資料６

「国際社会の平和・安定及び我が国の安全保障への寄与」に係る取組状況について

資料６－１　「国際社会の平和・安定及び我が国の安全保障への寄与」に係る取組状況について

資料６－２　「国際社会の平和・安定及び我が国の安全保障への寄与」に係る取組状況（詳細資料）

「国際社会の平和・安定及び我が国の安全保障への寄与」に係る取組状況について

資料6-1

■ サイバーセキュリティ戦略（2018年7月27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への寄与を達成するための施策：①自由、公正かつ安全なサイバー空間の堅持、②我が国の防御力・抑止力・状況把握力の強化、③国際協力・連携によって、達成していくことを宣言

■ 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）

- 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・認識の共有の分野で、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

■ 取組実績（2019年1月現在）

- 首脳・閣僚のハイレベル協議や国連政府専門家会合、 G7、GCSC、IGF等各種国際会議への参加、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推進、自由、公正かつ安全なサイバー空間の堅持に積極的に寄与。2018年12月、中国を拠点とするAPT10といわれるグループによるサイバー攻撃に関する非難声明を発出。
- 二国間協議（2019年1月現在13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。2017年８月には「サイバーセキュリティに関するARF会期間会合」を立上げ。
- National CERTのコミュニティ（Meridian、IWWN、日ASEANサイバーセキュリティ政策会議、FIRST等）への参加を通じ、ベストプラクティスの共有や平時からの脅威情報共有などの活動を促進。特に日ASEANサイバーセキュリティ政策会議では、平時の情報共有の一層の充実に合意。
- 重大な情報セキュリティ事案発生時における国際連携対処にかかる国外関係機関との連絡体制の整備、またこれを検証するための国際サイバー演習の主催や積極的な参加を通じ、国内情報共有体制についても検証。
- NISC及び関係省庁で主にASEANを対象とした能力構築支援を実施。サイバーセキュリティ政策能力向上等をテーマとした短期研修コースを提供したほか、昨年９月タイに日ASEANサイバーセキュリティ能力構築支援センター（AJCCBC）を設置。また、産業サイバーセキュリティセンター（ICSCoE）が東京で制御システムに係るASEAN等向け日米サイバー共同演習を初めて実施。

資料6-2

第21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への寄与」に係る取組状況（詳細資料）

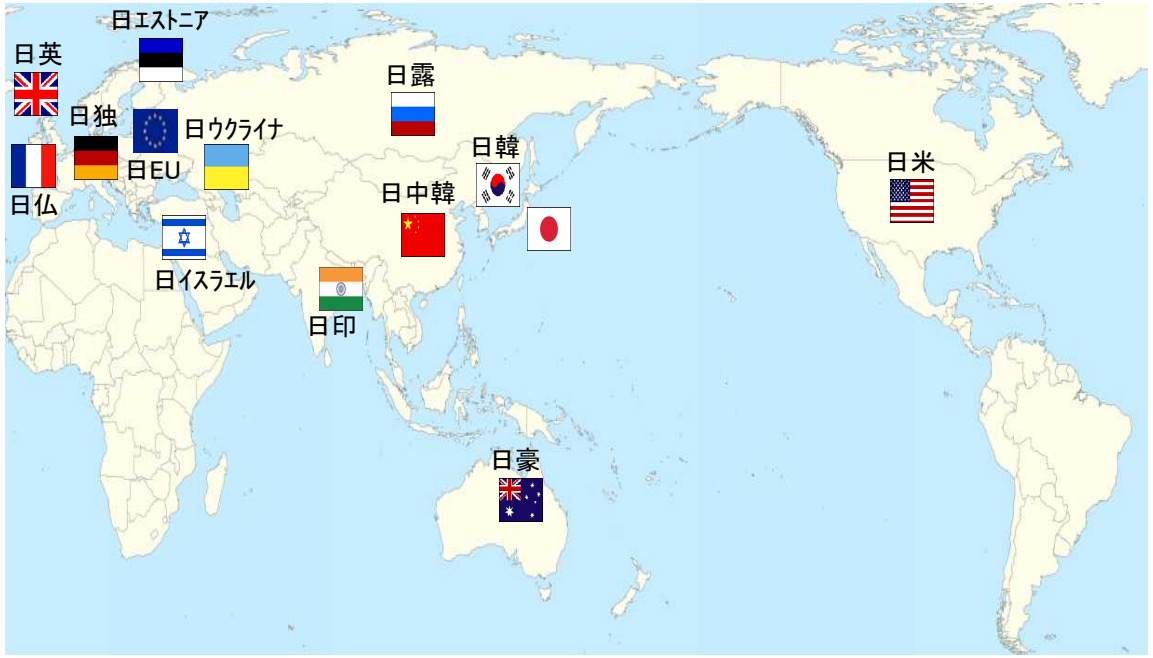
平成31年1月
内閣官房内閣サイバーセキュリティセンター

国際戦略推進のための国際会議等

～二国間協議～

● 二国間サイバー協議

各国との知見の共有・政策調整を目的として、英国、インド、米国、EU、中韓、イスラエル、仏、エストニア、豪州、ロシア、独、韓及びウクライナとの間でサイバー協議を実施。各国との間でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論。



各年別二国間サイバー協議等の開催実績	
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、韓、露、ウクライナ
2017年	仏、EU、エストニア、中・韓、米、印、イスラエル、豪
2018年	EU、英、仏、米、イスラエル

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

● 二国間協議の取組状況（2017年12月～2019年１月）

■ 第３回日豪サイバー政策協議（2017年12月、東京）

サイバー空間における脅威動向、地域的・国際的な文脈におけるサイバーセキュリティ協力、二国間の文脈でのサイバーセキュリティ協力に関する主要な課題、既存の国際法のサイバー空間への適用等について議論。

両国は、国際的なサイバー空間の安定に関する戦略的枠組みを促進することに取り組むことを再確認。また、両国は、国連サイバー政府専門家会合におけるICT分野の発展に関するGGEレポートに一致する形で行動することを再確認し、国際法及び規範の精緻化、信頼醸成措置並びに能力構築支援に関し、協力を続けていくこと、関連する国内法及び国際法に従って、重大なサイバー事案を抑止し、また対処することを含む、悪意あるサイバー活動に対して対処していくための協力を強化し続けることを再確認。

国際戦略推進のための国際会議等

～二国間協議～

■ 第３回日EUサイバー対話（2018年3月、東京）

サイバー分野における最近の取組を共有するとともに、国際的なサイバーセキュリティ上の課題、サイバー犯罪対策及び能力構築支援、サイバー空間における脅威動向等について議論。

両国は、サイバー空間において責任ある行動を促進し、同空間において悪意ある活動を行う者を制止し、悪意あるサイバー活動を抑止し対応するために引き続き協力を強化する目的で協働することの重要性を強調し、サイバーにおける信頼醸成措置の進展・履行を含め、サイバー空間における責任ある国家の行動を促進するための作業を続けていくことについてのコミットメントを確認。また、自由で開かれたインターネットについての強い支持及びインターネット・ガバナンスについての全ての利害関係者の参加と貢献を含むマルチ・ステークホルダー・アプローチへの支持を再確認。

■ 第４回日英サイバー協議（2018年3月、ロンドン）

サイバーセキュリティ分野における両国の取組や戦略、２０２０年東京オリンピック・パラリンピック競技大会を含む両国それぞれが開催する大規模行事に向けたサイバーセキュリティ、能力構築支援、モノのインターネット（ＩｏＴ）の安全性及びサイバー空間におけるルールに基づく国際秩序の適用を支援するための協力を含む様々な事項に係る二国間の協力について議論。

自由で、開かれ、平和的で、公平かつ安全なサイバー空間の促進へのコミットメントを改めて表明し、それが世界的な社会・経済の発展に不可欠であること並びに表現の自由を含む人権及びインターネット・ガバナンスにおけるマルチステークホルダー・アプローチの重要性を再確認。

両国は、既存の国際法の適用、自発的で非拘束的な責任ある国家の行動に係る合意された規範、信頼醸成措置及び能力構築支援から成る、サイバー空間のための国際的な安定の枠組みを促進し、関連する国内法及び既存の国際法に従い、適切な枠組みを通じ、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するため情報交換を含む協力を強化していくことへのコミットメントを再確認。また、２０１８年２月２２日にブルネイのバンダル・スリ・ブガワンで日英が共催したＡＳＥＡＮ諸国向けサイバーワークショップの成功及び、信頼醸成措置を策定し、実施するためのASEAN地域フォーラム（ＡＲＦ）の枠組みにおけるイニシアティブを歓迎した。

■ 第4回日仏サイバー協議（2018年6月、東京）

サイバーセキュリティ分野における両国の最近の取組、オリンピック・パラリンピック競技大会を含む大規模行事に向けたサイバーセキュリティ、重要インフラの保護、モノのインターネット（ＩｏＴ）機器のサイバーセキュリティ、サイバーセキュリティにおける民間部門の役割、能力構築支援、第三国との二国間協議及び地域又は多国間におけるサイバーセキュリティ協力を含む様々な事項について議論。

日仏両国は、開かれた、自由、公正、かつ安全なサイバー空間へのコミットメント、サイバー空間への既存の国際法の適用可能性を確認することの重要性並びに合意された、自発的で、非拘束的な責任ある国家の行動規範、信頼醸成措置及び能力構築支援の推進及び実行を再確認。また、G7の議長国であるフランスとG20の議長国である日本との間でのサイバーセキュリティを含むデジタル分野における協働の可能性を議論。また、関係する国内法及び既存の国際法に沿った適切な枠組みを通じた、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するための情報交換を含む協力を強化することを再確認。日本は、２０２０年東京オリンピック・パラリンピック競技大会及び２０２４年パリオリンピック・パラリンピック競技大会のサイバーセキュリティの確保において日本と協力するというフランスの提案を歓迎。フランスは、サイバーセキュリティ分野における協力を強化するために、サイバー・クラスターを訪問するよう日本側関係者を招待。

■ 第6回日米サイバー対話（2018年7月、ワシントン）

情勢認識、両国におけるサイバー政策、国際場裡における協力、能力構築支援等、サプライチェーン対策、サイバーに関する日米協力について議論。

■ 第4回日イスラエル サイバー協議（2018年11月、テルアビブ）

両国のサイバー政策のアップデート、サイバー分野における現状認識、サイバーにおける危機管理等について議論。

国際戦略推進のための国際会議等

～National CERTの多国間の取組～

NISCは日本のNational CERTに相当する機関として、諸外国のNational CERTとの連携にかかる連絡窓口（PoC）機能を有する。NISCは海外のNational CERTが参加する主要なコミュニティに参加して、National CERT間の連携を強化している。

■ Meridian

重要情報インフラ防護（CIIP）等に関する国際連携を推進する場として2005年にイギリスで始まった会合。先進国を中心に約70カ国のサイバーセキュリティ所管省庁がメンバー。日本からはNISC、総務省、JPCERT/CCが参加。

■ IWWN（International Watch and Warning Network）

サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組を促進することを目的として、2004年に創設された国際的な枠組み。先進国15か国のNational CERT相当機関がメンバー。日本からは、NISCとJPCERT/CCが参加。

■ 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政策会議は、日本とASEAN加盟国間のサイバーセキュリティ分野での連携・協力を進めるため、2009年2月に創設された国際的な枠組み。ASEAN加盟 10か国と日本のサイバーセキュリティ所管省庁及びASEAN事務局がメンバー。政策レベルの議題だけではなく、National CERTの実務レベル協力の議題も扱う。

日本のリードの下、政策会議のほか3回の実務会合を開催して情報共有、重要インフラ防護、意識啓発等をテーマとした協力活動を推進。また、サイバー演習や重要インフラ防護ワークショップなどを開催している。

■ FIRST（Forum of Incident Response and Security Teams）

世界各国の官民のCSIRT間の情報交換や事案対応における協力関係の構築などを目的としたフォーラム。例年、FIRST会合の機会に合わせて、各国のNational CERT相当機関が一堂に会するNatCSIRT会合が開催される。日本からは、NISCとJPCERT/CCが参加。

①自由、公正かつ安全なサイバー空間の堅持

～ハイレベルの協議を通じた連携～

- 日英首脳会談（2017年８月、 2019年1月）
  - 両首脳は、「日英共同ビジョン声明」、「安全保障協力に関する日英共同宣言」を発出。「安全保障協力に関する日英共同宣言」においては、「日英両国は、既存の国際法の適用、自発的で非拘束的な責任ある国家の行動に係る合意された規範、信頼醸成措置及び能力構築措置から成る、サイバー空間のための国際的な安定の枠組みを促進し、関連する国内法及び既存の国際法に従い、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するため、情報交換を含む協力を強化」することを確認。（2017年8月）
  - 「日英共同声明」において、「自由で、開かれ、平和で、公正かつ安全なサイバー空間を促進することに対するコミットメントを改めて表明」するとともに、「サイバー攻撃を抑止し、対応し、緩和するために共に取り組み、国家の無責任な行動を非難」し、「サイバーにより可能となる知的財産の窃取その他の脅威から技術を保護するにあたり協力を強化すること」を表明。（2019年1月）
- 日エストニア首脳会談（2018年１月）
  - 両首脳は、サイバー協議等の機会を活用し、引き続き両国の協力を進めていくことで一致し、その観点からエストニアに所在するNATOサイバー防衛協力センターへの日本の参加が承認されたことを歓迎。
- 第４回日仏外務・防衛閣僚会合（2018年１月）
  - 四大臣は、悪意のあるサイバー活動を抑止し、軽減し、原因を特定するため、日仏両国が強調した対応及び情報共有を強化することを確認。
- 日イスラエル首脳会談（2018年５月）
  - 両首脳は、サイバー面での協力を強化していくことを確認。両首脳は、イスラエルのベイルシェバにあるサイバーセキュリティーコンプレックスへ専門家を派遣することに合意し、本合意に基づき、2018年６月、11月に専門家を派遣。
- 櫻田大臣海外主張（2019年１月）
  - イスラエル、英国及びフランスに出張し、東京大会の成功に向けた協力関係の構築の確認、サイバーセキュリティの課題の共有や対応策に関する意見交換を実施。

①自由、公正かつ安全なサイバー空間の堅持

～サイバー空間における法の支配の推進への取組～

- 国連サイバー政府専門家会合（UNGGE）
  - 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。
  - 2013年9月には、サイバー空間においても既存の国際法が適用されるとする報告書（第3会期）が提出された。
  - 2015年9月の報告書（第４会期）では、2013年の報告書の内容を踏まえつつ、国家の責任ある行動規範に係る章において具体的なルールに係る勧告が盛り込まれているほか、ICTの使用に対する国際法の適用に係る章において、「国家が国際法に従って、かつ、国連憲章で認められた形でとり得る固有の権利に留意する」ことが明記された。
  - ただし、2016年～2017年の第5会期では、国際法の適用のあり方等について参加国のコンセンサスを得られなかった。
  - 2018年国連総会決議に基づき、2019年に第6会期が立ち上がる予定。
- G7伊勢志摩サイバーグループ
  - サイバーセキュリティ環境及びＧ７各国のサイバーセキュリティ関連政策に係る情報共有並びにＧ７の政策調整に関する議論とサイバー空間における法の支配を促進するための国際的議論の加速を目的として設置。
  - ２０１６年５月G7伊勢志摩サミットの首脳宣言及び附属文書において、以下を確認。
    - 国連憲章をはじめとする既存の国際法のサイバー空間への適用を確認するとともに、サイバー空間を通じた武力攻撃に対し、国連憲章第５１条で認められた個別的又は集団的自衛権が行使可能である。
  - ２０１７年４月Ｇ７ルッカ外相会合の外相共同コミュニケ及び「サイバー空間における責任ある国家の行動に関するG7（ルッカ）宣言」において、以下を確認。
    - 国際違法行為について責任を有する国家に対して均衡性のある対抗措置をとり得る。
    - 事実を評価し、他の国家にサイバー行為を帰属させることについて国際法に従って独自の決定を自由に行うことができる。
  - ２０１８年４月G7トロント外相会合の外相共同コミュニケ及び「G7伊勢志摩サイバーグループ会合議長報告書」において、以下を確認。
    - 悪意のあるサイバー行為を阻止し、抑止し、妨げ、対抗するための措置を展開するために協働し、適時にコストを課すことで、悪意のあるサイバー行為を行う者を抑止する。
- 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。
  - 国境を越えるサイバー犯罪者の検挙に向けた国際協力の推進。
- その他、GCSC、GCCS等、各種国際会議への参加

②我が国の防御力・抑止力・状況把握力の強化

～信頼醸成措置：サイバーセキュリティに関するARF会期間会合（ARF-ISM on ICTs Security）について～

1. 本会合設立の経緯

- 世界中でサイバー攻撃が多発し、サイバー攻撃対処への重要性が一層高まる中、国連や各地域枠組みにおいて、サイバーセキュリティに関する諸問題を議論する会議体が設立
- かかる情勢の中、日本は、マレーシア、シンガポールと共に「サイバーセキュリティに関するARF会期間会合」（ASEAN Regional Forum Inter-Sessional Meeting（ISM） on Security of and in the Use of Information Technology）の立上げを提案、2017年8月にARF閣僚会合において全会一致で承認
- 本ISMは、ARFワークプランの包括的な実施を通じてARF加盟国の協力を強化し、平和で安全、公正かつ協力的なサイバー環境を発展、相互の信頼醸成の促進により紛争や危機の防止に寄与

※ARFメンバー国等：ASEAN（ブルネイ、インドネシア、マレーシア、タイ、フィリピン、シンガポール、ベトナム、ラオス、ミャンマー、カンボジア）、非ASEAN（日本、米国、カナダ、オーストラリア、ニュージーランド、パプアニューギニア、韓国、北朝鮮、モンゴル、中国、ロシア、インド、パキスタン、東ティモール、バングラデシュ、スリランカ）及びEU

2. 活動実績

日本はマレーシア及びシンガポールと共に共同議長国として、これまで以下の3会合を開催

- 2018年1月　第1回専門家会合　於　東京
- 2018年4月　第2回専門家会合　於　クアラルンプール
- 　　同　　第1回会期間会合（ISM）　於　クアラルンプール

※上記専門家会合（Open Ended Study Group on Confidence Building Measures（SG））は、信頼醸成措置及びサイバーセキュリティに関する幅広い問題に対処するための提言を作成し、ARF会期間会合における議論に貢献するもの

第１回会期間会合の様子（於：クアラルンプール）

3. 信頼醸成措置に係わる提案等の状況（協議中のものを含む）

項目		提案国	内容
Terms of reference（TOR）		日本	Study Group（専門家会合）の手続的事項を規定
信頼醸成措置	①	マレーシア・オーストラリア	ARFサイバー関係当局間のコンタクト・ポイント設立
	②	フィリピン・日本	各国国内法令・政策・戦略・取組の紹介・共有
	③	シンガポール・EU	重要インフラ防護に関わる協議メカニズム
	④	シンガポール・カンボジア・中	サイバー事案対応のための意識啓発・情報共有
	⑤	シンガポール・カナダ	サイバーセキュリティ原則（戦略）策定のためのワークショップ開催
Priority　Area		シンガポール	ARFとして取り組むべき優先分野の策定

②我が国の防御力・抑止力・状況把握力の強化

～実効的な抑止のための対応・脅威情報連携～

■ サイバー攻撃に対する抑止力の向上：実効的な抑止のための対応

サイバー攻撃を抑止するため、悪意あるサイバー活動に関する非難声明を発出

- 2017年12月、「ワナクライ」事案の背後に北朝鮮の関与があったことを非難。
- 2018年12月、中国を含むG20メンバー国に対し責任ある対応を要請。**中国を拠点とするAPT10といわれるグループによるサイバー攻撃に関する非難声明を発出**。

■ サイバー攻撃の状況把握の強化：脅威情報連携

国の関与が疑われるサイバー攻撃、非政府組織による攻撃等多様な脅威に的確に対処し、抑止するため、同盟国・有志国との間で、脅威情報の共有を推進

- NISCはJPCERT/CCとともに、National CERTの国際コミュニティに参加して、各種の情報共有に取り組んでいる。
  - IWWNコミュニティの一員として、電子メール等を活用した任意の情報共有を実施。
  - 日ASEANサイバーセキュリティ政策会議下の協力活動として、電子メール等を活用した任意の情報共有を実施。
    - 特に、2018年10月に東京で開催した政策会議では、**平時の情報共有の一層の充実に合意**。

③国際協力・連携

～事故対応等に係る国際連携の強化～

国際サイバー演習への参加や共同訓練等を通じて、連携対処能力の強化を図る。

- NISCはNational CERTとして国際サイバー演習への参加を通じて、国際PoCとしての立場を明らかにするとともに、国際的な連携対処のための国際連絡手順等を確認。
  - NISCはこの機会を捉えて、海外からの情報を国内関係機関と共有する際の連絡手順及び国内の情報を海外に提供する際の連絡手順等の、国内情報共有体制を検証。
  - 本年は、**日ASEANサイバーセキュリティ政策会議等の国際サイバー演習に参加。**

- NISCは**「サイバー演習国際ワークショップ」を主催**し、参加国とサイバー演習の運営に関する知見を共有。
  - 日本の分野横断的演習へ海外の6カ国からの視察を受け入れた。また、これらの国と「サイバー演習国際ワークショップ」を開催し、各国の演習運営に関する知見を共有した。

③国際協力・連携

～能力構築支援～

■ NISC及び関係省庁は、主にASEAN諸国向けに各種の能力構築支援プロジェクトを主催または支援。昨年の主な取り組みは以下の通り。

分類	名称	実施時期	実施組織
日ASEAN政策会議	情報連絡演習	5月	NISC
	机上演習	7月	NISC
	CIIPワークショップ	7月	NISC
短期研修	ASEAN地域のサイバーセキュリティ対策強化のための政策能力向上	2月	JICA
	サイバー攻撃防御演習	2月	JICA
	日ASEAN・サイバーセキュリティ能力構築センター(AJCCBC)	9月～	総務省・ETDA(タイ)
	制御システムに係るASEAN等向け日米サイバー共同演習	9月	経産省
	日・ASEAN ISP向け情報セキュリティワークショップ		総務省
	APTサイバーセキュリティ技術研修	10月	APT(*1)
情報共有	DAEDALUS ： サイバー攻撃アラートシステム	通年	総務省
	TSUBAME ：インターネット定点観測システム	通年	JPCERT/CC

■ 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」

■ 日・ASEAN首脳会議（2018年11月14日）

- 安倍総理席上発言: 「本年9月、バンコクに日ASEANサイバーセキュリティ能力構築支援センターを構築するなど、サイバー分野でも協力していく」
- 議長声明:「サイバーセキュリティを含む非伝統的安全保障上の課題及び伝統的犯罪に対処すべく、引き続き協力強化を決意。産業制御システムに係る日米共同サイバーセキュリティ演習を東京で実施したことに関し、日本の産業サイバーセキュリティセンター（ICSCoE）を称賛。ARF会期間会合並びに日ASEANサイバーセキュリティ能力構築支援センターの開設といった進捗を歓迎」