事業事前評価表

国際協力機構社会基盤・平和構築部
運輸交通・情報通信グループ第二チーム

１．案件名（国名）

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の現状・課題及び本事業の位置付け

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。

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。

（２）サイバーセキュリティセクターに対する我が国及び JICA の協力方針と本事業の位置付け

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。

（３）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[1]やオープンコースウェア[2]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。

[1] 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
[2] 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

（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 6 月～2024 年 5 月を予定（計 60 ヶ月）
（５） 総事業費（日本側）
5.03 億円（概算額）
（６） 事業実施体制
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
【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）他事業、他援助機関等との連携・役割分担
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）他援助機関等の援助活動
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。

（９）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： 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)横断的事項

特になし

3)ジェンダー分類

「ジェンダー対象外」

（１０）その他特記事項

特になし

４．協力の枠組み

（１）協力概要

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。

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：

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：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。

５．前提条件・外部条件 (リスク・コントロール)

（１）前提条件

特になし。

（２）外部条件

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．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（活用）

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。

７．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。

８．今後の評価計画

（1）今後の評価に用いる主な指標

４．のとおり。

（2）今後の評価計画

事業開始７ヶ月以内　ベースライン調査

事業終了３年後　　事後評価

以　上