリティ能力向上プロジェクト（技術協力プロジェクト：2014 年～2017 年）において、同国通信情報省の情報セキュリティ対策実施能力向上のため、情報セキュリティマネジメントシステム(ISMS)制定促進、技術研修、パイロット事業を通じた地方行政機関の ISMS 取得や、Computer Security Incident Response Team (CSIRT)立ち上げの手順の整備、セキュリティ意識啓発を並行して実施した。

（2）本事業への教訓

サイバーセキュリティにかかる研修や国際会議は多数開催されており、主要な C/P がそれらに参加するために不在となることが多い。また日常業務も多忙のため継続的な研修参加が困難など活動の進捗への影響が懸念される。従って、支援計画の検討に際しては、先方の体制や実際の業務状況を十分に確認すると共に、特に日本の内閣サイバーセキュリティセンターを中心とした本邦関係機関とは密な情報共有を行うこととする。人員数が不足する C/P の場合、技術移転が効率的に行われるよう短期専門家を同時期に複数派遣し、C/P の業務状況を踏まえながら集中的に技術移転を行う等、柔軟な投入を必要に応じて検討する。

８．今後の評価計画

（1）今後の評価に用いる主な指標

４．（１）のとおり。

（2）今後の評価計画

事業開始 7 か月　　ベースライン調査

事業終了 3 年度　　事後評価

（3）実施中モニタリング計画

事業開始　6 か月／年　JCC における相手国実施機関との合同レビュー事業終了　6 か月前　　終了前 JCC における相手国実施機関との合同レビュー

９．広報計画

（1）当該案件の広報上の特徴

1）相手国にとっての特徴

2017 年 5 月に発生した世界規模のサイバー攻撃は、全世界 150 超国・地域におよんだ。サイバーセキュリティ対応能力向上は、インドネシア政府、外資系企業含んだ民間企業、インドネシア国民含め、国や地域全体への裨益案件と印象付ける。

2）日本にとっての特徴

2016 年 10 月に「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」が内閣サイバーセキュリティセンター他関係省庁合意で示され、本案件は二国間協力の具体的な取り組みとして、インシデント・レスポンス等の能力の向上支援と位置づけられる。

（2）広報計画

特に無し。

以上

事業事前評価表

国際協力機構ガバナンス・平和構築部 STI・DX 室

１．案件名（国名）

国　名：　カンボジア王国

案件名：　和名　サイバーセキュリティ能力向上プロジェクト

英名　Project for Improvement of Cyber Resilience

２．事業の背景と必要性

（１）　カンボジアにおけるサイバーセキュリティ及び ICT 分野の現状・課題及び本事業の位置づけ

カンボジアは国家最高位の戦略である「第四次四辺形戦略」の下、2030 年に中所得国、2050 年に高所得国入りを目指しており、その目的達成に向けた重要な政策として、「デジタル経済・社会政策フレームワーク（Cambodia Digital Economy and Society Policy Framework）」（2021－2035）が 2021 年 5 月に国会承認された。社会のすべてのセクター（国家、市民、企業）でデジタルの導入とデジタルトランスフォーメーションの基盤を築き、活力あるデジタル経済と社会の構築を目指すものである。2022 年にはカンボジア首相の指示の下、「国家デジタル経済・社会評議会（National Digital Economy and Society Council）」が創設され、今後その傘下にサイバーセキュリティの担当を担う「デジタルセキュリティ委員会（Digital Security Committee：DSC）」も創設される予定である。郵政通信省（Ministry of Post and Telecommunications、以下「MPTC」という。）は「デジタル政府政策（Cambodia Digital Government Policy）」（2022-2035）を策定し、行政のデジタル化を通じた質の高い公共サービスの提供を通じて市民の生活の質向上を目指している。サイバーセキュリティの確保は政府戦略の実現に向けて極めて重要な行政能力の一つとされており、2007 年には MPTC 内の ICT セキュリティ局　（Department of ICT Security）傘下にサイバーセキュリティインシデント対応チーム「CamCERT（Cambodia Computer Emergency Response Team）」も設置されている。カンボジアでは、新しい経済成長と社会福祉のため、サイバーセキュリティも含めたデジタル経済、社会の推進に力を入れている。しかし、国際電気通信連合（International Telecommunication Union、以下「ITU」という。）が発行している Global Cybersecurity Index（以下「GCI」という。[11]）2020 においては、カンボジアは、全世界 194 か国中 132 位（アジア太平洋 38 か国中 26 位）であり、CamCERT の体制及び能力は日に日に高度化するサイバー攻撃に対応するためのスキルや最新技術に関する知識が十分に備わってはおらず、政府省庁や関連機関からサイバーセキュリティ人材と基礎的な能力の不足が指摘されている。

本事業は、カンボジアの郵政通信省傘下の ICT セキュリティ局を中心にサイバーセキュリティ能力向上の支援を行い、同局と重要情報インフラ（Critical Information Infrastructure：以下「CII」という。）産業や他の政府省庁間のサイバーセキュリティに関する組織間の連携を強化することで、ICT セキュリティ局のサイバーセキュリティ能力向上、また将来的にカンボジアにおけるデジタル社会のサイバーセキュリテ

[11]ITUが設定している、グローバルレベルでの各国のサイバーセキュリティの取り組みを想定する指標であり、「法規制（Legal）」「戦略・組織体制（Organizational）」「技術力（Technical）」「能力構築（Capacity Developing）」「組織間連携（Cooperative）」の5つの要素に沿って評価し、総合スコアとして集約したもの。
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ィ・レジリエンスの強化に資するものである。

（２） カンボジアに対する我が国及び JICA の協力方針等と本事業の位置づけ
課題別事業戦略における本事業の位置づけ
我が国の「対カンボジア国別開発協力方針」（2017 年 7 月）では、重点分野として「ガバナンスの強化」を挙げており、サイバーセキュリティの能力強化を行う事はデジタル経済の急速な進展が進むカンボジアにおいては重要な支援対象である。
日本政府は 2009 年以降、我が国と ASEAN 諸国との国際的な連携・取組を強化することを目的として、日 ASEAN サイバーセキュリティ政策会議を継続して開催しており、同地域では十数年にわたる継続的な支援により、良好な信頼関係を構築している。ASEAN 地域を中心とした多様な主体との国際的な連携によってサイバーセキュリティの確保に取り組んでいくこと、ASEAN 地域の支援や重要インフラ向けの支援強化が求められている。
JICA における課題別事業戦略（グローバル・アジェンダ）「No.15 デジタル化の促進」では、サイバーセキュリティを重要クラスターとして位置付けて、特に東南アジア地域を重点協力地域と位置付けており、本事業は当該戦略とも合致するものである。
SDGs においては、全目標においてデジタル技術の活用が期待されるものであることを踏まえ、本事業は全ての SDGs 達成を支える取り組みとなる。特に本事業はゴール 9「産業と技術革新の基盤をつくろう」、ゴール 17「パートナーシップで目標を達成しよう」との関連が深く、同 SDGs 達成に資する内容となる。
（３） 他の援助機関の対応
詳細計画策定調査では、他機関・ドナーによる協力は確認されていない。

３．事業概要

（１） 事業目的
本事業は、MPTC 傘下の ICT セキュリティ局を中心にサイバーセキュリティ能力向上のための研修やセミナーを提供し、同局と CII 産業や他の政府省庁間のサイバーセキュリティに関する組織間の連携を強化することで、ICT セキュリティ局のサイバーセキュリティ能力向上を図り、もってカンボジアにおけるデジタル社会のサイバーセキュリティ・レジリエンスの強化に資するもの。
（２） プロジェクトサイト／対象地域名
プノンペン都／カンボジア
（３） 本事業の受益者（ターゲットグループ）
直接裨益者：政府機関職員（MPTC、関係省庁、地方政府）、CII 産業関連機関職員
間接裨益者：カンボジア国民、カンボジア関連企業
（４） 総事業費（日本側）
274 百万円
（５） 事業実施期間
2023 年 5 月～2026 年 10 月（計 42 か月）
（６） 事業実施機関
郵政通信省（MPTC）、ICT 総局（General Department of ICT）傘下の情報セキュリティ局（Department of ICT Security）
（７） 投入（インプット）
1）日本側：

① 専門家派遣

長期専門家：業務調整／サイバーセキュリティ

短期専門家：チーフアドバイザー、サイバーセキュリティ人材育成、CSIRT[12]サービス強化、普及啓発活動等

② 研修員受け入れ：サイバーセキュリティ分野

③ 機材供与：サーバー、ネットワーク機器、各種ソフトウェア等

④ 調査団派遣：サイバーセキュリティ関連機関職員等

2）カンボジア国側

① カウンターパートの配置

プロジェクトディレクター1 名：Secretary of State（MPTC）、副プロジェクトディレクター1 名：Director General（ICT 総局）、プロジェクトマネージャー1 名：Director（ICT セキュリティ局）、その他

② 案件実施のためのサービスや施設、現地経費の提供

執務室（執務用機材含む）、光熱費、管理運営費、研修用会場設備など

（８） 他事業、他開発協力機関等との連携・役割分担

1） 我が国の援助活動

ASEAN 諸国向けに、内閣サイバーセキュリティセンター（NISC）を中心に総務省、経済産業省にて様々な支援を実施している。本邦の各サイバーセキュリティ関係機関には定期的に本事業の活動内容を報告し、専門家派遣等、連携を検討していく。具体的には、CII 産業防護や、組織間連携強化、民間企業や国民に対する啓発活動に関する本邦における取り組みに関連した連携を想定する。

2） 他の開発協力機関等の援助活動

詳細計画策定調査中に実施した MPTC への聞き取り調査の中で、具体的な援助活動は確認できなかった。

（９） 環境社会配慮・横断的事項・ジェンダー分類

1） 環境社会配慮

① カテゴリ分類：C

② カテゴリ分類の根拠：本事業は、「国際協力機構環境社会配慮ガイドライン」（2010 年 4 月公布）に照らし、環境への好ましくない影響は最小限であると判断されるため。

2） 横断的事項：特になし

3） ジェンダー分類：【対象外】■（GI）ジェンダー主流化ニーズ調査・分析案件

＜分類理由＞詳細計画策定調査にてジェンダー主流化ニーズが調査されたものの、ジェンダー平等や女性のエンパワメントに資する具体的な取組について指標等を設定するに至らなかったため。ただし、事業開始後、女性を対象として一般向けのサイバーセキュリティに関する普及啓発活動など、

[12] CSIRTは、Computer Security Incident Response Teamの略であり、セキュリティインシデントが発生した場合に、適切な対応を実施する組織のことを指す。

ジェンダーの視点を踏まえた具体的な取り組みを実施する予定。

（１０）　その他特記事項

特になし

４．事業の枠組み

（１）　上位目標：カンボジアにおけるデジタル社会のサイバーセキュリティ・レジリエンスが強化される

指標：定量指標① ITU の GCI スコアが改善される（成長ステージとして設定した 30-80 程度を目標数値とする）

② 国家レベルで、いくつかの関連省庁で CSIRT が設立される[13]

定性指標③ プロジェクト期間中に策定された標準やガイドラインが他省庁で利用される

④ 国家または地方レベルでの普及啓発活動が、サイバーセキュリティ関連組織によって継続的に実施される

（２）　プロジェクト目標：ICT セキュリティ局のサイバーセキュリティ能力が強化される

指標：定量指標① ICT セキュリティ局が提供する CSIRT サービス範囲の数が××数増加する[14]、またインシデント検知数、インシデント対応数等増加する[15]

定性指標② 明確になった CSIRT サービスの運用レベル[16]と法整備の準備状況（CSIRT 組織成熟度の評価）が改善される

（３）　成果

成果１：CSIRT サービスの提供能力が改善される

成果２：関係機関（他省庁）・CII 事業者や、一般国民等におけるサイバーセキュリティの活動が促進される

成果３：サイバーセキュリティを強化するために必要な法律・規制・標準等が特定される

（４）　主な活動

【成果 1 の主な活動】

- 国家 CSIRT としての機能はもとより、普及啓発や関係省庁・CII 事業者との連携に資するサイバーセキュリティ人材育成を特定・計画し実施する。
- 研修の成果を評価しフィードバックも含め、次の研修計画に反映させる。
- CSIRT 業務に必要な技術文書を作成する。

【成果 2 の主な活動】

- オンライン上の社会的弱者（女性・子供・年配者等）を中心とした一般向けのサイバーセキュリティに関する普及啓発活動のニーズを特定の上、教材を作成

[13]ベースライン調査時に設定する。

[14]ベースライン調査時に設定する。

[15]インシデント検知数とインシデント対応数は、サイバー攻撃自体の規模（測定不能）や検知・対応する攻撃レベルによって変化するため目標値は設定せず、実績値を分析することで、サイバー攻撃の情勢とともにC/Pの防御・対応態勢が強化されたかを判断する。

[16]成果1において特定されたC/Pへ求められるCSIRTサービスを運用する体制や仕組みが整っているかの程度を意味している。運用レベルは成熟度評価ツールにより測定する。

し、普及啓発活動を行う。
- 成果 1 で作成した技術文書を関連機関に対して普及させる。

【成果 3 の主な活動】
- 調査対象の政策・法律・標準を特定の上、研究した後、カンボジアに必要な政策・法律・標準等を取りまとめる。
- 関係者に対してコンサルテーションを実施し、カンボジアに必要な政策・法律・戦略等に関する提言を作成する

５．前提条件・外部条件

（１） 前提条件
- CSIRT 業務提供維持のための予算と人材が継続的に提供される
- ICT セキュリティ局の責務が大幅に変更されない

（２） 外部条件（リスクコントロール）
- ICT セキュリティに関する政策の方向性が大きく変更されない
- ICT セキュリティ局の責務と人員配置が維持される
- プロジェクト活動の成果が MPTC 内で効果的に活用される

６．過去の類似案件の教訓と本事業への活用

インドネシア国「情報セキュリティ能力向上プロジェクト」（2014 年～2017 年）では、インドネシア国通信情報省の情報セキュリティ対策実施能力向上に向け、多数のセキュリティ意識啓発を並行して実施したが、教訓としてカウンターパートの時間の確保が挙げられる。本プロジェクトでは、一部のカウンターパートにプロジェクト業務が集中しないよう詳細計画策定調査期間中に、MPTC の関係各部署の所掌業務をヒアリングし、プロジェクト活動に関連する部署から協力が得られる体制を提案し、MPTC 側から合意を取り付けた。

コロンビア国「土地返還政策促進のための土地情報システムセキュリティ管理能力強化プロジェクト」（2013 年 7 月～2016 年 6 月）、カンボジア国「人間の安全保障実現化のための CMAC 機能強化プロジェクト」(2008 年 4 月～2010 年 9 月) 及び、キルギス国「IT 人材育成（国立 IT センター）プロジェクト」（2004 年 10 月～2008 年 5 月）では、事業終了後のカウンターパートの財政状況の悪化、異動や離職等が持続性を確保する上での問題となった。事業完了後の持続性確保に向けた動きとして、MPTC 内に 2021 年に新たに設立された人材育成機関（Cambodia Academy of Digital Technology : CADT）の活用の可能性を探るべく、プロジェクト活動において、MPTC 側と協議の場を設定した。また、MPTC 内での技術の標準化と移転した技術の持続性を担保していくための対策として、活動の中に標準運用手順書やガイドライン等の作成も盛り込んでいる。

７．評価結果

本事業は、当国の開発課題・開発政策並びに我が国及び JICA の協力方針・分析に合致し、サイバーセキュリティの推進を通じて、デジタル社会のサイバーセキュリティ・レジリエンスの強化に資するものであり、SDGs の特に、ゴール 9「産業と技術革新の基盤をつくろう」及びゴール 17「パートナーシップで目標を達成しよう」に貢献すると考えられることから、事業の実施を支援する必要性は高い。

８．今後の評価計画

（１）今後の評価に用いる主な指標

４．（１）のとおり。

（２）今後の評価スケジュール

事業開始６か月：ベースライン調査

事業終了６カ月前：終了時評価

事業終了３年後：事後評価

以上

案件概要表

１．案件名（国名）

国　名： フィリピン共和国（フィリピン）
案件名： サイバーセキュリティ能力開発
Capacity Development for Cybersecurity

２．事業の背景と必要性

（１）当該国におけるサイバーセキュリティ分野の現状・課題及び本事業の位置付け

デジタル化の進展に伴い、ヒト、モノ、カネ、行政機関を含めた組織やインフラシステムの多くがサイバー空間で繋がっており、サイバーセキュリティのリスクが甚大化している。多くの開発途上国各国ではサイバーセキュリティの対策体制・能力の不足と人材不足がリスクを増大させており、世界的に猛威を振るったランサムウェアによる被害、エネルギー・金融・通信・保健等の重要情報インフラ（CII）が受ける深刻な被害、サプライチェーン通じた機密情報漏洩、偽情報による社会的混乱、個人情報漏洩等の被害が多発している。

USAID と IBM が 2022 年に実施した「National Cybersecurity Talent Workforce Assessment Report of the Philippines」によると、フィリピンは悪意のあるソフトウェアの一種であるバンキング型トロイの木馬によって攻撃されたユーザ数が、アジア太平洋地域で最も多かった。また同報告書によれば、フィリピンは 2021 年にサイバー犯罪者によって標的にされた回数が、全世界で 4 番目に多い国であった。また、国際電気通信連合（International Telecommunication Union 以下 ITU）が発行している Global Cybersecurity Index（GCI）2020 において、フィリピンは全世界 194 か国中 61 位（アジア太平洋 37 か国中 13 位）となっている。

フィリピン国の「国家サイバーセキュリティ計画（NCSP）2022」では、信頼性と強靭性を備えた情報インフラ構築を目指して、①重要インフラの強化およびレジリエンスの向上、②政府情報システムの準備と安全確保、③サイバーリスクに関する民間企業の意識向上と攻撃の予防・保護・対応・回復のための企業のセキュリティ対策、④サイバーリスクに対する個人の意識向上に取り組むとしている。同計画を推進している情報通信技術省（Department of Information and Communications Technology 以下 DICT）サイバーセキュリティ局（Cybersecurity Bureau）は、国家コンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team 以下 CSIRT）としての技術力向上、政府及び CII との連携体制強化、政府機関・民間企業・国民へのサイバーセキュリティの認知度向上を課題として認識しており、本事業を通じた人材及び組織能力強化の実施意義は高い。

（２）フィリピンに対する我が国及び JICA の協力方針等と本事業の位置づけ、課題別事業戦略における本事業の位置づけ

本事業は、我が国の「対フィリピン国別開発協力方針」（2018 年 4 月）の内、重点分野「持続的経済成長のための基盤の強化」に該当する。

日本政府は 2009 年以降、我が国と ASEAN 諸国との国際的な連携・取組を強化することを目的として、日 ASEAN サイバーセキュリティ政策会議を継続して開催しており、サイバーセキュリティ戦略本部が決定した「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2021 年）においても、ASEAN 地域を中心とした多様な主体との国際的な連携によってサイバーセキュリティの確保、および ASEAN 地域の支援や重要インフラ向けの支援強化に取り組むとしている。更に、「自由で開かれたインド太平洋（FOIP）のための新たなプラン」

（2023 年）取組の柱 2「インド太平洋流の課題対処」事例 23「自由、公正かつ安全なサイバー空間の確保」にも本事業は合致する。

「JICA 国別分析ペーパー」（2020 年）においても、重点分野「持続的経済成長のための基盤強化」の「経済成長の質」に位置付けられる。

JICA における課題別事業戦略（グローバル・アジェンダ）「No.15 デジタル化の促進」ではサイバーセキュリティを重要クラスターとして位置づけており、特にサイバー空間における脅威への対応技術の向上と政府体制を整備する本事業の内容は、当該クラスターの方針とも合致する。

SDGs においては、全目標においてデジタル技術の活用が期待されるものであることを踏まえ、本事業は全ての SDGs 達成を支える取り組みとなる。

（３）他の援助機関の対応

USAID が Better Access and Connectivity Project （BEACON）を実施し、5 年間で約 40 億円を DICT へ拠出し、DICT を含む全公務員向けのサイバーセキュリティ専門人材育成支援を実施している。BEACON では CISSP というサイバーセキュリティの資格の中でも難易度の高い資格取得を支援しており、本事業ではより基礎的な研修を実施し、重複を避けるとともに事業間の補完し合うことを検討する。また、オーストラリア政府が国家サイバーセキュリティ機関委員会（National Cybersecurity Inter-Agency Committee）とサイバーセキュリティ能力向上を目的としたパートナーシップを締結している。

３．事業概要

（１） プロジェクトサイト／対象地域名：フィリピン国 マニラ

（２） 事業実施期間：2023 年 9 月～2025 年 8 月を予定（計 24 カ月）

（３） 事業実施体制

実施機関：情報通信技術省（DICT）サイバーセキュリティ局（Cybersecurity Bureau）

４．事業の枠組み

（１） 成果

成果１：サイバーセキュリティ局の技術力が向上する。

成果２：重要情報インフラ産業の各セクターにおける調整・連携能力が向上する。

成果３：サイバーセキュリティ教育プログラムが拡充する。

（２） 主な活動

１-１サイバーセキュリティ局職員を主な対象とした研修計画を作成する。

１-２セキュリティ研修を実施する。

１-３サイバーセキュリティ局の業務に対する助言を行う。

２-１セクター毎の調整・連携スキームに関する助言を行う。

２-２セクター毎の調整・連携にかかるセミナー等を実施する。

３-１サイバーセキュリティの普及啓発活動にかかる教材開発を支援する。

３-２サイバーセキュリティに関する普及啓発活動の実施を支援する。

以上

別紙

共通留意事項

１．必須項目

（１）討議議事録（R/D）に基づく実施

- 本業務は、発注者と相手国政府実施機関とが、プロジェクトに関して締結した討議議事録（R/D）に基づき実施する。

（２）C/P のオーナーシップの確保、持続可能性の確保

- 受注者は、オーナーシップの確立を充分に配慮し、C/P との協働作業を通じて、C/P がオーナーシップを持って、主体的にプロジェクト活動を実施し、C/P 自らがプロジェクトを管理・進捗させるよう工夫する。
- 受注者は、プロジェクト終了後の上位目標の達成や持続可能性の確保に向けて、上記 C/P のオーナーシップの確保と併せて、マネジメント体制の強化、人材育成、予算確保等実施体制の整備・強化を図る。

（３）開発途上国、日本、国際社会への広報

- 発注者の事業は、国際協力の促進並びに我が国及び国際経済社会の健全な発展に資することを目的としている。このため、プロジェクトの意義、活動内容とその成果を相手国の政府関係者・国民、日本国民、他ドナー関係者等に正しくかつ広く理解してもらえるよう、発注者と連携して、各種会合等における発信をはじめ工夫して効果的な広報活動に務める。

（４）他機関/他事業との連携、開発インパクトの最大化の追求

- 発注者及び他機関の対象地域／国あるいは対象分野での関連事業（実施中のみならず実施済みの過去のプロジェクトや各種調査・研究等も含む）との連携を図り、開発効果の最大化を図る。
- 日本や国際的なリソース（政府機関、国際機関、民間等）との連携・巻き込みを検討し、開発インパクトの最大化を図る。

（５）根拠ある評価の実施

- プロジェクトの成果検証・モニタリング及びプロジェクト内で試行する介入活動の効果検証にあたっては、定量的な指標を用いて評価を行う等、根拠（エビデンス）に基づく結果提示ができるよう留意する。

２．選択項目

（１）他の専門家との協働

- 発注者は、本契約とは別に、長期専門家及び／もしくは短期専門家を派遣予定である。受注者は、これら専門家と連携し、プロジェクト目標の達成を図ることとする。ワーク・プラン、モニタリングシート、業務進捗報告書、業務完了報告書、事業完了報告書の作成に際しては、上記専門家と協働して作成する。
- 同専門家との役割分担は、第４条「２．本業務にかかる事項」を、同専門家の活動内容は、別添「（参考）別途派遣する専門家の業務内容」をそれぞれ参照する。同専門家の活動に係る費用は発注者が別途手配する。
- 発注者は受注者の求めに応じ、同専門家への役割分担の理解を促進する。

別紙

共通業務内容

１．業務計画書の作成／改定

- 受注者は、業務計画書を作成し、その内容について発注者の承認を得る。

２．広報活動

- 受注者は、発注者ウェブサイトへの活動記事の掲載や、相手国での政府会合やドナー会合、国際的な会合の場を利用したプロジェクトの活動・成果の発信等、積極的に取り組む。
- 受注者は、各種広報媒体で使用できるよう、活動に関連する写真・映像（映像は必要に応じて）を撮影し、簡単なキャプションをつけて発注者に提出する。

３．業務完了報告書の作成

- 受注者は、プロジェクトの活動結果、プロジェクト目標の達成度、上位目標の達成に向けた提言等を含めた業務完了報告書を作成し、発注者に提出する。
- 上記報告書の作成にあたっては、受注者は報告書案を発注者に事前に提出し承認を得た上で、最終版を発注者に提出する。