サイバーセキュリティ
国際連携取組方針
～j-initiative for Cybersecurity～

平成 25 年 10 月2 日

情報セキュリティ政策会議

目　次

１　趣旨

情報通信技術の普及・高度化と利活用の進展に伴い、情報通信は、社会・経済・文化などあらゆる活動の基盤となり、情報通信技術の発展によりもたらされたサイバー空間は国の成長を支える重要なプラットフォームとなっている。一方で、情報通信技術への依存度の更なる高まりや、サイバー攻撃手法の複雑・巧妙化、攻撃対象の範囲の拡大などに伴い、実空間における行政機能や社会機能を麻痺させる事態も現実のものとなりつつあるなど、サイバー脅威の深刻度が増している。サイバー空間は、国境を越えて拡がり続け、様々な主体による利活用が急速に拡大しており、それに伴うリスクも甚大化し、拡散し、グローバル化している。いまや、サイバー脅威は、世界共通の切迫した課題として顕在化している。

世界各国がサイバー空間で共存しその恩恵を最大限享受するためには、各国が相互に異なる価値観を認識するとともに信頼関係を構築し、協力して課題解決にあたることが不可欠である。このため、我が国として、安全で信頼できるサイバー空間の確保に向け、各国との積極的な連携・共助を強力に進めていく。

特に、我が国は、情報通信インフラの整備において世界最高水準となり、情報通信技術の利活用が進むことにより、幾多のサイバー脅威にも既に直面してきている。こうした中、サイバーセキュリティの確保に向け、政府は累次にわたる戦略や年次計画、分野別の取組方針などを作成・改訂し、それらの戦略などに基づき、産・学・官等の関係者が協力し課題解決を図るなど、世界に貢献できる豊富な経験と十分な知見を有しており、それらを活かし、国際連携の取組を推進していくことが、我が国の使命である。

本取組方針は、2013 年６月に策定された「日本再興戦略」及び「サイバーセキュリティ戦略」を踏まえつつ、サイバーセキュリティ分野における国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理し、それらを一体のものとして国内外に示すものである。我が国は、本取組方針に基づき、サイバーセキュリティ分野において産学官など国内の全ての関係者（ステークホルダ）が共通の基本認識の下に国際連携・共助の取組を進めるとともに、世界の国々と有機的な協力関係を構築し、情報の自由な流通が確保された安全で信頼できるサイバー空間の構築に積極的に貢献していく。

２　基本原則

①　情報の自由な流通の確保

サイバー空間は、あらゆる主体が自由に活用することにより、社会経済の成長の基盤となるまでに発展してきた。過度な管理や規制は、そのようなサイバー空間の便益を損ない、社会経済の成長を阻害する要因となりかねない。

このため、過度な管理や規制を行うことなく、開放性や相互運用性を確保することにより、情報の自由な流通が確保された安全で信頼できるサイバー空間を維持し、発展させていくことが不可欠である。

その結果、表現の自由や活力ある経済活動等が確保され、イノベーションの促進、経済成長、社会的課題の解決などの様々な恩恵を世界各国が享受できる。

②　深刻化するリスクへの新たな対応

サイバー脅威は深刻化しており、甚大化し、拡散し、グローバル化するリスクに対しては、これまでの対策や取組の延長では、十分に対応できなくなっている。サイバー空間がサイバー脅威に対し脆弱な場合には、サイバー空間における活動が阻害され、情報の自由な流通の確保が困難になる恐れがある。

そのため、これまでの対策や取組に加え、情報通信技術の革新等に伴うリスクに的確に対応できるよう、国際連携による新たなメカニズムが必要である。

③　リスクベースによる対応の強化

サイバー攻撃を事前に完全に阻止することは理想であるが、サイバー空間の拡がり、サイバー脅威の巧妙化・高度化に伴い、事実上困難となっている。このような状況下では、一定のリスクが発生し、事案化することを前提としつつ、適時適切な資源配分の下で、その事案に各国が協力して迅速かつ適切に対応し、速やかな回復と被害拡散の防止を図ることがサイバー脅威への対応として現実的である。

このため、リスクベースアプローチを採り、時々刻々変化するリスクを迅速かつ適切に把握し、そのリスクの性質を踏まえた動的な対応が確実に実施できる体制の構築が国際的に急務である。

④　社会的責務を踏まえた行動と共助

サイバー空間の拡がりに伴い、多種多様な主体がサイバー空間の恩恵を享受しており、その結果、様々な主体においてサイバー脅威が現実のものとなり、また、その脅威が広く伝播する状況になっている。このような状況下では、それぞれの主体が自らサイバーセキュリティ確保のための対策を行うなど主体的に行動することとともに、サイバー脅威に対し社会全体の参加による予防的な取組として「サイバー空間の衛生」が重要である。

このため、国境を越えてグローバルに形成されたサイバー空間における全ての主体（ステークホルダ）がそれぞれの社会的立場に応じた役割を発揮しながら、相互に連携し、共助することが必要である。

3　基本方針

①　グローバルな共通認識の漸進的な醸成

サイバー空間は、政府、企業、個人等の多様な主体によって利用されることで発展し、また、文化や価値観の異なる国々が共存することでその活力が向上してきた。

このため、サイバー空間における多種多様な主体や価値観の存在を認識し、共にサイバー空間の恩恵を最大限享受できるような形で、サイバーセキュリティの確保のための国際連携に取り組むことが重要であり、多様性を認識しながら、グローバルな共通認識の醸成を図ることが必要である。

サイバーセキュリティに係る課題は、社会経済面から安全保障面まで多岐に渡っており、解決が容易なものから困難なものまで幅広いスペクトラムを有し、共通認識の醸成の程度、参画可能な主体の範囲なども、千差万別である。そのため、多様な価値観を認識しつつ、可能なところから漸進的に共通認識の醸成を図ることが必要である。

その取組の推進に際しては、二国間、多国間、地域的枠組、国連会合その他あらゆる場を活用する。

②　グローバルコミュニティへの我が国の貢献

我が国では、光ファイバ網や高速無線網など世界最先端の情報通信インフラの全国的な整備等に伴い、あらゆる世代の様々な主体によるサイバー空間の利活用が進んでおり、サイバーセキュリティ上の深刻な課題に先んじて直面している。同時に、官民など関係主体が協力・連携しながら、それらの課題に対する実効的な対応も多種多様な形で実施し、成果を挙げている。

こうした我が国の豊富な経験と先駆的な知見を活かし、人材育成、事案対処体制や情報共有体制の構築支援をはじめとしたグローバルレベルでのキャパシティビルディングに積極的に貢献するなど、より効率的・効果的な課題の解決に向けたグローバルな取組に寄与していく。

③　技術フロンティアのグローバルな拡大

情報通信技術の高度化や利活用の幅の拡がりに伴う新たなリスクやサイバー攻撃の高度化・複雑化に的確に対応するためには、優れた技術を最大限活用して課題解決を図るべきである。この点、我が国は、サイバーセキュリティ対策技術の開発や、その実用化の取組を実施するなど、サイバー脅威への技術的な対応の知見を豊富に蓄積してきている。

このため、安心してサイバー空間を利用するための技術の開発を着実かつ継続的に実施し、その技術フロンティアをグローバルレベルで拡大し、低廉かつ優れた技術による効用を拡げていくことが重要である。

その際、情報通信技術は利用方法によってはリスクの要因となるおそれもあるが、このために技術の開発を阻害したり、悪用されるおそれのある技術を規制したりするのではなく、技術の開発・利活用を持続的に行っていくことが肝要である。

4　重点取組分野

(1)　サイバー事案への動的対応の実践

サイバー事案の発生の可能性を前提としたリスクベースの取組にあたっては、時々刻々変化するリスクに対応しつつ、サイバー事案のインパクトを最小限に抑えるための対応が必要であり、サイバー空間の拡がりに対応し、グローバルな対処を迅速に実施することが不可欠である。

サイバー脅威は現実化しており、サイバー事案の発生を迅速に把握し、その影響度を的確に分析した上で、被害拡大防止、早期解決促進や原因解明、類似事案発生の防止などを行う動的な対応を各国が協力して実施可能とする国際連携・協調体制の構築が急務である。

①　多層的な情報共有体制の強化

瞬時に影響がグローバルに拡大するサイバー事案に対して動的に対応する体制の整備にあたっては、国際的な情報に基づく対応や解決手法の共有などを可能とするグローバルな情報共有体制の構築が重要である。

サイバー空間には様々な主体が関与し、対策を講じてきていること、変化の激しい情勢に対する迅速かつ的確な判断には幅広い情報源の存在が有益なことから、情報共有に当たっては、技術面、法執行面、政策面、外交面など、多層的な情報共有体制を構築することが有意義である。

具体的には、サイバー事案の検知やマルウェアや IP アドレスの解析、実際の対処といった運用面での課題解決に当たる CSIRT (Computer Security Incident Response Team) 間の連携、捜査権限を行使し被害拡大防止等に当たる法執行機関間の連携、サイバー事案での全体像を早期に把握し必要な政策的対応を行う政策レベルの連携、当事者が意図せぬ形でのエスカレーションによる不測の事態を回避するための外交レベルの情報共有、最先端技術の研究開発を行う研究者間の連携などが重要である。

このため、サイバー事案の発生時にこうした多層的な情報共有体制が適切に機能するよう、平素から積極的に各層におけるグローバルな情報共有体制の構築に向けた対応に積極的に貢献する。

②　サイバー犯罪への適切な対応

容易に国境を越えて敢行されるサイバー犯罪に効果的に対処するためには、国際連携の強化が必要である。

具体的には、G8 ローマ／リヨン・グループのハイテク犯罪サブグループやアジア大洋州地域サイバー犯罪捜査技術会議等を通じた各国捜査機関等とのサイバー犯罪・解析技術に関する情報交換の継続的実施、サイバー犯罪に関する最新の捜査手法に係る情報交換や外国捜査機関との連携強化のための職員の派遣、外国捜査機関に対する捜査共助の積極的な要請等の取組を実施する。また、サイバー犯罪条約の締約国拡大に資する働きかけやサイバー犯罪対策のためのキャパシティビルディングなどを通じ、サイバー犯罪条約の普及に積極的に参画し、サイバー犯罪対策に関する国際規範の形成及び国際連携

の促進に貢献する。

また、ICPO（International Criminal Police Organization）事務総局を補完する組織として新たにシンガポールに設立される IGCI（INTERPOL Global Complex for Innovation）の初代総局長を日本から派遣するなど、積極的な取組を実施しており、より迅速なサイバー犯罪対応に貢献するための協力を強化する。

③　サイバー安全保障における協力体制の確立

サイバー空間は、安全保障の観点からみても、情報収集、攻撃、防御といった様々な活動が行われる陸・海・空・宇宙と並び得る新たな「領域」であり、その安定的な利用を確保するためには、国際連携を積極的に推進し、協力体制を確立することが重要である。

具体的には、サイバー空間の利用に関する国際的なルール作りへの参画、二国間協議・対話や ASEAN 地域フォーラム（ARF : ASEAN Regional Forum）等の地域的な枠組みによる対話や意見交換を通じた信頼醸成措置の構築及び国際社会にセキュリティ上脆弱な地域を作らないためのキャパシティビルディングなどを積極的に推進する。

同盟国である米国との協力については、我が国の安全保障にとって極めて重要な意義を有していることから、日米防衛当局間で開かれている日米 IT フォーラムや日米の関係省庁による日米サイバー対話等、様々なレベルで行われている協議での議論を加速させる。今後も、サイバー脅威に関する情報の収集やサイバー攻撃対処に関するベストプラクティスの交換等の緊密な情報共有、より実践的な共同訓練の実施、日米防衛当局間で共有するシステムのセキュリティ確保のための体制強化等の協力等を通じ、米国との連携を更に強化し、もって日米安全保障体制の実効性を高め、抑止力の向上に寄与する。

また、サイバー空間がグローバルに拡大していることを踏まえ、関係国や国際機関等との協力を積極的に推進するため、今後も、様々なレベルでの協議等を通じ、情報共有や関連施策に関する意見交換を実施するとともに、相互理解や信頼醸成措置の構築を推進し、グローバルなサイバー安全保障における協力体制の構築に積極的に寄与する。

(2) 動的対応に備えた「基礎体力」の向上

サイバー事案に対して国際連携・共助により動的に対応するためには、それを可能とする十分な「基礎体力」として、各国における基本的な能力や対応体制の存在が不可欠である。サイバー空間はグローバルにつながっており、グローバルレベルでのサイバーセキュリティ水準の底上げを図り、サイバー空間という輪の中で、脆弱なノードを減少させることが必須である。

そのような取組の結果として、サイバー空間における悪意ある活動等の抑止効果も期待される。

① グローバルな浄化活動体制の構築支援

サイバー事案に対して各国が協力し、動的な対応をしていくための基礎となるのが、各国におけるサイバー事案の検知、分析や対処のための体制である。サイバー事案のグローバル化に対応し、こうした体制の構築をグローバルレベルで進めていくことが必要である。

このため、我が国の経験を活かし、CSIRT 構築支援や運用能力の開発支援や、ボット駆除対策、悪性サイト検知・マルウェア対策、重要インフラのサイバーセキュリティに係る情報共有の仕組みなどの知見を提供する。

特に、我が国は、アジア太平洋地域、アフリカ諸国等幅広い地域に対する CSIRT 構築支援の豊富な実績や、近年重要性が増している制御システムに関し CSIRT 構築を実施した知見を有しており、それらの経験を活かした支援を拡充していく。

また、我が国では、世界に先駆けて 2006 年から ISP 事業者等の協力を得てネットワーク型のボットウィルス感染対策を実施し、ボット感染率が劇的に低下するなど先進国におけるモデルとなっており、今後、ISP 事業者等の協力のもと悪性サイト情報を蓄積するデータベースの構築、当該サイトへのアクセスに対する注意喚起等の新たな取組を開始予定であり、そこで得られた知見を積極的に提供していく。さらに、多国間の CSIRT 連携によるボット駆除の取組も推進していく。

重要インフラシステムについては、社会経済活動の根幹をなすとともに、安全保障面からも高い安全性が求められており、我が国では、サイバー攻撃への耐性面等において高い安全性を有するよう構築されている。重要インフラシステムの構築支援の際には、こうしたサイバーセキュリティ面の優れた対策もあわせて提供する。

なお、浄化活動体制の構築に際しては、各国におけるサイバー攻撃、サイバーセキュリティの取組の実態を定量的に評価できる指標が重要であり、OECD（Organization for Economic Cooperation and Development）等における指標の策定・測定等の取組に対し、我が国として積極的に協力、貢献していく。

② 啓発活動の推進

サイバー事案への対応が十分に機能するためには、それを支える運用や政策の担当者が一定の能力を有すること、あらゆる主体が一定のセキュリティ意識・能力を有することなど、関係主体のサイバーセキュリティに対する認識、基本的な人的対応能力の確保

が必要である。我が国は、高度な能力を有する人材や高い水準の技術施設等を活用し、種々の能力開発や意識啓発活動を継続的に実施してきており、様々な知見の十分な蓄積がある。

このため、我が国の知見を活かし、政府や企業のサイバーセキュリティ担当者や CSIRT 担当者などに対するサイバーセキュリティ確保に関する研修の実施等を通じたキャパシティビルディングや周知啓発用の素材の提供など意識啓発の動きを世界に拡げる活動を行うことにより、国際的なセキュリティレベルの底上げに寄与する。

特に、我が国では、サイバーセキュリティに関する国際的な意識啓発キャンペーンを毎年 10 月に実施しており、同様の意識啓発活動を実施する国々と連携して、こうしたキャンペーンをよりグローバルレベルで拡充するための働きかけを行う。

③　国際連携による研究開発の強化

高度化・巧妙化するサイバー脅威に対処するための技術的な対応にあたっては、より高度な対策技術の開発が必須である。

このため、サイバー攻撃等に的確に対応できる高度な対策技術の開発に向け、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効であり、国際連携による研究開発を積極的に推進する。

また、開発した対策技術を速やかに実用化し、サイバー事案への動的対応や、浄化活動体制の構築支援に用いていくことが重要である。

特に、我が国では、サイバー攻撃、マルウェア等に関する情報を収集するネットワークを諸外国と連携して構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発・実証実験を実施するプロジェクト PRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）を進めている。本プロジェクトのパートナーを更に拡大することにより、グローバルレベルでのサイバー攻撃予知・即応能力の向上に貢献する。

(3) サイバーセキュリティに関する国際的なルール作り

サイバー空間において、価値観や制度の異なる様々な国が共存し、また、多様な主体により多様な利用が行われる中で、サイバー空間の便益を最大限享受するためには、サイバー空間の安定的利用の確保が重要である。中長期的な人的関係を強化しつつ、サイバー空間を利用した各種活動に対して国際的なルール作りを進めていくことが必要である。

① 国際的な技術基準策定

サイバー空間のセキュリティを確保するためのシステムなどは広く国際的に取引されるようになってきているが、その相互運用性や求められるセキュリティ水準を確保するための技術的な標準の重要性が増している。

このため、様々な国際標準化の取組が行われている中で、サイバーセキュリティ技術に関する国際標準の策定・普及や相互承認枠組作りを進めていくことが重要である。その際、実際に基準を用いて取引を行うのは企業などの主体であり、官民の連携による対応が不可欠となる。

我が国では、2013 年に制御システムセキュリティセンター（CSSC: Control System Security Center）を設立したところであり、CSSC を拠点として制御システムセキュリティの評価・認証技術を確立するとともに、その技術の利用促進のための評価・認証機関を設置し、CSSC に参加する企業や団体を中心として CSSC の活用による新たな国際標準の提案活動にも寄与する。また、サイバーセキュリティ対策の一環として、認証の国際的な相互承認の枠組みである CCRA（Common Criteria Recognition Arrangement）スキームを活用した調達を積極的に進める。さらに、ITU (International Telecommunication Union)におけるサイバーセキュリティ情報交換フレームワーク（CYBEX：Cybersecurity Information Exchange Framework）策定にも貢献してきており、引き続き、各国と連携を図りつつ推進していく。

クラウドサービスについては、我が国は、安全・安心にクラウドサービスを活用できるための ISO（International Organization for Standardization）・ITU におけるクラウドセキュリティの国際標準化のための活動を先導しており、早期の国際標準化に向けた活動に積極的に貢献するとともに、国内外の関連企業と具体的な対応マニュアルの策定・普及を進め、それにより得られた知見の共有の推進を図る。

なお、サイバーセキュリティの確保は重要であるが、自国の技術を優先させるなどの規制は国外の最先端セキュリティ技術等を排除し、その意に反して自国のセキュリティの低下に繋がることから、関係国相互の繁栄を念頭に置きつつ、行き過ぎた規制とならぬよう、透明性や公平性に配慮した国際的な貿易ルールに整合するように求めていく。

② 国際的な規範作り

サイバー空間の便益を最大限享受するためには、サイバー空間の安定的利用の確保が重要であり、国連総会第一委員会の下に設置された政府専門家会合（GGE：Group of Government Experts）による 2013 年 6 月の報告書において、国家の情報通信技術の利用

に関する規範に言及されるなど、サイバー空間の利用に関する国際的な規範作りのための取組が進んでいる。そのような取組が世界的に行われる中で、我が国として、あらゆる場を通じ基本的考え方を発信するなど、引き続き、積極的に貢献する。

具体的には、国家の情報通信技術の利用に関する規範に関し、サイバー技術の急速な発達に鑑み、サイバー空間を利用した各種行為に対して、過度な国家統制を行わない形で、法的拘束力のない緩やかな規範作りを早急に進めることが現実的である。我が国は、サイバー空間を利用した行為に対し従来の国際法が当然適用されるとの立場であり、国連憲章や国際人道法等は適用されるものと考えており、情報通信ネットワーク技術の特性に鑑み個別具体的な法規範がどのように適用されるかについて、更に検討を深めていく。また、上記の国連政府専門家会合の報告書策定には、我が国も参加国として積極的に議論に貢献し、サイバー空間を利用した行為に対する国際法の適用が確認されており、今後は、国際法の具体的な適用のあり方について、国際的な議論をリードしていく。

一方、サイバー脅威は現実のものとなっており、攻撃主体の特定が困難であることを踏まえ、攻撃主体の誤認など当事者が意図しない形でのエスカレーションによる不測の事態を回避するため、サイバー空間における各国・地域の行動の予測可能性を高め、信頼醸成措置を進めることが重要であり、引き続き、各種戦略の公表、CSIRT 間連携の強化、情報共有体制の構築等を通じ、各国との信頼醸成を積極的に図る。

なお、OECD における「情報システム及びネットワークのセキュリティのためのガイドライン」の見直しなど、社会経済面に力点を置いたサイバーセキュリティに関する政策枠組み構築のための取組が行われてきているが、そのような取組も規範作りに寄与するものである。我が国は、OECD における議論などに主体的な参画を図ってきており、引き続き、こうした取組を各国と連携し強力に推進する。

5　地域的取組

(1)　アジア太平洋地域

アジア太平洋地域は、我が国と最も地理的に近接し、経済的にも密接な関係があるため、サイバー脅威への対策でも、緊密な連携が必要であり、地域が団結・協力していくことが重要である。

アジア太平洋地域の中では、従前より我が国との関係が深いことに加え、近年の我が国企業による投資の増加等を踏まえ、特に ASEAN との関係は重要である。これまで ASEAN との間では、日・ASEAN 情報セキュリティ政策会議等を通じた継続的な取組に加え、日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議を実施しており、人材育成や、情報共有、重要インフラ防護等の体制構築などのキャパシティビルディングを推進するなど、更に連携を強化する。また、PRACTICE プロジェクトとマルウェア感染端末への警告を組み合わせた JASPER（Japan-ASEAN Security PartnERship）プロジェクトの推進により、日 ASEAN 間のサイバーセキュリティ技術協力を包括的に進める。このほか、TSUBAME プロジェクトとして、アジア域内の CSIRT と連携し、センサーを各 CSIRT に設置することで、アジア域内におけるサイバー攻撃にかかる傾向を早期に把握し警戒・対応策を迅速に採っており、このプロジェクトを通じたサイバー環境の浄化を強化する。さらに、サイバー犯罪対策分野においては、日・ASEAN 国境を越える犯罪に関する閣僚会合及び高級実務者会合等の枠組みを通じ、キャパシティビルディングや知見の共有などの日 ASEAN 協力を強化する。

その他諸国についても、重要なパートナー国として関係を深化させ、連携・共助によりサイバーセキュリティの課題解決を図る。特に、インドとの間においては、日印サイバー協議を行うなどの取組を行ってきており、引き続き連携を強化していく。

(2)　欧米

日米安保体制を基軸とした同盟関係にある米国との協力は重要であり、日米サイバー対話、インターネットエコノミーに関する日米政策協力対話や関係機関間での個別の対話の場などを通じ、政策協議や情報共有、サイバー事案対処等について具体的な協力を深めるなど、協力して様々な取組を進めていく関係を構築してきており、引き続き、そのパートナーシップを深化させる。

欧州諸国については、日英サイバー協議、日 EU インターネット・セキュリティフォーラムの実施や、欧州評議会で採択されたサイバー犯罪条約の締結など、共通の価値観を基礎に協力して様々な取組を進めていく関係を構築してきており、引き続き連携を強化していく。

(3)　その他の地域

南米やアフリカ地域などにおいても、サイバー空間の利活用が急速に進んできており、それに伴いマルウェアの感染をはじめとするサイバー脅威も拡大するなど、サイバーセキュリティ面での課題が顕在化してきている。我が国は、これら地域の国々との間でも、

CSIRT 構築支援などの協力を実施してきており、こうした取組を更に拡げていく。

(4) 多国間枠組

安全で信頼できるサイバー空間の構築に向けた取組は、多国間枠組みでも積極的に行われている。

サイバーセキュリティに関する国際的なルール作りやキャパシティビルディングに関して、国連、G8、ARF、OECD、APEC（Asia-Pacific Economic Cooperation）、NATO（North Atlantic Treaty Organization）等で活発に議論が進められている。また、重要インフラ防護や迅速な事案対処のための方策に関して、政府機関を中心とした Meridian、IWWN（International Watch and Warning Network）のほか、官民の幅広い主体が参加する FIRST（Forum of Incident Response and Security Teams）、アジア太平洋地域の CSIRT コミュニティである APCERT、サイバー空間に関するロンドン会議のフォローアップ会合などの場で、グローバルな取組が行われている。さらに、サイバー犯罪に対しては、ICPO 等を通じ、国際捜査協力の深化を図っている。

このような様々な場における取組に、我が国も積極的に参画してきており、安全で信頼できるサイバー空間の構築に貢献していくため、あらゆる場の議論に更に積極的に寄与していく。その際、これまで以上に有意義な貢献をするためには、我が国として、「顔の見える」形での貢献が重要である。そのため、2014 年に Meridian を日本で開催するなど、国際会議の開催を積極的に招致することなどにより国際社会への積極的な貢献を図る。

参考プロジェクト

【制御システムセキュリティセンター（CSSC：Control System Security Center）】

○　昨今、社会インフラを狙ったサイバー攻撃が世界的に増加し、社会に甚大な被害をもたらすおそれのあるリスクが出現。インフラを制御する情報通信技術システムの安全性確保の必要性の急速な高まりを背景に、2012 年 3 月、制御システムメーカー等が技術研究組合を結成。2013 年 9 月現在、18 社が同組合に加盟。

○　2013 年 4 月には、宮城県多賀城市に制御システムのセキュリティ検証施設である制御システムセキュリティセンター（CSSC）東北多賀城本部を構築。技術研究組合加盟メンバーが、制御システム向けの高セキュア化技術の開発や制御システムセキュリティ人材の育成等の活動を実施。

○　施設には、電力、ガス、ビルオートメーション、自動車工場、下水処理、スマートコミュニティ、化学プラントを模した小規模模擬プラントがあり、2013 年度に、これらを活用したサイバー攻撃に対処する演習や普及啓発事業を実施予定。

○　国内で制御システム機器のセキュリティ評価をできるよう、制御システム機器のセキュリティ評価・認証機関を設置し、国際的な評価・認証機関を目指す。

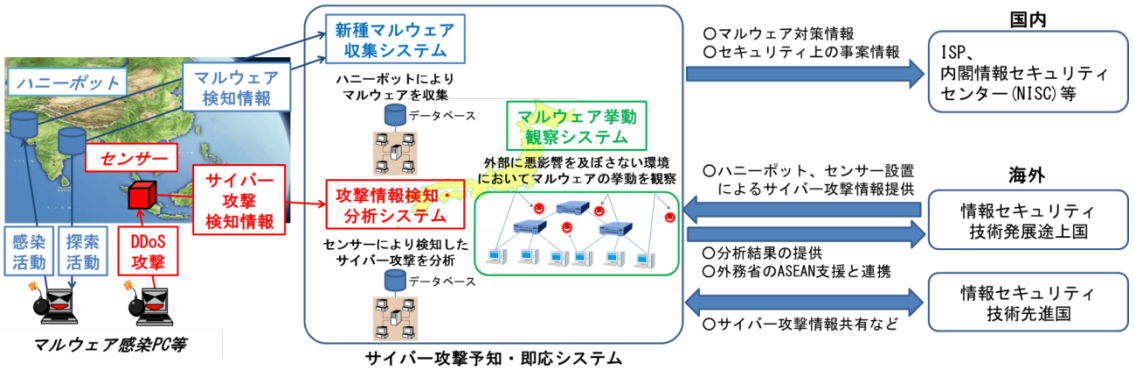
○　更に、海外からの関係者の視察の受入れや研修の実施、国際会議の開催等の活動も進めていく。

【PRACTICE（国際連携によるサイバー攻撃予知・即応技術の研究開発： Proactive Response Against Cyber-attacks Through International Collaborative Exchange）】

○　近年被害が拡大しているサイバー攻撃（分散型サービス妨害攻撃、マルウェアの感染活動等）に対処し、サイバー攻撃のリスクを軽減することを目的とし、2011 年度から実施中のプロジェクト。

○　日本内外のインターネットサービスプロバイダ、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術についての研究開発及び実証実験。

○　国際会議（二国間・多国間）等を活用し、諸外国の組織（インターネットサービスプロバイダ、大学等）に対し、サイバー攻撃観測データや分析結果等の情報共有や研究開発等での連携を呼びかけ。



（参考）プロジェクトの概要

－　ネットワークセキュリティの ISP 団体であるテレコムアイザックジャパンや、研究機関である NICT、パートナー企業等とともに実施。

－　攻撃の予兆をつかむため、いくつかの要素技術の研究開発を実施中。2015 年までに技術を確立し、即応能力の向上に貢献することを目指す。

※　JASPER（Japan-ASEAN Security Partnership）

・　日本と ASEAN 間のネットワークセキュリティの技術協力の強化を目的とする日本と ASEAN 間の連携プロジェクト

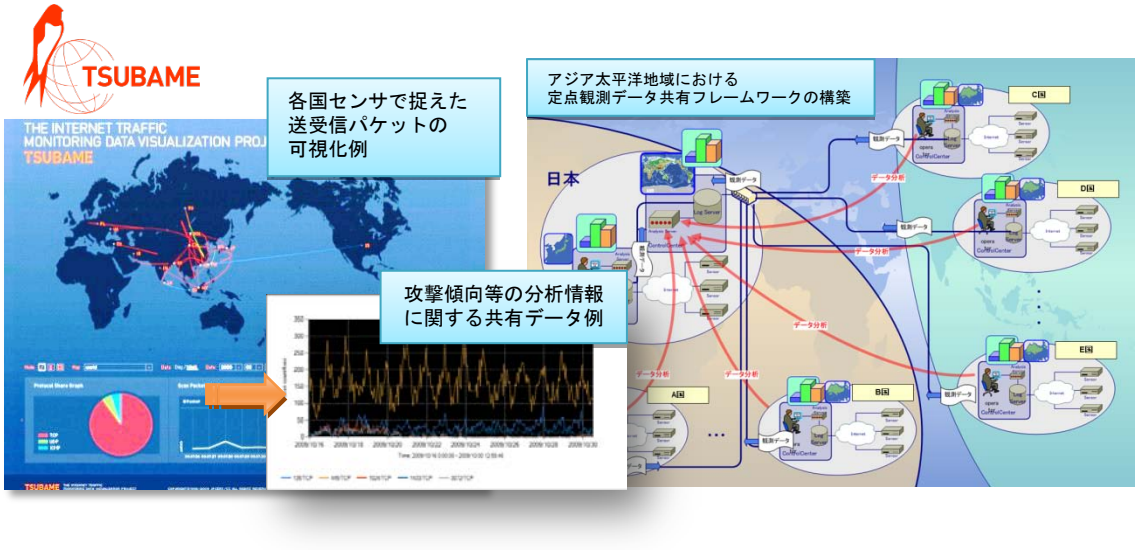
・　2013 年 9 月に開催された「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」で開始を確認

・　PRACTICE プロジェクトに、マルウェア感染端末への警告を併せて構成

【TSUBAME（国際協働ネットワーク定点観測プロジェクト）】

○　TSUBAME は、2007 年から実施しているインターネット定点観測可視化プロジェクト。アジア太平洋地域のコンピュータセキュリティインシデント対応チーム（CSIRT※）のコミュニティであるアジア太平洋コンピュータ緊急対応チーム（APCERT）の枠組みで展開しており、JPCERT/CC が中心となって取組を実施。

○　本プロジェクトは、アジア太平洋地域におけるインターネットの定点観測結果を可視化するものであり、主に同地域のナショナル CSIRT との協力により、観測のためのセンサーを設置（2013 年 9 月現在、20 経済地域/23 チームに設置済）。各センサーで検知されたネットワーク上の悪意のある活動が一つにまとめて表示され、それを全てのメンバーで共有し、対応するというプロセスを通じて、CSIRT 間連携（国境を越えて発生するセキュリティインシデントへの対処や脅威情報の共有、分析協力等に関する平常時からの協力）を強化するのが狙い。



（参考）プロジェクトの概要

－　各国の CSIRT と連携して観測されたデータを共有し、状況把握と早期対応の分析基盤を作ることでインシデント対応等のオペレーションレベルでの連携が可能に。

－　観測データを分析した結果を共有し、レポートを発行するなどにより、インシデント対応に使用。また、定期的に TSUBAME ワークショップ（年 1 回）を開催し、分析手法の共有や分析能力の向上、インシデント対応への応用のスキルアップ等を実施。

－　参加メンバーで、各地域のワームの感染活動や弱点探索のためのスキャンの動向の分析・情報交換の実施、ワームの感染活動や弱点探索のためのスキャンの動向を効率的に把握するための脅威の可視方法などもテーマとして共同で研究。

※ Computer Security Incident Response Team の略。サイバー攻撃発生時等の連絡窓口となり、また、その際の対処を行う専門組織。