

対象国の条件 :ASEAN諸国

研修コース番号 :J1804138

案件番号 :1884579

主分野課題 :情報通信技術/情報通信技術

副分野課題 :

使用言語 :英語

案件概要

ASEAN地域におけるサイバーセキュリティ対策の強化に向けて、ASEAN加盟国のサイバーセキュリティにかかる政策担当者を対象に、日本及びASEAN各国のサイバーセキュリティ関連政策に関する情報交換、重点分野での日本の取組みの紹介を行うとともに、これらをどのように自国に活用できるかの考察を通じ、ASEAN各国のサイバーセキュリティ政策の立案及び実施に必要な能力を向上させる。

目標/成果	対象組織/人材	
<p>【案件目標】 ASEAN地域におけるサイバーセキュリティ対策の強化に向けて、ASEAN各国で適切なサイバーセキュリティ政策の立案及び実施がなされるよう、能力向上を図る。</p> <p>【成果】 (1) 日本及びASEAN各国におけるサイバーセキュリティ政策及び関連した重点分野（重要防護インフラ、意識啓発、人材育成、官民連携、インシデントマネジメント等）に関する基本事項について知識を習得し、自国と日本との政策・組織体制の違いを説明できる。 (2) サイバーセキュリティ政策に関連した重点分野における日本の取組について理解を深め、自国のサイバーセキュリティ政策への応用について検討できる。 (3) サイバーセキュリティ政策に関して得られた知識・理解を基に、自国のサイバーセキュリティ政策の改善に向けた提案ができる。</p>	<p>【対象組織】 各国の政府機関（省庁） 政府CSIRT (Computer Security Incident Response Team) National CSIRT</p> <p>【対象人材】 ア. サイバーセキュリティにかかる政策を担当する者（具体的には、サイバーセキュリティに関する枠組み作り、戦略策定、法制度の整備、政策の立案、必要な取組みの実施等を行う者） イ. 課長、課長補佐、もしくは同等の職位の者</p>	
<p style="text-align: center;">内 容</p> <p>1. 事前活動： インセプションレポートの作成</p> <p>2. 本邦研修 (1) 発表 ① インセプションレポート発表（参加国のサイバーセキュリティに関する課題や対策、体制等の共有）② アクションプランの作成及び発表 (2) 講義、意見交換 ① 日本におけるサイバーセキュリティ政策、組織体制 ② 日本におけるサイバーセキュリティインシデントの現状と課題 ③ 日本のサイバーセキュリティに関する人材育成、意識啓発の現状と課題 ④ 日本のサイバーセキュリティに関する官民連携の現状と課題 ⑤ 日本のASEAN地域におけるサイバーセキュリティに関する国際協力 ⑥ サイバーセキュリティに関する最新の技術動向、脅威 ⑦ サイバーセキュリティに関する標準化の動向 ⑧ 重要防護インフラ、IoTに関するサイバーセキュリティ対策 ⑨ サイバーセキュリティ製品やソリューションを扱う本邦企業との意見交換 (3) ワークショップ、ディスカッション 研修を通じて理解した日本及び参加国のサイバーセキュリティ政策・体制等の違い、参加国における課題やそれに対する取組み、アクションプラン等に関するワークショップ、ディスカッション</p> <p>3. 事後活動： 所属組織へのアクションプランの共有及び研修報告</p>	<p>本邦研修期間</p>	<p>2019/1/27～2019/2/7</p>
		<p>担当課題部</p>
	<p>所管国内機関</p>	<p>JICA東京（経済環境）</p>
		<p>関係省庁</p>
	<p>実施年度</p>	<p>2017～2019</p>
<p>主要協力機関</p>	<p>株式会社富士通ラーニングメディア、JPCERT/CC, 情報処理推進機構（IPA）、ICT-ISAC, 日本情報経済社会推進機構（JIPDEC）等</p>	
<p>特記事項及びホームページ</p>	<p>本件は、2014年度～2016年度に実施していた、JICA課題別研修「情報セキュリティ政策能力向上」をもとに、ASEAN向けのサイバーセキュリティ政策に関する研修として、内容を修正し、実施するものである。</p>	