公示番号：190086
国　名：ベトナム
担当部署：社会基盤・平和構築部運輸交通・情報通信グループ第二チーム
案件名：サイバーセキュリティに関する能力向上プロジェクト（キャリア開発計画）

１．担当業務、格付等

（１）担当業務：キャリア開発計画
（２）格　付：2 号
（３）業務の種類：専門家業務

２．契約予定期間等

（１）全体期間　：2019 年 6 月中旬から 2021 年 11 月下旬まで
（２）業務 M/M　：国内　1.00M/M、現地　8.00M/M、合計　9.00M/M
（３）業務日数　：

準備期間	4 日
第 1 回現地業務期間	60 日
国内業務期間	3 日
第 2 回現地業務期間	45 日
国内業務期間	3 日
第 3 回現地業務期間	45 日
国内業務期間	3 日
第 4 回現地業務期間	45 日
国内業務期間	3 日
第 5 回現地業務期間	45 日
整理期間	4 日

３．簡易プロポーザル等提出部数、期限、方法

（１）簡易プロポーザル提出部数：1 部
（２）見積書提出部数：1 部
（３）提出期限：5 月 15 日(12 時まで)
（４）提出方法：専用アドレス (e-propo@jica.go.jp)への電子データの提出又は郵送
（〒102-8012 東京都千代田区二番町 5 番地 25 二番町センタービル)
（いずれも提出期限時刻必着）

提出方法等詳細については JICA ホームページ（ホーム＞JICA について＞調達情報＞公告・公示情報／結果＞コンサルタント等契約案件公示（業務実施契約（単独型））＞業務実施契約（単独型）公示にかかる応募手続き）（https://www2.jica.go.jp/ja/announce/pdf/competition_2019.pdf）をご覧ください。なお、JICA 本部 1 階調達部受付での受領は廃止しておりますので、ご持参いただいても受領致しかねます。ご留意ください。

（５）評価結果の通知：提出されたプロポーザルは JICA で評価・選考の上、各プロポーザル提出者の契約交渉順位を決定し、2019 年 5 月 28 日（火）までに個別に通知します。

４．簡易プロポーザル評価項目及び配点

（１）業務の実施方針等：

①業務実施の基本方針	16 点
②業務実施上のバックアップ体制等	4 点

（２）業務従事者の経験能力等：

①類似業務の経験	40 点
②対象国又は同類似地域での業務経験	8 点
③語学力	16 点
④その他学位、資格等	16 点
	（計 100 点）

類似業務	IT 人材育成やサイバーセキュリティに係る各種調査・プロジェクト
対象国／類似地域	ベトナム／全途上国
語学の種類	英語

５．条件等

（１）参加資格のない社等：特になし

（２）必要予防接種：特になし

（３）資格等：本業務については、以下の資格・経験を有することが望ましい。

・ サイバーセキュリティの実務経験（例：インシデントハンドリング、フォレンジックなど）あるいはシステム開発等の実務経験

・ サイバーセキュリティ系資格の保持者（例：CISSP、CEH、CCNP Security、情報処理安全確保支援士など）

・ 途上国における IT 関連の人材育成業務経験

６．業務の背景

サイバーセキュリティを取り巻く環境は、世界的に急速に変化しており、そのリスクは甚大化し、グローバルレベルのものとなっている。多くの国において、国家や重要インフラ（交通、エネルギー、医療、ファイナンス等）に対するサイバー攻撃が現実のものとなり、サイバーセキュリティの確保は、特にサイバー攻撃に対する十分な予防策がとられてこなかった途上国において国家的課題となっている。

ベトナム社会主義共和国（以下、「ベトナム」という）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）。また、インシデントの種類に関しても外部からの侵入や DoS/DDoS 攻撃 が増加傾向にある。サイバー攻撃の規模と数は増大しており、特に APT 攻撃（Advanced Persistent Threats）が増加している。また、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。さらに、マルウェア感染の状況、特に悪意のあるソフトウェアの脅威は、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。

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、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」、及び 2016 年の「首相決定第 898 号」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」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されている。

ベトナム情報通信省（Ministry of Information Communication、以下「MIC」という）傘下の情報セキュリティ局（Authority of Information Security、以下「AIS」という）はサイバーセキュリティ政策を策定し、セキュリティオペレーションセンター（Security Operation Center、以下「SOC」という）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、以下「CSIRT」という）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、今後もサイバー攻撃が増加することが予想される中で、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。

このような状況の下、ベトナム情報通信省より「サイバーセキュリティに関する能力向上プロジェクト」実施の要請がなされた。要請された内容は、政府サイバーセキュリティ人材の能力向上、政府情報ネットワークをサイバー攻撃から守る機材・技術の供与、サイバーセキュリティ啓発活動などとなっている。2017 年 11 月に詳細計画策定調査が実施され、2019 年 3 月にベトナム政府との間で討議議事録（Record of Discussions: R/D）が署名された。今回募集のコンサルタントは、同プロジェクトにキャリア開発計画として参加する。

７．業務の内容

本業務の業務従事者は、別添のベトナム「サイバーセキュリティに関する能力向上プロジェクト」のプロジェクト目標の達成に向けて、キャリア開発計画の策定及びレビューを行う（別添の活動 1-1、1-2、1-3、1-5、2-1、2-3、3-1、3-3）。また、研修（別添の活動 1-4、2-2、3-2）がキャリア開発計画通りに実施されているかモニタリングを行う。

キャリア開発計画は、計画的かつ包括的にサイバーセキュリティに関する各種能力を向上できるよう、C/P 機関の対象者（約 40 名）各々に対して策定されるもので、業務上の目標、現状スキル、必要な研修などを明らかにしたものである。策定に当たっては、C/P および長期専門家と協議の上ドラフトし、チーフアドバイザーにコメントを求め、最終化する。研修の実施（調達）は長期専門家（サイバーセキュリティ／業務調整）が行うが、業務従事者は、適宜、長期専門家から研修進捗や結果の報告を

受け、問題があれば長期専門家に助言を与えるとともに、チーフアドバイザーに報告する。キャリア開発計画のレビューは、C/P へのインタビューや、長期専門家からの報告（例：研修参加履歴、研修成績）などを元に行い、各対象者の、その時点でのスキルや希望を把握するとともに、必要があれば、キャリア開発計画内容の変更を行う。変更の際は、C/P や長期専門家と十分協議を行い、結果をチーフアドバイザーに報告する。

その他、プロジェクト目標達成に向けて必要と思われる事項について、C/P 及び長期専門家と協議を行う。プロジェクトの枠組み変更（例：PDM（Project Design Matrix）、PO（Plan of Operation）の修正）が必要と思われる場合は、チーフアドバイザーに報告する。

各活動時期における具体的担当事項は次のとおりとする。

（１）国内準備期間（2019 年 6 月中旬）

①既存文献（要請書、案件概要表、ASEAN 諸国における情報セキュリティ情報収集・確認調査報告書、詳細計画策定調査報告書、R/D 等）をレビューした上で、長期専門家（サイバーセキュリティ／業務調整）、JICA 社会基盤・平和構築部やチーフアドバイザーと協議を行い、プロジェクトの全体像をとらえ、キャリア開発計画に関する詳細な活動計画を立てて、ワークプラン（和文・英文）を提出する。

②情報セキュリティ人材スキルマップ[1]である NPO 日本ネットワークセキュリティ協会の SecBoK（2019 年度版）、アメリカ国立標準技術研究所のサイバーセキュリティフレームワーク（National Initiative for Cybersecurity Education（NICE）Cybersecurity Workforce Framework）を入手し、研修計画案を検討する際にスキルマップ上のどこに位置づけられるかを把握するために、内容を理解する。

SecBok: https://www.jnsa.org/result/2018/skillmap/
NICE Cybersecurity Workforce Framework:
https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

（２）第 1 回現地業務期間（2019 年 7 月下旬～9 月中旬）

① JICA ベトナム事務所、長期専門家（サイバーセキュリティ／業務調整）及びベトナム側関係機関との協議し、業務方針・計画を確認する。

② 詳細計画策定調査で作成した研修計画、及びベトナム国内で提供可能な研修について再確認を行い、必要に応じて修正する。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再確認する。具体的には、AIS と協議を行い、セキュリティ業務で必要な役割を SecBoK で定義された CISO・コマンダー・トリアージ・インシデントハンドラー等の役割にマッピングし、優先度が高い考える役割を選択・確認する。

[1] 情報セキュリティ人材スキルマップとは、情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理した一覧表のことである。情報セキュリティ責任者、インシデントマネージャ、IT システム部門などの役割を担う人材に必要な技術分野（ネットワークセキュリティ、データベースなど）を特定することができる。

③ 詳細計画策定調査の結果を踏まえて、長期専門家と協力して、対象職員（対象職員は、CISO・コマンダー・トリアージ・インシデントハンドラー等の役割を有する約 40 名）に対してキャリア開発計画を策定する。なお、プロジェクト全体を通して、キャリア開発計画には対象者が受講すべき研修リストを含み、研修コースのアレンジは長期専門家が行う。

キャリア開発計画の具体的な策定方法は、キャリア開発計画作成の対象者にインタビューを行い、業務（役割）、現在のスキル及び不足しているスキルを洗い出し、各対象者に対して現地で提供可能な商用研修やプロジェクトでカスタマイズする研修を割り当てる。研修設計には SecBoK を用いて、漏れがなく一貫した研修が設定されることが期待されている。詳細計画策定調査時に商用研修は General Security knowledge、Manager／Auditor、Analysis／Hacking、Coding／Forensics、Administrator／Specialist にカテゴライズされており、具体的には CompTIA Security+、CCNA Security、Certified Ethical Hacker (CEH)、Certified Information Systems Security Professional (CISSP)、Network Forensics 等の研修を適切に対象者に割り当てる。詳細計画策定調査時ではカスタマイズ研修は情報セキュリティマネジメント、マルウェア解析、CSIRT 組織・プロセス・活動、法律・規則・ガバナンス・情報セキュリティ、政策策定を想定したが、状況に応じて必要な研修を設計・提案する。なお、キャリア開発計画の作成には、長期専門家以外にプロジェクトが傭上する現地スタッフがサポートする（「１０．特記事項　キ）」参照）。

④ 詳細計画策定調査で選定し、長期専門家が再確認した機材について、調達状況を確認する（調達自体は長期専門家が実施する）。

⑤ その他、プロジェクト目標達成に向けて必要と思われる事項（PDM、PO の修正を含む）について、C/P と協議を行いながら各活動方針の修正を行う。

（３）国内作業期間（2019 年 10 月上旬～12 月下旬）

① 長期専門家（サイバーセキュリティ／業務調整）からの活動進捗に関する報告を確認し、JICA 社会基盤・平和構築部やチーフアドバイザーと協議を行い、現地活動方針の確認を行う。

② 長期専門家と協力して、モニタリングシートの取り纏めを行い、提出する。ただし、次回以降は、派遣時期によっては現地業務期間中にモニタリングシートを作成する場合もある。

（４）第 2 回現地業務期間（2020 年 1 月中旬～2 月下旬）

① 長期専門家（サイバーセキュリティ／業務調整）と協力して、キャリア開発計画のモニタリングを行い、必要に応じて計画を修正し、受講すべき研修リストを更新する。

プロジェクトを通して、モニタリングの具体的な方法は、対象者にインタビューを行い、業務（役割）、現在のスキル及び不足しているスキルを再確認し、各対象者に対して割り当てられた商用研修やカスタマイズ研修の修正・更新を行う。新規でキャリア開発計画の対象者となった新入職員等に対しては新規でキャリア開発計画を策定する。（策定の対象となるかは長期専門家及び C/P と協議の上決定する。）

② 長期専門家と協力して、JCC（Joint Coordinating Committee）を開催する。

JCC において現状や課題を確認し、今後の指導計画への反映やキャリア開発計画の修正を行う。
③ その他、プロジェクト目標達成に向けて必要と思われる事項（PDM、PO の修正を含む）について、C/P と協議を行いながら各活動方針の修正を行う。

（５）国内作業期間（2020 年 3 月上旬～7 月中旬）
① 長期専門家（サイバーセキュリティ／業務調整）からの活動進捗に関する報告を確認し、JICA 社会基盤・平和構築部やチーフアドバイザーと協議を行い、現地活動方針の確認を行う。
② 長期専門家と協力して、モニタリングシートの取り纏めを行い、提出する。

（６）第 3 回現地業務期間（2020 年 7 月下旬～9 月上旬）
① 長期専門家（サイバーセキュリティ／業務調整）と協力して、キャリア開発計画のモニタリングを行い、必要に応じて計画を修正し、受講すべき研修リストを更新する。
② その他、プロジェクト目標達成に向けて必要と思われる事項（PDM、PO の修正を含む）について、C/P と協議を行いながら各活動方針の修正を行う。

（７）国内作業期間（2020 年 9 月中旬～2021 年 2 月上旬）
① 長期専門家（サイバーセキュリティ／業務調整）からの活動進捗に関する報告を確認し、JICA 社会基盤・平和構築部やチーフアドバイザーと協議を行い、現地活動方針の確認を行う。
② 長期専門家と協力して、モニタリングシートの取り纏めを行い、提出する。

（８）第 4 回現地業務期間（2021 年 2 月中旬～3 月下旬）
① 長期専門家（サイバーセキュリティ／業務調整）と協力して、キャリア開発計画のモニタリングを行い、必要に応じて計画を修正し、受講すべき研修リストを更新する。
② 長期専門家と協力して、JCC を開催する。JCC において現状や課題を確認し、今後の指導計画への反映やキャリア開発計画の修正を行う。
③ その他、プロジェクト目標達成に向けて必要と思われる事項（PDM、PO の修正を含む）について、C/P と協議を行いながら各活動方針の修正を行う。

（９）国内作業期間（2021 年 4 月上旬～9 月中旬）
① 長期専門家（サイバーセキュリティ／業務調整）からの活動進捗に関する報告を確認し、JICA 社会基盤・平和構築部やチーフアドバイザーと協議を行い、現地活動方針の確認を行う。
② 長期専門家と協力して、モニタリングシートの取り纏めを行い、提出する。

（１０）第 5 回現地業務期間（2021 年 9 月下旬～10 月中旬）
① 長期専門家（サイバーセキュリティ／業務調整）と協力して、キャリア開発計画のモニタリングを行い、必要に応じて計画を修正し、受講すべき研修リストを更新する。
② 長期専門家と協力して、モニタリングシート及びプロジェクト成果の取り纏

めを行い、C/P と共に内容（成果、進捗状況）の確認を行う。
③ 長期専門家と協力して、最終 JCC を開催し、プロジェクトの最終成果を C/P を含む関係者と確認する。
④ その他、プロジェクト目標達成に向けて必要と思われる事項（PDM、PO の修正を含む）について、C/P と協議を行いながら各活動方針の修正を行う。

（１１）整理期間（2021 年 10 月下旬～11 月下旬）
①専門家業務完了報告書（和文）、事業完了報告書（和文・英文）を提出する。事業完了報告書については長期専門家と協力して作成する。
②帰国報告会に出席し、担当業務及びプロジェクトに係る報告を行う。

８．報告書等

業務の実施過程で作成、提出する報告書等は以下のとおり。
提出先は、JICA 社会基盤・平和構築部、JICA ベトナム事務所とする。

報告書	時期等	言語・形式
ワークプラン	業務開始後 1 か月以内	和文・英文 電子データ
Monitoring Sheet	業務開始後 6 か月ごと	英文 電子データ
専門家業務完了報告書	プロジェクト終了時	和文 電子データ
事業完了報告書（Project Completion Report）	プロジェクト終了時	和文・英文 電子データ

９．見積書作成に係る留意点

本公示の積算を行うにあたっては、「コンサルタント等契約における経理処理ガイドライン」（http://www.jica.go.jp/announce/manual/guideline/consultant/quotation.html）を参照願います。留意点は以下のとおりです。
（１）航空賃及び日当・宿泊料等
航空賃及び日当・宿泊料等は契約に含みます（見積書に計上して下さい）。
航空経路は、日本⇒ハノイ⇒日本を標準とします。

１０．特記事項

（１）業務日程／執務環境
①現地業務日程
最初の現地業務期間は 2019 年 7 月 21 日～9 月 18 日を予定しています。
2 回目以降の派遣については JICA 社会基盤・平和構築部、及び長期専門家と調整の上、決定する。

②現地での業務体制
本業務に係るプロジェクト団員構成は、以下のとおりです。
ア）チーフアドバイザー（国際協力専門員、シャトル派遣）
イ）キャリア開発計画（本コンサルタント）

ウ）サイバーセキュリティ／業務調整（直営）

③便宜供与内容

JICA ベトナム事務所・プロジェクトによる便宜供与事項は以下のとおりです。

ア）空港送迎

あり

イ）宿舎手配

第 1 回現地業務到着時のみあり

ウ）車両借上げ

全行程に対する移動車両の提供

エ）通訳傭上

あり（必要に応じて）

オ）現地日程のアレンジ

あり

カ）執務スペースの提供

あり（C/P 機関より提供）

キ）現地業務サポートスタッフ

あり（プロジェクトで、IT バックグラウンドを持つ現地スタッフを傭上する。現地スタッフは機材調達、キャリア開発計画の作成・モニタリングなど、プロジェクト全般で補助的業務を行うことを想定。）

（２）参考資料

①本業務に関する以下の資料を当 JICA 社会基盤・平和構築部運輸交通・情報通信グループ（TEL:03-5226-3196）にて配布します。

1. ベトナム社会主義共和国「サイバーセキュリティに関する能力向上プロジェクト」要請書（写）
2. ベトナム社会主義共和国「サイバーセキュリティにかかる情報収集・確認調査」ファイナルレポート
3. ベトナム社会主義共和国「サイバーセキュリティに関する能力向上プロジェクト」詳細計画策定調査報告書

②本契約に関する以下の資料を当機構調達部契約第一課にて配布します。配布を希望される方は、代表アドレス（prtm1@jica.go.jp）宛に、以下のとおりメールをお送りください。

ア） 提供資料：「独立行政法人国際協力機構情報セキュリティ管理規程」及び「情報セキュリティ管理細則」

イ）提供依頼メール：

・タイトル：「配布依頼：情報セキュリティ関連資料」

・本文 ：以下の同意文を含めてください。

「標記資料を受理した場合、プロポーザル作成に必要な範囲を超えての使用、複製及び第三者への提供は行わず、プロポーザル提出辞退後もしくは失注後に速やかに廃棄することに同意します。」

（３）その他

①業務実施契約（単独型）については、単独（１名）の業務従事者の提案を求めている制度ですので、複数の業務従事者によるプロポーザルは無効とさせて頂きます。

②現地業務期間中は安全管理に十分留意してください。現地の治安状況については、JICA ベトナム事務所などにおいて十分な情報収集を行うとともに、現地業務の安全確保のための関係諸機関に対する協力依頼及び調整作業を十分に行うこととします。また、同事務所と常時連絡が取れる体制とし、特に地方にて活動を行う場合は、現地の治安状況、移動手段等について同事務所と緊密に連絡を取る様に留意することとします。また現地業務中における安全管理体制をプロポーザルに記載してください。なお、現地業務に先立ち外務省「たびレジ」に渡航予定の業務従事者を登録してください。

③本業務の実施にあたっては、「JICA 不正腐敗防止ガイダンス（2014 年 10 月）」（http://www2.jica.go.jp/ja/odainfo/pdf/guidance.pdf）の趣旨を念頭に業務を行うこととします。なお、疑義事項が生じた場合は、不正腐敗情報相談窓口または JICA 担当者に速やかに相談してください。

④本業務にかかる契約は「業務の完了を約しその対価を支払う」と規定する約款を適用し、国外での役務提供にかかる対価について消費税を不課税とすることを想定しています。、

以上

別添

ベトナム　サイバーセキュリティに関する能力向上プロジェクト

〇プロジェクト目標

AIS のサイバーセキュリティ能力が強化される。

〇成果

1. セキュリティ品質管理能力が強化される。
2. 事後対応型サービス能力が強化される。
3. 事前対応型サービス能力が強化される。

〇活動

1-1　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。

1-2　SecBoK のフレームワークに基づき、それぞれの職員のキャリア開発計画を策定する。なお、キャリア開発計画策定の対象職員は約 40 名である。

1-3 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。

1-4　研修を実施する。

1-5　キャリア開発計画をレビューする（例：6 ヶ月毎）。

1-6　政策策定者に対する研修を計画・実施する。

1-7　啓発教材を開発、ローカライズする。

2-1 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：インシデントマネージャ、インシデントハンドラー、トリアージ）の研修コースを計画する。

2-2　研修を実施する。

2-3　キャリア開発計画をレビューする（例：6 ヶ月毎）。

2-4　事後対応基幹設備（例：DDoS 攻撃緩和）が拡張される。

3-1 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：リサーチャー、ソリューションアナリスト、脆弱性診断士、情報セキュリティ監査人）の研修コースを計画する。

3-2　研修を実施する。

3-3　キャリア開発計画をレビューする（例：6 ヶ月毎）。

3-4　事前対応基幹設備（例：ネットワーク監視）が拡張される。