ベトナム国
情報通信省、情報セキュリティ局

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
（キャリア開発計画）

事業完了報告書

2022 年 2 月

独立行政法人
国際協力機構（JICA）

株式会社日本開発サービス（JDS）

ガ平
JR
22-033

目次

付録

表リスト

I. プロジェクトの基本情報

1. 対象国

ベトナム社会主義共和国

2. プロジェクト名

サイバーセキュリティに関する能力向上プロジェクト
（Project on Capacity Building for Cyber Security in Viet Nam）

3. プロジェクト期間（計画と実績）

計画： 2019年6月26日 – 2021年11月25日（30ヵ月）
実績： 2019年6月26日 – 2022年6月25日（37ヵ月）

4. 背景

独立行政法人国際協力機構（JICA）は、ベトナム社会主義共和国（以下、ベトナム）政府からの要請を受け、2017年10月1日から11月15日まで、技術協力プロジェクト「ベトナムにおけるサイバーセキュリティ能力強化プロジェクト」（以下、本プロジェクト）に関する協議のため計画調査チームを派遣した。 JICAは、2017年11月15日にベトナム社会主義共和国情報通信省（カウンターパート）とJICAとの間で締結された「事業詳細計画調査に関する議事録」に基づき、カウンターパート及び関係機関と本事業の詳細計画策定に向けた協議を重た。協議の結果、双方は2019年3月8日に署名された協議記録（R/D）に言及された事項について合意した。R/D署名後、2019年6月26日から2021年11月25日までを予定して長期専門家派遣により、本事業が開始された。

2020年8月14日の第2回合同調整委員会（JCC）において、2022年3月まで延長することが決定された。2022年1月に機器納入の遅れに伴い、カウンターパートとJICAは2022年6月までのプロジェクト期間延長を決定した。

なお、本報告書は2022年2月時点での情報をまとめた暫定版である。最終版はプロジェクト終了時（2022年6月）に発行されるものを参照されたい。

5. プロジェクト目標と上位目標

上位目標　　：ベトナム政府のサイバー攻撃耐性が向上する
プロジェクト目標　：AISのサイバーセキュリティ能力が強化される

6. 実施機関

情報通信省　　：Ministry of Information and Communications (MIS)
情報セキュリティ局：Authority of Information Security (AIS)

II. プロジェクト実績

1. プロジェクトの実績

1-1 日本側の投入

(1) 日本側の協力金額：31,900万円

（計画額：15,300万円）

(2) 専門家派遣：2名

- 長期専門家：1名
- 短期専門家：1名（他の専門家は日本から遠隔支援）

(3) 研修生：646名

研修種別	研修実施数	受講者数
現地研修 合計	77	635
（資格関連研修）	(52)	(333)
（カスタム研修）	(25)	(302)
本邦研修：日本	1	2
本邦研修：リモート	8	13
第三国研修（インドネシア）	1	2
合計	87	652

* 本邦研修（オンライン、オンサイト）は、本プロジェクトが独自に企画・実施する研修ではなく、JICA または日本政府が実施する研修。本プロジェクトのカウンターパートスタッフが優先的に参加した。

* インドネシアでの研修は同国で実施中の「サイバーセキュリティ人材育成プロジェクト（2019 年 5 月 22 日～2024 年 5 月 21 日）の活動に関連する第三国での研修。

(4) 供与機材：7,800万円

- DDoS攻撃防御システム
- マルウェア解析システム
- 国際規格コモンクライテリアに準拠した支援実習用機器

(5) 現地運営費用：12,800万円（現地研修：9,200万円、現地費用：3,600万円）

主な用途：現地プロジェクトスタッフ、普及啓発教材の開発、現地トレーニング、ISAC調査、Common Criteria運用支援用機材、など。

1-2 ベトナム側の投入

(1) 主要なカウンターパート：6人

- プロジェクト・スーパーバイザー：情報通信省　副大臣1人

- プロジェクトディレクター：情報セキュリティ局　局長1人
    - 2020年2月に局長は変更された。
- 副プロジェクトディレクター：情報セキュリティ局　副局長1人
    - 副局長は、2021年11月に他のポジションに移動した。2022年1月末現在、同ポジションは空席。
- 連絡窓口（POC）：法務監査課3人

(2) 事務所等の提供：プロジェクト事務所、施設、水道、電気、インターネット等。

(3) その他ベトナム政府の負担：0 ベトナム・ドン

1-3 プロジェクト活動（計画と実績）

活動1-1.（成果1）

SecBoKのフレームワークに定義された役割（ロール）のうち必要とされるものを明らかにする

2017年に行われた計画調査では、SecBokの19ロールを高・中・低の3段階の重要度に分け、そのうち高・中に振り分けられた14ロールに該当するAIS職員をCDPの対象とする方針が示された。ところがプロジェクト開始直後に行ったAIS職員の面談の結果、主要14ロールでは多くの取りこぼしが発生することがわかり、結果としてSecBok19ロールに3ロールを加えた計22ロールでのCDP運用を開始した。次の表はこの分類を示すものである。結果的にこの表に掲載したすべてのロールを対象とした。

表 1　ロールの分類

SecBok 高・中分類 14 ロール	CISO, Commander, Triage, Incident manager, Incident handler, Vulnerability diagnostic consultant, Information security auditor, POC, Curator, Researcher, Solution analyst, Self assessment, Forensic engineer, Investigator
SekBok 低分類 5 ロール	Notification, Education / Awareness raising, Legal advisor, IT planning division, IT system division
追加 3 ロール	Licensing, Policy making, SOC (Security Operation Center)

なおSecBokで定義されたロールは、部門レベルでの対応にはほぼ問題ないものの、組織内の個々人の役割を対応付けるには粒度が大きすぎ、適切な研修を割り当てる上で改善が必要との意見がある。この点に関してキャリア開発計画の短期専門家がCDPマニュアル内に検討と提案を掲載しているので参考にされたい。本プロジェクトでは上の表に示したSecBokをベースとした22ロールでの運用を行った。

活動1-2.（成果1）

SecBoKのフレームワークに基づき、それぞれの職員のCDPを策定する

2019年8月からAIS職員の個人面談を開始し36名分のCDPを作成した。その後11月に

VNCERT/CCがAISに統合されて対象範囲が広がった結果、2019年末までに67名の職員の面談とCDP作成を行った。AISではその後も職員採用が積極的に行われたことにより、対象人員はプロジェクト終了時点で106名にまで増加した。以下の表に、この対象人員増の経緯をモニタリングシートのタイミングと共にまとめる。

表 2　職員面談数とCDP作成数の推移

モニタリングシートのバージョン（時期）	面談実施数	新規 CDP 数	累積 CDP 数	CDP 対象人数
Ver.1 (as of 30th December 2019)	67	67	67	**67**
Ver.2 (as of 30th June 2020)	25	25	(no data)	**80**
Ver.3 (as of 30th December 2020)	16	16	(no data)	**88**
Ver.4 (as of 30th June 2021)	20	20	(no data)	**106**
Ver.5 (as of 31st December 2021)	0	0	144	**106**
Project Completion Report (as of 30th October 2021)	0	0	144	**106**

累積CDP数とCDP対象人数の差は退職者の数に相当する。

なお「CDP作成」とは、面談の結果をExcelによるCDPフォーム記入することである。実際のCDPフォーム（記入済み例）を付録に添付する。またCDPフォームへの記入項目を次の表にまとめる。

表 3　CDP記入項目

CAREER DEVELOPMENT PLAN	
1	Division & Title
2	Job Description, Responsibility
3	Assigned Security Role(s)
4	Required Knowledge and Skills for the Roles (General description)
5	Knowledge and Skills to be acquired or improved
6	Training plan, progress and result
	Course Title, Couse Code, Vendor, Course Provider, Planned Month Attending Date, Number of Hours, Certification, Progress, Remark
PROGRESS REVIEW	
1	Review 1
2	Review 2
3	Review 3
4	Review 4

なお100本以上のExcelファイルからなるCDPを更新・保守するのは容易ではないため、それらを集中管理するためのCDPデータベースの作成・運用も行った。CDPデータベースの詳細は別途作成のCDPマニュアルに記載する。

活動1-3, 2-1, 3-1.（成果1,2,3）

SecBoKのフレームワークに定義された役割（ロール）のうち優先度の高いもの（例：CISO／最高情報セキュリティ責任者、コマンダー）の研修コースを計画する

プロジェクト開始当初は対象者のCDPに記載されたSecBokロールに従い、要求されるKSA

（Knowledge-Skill-Ability）を満たす研修を割り当てることを想定していた。しかしながら実際の運用においては、活動1-1.（成果1）で述べた通り、SecBokで定義されたロールは、部門レベルでの対応にはほぼ問題ないものの、組織内の個々人の役割を対応付けるには粒度が大きすぎて適切ではないという問題に直面した。この問題には以下に示す2つの側面がある。

1) 例えばEducation / Awareness raising のカテゴリーでは、サイバー演習を企画・開発する職員にはサイバー攻撃の攻守に亘る高度な知識とインフラ構築技術が必要だが、一方でChild Online Protectionを担当する職員にはそのような専門技術より、メディア戦略や学校教育に関する知識が求められる。つまりEducation / Awareness raisingのカテゴリーがカバーする範囲が広すぎて、個々の職員に必要な知識・技術を特定できない。

2) 一人の職員に割り当てられる職務は複数のSecBokロールとなることが多い。例えばある職員はIncident handler、Vulnerability diagnostic consultantおよびForensic engineerの3つのロールを持つが、これらをKSAベースで研修にマッピングすると、ほぼ全ての商用コースを受講することになる。これはSecBokロールの粒度が大きく、各ロールに対応するKSAの量が多いためである。

このような問題に対処するため、本プロジェクトではSecBokロールの他に、以下に示す項目を面談により明確化し、CDPに含めることで、各職員の研修計画作成時の参考情報とした。

- Job Description, Responsibility
- Required Knowledge and Skills for the Roles (General description)
- Knowledge and Skills to be acquired or improved

すなわち本プロジェクトでは各職員の研修計画の根拠を、SecBokロールと、個人別の職務およびスキル分析とした。なおこの手順をより明確かつ論理的に行う方法として、研修計画の根拠をSecBokの元となったNICEフレームワークに求めるべきとの検討がキャリア開発計画の短期専門家によりなされている。この結果は別途作成のCDPマニュアルにまとめられる予定である。

活動1-2, 2-2, 3-2.（成果1,2,3）

研修を実施する

プロジェクト期間中に研修87回実施した。総じて予定通りに研修が終了しており、効率性は高いといえる。実施した研修の詳細は付録を参照。

活動1-5, 2-3, 3-3.（成果1,2,3）

CDPをレビューする（例：6ヶ月毎）

計画したレビューの手順は以下の通り。プロジェクトチームは計画通り半年に一度、CDPレビューを行っており、CDPレビュー活動の効率は高い。

1) 事前アンケートと対象スタッフの上司へのインタビュー
2) CDPの更新と研修計画の修正

CDPレビューの実施期間と対象者数は以下の通り。

表 4　CDPレビューの実績

CDP レビュー	機関	対象者数	備考
1st review	May – June 2020	57	最初のレビューまでに1人の職員が退職した。
2nd review	November 2020 – January 2021	82	-
3rd review	May – July 2021	82	当時のレビュー時に、離職や昇進により対象外となった職員は10名。
4th review (Final)	29th November 2021 – 29th December 2021	104	-

以下からの表は、CDPレビューで対象スタッフへの質問に対する回答をまとめたものである。

- **前回面接時からの職務内容や日々の業務内容の更新状況**

レビュー時期	変化なし	変化あり	合計	備考
1st review (2020)	16	41	57	2019 年 11 月に VNCERT/CC が AIS に所属することになった後も、組織再編は現在も進行中である。各人の業務内容の変化の詳細は資料に記載していないが、スタッフの役割や業務内容は常に変化していることがわかった。CDP レビュー時に役割・業務の見直しを繰り返し、スタッフの状況の変化に応じた教育を行うことが重要であると考える。
2nd review (2021)	46	27	73	部署内での役割が増えた、スタッフの役割が変わった、担当業務が増えた（ただし同じポジション）等
3rd review (2021)	68	14	82	部署内での役割が増えた、スタッフの役割が変わった、担当業務が増えた（ただし同じポジション）等
4th review (final)	95	9	104	更新の例は以下の通り。 • 秘書課（省令室)、副大臣秘書課 • 前回のインタビューから日々の業務が増え、業務でもプロジェクトに参加することが増えた。 • ソフトウェア、セキュリティソフトのソリューション、アーキテクト • 事業部の副課長 • 2022 年から実システムでの訓練と地方や組織での CSIRT の成熟度評価に関連するサービス活動をより多く展開している。 • 地域における情報セキュリティサービスの総合的な管理や展開

- **日々の業務や役割に応じた課題**

	No challenge	Have challenges	合計	備考
1st review (2020) ( ) shows the answer of superiors	22 (1)	35 (13)	57 (14)	ほぼすべての部門が、それぞれの業務に特化した課題を抱えている。課題がないと回答した部門は、NCSC（National Cyber Security Center）のインシデントモニタリング部門。 しかし、インタビューでは監視やインシデント対応能力の向上の必要性を訴えていることから、インタビュー対象者（部門長）は同部門の能力不足を認識しているものと思われる。注意すべきは、全ての部門が能力不足を認識していることである。プロジェクトは、これらの課題に対応するために適切なトレーニングを提供する必要がある。
2nd review (2021)	61	12	73	コメントの多くは、人材やスキルの不足を指摘することであった。プロジェクトでスタッフの増員を促すことはできないが、プロジェクトで実施している CDP を使った体系的なトレーニング方法を今後も AIS に提供することを確認。
3rd review (2021)	59	23	82	ソフトウェアアーキテクチャ、ダナン・ホーチミン市を中心とした人材配置・育成、国際・国内規格に則った認定スキル、新領域でのポリシー設計の難しさ、インターネット上での子どもの保護、外国語、サイバーセキュリティ演習のシナリオ立案、Web アプリケーションペンテスト、モバイルアプリケーションペンテスト、フォレンジックス
4th review (final)	85	19	104	課題の例は以下の通り。 • サイバーセキュリティにおける英語 • マルウェア解析 • より効果的に仕事をするための知識と計画 • 知識が浅い、経験が浅い • サイバーセキュリティ/情報セキュリティの知識不足 • ソフトウェアアーキテクト、システムアーキテクト • CTF LAB の構築 • 政策立案経験 • ワークマネジメントスキル、コラボレーションスキル、定量分析スキル、ネゴシエーションスキル、パブリックスピーキングスキル、総合的なスキル • 情報セキュリティ、データ保護分野の規制や政策についての情報不足 • 検査、セキュリティ評価に関する知識 • リモートサイトでの作業 • ウェブセキュリティに特化した業務 • 一般的なスキル

- **研修の効果と行動変容（研修生向け）**

	Improved	Negative effect	Not feel	Don't know	合計
1st review (2020)	30	0	9	1	40
2nd review (2021)	56	2	7	8	73
3rd review (2021)	67	4	6	5	82
4th review (final)	重複を許した回答なので、以下の表を参照				104

- 第2回CDPレビュー

研修の結果、日常業務おいての負の影響を感じたと選んだ2名の理由は以下の通りである。

- 研修の内容が優れておらず、確かな自信に結びつかなかった。
- PMP研修では、もっと実践的な内容を期待した。

- 第4回CDPレビュー

1	**Become more confident**	57
2	**Broader scope of work**	33
3	**Career path becomes clear**	30
4	Better recognition by supervisor	12
5	Promoted	7
6	Nothing has changed	7
7	Have negative impact	2

- **研修に参加して、仕事に対する姿勢や考え方がどのように変わったか？**

第2回、第3回CDPレビューのコメントより、多くの受講生は研修によりセキュリティ技術・英語・プロジェクトマネジメントの知識を得ただけではなく、彼らの業務へも応用している姿勢が見受けられた。（詳細は付録参照）

- **（第4回レビューでの質問）今後の講座・資格取得に関する要望**

- メディア・コミュニケーションコース
- プログラム/プロジェクトマネジメント、プロジェクトマネジメントプロフェッショナル（PMP）
- マルウェア解析
- ソフトウェアエンジニアのキャリアパスに向けたコース
- リーダーシップスキル
- ITやサイバーセキュリティに関する英語コース
- 情報セキュリティポリシー
- ISC2認定情報のCISSP
- EC-Councilのコース（CEH、CHFI、CNP）
- SANS （GREM - GIACリバースエンジニアリングマルウェアコース）
- Offensive Securityコース（OSWE、OSEP、OSED）
- クラウドセキュリティ：GIACクラウドセキュリティオートメーション／ISC2認定クラウドセキュリティプロフェッショナル（CCSP）

- **（部門長への質問）研修に参加した後、部下の仕事に対する姿勢や考え方に変化はあったか？**

1回目のレビュー時は各研修生から回答を得たが、2回目レビュー以降はそれぞれの上司から得た回答となる。

	Improved	Negative effect	Not feel	Don't know	合計
1st review (2020) ( ) 内回答は上司による	30 (30)	0 (0)	9 (4)	1 (1)	40 (35)
2nd review (2021)	11	1	0	0	12
3rd review (2021)	10	2	0	0	12
4th review (final)	17	1	0	0	18

- **（第4回レビュー時の質問）プロジェクト終了後も、CDPに基づく研修計画手法を使い続けたいか？**

Yes	95
No	9
合計	104

得られた理由は以下の通り。

[Yes]

- キャリアパスが明確になり、仕事に必要な知識や資格を効率的に取得できた。CDPは自分のキャリア開発計画を描き、追跡するのに役立つツール。CDPを使った研修はスキルや経験を向上させるためのロードマップとして適しているから、自分のキャリアパスの基礎を築くのに最適な方法だった。
- トレーニングコースは非常に有用であり、ビジネスや組織の発展に大きな役割を果たした。必要なスキルを向上させるのに役立っている。トレーニングコースが日々の業務に役立っている。サイバーセキュリティに携わる職員が段階的に向上させるべき知識やスキルの必要性を全体的に把握することができるから。
- 年間を通じて、自分の成長を確認することができた。
- このプロジェクトは、AISの人材育成の質を大きく向上させるものであった。このプロジェクトがもっと広がることを願っている。CDPを活用した研修企画手法は、社内研修にも活用できる。
- 英語を使う機会があり、サイバーセキュリティやプロジェクトの管理方法について練習し、学ぶことができたから。

[No]

- 知識向上のために割く時間的な余裕は今のところない。
- 日常業務が経理なので、それだけを学べばよい。
- 学習経路が不明確で、フィードバックは基本的に形式的なものである。
- 研修が基本的なことのため、業務には役立たない。

- **（部門長への質問）CDPについてどう思うか？組織や経営に役立っているか？**

	Yes, it is useful but need improvement	Yes, it is useful very much.	合計
1st review	8	6	14
2nd review	1	11	12
3rd review	1	11	12
4th review (Final)	15	3	18

- **CDP方式を改善するためのアイデアはあるか？**
  - コースはどれも研修生一人ひとりの学習ニーズに沿っており、とても良い。ただ、学習時間がもう少し延長されれば、より効果的だと思う。
  - トレーニングコースの時間をもっと長くし、バッチに分けることで、生徒がよりよく知識を把握できるようになる。
  - CDPはすでにかなり効果的な方法だと思う。このCDP方式は、研修の方向性やスキルアップを管理するのに便利で優れている。今のところ、これ以上改善すべき点はありません。
  - ベトナムにおいても、日本やアメリカのようにSecBoKのような国家レベルのセキュリティの知識体系を構築すべき。
  - より実践的なコース。

活動1-6.（成果1）

政策策定者に対する研修を計画・実施する

プロジェクト開始以降に実施された政策立案関連講の研修は以下の通り。

表 5　政策策定に関連する研修

No	コース名	日程	場所	内容
1	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	2020 年 1 月から 2 月	オンサイト（日本）	日本の政策や戦略
2	日本の省庁および大学によるサイバーセキュリティ政策策定に関するオンラインセミナー	2021 年 7 月 19 日から 21 日	オンライン	日本の政策や戦略
3	普及啓発オンラインセミナー	2021 年 8 月 30 日から 9 月 1 日	オンライン	普及啓発、COP
4	課題別研修（上乗せ）: 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	2021 年 10 月 25 日から 11 月 3 日	オンライン	日本の政策・戦略、インターネット・サイバー空間ガバナンス、国連の 11 行動規範等

活動1-7.（成果1）

啓発教材を開発、ローカライズする

普及啓発に関する活動は、アニメーション動画制作、ポータルサイト開発、ブランディングキット（デザイン）開発、専門家による日本の調査研修・コンサルティングに分かれている。

1) 動画制作

プロジェクト期間中、以下のような青少年・子ども向けアニメーション映像が制作された。

- 1本目

Theme	Staying vigilant with strangers in virtual space, especially on social media
Target	Children studying in secondary schools (from 11 to 14 years old)
Duration	180s
Creation company	KYX
Quality	Full HD (1920x1080)
Development Term	August 19th 2020 – December 9th 2020

- 2本目

Theme	Save the Children on Internet
Target	Children studying in primary schools (from 6 to 10 years old)
Duration	180s
Creation company	DeeDee
Quality	Full HD (1920x1080)
Development Term	December 28th 2020 – 23rd March 2021

- 3本目

Theme	Introduction an Online Contest of Information Security for students
Target	Children studying in secondary schools (from 11 to 16 years old)
Duration	Full version (max 180s) Short version (~1 min)
Creation company	DeeDee
Quality	Full HD (1920x1080)
Development Term	3rd May 2021 – 14th June 2021

2) ブランディングキット

AIS、公安省、教育訓練省、労働・障害・社会省などの関連省庁や多くの国際・非政府組織の協力により設立されているベトナム児童オンライン保護（VN-COP）ネットワークを、信頼できるコミュニティとし、このコミュニティを子供とその保護者が簡単に、すぐに認識できるようにすることをAISは目指している。VN-COP Networkを信頼できる場所にすること、そしてVN-COP Networkを子どもたちや保護者が簡単に、すぐに認識できるようにすることを目的として、以下のようなVN-COP Networkのブランドキットを開発した。

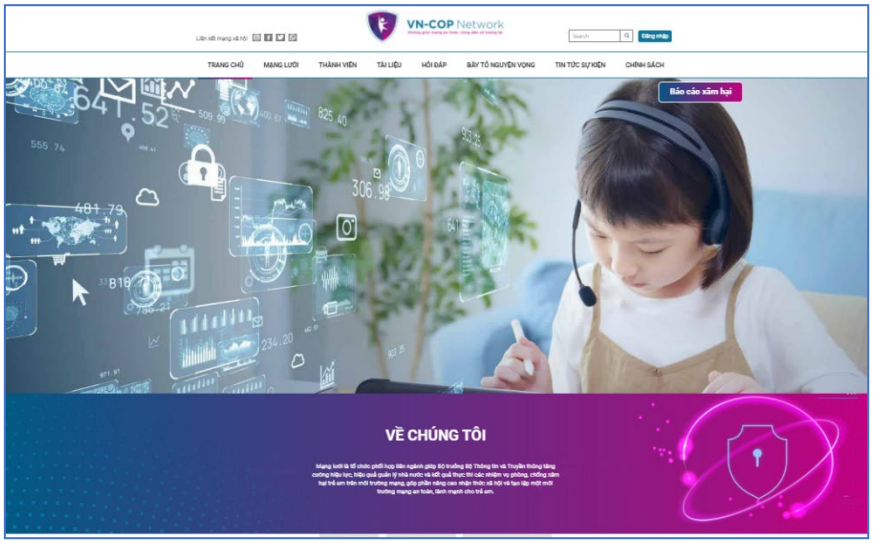
- ブランドキットのコア部分　：ロゴマーク、ウェブサイトテンプレート、ソーシャルメディア、スローガン、ユニフォーム
- ブランドキットのオフィス活用　：証書、名刺、便箋、封筒、ファイルフォルダ、スライドテンプレート
- ギフトセットデザイン　：VN-COP Networkのロゴ入り記念メダル・バッジ、その他記念品

3) ポータルサイト開発

本プロジェクトでは、2021年4月から6月まで、COPポータルサイトの開発に関するコンサルティングとAISとのシステム要件の協議を行った。その結果を受けて、現地企業SolidTech社と協力して、アジャイル方式により以下のサービスを備えたポータルサイトを開発した。

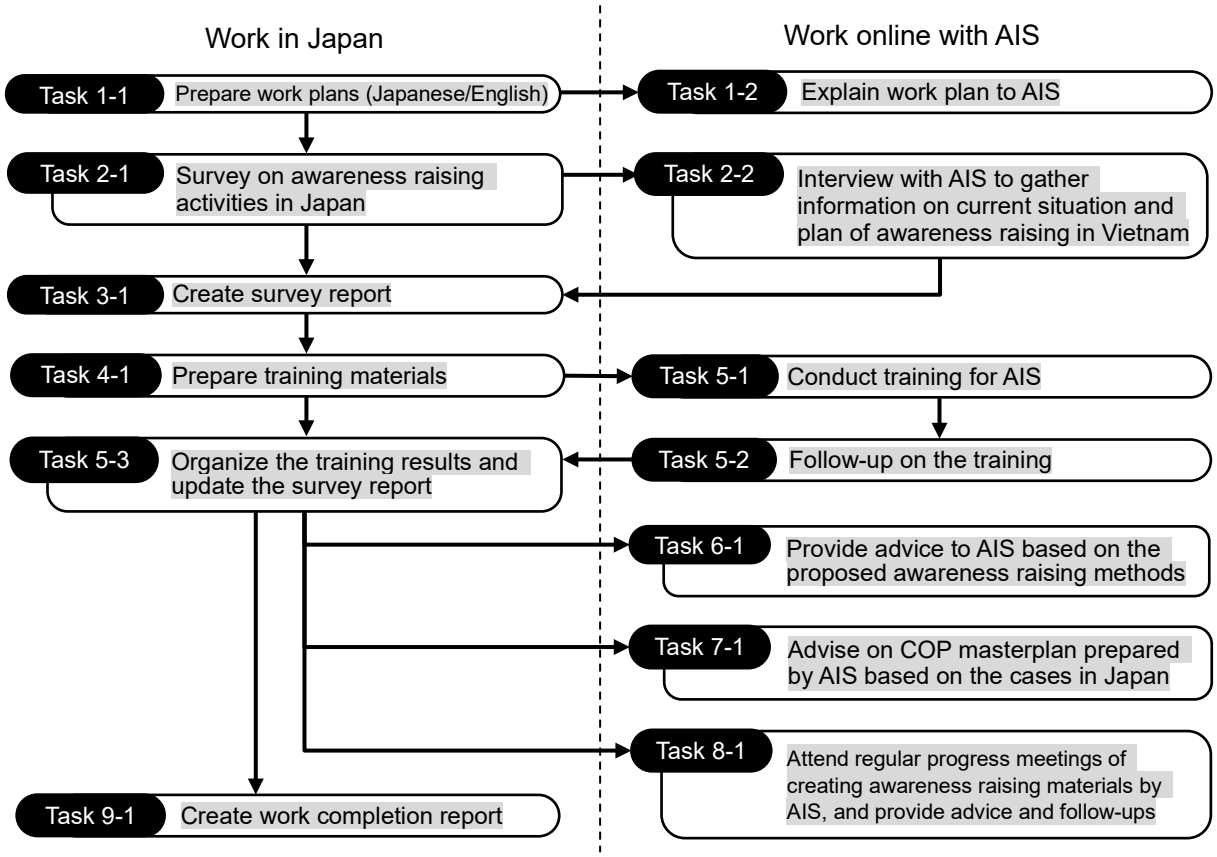
1）登録、2）法律文書公開、3）質問・問い合わせへの回答、4）フィードバックと要望受付、5）ニュースとイベント情報の公開、6）ユーザー情報保護方針（AISポリシー設定）、7）レポーティング

URL: https://vn-cop.vn/



4) 普及啓発専門家による活動

2020年8月の第2回JCCにおいて、当初のPDMの枠組みは変えずに、活動「1-4. 研修を実施する」、「1-7. 啓発教材を開発、ローカライズする」に専門家の活動を追加した。日本におけるサイバーセキュリティの普及啓発活動と、その活動を推進するために必要なマーケティング手法の調査を行った。この調査結果を報告書にまとめ、AIS職員向けに実施した研修の教材とした。また、研修の結果を踏まえ、専門家チームは追加調査のフォローアップとAISへ提言を実施した。 当初はベトナムのプロジェクトサイトを訪問する予定であった。しかし、COVID-19の影響で、現地での活動はすべて、プロジェクトサイトと日本の啓発専門家をつなぐオンライン活動に変更することになった。



- **タスク1-1　ワークプランの作成（日／英）**

JICA本部、チーフアドバイザー、短期専門家、長期専門家から本プロジェクトに関する情報を入手し、ベトナム政府のサイバーセキュリティに関するこれまでの取り組みや本プロジェクトの活動全般を把握し、日本語と英語で作業計画を作成した。日本語版はJICAに提示・説明し、承認を得た。

- **タスク1-2　AISへの作業計画の説明**

- **タスク2-2　ベトナムにおける現状と啓発計画の情報収集のためのAISへのインタビュー**

2021年7月30日にオンラインミーティングで、作業計画の説明とAISへのヒアリングを同時

に行った。

Date & Time	July 30th, 2021 9:00-11:00 (Vietnam time)
Participants	AIS: 7 including Deputy Director General JICA: 3 including 1 awareness raising expert
Main Points	• Work plan was explained and AIS side agreed with the content of plan • AIS side explained about the current status of master plan 2020-2025 that includes awareness activities scheme. • The strategy has 3 focuses: 1. Mass media channel where they believe most of the youth are landing as targets. 2. Fostering the domestic products and services serving the creative cyberspace for children 3. Developing the educational materials and implementing such stuffs into the school system • Facebook Messenger, Viber, Instagram, Zalo are popular instant message app in Vietnam. YouTube is still popular besides the social media, especially for the children, but they cannot judge whether the content is good or bad without support from the parents. • IT subjects are integrated in the current educational curriculum but the influence of massive information from SNS is overwhelming. From the scheme of Child Online Protection (COP), the target of communication should not only be children, but also their parents. Hotline is needed for children because children may not prefer to directly talk to their parents. • Vietnam is trying to establish the COP network including the schools as a top-down method. This network is not only for the school system, but also for the parents, children themselves and front-line staffs (social services employees). • There is very limited cooperation between Government and private sectors in Vietnam. However, the scheme is also trying to foster the domestic products and services toward the children. • The current master plan approved by the Prime Minister last year mentions about the 64 provincial Government to take their responsibility. Inside MIC, they have also got the monitoring plan to follow up the strategy. • As for the content of planned training, the proposed plan is fine. AIS would like to know the “know-how” of applying the Japanese policy in daily operation of awareness raising. For the education materials, it seems the animations are strong advantages, for example. It would be helpful if there is some content about prevention of child abuse.

- **タスク2-1　日本の普及啓発活動に関する調査**

研修教材開発のため、日本における普及啓発活動に関する情報を調査した。これらの情報源は、調査報告書にまとめられた。

- **タスク3-1　調査報告書の作成**

上記の調査で得られた結果を整理し、統計的手法を用いて数値情報を分析し、英文の調査報告書を作成した。

- **タスク4-1　Prepare training materials**

英語での調査結果をもとに、研修資料を作成した。これは調査結果で判明した日本語の普及啓発・教育資料の入手先などの参考情報を網羅した資料となっている。

- **タスク5-1　Conduct training for AIS**

2021年8月30日から9月1日の3日間、上記活動で開発した教材を使用し、オンラインで研修を実施した。参加者はAISのスタッフ11名であった。本セミナーの目的は、これらの教材の活用に関連し、以下を目的としたものであった。

- 日本での普及啓発活動の経験を理解し、ベトナムに適用できる教材や活動を検討すること
- サイバーセキュリティに関する普及啓発活動にマーケティング理論を適用する方法を学ぶこと

各日の研修の最後には質疑応答が行われ、翌日へのフィードバックに努めた。参加者からの質問・要望で追加調査が必要なものは、次項のフォローアップ活動で回答した。

- **タスク5-2　研修のフォローアップ**

研修期間中、参加者から下記のような追加情報・内容の要望がいくつか出され、専門家が追加情報・資料を作成した。これらの追加情報は、教材の更新や調査報告書の更新に反映された。

- サイバーセキュリティ普及啓発にかかる日本の国家予算
- 研修で紹介された情報へのリンク集
- IPA「サイバーセキュリティお助け隊サービス制度」詳細情報

- **タスク5-3　研修結果の整理と調査報告書の更新**

研修で得られたフィードバックや、その後のAISとのオンラインディスカッションの結果を踏まえ、専門家による研修結果の整理と調査報告書の更新を行なった。

- **タスク6-1　提案した普及啓発方法に関してAISへアドバイスを提供**

研修で指導した効果的な普及啓発活動のための理論や戦略をもとに、9月29日のフォローアップ・オンラインミーティングで、今後の啓発活動に必要な提言を以下のように行なった。

Date & Time	September 29th, 2021 11:00-12:00 (Vietnam time)
Participants	AIS: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert team has provided advice on the following topics. • The 4th awareness raising video • Development of branding kit • Development of COP portal site AIS and JICA team has discussed on the following topics. • Plan to support COP master plan – Draft is available in early October 2021 • Extended support from awareness raising experts until January 2022

- **タスク7-1　AIS作成のCOPマスタープランに対する日本の事例を元にしたアドバイス提供**

2021年10月8日にAISからCOPマスタープラン案を受け取った。専門家はそれに対して様々なコメントや提案を行い、コメント附与してAISに返送した。AISは、次回の会議（後述）において、コメント・提案を検討し、適切に対応すると返答した。

- **タスク8-1　AISとの定例進捗会議における普及啓発に関するアドバイスとフォローアップ**

専門家チームは以下の定例会議に出席し、AISの啓発活動に関するアドバイスやフォローアップを行なった。各会議では、AISから日本での追加情報についての要望や、活動への提言がいくつか出された。

Regular meeting with AIS on awareness raising activities #1

Date & Time	November 5th, 2021 11:00-13:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	Review of the COP masterplan (The expert has already sent commented version before). • The expert recommended to add "Child emergency call" telephone number as well as email/SNS contacts like in Japan. • Vietnam has the 111-call center for similar purpose, but people do not remember well about it. Regarding cybersecurity education contents • Since there is no cybersecurity education in Vietnam, AIS is looking for the focused and consolidated contents for awareness raising of each target age group. • Three content types in Japan now: message based, storytelling based and case study.

Regular meeting with AIS on awareness raising activities #2

Date & Time	December 6th, 2021 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent a material containing the answers to the request made in the previous meeting ("Information Moral Education - Model Curriculum"). • Enhancing the management ability is the answer for the question about how to manage many tasks with limited time and resources. • It is hard to create KPI for evaluating contents for each target age group. The expert created sample CyberSec KPIs so it would be a reference. • Evaluation should be done hired consultant company, but it does not have to be expensive foreign consultants.

Regular meeting with AIS on awareness raising activities #3

Date & Time	January 6th, 2022 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent a material (before the meeting) containing the answers to the request made in the previous meeting ("Government control on applications for children in Japan"). • There is no government control on applications for children in Japan, but some industry associations do the screening. • AIS is aiming to establish the criteria to evaluate the application, games to ensure the child protection policy. Game rating or equivalent criteria is supposed to be issued by Government, but the actual evaluation may be done by other entity. Such request is to protect children from abusive activities via the reporting system. • No update for COP masterplan Questions of AIS to the experts (to be answered in the next meeting) • Is there any fee required for evaluation from the organization such CERO? What is their evaluation criteria? Who will do the evaluation? • Is there any example of evaluation criteria (such as checklist or template) in Japan that can be obtained? • Recently, VNCERT/CC has been assigned more tasks about the communication e.g., YouTube and FB channel to gain 100,000 followers/subscribers for each channel. How to do that with the limited budgets? Now they have the support from Google, but they are looking for the expert's support to build such plan as adapting KPIs.

Regular meeting with AIS on awareness raising activities #4

Date & Time	January 24th, 2022 14:00-15:40 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert team prepared and sent a material containing the answers to the requests made in the previous meeting (updated version of "Government control on applications for children in Japan", presentation on how to design KPI for reaching 100,000 followers/subscribers). • CERO is for game evaluation only, but how should we control PC applications? • There is no rating system for general application in Japan except for some. There are filtering software for mobile phone, but kids tend to bypass it. The expert did comprehensive presentation on how to reach 100,000 followers/subscribers including analysis of existing YouTube videos on COP in Japan and the setting up of KPI.

- **タスク9-1　作業完了報告書の作成**

すべての活動結果を作業完了報告書にまとめて、JICAに提出した。

活動2-3.（成果2）

事後対応基幹設備（例：DDoS攻撃緩和、マルウェア解析）が拡張される

活動2-3,3-4を通して本プロジェクトで供与した機材の総数は以下の通り。

パッケージタイプ	ハードウェア数	ソフトウェア数	合計
DDoS 攻撃防御システム	98	0	98
マルウェア解析システム	29	52	81
CC 評価システム	19	3	22
合計	146	55	201

※ JPCERT/CC による提供された TSUBAME センサーのソフトウェアは、
本プロジェクトの直接の活動ではないため、上記には含まれていない。

活動2-3では、事後対応基幹設備として、DDoS攻撃緩和システムおよびマルウェア解析システムを調達した。

- **DDoS攻撃緩和システム**

2021年3月13日にDDoS攻撃緩和システムに関連する機器（サーバー、ネットワーク機器、付属品）が納入された。これらの機器により、最大で約75GbpsまでのDDoS攻撃に対応できるようになることが期待される。2021年11月3日にプロジェクトチームはAISのオフィスとサーバールームを訪問し、それらが適切に設置されているかどうかを確認した。その時点で、74.5%（73/98）の機器が使用されていることを角煮員して、設置機器の運用管理状況に問題はなかった。なお、すべての機器の設置・運用が完了していないため、AISでは早急に運用を開始する予定である。

- **マルウェア解析システム**

2020年8月2日の第2回JCCにおいて、プロジェクトの延長に伴い、マルウェア解析機器のリストに機材が追加された。更新されたマルウェア解析システムの機器リストを含むプロジェクト文書が2021年7月16日に承認された。当初は2020年中の調達開始予定であったが、この承認を受けて数か月遅れて調達が開始された（2021年11月15日に機材ベンダーであるKDDI Viet Namと契約）。多くのマルウェア解析関連機器は2022年3月末までに納品される予定であるが、COVID-19の影響により一部の機材は2022年4月以降に納品されることとなった。

なお、JPCERT/CCの協力のもと、2021年12月にマルウェア解析に関する研修が、2022年2月にマルウェア解析装置の環境構築に関するミーティングを実施した。

活動3-4.（成果3）

事前対応基幹設備（例：ネットワーク監視、国際標準Common Criteriaに則った実習のための機材）が拡張される

活動3-4では、事前対応基幹設備として、DDoS攻撃緩和システムおよび国際標準Common Criteriaに則った実習のための機材（セキュリティ評価機材）を調達した。

- **DDoS攻撃緩和システム（ネットワーク監視機材）**

活動2-3を参照。

- **セキュリティ評価機材**

2020年8月2日の第2回JCCにおいて、プロジェクトの延長に伴い、ニーズの高かったセキュリティ評価機材が追加された。評価機材リストを含むプロジェクト文書が2021年7月16日に承認された。当初は2020年中の調達開始予定であったが、この承認を受けて数か月遅れて調達が開始された（2021年11月15日に機材ベンダーであるKDDI Viet Namと契約）。多くの機器は2022年3月末までに納品される予定であるが、COVID-19の影響により一部の機材は2022年4月以降に納品されることとなった。

セキュリティ評価に関しては、Common Criteriaに関する研修を複数回実施した。研修に加えて、機器の適切な運用（セキュリティおよび評価手続き）のために、2021年9月から2022年1月にかけて、現地企業とベトナム人専門家の協力のもとで、以下のドキュメントの作成とAISへの教育を行った。

- Lab security manual
- Lab evaluation procedure
- Evaluation Technical Report (ETR) Template

- **TSUBAME**

本プロジェクトの活動範囲内ではないが、JPCERT/CCが2008年から運用しているアジア太平洋地域インターネット定点観測システム（TSUBAME）[1]をAISにインストールする作業をプロジェクトチームが支援した。長年、ベトナムはTSUBAMEに加盟していなかったが、2020年末に本プロジェクトを通じて、VNCERT/CCはTSUBAMEに参加することを決定した。TUSBAMEセンサーの設置後、TSUBAMEの情報をもとにした加盟国の観測動向や情報、インシデントに対するアラートが共有されるようになり、AISの脅威情報収集能力を向上させることに貢献した。

[1] https://www.jpcert.or.jp/tsubame/

2. プロジェクト成果

2-1 成果と指標

ここではアウトプットの達成度と有効性（アウトプットとプロジェクト目的の因果関係の妥当性）の観点から記述する。各アウトプットの結果は以下の通りである。

成果1-1：CDPが作成される

当初予定していたCDP対象者数は40名だったが、最終的に個別面談に基づき106件のCDPを作成した（総面談件数は139件）。CDP数増加の理由は、AISからの研修参加者数増加の要請と、2019年11月にMIC傘下の独立組織であったVNCERT/CCがAISに統合されたことによる人員増加によるものである。プロジェクトにより作成されたCDPは、対象者の上司によりすべて承認された。2021年7月に最後のCDPの追加を終了したが、AISからの要望が多かったため、2021年10月まで新たなCDPを作成した。また、プロジェクト後半ではCDP を作成していない AISの職員も、枠があれば研修に参加できるようにした。

よって、成果1-1「CDPが作成される」は達成されたと判断される。

成果1-2, 2-1, 3-1：研修生の能力が向上する

事後テストの得点、オンライン学習の得点、認定試験の得点について、ほとんどの研修で事前テストの得点と比較して上昇してることを確認した。また、事後アンケートにおいても、受講者とトレーナーからの高い評価が得られた。国際認定試験の合格率については、目標値を設定していないものの、プロジェクト期間を通して着実に合格者を増やした。CDP レビューの結果、ほとんどの研修生およびその上司が研修によって業務に対する意識が変わり、日常業務（インフラ、モニタリング、ペンテスト等）が改善されたと感じている結果となった。

したがって、成果 1-2, 2-1, 3-1 の「研修生の能力が向上する」は達成された。

プロジェクトでは、各研修の評価を以下のように段階的に行った。

1) 反応 ： 受講者が研修に満足しているかどうか、受講者からフィードバックを得る。
2) 学習 ： 研修で何を学んだか、事前・事後のテスト結果を入手する。
3) 結果 ： 学んだことをもとに、受講者の行動が変わったか、日々の業務が改善されたかどうかを確認する。その結果、ベトナム国内の組織やサイバーセキュリティの強靭性にプラスの影響を与えたかどうかを確認する。

(1) 反応：研修生からのフィードバック

各研修の終了時には、研修生の満足度を測るためのアンケートを取った結果から、プロジェクトチームは、研修生の研修に対する満足度は高いと判断した。（付録を参照）

(2) 学習：事前テスト・事後テスト・資格試験

受講者の実際の知識の向上を測定するため、事前テストと事後テスト、研修後のオンライン自己学習状況、認定試験の受験状況などを比較し、総合的に評価した。国際資格関連コー

スについては、研修前後の確認テストの比較、研修前のテストとオンライン学習の得点比較、資格試験の受験状況を付録に記載。（各試験の難易度が異なるため、単純なスコア比較は意味を持たない点に注意）

［集中研修］

「Planned Num. of trainee」は、研修実施前に計画していた受講者数、「Actual Num. of trainee」は、実際に研修を受講した人数である。研修実施の直前や途中で研修に参加できなくなる人もいるので、研修実施後に受講者が減らないように、研修調達のプロセスを改善し続けた。キャンセルが発生しても、同じ研修会社に次回の研修を依頼することで、キャンセルした枠の分の追加費用が発生しないようにすることができた。「Increased point (pre vs. post-test)」とは、研修前後のテストの結果を比較（パーセンテージを算出した後の差を比較）したもので、研修によって（一時的に）知識が増えたことを示すものである。OSCP、LPT、OSWE等の研修では、前後テストは単純な選択問題ではなく演習問題なので、単純な比較は意味がない点に注意。

［オンライン学習］

「Actual Num. of trainee」は、オンライン学習に実際に取り組んだ研修生の数である。「Increased point (pre vs online-test)」は、事前テストとオンライン学習の点数の比較である。

オンライン学習に取り組んだ研修生数／研修受講者数：62.6%

［資格試験］

「Increased point (pre vs exam test)」は、試験前と試験後の点数の比較である。事前テストと認定試験の結果を比較すると、事後テストより大幅に向上していることがわかる。主な比率は以下の通り。

1) 受験者／受講者 55.6%
2) 合格者／受験者 79.5%
3) 合格者／受講者 44.1%

本プロジェクトでは、OSCPやOSWEなど特定の研修を除き、資格試験の合格を目指すものではなかった。しかし、資格試験の勉強をすることで、集中研修で学んだことを定着させることを期待していた。そこで、プロジェクトでは、研修前後のアナウンス、メールによる受験の呼びかけ、CDPレビュー時の提言などを行い、上記3点の比率が高まるように配慮していた。PDMでは、成果の達成度を判断するための補完的な定量指標として、事前・事後テストの結果や、事前学習とオンライン学習のスコア比較を用いている。そのため、プロジェクトの主目的は試験合格ではないことから、試験結果は参考値として扱われる。

以上より、研修の短期的な効果は十分に達成されたと判断される。

成果1-3：普及啓発教材の数が増加する

プロジェクト開始当初は、普及啓発教材の開発目標数は設定されていなかった。当時は、普及対象者や教材の内容がまだ決まっておらず、検討するのに時間がかかると想定されたからである。最終的な成果物は以下の通りである。したがって、成果1-3「普及啓発教材の数が増加する」は達成された。

成果物	成果物の数	コンテンツ
普及啓発動画	動画 3 本	タイトル: 1) Staying vigilant with strangers in virtual space, especially on social media 2) Save the Children on Internet 3) Introduction an Online Contest of Information Security for students
デザインキット	1 式	• ブランドキットのコア部分：ロゴマーク、ウェブサイトテンプレート、ソーシャルメディア、スローガン、ユニフォーム • ブランドキットのオフィス活用：証書、名刺、便箋、封筒、ファイルフォルダ、スライドテンプレート • ギフトセットデザイン：VN-COP Network のロゴ入り記念メダル・バッジ、その他記念品
COP ポータルサイト	1 式	提供サービス: • 登録 • 法律文書公開 • 質問・問い合わせへの回答 • フィードバックと要望受付 • ニュースとイベント情報の公開 • ユーザー情報保護方針（AIS ポリシー設定） • レポーティング

成果1-4：開発された普及啓発教材が活用される

本プロジェクトで作成した3本のアニメーション動画は、現在、以下のサイトで活用されている。

- *Học sinh với An toàn thông tin*

  https://www.youtube.com/channel/UCz39i69Rz9nbqzffczICqsw

動画の再生回数は以下の通り。

動画名	公開日	視聴数	リンク
1st video (Câu chuyện Công chúa và Thạch Sanh)	2021/05/26	55	https://www.youtube.com/watch?v=kSPXEgVa7SU&t=101s
2nd video (Bảo vệ trẻ em trên mạng)	2021/05/25	133	https://www.youtube.com/watch?v=Zsfrgmdh6wg&t=11s
3rd video (Cuộc thi Học sinh với ATTT 2021)	2021/06/25	721	https://www.youtube.com/watch?v=ja1tQ8saJAo

3本目の動画は、ベトナム情報セキュリティ協会（VNISA）による「Security Day」（2021年11月25日）において上映さた。

普及啓発セミナーを通じて、JICA専門家が日本の知見に基づき、ベトナムの普及啓発戦略や効果測定方法について指導を行ったが、これらのノウハウをAISは具体的に活用できていない。

まとめると、開発した動画はすでにアップロードして使用しているが、プロジェクトで提供した知見のすべてを有効に活用しきれていない。従って、成果 1-4 の「開発された普及啓発教材が活用される」は部分的に達成された。

成果1-5：政策立案の実践のために習得した知識が活用される

実施した政策立案関連の研修は以下の通り。各コース終了後のアンケートやCDPレビューによると、対象職員はコースを通じて各政策の知識を習得しているようだが、実際の政策立案活動としては活用されていないようである。

従って、成果 1-5「政策立案の実践のために習得した知識が活用される」は部分的にしか達成できていない。

表 6　政策策定関係研修結果の活用例

No	コース名	習得した知識の活用例
1	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	今後活用を期待
2	日本の省庁および大学によるサイバーセキュリティ政策策定に関するオンラインセミナー	今後活用を期待
3	普及啓発オンラインセミナー	COP の政策立案・実施に活用
4	課題別研修（上乗せ）：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	今後活用を期待

成果2-2：事後サービスのためのインフラが強化される

事後サービス能力を向上させる機器としては、DDoS 攻撃緩和システム、マルウェア解析システムが挙げられる。既に提供・導入されているDDoS攻撃緩和システムによってAISのDDoS攻撃緩和能力は約75Gbps向上していると試算される。マルウェア解析機器はまだ運用開始前である。したがって、成果 2-2「事後サービスのためのインフラが強化される」の達成は部分的である。

成果3-2：事前サービスのためのインフラが強化される

事前サービス能力を向上させる機器は、DDoS攻撃緩和システムおよびセキュリティ評価機材である。DDoS攻撃緩和システムの運用は開始されているが、セキュリティ評価機材の運用はまだ始まっていない。

したがって、成果 3-2 「事前サービスのためのインフラが強化される」の達成は部分的である。

2-2　プロジェクト目標と指標

プロジェクト目標「AISのサイバーセキュリティ能力が強化される」に対する指標は次に示す通りである。

指標		検証手段
1	AIS の組織能力が最適化されるように、職員それぞれに適切な役割（ロール）が割り当てられる。	職員の役割が記述された組織表
2	職員それぞれが割り当てられた役割（ロール）を果たす。	キャリア開発計画（CDP）に基づく職員の評価

指標1については、全職員の役割をSecBokのロールに割り当てることで達成されたといえる。

指標2に関しては、CDP手法の実践を通して測定することができる。CDP手法では、割り当てられた役割に適した研修を提供し、その効果をCDPレビュー面談やアンケートを通じてモニタリングする。このモニタリング結果に加え、研修前後の試験点数の比較や資格試験の合格者数などから、達成状況を定量的に捉えることができる。これらの結果は「活動1-5, 2-3, 3-3.（成果1,2,3）」および「付録9：研修結果」にまとめているが、いずれも良好であり、目標を達成できているといえる。

またCOP担当者は、啓発に関する活動を通じて、啓発資料の内容に関する考え方や、映像制作会社との調整方法をはじめ、啓発セミナーを通じて広範な普及戦略やターゲット層の分析能力を得ることができた。つまり研修と啓発を通じた各人の能力向上という目標は達成されつつある。

一方で、機材提供に関しては納期の遅れにより、機材構成と運用能力の確保という目標を達成するためのリスクが顕在化している。具体的には2種類の機材の提供が遅れる見込みで、設置や運用のための時間が十分確保できない可能性がある。

以上により、現時点ではプロジェクト目標を達成できていないが、着実に達成に向かっているといえる。

(1)　研修の効率性と有効性

研修を受講した職員とその上司に、業務で研修の効果を感じたかどうかを質問した。上司には、研修生である部下一人ひとりについて、研修の効果が認められるかどうか尋ねた。その結果は「活動1-5, 2-3, 3-3.（成果1,2,3）」でまとめているが、研修者自身と上司は、研修者の約8割は研修の効果ありと回答している。しかし、具体的にどのような場面で研修が効果的であったのかについては、ほとんど情報が得られなかった。彼らが最も多く受講した研修は、CompTIA Security+、ECSS、Linuxなどの基礎的なものであり、日々の業務に役立っているとしても、具体的に効果的な場面を説明することが難しいのではないかと考える。今後、より業務に直結した研修が実施されるようになれば、より具体的な成果が確認できるものと期待している。

(2)　CDPの有効性

以下の上司への質問に対する回答結果に示す通り、14人のうち8人の上司がCDPは有効であると回答した。残りの 6 人は、CDP は有効であるが改善が必要であると回答している。改善要望の内容とプロジェクトアクションについては、次項にまとめる。

Question				
What do you think of CDP? Is it useful for your organization and your management? Please select one from the list and describe the reason why you selected it.				
Useful	Useful but need improvement	Not useful must be changed	Not useful at all	Total
8	6	0	0	14

(3) CDPと研修の改善に関する意見

AIS 職員や部門長から得た研修や CDP に関する主な要望と、それに対するプロジェクトの対応を以下の表にまとめる。

表 7　CDPと研修に対する改善意見とプロジェクトとしての対応

No	Comments or Opinions	Action
1	SecBoK のロールについて:： SecBok に示されたセキュリティロールはわかりにくい。 SdcBok のロールと VNCERT/CC のロールの対応が難しい。それらの関係を明確にしてほしい。	SecBok と NIST の対応表はすでに存在するが、ロールの対応について理解するのは現時点では難しい。プロジェクトではこれまで SecBok のロール対研修マッピングを直接利用しておらず、主に職能定義と面談によるニーズ把握により研修割り当てを行っている。ベトナムにおけるセキュリティロールの標準ができれば、NIST との対応表を作ることが可能になると考える。
2	業務と研修のバランスについて： 日々の業務をこなしながら研修に参加することは大変である。上司によっては研修より業務を優先させる風潮がある。	CDP は作成時・レビュー時に上司に共有され、研修への参加についての同意が得られていることになっている。上司は AIS にとって部下の研修への参加が重要であることを理解し、研修参加を応援する立場にある。このようなポリシーを記述した説明文書を再度上司に共有する。
3	研修期間について： 研修の内容を理解するのに研修期間が短すぎる。研修の内容に比べ 5 日間のフルタイム研修は短すぎる。	研修期間を 5 日間より増やすことは難しい。5 日間の研修で概要を学び、その後 1〜3 か月をかけて Web での学習サイト（試験対策用）で自習することを勧める。
4	試験対策授業追加について： 試験対策のための追加授業を増やしてほしい。	研修はコンセプトと全体像を学ぶことを目的としており、試験対策を目的とするものではないので追加授業の提供はできない。
5	実習の増加について： 研修中の実習の機会が少ない。デモだけの場合もあり、より多くの実習を望む。	実習を主体としたカスタムトレーニング（CSIRT 研修やマルウェア研修など）を提供しており、今後もニーズを把握してサイバーセキュリティ活動に役立つカスタム研修を企画していくことで要望に応えたい。
6	英語について：英語が学習の障害となる。	技術英語研修を提供する。
7	研修対象について： AIS だけでなく MIC やその他省庁の人間も対象としてほしい	プロジェクトのカウンターパートである AIS が最も優先される。また研修対象者は CDP を持つことも前提である。仮に研修スロットに空きがあり、コストを増やすことがなければ AIS 以外の人間（但し防衛省や軍関係者を除く）も含めることができなくはないが、以下の理由から実現は困難である。 - AIS だけでも 80 人の職員を研修対象としており、AIS 職員を優先しながら、コスト増を招かずに AIS 外の人間を参加できるよう研修を調整することは、限られたリソースの中では困難である。 - AIS 外の部署の参加を認めた場合、それ以外の部署からも参加要望が出てくる可能性が高い。何らかの形で優先度をつけたとしても不公正感は拭えず、問題化する可能性があり、プロジェクト活動の障害になることが懸念される。

3. PDM変更の履歴

PDMは2nd JCC （14th August 2021）において大きく変更されている。変更理由は、2021年8月27日付けのMinutes of Meetingに記載。JCCのMinutes of Meeting とPDMについては、Appendixとして本報告書に添付している。

4. その他

4-1 環境・社会配慮の結果

カテゴリーC[2]（環境・社会への悪影響が最小限またはほとんどないと考えられるもの）であるため、考慮しない。

4-2 ジェンダー／平和構築／貧困削減に関する配慮の結果

本プロジェクトでは、ジェンダー／平和構築／貧困削減に関しては特段の配慮はしていない。

III. 合同評価の結果

1. DAC評価基準に則った評価結果

1-1 妥当性

1.1.1 開発政策との整合性

プロジェクト開始時点において、ベトナムでは、IT技術開発や利活用において政府、組織、個人が有する権利と責務を規定する「国家IT法」、及びインターネット上の情報セキュリティ確保のための政令や省令が2007年に制定された。2010年には情報セキュリティに関する刑法が改正され、DDoS攻撃、コンピュータウイルスの意図的拡散、オンライン詐欺等の具体的な内容と罰則が規定され、国家として情報セキュリティ対策に注力している。

サイバーセキュリティに係る国家戦略・計画も制定されており、2010年の首相決定第63号「2020年までのデジタル情報セキュリティの発展に関する国家計画の承認」、および2016年の首相決定第898号「2016年から2020年までのサイバー情報セキュリティを確保するための方向性、目標、義務の承認」では、ベトナム政府として2020年までに達成するサイバーセキュリティの諸目標、計画、組織体制などが規定されている。また、2015年の首相決定第893号「2020年までの情報安全に対する意識と責任の伝播、普及、強化に関するプロジェクトの承認」では、2020年までの サイバーセキュリティの伝達・普及・促進に関する目標や広報活動が規定されている。2014年の首相決定第99号「情報の安全性とセキュリティに関する人材育成研修と開発」に関するスキームの承認」では、2020年までのサイバー情報セキュリティ分野における人材育成の目標・計画が規定されている。2018年には「サイバーセキュリティ法」が制定され、特にベトナム国内でネットサービスを展開する場合、利用者の本人性を保証する仕組みを確保し、要求に応じて管轄当局にデータを提供・削除すること等が規定されている特徴がある。

プロジェクト終了時点においては、2020年の首相決定第749号「2025年までの国家デジタルトラ

[2] https://www.jica.go.jp/english/our_work/social_environmental/index.html

ンスフォーメーションプログラム」の中で「デジタル社会の発展とデジタルデバイドの解消」が目的の1つに掲げられており、国際電気通信連合（International Telecommunication Union）が公表しているグローバル・サイバーセキュリティ・インデックス（GCI）が2025年までに上位40位以内、2030年までに上位30位以内にランクインすることを目指している（2020年のGCIにおいてベトナムは25位）。また、サイバーセキュリティはデジタルトランスフォーメーションを成功させ、社会を持続可能なものにするための鍵であると捉えている。一般のユーザーの中でも特に脆弱な若年層へのセキュリティ教育に注力することを目標として、「創造的で安全にサイバー空間を利用する青少年の保護と支援プロジェクト（2020年～2025年）」が2021年6月に首相決定第830号された。この決定を根拠としてベトナムは特に青少年へのサイバーセキュリティ・情報セキュリティに関する普及啓発活動を推進している。（報告書最終化までに他の最新の政策も追記）

したがって、本プロジェクト計画時および終了時において、本プロジェクトとベトナム政府の政策は整合している。

1.1.2 開発ニーズとの整合性

本プロジェクト実施前、ベトナムにおいては、2014年からインシデントの数が急激に増加しており、2015年にはフィッシング攻撃、ウェブサイト改竄、マルウェア等確認されているもので3万件を超えている（2013年は6千件程度）。2016年には同攻撃被害が確認されているもので12万件を超えている。また同年には、ベトナム航空のウェブサイト、音声システム及び運航情報に関する電光掲示板がハッキングされ、航空会社の顧客情報が漏洩した。その後、2019年には上記3種類のサイバー攻撃件数は5千件程度となっている。なお、サイバー攻撃手法や件数の調査方法は各年で異なる場合があり、またサイバー攻撃の質が異なる可能性もあるため、件数の単純な比較は注意が必要である。

政府機関や組織の情報システムには多くの脆弱性があり、サイバーセキュリティのリスクが大きいことが明らかになってきている。インシデントの種類に関しては上記3種類以外に、外部からの侵入やDoS/DDoS攻撃 やAPT攻撃（Advanced Persistent Threats） が増加している。さらに、マルウェア感染は年々増加し、特にソーシャルネットワークを介した被害が増大している。オンラインフィッシングも依然として蔓延しており、多くのユーザーが情報セキュリティへの過信と不注意から、経済的損失を被っている。加えて、ルータやセキュリティカメラなどのIoTデバイスをターゲットにした大量の攻撃を伴う DDoS攻撃が多く発生し、多くの通信サービスの運用に損害・影響が生じている。個人情報漏洩も著しく、銀行・金融・電子商取引において、ユーザーに経済的損失をもたらしたインシデント数は増加している。

本プロジェクト終了時点においても、それまでのサイバー攻撃に加えて、ベトナムの中小企業がサイバー攻撃被害を認識したケースが50%を超えたり、国の重要機関や青少年や子供を狙ったサイバー攻撃が増加していたりする等、サイバーセキュリティに関する脅威は増加し続けている。

ベトナムの情報・サイバーセキュリティ体制では、国防省と公安省がそれぞれサイバー防衛とサイバー犯罪の捜査を担当している。本プロジェクトのカウンターパートである情報通信省（MIC）傘下の情報セキュリティ局（AIS）は国家サイバーセキュリティ戦略を策定し、セキュリティオペレーションセンター（Security Operation Center：SOC） やセキュリティ問題を専門に扱うインシデント対応チーム（Computer Security Incident Response Team：CSIRT） 機能を有する機関である。AISは啓発活動、インシデント対応、サイバー攻撃防御などの運用を一定程度行うこと

ができているが、高度化かつ増加し続けるサイバー攻撃に対して、政府のネットワーク監視、サイバー攻撃防御、インシデント対応機能の強化のためにはセキュリティ技術者のさらなる能力強化が重要な課題となっている。

本プロジェクト開始当初、MIC内には、AISよりも設立が早かった別組織のベトナムコンピュータ緊急対応チーム（VNCERT）が存在しており、AISと同様にSOCやCSIRTの機能を備えていた。ただし、AISが政策策定機能、DDoS攻撃緩和システムを備えているのに対し、VNCERT/CCは関係諸機関間の統制機能、他組織のCSIRT設立支援機能を有している点に違いがあった。なお、プロジェクト開始後の2019年11月、VNCERTはVNCERT Coordination Center（VNCERT/CC）としてAISに編入された。

電力や交通にかかる重要情報インフラを運用するオペレーター（中央・地方政府機関含む）をセキュリティ面で支援する政府機関は、VNCERT/CC、AIS（内部組織の国家サイバーセキュリティセンター（NCSC））を含め5つ存在し（他は、国防省、公安省内に設置）、各々がSOC、CSIRT、および日本国の情報セキュリティ緊急支援チーム（Cyber Incident Mobile Assistant Team：CYMAT）に近い機能を有している。オペレーターは、上記5つの機関に対し支援を要請でき、 一つのオペレーターが、VNCERT/CCとAISの両方によるモニタリングセンサーを設置する例もある。

サイバー攻撃に対する防御機能の冗長性（ある防御システムが破られても、他のシステムにより防御が果たせる）の確保という観点からは、複数のSOCとCSIRTの設立・能力強化は支持される。特に、サイバー攻撃緩和システムを有し、サイバーセキュリティ政策策定も行うAISを支援することはベトナム政府全体のサイバーセキュリティ体制の強化のためには重要である。

したがって、本プロジェクト計画時および終了時において、サイバーセキュリティに関する開発ニーズは高いといえる。

1.1.3 日本の援助政策との整合性

我が国の「開発協力大綱」（2015年2月）の重点課題「普遍的価値の共有、平和で安全な社会の実現」の政策として、「海洋・宇宙空間・サイバー空間といった国際公共財に関わる開発途上国の能力強化等」が挙げられており、本案件の目的と合致する。

プロジェクト開始時において、2018年7月に閣議決定された「サイバーセキュリティ戦略」においては、国際社会の平和と安定の実現及び我が国の安全保障のため、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としている。2013年10月の「サイバーセキュリティ国際連携取組方針」においては、我が国と最も地理的に近接し、経済的にも密接な関係があるアジア太平洋地域、特にASEAN諸国に対するキャパシティビルディングや知見の共有などの協力を強化するとしている。さらに、G7伊勢志摩サミット（2016年）で合意された「サイバーに関するG7の原則と行動」でも、CSIRTs間の国際協力、能力向上、意識啓発、支援を支援し、サイバーセキュリティを強化する方針が示されている。加えて、サイバー分野の協力は2017年1月の日越首脳会談でベトナム側から日本の協力を要請されている。

プロジェクト終了時においては、2021年9月28日に閣議決定された「サイバーセキュリティ戦略」においても引き続き、他国で生じたサイバー事案は我が国にも容易に影響を及ぼす可能性があることから、各国政府・民間等様々なレベルで重層的に協力・連携することが重要であるため、知見の共有・政策調整、サイバー事案等に係る国際連携及び能力構築支援を推進するとしている。

本事業は外務省の「対ベトナム社会主義共和国国別開発協力方針」（2017年12月、2012年12月）

における重点分野「(3) ガバナンス強化」に位置付けられるものである。また、サイバーセキュリティの強化により、安定したICTインフラ運用が実現されることから、「(1) 成長と競争力強化」にも寄与する。

プロジェクト開始時において、「対ベトナムJICA国別分析ペーパー」(2014年3月）では、ガバナンス強化のための司法・行政機能強化が重要な開発課題として挙げられていた。プロジェクト終了時の最新の「対ベトナムJICA国別分析ペーパー」(2020年6月）でも、ガバナンス強化（統治能力向上）を重点分野として挙げている。特に法務執行能力強化について、サイバーセキュリティ能力向上に向けた人材の育成及び適切な法運用が必要とされている。

したがって、本プロジェクト計画時および終了時において、日本の政策との整合性があったといえる。

以上より、本プロジェクトの実施はベトナムの開発政策、開発ニーズ及び日本の援助政策と十分に合致していることから、妥当性は高いと判断される。

1-2 効率性

1.2.1 投入

投入	計画 (プロジェクト開始時)	実績 (プロジェクト終了時)
日本側		
協力金額	15,300 万円	31,900 万円
プロジェクト期間	2019 年 6 月 – 2021 年 11 月 （30 ヵ月）	2019 年 6 月 – 2022 年 6 月 （37 ヵ月）
専門家派遣	派遣： 2 遠隔支援：1	派遣：2 遠隔支援：4
本邦研修 （オンライン研修含む）	-	14
対象研修員数	40	106（最終的な研修生数） 144（累積研修生数）
第三国研修	-	2
機材	4,500 万円 （DDoS 攻撃防御システム、ネットワーク監視、マルウェア解析システム）	7,800 千万円 （DDoS 攻撃防御システム、ネットワーク監視、マルウェア解析システム、評価機材）
現地運営費用	4,400 万円 （現地研修、現地機材、プロジェクトスタッフ等）	12,800 万円 （現地研修、現地機材、プロジェクトスタッフ等
ベトナム側		
カウンターパートスタッフ （管理スタッフ）	3	6
プロジェクト環境	プロジェクトオフィス、インターネット、電気等	プロジェクトオフィス、インターネット、電気等

1.2.1 投入要素

本事業の投入要素は成果産出に対して一部問題があったと考えられる。

まず日本側の投入に関して、当初、専門家は長期専門家、短期専門家（チーフアドバイザー・キャリア開発計画）であったが、ベトナム側のニーズをくみ取り普及啓発活動、ISAC等の専門家が追加された。日本側の関係機関による研修や、現地研修もCOVID-19の状況の中で、オンラインビデオ会議システムを駆使して、おおむね適切な時期に実施することができた。本事業ではプロ

ジェクト開始1年後のJCCで、複数の供与機材を追加したが、その大部分の供与がプロジェクト終了間際となり、一部機材はプロジェクト終了後の納品となることが判明したため、二度目のプロジェクト延長をせざると得なかった。

ベトナム側投入には大きな問題はみられない。プロジェクト終了3カ月前にベトナム側の調整を担当していたプロジェクト副ディレクターが異動となった。その後、プロジェクトディレクターと会議等で調整する機会はなかったが、必要な調整がほぼ完了しており、活動も完了に近づいていたため大きな問題とはならなかった。

1.2.2 協力金額

協力金額については、1億5,300万円を計画していたところ、3億1900万円（計画の208%）となり、当初計画を大きく上回った。

1.2.3 協力期間

協力期間については、30ヵ月を計画していたところ、37ヵ月（計画の123%）となり、当初計画を大きく超過した。

以上より、本事業は協力金額・期間を大幅に増加したが、プロジェクト成果達成に必要な投入のみを追加し、かつ適切なプロセスに則って変更を決定したため問題はないと考える。一方で、多くの機材供与の時期がプロジェクト後半に集中したため、事業効果発現に十分に寄与できなかったことから、効率性はやや低いと判断される。

1-3 有効性

1.3.1 成果

(1) セキュリティ品質管理能力が強化される

指標1−1： 職員毎のキャリア開発計画（CDP）が準備される

キャリア開発の短期専門家とのインタビューを通して、AIS職員1人1人に対するキャリア開発計画が作成されて、CDPレビューのタイミング等で更新された。作成したCDPの総数は144であり、プロジェクト終了時点で有効なCDPの数は106である。（減少分は作成後の退職や異動による）

指標1−2： 研修受講者の能力が向上する。（研修前後のテストで判断）

職員毎のキャリア開発計画に則り、セキュリティ技術、プロジェクトマネジメント、サイバーセキュリティに関連するビジネス英語等に関する研修がおおむね計画通りに実施された。研修の前後で実施した知識確認テストの結果では、研修生の多くが研修前後で知識の向上が見られた。集中研修後の数か月間のオンライン自己学習においても、取り組んだ研修生のほぼすべてが研修前よりも技術知識を大きく伸ばしていることが確認された。さらに、資格に関連する研修のみを対象として、オンライン学習で一定レベルに達した研修生が受験した国際資格試験の成績も研修前よりも向上し、資格試験に関連する研修生のうち約50%が合格した（受験者数に対する合格者数に限ると約80%となる）。CDPレビューにおいても、研修で得た知見を業務に活用した事例や、資格合格を1つのモチベーションとしてさらに学習す

る意欲が増えた研修生等が多く見受けられた。

以上より、プロジェクト終了時点において、定量的にも定性的にも研修生のセキュリティ等に関する能力が向上した形跡が見られた。

指標1−3： 啓発教材が増加する

本プロジェクトを通して、青少年や子供のためのサイバーセキュリティに関するアニメーション動画（3本）、国民に馴染みやすいデザインキット、そして情報公開や国民からの不正なコンテンツの通報等の機能を持つポータルサイトを開発した。

指標1−4： 開発された啓発教材が利用される

作成したアニメーション動画はすでにAISのYoutubeチャネルで公開されている。また、動画のうちの1つである「Introduction an Online Contest of Information Security for students」は、情報通信大臣も出席されたVIETNAM INFORMATION SECURITY DAY 2021（2021年11月25日開催）においてコンテストの案内のために上映された。デザインキットは今後の普及啓発活動で積極的に使われることで、国民のサイバーセキュリティに関する普及が促進されることが期待される。ポータルサイトはAISが運用を続けることで国民にとって必要な情報が公開され、国民も政府側とのコミュニケーションのためのツールとして活用されることが期待されている。

指標1−5： 本事業で得られた政策策定にかかる知識が活用される。（AISへのインタビュー調査で判断）

政策策定に関わる研修を受講した研修生のCDPインタビューにおいて、日本の政策（特に製品セキュリティ検査、情報共有体制、中小企業への支援等）やGDPRの取り組み等が業務上非常に参考になったという声が多く聞かれた。しかし、実施した政策に関する研修の内容を具体的にベトナムの政策に取り入れる等の事例はプロジェクト終了時までに確認できなかった。

以上より、指標1-1,1-2,1-3は十分達成されたが、指標1-4,1-5は今後も引き続き効果発現のために活用されことが必要であることから、成果1はおおむね達成されたと判断される。

(2) 事後対応型サービス能力が強化される

指標2−1： 研修受講者の能力が向上する

指標1−2を参照。

指標2−2： 事後対応のための基幹設備が強化される。（AISからの報告で判断）

DDoS攻撃防御システムは2021年3月に納品され同年11月に設置済かつ運用されていることが確認された。直接的な運用のための技術としてLinux OSや仮想マシン（VMWare）に関する研修はプロジェクト中に実施した。

マルウェア解析機材については、2022年2月末で時点では納品されておらず、プロジェクト

終了直前に納品される予定である。解析方法のための研修と運用に関するアドバイスをJPCERT/CC協力のもとで実施した。

以上より、指標2-1は十分達成されたが、指標2-2はプロジェクト活動による効果が十分に発現しておらず、引き続きAISによる継続的な運用が必要であることから、成果2はおおむね達成されたと判断される。

(3) 事前対応型サービス能力が強化される

指標3−1： 研修受講者の能力が向上する

指標1−2を参照。

指標3−2： 事前対応のための基幹設備が強化される

DDoS攻撃防御システムについては指標2-2を参照。

Common Criteriaに関連する評価機材については、2022年2月末で時点では納品されておらず、プロジェクト終了直前に納品される予定である。評価機材のセキュリティ対策や運用手順に関しては、現地企業によるコンサルティングを実施して、必要なドキュメントや手順を整備し、研修によって技術移転を実施した。

以上より、指標3-1は十分達成されたが、指標3-2はプロジェクト活動による効果が十分に発現しておらず、引き続きAISによる継続的な運用が必要であることから、成果3はおおむね達成されたと判断される。

1.3.2 プロジェクト目標

- **プロジェクト目標：AISのサイバーセキュリティ能力が強化される**

指標1： AISの組織能力が最適化されるように、職員それぞれに適切な役割（ロール）が割り当てられる

★

情報入手元：職員の役割と組織構造

指標2： 職員それぞれが割り当てられた役割（ロール）を果たす

★

情報入手元：CDPの評価

以上より、3つの成果はそれぞれ「おおむね達成」されたと判断される。また、プロジェクト目標の指標1,2について一部達成が認められるものの、十分に「達成」されたとは判断することが難しい。よってプロジェクトの有効性は中程度と判断される。

1-4　インパクト

1.4.1　上位目標の達成状況

- **上位目標：ベトナム政府のサイバー攻撃耐性が向上する**

  指標：サイバーセキュリティ関連の政策目標（首相決定「2010年第63号」、「2016年第898号」、「2015年第893号」）の達成にAISが貢献する。※政策は2020年までのものであり、事業完了時の評価に有効なサイバーセキュリティにかかる国家戦略・計画、組織体制、広報活動等に関する諸政策はプロジェクト開始後に再確認する。

AISへのヒアリング、AISが発行するAnnual Reportや統計情報をもとに政策目標達成にかかるAISの貢献度を評価し、全体目標に対するプロジェクトの貢献度を測定していく方針であったが、AISは2018年、2019年、2020年、2021年のAnnual Reportを発行していない。よって、CDPレビューを含む職員へのインタビューによって、上位目標の効果の発現および可能性を推察することとする。

上位目標のサイバーレジリエンスとは、サイバー攻撃によるシステムや組織への影響を最小限に抑え、迅速に元の状態に戻すための仕組みや能力のことである。つまり、サイバー攻撃によって重要情報インフラが停止したり、政府の業務が停止したりする可能性があるため、政府の行政や業務を継続するための対応力をサイバーレジリエンスという。NISTのサイバーセキュリティフレームワークVersion1.1[3]におけるサイバーセキュリティの5つの機能、すなわち「特定」「保護」「検知」「対応」「回復」のうち、「検知」「対応」「回復」の3つの機能は、レジリエンスを構成する要素である。脅威インテリジェンスを用いて脅威や攻撃者、脆弱性を「特定」し、セキュリティ対策でシステムを「保護」した後、被害や侵入を想定して「検知」「対応」「回復」の機能を並行して強化する必要がある。サイバーレジリエンスのポイントは、セキュリティポリシーやガイドラインの策定、セキュリティ対策の構築、ネットワークトラフィックの監視による状況把握、異常発生時の検知・対応体制の確立にある。

これらの体制や能力を強化するため、本プロジェクトでは、欧州連合サイバーセキュリティ機関（ENISA）が定める3つのサービス能力（セキュリティ品質管理サービス、プロアクティブサービス、リアクティブサービス）の強化を成果として掲げていた。AISの人材や機器の能力が向上することで、ポリシーやガイドラインの策定、監視、対応などの能力が強化され、AISのサイバーレジリエンスの向上につながる。プロジェクトでも支援した情報共有・分析センター（ISAC）、Common Criteriaセキュリティ評価認証、COPなどの活動を強化することで、政府機関、地方政府、民間企業との連携を強化し、ベトナム全体のレジリエンス強化に貢献できると推論される。サイバーセキュリティの成熟度を体制・技術・組織・能力強化・協力の観点から評価しているグローバル・サイバーセキュリティ・インデックス（GCI）において、2020年は25位（2019年50位、2017年は101位）となったことから、ベトナムのサイバーセキュリティは相対的に強化されていることがわかる。

したがって、プロジェクト期間中と同程度の進捗を維持し、プロジェクト終了後もその効果が継続かつ強化するようにAISがミッションを継続すれば、プロジェクト終了から数年後

[3] https://www.nist.gov/cyberframework/framework

にインパクトが顕在化する可能性が高い。

1.4.2 その他のインパクト

(1) 自然環境へのインパクト

既存の施設内にPCやサーバー等が設置されたのみであり、自然環境への負のインパクトは出現していない。

(2) 住民・用地取得

既存の施設内にPC やサーバー等が設置されたのみであり、住民移転や用地取得は発生していない。

(3) その他の間接的効果

特になし。

以上より、本プロジェクトの実施により期待された上位目標については十分なインパクトが発現しているとは言えないが、達成に向けて着実に進展していると判断される。

1-5 持続性

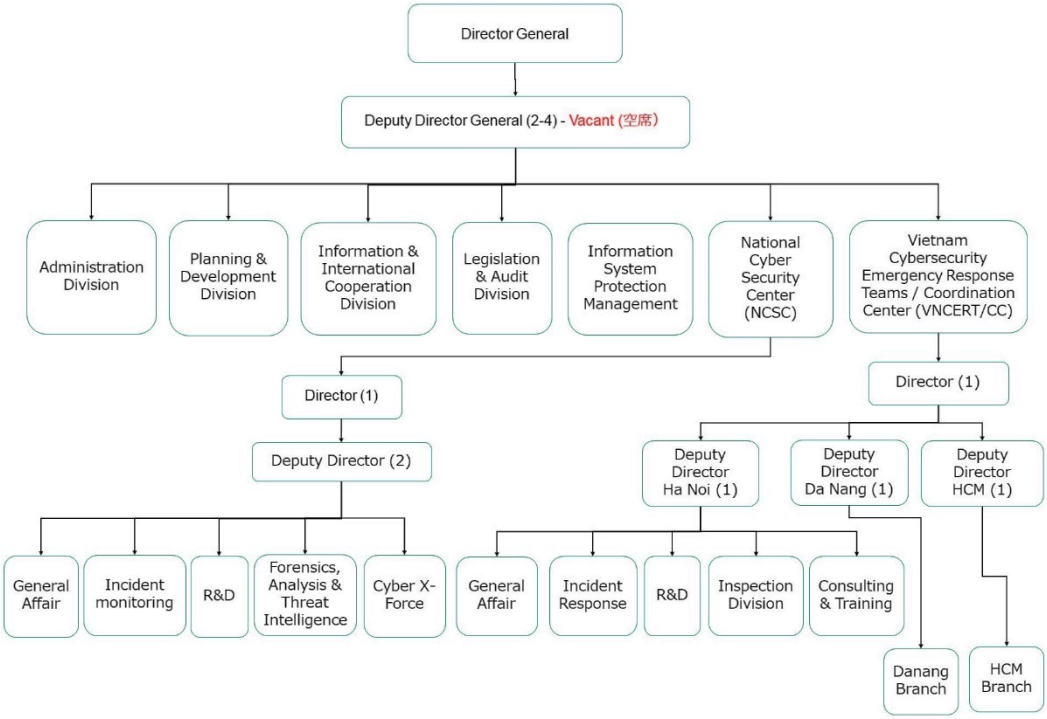
1.5.1 政策・制度面

2020年の首相決定第749号「2025年までの国家デジタルトランスフォーメーションプログラム」の中でサイバーセキュリティはデジタルトランスフォーメーションを成功させ、社会を持続可能なものにするための鍵であると捉えている。2021年6月の首相決定（第830号）「創造的で安全にサイバー空間を利用する青少年の保護と支援プロジェクト（2020年～2025年）」を根拠として、特に脆弱な若年層や青少年へのサイバーセキュリティ・情報セキュリティに関する普及啓発活動を推進している。これらの戦略中でAISの果たすべき役割に変更はない。

したがって、政策・制度面での持続性は高いと判断される。

1.5.2 体制面

AISは2020年11月にVNCERT/CCを併合して以降も業務効率化のため小規模な組織変更を進めている。2022年2月時点でのAISの組織構造は以下の通りである。



VNCERT/CCの支所があるダナン市とホーチミン市はリソースが不足しているが、これらの支所を含めて各部署において積極的に人材確保に努めている。2022年2月時点で、プロジェクト開始時に4名いたAIS副局長が0人となっており、業務管理体制が脆弱になっている。ただし、予定されている副局長2名が2022年3月頃に着任すれば、体制に概ね問題はないものと判断される。

1.5.3 技術面

異動や退職というリスクは常にあるものの、本プロジェクトによって教育を受けた職員が業務を継続する限り、技術については大きな問題はない。ITやサイバーセキュリティに関しては一度技術を学べば終わりではなく、常に新しい技術を学んでいく必要がある。MICは定期的な研修のための予算を確保しており、本プロジェクトを通じてキャリア開発の重要さを理解した職員であれば、どのような研修からも一定の新しい知見を学べるはずである。本プロジェクトにより移転された技術・知識は研修教材やマニュアル等で蓄積されており、それらはOJT教育として活用されれば、十分に技術継承することが可能である。新しい人材の確保についても引き続き、大学レベルの知識と意欲を持った職員を確保し続けていることから、異動が多い業界においても技術を持った一定数の人員が確保されることが期待される。供与された機材については、類似の機材はこれまでも運用・維持管理してきた実績があることから、大きな問題はないものと考えられる。

以上より、技術に関して、問題はないものと判断される。

1.5.4 財務面

MICの財務に関する詳細情報は入手できていない。ただし、AISが引き続き取り組むべき課題であるCOP、CC評価認証制度、ISAC設立等については2022年以降政府のプロジェクト予算が確保されているとのことである。

以上より、本プロジェクト終了後の財務に関しては詳細情報がなく判断できない。また、体制に軽度な課題があることから、本事業によって発現した効果の持続性は中程度である。

2. 実施と結果に影響を与えた主な要因

プロジェクト開始時から終了時までに管理していたリスクとその対応方法は以下の通りである。[ ]内は対応したときのモニタリングシートのバージョンを示している。

リスク	インパクト レベル [4]	状況と対応
1. 機材供与免税の問題	効率性 低い	[MS1] 2019 年 6 月のプロジェクト開始直後、外務省・財務省が免税手続きに必要な「援助証明書」を発行していないことが判明した。その結果、ベトナムのプロジェクト実施機関が、提供された機材の免税手続きを行えないケースがあった。 [PCR] 免税問題は 2019 年 11 月に解決済み。
2. SecBoK 定義の役割とスキルマップの問題	効率性 有効性 低い	[MS1] SecBoK の役割の定義と役割への技術のマッピングが曖昧であったり、間違っていたりする場合がある。大きな問題が発生しない場合は、SecBoK の役割とマッピングをそのまま使用する。問題が発生した場合は、プロジェクトで独自にマッピングを調整する。
3. SecBoK への研修マッピング	効率性有効性 低い	[MS1] マッピングは未実施のため、次回の CDP レビューのタイミングでマッピングを行う。 [PCR] 2022 年にキャリア開発計画の成果物としてマニュアルに組み込んで作成。
4. トレーニングの欠席	効率性 有効性 中	[MS1] これまで実施された CompTIA Security+、CEH において、欠席した研修生がいた。CEH の資格取得だけを目的にして、研修自体に参加しなかった研修生もいた。 研修生は資格取得が目的ではなく、業務上の実務能力を向上させることが目的であることを理解する必要がある。 [MS2] これまで実施した CompTIA Security+、CEH、CCNA Security の一部の講義を欠席した研修生がいる。CEH の資格だけが目的で講義を欠席したり、CCNA Security で受講を断念した研修生もいた。その対策として、ECSS の講座からは、プロジェクトチームが受講者の受講意思を確認するようにした。講義の冒頭で、研修生は全講義に出席すれば認定試験を受ける要件を得られること、やむを得ず欠席する場合は事前に JICA に連絡することを再度アナウンスした。研修生は、資格取得が目的ではなく、業務上の実務能力を向上させることが目的であることを理解する必要がある。

[4] 低い, 中, 高い, 非常に高い

5. 資格試験の受験	効率性 有効性 中	[MS1] 研修後に資格試験を受けるのは、研修の成果を測定することが目的。資格試験の合格率を高めるために、以下の条件を適用する。（3 回目の研修から適用） (1) 全ての講義に出席すること（合理的な理由による欠席を除く） (2) 研修の 1 ヵ月後に実施する模擬試験で合格率 90%以上であること 合格した場合はプロジェクトが資金を提供し、不合格の場合はカウンターパートが負担する。資格試験受験の目的は研修の成果を測定することであるため、今後はすべての研修生が資格試験を受験することを検討する。 [PCR] 最終的には、オンライン模擬試験において以下を満たす受講生が 1 度だけ資格試験を受験できることとした。 (1) 最低でも 10 回は挑戦すること（書籍等で学習している場合は適用しない） (2) 直近過去 3 回分の平均スコアが 90%以上」または「連続 2 回 90%以上」
6. 機器調達の遅れ（DDoS attack mitigation system）	効率性 有効性 中	[MS1] プロジェクトドキュメントの承認に時間がかかっている。このプロセスは、ベトナムの様々な省庁が関与しているため、コントロールが困難である。AIS に働きかけて、2020 年までに機材調達する。 [MS2] 2020 年 6 月 3 日にプロジェクトドキュメントが承認された。今後は、2020 年までに AIS の整備と機器の調達を行う予定。 [PCR] 2021 年 3 月に納品完了。
7. 普及啓発教材開発の遅れ	効率性 有効性 中	[MS1] プロジェクト開始後、普及啓発担当者との調整に多くの時間（8 カ月）を費やし、教材開発が開始されなかった。2020 年 3 月に活動の方向性を合意したため、2020 年 4 月以降に教材作成を再開する予定。 [MS2] 第 1 弾のビデオ作成に着手。 [PCR] プロジェクト終了までに 3 本のアニメーション動画を作成した。
8. プロジェクト終了後の持続可能性の確保	持続性 中	[MS1] • 開発援助委員会（DAC）の 5 つの評価項目である（政策、技術、組織、財政の面でプロジェクトの成果が持続するか）のうち、持続可能性に関するベトナム側の方針と取り組みについて。2020 年 1 月現在、AIS では政府におけるセキュリティ担当者の役割と必要な技術分野の分類を検討していた。SecBoK や NICE Framework とは異なる分類だが、これらとのマッピングを作成することで、今後の効率的な研修計画や人材育成に役立てることができるかもしれない。プロジェクトチームでは、今後、CDP の作成・管理方法を指示するガイドラインを作成し、プロジェクト終了後も活用できるようにする予定である。

		• 技術力を持った職員が転職してしまうリスクは常にある。しかし、プロジェクト側からそれをコントロールすることは難しい。例えば、資格を保持する職員には AIS から何らかのインセンティブを与えるなどすれば、多少の改善につながるかもしれない。 • 啓発活動について、サイバーセキュリティは変化が激しい分野である。それに対して、パスワードの強化やフィッシング攻撃への対策は、しばらくは重要であり続けるだろう。教材を開発した後は、継続的な活用が期待される。 • 機器について、必要なメンテナンスを行うことで、継続的に利用されることが期待される。それでも、IT 機器は年々仕様が向上していくので、必要なタイミングで更新していく必要がある。
9. ベトナムで開催可能なコースの制限	効率性 有効性 中	[MS2] 以下の予定されているコースは、場所（海外）や費用の問題で実施が困難である。 SEC542: Web App Penetration Testing and Ethical Hacking, SEC511: Continuous Monitoring and Security Operations, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting, FOR578: Cyber Threat Intelligence, SEC560: Network Penetration Testing and Ethical HackingFOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
10. オンライン学習と資格試験の受験 No.5 リスク関連	効率性 有効性 中	[MS3] 1. 状況：報告対象期間である過去半年間で、オンライン学習や資格試験を受けた研修生が非常に少なかった。第 2 回 CDP レビューでその理由を尋ねたところ、以下のような理由が挙げられた。プロジェクトマネジメント研修（CAPM、PMP）において、国際標準のプロジェクトマネジメント手法がベトナムのマネジメントにそぐわないと感じている。そのため、学習意欲が保てなかった。 2. 年末にかけて研修生が業務に忙殺された。 対策： • プロジェクトマネジメント研修では、以下を理解し、できるだけオンラインで学習することを推奨した。 o すべての内容を業務に適用する必要はない。 o スケジュール管理、人材管理など部分的に適用できる内容は取り入れるようにする。 o 海外のステークホルダーと仕事をする際に、国際標準のマネジメント手法が参考になる場合がある。 • 2020 年 11 月までに実施した研修については、オンライン学習期間を 2021 年 3 月まで延長し、条件を満たせば資格試験を受けることができるようにする。 • 将来的には、集中研修後のオンライン学習期間を約 3 ヶ月以上に延長する予定。 オンライン学習状況のモニタリングを強化し、学習や資格試験受験を促すメールを頻繁に送信する。

11.プロジェクトドキュメントの承認と更新 R/D への署名の遅れ No.6 リスク関連	効率性 有効性 高い	[MS3] 状況： 2020 年 8 月の第 2 回 JCC で決定したプロジェクト期間の延長については、更新されたプロジェクトドキュメントの承認と更新された R/D への署名に時間がかかる可能性がある。以下は、承認・署名後に調達が可能となるため、プロジェクト活動に大きな影響を与えることになる。 • マルウェア解析機器 • 評価用ラボ機器 • ISAC 専門家 • 普及啓発の専門家 対策： • 各工程の状況をこまめに把握し、AIS 幹部、JICA ベトナム事務所の協力を得て、工程を進める。 • 更新 R/D の内容を前倒しで確定し、更新プロジェクトドキュメントの承認後、直ちに署名できるようにする。 承認・署名後すぐにプロセスを進められるよう、追加機材や専門家の調達を前倒しで準備する。
12.マルウェア解析・評価用ラボ機器の納期遅れ	効率性 有効性 高い	[MS4] 2020 年 8 月に第 2 回 JCC で追加が決定した評価ラボと、当初からコンポーネントとして含まれていたマルウェア解析機材について、AIS から数回の追加要求があった。その後、仕様決定が 2021 年 1 月までかかった。その後、ベトナム政府内のプロジェクトドキュメント承認手続きに時間がかかり、2021 年 6 月 30 日現在、承認が完了していない。2021 年 7 月に承認された後、更新された RD の署名手続きにさらに 1 カ月ほどかかると想定される。 したがって、機器の調達は 2021 年 7 月末頃から始まり、納品は早くても 2021 年 9 月末から 10 月頃になる。2022 年 1 月～3 月がプロジェクトの整理期間であり、この期間をバッファーとしたとしても、2021 年 12 月までに機器をセットアップして稼働させる必要がある。プロジェクトドキュメントが承認された後、円滑かつ効率的に機器の調達とセットアップを行うために、次のような対策を取ることとする。 • RD の事前準備：AIS の事前確認、JICA 本部の事前確認が完了。 • 機材見積もり作成：2021 年 4 月末に最新版を入手したが、2021 年 6 月に期限切れとなったため、2021 年 7 月に最新版を入手する予定。 • セットアップの事前準備を十分に行う：受入準備として、AIS は設置場所の確保とネットワーク設定の確認を事前に行う必要がある。 • 運用サポート：マルウェア解析機材や評価ラボに関する運用ポリシーや手順書の作成を現地企業に依頼する予定。また、JPCERT/CC は、マルウェア解析機材に関するアドバイスも行う。 [MS5] 状況： マルウェア解析機材およびラボ機器の一部は、プロジェクト終了日（2022 年 3 月）より遅れて納入される可能性が高い。

		対策： プロジェクトと JICA は、2022 年 4 月以降の納入を可能にするため、数ヶ月の延長を検討している。 ただし、機材領以外の活動は 2022 年 3 月末に完了する予定。
13. COVID-19	効率性 有効性 高い	[MS4] 2021 年 5 月以降、ベトナム全土で COVID-19 の状況が悪化している。ダナンまたはホーチミンの研修生は、状況に応じてオンラインで研修に参加することとする。講師がホーチミンに在住している場合は、研修自体をオンラインで実施する予定。 [MS5] 2021 年後半から、ベトナム政府はロックダウンなどの厳しい措置は取らず、COVID-19 の接種と共存を促進する姿勢を取っている。本プロジェクトは、政府の感染症対策に則り、十分な注意を払いながら活動を続ける。
14. フェーズ 2 要請の遅れ	- 高い	[MS4] フェーズ 2 のプロジェクトで想定されているコンポーネントについて、現プロジェクトでも職員の能力強化の面で一定の支援が行われている。プロジェクトの効果を最大化するために、フェーズ 2 プロジェクトは現プロジェクト終了までに開始することが推奨される。また、要請期限が 2021 年 8 月末であることから、正式な要請書の提出に向け、可能な範囲で協議を進めている。

この中で特にプロジェクトの実施と結果に影響を与えたのは以下であった。

6. 機器調達の遅れ（DDoS attack mitigation system）
11. プロジェクトドキュメントの承認と更新R/Dへの署名の遅れ
12. マルウェア解析・評価用ラボ機器の納期遅れ

第2回JCCにおいて当初から計画していたマルウェア解析機材の種類を増やし、またCC評価機材も追加したが、これらの機材調達は遅れたことにより、2回目のプロジェクト延長が必要になってしまった。COVID-19の影響が大きいと言えるが、機材調達を早くに開始できていればプロジェクト期間内に間に合った可能性がある。機材調達はベトナム政府内でのプロジェクトドキュメント承認を待つ必要があったが、この承認は機材追加と延長が決定した第2回JCCから1年後になされたため、調達を早くに開始することは難しかった。

3. リスク・マネジメントの結果に関する評価

(1) リスク・マネジメント結果

リスクとその対処内容は「2. 実施と結果に影響を与えた主な要因」に記載。

(2) 過去の教訓の活用結果

過去の類似案件の教訓と本事業への活用は以下の通りであった。

- 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のため、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情報セキュリティマネジメントシステム（ISMS: Information Security Management System）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。

ASEAN地域諸国においては、サイバーセキュリティに係る担当者は限定的な一方、サイバーセキュリティにかかる研修や国際会議は本邦、他国含めて数多く行われており、主要なカウンターパートが不在、国内にいても日常業務が多忙とすることが多く、活動の進捗に影響を及ぼす可能性がある。

- 本事業への教訓

実施計画の検討に際しては、AISの体制や実際の業務状況を十分に確認した上で支援計画を検討すると共に、特に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。

教訓の活用結果については以下の通り。

AISはJICAプロジェクト以外の研修の受講状況を事前に共有することはなかった。またプロジェクトからも毎回NISC等に研修状況を確認することは難しかった。しかし、CDPレビューや現地研修の調整の段階で、他の研修の状況を把握できたため、他の研修と被ることによる研修生の不参加等はなかった。

AISの幹部を通して研修生への業務の調整を依頼しても、突発的な業務が発生することは防げなかった。

4. 教訓

本プロジェクトから得られた教訓は以下の通りである。

(1) 中長期的な知識・技術向上のための方法（資格試験に紐づく研修）

本プロジェクトでは、研修員の知識を定着させるために、5日間程度の短期集中研修の後に、3−5カ月のオンライン自己学習あるいは講師によるコーチングを実施した。さらに、オンライン学習で高得点を取った研修生に対しては、1度だけ資格試験を受験できる機会を提供した。技術者にとっては一部の資格はキャリアにとって重要視されている一方で、高額なため個人での受験が難しい場合がある。本プロジェクトでは、資格試験受験をモチベーションとして、中長期的な知識定着を目指すことに成功した。なお、資格試験の合格はプロジェクトの目標とはせず、研修員のモチベーションを高めるために、条件を満たす場合に受験機会を提供するのみとした。

(2) 研修に集中できる環境の準備

本プロジェクトでは、合計87回の研修を実施し、600名以上の研修員が参加した。多くの研修員は研修に集中していたが、一部の研修員は直前でキャンセルしたり、研修への参加率が低かったりした。その理由は、研修日の開始前と終了後に業務があり集中できなかった、上司（場合によっては副大臣級から）至急の業務を依頼された、セキュリティインシデント対応していた、求めている研修内容ではなかった、等であった。

今後の技術協力プロジェクトで、集中研修を実施する場合は、以下のように各要因に対して対応することが望ましい。

- 通常業務への対応

研修は研修員の職場があるハノイで行われることがほとんどであったため、研修員は容易に業務へ戻ることができる状況であった。地方都市から出張で参加している研修生は、職場から離れているということもあり、集中できていたようであった。研修員本人と所属組織幹部に対して、研修員が研修に集中できるように調整を依頼しても、適切に実施されないことがあった。研修を実施するペースや予算にもよるが、研修に集中させるために、職場から離れた場所に宿泊して実施することが望ましい。

- 研修内容の共同設計

カスタム研修は研修員とともに、時間をかけて共に内容を設計していることが望ましい。そのようにすれば、研修開始後に内容に対して意見が出ることは減ると思われる。

(3) 現地リソースと日本リソースの使い分け

本プロジェクトでは、ほとんどの現地研修・調査・ポータル開発・動画作成等については、現地のリソースを活用した。特に研修やコンサルティングについては、サイバーセキュリテ

ィの分野に限定したとしても、協力国内に一定レベルの人材が存在しており、本プロジェクトの様々なニーズに対して重要な協力を提供してもらうことができた。現地リソースで対応できない課題や、日本の経験が必要な場合は日本の専門家が指導することで、コスト・調達・人材のバランスを取りつつ活動することができた。

今後のサイバーセキュリティ（広くはICT分野）の技術協力プロジェクトにおいては、現地のリソースを活用できるか十分に検討することが望ましい。現地リソースの場合、コストを低く抑えることができ、契約までの時間も短くすることが可能である。また、現地の公用語を話せる場合は、コミュニケーションが円滑に進み、内容に集中することができる。

(1) ベトナムにおける機材調達プロセス

本プロジェクトでは総数201（ハードウェア146、ソフトウェア55）の機材を調達した。機材仕様をカウンターパートと調整した後、ベトナム政府内の文書であるプロジェクトドキュメントに同仕様を記載の上、承認後に機材調達を開始した。基本的にはプロジェクトドキュメントに記載した仕様通りの機材を調達する必要があるが、調達プロセスの中で以下のような問題が発生した。

- 承認までに数か月かかり、仕様決定から調達までの時間があいたことで、当初定めた仕様が古くなった。
- 調達段階になって初めてベトナム国内で販売されている製品の情報が明確になった。
- 調達の段階で漏れていた仕様が明確になった。（生産国等）
- CPU・メモリなどの仕様は満たすが、実際に求めている機種がベンダーから提案されないケースがあった。

結果として調整に時間がかかってしまい、当初のプロジェクト期間内にすべてを調達することができなかった。また、機材設置や運用に関する技術的な支援も十分に提供することができなかった。プロジェクトドキュメントの承認に時間がかかることは避けがたい。また、時間が経過するにつれて求める条件が変わり、設定した仕様が古くなることもITシステム開発ではよく発生する事象である。

本件の問題は、プロジェクトドキュメントと実際の調達書類の仕様をまったく同じものとして記載していたことに1つの原因があると考えられる。よって、今後のベトナムにおける技術協力プロジェクトで機材供与する場合は、以下のように対応することが望ましい。これらのよって、プロジェクトドキュメントと調達書類の一貫性を保ちつつ、手戻りを少なくすることが可能となる。

- プロジェクトドキュメントには、機材の種類（ワークステーション・ストレージ等）、CPUやメモリ等の最低限の仕様のみを記載する。
- 調達の段階で、プロジェクトドキュメントに記載した仕様を満たしつつ、具体的な機種・原産国等を明記する。

IV. プロジェクト終了後の上位目標達成のために

1. 上位目標達成の見込み

上位目標については、「III.合同評価の結果 1. DAC評価基準に則った評価結果1-4. インパクト」を参照。ここでは、上位目標の指標の適切性について述べる。（見直しは行わない）

上位目標の指標をAISが発行する定期レポートとしていたが、プロジェクト開始から終了までの間にこのレポートは発行されていない。そのため、上位目標の達成状況を判断することができない。一方で、2021年にベトナム政府はサイバーセキュリティに関してGlobal Cybersecurity Index（GCI）を向上させることを目標として掲げた。CGIの評価項目が上位目標に貢献すると考えられるAISのミッションの成果を反映するものであるならば、CGIを指標の1つに追加することも考えられる。

2. 上位目標達成のためのベトナム側の計画・実施体制

上位目標達成に向けて、プロジェクトで関わった各ミッションのAISの実施体制は以下の通り。これらのミッションに関する政策や計画は「III.合同評価の結果 1. DAC評価基準に則った評価結果 1-1. 妥当性」に記載したベトナムの政策に記載されている。

ミッション	責任組織
Common Criteria 評価制度構築	VNCERT/CC (Inspection Division)
COP 政策実施	VNCERT/CC (Inspection Division)
ISAC 設立	AIS (Threat Intelligence Division)
CSIRT 業務	NCSC, VNCERT/CC
TSUBAME 運用	VNCERT/CC

3. ベトナム側への提言

プロジェクト活動を通じて様々な場面でAISに対して、サイバーセキュリティに関する持続的な能力強化のために以下のような提言を行ってきた。詳細はここでは記載しないが、上位目標の達成に向けて、これらの優先度をつけて対応していくことが望ましい。

3-1 CDP方法の継続的な運用

プロジェクトが実施した方法をそのまま継続することはリソース的にも非常に難しいが成果品の1つであるCDPマニュアル等を活用して、部分的に導入することを検討して、キャリアを意識した体系的な研修を実施することが望ましい。

3-2 ISAC設立

ベトナムの周辺国のISAC設立運用についての調査結果報告書がVietnet-ICTによって作成された。この報告書には調査結果を踏まえたコンサルタントからの具体的な提言もあることから、今後のベトナムにおけるISAC設立のための参考として利用できる。

日本の金融ISACやICT-ISACによるセミナーを実施して日本の知見や経験を共有した。ISAC設立に向けて、セミナー資料や日本の専門家からの提言を参照することが望ましい。

3-3　COP政策の推進

日本の普及啓発活動および教材、マーケティング手法のセミナーを実施した。また、普及啓発のマスタープランやAISが取り組んでいる政策についてJICA専門家から助言を行った。特にCOP政策は今後もAISの重要な政策であり、国民へのインパクトも大きいことから、プロジェクトで得られた知見を具体的に活用することが望ましい。

3-4　機材における運用管理

機材の使用者やステータスを資産管理の一部とし管理することが望ましい。また、解析ツール等は利用期限があるため、使い続けるための更新費用を確保することが望ましい。

3-5　Common Criteria評価制度構築

研修やコンサルティングを通じて、評価制度に関する多くの情報を提供した。供与した機材を利用した簡易評価制度の仮運用から始めることが望ましい。また並行して、CCRAへの加入も進めることが望ましい。

3-6　TSUBAME運用

2021年6月に実施したJPCERT/CCによるCSIRT研修において、TSUBAMEによる運用のアドバイスやベトナム国内の脆弱性に関する情報が共有された。これらの助言を計画的に実施することで、脅威情報の収集能力や脆弱性対応の能力が向上することが期待される。

4. プロジェクト終了から事後評価までの間のモニタリング計画

供与の遅れた機材（マルウェア解析、Common Criteria評価機材）の運用状況と、国民へのインパクトの大きさから普及啓発教材の活用状況に関して、JICAから四半期（3ヵ月）毎にメール等で遠隔モニタリングする。

【確認項目】

- マルウェア解析機材の運用状況
- CC評価機材の運用状況
- 普及啓発教材（動画、デザインキット、ポータルサイト）状況の活用状況
- 研修で得た知見や教材の活用状況等

付録

1. Plan of Operation (PO)
2. Project Design Matrix (PDM)
3. 専門家派遣
4. 活動と成果の関係
5. CDPフォーム記入済み例
6. 研修リスト
7. 成果と研修の対応表
8. プロジェクトの成果物
9. 研修結果
10. 研修生からのフィードバック
11. 機材リスト
12. 活動、投入、成果
13. R/D, M/M （写し）
14. モニタリングシート（写し）
15. 合同調整委員会（Joint Coordination Committee (JCC)）
16. CDPレビューのコメント集7

付録1：Plan of Operation (PO)

POを添付

付録2：Project Design Matrix (PDM)

PDM version 1（2019年3月8日署名）を添付

PDM version 2（2021年8月24日署名）を添付

PDM version 3（2022年3月X日署名）を添付

付録3：専門家派遣

計画		実績
	長期専門家	
	サイバーセキュリティ／業務調整	役割：プロジェクトの全体調整 2019 年 6 月 26 日から 2022 年 3 月 14 日まで派遣
	短期専門家　*マークは第 2 回 JCC で追加された	
	チーフアドバイザー	役割：JICA 専門家チームの統括 専門家のすべての活動はオンラインで行った。
	サイバーセキュリティ／キャリア開発	役割：キャリア開発計画の作成とレビュー、プロジェクト活動の支援 第 1 回目派遣：2019 年 7 月 28 日から 9 月 25 日（60 日間） 第 2 回派遣：　2019 年 11 月 6 日から 12 月 10 日（35 日間） 第 3 回派遣：　2021 年 11 月 25 日から 2022 年 1 月 22 日（60 日間） CoVID-19 のため、第 3 回派遣以降の派遣は中止または延期となった。その間は、専門家はすべての活動をオンラインで行った。
*	ISAC 専門家	役割：研修活動の一環として ISAC の設立を支援 専門家のすべての活動はオンラインで行った。
*	普及啓発専門家	役割：日本の普及啓発活動・教材の調査、および研修 専門家のすべての活動はオンラインで行った。

以下の専門家は、PDMに詳細を計画していなかった、セミナーやオンライントレーニングを通じてプロジェクトに協力した。

総務省、経済産業省、明治大学、JPCERT/CC、情報処理推進機構（IPA）、金融ISAC、ICT-ISAC、株式会社ECSEC、株式会社あるモリス、牛島総合法律事務所、

付録4：活動と成果の関係

No	Activity	Output 1	Output 2	Output 3
1	Clarify the required roles defined in SecBoK framework	1.1	-	-
2	Develop a Career Development Plan (CDP) for each staff based on SecBoK Framework	1-2	-	-
3	Develop a training course plan for high prioritized roles defined in SecBoK Framework	1-3 CISO, Commander, etc.	2-1 Incident manager, Incident handler, Triage, etc.	3-1 Researcher, Solution analyst, Vulnerability diagnostic consultant, Information security auditor, etc.
4	Conduct training	1.4	2-2	3-2
5	Review CDP (e.g., every six months)	1.5	2-3	3-3
6	Plan and conduct training for policy maker	1-6	-	-
7	Develop/localize awareness raising materials	1-7	-	-
8	Expand reactive and proactive infrastructure in AIS	-	2-4 reactive infrastructure (e.g., DDoS attack mitigation)	3-4 proactive infrastructure (e.g., network monitoring)

付録5：CDPフォーム記入済み例

CAREER DEVELOPMENT PLAN [DDDD] LAST UPDATE: 10 Feb 2022

Name	Mr. Sample	CDP-ID	CDP-X-XXX

1 Division & Title

Division: Monitoring & Incident Response

Title: N.A.

2 Job Description, Responsibility

(1) Monitoring Server, PCs, Networks. Execute the monitoring tasks in real-time in order to provide notification, alert or warning in time.

(2) Support evaluating infrastructure of clients (NCSC's business).

3 Assigned Security Role(s)

☐ CISO ☐ POC (Point of Contact) ☐ Notification ☐ Commander ■ Triage

☐ Incident manager ■ Incident handler ☐ Curator ☐ Researcher ☐ Self assessment

☐ Solution analyst ☐ Vulnerability diagnostic consultant ☐ Education / Awareness raising

☐ Forensic engineer ☐ Investigator ☐ Legal advisor ☐ IT planning division

■ IT system division ☐ Information security auditor ☐ Licensing ☐ Policy making

■ SOC (Security Operation Center)

☐ Other ( ) ■=marked

4 Required Knowledge and Skills for the Roles (General description)

(1) Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration , hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).

(2) Skill & understanding of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). Insight of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.

(3) Understanding of crisis management protocols, processes, and techniques. Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.

5 Knowledge and Skills to be acquired or improved

To the date of the 2nd review, he has get more progression in his career path in AIS also. Now he is primary official responding to the infrastructure services. He will keep on track with latest Linux foundation to manage the servers with LPIC-1 training, heading towards LPIC-2 if possible. Starting from Dec 2020, English training for the A2 level (CEFR) brings him two sessions per week with native speaker, also with customized content in cybersecurity. In preparation for a dynamic future of his career, Certified SOC Analyst (CSA) is assigned to him within next 6 months. Per his good performance, CEH is also added after the 3rd review.

6 Training plan, progress and result

No.	Course Title	Code	Vendor	Course provider	Planned Month	Attending Date		# hours	Cert.	Progress	Remark
						From	To				
e.g.	CompTIA Security Plus	CompTIA S+	CompTIA	XXX Corp.	Dec 2019	1 Dec 2019	7 Dec 2019	40	Passed	100%	Memo
1	Certified Network Associate	CCNA	Cisco	iPMAC	Jan 2020	13 Jan 2020	17 Jan 2020	40	Failed	70%	
2	Certified Security Specialist	ECSS	EC-Council	iPMAC	Mar 2020	02 Mar 2020	27 Mar 2020	40	Passed	70%	
3	VMware: vSphere Install, Config, Manage	VCP-DCV 1	VMware	Qnet	Nov 2020	30 Nov 2020	04 Dec 2020	40	Passed	100%	
4	VMware: vSphere Optimize & Scale	VCP-DCV 2	VMware	Qnet	Dec 2020	21 Dec 2020	25 Dec 2020	40	Passed	100%	
5	Linux Administrator	LPIC-1	LPI	SaigonCTT	Apr 2021	22 Apr 2021	29 Apr 2021	40	In Progress	80%	completed 11 times but avg. score is about 92.00 in June 2021.
6	*CSIRT organization, process and activity	CSIRT	Custom	JPCERT/CC	Jun 2021	15 Jun 2021	18 Jun 2021	24	N/A	75%	
7	Certified SOC Analyst	CSA	EC-Council	iPMAC	Jun 2021	21 Jun 2021	06 Jul 2021	40	Passed	100%	
8	Certified Ethical Hacker	CEH	EC-Council	iPMAC	Sep 2021	20 Sep 2021	24 Sep 2021	40	Failed	100%	
9	*Business English Course for Cybersecurity Beginner	ESP-BEG	Custom	Language Link	Dec 2020	01 Dec 2020	01 Jun 2021	48	Passed	75%	
10											
11											
12											
13											
14											
15											

PROGRESS REVIEW

Name	Mr. Sample	CDP-ID	CDP-X-XXX

1	**Review 1**	[Date	11 Jun 2020]
	His Infrastructure management task is now covered for both server and network. He found out the ECSS is more simpler than CCNA S. For the CCNA S, he found new knowledge which could master the skill & harden the current AIS system and evaluating clients' system.		
2	**Review 2**	[Date	14 Dec 2020]
	No change in his position, but his task list are huge now because a senisor guy who was primary in charge for the infrastructure moved out of AIS. Now he and one new official are assigned to work as system admin. He enjoys the English class with native speaker, also appreciates the training for virtualization technology as a helpful chance to consolidate his knowledge for the daily tasks. The continuous connection with trainer is also advantage to give him supportive resources after the training.		
3	**Review 3**	[Date	11 May 2021]
	LPIC-1 helps him to enhance his knowledge about the Linux operating system. VMware is also one of his familiar area, but the training is also helpful to him e.g. Virtual SAN, network. English (LL) course is quite simple for him, the approach for training is fine. For the next six month, CEH is added to support for further incident response activity.		
4	**Review 4**	[Date	29 Nov 2021]
	Within two years, he has joined several trainings, and having understanding in several courses. The course helped him to understand the procedures in incident response. The whole course seems to help him see the policy than the technical training. He will try to take the LPIC-1 exam within December 2021. It seems the new CEH exam was tough for him, but he has gained the core value from the intensive training.		
5	**Review 5**	[Date	]
6	**Review 6**	[Date	]
7	**Review 7**	[Date	]

付録6：研修リスト

No	Category	Course Name	Vendor	Training Institutes	Date
1	General Security knowledge	CompTIA Security +	CompTIA	NetPro NetPro SaigonCTT NetPro NetPro	September 2019 June 2020 June 2020 October 2020 September 2021
		Certified Security Specialist (ECSS)	EC-Council	iPMAC iPMAC iPMAC iPMAC iPMAC iPMAC	Mar 2020 May 2020 October 2020 April 2021 August 2021 October 2021
2	Network, Network Security	Cisco Certified Network Associate (CCNA)	Cisco	NetPro	May 2021
		Cisco Certified Network Professional Security (CCNP Security)	Cisco	NetPro NetPro	January 2020 January 2020
3	Security Manager, Auditor	Certified Information Systems Security Professional (CISSP)	(ISC)2	iPMAC	June 2021
		Certified Information Security Manager (CISM)	ISACA	Qnet Qnet	July 2020 August 2021
		Certified Information Systems Auditor (CISA)	ISACA	iPAMC	March 2020
4	Hacking, Pentesting	Certified Ethical Hacker (CEH)	EC-Council	Cecomtech Cecomtech iPMAC iPMAC Cecomtech iPMAC iPMAC iPMAC iPMAC	December 2019 May 2020 November 2020 January 2021 April 2021 September 2021 September 2021 January 2022 January 2022
		Licensed Penetration Tester (LPT)	EC-Council	Cecomtech	August 2021
		PEN200: Penetration Testing with Kali Linux (OCSP)	Offensive Security	Cecomtech Cecomtech Cecomtech iPMAC	November 2020 May 2021 August 2021 January 2022
		Offensive Security (OSWE) | Advanced Web Attacks and Exploitation (WEB-300)	Offensive Security	Cecomtech Cecomtech	December 2021 January 2022

No	Category	Course Name	Vendor	Training Institutes	Date
5	Coding, Development	Cyber Secure Coder (CSC)	Logical Operations	Qnet	July 2021
6	Project Management	Certified Associate in Project Management (CAPM)	PMI	iPMAC	September 2020
		Project Management Professional (PMP)	PMI	iPMAC iPMAC iPMAC iPMAC	August 2020 September 2020 October 2021 January 2022
7	Infrastructure	Linux Administrator (LPIC-1)	LPI	SaigonCTT SaigonCTT	June 2020 April 2021
		VMware: vSphere Install, Config, Manage	VMware	Qnet	November 2020
		VMware: vSphere Optimize & Scale	VMware	Qnet	December 2020
8	Threat Intelligence	Certified Threat Intelligence Analyst (CTIA)	EC-Council	iPMAC iPMAC	May 2021 January 2022
9	SOC, CSIRT	Certified SOC Analyst (CSA)	EC-Council	iPMAC iPMAC	June 2021 August 2021
		Defense Practice against Cyber Attacks	Training in Japan (online)	JICA	September 2020 February 2021 November 2021
		CSIRT organization, process and activity	Custom	JPCERT/CC	July 2021
		Cyber Exercise	Custom	Cecomtech	November 2021
		Building and Operation of Cyber Exercise	Custom	JICA	January 2022
10	Forensics, Malware Analysis	Malware Analysis	Custom	JPCERT/CC	December 2021
		Malware Analysis Tools	Custom	iPMAC	February 2021
		Computer Hacking Forensic Investigator (CHFI)	EC-Council	Cecomtech Cecomtech NetPro	July 2020 June 2021 September 2021
11	Policy, Regulation, Governance	Security Policy Making	Custom	JICA	June 2021
		Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	Training in Japan	JICA	February 2020
		Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity	Training in Japan (online)	JICA	October 2021
12	Awareness Raising	Awareness raising seminar	Custom	JICA	August 2021
13	International Standard	International Standards: ISO/IEC 27000 family	Custom	SaigonCTT	March 2021
		International Standards: US NIST SP800	Custom	NetPro	September 2021
		International Standards: GDPR	Custom	iPMAC	November 2021

No	Category	Course Name	Vendor	Training Institutes	Date
14	Security Evaluation	International Standard: Common Criteria	Custom	Individual	August 2020
		International Standard: ISO/IEC 17025	Custom	SmartPro	February 2021
		Security Evaluation Online Seminar	Custom	JICA	February 2021 March 2021
		Common Criteria (Protection Profile-Security Target-Target of Evaluation)	Custom	SmartPro	July 2021 August 2021
		Evaluation Lab Operation	Custom	SmartPro	January 2022
15	Critical Information Infrastructure	ISAC Online Seminar	Custom	JICA	February 2021
		JP-US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region	Training in Japan (online)	METI	March 2021 October 2021
		Critical Information Infrastructure Protection	Custom	NetPro	November 2021
		Industrial Control Systems Cybersecurity Training for Indo-Pacific Region	Training in Japan (online)	JICA Tokyo	February 2021
		Strengthening of Cooperation Among Organizations Against Cyberattacks	Training in Japan (online)	JICA Tokyo	February 2021
16	English	Business English Course for Cybersecurity 1 (HN)	Custom	British Council	October 2020 – December 2021
		Business English Course for Cybersecurity 2 (HN)	Custom	ILA	December 2020 – August 2021
		Business English Course for Cybersecurity 3 (HN)	Custom	British Council	October – December 2021
		Business English Course for Cybersecurity 4 (HCMC)	Custom	British Council	November – December 2021
17	Training in Third Country	Third country training in Indonesia	Training in third country	JICA	December 2019

付録7：成果と研修の対応表

★
◎：強い関連あり
○：関連あり

No	Category	Course Name	**Output 1** Management	**Output 2** Reactive	**Output 3** Proactive
1	General Security knowledge	CompTIA Security +	◎	◎	◎
		ECSS	◎	◎	◎
2	Network, Network Security	CCNA	◎	◎	◎
		CCNP Security	◎	◎	◎
3	Security Manager, Auditor	CISSP	◎	○	○
		CISM	◎	○	○
		CISA	◎	○	○
4	Hacking, Pentesting	CEH			◎
		LPT			◎
		OCSP			◎
		OSWE			◎
5	Coding, Development	CSC		○	○
6	Project Management	CAPM	◎	○	○
		PMP	◎	○	○
7	Infrastructure	LPIC-1	○	○	◎
		VMware: vSphere Install, Config, Manage	○	○	◎
		VMware: vSphere Optimize & Scale	○	○	◎
8	Threat Intelligence	CTIA			◎
9	SOC, CSIRT	CSA			◎
		Defense Practice against Cyber Attacks		◎	
		CSIRT	○	◎	◎
		Cyber Exercise	○	◎	◎
		Building and Operation of Cyber Exercise	○	◎	◎
10	Forensics, Malware Analysis	Malware Analysis		◎	
		Advanced Malware Analysis		◎	
		CHFI		◎	
11	Policy, Regulation, Governance	Security Policy Making	◎		
		Capacity Building in Policy Formation in ASEAN Region	◎		

No	Category	Course Name	**Output 1** Management	**Output 2** Reactive	**Output 3** Proactive
		Capacity Building in International Law	◎		
12	Awareness Raising	Awareness raising	◎		○
13	International Standard	ISO/IEC 27000 family	◎		○
		US NIST SP800	◎	◎	◎
		GDPR	◎		
14	Security Evaluation	Common Criteria	○		◎
		ISO/IEC 17025			◎
		Security Evaluation Online Seminar			◎
		Common Criteria (PP-ST-TOE)			◎
		Evaluation Lab Operation			◎
15	Critical Information Infrastructure	ISAC Online Seminar	○		◎
		JP-US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region		◎	◎
		CIIP	◎	◎	◎
		Industrial Control Systems		◎	◎
		Strengthening of Cooperation		◎	◎
16	English	Business English for Cybersecurity	◎	◎	◎
17	Training in Third Country	Third country training in Indonesia	○	◎	○

付録8：プロジェクトの成果物

No.	Products	Related Activity
1	CDP format	1-1. 1-2. 1-3. 1-5. 2-1. 2-3. 3-1. 3-3.
2	CDP manual	
3	Created CDPs	
4	CDP portal site	
5	Training materials	1-4. 1-6. 2-2. 3-2.
6	ISAC survey report	3-2.
7	Animation video 1	1-7.
8	Animation video 2	
9	Animation video 3	
10	Branding kit (Logo, slogan, etc.)	
11	COP portal site	
12	Lab Security Manual	3-4.
13	Security Evaluation Procedure (lightweight)	
14	Security Evaluation Procedure (EAL2+ Common Criteria)	
15	Evaluation Template	

付録9：研修結果

- 資格関連研修についての事前事後テスト、オンライン学習結果、資格試験結果

No.	Course	Month Year	Training			Online Practice		Certification Exam		
			Planned Num. of trainee	Actual Num. of trainee	Increased point (pre vs post-test)	Actual Num. of trainee	Increased point (pre vs online-test)	Examinees	Passed	Increased point (pre vs exam test)
1	CompTIA S+ Gr1	09/2019	4	4	**12.59**	-	-	4	1	34.00
2	CEH Gr1	12/2019	6	4	**20.08**	-	-	4	4	32.98
3	CCNA Security Gr1	01/2020	6	3	**16.42**	2	52.92	0	0	-
4	CCNA Security Gr2	01/2020	6	6	**3.33**	6	65.42	3	0	36.02
5	ECSS Gr1	04/2020	7	8	**31.43**	8	55.37	8	7	46.12
6	ECSS Gr2	05/2020	10	9	**32.94**	5	43.69	6	5	48.11
7	CEH Gr2	05/2020	8	7	**6.47**	5	25.85	7	7	27.90
8	CompTIA S+ Gr2	05/2020	5	4	**21.35**	2	20.78	1	1	(pending)
9	CompTIA S+ Gr3	06/2020	5	6	**3.92**	3	26.42	1	0	32.86
10	LPIC-1 Gr1	07/2020	6	5	**29.08**	3	23.98	0	0	-
11	CHFI Gr1	07/2020	5	4	**4.17**	4	24.17	4	4	0.84
12	CISM Gr1	08/2020	6	6	**20.00**	5	59.86	5	1	14.01
13	PMP Gr1	08/2020	5	5	**19.55**	0	0	0	0	-
14	CAPM	08/2020	8	8	**17.70**	2	-2.38	1	1	(pending)
15	PMP Gr2	09/2020	8	7	**23.49**	0	-	0	0	-
16	ECSS Gr3	10/2020	9	4	**30.07**	1	70.07	1	1	(pending)
17	CompTIA S+ Gr4	10/2020	10	10	**3.16**	5	33.49	6	5	21.03
18	OSCP Gr1	10/2020	4	4	**-6.10**	4	-	4	3	-
19	CEH Gr3	11/2020	5	5	**5.27**	4	22.78	4	4	(pending)
20	VCP-1	12/2020	5	5	**6.33**	4	19.47	5	5	(pending)
21	VCP-2	12/2020	5	5	**16.26**					
22	CEH Gr4	01/2021	5	6	**29.00**	5	64.83	5	3	(pending)
23	CISA	03/2021	6	6	**54.50**	4	(pending)	2	2	(pending)
24	ECSS Gr4	04/2021	15	15	**66.03**	15	(pending)	15	15	48.36
25	CEH Gr5	04/2021	5	5	**19.40**	5	30.90	5	2	9.20
26	LPIC-1 Gr2	05/2021	8	8	**41.67**	6	(pending)	6	(pending)	(pending)
27	OSCP Gr2	05/2021	4	4	**23.60**	4	-	4	3	-

No.	Course	Month Year	Training			Online Practice		Certification Exam		
			Planned Num. of trainee	Actual Num. of trainee	Increased point (pre vs post-test)	Actual Num. of trainee	Increased point (pre vs online-test)	Examinees	Passed	Increased point (pre vs exam test)
28	CTIA Gr1	05/2021	10	10	**5.65**	3	(pending)	8	8	-
29	CCNA	05/2021	5	5	**12.33**	5	(pending)	5	5	(pending)
30	CHFI Gr2	05/2021	10	10	**10.13**	10	(pending)	10	10	(pending)
31	CSA Gr1	05/2021	7	7	**19.11**	7	(pending)	7	7	(pending)
32	CISSP	06/2021	6	6	**-7.86**	2	(pending)	2	1	(pending)
33	CompTIA S+ Gr5	07/2021	7	7	**10.63**	6	(pending)	6	4	13.72
34	CSC	07/2021	7	7	**-5.04**	5	(pending)	5	0	(pending)
35	ECSS Gr5	08/2021	11	11	**25.45**	9	(pending)	9	9	34.79
36	CSA Gr2	08/2021	7	7	**3.35**	6	(pending)	6	6	32.41
37	OSCP Gr3	08/2021	4	4	**15.74**	4	-	2	1	-
38	LPT	08/2021	5	5	**-5.70**	5	(pending)	(pending)	(pending)	(pending)
39	PMP Gr3	08/2021	7	7	**30.00**	1	(pending)	1	0	(pending)
40	CISM Gr2	08/2021	5	5	**-29.80**	3	(pending)	2	2	(pending)
41	CHFI Gr3	09/2021	5	5	**14.86**	1	(pending)	1	1	(pending)
42	CEH Gr6	09/2021	8	8	**17.19**	8	(pending)	8	8	24.59
43	CEH Gr7	09/2021	6	6	**0.83**	6	(pending)	6	6	9.30
44	PMP Gr4	10/2021	9	9	**8.89**	1	(pending)	1	0	(pending)
45	ECSS Gr6	10/2021	7	7	**25.35**	7	(pending)	7	6	35.43
46	OSWE Gr1	12/2021	4	4	**-23.43**	4	(pending)	(pending)	(pending)	(pending)
47	CEH Gr8	01/2022	9	9	**23.89**		(pending)	(pending)	(pending)	(pending)
48	PMP Gr5	01/2022	8	8	**17.50**	(pending)	(pending)	(pending)	(pending)	(pending)
49	OSWE Gr2	01/2022	4	4	**8.57**	4	-	-	(pending)	-
50	CEH Gr9	01/2022	7	7	**14.64**	(pending)	(pending)	(pending)	(pending)	(pending)
51	CTIA Gr2	01/2022	8	8	**-0.31**	(pending)	(pending)	(pending)	(pending)	(pending)
52	OSCP Gr4	01/2022	4	4	**-3.33**	4	(pending)	(pending)	(pending)	-
	Total	**-**	**346**	**333**	**-**	208	-	185	147	-

- カスタム研修

No.	Course	Month Year	Training		
			Planned Num. of trainee	Actual Num. of trainee	Increased point (pre vs post-test)
1	Common Criteria	06/2020	12	11	18.68
2	Business English for Cybersecurity Group 1	12/2020	13	14	-
3	Business English for Cybersecurity Group 2	12/2020	19	18	-
4	ISAC Online Seminar	02/2021	10	10	-
5	ISO 17025	02/2021	9	10	3.00
6	Security Evaluation Online Seminar 1	02/2021	12	12	-
7	ISO 27000 family	03/2021	12	10	24.70
8	Security Evaluation Online Seminar 2	03/2021	9	8	-
9	CSIRT Training	05/2021	11	11	-
10	Common Criteria (PP, ST, TOE) 1	07/2021	9	8	-1.60
11	Policy making Seminar	07/2021	31	27	-
12	Common Criteria (PP, ST, TOE) 2	08/2021	9	5	-43.06
13	Awareness-raising	08/2021	18	14	-
14	NIST SP800	09/2021	20	17	18.30
15	Business English for Cybersecurity Group 3 (Hanoi)	10/2021	17	17	-
16	Business English for Cybersecurity Group 4 (HCMC)	11/2021	13	12	-
17	ISAC Meeting	11/2021	3	3	-
18	GDPR	11/2021	13	12	-4.40
19	CIIP	11/2021	13	8	6.10
20	Cyber Exercise	12/2021	14	14	2.00
21	Python Programming	12/2021	6	6	10.60
22	JPCERT/CC Malware Analysis	12/2021	15	20	-
23	Building and Operation of Cyber Exercise	01/2022	17	17	-
24	Evaluation Lab Operation	01/2022	3	3	-
25	Malware analysis tool	02/2022	15	15	-
	Total		**323**	**302**	

- その他の研修（本邦研修、第三国研修）

			Training		
No.	**Course**	**Month Year**	**Planned Num. of trainee**	**Actual Num. of trainee**	**Increased point (pre vs post-test)**
1	Training in Indonesia	09/2019	4	3	-
2	Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	02/2020	2	2	-
3	Defense Practice against Cyber Attacks	09/2020	1	1	-
4	Defense Practice against Cyber Attacks	02/2021	1	1	-
5	JP-US ICS Cybersecurity Week	03/2021	2	2	-
6	JP-US ICS Cybersecurity Week FY2021	10/2021	2	2	-
7	International Law 2021	10/2021	2	2	-
8	Defense Practice (A) 2021	11/2021	1	1	-
9	Industrial Control Systems Cybersecurity Training for Indo-Pacific Region	02/2022	2	2	-
10	Cooperation Among Organizations Against Cyberattacks 2022	02/2022	1	1	-
	Total		**18**	**17**	

付録10：研修生からのフィードバック

- 研修生からのアンケート結果（集計結果）

		Total				
Options**: Strongly Agree (A), Agree (B), Neutral (C), Disagree (D), Strongly Disagree (E)**		E	D	C	B	A
1	The trainer was knowledgeable about the training topics.	1	0	19	101	99
2	The trainer was professional and well prepared.	0	9	17	85	108
3	The trainer helped when I had difficulty understanding the content or performing activities	0	2	25	102	91
4	The trainer promptly answered questions and provided constructive feedback.	0	0	25	93	102
5	The objectives of the training were clearly defined.	0	1	23	93	104
6	Participation and interaction were encouraged.	0	2	28	102	89
7	Overall, the trainer exceeded my expectations.	0	12	27	110	72
8	The training room and facilities were adequate and comfortable.	0	0	14	135	72
9	The topics covered were relevant to me.	0	0	15	137	69
10	The content was organized and easy to follow.	1	0	36	112	72
11	The training activities helped me understand the content provided.	0	12	25	98	86
12	The materials distributed were helpful.	0	2	26	112	81
13	The training objectives were met.	0	13	21	120	67
14	The time allotted for the training was sufficient.	0	8	37	112	64
15	This training experience will be useful in my work.	0	11	15	110	85
16	The training experience encouraged me to seek out future training courses.	0	2	19	132	68
17	Overall, I am satisfied with the results of the training course	0	13	15	118	75
18	Further comments in example: “The training provides me practical knowledge about current working environment? It helps me prevent making mistakes at work place via organized content and activities.”					

- 研修生からのコメント

CompTIA Security+ training (group 1)	
	Yes. (answer for the example)
	It helps me prevent making mistakes at workplace via organized content and activities
	yes, i think so (answer for the example)
CEH training (group 1)	
	The training provides me practical knowledge about current working environment.
	I think it is such a good choice I make. It helps me know the key points about CEH
	We I need more time to prepare for the upcoming exam
	the training provides me new knowledge, help me in my work. i hope have many more time to learn and practice
CCNA Security training (group 1)	
	No Comment
CCNA Security training (group 2)	
	In my current working environment, we using a lot of network equipment from cisco and the other products. After this training, we know how to protect my
ECSS training (group 1)	
	Mr. Giang (trainer) is a good teacher with great enthusiasm. The staff at IPMAC also communicates regularly and provides good student support.
ECSS training (group 2)	
	No Comment
CEH training (group 2)	
	The training provides me practical knowledge about current working environment.
	The training brings me more useful knowledges and get clearer about risks existing on cyber environment. It is good for me to work as Government officer in making regulation and policy later.
CompTIA Security* training (group 2)	
	Thank you very much to all of you.
	The training is very useful and effecive, especially materials for the course, such as exercises, video and labs with a 3-month period in Comptia website. It gives me more knowledge about theory and practices in the field of security.
CompTIA Security* training (group 3)	
	The training provides me a lot of knowledge. It helps me a lot in my current job, understands more technical information, makes it easier to analyze my technical work.
LPIC-1 training (group 1)	
	No comment
CHFI	
	Responder 01: The CHFI course provides a strong baseline knowledge of key concepts and practices in the digital forensic for me.

CISM (group 1)	
	Responder 01: I know overview of information security management and update my knowledge to keep pace with rapid changes in the management, design, oversight and assessment of information security. I will going to apply it much in my job. Responder 02: It helps me see the overview of cybersecurity, not just technical part. Responder 03: The training provides me practical knowledge in information security management. Studying more on this course will give me the way to do right in daily activities.
PMP (group 1)	
	No comment
CAPM (group 1)	
	Responder 01: The training provides me practical knowledge about current working environment. Responder 02: Yes, I do.
PMP (group 2)	
	Responder 01: Thank you JICA for organization this course. Responder 02: Not completely, However its supported me in part of the work. Responder 03: Not completely, However its supported me in part of the work.
ECSS (group 4)	
	Responder 01: The training course has provided me with practical experience. It helps me avoid mistakes at work. Responder 02: The training course has provided me with practical experience. It helps me avoid mistakes at work. Responder 03: The course is very helpful, however, I prefer training in designing policies for further Responder 04: It helps me prevent making mistakes at work place via organized content and activities.
CompTIA S+ (group 4)	
	No comment
OSCP (group 1)	
	(Pending)
CEH (group 3)	
	(Pending)
VCP-1	
	(Pending)
VCP-2	
	(Pending)
CEH (January 2021)	
	Responder 01: “I know an overview of security Certified Ethical Hacker (CEH) , provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach I how hackers think and act so you will be better positioned to set up your security infrastructure and defend against attacks.” Responder 02: “good”

CISA (March 2021)	
	Besides knowledge and methodology of the course, the training should provide more templates that can be used in actual activities. For example, an full set of forms and templates to use in audit the information system of an organization.”
ECSS (April 2021)	
	Responder 01: “It is wonderful to take this course. Thank you to the Organizing Committee” Responder 02: “The training helped me increase my knowledge. I had a lot of interesting experiences with IT. Thank JICA very much!” Responder 03: “The training provides me practical knowledge about current working environment?. It helps me prevent making mistakes at work place via organized content and activities” Responder 04: “Perfect” Responder 05: the training has provide me more practical knowledge which will help me be more careful in working, as a result it might be safer for me and my assigned tasks.
CH (April 2021)	
	Responder 01: “Yes of course the training was improved my skill and very useful for my incident response career. I would like to thank JICA for giving me the opportunity to study to improve my work.” Responder 02: “This course is very helpful for my work and I love it” Responder 03: The training has provided me more practical knowledge about current working environment. It helps me prevent making mistakes at workplace via organized content and activities.
LPIC-1 (May 2021)	
	Responder 01: “The training provides me prevent making mistakes at work place via organized content and activities. Thanks!” Responder 02: “For convenience of review, for each test, the candidate should know which answer is correct”
OSCP (May 2021)	
	Responder 01: “The training help me a lot. Thanks” Responder 02: “The training provided me with more comprehensive knowledge and made it easier to work in the real world.”
CTIA (May 2021)	
	Responder 01: The training provides me practical knowledge about current working environment Responder 02: “The course covers the knowledge related to my work, support me a lot in the process of working.”
CCNA Security (June 2021)	
	Responder 01: “It is very helpful for me.” Responder 02: “The training provides me practical knowledge about current working environment.”
CHFI (June 2021)	
	Responder 01: “The training provides me practical knowledge about current working environment” Responder 02: “I think this course that is suitable for someone who want to know about forensic.” Responder 03: “the course gave me the necessary skills to identify the signs of computer network intruders, collect the necessary evidence to serve the work of continuing the investigation, thank you very much JICA” Responder 04: “It helps me prevent making mistakes at work place via organized content and activities” Responder 05: “The training is helpful and provides me more practical knowledge for working

CSA (June 2021)	
	Responder 01: "It helps me prevent making mistakes at work place via organized content and activities"
CISSP (June-July 2021)	
	Responder 01: "Thank you JICA, and IPMAC for co-operating this course." Responder 02: "this training provides me a broader view of cyber security, not only technical but also management, operation, development, It helps me prevent making mistakes at work place via organized content and activities and prove my skillset."
CompTIA Security+ Group 5	
	The training provides me practical knowledge about current working environment
ECSS Group 5	
	The training provides me practical knowledge about current working environment.
	The training provides me lots of valuable basic knowledge about information security, which is very useful for my work.
	The training helps me improve my knowledge and some skills about cybersecurity.
CSA Group 2	
	Instructors are very enthusiastic, knowledgeable and experienced. The teacher fully guides the course content, but there are many parts that the teacher has not selected and clarified the main content, and lectures regularly for the sections. The teacher teaches a lot, a little bit less interaction
	About the Lab: Instructors should choose content in mind to practice specifically. Similar posts do not need to do.
	Offer: After the course, students are provided with a lab system so that it doesn't take much time to rebuild.
OSCP Group 3	
	This training is very relevant to the reality of my work. I will try to improve my expertise and complete the certification.
LPT	
	The training provided me a lot of knowledge and experience in penetration. It will help me a lot in the process of doing related work.
	The training provides me practical knowledge about current working environment. It helps me prevent making mistakes at work place via organized content and activities
PMP Group 3	
	The course is very useful and necessary for my work in the future.
CISM Group 2	
	The time allotted for the training should have been more extended so that trainees would have more time gaining practical knowledge from trainers.
CHFI Group 3	
	The training provides me practical knowledge about current working environment.
CEH Group 6	
	The training course helped me to know new knowledge, deepen my understanding of known knowledge. At the same time, I would like to thank Mr. Pham Dinh Thang for his dedication in imparting knowledge as well as answering questions for students.

JPCERT/CC Malware Analysis	
	The training provided me with Malware knowledge and tools to analyze and identify it. It's useful.
	The training has helped me to me gain necessary knowledge for malware analysis. I could bring the absorbed knowledge into play and having fruitful outputs. Thank you JICA and experts from JPCERT, also the support team to facilitate all the favor conditions for the training. I hope to have chance attending further training in future. Thank you very much!
	In the static analysis part, I think if the training time is longer, the effect of the course will be even better.
	The training helped me better understand malware and how to analyze it. I hope to get more similar or advanced courses. Thank you.
	The training has brought the fruitful and necessary experience to detect and analyze malwares. Thanks to such effort, I could apply to the on-demand tasks with proven tracks. Please take my thanksful message to JICA, JPCERT/CC experts from Japan and organizers helping me to complete this training. I wish to attend more related training in future. Thank you very much!

付録11：機材リスト

- パッケージ1：**DDoS攻撃防御システム**

No	種別	仕様	数	参考モデル
1	Servers type 1	Xeon E5-2640v3 | 128GB DDR4 | SAS 5x600GB 10k rpm | NIC 4x1Gb & 2x10Gb | PSU x2 | SAN Support	7	FUJITSU Server PRIMERGY RX2540 M5
2	Servers type 2	Xeon E3-1200 v3 | 32GB DDR3 (4x8) 1600MT/s | SAS 3x600GB 10k rpm | PSU x2 | NIC 4x1Gb	20	FUJITSU Server PRIMERGY RX1330 M4
3	Workstation	i7 6700 | 16GB DDR4 2400MT/s | Intel HD530 | HDD 1TB & SSD 512GB | NIC 1Gb	12	Workstation Fujitsu CELSIUS W5010
4	Notebook	i5 6300 | 16GB DDR4 2133MT/s | SSD 512GB SATA M.2 SED | Intel UHD620 | Intel 8265 AC & Bluetooth	5	Laptop Fujitsu LIFEBOOK U7410
5	Monitor	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP)| VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4	30	Monitor Fujitsu FUJITSU Display P24-9 TE
6	Projector	3LCD 16mm (0,63 inch) | P-Si TFT x3 | ANSI Lumens 4200 (normal) 3444 (eco1) 2814 (eco2) | Constrast 2000:1 | Lamp life: 5000h (normal) | 8000h (eco1) | 10000h (eco2) | Manual Zoom 1.2x | Throw Distance 0.9 - 9.1m (wide); 1.0 - 10.9m (tele) | HDMI in x1 | VGA/DSUB in x2 | RCA in x1 | RS232 | Audio in	1	Maxcell MC-EX403E
7	Hard disk	SAS 300GB 6Gb 10K rpm HotPlug 2.5 EP	10	HDD SAS 12G 300GB 10K 512n HOT PL 2.5’ EP
8	Hard disk	SSD 2.5 256GB SATA	5	Hard disk SSD SATA III 256GB 2.5”
9	Hard disk	SAS SSD 300GB	5	Hard disk SAS SSD 400GB
10	SAN Switch	SAN Switch: Fibre Channel ports: Switch mode (default): 24 ports or more | Scalability: Full fabric architecture with a maximum of 239 switches or more | Certified maximum: 6000 active nodes or more | 56 switches or more, 19 hops or more in Brocade Fabric OS® fabrics | 31 switches or more, 3 hops in Brocade M-EOS fabrics or more | larger fabrics certified as required | Aggregate bandwidth: 768 Gbps or more, end-to-end full duplex	2	SAN Switch Fujitsu Brocade G610
11	SAN Storage	Max raw capacity: 68.4TB system shelf, 1.7PB with disk shelves (using 1.8TB,3.2TB, and 10TB drives) | Max drives: 192 with mixed shelves, 120 SSD (25 SSD per 60-drive shelf) or bigger | Drives supported: 900GB, 1.2/1.8TB | SAS 10K | FDE/non-FDE, 1.8TB | SAS 10K FIPS, 800GB | 1.6/3.2TB or larger ; SSD non-FDE, 800GB | SSD FDE, 1.6TB | SSD FIPS | System memory: 8GB/16GB | Optional host I/O ports: 4 ports 10Gb iSCSI (copper) | 4 ports or 8 ports 10Gb iSCSI (optical) | 4 ports or 8 ports 16Gb FC | 4 ports or 8 ports 12Gb SAS.	1	SAN Storage Fujitsu Eternus DX200 S5

- パッケージ2：マルウェア解析システム

No	種別	仕様	数	参考モデル
1	Workstation	1U | Xeon E5-W2102 | 128GB | SSD 512GB | HDD 2x1TB | HDD 2x2TB | DVD+RW | W10 Pro | Dual monitors support | Wireless Keyboard & Mouse | 3y RMA	2	Precision 5820 Tower Custom | Convertable to Rack Mount
2	Workstation	1U | Xeon E5-W2102 | 128GB | SSD 512GB | HDD 2x1TB | DVD+RW | W10 Pro | 3y RMA	1	Precision 5820 Tower Custom | Convertable to Rack Mount
3	Server	1U | Xeon E3-1230 v6 | 128GB | SSD 512GB | HDD SATA 5x4TB (Raid 6) | Wireless Keyboard & Mouse | WS 2019 Datacenter | 3y RMA	3	DELL PowerEdge T330 Custom | Convertable to Rack Mount
4	Workstation (Client PC)	i9-10900K | 32GB DDR4 | HDD 1TB | DVD+RW | SSD 480GB | W10 Pro | 3y RMA	2	Dell OptiPlex 7080 Tower
5	Monitors	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP) | VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4 | 3y RMA	8	Dell U2419H
6	Network device (Firewall)	2 x 1Gb RJ45 WAN | 2 x 4 SFP | 2 x 1Gb RJ45 Mgmt/HA | 14 x 1Gb RJ45 | 1 x Console RJ45 | Local Storage SSD | FW throughput (1518-byte UDP): 20 Gbps | FW throughput (512-byte UDP): 20 Gbps | FW throughput: 9 Gbps | VPN throughput (IPSec): 7200 Mbps | IPS throughput: 2200 Mbps | Threat protection throughput: 1200 Mbps | Multi-Tenant supported (VDOM) (license for 2y) | 2y RMA	2	Firewall Fortinet 200E Series
7	Network device (Switch)	24 x 10/100/1000 RJ45 PoE+ interfaces | 2 x 1Gb SFP uplinks & 2 x 10Gb SFP+ uplinks | Full duplex switching bandwidth: 254 Gbps | Forwarding rate: 68.45 Mbps | PoE Power 390W | PSU 640W | 4GB DRAM | 2048MB flash | 2y RMA	1	Cisco 3650 – 24 PDM
8	Network device (SIM)	Internet via cellular network - max speed (avg. 100Mbps Upload - Download) - unlimited bandwidth (1y subscription)	2	Mobifone
9	Network device (Gateway)	LTE CAT 20, up to 2Gbps download & 150Mbps upload | 3GPP, Rel. 14 | 5CA with 20 simultaneous Downlink layers | 4x4 MIMO | 256QAM DL / 64QAM UL CA 3C, 7C | 11ac Dual band dual concurrent | 5040mAh Battery | 1y RMA **OR** LTE CAT 6, up to 300Mbps download & 50Mbps upload | IEEE 802.11a/n/ac 5 GHz, IEEE 802.11b/g/n 2.4 GHz | 1 × 10/100/1000 Mbps LAN/WAN Port | 3 × 10/100/1000 Mbps RJ45 Ports | 1 × Micro SIM Card Slot | 2y RMA	2	Netgear Nighthawk M2 (MR2100) **OR** TP-Link Archer MR600
10	Network device (Accesspoint)	IEEE 802.11 a/b/g/n/r/k/v/ac/ac-wave2 5GHz 1733Mbps, IEEE 802.11b/g/n 2.4GHz 300Mbps | 1 × 10/100/1000 Mbps LAN PoE Port | Wireless Security: WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES), 802.11w/PMF | 2y RMA	1	JW797A Aruba AP-315 **OR** Ubiquity AP-nanoHD
11	Rack	Server Rack for Malware Analysis system's equipments >27U	1	27UD800, 27U
12	UPS	Online/Interactive UPS 5kVA | NMC controller | 2y RMA	3	APC SURTD5000XLI
13	Network device	KVM Switch for Malware Analysis system's equipments with related cables bundled (HDMI, USB, etc.) | 2y RMA	1	Tripple Lite B024-HU08
14	Software	Windows 10 Pro & Enterprise 64bit EN + Software Assurance (2y)	12	

No	種別	仕様	数	参考モデル
15	Software	VMware Workstation Pro (upgradable within 2y)	5	
16	Software	Microsoft Office Professional Plus 2016 32bit (downgradable to 2013)	5	
17	Software	Visual Studio 2010 Premium with MSDN (1y)	2	
18	Software	Burp Suite Pro 1 user / 1 year	2	
19	Software	Zynamics BinDiff 5 User License	1	
20	Software	ARM64 Decompiler Fixed License [Windows]	1	
21	Software	ARM32 Decompiler Fixed License [Windows]	1	
22	Software	MIPS Decompiler Fixed License [Windows]	1	
23	Software	IDA x64 Decompiler Fixed License [Windows]	2	
24	Software	IDA x86 Decompiler Fixed License [Windows]	2	
25	Software	VB Decompiler 1 user Business License & License Update within 2y	2	
26	Software	Kaspersky Internet Security 2019	1	
27	Software	Symantec Internet Security 2019	1	
28	Software	McAfee Internet Security 2019	1	
29	Software	Veramine 1y license	1	
30	Software	Joe Sandbox Ultimate	1	
31	Software	NESSUS Pro 3y license	1	
32	Software	Cyber Triage (Team license)	1	
33	Software	IDA Pro Computer License [Windows]	2	

- パッケージ3：セキュリティ評価機材

No	種別	仕様	数	参考モデル
1	Workstations	Xeon E-2124G | 32GB | HDD 2TB | NVIDIA P620 | DVD+RW | W10 Pro | 3y RMA	2	Dell Precision 3630
2	Monitors	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP)| VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4 | 3y RMA	2	Dell Ultrasharp U2419H
3	Screen	3840 x 2160 (4x4 cabinet) | 806.4 x 453.6 x 29.9 mm (LxHxD) per cabinet | 0.8 Pixel Pitch | Flip-chip RGB LED | 2000cd/m2 | 10,000:1 | IP20 | 2y RMA **OR** 49 inch 3840 x 2160 | 16:9 | 700cd/m2 | 8ms | 4000:1 | HDMI x 2 | Display Port x 1 | DVI-D x 1 | RJ45 | Speaker | Audio in 3.5mm | USB ports x 2 | SSSP 6.0 | IP5X | VESA | 2y RMA **OR** 49 inch 5120 x 1440 | 32:9 | 350cd/m2 | 1ms & 144Hz | HDMI x 2 | Display Port x 1 | Speaker | Audio in 3.5mm | USB ports x 2 | Picture-by-Picture | VESA 100mm x 100mm | 2y RMA	2	Samsung LED IWJ Samsung LED QHR Samsung CRG9

No	種別	仕様	数	参考モデル
4	Servers	Xeon Gold 5520 | 128GB | SSD 1TB | NVIDIA P620 | DVD+RW | 3y RMA	2	Dell Power Edge R740
5	Storage devices (SAN)	2U | Intel Dual core 2.2GHz | Dual Controller 4 x 16Gb FC ports & 4 x 10Gb SFP+ | 4 x 10Gb SFP+ SR | 4x SFP 16Gb FC | 4 x 1x Multi-mode 2m LC-LC FC cable | 16 x 2.4TB SAS HDD 10K rpm 2.5 | 24 x 2.5” drive bays | Up to 276 drives | Up to 3.0PB capacity | Drive support: NLSAS 7.2K 3.5: 4-12TB | 7.2K 2.5 2TB | SAS 10K 2.5: 1.2-2.4TB | SAS 15K 2.5: 0.9TB | SSD: 0.48-1.92TB | SED & non SED FIPS certified | PSU 580W x 2 | 3y 24x7 ProSupport Plus & NBD Onsite Warranty	1	Dell EMC ME4024 Storage Array
6	SAN Switch	24 ports FC16 (16Gb max) & 12 x Module 16Gb SFPs+ | Module Singlemode fiber 1Gb | OM4 LC/LC Fiber Cable, (Optics required) 3m | Aggregate bandwidth: 384Gb full duplex | Rack Mount rails for 4-post Rack | 3y 24x7 ProSupport & NBD Onsite Warranty	1	Connectrix DS6505B 12-24 Port FC16 Switch
7	Switch L3	L3 Switch | 24 x 10/100/1000 Mbps RJ45 PoE+ interfaces | 2 x 1Gb SFP uplinks & 2 x 10Gb SFP+ uplinks | Full duplex switching bandwidth: 160 Gbps | Forwarding rate: 65.5 Mbps | PSU 350W | 512MB DRAM | 128MB flash | 2y RMA	2	3750WS-C3750X-24T-S
8	Switch L2	24 x 10/100/1000 Mbps RJ45 PoE+ interfaces | 4 x 1Gb SFP uplinks | Full duplex switching bandwidth: 216 Gbps | Forwarding rate: 108 Gbps | PSU 250W | 512MB DRAM | 128MB flash | 2y RMA	4	2960X-24TS-L (PORT 1 Gigabit)
9	UPS	Online/Interactive UPS 50KVA | NMC controller | 2y RMA	1	
10	Firewall	1U | 8 x 1Gb RJ45 | 6 x 1Gb SFP | 1Gb RJ45 Mgmt | Console RJ45 | Local Storage SSD (120GB SED) | FW throughput (1500-byte UDP): 2 Gbps | FW throughput (450-byte UDP): 350 Mbps | VPN throughput (IPSec): 300 Mbps | IPS throughput: 650 Mbps | Threat protection throughput: 1100 Mbps |CSC-SSM-20 Plus license & 3DES/AES (license for 2y) | 2y RMA	1	Fortinet FG-80E Fortigate FG-300E Check Point 5200
11	Network Tap	2 x 1Gb RJ45 8 pins | 2 x 10Gb SFP+ | Link Failure Propagation (LFP) | Aggregation/ Regeneration | 802.3af & VoIP compliant | PoE passthrough | Redundant powering | 2y RMA	1	
12	Fortify static code analyzer (or equivalent) for source code review	Software development tools | Integrated Development Environments (IDE): Eclipse, Visual Studio, IntelliJ IDEA | Build Servers: Jenkins, Bamboo, Visual Studio, Gradle, Make | Issue Trackers: Bugzilla, Jira, ALM Octane | Open Source Security Management: Sonatype, Snyk, WhiteSource, BlackDuck | Code Repositories: GitHub, Bitbucket | Swaggerized API for unlimited customization | 1y license	1	
13	Acunetix 360	Acunetix 360 | 3y license	1	
14	Nessus Professional	Nessus Professional | 3y license	1	

付録12：活動、投入、成果

成果1. セキュリティ品質管理能力が強化される

活動	投入	アウトプット	成果品
1-1. Clarify the required roles defined in SecBoK framework	JICA Expert	• CDP format • CDP manual (incl. CDP DB, Source Code)	• CDP_FORM-rev08 • CDP manual
1-2. Develop a CDP for each staff based on SecBoK Framework	JICA Expert	• Created CDPs	• CDPs
1-3. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. CISO, Commander)	JICA Expert	• Training list	• Training List, Google Spread Sheet
1-4. Conduct training	JICA Expert local training, raining in Japan	• Training result • Created CDPs • Training materials	• Training Reports • CDPs • Training materials (Japanese Survey result, Marketing theory, Building cyber exercise environment, Malware analysis, GDPR, etc.)
1-5. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
1-6. Plan and conduct training for policy maker	JICA Expert local training, training in Japan	• Training list • Training result • Created CDPs	• Training List • Summary of Training, Training Reports • CDPs
1-7. Develop/localize awareness raising materials	JICA Expert local procurement	• 3 video material • COP portal site • Branding kit	• Awareness-raising materials

成果2.　事後対応型サービス能力が強化される

活動	投入	アウトプット	成果品
2-1. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. Incident manager, Incident handler, Triage)	JICA Expert	• Training list	• Training List, Google Spread Sheet
2-2. Conduct training	JICA Expert local training, training in Japan	• Training result • Created CDPs	• Summary of Training, Training Reports, Training materials • CDPs
2-3. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
2-4. Expand reactive infrastructure (e.g. DDoS attack mitigation, malware analysis) in AIS	JICA Expert	• Equipment list	• Equipment List (DDoS Mitigation System) • Equipment List (Malware Analysis)

成果3.　事前対応型サービス能力が強化される

活動	投入	アウトプット	成果品
3-1. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. Researcher, Solution analyst, Vulnerability diagnostic consultant, Information security auditor)	JICA Expert	• Training list	• Training, Google Spread Sheet
3-2. Conduct training	JICA Expert local training, training in Japan	• Training result • Created CDPs • ISAC survey report	• Summary of Training, Training Reports, Training materials • CDPs • ISAC Report
3-3. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
3-4. Expand proactive infrastructure (e.g. network monitoring, equipment for support practice according to international standard Common Criteria) in AIS	JICA Expert local support	• Equipment list • Lab Security Manual • Security Evaluation Procedure (lightweight) • Security Evaluation Procedure (EAL2+ Common Criteria) • ETR Template	• Equipment List (DDoS Mitigation System) • Equipment List (Security Evaluation) • Lab Security Manual • Security Evaluation Procedure • ETR Template

付録13：R/D, M/M, Minutes of JCC（写し）

写しを添付

付録14：モニタリングシート（写し）

写しを添付

付録15：合同調整委員会（Joint Coordination Committee (JCC)）

No	日付	参加者数		議論のポイント
		ベトナム	日本	
1	2019 年 9 月 24 日	8	9	プロジェクトチームから進捗状況と今後の予定が報告された。
2	2020 年 8 月 14 日	9	8	AIS と JICA 専門家は、プロジェクト開始後 1 年間の活動報告と今後の計画について協議した。当初 2021 年 11 月に終了予定だったプロジェクトは、セキュリティ製品評価や新たな普及啓発活動、情報共有システムなどの新たな活動を盛り込み、2022 年 3 月まで延長が決定された。
3	2021 年 9 月 15 日	8	11	AIS と JICA の専門家が、これまでの進捗状況や成果、プロジェクト終了に向けた今後の計画について説明した。AIS からは、本プロジェクトのフェーズ 2 の依頼に際しての目的、想定される内容、手続きの状況について共有した。
4	2022 年 3 月 1 日（計画）	TBU	TBU	TBU

付録16：CDPレビューのコメント集

質問：研修に参加して、仕事に対する姿勢や考え方はどのように変わったか？

- **第2回CDPレビュー（62の回答から抜粋）**

- ✓ I hope that after the next course I will have a better knowledge base in my daily work.
- ✓ need to arrange time more to spend the time to join the training course be on time.
- ✓ After I have completed the CEH-V10 course, I have knowledge from basic to specialized in security, know how to use the tools and methods of hacker attacks by Modules, then master. attack methods that hackers often use and have the ability to prevent and prevent unauthorized attacks and network sabotage in organizations.
- ✓ I have much more useful knowledge on the field of Information Security and Common Criteria. I feel everything about these fields become clearer and they attract me more to study and work about them.
- ✓ Trainings helps to better manage the team and consult supervisors how to develop cybersecurity.
- ✓ My attitude to work has changed and raised higher for information security.
- ✓ "After I completed the CEH course I applied a lot of knowledge in my work such as: I learned Attack Techniques, Attack Tools and Countermeasures, System Security Assessment and website applications, wireless hacking methods, wireless hacking tools and WiFi security tools, malware analysis and removal, ... Specifically, I participated in training to raise awareness for the provinces. in the southern region, take part in information security drills that the organization trains for the units, ... In addition, I also completed training CISM, I understood the role of each position in the organization, outlined the work goals of each person and the responsibilities of each position of the organization."
- ✓ Although her job is not related to project management much but the PMP course helps her identify which stage of projects her job is. PMP also improves her terminology of project management.
- ✓ It's very useful and helps me to feel more confident to communicate in English.
- ✓ Knowledge studied in trainings help him much in his daily task, for i.e., thanks to CHFI, he could analyze Wireshark package.
- ✓ The courses provide him foundation knowledge of system management. But now his job mainly is related to monitoring so CEH is more useful for his daily tasks.
- ✓ After joining courses, I feel more confident at work.
- ✓ VMware course provides me basic and systematic knowledge on system admin which is useful for my job. I expect that the 2nd VMware course could be more practical and more related to my daily tasks.
- ✓ I learn a lot of practical knowledge through ECSS, CEH and English which are useful for my job, especially CEH course.
- ✓ I gain deeper understanding and practical knowledge on cybersecurity thanks to CEH course. For English course, it helps me to practice pronunciation and communicate with people confidently.
- ✓ better support in the process of pentesting systems, as well as technical troubleshooting
- ✓ Thanks to CAPM course, even I attended just 50% of the training, it helps me to
- ✓ make working plan and manage work better.
- ✓ The CC course is useful for AIS. After the course, we published 2 based standards, 12 criteria and some process to evaluate system.
- ✓ The most helpful and interesting part of the CAPM course is how to make plan (Planning). Because the duration is quite short (5 days) in comparison with big content of the course, so it is not easy to apply all in my daily tasks. But it still helps me somehow in my job.
- ✓ The CompTIA S+ training is useful, which I can utilize in inspection activity.
- ✓ It's helpful for me, but the course duration is not enough to absorb huge knowledge of the CompTIA S+

- ✓ Although I studied the CompTIA S+ by myself but thanks to the course, I discussed with the trainer and find answers for some of my concerns/questions related to my job.
- ✓ The ECSS is a basic course which provides overview of cybersecurity. The knowledge is quite new and useful for my job.
- ✓ The courses are very helpful because they provide exact answers for my questions on what I concern. For English, it helps us to speak, write fluently.
- ✓ Although the PMP course provides only theory, a part of the course (Planning) is still helpful, and I could apply a little into daily jobs.
- ✓ Thanks to the course, I know terminology of cybersecurity and apply English reading skill into my translation job when I collect information to make news.
- ✓ Knowledge and skills provided in the training are important and useful for VNCERT HCMC. However, the course contains huge knowledge and 5 days duration is not enough.
- ✓ ECSS course provides fundamental technical knowledge which is useful for me. I know how to protect my personal computer by using firewall, or be more careful when I open emails, use the Internet.
- ✓ PMP course is useful, which help me to make plan and allocate human resource for each task. CISM provides risk management knowledge which is essentially necessary for VNCERT while we plan to formulate regulations on this content.

- **第3回CDPレビュー**

- ✓ The knowledge in ECSS course has helped me a lot in my working process, from providing more basic knowledge about computers such as OSI network model, TCP/IP network model, network protocols. often used as HTTP, HTTPS, DNS.. to in-depth encryption knowledge like RSA MD5.. knowledge related to safety and network security such as viruses, trojans or network attacks such as XSS, SQL injection.
- ✓ I feel more confident at work
- ✓ It is my daily job to analyze cyber threats to warn. So after taking some courses like CEH. It helped me to be more at the process of a network attack
- ✓ “CISM: the course is useful which provides general view on security management, however, it's difficult to apply methodology or concepts (job title, task...) into Vietnam system because of the difference between international models and Vietnam model.
- ✓ Every course make me understand more and more. We really need the courses like these.
- ✓ The courses help me to understand English terminology
- ✓ LPIC-1: Provide overview of system while I have to work with Linux. English course (Language Link): It helps me to improve English skills. The course is much better than other courses which I have to pay by myself.
- ✓ English course provides basic English which helps me to systematize the language.
- ✓ ECSS course provides general foundation of cybersecurity which could be useful for me.
- ✓ ISO 27000 Family helps me with risk evaluation which could be utilized in my daily job.
- ✓ CAPM helps me to well manage working schedule to improve daily tasks; English course sounds an interesting course in which the trainer knows how to motivate students and provides systematic basic knowledge
- ✓ ISO 27000 Family course which contain practical knowledge is quite useful for my tasks
- ✓ ISO/IEC 17025: Provide templates to evaluate products
- ✓ I feel improvements in my awareness of security, how our information systems can be affected or attacked by internal and external threats, and how we can reduce detrimental outcomes by some basic mesures.
- ✓ ECSS is an useful and practical course which helps me how to protect data by encryption. The duration is short, it is still considered to provide helpful practice. Although the course material is in English, I have to translate every page, and being a non-technician, I still enjoy the course

much.

- ✓ CISA is an interesting course for me but because of my workload so I cannot attend the course fully. For CTIA, it provides basic knowledge.
- ✓ Make me feel confident, approach and solve problems faster
- ✓ I have formed a security mindset in my daily work
- ✓ ECSS: provide knowledge on VPN which is helpful when I have to work remotely by knowing and understanding cybersecurity.
- ✓ CTIA: though the course is more difficult than ECSS, it closely links with my daily tasks while I have to collect information. The part of Zero day vulnerability is especially interesting.
- ✓ English: Trainer is good but curriculum is so basic, simple and has not improved my skills.
- ✓ After the course, I used the knowledge combined with the Team to organize training to raise awareness of information security, analyze and remove malicious code. then organize a rehearsal for the training participants. To visualize the incident response process at the agency and the steps to take.