資料９

国際社会の平和・安定及び我が国の安全保障に係る
サイバーセキュリティ戦略の推進状況

資料９－１　国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況

資料９－２　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）

資料９－３　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（基本方針）

資料９－１

第10回 サイバーセキュリティ戦略本部 資料

国際社会の平和・安定及び我が国の安全保障に係るサイバーセキュリティ戦略の推進状況

平成28年10月
内閣官房内閣サイバーセキュリティセンター

■ サイバーセキュリティ戦略（2015年9月4日 閣議決定）

- 政策目的：自由、公正かつ安全なサイバー空間を創出・発展させ、もって①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせる社会の実現、③国際社会の平和・安定及び我が国の安全保障に寄与すること
- 国際社会の平和・安定及び我が国の安全保障を達成するための施策：①我が国の安全の確保、②国際社会の平和・安定、③各国との協力・連携によって、達成していくことを宣言

■ 取組実績（2016年10月現在）

- サイバーセキュリティ戦略及び日米防衛協力のための指針を踏まえ、日米サイバー協力を強化
- G7サミット等、首脳・閣僚のハイレベル国際協議や国連政府専門家会合、法執行機関間の連携強化により、サイバー空間における法の支配の確立に積極的に寄与
- サイバーセキュリティ国際キャンペーン（毎年10月）を開催し、ASEAN及び米と連携した意識啓発を推進
- 国際サイバー演習の主催や積極的な参加を通じ、重大な情報セキュリティ事案発生時における国外関係機関との連絡体制の整備を推進
- 二国間協議（2016年10月現在12か国・地域との間でサイバー協議等を実施）や多国間会議を通じ、我が国のサイバーセキュリティ関係施策や考え方等の積極的な発信、連携の具体化や信頼醸成を推進
- 関係省庁間で、サイバーセキュリティ分野における能力構築支援に関する基本方針を策定。引き続きオールジャパンでASEANを中心とした支援の取組みを強化

■ 「戦略」と「指針」(注)を踏まえた日米サイバー協力の強化

- 日米サイバー対話
  - サイバーに関する日米両国の政府横断的な取組の必要性を踏まえ、外交・防衛・法執行関係当局を含む日米双方の幅広い政府関係者が、情勢認識、重要インフラ防護、能力構築を含む国際場裡における協力等、サイバーに関する幅広い日米協力について議論を実施
- 日米サイバー防衛政策ワーキンググループ
  - 防衛当局間で、日米サイバー防衛政策ワーキンググループを開催し、情報共有や訓練・人材育成等、様々な協力分野に関する専門的、具体的な意見交換を実施

（注）日米防衛協力のための指針（ガイドライン）（2015年4月27日）（概要）

- 日米両政府:
  - サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切に共有
  - 自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するため協力（任務保証）
- 自衛隊及び米軍:
  - 各々のネットワーク及びシステムについて監視態勢を維持するとともに、任務保証を達成するためにネットワーク及びシステムの抗たん性を確保
  - サイバーセキュリティに関する知見の共有、教育交流、共同演習の実施
  - サイバーセキュリティを向上させるための政府一体となっての取組に寄与
- サイバー事案への対処:
  - 日本に対するサイバー事案が発生した場合、日本が主体的に対処し、米国は適切な支援を実施
  - 日本の安全に影響を与える深刻なサイバー事案が発生した場合、日米両政府は、緊密に協議し、適切な協力行動をとり対処

国際社会の平和・安定

～ハイレベル外交を通じたサイバー空間における法の支配の確立への取組み～

■ G7伊勢志摩サミット首脳宣言及び付属文書（2016年5月27日）

- 目指すべきサイバー空間
  - 経済成長及び繁栄のための一つの不可欠な基盤として、アクセス可能で、開かれた、相互運用可能な、信頼できる、かつ、安全なサイバー空間を支持
  - オンラインにおける人権と法の支配の原則の促進・保護
- デジタル経済の促進
  - サイバー空間における営業上の秘密その他の企業秘密に係る情報を含む知的財産の窃取等に反対
- サイバー空間における安全及び安定の促進
  - 国際法はサイバー空間において適用可能であり、一定の場合には、サイバー活動が国連憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認
  - 平時における国家の責任ある行為に関する自発的な規範の促進、国家間の実務的な信頼醸成措置等の戦略的枠組みを促進
- G7の一致した行動・政策協調及び実務的な協力強化
  - サイバー空間の安全と安定を促進するため、オリンピック等の大規模国際イベント、重要インフラ防護、CSIRT間連携等においてG7間の協力を強化
  - これら、サイバー空間の安全・安定を促進するための政策協調・実務的な協力を強化するため、サイバーに関する新たなG7作業部会（G7伊勢志摩サイバーグループ）を立ち上げ

国際社会の平和・安定

～外交努力を通じたサイバー空間における法の支配の確立と信頼醸成への取組み～

■ サイバー空間における国際的な法の支配の確立

- 国連政府専門家会合（UNGGE）への参加
  - サイバー空間における国際法の適用、規範の形成に積極的に関与
- サイバーに関する新たなG7作業部会（G7伊勢志摩サイバーグループ）の立ち上げ
  - サイバー空間における国際法の適用や規範等に関する議論の実施
- サイバー犯罪条約の締約国の拡大・推進
  - 迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化
  - 国境を越える犯罪者の検挙に向けた国際捜査の推進

■ 国際的な信頼醸成措置

- ARF等多国間会議や二国間協議の実施
  - サイバーによる紛争を予防するため、サイバーセキュリティ戦略等、各国のサイバー政策に関する情報共有及び理解促進
  - 我が国の基本的な立場の発信
- 国際的な連絡体制の構築・連絡演習の実施

各国との協力連携

～サイバーセキュリティ国際キャンペーン月間を通じた普及啓発～

■ サイバーセキュリティ国際キャンペーン（国際的な人材育成を含む）

- 毎年10月、「サイバーセキュリティ国際キャンペーン」を実施
  - サイバー攻撃は、容易に国境を超えるため、国際協調してサイバーセキュリティの意識涵養、取組みの普及を図るもの
- サイバーセキュリティに関する普及啓発のため、次を行う。
  - 若い世代を対象にしたキャリアトーク・イベント（在日米国商工会議所と協力）
  - ポスター、コミックブックによる啓発活動（ASEAN各国と共同）
  - SNSを活用した幅広い対象への働きかけ
- キャンペーン期間中には、第9回日・ASEAN情報セキュリティ政策会議（日・ASEAN各国の局長級会議）を東京において開催
- 政府、警察、大学、民間等のサイバーセキュリティ関連イベントも本キャンペーンの一環

日・ASEAN情報セキュリティ政策会議（局長級）
※毎年開催しており、共同意識啓発活動、サイバー演習、人材育成などの協力を実施

国際連携による学生向けのイベントを実施

キャンペーンポスター及び日ASEAN共同ポスター

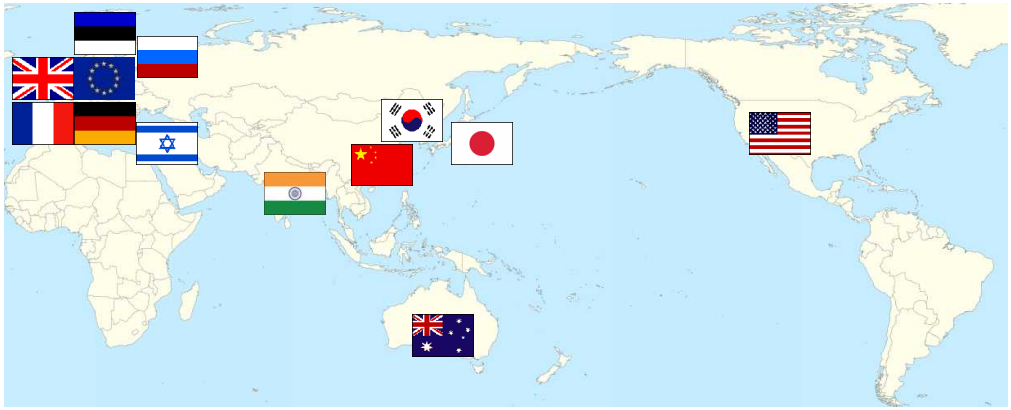
コミックブック制作

各国との協力連携

～国際的なサイバー攻撃即応体制の確立と各国との連携・信頼醸成の推進～

■ 二国間サイバー協議等の開催状況（2016年10月現在）

- 計12か国・地域との間でサイバー空間に関する省庁横断的な協議・対話を開催



各年別二国間サイバー協議等の開催実績	
2012年	英、印
2013年	米
2014年	米、EU、中･韓、イスラエル、エストニア、仏、英
2015年	豪、露、米、中･韓、エストニア
2016年	仏、イスラエル、米、豪、独、英

注1: 米国とは上記以外にもサイバー空間に関する経済面や安全保障面ついての協議を開催
注2: 中国及び韓国とは三カ国協議を開催

- 日米間では、日米防衛協力のための指針も念頭に、日米サイバー対話等を通じた連携を一層強化
- 有志国との間で、関連施策動向の紹介や脅威認識等に係る情報共有、サイバー演習等の具体的な連携を進め、重大な情報セキュリティ事案発生時における国外関係機関との連絡体制を整備
- 各国との間で、サイバーセキュリティ戦略の共有等により信頼醸成を推進

■ 多国間会議の参加状況（2016年10月現在）

- 首脳・閣僚等ハイレベル: G7、G20、日・ASEAN首脳会議、サイバー空間に関するロンドンプロセス会議等
- 高級実務者レベル: G7伊勢志摩サイバーグループ、国連政府専門家会合、日･ASEAN情報セキュリティ政策会議、日・ASEANサイバー犯罪対策対話、サイバー犯罪条約委員会会合等
- 政策担当者・実務担当者レベル: MERIDIAN、IWWN、FiRST、NatCSIRT、OECD WPSPDE、APEC-TEL、ARFサイバー関連会合等

各国との協力連携

～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～

■ 能力構築支援の重要性と我が国の取組み

- 我が国にとっての途上国の能力構築支援の重要性: ①世界全体のリスク低減、②支援対象国の重要インフラ等に依存する在留邦人・日本企業の活動の安定確保、③サイバー空間に関する我が国の立場への理解浸透、④我が国情報通信産業等の現地展開に向けた基盤形成の可能性
- 我が国の国家戦略等（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）や、国連・G7等の国際場裡においても、重要性と協力強化の必要性を指摘
- ASEAN諸国を中心に、日・ASEAN情報セキュリティ政策会議や日・ASEANサイバー犯罪政策対話等の場を活用した能力構築支援を実施

■ 日・ASEAN首脳会議（2016年9月7日）

- 安倍総理席上発言: 「サイバーセキュリティの確保のため、能力構築支援の方針を策定し、引き続きオールジャパンでASEANを支援していく」
- 議長声明:「ASEAN諸国のサイバーセキュリティ確保の取組みに対する日本の積極的な支援の決意を歓迎」

■ 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）（2016年10月 関係省庁合意）

- サイバーセキュリティ分野における能力構築支援の重要性を確認しつつ、オールジャパンで戦略的・効率的支援を行い、その効果を極大化するため、内閣官房を中心とした関係省庁間の緊密な連携の重要性を確認
- 能力構築支援を①インシデント・レスポンス等の能力の向上支援、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・認識の共有の3つに大別。それぞれについて整理した基本的な支援の在り方に沿って、ODAを含む様々な政策手段を活用し、積極的に支援を実施

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

資料９－２

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。

資料９－３

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
（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）