モンゴル国
デジタル開発・イノベーション・通信省
モンゴル科学技術大学情報通信技術校

インドネシア国・モンゴル国
サイバーセキュリティ人材育成
プロジェクト（教員研修）

業務完了報告書
（モンゴル国）

2025 年 6 月

独立行政法人
国際協力機構（JICA）

株式会社日本開発サービス（JDS）

ガ平
JR
25-008

目　次

1. プロジェクトの概要 1
1.1 プロジェクト目的 1
1.2 業務期間、対象地域およびモンゴル側実施機関 1
1.3 業務従事者の従事実績および報告書・成果品等一覧 1
1.3.1 業務従事者の従事実績 1
1.3.2 報告書・成果品一覧 1
2. 投入実績と活動結果 2
2.1 投入実績 2
2.1.1 日本側の投入（本件業務は下線） 2
2.1.2 モンゴル側の投入 2
3. 成果の発現状況とプロジェクト目標の達成度 3
3.1 成果1の目標達成度 3
3.2 成果2の目標達成度 4
4. 活動結果 8
4.1 成果1に係る活動 8
4.2 成果2に係る活動 10
4.3 その他の活動 22
5. プロジェクト実施と成果に影響を及ぼした工夫または留意点 22
5.1 コミュニケーションに関する問題 22
5.2 カリキュラム設計に関する問題 23
5.3 TTT及びセミナー準備・実施上の問題 24
6. プロジェクト終了後の上位目標達成の見込みおよび提言 24

「成果物（科目以外)」(データ提出)

1 カリキュラム改訂マニュアル（ローカライズ版）
2 修士コースカリキュラム
3 CS人材育成の動向レポート
4 モンゴル国CS市場調査報告書
5 C/Pキャパシティ評価レポート
6 開発科目のKSAマッピング

図表リスト

（図）

図-1　CS Lows and Regulations 科目の Post-Test スコア 5
図-2　Advanced Web | OS Security 科目の Post-Test スコア 5
図-3　CS Governance and Auditing 科目の Post-Test スコア 6
図-4　Comprehensive Exercise: CSIRT 科目の Post-Test スコア 6
図-5　Comprehensive Exercise: SOC 科目の Post-Test スコア 7
図-6　Malware Analysis 科目の Post-Test スコア 7
図-7　2020 年版 GCI モンゴルのデータ 25
図-8　2024 年版 GCI モンゴルのデータ 25

（表）

表-1　モンゴルプロジェクト開発科目一覧 3
表-2　モンゴルプロジェクト TTT の参加者内訳 4
表-3　モンゴルプロジェクト第 1 回 CS トレンドセミナーの講演内容 8
表-4　モンゴルプロジェクト第 2 回 CS トレンドセミナーの講演内容 9
表-5　ローカライズ科目「Cybersecurity Law(s) and Regulation(s)」の詳細 12
表-6　新規開発科目「Adcanced Web Security and Operating System Security」の詳細 13
表-7　新規開発科目「Cybersecurity Governance and Auditing」の詳細 14
表-8　ローカライズ科目「Comprehensive Exercise: CSIRT」の詳細 15
表-9　ローカライズ科目「Comprehensive Exercise: SOC」の詳細 17
表-10　ローカライズ科目「Malware Analysis」の詳細 20

（写真）

写真-1　モンゴルプロジェクト第 1 回 CS トレンドセミナーの様子 9
写真-2　モンゴルプロジェクト第 2 回 CS トレンドセミナーの様子 10
写真-3　モンゴルプロジェクトカリキュラム改訂にかかるトレーニングの様子 11
写真-4　Cybersecurity Law(s) and Regulation(s)科目の TTT の様子 12
写真-5　Advanced Web and Operating System Security 科目の TTT の様子 13
写真-6　Cybersecurity Governance and Auditing 科目の TTT の様子 15
写真-7　Comprehensive Exercise: CSIRT 科目の TTT の様子 16
写真-8　Comprehensive Exercise: SOC 科目の TTT の様子 20
写真-9　Malware Analysis 科目の TTT の様子 21

略語表

略語	英語	日本語
CS	Cybersecurity	サイバーセキュリティ
CSIRT/CC	Public, Computer Security Incident Response Team	コンピューターセキュリティ・インシデント対応チーム
C/P	Counterpart	カウンターパート
MDDIC	Ministry of Digital Development, Innovation and Communications	デジタル開発・イノベーション・通信省
MUST-SICT	School of Information and Communications Technology of the Mongolian University of Science and Technology	モンゴル科学技術大学 情報通信技術校
NICT	National Institute of Information and Communications Technology	国立研究開発法人 情報通信研究機構
OSS	Open-Source Software	オープンソースソフトウェア
QCBS	Quality- and Cost- based Selection	品質とコストに基づいた選定
SecBok	Security Body of Knowledge	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もの
SICT-WG	School of Information and Communications Technology Working Group	サイバーセキュリティ学科のカリキュラム策定などを行うワーキンググループ
SOC	Security Operation Center	セキュリティ・オペレーション・センター
SOP	Standard Operating Procedure	標準作業手順書
ToR	Terms of Reference	業務仕様書
TTT	Training The Trainers	トレーナー研修
UI	University of Indonesia	インドネシア大学

1. プロジェクトの概要

1.1 プロジェクト目的

本件業務は、モンゴル国において、サイバーセキュリティ人材育成のための産学官連携ネットワークを構築し、学生、現役講師、公務員向けのサイバーセキュリティ教育プログラムを開発することにより、モンゴル国のサイバーセキュリティ教育の向上を図り、もってモンゴル国の安全なデジタル社会の推進に寄与するもの。

1.2 業務期間、対象地域およびモンゴル側実施機関

業務期間： 2023年7月～2025年6月

対象地域： ウランバートル市

モンゴル側実施機関： デジタル開発・イノベーション・通信省（Ministry of Digital Development, Innovation and Communications、以下「MDDIC」）、及びモンゴル科学技術大学情報通信技術校（Mongolian University of Science and Technology - School of Information and communication Technology、以下「MUST-SICT」）

1.3 業務従事者の従事実績および報告書・成果品等一覧

計3名の専門家を投入した。派遣実績は別添3.の「専門家派遣実績」の通りである。

1.3.1 業務従事者の従事実績

石川泰光： 業務主任者／サイバーセキュリティ技術

石田光彦： 研修計画①

Toan Nguyen Ngoc： 研修計画②

※ 石川、Toanはインドネシアプロジェクトと兼任

1.3.2 報告書・成果品一覧

(1) 報告書

報告書名	提出時期	部数等
業務計画書	契約締結後 10 日以内	和文 1 部（インドネシア業務とモンゴル業務を統合）：電子ファイル
ワークプラン	各国での現地業務開始から 1 ヵ月以内、および各年度末に改訂版	英文 2 部（インドネシア業務 1 部、モンゴル業務 1 部で分割）：電子ファイル
業務完了報告書	契約履行期間の末日	和文：インドネシアとモンゴル分それぞれ 5 部製本（計 10 部）、CD-R：2 か国分それぞれ 2 部（計 4 部） 英文：2 部（インドネシア業務 1 部、モンゴル業務 1 部で分割）：電子ファイル

(2) 技術協力作成資料

カリキュラム改訂マニュアル
修士コースカリキュラム
新規開発・及びローカライズしたカスタム科目の教材一式 （生徒用教材、講師用教材、シラバス、演習データ、受講者評価テスト）*
セミナー及び、短期講習で用いた教材、及び当日の撮影ビデオ
C/P キャパシティ評価レポート
開発科目の KSA マッピング

* カリキュラム、シラバス、生徒用教材、演習用教材、演習教材等の言語は原則、英語とする。

2. 投入実績と活動結果

2.1 投入実績

2.1.1 日本側の投入（本件業務は下線）

(1) 専門家：

チーフアドバイザー、サイバーセキュリティ／業務調整、サイバーセキュリティ技術、研修計画①、研修計画②

(2) 研修員受け入れ：

サイバーセキュリティ分野

(3) 機材供与：

研修用機材（サーバー、PC、各種ソフトウェア等）

(4) 第三国研修：

本邦大学職員、サイバーセキュリティ関連機関職員等

2.1.2 モンゴル側の投入

(1) カウンターパートの配置：

プロジェクト・ダイレクター、及び、副プロジェクト・ダイレクター（MDDIC）、プロジェクト・マネージャー（MUST-SICT）、副プロジェクト・マネージャー（MDDIC、MUST-SICT、NAoG）

(2) 執務スペースの提供：

MUST-SICTに執務室、MDDICとNAoGにデスク

(3) 案件実施のためのサービスや施設、現地経費の提供

3. 成果の発現状況とプロジェクト目標の達成度

モンゴルプロジェクトにおいては、成果1と成果2に関わる活動を実施した。以下、それら各成果におけるプロジェクト目標の達成度を、指標を基に報告する。

3.1 成果1の目標達成度

成果1：	サイバーセキュリティ人材育成の為の産学官連携ネットワークが構築される

指標1-1： 産学官連携のもと、XX回以上のセミナーやイベントが開催される

デジタル開発・イノベーション・通信省（MDDIC）の年間活動計画に従い、2024年1月25日に第1回セミナー「Cybersecurity Capability Maturity Models and Standards」を、2024年12月12日に第2回セミナー「Cybersecurity in Critical Information Infrastructure (CII)」を実施した。したがって、本件業務による本指標への貢献は最終的に2回である。

指標1-2： 産学官連携のもと、サイバーセキュリティ教材が作成される

本件業務で実施した教材開発とTTTを次の表にまとめる。なお「分類」に記した「新規」は、モンゴルプロジェクトで独自に開発したものであることを示し、「ローカライズ」はインドネシアプロジェクトで開発済みの科目教材を、モンゴル国に適した内容に改変したものであることを示す。

表-1　モンゴルプロジェクト開発科目一覧

No.	実施時期	科目名	分類	実施状況
1	2024年1月	Cybersecurity Law(s) and Regulation(s)	ローカライズ	完了
2	2024年6月	Advanced Web and Operating System Security	新規	完了
3	2024年6月	Cybersecurity Governance and Auditing	新規	完了
4	2024年12月	Comprehensive Exercise: CSIRT	ローカライズ	完了
5	2025年1月	Comprehensive Exercise: SOC	ローカライズ	完了
6	2025年2月	Malware Analysis	ローカライズ	完了

このように、合計6科目のサイバーセキュリティ教材の新規開発またはローカライズにより、本指標に貢献している。

3.2　成果2の目標達成度

成果2：	学生及び現役講師向けのサイバーセキュリティ教育プログラムが開発･提供される

前述の通り、モンゴルプロジェクトでは合計6件の新規またはローカライズによる科目開発とTTTを実施している。これを前提に、以下各指標の達成度を評価する。

指標2-1： XX名の講師が訓練される

実施した6件のTTTの参加者とその内訳を次表にまとめる。

表-2　モンゴルプロジェクトTTTの参加者内訳

No.	科目名	参加者数	参加者の内訳
1	Cybersecurity Law(s) and Regulation(s)	15	MUST：　9名 Police school：　4名 Public CIRT (CSIRT/CC)：　2名
2	Advanced Web and Operating System Security	20	MUST：　11名 MUST以外の大学：　4名 民間企業：　2名 Public CSIRT/CC：　2名 MDDIC：　1名
3	Cybersecurity Governance and Auditing	20	MUST：　9名 MUST以外の大学：　4名 Public CSIRT/CC：　3名 MDDIC：　2名 民間企業：　1名 MDDIC以外の省庁：　1名
4	Comprehensive Exercise: CSIRT	20	MUST：　10名 MUST以外の大学：　2名 Public CSIRT/CC：　4名 National CSIRT：　4名
5	Comprehensive Exercise: SOC	21	MUST：　10名 MUST以外の大学：　3名 Public CSIRT/CC：　4名 National CSIRT：　4名
6	Malware Analysis	20	MUST：　9名 MUST以外の大学：　3名 Public CSIRT/CC：　3名 National CSIRT：　3名 MNCIRT：　2名

表-2の通り、本件業務により、本指標ではこれまで「116名の講師が訓練された」となる。

指標2-2： 60%以上の講師が最終試験で60%以上の正答率を得る

次のグラフは参加者の最終テスト（事後テスト）の6件のTTTにおける正答率をグラフ化したものである。

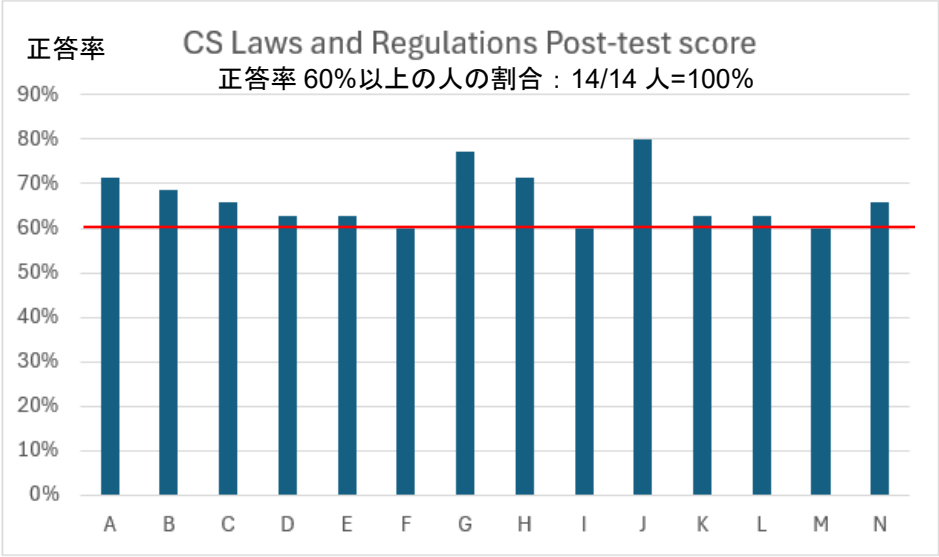


図-1　CS Lows and Regulations科目のPost-Testスコア

本科目で指標の表現を用いると「100%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。ただし本科目の事後テストでは5名が合格ラインである正答率60%を達成できず、1回の再テストを受けている。上記グラフは再テストの結果を示している。

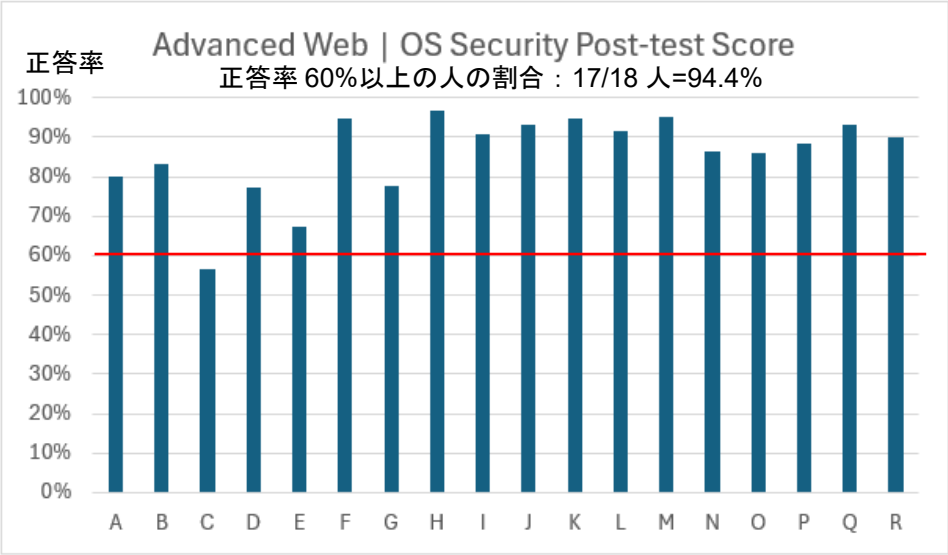


図-2　Advanced Web | OS Security科目のPost-Testスコア

本科目で指標の表現を用いると「94.4%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。

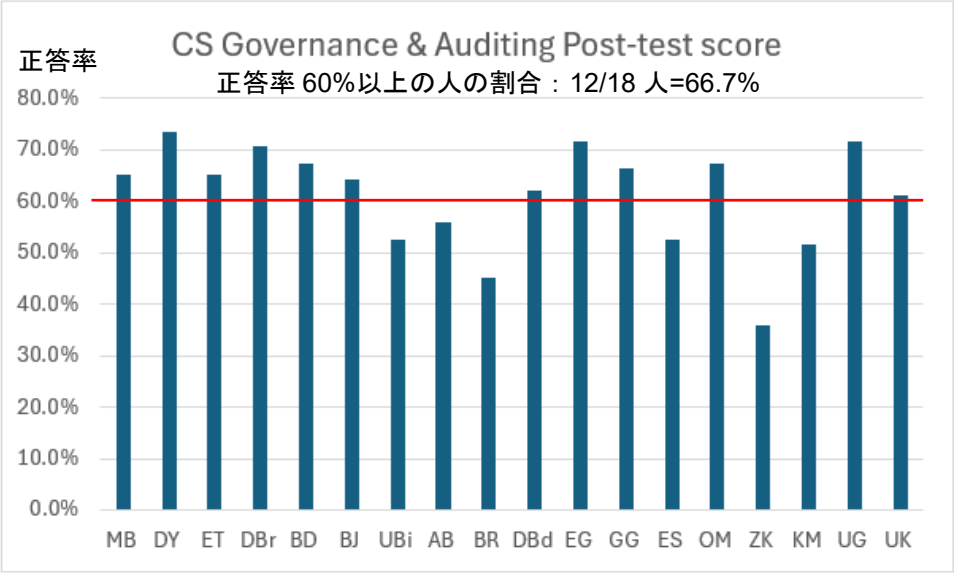


図-3　CS Governance and Auditing科目のPost-Testスコア

本科目で指標の表現を用いると「66.7%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。

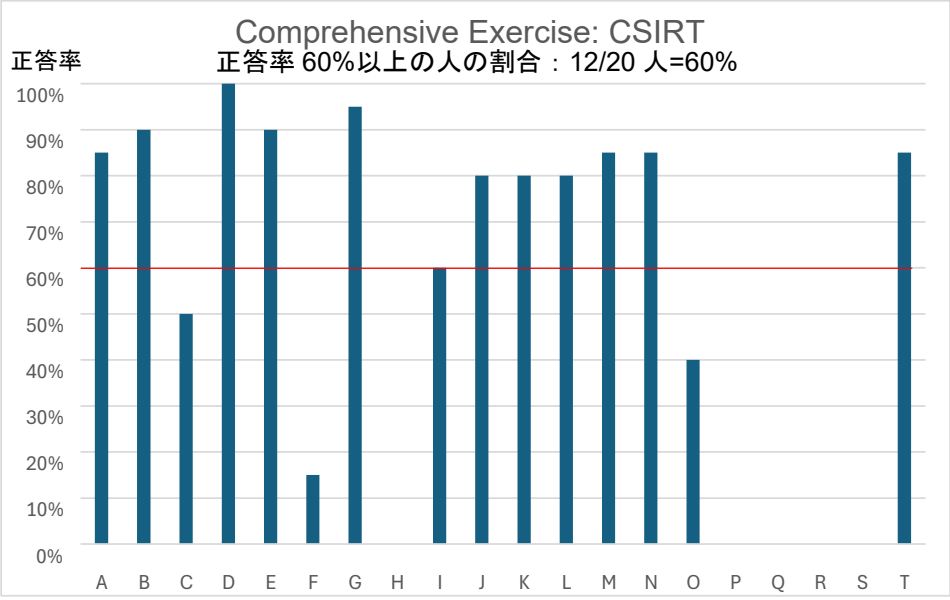


図-4　Comprehensive Exercise: CSIRT科目のPost-Testスコア

本科目で指標の表現を用いると「60%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。

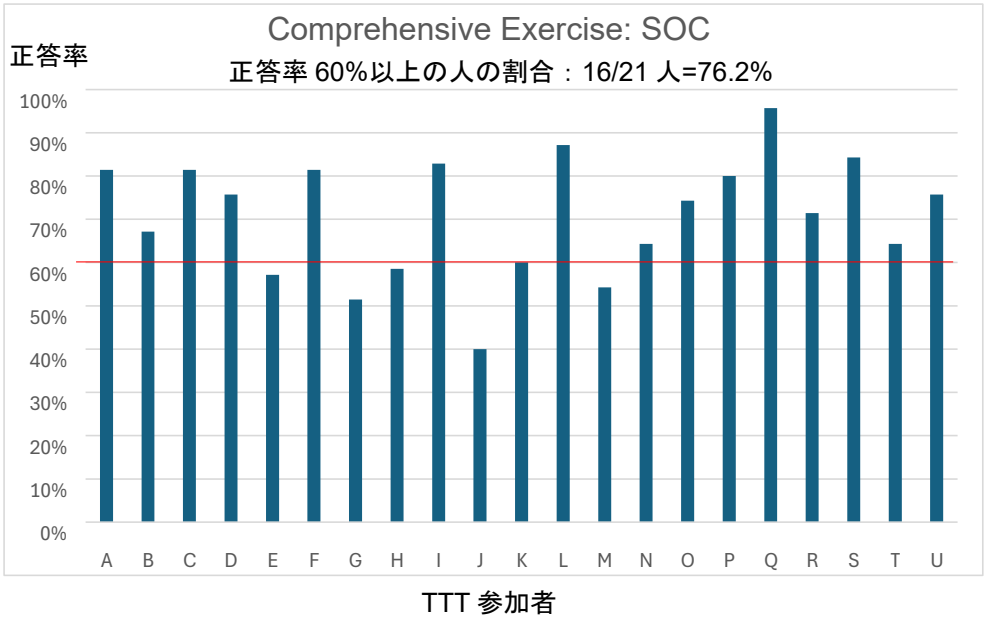


図-5　Comprehensive Exercise: SOC科目のPost-Testスコア

本科目で指標の表現を用いると「76.2%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。

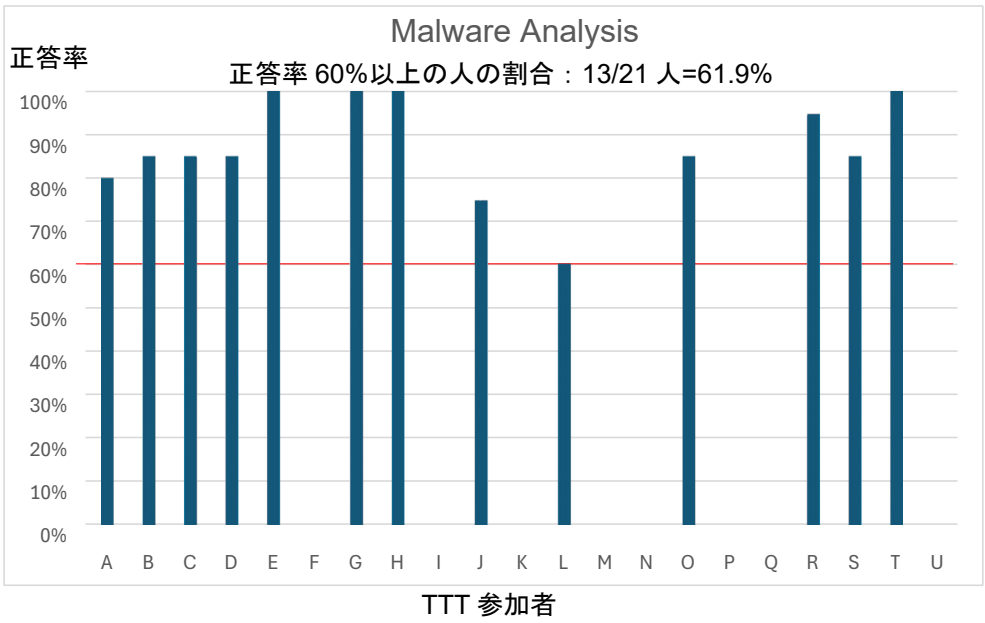


図-6　Malware Analysis科目のPost-Testスコア

本科目で指標の表現を用いると「61.9%の講師が最終試験で60%以上の正答率を得ている」となり、達成しているといえる。

指標2-3：　XX人以上の学生と社会人が訓練を受けた講師による授業を受ける

本件業務には学生と社会人を対象とした研修をモニタリングする活動は含まれていないため、本指標は評価できない。

4. 活動結果

4.1 成果1に係る活動

活動 1-1

➢ 日本と他国のCS人材育成の動向についての情報をC/Pや直営専門家と協議の上、提供する

本活動はCSトレンドセミナー向けのインプットとして必要に応じて実施する想定であったが、MDDICと協議して設定したセミナーのテーマとの関連性が低く、直営専門家と協議した結果、本活動は不要との結論に至ったため、実施していない。

活動 1-3

➢ 活動1-1に貢献するセミナーを実施する

■ 第1回CSトレンドセミナー

- System Center社への再委託により、2024年1月25日に第1回CSトレンドセミナーとして「Cybersecurity Capability Maturity Models and Standards」をテーマとしたオンライン／オフラインのハイブリッド形式にてセミナーを実施した。
- 本セミナーの企画はMDDICと協議の上行ったもので、同省の年間イベント計画にそったものである。
- 実施場所はウランバートル市内のイベント会場である「Millennium plaza」で、9時から17時の間に4トピックの講演を行った。

セミナーの各トピックと講演者は次の通り。

表-3 モンゴルプロジェクト第1回CSトレンドセミナーの講演内容

No.	トピック	講演者
1	Cybersecurity Measures for SMEs Presentation of cybersecurity measures for SMEs	［当チーム専門家］ 石田光彦氏
2	NIST Cybersecurity Framework (CSF)	［System Center 社］ Mr. Baasandorj Batbaatar 氏
3	ISO 27001 (ISMS)	［System Center 社］ Ms. Enkhutugalag Ulziit 氏
4	Cybersecurity Capability Maturity Models (Incl. Group activities & case study)	［System Center 社］ Mr. Baasandorj Batbaatar 氏

セミナーの様子を以下、掲載する。

写真-1　モンゴルプロジェクト第1回CSトレンドセミナーの様子

■　第2回CSトレンドセミナー

・　Info Sec Plus社への再委託により、2024年12月12日に第2回CSトレンドセミナーとして「Cybersecurity in Critical Information Infrastructure (CII)」をテーマとしたオンライン／オフラインのハイブリッド形式にてセミナーを実施した。

・　本セミナーの企画はMDDICと協議の上行ったもので、同省の年間イベント計画にそったものである。

・　実施場所はウランバートル市内のイベント会場である「Holiday Inn Hotel」で、9時から17時の間に4トピックの講演を行った。

・　セミナーの各トピックと講演者は次の通り。

表-4　モンゴルプロジェクト第2回CSトレンドセミナーの講演内容

No.	トピック	講演者
1	The Importance and Future of Cybersecurity in Fintech	［Info Sec Plus 社］ Ganbayar Uuganbayar 氏
2	Cybersecurity in OT environments	［株式会社東芝］ 大橋健一郎氏
3	Zero Trust Infrastructure Architecture (ZTIA)	［Info Sec Plus 社］ Telmuun Tumnee 氏
4	Supply Chain Cyber Risk and Measures	［フォーティネットジャパン合同会社］ 佐々木弘志氏

セミナーの様子を以下に掲載する。

写真-2　モンゴルプロジェクト第2回CSトレンドセミナーの様子

4.2　成果2に係る活動

活動 2-1

> ➢ **インドネシアで開発したカリキュラム改訂マニュアルをモンゴルの法制度や現地の事例を考慮したうえで、ローカライズする**

これまでの経緯を以下にまとめる。

- 2023年12月の現地業務にて、カリキュラム策定方法に関する技術移転（SecBokの内容及び活用方法の解説、その内容を踏まえた科目選定に係る協議）を実施した。
- C/Pに対し、カリキュラム改訂に係るSecBokマッピング方法を指導し、併せて当該活動に関する協議を行い、合意文書を作成した。
- 2024年6月の現地業務にて、カリキュラム改訂に係る協議とTTT実施科目の最終合意を行った。
- 2025年1月の現地業務にて、KSAマッピングとカリキュラム開発にかかるトレーニングを実施し、SecBokフレームワークを活用したカリキュラム開発の考え方及び方法、KSAマッピングの方法について、講義及びエクササイズを交えて解説した。

・ 2025年2月の現地業務にて、UIで作成されたカリキュラム改訂マニュアルをSICT向けにローカライズし、その内容についてSICTへ説明した。その後、先方との協議結果を踏まえて最終化し、マニュアル一式をSICTへ引き渡した。

トレーニングの様子を以下に掲載する。

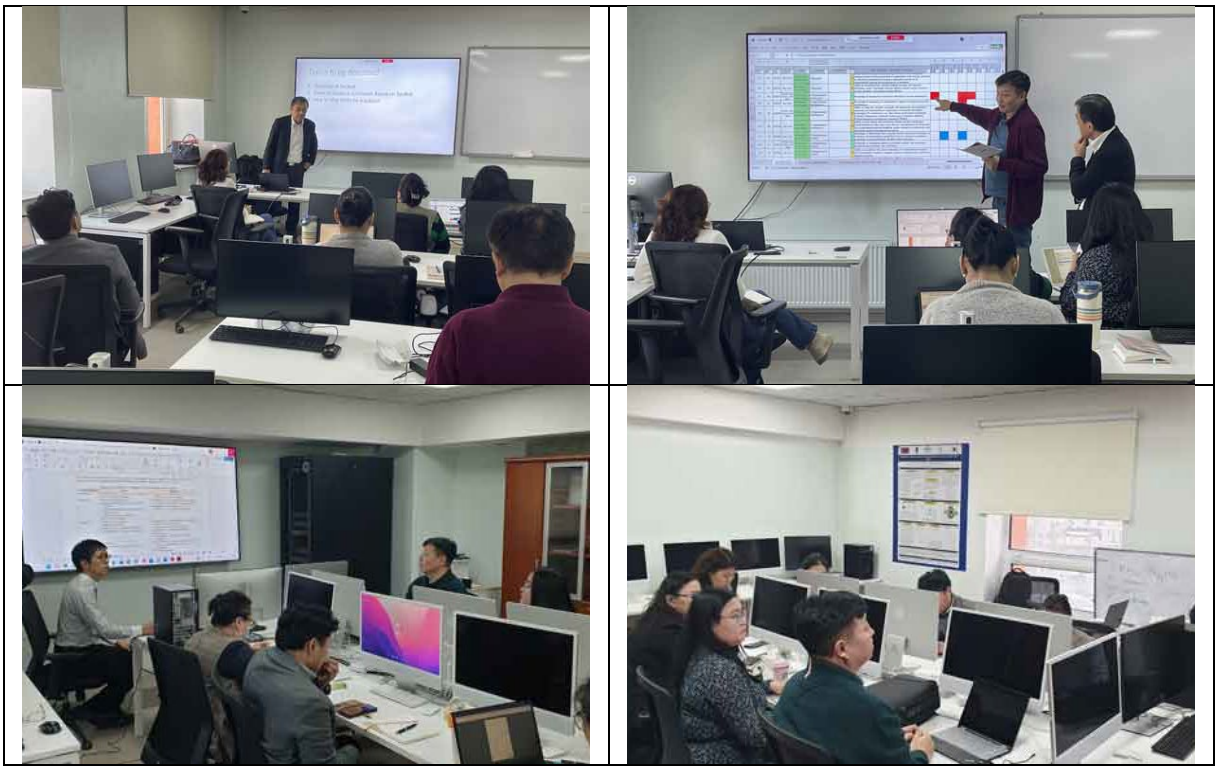


写真-3　モンゴルプロジェクトカリキュラム改訂にかかるトレーニングの様子

活動 2-2

- ➢ インドネシアで開発したインドネシアのカスタム科目のローカライズを行う（計4科目を想定）
- ➢ ローカライズ科目以外にも必要な新規科目を開発する（2科目を想定）

モンゴルプロジェクトでローカライズ、または新規開発を行っている科目の一覧は、「1.2.1 成果1の目標達成度　指標1-2」にて報告済みであるため、ここでの報告は割愛する。

活動 2-3

- ➢ 新規科目のTTTを実施する（ローカライズしたカスタム科目4つと、モンゴル用に新規科目の2つを想定）
- ➢ アクティブラーニングの手法を取り入れた研修設計にてTTTを実施する
- ➢ TTTの前後で、能力判定テストを行う。またTTT終了時には、各参加者が講師として授業運営が可能になったかの評価も行う
- ➢ 過去のTTT内容を自習できるような「教員育成用教材」を整備する

以下、TTTを実施した6科目について詳細を報告する。

(1) ローカライズ科目「Cybersecurity Law(s) and Regulation(s)」（2024年6月TTT実施）

・ モンゴル企業であるFidelitas社への再委託により、2024年1月22日から1月24日にかけてCybersecurity Law(s) and Regulation(s)科目のTTTを行った。

以下にTTTの詳細をまとめる。

表-5 ローカライズ科目「Cybersecurity Law(s) and Regulation(s)」の詳細

実施日時	2024 年 1 月 22 日～1 月 24 日（3 日間） 8 時 00 分～17 時 30 分（モンゴル時間）
参加者数	MUST： 9 名 Police school of the University of Internal Affairs Mongolia： 4 名 Public, Computer Security Incident Response Team (CSIRT/CC)： 2 名 計 15 名（うち 1 名は 1 日目のみ出席）
会場	Dorchester Restaurant のカンファレンスルーム
内容	＜1 日目＞ Module 1. Cyber Paradigm Module 2. Cyber ethics, norms, rules Module 3. Cyber Law in Global Perspective Module 4. Mongolian Law and Regulation on Cybersecurity ＜2 日目＞ Module 5. E-commerce and IPR Module 6. Personal data protection Module 7. IT Policy Development ＜3 日目＞ - Mock Class - Post-test - Gethering feedback

Cybersecurity Law(s) and Regulation(s)科目のTTTの様子を、以下掲載する。

写真-4 Cybersecurity Law(s) and Regulation(s)科目のTTTの様子

(2)　新規開発科目「Advanced Web and Operating System Security」（2023年1月TTT実施）

・　ベトナム企業であるiPMAC社への再委託により、2024年6月10日から6月18日にかけてAdvanced Web and Operating System Security科目のTTTを行った。

以下にTTTの詳細をまとめる。

表-6　新規開発科目「Adcanced Web Security and Operating System Security」の詳細

実施日時	2024 年 6 月 10 日～6 月 18 日（土日を除く 7 日間）
参加者数	MUST 教員：　13 名 MDDIC 職員：　1 名 Cybersecurity Incident Response Team Coordination Center 職員：　2 名 University of Internal Affairs Mongolia 教員：　2 名 Nationla University of Mongolia 教員：　2 名 計 20 名
会場	Conference room, 5th Fl., Naran Residence,
内容	・講義（Web Security 及び Operating System Security にそれぞれ 3 日間、合計 6 日間） ・モジュールごとにそれぞれ事前・事後テストを実施 ・参加者による模擬講義（1 日間） ・再現性担保のため、全内容を録画しモンゴル語字幕を付加して SICT へ納入予定。 **【Advanced Web Security 内容】** ＜1 日目＞ Module 1.　Overview of Web Security ＜2 日目＞ Module 2.　Understanding Common Web Vulnerabilities Module 3.　Secure Coding Practices ＜3 日目＞ Module 4.　Penetration Testing Methodologies **【Operating System Security 内容】** ＜1 日目＞ Module 1.　Practical Implementation of Linux Security Features Module 2.　SELinux Detailed Overview Module 3.　Common Vulnerabilities in Linux Operating Systems ＜2 日目＞ Module 4.　AppArmor Configuration and Use Cases Module 5.　Linux Vulnerability Analysis ＜3 日目＞ Module 6.　Introduction to Windows OS Architecture and Security Features Module 7.　Typical Windows Vulnerable Service Module 8.　Advanced Security Configurations in Windows

Advanced Web and Operating System Security科目のTTTの様子を、以下掲載する。


写真-5　Advanced Web and Operating System Security科目のTTTの様子

(3) 新規開発科目「Cybersecurity Governance and Auditing」（2024年6月TTT実施）

・ カンボジア企業であるSword and Shield Cecurity社（SSC社）への再委託により、2024年6月19日から6月24日にかけてCybersecurity Governance and Auditing科目のTTTを行った。

以下にTTTの詳細をまとめる。

表-7 新規開発科目「Cybersecurity Governance and Auditing」の詳細

実施日時	2024 年 6 月 19 日～6 月 24 日（土日を除く 4 日間）
参加者数	MUST 教員： 11 名 National University of Mongolia 教員： 2 名 National Academy of Government 職員： 1 名 MDDIC 職員： 2 名 Public CSIRT/CC 職員： 2 名 E-Mongolia academy 職員： 1 名 Regulatory Agency of Government Digital Services 職員： 1 名 計 20 名
会場	The Corporate Hotel Conference Room
内容	・講義を 3 日間、参加者による模擬講義 1 日間。 ・初日と最終日にそれぞれ事前・事後テストを実施。 ・再現性担保のため、全内容を録画しモンゴル語字幕を付加して SICT へ納入予定。 【内容】 ＜1 日目＞ Module 1. Internal Control: Lines of Defense and Lines of Assurance Module 2. Cybersecurity Governance Exercise 01: Plan for the development of cybersecurity governance by identifying needs and components for the development of cybersecurity governance for a Plan for the development of cybersecurity governance by identifying needs and components for the development of cybersecurity governance for an organization. ＜2 日目＞ Module 3. Risk Management Module 4. Internal Control: Lines of Defense and Lines of Assurance Exercise 02: Based on the output of Exercise 01, apply the risk management process Module 5. Policy Development Exercise 03: Based on the objectives and output of Exercise 01 and Exercise 02, develop a cybersecurity policy for the governance of the cybersecurity in Exercise 02. ＜3 日目＞ Module 6. Cybersecurity Auditing Exercise 04: Based on the objectives and outputs of Exercises 01, 02, and 03, develop a plan for the audit of the governance and cybersecurity domains in Exercise 04. Module 7. ISO/IEC 27001 Information Security Management System (ISMS) Audit Exercise 05: Based on the provided scenario, perform ISMS audit

Cybersecurity Governance and Auditing科目のTTTの様子を、以下掲載する

写真-6　Cybersecurity Governance and Auditing科目のTTTの様子

(4)　ローカライズ科目「Comprehensive Exercise: CSIRT」（2024年12月TTT実施）

・　オーストラリア企業であるZecureRight社への再委託により、2024年12月16日から12月20日にかけてComprehensive Exercise: CSIRT科目のTTTを行った。

以下にTTTの詳細をまとめる。

表-8　ローカライズ科目「Comprehensive Exercise: CSIRT」の詳細

実施日時	2024 年 12 月 16 日～12 月 20 日（5 日間） 9 時 00 分～17 時 00 分（モンゴル時間）
参加者数	MUST：　10 名 National University of Mongolia：　2 名 National CSIRT：　4 名 Public CSIRT：　4 名 計 20 名
会場	SICT の教室（Room 317）
内容	**Module 1:　Introduction of CSIRT and CSIRT activities** 1.1.　Cybersecurity overview 1.2.　Common TTP behind the incidents 1.3.　The Computer Security Incident Response Team (CSIRT) 1.4.　Establishment of an Incident Response Plan and Team (CSIRT) 1.5.　Operation of a Computer Security Incident Response Team (CSIRT) 1.6.　Security Assurance **Module 2:　Scenario briefing and team arrangement coordination** 2.1.　Introducing Management Policies 2.2.　Introducing Technical Policies 2.3.　Exercise Scenarios 2.4.　Participant Team Arrangement and Task Delegation

	Module 3: Scenario 1: Research Possible Attacks on the Constituencies and Give Report 3.1. Service Area 8: Situational Awareness 3.2. Data Acquisition Policy 3.3. Exercise - Data Acquisition of any possible attack 3.4. Communication to the Constituency **Module 4: SOC Introduction, Threat Visibility and Incident Handling Management** 4.1. Service Area 5: Information Security Event Management 4.2. SOC Introduction 4.3. SOC Core Activities – FIRST CSIRT Service Framework 2.1 4.4. Threat Visibility 4.5. Incident Handling Management 4.6. Incident Classification – FIRST CSIRT Case Classification 4.7. Ticketing System – The Incident Management Process Control **Module 5: Scenario 2: Receive a Report of Attacks and Analyze the Incident, Then Classify which Report Should be Handled by CSIRT** 5.1. Service Area 6: Information Security Incident Management 5.2. How to Form Incident Response Plan 5.3. Analyze Artifacts and Forensic Evidence 5.4. Mitigation and Recovery 5.5. Information Security Coordination with Internal & External Organizations 5.6. Traffic Light Protocol 5.7. Exercise - Cybersecurity Incident Response Simulation **Module 6: Scenario 3: Discover Vulnerability on the Constituency System and Develop an Advisory Report for Remediation** 6.1. Service Area 7: Vulnerability Management 6.2. Exercise - Finding Vulnerabilities **Module 7: Scenario 4: Develop an Awareness Material and Plan of Activities** 7.1. Service Area 9: Knowledge Transfer 7.2. Exercise - Improve Security Awareness **Module 8: CSIRT Maturity** 8.1. Development Stages of a CSIRT 8.2. Exercise - CSIRT Maturity Assessment

Comprehensive Exercise: CSIRT科目のTTTの様子を、以下掲載する。

写真-7　Comprehensive Exercise: CSIRT科目のTTTの様子

(5) ローカライズ科目「Comprehensive Exercise: SOC」（2025年1月TTT実施）

・ ベトナム企業であるiPMAC社への再委託により、2025年1月6日から12月10日にかけてComprehensive Exercise: SOC科目のTTTを行った。

以下にTTTの詳細をまとめる。

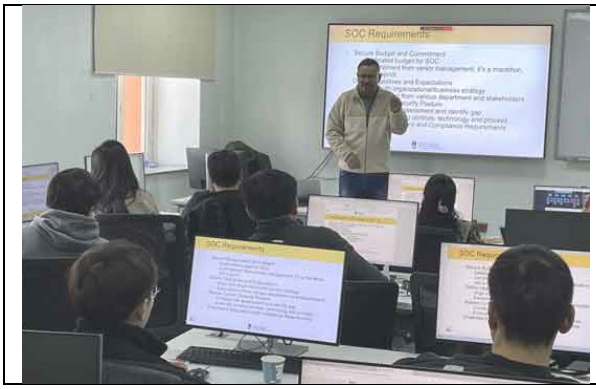
表-9 ローカライズ科目「Comprehensive Exercise: SOC」の詳細

実施日時	2025 年 1 月 6 日～1 月 10 日（5 日間） 9 時 00 分～17 時 00 分（モンゴル時間）
参加者数	MUST： 10 名 National University of Mongolia： 3 名 National CSIRT： 4 名 Public CSIRT： 4 名 計 21 名
会場	SICT の教室（Room 317）
内容	**<u>Day 1:</u>** **Chapter 1: SOC Overview** 1.1. Current Threats Landscape in Indonesia 1.2. What is SOC 1.3. Why we need a SOC 1.4. Regulations regarding SOC 1.5. Challenges in Operating a SOC **Chapter 2: SOC Planning** 2.1. SOC Requirements 2.2. SOC-CMM Overview 2.3. SOC Business Considerations 2.4. SOC People Considerations 2.5. SOC Process Considerations 2.6. SOC Technology & Service Considerations 2.7. Exercise: Defining SOC Charter **Chapter 3: SOC Operational Model** 3.1. Operational Model Overview 3.2. In-house SOC 3.3. MSSP 3.4. Hybrid SOC 3.5. Follow-the-sun 3.6. Fully remote SOC 3.7. Exercise: Defining SOC Operational Model **Chapter 4: SOC Services** 4.1. SOC Services Overview 4.2. Command Center 4.3. Security Monitoring 4.4. Incident Response 4.5. Threat Hunting 4.6. Threat Intelligence 4.7. Other SOC Services 4.8. Exercise: Defining SOC Services **Chapter 5: SOC People** 5.1. SOC People Overview 5.2. Roles and Hierarchy 5.3. People Management 5.4. Shifting Management 5.5. Training and Education 5.6. People Sizing and Allocation 5.7. Exercise: Defining SOC Analyst Knowledge Matrix

	Chapter 6: Building the SOC 6.1. Secure Architecture 6.2. SOC Facilities 6.3. Virtual SOC 6.4. Exercise: Building the SOC using Gantt Chart **Chapter 7: SOC Operations** 7.1. Operational Considerations 7.2. Reporting Management 7.3. SOC Metrics 7.4. Use Case Management 7.5. Detection Engineering 7.6. Exercise: Defining Shift Handover, SOC Regular Report **Day 2:** **Chapter 8: Service & Technology: Security Command Center** 8.1 Technology, People, and Process 8.2. Exercise: SIEM Hands-On: Wazuh 8.3. Exercise: Installing Wazuh and its Components **Chapter 9: Service & Technology: Security Monitoring & Threat Detections** 9.1. Technology, People, and Process 9.2. Exercise: Log Collection and Monitoring: Syslog and API 9.3. Exercise: Other Log Collection Mechanisms 9.4. Exercise: Threat Detections on Endpoint 9.5. Exercise: Threat Detections on Network 9.6. Exercise: Threat Detections on Cloud **Chapter 10: Service & Technology: Security Monitoring & Threat Detections** 10.1. Technology, People, and Process 10.2. Exercise: Hands-on Threat Hunting with Wazuh **Chapter 11: Service and Technology: Detection Engineering** 11.1. Technology, People and Process 11.2. Exercise: Detection Engineering: Sysmon 11.3. Exercise: Detection Engineering: Auditd 11.4. Exercise: Detection Engineering: Sigma Rules **Chapter 12: Service and Technology: Incident Response** 12.1. Technology, People and Process 12.2. Exercise: Alert Triage using Wazuh 12.3. Exercise: IR Automation on Wazuh **Chapter 13: Other SOC Services & Technology** 13.1. Forensic 13.2. Vulnerability Management 13.3. Log Management 13.4. Security Awareness 13.5. Exercise: Dashboard Monitoring, Alerting and Response **Day 3:** **Chapter 14: Security Monitoring: Phishing Emails** 14.1. Techniques for monitoring & investigating phishing emails 14.2. Exercise: Investigate Email Threats (BEC) **Chapter 15: Security Monitoring: Endpoint Threats & Intrusions** 15.1. Overview of endpoint security monitoring techniques 15.2. Exercise: Investigate Windows Intrusion - Long Tail Logs Analysis 15.3. Exercise: Investigate Windows Intrusion - Windows Event Logs **Chapter 16: Security Monitoring: Network Threats & Intrusions** 16.1. Techniques for monitoring and investigating network threats 16.2. Exercise: Investigate Network Intrusion - Malicious DNS Traffics 16.3. Exercise: Investigate Network Intrusion - TLS Encrypted Traffic 16.4. Exercise: Investigate Network Intrusion - C2 Traffic **Chapter 17: Security Monitoring: Cloud Threats & Intrusions** 17.1. Cloud security monitoring techniques 17.2. Exercise: Investigate Cloud Intrusion - Rogue VM

	17.3. Exercise: Investigate Cloud Intrusion - Data Exfiltration **Chapter 18: Security Monitoring: Linux Intrusions** 18.1. Monitoring and investigating Linux threats 18.2. Exercise: Investigate Linux Intrusion - Auditd Logs 18.3. Exercise: Investigate Linux Intrusion - Bash History 18.4. Exercise: Investigate Linux Intrusion - Web App Attack **Chapter 19: Other Case Studies & Group Discussions** 19.1. Review real-world case studies related to security monitoring 19.2. Group discussions on lessons learned and best practices 19.3. Exercise: IR Simulation (tabletop format) **Day 4:** **Chapter 20: Threat Hunting and Intelligence Overview** 20.1. Threat hunting and threat intelligence 20.2. Key concepts and objectives **Chapter 21: Other Case Studies & Group Discussions** 21.1. Planning Threat Hunting (Defining Hypothesis, Scoping, Execution) 21.2. Maturity model in threat hunting 21.3. Discussion on methodologies 21.4. Exercise: Threat Hunting Methodology & Maturity Model **Chapter 22: MITRE ATT&CK Overview** 22.1. The MITRE ATT&CK framework 22.2. Threat Attribution Mapping from Threat Intel Report 22.3. Exercise: Hands-on MITRE ATT&CK Navigator **Chapter 23: Threat Intelligence Process and Platform** 23.1. Lifecycle and platforms of different TI models 23.2. Exercise: Hands-on MISP 23.3. Exercise: Hands-on Open CTI **Chapter 24: Hunting on the Cloud** 24.1. Techniques & tools for threat hunting cloud-based 24.2. Exercise: Hunting for Lateral Movement in the Cloud **Chapter 25: Other Case Studies & Group Discussions** 25.1. Review real-world case studies related to security monitoring 25.2. Group discussions on lessons learned and best practices 25.3. Exercise: Hunting on Endpoint: Persistence 25.4. Exercise: Hunting on Endpoint: Credential Dumping 25.5. Exercise: Hunting on Endpoint: Lateral Movement 25.6. Exercise: Hunting on Endpoint: C2 Beacon

Comprehensive Exercise: SOC科目のTTTの様子を、以下掲載する。



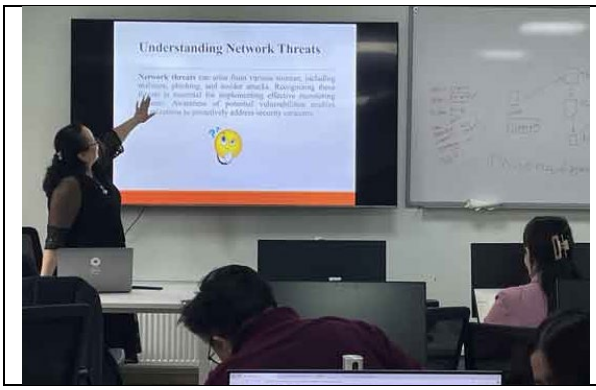


写真-8　Comprehensive Exercise: SOC科目のTTTの様子

(6)　ローカライズ科目「Malware Analysis」（2025年2月TTT実施）

・　モンゴル企業であるVKNC社への再委託により、2025年2月7～8日、14～15日、22日にMalware Analysis科目のTTTを行った。

以下にTTTの詳細をまとめる。

表-10　ローカライズ科目「Malware Analysis」の詳細

実施日時	2025 年 2 月 7, 8, 14, 15, 22 日（5 日間） 9 時 00 分～17 時 00 分（モンゴル時間）
参加者数	MUST：　9 名 National University of Mongolia：　3 名 National CSIRT：　3 名 Public CSIRT：　3 名 MNCIRT：　2 名 計 20 名
会場	SICT の教室（Room 317）
内容	**Module 1.　Basic Analysis Techniques** 1. Definition Introduction 2. Malware analysis 3. Basic Analysis Techniques Lab **Module 2.　Basic Static Techniques** 1. Definition Introduction 2. Basic static analysis 3. Antivirus scanning 4. Malware hashing 5. Malware string 6. Detect malware packer/obfuscated 7. Inspect Portable Executable (PE) Header 8. Exploring Dynamic Link Library (DLL) 9. Basic Static Analysis Lab **Module 3.　Basic Dynamic Analysis** 1. Dynamic analysis 2. Sandboxing 3. Dynamic analysis tools 4. Running malware 5. Malware runtime analysis 6. Network Monitoring 7. Basic Dynamic Analysis Labs

	Module 4. Advance Static Analysis 1. Core X86 assembly concept 2. Reverse engineering code analysis with IDA pro 3. Analyzing malicious code 4. Malware Behavior 5. Advance Static Analysis Labs 6. Code debugging 7. Malware debugging with OllyDbg 8. Loading DLL Kernel debugging with WinDbg 9. Advance Dynamic Analysis Labs **Module 5. Self-Defending Malware** 1. Packer and unpacking 2. Bypassing analysis defenses 3. Malware Defense Analysis Labs **Module 6. Automating Analysis** 1. In-Depth Code Analysis and Automation 2. Selective Exercises and Case Studies 3. Malware Handling Procedure and Lab Safety 4. De-obfuscating Code in Multi-Component Malware 5. Frida **Module 7. Data Sanitation** 1. Data Sanitation: Preparing for Safe Analysist 2. Advanced Analysis Techniques 3. Converged Environment and Open-Source Tools 4. Ghirda

Malware Analysis科目のTTTの様子を、以下掲載する。

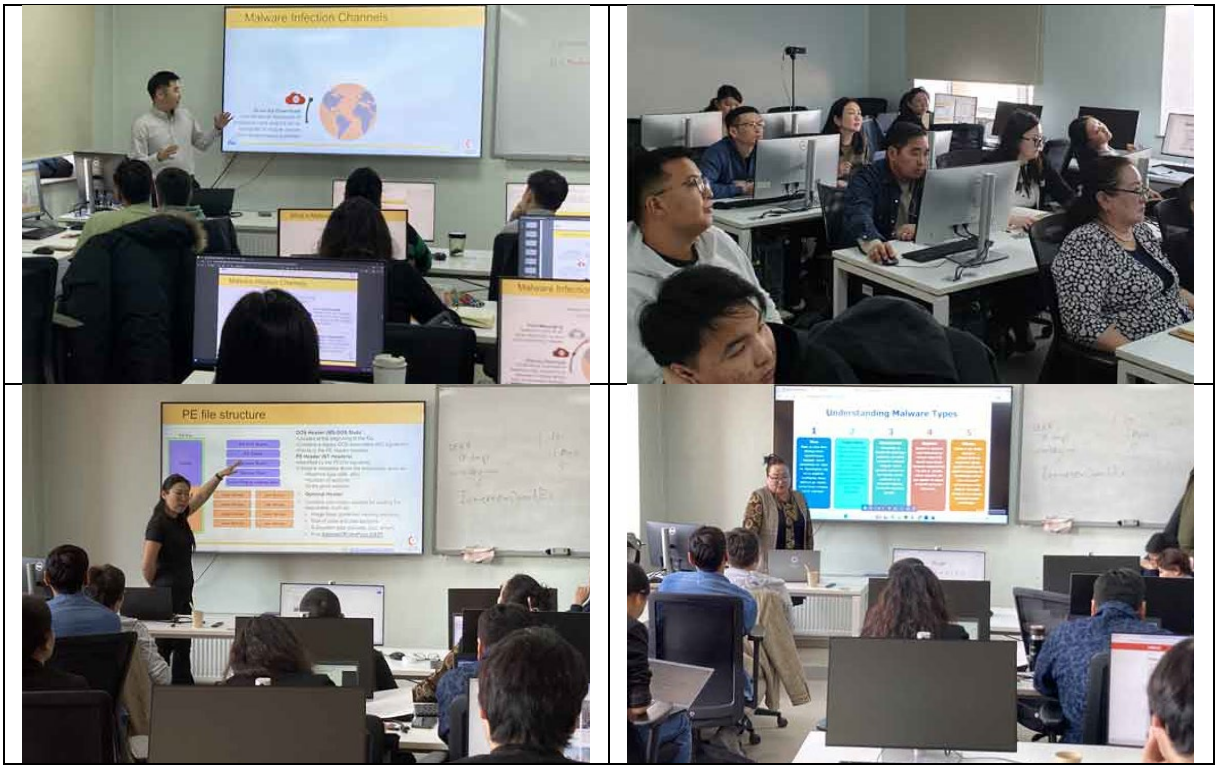


写真-9　Malware Analysis科目のTTTの様子

活動 2-5

➢ **活動2-3の新規カスタム科目をC/Pが実際に講義を行った後に、担当教員と改善点について意見交換する。**

各TTTの最終日に行う模擬授業にて、参加者に講義体験をさせ、講義内容や講義態度、および改善点について意見交換・指導を行った。

4.3 その他の活動

- 2023年10月の現地業務にて、全活動に関連するワークプランの最終化を行った。
- 2023年12月の現地業務にて、個別面談を通じたC/P（MUST-SICT講師陣）に対するキャパシティアセスメントを実施した（現状能力の評価及び今後の能力強化に関する方針や希望の確認）。

5. プロジェクト実施と成果に影響を及ぼした工夫または留意点

5.1 コミュニケーションに関する問題

(1) C/Pとのコミュニケーション不足

C/Pにコメントや決定を求めた際のレスポンスが遅く、プロジェクトの推進に影響した。特にメールやMattermost[1]を使った全員宛の連絡への反応が悪く、レスポンスが無かったケースも多々発生した。

【工夫】

- 複数のコミュニケーションチャネルを活用して前広に連絡することで、影響を極小化。特にメッセージアプリによる個別の依頼や問い合わせに対するレスポンスは比較的良いため、担当者を決めて個別に直接連絡することで改善した。

(2) 関係者間の議論方法

SICT-WGメンバーとの話し合いにおいて、議論が発散してしまい結論が出ないことが多く、複数回の会議を重ねても議論が前後することで進展がみられないことがあった。また時間をかけてようやく出した結論も後から覆されることもあった。

【工夫】

- 重要な議題は会議中でもモンゴル語による内輪の数十分の議論が発生し、その後突然結論が示されることがあった。その結論が的はずれであったり、後々覆されたりすることがあるなどの傾向が見られた。モンゴル側の真意や反対意見を正確に把握するには、内輪でのモンゴル語の議論内容を理解することが重要であることに気づき、ミーティングへの通訳同席や、録画音声を後で翻訳することにより、モンゴル側の内輪の議論の詳細

[1] Mattermost：Slack 似の OSS ビジネスコミュニケーションツール

な理解に努め、必要に応じてキーパーソンとの個別面談を行うなどの対応を取るようにした。

- SICT-WGメンバーだけでなく、より上位職である学務部長（Uuganbayar氏）を巻き込み、トップダウンの指示を依頼したり、決定事項に対して書面で彼の承認を得るようにしたりするなどして後から覆されないよう工夫した。

(3) その他

- 打合せの中で本音を言いたがらない、また若手メンバーが上位者に気を遣い発言を控える等の傾向があり、それらを踏まえたコミュニケーション上の工夫が必要であることがわかった。今後も①主担当者を据える、②個別に意見を聴取する、などスムーズなコミュニケーションを図っていく。
- 本件業務の活動当初、SICT-WGメンバーの中から事実上のリーダーを立てることで円滑な進捗を期待したが、本人の能力不足や人望の問題からか、期待した効果が得られなかった。そこでチーフアドバイザーの助言を得て、上位職者による関与・管理を求めることを実践することでWGグループの意思決定や方針の一貫性に改善が見られ、進捗も改善された。今後もリーダーを中心としたWGの体制は維持しつつ、最終的な決定や問題発生時の対処には上位職者を巻き込んでいく。

5.2 カリキュラム設計に関する問題

(1) C/Pのプロジェクト方針に従ったカリキュラム設計能力

SICT-WGメンバーのSecBokやKSA[2]に対する理解が不足しており、大学のマスターコースとしてのセキュリティ人材育成に適切なカリキュラムの策定が困難な状況だった。

【工夫】

- SICT-WGに対してSecBokやKSAマッピングの解説をして理解を深めてもらうとともに、こちらからあるべき姿を提示する提案型での議論を推進した。具体的にはカリキュラム策定に関し以下の提案を行った。

  ① 2つのPath（Technical Path及びAdministrative Path）を用意することを提案し、その有効性を説明した。

  ② 必修科目として、Comprehensive Security（CompTIAのSecurity+をベースとした科目）及びSecurity Governance and Auditingを含めることを提案し、その有効性を説明した。具体的には、両者ともSecBokにおけるKSAのカバー範囲が広く、内容が網羅的でセキュリティ人材としての土台を築くのに適しており、Technical PathとAdministrative Pathいずれを志向する上でも習得しておくべき内容であることを説明し、理解を得た。

[2] KSA: Knowledge, Skill, Ability（知識、スキル、能力）の略。SecBok で使われる用語

5.3　TTT及びセミナー準備・実施上の問題

(1)　モンゴル国内の再委託先候補企業の不足

モンゴル国内にサイバーセキュリティ分野のコンサルタントや専門家を擁する企業が少なく、複数の企業を比較して選定することが難しい。また競争が起こらないため、提示価格はかなり高めとなる傾向があり、想定価格を大幅に上回ることが多い。

【工夫】

- 他国でのサイバーセキュリティプロジェクトの実施経験を活かし、モンゴル国外の企業にも提案を呼びかけることで、十分な数及び質の再委託先候補を確保し、公正かつ適切な再委託先の選定を実現した。実際に2件の科目開発業務で、それぞれベトナムの企業とカンボジアの企業を選定している。
- ローカライズ科目については、候補先に対して既存コンテンツの情報を可能な範囲で共有し、説明することで理解を深めてもらった。これにより作業工数見積りの精度が高まり、当方の想定価格レベルに近けることができた。

(2)　TTTへの参加者選定プロセスの長期化

TTT参加者選考プロセスは複数機関が絡むため、複雑かつ不透明で、コンサルタントの力が及びにくい部分である。そのため選定に予想外の時間を要し、参加者への案内がTTT実施直前になるなどの問題が生じた。

【工夫】

- 参加者選定の取りまとめをSICT-WGの上位職者であるUuganbayar氏に依頼することで、選定時間の改善が見られた。
- 今後、本プロジェクトでの経験がある人間を特殊傭人として雇うなどして、このプロセスの推進と細かなフォローを実施することを想定している。

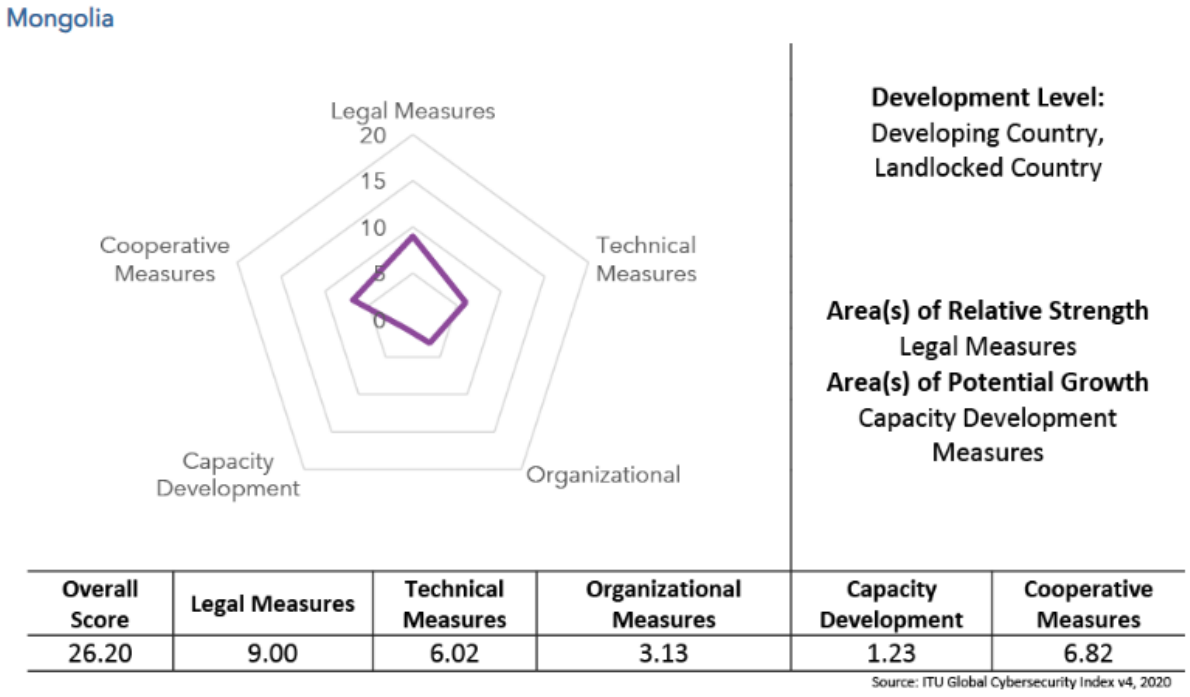
6.　プロジェクト終了後の上位目標達成の見込みおよび提言

プロジェクトが掲げる上位目標「モンゴル国の安全なデジタル社会を推進する」につき、以下その達成見込みに関する考察と提言をまとめる。

上位目標達成度を測る指標はITUが公表する世界サイバーセキュリティ指数（Global Cybersecurity Index: GCI）に基づいており、①GCIのトータルスコア、②GCIの「能力開発」の柱のスコア、③GCIの国家ランキングである。この内③の国家ランキングは2024年度以降廃止されており、現在は5段階の能力レベル（ティア1～5[3]）で示される。2024年度のモンゴルの総合能力は上か

[3] Tier1=Role-Modeling (score of 95–100), Tier2=Advancing (score of 55–85), Tier3= Establishing (score of 55–85), Tier4= Evolving (score of 20–55), Tier5=Building (score of 0–20)

ら3番目のティア3に分類されている。次の図は、モンゴルの2020年度と2024年度のGCIのデータである。



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.20	9.00	6.02	3.13	1.23	6.82

Source: ITU Global Cybersecurity Index v4, 2020

図-7　2020年版GCIモンゴルのデータ

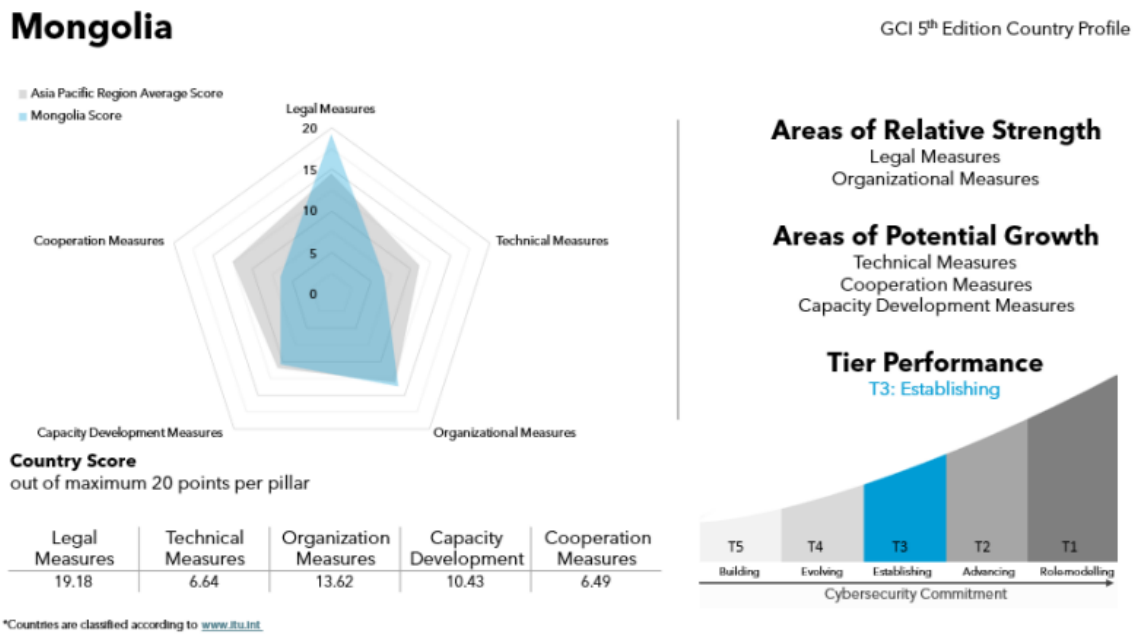


図-8　2024年版GCIモンゴルのデータ

これによれば、総合スコア（100点満点）は2020年の26.2から2024年56.36と大きく向上している。これはCS関連法の整備および国家CSIRT設立に向けた取り組みなどが評価されたものと推測できる。上位目標の指標にある「能力開発」の柱のスコアは、2020年度1.23から10.43に大きく向上しているものの、依然20点満点の約半分のスコアであり、十分とは言えない。

本プロジェクトではMUSTのSICTにおいて、CSマスターコースのカリキュラム整備と科目開発を行うことでコースの内容を充実させた。このことがモンゴル国内で認知され、入学希望者が増加し、より多くの卒業生を社会人として世に送り出すことができれば自ずとGCIスコアは向上すると考える。しかしながらこの効果を得るには今後数年以上かかると思われ、MUSTでの継続したCS教育の提供が必須となる。これを担保するための方策について、以下の取り組みを提案する。

(1) コース実施に関する管理・運用業務の分離

コースの宣伝、参加者の募集、実施場所確保などのロジ業務、講師募集・人事業務および会計業務など、付随業務を担う部門または組織を作り、講師陣がこのようなことに煩わされないようにする必要がある。

(2) 教材の定期的な見直しと最新化

サイバーセキュリティ技術の進歩は非常に早いため、比較的短い周期、少なくとも1年ごとに教材を見直し最新化することは必須である。これを怠ればマスターコースの評判を悪化させることになり、入学者確保が困難になる。本件業務においてMUST向けカリキュラム改定マニュアルを提供したが、この中に教材の見直し（改定・追加）に関する規定があるので、MUSTにおいてはこれを遵守することが重要である。

(3) CSマスターコースの宣伝

モンゴル国内に置けるMUSTのCSマスターコースの認知度向上のための宣伝活動を行うことで入学希望者の増加を図る。FacebookやLinkedIn、あるいはYouTubeなどのメディアを使った宣伝を積極的に行い、若者に対する認知度を上げていくことを提案する。