JICA グローバル・アジェンダ　No.15

「デジタル化の促進」

クラスター事業戦略
「サイバーセキュリティ」

独立行政法人国際協力機構（JICA）は持続可能な開発目標（SDGs）を支援しています。

2022.12

1. クラスターの目的と概要

1.1. クラスターの目的

JICA グローバル・アジェンダ「デジタル化の促進」の下、本クラスターは、サイバー空間において深刻化しつつある脅威に対応し、人々の生活と尊厳を守ることのできる社会の実現（Cybersecurity for All）を目的とし、インド太平洋地域を中心とした途上国のサイバーセキュリティに関するレジリエンス向上のための能力構築の協力を推進する。

1.2. クラスターの概要

近年、デジタル化は人々の暮らしや産業活動へ浸透しており、デジタル社会・経済がもたらす恩恵が拡大する一方で、開発途上国においても、ランサムウェアによる被害、重要インフラ（エネルギー、金融、通信、保健等）の被害、サプライチェーン通じた機密情報漏洩、偽情報による社会的混乱、個人情報漏洩等が発生しており、サイバー攻撃による脅威も深刻化している。サイバー攻撃が多様化、高度化する中で、多くの開発途上国においては、サイバーセキュリティへの自国の対応体制・人材、国際連携等で対応が不足している。具体的には以下への対応が必要である。

- サイバーセキュリティは各国において総合的な対応が必要である。求められる対応能力として、①関連する法制度整備、②国としての戦略策定と推進体制、③脅威への対応技術、④官民の能力向上、⑤国内外組織との連携が重要である。実際、国際電気通信連合（International Telecommunication Union, ITU）が毎年発表している Global Cybersecurity Index（GCI）では、この5項目（「法・規制」・「戦略・組織体制」・「技術力」・「能力構築」・「組織間連携」）から各国のサイバーセキュリティ対策能力が評価されている。サイバー空間の脅威は常に変化し、完全に安全なサイバー空間を実現することは困難である中、これら項目を総合的に強化することで、各国が変化するサイバーリスクに自律的に対応できる能力を高める、すなわち、サイバー空間のレジリエンスを高めることが協力の目標となる。
- 同時に、サイバー空間は今や一国の対応だけで守れるものではなくなっており、自由で公正かつ地域の安全なサイバー空間構築を国と国とで協力して推進することで、国際社会の安定的な発展を実現する必要がある。日本もサイバー空間については、情報の自由な流通の確保を基本とする考え方の下、その考えを共有する国と連携し、既存の国際法の適用を前提とした国際的なルール作りに積極的に参画するとともに、開発途上国への能力構築支援を積極的に行うとしている。このため、インド太平洋地域を中心とした、経済社会の相互の繋がりの強い地域全体が連携してサイバーセキュリティに取り組むためのネットワークづくりも協力上、重要である。

以上を踏まえ、各国が常に変化するサイバーリスクに自律的に対応し、自国のデジタル社会の安全性を確保するために適切な対応が出来る状態（レジリエンスが高い状態）、及びインド太平洋を中心とした地域の連携体制と安定が強化される状態を目指すゴールとし、本クラスターを推進する。

SDGs へのデジタル化の貢献が期待されており、本クラスターはその過程で生じうる負の側面への対処に必要な取り組みである。（関連目標：4.教育、5.ジェンダー、7. エネルギー、8. 経済成長、9. イノベーション、11. 都市、16. 平和、17. パートナーシップ）

2. 開発課題の現状と開発協力のアプローチ

2.1. 開発課題の現状

デジタル化の進展に伴い、ヒト、モノ、カネ、行政機関を含めた組織やインフラシステムの多くがサイバー空間で繋がっている。その結果、サイバーセキュリティのリスクも甚大化しており、世界経済フォーラムが発行する Global Risks Report においても、2018 年、2019 年は「データの不正利用または窃盗」、「サイバー攻撃」の 2 点が「発生する可能性が高いグローバルリスク」の上位 5 位内に挙げられている。Global Risks Report 2022 においては、2 年以内の短期リスクの 7 位に、5 年以内の中期的リスクの 8 位に「サイバーセキュリティ対策の失敗」が含まれている。サイバー空間における攻撃手法は技術の進展に伴い高度化・多様化し続けており、サイバー攻撃を 100%未然に防ぐという完全に安全なサイバー空間は存在し得ない状況となっている。米国国立標準研究所（National Institute of Standards and Technology, NIST）」が 2014 年に発行したセキュリティフレームワーク[1]では、サイバーセキュリティ対策として、脅威の識別、防御、検知、対応、復旧のサイクルが定義されており、インシデントが発生することを前提に、国・組織・個人が多層的に取り組み、連携することにより、「サイバー空間のレジリエンスを高める」ことが求められている。

一方で、開発途上国各国ではサイバーセキュリティの対策体制・能力の不足と人材不足がリスクを増大させている。2019 年時点で世界のサイバーセキュリティ人材が 200 万人不足していると指摘されるなど、多くの組織・事業者において人材の確保に苦慮している[2]。

実際に開発途上国では深刻な被害が多発している。世界的に猛威を振るったランサムウェア（WannaCry, 2017 年）は多くの開発途上国を含む世界 150 か国以上で通信機器・PC 等のコンピュータ機器 23 万台以上に被害をもたらしたとされている。また、重要情報インフラ（Critical Information Infrastructure, CII）を狙ったサイバー攻撃が増えてきており、開発途上国においても、電力システムの停止（ウクライナ 2018 年、南アフリカ 2019 年）、国民情

[1] Cybersecurity Framework | NIST
[2] A.T. Kearney (2018) Cybersecurity in ASEAN: Urgent Call to Action

報の流出(エクアドル 2019 年)、保健サービスの停止(ボツワナ 2020 年)、中央銀行から不正送金(バングラデシュ 2016 年、ウガンダ 2020 年)等、国家安全にかかわる影響が発生する事例が発生している。開発途上国においてもデジタル社会推進と並行して、人々の日々の生活に密接に関係する CII 防護や、個人情報の不正利用等のデジタル社会推進による負影響を軽減するためのサイバーセキュリティ体制整備が重要となってきている。

このような状況の下、開発途上国におけるデジタル社会推進における各国のセーフガードとして、また、国を越えて被害を及ぼすサイバー空間の地域レベルの安全性強化のため、数多くの開発協力機関や政府が開発途上国におけるサイバーセキュリティ能力強化にかかる支援を行っている。

日本政府はダボス会議(2019 年)や G20 大阪サミット(2019 年)において、信頼性のある自由なデータ流通(Data Free Flow with Trust, DFFT[3])を打ち出し、サイバー空間における国際的に自由なデータ流通の促進を目指している。かかる考え方に加え、「サイバーセキュリティ戦略」[4](2021 年 9 月 28 日)においては、国際社会の平和・安定に加えて、我が国の安全保障への寄与という観点から、自由、公正かつ安全なサイバー空間を実現に積極的な貢献することとしている。これら政策の中で、開発途上国への支援として「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」(2021 年 12 月)が策定され、国際的なサイバーセキュリティ上の弱点を減らし、日本を含む世界全体へのリスクを低減する等の観点より、特にインド太平洋地域において、重要インフラ防護(Critical Infrastructure Protection, CIP)等を通じたサイバーハイジーン確保、サイバー犯罪対策、国際的ルール作り、及び信頼醸成措置推進、人材育成等に関する国際協力を進めることとしており、その中でJICAによる途上国への協力推進が明記されている。また、サイバー空間を介した攻撃等による機微な技術・データ等の流出、重要インフラへの被害発生等に加え、本邦の重要技術流出等についても現実的な脅威が増大しつつある点を踏まえ、経済安全保障の観点にも十分な留意が必要な状況となっている。

2.2. 本ペーパーにおけるサイバーセキュリティの範囲

本ペーパーにおけるサイバーセキュリティについては、一般サイバーセキュリティ(Civil Cybersecurity)の範囲を対象とし、各国の基幹となる行政機関、重要情報インフラ事業者を含む民間セクター、市民・個人の能力向上に資するサイバーセキュリティを対象として記述する。

サイバーセキュリティには、行政機関、民間、個人の情報リスクの対応のみならず、サイバー防衛・攻撃、ないしサイバー諜報、つまり敵対する国家への軍事行動やインテリジェンス活動に関する技術も存在するが、JICA は開発協力機関として非軍事的協力を原則としていることを踏まえ軍事行動や諜報を職掌とする組織に関する記述は含まれない。

[3] 100167362.pdf (mofa.go.jp)
[4] cs-senryaku2021.pdf (nisc.go.jp)

2.3. サイバーセキュリティ能力の要素

各国が、常に変化するサイバーリスクに自律的に対応できるレベルの能力を備えるためには、①関連する法制度の整備、②国としての戦略策定と推進体制の構築、③脅威への対応技術の向上、④官民の能力向上体制の整備、⑤国内外組織との連携と、様々な観点からサイバーセキュリティ能力の向上を図る必要がある。本ペーパーにおいては、国際電気通信連合（ITU）が毎年発表している Global Cybersecurity Index（GCI）を踏まえ、5 要素に分けて方針やアプローチを構成する。

A）法・規制（Legal measures）

社会と国民を保護し、安全なサイバー空間利用を促進するために、サイバーセキュリティやサイバー犯罪に対処する法的枠組みに基づく措置（立法、規制、履行を含む）を取ることを目的とする。

具体的には、サイバーセキュリティ機能を国家が有するための法的基盤（責任機関設置法など）や可能な行動を規定する法的基盤（情報の保護・規制等に関する法律など）を設定する。法規制の枠組みには、サイバー空間での違法行為を特定する法律の制定に加え、サイバー犯罪の取り締まりと含めた調査、起訴、施行するために必要な手続きツールの定義が含まれる。また、利害関係者のためのサイバーセキュリティに関する紛争解決の仕組みとコンプライアンスのメカニズムを確立することも含まれる。これら法的枠組みの検討に際しては、各国で独自の内容で制定するのではなく、基本的に地域・国際レベルでの慣習と整合させ、サイバー犯罪に対する国際的な協調を簡素化することに留意する必要がある。

具体的に設置すべき法・規制の例として、サイバーセキュリティ責任機関設置法、不正行為防止関連（不正アクセス/干渉防止、コンピュータ偽造防止）、個人情報保護法、ID・データ盗難関連法、データ漏洩等インシデント報告義務、サイバーセキュリティ監査要件、サイバーセキュリティ基準、CII 定義、オンライン人種差別防止関連法、オンライン・ハラスメント防止関連法、オンライン児童保護法などがあげられる。

B）戦略・組織体制（Organizational measures）

国家レベルでサイバーセキュリティ推進を実施するため、組織的な整備及び同組織による政策・戦略の立案に関する措置を取ることを目的とする。具体的には、サイバーセキュリティの目的・戦略・計画の策定、およびそれらの実装を確実にするための組織の役割、責任、および説明責任の正式な定義を設定する。戦略にはサイバーセキュリティ対策のロードマップ、CII の責任機関の特定なども含まれる。サイバーセキュリティ戦略を策定することで、責任所在と計画が明確になる。また、定期的にサイバーセキュリティ戦略を更新することで、サイバーリスクの変化に柔軟に対応できるようになる。

金融・電力・情報通信などの重要情報インフラは多くのサイバーセキュリティリスクに直面しており、影響の大きいインシデントの可能性とエスカレーションを減らすことを目的としたリスク管理の取り組みを進める必要がある。リスク管理は、サイバーセキュリティ介入に優先順位

を付け、進捗状況を追跡することできるようになるために、国レベルで評価するための指標を定義することが重要である。

C）技術力(Technical measures)

サイバーセキュリティを扱う機関や枠組みに基づく適切な技術的対応措置を取ることを目的とする。この取り組みは、インシデントを処理する国家機関、およびインシデントを監視、警告、対応するための国家的枠組みの下で実施される。特にインシデントに対応する組織である、コンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team, CSIRT）またはコンピュータ緊急対応チーム（Computer Emergency Response Team, CERT)が適切に運用されることで、各国は一元化されたコンタクトポイントを使用して国レベルでインシデントに対応し、迅速かつ体系的なアクションを促進することを通じて経験から学び、サイバーセキュリティの回復力(レジリエンス)を強化することができる。

国家 CSIRT は多くの場合、法律または国の政策に従って設置され、独立した政府機関の場合もあれば、特定の省庁または別の組織の傘下にある場合もある。国家 CSIRT は国内のサイバーセキュリティに対応する過程で、政府ネットワークの監視を広げ、並行して普及啓発活動を進めていく必要がある。さらに、地域あるいは世界的なセキュリティグループへの加盟を通して、国家 CSIRT としての機能が強化される。政府機関に対する CSIRT 機能が一定程度定着した後は、セクターCSIRT やセクターISAC（Information Sharing and Analysis Center)の設置および強化訓練を行い、国内の重要なすべてのセクター(政府含む)において、サイバー脅威の共有やインシデント対応を成熟させることが重要となる。

また、企業や国民が効率的に ICT を利用するためには、信頼とセキュリティが確保されたサイバー空間が必要である。したがって、各国は、A)法・規制や B)戦略・組織体制にて策定されたソフトウェアおよびシステムに対してのセキュリティ基準や方針を踏まえ、認定の仕組みを構築および実装するための技術的能力が必要である。

D） 能力構築(Capacity Development measures)

研究開発、教育、訓練、専門家育成、および能力開発を促進する公的機関による国内官民等の能力向上の措置を取ることを目的とする。能力構築には、一般国民への普及啓発活動、官民のサイバーセキュリティ専門家の育成と認定のためのフレームワーク設定、サイバーセキュリティの専門的なトレーニングコース提供、教育プログラムまたは学術カリキュラムの設置などが含まれる。

行政機関の能力強化にあたっては、各種省庁・公機関、地方自治体において、適切なセキュリティ措置を計画・実行し、インシデント発生時に対処できる能力を強化する必要がある。

重要インフラ・民間向けには、回復力のある重要情報インフラを構築し、持続可能な産業化とイノベーションを促進するために、各組織のサイバーセキュリティ能力開発のためのプロセス、スキル、リソース、研究開発を強化することが必要である。 このとき、技術問題だけではなく、ビジネスの効率化とパフォーマンスを改善するための視点を持ってサイバーセキュリテ

ィを捉える必要がある。

一般国民や各組織の専門家以外の人員への普及啓発の観点では、サイバーセキュリティ文化の醸成を伴う意識向上活動が広く実施されることが必要となる。さらに、特定層（高齢者、若年層、少数民族等）への普及啓発も進め、全国民がサイバーリスクを認識できるようになることで国家としてのサイバーセキュリティを高めることへつながる。

E） 組織間連携（Cooperative measures）

サイバーセキュリティに関わる組織間のパートナーシップ、協力枠組み、情報共有ネットワーク等を構築する措置を取ることを目的とする。サイバーセキュリティは国境を越えて共通で取り組むべき課題であり、国内外の連携が不可欠となる。国際機関、国家機関および民間企業とのより強固な協力により、強力なサイバーセキュリティ機能の実現が可能になり、サイバーリスクを軽減することに繋がる。

取り組みの順序としてはボーダレスなサイバーリスクに対応するために、二国間連携・多国間連携からはじめる。国際的な協力により、サイバー脅威やインシデントの情報が広く共有されることとなる。外国政府や国際機関との連携の進展とともに、民間との連携を進めることが重要である。外国あるいは国内のサイバーセキュリティ企業と政府が協力することで、研究開発の促進、セキュリティ市場の活性が生じて、サイバーセキュリティエコシステムが機能するようになる。組織間連携を進めることで、国内の官民および国際的なサイバーセキュリティ強化へ貢献することになり、それが当該国のサイバーセキュリティのさらなる強化へとつながる。

2.4. 参照する指標

国際電気通信連合（ITU）が毎年発表している Global Cybersecurity Index（GCI）では、一般サイバーセキュリティ（Civil Cybersecurity）に特化して、各国のサイバーセキュリティに対する取組みを多面的に評価している。具体的には、前述の「法・規制（Legal）」・「戦略・組織体制（Organizational）」・「技術力（Technical）」・「能力構築（Capacity Development）」・「組織間連携（Cooperative）」の 5 つの観点での評価項目を設定し、網羅的に測定しており、全世界（193 か国（2020 年））を対象に 2014 年以降継続的に評価結果が毎年更新されている。

なお、各国のサイバーセキュリティを評価する指標は、GCI の他にも、Oxford 大学が開発した Cybersecurity Capacity Maturity Model for Nations（CCMM）、International Institute for Strategic Studies（IISS）が発表した Cyber Capabilities & National Power Rankings や、e-Governance Academy（eGA）が発表した National Cyber Security Index（NCSI）等複数存在 する。しかし、他指標は軍事面でサイバーセキュリティを重点的に評価する項目として含んでいるもの、一部の国・地域・産業に特化したもの、継続して評価結果が実施されていないもの、となり、一般サイバーセキュリティに関する継続的なモニタリングに適さない。

本クラスターでは、GCI スコアをベースに各国のサイバーセキュリティの対応能力を4ステージに分けて評価、能力の強化状況を把握する。一方で、GCI スコアは各要素の合成指標であり、

協力が真に成果を上げているかを把握するために、協力した要素の能力向上度合いについて、個別の定量指標、定性指標を設定しモニタリング・評価する。

2.5. 開発課題へのアプローチ

サイバーセキュリティにおいては「100%安全なサイバー空間」というゴールは存在し得ない。そのため、本クラスターで目指すべき到達点とは、「各国が常に変化するサイバーリスクに自律的に対応し、自力で自国のデジタル経済の安全性を確保するために適切な活動が出来る状態」となる。そのため、GCI の 5 項目をバランスよく、それぞれのステージで必要な取り組みを推進すること、強化することが重要となる。

また、経済レベルが上昇に応じたサイバー空間の情報量および通信量の増加や、各国が置かれた地政学的な状況によっても、サイバーセキュリティへの優先度が異なるため、各国への協力を検討する際には、その両面を踏まえ、協力すべき対象領域・内容を特定する。

その上で、協力対象国への協力の前後で GCI 及び定量・定性指標（協力領域の能力等等）を比較することにより、能力強化の進捗を測り、各国が常に変化するサイバーリスクに自律的に対応できる能力に至るステップを協力していく。

2.6. サイバーセキュリティ支援の国際的な動向

サイバーセキュリティの強化のため、様々な国から多岐にわたる協力が行われている。Global Forum on Cyber Expertise（GFCE）が運営するサイバーセキュリティに関するポータルサイト（Cybil ）においては、サイバーセキュリティに関連する案件概要や開発されたツール情報等が公開されており、約 800（2022 年 6 月時点）の活動が登録されている。

現時点での地域的な傾向としては、アフリカ地域は世界銀行に加え、EU や欧州諸国、アジア地域は ITU 等国際機関や日本、太平洋諸国はオーストラリアや APNIC、中南米はアメリカ及び関係機関による支援が多い傾向にある。各国開発機関や政府機関は各々の政策・戦略的重点国に対して、各国のリソースや方針に応じた支援を実施する一方で、現状では必ずしも連携が十分に図られているわけではなく、相互の活動補完やシナジーの検討等は十分な検討がなされていないように思われる。

ア） 国際電気通信連合（ITU）

国際電気通信連合（ITU）は GCI の評価・公開を行うと共に、主に GCI スコアが低い国を中心に能力強化支援を展開している。具体的には国際機関や開発機関と協力し、国家サイバーセキュリティ戦略策定（戦略・組織体制）、国家 CSIRT 設立のための事前評価（戦略・組織体制）、国家 CSIRT 成熟度評価（技術力）、GCI セミナー・サイバードリル（能力強化）、啓発マテリアルの開発・ローカライズ等を実施している。

イ） 世界銀行

サイバーセキュリティ主流化、知見・ツール展開、パートナーシップの3点を中心に進めてお

り、2020 年には、アフリカ・中東、カリブ海地域を対象とした約 6 件のサイバーセキュリティ支援を含む事業を開始した。また、知見ツール展開においては、デジタル関連事業におけるサイバーセキュリティ支援項目を含めた活動を実施している。パートナーシップでは、サイバーセキュリティマルチドナー基金（日本が拠出）の設立に加え、各種国際セミナー開催等を実施している。

ウ） FIRST（Forum of Incident Response and Security Teams）

世界中の CSIRT が相互の情報交換やインシデント対応に関する協力関係を構築する目的で設立されたフォーラムであり、年次会合に加え、最新のセキュリティ関連技術についてのチュートリアルや講演を多数実施している。

他に、地域等を限定した APCERT（Asia Pacific Computer Emergency Response Team）、AfricaCERT（Africa Computer Emergency Response Team）、OIC-CERT（Organization of The Islamic Cooperation – Computer Emergency Response Teams）等がある。

エ） APNIC（Asia Pacific Network Information Centre）

アジア太平洋地域を対象として、インターネットリソース管理を行う非営利団体であるが、アジア、大洋州諸国を対象に国家 CSIRT 設立にかかる技術支援を実施している。

オ）韓国

Korea Internet & Security Agency（KISA）を通じ、Cybersecurity Alliance Mutual Progress Network（CAMP）を運営。62 組織、47 か国が加盟しており、年次総会等を通じた情報交換や各種研修やセミナーを実施している。

カ）シンガポール

ASEAN Singapore Cybersecurity Centre of Excellence（ASCCE）を 2018 年に立ち上げ、ASEAN 諸国向けにサイバーセキュリティに関わる政策・規制等をテーマとした研修やセミナーを提供している。（JICA も 2022 年に1コース実施）

キ）日本

内閣サイバーセキュリティセンター（NISC）が司令塔となり、NISC、総務省、経済産業省等により主に ASEAN 諸国向けに、活動を実施している。NISC は、日 ASEAN サイバーセキュリティ政策会議の運営に加え、各種演習、ワークショップの実施等を実施しており、総務省は日・ASEAN ISP（Internet Service Provider）向け情報セキュリティワークショップ、APT（Advanced Persistent Threats）サイバーセキュリティ技術研修等を実施している。経済産業省は、インド太平洋地域向けの日米 EU 産業制御システムサイバーウィーク実施に加え、JPCERT/CC を通じたインターネット定点観測システムの提供等を行っている。

JICA は日本政府の方針を踏まえつつ、協力対象国のニーズに合わせた組織強化・人材育

成を中心とした協力を行っている。特に国家 CSIRT を中心とした技術的対応能力の向上、人材育成体制の強化に関する技術協力を核としている。

3. クラスターのシナリオとその根拠

3.1. クラスターのシナリオ

開発途上国においてもデジタル化が急速に進む中、サイバーセキュリティの重要性が高まりつつあるが、大多数の国において社会的な対応能力が十分とは言えない状況にある。その要因は、開発課題としての歴史が浅く社会全体での理解、認識が深まっていないこと、常に変化し多岐にわたるサイバー空間の脅威に対する体制強化と能力開発の継続が容易ではないことなどが挙げられる。

JICAのこれまでの協力対象国における事業経験、GCIの変化等を踏まえ、本クラスターでは、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実現するに至るためのパスとして、各国は「初期ステージ（Initial）」、「成長ステージ（Growing）」、「連携ステージ（Networking）」、「自律運用ステージ（Self-sustaining）」の4段階を辿るものと設定した。サイバーセキュリティについて開発途上各国と協力を行う際には、当該国がどの段階にあるかを見極めた上で、各段階に応じた最適な協力のアプローチを検討し実施する。

ア）初期ステージ（Initial Stage）

この段階では、サイバーセキュリティを所掌する専門機関が存在しないか、存在しても人員配置や予算が限定的である。専門機関がない中、関連省庁の課ないしはグループにより小規模な基礎的対応は行われているが、サイバーセキュリティ対応能力は極めて限定的で、サイバー攻撃や被害が発生していても把握できない状況にある。また、同国の状況に関する情報が周辺先進諸国と十分に共有されておらず、同国が地域の「セキュリティホール」となり得る状態にある。

政府内の関係部門においてサイバー攻撃の被害の重大性についての認識が深まり、国家コンピュータセキュリティインシデント対応チーム（CSRIT）などの体制整備や人材育成についての必要性が認知される。また、体制面ではサイバーセキュリティ所掌機関の体制と戦略の検討が行われる。それに連動して、周辺各国の状況の把握や法令面の課題の整理も行われる。

イ）成長ステージ（Growing Stage）

核となる中央政府機関の対応能力を中心として、社会のサイバーセキュリティ対応能力が持続的に高まっていく段階。

成長ステージにある国においては、サイバーセキュリティに対する政府内の認識が全般

的に向上すると共に、国家 CSRIT が技術力（セキュリティ対応能力）を徐々に高め、政府機関を対象とする啓発と人材育成の活動も拡大する。また、不正行為に対処する法規制が定められ、サイバーセキュリティに対応する専門機関が設立され、関連政府機関間の連携や人員のスキル強化についても予算が拡大する。

このような政府内の取り組みを踏まえ、一般企業や国民のレベルでもサイバー攻撃について認識が深まっていく。一部の企業が独自に対応を始めるが、政府による重要情報インフラ（CII）のサイバーセキュリティに関する方針等の整備や民間部門に対する施策の具体化が進んでおらず、リスクが依然として高い状態にあることが想定される。当該国が地域のセキュリティホールとなることを懸念する周辺先進国の働きかけ等により多国間枠組みへの参加や国際的企業との協力が徐々に進む。

ウ）連携ステージ（Networking Stage）

中央政府機関の取り組みに加えて、重要情報インフラ（CII）のあるセクターを中心とした民間部門や他公的機関においてサイバーセキュリティへの対応が拡大・深化する段階。

CII の制定や民間部門の対策を促す法令の整備が進み、関連する啓発活動が強化される。社会的な認識が一層深まり、政府予算も増大、公的機関と民間部門の双方において取り組みが促進される。国内のサイバーセキュリティ人材の需要が増大し、高等教育機関等での人材育成プログラムが拡充されると共に、国家CSIRTの役割も拡大し、サイバーセキュリティ戦略の進化、分野 CSIRT の立ち上げが進み、その中で専門機関が技術力と体制を高度化していく。政府機関間、官民間で連携も深化し、周辺国内での組織間連携による全体のセキュリティ強化のための活動も積極的に行われる。

エ）自律運用ステージ（Self-sustaining Stage）

サイバー空間に繋がる人々を守るための社会的な体制が広く整い、レジリエンスが高まる段階。

個人やマイノリティに配慮した対策など幅広い視点でサイバーセキュリティ対策が進む。新たな脅威に対応するため、自律的かつ適時に戦略と体制の見直しが行われ、技術力の向上が図られる。サイバーセキュリティに関連する国内産業を振興するための施策も実施される。また、サイバーセキュリティ先進国として周辺国とのパートナーシップをリードし、他国への技術支援なども行う。

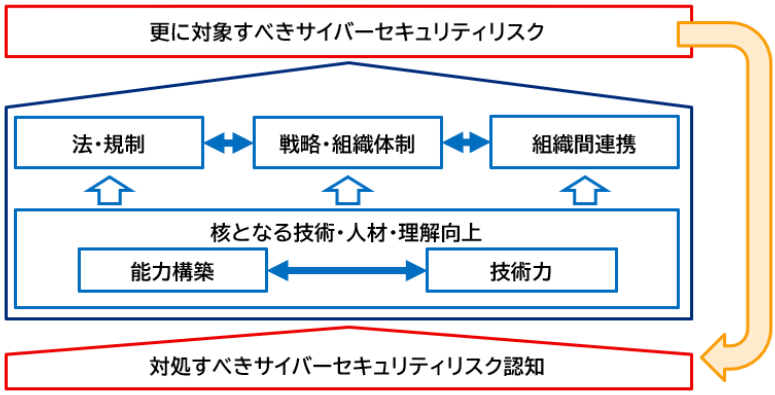
常に変化するサイバーリスクや顕在化する脅威に対して、社会のサイバーセキュリティ対応力が持続的に高まり、自国および地域のデジタル経済の安全性を確保するために必要な活動が自律的に強化される好循環が形成される。

3.2. シナリオの根拠

本クラスターの標準的なシナリオの根拠として、国際電気通信連合（ITU）の Global

Cybersecurity Index(GCI)でも用いられている Global Cybersecurity Agenda[5]モデルを用いる。同モデルは、①法・規制、②戦略・組織体制、③脅威に対応する技術力、④官民の能力構築、⑤国内外の組織間連携の5つの観点をサイバーセキュリティの重要な要素として定義しており、各観点における変化が同時に進むことにより、サイバーリスクに自律的に対応する社会の能力、すなわち、サイバー空間のレジリエンスが高まると想定する。

各要素は相互に連携しており、想定されうるケースとしては、当該時点で認識されているサイバーセキュリティリスクに対し、技術・人材及びリスク啓発が一定程度推進されると、法・規制、戦略・組織体制の整備、組織間連携の深化が進み、更に高度な技術、広範な人材育成、サイバーセキュリティ認知向上が求められるサイクルが続くことが考えられる。5つの観点が相互に関連しながらバランスよく高度化するにつれ、サイバーセキュリティのリスク及び重要性に対する社会的な認識が深まり、それが、更に各々の観点での状態の変化を促し、国・地域としてのレジリエンスが段階的に強化されていくと想定する。

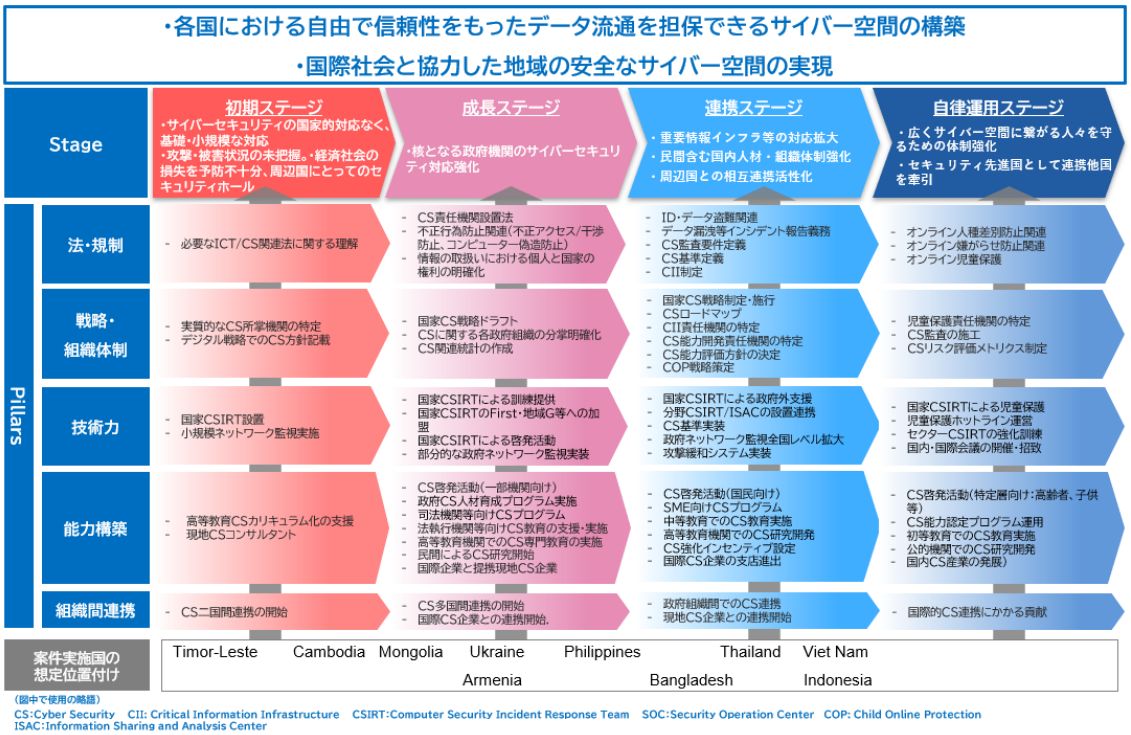


出展:JICA作成

以上の5つの観点について、4段階のシナリオの各ステージの標準的な到達点(マイルストーン)を図3. 2に示す。あくまで標準として整理したものであり、例えば、全体として成長ステージにあると判断される国の一部の課題が連携ステージや初期ステージの状態にあることもあり得る。

[5] Global Cybersecurity Agenda (GCA) (itu.int)

図 3.2 サイバーセキュリティ発展シナリオ(全体)



出展: JICA 作成

【5 つの観点における各ステージで目指す状態】

ア) 法・規制(Legal)

① 初期段階においては、今後対応すべき法規制の理解促進と対応すべき事項が整理されている。

② 成長段階においては、国家として不正行為を対処・規制する主体、法規制を定めることに加え、サイバーセキュリティに対応する専門機関設立が行われる。

③ 連携段階においては、政府(政府電子サービス等)や重要セクター、民間部門における適切な保護、対策が促されている。

④ 自律運用段階においては、広くサイバー空間に繋がる人々を保護するための法規制の整備が行われている。

イ) 戦略・組織体制(Organizational)

① 初期段階においては、サイバーセキュリティ推進するための戦略の構想や組織体制が検討されている。

② 成長段階においては、 サイバーセキュリティ戦略の策定に加え、実施体制の構築として、関連政府機関との役割明確化と連携が図られている。

③ 連携段階においては、重要セクターを含めた戦略の深化及び能力開発・業界団体等との所掌の明確化が行われている。

④ 自律運用段階においては、広くサイバー空間に繋がる人々への対応を進めるための対

応組織や評価体制が構築されている。

ウ）技術力（Technical）

① 初期段階においては、サイバー攻撃や被害の把握、予防に向けた基礎的な体制が構築されている。
② 成長段階においては、核となる政府機関・国家 CSIRT のサイバーセキュリティ対応能力が整備されている。
③ 連携段階においては、公的機関及び重要セクターのサイバーセキュリティ対応強化、分野 CSIRT の立ち上げが行われている。
④ 自律運用段階においては、広くサイバー空間に繋がる人々へのサイバーセキュリティ対応支援が実施され、新たな脅威への対応力が備わっている。

エ）能力構築（Capacity Development）

① 初期段階においては、国内人材育成の状況と課題が分析されている。
②成長段階においては、政府機関を中心とした人材育成及び啓発活動が実施されている。
③ 連携段階においては、重要セクターや民間企業を含めたサイバーセキュリティ対応を進めるための人材育成プログラム、啓発活動、インセンティブ展開が行われている。
④ 自律運用段階においては、全国民のサイバーセキュリティの理解向上を図るための対応や関連する国内産業の振興が行われている。

オ）組織間連携（Cooperative）

① 初期段階では、情報収集・協力を中心とした各国との初期的な連携が行われている。
② 成長段階においては、既設のサイバーセキュリティに関する多国間枠組みへの参加や国際的企業との協力が進められている。
③ 連携段階においては、国内の強靭性向上のため、政府機関間・民間部門との連携を進められている。
④ 自律段階においては、地域的なサイバーセキュリティ対応強化に向けた貢献が行われている。

4. クラスター展開の基本方針

4.1. シナリオ展開の基本方針

JICA は、DFFTを掲げる日本政府の方針を念頭に置きつつ、インド太平洋地域を中心に協力対象国および地域全体において、変化し続ける脅威に対するレジリエントで自律的なサイバーセキュリティが構築されるよう支援する。

具体的には、2030 年をターゲットとして、協力対象国が現状から「成長ステージ（Growing）」、「連携ステージ（Networking）」、「自律ステージ（Self-sustaining）」とより上位のステージに到達できるよう、3. で述べたシナリオに基づき、能力強化に向けた協力を実施する。

ア）重点対象地域

「自由で開かれたインド太平洋（FOIP）」の観点から、特に我が国との経済面での関係が強く越境データ流通が活発で、安全保障上重要な東南アジア・南アジア地域を重点とする。大洋州、アフリカ、中南米等についても各国のニーズに加え、当該分野の体制や他国・国際機関の活動にも留意しつつ協力を検討する。

なお、協力の検討にあたっては、情報の扱いに関する政府の方針等を理解の上、基本的人権に対する配慮、法の支配・ガバナンス、民主化といった当該国の状況にも留意する。

イ）協力対象機関

原則として、非軍事組織を協力対象とする。サイバーセキュリティ関連政策や戦略の策定、協力対象組織においては、軍事・諜報にかかる機能が含まれる場合があるため、協力内容については慎重に検討を行う。

ウ）協力展開計画

日本と経済・社会的繋がり、及び、各国のサイバーセキュリティ対応能力を踏まえた協力展開を検討する。

a）東南アジアのサイバー推進国

自律運用ステージ到達を目指した協力の検討を行う。

サイバーセキュリティが進んでいる国のおいても項目によって強化するべき内容が存在するため、相手国側の政策的優先順位も考慮しつつ内容を検討する。

b）東南アジアのサイバー後発国、南アジア、東・中央アジアを中心とした協力実施国

連携ステージ到達を目指した協力の検討を行う。

なお、協力時点で初期ステージにある国においては、特にJICAが協力可能な領域において成長ステージを目指すものとする。

c）大洋州等における初期ステージにある協力対象国

先方の体制に留意しつつ、成長ステージ到達を目指した協力の検討を行う。また、同志国・他国際機関による活動との連携も検討する。

d）上記以外の地域・国

研修・セミナー等を通じた基礎的な協力を実施する。また、同志国・他国際機関により活

動との連携も検討する。

エ）項目毎の協力内容

相手国の状況を踏まえ、JICAとして有効な協力が可能な分野を設定する。具体的なJICA による項目毎の協力方針は下記の通り。

a）法・規制（Legal）

サイバーセキュリティを所掌する機関指定、サイバーセキュリティ関連規制法、不正・犯罪防止、個人情報、重要情報インフラ等に関する法・規制の制定を経て、広く国民にとって安全で安心なサイバー空間を築くための法制度環境が整備された状態を目指す。

サイバーセキュリティに関する法・規制については各国の法・規制状況を深く把握した上で、各国の事情や国家方針に即した内容での検討を行う必要がある。また、承認行為には相手国側のプロセスに長い時間がかかることが多い。

上記を踏まえ、JICA は、法・規制に関する全体像の把握や検討促進に資する協力として、日本やサイバーセキュリティ先進国、あるいは既に協力を行った地域・国の法・規制を踏まえた調査・提言、講義、ワークショップ等を行う。また、これら協力を通して CS 法・規制に関する情報収集・研究を進め、今後、協力内容の拡充にも取り組む。

b）戦略・組織体制（Organizational）

サイバーセキュリティ国家方針の制定から、ロードマップ制定、所掌機関の明確化、評価体制の構築等を経て、広く国民にとって安全で安心なサイバー空間を築くための体制が整備された状態を目指す。

サイバーセキュリティ戦略の策定、組織立ち上げ等については、各国の状況、国家方針に大きく左右され、日本での経験が最適解とならないケースが多い。また、サイバーセキュリティ戦略においては、軍事・諜報に関する方針が含められることもあり、JICA による協力に合わないケースも想定される点は留意する。

上記を踏まえ、JICA は、戦略・組織体制に関する全体像の把握や検討促進に資する協力として、日本やサイバーセキュリティ先進国、あるいは既に協力を行った地域・国の法・規制を踏まえた調査・提言、講義、ワークショップ等を行うことで相手国の検討に資する情報をインプットすることを中心とする。これらの協力で知見を蓄積して、本項目での協力内容の拡充にも取り組む。

c）技術力（Technical）

サイバーセキュリティ対策を中心的に牽引する国家 CSIRT の能力強化から、政府機関、特定産業への対策強化、サイバーセキュリティ基準実装等を経て、広く国民にとって安全なサイバー空間を守るための技術的対応が整っている状態を目指す。

主に国家CSIRTを中心とした、政府機関のサイバーセキュリティ対応に求められるサービス開発、能力強化に資する協力を行う。既にJICAにて複数国での実績を有する領域で

あり、過去協力の成果、協力リソースを積極的に活用する。

ただし、特に初期段階の国等においては、相手国リソース（人員体制、予算配布）が不十分な状況であることが多く、協力を受け入れるための体制が不足しているケースもあるため、先方の状況に応じた、適切な投入量、内容を検討する。

技術的・人員的・予算的な体制が一定程度整っている組織においては、モニタリング能力向上等に資する機材供与（資金協力）の検討も視野にいれて検討する。

d）能力構築（Capacity Development）

サイバーセキュリティ教育、啓発や研究機関等の範囲の拡大、国内サイバーセキュリティ産業の強化等を経て、広く国民にとって安全で安心なサイバー空間を築くための人材が安定的に供給されている状態を目指す。

既にJICAにて複数国での実績を有する領域であり、過去協力の成果、協力リソースを積極的に活用する。本項目はサイバーセキュリティ教育、公務員向け訓練、啓発実施等多岐の領域にわたり、異なる機関が各々所掌しているケースも多い。そのため、相手国の責任機関及び、各項目におけるカウンターパート（C／P）側の所掌を適切に見極めた上で協力を検討する。実施機関として大学等も候補となり、JICA が行う高等教育機関への協力との連携にも留意する。

また、研究開発等の体制が一定程度整っている組織においては、人材育成・研究開発等に資する機材供与（資金協力）の検討も視野にいれて検討する。

e）組織間連携（Cooperative）

国家間連携の範囲拡大、官民連携の拡大等を経て、安全で安心なサイバー空間を築くための国際発信、情報共有が出来る状態を目指す。

サイバーセキュリティに関する国際的連携枠組みが出来ており、各国の主管省庁や国際機関による協力推進が行われている領域である。JICAにおいては、全世界・地域向け集合研修や広域協力等を通して日本と地域の関係諸国との連携強化、ネットワークづくりに貢献することを中心とする。

オ）ステージ毎の協力方針

a）初期ステージ（Initial Stage）

これらの国においては、このステージをいち早く脱し、国家としての組織的な対応に取り組む成長ステージへの移行を支援する。一方、サイバーセキュリティを所掌する職員等も限定的であることが多く、課題別研修や対象を絞った技術協力等を通じた基礎的な知識、他国事例の提供を実施する。

b）成長ステージ（Growing Stage）

本ステージを満足することが各国のサイバーセキュリティ対策の標準的な目標であり、国

内外の連携ステージに発展するために不可欠なステージである。本ステージ協力対象国に対しては、技術協力プロジェクト等を通じた核となる行政機関を中心として国家の組織的な取り組み体制強化について、サイバーセキュリティ対策の能力向上を実施する。

c）連携ステージ（Networking Stage）

本ステージは、特に国内における産官学連携を拡充と共に、地域内・日本とのパートナーシップを図っていくための能力を備える、連携強化を図る段階となる。東南アジアのサイバー先発国を中心に、技術協力プロジェクト、第三国研修等を通じ、官学連携体制の構築、国民への啓発に必要な能力向上を実施する。

d）自律運用ステージ（Self-sustaining Stage）

本ステージでは、共に地域でリーダーシップを発揮してもらうために必要な協力をピンポイントで実施する。また、日本と当該国とのネットワーキングや協働した他国支援を一層強化する。

4.2. 資金協力、技術協力、研修（本邦・第三国）等の事業スキームの活用方法

4.1 に記載の項目毎の協力方針に沿って JICA の事業スキーム活用を行う。

ア）資金協力

サイバーセキュリティ強化に必要な機材は維持管理に際しては最低限の知識にくわえ、24 時間体制での活用には人員体制の充足も重要。また、一般的に耐用年数が短く、ライセンス料、保守料が高額になるものが多い。そのため、協力国において、技術的・人員的・予算的な体制が一定程度整っていることが確認された場合においては、技術力（Technical）、能力構築（Capacity Development）の能力向上に資する設備、機材の整備を検討する。

イ）技術協力

サイバーセキュリティ協力の重点国においては二国間技術協力の実施を積極的に検討する。対象領域は協力対象国の現状を踏まえ、優先項目を設置する。また、過去協力の成果、協力リソースの積極的活用を検討する。

ウ）第三国研修

日本や先進国の事例だけでなく、近似する他国の取組等が参考になるケースも多い。ASEAN 地域を中心とし周辺国も含めた第三国研修の実施を通じ、協力国間の連携も促進する。

エ）本邦研修

課題別研修としては、広く協力の要望がある「法・規制（Legal）、戦略・組織体制

（Organizational）」を中心とした研修、及び「技術力（Technical）」を中心とした研修の二種類の研修を基本研修として実施する。上記以外の特定の要望については、技術協力、第三国研修での対応を優先するが、事業予算、政策的背景等により上記によらない場合は個別のテーラーメード型研修を検討する。

4.3. インパクトの最大化・最終アウトカム発現に向けた取組

2.5 に記載の通り、サイバーセキュリティに関する協力は各国の数多くの機関にて行われているものの、相互の連携は限定的となっている。JICA は①日本国内関係機関との途上国協力に関する政策面での密な連携と協力リソース面での協力、②マルチ・バイ機関とは得意分野の相互補完と連携を推進する。また、③開発途上国との関係では先発する途上国での経験・知見、リソースを他国支援に活かすこと、途上国間の連携の場を通じたネットワーク強化を促進する。以上を通してコレクティブ・インパクトの発現を目指す。

ア）国内関係機関との連携

内閣サイバーセキュリティセンター（NISC）、外務省、総務省、経産省、JPCERT/CC、情報処理推進機構（IPA）といった政府・関係機関と協働し、政策面での連携や協力リソースとしての協力参画を推進する。また、民間部門の安全で円滑な環境づくりに向けて、金融 ISAC 等の国内業界団体や民間企業との協力も促進する。

特に、日 ASEAN サイバーセキュリティ政策会合等、日本政府が行う地域的な枠組みを通じて協力成果の拡大が見込める場合は、積極的な貢献を検討する。

イ）先進国機関・国際機関との相互補完・連携

特に JICA による協力の範囲が限定的となる、「法・規制」、「戦略・組織体制」の領域においては、国際協力機関（世界銀行、ITU、APNIC）等が協力を行っている。協力国のニーズを踏まえ、他国際機関のリソースの活用、動員を図ることで、CS 能力全体の向上に資する協力を検討する。「組織間連携」においても、FIRST等の非政府組織による多国間連携の枠組みや地域協定等が存在することを踏まえ、必要に応じた仲介を行う。また、5 項目のその他の事項においても、先進的な国や開発協力機関との関係深化を進め、相互連携を通じた協力拡大を可能とするためのネットワーク強化を図っていく。

ウ）途上国の過去の成果・リソースの活用、国際連携の拡大

過去の技術協力での成果物として、東南アジアを中心に育成してきたコア人材を他国の協力においても協力・連携することで、成果の拡大をはかる。

エ）協力受入国の間での連携促進

各国の状況や方針では、日本の事例、情報が必ずしも参考とならないこともある。そのため、研修やプロジェクト間の連携等によって、類似した状況の国の知見を共有することで、

より相手国の状況にあった協力とすることも検討する。ただし、協力を検討するにあたっては、日本政府の方針との乖離が無いように留意する。

上記を行うにあたり、サイバーセキュリティ協力に参加した研修員やカウンターパート等、JICA の協力を起点としたネットワークを強化するとともに、これを触媒とした相互のサイバーセキュリティ連携の後押しにも繋げる。

オ）民間企業との連携

本領域は各国政府の機微な情報を扱う可能性のある内容となるため、現時点では民間企業との連携が限定的。民間企業の動員が可能な領域についての検討を継続して行い、連携を検討する。

5. クラスターの目標とモニタリング枠組

5.1. GCIスコアに基づく目標管理

各国のサイバーセキュリティの対応力の評価については、ITU の Global Cybersecurity Index（GCI）が国際標準として広く用いられている。それを踏まえ、本クラスターの目標管理も主に CGI を参考として実施する。

本クラスター戦略のシナリオにおける各ステージ（3.1参照）と想定されるGCIのスコアレンジの対照表は表 5.1.1のとおり。

GCI では、総合スコアの 100 となり、5つの観点の各項目のスコア（最大20）の合計値となっている。なお、各ステージのスコアはモニタリングのための目安のスコアとなり、必要に応じて、JICA 事業を通じて、あるいは他機関と連携しつつ、より詳細かつ定性的に協力対象国のサイバーセキュリティ能力の状況と変化を把握し、当該国がどのステージ位置しているか判断する。

各ステージにおいて具体的に目指すアウトカムについては、表5.1.2の内容が想定されるが、下記参考事例の通り、各国の状況は多様であるため案件計画時に策定する。

表5.1.1 GCIスコアとステージ

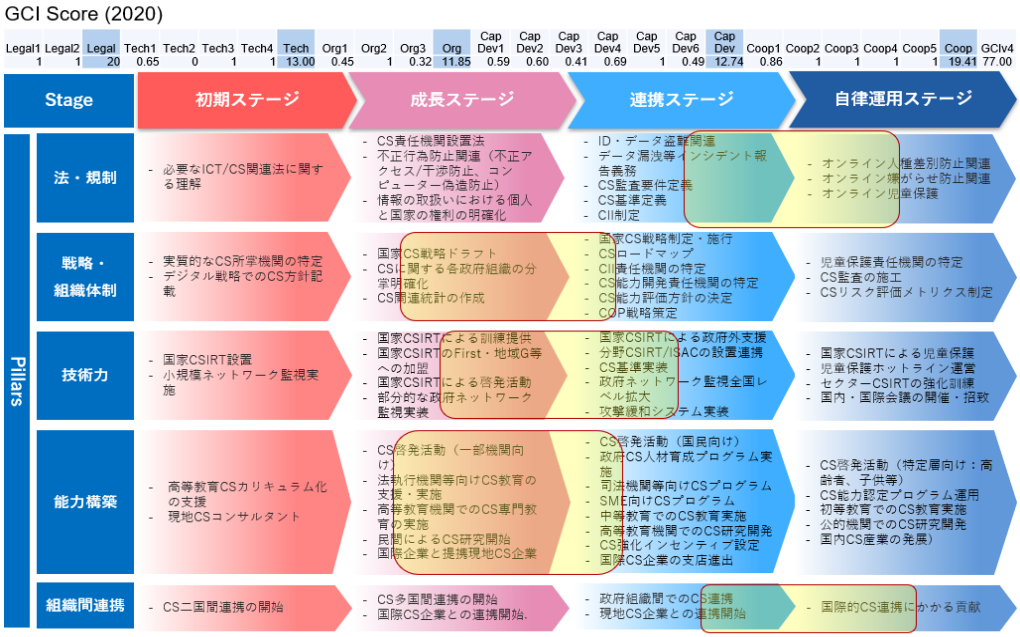
（2021 年度分布）	初期 ステージ *（50か国）*	成長 ステージ *（34か国）*	連携 ステージ *（26 か国）*	自律運用 ステージ *（22か国）*
総合スコア	**約 0-30**	**約 30-80**	**約 80-95**	**約 95-100**
法・規制	約 0-6	約 6-16	約 16-19	約 19-20
戦略・組織体制				

技術力				
能力構築				
組織間連携				

【参考事例】

以下はある開発途上国の事例である。当該国の総合スコアは 77 であり、成長ステージにあると言える。一方、5項目のうち法・規制、組織間連携においては、スコア上は既に自立運用ステージに達している。

このように、各国の総合的なステージと個々の5項目の各々ステージは異なることがあるため、協力に際しては5項目の中で重点を置く項目を定め、対象国の経済・社会環境や政策上の優先順位等に応じてサイバーセキュリティの能力を強化できるよう支援していく。



出展：JICA 作成

表5. 1.2 各ステージで目指すアウトカム

ステージ	【初期ステージ】(GCI30 点未満) ・サイバーセキュリティの対応を開始しているものの、国家的対応が行われておらず、基礎・小規模な対応。 ・サイバー攻撃や被害が発生しているかが十分に把握できない。将来に向けた予防が十分でない。 ・周辺国にとって、同国が対処困難なセキュリティホールとなり得る。	【成長ステージ】(GCI30～80点程度) ・核となる政府機関のサイバーセキュリティ対応が進む。 ・重要情報インフラ、民間、個人等の対応にまで至らないため、依然リスクが高い。 ・周辺国にとって、同国がセキュリティホールとなる懸念が依然存在。	【連携ステージ】(GCI80～95点程度) ・政府機関に加えて、重要情報インフラ等の重要セクターへの対応へと活動範囲を拡大していく。 ・公的機関に加え、民間も含めた国内人材育成や啓発活動もより広範囲となり、必要となるスキルや人員、組織体制が飛躍的に増加。 ・周辺国との相互連携を通じたセキュリティ強化のための活動が活性化。	【自律運用ステージ】(GCI95 点以上) ・広くサイバー空間に繋がる人々を守るための体制が整いつつある。 ・一方で、常に新たな脅威に対応する必要があり、適時の体制強化や戦略見直し、スキル向上、人材育成、国際連携の改善が求められる。 ・セキュリティ先進国として周辺国や他国との連携のパートナーシップを牽引していける。
以下、期待されるアウトカム				
①法・規制	●法規制で対応すべき事目が理解されている。具体的に以下の対応が図られている。 ・必要な ICT/CS 関連法に関する理解の向上	●不正行為を対処・規制する検討主体、法規制が定められる。具体的に以下の対応が図られている。 ・不正行為防止関連(不正アクセス/干渉防止、コンピュータ偽造防止) ・個人情報保護 ・CS 責任機関設置法 ・情報の取扱いにおける個人と国家の権利の明確化	●政府電子サービスや重要セクターを適切に保護するための法規制が定められる。具体的に以下の対応が図られている。 ・ID・データ盗難関連 ・データ漏洩等インシデント報告義務 ・CS 監査要件定義 ・CS 基準定義 ・CII 制定	●広くサイバー空間に繋がる人々を保護するための法規制が定められる。具体的に以下の対応が図られている。 ・オンライン人種差別防止関連 ・オンライン嫌がらせ防止関連 ・オンライン児童保護
②戦略・組織体制	●CS 対応を進める組織を明確化させる検討・準備が行われる。具体的に以下の対応が図られている。 ・(実質)CS 所掌機関の特定 ・デジタル戦略での CS 方針記載	●CS 対応を進めるにあたり行政関連組織の役割と連携が明確化される。具体的に以下の対応が図られている。 ・国家 CS 戦略ドラフト ・CS に関する各政府組織の分掌明確化 ・CS 関連統計の作成	●重要セクター等の民間部門に広げた対応を進めるにあたり、戦略や所掌が明確化される。具体的に以下の対応が図られている。 ・国家 CS 戦略制定・施行 ・CS ロードマップ ・CII 責任機関の特定 ・CS 能力開発責任機関の特定 ・CS 能力評価方針の決定 ・COP 戦略策定	●広くサイバー空間に繋がる人々への CS 対応を進めるにあたり、責任機関や評価体制が構築される。具体的に以下の対応が図られている。 ・児童保護責任機関の特定 ・CS 監査の施工 ・CS リスク評価メトリクス制定
③技術力	●サイバー攻撃や被害の把握、予防に向けた基礎的な技術専門機関の体制が構築されている。具体的に以下の対応が図られている。 ・国家 CSIRT 設置 ・小規模ネットワーク監視実施	●技術専門機関から核となる政府機関の CS 技術力強化が行われている。具体的に以下の対応が図られている。 ・国家 CSIRT による訓練提供 ・国家 CSIRT の First・地域 G 加盟 ・国家 CSIRT による啓発活動 ・部分的な政府ネットワーク監視実装	●技術専門機関から重要セクターの CS 技術力強化が行われている。具体的に以下の対応が図られている。 ・国家 CSIRT による政府外支援 ・分野 CSIRT/ISAC の設置、連携 ・CS 基準実装 ・政府ネットワーク監視全国レベル拡大 ・攻撃緩和システム実装	●技術専門機関から広くサイバー空間に繋がる人々への CS 対応支援が行われている。具体的に以下の対応が図られている。 ・国家 CSIRT による児童保護対応 ・児童保護ホットライン運営 ・セクターCSIRT の強化訓練 ・国内・国際会議の開催・招致
④能力構築	●国内の CS 人材育成が進められている。具体的に以下の対応が図られている。 ・高等教育 CS カリキュラム化の支援 ・現地 CS コンサルタントの育成	●核となる政府関連機関を中心に CS 人材及び CS 認知が進んでいる。具体的に以下の対応が図られている。 ・CS 啓発活動(一部機関向け) ・政府 CS 人材育成プログラム実施 ・司法機関等向け CS プログラム ・法執行機関等向け CS 教育支援 ・高等教育機関での CS 教育実施 ・民間による CS 研究開始 ・国際企業と提携現地 CS 企業	●民間の広くに CS 人材及び CS 認知が進んでいる。具体的に以下の対応が図られている。 ・CS 啓発活動(国民向け) ・SME 向け CS プログラム ・中等教育での CS 教育実施 ・高等教育機関での CS 研究開発 ・CS 強化インセンティブ設定 ・国際 CS 企業の支店進出	●全国民の CS 理解向上が図られ、常に新たな脅威に対応する強靭性を確保するための人材、理解が十分。具体的に以下の対応が図られている。 ・CS 啓発活動(特定層向け:高齢者、子供等) ・CS 能力認定プログラム運用 ・初等教育での CS 教育実施 ・公的機関での CS 研究開発 ・国内 CS 産業の発展
⑤組織間連携	●政府による必要な情報収集・協力が着手されている。具体的に以下の対応が図られている。 ・CS 二国間連携の開始	●政府による国際的な協力や情報交換が進展する。具体的に以下の対応が図られている。 ・CS 多国間連携の開始 ・国際 CS 企業との連携開始	●国内の政府機関や重要セクターの CS 対応の連携がされている。具体的に以下の対応が図られている。 ・国内政府組織間での CS 連携 ・現地 CS 企業との連携開始	●地域全体の CS 強化に向けた貢献・発信がされている。具体的に以下の対応が図られている。 ・国際的 CS 連携にかかる貢献

【留意事項】

ア）サイバーセキュリティ能力に関する国内の地域格差

GCI は、中央政府レベルで関連する取り組みがある場合は評価・加点されるシステムとなっている。

しかしながら、主要都市では対策が進んでいるものの、地方都市では未だ対策が不十分という国も多く存在する。そのため、GCI の総合スコアおよび全5項目のスコアが自律運用段階にある国であっても、一部の項目については成長ステージ、連携ステージに求められる取り組みが十分でない地域が存在するケースもあり、留意が必要である。

イ）各項目の取り組み内容の変化

上記シナリオは、直近の GCI における質問項目を参考にして設定している。サイバーセキュリティにおけるトレンドは年々変化しており、それに応じて GCI における5項目に関する質問内容（＝重視される事項）も見直しがなされている。従って、上記シナリオも CS トレンドの変化に応じ、改訂していくものとする。

表5.1.3（参考）質問項目の変遷

Category	2020	2018	2017	2014
Legal	1. Cybercrime substantive law 2. Cybersecurity regulation	1. Cybercrime law 2. Cybersecurity regulation 3. Containment/curbing of spam	1. Cybercrime legislation 2. Cybersecurity regulation 3. Cybersecurity training	1. Cybercrime legislation 2. Regulation and compliance
Technical	1. National/Government CIRT/CSIRT/CERT 2. Sectoral CIRT/CSIRT/CERT 3. National framework for implementation of cybersecurity standards 4. Child online protection	1. CERT/CIRT/CSIRT 2. Standards implementation framework 3. Standardization body 4. Technical mechanisms and capabilities (spam) 5. Use of cloud 6. Child online protection	1. National CIRT 2. Government CIRT 3. Sectoral CIRT 4. Standards for organizations 5. Standard and certification 6. Child online protection	1. CERT/CIRT/CSIRT 2. Standards implementation framework 3. Certification
Organizational	1. National cybersecurity strategy 2. Responsible agency 3. Cybersecurity metrics	1. National cybersecurity strategy 2. Responsible agency 3. Cybersecurity metrics	1. Cybersecurity strategy 2. Responsible agency 3. Cybersecurity metrics	1. Policy 2. Roadmap for governance 3. Responsible agency 4. National benchmarking
Capacity Development	1. Public cybersecurity awareness campaigns 2. Training for cybersecurity professionals 3. National educational program and academic curriculum 4. Research and development programs 5. National cybersecurity industry 6. Government incentive mechanisms	1. Public awareness campaigns 2. Framework for certification and accreditation 3. Professional training courses 4. Educational program or academic curriculum 4. Cybersecurity research and development programs 5. Incentive mechanisms	1. Standardization body 2. Good practices 3. R&D programs 4. Public awareness campaigns 5. Professional training courses 6. National educational program and academic curriculum 7. Incentive mechanisms 8. Home-grown industry	1. Standardization development 2. Manpower development 3. Professional certification 4. Agency certification
Cooperative	1. Bilateral agreements 2. Government participation in international mechanisms 3. Multilateral agreements 4. Public private partnership 5. Inter-agency partnerships	1. Bilateral agreements 2. Multilateral agreements 3. Participation in international associations 4. Public private partnership 5. Inter-agency partnerships 6. Best practices	1. Intra-state cooperation 2. Multilateral agreements 3. International for a participation 4. Public private partnership 5. Inter-agency partnerships	1. Intra-state cooperation 2. intra-agency cooperation 3. Public private partnership 4. International cooperation

出展：公開 GCI レポートより JICA 作成

5.2. クラスターの目標

ア）最終目標・最終アウトカム

経済・社会活動のデジタル化が人々の暮らしに大きな影響を及ぼす中、各国が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を構築することを目指す。同時にインド太平洋地域を中心に、国際社会と協力して地域の安全なサイバー空間を実現する。

なお、下記①②③の具体的な対象国は、今後の協力対象国を踏まえて決定する。

① 東南アジアのサイバー先行国における協力対象国が「自律運用ステージ」に到達する。
【2030年度までに総合 GCI スコアが95ポイント相当以上、または5項目の能力要素が19～20ポイント相当となり、「自律運用ステージ」を達成】

② 東南アジアのサイバー後発国、南アジア、東・中央アジアを中心とした協力対象国が「連携ステージ」に到達する。
【2030年度までに総合 GCI スコアが80ポイント相当以上、または協力対象項目の能力要素が16～19ポイント相当以上となり、「連携ステージ」を達成】

③ 主に大洋州、アフリカ等における初期ステージにある協力対象国が「成長ステージ」に到達する。
【2030年度までに GCI スコアが少なくとも30ポイント相当以上、または協力対象項目の能力要素が6～16ポイント相当以上となり、「成長ステージ」以上を達成】

イ）中間目標・中間アウトカム

- 各国のサイバーセキュリティ対応レベルの上昇
  【15 か国において、2026 年までに協力対象能力要素の GCI スコアの向上、対象国のサイバーセキュリティ能力評価の向上（定性評価）】

ウ）直接目標・直接アウトカム

- 対象項目における能力の向上
  【協力対象国のローカルシナリオを踏まえた対象能力要素の能力向上（定量・定性評価）】
  （5.3. ア）の「各項目の評価指標」を中心に案件毎に設定）
- JICA サイバーセキュリティ協力ネットワークの拡大
  【日本やサイバーセキュリティ先進国、あるいは既に協力を行った地域・国での研修・プロジェクト等の協力事業に 2026 年度までに 30 か国以上参加、2030 年度までに 50 か国以上参加】

5.3. モニタリングの枠組み

協力対象国毎にローカルシナリオを設定した上で、モニタリング指標（定量）の設定を行うと共に定性的な能力向上の評価を行う。想定される主な指標、情報の収集体制は下記の通り。

加えて、3. 2に記載のシナリオを補強するためのエビデンス情報の収集も並行して行う。

ア) モニタリング指標

	モニタリング指標 （2030 年時点）	指標の定義と入手手段
代表定量指標(全協力案件を対象)		
1	(全世界対象) ● GCI スコア ● GCI ランキング	GCIレポートより取得
2	サイバーセキュリティ・コア人材の育成数	以下をクラスター事務局にて集計 ● 課題別研修、技プロ、第三国研修、JICA-VAN 遠隔研修等によるサイバーセキュリティ協力プログラムの参加国 ● 上記の研修受講者数
3	間接裨益者	以下をクラスター事務局にて集計 ● 協力国と行うセミナーへの参加者数 ● 啓発プログラムの対象裨益者(対象組織や人口等からの推計を含む) ● 開発教育マテリアル開発、指導者育を通じた、最終受講者数(対象コースの受講者数等からの推計を含む)
4	サイバーセキュリティ協力ネットワーク	以下をクラスター事務局にて集計 ● 協力対象国 ● サイバーセキュリティ協力人材実績 ● 国際開発機関等との連携数
各項目の評価指標 （案件毎に対象とする項目を選定）		
5	(法・規制 分野支援国) ● CS 関連法の制定状況・更新状況 ➢ 法規制に関するセミナー等の参加人数 ➢ セミナー等の理解度	以下のような公開情報から取得 ● CS 担当省庁のホームページ ➢ プロジェクト情報より取得
6	(戦略・組織体制 分野支援国) ● CS 戦略・マスタープランの制定状況 ● 戦略・計画の更新状況 ➢ 戦略に関するセミナー等の参加人数	以下のような公開情報から取得 ➢ CS 担当省庁のホームページ ➢ プロジェクト情報より取得

	➢ セミナー等の理解度	
7	(技術力 分野支援国) ● 国家 CSIRT の継続性(例:予算、設置根拠) ● 国家 CSIRT のサービス内容(例:FIRST CSIRT Service Framework と比較したサービスの種類)と実績 ● 民間企業 CSIRT、セクター CSIRT の立ち上げ数、運用内容 ● サイバーセキュリティ業界団体の提供サービス内容と実績 ● セクターCSIRT／ISAC 設置数、運用状況 ● 国家 CSIRT が提供する CSIRT サービス範囲の数 ● 国家 CSIRT が監視する政府機関・CII 事業者等の数 ● インシデント検知数、対応数 ➢ 研修等の参加人数 ➢ 研修等の理解度 ➢ 国内・国際会議の開催・招致・参加回数	以下のような公開情報から取得 ● 国家 CSIRT 発行のインシデントレポート・活動レポート(例:年報)・RFC2350 ● セクターCSIRT 発行のインシデントレポート・活動レポート ● サイバーセキュリティ業界団体の調査レポート(例:年報) ● 国家 CSIRT の公開情報 ➢ プロジェクト情報より取得
8	(能力構築 分野支援国) ● 教育機関での CS カリキュラム開発状況 ● 教育機関での CS カリキュラム導入状況 ● CS 啓発活動の公的機関による実施回数・内容 ● CS 分野の研究開発における実施研究機関数、研究内容、国際的な認知状況 ● 特定分野向け(例:法執行機関、中小企業)の CS 教育実施状況 ➢ 研修等の参加人数 ➢ 研修等の理解度 ➢ 普及啓発活動の種類と数 ➢ 普及啓発活動に参加した人数 ➢ 教育プログラムに参加した人数	以下のような公開情報から取得 ● 主要 IT 系大学のカリキュラム(高等教育)、教育省の学習指導要領に相当する資料(初中等教育) ● サイバーセキュリティ業界団体の調査レポート ➢ プロジェクト情報より取得

	➢ 教育プログラムにおける成績 ➢ 大学卒業生の数 ➢ オープンソース教育プログラムの数	
9	（組織間連携　分野支援国） ● 国際的な CS 協力枠組みへの参加状況（例：FIRST、APCERT、OIC-CERT、CS 犯罪に関する条約等） ● CS 企業誘致・設立促進状況 ➢ 組織間連携に関するセミナー等の参加人数 ➢ セミナー等の理解度 ➢ 国内・国際会議の開催・招致・参加回数 ➢ CS 二国間連携の数 ➢ CS 多国間連携の数	以下のような公開情報から取得 ● 国家 CSIRT の活動レポート ● 各国際枠組みの加盟国リスト ● CS 担当省庁の Homepage、活動レポート ● 事前調査ヒアリング ➢ プロジェクト情報より取得

イ）モニタリングの実施方法

クラスター事務局を組成し、国際指標や、プロジェクトの成果指標の収集、分析、ローカルシナリオとの整合性の確認、各国のステージ判定を行う。

定性評価に際しても、学術的また実務的な観点から、適切な評価手法の検討を継続して行う。

5.4. SDGsへの貢献

SDGs の全目標においてデジタル技術の活用が期待されており、本クラスターによる取り組みはデジタル化に伴って発生する負の側面やリスクに対するセーフガードとなる。特に、デジタル指向が高い分野としては以下 SDGs 目標が挙げられる。（Integrating Cyber Capacity into the Digital Development Agenda, GFCE November 2021 他）

ゴール 4　　質の高い教育をみんなに
ゴール 5　　ジェンダー平等を実現しよう
ゴール 7　　エネルギーをみんなにそしてクリーンに
ゴール 8　　働きがいも経済成長も
ゴール 9　　産業と技術革新の基盤をつくろう
ゴール 11　　住み続けられるまちづくりを
ゴール 16　　平和と公正をすべての人に
ゴール 17　　パートナーシップで目標を達成しよう

以上