

対象国の条件 : 全世界

研修コース番号 : J1804211

案件番号 : 1884860

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**

増加するサイバー攻撃に対応するため、対象国政府のLAN管理者のインシデントレスポンス(被害の早期発見・検知ならびに対処)能力の向上を目的としており、日常の運用を考慮しながら、事業継続を脅かす攻撃に対応できる「総合力の高い情報システム管理者」の養成を目指すもの。

目標/成果	対象組織/人材	
<p><b>【案件目標】</b> 対象国政府において、最新のセキュリティ対策にかかる講義、及びインシデントハンドリングの演習を通じ、標準型攻撃に対するインシデントレスポンスに必要な組織、機能、技術、手順、人材を理解する人材が育成される。</p> <p><b>【成果】</b> 本邦研修修了時、研修員に期待される内容は以下の通り、                      (1) 最近のサイバー攻撃事例と対策を理解し、説明できる。                      (2) 標的型攻撃のインシデントハンドリングの一連の手順を理解し、説明できる。                      (3) 自国においてインシデントレスポンスに必要な組織、機能、技術、手順、人材を検討し、自国の関係組織に説明・共有できる。</p>	<p><b>【対象組織】</b> 各国の情報セキュリティを所管する官庁又は部局、CSIRTs、及びナショナルCERT</p> <p><b>【対象人材】</b> サイバーインシデント・ハンドリングを行う、セキュリティスペシャリストが選ばれることが望ましい。以下に当てはまる者を推薦することが期待される。                      (1) 今現在、CSIRTにてサイバーインシデント・ハンドリングを実施している者。                      (2) サイバーセキュリティの専門用語についての基本的な知識及びサーバー・ネットワーク運用についての基本的なスキルを有する者。                      (3) 英語での会話及び読み書きが堪能である者 (TOEFL iBTにて100またはそれ以上) (積極的なディスカッションへの参加が期待されるため、高度な英語力必要。可能であれば、語学力を証明する書類添付)                      (4) 心身ともに健康である者。                      母子共にリスクを伴う可能性があるため妊婦の参加は推奨していない</p>	
<p style="text-align: center;"><b>内 容</b></p> <p><b>【事前活動】</b> カントリーレポートの作成および提出</p> <p><b>【本邦研修】</b> 以下の内容の講義、実習、視察、討論を行う。                      1. セキュリティ技術概説                      2. セキュリティインシデントとその対応                      3. 最新の脅威情報とその対応                      4. 情報連携演習                      5. 実践的防御演習 (監視・分析業務、インシデントハンドリング、報告書作成)                      6. サイバーセキュリティ関連企業の視察                      7. アクションプランの作成</p> <p><b>【事後活動】</b> 所属組織への報告、アクションプランの実行、帰国後の活動報告                      ※研修員の作成するアクションプランの内容を鑑みて毎年2か国程度対象国を選択し、研修協力機関による現地フォローアップ活動を実施する</p>	<p><b>本邦研修期間</b></p>	<p>2019/2～2019/3</p>
	<p><b>担当課題部</b></p>	<p>社会基盤・平和構築部</p>
	<p><b>所管国内機関</b></p>	<p>JICA東京 (経済環境)</p>
	<p><b>関係省庁</b></p>	<p>総務省</p>
	<p><b>実施年度</b></p>	<p>2016～2018</p>

<p><b>主要協力機関</b></p>	<p>日本電気(株)</p>
----------------------	----------------

<p><b>特記事項 及び ホームページ</b></p>	
--------------------------------------	--