課題別研修
「サイバー攻撃防御演習」
業務完了報告書

令和元年9月
（2019年）

独立行政法人
国際協力機構（JICA）

日本電気株式会社

基盤
ＪＲ
19-100

課題別研修
「サイバー攻撃防御演習」
業務完了報告書

令和元年 9 月
（2019 年）

独立行政法人
国際協力機構（JICA）

日本電気株式会社

要約

1. プロジェクトの背景

近年、サイバー攻撃による被害の増大は世界的な潮流ともなっており、世界各国において、政府や重要インフラに対するサイバー攻撃が発生している。我が国でも、2011年以降、防衛関連企業、重要インフラ、衆参両議院、中央省庁などの行政機関が相次いでサイバー攻撃を受けていたことが判明し、サイバーセキュリティ対策の強化に乗り出している。一方、ASEAN 地域を始めとする途上国では、サイバーセキュリティに対し、政策／法律の未整備、不十分なセキュリティ対策、セキュリティを担う人材の不足等のため、独自での体制の整備が難しいことが課題となっている。その結果、各国政府機関において、サイバー攻撃によるホームページ改竄、政府システムのダウン、標的型メールによる被害等が多発している。さらに、途上国におけるシステムなどの脆弱性が、連鎖的に先進国への脅威になることも懸念されている。

我が国の ASEAN 地域のサイバーセキュリティにおける協力の枠組みとして、2009年より継続実施中の「日 ASEAN 情報セキュリティ政策会議」があり、同枠組みの下、内閣官房、総務省、経済産業省、外務省、JICA 等が、我が国を含む ASEAN 地域における安心安全な情報通信技術（以下、「ICT」という）の利用環境の構築に向け、政策、組織・制度、人材、技術の各面において支援を行っている。

そのような背景を受け、本研修は、世界的に増加する標的型攻撃等のサイバー攻撃への対応能力の向上を図るため、ASEAN 諸国を始めとする諸外国の標的型攻撃に対する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いる。

2. プロジェクトの内容

2017 年～2019 年の 3 年間にわたるプロジェクトで、ASEAN 諸国を始めとする対象国の、情報セキュリティを主管する官庁又は部局、ナショナル CERT、及び他省庁の LAN 管理部門において、管理職又は管理職に相当する役職の者、及びセキュリティ関連技術者を年 1 回日本に招聘し、2 週間に渡り本邦にてインシデントレスポンス能力の向上に向けた講義・実機演習・企業訪問等（以下、「本邦研修」という）を行った。講義では、セキュリティ技術の基礎知識のみならず、最新の脅威情報、サイバー攻撃の被害とその対策に関わるコンテンツを提供した。実機演習では、サイバー攻撃やインシデントが発生した際にインシデントの全貌を把握するために要求される関係者や関係機関への報告、情報共有等のコミュニケーションを訓練形式で学んでもらった。また、政府機関が標的型攻撃を受け、被害が発生した環境を演習環境として構築し、インシデントの発見・報告、問題個所の特定・隔離、分析・解析、被害状況の確

認等を行う実践的防御演習を提供し研修員を指導した。さらに、本邦研修に参加する前には、事前学習として各国政府がサイバーセキュリティインシデントに関し抱えている課題等に関するカントリーレポートを作成・提出してもらい、自身の国や組織における問題点・課題を整理し、発表・ディスカッションを実施した。本邦研修の最終日には、自身の国や組織における問題点・課題に対して、本邦研修で学習した内容をどう還元していくか、組織に対してどのような貢献をしていくかアクションプランを作成してもらい、発表・ディスカッションを実施した。帰国後、定期的にアクションプランに対する活動の進捗をレポートにて報告してもらい、適宜日本からアドバイスや関連情報を提供することでアクションプランの遂行を支援した。本邦研修から半年後を目途にアクションプランの進捗が良い研修員や自身の組織に積極的に貢献しようと活動している研修員を支援するため、対象国から 2 か国選定し現地フォローアップ活動として現地を訪問し、研修員の同僚等を招いた小規模なワークショップを開催した。

上記のような活動を通して、自身の国や組織におけるサイバーセキュリティ人材育成の推進役になれる人材を育成し、深刻なサイバーセキュリティ人材不足の解消に努めた。

3. プロジェクトの成果

3 年間を通して、ASEAN8 か国（カンボジア、インドネシア、ラオス、マレーシア、ミャンマー、フィリピン、タイ、ベトナム）＋イラン、イラク、ジンバブエからの研修員計 54 名を日本に招聘し、インシデントレスポンス[1]能力向上のための演習を実施した。演習実施後のアンケートでは、「研修を通じ、インシデントハンドリング[2]の一連の手順を理解し、その内容を他者に説明することができるか。」という目標に対する自己評価の回答として、3 年間を通して、2 年次の未回答 1 名を除いた全員が“達成できた”と評価している。また、最も高い評価である“十分達成できた”と回答した研修員が、1 年次に 11 名（64.7%）、2 年次に 10 名（62.5%(未回答除く)）、3 年次に 13 名（75.0%）となっており、カリキュラムや演習運営者による受講生のサポート等により研修員の能力向上に大きく貢献出来たといえる。

また、現地フォローアップ活動でのインシデントレスポンスに関する小規模なワークショップにおいては、本邦研修に参加した計 13 名の研修員にチューターとして参加

[1] インシデントレスポンス…インシデントハンドリングを実行する上で、核となる活動で、初動対応（対応方針の検討、証拠保全、封じ込め、根絶）、復旧措置、再発防止策の検討を実行すること。

[2] インシデントハンドリング…情報セキュリティを脅かす事件や事故に対して、事象を把握・分析し、原因追及、対応策の優先順位付け、対応策の検討、外部組織との連携、内部関係部門への注意喚起、復旧措置を実行すること。
参考：https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer_20151126.pdf

してもらい、自身の同僚に対し教える立場として運営側に回ってもらった。研修員は本邦研修にて学んだことを事前に再度学習するとともに、教わる立場からでは気づきにくかった細かな技術知識も習得し、知識を定着させることが出来た。何より、トレーナーとしての自覚を持ってもらう機会を提供することもでき、ワークショップ中、同僚から研修員に積極的に質問する姿が見られ、研修員に対する同僚の見方も変化したと考える。

更に、個々の能力向上のみならず、他国の CSIRT 実務関係者と 2 週間の研修を共にすることで、信頼関係を構築でき、研修が終わった後も SNS 等を通じて定期的に情報共有する様子も見受けられた。インシデントレスポンスの早期対処に不可欠な多国間・多組織連携のために必要な信頼関係も構築できているといえる。国境のない空間におけるサイバー攻撃に対抗するためには、個々の能力のみならず多国間での連携も重要な要素となってくるため、両面において本プロジェクトは大きく貢献したといえる。

4. 本邦研修の様子

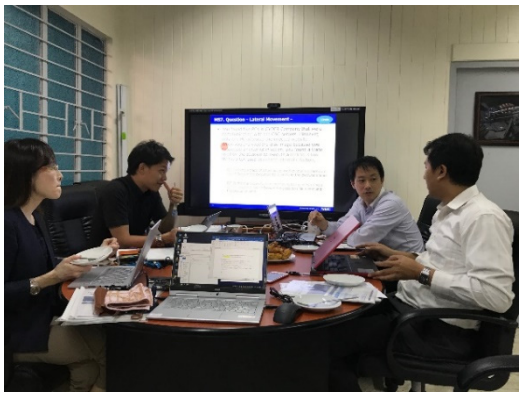
本邦研修（1 年次：情報連携演習）

本邦研修（2 年次：実践的防御演習（左）、反省会（右））

本邦研修（3 年次：研究機関の視察）

5. 現地フォローアップ活動の様子

現地フォローアップ活動（1 年次）



現地フォローアップ活動（2 年次）

現地フォローアップ活動（3 年次）

目次

1. 案件の概要 1
(1) 案件名 1
(2) 研修期間 1
① 研修事前活動 2
② 本邦研修 2
③ 研修事後支援活動（アクションプラン実行） 2
④ 現地フォローアップ活動 2
(3) 研修員人数、国名 3
① 研修事前活動・本邦研修・研修事後支援活動 3
② 現地フォローアップ活動 4
2. 研修内容 4
(1) 研修全体概念図 4
(2) 日程表 5
① 研修事前活動 5
② 本邦研修 6
③ 研修事後支援活動 9
④ 現地フォローアップ活動 9
(3) 単元目標ごとのカリキュラム構成 9
① 単元目標 1 11
② 単元目標 2 14
③ 単元目標 3 18
3. 案件目標（アウトカム）と単元目標（アウトプット）の達成度 23
(1) 案件目標 23
(2) 単元目標 25
① 単元目標 1 25
② 単元目標 2 27
③ 単元目標 3 30
(3) 達成度測定結果 36
① 案件目標 36
② 単元目標 1 36
③ 単元目標 2 36
④ 単元目標 3 38
4. 研修案件に対する所見 40

(1) 研修デザイン～研修期間・プログラム構成等.....40
(2) 研修内容（コンテンツ）～研修プログラム内容・研修教材等.....41
(3) 研修の効果を高める工夫.....48
(4) 研修対象の選定.....49
(5) 研修運営体制.....52
① 研修実施機関.....52
② 研修監理員.....52
(6) 事前活動・事後活動.....52
① 事前活動.....52
② 事後活動.....52
5. 次年度へ向けた改善点及び提案.....56
(1) 評価会及び反省会における指摘事項と改善結果.....56
(2) 次年度 GI に反映させるべき点.....59
① 対象機関.....59
② 対象人材等.....60
③ 研修目標.....60
④ 研修内容等.....61

1. 案件の概要

近年、サイバー攻撃による被害は世界規模で拡大している。中でも政府機関や重要インフラを対象とした標的型攻撃による被害が深刻化（図 1 1　米国 ICS-CERT による重要インフラへのインシデント報告件数）しており、サイバーセキュリティ能力の向上に向けた対策の必要性は世界各地で高まっている。

本研修は、世界的に増加する標的型攻撃等の新たなサイバー攻撃への対応能力の向上を図るため、これら攻撃に対する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する。

図 1-1　米国 ICS-CERT による重要インフラへのインシデント報告件数

（1）案件名

課題別研修「サイバー攻撃防御演習（Defense Practice against Cyber Attacks）」

（2）研修期間

本研修は、「研修事前活動」、「本邦研修」、「フォローアップ活動（アクションプラン実行）」（以下、「研修事後支援活動」という）、「フォローアップ活動（現地フォローアップ）」（以下、「現地フォローアップ活動」という）の 4 部に分かれ、それぞれ以下の日程で実施した。

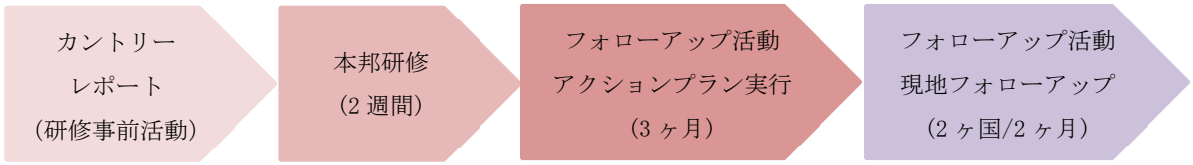


図 1-2　本研修の構成

① 研修事前活動

事前課題として、各国政府がサイバーセキュリティインシデントについて抱えている課題等に関するカントリーレポートを作成・提出してもらった。カントリーレポート作成においては、カントリーレポート作成要領を作成し、募集要項（以下、「GI (General Information)」という）に添付した。

1 年次：募集開始～2017 年 2 月 3 日（金）
2 年次：募集開始～2018 年 2 月 16 日（金）
3 年次：募集開始～2019 年 2 月 4 日（月）

② 本邦研修

セキュリティインシデントへの対応能力向上を目的とした、講義、視察、演習、アクションプラン（案）の作成から構成される 2 週間の本邦研修を実施した。

1 年次：2017 年 2 月 19 日（日）～2017 年 3 月 4 日（土）
2 年次：2018 年 2 月 25 日（日）～2018 年 3 月 10 日（土）
3 年次：2019 年 2 月 17 日（日）～2019 年 3 月 1 日（土）

③ 研修事後支援活動

本邦研修で作成したアクションプランについて、帰国後の実施状況、問題点、見直しスケジュール等を報告してもらい、メールでコメントやアドバイス等の支援を実施した。

1 年次：
2017 年 4 月 7 日（金）：第 1 回目提出
2017 年 5 月 12 日（金）：第 2 回目提出
2017 年 6 月 2 日（金）：第 3 回目提出

2 年次：
2018 年 4 月 6 日（金）：第 1 回目提出
2018 年 5 月 4 日（金）：第 2 回目提出
2018 年 6 月 1 日（金）：第 3 回目提出

3 年次：
2019 年 3 月 29 日（金）：第 1 回目提出
2019 年 4 月 26 日（金）：第 2 回目提出
2019 年 5 月 31 日（金）：第 3 回目提出

④ 現地フォローアップ活動

本邦研修参加国から各年次 2 ヶ国を対象に現地を訪問し、次年度以降の研修内容改善に必要な情報収集を行うとともに、フォローアップセミナーを実施した。

1 年次：
インドネシアとミャンマーの 2 ヶ国を訪問し、アクションプラン報告会と、1day seminar を実施した。

インドネシア：2017 年 7 月 30 日（日）~2017 年 8 月 4 日（金）

ミャンマー　：2017 年 8 月 29 日（火）~2017 年 9 月 2 日（土）

2 年次：

マレーシアとフィリピンの 2 ヶ国を訪問し、アクションプラン報告会と、1 day seminar あるいは 1.5day seminar（以下、「1/1.5 day seminar」という）を実施した。

マレーシア　：2018 年 8 月 26 日（日）~2018 年 8 月 31 日（金）

フィリピン　：2018 年 9 月 3 日（月）~2018 年 9 月 8 日（土）

3 年次：

ラオスとベトナムの 2 ヶ国を訪問し、アクションプラン報告会と、1.5 day seminar を実施した。

ベトナム：2019 年 8 月 5 日（月）~2019 年 8 月 9 日（金）

ラオス　：2019 年 8 月 19 日（月）~2019 年 8 月 24 日（金）

(3) 研修員人数、国名

本案件における参加国と研修員人数は以下の通りである。

① 研修事前活動・本邦研修・研修事後支援活動

1 年次：

インドネシア	3 名	
フィリピン	1 名	
カンボジア	3 名	
ラオス	4 名	
ベトナム	4 名	
ミャンマー	2 名	計 6 ヶ国 17 名

2 年次：

フィリピン	1 名	
カンボジア	3 名	
ラオス	3 名	
ベトナム	3 名	
マレーシア	3 名	
タイ	3 名	
ミャンマー	1 名	計 7 ヶ国 17 名

3 年次：

カンボジア	1 名
インドネシア	3 名
イラン	1 名
イラク	1 名
ラオス	3 名
マレーシア	3 名
ミャンマー	3 名
フィリピン	1 名
タイ	2 名

ベトナム　　1 名
ジンバブエ　　1 名　　計 11 ヶ国 20 名

② 現地フォローアップ活動

1 年次：

国名	帰国研修員	セミナー参加者
インドネシア	3 名	10 名
ミャンマー	2 名	8 名

2 年次：

国名	帰国研修員	セミナー参加者
マレーシア	3 名	7 名
フィリピン	1 名	8 名

3 年次：

国名	帰国研修員	セミナー参加者
ベトナム	1 名	14 名
ラオス	3 名	9 名

2. 研修内容

(1) 研修全体概念図

案件目標と単元目標の関係を「図 2-1　研修全体概念図」に示す。

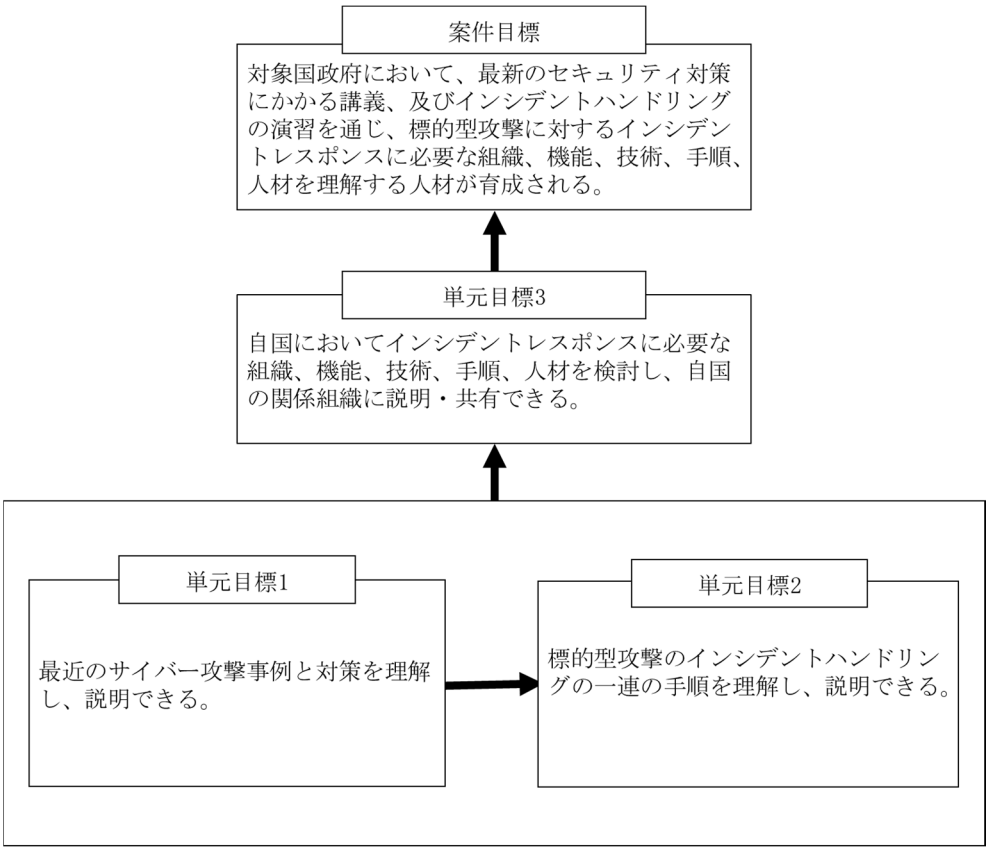


図 2-1　研修全体概念図

(2) 日程表

本案件における本邦研修の研修期間中に実施した研修内容と単元目標との関係をまとめた日程表は以下の通りである。

なお、各日程表の単元目標については、それぞれ以下に対応する。

単元目標 1　…　①

最近のサイバー攻撃事例と対策を理解し、説明できる。

単元目標 2　…　②

研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。

単元目標 3　…　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。

① 研修事前活動

研修事前活動の日程を「表 2-1　研修事前活動における提出締切日程」に示す。

表 2-1　研修事前活動における提出締切日程

	提出締切	単元目標
カントリーレポート（1 年次）	2016 年 12 月 16 日（金）	③
カントリーレポート（2 年次）	2018 年 2 月 16 日（金）	③
カントリーレポート（3 年次）	2019 年 2 月　4 日（月）	③

② 本邦研修

本邦研修の日程を「表 2-2　本邦研修日程表（1 年次）」、「表 2-3　本邦研修日程表（2 年次）」、「表 2-4　本邦研修日程表（3 年次）」に示す。

表 2-2　本邦研修日程表（1 年次）

日付	時刻			形態	研修内容	単元目標
2/20(月)	10:00	～	12:30	講義	ブリーフィング	
	13:30	～	14:30	講義	研修コースオリエンテーション	
	15:00	～	16:30	発表	カントリーレポート説明、発表準備	③
2/21(火)	9:00	～	12:30	発表	カントリーレポート発表	③
	13:30	～	17:00	講義	セキュリティ技術概説	①
2/22(水)	9:00	～	17:00	実習	セキュリティインシデントとその対応	①
2/23(木)	9:00	～	11:00	見学	日本電気株式会社 NECイノベーションワールド視察	①
	11:30	～	17:00	実習	情報連携演習	②
2/24(金)	10:00	～	11:00	見学	株式会社ラック セキュリティオペレーションセンター視察	①
	13:30	～	15:30	見学	日本文化理解研修（浅草ツアー）	①
	16:30	～	17:30	討議	討論会	①
2/25(月)					休息日	
2/26(日)					移動（東京→石川）	
	13:30	～		見学	日本文化理解研修（金沢ツアー）	①
2/27(月)	10:00	～	11:00	見学	国立研究開発法人情報通信研究機構（NICT） 視察	①
	11:00	～	12:00	見学	国立大学法人北陸先端科学技術大学院大学 （JAIST）視察	①
	13:00	～	15:00	講義	実践的防御演習（1日目）	②
					移動（石川→東京）	
2/28(火)	9:30	～	17:00	実習	実践的防御演習（2日目）	②
3/1(水)	9:30	～	17:00	実習	実践的防御演習（3日目）	②
3/2(木)	9:30	～	12:00	講義	最新の脅威情報とその対策	①
	13:00	～	17:00	発表	アクションプラン作成	③
3/3(金)	9:30	～	14:30	発表	アクションプラン発表	③
	15:00	～	16:00		評価会	
	16:00	～	16:30		閉講式	
	17:00	～	18:00		閉講パーティー	

表 2-3　本邦研修日程表（2 年次）

日付	時刻			形態	研修内容	単元目標
2/26(月)	10:00	～	12:30	講義	ブリーフィング	
	13:30	～	15:00	講義	研修コースオリエンテーション	
	15:00	～	16:30	発表	カントリーレポート説明、発表準備	③
2/27(火)	9:00	～	12:30	発表	カントリーレポート発表	③
	13:30	～	17:00	講義	実践的防御演習（1日目） - セキュリティ技術概説 - 最新の脅威情報とその対策 - 実力テスト	②
2/28(水)	10:00	～	11:00	見学	株式会社ラック セキュリティオペレーションセンター視察	①
	13:30	～	15:30	見学	日本文化理解研修（浅草ツアー）	①
3/1(木)	9:30	～	17:00	講義	セキュリティインシデントとその対応	①
3/2(金)					移動（東京→石川）	
	14:00	～	15:30	見学	国立研究開発法人情報通信研究機構（NICT） 視察	①
	15:30	～	17:30	見学	国立大学法人北陸先端科学技術大学院大学 （JAIST）視察	①
3/3(土)	9:00	～	12:00		日本文化理解研修（金沢ツアー）	①
					移動（石川→東京）	
3/4(日)					休息日	
3/5(月)	9:30	～	17:00	実習	実践的防御演習（2日目） - ツール使用方法説明	②
3/6(火)	9:30	～	17:00	実習	実践的防御演習（3日目）	②
3/7(水)	9:30	～	11:00	実習	実践的防御演習（4日目）	②
	11:00	～	11:30		達成度テスト	②
	13:00	～	17:00	実習	情報連携演習	②
3/8(木)	9:30	～	11:00	見学	日本電気株式会社 NECイノベーションワールド視察	①
	13:00	～	17:00	発表	アクションプラン作成(グループ討論会)	③
3/9(金)	9:30	～	14:30	発表	アクションプラン発表	③
	15:00	～	16:00		評価会	
	16:00	～	16:30		閉講式	
	17:00	～	18:00		閉講パーティー	

表 2-4　本邦研修日程表（3 年次）

日付	時刻			形態	研修内容	単元目標
2/18(月)	10:00	～	12:30	講義	ブリーフィング	
	13:30	～	15:00	講義	研修コースオリエンテーション	
	15:00	～	17:00	発表	カントリーレポートディスカッション・発表	③
2/19(火)	9:30	～	16:30	講義	OSINT演習	②
2/20(水)	9:30	～	16:30	講義	実践的防御演習（1日目） - セキュリティ技術概説 - 最新の脅威情報とその対策 - 実力テスト - ツール使用方法説明	②
2/21(木)	9:30	～	16:30	実習	実践的防御演習（2日目）	②
2/22(金)	9:30	～	16:30	実習	実践的防御演習（3日目） （グループディスカッション含む）	②
2/23(土)					休息日	
2/24(日)					移動（東京→石川）	
	13:30	～			日本文化理解研修（金沢ツアー）	①
2/25(月)	10:00	～	11:30	見学	国立大学法人北陸先端科学技術大学院大学（JAIST）視察	①
	13:00	～	15:00	見学	国立研究開発法人情報通信研究機構（NICT）視察	①
					移動（石川→東京）	
2/26(火)	9:30	～	14:50	実習	情報連携演習	②
	15:00	～	16:00	講義	JPCERT/CC活動紹介	①
	16:00	～	16:30		達成度テスト	②
2/27(水)	9:30	～	16:30	講義	セキュリティインシデントとその対応	①
2/28(木)	9:30	～	11:00	見学	株式会社ラック セキュリティオペレーションセンター視察	①
	13:30	～	16:30	発表	アクションプラン作成	③
3/1(金)	9:30	～	14:30	発表	アクションプラン発表	③
	15:00	～	16:00		評価会	
	16:00	～	16:30		閉講式	
	16:30	～	17:30		閉講パーティー	

③　研修事後支援活動

研修事後支援活動について、アクションプランの提出締切の日程を「表 2-5　アクションプラン提出締切の日程」に示す。

表 2-5　アクションプラン提出締切の日程

		アクションプラン提出締切	単元目標
1 年次	1 回目	2017 年 4 月 7 日（金）	③
	2 回目	2017 年 5 月 12 日（金）	③
	3 回目	2017 年 6 月 2 日（金）	③
2 年次	1 回目	2018 年 4 月 6 日（金）	③
	2 回目	2018 年 5 月 4 日（金）	③
	3 回目	2018 年 6 月 1 日（金）	③
3 年次	1 回目	2019 年 3 月 29 日（金）	③
	2 回目	2019 年 4 月 26 日（金）	③
	3 回目	2019 年 5 月 31 日（金）	③

④　現地フォローアップ活動

現地フォローアップ活動の日程を「表 2-6　現地フォローアップ活動の日程」に示す。

表 2-6　現地フォローアップ活動の日程

		アクションプラン 報告会	1/1.5day seminar	単元 目標
1 年次	インドネシア	2017 年 8 月 1 日（火）	2017 年 8 月 2 日（水）	③
	ミャンマー	2017 年 8 月 31 日（木）	2017 年 9 月 1 日（金）	②
2 年次	マレーシア	2018 年 8 月 28 日（火）	2018 年 8 月 29 日（木）	③
	フィリピン	2018 年 9 月 4 日（木）	2018 年 9 月 6 日（木） ～9 月 7 日（金）AM	②
3 年次	ベトナム	2019 年 8 月 7 日（水）	2019 年 8 月 8 日（木） ～8 月 9 日（金）AM	③
	ラオス	2019 年 8 月 21 日（水）	2019 年 8 月 22 日（木） ～8 月 23 日（金）AM	②

(3) 単元目標ごとのカリキュラム構成

各年次における単元目標ごとのカリキュラムを「表 2-7　単元目標ごとのカリキュラム」に示す。

表 2-7　単元目標ごとのカリキュラム

項目	内容
単元目標１	最近のサイバー攻撃事例と対策を理解し、説明できる。
本邦研修	
	実践的防御演習（1日目：講義） － セキュリティ技術概説 － 最新の脅威情報とその対策
	セキュリティインシデントとその対応
	国立研究開発法人情報通信研究機構（NICT）視察
	国立大学法人北陸先端科学技術大学院大学（JAIST）視察
	株式会社ラック　セキュリティオペレーションセンター視察
	日本電気株式会社　NECイノベーションワールド視察 ※1年次、2年次のみ
	討論会（ICT関連企業のソリューション紹介、討議）※1年次のみ
	JPCERT/CC活動紹介　※3年次のみ
項目	内容
単元目標２	研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。
本邦研修	
	実践的防御演習（1日目：実習） － 実力テスト － ツール使用方法説明
	実践的防御演習（2日目）
	実践的防御演習（3日目：グループディスカッション含む）
	情報連携演習
	OSINT演習　※3年次のみ
現地フォローアップ研修	
	1/1.5 day seminar
項目	内容
単元目標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。
研修事前活動	
	カントリーレポート作成
本邦研修	
	カントリーレポート発表準備
	カントリーレポート発表
	アクションプラン作成
	アクションプラン発表
研修事後活動	
	アクションプラン実行
現地フォローアップ研修	
	アクションプラン報告会

① 単元目標 1

最近のサイバー攻撃事例と対策を理解し、説明できる。

・本邦研修

➢ 講義

インシデントレスポンス能力強化の必要性を理解することを目的として、最新の脅威動向及びその対策の概要について講義を実施した。

1 年次は、提出されたカントリーレポートの内容や各国のサイバーセキュリティ対策の状況を鑑みて、各国のニーズに対応するように研修カリキュラムを設定した。特に、参加各国のサイバーセキュリティに対する取り組み状況が異なることを踏まえ、概論だけでなく具体的な事例の紹介を盛り込むこと、日本のみに偏らず多様な事例を扱うこと等、研修員の理解を促進する内容となるように留意した。

2 年次以降は、前年の研修員の理解度や単元目標の達成度、アンケート結果を踏まえ、講義で取り扱う題材、講義時間の配分を調整し、講義パートの品質向上を図っていった。具体的には、実機演習で研修員に扱ってもらうツールの使い方の講義の時間を増やしたり、極力移動が少なくなるようなカリキュラム構成に変更したりした。また、3 年次には一部の日本文化理解研修の時間を無くし、講義・実機を活用した OSINT 演習を追加した。

そして、3 年次は JPCERT/CC から講師を招き、国内での活動や ASEAN をはじめとする海外のナショナル CSIRT との連携・活動に関しての紹介を研修カリキュラムに追加した。この講義を通して、ナショナル CERT の役割や活動内容、他国間連携の重要性を理解できる構成とした。

表 2-8 講義内容

項目	内容	実施年
セキュリティ技術概説	セキュリティに関する用語、構成、仕組み等技術面を中心に基礎知識を学習する。	1 年次 2 年次 3 年次
最新の脅威情報とその対策	サイバー攻撃の被害と対策に関わる様々な組織及び担当者の役割や通常のアクションを学習する。	
セキュリティインシデントとその対応	サイバー攻撃発生までの流れと感染時の挙動を再現し、技術的な対策や対応の重要性を理解する。	
実践的防御演習（講義）	典型的な標的型攻撃の手法および攻撃者の行動など最新の脅威、およびその対策について学習する。	
JPCERT/CC 活動紹介	JPCERT/CC の日常業務やインシデント発覚後の対応方法、国際的な枠組みでの活動などの説明を通じて、ナショナル CERT の役割、活動概要を理解する。	3 年次

講義内容のテキストの一部を以下に示す。

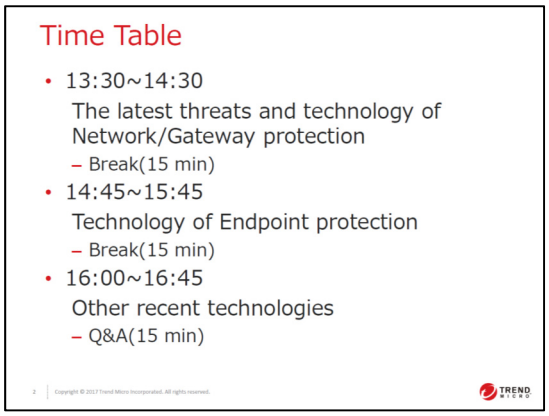
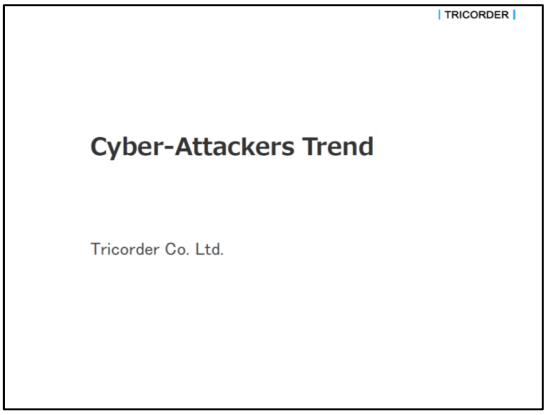


図 2-2 セキュリティ技術概説（一部）



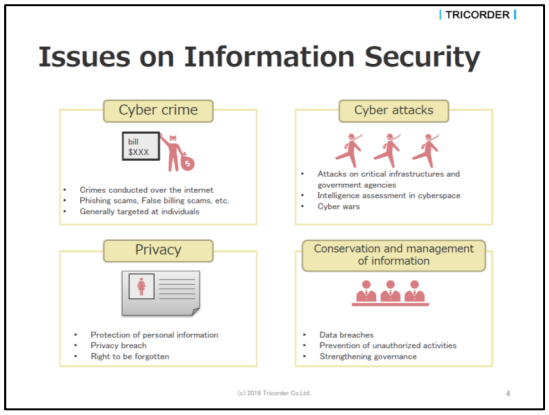


図 2-3 最新の脅威情報とその対策（一部）

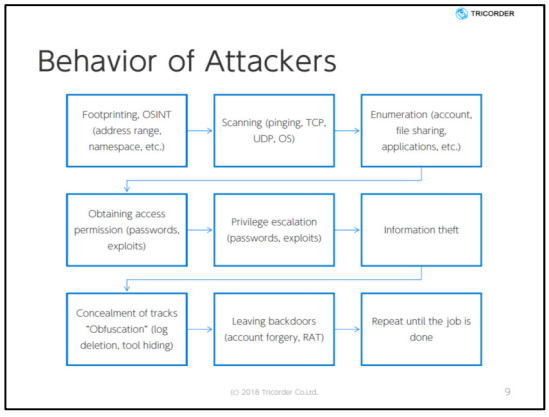


図 2-4 セキュリティインシデントとその対応資料（一部）

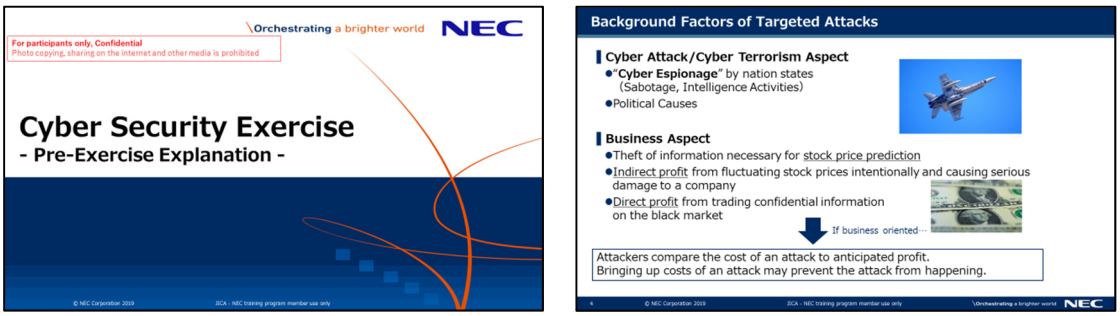


図 2-5 実践的防御演習資料（講義）（一部）

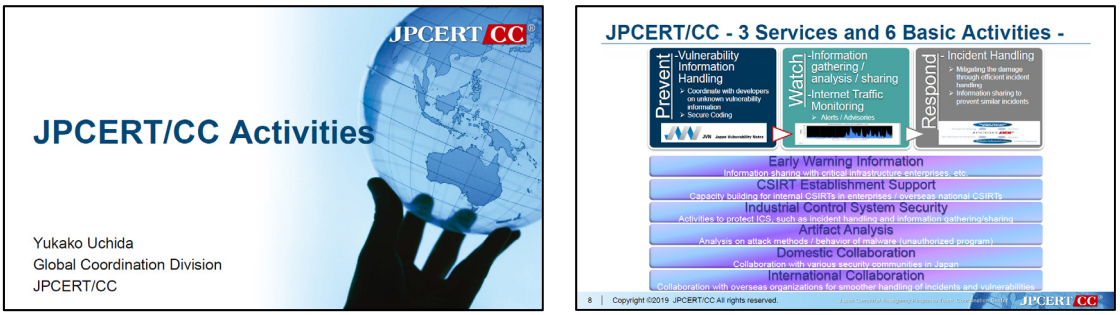


図 2-6 JPCERT/CC 活動紹介資料（一部）

➢　サイバーセキュリティ関連企業の視察（研修旅行）

サイバーセキュリティ対策に有効な機材や施設を視察し、提供されているサービス内容や官民連携について学ぶことを目的とした。我が国におけるサイバーセキュリティ対策の実例を学ぶため、サイバーセキュリティに関連したサービス提供を行う民間企業、大規模なサイバー演習環境を保有する国立研究開発法人情報通信研究機構（以下、NICT という）や、サイバーレンジ構成学をはじめとしたサイバー人材育成に関する研究を行っている国立大学法人北陸先端科学技術大学院大学（以下、JAIST という）といった研究機関を訪問した。

表 2-9 本邦研修における視察先

視察先
日本電気株式会社　NEC イノベーションワールド　※1 年次、2 年次のみ
国立大学法人北陸先端科学技術大学院大学（JAIST）
国立研究開発法人情報通信研究機構（NICT）
株式会社ラック（LAC） JSOC（ジャパンセキュリティオペレーションセンター）

② 単元目標 2

研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。

・ 本邦研修

➢ 演習（実習）

各国の実務環境に即したインシデントレスポンス能力が養成されるよう演習を行った。演習に際しては以下の点に従って演習環境の構築、演習プログラムの運営を実施した。

- ✓ 演習は、研修員を 6 つのグループに分け、同時に複数グループが独立して実施できるものとし、互いに干渉しないようにすること。（3〜4 名で 1 グループ）
- ✓ 演習の実施にあたっては、研修員に対して演習プログラムを実施する者（以下、「講師」という）、実習において研修員の技術的支援や実践的防御演習システムの運用を行う者（以下、「チューター」という）、を確保すること。
- ✓ 演習プログラムの運営については、能力を有する人員（講師、チューター）により運営すること。
- ✓ 講師及びチューターは、研修員の進捗状況に応じた指導を行うこと。

研修員のグループ分けについて、研修員同士のコミュニケーション促進及び各グループの総合的な技術レベルの均等性を考慮してグループ編成を実施した。1 年次については、当初国ごとにチームを編成し演習を実施したが、国ごとに参加人数が異なること、他国からの参加者と話す時間を増やしてほしいなどの要望もあり、2 年次以降は一つのチーム内に同じ国の研修員が複数人にならないように極力分散させ、各国の研修員同士協力して演習に取り組む機会を設けた。これにより、それぞれの国が抱える課題や活動内容の共有を促進する事ができた。

演習コンテンツについて、3 年次に新たに OSINT（オープンソースインテリジェンス）演習を追加し、攻撃者が情報収集の際に実際に使う Web サイトやツールを紹介した。同時に、研修員が同 Web サイトやツールを操作できる環境を提供し、攻撃者がどのように情報を収集し、どのような情報を基に標的を定めているのかを体験できる構成とした。

表 2-10 演習内容基本項目

項目	内容	実施年
実践的防御演習 （実習）	サイバー攻撃に関わるインシデントハンドリングについて、政府機関への標的型攻撃を想定した訓練演習を行う。研修員は被害を受けた環境に対し、インシデントの発見と報告、問題個所の特定と隔離、原因分析と検体の解析、被害状況の確認等を行う。	1 年次 2 年次 3 年次
情報連携演習	架空の国で発生したインシデントについて、各国の CERT 組織と CERT への状況報告を模擬し、インシデントレスポンスに関わる組織間の情報連携を行う。	
OSINT 演習	一般に公開された情報を活用したセキュリティ情報収集・分析方法を知る。また、実習を通じて攻撃者の活動の一部を理解する。	3 年次

演習テキストの一部を以下に示す。

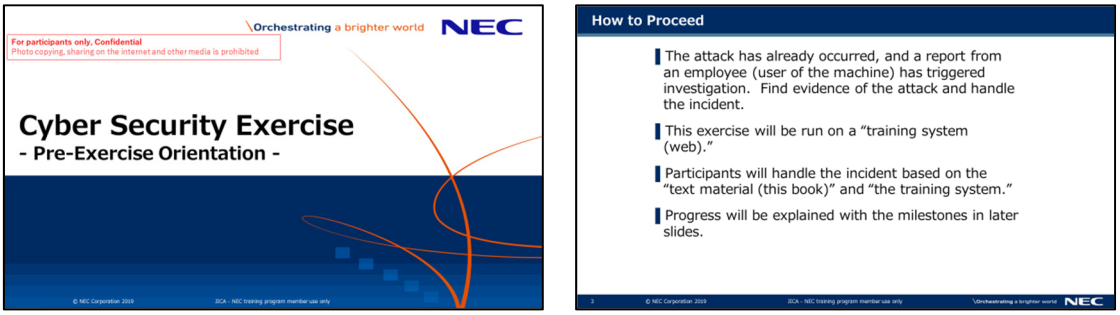


図 2-7 実践的防御演習資料（一部）

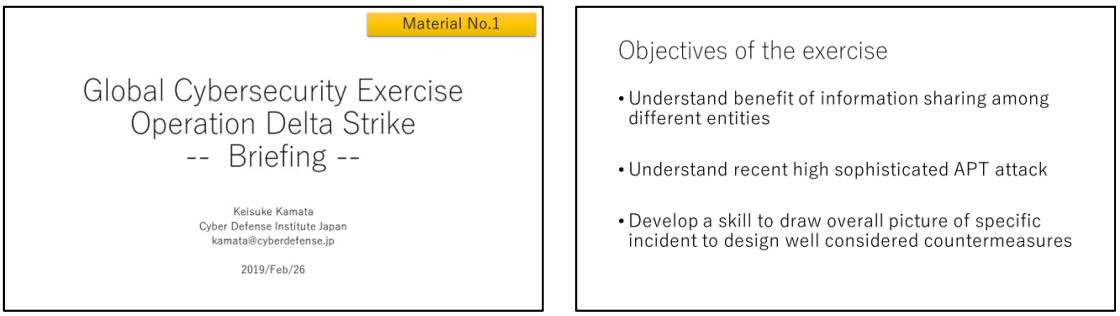


図 2-8 情報連携演習資料（一部）

図 2-9 OSINT 演習資料（一部）

・ 現地フォローアップ活動

➢ 1/1.5 day seminar

1 /1.5 day seminar では、本邦研修で習得したスキルの定着を図るために、帰国研修員がチューターとして参加した。

1 /1.5 day seminar においては、本邦研修にて実施した実践的防御演習を基にしたワークショップを実施した。本邦研修での実践的防御演習は、講義、実機演習、グループディスカッションからなる 2.5 日～3 日間にわたる演習であるが、本ワークショップは以下の点を踏まえてカリキュラムを再編成し、1~1.5 日で完結できるよう開発した。

✓ 講義
本邦研修のアンケート結果を考慮し、人気の高いハンズオン演習が中心となるよう講義内容を構成し、演習実施時必要となるツールの説明及びその操作方法の確認を中心に実施した。

✓ 演習
元々ディスカッション問題とテクニカル問題から成る 16 個のマイルストーンを、ツールを用いたテクニカル問題を中心に、マイルストーン 7 個から成るように演習を再構築した。また、ひとつのマイルストーンが終わるたびに解説を入れる進行方針に変更し、全体の進捗を管理した。
その他、難易度の高いマイルストーンについては、休憩時間を利用して解説を行い、全体の時間を短縮した。なお 1.5 day seminar のみ最終演習としてレポートの作成・発表を実施した。

✓ グループディスカッション
演習の中のディスカッション問題に組み込む形にし、独立したパートとしては削除した。

1/1.5 day seminar のタイムテーブルを下図に示す。

表 2-11　1/1.5 day seminar のタイムテーブル

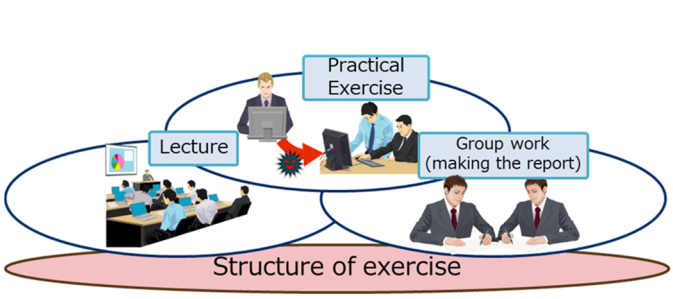
1day seminar		
Day	Time	Contents
Day1	09:30 - 10:00	Self Introduction
	10:00 - 12:00	Tool explanation
	12:00 - 13:00	Lunch break
	13:00 - 13:15	Orientation
	13:15 - 16:00	Hands-on
	16:00 - 16:30	Wrap-up

1.5day seminar		
Day	Time	Contents
Day1	09:30 - 10:00	Self Introduction
	10:00 - 12:00	Tool explanation
	12:00 - 13:00	Lunch break
	13:00 - 14:00	Tool explanation
	14:00 - 14:15	Orientation
	14:15 - 16:30	Hands-on
Day2	09:30 - 11:30	Hands-on & Presentation
	11:30 - 12:00	Wrap-up & Closing

また、本ワークショップのマイルストーンの構成を「図 2-10 マイルストーンの構成」に示す。

1.5 day seminar では、1 day seminar より実習演習時間を長めにするとともに、演習の最後に受講生がレポートを作成し発表する時間を設けた。演習時間を長めに確保することで、一部の受講生が理解不足のまま演習を進めてしまわない様留意した。

また、レポートの作成から発表までを実施することで、技術的な内容にのみ終始せず、ディスカッションや資料作成・プレゼンという様々なトレーニングの機会を提供できた。受講生の中には技術スキルが低くても、レポート作成・発表の場で積極的に対応し、活躍することができるものもいた。単に Linux や Windows 等の技術スキルを問うだけではなくコミュニケーション能力や統率力も活かせる様な構成にすることで、多用なスキルセットを持った受講者のニーズに応えることができ、チーム全体で課題に取り組んでもらうことができたと考える。またレポート発表を受け、帰国研修員から参加者に対してコメントをしてもらうことで、帰国研修員自身のリーダーとしての自覚を促すきっかけにもなった。



1. Detection of incident
2. Report of incident
3. Access to falsified website
4. Drive-by download
5. Obtaining sample and identification of vulnerability
6. Detection of infiltration
7. Evidences of infiltration

図 2-10 マイルストーンの構成

③　単元目標 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。

・　研修事前活動

➢　カントリーレポート作成

研修員は、本邦研修を受ける前に、事前に配布したフォーマットに基づいて、各国政府の組織体制やサイバーセキュリティインシデントについて抱えている課題等についてレポートを作成・提出した。

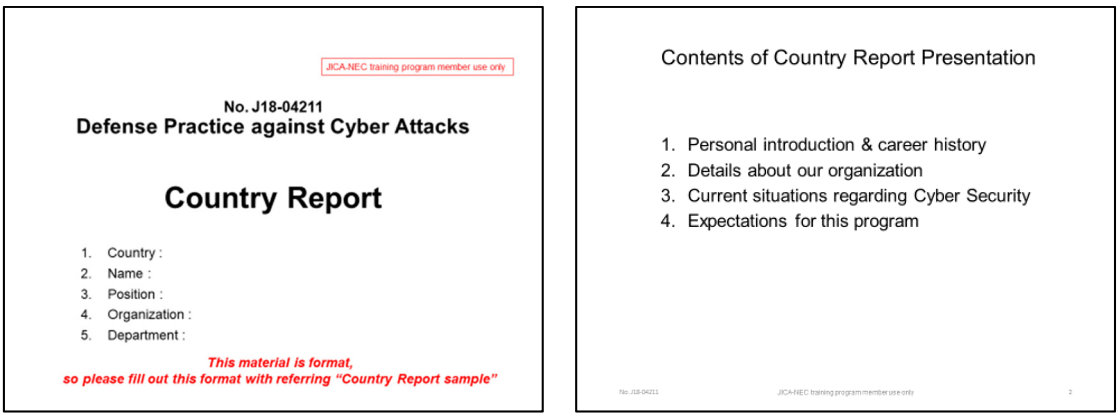


図 2-11 カントリーレポートのフォーマット（一部）

・　本邦研修

➢　カントリーレポート発表準備・発表（討議）

事前に提出されたカントリーレポートについて発表を行い、研修員の所属組織の概要と役割、自組織のサイバーセキュリティに係る課題、本研修への期待等を説明し、その内容について議論を行った。3 年次は研修員人数が増加した中で、演習時間を極力多く確保するため、三つのグループに分けた上で、グループ内で発表と議論を実施し、代表者がグループの総括を全体に共有する構成とした。

各年次におけるカントリーレポート発表の状況を以下に示す。

1 年次：

各国ともに、セキュリティインシデントが年々増加しているにも関わらず、適切に対処するためのセキュリティ人材が不足していること、人材を育成するための要員（トレーナー）が不足していること、およびネットワーク状況を適切に監視するための SOC が構築されていないなど設備の不足を挙げていた。

その他、ベトナム、ミャンマーは、サイバーセキュリティに関する法整備の不足を、インドネシア、ラオス、カンボジアなどは情報共有（信頼関係構築）のための枠組みが適切に整理されていないことを課題として挙げていた。

2 年次：
各国から報告された重大脅威（トップ 3）については、Malware（カンボジア、タイ、マレーシア、ベトナム、フィリピン、ラオス）、Intrusion（マレーシア、タイ、ラオス、カンボジア）、Spam & Phishing（フィリピン、ラオス、ベトナム、ミャンマー）、Web Defacement（フィリピン、ミャンマー、ベトナム）、Fraud（マレーシア、タイ）などが多く挙げられていた。
また、各国の課題としては、セキュリティ人材の不足、システム、予算の不足などを問題としてあげる研修員が多く、人材育成の必要性を訴えるとともに、本研修を通じ、インシデントハンドリングで必要となるツールの使用方法、各種手順などの習得に強い意欲を述べていた。

3 年次：
例年通り、各国の課題としては、セキュリティ要員の人材不足、システム、予算の不足などを問題としてあげる研修員が多く、人材育成の必要性を訴えるとともに、本研修を通じ、インシデントハンドリングで必要となるツールの使用方法、各種手順などの習得に強い意欲を述べていた。
一方で今回初参加の ASEAN 諸国以外のイラン、イラク、ジンバブエに関しては、上記課題に加えて下記のような課題を挙げていた。

- 国外でセミナーに行く機会があまりない
- 国外と情報交換をする場がない
- 最新技術に触れる機会があまりない
- 国内に実践的・高度な演習プログラムがない
- 組織が新設されたばかり
- 政府内の組織が整備されていない（役割分担が不明確、セキュリティ専門の組織がなく意思決定する独立した組織がない）
- 政府のガイドラインが整備されていない。
- （IT）インフラが整っていない

特に、3 ヶ国共通して「国外との情報共有、情報交換の機会の不足」ということを課題と考えていた。
1 年次、2 年次は、各国から全体への共有セッションとしていたが、3 年次は全体を三つのグループに分割し、グループ内で発表してもらうことで、効率的に自組織の問題点や研修受講にあたっての目標などを共有できるようにした。これにより、1 年次、2 年次と比較して、グループ内で質疑応答がかなり活発に実施されている様子が伺えた。また、初日から研修員同士で議論する機会を与えたことで、本邦研修の 2 週間を通しても例年と比較して国を超えたコミュニティー形成・コミュニケーションが多く見られた。

➢ アクションプランの作成・発表（討議）
アクションプランは、カントリーレポートや各国のセキュリティ状況を勘案の上、研修

員が自国に帰国した後、研修員所属組織および研修員自身のインシデントレスポンス能力向上に向けてどのような活動を実施していくのか、その計画を作成するものとした。
本邦研修では、研修時に指定したフォーマットをベースとし、国ごとではなく、各個人の作業としてアクションプランの作成を実施し、チューターによるレビューを受けた上で、最終日に発表会を開催した。
各自、本研修期間中に学んだことを整理し上司等に報告する、演習を通じて学んだ事項を纏め自組織の関係者に展開する、自らが学んだ内容をカスタマイズしてセミナーを開催する等、研修で得た知識をベースに今後のアクションプランをまとめ発表した。

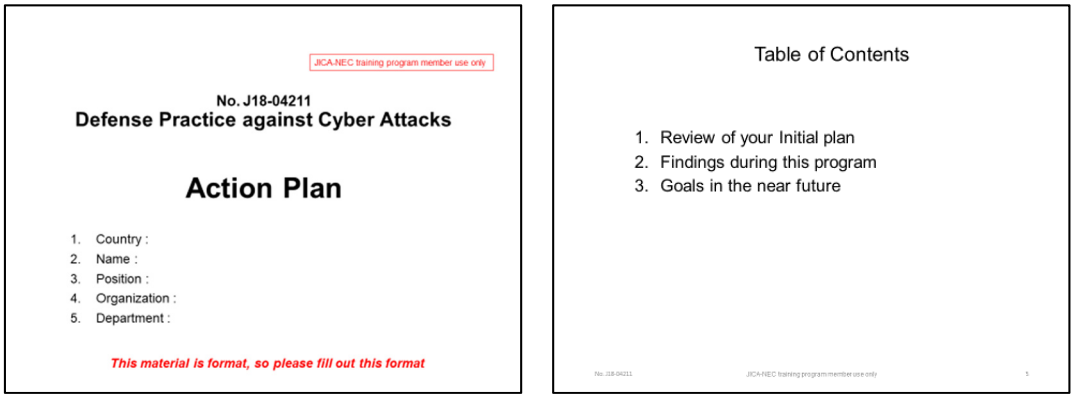
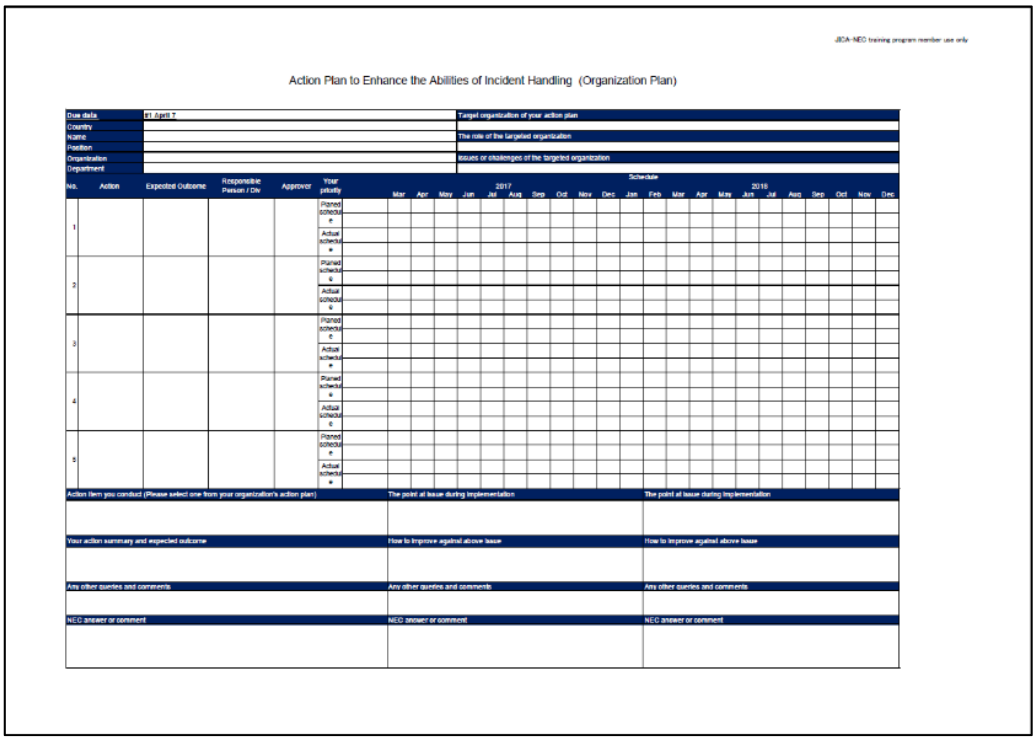


図 2-12　アクションプラン（本邦研修）フォーマット　（一部）

・　研修事後支援

➢　アクションプラン実行

アクションプランの見直し及び実行状況の報告について、帰国後、研修員が帰属する組織内でのアクションプランのレビュー結果やそれに応じて実行したアクションプランの進捗状況に則って、あらかじめ配布したアクションプラン進捗レポート（以下、「進捗レポート」という）を更新してもらう形とした。進捗レポートを 3 ヶ月間に渡って月に 1 回提出してもらい、その進捗レポートを確認し、進捗状況や直面している課題に沿った形で、遠隔でのアドバイスを継続的に行った。本邦研修で学んだことをどうやって自らが所属する組織に還元していくのか、予算をかけない方法で何ができるのか考えてもらう様にアドバイスを心がけ、時には参考情報の URL やツール名を共有する様にした。
（別紙 1～3:　フィードバックコメント参照）
進捗レポートのフォーマットに関して、1 年次には下記「図 2-13　進捗レポートのフォーマット（1 年次）」に示す通り、エクセルファイルをベースとして進捗を確認する形で実施していた。



JICA-NEC training program member use only

Action Plan to Enhance the Abilities of Incident Handling (Organization Plan)

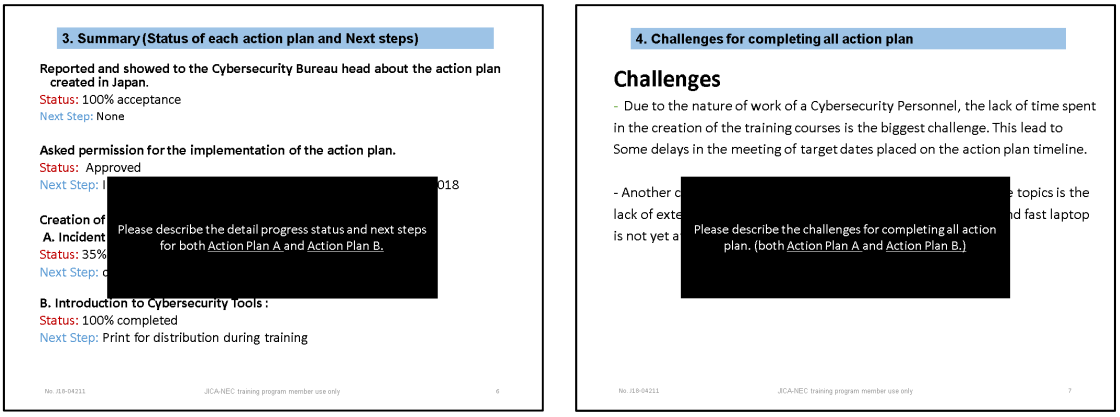
Due date	01 April T			Target organization of your action plan	
Country				The role of the targeted organization	
Name					
Position				Issues or challenges of the targeted organization	
Organization					
Department					

No.	Action	Expected Outcome	Responsible Person / Div	Approver	Your priority	Schedule: 2017 Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan / 2018 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
1					Planned schedule	
					Actual schedule	
2					Planned schedule	
					Actual schedule	
3					Planned schedule	
					Actual schedule	
4					Planned schedule	
					Actual schedule	
5					Planned schedule	
					Actual schedule	

Action item you conduct (Please select one from your organization's action plan)	The point at issue during implementation	The point at issue during implementation
Your action summary and expected outcome	**How to improve against above issue**	**How to improve against above issue**
Any other queries and comments	**Any other queries and comments**	**Any other queries and comments**
NEC answer or comment	**NEC answer or comment**	**NEC answer or comment**

図 2-14　進捗レポートのフォーマット（1 年次）

一方で、2 年次の 1 回目に提出されたフィリピンの研修員の進捗レポートが、アクションプランの具体的な活動内容や経過、目標実現に対する課題を非常によく表現できていたため、以降はこれをベースとしてフォーマットを作成し、それ活用してもらうこととした。提出に当たっては、本邦研修で立てたプラン、目標と現状のギャップ及び直面している課題、今後の活動予定を明確に報告するよう依頼した。



3. Summary (Status of each action plan and Next steps)

Reported and showed to the Cybersecurity Bureau head about the action plan created in Japan.
Status: 100% acceptance
Next Step: None

Asked permission for the implementation of the action plan.
Status: Approved
Next Step: I 018

Creation of
A. Incident
Status: 35%
Next Step: c

Please describe the detail progress status and next steps for both Action Plan A and Action Plan B.

B. Introduction to Cybersecurity Tools :
Status: 100% completed
Next Step: Print for distribution during training

No. J18-04211 JICA-NEC training program member use only 6

4. Challenges for completing all action plan

Challenges

- Due to the nature of work of a Cybersecurity Personnel, the lack of time spent in the creation of the training courses is the biggest challenge. This lead to Some delays in the meeting of target dates placed on the action plan timeline.

- Another c topics is the lack of exte d fast laptop is not yet a

Please describe the challenges for completing all action plan. (both Action Plan A and Action Plan B.)

No. J18-04211 JICA-NEC training program member use only 7

図 2-15　進捗レポートのフォーマット（2 年次以降）

- 現地フォローアップ活動

➢ アクションプラン報告会

研修事後支援活動で研修員が作成・実行したアクションプラン及びその進捗について、

研修員による 15～20 ページの資料によるプレゼンテーションを行った。

〔アクションプラン報告会資料　作成要綱（概要）〕

- ✓ 30 分のプレゼンテーションを実施（発表 20 分、質疑応答 10 分）
- ✓ アクションプランの紹介　（毎月毎の実行内容、議論した相手、困難だった点）
- ✓ 本邦研修の振り返り（最も有益だった研修、さらに学びたい内容、その他、本邦研修全般についての意見）

3. 案件目標（アウトカム）と単元目標（アウトプット）の達成度

以下に、案件目標（全体）に対する達成度、各単元目標（単元目標 1、単元目標 2、単元目標 3）に対する達成度を記載する。

(1) 案件目標

本研修における案件目標は以下の通りである。

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、標的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。

(ア) 指標

案件目標に対する目標達成度を評価する指標は、本研修に設定された単元目標 1～3 のすべてが達成されたかを指標とする。

(イ) 達成度

案件目標に対する達成度については、各単元目標 1～3 について、いずれも指標を達成していることから、計画した研修を滞りなく実施するとともに、本案件目標は達成されたと評価する。

(ウ) 貢献要因、阻害要因

・　貢献要因

案件目標に対する貢献要因については、各単元目標の貢献要因にあるように、本邦研修前から各国の状況把握に努めたこと、また、研修では座学だけでなく、実習形式などの体験型カリキュラムを用意したこと、カントリーレポートやアクションプラン等の発表資料のフォーマットを事前に提示し統一したことが、研修員の積極的な研修への参加を促進し、高い満足度（達成感）につながったと思われる。

「実践的防御演習」では、チーム内で理解度に差が出ないように事前に受講者の出身国や技術的バックグラウンドを考慮してチームを編成したことにより、各チームが想定していた時間より早くすべての課題をクリアすることができた。進捗に遅れが出ていたチームにおいては、チューターが積極的に声掛けをし、チーム全員が理解してから次の課題へ進むように促すことが効果的であった。

更に 3 年次には、初日のカントリーレポート発表のグループを三つに分けて実施したことで、1 年次、2 年次と比較して質疑応答が各チームで積極的に行われ、初日から国を超えた研修員同士でのコミュニケーションを促進できたと思われる。

また、3 年次には新たに研修員による日直制度を導入し、各講義や演習の前に講師の紹介及びその日の全体のアジェンダを研修員に通知してもらう様にした。その結果、各研修員が主体的に研修に参加でき、時間を意識しながら研修に取り組んでもらうことができたと考える。

・　阻害要因

案件目標に対する阻害要因については、各単元目標の達成度については概ね高い評価ではあったが、研修員の技術レベルにばらつきがあったためか、1 年次から 3 年次を通して実習時間を長くして欲しいという意見やツールの使い方の説明の時間を長くして欲しいという意見、更に高度な内容を学びたいという意見まで、研修に求めるレベルが研修員によって様々であった。

具体的には、1 年次は「研修員との交流の時間がコースの最初に欲しい。」「「セキュリティインシデントとその対応」や「実践的防御演習」の実習パートなど、ツールを使用する技術的な演習時間や、解説時間をもっと増やして欲しい」という要望があった。特に「セキュリティインシデントとその対応」に関しては、単にコマンドの使い方を学ぶだけではなく、そのコマンドを実行する背景や意味、その他のコマンドも学びたかったという意見があった。2 年次以降、上記反省を活かしコースの最初にアイスブレイクセッションを追加し、移動時間や研修旅行の時間を削減することで実習の時間を増やす等改善を試みたが、その結果研修員同士の交流に関する要求は改善されたものの、「実習の時間を増やして欲しい」という意見はなくならなかった。

また 1 年次、2 年次には、言葉の問題によるディスカッションの停滞が複数のチームで見られていたが、3 年次はそのような問題は見られなかった。一方で、講師が説明する専門的な内容に英語でついていくのが難しいため、説明資料を事前に配布してもらいたいという意見が本邦研修中に挙がった。しかし、資料を事前に配布すると、研修員が演習会場に持参するのを忘れてしまうリスクや、一部の演習資料に解答が含まれている等の理由により、本邦研修では事前に資料を配布することはしなかった。また、配布する演習資料についてハードコピーだけでなくソフトコピー（データ）でも提供してほしいという意見があったので、研修員の理解度向上につながるよう提供方法を検討していきたい。

(2) 単元目標

本案件の各単元目標は以下の 3 点とする。

単元目標 1

最近のサイバー攻撃事例と対策を理解し、説明できる。

単元目標 2

研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。

単元目標 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。

以下に各単元目標に対する達成度を示す。

① 単元目標 1

単元目標 1 に対応したカリキュラムとして「表 3-1 単元目標 1 に対応したカリキュラム」を本邦研修で実施した。

表 3-1 単元目標 1 に対応したカリキュラム

項目	内容
単元目標 1	最近のサイバー攻撃事例と対策を理解し、説明できる。
本邦研修	
	実践的防御演習（1日目：講義） - セキュリティ技術概説 - 最新の脅威情報とその対策
	セキュリティインシデントとその対応
	国立研究開発法人情報通信研究機構（NICT）視察
	国立大学法人北陸先端科学技術大学院大学（JAIST）視察
	株式会社ラック　セキュリティオペレーションセンター視察
	日本電気株式会社　NECイノベーションワールド視察 ※1年次、2年次のみ
	討論会（ICT関連企業のソリューション紹介、討議）※1年次のみ
	JPCERT/CC活動紹介　※3年次のみ

(ア) 指標

本目標の達成度は、質問票による研修員の評価により判定するものとする。

研修員による評価では、単元目標 1「最近のサイバー攻撃事例と対策を理解し、説明できる。」について 4 段階（十分達成できた～全く達成できなかった）で評価を行った。

(イ) 達成度

質問票による研修員の自己評価結果では、3 年間を通して、2 年次の未回答 1 名を除いた

全員が達成できたあるいは、十分に達成できたと評価している。また最高評価の十分達成できたと評価した割合は全体で、1 年次が 4 名で 23.5%、2 年次が 10 名で 62.5%(未回答除く)、3 年次が 13 名で 65.0%と年次を追うごとに増加傾向にあり、カリキュラムや運営方法の改善によって単元目標達成に貢献できたといえる。
コメントでも、3 年間通して「自組織に有益な知識を得るのに良い講義だった」、「すべてが良かった」、「サイバーセキュリティのトレンドや様々なツールの使い方を理解する上で非常に役に立った」といった、高い評価が寄せられた。
このことから、計画していたカリキュラムを滞りなく実施するとともに、全員が目標を達成できたと評価する。

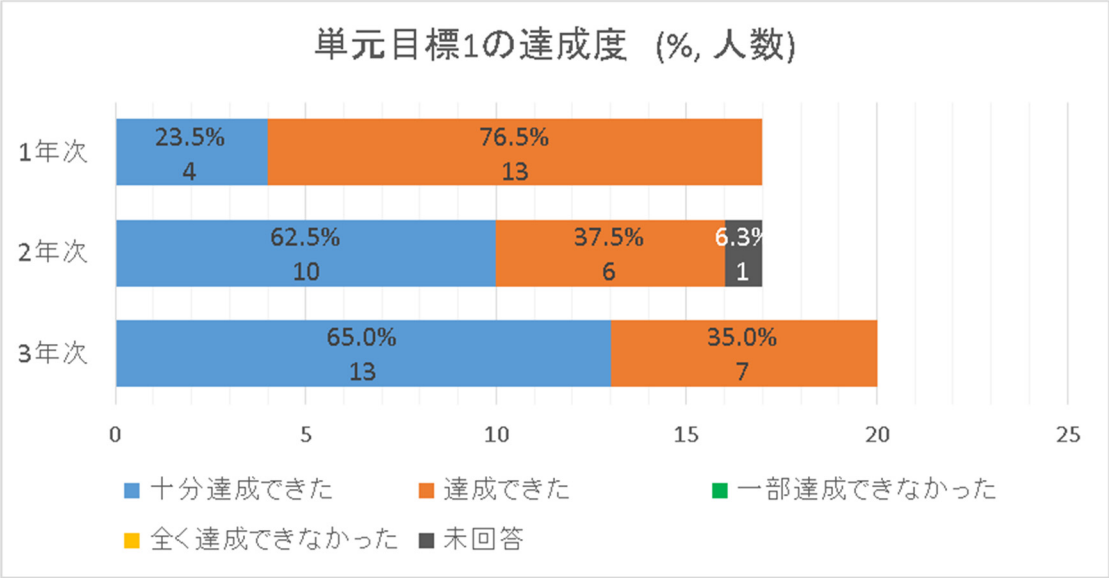


図 3-1　単元目標 1 の達成度

(ウ) 貢献要因、阻害要因

・　貢献要因

3 年間通して、研修員の講義への理解を深めるとともに、復習が行えるよう、紙資料の配布を行った。また、企業訪問として日本の先進的なセキュリティオペレーションセンターを見学し、実際の現場で起きている最新のサイバー攻撃や、防御のための取り組みを説明する場を設けた。これらの要因によって、研修員の最新のサイバー攻撃に対する理解促進に繋がったと考えられる。

・　阻害要因

研修員は全体を通して非常に満足していたと考えられるが、一方で演習プログラムのコンテンツやその時間配分に関して改善を求める意見が寄せられた。1 年次及び 2 年次には、実習を通じてさらに理解を図りたいという考えのもと、実習に掛ける時間をもっと増やして欲しいという意見が多く上がった。3 年次には、演習プログラムのコンテンツに関しては、一部の研修員から「OSINT 演習でもっと高度なツールを合わせて使いたかっ

た。」という意見が挙がった。演習中の時間配分に関しては、演習の解説について、「もう少し時間をかけてわかりやすく説明してほしかった」という意見があったため、今後の計画策定の参考としたい。

② 単元目標 2

単元目標 2 に対応したカリキュラムとして「表 3-2 単元目標 2 に対応したカリキュラム」を本邦研修で実施した。

表 3-2 単元目標 2 に対応したカリキュラム

項目	内容
単元目標２	研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。
本邦研修	
	実践的防御演習（1日目：実習） - 実力テスト - ツール使用方法説明
	実践的防御演習（2日目）
	実践的防御演習（3日目：グループディスカッション含む）
	情報連携演習
	OSINT演習 ※3年次のみ
現地フォローアップ研修	
	1/1.5 day seminar

(ア) 指標

本目標の達成度は、質問票による研修員の評価により判定するものとする。

研修員による評価では、単元目標 2「研修を通じ、インシデントハンドリングの一連の手順を理解し、その内容を他者に説明することができる。」について、4 段階（十分達成できた～全く達成できなかった）で評価を行った。

また、現地フォローアップ研修で実施した 1/1.5 day seminar における研修員のスキル定着の達成度については、セミナー参加者の満足度調査により判定するものとする。満足度調査は、4 段階（十分達成できた～全く達成できなかった）で評価を行った。

(イ) 達成度

本邦研修の達成度に関して、下図の通り質問票による研修員の自己評価結果では、十分達成できたと評価した割合は、1 年次が 11 名で 64.7%、2 年次が 10 名で 62.5%(未回答除く)、3 年次が 13 名で 75.0%と 3 年次にかけて増加しており、カリキュラムや運営方法の改善によって単元目標達成に貢献できたといえる。また、それ以外の評価についても、2 年次の未回答 1 名を除いた全員が達成できたと評価している。

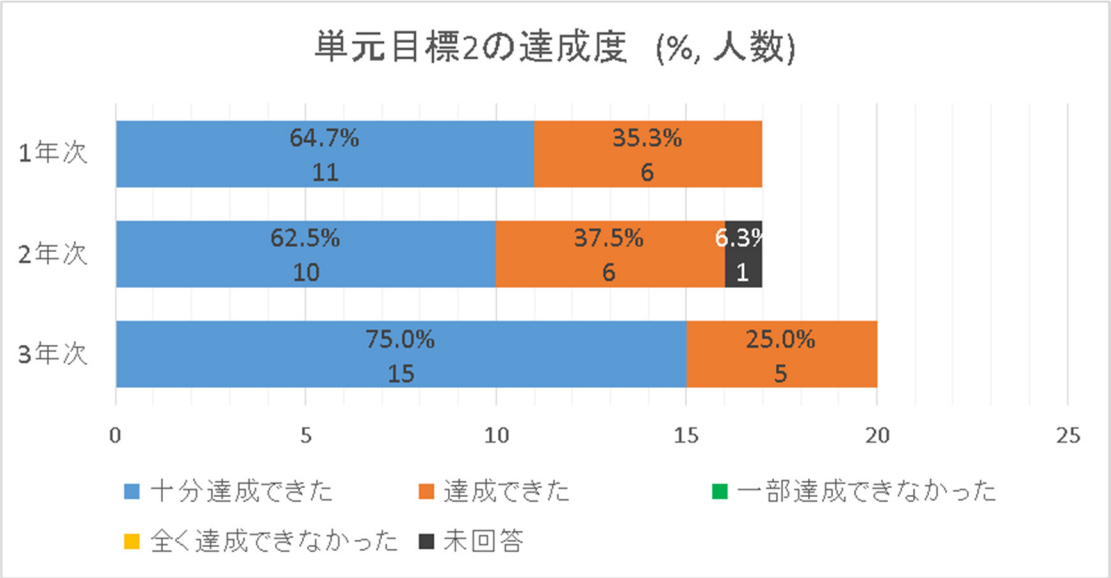


図 3-2　単元目標 2 の達成度

また現地フォローアップ活動に関しては、1/1.5 day seminar では、本邦研修で習得したスキルの定着を図るために、帰国研修員にチューターとして参加してもらった。帰国研修員の準備は、セミナー前日の数時間のみの短時間であったが 1/1.5 day seminar 中、毎年各国の研修員が積極的に参加者を支援する様子が見られた。これは現地フォローアップで訪問した国の研修員が帰国後のアクションプラン実行フェーズにおいて、自身でツール使用方法のマニュアルを作成する、セミナーを開催する等の取り組みを積極的に行っていたことにより、知識がある程度定着していたためと考えられる。
また、各年次においてセミナー参加者の大部分が、質問票で午後のセッション（演習）を理解できたと回答していることからも、研修員によるチューターとしての指導がセミナー参加者に対し適切に実施できていたと判断できる。

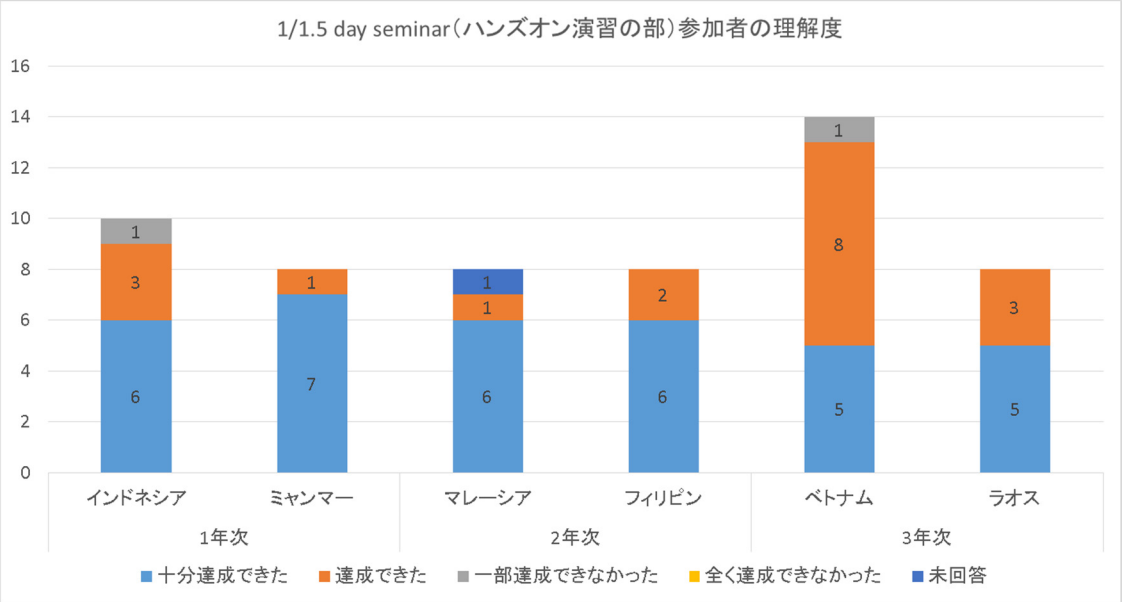


図 3-3　1 /1.5 day seminar 参加者の理解度

1/1.5 day seminar は、通常 2.5 日間かけて行う実践的防御演習を圧縮したものであったが、実践的防御演習のエッセンスを十分に伝えることができた。これは、セミナー参加者に対して、チューターの的確な支援があったためであり、支援しているチューターが本邦研修での知識を元に演習内容を正しく理解していたためといえる。これにより、本研修の研修員（チューターとして 1/1.5 day seminar に参加した帰国研修員）が、自国におけるサイバーセキュリティの向上に貢献できる人材となったと評価できる。
このことから、計画していたカリキュラムを滞りなく実施するとともに、全員が目標を達成できたと評価する。

(ウ) 貢献要因、阻害要因

・　貢献要因

3 年間通して、本邦研修での実機を使用した演習（ハンズオントレーニング）では、チューターによる献身的なサポートにより、進捗が悪いチームには積極的に声をかけ、チーム間での進捗率に大きな差が出ないよう努めた。これにより、研修員の満足度（達成感）が非常に高かったと思われる。また研修員からは、「シナリオがあり、（一つずつ課題を解決していく手法だったため）理解しやすかった。」という意見や、「インシデントハンドリングの手法をよく理解できた」という意見が寄せられ、研修員の理解も深まったと考えられる。
現地フォローアップ活動では、日本語 - 現地語の通訳を手配し、1/1.5 day seminar を行った。これにより、セミナー参加者に内容を的確に理解してもらい、また活発な質疑応答を行うことができたことが、演習を促進し高い満足度につながった一因であると考えられる。
またセミナーの最後に、参加者及び帰国研修員（チューター）に対して修了証を発行した。これにより、モチベーションの向上、上司へのアピール等の一助になったことも、

満足度を向上させる要因になったと思われる。
さらに、現地法人及びグループ会社を活用することにより、特に帰国研修員との事前連絡や、会場手配等の面において、万全な体制で現地フォローアップ活動を滞りなく実行することができた。
なお、1 年次の現地フォローアップでは、紙による記述式のアンケートを活用したところ、セミナー参加者によっては、限られた時間の中で急いでアンケートに回答したため、一部記載内容の判別が難しいケースがあった。そのため、2 年次以降は各セミナー参加者に配布した USB メモリ内にあらかじめアンケートのファイル（word 形式）を格納しておき、1/1.5 day seminar 終了後に PC を用いて当該ファイルに直接回答を記載してもらうことで、記載内容の判別ができない事態を改善した。

・　阻害要因
「図 3-2　単元目標 2 の達成度」から読み取れる様に、本邦研修において、受講生は全体を通して非常に満足していたと考えられるが、演習の細かいタイムスケジュールや進め方等に関して改善を求める要望が寄せられた。具体的には、2 年次に「（実習に）もっと時間が欲しい」、「ツールの詳しい使い方についても教えて欲しい」という意見が寄せられた。3 年次にも「演習とスキルテストの時間がもっと欲しかった。」「より高度な演習を体験してみたかった。」という意見が寄せられた。
また、現地フォローアップにおいては、1 年次の質問票に「Linux のコマンドがわからないと先に進めない」といった意見や、「（ログを解析するマイルストーンにおいて）もっと時間が欲しい」、「講義の部分で説明したツールのより詳しい使い方についても教えて欲しい」といった意見も寄せられた。
加えて、1 年次の現地フォローアップセミナー時に、参加者が持参したノート PC が有線 LAN での接続ができないものや、処理能力が非常に低く、研修の円滑な進行に支障を与えるもの、セキュリティツールが入っていることで、演習に利用するマルウェアをうまく配布できない場合もあった。また、2 年次は組織の PC を持参したことで管理者権限が必要なツールを実行できなかった。3 年次は、MacOS の PC を持参した参加者が Windows ベースのツールを上手く実行できない等の事象が発生した。

③　単元目標 3
単元目標 3 に対応したカリキュラムとして「表 3-3　単元目標 3 に対応したカリキュラム」を実施した。

表 3-3　単元目標 3 に対応したカリキュラム

項目	内容
単元目標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。
研修事前活動	
	カントリーレポート作成
本邦研修	
	カントリーレポート発表準備
	カントリーレポート発表
	アクションプラン作成
	アクションプラン発表
研修事後活動	
	アクションプラン実行
現地フォローアップ研修	
	アクションプラン報告会

(ア) 指標

本目標の達成度は、質問票による研修員の評価、および参考として、アクションプランの提出状況を指標とする。

研修員による評価では、単元目標 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。」について、4 段階（十分達成できた～全く達成できなかった）で評価を行った。

(イ) 達成度

質問票による研修員の自己評価結果では、2 年次の未回答 1 名を除いた全員が達成できたと評価している。また最高評価である十分達成できたと評価した割合は、1 年次が 7 名で 41.2%、2 年次が 6 名で 37.5%(未回答除く)、3 年次が 10 名で 47.6%(1 名が「十分達成できた」と「達成できた」を重複回答した分を含む)と 3 年次にかけて増加しており、カリキュラムや運営方法の改善によって単元目標達成に貢献できたといえる。

研修員からは、「トレーニングを実施したことでインシデントレスポンスに不可欠な体制をよく理解できた」というコメントが寄せられた。

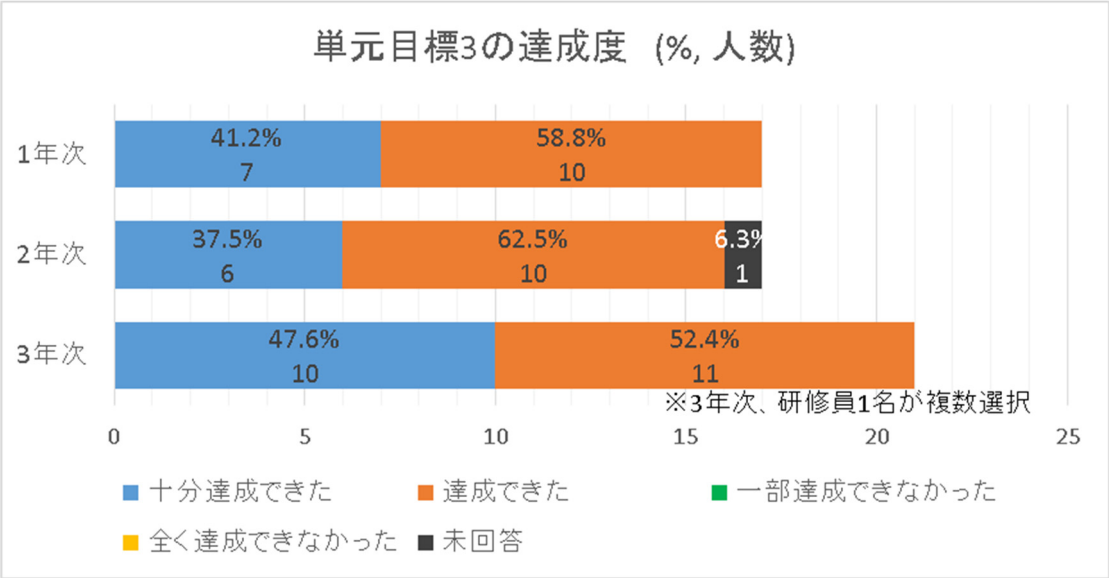


図 3-4　単元目標 3 の達成度

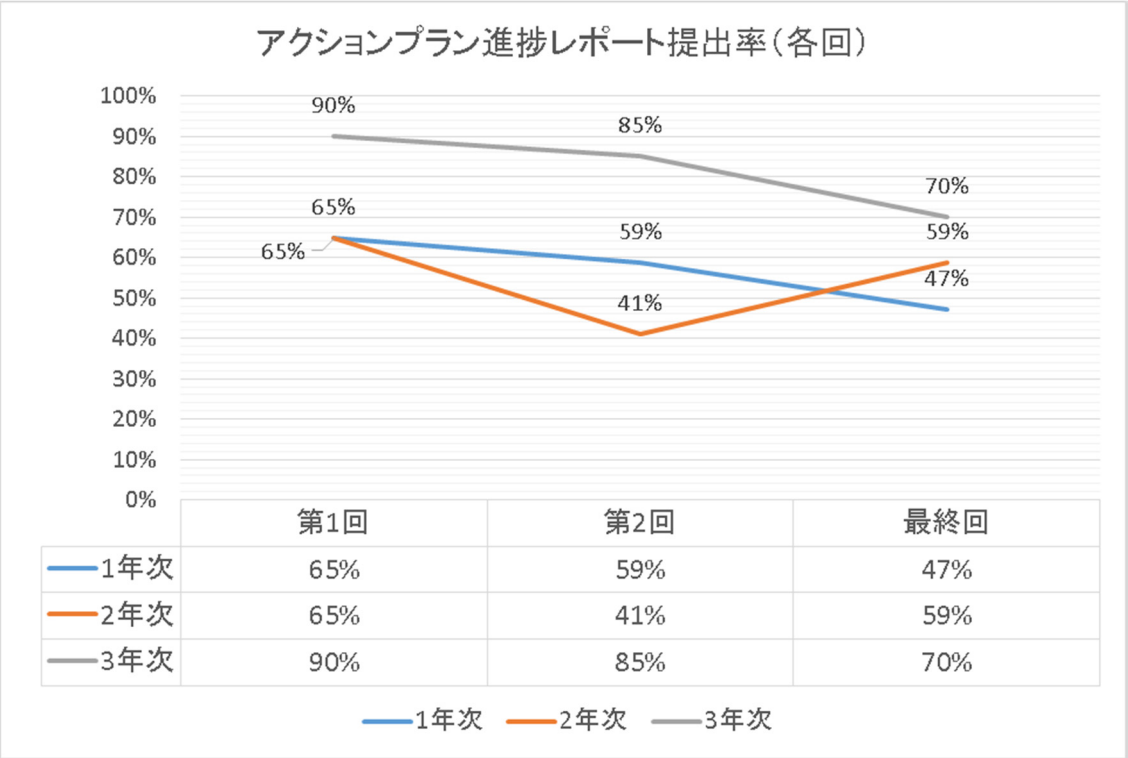
また、アクションプラン作成については、本邦研修で作成するだけではなく、自国に帰国した後のアクションプラン実行状況の確認・指導を定期的に研修員に対して実施することで、研修員が所属する組織へ自らが本邦演習にて学んだことを還元できるように促した。

その結果、1 年次の研修員の中には、既存のインシデントレスポンス手順書を見直し更新したり、他の組織の CSIRT 向けのインシデントレスポンス手順書を作成したりする活動が見られた。2 年次の研修員の中には、1 年次の研修員の活動に加えて、ツールの利用マニュアルを作成し、自組織に配布するなどの活動が見られた。3 年次の研修員の中には、本邦研修の内容の一部を活用し、研修員が提供している既存教育コンテンツに組み込んだり、本邦研修で学んだ内容を活用して大学生向けの演習を改編したりするなどの活動が見られた。

研修事後支援活動として実施したアクションプラン進捗レポートの提出率については、下図に示す通り、完成版（最終回）の提出状況に限定すると、1 年次が 47%、2 年次が 59%、3 年次が 70%となった。計 3 回の締め切り前の事前アナウンスメール（リマインドメール）の送付、締め切り直前の催促メールの送付、締め切り後の催促メールの送付を実施したが、1 年次、2 年次の提出率があまり思わしくない状況であった。

提出率が低い要因として、普段の業務が忙しくて中々アクションプランに取り組めていない、選挙等政府関連のイベント期間と重なったことにより時間を割くことが難しいというようなことが考えられる。一方で、3 年次は過去 2 回の成果を事前提示したことにより、具体的なイメージを持つことができ、多くの研修員が進捗レポートを提出してもらえたと考えられる。また、3 年次以降から研修員の上司が本活動を理解し、自国に帰国後の研修員によるアクションプラン実行に理解をしていただけるよう、上司のコンタクト情報も確認し、提出率が悪い研修員の上司にも一報を入れる様にすることで、提出率向上に努めた。

アクションプラン進捗レポート提出率の合計を見ると、6 割以上の研修員が 1 回以上は進捗レポートを提出しており、3 年次は 95%の提出率となった。



	第1回	第2回	最終回
1年次	65%	59%	47%
2年次	65%	41%	59%
3年次	90%	85%	70%

図 3-5　アクションプラン進捗レポートの提出率（各回）

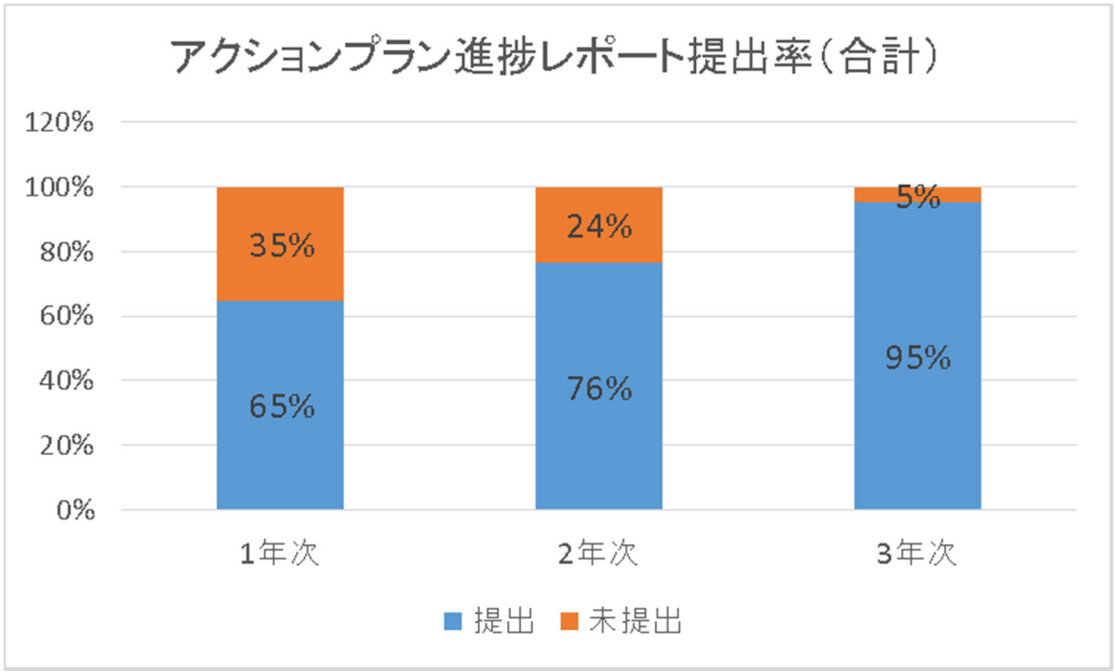


図 3-6　アクションプラン進捗レポートの提出率（合計）

また、1 年次から 3 年次まで通して実施した現地フォローアップ活動のアクションプラン報告会では、研修員がアクションプラン（完成版）について、10～15 ページの資料によるプレゼンテーションを行った。帰国した研修員は皆母国に帰った後、積極的に上司、同僚等に知識を共有する施策を実施していた。加えて、現地フォローアップ活動でのセミナー開催においても、1 年次から 3 年次まで通して実施し、帰国研修員に教える立場として参画してもらうことで、教わる立場からでは気づきにくかった細かい技術知識等を学んでもらい、知識の定着に貢献すると共に、リーダーとしての自覚を持ってもらうことができたと考える。
このことから、計画していたカリキュラムを滞りなく実施するとともに、目標を達成できたと評価する。

(ウ) 貢献要因、阻害要因

・　貢献要因

カントリーレポートの発表フォーマット及び関連質問票を GI に添付して送付したことにより、各国の状況をスムーズに把握することができた。また、本邦研修内で作成したアクションプランについても、発表フォーマットを用意することで、各研修員の発表内容について、抜けがないよう統一性を持たせることができた。結果として、ナショナル CERT など、本来の研修主旨と目的が合致した研修員は、アクションプランの実行状況が良かったといえる。
また 1 年次の要望を受け、2 年次以降、本邦研修の初日に研修員同士の親睦を深めるためのアイスブレイクセッションを導入し、お互いの趣味や最近の嬉しかったこと等々を他の研修員から聞き出し、国が違う研修員同士が和気藹々と議論ができる雰囲気づくりを心掛けた。
研修事後活動については、あらかじめ進捗レポート作成フォーマットを配布し、提出締切前のアナウンスを行うことで、研修員からの提出を促進した。
現地フォローアップ活動についても、事前にプレゼンテーションの作成要領や細かい日程表、依頼リストを共有・更新する運用を取ったことで、現地フォローアップ前の細やかな調整を完了させることができ、現地での議論の場でも活発な議論を行うことができた。

・　阻害要因

1 年次は、警察関連組織など、本来の研修主旨と目的が異なる研修員が複数名参加しており、その研修員らのアクションプラン実行状況は思わしくなかった。これは、彼らの組織の性質上、アクションプラン進捗レポート作成に求められる情報の開示に限界があったこと、また、あくまで犯罪捜査の手法としてのセキュリティ情報や技術を必要としていたためと考えられる。2 年次の本邦研修において、言葉の問題で、発表に対する質問、ディスカッションが円滑に進まない様子も見られ、「もう少し各発表者の内容を理解し、活発な意見交換を実施したい」という意見もあったが、3 年次は初日にグループ形式でのカントリーレポート発表を導入したため、初日から活発なディスカッションができ

ていた。一方で、グループ形式にしたことにより、全研修員のカントリーレポート発表を聞くことができず、「もっと他の国の状況も聞きたかった。」という意見も寄せられた。今後の改善すべき事項として検討していきたい。

(3) 達成度測定結果

(2)単元目標で述べた達成度の測定結果は以下の通りである。

① 案件目標

各単元目標の達成度測定もとに評価を行った。各単元目標の達成度測定については、以下を参照すること。

② 単元目標 1

・ 質問票による研修員の評価結果

質問票による研修員の評価結果は以下の通りである。（4 段階評価）

表 3-4 達成度（単元目標 1）

	← 十分達成できた		達成していない →	
	4	3	2	1
1 年次	23.5% (4 人)	76.5% (13 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *	62.5% (10 人)	37.5% (6 人)	0.0% (0 人)	0.0% (0 人)
3 年次	65.0% (13 人)	35.0% (7 人)	0.0% (0 人)	0.0% (0 人)

** 1 名未回答*

③ 単元目標 2

・ 質問票による研修員の評価結果

質問票による研修員の評価結果は以下の通りである。（4 段階評価）

表 3-5 達成度（単元目標 2）

	← 十分達成できた		達成していない →	
	4	3	2	1
1 年次	64.7% (11 人)	35.3% (6 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *	62.5% (10 人)	37.5% (6 人)	0.0% (0 人)	0.0% (0 人)
3 年次	75.0% (15 人)	25.0% (5 人)	0.0% (0 人)	0.0% (0 人)

** 1 名未回答*

・　現地フォローアップ活動

1/1.5 day seminar 実施時は、帰国研修員がメインでチューター対応を行った。なお、質問票を活用したセミナー参加者の満足度調査結果は以下の通りである。（4 段階評価）

1 年次のインドネシアでのセミナーの理解度（午後）で 2（一部のコンテンツを理解できなかった）と回答した参加者が 1 名いた。理由に関しては、コーヒーブレイクのところで解説する Java script のコードを解析してマルウェアの挙動を推測するパートにおいて、「Java script に精通していないため難しかった」と記載があった。

また、3 年次のベトナムでのセミナー理解度（午後）で 2（一部のコンテンツを理解できなかった）と回答した参加者が 1 名いた。理由に関しては、明記されていなかったが、一部の参加者は、業務等の影響で演習に集中できなかったため、講義内で説明した細かいツールの使い方や注意点を把握できずに演習に取り組んでしまったのではないかと考えられる。加えて、参加者の人数もセミナー前日になって急増したことから、チューターによる細やかなサポートが十分に得られなかったことも要因として考えられる。

表 3-6　満足度調査結果（1 年次）

1 年次	←理解できた/期待以上			理解できず/期待以下→
インドネシア	4	3	2	1
理解度（午前）	4	6	0	0
理解度（午後）	3	6	1	0
期待との差	3	7	0	0
実践的防御演習の受講意向	受講したい	受講しない		未回答
	10	0		0
1 年次	←理解できた/期待以上			理解できず/期待以下→
ミャンマー	4	3	2	1
理解度（午前）	1	7	0	0
理解度（午後）	1	7	0	0
期待との差	0	8	0	0
実践的防御演習の受講意向	受講したい	受講しない		未回答
	6	0		2

表 3-7　満足度調査結果（2 年次）

2 年次	←理解できた/期待以上			理解できず/期待以下→
マレーシア	4	3	2	1
理解度（午前）	6	1	0	0
理解度（午後）	6	1	0	0
期待との差	4	3	0	0
実践的防御演習の受講意向	受講したい	受講しない		未回答
	6	0		1

2 年次	←理解できた/期待以上			理解できず/期待以下→
フィリピン	4	3	2	1
理解度（午前）	8	0	0	0
理解度（午後）	6	2	0	0
期待との差	6	2	0	0
実践的防御演習の受講意向	受講したい	受講しない		未回答
	7	0		1

表 3-8　満足度調査結果（3 年次）

3 年次	←理解できた/期待以上			理解できず/期待以下→
ベトナム	4	3	2	1
理解度（午前）	7	7	0	0
理解度（午後）	5	8	1	0
期待との差	3	11	0	0
実践的防御演習の受講意向	受講したい	受講したくない		未回答
	11	0		3
3 年次	←理解できた/期待以上			理解できず/期待以下→
ラオス※	4	3	2	1
理解度（午前）	6	2	0	0
理解度（午後）	5	3	0	0
期待との差	4	4	0	0
実践的防御演習の受講意向	受講したい	受講したくない		未回答
	8	0		0

※1 名未回答（アンケートファイルが適切に保存されなかったと推測）

④　単元目標 3

・　質問票による研修員の評価結果

質問票による研修員の評価結果は以下の通りである。（4 段階評価）

表 3-9　達成度（単元目標 3）

	←　十分達成できた			達成していない →
	4	3	2	1
1 年次	41.2% (7 人)	58.8% (10 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *[1]	37.5% (6 人)	62.5% (10 人)	0.0% (0 人)	0.0% (0 人)

	← 十分達成できた		達成していない →	
	4	3	2	1
3 年次 *2	47.6% (10 人)	52.4% (11 人)	0.0% (0 人)	0.0% (0 人)

**1 1 名未回答*

**2 研修員 1 名が"4"と"3"を両方回答*

4. 研修案件に対する所見

(1) 研修デザイン～研修期間・プログラム構成等

事前のアンケート結果をもとに各国のセキュリティ対策レベル、各研修員の業務、知識レベルを把握し、各国のニーズ、研修員のレベルにあった対応ができるよう研修実施にあたり留意した。

実践的防御演習など各プログラムに要する時間については、日本人向けに実施している研修カリキュラムよりも長い時間を設定し、ゆっくりとしたスピードで講義・実習を行うことができるよう配慮した。また、プログラム構成について、3 年次は 1 年次、2 年次までの要望を考慮し、より実習の時間を長くできるよう配慮した。

表 4-1　研修期間は適切だったか

	長い	適切	短い
1 年次	11.8% (2 人)	23.5% (4 人)	64.7% (11 人)
2 年次 *	6.7% (1 人)	86.7% (13 人)	6.7% (1 人)
3 年次	20.0% (4 人)	55.0% (11 人)	25.0% (5 人)

** 2 名未回答*

また、質問票には 1 年次から「期間が短い。もっとスキルテストやハンズオンテストの時間を長くして欲しかった。」、「もっと高度な APT 攻撃の演習を追加し、コースの期間を長くした方が、研修員全体がより深く理解できる。」といったコメントが寄せられたため、可能な限り演習時間を増やす構成に変更した。

2 週間という研修期間のうち、1 年次と 2 年次は半分を貴機構の研修施設で、半分を弊社の施設や外部見学とした。3 年次は、初日、最終日 1 日前、最終日は貴機構の研修施設で、その他は弊社の施設と外部見学で研修を実施した。

プログラム実施時間に関しては、1 年次、2 年次は 9 時から 17 時（または 17 時半）までであったことと、貴機構の東京センターからの移動時間を考慮すると、一日の拘束時間が少し長かった。そのため、3 年次は 9 時 30 分から 16 時 30 分（もしくは 17 時）までとし、2 年次に寄せられた「一日の拘束時間（9 時から 17 時）が少し長い」という意見を元に、プログラムの前後 30 分を短縮した。

3 年次の評価会では、貴機構の研修施設から弊社の演習会場までのバス移動をなくし、ムスリムの方のお祈り場所と食事の確保のため、可能であれば貴機構の施設で演習を実施して欲しいという意見もあった。

3 年次は、昨年度まで実施していた日本文化研修プログラムの浅草ツアーを廃止し、その時間を OSINT 演習や JPCERT/CC の活動紹介に充てたが、それでもなおハンズオン演習の時間を確保して欲しいという意見が少数ではあったが寄せられた。

加えて、講義による概要説明ののちに、実習によるハンズオントレーニング、企業訪問や研究施設訪問により、実際の運用現場の見学を行うことで、研修員の知識理解が円滑に進むよう構成に留意した。
前述の、各単元目標の達成度からも構成は適切であったと評価するが、実施時間、実施場所については、準備や運用面での実現可能性を考慮しながら改善検討を行っていきたい。

(2) 研修内容（コンテンツ）～研修プログラム内容・研修教材等
研修内容については、インシデントレスポンス能力向上のために必要となる要素を整理し、セキュリティ技術概要～最新のセキュリティ事例と対策、及び実習によるインシデントハンドリングの一連の流れを体験し、自国に戻ったのちに業務に活かすことができるよう留意した。
研修内容について、質問票による回答は以下の通りであった。

表 4-2　本研修において研修参加者の経験から学ぶことができたか

	←　できた			できなかった　→
	4	3	2	1
1 年次	47.1% (8 人)	47.1% (8 人)	5.9% (1 人)	0.0% (0 人)
2 年次 *	13.3% (2 人)	80.0% (12 人)	6.7% (1 人)	0.0% (0 人)
3 年次	50.0% (10 人)	45.0% (9 人)	0.0% (0 人)	5.0% (1 人)

** 2 名未回答*

上記の通り、「本研修において研修参加者の経験から学ぶことができたか」という問いに対し、1 年次はカンボジアの研修員 1 名が「あまり出来なかった」と回答した。コメント欄には「もっとトピックに対して積極的なディスカッションをすべきだった。」と記載があった。1 年次は一部の演習チームにおいて、語学力、技術知識の不足から議論が活性化されないチームもあった。チューターが積極的に介入することで次年度以降改善を図った。
2 年次にもカンボジアの研修員 1 名があまりできなかったと回答し、3 年次には、イラクの研修員 1 名が全く出来なかったと回答した。3 年次研修員のコメント欄には、「もっと他の研修員と意見交換したかった。」といった内容が記載されていた。1 年次の改善事項として、2 年次以降は研修員同士の親睦を深めるためのアイスブレイクセッションを実施し、会話しやすい雰囲気作りに留意したが、個人差があったと考えられる。

表 4-3　視察や実習など直接的な経験を得る機会が十分あったか

	←　十分あった			なかった　→
	4	3	2	1
1 年次	47.1% (8 人)	52.9% (9 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *	33.3% (5 人)	66.7% (10 人)	0.0% (0 人)	0.0% (0 人)
3 年次	65.0% (13 人)	30.0% (6 人)	5.0% (1 人)	0.0% (0 人)

** 2 名未回答*

上記の通り、「視察や実習など直接的な経験を得る機会が十分あったか」という問いに対し、3 年次にイラクの研修員 1 名のみがあまり出来なかったと回答したが、明確なコメントは記載されていなかった。

表 4-4　討議やワークショップなど、主体的に参加する機会が十分あったか

	←　十分あった			なかった　→
	4	3	2	1
1 年次 *[1]	50.0% (8 人)	50.0% (8 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *[2]	26.7% (4 人)	73.3% (11 人)	0.0% (0 人)	0.0% (0 人)
3 年次 *[3]	61.9% (13 人)	33.3% (7 人)	4.8% (1 人)	0.0% (0 人)

**[1] 1 名未回答*

**[2] 2 名未回答*

**[3] 研修員 1 名が"2"と"3"を複数回答*

上記の通り、「討議やワークショップなど、主体的に参加する機会が十分あったか」という問いに対し、3 年次にイラクの研修員 1 名が"2"と"3"を複数回答した。理由としては、「たくさんの研修カリキュラムがあり、ほとんどの演習で質問をする十分な時間がなかった」と記載していた。グループワークでの演習を進める上で、英語でのコミュニケーションが必須であるが、そのコミュニケーションが十分に行われずに、十分に理解できないまま他の研修員のペースで進んでしまったことが原因と考えられる。研修中も当研修員はアジア訛りの英語にかなり苦戦している様子が見受けられた。

表 4-5　講義の質は高く、理解しやすかったか

	←　良かった			良くなかった　→
	4	3	2	1
1 年次	82.4% (14 人)	17.6% (3 人)	0.0% (0 人)	0.0% (0 人)
2 年次 *	46.7% (7 人)	53.3% (8 人)	0.0% (0 人)	0.0% (0 人)
3 年次	70.0% (14 人)	30.0% (6 人)	0.0% (0 人)	0.0% (0 人)

** 2 名未回答*

表 4-6　テキストや研修教材は満足するものだったか

	←　満足した			満足していない　→
	4	3	2	1
1 年次	52.9% (9 人)	41.2% (7 人)	5.9% (1 人)	0.0% (0 人)
2 年次 *	50.0% (8 人)	43.8% (7 人)	6.3% (1 人)	0.0% (0 人)
3 年次	85.0% (17 人)	15.0% (3 人)	0.0% (0 人)	0.0% (0 人)

** 2 名未回答*

上記の通り、「テキストや研修教材は満足するものだったか」という問いに対し、1 年次にミャンマーの研修員 1 名があまり満足出来ないと回答した。明確なコメントは記載されていなかったが、持ち帰りできない資料などがあったことが原因と推測される。

全体の質問票には、「各国のサイバーセキュリティの状況についてもっと他国の人と議論したかった」「深く理解するために、もっと（チーム内で）議論をする時間が欲しかった。」といったコメントが寄せられた。

各カリキュラムの評価について、JICA の質問票及び NEC のアンケート結果に基づき以下に述べる。

本邦研修で有益と感じたカリキュラムについて、1 年次は「実践的防御演習」（16 名）、「情報連携演習」（9 名）、「セキュリティインシデントとその対応」（7 名）が上位 3 項目だった。2 年次も同様に「実践的防御演習」（12 名）、「情報連携演習」（11 名）、「セキュリティインシデントとその対応」（6 名）が上位となった。3 年次は、「セキュリティインシデントとその対応」が最も多くの研修員が有益と回答した（15 名）。続いて「情報連携演習」（14 名）、「JAIST&NICT ツアー」（14 名）、「実践的防御演習」（13 名）が上位となった。

選択の理由として、「たくさんの新しいことを知った。自身の業務にすぐに適用でき

る。」、「有用なオープンソースのツールを知ることができた。」といったコメントが寄せられた。自身の業務との関連性の強さ、および有用なフリーのツールの存在やその使い方を新たに知ることができた点が上記の結果につながったと考えられる。

表 4-7　有益と感じたカリキュラム（複数回答）

年次	講義内容	回答数
1 年次	実践的防御演習	16
	情報連携演習	9
	セキュリティインシデントとその対応	7
	NICT&JAIST ツアー	5
	最新の脅威情報とその対策	5
	セキュリティ技術概説	3
	企業研修（LAC）	3
	金沢ツアー	3
	浅草ツアー	2
	NEC イノベーションワールド研修	1
2 年次	実践的防御演習(ツール説明)	12
	実践的防御演習(Hands-on)	12
	情報連携演習	11
	セキュリティインシデントとその対応	6
	実践的防御演習(解説)	5
	実践的防御演習(講義)	4
	NICT&JAIST ツアー	4
	NEC イノベーションワールド研修	3
	企業研修(LAC)	2
	浅草ツアー	2
3 年次	セキュリティインシデントとその対応	15
	NICT&JAIST ツアー	14
	情報連携演習	14
	実践的防御演習（ツール説明）	13
	実践的防御演習（Hands-on）	12
	OSINT 演習	9
	実践的防御演習（講義）	9
	実践的防御演習（解説）	7

年次	講義内容	回答数
	日本文化理解研修（金沢）	6
	JPCERT/CC 活動紹介	6

本邦研修のカリキュラムについて、1 年次、2 年次は特定のカリキュラムに対して有益でないという意見が集中することは無く、「自分（の業務）には必要がない」、「すでに知っている内容である」、「すべて良い経験・知識になった」等のコメントがあった。しかし、3 年次は JPCERT/CC 活動紹介に対して、「JPCERT/CC 活動の概要は、様々なカンファレンスにて出ているため、すでに知っている内容である」、「もっと技術的な内容を求めていたが、内容が初心者向けで一般的であった。」という意見が挙がった。これは自国の組織内で CSIRT がある程度の規模を持ち、関係組織との連携を含めてすでに機能している国の研修員からのコメントであったが、これから CSIRT を設立し、拡大していく国の研修員にとっては、JPCERT/CC の活動紹介は有意義であったと考えられる。そのため、今後プログラムの内容を検討する上では、参加する研修員の国の状況等を鑑みた上で判断する必要がある。これらのことから、周知されている内容を含むカリキュラムに対して改善を求める声があったものの、コンテンツの内容を否定するものではないことがうかがえる。応募時に回答いただく事前調査を活用し、研修員の役割やレベルを把握し、研修員の技術レベル、ニーズに合わせた内容になるよう考慮したい。

表 4-8　JPCERT/CC 活動紹介に対するコメント（抜粋）

Our training is especially for technical detail. Not for policy I think. JPCERT' presentation is very informative for us. But, I'd like to request from JPCERT to give technical lectures and exercises rather than overview.
Actually this subject is okay but the content is too general when compare with JAIST or NICT.

自組織（自国）の教育プログラムに導入したい研修コンテンツについて、以下に述べる。

3 年間を通して最も回答が多かったのは「実践的防御演習」で、その他「セキュリティインシデントとその対応」、「情報連携演習」等、ハンズオン演習のあるカリキュラムが選ばれる傾向にある。

表 4-9　自組織（自国）の教育プログラムに導入したい研修コンテンツ（複数回答可）

年次	講義内容	回答数
1 年次	実践的防御演習	13
	セキュリティインシデントとその対応	11
	情報連携演習	10
	最新の脅威情報とその対策	6

年次	講義内容	回答数
	セキュリティ技術概説	6
	企業研修（LAC）	6
	NICT&JAIST ツアー	-
	金沢ツアー	-
	浅草ツアー	-
	NEC イノベーションワールド研修	-
2 年次	実践的防御演習(Hands-on)	15
	実践的防御演習(ツール説明)	14
	実践的防御演習(解説)	12
	情報連携演習	11
	実践的防御演習(講義)	7
	NICT&JAIST ツアー	5
	企業研修(LAC)	5
	セキュリティインシデントとその対応	4
	NEC イノベーションワールド研修	4
	浅草ツアー	2
3 年次	セキュリティインシデントとその対応	15
	情報連携演習	15
	実践的防御演習（ツール説明）	15
	実践的防御演習（Hands-on）	15
	実践的防御演習（講義）	14
	実践的防御演習（解説）	14
	OSINT 演習	13
	NICT&JAIST ツアー	9
	JPCERT/CC 活動紹介	5
	日本文化理解研修（金沢）	4

本邦研修にて、日本文化への理解を深めるために、浅草、金沢の見学を日程に含めた。見学コースは以下の通りである。

浅草：浅草文化観光センター→雷門→仲見世通り→浅草寺、浅草神社→二天門
（東京シティガイドクラブの英語ガイドを活用）
金沢：金沢駅観光案内所→ひがし茶屋街→兼六園→金沢城公園（1 年次）
（全行程にガイドによる同行あり）

尾山神社→金沢城公園→兼六園→金沢駅（2 年次）
（全行程にガイドによる同行あり）
ホテル→金沢城公園→兼六園→ホテル（3 年次）

この研修について、「日本の社会的・文化的背景を理解できたか」という問いの結果を「表 4-10　日本の社会的・文化的背景を理解できたか？」に示す。

表 4-10　日本の社会的・文化的背景を理解できたか？

	←　十分できた			できなかった　→
	4	3	2	1
1 年次	47.1% (8 人)	47.1% (8 人)	5.9% (1 人)	0.0% (0 人)
2 年次 *	50.0% (8 人)	43.8% (7 人)	6.3% (1 人)	0.0% (0 人)
3 年次	50.0% (10 人)	40.0% (8 人)	10.0% (2 人)	0.0% (0 人)

** 2 名未回答*

印象に残った日本人の特徴や日本の特性について、「表 4-11　日本滞在中に強く印象に残った日本人の特徴や日本の特性」に結果を示す。
「日本人は親切で、他国の人を互いに敬う」、「街が清潔/きれいであった」といったコメントが多く寄せられたほか、「日本の電車（公共交通機関）は素晴らしい」というコメントや、「日本人はルールを守る」といったものもあった。
また、「表 4-7　有益と感じたカリキュラム（複数回答）」で浅草・金沢ツアーが有益だったという回答があり、今後も日本文化理解のための研修は有益であると考える。

表 4-11　日本滞在中に強く印象に残った日本人の特徴や日本の特性

日本人の特徴や日本の特性	1 年次	2 年次	3 年次
親切	13	10	19
時間に正確	14	10	15
規律を守る	9	10	12
勤労・勤勉	14	13	18
礼儀正しい	14	14	18
物静かである	8	5	8
働きすぎである	2	0	2
細部までこだわる	12	10	11
文化と歴史が素晴らしい	11	11	14
食事がおいしい	11	8	13
清潔・きれい	16	15	19

日本人の特徴や日本の特性	1 年次	2 年次	3 年次
治安が良い	15	14	19
交通渋滞が激しい	3	1	0
自然豊か	5	8	12
その他(Handsome and gorgeous people)	0	0	1

研修コンテンツに対する評価は、研修員ごとにさまざまであったが、概ね好評であったといえる。一方で、3 年間通して「実習の時間を多くしてほしい」という要望があったため、次年度以降の計画時の参考にしていきたい。その他、事前の発表テンプレートの送付、使用するツール等の情報の展開、配布資料の事前展開や配布資料の形式に関する研修員からの要望等についても、改善すべき事項として考慮していきたい。

(3) 研修の効果を高める工夫

講義による概要説明ののちに、実習によるハンズオントレーニングを行う、また、企業研修等により実際の運用を見学頂くなど、研修員の知識理解が円滑に進むようプログラム構成に留意した。

実習においては、研修員の理解を促進するためチューターを配置し、実機操作での不明点、ディスカッション実施時の躓き等を早期に把握し、研修が円滑に進むよう留意した。また、ツールを使ったハンズオンテストの解説の際に研修員から解説を実施してもらうことで、演習への取り組む姿勢に対する自主性や、教えることを前提として深く理解してもらうことの促進を図った。

また現地フォローアップ活動では、帰国研修員に 1/ 1.5 day seminar のチューターを担当させることで、本邦研修で獲得したスキルの定着を図った。

1 年次について、インドネシアの帰国研修員は、本邦研修の際は特に目立つ積極性はなかったが、1 day seminar の場では、率先してセミナー参加者の支援をするなど、著しい行動変容が見られた。また、ミャンマーの帰国研修員は、研修カリキュラムの作成委員や、インターンシップ受入れ責任者の立場の者であったため、本邦研修の内容を、ミャンマーの既存の枠組み（研修センターでの研修や、インターンシップ）に反映し、効果的に展開していた。

2 年次については、マレーシアの帰国研修員 3 名が、セミナー前日のチュータートレーニングにて 1 day seminar の内容を理解し、セミナー当日は、各所属組織の参加者に対して丁寧に現地語で説明を実施していた。気心の知れた同僚に対して遠慮なく質問できる環境を与えることで高い理解度と満足度を得ることができた。フィリピンの帰国研修員は、1 名だけであったが責任感をもって、1.5 day seminar 前日のチュータートレーニングから積極的に質問をしていた。セミナー当日においても 2 チーム（4 名/1 チーム）の参加者の様子を逐次観察し、進捗が思わしくないチームを中心に支援していた。元々職場においてリーダー的職務に配置されており、参加者からも積極的な質問がされていた。また、参加者の中でもツールの使用方法を熟知し理解が早いものが、同チームのメンバー

に対して積極的に情報展開し、チューターの様な働きをしていたため、研修員によるサポートが 1 名であっても円滑に演習を進めることができた。
3 年次については、ベトナムの帰国研修員 1 名は、本邦研修時から群を抜いて技術スキルが秀でていたこともあり、セミナー前日のチュータートレーニングにて 1.5 day seminar の内容をスムーズに理解し、セミナー当日は、各所属組織の参加者に対して丁寧に現地語で説明を実施していた。気心の知れた同僚に対して、リーダーとして質問応答のみならず、参加者に考えさせるように質問を投げかける様子が見られた。
ラオスの帰国研修員 3 名は、一部ツールの使い方を忘れている様子も見られ、1.5 day seminar 前日のチュータートレーニングに時間がかかったが、積極的に質問し理解を深めていた。セミナー当日においても 3 チーム（3 名/1 チーム）の参加者の様子を逐次観察し、進捗が思わしくないチームを中心に支援していた。英語でのコミュニケーションが難しい参加者に対して、現地語でのサポートを積極的に実施したことで、参加者の理解も深まったものと考えられる。

(4) 研修対象の選定

それぞれ 2016、2017、2018 年度の本課題別研修の参加実績状況を「表 4-12 課題別研修の割当国と参加実績」に示す。

表 4-12 課題別研修の割当国と参加実績

	1 年次 (7 ヶ国 15 名)	2 年次 (7 ヶ国 17 名)	3 年次 (11 ヶ国 20 名)	合計
カンボジア	3	3	1	**7**
インドネシア	3	0	3	**6**
ラオス	4	3	3	**10**
マレーシア	0	3	3	**6**
フィリピン	1	1	1	**3**
ベトナム	4	3	1	**8**
タイ	0	3	2	**5**
ミャンマー	2	1	3	**6**
イラン	-	-	1	**1**
イラク	-	-	1	**1**
ジンバブエ	-	-	1	**1**
合計	**17**	**17**	**20**	**54**

・ 参加資格要件

➢ 対象機関

各国のナショナル CERT、情報セキュリティを所管する官庁または部局

➢ 対象人材

インシデントハンドリングを行うことが想定されている者（管理者と技術者のセット

で申し込むこと）

上記の参加資格要件をもとに、GI（案）を作成した。

「表 4-13　課題別研修対象機関の参加実績」に、本課題別研修の参加者 11 ヶ国 54 名について、各機関の参加実績の内訳を示す。

表 4-13　課題別研修対象機関の参加実績

国名 － 組織名	1 年次	2 年次	3 年次	合計
カンボジア	**3**	**3**	**1**	**7**
ICT Security Department Ministry of Posts and Telecommunication	1	1	1	3
Dept. of E-government, Ministry of Posts and Telecommunications	1	0	0	1
Software & Content, Ministry of Posts and Telecommunications	0	1	0	1
National Information Infrastructure, Ministry of Posts and Telecommunications	1	0	0	1
National Institute of Posts, Telecoms & ICT, Ministry of Posts and Telecommunication	0	1	0	1
インドネシア	**3**	**0**	**3**	**6**
Ministry of Communication and Information Technology	2	0	0	2
Id-SirtII/CC (Indonesia Security Incident Response Team on Internet Infrastructure)	1	0	0	1
National Cyber & Crypto Agency	0	0	3	3
ラオス	**4**	**3**	**3**	**10**
Lao Computer Emergency Response Team　(LaoCERT) Ministry of Post & Telecommunications	4	3	3	10
マレーシア	**0**	**3**	**3**	**6**
MyCERT, Cyber Security Malaysia	0	1	2	3
National Cyber Security Agency, National Security Council	0	1	0	1
Malaysian Communication & Multimedia Commission	0	1	1	2
フィリピン	**1**	**1**	**1**	**3**
Philippine National Police	1	0	0	1
Cybersecurity Bureau, Department of Information and Communications Technology (DICT)	0	1	1	2
ベトナム	**4**	**3**	**1**	**8**
Department of Cyber Security, Ministry of Public Security	3	0	0	3
Information Technology Department, Ministry of Public Security	0	1	0	1
Vietnam Computer Emergency Response Teams (VNCERT)	1	1	0	2

国名 － 組織名	1 年次	2 年次	3 年次	合計
National Cyber Security Center, Authority of Information Security	0	1	1	2
タイ	**0**	**3**	**2**	**5**
Electronic Transactions Development Agency	0	1	1	2
Computer and Communication Services Division National Science and Technology Development Agency (NSTDA)	0	1	1	2
Engineering and Operation Dept. Electronic Government Agency(EGA)	0	1	0	1
ミャンマー	**2**	**1**	**3**	**6**
Myanmar Computer Emergency Response Team (mmCERT) , Ministry of Transport and Communications	1	1	0	2
Communication Technology & Engineering, Ministry of Transport and Communications	1	0	0	1
National Cyber Security Center, Information Technology and Cyber Security Department	0	0	2	2
e-Government Department, Information Technology and Cyber Security Department	0	0	1	1
イラン	**-**	**-**	**1**	**1**
Security Lab, Information and Communication Technology	-	-	1	1
イラク	**-**	**-**	**1**	**1**
Responsible for network monitoring, International internet gateway, Al Salam State Company	-	-	1	1
ジンバブエ	**-**	**-**	**1**	**1**
e-Enabled & Cyber-based services, Office of the President	-	-	1	1
合計	**17**	**17**	**20**	**54**

・　現地フォローアップ活動の選定　2 ヶ国

それぞれの年のレポート提出状況、各国の情勢（渡航時のリスク）などを考慮し、貴機構と協議の上、現地フォローアップ国を選定した。レポート提出率、アクションプラン実行状況などを評価し、6 ヶ国訪問した。

表 4-14　現地フォローアップ対象国

年次	対象国
1 年次	インドネシア
	ミャンマー
2 年次	マレーシア

	フィリピン
3 年次	ラオス
	ベトナム

(5) 研修運営体制

① 研修実施機関

研修の特性を考慮し、適切な講師、チューターを選定・配置することにより円滑な研修実施に努めた。

② 研修監理員

事前の打ち合わせ実施により、研修カリキュラムを考慮した研修監理員の配置を実現していただいた。グループごとの見学研修等では研修監理員を常に複数人配置していただくことにより円滑な研修実施を実現できた。

実践的防御演習などチューターが個別にアドバイスする必要がある演習などについても、研修監理員を 2 名配置いただくことにより、研修員の躓きを早期に把握・対処できるとより円滑な研修が実現できたと感じた。

(6) 事前活動・事後活動

① 事前活動

GI に添付した関連質問票を活用し各国のセキュリティ対策状況、セキュリティ関係組織だけでなく、研修員個人のスキル、業務経験を把握できるよう質問項目検討に当たり考慮した。事前に担当業務及び使用経験のあるツール類を把握できたことは、演習時のグループ分け、演習サポートの実施に当たり大変有益であった。

また、GI 送付時、課題として指定したカントリーレポートについては、資料作成フォーマットとともに、サンプルレポートも事前作成し送付したことにより、適切なレベル・内容のレポートを受領することができた。

② 事後活動

・ アクションプランの作成

本邦研修終了後、研修最終日に研修員が作成したアクションプランをベースとして、帰国後に研修員所属組織で議論した結果をもとに、アクションプランの改善及びその実行状況についてメール等により遠隔指導した。

・ 現地フォローアップ活動

帰国後のアクションプラン実行状況、現地で発生しているセキュリティインシデント等の課題など状況把握、次年度以降の研修改善に必要な情報の収集を目的として、下表に示す日程にてフォローアップのための現地訪問を実施した。訪問先各国において、アクションプラン報告会、職場訪問、現地セミナー等を実施し、各国の現状把握に努めた。

アクションプラン報告会では、研修員による 10～15 ページの資料によるプレゼンテーションを実施してもらい、帰国後の活動状況、活動実施に当たっての問題点などについて

説明を受けた。
セミナーでは、本邦研修で習得したスキルの定着、および各国での技術展開を促進するため、帰国研修員に事前にチューターを担当してもらい、参加者である同僚を指導した。また現地語及び英語と日本語の通訳者を配置することにより、セミナー参加者が講義内容を理解しやすいよう配慮した。

表 4-15　現地フォローアップ日程（1 年次）

日程		曜日	JICA 筬　正雄 統括	NEC 矢野　由紀子 総括／研修計画	NEC 榎本　敦之 セキュリティ調査	NEC 澤田　昭浩 （技術スタッフ）
7月	30	日	移動（東京→インドネシア）			
	31	月	・在ジャカルタ日本大使館訪問			・演習環境 セットアップ
			・現地JICA事務所訪問			
8月	1	火	・内部会議 ・チュートートレーニング ・通訳との事前打ち合わせ			
	2	水	・フォローアップサマリ プレゼンテーション ・移動 （インドネシア→東京）	・フォローアップサマリプレゼンテーション		
	3	木		・1-day seminar（ワークショップ） ・移動（インドネシア→東京）		
8月	27	日	移動（東京→ミャンマー）			
	28	月	・内部会議 ・日本大使館訪問 ・現地JICA事務所訪問			
	29	火	・フォローアップサマリプレゼンテーション ・チュートートレーニング			
	30	水	・1-day seminar（ワークショップ）			
	31	木	移動（ミャンマー→東京）			

表 4-16　現地フォローアップ日程（2 年次）

日程		曜日	NEC 矢野　由紀子	NEC 佐藤　和代	NEC 澤田　昭浩	NEC 鈴木　康太
			総括／研修計画	セキュリティ調査	（技術スタッフ）	（技術スタッフ）
8月	26	日	移動（東京→マレーシア）			
	27	月	・内部会議 ・通訳との事前打ち合わせ ・現地JICA事務所訪問 ・演習環境セットアップ			
	28	火	・フォローアップサマリプレゼンテーション ・チュータートレーニング			
	29	水	・1-day seminar（ワークショップ）			
	30	木	・Cyber Security Malaysia訪問			
	31	金	移動（マレーシア→東京）		マレーシア滞在	
9月	1	土			移動（マレーシア→フィリピン）	
	2	日			フィリピン滞在	
	3	月	移動（東京→フィリピン）			
	4	火	・フォローアップサマリプレゼンテーション ・チュータートレーニング ・通訳との事前打ち合わせ			
	5	水	・内部会議 ・現地JICA事務所訪問 ・在ﾏﾆﾗ日本大使館訪問			
	6	木	・演習環境セットアップ			
	7	金	・1.5-day seminar（ワークショップ）			
	8	土	移動（フィリピン→東京）			

表 4-17　現地フォローアップ日程（3 年次）

日程		曜日	JICA 相原　祐太 統括	NEC 矢野　由紀子 総括／研修計画	NEC 佐藤　和代 セキュリティ調査	NEC 澤田　昭浩 （技術スタッフ）	NEC 鈴木　康太 （技術スタッフ）
8月	5	月	移動（東京→ハノイ）				
	6	火	・内部会議 ・通訳との事前打ち合わせ				
	7	水	・フォローアップサマリプレゼンテーション ・チュータトレーニング ・演習環境セットアップ				
	8	木	・1.5-day seminar（ワークショップ）				
	9	金	・在ハノイ日本大使館訪問 ・現地JICA事務所訪問				
	10	土	移動（ハノイ→東京）				
	19	月		移動（東京→ヴィエンチャン）			
	20	火		・現地JICA事務所訪問 ・内部会議 ・通訳との事前打ち合わせ ・演習環境セットアップ			
	21	水		・フォローアップサマリプレゼンテーション ・チュータトレーニング			
	22	木		・1.5-day seminar（ワークショップ）			
	23	金		・LANIC及びLaoCERT訪問 ・在ラオス日本大使館訪問			
	24	土		移動（ヴィエンチャン→東京）			

5. 次年度へ向けた改善点及び提案

(1) 評価会及び反省会における指摘事項と改善結果

評価会、反省会等における指摘事項、及び貴機構との反省会での議論を踏まえ実施した改善結果・対策案を下表に年次別に纏める。

表 5-1　研修関連での指摘事項と改善計画(1 年次)

改善要望・検討すべき事項	検討・対策結果
実践的防御演習等の演習概要が、募集要項（GI）を読んだ際に分かるように資料を追加すること。	募集要項（GI）に、実践的防御演習の演習概要および使用するツールについて説明した資料を作成し、添付した。
実践的防御演習のチーム編成について、参加国単位で実施すべきか。	参加国単位でのチーム編成を実施するには、各国 3～4 名程度の人数が必要であるが、国ごとに参加人数が均等でないため実現は困難である。他国からの参加者との交流時間を確保することも考慮し、チーム間の技術レベルが偏らないような国混合のチーム編成とした。
他国からの参加者ともっと話をする時間が欲しいという意見があった。改善を検討すること。	チーム編成を国混合で組むことにより、ディスカッション演習等を通して他国の取り組みを話し合うことができるようにカリキュラムを構成した。
ディスカッションをより活発に行えるような工夫をすること。	研修初日に、アイスブレイク、軽食付きディスカッションの時間を設け、気軽な雰囲気の中で意見交換できるようにカリキュラムを構成した。
研修員にとって、余裕のある研修スケジュールとなるように改善すること。	研修スケジュールについて、研修員の負担を考慮し、朝の開始時間を遅らせることによって一日の拘束時間を短くした。
研修で配布する資料の管理を改善すること。	研修資料をひとまとめに管理できるように紙ファイルを配布し、すべての資料を綴じられるような提供方法に変更した。
本邦研修最終課題資料（アクションプランフォーマット）の事前配布をすること。	研修初日から最終課題を意識して取組むことができるように、アクションプラン作成のための説明資料とフォーマット資料を事前に送付した。

改善要望・検討すべき事項	検討・対策結果
演習時間を増やすこと。 ツール使用方法を詳しく説明すること。	講義時間を削減し、ハンズオン演習の時間を増やすことができるようにカリキュラムを構成した。特に実践的防御演習では、ツール説明のための独立した時間を設け、シナリオベースの演習実施前にツールの操作を実習する時間を確保できるように変更した。

表 5-2　研修関連での指摘事項と改善計画(2 年次)

改善要望・検討すべき事項	検討・対策結果
SOC 視察の際に技術的なことを学びたいという意見があった。改善を検討すること。	SOC は運用方法や詳細な技術情報を非公開としている場合が多いため、視察の際に研修員が技術的に学びたい項目を質疑応答形式で確認できるような構成とした。
インシデントハンドリングに係る演習のみではなく、環境構築実習も研修に構成できるか検討すること。	都内日本文化理解研修、会社訪問等視察先の削減などを実施したが、3 年次カリキュラム検討の結果、OSINT など他演習実施を優先し、環境構築実習の導入については見送った。
本邦研修でアクションプランを作成する際に、会場の通信環境が悪く、フォーマットのダウンロードに時間を要した。時間短縮のために運用方法を改善すること。	レポートのフォーマットを来日後再度事前に提供することで、会場でダウンロードさせる手間を省略させ、研修員が事前にアクションプラン作成に取り組めるよう配慮した。
カントリーレポートやアクションプラン発表の際に、それぞれの発表内容についてディスカッションの時間の導入を検討すること。	カントリーレポートについては、全体を三つに分けたグループ内での発表とすることで一人当たりの持ち時間を増やし、且つ質疑応答やディスカッションを自由に行いやすい場となるように発表形式を変更した。初日にこのような雰囲気作りをすることができたため、最終日のアクションプラン発表では研修員が自発的に質疑を行い、なかなか発言できない研修員に対しても意見を求める等、積極的にディスカッションを行う姿勢が見て取れた。

表 5-3　研修関連での指摘事項と改善計画(3 年次)

改善要望・検討すべき事項	検討・対策結果
JPCERT/CC 活動紹介について、技術的な話題の追加、もしくは研修自体の削除を検討すること。	JPCERT/CC 活動紹介について、研修員からは技術的な話題を追加してほしいという意見があった。一方で、体制や人材管理等、組織の運用面での話もしてほしいという意見もあった。そのため、次年度カリキュラム検討時、講義時間、講義内容など検討の上、実施可否を決定する。
OSINT 演習について、Kali Linux にインストールされている高度なツールを用いたハンズオン演習の導入を検討すること。	OSINT 演習におけるより高度なツールを用いたハンズオン演習の追加、セキュリティインシデントとその対応におけるコマンドやツールの使用目的の明確化の二点について、どちらも演習内容の修正にて対応できると考えられる。しかし、今年度は研修員間の技術レベルの差異が顕著であり、高度なハンズオン演習を追加すると一部の研修員の理解が追いつかないままになる可能性があり、また詳細な説明に時間を割くとハンズオン演習のボリュームが減り、一部の研修員にとっては物足りなくなる可能性がある。研修員のスキルレベルを考慮しつつ、演習内容の難易度調整を行う。
セキュリティインシデントとその対応について、コマンドやツールの使用目的が不明確だという意見があった。コマンドやツールの必要性をより詳細に説明するように改善すること。	
カントリーレポートの発表について、各グループ内の発表で得た気づきを全体で共有することでディスカッションの機会を増やすように改善すること。	参加人数なども考慮しながら、グループ発表後、研修員全体での共有・ディスカッション時間を設けることができるか検討する。
研修時間を確保するため、アクションプラン作成の時間の削減を検討すること。	アクションプラン発表及びディスカッションの時間確保のため、アクションプラン作成の時間を削減する。
アクションプラン発表について、質疑応答が途中で遮られないように一人当たりの持ち時間の調整を検討すること。	参加人数なども考慮し、発表・質疑応答が適切に実施できるよう次年度カリキュラム検討時に考慮する。
研修教材の使用制限がアクションプラン実施の阻害要因となっている可能性があるため、改善すること。	帰国後、各国において教育実施する際有効活用できるよう、使用制限の見直しを検討する。
ディスカッションの時間を増やすため、講義終了後、又は翌日の講義開始前に 15 分程度の振り返り時間を設けることを検討する	定着度を高め、他研修員とのディスカッション時間を増やす観点からも次年度カリキュラム検討時に考慮する。

改善要望・検討すべき事項	検討・対策結果
こと。	
演習シナリオに関する資料を除き、研修員が予習できるよう事前に配布することを検討すること。	演習実施内容の理解を促進するため、演習シナリオに関する資料を除き、事前配布により研修員に予習してきてもらう。
演習の内容やインストラクションについて、翻訳資料のチェック体制を提示すること。	講義で使用する英語資料について、ネイティブによるチェックを継続実施するなど、適切な記載となるよう留意する。

・ 本邦研修に追加して欲しい研修カリキュラム
- フォレンジック
- マルウェア解析
- ネットワークセキュリティ
- 日本のセキュリティ関連政策（1 年次）
- CERT 見学（1 年次評価会）
- インシデントハンドリング（導入レベル）（2 年次）
- サイバードリルのような研修科目（2 年次）
- 認定ホワイトハッカー資格のような研修科目（2 年次）
- レッドチーム（攻撃)、ブルーチーム（防御）に分かれての演習（3 年次）
- ハッキング方法とその対策（3 年次）
- 高度な標的側攻撃の検知と対処（3 年次）
- ソーシャルメディアサイトの防御方法（3 年次）
- Web サーバのセキュリティ（3 年次）
- メールサーバのセキュリティ（3 年次）
- SOC（セキュリティオペレーションセンター）（3 年次）

・ 現地フォローアップ活動に追加してほしい研修項目
- ランサムウェア
- APT
- フォレンジック

(2) 次年度 GI に反映させるべき点

① 対象機関

対象機関については、「政府機関や重要インフラに対するサイバー攻撃に対応している機関」と補足記載することにより、適切な組織に GI が配布され警察関係組織など想定外からの応募が発生しないよう留意する。具体的には以下の機関に GI を配布することが望ましいと思われる。

表 5-4　来年度の GI 配布（対象候補）

No.	Country	Organization
1	Cambodia	Ministry of Post and Telecommunications
2	Indonesia	National Cyber & Crypt Agency
3	Malaysia	CyberSecurity Malaysia Ministry of Science, Technology & Innovation
		Malaysian National Security Council
		Malaysian Communications and Multimedia Commission Ministry of Communications and Multimedia
4	Myanmar	Myanmar Computer Emergency Response Team (mmCERT), Ministry of Transport and Communications
		Communication Technology & Engineering, Ministry of Transport and Communications
		National Cyber Security Center, Information Technology and Cyber Security Department
		e-Government Department, Information Technology and Cyber Security Department
5	Philippines	Department of Information and Communications Technology
6	Vietnam	Authority of Information Security Ministry of Information and Communications
		Vietnam Computer Emergency Response Team
7	East Timor	National Communications Authority
8	Bangladesh	Bangladesh e-GOV CIRT Bangladesh Computer Emergency Response Team Ministry of Posts, Telecommunications and Information Technology
9	Nepal	Information Security Response Team Nepal Department of Information Technology
10	Palestine	Ministry of Telecommunications and Information Technology
11	Zimbabwe	Ministry of ICT and Courier Service
		e-Enabled & Cyber-based Services, Office of the President
12	Botswana	Ministry of Transport and Communications
13	Lesotho	Ministry of Communications, Science and Technology
14	Ukraine	The State Service of Special Communications and Information Protection of Ukraine

② 対象人材等

対象人材の記載については、「インシデントハンドリングを行うことが想定されている者」と記載する。また、受講後に研修員から同僚に知識を共有するためには、研修員の立場が非常に重要であるため、「グループリーダー格」の応募を推奨する旨を記載する。

③ 研修目標

案件目標にて、「チームで実践的に行うインシデントハンドリングの演習を通じ、分析に必要となる要員、ツール及び各種報告要領について理解し、」と実践的防御演習の特性が分かるよう記載する。

④　研修内容等

実践的防御演習の演習概要が応募者に伝わるよう GI 内に記載する。

演習にて使用するツールについて GI の ANNEX 内に記載し、事前に学習すべき事項が分かるようにする。

以　上

課題別研修 サイバー攻撃防御演習 1年次アクションプラン実績とコメント

No	国名	所属組織、ポジション	活動実績	指導概要
1	Indonesia	Digital Forensic Analyst, Directorat of Information Security, Ministry of Communication and Information Technology of Indonesia	・ガバメントSOC立ち上げ支援 ・自組織内のインシデントレスポンスドキュメントのレビュー ・運用手順書 (Standard Operation Procedure)の策定	・海外の標準ドキュメント、ガイドライン、ベストプラクティスなども参考にしているとのことで、NISTやCMUなどの参考ドキュメントを紹介 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf http://www.sei.cmu.edu/reports/04tr015.pdf ・また自組織に適したものとなるようよく組織間で運用フローなどを話し会うことを提言した。
2	Indonesia	Data analyst staff, Directorate of Information Security, Ministry of Communication and Information Technology	・国家サイバーセキュリティ戦略の策定支援 ・ガバメントSOC立ち上げ支援 ・セキュリティ専門家の人材育成	・国家サイバーセキュリティ戦略策定のプロセスにおいて、各セクター間調整が非常に難しく、時間を要している旨報告を受けた。 ・現状をよく分析するとともに実現すべき姿を定義して、やるべき事項を整理できるとよい旨アドバイスを実施した。
3	Indonesia	Staff, Database Application Datacenter, Id-Sirtll/CC (Indonesia Security Incident Response Team on Internet Infrastructure)	・ID-SirtII/CC情報システムのリスクアセスメントの実施 ・Sandbox導入に向けた活動実施	・Id-Sirtll/CCの組織再編が行われている中、リスクアセスメントの実施とともに本邦研修にて興味をもったSandboxについて、実際にローカル環境に実装し、マルウェア検知を試みる報告がされた。上記を継続実施することにより、よりセキュアな環境が実現できるようアドバイスを実施した。
4	Cambodia	Chief of Bureau of CamCERT, ICT Security Department, Ministry of Posts and Telecommunications	（レポート提出なし）	
5	Cambodia	Deputy Director, Dept. of E-government, Ministry of Posts and Telecommunications	・電子政府用Webサーバの性能向上及びセキュリティ対策強化のための、セキュリティツールの調査実施	・サーバやメールのセキュリティ対策について、フリーツールなどでの実現方法について、アドバイスがほしいとの要望に基づき、診断、FW・IDS、AntiVirus、監視などの領域において、使用できるツールなどを紹介し、アドバイスを実施した。
6	Cambodia	Chief of Network, National Information Infrastructure, Ministry of Posts and Telecommunications	（レポート提出なし）	
7	Philippine	OIC Training & Research, Info Tech Mgt. Serv., Philippine National Police	（レポート提出なし）	
8	Vietnam	Officer, Division 1, Department of Cyber Security, Ministry of Public Security	・システム管理者向けのインシデントレスポンス演習実施 ・上級者向け、初級者向けの演習コースの作成	・初級者向け、上級者向けのトレーニングプラン策定、準備、実施、振返りの計画が提示されたが、より具体的な内容や計画を策定するようアドバイスを実施した。
9	Vietnam	Officer, Division 3, Department of Cyber Security, Ministry of Public Security	（レポート提出なし）	
10	Vietnam	Officer, Division ５, Department of Cyber Security, Ministry of Public Security	・インシデントハンドリングプロセスの改善予定 ・サイバーセキュリティトレーニングコース開催準備	・自身が推進するAction Planについて、より具体的に計画を立て、進捗を報告するようアドバイスを実施した。
11	Vietnam	Deputy Head, System Technology, Vietnam Computer Emergency Response Teams, Ministry of Information Communication	（レポート提出なし）	

No	国名	所属組織、ポジション	活動実績	指導概要
12	Myanmar	Executive Engineer, Communication Technology & Engineering, Ministry of Transport and Communications (MPT)	・同僚への情報共有会の実施 ・MPTトレーニングセンターでのサイバートレーニング実施の提言	・自組織での演習開催のため、活動が優先順位付けされ、適切にレポート報告されていた。 ・今後も組織の人材育成事業推進のリーダーとして活動していくようアドバイスを実施した。
13	Myanmar	Software Engineer, Myanmar Computer Emergency Response Team Ministry of Transport and Communications	・Cyber Crime Investigation Department(CID)向けにインシデントレスポンス演習実施 ・インシデントマネージメントガイドラインの更新と修正 ・Government Technological University (GTU)学生へのセミナ実施計画の策定	・他研修員においてもガイドラインの修正・更新については、時間を要していることを共有。 ・演習開催については、今回の経験を今後にも活かすとともに、インターネット等でも様々な情報を収集することができるため、活用するようアドバイスを実施した。
14	Laos	Head of Technical Division, Lao Computer Emergency Response Team, Ministry of Post and Telecommunications	・人材育成 ・IDS、IPS等監視システムの導入 ・インシデントハンドリング実施における官民連携強化 ・アンチウィルス対策の策定 ・サイバーセキュリティ啓発活動	・人材育成、システム開発、マルウェア対策、組織間連携など必要な分野を組織内で役割分担し、全員の状況を整理してレポート提出できている点を評価した。
15	Laos	Engineer, Lao Computer Emergency Response Team, Ministry of Posts and Telecommunications		
16	Laos	Engineer, Lao Computer Emergency Response Team, Ministry of Posts and Telecommunications		
17	Laos	Engineer, Lao Computer Emergency Response Team, Ministry of Posts and Telecommunications		

課題別研修 サイバー攻撃防御演習 2年次アクションプラン実績とコメント

No	国名	所属組織、ポジション	活動実績	指導概要
1	Myanmar	Technical Engineer, Myanmar Computer Emergency Response Team (mmCERT), Ministry of Transport and Communications	・少人数でのインシデントレスポンス演習の実施 ・少人数でのツールの使い方講座実施	・自身が計画したアクションプランの各アイテムについて、実施後の結果（同僚からのコメント等）詳細記録し、レポートすると尚よい旨をコメント送付。 ・組織に新たに迎え入れるインターンシップ生に対して、チュータ・講師として教える立場での活躍を期待する旨のコメント送付。
2	Laos	Engineer, Lao Computer Emergency Response Team (LaoCERT),Ministry of Post and Telecommunications	（レポート提出なし）	
3	Laos	Engineer, Lao Computer Emergency Response Team (LaoCERT),Ministry of Post and Telecommunications	・一般の方向けのセキュリティ啓発のためのドキュメントを作成中	・まずは、同僚や上司にトレーニングの内容を報告すべきとアドバイスを実施。 ・予算や時間の問題があるというレポートに対して、お金のかからない知識共有の方策、時間をかけずに効果的に共有するスモールスタートな施策を実施してくべきとアドバイスを実施
4	Laos	Lao Computer Emergency Response Team (LaoCERT),Ministry of Post and Telecommunications	（レポート提出なし）	
5	Vietnam	Deputy Director General, Information Technology Department, Ministry of Public Security	（レポート提出なし）	
6	Vietnam	Head of Division, Incident Coordination and Response, Vietnam Computer Emergency Response Teams (VNCERT)	（レポート提出なし）	
7	Vietnam	Official, Authority of Information Security, Ministry of Information and Communications	・少人数でのインシデントレスポンス演習の実施 ・同僚にSOCの概要について共有会実施	・帰国後にNECやKasperskyなどとの企業連携を含む新規のアクションアイテムを追記している点について、積極性があり評価するもその実現可能性や実現方法について確認するコメントを送付 ・組織内部のみならず、外部の職員に対しても日本で学んだことを共有していった方がよいとアドバイスを実施。
8	Malaysia	Senior Analyst, Cyber Security Responsive, Cyber Security Malaysia	・同僚への情報共有会議開催	・同僚（職場）へ配布する予定のハンドブックを、同僚にレビューしてもらい、そのフィードバックを元にさらに更新すると良いとコメント送付。
9	Malaysia	Assistant Director, National Cyber Security Agency, National Security Council (NSC)	・同僚へのツールの使い方講座準備中 ・自国での対規模サイバーセキュリティ演習の準備中	・X-Mayaと呼ばれるマレーシア内でのサイバーセキュリティトレーニングをどのように更新していくのか、日本で学んだ内容を元に参考にして欲しい旨のコメント送付。 ・元々存在していた、運用手順のレビューをアクションプランから除外した理由に関して確認。 ・他の業務と並行しながら充実したトレーニングを実施できたことに対する評価のコメントを送付。 ・今後は同僚だけでなく重要インフラなどの外部機関との知識共有も視野に進めてほしい旨のコメント送付。
10	Malaysia	Assistant Director, Network Surveillance Dept., Digital Surveillance Div. Malaysian Communication & Multimedia Commission	・同僚へのツールの使い方講座実施 ・ツールの使い方マニュアル作成し、配布 ・インシデントハンドリングのガイドライン作成	・既存業務を遂行しながら時間を確保し、セキュリティツールの使い方講座を実施し、そのフィードバックをもとにマニュアルおよびハンドブックを更新した点について評価。 ・引き続きチーム内での展開を推奨するとともに外部機関との定期的な連携ができたら良い旨のコメント送付。

No	国名	所属組織、ポジション	活動実績	指導概要
11	Cambodia	Head of Office, Software & Content, Ministry of Posts and Telecommunication	・インシデントレスポンス演習の実施 ・ツールの使い方講座実施	・自組織のチーム力向上という難し目標ではあるが、ひとつずつ課題を克服し、チーム全体の活性化を促すようコメント送付。 ・まずはドラフト版でもいいのでスタートしてみてくださいとのアドバイスを実施。 ・Burp Suiteや OWASP ZAPなどの脆弱性診断ツールについて紹介し習得するようコメント送付
12	Cambodia	Official, ICT Security Department, Ministry of Posts and Telecommunication	・同僚への情報共有会議開催 ・組織内のセキュリティアセスメントを実施 ・サイバーセキュリティコンテスト準備中	・脆弱性アセスメントについて、実施している点を評価し、その手法等について、詳細の報告を依頼。 ・Angkor Warrior (CTF) を含むトレーニングや啓発活動についての業務に携わっている点について言及し、その立場を最大限に活用してアンケートなどを実施し、自組織での課題などを明確にしてほしい旨コメントを送付。
13	Cambodia	Chief Technical Support Office, National Institute of Posts, Telecoms & ICT, Ministry of Posts and Telecommunication	・インシデントレスポンス演習の準備中 ・セキュリティチーム立ち上げ準備中	・セキュリティチーム立ち上げという高い目標を実施するにあたり、上司などの承認も必要となる点から、まずはその目的を明確にすすめることが近道である旨アドバイスを実施。 ・また、チーム立ち上げ後、そのチームリーダとしての活躍を期待する旨をコメントを送付。
14	Thailand	Head of Information Security Management Section (ISM), Computer and Communication Services Division, NSTDA (the National Science and Technology Development Agency)	・ツールの使い方講座準備中	・セキュリティトレーニングコースを一人で構築するのは困難（時間を要する）ため、チームで協力し分担しながら実現するようコメント送付
15	Thailand	Asst. Director, Information Security Division, Electronic Transactions Development Agency(ETDA)	・同僚への情報共有会議開催 ・インシデントレスポンス演習の準備中	・Cyber Security awareness training構想について評価。これが自組織およびタイでの若者のスキル向上に貢献できることを期待する旨のコメント送付 ・国をまたいだセキュリティ情報共有について、JICAトレーニングで知り合った仲間とうまく連携していって欲しいとのコメント送付
16	Thailand	System Engineer, Engineering and Operation Dept. Electronic Government Agency(EGA)	・自組織の現状確認実施（リスクアセスメント）	・自組織にどんなセキュリティツールが導入されているか確認することは非常に重要である旨のコメント送付。 ・同時に、インシデントハンドリングの手順書なども見直し、JICAで学んだものを生かして欲しい旨のコメント送付。
17	Philippine	Information systems Analyst III, Department of Information and Communications Technology (DICT)	・インシデントレスポンス演習の実施（組織内外向け） ・ツールの使い方講座実施	・同僚や上司を巻き込み、セキュリティトレーニングコース作成したことに対して評価するコメント送付。 ・CSIRT構築において、以下参考URLを展開。同時に、ENISAなどの関連ドキュメントも参照するようアドバイスを実施。 http://www.nca.gr.jp/activity/build-wg-document.html ・日常業務の中で時間を確保し自身および組織としてのスキルレベル向上を継続し、組織の垣根を超えた活動を期待するコメントを送付。

課題別研修 サイバー攻撃防御演習 3年次アクションプラン実績とコメント

No	国名	所属組織、ポジション	活動実績	指導概要
―	ALL	―	―	・サイバーセキュリティの演習教材として下記ENISA等のサイト情報を紹介 https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material ・自己スキル向上に向けたネットワークの問題の参考情報を紹介 https://www.malware-traffic-analysis.net/
1	Cambodia	Officer, ICT Security Department, Ministry of Posts and Telecommunication(2015)	・CTF勉強会準備中 ・カンファレンス開催支援 ・既存のインシデントレスポンスドキュメント確認予定	・CTFの準備のために、日本で使用したCTFdやLimesurveyなどのOSSを紹介 https://github.com/CTFd/CTFd ・「インシデント対応と脅威ハンティング」について、日本で学んだことを講師として同僚に説明してほしい旨アドバイス実施。 ・サイバーセキュリティガイドラインのドキュメントを定期的に更新する必要性についてアドバイス実施。
2	Indonesia	Incident Response Team, Operational & Network Security Dept., National Cyber & Crypto Agency(2012)	・OSINT演習の準備中 ・インシデントレスポンス演習の準備中	・学習管理システムの一例として、日本の演習で使用したCTFdやLimesurveyなどのOSSを紹介 https://github.com/CTFd/CTFd ・JAISTにて紹介のあったCyTrONEについては、まずはトレーニング環境ではなくデモとして利用（動作確認）した方がよい旨アドバイス実施 ・スモールスタートとして小規模での同僚へのセミナーを実施した方がよい旨アドバイス実施
3	Indonesia	Staff, National Cyber Security Contact Center, National Cyber & Crypto Agency(2017)	・インシデントレスポンス演習のデモ実施 ・情報共有演習のデモ実施 ・ガイドラインの改版済み。関係者レビュー中	・組織を新設する場合のセキュリティ文書統合の重要性についてアドバイス実施。 ・新たに作成したサイバーセキュリティガイドラインのドキュメントを定期的に更新する必要性についてアドバイス実施。 ・日本で学んだことに基づいてインシデントレスポンスで使うツールのデモを行ったことに対する、評価のコメント送付。
4	Indonesia	Staff, Directorate Response & Recovery for Government, National Cyber & Crypto Agency(2018)	・インシデント対応のガイドライン作成予定	・単独でアクションプランを進めることは難しいため、まずは少人数のチームを同僚と結成し、支援を仰いでみたほうが良い旨、アドバイス実施。
5	Iran	Head, Security Lab, Information and Communication Technology(2008)	・報告書配布済み ・インシデントレスポンス対策チーム設立中	・同僚をアクションプラン実行に巻き込んで実施していたことに対して、評価するコメント送付。 ・事前にセキュリティインシデントの予防・予防計画を実施することも重要だという旨、アドバイス実施。
6	Iraq	Responsible for network monitoring, International internet gateway, AL Salam State Company(2018)	（レポート提出なし）	
7	Laos	Technical Staff, Lao Computer Emergency Response Team, Ministry of Post & Telecommunications(2014)	・ツール紹介実施 ・インシデントレスポンス手順書作成完了	・インシデントレスポンス手順書を作ったことに対して、評価するコメント送付。 ・また組織内でレビューしてもらう必要性に関して、アドバイス実施。 ・定期的にレビューすることの必要性に関してもアドバイス実施。
8	Laos	Deputy Division Director, Lao National Internet Center, Ministry of Post & Telecommunications(2017)	・インシデントレスポンス演習実施 （一部現地語翻訳） ・ツール使い方トレーニング実施	・現地の言語に翻訳して、同僚に演習コンテンツの一部を共有したことに対する評価コメント送付。 ・セミナー開催について、一度にたくさんの人を招待できないのであれば、まずは小規模でのセミナーを実施した方がよい旨アドバイスを実施。もしくは、作成したツール使用方法などの文書を関係者に配布し、フィードバックをもらいながら資料を更新していく方法でもよい旨アドバイスを実施。 ・日本で学んだことに基づいてインシデントレスポンス演習を行ったことに対する、評価のコメント送付。
9	Laos	Technical Staff, Lao Computer Emergency Response Team, Ministry of Post & Telecommunications(2014)	・OSINT演習実施 ・インシデントレスポンス演習準備中	・日本で学んだことに基づいてOSINT演習の資料を作成し、演習を行ったことに対する、評価のコメント送付。 ・個人のスキル開発に関しては、攻撃を防ぐために「攻撃者の行動」を学ぶことの重要性についてアドバイス実施。

No	国名	所属組織、ポジション	活動実績	指導概要
10	Malaysia	Senior Executive, MyCERT, CyberSecurity Malaysia(2007)	・演習準備中 ・マガジン/冊子作成中 ・同僚向け情報共有会実施	・内部組織向けに発行しているセキュリティ記事の中に、日本で学んだことを含めたほうが良いという旨アドバイス実施。
11	Malaysia	Senior Analyst, MyCERT, CyberSecurity Malaysia(2016)	・現地JICA事務所に活動報告実施 ・手順書更新中 ・インシデントレスポンス演習準備中	・一度にたくさんの人を招待できないのであれば、まずは小規模でのセミナーを実施した方がよい旨アドバイスを実施。もしくは、作成した演習資料、ツール説明資料などの文書を関係者に配布した上で、フィードバックコメントをもらい、資料を更新していく方法でもよい旨アドバイスを送付。
12	Malaysia	Deputy Director, Digital Forensic Department, Malaysian Communications & Multimedia Commission (MCMC)	・インシデントレスポンス演習準備中 ・政府機関への講演準備中	・Kali Linuxの機能に基づき、攻撃者の観点からインシデントレスポンスの手順を同僚に説明したことに対する、評価のコメントを送付。 ・（当研修員が）法執行機関への講演にて、講演者になり日本で学んだことに基づいた内容を共有することへの期待のコメントを送付。
13	Philippine	CM Technologist III, Cybersecurity Bureau, DICT(2016)	・攻撃手法理解演習実施 ・情報共有演習準備中	・日本で学んだことを踏まえてインシデントレスポンス手順書を修正したことに対する、評価のコメント送付。 ・同僚を巻き込んでトレーニングコースを作成したことに対する、評価のコメント送付。
14	Vietnam	Official, National Cyber Security Center, Authority of Information Security(2017)	・自組織の演習プログラム/基盤の見直し実施 ・研修員との情報共有基盤(Slack)作成	・日本で学んだことを基にベトナムで開催しているトレーニングコースをアップデートしたことに対する、評価のコメントを送付。 ・今年のJICA研修生と情報共有するためのプラットフォームを作成し、情報共有していることに対する、評価のコメントを送付。
15	Zimbabwe	Head of Unit, e-Enabled & Cyber-based services, Office of the President(2018)	・小規模CERTの立ち上げ準備中 （予算取り、人材採用） ・インシデントレスポンス演習準備中	・組織のトップを巻き込んで組織を変えようとしていることに対する、評価のコメントを送付。 ・小さなCERTを設立するために、セキュリティツールとネットワークに精通した人々を採用する活動をしていることに対する、評価のコメントを送付。
16	Thailand	Security Engineer, Office of Information Security, Electronic Transactions Development Agency (Public Organization)(2017)	・CERTアセスメント実施予定 ・海外でのセキュリティイベントでスピーカー予定	・海外でのカンファレンスにて、講演者になり日本で学んだことに基づいた内容を共有することへの期待のコメントを送付。 ・組織を新設する場合のセキュリティ文書統合の重要性についてアドバイス実施。
17	Thailand	Senior Engineer, Information Security Management Section, National Science and Technology Development Agency (NSTDA)(2014)	・職場上司関連部門長への研修報告 ・同僚への技術展開資料（文書、演習環境）準備中 ・職場へのセキュリティニュース配信	・日本で学んだことを上司や同僚と共有していることに対する、評価のコメントを送付。 ・日々進歩しているセキュリティ技術や脅威情報を継続的に収集し、同僚と共有することの重要性についてアドバイス実施。

No	国名	所属組織、ポジション	活動実績	指導概要
18	Myanmar	Assistant Director, National Cyber Security Center, Information Technology and Cyber Security Department	・インシデントレスポンス(手順、プロセス)演習実施 ・現地大学でのインシデントレスポンス講座実施	・日本で使用されていた演習環境を自分で再現し、知識を向上させていることに対する、評価のコメントを送付。 ・また同演習環境を活用して、現地大学生向けにトレーニングを実施したことに対する、評価のコメント送付。 ・JAISTにて紹介のあったCyTrONEについては、まずはトレーニング環境ではなくデモとして利用（動作確認）した方がよい旨アドバイスを実施。
19	Myanmar	Assistant Director, National Cyber Security Center, Information Technology and Cyber Security Department	・インシデントレスポンス演習実施	・日本で使用されていた演習環境を自分で再現し、知識を向上させていることに対する、評価のコメントを送付。 ・学習管理システムの一例として、日本の演習で使用したCTFdやLimesurveyなどのOSSを紹介 https://github.com/CTFd/CTFd
20	Myanmar	Staff Officer, e-Government Department, Information Technology and Cyber Security Department	・OSINT演習実施 ・インシデントレスポンス(ツール)演習実施	・日本で使用されていた演習環境を自分で再現し、知識を向上させていることに対する、評価のコメントを送付。

別添（詳細研修計画書）

研修詳細計画書（一年次）

JICA担当課	
課長	担当

研修コース名：　サイバー攻撃防御演習

研修コース番号：　J1604010　　受入形態：　課題別研修

研修期間：　2017/2/19　～　2017/3/4　　研修員数：　17 人

JICA国内機関担当課　JICA東京　経済基盤開発・環境課　（更新日）2017/3/3

案件担当者氏名　眞田　英子　（連絡先）

現場担当者氏名　芝　由紀子　（連絡先）

研修監理員氏名　福田　典子　（連絡先）

研修監理員氏名（単発業務）和田　美佳

日付	時刻	形態	研修内容	講師又は見学先担当者等			講師使用言語	研修場所	宿泊先	研修旅行・近距離移動行程						切符手配人数			車輌借上時乗車人数	請求先		研修員+同行CDN				★CDN単独移動	★CDN旅費			技術研修扱い施設入場料（ただし委託契約に含むものは記載対象外）		日本文化理解を目的とする拝観料（上限額2,000円/人）		福田CDN配置日数	和田CDN配置日数
				氏名(敬称略)	所属先及び職位	連絡先				・研修旅行は移動手段（列車名/便名/車輌情上（車種・台数及び出発・到着時刻））等を記載 ・近距離移動時は行程を記載						研修員	CDN	研修実施機関	車輌借上時乗車人数	JICA	受注者	交通費（近距離移動のみ）			タクシー代	交通費＋タクシー代	日当	宿泊料	金額計	人数	金額計	人数	金額計		
										移動手段	出発時刻	出発地	経由地	到着時刻	到着地							単価	人数	金額										
1/23(月)	10:00 ～ 12:00		事前打合せ					TIC SR303																										0.5	
2/19(日)			来日						TIC																										
2/20(月)	10:00 ～ 12:30		ブリーフィング				英	TIC SR	TIC																										
	13:30 ～ 14:30		研修コースオリエンテーション	眞田 英子 矢野 由紀子	JICA東京 経済基盤開発・環境課 日本電気（株）		英	TIC SR(406)																										0.5	
	15:00 ～ 16:30		カントリーレポート説明、発表準備	矢野 由紀子	日本電気（株）		英																											
2/21(火)	9:00 ～ 12:30	発表	カントリーレポート発表	矢野 由紀子	日本電気（株）		英	TIC SR(406)	TIC																										
	13:30 ～ 17:00	講義	セキュリティ技術概説	太田 浩二	トレンドマイクロ（株）		英																										1.0	
2/22(水)	9:00 ～ 17:00	講義	セキュリティインシデントとその対応	上野 宣	（株）トライコーダ		日	NEC（品川）	TIC	JICAバス(1)	8:15	TIC	⇔	8:45	NEC																		1.0	
											18:00			17:10																				
2/23(木)	9:00 ～ 11:00	見学	NECイノベーションワールド研修	佐藤 和代	日本電気（株）		英	NEC（品川）	TIC	JICAバス(ﾚ3)	8:15	TIC	⇔	8:45	NEC																				
	11:30 ～ 17:00	実習	情報連携演習	鎌田 敬介	サイバーディフェンス研究所		英				18:00			17:10																		1.0	0.5
2/24(金)	10:00 ～ 11:00	見学	企業研修（LAC）	佐藤 和代	日本電気（株）		英	LAC(永田町)	TIC	JICAバス(ﾚ1)	9:15	TIC	→	9:45	LAC																				
	11:00 ～ 13:30		移動(→浅草）、昼食								11:30	LAC	→	12:00	浅草																			
	13:30 ～ 15:30		日本文化理解研修(東京シティガイドクラブ)					浅草			15:30	浅草	→	16:00	TIC																		1.0	
	16:30 ～ 17:30		討論会	矢野 由紀子	日本電気（株）		英	TIC SR(201)																										
2/25(土)									TIC																									
2/26(日)	13:30 ～ 16:30		移動（東京→石川） 日本文化視察（兼六園、金沢城等）						金沢 (ﾎﾃﾙﾙｰﾄｲﾝ金沢駅前)	傭上バス 新幹線かがやき507 北鉄バス一日フリー券	7:50 9:20	TIC 東京	→ →	8:40 11:54	東京駅 金沢	17	1	18		18														1.0	
2/27(月)	10:00 ～ 11:00	見学	NICTツアー	矢野 由紀子	日本電気（株）		英	NICT(能美市旭台2-12)	TIC	傭上バス	9:00	ホテル	→	9:50	NICT			25																
	11:00 ～ 12:00	見学	JAISTツアー	矢野 由紀子	日本電気（株）		英	JAIST(能美市旭台1-1)			(NICT→JAISTへは徒歩移動)																							
	13:00 ～ 15:00	講義	実践的防御演習（1日目）	鎌田 敬介	サイバーディフェンス研究所		英				15:10	JAIST	→	16:00	金沢駅																		1.0	
			移動（石川→東京）							新幹線かがやき510	16:47	金沢	→	19:20	東京	17	1			18															
										JICAバス(1)	19:30	東京駅	→	20:00	TIC																			
2/28(火)	9:30 ～ 17:15	実習	実践的防御演習（2日目）	鎌田 敬介	サイバーディフェンス研究所		英	NEC（品川）	TIC	JICAバス(2)	8:45	TIC	⇔	9:15	NEC																		1.0	
											18:00			17:10																			
3/1(水)	9:30 ～ 18:00	実習	実践的防御演習（3日目）	鎌田 敬介	サイバーディフェンス研究所		英	NEC（品川）	TIC	JICAバス(1)	8:45	TIC	⇔	9:15	NEC																		1.0	
											18:00			17:10																			
3/2(木)	9:30 ～ 12:00	講義	最新の脅威情報とその対策	上野 宣	（株）トライコーダ		英	TIC SR(406)	TIC																								1.0	
	13:00 ～ 17:00	発表	アクションプラン作成	矢野 由紀子	日本電気（株）		英																											
3/3(金)	9:30 ～ 14:30	発表	アクションプラン発表	矢野 由紀子	日本電気（株）		英	TIC SR(201)	TIC																								1.0	
	15:00 ～ 16:00		評価会	眞田 英子 矢野 由紀子	JICA東京 経済基盤開発・環境課 日本電気（株）		英																											
	16:00 ～ 16:30		閉講式	眞田 英子	JICA東京 経済基盤開発・環境課		英	TIC SR(302)																										
	17:00 ～ 18:00		閉講パーティ					TIC SR(303)																										
3/4(土)																																		
																						合計										10.5	0.5

研修詳細計画書(二年次)

様式:2015年4月版(TIC)

研修コース名	サイバー攻撃防御演習
研修コース番号	J1704360
研修期間	2018/2/26 ～ 2018/3/9

受入形態	課題別研修
研修員数	17 人

JICA国内機関担当課	JICA東京 経済基盤開発・環境課		
案件担当者	亀井 千裕		
現場担当者	亀井 千里		
研修監理員 （メイン）	福田 典子	（英 語）	
研修監理員 （単発）	會澤 由華	（英 語）	

（作成日）	2018/2/19
（連絡先）	
（連絡先）	
（連絡先）	
（連絡先）	

JICA担当課	
課長	担当

日付	時刻	形態	研修内容	講師又は見学先担当者等			講師使用言語	研修場所	宿泊先	研修旅行・近距離移動行程						切符手配人数			車輌借上時乗車人数	請求先		研修員＋同行CDN				技術研修扱い 施設入場料 (ただし委託契約に含むものは記載対象外)		日本文化理解を目的とする 挨拶料 (上限額 2,000円/人)		ガイド料	★CDN単独移動	★ CDN旅費			福田CDN配置日数	★ CDN旅費			會澤CDN配置日数
				氏名(敬称略)	所属先及び職位	連絡先				・研修旅行は移動手段(列車名/便名/車輌情上(車種・台数及び出発・到着時刻))等を記載 ・近距離移動時は行程を記載						研修員	CDN	研修実施機関同行者		JICA	研修実施機関	交通費(近距離移動のみ)			タクシー代	人数	金額計	人数	金額計	金額計	交通費+タクシー代	日当	宿泊料	金額計		日当	宿泊料	金額計	
										移動手段	出発時刻	出発地	経由地	到着時刻	到着地							単価	人数	金額													
2/13(火)	16:30 ～ 18:00		（事前打ち合わせ）					TIC SR401																													0.5				
2/25(日)	～		（来日指定日）						JICA東京																																
2/26(月)	10:00 ～ 12:30	講義	ブリーフィング	JICA			英語	TIC SR403	JICA東京																																
	13:30 ～ 15:00	講義	研修コースオリエンテーション	矢野由紀子/JICA	日本電気（株）		英語	TIC SR406																													0.5				
	15:00 ～ 16:30	発表	カントリーレポート説明、発表準備	矢野由紀子	日本電気（株）		英語																																	
2/27(火)	9:00 ～ 12:30	発表	カントリーレポート発表	矢野由紀子	日本電気（株）		英語	TIC SR406	JICA東京																																
																																				1.0				
	13:30 ～ 17:00	講義	実践的防御演習（1日目） - セキュリティ技術概説 - 最新の脅威情報とその対策 実力テスト(15分間)	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語																																	
2/28(水)	10:00 ～ 11:00	見学	施設見学（LAC）	矢野由紀子	日本電気（株）		英語	LAC(千代田) 株式会社LAC: 東京都千代田区平河町2-16-1 平河町森タワー	JICA東京	JICAバス(送迎のみ)	9:15	JICA東京		9:45	株式会社LAC																									
	13:30 ～ 15:30		日本文化理解研修	矢野由紀子	日本電気（株）		英語	浅草文化観光センター前～浅草寺二天門前		JICAバス(送迎のみ)	11:20	株式会社LAC		11:50	浅草文化観光センター																							1.0				
										JICAバス(送迎のみ)	16:00	二天門前		16:30	JICA東京																									
3/1(木)	9:30 ～ 17:00	講義	セキュリティインシデントとその対応	上野 宣	（株）トライコーダ		英語	NEC（品川）: 東京都港区港南2-16-1	JICA東京	JICAバス(送迎のみ)	8:45	JICA東京		9:15	NEC																									
										JICAバス(送迎のみ)	17:15	NEC		17:45	JICA東京																							1.0				
3/2(金)	9:00 ～ 12:00		移動（東京→石川） （昼食：車内で弁当）	JICA						JICAバス	8:50	JICA東京		9:40	東京駅	17	1			18																				
	14:00 ～ 15:30	見学	NICTツアー	矢野由紀子	日本電気（株）		英語	(NICT) 北陸StarBED技術センター 石川県能美市旭台2-12	金沢ニューグランドホテル(住所)石川県金沢市南町4番1号（尾山神社正面・金沢市文化ホール前）TEL.076-233-1311	JR新幹線かがやき509号	10:24	東京駅		12:52	金沢駅																									
	15:30 ～ 17:30	見学	JAISTツアー	矢野由紀子	日本電気（株）		英語	(JAIST)北陸先端科学技術大学院大学 石川県能美市旭台1-1		傭上バス	13:10	金沢駅		14:00	(NICT) 北陸StarBED技術センター					23																			1.0				
										(NICT→JAISTは徒歩移動)																																
											17:40	(JAIST)北陸先端科学技術大学院大学		18:30	ホテル																									
3/3(土)	9:00 ～ 12:00		日本文化理解研修	矢野由紀子	日本電気（株）		英語	金沢	JICA東京	周遊バス(1日フリー乗車券)	8:50	金沢ニューグランドホテル	ひがし茶屋、兼六園、金沢城公園	12:00	金沢ニューグランドホテル																									
			(12:30～13:30 昼食)									金沢ニューグランドホテル			金沢駅																									
	13:56 ～ 16:52		移動（石川→東京）							はくたか566号	13:56	金沢駅		16:52	東京駅	17	1			18																			1.0				
	16:30 ～ 17:30									JICAバス	17:20	東京駅		18:00	JICA東京																									
3/4(日)			休息日						JICA東京																																
3/5(月)	9:30 ～ 17:00	実習	実践的防御演習（2日目）- ツール使用方法説明	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC（品川）	JICA東京	JICAバス(送迎のみ)	8:45	JICA東京		9:15	NEC																									
	～									JICAバス(送迎のみ)	17:15	NEC		17:45	JICA東京																							1.0				1.0
3/6(火)	9:30 ～ 17:00	実習	実践的防御演習（3日目）	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC（品川）	JICA東京	JICAバス(送迎のみ)	8:45	JICA東京		9:15	NEC																									
	～									JICAバス(送迎のみ)	17:15	NEC		17:45	JICA東京																							1.0				1.0
3/7(水)	9:30 ～ 11:30	実習	実践的防御演習（4日目）/達成度テスト	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC（品川）	JICA東京	JICAバス(送迎のみ)	8:45	JICA東京		9:15	NEC																									
	13:00 ～ 17:00	実習	情報連携演習	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC（品川）		JICAバス(送迎のみ)	17:15	NEC		17:45	JICA東京																							1.0				1.0
3/8(木)	9:30 ～ 11:00	見学	NECイノベーションワールド研修	矢野由紀子	日本電気（株）		英語	NEC（品川） 東京	JICA東京	JICAバス(送迎のみ)	8:45	JICA東京		9:15	NEC																									
	13:00 ～ 17:00	発表	アクションプラン作成(グループ討論会)	矢野由紀子	日本電気（株）		英語	TIC SR406		JICAバス(送迎のみ)	11:15	NEC		11:45	JICA東京																							1.0				
3/9(金)	9:30 ～ 14:30	発表	アクションプラン発表	矢野由紀子	日本電気（株）		英語	TIC SR406	JICA東京																																
	15:00 ～ 16:00		評価会	JICA																																	1.0				
	16:00 ～ 16:30		閉講式	JICA				TIC SR403																																
3/10(土)	～		（離日指定日）																																					
																						合計													10.5				3.0

研修詳細計画書（三年次）

様式:2015年4月版(TIC)

JICA担当課	
課長	担当

研修コース名	サイバー攻撃防御演習
研修コース番号	J1804211
研修期間	2019/2/17 ～ 2019/3/2

受入形態	課題別研修
研修員数	21 人

JICA国内機関担当課	JICA東京 経済基盤開発・環境課		（作成日） 2019/2/13
案件担当者	亀井 千裕		（連絡先）
現場担当者	有働 敦子		（連絡先）
研修監理員 （メイン）	會澤 由華	（英 語）	（連絡先）
研修監理員 （メイン）	水無瀬 薫	（英 語）	（連絡先）

日付	時刻	形態	研修内容	講師又は見学先担当者等			講師使用言語	研修場所	宿泊先	研修旅行・近距離移動行程						切符手配人数			車輌借上時乗車人数	請求先		研修員＋同行CDN				技術研修扱い施設入場料（ただし委託契約に含むものは記載対象外）		日本文化理解を目的とする視察料（上限額2,000円/人）		ガイド料	★會澤CDN単独移動	★會澤CDN旅費			會澤CDN配置日数	★水無瀬CDN単独移動	★水無瀬CDN旅費			水無瀬CDN配置日数
				氏名(敬称略)	所属先	連絡先				・研修旅行は移動手段（列車名/便名/車輌備上（車種・台数及び出発・到着時刻））等を記載 ・近距離移動時は行程を記載						研修員	CDN	研修実施機関同行者		JICA	研修実施機関	交通費（近距離移動のみ）			タクシー代								交通費+タクシー代	日当	宿泊料	金額計		交通費+タクシー代	日当	宿泊料	金額計	
										移動手段	出発時刻	出発地	経由地	到着時刻	到着地							単価	人数	金額		人数	金額計	人数	金額計	金額計	金額					金額				
2/7(木)	14:30 ～ 15:30		事前打ち合わせ					TIC SR408																														
2/17(日)	～		来日指定日						JICA東京																													
2/18(月)	10:00 ～ 12:30	講義	ブリーフィング	JICA			英語	TIC SR411	JICA東京																													
	13:30 ～ 15:00	講義	研修コースオリエンテーション	JICA/ 矢野由紀子	日本電気（株）		英語	TIC SR406																														
	15:00 ～ 17:00	発表	カントリーレポートディスカッション・発表	矢野由紀子	日本電気（株）		英語																															
2/19(火)	9:30 ～ 11:30	講義	OSINT演習	竹田 春樹	Planetway Japan		英語	NEC田町216 東京都港区芝四丁目14-1 第二田町ビル	JICA東京	JICAバス（レンタカー）	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	13:00 ～ 16:30	実習									16:40	NEC		17:10	JICA東京																							
2/20(水)	9:30 ～ 11:30	講義	実践的防御演習（1日目） -セキュリティ技術概説 -最新の脅威情報とその対策 実力テスト	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC田町211-212	JICA東京	JICAバス	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	13:00 ～ 16:30	実習	ツール使用方法説明								16:40	NEC		17:10	JICA東京																							
2/21(木)	9:30 ～ 11:30	実習	実践的防御演習（2日目）	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC田町211-212	JICA東京	JICAバス（レンタカー不可）	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	13:00 ～ 16:30	実習									16:40	NEC		17:10	JICA東京																							
2/22(金)	9:30 ～ 11:30	実習	実践的防御演習（3日目） （グループディスカッション含む）	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC田町211-212	JICA東京	JICAバス	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	13:00 ～ 16:30	実習									16:40	NEC		17:10	JICA東京																							
2/23(土)			休息日						JICA東京																													
2/24(日)	～		移動（東京→石川）							JICAバス（2台）	8:20	JICA東京		8:50	東京	21	2		23																				
										かがやき507号	9:20	東京		11:54	金沢	21	2			○																				
	13:30 ～		日本文化理解研修	矢野由紀子	日本電気（株）		英語	金沢	金沢	路線バス		金沢駅			金沢ニューグランドホテル（南町バス停）																			1.0				1.0
2/25(月)	10:00 ～ 11:30	見学	JAISTツアー	矢野由紀子	日本電気（株）		英語	(JAIST)北陸先端科学技術大学院大学 石川県能美市旭台1-1	JICA東京	傭上バス（大型バス）	9:00	金沢ニューグランドホテル	19k/40分＋α	9:50	JAIST	21	2	3	26	○																1.0				1.0
											11:35	JAIST	（徒歩移動）	11:40	昼食場所（石川ハイテク交流センター）																							
	13:00 ～ 15:00	見学	NICTツアー	矢野由紀子	日本電気（株）		英語	(NICT) 北陸StarBED技術センター 石川県能美市旭台2-12			12:40	昼食場所（石川ハイテク交流センター）	（徒歩移動）	12:50	NICT																							
											15:10	NICT	19k/40分＋α	16:00	金沢駅																							
										かがやき512号	16:47	金沢		19:20	東京	21	2			○																				
	15:00 ～ 18:00		移動（石川→東京）	JICA						JICAバス（2台）	19:35	東京		20:00	JICA東京	21	2		23																				
2/26(火)	9:30 ～ 12:30	実習	情報連携演習	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語	NEC田町216	JICA東京	JICAバス	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	14:00 ～ 14:50	実習	情報連携演習	鎌田 敬介	ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所		英語																															
	15:00 ～ 16:00	講義	JPCERT/CC活動紹介	内田由香子	JPCERTｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ		英語																															
	16:00 ～ 16:30		達成度テスト/アンケート								16:40	NEC		17:10	JICA東京																							
2/27(水)	9:30 ～ 11:30	講義	セキュリティインシデントとその対応	上野 宣	（株）トライコーダ		英語	NEC田町211-212	JICA東京	JICAバス	8:50	JICA東京	14k/25分＋α	9:20	NEC	21	2	2	25																	1.0				1.0
	13:00 ～ 16:30	実習									16:40	NEC		17:10	JICA東京																							
2/28(木)	9:30 ～ 11:00	見学	施設見学（LAC）	矢野由紀子	日本電気（株）		英語	（株） LAC: 東京都千代田区 平河町2-16-1 平河町森タワー	JICA東京	傭上バス	9:00	JICA東京	8k/15分＋α	9:20	LAC	21	2		23	○																1.0				1.0
	13:30 ～ 16:30	発表	アクションプラン作成	矢野由紀子	日本電気（株）		英語	TIC SR201			11:10	LAC	8k/15分＋α	11:30	JICA東京																							
3/1(金)	9:30 ～ 14:30	発表	アクションプラン発表	矢野由紀子	日本電気（株）		英語	TIC SR411	JICA東京																													
	15:00 ～ 16:00		評価会	JICA																																	
	16:00 ～ 16:30		閉講式	JICA				TIC SR406																													
	16:30 ～ 17:30		閉講パーティー	JICA				TIC SR405																													
3/2(土)	～		離日指定日																																			
																																		11.0				11.0

ジャイカ
JICA