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

（令　和　３　年　１２　月　１４　日
サイバーセキュリティ戦略本部決定）

１　基本認識

（１）サイバーセキュリティ分野における能力構築支援について、国家安全保障戦略（平成25年12月閣議決定）では、「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。」ことが定められている。また、開発協力大綱（平成27年２月閣議決定）では、重点課題である「普遍的価値の共有、平和で安全な社会の実現」のための施策の一つとして、サイバー空間に関わる開発途上国の能力強化が挙げられている。また、デジタル社会の実現に向けた改革の基本方針（令和２年12月閣議決定）では、デジタル社会を形成するための基本原則に「サイバーセキュリティ対策で安全性を強化すること」と掲げられるとともに、国際的な協調と貢献を積極的に行うことが定められている。

また、G7が伊勢志摩サミットにおいて発出した「サイバーに関するG7の原則と行動」（平成28年５月）において、G7首脳は、サイバー空間における安全及び安定を促進するため、能力構築を含めた協力を強化していくことに努めることが確認されている。また、サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG）の報告書（令和３年３月）において、「更なる国際連携の促進、能力構築支援が実施されること」が勧告されるとともに、サイバーセキュリティに関する国連政府専門家会合（GGE）によるサイバー空間における責任ある国家の行動に関する報告書（令和３年７月）においても、「すべての国が国際平和及び安全保障に貢献できることを保証するため、国際協力及び能力構築支援を更に強化すること」が必要とされている。

さらに、サイバーセキュリティ戦略（令和３年９月閣議決定）では、デジタル経済が浸透し、「自由、公正かつ安全なサイバー空間」を確保することの重要性がこれまで以上に増す中、国際協力・連携の一層の強化が必要とされ、サイバーセキュリティに関する能力構築支援について、「他国においても様々な支援が実施されている中、我が国の基本的な理念の下、同志国、世界銀行等の国際機関、産学といった多様な主体と連携して重層的に、かつオールジャパンで戦略的・効率的な支援を実施していく。」ことが定められたところである。

（２）こうした支援は、我が国にとって次のような重要性を有する。

①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させる。

②支援対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保する。

③情報の自由な流通や法の支配を基本原則とする日本の立場への理解を対象国に

浸透させる。
④日本の情報通信産業等の現地展開を進める上での基盤を形成し得る。
⑤インフラ輸出戦略や自由で開かれたインド太平洋等の政府方針の強化に寄与し得る。

（3）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は、多くの省庁によって実施されているが、厳しい財政事情の中、オールジャパンで戦略的・効率的支援を行い、支援の効果を極大化するために、関係省庁間の連携はもとより、官民による連携の緊密化がますます重要となっている。

さらに、欧米諸国からインド太平洋地域への注目が高まる中、世界的な新型コロナウイルスの感染拡大により、当該地域に対して各国から官民問わずオンラインでの能力構築支援の提供機会が増加している。我が国においてもテレワーク環境の急速な普及を好機と捉え、官民の多様な専門家が場所にとらわれず柔軟に能力構築支援を行える環境を整備し、開発途上国の多様なニーズに応じて、求められる支援を同志国、世界銀行等の国際機関、産学といった多様な主体と連携して、効果的に支援できる体制を整えることが重要となっている。

2 支援の在り方

サイバーセキュリティ分野における能力構築支援は、（1）重要インフラ防護等を通したサイバーハイジーンの確保支援と、（2）サイバー犯罪対策支援、（3）サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有、（4）人材育成等横断的な領域に大別される。但し、支援対象となる開発途上国それぞれの同分野での制度・態勢等の整備状況は千差万別であり、サイバー空間における新たな脅威や各国のニーズを特定した上で、日本の強みを活かす形で支援を行う必要がある。

また、これらの取組について、特に同盟国たる米国を始めとする同志国との間では、引き続き可能な範囲で情報交換、政策協調を図り、支援の重複を避けるのみならず、相乗効果も追求し、より効率的・効果的な支援となるよう留意する。

（1）重要インフラ防護等を通したサイバーハイジーンの確保支援

これまでASEAN諸国を中心に主に政府機関向けの支援がなされてきたところであり、今後も政府機関向け支援を継続しつつ、その関係を基盤として、各国におけるインフラ整備等の進展に伴って対策支援ニーズが高まりつつある重要インフラ向けの支援を強化する。

さらに、これまでのASEAN地域における能力構築支援の成果と経験を基に、インド太平洋地域における支援対象の拡大を図る。

（ア）ASEAN地域

ASEAN 諸国の政府機関向けには、日 ASEAN サイバーセキュリティ政策会議、日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）、（独）情報処理推進機構の産業サイバーセキュリティセンター（ICSCoE）等の取組を通じて、同志国とも連携しつつ、十数年にわたる継続的な支援により、良好な信頼関係を構築している。特に、AJCCBC

に関しては、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等のオンライン化や研修メニューの拡充等を図りつつ、近年その取組を強化している。加えて、経済産業省及び ICSCoE が米欧との協力の下、ASEAN 諸国を含めたインド太平洋地域向けの産業制御システムサイバーセキュリティ演習を実施しており、インド太平洋地域におけるサプライチェーン全体のサイバーセキュリティ能力向上及び各国との連携強化を図っている。

また、国際協力機構（JICA）では、各国固有の課題に対して、インドネシア、ベトナム等で国別の支援が開始された。特に、2019 年開始のインドネシアにおける技術協力プロジェクトでは、現地大学と連携し、重要インフラ事業者向けの人材育成支援が行われるなど、政府間の枠組みを超えた産官学連携による能力構築支援が進められている。

近年は、 ASEAN各国の政府能力向上及び経済発展に伴うインフラ整備、デジタル化の進展に伴い、民間分野を含む重要インフラ分野向けの対策支援の重要性が高まりつつあり、また、ASEAN域内でも国によってサイバーセキュリティ能力に差が広がりつつある。

このような状況を踏まえ、今後は、相対的に能力の向上が進んだ国に対しては、相手国側の企業育成及びインフラ分野等で強みを有する我が国の事業者も含めた官民連携による重要インフラ分野等への対策支援を強化することが重要である。

その際、政府に求められる役割としては、各国政府と協調しつつ、現地のサイバーセキュリティ政策を後押しする形で、民間事業者の取組を促すことであり、民間活動による持続的な対策を進めるためには、民間事業者の自由な経営判断に沿う形での支援検討となることに留意する必要がある。

さらに、このような取組を効果的に進めるためには、官民連携の下、ASEAN等地域におけるサイバーセキュリティニーズを把握し、オールジャパンによる最適な対策を提供できる枠組みを整備しつつ進める必要がある。

また、相対的に能力向上の余地が残されている国・地域に対しては、相対的に進んだ国やASEAN域外の同志国とも連携しつつ、日メコン協力や「東ASEAN成長地域（BIMP-EAGA）＋日本」の枠組等も活用し、引き続き政府機関向けの能力構築を支援することが必要となる。

これらの点に留意しつつ、AJCCBCに関しては、今後の活動の強化に向けて、同志国等の第三者との連携を図るとともに、ASEAN諸国による自立的な演習の実施を可能とするための研修メニューの一層の拡充、ASEAN諸国の要望を踏まえた活動の多様化等を推進する。同時に、昨今、欧米諸国等によるASEAN地域を一括りとした支援の枠組みが増えつつある中で、JICA等による能力に応じた国別の支援の必要性が高まっており、今後も継続的に支援を強化する。

（イ）ASEAN以外の地域

これまでのASEAN諸国向け支援において培った経験及びASEAN諸国との関係を基盤とし、インド太平洋地域（アジア、 オセアニア等）を中心にASEAN以外の地域における支援を強化する。

当面は、例えばこれまで経済産業省とICSCoEが米欧と協力しながら実施してきたインド太平洋向け産業制御システムサイバーセキュリティ演習を引き続き実施するととも

に、JICA等による多様なニーズに応じた国別の政府機関等向け支援を実施する。

支援先の国の選定においては、我が国事業者等の活動状況、通信ネットワークの結節点等の地理的重要性、同志国や国際機関による支援状況等を考慮し、限られた予算で最大限の成果が見込める国に注力する。また、アフリカへの支援の可能性についても検討する。

（2）サイバー犯罪対策支援

個人・企業情報及び知的財産の窃取や、日常生活・経済活動に必要不可欠な基盤を提供する政府機関・事業者のシステムへの不正アクセスといった犯罪への対処能力・捜査能力を高めつつ、犯罪の発生自体を可能な限り抑止し、法の支配に基づく自由・公正・安全なサイバー空間を確保していくに当たり、途上国を含む国際社会との（特に法執行機関間の）連携が必須となっている。この点、サイバー犯罪対策関連法制度の整備や犯罪捜査手法に関する研修、国連薬物・犯罪事務所（UNODC）のサイバー犯罪対策技術援助プロジェクトへの出資、国連アジア極東犯罪防止研修所（UNAFEI）等とも連携した刑事司法関連研修等の具体的支援に加え、サイバー犯罪対策対話、サイバー犯罪条約締約国による関連会合といった枠組みも活用し、引き続き積極的に取り組むことが必要である。

（3）サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有

日本として、サイバー空間においても既存の国際法が適用されるとの考えの下、個別具体的な国際法の適用についての議論への関与等を通じ、サイバー空間における国際的なルール作りや規範の形成を主導していくことが必要であることから、そのような国際法の適用や国家の行動規範について、各国の能力構築支援を進める。

また、サイバー攻撃を発端とした不測の事態の発生をいかに防ぐか等につき、各国の認識を共有し、相互の意識啓発に努めると共に、国際的な連絡態勢を平素から構築し、信頼醸成を進めていくことが必要である。

そのため、サイバーセキュリティに関する意識啓発活動（ASEAN との意識啓発コンテンツの合作、留学生の意見交換等）や、二国間・多国間ワークショップやサイバー対話の実施といった取組を引き続き進めるとともに、国連の GGE 及び OEWG、サイバーセキュリティに関する ARF（ASEAN 地域フォーラム）会期間会合等の多国間協議の場も活用し、国際的ルール作りや各国との認識の共有を積極的に進めていく。

また、民間企業、学術界、技術コミュニティ等を含むマルチステークホルダーによる取組を通じて、ICT の利用における責任ある行動をとるための能力構築を支援する。

（4）人材育成等横断的な領域

これまで関係省庁が連携しつつ、それぞれの分野において相手国の政府機関における支援ニーズに応じた人材育成プログラムを提供しているが、今後は、デジタルトランスフォメーション（DX）の取組への対応や重要インフラ分野等の支援ニーズの拡大に対応し、限られた予算で支援をより一層効率的に進めることが求められる。

そのため、各分野における人材のスキルセットの基本部分を共通化する等、関係省

庁間でより一層の緊密な連携を取るための検討を行う。
　さらに、世界的なサイバーセキュリティ分野における高度専門人材の不足から、ASEAN域内で事業活動を行う我が国事業者にとって、高度専門人材の確保が事業拡大の上での大きな課題となっていることを踏まえ、ASEAN等海外における我が国事業者の活動を中長期的に支える人材を育成するとともに、我が国の事業者において多様な文化を理解し外国人材を受け入れやすい環境を産官学で連携して整備する。

　以上を基本方針とし、内閣官房を中心に、関係省庁間及び官民の緊密な連携によるオールジャパン体制の下、様々な政策手段を活用し、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を積極的に実施していく。

（了）