カンボジア国
サイバーセキュリティ能力向上
プロジェクト

詳細計画策定調査
報告書

2022年10月

独立行政法人　国際協力機構
ガバナンス・平和構築部STI・DX室

カンボジア国サイバーセキュリティ能力向上プロジェクト詳細計画策定調査

報告書　目次

表　目次

図　目次

添付資料

対象地域　位置図


タイ
ベトナム
カンボジア王国
カンボジア
プノンペン
ホーチミン
Hồ Chí Minh
タイランド湾
Google
地図データ ©2022 Google


プロジェクトサイト
郵政通信省 (MPTC)
ボエン・プレア
Lvea Aem
Kien Svay
Prey Sar
SANGKAT CHAOM CHAU
タクマウ
スペイ・ロラム
シエムリアップ
Google
地図データ ©2022

巻頭写真

運輸通信省（MPTC）ICT セキュリティ局職員

MPTC ICT セキュリティ局での協議の様子

MPTC SOC 入口の様子

Association of Banks in Cambodia での面談の様子

内務省（MOI）の職員

内務省（MOI）での面談の様子

経済財務省（MEF）での面談の様子

情報通信省（MPTC）Department of Rural ICT での面談の様子

略語表

AEC	Authority of Electric of Cambodia	カンボジア電力庁
AJCCBC	ASEAN-Japan Cybersecurity Capacity Building Center	ASEAN サイバーセキュリティ能力構築センター
APCERT	Asia Pacific Computer Emergency Response Team	アジア太平洋地域における CSIRT の国際的な非営利団体
APNIC	Asia-Pacific Network Information Centre	アジア太平洋ネットワーク情報センター
AWS	Amazon Web Service	アマゾン・ウェブ・サービス
CADT	Cambodia Academy of Digital Technology	カンボジアデジタル技術アカデミー
CamCERT	Cambodia Computer Emergency Response Team	カンボジア国コンピュータ緊急対応チーム
CTF	Capture the Flag	情報セキュリティのスキルを競い合うセキュリティコンテスト
CIESF	Cambodia International Education Support Foundation	シーセフ
CII	Critical Information Infrastructure	重要情報インフラ
COP	Child Online Protection	児童オンライン保護
C/P	Counterpart	カウンターパート
CSIRT	Computer Security Incident Response Team	コンピュータセキュリティインシデント対応チーム
DDoS	Distributed Denial of Service	分散型サービス拒否攻撃（サイバー攻撃）
DSC	Digital Security Committee	デジタルセキュリティ委員会
EDC	Electricite du Cambodge (Electricity of Cambodia)	カンボジア電力公社
FIRST	Forum of Incident Response and Security Teams	CSIRT の国際的な非営利団体
GCI	Global Cybersecurity Index	世界サイバーセキュリティ指数
GCP	Google Cloud Platform	グーグル・クラウド・プラットフォーム
IBF	Institute of Banking Finance	銀行金融研究所
ISMS	Information Security Management System	情報セキュリティマネジメントシステム
ISP	Internet Service Provider	インターネット・サービス・プロバイダー
ITU	International Telecommunication Union	国際電気通信連合
MAFF	Ministry of Agriculture, Fishery and Forestry	農林水産省
MEF	Ministry of Economy and Finance	経済財務省
MISTI	Ministry of Industry, Science, Technology and Innovation	産業科学技術イノベーション省
MOI	Ministry of Interior	内務省
MPTC	Ministry of Post and Telecommunication	郵政通信省
MCS	Ministry of Civil Service	国家公務員省
NCDD	National Committee for Sub-National Democratic Development	民政的地方開発委員会
NiDA	National Information Communication Technology Development Authority	国家 ICT 開発庁
PO	Plan of Operation	活動計画
PPSEZ	Phnom Penh Special Economic Zone	プノンペン経済特区
SCADA	Supervisory Control And Data Acquisition	産業制御システム（コンピュータによるシステム監視とプロセス制御）
SDN	Software Defined Network	ソフトウェア定義ネットワーク
SecBoK	Security Body of Knowledge	情報セキュリティ知識項目
SIEM	Security Information and Event Management	セキュリティ情報イベント管理システム
SOC	Security Operation Centre	セキュリティ・オペレーション・センター（ネットワーク・モニタリング設備）
SOP	Standard Operation Procedure	標準運用手順書

第1章　調査概要

1-1　調査団派遣の背景

1-1-1　カンボジアのサイバーセキュリティの現状

過去30 年間で飛躍的に普及した携帯電話とインターネットは世界的な情報化とデジタル経済の進展をもたらす中で、開発途上国では、例えば固定電話の普及を待たずにスマートフォンやWi-Fi通信が整備されるような、いわゆる「リープフロッグ型」と呼ばれる経済発展が期待されている。一方、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きており、その結果、サイバーセキュリティのリスクも甚大化している。世界経済フォーラムが発行するGlobal Risks Reportにおいても、2021年に「発生の可能性が高いリスク」の第9位に「サイバーセキュリティ対策の失敗」、「影響が大きいリスク」の第10位に「重要情報インフラとネットワークの機能停止」が挙げられており、人々がデジタル活動を行うためにサイバー空間における安全性、信頼性をいかに確保するかが全世界的な課題となっている。

カンボジアは国家最高位の戦略である「第4次四辺形戦略」（Rectangular Strategy Phase 4）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の推進に向けた産業革命4.0（Industrial Revolution 4.0）の実現、経済の多様化等の重要性について言及している。かかる状況下、「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年～2035年」では、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し、様々な政策施策を提示している。さらに2022年1月には、包括的なデジタル経済・社会を発展させるために、透明で信頼できる方法でガバナンスシステムの近代化及び改革のためのエコシステムでもあるデジタルインフラと技術を活用し、スマート政府を構築していくことを目的に郵政通信省（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年～2035年」を発表した。

サイバーセキュリティはこれらの政府戦略の実現に向けて極めて重要な行政能力の一つであり、カンボジアにおいて過去に発生しているDDoS攻撃やマルウェア・フィッシング等を予防し、政府・市民・ビジネスすべての面において、正常な生活が維持されるために必要不可欠な要素となっている。

なお、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として設置されたCambodia Computer Emergency Response Team（以下、「CamCERT」という。）は2007年に創設されている。ICTセキュリティ局は、CamCERT以外にデジタルフォレンジック・規範・監査・リスク管理・公開鍵基盤の機能を有している。

1-1-2　カンボジアにおけるサイバーセキュリティの課題

近年、カンボジアではサイバーセキュリティに関する体制整備が進められてきたが、日に日にサイバー攻撃は高度化してきている。カンボジア政府の調べによると、省庁や関連機関内職員のおよそ7割がウイルス対策ソフトの導入や更新、定期的なウイルススキャンを適切に施しておらず、また、サイバーセキュリティ専任の職員やスタッフを配置している組織はおよそ2割に留まるという。

このような状況において、カンボジア政府は情報セキュリティやサイバーセキュリティに関する明確な指針を中央省庁や民間企業に対して示すことができていない。また、重要情報インフラ（Critical Information Infrastructure ）（以下、「CII」という。）の分野も定義できておらず、CIIの防御責任

の省庁も明確ではない（本調査時点で、CIIの定義を含む、サイバーセキュリティ法を策定中）。サイバー攻撃から守るべきITシステムの開発標準やアプリケーションセキュリティの標準等も未策定であり、進んでいるIT企業は独自にセキュリティ基準を設けてシステムを実装している状況である。総じて、カンボジア政府が政府機関や民間企業に対して明確なサイバーセキュリティの指針や標準を提示できていないため、技術者の育成やサイバーセキュリティ対策の確保が不十分であるという課題がある。

カンボジアではサイバーセキュリティ以前に、特に地方部ではそもそも電力が安定しておらず、インターネット環境が非常に不安定である。システムをクラウドに配備しても、インターネットが切れてしまうことが多い。そのため、回線が切れても業務が継続でき、データの整合性を保つ仕組みが必要とされている。そのような脆弱なインターネット接続環境では、インターネット上のサイバー空間の信頼性を高めようとする意識は非常に低い。

こうした中、カンボジア政府は我が国に対して、政府職員の能力向上を通じたサイバーセキュリティの強化に向けた技術協力プロジェクトの実施を要請し、2022 年 9 月に JICA は調査団を現地に派遣し、新規プロジェクトの立ち上げに向けた詳細計画策定調査を実施した。

1-2　本調査の目的

上記のカンボジア政府からの要請を踏まえ、新規プロジェクトの立ち上げに向けた本詳細計画策定調査を実施した。調査の目的は以下のとおり。

- 要請背景、サイバーセキュリティの現状と課題、関係機関の組織構造、体制、能力等を確認し、本プロジェクトの実施体制を検討するための情報を収集する
- 協力の枠組（上位目標、プロジェクト目標、成果、指標、活動、協力期間、実施体制、投入等）について確認・協議する
- 本格協力の実施方法、留意事項等について確認し、本プロジェクト実施に関する合意文書（M/M: Minutes of Meeting）を締結する

1-3　調査団構成

調査団の構成は

表 1－1　のとおり。

表 1－1　調査団員の構成及び調査期間

担当事項	氏名	所属、職位	現地調査期間
総括・技術団員	山崎　大人	JICA 国際協力専門員	2022 年 9 月 25 日～10 月 6 日
調査企画	中島　由希子	JICA STI・DX 室	2022 年 9 月 25 日～10 月 6 日
評価団員	中村　祐美子	合同会社適材適所　コンサルタント	2022 年 9 月 21 日～10 月 5 日

1-4　調査団日程

2022年9月21日から10月6日の日程で調査を実施した。調査の詳細日程は添付資料1のとおり。

1-5　主要面談者

調査期間中、MPTC内ICTセキュリティ局、経済財務省（Ministry of Economy and Finance：MEF）、内務省（Ministry of Interior：MOI）、民間研修実施会社、CIIオペレーター等の関係者へのインタビュー調

査を実施した。主要面談者の詳細は添付資料2、面談内容の詳細は添付資料3、収集情報については、添付資料4を参照されたい。

1-6　協議概要及び合意事項

1-6-1　要請内容の確認

2016 年度当初の先方の要請内容と本調査後の本プロジェクトの構成は、以下の表 1-2 のとおりである。大枠の構成に変更はないが、本調査でカウンターパート（以下、「C/P」という。）である ICT セキュリティ局の体制が想定よりも小規模であること、他省庁への影響力が限定的であることが確認された。そのため、関係省庁、CII 事業者との連携のスコープを小さくし、普及啓発活動においてそれらの関係機関との連携を強化していく形で整理した（詳細計画策定調査結果、成果 2 の箇所）。

表 1−2　本プロジェクトの構成

	要請段階（2016 年）	詳細計画策定調査結果（2022 年）
上位目標	政府のサイバーセキュリティ能力が強化され、包摂的で安全・安心なデジタル社会経済が実現する。	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
プロジェクト目標	CamCERT において、サイバーセキュリティ関連業務（以下）の実施能力が強化される。 1. 他省庁に設置するセキュリティ・オペレーション・センター（SOC）の運営管理 2. サイバー攻撃等に対する検知・分析 3. Critical Information Infrastructure (CII)がサイバー攻撃の検知・リスクの評価を行うためのサイバー防御メカニズムの策定 4. サイバーセキュリティ関連の計画・戦略、オペレーションマニュアル等の策定	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
成果	1. 必要な国家サイバーセキュリティ政策と関連法が明確になる 2. Computer Security Incident Response Team (CSIRT)の業務実施能力が向上される 3. 他省庁や CIIs オペレーターとの連携を通じたレジリエントなサイバーセキュリティが構築される	1. CSIRT サービスの提供能力が改善される 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 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
プロジェクトサイト	プノンペン都	プノンペン都
プロジェクト期間	3 年間（2023 年 8 月～2026 年 7 月予定）	3 年 6 カ月（2023 年 6 月～2026 年 10 月予定）

出所：調査団作成先方の実施体制の確認

① 郵政通信省（Ministry of Post and Telecommunications：MPTC）

MPTC は、大臣、国務長官、国務次官の下に、6 つの総局、2 つの部局、並びに国家郵政・ICT 研究所で構成されている。今回 C/P となるのは、6 つの総局の内の ICT 総局（General Department ICT）傘下の ICT セキュリティ局である。MPTC では、ICT セキュリティ局のようなセキュリティに関する事業から、通信郵便等の事業を管轄している。本調査時点での職員数は、MPTC 全体で総勢 1,247 名であることを確認した（出所：MPTC への質問票調査の結果）。詳細は、「2-5 MPTC 組織概要 2-5-1 組織体制」を参照されたい。

② CamCERT の体制、活動内容の確認

MPTC の ICT 総局傘下の ICT セキュリティ局に帰属している。活動内容については大臣命令（PRAKAS）にて明確となっているものの、文書での定義はされていない。主な活動内容は以下のとおりである。

- 国の情報インフラ基盤と政府のサーバに関する調査、研究等
- 情報セキュリティに関する早期警告システムの開発
- ウェブサイトやメールの管理と更新
- 政府及び民間部門への DDoS 攻撃の監視
- ICT のセキュリティ強化のための新技術の研究
- 多国間・地域間連携
- 国家セキュリティ・オペレーション・センターの管理
- 月次、四半期、半年及び年次レポートの作成

③ 重要情報インフラ事業関係者の組織体制やニーズを確認する

ICT セキュリティ局から通信・電力・水道・銀行セクターを重要視する重要情報インフラ事業者として紹介された。具体的には以下のとおり。

- 通信：EZECOM
- 電力：Electricity of Cambodia
- 水道：Phnom Penh Water Supply Authority (PPWSA)
- 銀行：Association of Banks in Cambodia

事業規模や内容は異なるものの、どの事業者についても、政府からの統制やガイドライン等の整備が必要であると認識している。具体的には、電力セクターとして訪問した Electricity of Cambodia は、プノンペン都以外にも地方に 15 支部があるが、そもそもカンボジアは電力供給が安定していない、プノンペン都と地方での電力格差がある等、セキュリティ以前の問題があるとの声も別途聞かれた。また水道セクターである PPWSA は半官半民の事業者で、事業展開はプノンペン都のみである。IT 担当部門はあるもののサイバーセキュリティの対策チームはなく、セキュリティへの認識が薄いことが分かっている。詳細は、「2-6 関係機関・団体・企業への訪問結果 2-6-2 民間事業者及びその他の関係機関」を参照されたい。

④ 関係省庁の検討・特定、関係省庁が期待する事業内容の確認

ICTセキュリティ局内の5課（課長）に対するインタビューを行い、各課の業務体制及び業務内容について確認するとともに、経済財務省（MEF）、内務省（MOI）などの関係省庁関係者との面談を通じ、所掌業務の確認、サイバーセキュリティ対策の現状と課題等を確認した。詳細は「2-5 MPTC の組織概要　2-5-2 各部局の業務内容」を参照されたい。

1-6-2　現地・第三国リソース活用の可能性

過去に JICA が実施したベトナム国「サイバーセキュリティに関する能力向上プロジェクト」においては、コストを低く抑え、契約までの時間も短くすることが可能な現地リソースを活用することが教訓として挙げられている。現地リソースを活用することができれば、現地の公用語によりコミュニ

ケーションが円滑に進む可能性も高まる。ほかにも、日本国内及び現地において、サイバーセキュリティに関する活動のリソースが限定的であることから、第三国リソースや国際電気通信連合（International Telecommunication Union）（以下、「ITU」という。）、Forum of Incident Response and Security Teams（FIRST）、Asia Pacific Computer Emergency Response Team（APCERT）、Asia-Pacific Network Information Centre（APNIC）等の国際機関の協力を仰ぐことも一案として提言されている。これらの教訓を踏まえ、本調査では以下のような現地及び第三国リソースを活用する可能性を検討した。

表 1−3　現地・第三国のリソース候補

リソース	提供元	想定する協力内容案
現地	現地研修企業	国際標準レベルの商用研修の実施（EC-Council, CompTIA, Cisco 等）
	現地 IT 企業 （日系企業含む）	供与機材の調達 IT／セキュリティコンサルティングサービスの提供
第三国	タイ AJCCBC（ASEAN-Japan Cybersecurity Capacity Building Center）技術協力 （2023 年度より実施）	集合技術研修の実施 現地フォローアップ活動の提供
	インドネシア 技術協力 （2019 年～2024 年）	第三国研修の実施
	ITU	GCI の理解促進ワークショップの実施 サイバー演習の実施
	UK オックスフォード大学	国家としてのサイバーセキュリティ成熟度のアセスメント実施

1-6-3 外務省無償資金協力による SOC[1]機材の導入について

本調査時点において、外務省の無償資金協力によるサイバーセキュリティに係る機材供与が計画されている。これらの機材供与により、サイバー攻撃の兆候に対する早期段階での検知・分析・通知を政府横断的に行う GSOC（Government Security Operation Center）の機能を担うことが期待されている CamCERT のセキュリティインシデント対応能力の向上を目指している。

機材の供与先は本プロジェクトの C/P と同じ ICT セキュリティ局であり、具体的な開始時期は未定であるが、本プロジェクト期間中に供与が開始される見込みである。そうなれば、一定期間、MPTC の CamCERT を対象に無償資金協力と本プロジェクト活動が同時に並行して行われることになるため、本調査期間中の MPTC 側との協議において、案件のダブルアサインで一部の C/P に短期間に高負荷がかからないよう内部での案件協調の徹底を要請した。本プロジェクトでは、成果 1 の活動において、上記供与予定機材も含めた SOC の標準運用手順書（以下、「SOP」という。）の策定や技術研修の実施を計画し、無償資金協力事業で供与された機材の有効活用を促していくとともに適切かつ持続的な運営維持管理能力の向上を図っていく。

1-6-4　カンボジアへの長期研修

本プロジェクトのスコープ外であるが、カンボジアは「ICTによる社会課題解決（サイバーセキュリティ）」（2023年度）の対象国（1名）となっている。本調査期間を通して、ICTセキュリティ局へ候補生の打診をお願いした。人員の関係から、ICTセキュリティ局だけでは候補生が見つからないことも加味し、MPTCまた関係機関への周知も今後検討することをICTセキュリティ局と確認した。

[1] SOC：Security Operation Centre、通称 SOC。ネットワーク・モニタリング設備のことを指す。

1-6-5　ジェンダー配慮について

ジェンダー配慮に関する記載は、カンボジア政府が定める国家戦略開発計画（2014-2018）において確認される。同計画の制定によりジェンダーの主流化の促進に向けた具体的な計画が公表され、2014 年以降、28 省庁・機関でジェンダー主流化に向けた取組みが試行されてきた。加えて、経済面における女性のエンパワーメント、女性や女児、脆弱な層に対する法的保護、公的セクターで働く女性、ジェンダーと健康、社会道徳、女性の価値、女性を含むクメール人家族の推進と教育等への課題にも取り組みが広げられている。特に公共セクターでは、公共サービス省の職員採用ガイドライン[2]や女性の定年年齢の引き上げを定めた Loyal Decree[3]が制定され、その結果、公的機関での女性の採用数は、2012 年の 35%から 2017 年には 41%まで増加したとの報告が挙げられている。

一方、サイバーセキュリティ及び ICT 分野においては、女性起用の目標値は定めていないものの、上記の計画に基づき、近年ジェンダーを考慮した職員の採用促進が図られている[4]。本調査実施時点（2022 年 10 月）で MPTC では 1,247 名の職員が配置されており、男女比は 7 対 3 となっている。ICT セキュリティ局については、女性は 1 名と極めて少ない状況である。その背景には、サイバーセキュリティを含む IT 分野はもともと人材の層が薄く、女性の技術者の割合は皆無に等しいことが要因として考えられる。

本プロジェクトにおいても、カンボジア政府の政策・計画との足並みを揃えて活動を進めていくが、プロジェクト活動に女性職員の参画を求める事は現実的とはいえず、現実的かつ実効性の高さを重視し、協力期間内で対応しうる内容及びレベルで活動を進めていくことで合意した。具体的には、上記の政府内での動きや MPTC 内部の状況を踏まえた上で、成果 2 で行う「市民向けの普及啓発活動」において「女性や社会的な脆弱層」を活動の対象として含めていく。

1-6-6　その他ドナーをはじめ関連活動との調整・連携について確認する

カンボジアに対しては、複数の課題別研修、タイの AJCCBC、シンガポール、ITU 支援等様々な機関が様々なスキームでサイバーセキュリティに関する支援を実施している（ただし、継続的なプロジェクトの実施は確認されなかった）。本プロジェクトの対象組織の人数が多くないことから、同一職員が複数の研修に参加することが想定される。

こうした点を踏まえ、プロジェクト開始後は、長期専門家を中心に本プロジェクト以外の支援メニューの全体像の把握に努め、研修科目の重複をできるだけ避ける形で効率的に必要な研修科目が網羅されるよう事業を運営していく。具体的には、プロジェクトの活動計画（Plan of Operation：PO）に基づく月例進捗会議の場で、他事業による研修や支援の状況を把握し、研修日程等を調整する。

[2] 同ガイドラインでは、女性公務員の採用数を 20%から 50%に引き上げるよう定められている（出所：カンボジア政府（2019）「国家戦略開発計画（2019-2023）」）。
[3] 同 Decree では、女性公務員の定年年齢を 60 歳に引き上げることが定められている（出所：同上）。
[4] ICT セキュリティ局へのヒアリング調査の結果（2022 年 9 月）

第2章プロジェクト実施の背景

2-1　カンボジアの基本情報

カンボジアは、正式名称はカンボジア王国であり、東南アジアのインドシナ半島に位置する立憲君主制の国である。西にタイ王国、北にラオス人民民主共和国、東にベトナム社会主義共和国と接している。国の面積は 181,035 km2[5]、人口は、1,694 万人[6]、人口の 90%がカンボジア人（クメール人）であり、一部の少数民族を除き大半が仏教徒である。19 世紀末フランス保護領「カンボジア王国」となったのち大戦を経て、1953 年にカンボジア王国として独立した。1975 年から 1979 年に全土を実効支配したクメール・ルージュ政権・民主カンボジア（ポルポト首班）時代に、飢餓と処刑で 100 万もしくは200万人もの人々が死亡したとされている。1979年からは10年にも及ぶ内戦となるが、1991年に和平協定が署名され、1993 年には新生カンボジア王国が誕生した。政治は議院内閣制であり、首相の下に閣僚評議会及び 28 省 1 庁となっている。現在はフン・セン首相率いる人民党が 1985 年より政権を維持しているものの、2010 年代には野党が躍進している。2013 年 9 月には、「第 3 次四辺形戦略」にて諸改革を実施。重点的開発分野として、4 分野、農業セクター、民間セクター、インフラ整備、人材育成が挙げられた。経済は、1 人当たりの GDP は 1,662 ドル、GDP 構成比は、農業、建設業、製造業となっている[7]。外務省の国別データ集によると、2020 年の 1 人あたりの GNI は 1,490 ドル、経済成長率は-3.1%で低中所得国とみなされている。日本からの援助は、円借款、無償資金協力、技術協力の 3 形態で実施され、累計額では無償資金協力の金額が大きいものの、近年は円借款事業の割合が多くなっている。主要国の経済協力実績は 2018 年まで日本が 1 位であったが、2019 年はフランスが 1 位、日本が 2 位である。

2-2　カンボジアのサイバーセキュリティに関する課題

カンボジアにおいては、政府機関や民間企業に対して明確なサイバーセキュリティの指針や標準を提示できておらず、それが技術者の育成やサイバーセキュリティ対策の遅れを招く一因となっている。指針や技術標準を公開するためには、まず MPTC に法的な根拠のある権限が付与される必要がある[8]（サイバーセキュリティ法（Law on Cybersecurity）案を策定中）。また、CII を中心としたの組織のサイバーセキュリティの確保のためには、政策の実施能力を含めた MPTC 職員の技術力向上が不可欠である。

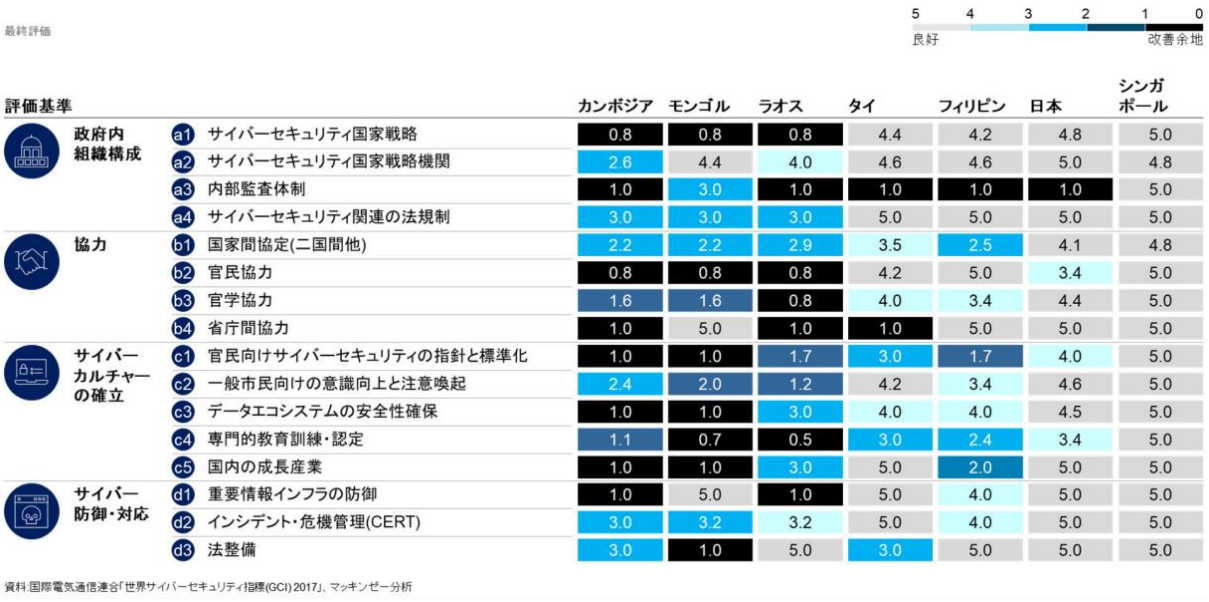
JICA が 2021 年度に実施した「インクルーシブで安全なデジタル経済の推進に係る情報収集･確認調査」においても、ITU の世界サイバーセキュリティ指数（Global Cybersecurity Index）（以下、「GCI」という。） 等、外部調査機関の指標を組み合わせた診断フレームワークに基づき 4 分野 12 項目について政府の成熟度診断を評価した結果、カンボジアは成熟度が低いグループであることがわかっている。

[5] https://www.mofa.go.jp/mofaj/area/cambodia/data.html#section1

[6] https://data.worldbank.org/country/cambodia

[7] https://www.globalnote.jp/post-2422.html?cat_no=101#posi

[8] 本調査時点で、「サイバーセキュリティ法案」が策定中であった。



評価基準			カンボジア	モンゴル	ラオス	タイ	フィリピン	日本	シンガポール
政府内組織構成	a1	サイバーセキュリティ国家戦略	0.8	0.8	0.8	4.4	4.2	4.8	5.0
	a2	サイバーセキュリティ国家戦略機関	2.6	4.4	4.0	4.6	4.6	5.0	4.8
	a3	内部監査体制	1.0	3.0	1.0	1.0	1.0	1.0	5.0
	a4	サイバーセキュリティ関連の法規制	3.0	3.0	3.0	5.0	5.0	5.0	5.0
協力	b1	国家間協定(二国間他)	2.2	2.2	2.9	3.5	2.5	4.1	4.8
	b2	官民協力	0.8	0.8	0.8	4.2	5.0	3.4	5.0
	b3	官学協力	1.6	1.6	0.8	4.0	3.4	4.4	5.0
	b4	省庁間協力	1.0	5.0	1.0	1.0	5.0	5.0	5.0
サイバーカルチャーの確立	c1	官民向けサイバーセキュリティの指針と標準化	1.0	1.0	1.7	3.0	1.7	4.0	5.0
	c2	一般市民向けの意識向上と注意喚起	2.4	2.0	1.2	4.2	3.4	4.6	5.0
	c3	データエコシステムの安全性確保	1.0	1.0	3.0	4.0	4.0	4.5	5.0
	c4	専門的教育訓練・認定	1.1	0.7	0.5	3.0	2.4	3.4	5.0
	c5	国内の成長産業	1.0	1.0	3.0	5.0	2.0	5.0	5.0
サイバー防御・対応	d1	重要情報インフラの防御	1.0	5.0	1.0	5.0	4.0	5.0	5.0
	d2	インシデント・危機管理(CERT)	3.0	3.2	3.2	5.0	4.0	5.0	5.0
	d3	法整備	3.0	1.0	5.0	3.0	5.0	5.0	5.0

資料:国際電気通信連合「世界サイバーセキュリティ指標(GCI) 2017」、マッキンゼー分析

図 2−1　カンボジアのサイバーセキュリティの成熟度

出所：JICA（2022）、インクルーシブで安全なデジタル経済の推進に係る情報収集･確認調査

本調査期間中に、政府としての成熟度に加え、重要な情報資産を大量に所有する通信セクターと金融セクターの民間企業に対して 2 成熟度診断を実施した結果、政府の成熟度診断結果と同様にカンボジアの民間企業は世界平均から大きく劣る成熟度と診断された。これらの診断結果から、政府組織だけでなく民間においてもサイバーセキュリティ人材が不足していることが明らかとなり、人材育成を支援する組織や政府機関の成熟度の低さも推計される。加えて、政府及び民間のサイバーセキュリティの取り組み状況から、12 の評価項目の中で最も重要度が高い a1.「サイバーセキュリティ国家戦略」、a2.「サイバーセキュリティ国家戦略機関」は十分に機能していないことがわかった。また、b1.「国家間協定(二国間他)」.b2.「官民協力」.b3.「官学協力」.c2.「一般市民向けの意識向上と注意喚起」.c4.「専門的教育訓練・認定」.d2.「インシデント・危機管理(CERT)」も同様に重要度が高く、早期の支援対象として推奨される。同調査において、MPTC 及び CamCERT へのヒアリングを実施した結果、上流戦略、人材育成、CamCERT 支援の 3 つの領域において特に課題を抱えており、中でも CamCERT の直接的な支援に対するニーズが高いことが判明した。

国際電気通信連合（ITU）が発行している Global Cybersecurity Index（GCI）2020[9]（以下、「CGI2020」という。）において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）となっている。ただし、カンボジアは GCI の調査へは正式に回答がなく、GCI2020 の結果はオンラインの公開情報をもとに ITU が推察した結果である。過去に GCI におけるカンボジアの順位は、GCI2018 では 193 か国中 131 位（アジア太平洋 38 か国中 27 位）、GCI2017 では 193 か国中 91 位（アジア太平洋 38 か国中 20 位）となっている。GCI の 5 つの基準のうち、法・規制がわずかに整備されているのみで、技術力、戦略・組織体制、能力構築、組織間連携は特に低いレベルとなっている。一部 Growing ステージに入りつつある要素もあるが、5 要素すべてが Initial ステージであり、カンボジアのサイバーセ

[9] ITU Publications

キュリティは全般的に低い成熟度となっている（上述の情報収集・確認調査の結果とも整合）。なお、ステージの定義は、本調査時点で策定中の「サイバーセキュリティ・クラスター戦略」によるものであり、5 要素の成熟度によって「Initial」「Growing」「Networking」「Self-sustaining」の 4 段階に分けている。

表 2−1　GCI におけるカンボジアのスコア

項目（最高スコア）	スコア	ステージ
総合（100）	19.12	Ranking 132/194
法・規制（20）	7.38	Initial
技術力（20）	2.50	Initial ～ Growing
戦略・組織体制（20）	1.66	Initial ～ Growing
能力構築（20）	3.29	Initial
組織間連携（20）	4.26	Initial

出所：GCI2020

2-3　開発計画

2-3-1　第 4 次四辺形戦略

カンボジアでは、2018 年 7 月に行われた総選挙後に同国の国家開発計画として「第 4 次四辺形戦略」（Rectangular Strategy Phase 4）が発表された。同戦略の中心課題には、「ガバナンス改革の加速」が挙げられており、それを支える 4 つの戦略の柱として、1) 人的資源開発、2) 経済の多様化、3) 民間セクター開発と雇用創出、4) 包括的・持続的な開発が示されている。第 4 次戦略では、第 3 次四辺形戦略の評価の結果導出された次の 2 点を踏まえ、4 つの目標（ゴール）が掲げられ、その下に、1) 戦略の核、2) 戦略の実施のために求められる環境、3) 四辺形戦略の柱、4) 各戦略に対する着眼点が設定されている。

表 2−2　第 3 次四辺形戦略の評価結果から導出されたポイント

第 3 次戦略の実施により導出されたポイント	
①	平和、政治的安定、安全、社会秩序の強化、法治国家、人権と尊厳、自由な複数政党制民主主義の促進、人々の生活と福祉を向上させる具体策の実施、特に統治と社会正義における「効率」の問題の解決、公共サービスの質の向上への対応
②	2030 年までに上位中所得国、2050 年までに高所得国になるという目標の達成に向け、高く持続可能な経済成長を確保するための新しいリソースの探索

表 2−3　第 4 次四辺形戦略における 4 つのゴール

第 4 次四辺形戦略の目的（ゴール）	
①	インフレの抑制、リエルの為替相場の安定、国債管理を通じたマクロ経済の安定化を図りつつ成長基盤を拡大していくための新しい成長資源の多様化や競争力の向上のための年間経済成長 7 %に維持する
②	技能訓練、雇用市場に関する情報の提供、労働条件の改善、国内外のビジネスと投資の促進を通じて、カンボジア国民、特に若者のために、質と量の両面でより多くの雇用を創出する
③	貧困削減目標 10%以下を達成し、市場参加の強化、社会保護政策の実施、質の高い公共サービスの提供による日常生活の負担軽減、社会的格差の縮小により貧困を削減する
④	国民へのサービス向上とビジネス・投資環境の改善を目的とした公共サービス提供の有効性と効率性を確保するため、国と地方の両レベルで、公共機関の能力とガバナンスをさらに強化する

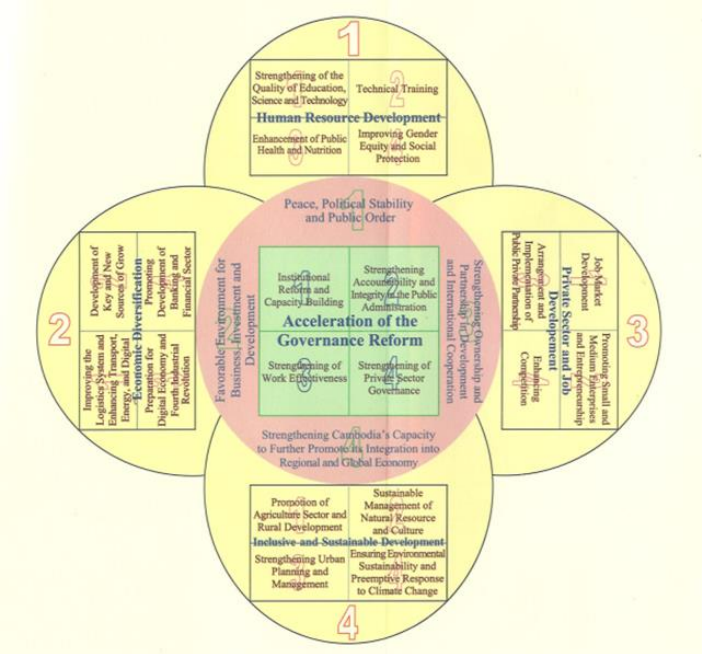


図 2−2　第 4 次四辺形戦略

出所：Royal Government of Cambodia (2018), Rectangular Strategy IV

表 2−4　第 4 次四辺形戦略の全体像

1)	**戦略の核**	
	ガバナンス改革の加速化	①　制度改革及び能力開発
		②　クリーンな行政
		③　業務の効率性の強化
		④　民間セクターのガバナンス強化
2)	**戦略の実施のために求められる環境**	
	①　平和、政治、公序	
	②　ビジネス・投資、開発のための良好な環境	
	③　主体性の強化及び開発パートナーとのパートナーシップの強化	
	④　地域及びグローバル経済への更なる統合促進のためのカンボジアの能力強化	
3)	**戦略の柱及び 4) 各戦略の着眼点**	
	①　人的資源開発	a. 教育・科学技術の質的向上、b. 職業訓練、c. 公的医療及び栄養改善、d. 男女平等や社会的保護の強化
	②　経済の多様化	a. 物流・輸送システムの改善と向上、b. 重要かつ新しい経済成長源の開発、c. デジタル経済や産業革命 4.0 への準備、d. 財政・金融セクター開発の促進
	③　民間セクターの開発と雇用	a. 雇用市場の発展、b. 中小企業及び起業の促進、c. 官民パートナーシップ、d. 競争力の強化
	④　包括的・持続的開発	a. 農業・農村開発の促進、b. 自然・文化財の持続的な管理の強化、c. 都市化の管理強化、d. 環境の持続性と気候変動への準備・対応

2-3-1 国家戦略開発計画（2019 年～2023 年）

国家戦略開発計画（National Strategic Development Plan）（2019 年～2023 年）は、前計画（2014 年～2018 年）の結果及び第 4 次四辺形戦略に基づき策定された国家開発計画であり、上記の 4 つの戦略の柱に対する具体的な行動計画や目標値が設定されている。これら 4 つの戦略の柱のうち「②経済の多様化」において、ICT セクターに対する活動の中長期的な方向性が示されている。

表 2−5　国家戦略開発計画（2018-2023）における ICT 分野の取組みに関する記載

4. 経済の多様化　（ICT 該当箇所のみ抜粋）		
	4.2 重要かつ新たな成長源の開拓	• 政策的枠組み及び規制の策定を継続 • 研究及び技術革新 • 研修能力を強化するための民間企業や大学との協力 • より良いカリキュラムの開発／e-learning 研修の推進 • 海外、国際的な研究者等の登用
	4.3 デジタル経済及び第４次産業革命への準備	（7 つの具体的取組が示されており、うち以下が該当） • デジタル政府、情報セキュリティ戦略、電子商取引法、サイバー犯罪法の実施、同分野の成長とリスク防止に向けた法律や関連規制の改正等デジタル経済の発展を支える法的枠組みの確立と推進

2-4　サイバーセキュリティに関連する政策、制度、開発計画

2-4-1　デジタル経済・社会政策フレームワーク（2021 年～2035 年）

近年、カンボジアの ICT システムは目覚しい発展を遂げているものの、同セクターをサポートするインフラが極めて限られていること、信頼性やコンフィデンス（自信）、知識、スキル、デジタルリーダーシップなどの面においても、デジタルセクターの変化・発展を受け入れるための体制は依然として十分とはいえない状況である。こうした状況に鑑み、カンボジア政府は、将来的なビジョンを明確に示していくために、公共及び民間の両セクターにおけるニーズ、潜在力、資源、能力に基づき、将来的なデジタル変革プロセスについて検討を進めていくための枠組みとして「デジタル経済・社会政策フレームワーク 2021 年～2035 年」を作成した。その中で、デジタル経済・社会がもたらす便益を最大化するとともに、負の影響を吸収し最小化する」というコンセプトのもと、各要素に対応した政策手段を準備し、経済・社会的側面を考慮しながら、負の影響を確実に低減するとともに、デジタル経済・社会がもたらす便益を最小化するための政策手段を準備するとしている。そのうえで、2035 年までの 15 年間で達成すべきビジョンとして「ニューノーマルの流れの中で、新たな経済成長を加速し、社会福祉を促進するため、活力あるデジタル経済・社会を構築する」を打ち立て、①デジタル基盤の構築、②デジタルの導入、③デジタル変革という 3 つ原則に沿った形で、個別の原則に対応する施策を優先しつつ、全ての施策を同時に実施していくことの重要性を強調している。同枠組における重点項目は、以下に記す 2 つの基盤及び 3 つの柱から構成されている。

表 2−6　デジタル経済・社会政策フレームワーク 2021 年～2035 年における重点 5 領域

構成	概要	優先戦略	備考
2 つの基盤	デジタルトランスフォーメーションを可能にするインフラの整備	デジタルコネクティビティ フィンテック・インフラとデジタル決済システム 物流・最終拠点からエンドユーザーへの物流サービス	44 の政策施策
	デジタルシステムの信頼性と信用性の構築	デジタルフレームワーク サイバーセキュリティ管理	
3 つの柱	デジタル市民の構築	デジタルリーダーシップ デジタル人材の確保 デジタル市民	82 の政策施策
	デジタル政府の構築	デジタル政府・公共サービス デジタルパフォーマンス促進の鍵 データに基づく政府	
	デジタルビジネスの実現	企業デジタル改革 起業家精神とスタートアップエコシステム デジタルバリューチェーン	

出所：デジタル経済・社会政策フレームワーク 2021 年～2035 年

このほかも、デジタルセクターにおけるインクルーシブな参加を促していくための施策として、労働構造や税制の変更、政府支出の増加、文化・伝統、コミュニケーションへのインパクト、個人情報の紛失やサイバー犯罪に対する具体的な 13 の施策も検討している。

カンボジア政府は、デジタル変革の実現には、デジタルプラットフォームとデータベースの構築に向けた準備（具体的にはデータベースを相互に活用していくための準備）が不可欠であるとし、政策の実施促進やモニタリングの実施メカニズムの一つとして、常設の「国家デジタル経済・社会評議会（National Digital Economy and Society Council）」の設立を決定した。この国家評議会の下には、「デジタル経済・ビジネス委員会（Digital Economy and Business Committee）」、「デジタル政府委員会（Digital Government Committee：DGC）、「デジタルセキュリティ委員会（Digital Security Committee：DSC）」の 3 つの委員会が設置され、技術的な作業を担当する。

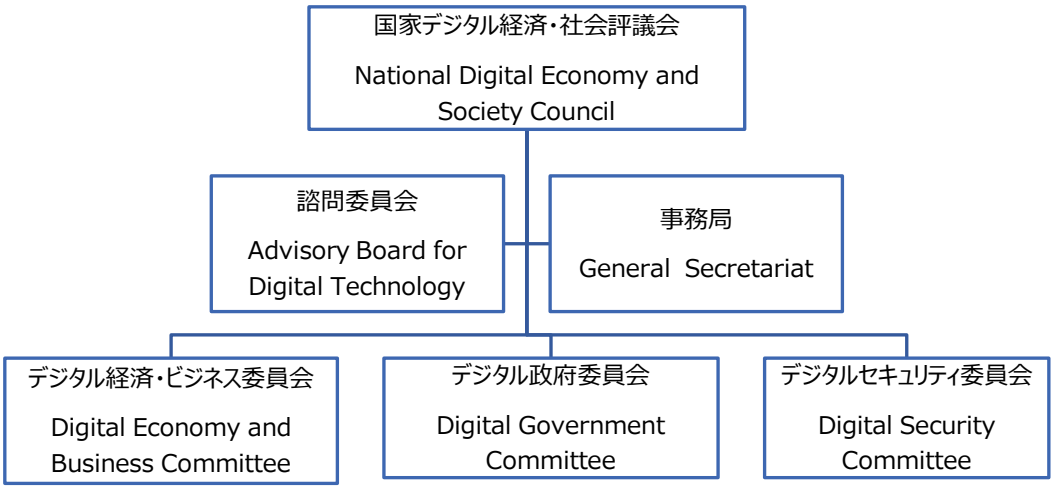


図 2−3　国家デジタル経済・社会評議会の体制図

出所：デジタル経済・社会政策フレームワーク 2021 年～2035 年

2-4-2　デジタル政府政策（2022 年～2035 年）

カンボジア政府は、包括的なデジタル経済・社会を発展させるために、透明で信頼できる方法でガバナンスシステムの近代化及び改革のためのエコシステムでもあるデジタルインフラと技術を活用し、スマート政府を構築していくことを目的に「デジタル政府政策 2022 年～2035 年」が策定した。同政策の制定により、デジタル政府を確立し、より良い公共サービスの提供を通じて、市民の生活の質を向上させ、信頼を築くことが期待されている。そのための戦略として 4 つの戦略目標と 10 の具体的戦略が設定されている。

表 2−7　政策目標及び具体的施策

戦略目標	具体的戦略・施策
1. デジタルガバメントインフラの整備・推進	1) デジタルコネクティビティインフラの構築と改善 2) 公共サービスのためのデジタル決済システムのインフラを構築・改善 3) デジタルセキュリティインフラの構築と強化 4) 郵便サービスのインフラ整備
2. デジタルガバナンスの構築／デジタル公共サービスを創出	5) 政策の策定と改善、法的枠組みと関連規則の作成と改善、デジタル政府標準など、デジタル政府ガバナンスの組織化 6) 政府間（G2G）、市民間（G4C）、企業間（G2B）の公共サービスの改善、政府と公共サービスをデジタルへの変革
3. デジタル人的資源開発・革新	7) デジタル人材の育成 8) デジタル研究・イノベーションの推進
4.　官民連携・パートナーシップの推進	9) デジタル技術企業とのコラボレーションを組織 10) デジタルスタートアップの推進

出所：デジタル政府政策 2021 年～2035 年

表 2−8　デジタル政府政策の概要

ビジョン	より良い公共サービスの提供を通じて国民の生活の質の改善や信頼を構築していくためのデジタル政府の確立				
ゴール	包括的なデジタル経済や社会を確立していくために、透明で信頼できる方法でガバナンスシステムを近代化・改革していくためのエコシステムとして、デジタルインフラや技術を活用したスマート政府を構築する				
政策目標	1. デジタル政府インフラストラクチャーの整備・推進		2. デジタルガバナンスの構築／デジタル公共サービスを創出	3. デジタル人的資源開発・革新	4. 官民連携・パートナーシップの推進
戦略	デジタル接続インフラ	公共サービスの電子支払いシステムのためのインフラ	デジタル政府のガバナンス	デジタル人的資源開発	デジタルテクノロジー企業との協力
	デジタルセキュリティインフラ	郵便サービスインフラ	デジタル政府と公共サービスの変革	デジタルリサーチ・革新	デジタルスタートアップ

出所：デジタル政府政策 2022 年～2035 年

なお、本調査時点で「サイバーセキュリティ法」及び「デジタル開発 2030 に関する国家政策」（National Policy on Digital Development 2030）の作成作業が進められている。

2-5　MPTC の組織概要

2-5-1　組織体制

MPTC は、大臣、国務長官、国務次官の下に、6 つの総局、2 つの部局、並びに国家郵政・ICT 研究所で構成されており、MPTC の傘下には通信規制当局（Telecommunication Regulatory of Cambodia）や財務統制ユニット、カンボジア郵便（Cambodia Post）、テレコム・カンボジア、カンボジアデジタル技術アカデミー（Cambodia Academy of Digital Technology）（以下、「CADT」という。）が設置されている[10]。なお、MPTC では 2019 年に組織再編を行い、それに伴い、2020 年には National Institute of Posts,

[10] MPTC's Structure – រចនាសម្ព័ន្ធសង្ខេប និងមុខងារចាស់

Telecommunications & ICT が CADT に吸収されたものの[11]、その他の部局については、特段大きな体制変更は生じていない。

2-5-2　業務内容

(1) サイバーセキュリティ業務

MPTC では、ICT セキュリティ局がサイバーセキュリティ担当部局として位置づけられており、2007 年に設置された CamCERT がインシデント対応の専属部署となっている。組織体制に係る大臣令（PRAKAS）の中で ICT セキュリティ局の役割や業務内容に関する定めはあるが（下表）、内部の詳細業務については、2019 年に別途 ICT セキュリティ局局長名で定められている。TOR の詳細については、添付資料 5 を参照されたい。

(a) ICT セキュリティ局

権限
現状では関係省庁からの要請に応じた技術的な助言・支援の提供
役割
• 関連法規制、戦略の策定 • CII の組織、サイバーセキュリティサービスプロバイダー（CSP）、その他の関係者間の連携調整、支援・促進 • 外国の国家サイバーセキュリティ機関や国際機関との調整・協力 • 官民におけるサイバーセキュリティ実践のパフォーマンスの監視・調査・評価 • サイバーセキュリティランドスケープの発行（毎年）

(b) Office of CamCERT

概要
• 現状では関係省庁からの要請に応じた技術的な助言・支援の提供に留まっており、インシデントについての報告の法的義務は課していない。 • 主な役割 ➢ 国家情報インフラ基盤と政府サーバへの攻撃に関する調査・研究・報告 ➢ ICT セキュリティに関する早期警戒システムの開発 ➢ CamCERT の Web サイトと電子メール システムの管理と更新 ➢ 政府のサーバにおける攻撃トラフィックの監視と情報収集 ➢ セキュリティ問題提起のための新技術の研究 ➢ 地域的およびグローバルな国際的なサイバーセキュリティ機関との調整と協力 ➢ 国家サイバーセキュリティ センターの管理

(c) Office of Norm, Control and Risk

概要
• ICT セキュリティポリシーやデジタル活動に関する新しいルールを策定することを目指している。 • Information Security Management System （ISMS）等のセキュリティ標準やガイドラインの翻訳（英語⇒クメール語）を通して研究している。クメール語に対応する専門用語がない場合は、英語の専門用語を流用。 これまで約 24 のセキュリティポリシー等を翻訳した。データ保護やネットワークにおけるインシデント検知に関する包括的なドキュメントも研究した。セキュリティガイドラインについては、オーストラリアやイギリスなど他国の国家安全保障機関のものを参照している。 • ポリシーに関する提案を検討・作成する際には ICT 総局内の他局にコメントを求め、検討の質を高め、より実用的なものにしている。ポリシーとして策定する場合は、組織に採用されるように精緻化していくために上層部のワーキンググループのメンバーが内容を審査する（Office Head も同ワーキンググループのメンバー）。同ワーキンググループでは個人情報保護に関するポリシーについても審査している。

(d) Office of Public Key Infrastructure (PKI)

[11] 出所：CADT ホームページ

概要
• 韓国、ASEAN で制定された PKI ガイドラインを研究している。PKI に関連して関係する国際標準や公開鍵暗号方式に関する技術標準も研究。 • 標準やライセンスに関する省令（PRAKAS）のドラフトを作成するためのワーキンググループに参加し、2 つの PRAKAS を起草。（政府、民間セクターの認証局モデルに関する PROKAS は MEF で承認される見込み） • PKI に関する準政令（Sub Decree）を作成するために、韓国がサポート提供。

(e) Office of Quality Assurance and Digital Forensic

概要
• 同室は脆弱性調査を所掌しており、外部からの依頼でフォレンジックも実施している（対象となるドキュメント等も提供される）。 • マルウェア解析も担当（ただし、静的分析はせず、動的分析もオンラインで実施するのみ）。結果はレポートとして提出している。 • 毎月、76 の MPTC が所掌する政府ウェブサイトの脆弱性スキャンを実施。さらに他に 20 程度のスキャン対象ウェブサイトリストがある • 2018 年には Cyber SEA Game (AJCCBC)で CTF (Capture the Flag)を担当した。

(f) Office of Administration

概要
• 同室は人員配置に関するリエゾンオフィスとして機能している。毎月、ICT 総局長及び人事部長へ人事依頼の報告を行っている。

(2) 他部局の業務内容

本調査期間中に実施した ICT セキュリティ総局 ICT セキュリティ局を除く 6 部署の業務・実施体制の概要は以下のとおり。

(a) Department of ICT Infrastructure and Video Conference

職員数
• 職員総数は 30 名。そのうちエンジニアが 15 名。（ネットワーク担当：5 名、その他の技術的業務 10 名）
概要
• 60 以上の政府組織を対象としたネットワーク・インフラを管理している • Cabinet 向けのオープンプラットフォームやビデオ化会議システムを保有している。 • E-Government 推進においては ICT セキュリティ局と協力している。 • ネットワークはルーターやスイッチ等で物理的に構成されているが将来は Software Defined Network（SDN）とすることを目指している

(b) Department of Application and Content[12]

職員数
• 28 名（うちエンジニアは 15 名）
概要
• 省内のデスクトップアプリやウェブベースのアプリケーション等のソフトウェアを開発。要素技術として、Microsoft の.NET、SQL Server、C#、あるいは Open source（My SQL, PHP, Ubuntu 等）も活用している • 国土交通省の要望で車両登録用のオンラインシステムを構築済 • 2002 年国家 ICT 開発庁のプロジェクトが実施され TIAS という活動を実施 • 他省庁からの依頼を受けて、ソフト開発を行っており、現状では、Vehicle Registration のオンライン登録などのソフトを開発。年間開発件数は 1～10 個。 • システム開発はプロトタイプで対応。他省庁の要請に基づき調整を図り一定の基準に基づき開発。 • セキュリティテストでは ICT セキュリティ局からの協力を得ているが、テストに対する基準は設けられておらずシステム開発後は機能テストのみ実施。

(c) ICT Policy Department

職員数
• 18 名
概要

[12] MPTC 内のシステム開発担当部局は、同部局の他 E-government Department がある（県事務所や他の省庁に対するシステム開発）

① 政策策定に向けた研究活動
- 上層部からの要請を受けて政策文書の起案に向けた研究活動を実施
- 近年は「e-government 政策」を策定していくための e-government に関する研究を実施
- 現在は「個人データ保護法[13]」（Personal Data Protection Law）の起草に向けた政策研究を実施

② 活動の実施促進
- 草の根資金協力事業による「地域テクノロジーセンター」のパイロット事業の実施促進支援（実施中。成功すれば全国展開の予定）。
- 他省庁を対象に Awareness 活動も実施。
- Child Online Protection（COP）に関するパイロット活動を助言委員会（Advisory Committee）の監督の下で実施中
- COP の活動基準となるガイドラインを策定準備中

(d) ICT Industry Department

職員数
- 18 名

概要
- ASEAN 諸国の民間セクターの投資促進に向けた調整
- ビジネスフォーラム（JETRO との共同開催）を開催し、日本の ICT 企業とカンボジアの企業のマッチング
- 中国企業との共同で意見交換などの実施
- Digital Cambodia を再結成・再出発に向けた検討[14]
- ポスト・コロナでのテクノロジーの活用した活動展開を検討中

(e) Department of Rural ICT

職員数
- 28 名

概要
- 地方への ICT 促進、インターネット環境の改善、インターネットセキュリティの実施促進等
- 近年は ADB 支援や他省庁との連携でプロジェクトを実施

① トンレ・サップ貧困削減及び小規模農家開発プロジェクト (TSSD)（TONLE SAP POVERTY REDUCTION AND SMALLHOLDER DEVELOPMENT PROJECT）
• ADB、国際農業開発基金 (IFAD)、フィンランド政府の支援のもと、内務省（MoI）及び民政的地方開発委員会 National Committee for Sub-National Democratic Development (NCDD) が協力し MPTC と農林水産省（Ministry of Agriculture, Fishery and Forestry（MAFF） が実施するプロジェクト。2014 年～2022 年 1 月で第 2 フェーズ完了。 • 同局は、デジタルスキルに関する研修やワークショップを実施。
② メコンランチャン連結プロジェクト（Mekong Langchang connectivity project：MLC）
同局は、農業活動の接続センターとして活動に関与
③ デジタルコミューンプロジェクト（Digital Commune Project）
• タケオ州バティ地区で実施されている当局の主要プロジェクトであり、地区内の約 4～7 つのコミューンのデジタル・カバレッジの改善、地区からコミューンレベルまでの地方自治体におけるデジタル能力構築の提供を計画。基本的にパイロット地区での実施。プロジェクトは長官、副長官が管理。 • 同局は、プロセス管理、文書化とトレーニング、運用、及び MPTC の国家レベルから地方レベルへのパートナーシップの構築を担当
④ スマートシティプロジェクト
MPTC が実施機関となるプロジェクト。プノンペン都、Sihanuak Ville、Siem Reap などの市や州が対象
⑤ Safe-App プロジェクト
• 女性省が実施するプロジェクト。脅威から女性や少女を支援することを主な目的としている。 • 同局もアプリ開発委員会のメンバーの一つ
⑥ デジタルブロックチェーン技術を利用した農業バリューチェーンにおけるアグリビジネスのリスク軽減
• 農林水産省が実施、当局も関与。

[13] 個人データ保護法は、長官（Secretary of State）を議長としたワーキンググループが設置されており、同局長はメンバーの一人となっている。現在、ドラフト作成に向けた研究・議論が進められている。個人データ保護に焦点をあてたものでありデータのローカライゼーションは対象外。

[14] 2019 に設置する予定であったが新型コロナウイルス感染症の拡大の影響を受け頓挫していた。2022 年の再稼働を検討していたが、具体的な動きは来年以降となる見込み（出所：2022 年 9 月 28 日 Department of ICT Industry 局長へのインタビュー調査結果）

(f) e-Government Department

職員数
• 22名（5〜7名増員予定）。うちエンジニアは10名程度。
概要
• 全省庁・地方政府を対象としたe-Governmentに関する普及活動（Awareness）を実施 • 政策研究・策定作業 • Co-locationシステムなどのオペレーションサービスの構築 • e-Government委員会の設立準備 • MPTC共通のシステムにおけるメールシステムを管理しており、サーバのログのフォレンジックを実施 • CADTなどのベンダーと協力してシステムを開発している

2-5-3 人員体制

2022年9月現在のMPTCの職員数は合計1,247名（男性862名、女性385名、男女比7:3）である。

表 2−9 MPTC本省の職員数

確認時	全体	男性	女性
MPTC全体	1,247名	862名	385名

出所：MPTCへの質問票調査の結果

2-5-4 職員採用・管理・育成

(1) 職員採用

カンボジアでは、政府が定める優先順位に基づき国家公務員省（Ministry of Civil Service）（以下、「MCS」という。）が各省庁への割当て人数を決定し、その決定に基づき、各省庁で採用手続きが進められる。MPTCによれば、2022年度の同省への割り当て任数は100名であり、年に1度採用試験（筆記試験と面接）を行っている。正職員の採用手続きには凡そ2カ月を要する。一方、契約職員の採用については都度必要に応じてMPTCの裁量により行われている。人事異動の頻度はさほど高くない[15]。

(2) 人材資源管理／人材育成

MPTCにおける人材資源管理は、毎年作成される年次計画によって管理されており[16]、毎年1回人事評価が行われている。評価の結果は、人事院に相当するMCSに提出され、結果に応じた昇給手続きが進められる。カンボジアの官庁では、3年に1度の昇給が一般的であるが、人事評価の結果優秀な成績を収めた職員はその限りではない[17]。

職員教育については、常設の研修はなく、ニーズに応じた独自予算による研修または、他ドナー・関係機関提供の研修を活用している。

[15] 出所：MPTCへの質問票調査及びインタビュー調査の結果（2022年9月22日）

[16] 出所：ICTセキュリティ局向け質問票調査結果

[17] 出所：ICTセキュリティ局への質問票調査・インタビュー調査の結果（2022年9月27日）

独自予算による研修については、近年人材開発政策の一環として制定された「Digital Skill Essentials」プログラムが挙げられる。同プログラムは、CADT や MPTC から講師を迎え、職員から局長を対象とした 14 の科目に対する 3 つの研修プログラムを実施している（下表）。昨年（2021 年）1 年間の受講者数は合計 568 名のであり[18]、このうち 19 名が ICT セキュリティ局の職員となっている[19]。同プログラムは、当初中央省庁職員向けの研修として開設されたが、今年度から、対象を地方自治体職員までに拡大している。MPTC 側が定めた 2022 年度の研修候補者数は 2,520 名であり、本調査実施時点（2022 年 9 月）で 900 名の職員が同プログラムに関する研修を受講済である[20]。なお、同研修は毎年定期的に実施されるものではなく、予算とタイミング、必要性に鑑み実施されている。このほか、2022 年 8 月には、MPTC 職員向けの奨学金制度が新設された[21]。

図 2−4　Digital Skill Essentials のパンフレット

表 2−10　Digital Skill Essentials の概要

項目	概要	
対象	MPTC 職員及びその他の職員	
目的	公共サービスを効率的かつ安全に提供するための職員のデジタル能力の強化	
費用	年間 350 米ドル	
研修コース概要*	①デジタルリタラシー	A101: Computer Knowledge Required A102: Essential Online Skills A103: Information Professionals A104: Privacy, Information and Records A105: Media Literacy
	②デジタルツール・管理	A201: Create a document A202: How to fish and analyse data A203: Creating Digital Content A204: Online Cooperative Software A205: Taiwan Mobile Phone Software
	③デジタル経済	A301: Research and Digital Services A302: Communication and Information Technology For development A303: Digital Development A304: Post office matters of the Ministry of Post and Telecommunications
講師	MPTC 交換及び CADT 講師	

[18] 出所：Digital Skill Essentials 2021 年研修概要
同サイトによれば、2022 年 1 月にも MPTC の職員 523 名に対して同様の研修を実施している。
[19] 同上
[20] 出所：CADT へのヒアリング調査結果（2022 年 9 月 28 日）
[21] 応募締め切りは 2022 年 9 月末日で設定されていた。

*研修受講登録前にPC能力テストあり

出所：Digital Skill Essentials及びCADTへのヒアリング調査結果を基に調査団作成

上記のMPTC独自の研修に加え、AJCCBCやシンガポールをはじめとするドナー（国際機関）の支援による研修機会も設けられている。詳細は、「2-8　他ドナー支援の概要」を参照されたい。

2-5-5　財務状況

MPTCの2019年から2021年度までの過去3年間の政府承認予算は以下のとおりである。

表 2－11　MPTCへの予算配賦状況（2019年～2021年）

年次	MPTCの配賦予算（Million KHR）	日本円相当額*
2019年度	73,963.9	25.3億円
2020年度	89,594.6	30.6億円
2021年度	77,655.0	26.6億円

出所：ICTセキュリティ局への質問票調査の結果　*2022年度JICA換金レート（9月：KHL1＝0.034260円）で計算

カンボジアでは、経済財務省（MEF）が設定する予算の上限に基づく予算計画を立て、申請・承認手続きが進められるが、各年度の歳出の詳細については、年度毎に経済財務省（MEF）が財務文書を確認し、国会で最終承認された後に確定する。その手続きに約3年を要することから、本調査時点で当該年度の歳出に関する情報入手は困難であった。

2-5-6　省内決裁手続・プロセス

カンボジアでは、法・規定等の文書に関し次のような階層が設けられており、作成する文書の階層によって承認手続きは異なってくる。例えば、サイバーセキュリティ法の場合、起草後、省内マネジメントレベルで内容が精査の後、パブリックヒアリング（公聴会）を開き一般市民からの意見を聴取し、大臣の承認の後、政府の所定の手続きへと移っていく。政府内での手続きには、本年に設立されたデジタル政府委員会（DGC）などへの提出が求められ、そこで一定期間をかけて審議された後、首相へと提出される[22]。

表 2－12　カンボジアにおける公文書の階層

文書の階層	手続き
Law and Regulation 法規定	所管省庁→内閣（Cabinet）→国会（議会）→　憲法制定会議→国王承認
Sub-decree 政令	所管省庁→関係省庁との協議→大臣の上級議長の承認
PRAKAS 省令	大臣承認
Strategies 政策	所管省庁→首相への提出・承認
Guideline 運用指針	大臣承認

出所：ICTセキュリティ局へのヒアリング調査結果を基に調査団が作成

[22] 出所：ICTセキュリティ局へのインタビュー結果（2022年9月27日）

一般的には上記の流れであるが、CSIRT の設立などサイバーセキュリティに関する文書については、首相の下に設置された国家デジタル経済・社会評議会（General Secretariat of the National Digital Economy and Society Council）等での審議が求められる可能性が高い。

2-6　関係機関・団体・企業への訪問結果

2-6-1　関係省庁

本来国家 CERT は、普及啓発、政府間連携、国際連携を一元的にリードする存在である。将来的に、CamCERT が国家 CERT として機能していくために、本調査では、関係省庁へ訪問しセキュリティ対策の状況や体制を確認した。訪問した先は、内務省（MOI）のサイバー犯罪局と IT 局、経済財務省（MEF）の IT 局である。

聞き取り調査の結果、双方の組織がセキュリティ対策はそれぞれで独自で対応していることが確認された。内務省（MOI）については、サイバー犯罪の取り締まりを担当しており、一般向けの普及啓発活動への関心が高いことを確認した。

(1) 内務省（MOI）

概要
（Anti-cybercrime Department/ IT Department と面談） ➢ IT 局の職務： ICT マスタープランの作成、人事研修・知識共有、技術インフラの開発、サイバーセキュリティ対策、ICT ガバナンス、ICT Development、仕事と公共サービスの質の向上。 ➢ 最近のサイバー犯罪への対応： フィナンシャル犯罪、インターネット詐欺、ネットいじめ・ネット名誉棄損、フェイクニュース等の監視と、ウイルスとマルウェア、違法オンライン賭博、ハッキング、情報漏洩、テロイデオロギーの促進に関する活動を実施。 ➢ サイバーセキュリティマネジメントの枠組み： • Information Security Management System (ISMS, ISO 20071) に基づく管理を実施。カンボジアでは 2 年前（2020 年）に ISMS を導入。 • 国内の政策や基準／国際的な政策基準との連携。 • 内務省（MOI）には、デジタル政府チームがある。サイバーセキュリティ関しては、デジタル政府チームの下にある Infrastructure, software and data system, operating system and services を担当している部署と連携を図っている。 ➢ その他 • 過去 2 年間で、2 名（女性）が 1 名サイバー分野、もう 1 名別の領域で留学中。 • デジタル政府のための活動計画を作成中。多くのアクションプランあり。 • 他ドナーからの協力はなく、アクションプランを進める協力者を求めている。 • 内務省（MOI）が何かしらの研修を受けた後、その知見を内部で広げていくために以下のような仕組みがある。情報・マテリアルの共有のためのプラットフォームがある（地方にもフォーカルポイントあり） • デジタルセキュリティ委員会（DSC）が設立された場合には、内務省（MOI）もメンバーとなる予定。
協力の可能性
• 技術文書の提供及び研修への参加、成果 2 の普及啓発活動での協力

(2) 経済財務省（MEF）

概要
（IT Department と面談） • IT Department は General Secretariat の下に設置された 1 オフィス（他にも複数の IT Department がある）。 • 一般的な IT サポート、IT インフラ・ネットワーク（LAN）の維持管理、データセンターの維持・運営を担当している。 • IT Department of General Custom Department などあるが、IT Department of General Secretariat が IT Council の中核を担っている。Financial Information Management System (FIMS)を管理。
協力の可能性
• 技術文書の提供及び研修への参加

2-6-2　民間事業者及びその他の関係機関

本調査では、活動における協力の可能性及び現地における IT／サイバーセキュリティ市場を確認するために、IT 系企業 4 社（SpaciaNET、Proseth Institute、Cam Info Services、Forval Cambodia）、CII 企業 3 社（EZECOM、Electricity of Cambodia、Phnom Penh Water Supply Authority）、銀行をメンバーに持つ Association of Banks in Cambodia を訪問した。

聞き取り調査の結果、すべての組織から政府によるサイバーセキュリティの方針や標準の指導が十分ではないという声が聞かれた。また、ウェブサイトを構築した際の MPTC によるセキュリティ検査も表面上の対応であり、十分に実施できていないということであった。民間企業もサイバーセキュリティの重要性を認識し、それぞれで独自に対応しようとしているが、政府からの支援を必要している状況であることがわかった。ただし、これらは一部の企業から情報であり、カンボジアの IT／サイバーセキュリティの全体像を推察する際は注意が必要である。

(1) SpaciaNet

概要
• 日本の顧客を持つカンボジアの民間 IT 企業。社員約 50 人中システム開発に関するエンジニアは 7～8 人。 • JICA 事業について経験あり。 • 主事業の Air Xpress は、日本人を対象として日本の旅行会社と組んで、インターネットでの旅行手続き業務を実施している。また、楽天、Airbnb などにおいて民泊管理のサービスを提供している。 • サービスはオンプレミスではなくクラウドベース。（コスト面から）現地のデータセンターに設置。Amazon Web Service（AWS）を利用する場合は、日本の顧客であれば東京リージョンのデータセンターを利用している。
協力の可能性
• サイバーセキュリティに関する協力は難しい • 必要に応じて小型のシステム開発は発注可能

(2) Proseth Institute

概要
• 職員 6 人（研修を実施する際はロジサポート可能）で IT／セキュリティ系の研修を提供。
協力の可能性
• 研修の準備やロジ、クメール語へ翻訳 • 研修の実施（講師と教材の提供）、講師はカンボジア人または外国人
提供可能な研修コースの例
• コース例 F5 A―Cyber Security Essentials（450 USD/student, 60 hrs, 3 weeks）、CyberOps Associate、CCNA、CCNP PMI ―Certified Associate in Project Management（CAPM） Microsoft 365 security administration etc. CompTIA、EC-Council とは 2022 年 10 月にパートナー契約を結ぶので、11 月からコースの提供が可能になる予定。 Certified Information Systems Security Professional （CISSP）、Certified Information Security Manager （CISM）、Certified Information Systems Auditor （CISA）はレベルが高く、カンボジアで提供できる企業はない。 • テイラーメイドコース 対応可能 • 学習管理システム（LMS） 独自の LMS を持っているが基本的には管理のみ。一部、Question Bank を保有している。 • テスト Administering & Configuring BIG-IP local traffic manager (LTM), 600 USD/student Cloud Security Alliance 系: 1000 USD/student Cisco 講座開始前・終了後に研修生へのアセスメントテストを行う（講座に含まれる）。資格試験は別契約が必要。

(3) Cam Info Services Co., Ltd.

概要
• 2004 年からウェブサイトやシステム開発のビジネスを開始。民間企業、NGO、政府等色々なセクターでの開発経験あり。パッケージソフトの販売ではなく、オープンソースを活用したスクラッチ開発が主ビジネス。 • 現在は、IT ネットワーク・セキュリティカメラ・ウェブサイトのホスティング・ドメイン登録・電子政府関係

等について各セクターでカスタマイズした開発を行っている。
- 海外顧客は、JICA, ADB, World Bank 等。
- 社員は 16 人で全員エンジニア。経理や工事等はアウトソースしている。
- エンジニアリング分野は、Front-End, Back-End, Infrastructure に分かれている。SaaS, PaaS, IaaS を活用しているが、Google Cloud Platform（GCP）や、AWS 等のクラウドシステムでの開発が多い（オンプレミス開発もあり）。
- 同社は ASP.NET 等のフレームワークはあまり活用せず、すべてオープンソースで開発している。

協力の可能性
- サイバーセキュリティに関する協力は難しい
- システム開発、IT コンサルティング

(4) Forval (Cambodia) Co., Ltd.

概要
- 同社は 2010 年 4 月に創業し 13 期目にあたる。2013 年に合併で機械警備会社 ESS をカンボジアで立ち上げた。社員は 60 名（日本人 3 名）。事業所はプノンペン都、プノンペン経済特区（PPSEZ）、Bavet（技術者のみの配置）にある。
- 技プロ「光ファイバーネットワーク改善プロジェクト／監視カメラの構築支援」や「技術職業教育訓練（TVET）」関係で JICA とも連携・関係にある。
- 「ビジネスにおけるよろず屋」を会社ビジョンとしている。ただし、自社ですべて完結できるとは考えておらず、自社のネットワークを広げて、カンボジアでビジネスをする方々をサポートしている。日系企業における市場開拓・進出を支援。
- ESS（2013 年～）合同会社については、4 割が Forval、Saxa（4 割）、SCI（空港の持ち株会社）（11%）。人的リソースはカンボジア側が担当。社員 43 名。24 時間管制センターがあり、防災を管理してる。
- Forval 関連団体として NGO の Cambodia International Education Support Foundation （CIESF）を 2008 年 7 月に設立。職員は 45 名。ベトナム、ミャンマー、インドネシアに現地法人があり。タイに最近営業所（2022 年 7 月）を開設。
- CIESF の教育分野では、小学校から中学校までの学校を設立。各学校で 30 名程度。小学校から中学まで 120 名。カンボジアで最も競争率の高い学校。運営費は、CIESF の寄付金で賄っている。
- ビジネスコンテストを毎年開催。優勝者には、カンボジア、ベトナム、ラオスを含めたコンペがあり、それに通るとアメリカの大会に出場できる。マイクロソフトもサポートしているビジネスコンテストをカンボジアでも開催。拠点はプノンペン。バッタンバン（タイ国境側）、スバイリエン（ベトナム国境側）で支援している。
- IT リテラシーの向上のための草の根無償で、地方出張して日本でいう IT パスポートの展開を支援していた（コロナ前）。

協力の可能性
- 機材調達ベンダーの候補
- カンボジアの民間企業で発生したサイバーセキュリティインシデントに関する状況の相談
- 協力の可能性のある日系企業に関する相談

(5) EZECOM （インターネット・サービス・プロバイダー）

概要
- EZECOM 社は 2008 年に創業したカンボジアで最初の ISP。2011 年に ISO-27001 を取得。海底ケーブルやデータセンター事業も行っている。
- ネットワークセキュリティも対応しており、DDoS 攻撃の防御システムは保有している。
- カンボジアの現在の ISP 数は、2020 年には 70、2022 年には 42-44 程度ある。EZECOM がサイバーセキュリティ産業と市場を成長させていくべきと考えている。
- 人材育成については、Certification が得られるコースを受講させている（Microsoft、AWS 等）。

協力の可能性
- 技術文書の提供及び研修への参加

(6) Electricity of Cambodia （電力会社）

概要

（IT Department と面談）
- 職員総数 6077 名、うち ICT 局 23 名（現時点）5 課配置- ほとんどが IT 技術者。Transition Department は 948 名。プノンペン都に 5 支部（支社）あり、地方に 15 支部（支社）ある。
- EDC は State owned entity（国営企業）であり、政府規定によって管理されている。水事業体や Telecom Cambodia

も同様。カンボジア国内には大小合わせて 100 以上の電力企業がある。（EDC はもっとも大きい）
- Authority of Electric of Cambodia（AEC）は規制当局。鉱物エネルギー省（Ministry of Mine and Energy）が所管。EDC は AEC 配下の電力事業体（CII 事業者）。
- EDC の保有する機材の維持管理は問題なく実施できている。（毎年更新）
- 顧客向けのオンラインサービスの構築、IT インフラ、IT セキュリティの構築を主業務としている。現地一般向けのシステムは、現地の IT ベンダーが開発しており、web application や mobile app がある。銀行向けには、顧客がオンラインで支払いができる支払い（Billing）に関するシステムを導入している。
- SCADA(Supervisory Control And Data Acquisition)システムについては、IT Department ではなく別の部局（Under department of Transmission と Commercial and Distribution Department）が担当している。（関連して全国に 100 以上の配電部門がある）
- セキュリティ対策について、公共サービスの通信をモニタリングしており、不審な通信はブロックしている。EDC の保有するシステムには、Brute Force 攻撃やポートスキャニングが行われている。ファイアウォールアプライアンスにより一部の攻撃は防ぐことができている。アプリケーションレベルの End Point Security も実装済。

協力の可能性
- 技術文書の提供及び研修への参加

(7) Phnom Penh Water Supply Authority (PPWSA)（プノンペン都の水道事業体）

概要

（IT Department と面談）
- IT 部門は、請求書作成、システム保守、ユーザーのサポートが主な業務。3 つの業務に対してそれぞれチームがある：1) システム保守のためのインフラチーム（LAN やサーバの管理）、2) 請求書作成チーム、3) ユーザー向けのアプリケーションを作成する研究開発チームがある。
- 業務のコアシステムは「Microsoft Dynamics 365」で、水道料金の請求、在庫管理、人事、財務などすべてを管理している。顧客に請求書を発行する「スポット課金システム」も保有している。
- 機器を制御する SCADA システムは生産部門が管理している。
- カスタマーケア部門に来年度の予算が割り当てられる見込みで、モバイルアプリケーションの導入を計画中。（請求書発行はモバイルですでに可能）
- PPWSA は独立した水道事業体であるが、政府（予算経済財政部、工業技術革新部）の管理下にあるため半官半民の組織であるといえる。PPWSA はプノンペン都で水道事業を行っている唯一の企業である（用水量 65,000m^3）。
- 水道会社は全国（25 の県）に 100 社以上存在している。各地域にはそれぞれ異なるシステムを有する水道会社がある。
- プノンペン都及び他の地域を対象とした水道事業の規制当局は Ministry of Industry, Science, Technology and Innovation（MISTI）の Water Department である。MISTI は水道事業に関する規制のみで、サイバーセキュリティに関する指導は無し。ただし、2021 年に ISO 27001 に関する一般的な情報セキュリティに関する通知は発行している。
- ハードウェアも必要であるが、CS が一番の優先事項。民間企業が実施する CS 研修も参加している。（3～6 か月）

協力の可能性
- 技術文書の提供及び研修への参加

(8) Association of Banks in Cambodia (ABC)

概要
- 事務局スタッフは 15 名。 組織内に 8 つの委員会が設置されている（リスク管理、ペイメント、教育等）。
- ABC には 59 の商業銀行、7 つの専門銀行、18 のカンボジア・マイクロファイナンス機関、カンボジア・フィンテック協会が加盟している。
- なお、カンボジアの国立銀行は、他の省庁から独立した機関であり、財政政策や監督を行っている。

協力の可能性
- 技術文書の提供及び研修への参加（ベンダーロックインした研修以外）
- 協会メンバーの銀行への普及啓発活動

2-7　セキュリティ知識分野人材スキルマッピング（SecBoK）

本調査において、サイバーセキュリティ人材の能力向上のための研修計画は、Security Body of Knowledge（以下、「SecBoK」という。）[23]を元にした分析により作成する方針を示し、C/P からも合意が得られている。具体的には、ベトナム国「サイバーセキュリティに関する能力向上プロジェクト」において実施した、SecBoK を適用した「キャリア開発計画」の方法論を ICT セキュリティ局に対する研修計画に活用する。

2-8　他ドナー支援の概要

2-8-1　AJCCBC（ASEAN-Japan Cybersecurity Capacity Building Center）

ASEAN サイバーセキュリティ能力構築センター（ASEAN-Japan Cybersecurity Capacity Building Center）（以下、「AJCCBC」という。）は、2018 年に TELMIN/SOM の指導の下に設立された団体で、Japan ASEAN Integration Fund (JAIF 2.0) の資金支援の下、AMS の参加者にトレーニングやその他の活動を提供することにより、AMS のサイバーセキュリティの専門家と専門家の能力を向上させ、4 年間で 700 人以上のサイバーセキュリティ人材を育成することを目的としている 。本調査時点で、AJCCBC では以下の 3 コースを提供している。

表 2－13　AJCCBC が提供する研修コース概要

コース名	概要
1. Cyber Defense Exercise with Recurrence (CYDER)	総務省が実施しているサイバー攻撃に対応するためのインシデントレスポンス能力の向上に焦点を当てた「実践的サイバー防御演習（CYDER）」に基づいたコース。研修は、講義、実習、チームディスカッション（反省会）の 3 部構成である。
2. Hands-on Network Forensics	DMZ 内のサーバやクライアント PC を狙った APT 攻撃に基づいた、ネットワーク・フォレンジック手法を提供。参加者は複数のログ分析と詳細なパケット分析を実行し、検出ルールの記述方法を学ぶことができる。
3. Hands-on Malware Analysis	表層分析、動的分析、静的分析によってマルウェアの動作とその影響を特定する方法スキルを提供する。

出所：AJCCBC ホームページ

また、AJCCBC は ASEAN Youth Cybersecurity Technical Challenge「Cyber SEA Game」を開催している。これは、ネットワーク（パケット分析）、OS、インシデント対応、フォレンジック、暗号化、プログラミングなどの幅広い知識を持つ、ASEAN 諸国から選抜された 30 歳以下の学生・若手技術者 4 名のチームが対象となっている。Cyber SEA Game は CTF (Capture the Flag) と呼ばれる形式のコンピューターセキュリティの問題を解決することを目的とした技術的なコンテストである。このコンテストを通じて、参加者はサイバーセキュリティ関連のスキルを開発し、参加者同士関係を築くことができる。なお、2023 年度からは JICA 技術協力の一環として AJCCBC を運営する。

[23] SecBoK は、日本ネットワークセキュリティ協会（JNSA）が「情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキル」を体系的に整理し公開している資料で、組織内での役割（ロール）とその役割に求められる知識・スキルの関係を一覧でまとめたものある。

2-8-2　シンガポール

シンガポール政府も域内協力の一環で不定期ではあるが必要に応じて、サイバーセキュリティに関する短期研修プログラムを（対面及びオンライン）提供している。開催回数はこれまで年に 2～3 回程度ということである。

2-8-3　日本の支援実績

カンボジア国のサイバーセキュリティ分野に対する支援実績としては、本邦で実施されている課題別研修への研修員招聘事業が挙げられる。過去 2 年間の実績は下表のとおり。

表 2－14　日本による支援実績（2020 年～2022 年）

年度	研修名	人数
2020 年度	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	1
	サイバー攻撃防御演習	1
2021 年度	ICT 実践力強化のためのコア人材育成	1
	サイバー攻撃防御演習	1
2022 年度	ICT 実践力強化のためのコア人材育成	1
	サイバー攻撃防御演習	1
2023 年度（予定）	ICT 実践力強化のためのコア人材育成	1
	サイバー攻撃防御演習	1
	サイバーセキュリティ対策強化のための国際法・政策能力向上	1
合計	**4 分野**	**9 名**

出所：JICA 提供資料

このほかの類似事業として、JICA による「国家 ICT 開発庁に対する技術協力プロジェクト」が挙げられる。同プロジェクトは、2000 年にアセアン地域における ICT 普及を目的に設立された eASEAN の受け皿としてカンボジアに設立された国家 ICT 開発庁（NiDA）に対して 2008 年 2 月から 2010 年 1 月の 2 年間にわたって実施された事業である。2 年間の事業を通じ NiDA 職員の実践的人材開発が実現するとともに、情報セキュリティに対する NiDA のイニシアティブが発揮され、ITEE（Information Technology Engineers Examination：情報処理技術者試験）が試行的に導入されることにより NiDA による ICT 管理能力が向上し、ひいてはカンボジアにおける ICT 開発環境の改善に寄与することが期待されていた。

第3章プロジェクトの計画概要

3-1　プロジェクトの概要

3-1-1　プロジェクト名称

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

3-1-2　期間

2023 年 5 月～2026 年 10 月（42 か月）

3-1-3　対象地域

プノンペン都

3-1-4　ターゲットグループ（受益者）プロジェクト名称

直接受益者：政府機関職員（郵政通信省、関係省庁、地方政府）、重要インフラ産業関連機関職員

間接受益者：カンボジア国民、カンボジア関連企業

3-1-5　運営実施体制

プロジェクトの実施体制は下図のとおり。

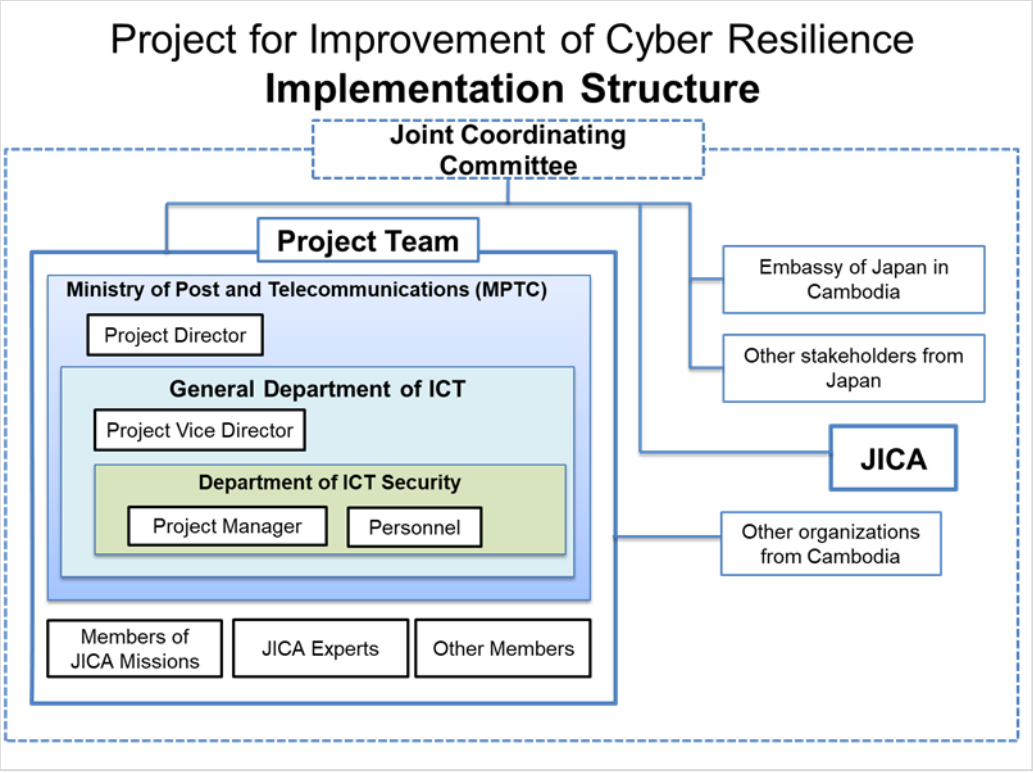


図 3−1　実施体制図

(1) プロジェクトディレクター：MPTC 長官（Secretary of State）

(2) 副プロジェクトディレクター：ICT 総局総局長（Director General）

(3) **プロジェクトマネージャー**：ICT セキュリティ局局長（Director）

3-1-6　案件概要

プロジェクトの案件概要は下表のとおり。

表 3−1　案件概要

PDM 要約		指標
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	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. 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
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	1. 定量指標：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、インシデント検知数、インシデント対応数等が増加する 2. 定性指標：明確になった CSIRT サービスの運用レベルと法整備の準備状況（CSIRT 組織成熟度の評価）が改善される
成果 1	CSIRT サービスの提供能力が改善される	1-1 協力期間中に実施される研修に参加した半数以上の研修員の ICT セキュリティに関する理解が向上する 1-2 上司のサイバーセキュリティ担当者への評価が改善する 1-3 日常業務で用いるガイドラインやマニュアルが整備される 1-4 xxx などの IT 機材が導入・更新される （※xxx の機材については、プロジェクト開始時点で確定する）
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	2-1 一般市民向け及び関連組織向けの普及啓発資料が策定される 2-2 一般市民向けの活動がプノンペンまたその他の市で最低 2 回開催される 2-3 策定された各ガイドライン関する普及啓発セミナーが関係機関に対して実施される
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	3-1 ASEAN、日本、中国、米国、EU、及び ITU などの国際機関で規定されている法律、規制、ガイドラインなどの調査が実施される 3-2 プロジェクト期間中に比較検討され作成された提案事項が郵政通信省の上層部へ提出される
活動		
［成果 1］ 1-1 各CSIRTサービス領域の提供対象を明確にする（ベースライン） 1-2 国家CSIRTとしての成熟度を測定するためセキュリティ・アセスメントを実施する（ベースライン） 1-3 活動1-1に基づき、CSIRTサービスの質の向上のために必要な教材を作成する（例、ガイドライン、標準運用手順書、サービスレベル合意書、普及啓発教材等） 1-4 セキュリティスキルフレームワークを活用した研修計画を立案する 1-5 セキュリティフレームワークを活用した研修やドリルを実施する 1-6 研修の成果を評価し、研修計画やセキュリティ上の役割を見直す（自己評価及び管理職評価） 1-7 将来の研修プログラムの実施ついて局内で議論し提案を立案する 1-8 ICTセキュリティ局のサイバーセキュリティ能力強化のためのIT環境を整備する		
2-1 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する 2-2 普及啓発活動の教材を作成する		

2-3　子どもや女性、高齢者へ等社会的弱者への普及啓発活動を実施する（ジェンダー配慮）
2-4　関連機関向けにガイドラインや手順書等に関する普及啓発活動を実施する（例：セキュリティ評価、リスク評価、SOC、インシデント対応等）
2-5　関連機関とフィードバックセッションを実施し、必要に応じて教材を改定する
3-1　研究するべき政策・法律・標準を特定する
3-2　国際標準や他国のサイバーセキュリティ政策・法律等を机上調査とスタディツアーを通じて研究する（戦略、フレームワーム、ロードマップ、標準含む）
3-3　調査結果をまとめて、カンボジアに必要な政策・法律・標準等を特定する
3-4　郵政通信省内の関連部局と関係機関に対してコンサルテーションを実施する
3-5　カンボジアに必要な政策・法律・戦略・標準等に関する提言を作成する

3-2　投入計画

(1) 日本側投入

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 サービス強化、普及啓発活動、法整備等
研修	本邦研修、第三国研修、現地研修	
機材・設備	サーバ、ネットワーク機器、各種ソフトウェア等	
調査団派遣	サイバーセキュリティ関連機関職員等	

(2) カンボジア側

人員配置	プロジェクトディレクター1名：郵政通信省（MPTC）長官（Secretary of State） 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 C/P
執務環境	執務室（執務用機材含む）
現地費用	光熱費、管理運営費、研修用会場設備、プロジェクト活動のための現地活動費用など

3-3　外部条件・リスク分析

(1) 上位目標達成に関する外部条件

- 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郵政通信省内で効果的に活用される
- サイバーセキュリティに関する組織の関与が増加する

(2) プロジェクト目標を達成に関する外部条件

- 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が維持される
- 研修を受けた ICT セキュリティ局と他の関連機関の職員が同じ職場で勤務し続ける

(3) 成果の発現に関するの外部条件

- 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が維持される
- C/P の配置人数が大幅に減員されない

3-4　前提条件

本プロジェクトを実施していく上での前提条件は以下のとおり。

- 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

3-5 プロジェクト実施上の留意点

3-5-1 プロジェクト成果の考え方と留意点

(1) 成果 1：

(a) 成果 1 の考え方

成果 1 では、主に CSIRT サービス提供の技術的基盤を強化する。プロジェクト初期において、CSIRT サービスの提供範囲（インシデント対応、SOC、普及啓発活動、セキュリティ・アセスメント等）の特定や組織の成熟度アセスメントを通して、サイバーセキュリティ業務における現在の状況とあるべき姿を明確にする。目標とするサイバーセキュリティ組織に近づくために、スキル・フレームワークを活用した研修計画に基づいた技術研修の提供を通して、CSIRT サービスが改善されることが期待される。また、人材育成とともに機材供与により業務環境の改善も改善される。

(b) 留意点

- 活動 1-2 の成熟度診断（評価）について、ICT セキュリティ局で既に類似するアセスメントを実施済みであることから、プロジェクト活動でゼロから情報を収集していくのではなく、既存の情報等を利活用し、活動の効率化を図っていく。具体的には、成熟度診断に活用されていた「セキュリティインシデント管理成熟度モデル」（Security Incident Management Maturity Model：SIM3）でカバーされる CSIRT サービスの領域だけでなく、法律の領域もアセスメントの範囲に含めて横断的に実施していけるよう調整していく必要がある。
- 活動 1-3 における技術文書の策定では、3 年間という協力期間に鑑み、作成が必要となる技術文書リスト（要請）から優先度の高いものを 3 つ程度選択する。調査時点の候補と優先度は以下のとおり。プロジェクト開始前後において、作成が必要な技術文書と優先順位付けに関して先方の意向を確定する。成果 1 の活動における技術文書の策定は、成果 2 の活動とも連結しており、成果 1 での作業の遅延は直接成果 2 の活動に影響を及ぼす事になる（クリティカルパスとなる）ため、成果 1 での活動実施運営管理には細心の注意を払っていく必要がある。
- MPTC での決裁手続きは、総局長から副長官へ提出され、長官を経て、大臣へと最終的に提出される。具体的には、プロジェクト側から成果品を MPTC マネジメントに提出した場合、総局長レベルで一度内容に対するフィードバック（コメント）を受け、対応の上、上層部へと提出されることになる。これら一連の手続きには、最低 1 週間はかかる見込みである。技術的なコメントは ICT 総局内から出ることがほとんどであり、より上位の承認者に対してはレターにおいて概要を説明するため、承認プロセスは比較的スムーズに進むと考えられる。活動の実施に際しては、成果品作成後の決裁手続きに要する時間も想定し、その後の活動計画を策定・調整していくことが望まれる。

- 活動 1-7　提案の策定については、人材育成に関するプロジェクト活動の事業完了後の持続性を担保していくために、CADT の組織体制の整備状況、CADT の位置づけ、活用の可能性を MPTC 側と協議をし、将来の活用の可能性を探っていくことが肝要である。

表 3−2　必要書類の優先度の目安

文書名	優先度
CSIRT Guideline (including CSIRT Establish Guideline, Operation Procedure, SLA etc.)	高
SOC Standard Operation Procedure (SOP)	
Incident Handling Standard Operation Procedure (SOP)	
Cybersecurity Risk Assessment Framework	
Pentest Standard Operation Procedure (SOP)	
Forensics Standard Operation Procedure (SOP)	
Malware Analysis Standard Operation Procedure (SOP)	
Security Assessment Framework (CSIRT Assessment)	
Incident Response Play Book	
Cybersecurity Policy and Guideline (Operation level)	低

(2) 成果 2：

(a) **成果 2 の考え方**

成果 2 では技術者向け及び一般国民向け普及啓発活動が主たる協力となる。成果 1 で作成したサイバーセキュリティにかかる運用手順書等の技術文書を、MPTC 内及び関連中央省庁、CII 事業者等と共有し、理解向上及び普及のためのセミナーやワークショップを実施する。この活動を通じて、MPTC と関連機関（他省庁・CII 事業者等）とのサイバーセキュリティのための活動が強化されることを目指す。また、一般国民、特に若年層や女性等、高齢者等のオンライン活動における脆弱層に対してサイバーセキュリティに普及啓発活動を通じて、オンライン活動を推進するためのサイバー空間の安全性の確保が進むことが期待される。

(b) 留意点

- 内務省（MOI）はサイバー犯罪に関する普及啓発活動を実施しており、情報や経験が豊富である。したがって、活動 2-2 普及啓発活動の実施に際しては、実例を交えた資料を作成していけるよう内務省（MOI）とも密に連携を図っていけるよう調整していく必要がある。
- 活動 2-4 の普及啓発活動は、その他の省庁や関係機関も対象に含んでいる。プロジェクトの成果品（ガイドライン等の技術文書）の活用に際しては、一般的に MPTC の大臣からの承認を得ることが求められるが、普及啓発活動については、総局長決裁となるため、これら一連の手続きに要する時間を想定の上、普及啓発活動の実施時期を調整・決定していくことが肝要である。
- 活動 2-3 の市民向け普及啓発活動については、MPTC では毎年 10 月が普及啓発月間であるため、本プロジェクトでの普及啓発活動についても同月に合わせて実施し活動の効率性、波及効果を高めていく。
- 活動 2-5 フィードバックセッションについては、別の日程を設定し MPTC から特定の参加者に対してフィードバックを求めた場合には十分な返答が得られない可能性が高いことから、普及啓発活動セッションの最終日等にフィードバックセッションを設け、可能な限り多くの意見を参加者から抽出できるよう調整を図っていくことが重要である。

(3) 成果 3

(a) **成果 3 の考え方**

成果 3 は法・規制の準備にかかる協力である。日本・欧米・中国・周辺国等の事例研究を通して、カンボジアにとって必要なサイバーセキュリティに関する法律・政策・戦略・技術標準・規制等を特定し、提言として提出する。また、MPTC を中心として法規制に関わる関係者へのセミナー等を通して、これらの国際標準や他国政策・法律に関する理解が促進される。

(b) 留意点

- サイバーセキュリティに関しては周辺国においても積極的な動きがみられる。カンボジアにおいてより実効性の高い政策を策定していくために、プロジェクト活動期間中に周辺国へのスタディツアーの実施についても検討していくことが望まれる。
- 提言を受けての法律や標準等の策定は先方負担事項であり、政策提言に結び付けていけるよう先方の継続的なコミットメントを後押ししていく必要がある。。

(4) 全成果共通の留意事項

- カンボジアは年度末～年始（12 月～１月）、カンボジア新年（4 月）、ボートレース（11 月ごろ）が繁忙期とされ、その時期は職員の動き、省内での活動が停滞する可能性が高い。それらの時期の活動については慎重に計画していく必要がある。
- CamCERT に配置される人材の効率的な配置が事業効率に大きく影響を及ぼす事になる。したがって、プロジェクト活動の実施に際しては、ICT セキュリティ局への活動計画の事前の周知が不可欠であり、長期専門家を中心に、同局の予定や動向をつぶさにチェックし、プロジェクト活動の円滑な実施に向けた調整を図っていくことが求められる。

3-5-2　プロジェクトを取り巻く環境への配慮

- 2021 年に入り政府内部ではデジタル政府委員会（DGC）や Digital Economy and Business Committee の設立の動きがみられ、今後デジタルセキュリティ委員会（DSC）の設立も予定されている。デジタルセキュリティ委員会（DSC）の設立に伴い関連省庁の体制や業務分掌に変更が生じる可能性があることから、政府内の今後の動きに注視していく必要がある。また、組織体制に変更が生じた場合には、新体制下でのプロジェクトの実施体制について ICT 局と協議を行い、体制変更によりプロジェクト計画に変更が生じる場合には、本プロジェクトの合意文書（Record of Discussion：R/D）の改訂を含めた手続きを進めていくことが求められる。
- 前述したように、本プロジェクトと並行して MPTC 向けに日本外務省による無償資金協力事業の実施が計画されており、本プロジェクトでは、供与予定機材に関する SOP 等の策定を活動計画に盛り込んでいる。本プロジェクトと無償資金協力事業の協調の方向性等については、同事業開始以降の関係者協議で決定することになる。プロジェクトの活動スコープやインプット等に変更が生じる場合には、速やかに PDM の見直しを進めていく必要がある。

3-5-3　ジェンダー・脆弱層への配慮

本事業はジェンダー主流化にかかる活動は想定されていないものの、社会的弱者への対応として若年層や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を実施する。

3-6　モニタリングと評価

半年ごとにモニタリングシートを用いたモニタリング活動を実施するとともに、プロジェクト終了前 6 カ月の時点で終了時評価を実施する。また事業完了後 3 年目には、事後評価を実施することとする。

第4章プロジェクトの事前評価（六項目評価）

4-1　妥当性

サイバーセキュリティ能力の強化に焦点をあてた本プロジェクトは、経済の多様化におけるデジタルシステムの信頼性と信用性の構築を目指すカンボジア政府の政策方針と整合しており、そのためのMPTC、特にICTセキュリティ局の技術力向上に対するニーズに対応する計画となっている。また、技術・ノウハウ強化を通じた組織力強化を図っていくために体系的な活動を計画しており、支援のアプローチとしての適切性も認められる。

以上のことから、本プロジェクトの妥当性は高いと評価できる。

4-1-1　カンボジア政府の政策との適合性

本プロジェクトの内容及び方向性は、以下の理由からカンボジア政府が掲げる政策・方針と整合している。

カンボジア政府は、2019年に国家最高位の戦略である「第4次四辺形戦略」を策定し、それを受ける形で「国家戦略開発計画（2019年～2023年）」を策定している。第4次四辺形戦略では「ガバナンス改革の加速」を中心課題としてとらえ、今後5年間の戦略の柱として4つの柱を掲げられており、そのうち「柱2.の経済の多様化」において、デジタル経済や産業革命4.0への対応の重要性が示されている。また、上記計画において、デジタル政府、情報セキュリティ戦略、電子商取引法、サイバー犯罪法の実施、同分野の成長とリスク防止に向けた法律や関連規制の改正等のデジタル経済の発展を支える法的枠組みの確立と推進といったサイバーセキュリティを含むICTセクターにおける中期的な活動の方向性が示されている。

また、デジタルセクターの発展を推進していくための体制構築に向けた施策として、カンボジア政府は、2021年に「デジタル経済・社会政策フレームワーク2021年～2035年」を策定し、2035年までの15年間で「ニューノーマルの流れの中で、新たな経済成長を加速し、社会福祉を促進するため、活力あるデジタル経済・社会を構築する」ことを示している。同文書では、①デジタル基盤の構築、②デジタルの導入、③デジタル変革という3つ原則の下、重点5領域（2つの基盤及び3つの柱）が定められており、2つの基盤の1つにデジタルフレームワークの構築やサイバーセキュリティ管理体制の構築を対象とした「デジタルシステムの信頼性と信用性の構築」の重要性が謳われている。

さらに、カンボジア政府は2021年に包括的なデジタル経済・社会を発展させるために、透明で信頼できる方法でガバナンスシステムの近代化及び改革のためのエコシステムでもあるデジタルインフラと技術を活用し、スマート政府を構築していくことを目的に「デジタル政府政策2022年～2035年」を制定した。同政策では、「デジタルガバメントにおけるインフラの整備」や「デジタル人的資源開発・革新」を含む4つの戦略目標が定められている。

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向け、3年間のプロジェクトを通じてCamCERTを中心としたサイバーセキュリティに関する能力の向上とCamCERTとCII産業及び他省庁間との組織間連携を強化していくことで、MTPCのICTセキュリティ局の組織としての能力の向上を目指す本プロジェクトは、カンボジア政府が掲げる戦略や政策の実現に向けた重要な取組みであり、政府、市民生活、ビジネス活動の全ての面において大きく貢献しうるものである。

4-1-2　アプローチ（ロジック）の適切性

本プロジェクトで採用するアプローチは以下の理由から適切であると判断できる。

カンボジアでは、国家 CERT にあたる CamCERT における日一日と高度化するサイバー攻撃に対応していくためのスキルや最新技術に関する知識の向上、CamCERT を含む政府省庁や関連機関におけるサイバーセキュリティ人材の不足への対応が喫緊の課題となっている。これらの課題に対して、本プロジェクトでは、主に知識とスキルの向上という課題への対応策としてインプットやアウトプットだけでなく将来的な制度整備への提言などを含む活動を通じて、カンボジアにおけるサイバーセキュリティ能力の底上げを図っていく計画となっている。

- **インプット**：成果 1 の活動が知識のインプットに該当する活動であり、CamCERT の現業業務の範囲を確認と一般的な CSIRT サービス領域との比較を通じた国家 CSIRT としての成熟度を診断し、CSIRT サービスの質的な向上に向け能力強化が必要とされる領域を特定する。そのうえで、該当領域に対する教材（ガイドライン、SOP、普及啓発資料等）を作成し、個別具体的な研修を実施していくことになる。研修の実施に際しては、セキュリティスキルフレームワークを活用し、職員の技術到達度に合わせた研修計画を策定していくことで段階的かつ着実に知識をインプットしていくことを想定している。
- **アウトプット**：成果 2 が知識のアウトプットに対する活動であり、サイバーセキュリティに対する現状を確認した上で、必要となる普及啓発活動の資料・教材を作成し、子どもや女性等社会的弱者を含む一般市民向け及び関係機関向けの普及啓発活動を実施していく。その際、サイバー犯罪防止に向けた啓発活動の実績を多数有する内務省（MOI）と密な連携を図っていくことで活動の幅と深度を深めていく。
- **制度整備への提言**：成果 3 が制度整備に向けた活動である。ここでは、サイバーセキュリティ分野における今後の発展的展開を見据え、主に法規や政策、基準に対する調査研究を行うことを想定しており、国際基準や周辺国を含む諸外国が定める政策や法律を対象とする。ただし、実際の法整備には多大な時間を要することから、本活動においては、カンボジア政府による法整備に向けた主体的な取り組みを側面支援する形をとる。

4-2　整合性

本プロジェクトは、以下の理由から日本の国家政策や他の類似事業を踏まえた内容であるとともに国際的な枠組みに沿った活動であると判断できる。

4-2-1　日本の対カンボジア援助政策との整合性

本プロジェクトは、日本政府の対カンボジア援助政策と整合している。

我が国の「対カンボジア国別開発協力方針」（2017 年 7 月）では、2030 年までの高中所得国入りの実現に向けた経済社会基盤の更なる強化を支援することを方針として掲げており、そのための支援重点分野として、①社会振興支援、②生活の質向上、③ガバナンスの強化を通じた持続可能な社会の実現を挙げている。ICT／サイバーセキュリティ分野に対する支援は、「③ガバナンスの強化」における行政機構の組織強化、公務員の能力強化を通じた行政サービスの質の向上として位置づけられる。

以上のことから、本プロジェクトで計画している活動は、我が国の協力指針に沿った内容であると判断できる。

4-2-2　日本の他事業及び他ドナーによる支援との整合性

(1) 日本の他事業との整合性

本プロジェクトは、以下の理由から日本の他事業と整合した取り組みであると判断できる。

ASEAN 諸国では、当該地域向けに内閣官房（内閣サイバーセキュリティセンター（NISC））、総務省、経済産業省を中心としたリモートサイバー演習、机上演習、重要インフラ防護、意識啓蒙、能力構築、インシデント相互通知、リファレンス（便覧）、ワーキンググループ運営及び産官学連携などの活動を実施展開している。令和 4 年 10 月に開催された第 15 回政策会議において、(1) 情報共有体制及びサイバーインシデント発生時の対処体制の強化、(2) 情報インフラ防護に関する取り組みの推進、(3) 能力構築及び意識啓発における協力の推進、(4) 産官学連携の推進について日・ASEAN の連携及び協力についての検討が行われている[24]。本プロジェクトで計画している活動は、上記 (3) の活動との関連性が高く、タイに拠点を置く日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）と連携した活動の実施展開も想定した内容となっている。

(2) 他ドナー・関係機関による事業との整合性

本プロジェクトの活動は、以下の理由から他関係機関による活動と整合した取り組みであると判断できる。

本調査時点で、MPTC の ICT セキュリティ局に対する他ドナー支援の実績は認められなかった。一方で、依然としてニーズの高いサイバーセキュリティ人材の育成については、タイに拠点を置く AJCCBC での研修事業や ASEAN の域内協力の一環として年に数回実施されるサイバーセキュリティに関する研修に MPTC から職員が派遣されている。

本プロジェクトにおいても、成果 1 の取組みにおいて、サイバーセキュリティ人材の知識と能力の底上げを図っていく活動を計画しており、域内における取組と整合した活動であるといえる。

4-2-3　国際的な枠組みとの整合性

以下の理由から、本プロジェクトの活動は、我が国のみならず国際的な取り組みにも整合した内容であると判断できる。

(1) 我が国の国際的な取り組みとの整合性

我が国では、2021 年 9 月のデジタル庁の設置に合わせて「サイバーセキュリティ戦略」（2021 年 9 月閣議決定）を制定しており、自由で公正かつ安全なサイバー空間を確保するための施策の一つとして、国際社会の平野・安定及び我が国の安全保障への寄与を打ち立てており、この中で国際協力や地域連携について述べている。加えて、サイバーセキュリティ戦略本部が 2021 年に決定した「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）」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も言及されている。

また、JICA の課題別戦略（グローバルアジェンダ）15 番目の戦略として、「デジタル化の推進」が取り上げられており、その中で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いる。同戦

[24] 出所：第 15 回 日・ASEAN サイバーセキュリティ政策会議の結果

略では、自由で安全なデジタル社会の実現の価値観の共有と共に、サイバーセキュリティへの対応能力強化を主に東南アジア・南アジアを中心に行い、地域のサイバーセキュリティの実現、経済社会活動の基盤であるサイバー空間の安定的な利用を実現していくことを目指し、①ベースとなるサイバーセキュリティ政策・制度及び施策実施のための組織作り、②各種インシデント対応態勢強化（組織及び国内重要インフラのセキュリティ対策強化を含む)、③公的セクター・民間セクターでの官民連携対応態勢構築、④一般国民のリテラシー向上、⑤国際連携促進に関する支援を行っていくとしている。

(2) 国際的な枠組みとの整合性

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。特に以下 SDGs については、デジタル指向が高い分野となり関係性が高い[25]。

ゴール 4 質の高い教育をみんなに
ゴール 7 エネルギーをみんなにそしてクリーンに
ゴール 8 働きがいも経済成長も
ゴール 9 産業と技術革新の基盤をつくろう
ゴール 11 住み続けられるまちづくりを
ゴール 16 平和と公正をすべての人に

4-3　有効性

4-3-1　計画の論理性

以下の理由から、プロジェクト計画における論理性は確保されていると判断できる。

カンボジアにおけるサイバーセキュリティ分野における現状と課題を踏まえ、本プロジェクトでは、当該分野の中心問題を「ICTセキュリティ局のサイバーセキュリティ能力の不足」と捉え、中心問題に影響を及ぼす主たる要因として、① CSIRTサービスの提供能力の低さ（成果1：GCIのTechnicalに該当)、ICT関係機関（他省庁）やCII事業者や一般国民等の関係者に対するサイバーセキュリティに関する普及啓発活動の未徹底（成果2：GCIのCapacity Developmentに該当)、サイバーセキュリティの強化に向けた法律・規制・標準の未整備（成果3：GCIのLegalとOrganizationalに該当）を取り上げている。

これら3つの成果の発現を下支えする活動は、比較研究、教材作成、OJTや現場での普及活動など多岐にわたるものの、成果間での連続性と関連性も保たれており、プロジェクト期間中に活動が計画に基づいて適時適切に実施されることで、協力期間内に所期の目標を達成できる設計となっている。

4-3-2　プロジェクト目標に対する指標

プロジェクト目標の達成状況を測る指標は目標の内容を的確に捉えており、指標データの入手手段に問題はなく、指標の達成度も測定可能な内容となっている。

本プロジェクトでは、プロジェクト目標で設定した「ICT セキュリティ局のサイバーセキュリティ能力の強化」の成否を測る指標として、定量及び定性の両側面からそれぞれ 1 つの指標を設定した。

[25] 出所：GFCE November 2021, Integrating Cyber Capacity into the Digital Development Agenda

定量指標としては、ICT セキュリティ局が提供する CSIRT サービスを提供している範囲（項目）の数、インシデント検知数、インシデント対応数の増加の有無を指標として設定しており、成果 1 の活動で明らかになった CSIRT サービスの現状とプロジェクト活動を通じて拡充されたサービスの提供数（状況）の増加幅を定期的に計測していくことで、能力向上の成否を測っていく。定性指標については、成果 1 の活動を通じて明らかになった CSIRT サービスの運用レベル（成熟度）と法整備の準備状況が改善されるという指標を置いており、ベースライン値と GCI のアセスメントの結果との比較結果を用いて、改善状況を把握していく。

4-3-3　成果（アウトプット）に対する指標

プロジェクトにおける各成果指標は、求める成果レベルを的確に捉えてたものであり、プロジェクト活動の成果やデータを用いて測定可能な内容となっている。

本プロジェクトでは、3 つの成果を設定している。そのうち成果 1 については、協力期間中に実施される研修に参加した半数以上の研修員の ICT セキュリティに関する理解や（指標 1-1）サイバーセキュリティ担当者の上司の評価が改善する（指標 1-2）ことに加え、日常業務で用いるガイドラインやマニュアル（指標 1-3）や IT 機材が導入・更新される（指標 1-4）ことをもって「CSIRT サービスの提供能力が改善した」と判断することになる。

また、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」については、一般市民向け及び関連組織向けの普及啓発資料が策定され（指標 2-1）、一般市民向けの活動がプノンペンまたその他の市で最低 2 回開催されるとともに（指標 2-2）、策定された各ガイドライン関する普及啓発セミナーが関係機関に対して実施される（指標 2-3）ことで、当該指標の達成の成否を測る計画となっている。

さらに、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・規則・標準等が特定される」については、ASEAN、日本、中国、米国、EU、及び ITU などの国際機関で規定されている法律、規制、ガイドラインなどの調査の実施の有無（指標 3-1）やプロジェクト期間中に比較検討され作成された提案事項の郵政通信省の上層部への提出（指標 3-2）の有無が達成根拠となる。

4-3-4　プロジェクトの有効性に対する外部条件及び主なリスク

プロジェクト目標の達成に影響を及ぼしうる内容が外部条件として適切に認識されており、そのための対応についても十分に検討がなされている。

本プロジェクトでは、前述のとおり「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」をプロジェクト目標に据えており、それを実現していくために CSIRT サービスの提供能力の強化、市民及び関係機関に対するサイバーセキュリティの活動の実施促進、サイバーセキュリティを強化するための必要な法規定等が特定されるという 3 つの成果を設定している。これら 3 つの成果が発現し、効果継続していくための外部要因（条件）として、本プロジェクトでは、次の 3 点を取り上げている。①ICT 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こと、②ICT セキュリティ局の責務が維持されること、③研修を受けた ICT セキュリティ局と他の関連機関の職員が同じ職場で勤務し続けること。

本調査時点での政府の政策動向を見る限り、MPTC の責務、さらには ICT セキュリティ局の責務が大幅に変更される可能性は低いと考えられるものの、現在進行中の National Digital Economy and Society

Council の体制整備に伴うデジタルセキュリティ委員会（DSC）の設立に向けた動きについては、プロジェクト開始以降もモニタリングを継続し、プロジェクトの実施体制への影響を最小限に留められるよう適時適切な対応が求められる。また、③については、MPTC 側の自助努力のみならず、研修受講者の継続的な関与を引き出していけるようなプロジェクト側からの働きかけも不可欠である点に留意が必要である。

4-4　効率性

成果と活動の因果関係は明確に定められており、期待される成果を産出するために十分な活動が計画されている。よって、計画に基づき活動を実施していくことができれば、協力期間を通じて効率的な活動を実施していくことが出来ると判断できる。

4-4-1　活動と成果との因果関係

既定の 3 つの成果を産出していくために、現状を確認・調査したうえで、現状を踏まえた技術的インプットを実施し、習得した知識や技術ノウハウを対外的に発信していくという流れで段階的に活動が組まれている。活動から成果発現までの道筋や論理性は明確に定められており、特段大きな大きなずれは認められない。

4-4-2　投入計画及び活動内容

本プロジェクトでは、成果を算出するために必要かつ効率的な活動が計画されており、投入のタイミングも十分に考慮された内容となっている。

本プロジェクトでは、詳細計画策定調査期間中の ICT セキュリティ局との協議において、プロジェクトの効果的・効率的な実施に向けた留意点及び対策について相互に確認した。確認事項としては、1) 類似プロジェクトの成果の活用（SecBoK）、2) 機材供与に向けた事前準備、3) プロジェクトの成果品（ガイドライン）等の承認手続きの円滑化、4) 他省庁との連携体制の維持、5) プロジェクトの成果品の将来的な活用に向けた省内手続きが挙げられる。このほかにも、本プロジェクトでは過去の類似事業からの教訓やカンボジアの政府内の動きを踏まえ、プロジェクトの活動実施をより効率的かつ効果的に実施していくための工夫を計画の随所に盛り込んでいる。

成果 1 の活動での CSIRT サービスの対象領域の特定や成熟度の測定において、評価基準の客観性を担保していくために国際的な基準に基づくアセスメントツールを採用する。一方で、MPTC では過去に数多くの類似のアセスメントを実施していることから、その時に得た情報やデータも可能な限り活用していくことで作業効率を高めて行く。また、研修計画の策定においては、職員の所掌業務に対する能力レベルを的確かつ効率的に確認していくために、JICA がベトナムで実施した類似案件で高い評価を得たスキルマッピングツールの一つ（SecBoK）を活用していくことを合意・決定している。さらに機材調達については、過去の JICA 類似案件における教訓を踏まえ、本調査期間中に MPTC 側とカンボジア国内における機材調達手続きや所要時間を確認し、調達機材のスペックの提出時期や調達予定の機材を用いた活動の実施時期を設定している。

成果 2 の活動では、サイバーセキュリティ能力の向上に向けた体系的な活動を通じた組織能力の向上に向け、成果 1 で作成するガイドラインやマニュアルを活用した活動を計画している。活動は他機関を対象とするものも含まれていることから、これらの成果品については、MPTC からの事前の内容

承認が必要となる。したがって、本調査期間中には、成果品の活用の道筋やタイミングをMPTC側と入念に確認した上で、成果品の円滑かつ迅速な承認手続きをMPTC側に要請した。

カンボジアでは、新年度は西暦どおりに1月に会計年度が開始するが、4月には新年の祝日、11月にはボートレースなどの大きな国民的行事があり、その時期は職員の動き、省内での活動が停滞する可能性が高い。そのため、多くのC/Pや他機関の関係者を巻き込む活動の実施や、上層部への決裁手続きが求められる活動については、できる限り上記の動きを配慮した形で各種投入のタイミングを設定した。なお、本調査時点で作成したPOは、2023年5月開始を想定したものであり、開始時期に変更が生じる場合には、適宜上記の政府・社会の動きを踏まえた形で修正していくことが求められる。

4-5　インパクト

本プロジェクトの実施により、想定される直接的及び間接的な効果は以下のとおりである。

4-5-1　上位目標（直接的効果）

3年間の協力終了後も、ICTセキュリティ局が協力期間中に技術移転を受けた知識やノウハウを継続的に活用していくことで、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のレジリエンスが強化されることが期待されている（上位目標）。そのためには、ICTセキュリティに関する政策の方向性に大きな変更が生じないこと、ICTセキュリティ局の責務と人員配置が維持されること、プロジェクト活動の成果がMPTC内で効果的に活用されること、サイバーセキュリティに関連する組織の関与が増加することが条件となる（外部条件）。

4-5-2　その他に期待される正のインパクト

本プロジェクトの実施により発現が期待されるその他の間接的なインパクトは以下のとおり。

- 成果3の活動を通じて作成した提言内容がカンボジアにおけるサイバーセキュリティに関する政策、法律、戦略、標準・基準等に反映・整備される。
- CII事業者を含む民間企業のサイバーセキュリティの強化につながる。
- 関係省庁においてCSIRTの体制やサービスが整備される。
- サイバー空間の安全性が高まることで、オンラインでの社会・経済活動が促進される。

4-5-3　ジェンダー・脆弱層へのインパクト

本プロジェクトの事業効果が継続的かつ発展的にカンボジア国内に波及していくことで、女性や子どもをはじめとする社会的脆弱層のサイバー攻撃やセキュリティリスクが軽減（低減）されるなどの波及効果が期待される。

4-5-4　負のインパクト

本調査時点で、本プロジェクトの実施により生じうる負のインパクトは認められない。

4-6　持続性

本プロジェクト効果の持続性は、プロジェクト完了後も一定程度確保される見込みである。

4-6-1　政策・制度面

情報通信技術セクターは、カンボジア政府の最高位の政策である「第 4 次四辺形戦略」及び「国家戦略開発計画（2019 年～2023 年）」において定められた 4 つの戦略の柱のうち「経済の多様化」を支える取組みの一つであり、本プロジェクトの方向性はこれらの政策との整合も高い。したがって、今後もカンボジアにおける政策路線が大幅に変更されない限り、プロジェクト完了後も効果の持続に向けてカンボジア政府からの政策面における持続性は担保される可能性が高い。ただし、現在 MPTC を中心に「サイバーセキュリティ法」及び「デジタル開発 2030 に関する国家政策」を起案中であることから、政策面において今後何等かの変更が生じる可能性も否めない。したがって、プロジェクト開始以降も当該分野における政府の政策動向には引き続き注意を払っていく必要がある。

4-6-2　組織面・人員体制面

CamCERT は 2007 年の設立以降、カンボジアにおける国家 CSIRT として位置づけられており、今後その位置づけが変更される可能性は極めて低いものの、今年中あるいは来年の早い段階で National Digital Economy and Society Council 下にデジタルセキュリティ委員会（DSC）が発足する予定であり、デジタルセキュリティ委員会（DSC）の体制や付与される役割によっては、CamCERT の所管が MPTC からデジタルセキュリティ委員会（DSC）へと移管される可能性もある。したがって、政策面同様、組織面においても今後のカンボジア政府側の動向を十分にモニタリングしていく必要がある。

人員体制について、本調査期間中に実施した MPTC との協議では、本プロジェクトを通じた CamCERT の機能の拡充と足並みを揃える形で人員体制についても強化を図っていけるよう MPTC 側の積極的な対応を要請した。プロジェクト開始以降も、人員体制の強化に向けた継続的な働きかけが求められる。

4-6-3　財政面

2021 年度までの過去 3 年の MPTC への予算配賦は 25 億円から 30 億円で推移しているものの、ICT セキュリティ局への予算配賦額は、新型コロナ感染症拡大の影響により活動費が大幅に削減されたことを受け、2021 年の同局向け配賦予算は前年度比の 58%まで減額されている。2022 年度の配賦予算においても同様の傾向が認められ、今後の予算増額の目途は立っていないことから、財政面においては極めて厳しい状況であるといえる。

前述のとおり、本調査時点で、「サイバーセキュリティ法」及び「デジタル開発 2030 に関する国家政策」が起案中であり、また、デジタルセキュリティ委員会（DSC）の設立準備が進行中であるなど、情報通信セクターは制度改革の過渡期であることから、プロジェクト開始後も引き続き MPTC の財政状況の推移をモニタリングしていくとともに、外部関係機関への財政支援の模索も含め、事業効果の財政面における持続性を確保していくための方策を MPTC 側と継続的に協議していくことが求められる。

4-6-4　技術面

ICT セキュリティ局は人事異動の頻度は高くなく、職員が退職しない限り事業効果の技術面における持続性はある程度担保できる見込みである。本プロジェクトでは、現状、基礎的なレベルに留まっている職員の技術・技能レベルを、プロジェクト期間中に数次にわたって実施する研修やドリルを通

じてさらに拡充していくことを計画している。習得した技術の持続性を担保していくために、本プロジェクトでは、専門家と C/P とが協働して各種マニュアルや手順書、SOP を策定する活動を盛り込んでおり、同活動を通じて個人レベルでの能力強化を図っていくとともに、作成文書の省内での利活用を促進していくことで組織内部での技術・ノウハウの面的拡大（組織力の強化）を図っていくことを想定している。

4-7　過去の類似案件からの教訓と本プロジェクトでの対応

4-7-1　類似案件の評価結果

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、情報セキュリティマネジメントシステム制定促進、技術研修、パイロット事業を通じた地方行政機関の Information Security Management System（ISMS）取得や、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、1) C/P の時間の確保、2) 事業成果の持続性確保に向けた対策の実施を類似案件への教訓として指摘している。2) の持続性の確保については、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～2010 年）、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～2008 年）、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～2016 年）に関する事後評価において、特に財政的・技術的な持続性を担保していくための事業実施期間中の取組みや対策の重要性を指摘している。

また、政策立案者及び技術担当者を対象とした研修の実施を通じ、サイバーセキュリティに関する品質管理・事前・事後対応能力の強化を図り、ベトナム政府全体のサイバー攻撃耐性の向上を目指した「ベトナム国サイバーセキュリティに関する能力向上プロジェクト（2019 年～2022 年）」の終了時評価報告書では、1) 資格試験に紐づく研修の実施、2) 研修に集中できる環境の整備、3）現地及び日本のリソースの使い分け、4) 機材調達プロセス等を教訓として導出している。

4-7-2　本プロジェクトでの対応

これらの教訓を踏まえ、本プロジェクトでは、詳細計画策定調査の段階で以下の対策を講じた。

- 一部の C/P 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ている。
- 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（CADT）の活用の可能性を探るべく、プロジェクト成果 1 の活動（1-7）において、MPTC 側と協議の場を設定している。
- 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、成果 1 及び成果 2 の活動を通じ、SOP やガイドライン等の作成も盛り込んでいる。
- 国際標準レベルの研修も含めた研修の実施を計画している。
- 詳細計画策定調査期間中には現地研修実施機関への調査を実施し、現地リソースについての基礎情報を収集しており、プロジェクト開始とともに、同調査で収集した情報を基に具体的なリソースの活用方法を決定していく。

- カンボジア国内での機材調達の現況に鑑み、調達機材を用いた研修等の活動は2年目以降の活動として計画している。

第5章 団長所感

- 要請元であるカンボジア郵政通信省（MPTC）・ICT セキュリティ局は、局長が過去の JICA 技術協力の C/P であることもあり、当時の成果を認識した上で、今回のプロジェクト活動や目的に対しても具体的なイメージを持っていた。そのため、同局は組織として体制面に若干の不安はあるものの、プロジェクト実施機関として信頼できると感じた。一方で、今後、政府のセキュリティ対策を一元的にリードしていくことが期待されるデジタルセキュリティ委員会（DSC）が設立されることから、現在の所掌が変更される可能性がある。国家におけるサイバーセキュリティを統括する組織が形成されることは望ましいものの、所掌範囲や組織構造を注視し、必要に応じてプロジェクト体制を適切に調整する必要がある。
- 成果 2 に関連して、当初「サイバーレジリエンス強化に向けた他省庁・CII 事業者とのネットワーク構築」という要請であったが、MPTC・ICT セキュリティ局は他省庁や CII に対して指示を出す法的権限がないことから、技術文書の普及という活動を通して関係性を強化することとした。国家のサイバーセキュリティ強化はサイバー防衛やサイバー犯罪捜査、産業関連等、幅広いアクターが相互に関連しながら行っている。サイバー空間における社会経済活動の基盤となるインターネット整備を担当し、防衛・犯罪捜査以外のサイバーセキュリティを所掌する MPTC の立ち位置を理解した上で、他省庁や CII に対して技術面で協力・支援することが重要である。
- 本プロジェクトは、グローバルアジェンダ「デジタル化の促進」の重点分野として設定されたクラスター事業戦略にかかるインドネシア、ベトナムに続く技術協力プロジェクトとして位置付けられている。本案件の活動、成果及びそれらの評価はクラスター事業戦略への重要なフィードバックとなることから、同事業戦略で設定された目標や評価指標を意識したプロジェクト運営を心掛けるべきである。
- 本プロジェクトと並行して外務省の無償資金協力による SOC 機材を供与する計画が進んでいる。ICT セキュリティ局が運用担当となる可能性が高いとのことであるが、SOC 運用体制には不安がある。大規模システムの導入にあたっては、ライセンス料や故障機材の修理等を含む維持管理について JICA には多くの教訓が蓄積されている。SOC 機材導入は本プロジェクトのスコープ外であるが、プロジェクト内において SOC 標準運用手順書の作成・普及にかかる活動や SOC 技術研修を実施する計画であることから、同供与機材が適切に運用維持管理されるように教訓を踏まえた上で、技術協力と無償資金協力による相乗効果が最大限得られることを目指すべきである。

添付資料 1：調査日程

Date		time	Meetings
22-Sep	Thu	9:00	Nakamura: Arrive to Phnom Penh
		PM	Docmentation
23-Sep	Fri	9:00	Meeting with MPTC/ Questionnair Collection/Interview
		PM	Documentation
24-Sep	Sat		Documentation
25-Sep	Sun		Documentation
26-Sep	Mon	8:00	Yamazaki/Nakajima: Arrive to Phnom Penh
		15:00	Meeting with SpaciaNet社
27-Sep	Tue	09:00-12:00	Meeting with MPTC/Department of ICT Security
		14:30	Meeting with proseth institute社
28-Sep	Wed	08:30-10:30	Meeting with MPTC/General Department of ICT (Head of Department)
		10:45-12:00	Meeting with ICT Security Department
		13:30	Meeting with Cambodia Academy of Digital Technology (CADT)
		15:30	Meeting with MPTC/General Department of ICT (Head of Department)
29-Sep	Thu	09:00-9:45	Meeting with Ministry of Economy and Finance, IT Department under General Secretary
		10:00-11:30	Meeting with Ministry of Interior ANTI Cyber crime department and IT Department
		15:30-17:00	Meeting with EZECOM (ISP)(CII Operator)
30-Sep	Fri	10:00-11:30	Meeting with Electricity of Cambodia(CII Operator)
		13:00	Meeting with Phnom Penh Water Supply Authority (PPWSA) (CII Operator)
		14:30-16:30	Meeting with MPTC/Department of ICT Security
1-Oct	Sat		Preparing M/M, PDM
2-Oct	Sun		Preparing M/M, PDM
3-Oct	Mon	09:00-12:00	Meeting with MPTC (confirmation of MM)
		14:00-15:00	Meeting with Forval Cambodia社
		16:00-17:00	Meeting with The Association of Banks in Cambodia
4-Oct	Tue	9:00-10:00	Meeting with MPTC (final confirmation of MM)
		14:00-15:00	Meeting with CamInfo Services社
		16:00-17:00	Meeting with JICA Cambodia Office
5-Oct	Wed	AM	Nakamura: Depart Phnom Penh (SQ 153) Yamazaki/Nakajima: Documentation
		18:25	Nakamura: Arrive Haneda Yamazaki/Nakajima: Depart Phnom Penh (SQ157)
6-Oct	Thu	8:00	Arrive NARITA

添付資料 2：主要面談者リスト

MPTC

月日	氏名	役職	部局
9 月 23 日	Mr. Kim Ann	Deputy Director	ICT Security Department
9 月 23 日	Mr. Tan Sopheak	Deputy Director	ICT Security Department
9 月 23 日	Mr. Bin Chamroeun	Deputy Chief	CamCERT
9 月 23 日	Mr. Chan Pheaktra	Deputy Chief	CamCERT
9 月 23 日	Mr. Phal Winna	Officer	CamCERT
9 月 23 日	Mr. Sok Sovan	Chief	Digital Forensics Office
9 月 27 日	Mr. Ou Phannarith	Director	ICT Security Department
9 月 28 日	Mr. Than NAKARA	Director	Department of ICT Infrastructure and Video Conference
9 月 28 日	Mr. Tan Opeak	Deputy Director	Department of ICT Infrastructure and Video Conference
9 月 28 日	Mr. Sokphath Ly	Deputy Director	Department of Contents and Application
9 月 28 日	Mr. Hor Pranet	Deputy Director	Department of Contents and Application
9 月 28 日	Ms. Yin Hootely	Chief Officer	Department of Contents and Application
9 月 28 日	Ms. Sodany Tan	Director	ICT Policy Department
9 月 28 日	Mr. Eang Kamrang	Director	ICT Industry Department
9 月 28 日	Mr. Tuon Soukvirak	Director	Rural ICT Department
9 月 28 日	Mr. Meas Sokchea	Deputy Director	Rural ICT Department
9 月 28 日	Mr. Preap Sovannarith	Deputy Director	Rural ICT Department
9 月 28 日	Mr. Hobm Thola	Senior Officer	Rural ICT Department
9 月 28 日	Mr. Vou Changeung	Officer	Rural ICT Department
9 月 28 日	Mr. Sen Dine	Officer	Rural ICT Department
9 月 28 日	Mr. Mok Khemera	Director	e-Government Department
9 月 28 日	Ms. Chea Lina	Chief	e-Government Department
9 月 30 日	Mr. Yim Sure	Deputy Chief of Office	Office of Norm, Control and Risk
9 月 30 日	Mr. Chan Raksmey	Chief	Office of Administration
9 月 30 日	Mr. Bin Chamroeun	Deputy Chief of Bureau	Computer Emergency Response Team
9 月 30 日	Mr. Chan Pheaktra	Deputy Chief of Bureau	Computer Emergency Response Team
9 月 30 日	Mr. Phal Winna	Officer	Computer Emergency Response Team
9 月 30 日	Mr. Chan Pheaktra	Officer	Office of Public Key Infrastructure
9 月 30 日	Mr. Ouk Visal, Officer	Officer	Office of Public Key Infrastructure
9 月 30 日	Mr. Sok Sovan	Chief of Bureau	Quality Assurance and Digital Forensic Office/ Office of Quality Assurance and Digital Forensic
9 月 30 日	Mr. Voeun Rath Sothanavath	Officer	Quality Assurance and Digital Forensic Office/ Office of Quality Assurance and Digital Forensic

CADT（MPTC）

月日	氏名	役職	部局
9 月 28 日	Ms. Nguon Somaly	Director General	CADT
9 月 28 日	Mr. Chea Vichet	Deputy Director General	CADT
9 月 28 日	Mr. Phan Daro	Director of GovTech	School of Digital Governance, CADT

Ministry of Economy and Finance (MEF)

月日	氏名	役職	部局
9 月 29 日	Mr. Iech Setha	Director	IT Department
9 月 29 日	Mr. Bi Nadin	Deputy Director	IT Department
9 月 29 日	Mr. Neau Vichetra	Deputy Director	IT Department
9 月 29 日	Mr. Lim Sileng	Deputy Director	IT Department
9 月 29 日	Mr. So Sokvibol	Chief	ICT Security Office
9 月 29 日	Mr. Sun Sokleng,	Deputy chief	ISO
9 月 29 日	Mr. Huoth Sophath,	Deputy chief	ISO
9 月 29 日	Mr. Seang Sanguarith	Deputy chief	PPO

Ministry of Interior（MOI）合計 9 名

月日	氏名	役職	部局
9 月 29 日	Col. Chhean Bunthan	Deputy Director	Anti-cybercrime Department
9 月 29 日	Maj. Rean Youda	Section Head	Anti-cybercrime Department
9 月 29 日	Brig Gen. Eat Tola	-	IT Department
9 月 29 日	Brig Gen. Nget Sokunthearith	-	IT Department
9 月 29 日	Brig Gen. Ly Vandy,	-	IT Department

Electricity of Cambodia

月日	氏名	役職	部局
9 月 30 日	Mr. Kan Thay	Director	ICT Department
9 月 30 日	Mr. Koamchuon Vichet	Deputy Director	IT Department
9 月 30 日	Mr. Mam Vuthy	-	Infrastructure security office
9 月 30 日	Mr. Cheung Sengngoun	Chief	ICT Admin officer

Phnon Penh Water Supply Authority (PPWSA)

月日	氏名	役職	部局
9 月 30 日	Mr. Oum Piseth,	Deputy IT Officer	
9 月 30 日	Mr. Vorng Chalavoan	Chief	Research and Development Section
9 月 30 日	Mr. Snown Sopheak	Chief	Infrastructure and Security
9 月 30 日	Mr. Tong Ponha Dethy	Member	Infrastructure and Development Section

民間企業: SpaciaNET Co., LTD

月日	氏名	役職	部局
9 月 26 日	Mr. Kora Va	CEO	SpaciaNET Co., LTD
9 月 26 日	Ms. Eang Huy	CEO Assistant	SpaciaNET Co., LTD
9 月 26 日	Ms. Chhech Houng SOY	General Manager	SpaciaNET Co., LTD

民間企業: Proseth Institute

月日	氏名	役職	部局
9 月 27 日	Ms. Veng Kanha	General Manager	Proseth Institute

民間企業：EZECOM

月日	氏名	役職	部局
9 月 29 日	Ms. Yuni Lee Heathcote	Chief Executive Officer	
9 月 29 日	Mr. Ashitha De Costa	Chief Information Officer	
9 月 29 日	Ms. Theng Tith Maria,	Manager	Legal & Contract
9 月 29 日	Mr. Ros Sophea, Director	Corporate Affairs	
9 月 29 日	Mr. CHEA Koemleng,	Head	Network and Design Architecture – on behalf of Director of Technical
9 月 29 日	Mr. Nuwan PERERA	Head	IT Infrastructure, Information Technology

民間企業: Foval Cambodia

月日	氏名	役職	部局
10 月 3 日	Takeharu Mizukosi	CEO	Forval Co., LTD

民間企業：The Association of Banks in Cambodia

月日	氏名	役職	部局
10 月 3 日	Mr. Trestew Kleine Buenc	CRO	ABA Bank
10 月 3 日	Mr. Thomas Schings	Head	Research
10 月 3 日	Ms. Cahn Sochinda,	Head	Business development
10 月 3 日	Mr. Sok Chan,	Head	Financial inclusion and public relations
10 月 3 日	Ms. Doung Sraynreh	Officer	Research Analysis

民間企業：Cam Info Cambodia

月日	氏名	役職	部局
10 月 4 日	Mr. Sun Socheat	President	Cam Info Cambodia
10 月 4 日	Mr. Sous Tidet	Managing Director	Cam Info Cambodia
10 月 4 日	Mr. Check Sophal	R&D Manager	Cam Info Cambodia