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（基本方針）概要

平成28年10月 内閣サイバーセキュリティセンター、警察庁、総務省、法務省、外務省、経済産業省、防衛省

基本認識

サイバーセキュリティ分野の能力構築支援は、既に多くの省庁が実施している。今後は、**オールジャパンで戦略的効率的な支援を行い、その効果を極大化するために、関係省庁間の緊密な連携が一層重要**

◎ サイバーセキュリティ分野の能力構築支援の重要性は、閣議決定である国家安全保障戦略、サイバーセキュリティ戦略、開発協力大綱のほか、Ｇ７伊勢志摩サミットで発出した「サイバーに関するＧ７の原則と行動」でも確認。

具体的取組

二国間中心の取組

① インシデント・レスポンス等の能力の向上支援

（ア）途上国政府の態勢作りの支援
（アウェアネスの向上、制度・政策面、態勢・機構面の知見提供）

（イ）機材・設備の供与

（ウ）機材・設備の運用能力の向上支援
（技術面の知見提供、人材育成）

米国等友好国との情報交換、政策協調も追求

- **蓄積された経験・知見、高度な技術**や、途上国側のニーズに応じ、官民で分担しつつ、**（ア）～（ウ）をシームレスに（必要に応じ、パッケージとして）提供可能（日本の強み）**
  - ⇨ 当面はASEAN諸国を中心に、政府開発援助（ODA）その他の政府資金等各種支援を、可能かつ適切な連携の下で積極的に実施（※当面は技術協力を中心に（ア）（ウ）に注力しつつ、態勢整備等と並行して（イ）で供与する機材の高度化を図る。）

多国間の枠組みを中心とした取組

② サイバー犯罪対策支援
サイバー攻撃等の犯罪への対処・捜査能力向上による犯罪の抑止

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

- サイバー関連法制度整備、犯罪捜査手法や刑事司法に関する研修、サイバー犯罪条約締約国による関連会合等の多国間の枠組みを積極的に活用
- 各国の認識の共有、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。国連サイバー政府専門家会合（ＧＧＥ）等の多国間協議の場も活用。

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
（基本方針）

平　成　２８年　１０月
内閣サイバーセキュリティセンター
警　　察　　庁
総　　務　　省
法　　務　　省
外　　務　　省
経　済　産　業　省
防　　衛　　省

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17日閣議決定）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。」と定めている。また，サイバーセキュリティ戦略（平成27年9月4日閣議決定）は，「世界各国におけるサイバーセキュリティ確保のためのキャパシティビルディングに協力することは，当該国への貢献となるのみならず，我が国と世界全体にとっても利益となる。」とした上で，「政府及び関係機関は一体となってキャパシティビルディングについて検討し，その効率的・効果的な実施を図る」と定めている。開発協力大綱（平成27年2月10日閣議決定）は，開発協力の重点課題である「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を挙げている。また，本年5月，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」においても，G7首脳は，「能力構築」に関する「協力を強化していくことに努める」旨確認したところである。

（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。

（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，関係省庁間の連携の緊密化がますます重要となっている。

2 支援の在り方

（1）サイバーセキュリティ分野における能力構築支援は，二国間を中心とする①インシデント・レスポンス等の能力の向上支援と，多国間の協力を主眼とする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（アセット）を活かす形で支援を行う必要がある。

（2）①インシデント・レスポンス等能力の向上支援は，さらに（ア）途上国政府の態勢作りの支援（アウェアネスの向上，制度・政策面（サイバーセキュリティ戦略の策定・改定支援等），態勢・機構面の知見の提供），（イ）機材・設備の供与，（ウ）機材・設備の運用能力の向上支援（技術面の知見の提供，人材育成）の3つに大別される。日本の強みは，日本の公的機関が頻繁にサイバー攻撃の標的となっていること等に伴い蓄積された経験や知見，高度な技術も活用しつつ，途上国側のニーズに応じ，官民で分担しつつ，（ア）～（ウ）をシームレスに（必要に応じ，パッケージとして）提供できる点であり，その強みを十分に活かした支援を行っていくことが重要である。

その一方で，高度な機材を供与しても，その運用能力が伴わない状態では，支援の効果が十分に発揮されないおそれがあるので，当面は技術協力を中心に，（ア）及び（ウ）に注力しつつ，途上国側の制度・態勢等の整備の進展と並行して，（イ）で供与する機材の高度化を図っていくことが必要である。

また，特に同盟国たる米国を始めとする友好国との間では，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。

サイバーセキュリティ分野における国際協力機構（JICA）による支援実績としては，ミャンマーに対する通信網の改善（有償資金協力，2015 年～現在実施中）のほか，ミャンマー，インドネシア，ベトナム等のASEAN諸国に対するサイバーセキュリティ専門家の派遣や研修（技術協力）を行った例がある。また，JICA による支援以外にも，日 ASEAN 情報セキュリティ政策会議の枠組みによるサイバー防護等に関する研修，日 ASEAN 統合基金（JAIF）を活用した日 ASEAN サイバーセキュリティ協力強化に向けた取組等がある。今後，二国間又は多国間協議の場を活用し，途上国側の個別のニーズをより詳細に調査・アップデートした上で，上記の方針に基づき，当面は ASEAN 諸国を中心に，政府開発援助（ODA），その他の政府資金等各種形態の支援の可能かつ適切な連携の下，積極的に支援を進めていくことが必要である。

（3）②サイバー犯罪対策支援については，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・事業者に対するサイバー攻撃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

バーセキュリティ関連法制度の整備や犯罪捜査手法に関する研修，UNODCのサイバー犯罪技術援助プロジェクトへの出資，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やアジア大洋州地域サイバー犯罪捜査技術会議のほか，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。

（4）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・認識の共有については，日本として，サイバー空間においても従来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。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。この点，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，国連サイバー政府専門家会合（GGE），ロンドン・プロセス，グローバルサイバーサミット，メリディアン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ことが必要である。

以上を基本方針とし，内閣官房を中心に，関係省庁間の緊密な連携の下，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）