



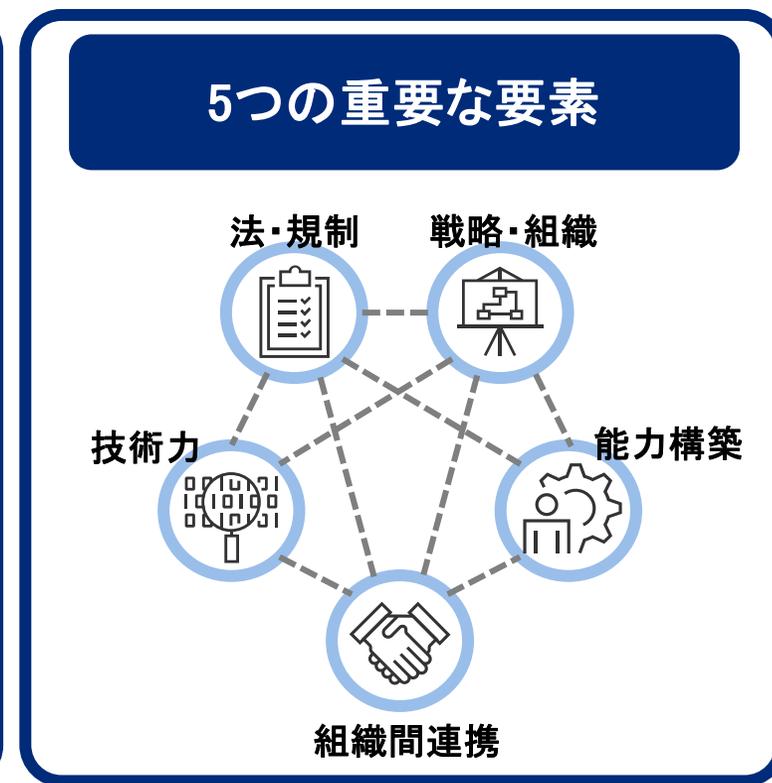
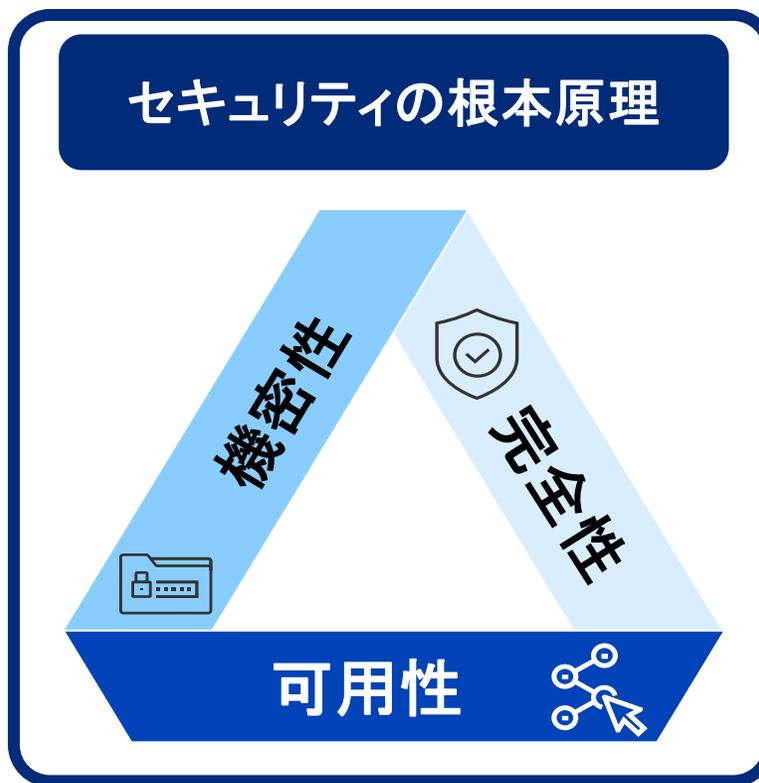
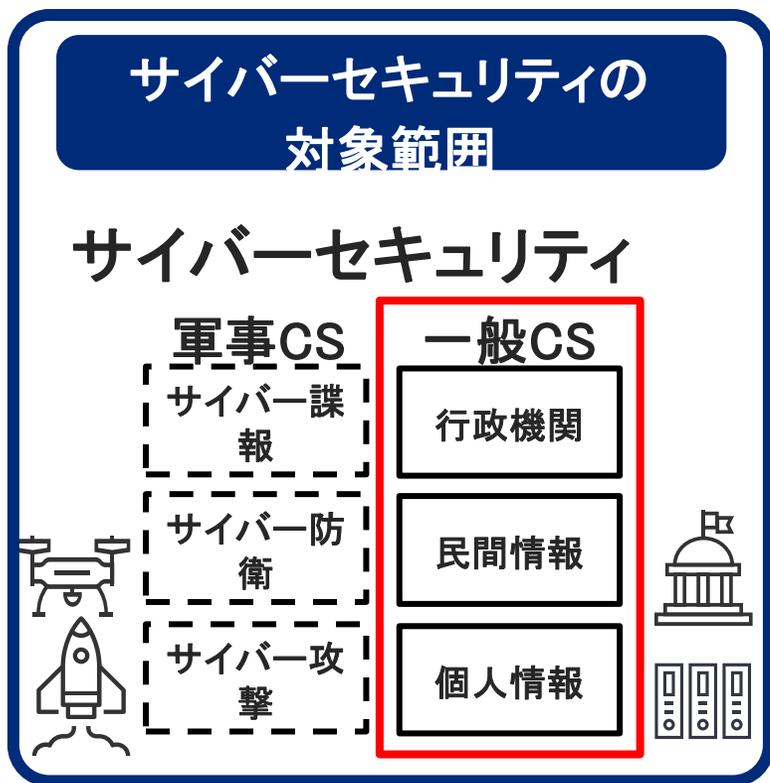
**Digital
transformation**

JICA サイバーセキュリティ協力事業 概要

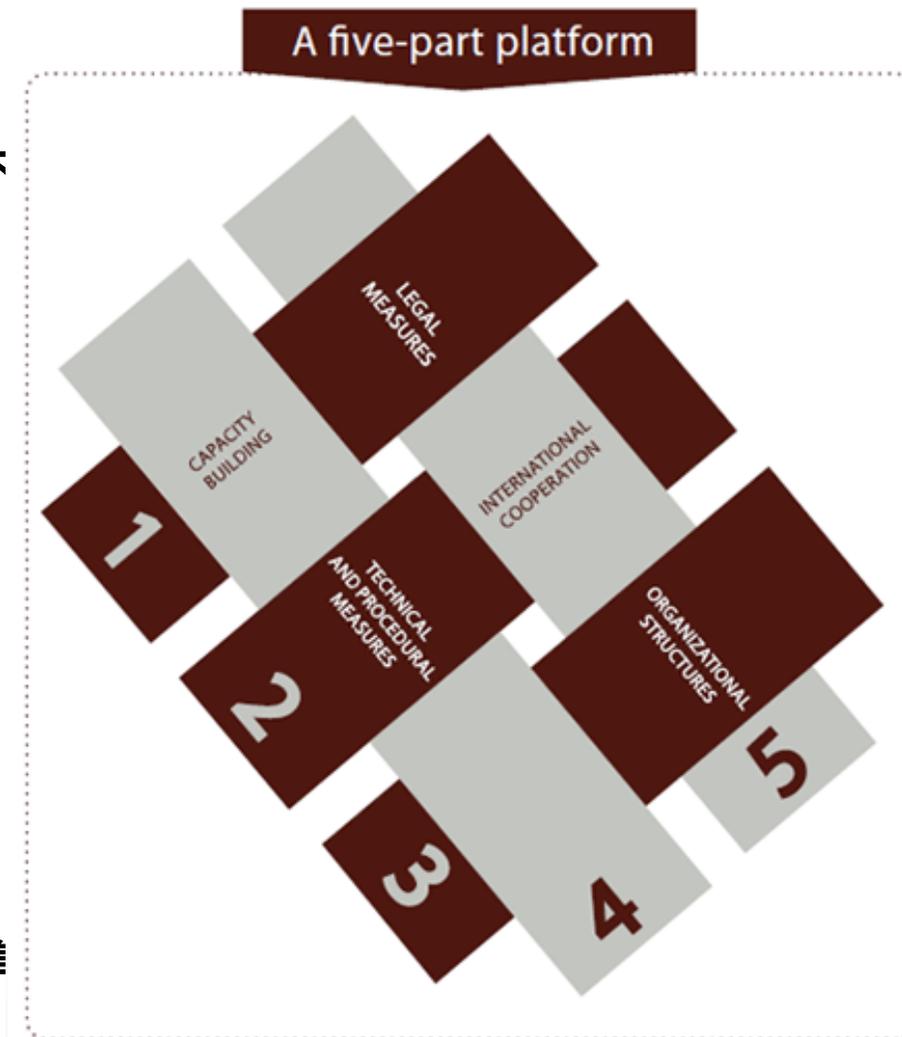
2024年 3月



- JICAでは一般サイバーセキュリティ(Civil Cybersecurity)の範囲を対象とし、情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)の確保に加え、国がサイバーセキュリティを推進するために必要な法令整備、体制整備、啓発活動などの重要な要素も含めた総合的な定義とする



- グローバル・サイバーセキュリティ・アジェンダ (GCA) は、ITUが2007年に公表した情報セキュリティ枠組み
 - 刻々と変化するサイバー脅威に各国が自律的に対応するためには、以下の5つの視点をバランスよく強化し、レジリエンスを高めていく必要がある
- (1) **法・規制** : 責任ある組織の設置、個人情報保護に関する法制度の整備、違法行為への対策など
 - (2) **戦略・組織** : 国家戦略と推進体制の構築
 - (3) **技術力** : リスク対応能力の向上
 - (4) **能力構築** : 公共部門および民間部門の人材育成、推進・啓蒙活動の体制整備
 - (5) **組織間連携** : 国内、海外、国際機関との協力
- グローバル・サイバーセキュリティ・インデックス (GCI) は、上記の5つの視点を評価し、各国のサイバーセキュリティへのコミットメントを測定する基準となるスコア



[Global Cybersecurity Agenda \(GCA\) \(itu.int\)](http://itu.int)

JICAのサイバーセキュリティの取り組み



■ STI・DX室は、JICA内の各課題・地域での取組みに対して、国内外の多様な連携パートナーと共創し、デジタル技術とデータの利活用による社会課題の解決とインパクト増大を図るため、事業DXを主導する。

WHY 目標

イノベーションエコシステム

経済成長と社会課題解決をデジタルで促進し、多様なプレイヤーがイノベーション創発するエコシステムを構築する

デジタル基盤

デジタル化の恩恵を享受し、またデジタル化による格差や安全リスクを削減するための基盤を整備する

WHAT 取組方針

SDGs各課題のDX推進

DXモデルの創出

フィジカルな協力アセットを活かしつつ、産業・広域データ連携やイノベーションエコシステム構築等、DXモデルを創出する(DPI・DPGの組成含む)。

交通DX

防災DX

医療DX

水道DX

農業DX

森林DX

デジタル基盤3本柱の支援

- 1 情報通信環境・基盤の整備
- 2 デジタル人材・産業の育成
- 3 サイバーセキュリティの強化

デジタル格差・CS主流化

データを社会に行き渡らせる情報通信環境の整備、デジタル化推進の担い手育成、自由で安全なサイバー空間の構築に係る事業を実施する。

JICAの多様な事業でのデジタル格差視点の組み込み、インフラ事業等でのサイバーセキュリティ主流化を図る。

HOW 具体施策

	内部支援	外部連携
デジタル	<p>DXアドバイザー</p> <ul style="list-style-type: none"> DX内部技術支援 	<p>デジタルパートナー共創</p> <ul style="list-style-type: none"> DXLab外部共創 DPG組成
データ	<p>JICAデータ活用</p> <ul style="list-style-type: none"> データカタログ ダッシュボード化 	<p>外部データ連携</p> <ul style="list-style-type: none"> データ連携基盤 DPI組成
科学技術	<p>SATREPS改革</p> <ul style="list-style-type: none"> 他事業と積極連携 国際頭脳循環 	<p>宇宙・AI</p> <ul style="list-style-type: none"> JAXA・AIST連携 APRSAF
タレント	<p>リスキリング</p> <ul style="list-style-type: none"> DX BootCamp ICT-KMN 	<p>外部人材NW</p> <ul style="list-style-type: none"> JICA-VAN LinkedIn活用

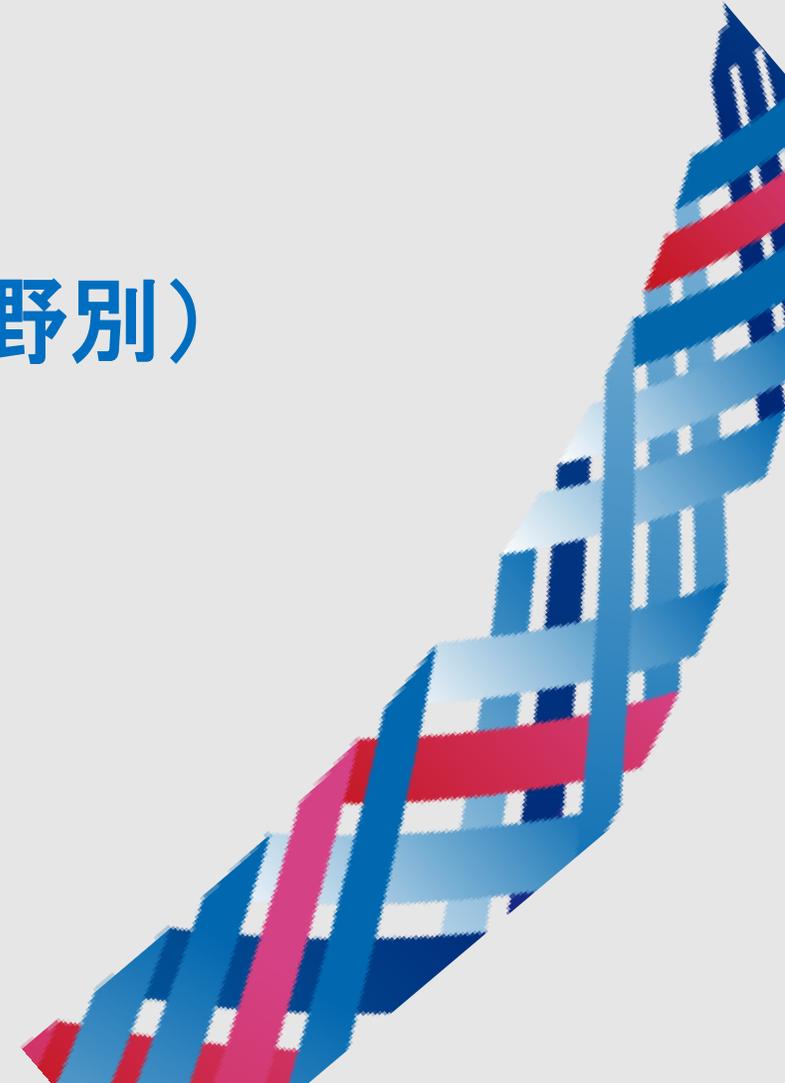
サイバーセキュリティの協力領域とステージ

・各国における自由で信頼性をもったデータ流通を担保できるサイバー空間の構築
 ・国際社会と協力した地域の安全なサイバー空間の実現



(図中で使用の略語) CS: Cyber Security CSIRT: Computer Security Incident Response Team

サイバーセキュリティ協力事業 事例(分野別)



- 本邦研修の実施をはじめ、日ASEANサイバーセキュリティ能力構築センター(AJCCBC)との協業と国家CSIRT強化事業によりASEAN地域全体のサイバーセキュリティ対応能力向上に貢献

サイバー攻撃防御演習

- 研修は4部構成で実施



- 案件目標と単元目標を基に研修を実施

案件目標

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の育成

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

単元目標1

最近のサーバ攻撃事例と対策を理解し、説明できる

単元目標2

標的型攻撃のインシデントハンドリング手順を理解し、説明できる

ASEAN地域協力

- CS及び関連技術のトレーニングの計画、実施、参加者のフォローアップ活動
- 研修機材の改善や最新化
- 若年層向けサイバーセキュリティ人材開発プログラム「Cyber SEA Game」の開催
- 第三者機関とのCS関連研修やセミナーの実施
- ASEANサイバーセキュリティにかかる情報収集と分析



Cyber SEA Game 2023時の交流風景(写真提供:NCSA)



Cyber SEA Game 2022優勝チーム(写真:AJCCBC)

カンボジアCS技術協力プロジェクト

CSIRT サービスの提供範囲の特定や組織の成熟度アセスメントを実施

あるべき姿を明確化

スキル・フレームワークを活用した研修の計画と実施

機材供与により業務環境の改善

ICTセキュリティ局のIT環境を整備

ガイドライン、標準運用手順書、サービスレベル合意書、普及啓発教材

政策・法律・戦略・標準等に関する提言

- 教育機関と協力し、教材開発と人材育成を実施。開発した教材を共有することで、プロジェクト間の相乗効果が得られCS教育に持続的な影響を与える

インドネシア大学(UI)におけるサイバーセキュリティ教育システムの開発

CS教育カリキュラムを共同開発

- 一般的なサイバー攻撃とマルウェア
- JNSAとNISTのフレームワーク (Body of Knowledge)
- 経営層にサイバーセキュリティを意識させるには

等…

マルウェア解析ラボ運営方針の策定

- 組織構造
- 資産管理
- 人事セキュリティ
- 運用ルール

等…

大学講師養成講座



攻撃検知アプリMata-Elangの開発



デジタル開発通信省、モンゴル科学技術大学と行政アカデミーのCS人材育成合同PJ

インドネシアのプロジェクトの成果物を利用し、CS教育改善に協力

大学院向け

- インドネシアと同様の方法論でカリキュラムを開発
- インドネシアで開発済みの9科目をモンゴルの事情に合わせてローカライズ
- モンゴル独自のニーズに合わせて新規科目開発

学部向け

- C/Pが大学院向け教材の一部を流用して、現行カリキュラムを改善

Train-the-trainer (TTT) の例

TTTの参加者は、MDDC、NAoG、MUST-SICTと共同で選出した講師とエンジニア

①サイバーセキュリティ啓発科目

インドネシアで実施された、CS関連する2つのテーマ:「経営層にサイバーセキュリティを認識させる方法」と「一般従業員にサイバーセキュリティを認識させる方法」を取り上げる。

②コンピューター・フォレンジック科目

コンピューター・システムについて深い知識を必要とする実践的なトレーニング。

参加者の演習をサポートするため実習環境も整えた。



- ベトナム情報セキュリティ局(AIS)のサイバーセキュリティ能力強化協力において、教材の開発、ブランディングキット制作およびプラットフォームの開発などを実施

ベトナム国 サイバーセキュリティに関する能力向上プロジェクト

普及啓発教材開発

「子供のインターネット脅威からの保護(COP)」政策に関連する映像製作



「Staying vigilant with strangers in virtual space, especially on social media」
(3分、対象 11-14歳)



「Save the Children on Internet」
(3分、対象 6-10歳)



オンラインコンテスト宣伝動画

ブランディングキット

VN-COP Networkを子どもたちや保護者が簡単に認識できるよう、ブランディングキットを用意



- ブランドキットのコア部分：ロゴマーク、ウェブサイトテンプレート、ソーシャルメディア、スローガン、ユニフォーム
- ブランドキットのオフィス活用：証書、名刺、便箋、封筒、ファイルフォルダ、スライドテンプレート - ギフトセットデザイン：VN-COP Networkのロゴ入り記念メダル・バッジ、その他記念

VN-COP: ベトナム児童オンライン保護ネットワーク

ポータルサイト開発

現地企業と協力し、ポータルサイトを開発



URL: <https://vn-cop.vn/>

- 主要機能:
 - 1) 登録
 - 2) 法律文書公開
 - 3) 質問・問い合わせへの回答
 - 4) フィードバックと要望受付
 - 5) ニュースとイベント情報の公開
 - 6) ユーザー情報保護方針
 - 7) レポート

普及啓発専門家による活動

プロジェクトサイトと日本の啓発専門家をつなぐオンライン活動

ベトナムにおける現状と啓発計画の情報収集のためのインタビュー

日本の普及啓発活動に関する報告書作成

研修資料の作成

研修の実施

研修のフォローアップ

普及啓発方法に関してAISへアドバイスを提供

- 各国のサイバーセキュリティ対策強化を目的とした本邦研修には世界各国からの参加者が集まり、日本での滞在を通して文化体験も可能

サイバーセキュリティ対策強化のための国際法・政策能力向上

目的

サイバーセキュリティの規制や政策に携わる職員の能力開発し、サイバーセキュリティ規制・政策の立案及び実施がなされるよう、能力向上強化を図る

参加条件

情報セキュリティを担当する政府機関、または政府/国のCSIRT (Computer Security Incident Response Team)

単元目標

- インターネットガバナンスや情報の自由な流通などについて自国の政策を議論できる
- 日本と各国のサイバーセキュリティ政策と関連分野について基本知識を獲得し、自国と日本との違いを説明できる
- 帰国後もサイバー政策とセキュリティ対策の改善に向けた継続的な議論ができる

研修科目

- サイバー政策が社会・経済に及ぼす影響
- 国際法、規制、行動規範、インターネットガバナンス等に関する国際的な議論の動向
- 日本におけるサイバーセキュリティ政策・組織体制、人材育成等の現状と課題
- 日本のサイバーセキュリティに関する官民連携の現状と課題

等…

参加国(2023)

アルメニア、バルバドス、クック諸島、フィジー、インドネシア、イラク、エチオピア、ヨルダン、ラオス、マレーシア、モーリタニア、モルドバ、モンゴル、ナイジェリア、パキスタン、フィリピン、ルワンダ、タイ、東ティモール、トリニダード・トバゴ、ウクライナ、ジンバブエ

研修形態

- オンライン自習
- レクチャー
- 視察
- ワークショップ&ディスカッション
- プレゼンテーション



研修風景



株式会社ラックとそのセキュリティ監視・運用センターJSOC(ジェイソック)の視察



東京駅前で集合写真

事業実績



アジアを中心に技術協力事業を展開



免責: 本地図上の表記は図示目的であり、いずれの国及び地域における、法的地位、国境線及びその画定、並びに地理上の名称についても、JICAの見解を示すものではありません。



個別国向け技術協力

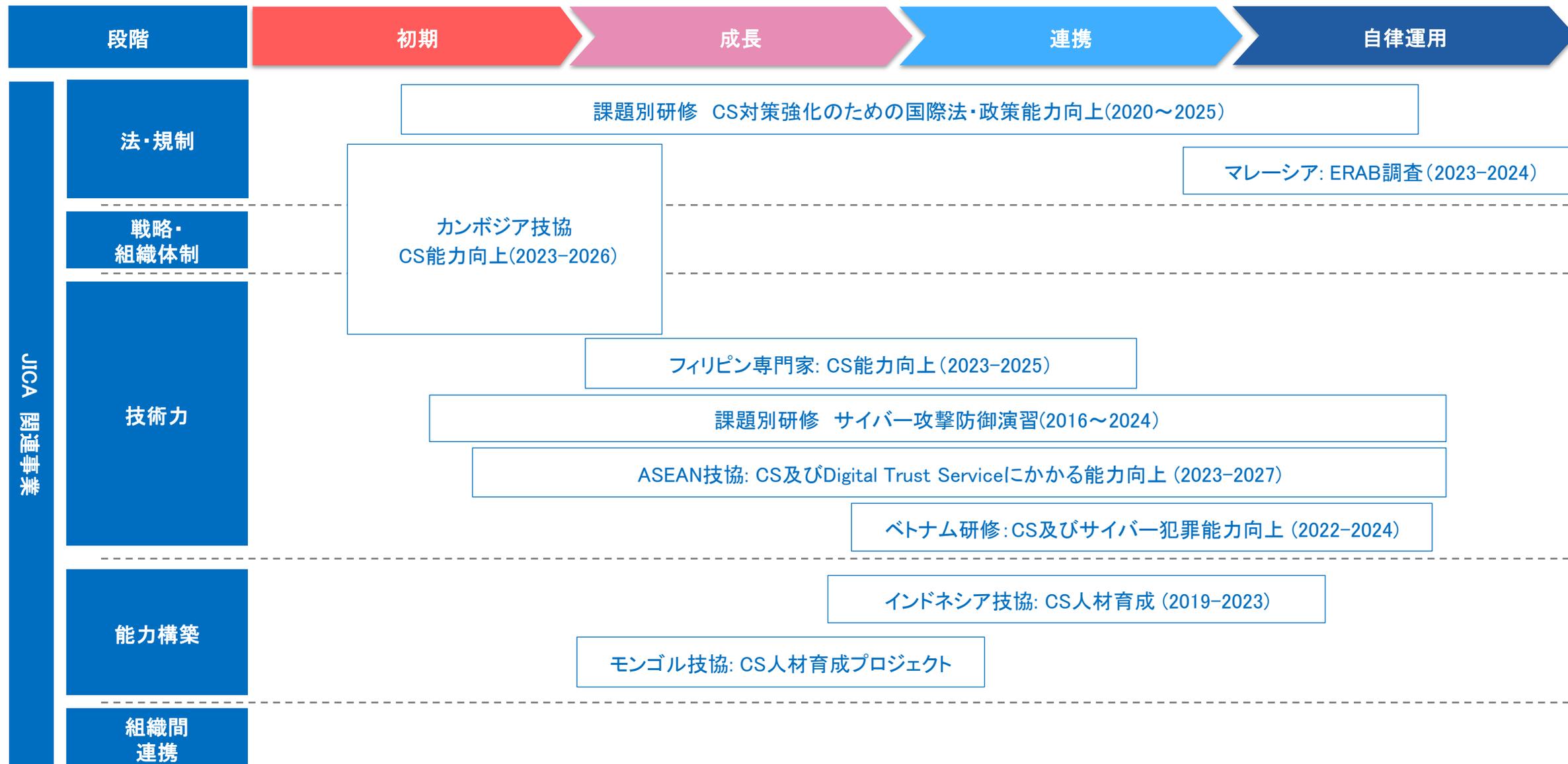
CS: Cyber Security

- ・インドネシア CS人材育成プロジェクト
- ・モンゴル CS人材育成プロジェクト
- ・ASEAN地域 CS及びDigital Trust Serviceにかかる能力向上
- ・カンボジア CS能力向上プロジェクト
- ・フィリピン CS能力向上
- ・マレーシア CS重要インフラ対応能力強化研修
(+慶応大学によるERAB提案調査)
- ・バングラデシュ CS人材育成研修
- ・モンゴル CS人材育成プロジェクト
- ・キルギス CS人材育成研修
- ・ウクライナ CS一般市民向け研修
- ・ベトナム サイバー犯罪対策強化

課題別研修

- ・サイバー攻撃防御演習
- ・CS対策強化のための国際法・政策能力向上
- ・サイバー犯罪対策強化

2023年度協力分野 分布



個別事業 事例



Period

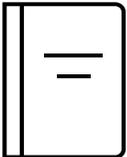
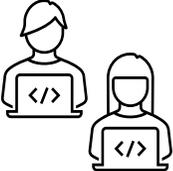
May 2019 to May 2025 (6 years)

Implementation Agency

University of Indonesia (UI)
Ministry of Communication and Information Technology

Outline and Activities

Outputs

- 
 - 最新かつ包括的なサイバーセキュリティのカリキュラムとシラバスを設計
 - 大学講師の養成
 - 各種短期トレーニングコースの開設
- 
 - 既存のオープンソースを活用したサイバーセキュリティ・ツールの研究
 - ローカライズ、開発されたツールの実装サポートの提供
- 
 - オープンコースウェアの開発
 - 開発したコースの一部公開
- 
 - 他国との戦略的なサイバーセキュリティ研修の実施
 - 国際／地域組織を通じてコースの成果の拡散

- 世界水準のサイバーセキュリティ・プロフェッショナル養成プログラムのインドネシア大学(修士課程)での実施
- オープンソースのサイバー・セキュリティ・ツールを現地化または開発
- サイバーセキュリティのオープンコースウェアを開発・公開
- 世界のサイバーセキュリティ関係者のネットワークを強化、コースへの参加者増加

Custom Courses @University of Indonesia

Course

How to make top managements aware of CS

How to make general employees aware of CS

Case Study & Practice: Malware analysis

Cybersecurity law and regulation

Case Study & Practice: Supply-chain risk

Case Study & Practice: How to make IT system forensic-enabled

Tabletop exercise for managers

Case Study & Practice: Cyber criminal investigation (TBD)

Comprehensive exercise: CSIRT

Comprehensive exercise: SOC (TBD)

Computer Forensic

Mobile device forensic

Cyber range (TBD)

Open Courseware (published)

Course

Introduction of NICE Framework SecBoK

Introduction of NIST Frameworks

Basic Computer and Network Architecture

Common Cyber Attacks and Malwares

Personal Data Protection Business Daily Operation

Personal Data Protection Law in Indonesia

Basic Information Security

[Open Courseware | IdCARE.UI](#)

CIO, CISO, IT dev. Head
(Course participants)



CEO, CFO etc.

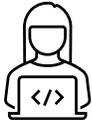
[Subjects | IdCARE.UI](#)

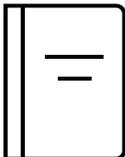
Period January 2023 to January 2027 (4 years)

Implementation Agency Ministry of Digital Development and Communications (MDDC)

Outline and Activities

Outputs

- 

 - モンゴルに必要な CS 人材を明確
 - MDDCの年次計画に沿った活動定義
- 
 - サイバーセキュリティエンジニア育成のための高度・網羅的なカリキュラムの開発
 - シラバス・教材の作成と教員訓練
 - カリキュラム改訂方法の確立
- 
 - 一般公務員向けの基礎的・網羅的なICT教育カリキュラムの開発
 - シラバス・教材の作成と教員訓練

- 産学官連携ネットワークの構築
- モンゴル科学技術大学におけるサイバーセキュリティ教育プログラム開発
- モンゴル行政アカデミーにおけるICT及びサイバーセキュリティ教育プログラム開発

Period

May 2023 to October 2026 (3.5 years)

Implementation Agency

Department of ICT Security
Ministry of Post and Tele-
Communications (MPTC)

Outline and Activities

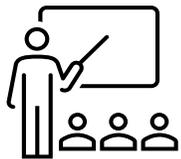
Outputs

1



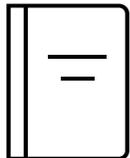
- サイバーセキュリティ成熟度評価
- CSIRTサービスの品質向上のために資料整備
- セキュリティ研修・訓練の実施

2



- 啓発資料の作成
- 子ども、女性、高齢者などの社会的弱者や関係機関への啓発活動の実施

3



- 机上調査や視察を通じた、国際標準や他国のサイバーセキュリティ政策・法律（戦略、フレームワーク、ロードマップ、標準を含む）の研究

1

サイバーセキュリティインシデント対応チーム（CSIRT）サービス提供能力の向上

2

CII事業者、一般市民などのステークホルダーに対するサイバーセキュリティに関する啓発活動の推進

3

サイバーセキュリティを強化するための法律、規制、基の特定

Period

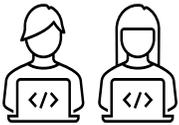
October 2023 to September 2025 (2 years)

Implementation Agency

Cybersecurity Bureau
Department of Information and Communications Technology (DICT)

Outline and Activities

1



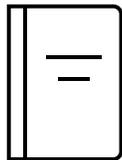
- 技術・インシデント対応に関する演習
- 訓練人材育成計画の提言

2



- セクター・コーディネーション計画への助言
- セミナー/ワークショップの実施

3



- 啓発・教育資料の作成支援
- 啓発活動の実施支援



Outputs

1

サイバーセキュリティ局の技術力向上

2

セクター間の調整能力が向上

3

サイバーセキュリティ啓発プログラムの充実

*There's a possibility of change in plan.

ASEAN地域におけるサイバーセキュリティと信頼されるデジタルサービスのためのサイバーセキュリティ専門家の能力と準備態勢を強化する。

Overview

Period

Mar. 2023 –
Feb. 2027

Target

ASEAN member states



Major Activities

01



- サイバーセキュリティ専門家のためのハンズオントレーニングの開催される(年6回)
- 例: CYDER演習、ネットワーク・フォレンジック、マルウェア解析、Trusted Digital Servicesコースなど

02



- Cyber SEA Game (ASEAN Youth Cybersecurity Technical Challenge)の開催
- 優勝者の日本招へい

03



- セミナー、ハンズオン、
- サイバーセキュリティ関連講座(第三者との共催)
- 研究活動

Please visit

[ASEAN-Japan Cybersecurity Capacity Building Centre \(ajccbc.org\)](http://ajccbc.org)

課題別研修では、開発途上国と日本、参加者が双方が互いに学び合い、共に成長・発展していくことを目的として実施。

Program

Outline

In 2023

サイバー攻撃防御
演習

- 政府機関/政府CSIRT/国家CERTのサイバーインシデント管理専門家が、インシデント対応能力を強化する。
- サイバーセキュリティ専門家同士のネットワークを構築する

- 7月2日～15日
- 主な参加国:カンボジア、インドネシア、マレーシア、ベトナム等
- 講義:大手サイバーセキュリティ企業によるインシデント対応実習

CS対策強化のための
国際法・政策能力向上

- 政府機関や政府・国家 CSIRT においてサイバーセキュリティ政策の立案・実施に携わる職員を対象に、サイバーセキュリティに関する国際法や政策形成に関する知見、理解の強化を行う。

- 8月20日～26日
- 主な参加国:カンボジア、インドネシア、マレーシア、フィリピン、タイ、ラオス等

開発途上国から未来のリーダーを日本に招き、修士号や博士号を取得する機会を提供

Outline

- 対象国のサイバーセキュリティ強化に貢献できる高度な人材を育成する
- 対象国と日本との中長期的な友好関係を構築・維持する

Target country

- インドネシア、ベトナム、バングラディシュ、カンボジア、タイ、モンゴル、フィリピン

University (Master and Doctoral Course)

- グロービス経営大学院
- 明治大学
- 会津大学
- 九州大学
- 芝浦工業大学

Expenses To Be Borne By JICA

- JICA will cover expenses and allowance to participants accepted to the program/course such as Tuition, Living Allowance, Airfare.

IC-AJCC
2023 | International Conference
on ASEAN-JAPAN
Cybersecurity Community

Collaboration for a Cyber-Safe ASEAN-Japan Community



• • • • • 5-6 OCTOBER 2023
• • • • • MEIJI KINENKAN - TOKYO - JAPAN



Hosted by National center of Incident readiness and Strategy for Cybersecurity(NISC), Cabinet Secretariat, Japan