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。[1]）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

[1]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

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[2]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

[2] 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。

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、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[3]

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

[3]ベースライン調査時に設定する。

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[4]、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[5]

定性指標② 明確になった CSIRT サービスの運用レベル[6]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。

---

[4]ベースライン調査時に設定する。

[5]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。

[6]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。

- 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

別添

サイバーセキュリティ能力向上プロジェクト地図