我が国の情報セキュリティ分野における
国際協調・貢献に向けた取組み

情報セキュリティ政策会議

２００７年１０月３日

目次

第１章　情報セキュリティ分野における国際協調・貢献[1]に向けた取組みの必要性

（１）我が国の情報セキュリティ政策において国際的な観点[2]が求められる理由

近年、我が国の国民生活・社会経済活動のあらゆる側面において、ＩＴへの依存度が高まってきている。国民生活では、医療、福祉、教育等の多方面において、ＩＴの利用・活用は、先進諸国等が直面する社会的課題を解決し、国民生活を向上させるために不可欠となりつつある。社会経済活動においては、企業がグローバル化・分散化に対応し、企業は強固な国際競争力と高い生産性を維持するため、ＩＴの利用・活用を急速に拡大している。このようにＩＴが国民生活、社会経済活動に不可欠となりつつある中、ＩＴの安心・安全の確保は重要な国家目標とされてきた。

ＩＴ基盤は、２４時間・３６５日、常時世界ともつながっているため、仮に我が国のＩＴ基盤に何らかの障害が発生した場合に、その影響が我が国に留まらず、諸外国に急速に拡大する可能性がある。逆に、諸外国において、ＩＴ基盤に何らかの障害が起こった場合には、我が国の国民生活・社会経済活動に負の影響が生じる可能性もある。さらに、非意図的な要素に起因するＩＴ障害に限らず、海外からの意図的な攻撃が、国境と関係なく容易に国・地域内の重要なビジネスインフラ等に被害を発生させる可能性がある。したがって、情報セキュリティ問題を考える上では、ＩＴのボーダーレス性という特徴を意識して、我が国を含む各国が連携・協調を図り、地球規模、すなわちグローバルな「ＩＴを安心して利用可能な環境（以下、「ＩＴ安心利用環境」という。)」の構築に向けた努力が不可欠である。

我が国では、世界一の高速で安価なブロードバンド網などＩＴ基盤が発達し、この基盤を利用したサービスやビジネスも進展している状況にある。そのため、我々は、世界のトップランナーとして情報セキュリティに関する問題解決を率先して進め、また積極的に情報セキュリティ分野における国際連携・協調を進めることで、グローバルなＩＴ安心利用環境の構築に大きな貢献を行うべき立場にあることを自覚する必要がある。

また、社会経済活動のグローバル化という現実の前においては、こうした取組みを通じて、グローバルなＩＴ安心利用環境を構築し、我が国のみならず世界全

---

1 ここで、「国際」とは「国内」に対比される概念であり、かつ一国家を超えるという意味での「国際」を意味している。しかし、本文書においては、「国際」を、原則、「グローバル（地球規模)」とは異なる概念であり、かつ「国家」と「国家」との際（例えば、日本と米国、日本とＥＵなど）という意味での「国際」という意味で用いる。

2 ここの「国際」も注１と同じ意味で用いている。

体の情報セキュリティ問題への対応が進むことが、ひいては我が国の国民生活・社会経済活動の安心を確保することにつながる。

こうしたことから、情報セキュリティ政策においては、国際的な観点が不可欠である。

（２）第１次情報セキュリティ基本計画と同計画での国際分野の位置付け

我が国において情報セキュリティ問題に対処するための中長期の戦略である「第１次情報セキュリティ基本計画」（以下、「第１次基本計画」という。）は、２００６年２月２日に情報セキュリティ政策会議によって策定された。

第１次基本計画では、基本目標[3]達成への方向性として、ＩＴ社会を構成するあらゆる主体が、それぞれの立場に応じた適切な役割分担の下で対策を実施する、情報セキュリティにおける「新しい官民連携モデル」を構築し、取組みを進めていくこととされている。そして、そのための方策として、「官民各主体の共通認識の形成」、「先進的技術の追求」、「公的対応能力の強化」、「連携・協調の推進」の４つの基本方針を、すべての主体が共有し、問題に取り組んでいくことが必要とされている。

「国際協調・貢献に向けた取組み」の策定を含む国際分野の取組みは、第１次基本計画における「基本目標」を達成するための一部であり、上記４つの基本方針のうち、「連携・協調の推進」に位置付けられる。

（３）国際分野に係るこれまでの取組みとその成果

情報セキュリティ政策の国際分野に関しては、我が国は第１次基本計画等に基づき、なるべく多くの国・機関が参加するフォーラムなどで国境を越えて取り組むべき課題を議論し、各国で足並みを揃えた対応策を採ることや、具体的な脅威にさらされる前の段階の予防的措置として、国際的なレベルでのセキュリティ文化の醸成や、情報セキュリティのリテラシー向上に努めるべく、取組みの第一歩を行ってきた。具体的には、内閣官房を中心とした日本国内における情報セキュリティ政策の取組みを多国間のフォーラム等で紹介するとともに、議論に積極的に参加してきた。

[3] ＩＴ安心利用環境の構築によって、ＩＴの利便性と情報セキュリティの両立を図り、「情報セキュリティ先進国」の実現を目指すことを基本目標としている。

また、このような多国間のフォーラム等で、諸外国の情報セキュリティ機関・関係者とコンタクトを取り、緊密に連携が取れるような窓口を確保すれば、海外からの情報が入手でき、情報セキュリティ面の国際的な流れに対する理解・対応を早めることができる。このように、国境を越えて取り組むべき情報セキュリティ問題に対応するため、内閣官房情報セキュリティセンターは、政府横断的な情報セキュリティ問題に関する我が国としてのＰＯＣ（Point of Contact）の機能を明確化し、一定の成果を収めてきたところである。

しかしながら、具体的な国際協調や貢献については、取組みはまだ一歩目に過ぎず、これから本格化が必要な段階である。この背景には、第１次基本計画は、情報セキュリティ政策を国際的な観点からどのように進めていくべきか、理念を明確に示す一方で、具体的な国際協調や貢献の内容や方法については踏み込んだ記述がなく、後日の検討に委ねられていたことが挙げられる。

（４）セキュアジャパン２００７（以下、「ＳＪ２００７」という。）における国際分野の規定と取組みの推進

こうしたことを踏まえ、ＳＪ２００７（２００７年６月１４日情報セキュリティ政策会議決定）においては、２００７年度に、「情報セキュリティ先進国」の実現を目指す上で、国際的に連携すべき具体的な事項や連携先等を明確化し、また、政府全体として戦略的に国際協調・貢献に取り組むための基本方針及び具体策を検討することが盛り込まれた。

本文書においては、各地域または情報セキュリティ政策領域に応じて、情報セキュリティ政策上の国際協調・貢献をどのように推し進めていくかの基本方針等を、第１次基本計画で言及される基本目標を達成するための一要素として明確化する。

その際、第１次基本計画において言及されている、我が国発の付加価値の高いイノベーションの創出、先見性をもった技術開発の国際的活用、「ベストプラクティス（模範例）」の普及・啓発、国際的な標準開発への貢献等を通じ、我が国の強みを発揮しつつ、ＩＴ先進国として国際社会における役割を積極的に果たしていくことにも留意する必要がある。

第２章　基本認識

（１）グローバルなＩＴ安心利用環境の実現に向けた取組分野

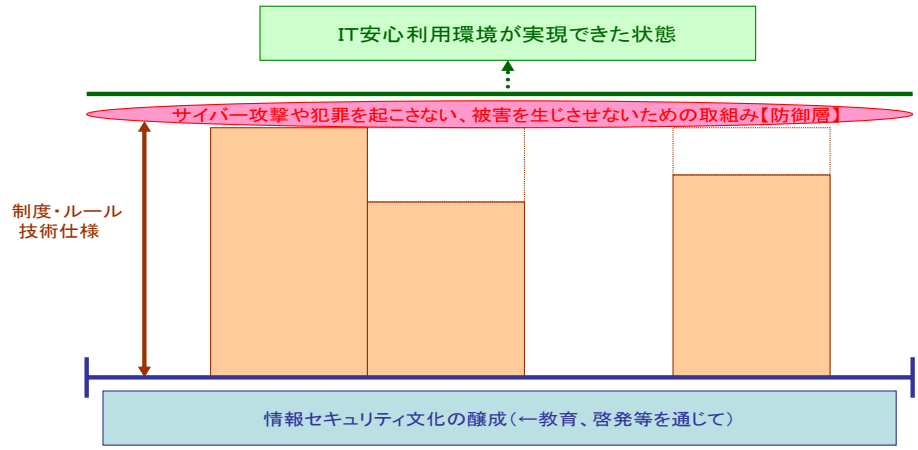
グローバルなＩＴ安心利用環境の実現に向けて努力を行うに際しては、どのような取組分野に関する手法を積み重ねていくべきであろうか。既にOECDなどの国際会議で議論がなされている方策や、我が国を含む各国が取り組んでいる政策との重複も意識しつつ改めて分類を行うと、以下の３つの分野（４つの方策）に分類されると考えられる。

第一に、ＩＴ利用者のモラル・認識の形成・向上に係る分野が挙げられる。これは、セキュリティ文化の醸成などの形で、国際機関をはじめとする様々な「場」において取組みが進められている。ＩＴ利用者の習慣や心理的なレベルに働きかけることで、グローバルにＩＴ安心利用環境の構築を進めるものである。

第二に、ＩＴ利用環境の整備に係る分野が挙げられる。具体的には、（１）ＩＴ利用に関連する制度やルール、（２）ＩＴ利用の際に使用される機器等の技術的な仕様、について利用者が主体的かつ安心して適切な利用を行える環境を整備することで、グローバルにＩＴ安心利用環境の構築を進めるものである。

第三に、サイバー攻撃やマルウェア[4]、サイバー犯罪、非意図的な要素に起因するＩＴ障害等、ＩＴ利用に対して若しくはＩＴを利用して被害を発生させる行為への対応に係る分野が挙げられる。これは、ＩＴ利用に関連した問題に適切な対応を実現することで、グローバルにＩＴ安心利用環境の構築を進めるものである。

グローバルなIT安心利用環境の実現に向けた取組分野の構造



4 コンピュータウイルス、ワーム、スパイウェア等の「悪意をもった」ソフトウェアのこと。

（２）グローバルなＩＴ安心利用環境の実現の過程

グローバルなＩＴ安心利用環境は、上記（１）のような分野に関して、様々な取組みを行うことで実現されるものと考えられるが、その実現に向けた過程は、個々の取組みに応じて以下のような二つの方向性が考えられる。

第一には、国際機関や各国政府等が協調して全世界的な取組みを進めることで実現に向かうという過程が考えられる。例えば、国際機関などのグローバルな枠組みにおいて、参加政府のコンセンサス方式でグローバルに効果が及ぶような取決めがなされていく過程が典型例である。最初から合意事項や合意ルールを決めて、合意の効力をグローバルに及ぼすという意味で、いわば「トップダウン方式」というべきものである。

第二には、各国が国内政策として進める取組みや、例えばＥＵの域内政策など、一主権国家の枠は超えるものの地域内において共通政策として進められる取組みが、国家間や地域間で調整を行いながら止揚され、最終的にグローバルな合意に辿り着くという過程が考えられる。地域内政府間や地域間などでＩＴ安心利用環境の構築に向けて調整を行っていく取組みが、最終的にグローバルなＩＴ安心利用環境に到達する、または到達し得るという意味において、「ボトムアップ方式」というべきものである。

実態的に見ると、情報セキュリティ問題は、必ずしも世界で均一に発生し顕在化するわけではなく、局地的に発生する場合も少なくない。これら局地的に発生する問題への対応については、問題の地域的な特性に応じた形で、各国ごと、地域ごとの取組みに着目しながら対応する必要があるため、「ボトムアップ方式」という観点が欠かせないのは事実であろう。局地的な問題の例としては、例えば、国外からの企業の進出が多い地域においては、事業上の秘密情報の入手を目的とした情報漏えいなど、経済上の動機に基づくものがある。また、ＩＴが重要な社会的・経済的活動を支えるインフラとして利用・活用されている現在、特定の国・地域内のビジネスインフラ等に対する意図的なサイバー攻撃等、ＩＴに起因する脅威が、ひいては当該国・地域の安全保障上の懸念を惹起する場合がある。さらには、災害や事故などにより、通信トラフィックの物理的なボトルネックにおいて情報セキュリティ問題が顕在化し、国民生活を支えるＩＴ基盤を脅かすような事態も実際に経験してきたところである。

したがって、我が国がグローバルなＩＴ安心利用環境の構築に向けて国際的な

協調・貢献[5]を進めるに際しては、取組みに応じてその効果が最大となるように、また課題ごとに世界における議論方式の趨勢がトップダウンであるのかボトムアップであるのかを見極めながら、どちらの過程に則って施策を進めることがグローバルなＩＴ安心利用環境の実現に向けて、より大きく貢献できるかという観点を考慮しながら決めていくことが不可欠である。

以上より、グローバルなＩＴ安心利用環境に向けた取組みについては、我が国がグローバルな観点を中心に作用すべき部分、リージョナルな観点を中心に作用すべき部分、また双方の観点から作用すべき部分が存在すると言える。

（３）グローバルなＩＴ安心利用環境の実現に関わる対応者（プレーヤー）

グローバルなＩＴ安心利用環境の実現に向けては、様々な対応者（プレーヤー）が、（１）で述べた取組分野についてグローバル、リージョナルな枠組みの下、様々な取組を積み重ねていくことが必要であり、また、実態としてもこのような構造となっていると考えられる。では、対応者としては実際にどのような「者」がグローバルなＩＴ利用環境の実現に向けた取組みを行い、役割を果たしているのであろうか。

第一に、国際機関が挙げられる。例えば、OECD のような先進国を中心とするメンバーによる国際機関や、欧州地域やアジア地域といった地域に立脚した（地域の）国際機関のように、様々な種類の国際機関が存在している。これらは、グローバルなＩＴ安心利用環境の実現に向けて、グローバルまたは地域内のコンセンサスを作っていくための「場」を提供する役割を果たしている。

第二に、各国政府が挙げられる。各国政府は、自国内の情報セキュリティに関する取組みを通じて、また、各国間、地域間等での議論を通じて、グローバルなＩＴ安心利用環境の実現に向けた取組みを進めていると言える。

第三に、重要インフラが挙げられる。重要インフラ事業者の提供するサービスには、それ自体国境を越えて提供される性質を持つものや、国境を越えて活動を行う企業等に代替が著しく困難なインフラを提供するものも多く存在し、このような重要インフラの情報セキュリティ水準の向上は、ＩＴ安心利用環境の実現に大きく貢献する。特に、OECD 等の国際機関において[6]、重要情報インフラ[7]保護に

---

[5] ここの「国際」も注１と同じ意味で用いている。

[6] その他、ITU、G8 においても「重要情報インフラ」の用語を元に、各国のベストプラクティスの共有、取組のための連携の強化等を推進する動きが存在している。

[7] 2007 年２月に発表された、重要情報インフラ保護に関するカナダ、韓国、英国、米国の政策比較報告書の

おける国際連携を強化することが模索されるなど、グローバルなＩＴ安心利用環境に向けた取組みが行われている。

第四に、企業が挙げられる。特に国際的に展開する企業は、国家という枠組みを超えて、グローバルにビジネス活動を展開することから、各国におけるビジネス活動に際して各々の現地で実現しようとする情報セキュリティ対策の取組みが、そのまま各々の現地の情報セキュリティ水準を向上し、ひいてはグローバルなＩＴ安心利用環境の実現に貢献することとなる。

第五に、ＮＧＯ・ＮＰＯが挙げられる。例えば、コンピュータソフトウェアの脆弱性に関する情報の共有等を行うようなCERT/CCのような組織や、ＩＴ利用に際してのモラル向上のための啓発活動を個人に対して行うような組織は、その活動がグローバルなＩＴ安心利用環境の実現につながるものであると言えよう。

第六に、個人が挙げられる。個々人の情報セキュリティ向上も、グローバルなＩＴ安心利用環境の実現に貢献していると言える。

（４）情報セキュリティ分野に関する国際協調・貢献

① 情報セキュリティ分野に関する国際協調・貢献とは

以上を踏まえて、本書において検討を行う「国際協調・貢献」について定義を行う。本戦略における取組みの主体は、「我が国政府及び我が国情報セキュリティ政策に関わりを有する者（以下、「取組主体」という。）」であることから、「国際協調・貢献」に向けた取組みは、グローバルなＩＴ安心利用環境の実現に向けた我が国の協調・貢献を進めるために、こうした取組主体が、グローバル社会での対応者（プレーヤー）の行う、モラル・認識の向上、情報セキュリティに関する制度・ルール、技術仕様を通じた環境整備、サイバー攻撃等に対する対応、の３つの分野（４つの方策）に対して、どのように、また具体的にどのような作用を行うべきかを記述するものである。

② 国際協調・貢献に向けた取組みの検討の視点

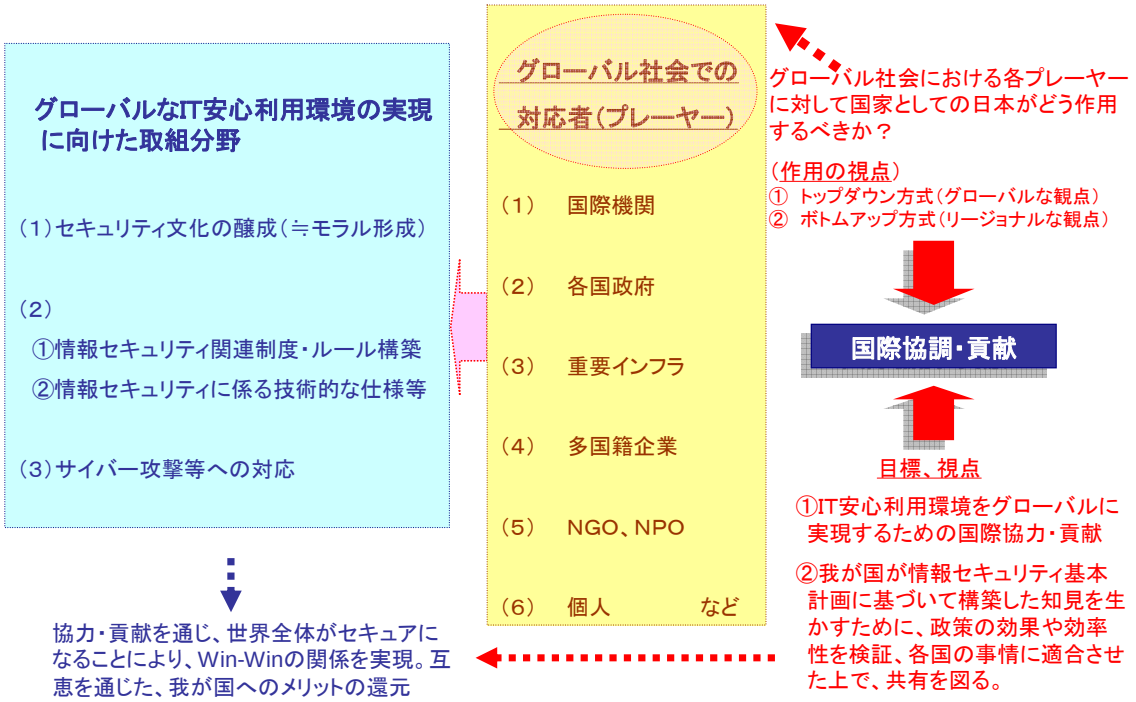
国際協調・貢献の取組みの検討にあたっては、グローバルなＩＴ安心利用環境の実現に向けて、我が国が如何に意味のある国際協調・貢献を行うかということが基本的かつ最重要な視点となる。このような視点に立つと、我が国が情報セキ

中で、①国家の重要インフラを支える情報の要素②政府の業務の不可欠な要素を支える情報インフラ③国家経済に不可欠な情報インフラの概念のうち、一つもしくはそれ以上の概念が重要情報インフラを描写すると考えられるとしている。

ュリティ基本計画に基づいて構築した政策体系の下で行ってきた取組みから得られた知見を生かすために、再度、政策体系の効果や効率性などの検証を行い、その上で世界全体や各国の実情等を十分考慮し、適合させた上で、共有していく必要がある。このように取り組むことで、知見の共有対象に対して、我々の政策体系からより効果的なものを的確に共有していけるものと考えられる。

また、国際協調・貢献の取組みの実施においては、我が国の国益という観点も無視することはできず、特に政府の取組みには、国益を預かる立場としての視点も加味する必要がある。しかしながら、グローバルなＩＴ安心利用環境という目標設定は、我が国の協調・貢献を通じて世界全体や各国がセキュアになり、その結果我が国もメリットが享受できるという win-win の関係を実現することにつながるため、互恵を通じて十分に我が国の国益に資するものであるといえる。

「情報セキュリティ分野における国際協調・貢献に向けた取組み」における
我が国政府等とグローバル社会での対応者（プレーヤー）達の関係



第３章　具体的方策と国際協調・貢献

（１）国際協調・貢献に向けた取組みの検討にあたっての考え方

グローバルなＩＴ安心利用環境の実現に向けた国際協調・貢献の検討は、２．に即して考えると、「グローバルなＩＴ安心利用環境の実現に向けた取組分野（３つの分野（４つの方策））ごとに、個々の「対応者（プレーヤー）」に対して、「我が国政府及び我が国情報セキュリティ政策の推進に関わりを有する者」がどのような作用、すなわち取組みを行うか、という方法で行うべきである。また、その際、取組みを、(i)「トップダウン方式」での実現を目指してグローバルな枠組みで取り組むものと、(ii)「ボトムアップ方式」での実現を目指してリージョナルな枠組み[8]で取り組むものに分けながら、検討を行うべきである。

しかし、実際にこの考え方に沿って、「トップダウン方式」を念頭に置いたグローバルな枠組み及び「ボトムアップ方式」を念頭に置いたリージョナルな枠組みの双方において、３つの取組分野（４つの方策）全てに関し、全ての対応者（プレーヤー）に対して遍く取組みを行うことは、投入可能な政策資源の限度という観点からも現実的ではない。

そこで、グローバル、リージョナル（米国、欧州、アジア）の枠組みごとの現状等を明らかにした上で、これらを踏まえた取組みを行うことで、その効果の向上及び政策資源の有効活用を図る。

8 リージョナルな枠組みでの検討においては、日本企業の経済活動の傾向や国民生活の現状、安全保障上の理由等を考慮し、重点的検討地域として、ａ）米国、ｂ）欧州、ｃ）アジアの３地域を設定する。

（２）グローバル、リージョナル（米国、欧州、アジア）に関する現状等の認識

（ア） グローバルな枠組みの現状等の認識

情報セキュリティの分野は、取組みの歴史が比較的浅いものの、グローバルレベルにおいては、各国の協力に基づく情報共有等の形をとり発展してきており、その重要性が徐々に認識されるようになりつつある。このような議論は、OECD、APEC、ITU、ISO 等の既存の国際機関による枠組みの他、セキュリティ課題の特性に応じた、事案対処や脆弱性情報のハンドリング等を扱う組織によるフォーラムである FIRST（Forum of Incident Response and Security Teams）、ベストプラクティスの交換に取り組む Meridian 等の国際的枠組みを通じた活動という形でも活発化しつつある。

ＩＴ先進国である我が国は、先進的な取組みの紹介、他の先進的取組を行っている国・地域との協調等を通じて、グローバルな意志決定過程に積極的に関与することが求められている。我が国は、横断的な情報セキュリティ問題に関するＰＯＣ（Point of Contact）の機能を明確化し、関係機関との情報交換・共有等において、一定の成果を上げてきたが、今後は、具体的な取組みのルールや標準の議論

についてもますます本格化していく可能性が高く、トップダウン方式での実現を目指す政策についての積極的な議論への参加が重要である。

（イ） リージョナルな枠組みの現状等の認識

(A) 米国

米国は、自由・民主主義・市場経済といった世界で拡大しつつある価値観を象徴する国であり、ＩＴを利用・活用した経済活動という側面においても、世界を牽引している[9]。また、サイバーテロ対策等、ＩＴに起因する新たな脅威・リスクへの対策を通じたＩＴの安心利用環境の実現という面においても、複数の関係機関が横断的に連携し、先進的な取組みを行い、グローバルな取組みにも影響を与えている。

情報セキュリティ面においても、取組みの進展している日米両国の間で密な関係を維持することはグローバルなＩＴ安心利用環境の実現に向けた取組みを推進するに当たって、不可欠な要素の一つである。

現在、日米関係は、良好に推移しており、社会経済面、安全保障面において、双方にとってかけがえのないパートナー国である。こうした両国の関係は、日米両国の経済的繁栄と平和の維持に大きく寄与しており、情報セキュリティ分野においても、今後ともこの関係を維持することが肝要である。特にサイバー攻撃への対応等のＩＴに起因する脅威に関する側面に関しては、協力関係が重要である。

(B) 欧州

ＥＵは市民社会の成熟等を背景に、環境、健康、安全等の分野で先進的な規制の策定・施行に積極的に取り組んでいる。ＥＵは、このような域内規制の効果を実質上域外に波及させる等、多様性に富む域内各国での合意を通じて、リージョナルな取組みを成功させ、国際社会における様々な取組みをリードしている。こうした取組みからも明らかなように、ＥＵは、個別の国家という枠を超えた、地域での取組みを続け、着実に成功してきた先駆者であると言える。

情報セキュリティ面に関しても、ＥＵは、従来、プライバシー保護等の側面で議論を進めてきたが、今後は情報セキュリティマネジメント、事業継続性や危機管理といった分野に関連して、国際社会の取組みに大きな影響を与える可能性がある。我が国は、先進的な取組みを行う立場として、ＥＵの取組みに積極的に関

---

9 米国は特にBtoC（Business to Consumer）分野の電子商取引（ＥＣ）において、2005年時点で日本の4.5倍以上の市場規模を持っている。（１ドル＝110.2円換算）「平成17年度電子商取引に関する市場調査（経済産業省）」この市場規模は、欧州全体の2006年時点での総額とほぼ同じである。（１ユーロ＝１５５円換算）（http://www.electronicretailermag.com/info/0607_euro.html を元に算出）

与し、我が国の戦略の参考としていくことを通じて、より効率的・効果的な形でのグローバルなＩＴ安心利用環境の実現に向けたコンセンサスを形成していくことが求められている。

日ＥＵ間は、直接投資、貿易ともに安定し、密接な経済関係が保持されている。情報セキュリティ面においても、これまで以上に関係を深化させていくことが必要である。

(C) アジア

アジアは、我が国を含め、元来、言語、文化、宗教等の様々な面において、他には見られないほど多様性に富む地域である。このような多様性は同時に社会経済、文化等の面で大きな付加価値を創造する潜在性を持っており、アジアのような多様性の存在する地域において受け入れられるものは、普遍的なものとしてグローバルにも受け入れられ易いものと期待される。また、経済面では、近年、アジアは、地域外からの直接投資に加え、域内でのアウトソーシングの規模も急速に拡大[10]しており、著しい発展を遂げている。また、アジア地域は、世界全体の６０％[11]もの人口が集中しており、多様かつ多数の人材の宝庫としての地位を確立するため、高度なＩＴ基盤をはじめとする社会インフラ分野のみならず、人材育成も極めて重要な課題となる。

日本は、アジアにおける多様性を代表する一国であり、またこのように成長著しい諸国と地理的に隣接することにより経済発展の恩恵を受けている。今後も、米国、ＥＵと並んだ経済大国として、アジア地域における経済の更なる活性化への原動力としての役割が求められている。情報セキュリティ面においても、アジア域内において、多様性に十分に配慮しつつも、多様性からより大きな価値を創造するために、試行錯誤を含めた努力を継続することが重要である。

我が国との関係で見ても、アジア地域への我が国からの直接投資や業務のアウトソーシングが拡大し、経済関係の深化が進んでいる。また、政府ベースでもＦＴＡ／ＥＰＡの締結などを通じて、関税撤廃や投資規制の緩和などの措置が実現しつつある。今後は、こうした経済関係の深化を担保するために、例えばビジネスインフラであるＩＴ基盤に関しては、ＩＴ安心利用環境の実現が極めて重要な状況にあり、情報セキュリティ面での協調・貢献が不可欠である。

---

10 2006 年 6 月の IDC 調査によると、日本を除くアジア太平洋地域のＩＴアウトソーシング市場は 100 億ドルを突破し、前年に比較して 10.9%の伸びを示している。

11 United Nations, World Population Prospect 2006 年版

（３）グローバルなＩＴ安心利用環境の実現に向けた具体的方策の検討

以下では、（２）で明らかにしたグローバル、リージョナル（米国、欧州、アジア）に関する現状の認識等に基づき、グローバルなＩＴ安心利用環境の実現に向けた我が国の国際協調・貢献のための方策を検討する。

① グローバルな枠組み

ここでは、グローバルな枠組みで作用を行うべき課題について整理を行うとともに、取組方策を検討する。また、取組方策を、２．の枠組みにも沿った形で整理を行う（以下、（　）内は「取組分野」、【　】内は作用を行う先の「対応者（プレーヤー)」である)。

- グローバルな経済活動の条件を規定する、情報セキュリティに係る国際的なルールや標準に係る議論への積極的な参加・貢献

（制度・ルール）【国際機関】

← （国内での検討後、）ITU、ISO 等の国際フォーラムにおける提案や議論への積極的な参加

（制度・ルール）【国際機関】

- 情報セキュリティに係る諸権利（ＩＴ安心利用環境で国民生活、経済活動を行うことができ、仮にＩＴに起因する脅威によって被害を受けた際の救済を受けることができる権利等）についての検討を行うこと

← OECD 等の国際フォーラムにおける議論への積極的な参加・貢献

（制度・ルール）【国際機関】

- 国際的に活躍する企業との協力による、グローバルな情報セキュリティ水準の向上に向けた貢献

← （国際的に活躍する企業が事業活動を行うに際して有するべき情報セキュリティの取組水準等について、十分に検討を行い、）技術面、組織管理面双方におけるベストプラクティスを構築するとともに、普及を目指す

（制度・ルール、技術仕様）【企業】

- 重要インフラ分野における、グローバルな情報セキュリティ水準の向上

に向けた議論への参加・貢献、及び国際機関で決定された制度・ルールと国内施策との整合性の確保

← OECD 等の国際フォーラムにおける議論への積極的な参加・貢献
（制度・ルール）【国際機関】

・ グローバルな規模でのセキュリティ文化醸成のための議論への積極的な参加・貢献

← OECD、APEC-TEL、IGF 等の国際フォーラムにおける議論への積極的な参加・貢献
（モラル）【国際機関】

・ 日本に投資を行う国際的に活躍する企業の情報セキュリティ水準確保による我が国国民生活の安心・安全の確保

← （日本に投資を行う国際的に活躍する企業が有するべき情報セキュリティの取組水準等について、十分に検討を行い、）技術面、組織管理面双方におけるガイドライン等を策定し、普及活動を推進する
（制度・ルール、技術仕様）【企業】

・ 国際的なＩＴ障害への対応のため、各国で協力してネットワークインフラの予備代替等についての検討を進めること

← （国内で検討後、）国際フォーラムにおける議論への積極的な参加・貢献を行う。
（技術仕様）【国際機関】

← 重要インフラ事業者との協力による取組みの推進、国際フォーラムにおける議論への積極的な参加・貢献を行う。
（技術仕様）【国際機関、重要インフラ】

・ 各国政府、とりわけハイレベルで、サイバー攻撃（特にビジネスインフラに対するもの）等、ＩＴに起因する脅威に関して問題意識を共有し、適切に対処していくことをコンセンサスとできるよう議論に参加・貢献すること

← 時宜を考慮しつつ、G8 首脳会合や APEC 首脳会合等のハイレベルな

国際フォーラムにおける議論への積極的な参加・貢献
（脅威対応）【国際機関、各国政府】

・ サイバー攻撃等が発生した場合に、必要に応じて事実等を公開し、各国と協力して適切な対処を行うこと。

← 時宜を考慮しつつ G8 首脳会合等のハイレベルでの会議における議論の喚起
（脅威対応）【国際機関、各国政府】

← Meridian、IWWN、FIRST、APCERT 等のフォーラムでの議論への積極的な参加・貢献
（脅威対応）【国際機関、ＮＧＯ等】

・ ＮＧＯ、ＮＰＯ等との協力による世界の情報セキュリティ水準の向上

← 情報セキュリティ関連の緊急対応組織等が諸外国の同様の組織と協力・連携を進めることによるグローバルな情報セキュリティ水準の向上
（脅威対応）【ＮＧＯ等】

② リージョナルな枠組み

(A) 米国

・ グローバルな経済活動の円滑化に貢献するため、我が国と諸外国地域の情報セキュリティに係る取組ルールや標準の関係や相違等を十分に検討し、望ましい取組ルールや標準を明確化すること

← （国内で検討を行うとともに、）「サイバーセキュリティ日米会合」等の米国との対話の機会等に情報交換や議論等を行う
（制度・ルール）【各国政府】

・ 情報セキュリティに係る諸権利（ＩＴ安心利用環境で国民生活、経済活動を行うことができ、仮にＩＴに起因する脅威によって被害を受けた際の救済を受けることができる権利等）についての検討を行うこと

← （国内で検討を行うとともに、）「サイバーセキュリティ日米会合」

等の米国との対話の機会等に情報交換や議論等を行う
（制度・ルール）【各国政府】

・ サイバー攻撃等、ＩＴに起因する脅威によって被害が生じた際の対応に係る各国間の協力について検討を進めること

← （国内で検討を行うとともに、）「サイバーセキュリティ日米会合」等の米国との対話の機会等に情報交換や議論等を行う
（制度・ルール、脅威対応）【各国政府】

・ 情報セキュリティ政策に係る二国間の協力関係について関係を維持・強化すること

← 「サイバーセキュリティ日米会合」等において、米国との対話を一層積極的に進める
（制度・ルール）【各国政府】

・ 情報セキュリティ技術研究に係る二国間の協力関係について関係を維持・強化すること

← 「日米安全・安心科学技術協力イニシアティブ」等の場を利用した米国との協力を一層積極的に進める
（技術仕様）【各国政府】

・ 日米間の協力を通じた、重要インフラの情報セキュリティ水準の向上を図ること

← 「サイバーセキュリティ日米会合」等において、米国との対話を一層積極的に進めるとともに、国際機関等グローバルな情報セキュリティ水準の向上に向けた議論に積極的に貢献する
（制度・ルール、技術仕様）【各国政府】

・ 日米で活動を行う企業との官民協力を推進し、両国の政策水準の向上を図る

← 「サイバーセキュリティ日米会合」等において、国際的に活躍する企業等の産業界からの課題のインプットを求め、官民連携を通じた、

グローバルな情報セキュリティ水準の向上
（制度・ルール、技術仕様）【企業】

・　ＮＧＯ・ＮＰＯ等との協力による世界の情報セキュリティ水準の向上

←　情報セキュリティ関連の緊急対応組織等が米国の同様の組織と協力・連携を進めることによるグローバルな情報セキュリティ水準の向上、緊急対応活動の推進
（脅威対応）【ＮＧＯ等】

(B) 欧州

・グローバルな経済活動の円滑化に貢献するため、我が国の情報セキュリティに係る取組ルールや標準と諸外国地域の取組ルールや標準との関係や相違等を十分に検討し、望ましいルールや標準を明確化すること

←　（国内で検討を行うとともに、）ＥＵとの対話の機会等に情報交換や議論等を行う
（制度・ルール）【各国政府（ＥＣを含む）】

・情報セキュリティに係る諸権利（ＩＴ安心利用環境で国民生活、経済活動を行うことができ、仮にＩＴに起因する脅威によって被害を受けた際の救済を受けることができる権利等）についての検討を行うこと

←　（国内で検討を行うとともに、）ＥＵとの対話の機会等に情報交換や議論等を行う
（制度・ルール）【各国政府（ＥＣを含む）】

・サイバー攻撃等、ＩＴに起因する脅威によって被害が生じた際の対応に係る各国間の協力について検討を進めること

←　（国内で検討を行うとともに、）ＥＵとの対話の機会等に情報交換や議論等を行う
（制度・ルール、脅威対応）【各国政府（ＥＣを含む）】

・日欧で活動を行う企業との官民協力を推進し、双方の政策水準の向上を図る

← 「日・ＥＵビジネスラウンドテーブルダイアログ」等における産業界からの課題のインプットに積極的に対応していくことにより、グローバルな情報セキュリティ水準の向上

（制度・ルール、技術仕様）【企業】

・ ＮＧＯ、ＮＰＯ等との協力による世界の情報セキュリティ水準の向上

← 情報セキュリティ関連の緊急対応組織等が欧州域内の同様の組織と協力・連携を進めることによるグローバルな情報セキュリティ水準の向上、緊急対応活動の推進

（脅威対応）【ＮＧＯ等】

(C) アジア

・ 我が国の情報セキュリティ分野に係る知見に基づいた国際協調・貢献を行うことで、経済活動が深化しているアジア地域におけるＩＴ安心利用環境の構築に寄与し、グローバルなＩＴ安心利用環境の実現を図る

← 技術協力の推進（専門家派遣、セミナー開催、我が国の取組基準等の翻訳・普及、人材受入れ（研修）等）

（モラル、制度・ルール、脅威対応）【各国政府、個人、国際機関】

← 政府機関による協力の推進（域内経済発展に向けた情報セキュリティ対策のセミナー等）

（モラル、制度・ルール）【各国政府、個人】

← アジア地域における情報セキュリティ政策や協力のあり方に関する研究の推進（ERIA における研究課題として情報セキュリティを設定）

（モラル、制度・ルール、技術仕様、脅威対応）

【（地域）国際機関、各国政府】

← ERIA 等による域内における啓発活動（シンポジウムの開催、キャパシティビルディング、関連研究の推進など）の推進

（モラル、制度・ルール、技術仕様、脅威対応）

【（地域）国際機関、各国政府】

← アジア地域の中で国際的な連携窓口となる情報セキュリティ関連の緊急対応組織等が未整備である地域に対し、同組織の構築・運営に関する支援を推進

（脅威対応）【ＮＧＯ等】

・ グローバルな経済活動の円滑化に貢献するため、我が国と諸外国地域の情報セキュリティに係る取組ルールや標準の関係や相違等を十分に検討し、望ましい取組ルールや標準を明確化すること

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」を創設し、この場において検討を行う
（制度・ルール）【（地域）国際機関、各国政府】

・ グローバルな経済活動の円滑化に貢献するため、企業の技術情報の流出に係る防止策や対処方法等について検討を進め、得られた結論を実施すること

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」を創設し、この場において検討を行う
（制度・ルール、技術仕様、脅威対応）
【（地域）国際機関、各国政府】

・ 国際展開している企業との協力によるグローバルな情報セキュリティ水準の向上

← （国際展開している企業が有するべき情報セキュリティの取組水準等について十分に研究を行い、）技術面、組織管理面双方におけるベストプラクティスを明確化するとともに、普及を目指す
（制度・ルール、技術仕様）【企業】

・ 日本と関係の深い地域における、啓発活動の推進を通じたＩＴ利用に係る国民（ローカル及び現地日本人双方）生活の安心・安全の確保

← 「アジア情報セキュリティ週間」のような啓発活動の推進
（モラル）【各国政府、個人】

・ 地域における国際ＩＴ障害への対応を検討できる体制を整備すること

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」の創設

（技術仕様）【（地域）国際機関、各国政府】

← 重要インフラ事業者との協力によるアジア情報セキュリティ会議（仮称）における議論への積極的な参加・貢献を行う
（技術仕様）【（地域）国際機関、各国政府】

・ 情報セキュリティに係る諸権利（ＩＴ安心利用環境で国民生活、経済活動を行うことができ、仮にＩＴに起因する脅威によって被害を受けた際の救済を受けることができる権利等）

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」を創設し、この場において検討を行う
（制度・ルール）【国際機関・各国政府】

・ サイバー攻撃等、ＩＴに起因する脅威によって被害が生じた際の対応に係る各国間の協力について検討を進めること

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」を創設し、この場において検討を行う
（制度・ルール、脅威対応）【国際機関・各国政府】

・ サイバー犯罪の取締りに関する技術情報を共有し、相互の技術水準の向上を図る

← サイバー犯罪技術情報ネットワークシステム（Cybercrime Technology Information Network System: CTINS）の運用
（脅威対応）【各国政府】

← アジア大洋州地域サイバー犯罪捜査技術会議の開催
（脅威対応）【各国政府】

・ ＮＧＯ、ＮＰＯ等との協力による世界の情報セキュリティ水準の向上

← 情報セキュリティ関連の緊急対応組織等がアジア域内の同様の組織と協力・連携を進めることによるグローバルな情報セキュリティ水準の向上、緊急対応活動の推進
（脅威対応）【ＮＧＯ等】

・ リージョナルな議論の場において、地域の特性を反映した議論を推進し、グローバルでの議論につなげていくこと

← （国内で検討後、）地域内の検討の場である「アジア情報セキュリティ会議（仮称）」の設置

（モラル、制度・ルール、技術仕様、脅威対応）
【（地域）国際機関、各国政府】

← 情報セキュリティ関連の緊急対応組織等がアジア地域の同様の組織（APCERT を含む。）と協力・連携を進めることによる迅速な緊急対応活動の推進

（脅威対応）【ＮＧＯ等】

← 日ＡＳＥＡＮ、ＡＳＥＡＮ＋３等の国際フォーラムの場において地域の論を進め、各種国際フォーラムにおける提案につなげていく

（モラル、制度・ルール、技術仕様、脅威対応）
【（地域）国際機関、各国政府】

（４）我が国の国際協調・貢献

（３）における検討も踏まえ、今後、以下の５つの方向性を我が国の情報セキュリティ政策に係る国際協調・貢献として、取組みを進めることとする。

① 経済関係の深化が進むアジア地域のビジネス環境向上に向けた協調・貢献の推進（セキュア・アジアビジネス環境（Secure-Asian Business Environment）構想）

アジア地域では、日本企業の域内各国へのアウトソーシング・オフショアリングは拡大しつつあり[12]、アジア諸国と我が国との経済関係が日々深化している。また、アジア域内の経済成長に合わせて、域内のアウトソーシングについても、急速に拡大してきている。このような状況の中、情報漏えい等の情報セキュリティ問題が発生した場合、漏えいが発生した現地の事業環境に関して国際的な評価が大幅に下がると同時に、日系の多国籍企業も損害を被る可能性がある。さらに、このようなリスクは企業のアジア地域への進出を躊躇させ、経済関係の深化を阻害する要因となる可能性がある。また、事前の対応に加え、情報セキュリティ問題が発生した後の事後の対応を強化することは、アジア地域におけるビジネスの継続性を確保するためにも不可欠である。したがって、アジア地域におけるセキ

[12] 経済産業省「平成 18 年度版通商白書」p110-111 によると、日本のオフショアリングは 2002 年から 2004 年にかけて 2.5 倍以上の伸びを示しており、そのうち、アジア地域へのオフショアリングが 2004 年時点で 8 割近くとなっている。

ュリティ文化の醸成やセキュリティ水準の向上などに向けた協調・貢献を行い、安心・安全に事業活動を行えるような事業環境の整備のための協調・貢献を進めることが必要である。そこで、情報セキュリティの対策に係る基礎的な枠組みなど、我が国が情報セキュリティ政策の取組みを通じて得た知見や経験をアジア地域に提供し、地域のセキュリティ水準の向上に向けた取組みを推進する。

具体的には、我が国から人材育成や啓発、セキュリティ対策のベストモデルの普及等の協調・貢献を行うとともに、域内各国による自発的な啓発活動などを促進する。

また、2006年末の台湾沖地震によって海底ケーブルが切断され、金融分野、航空分野等のインターネットを利用するサービスにおいてもＩＴ障害が生じた国が存在し、我が国を含めた周辺諸国の社会経済活動に影響が及んだ。このように、アジア内の一部の地域でＩＴ障害が発生した場合にも、我が国も含めてアジア地域全体に影響が生じる可能性があるという現実に、我が国は直面していることが改めて認識された。このため、アジア地域におけるＩＴ安心利用環境を担保するためにも、ＩＴ障害が地域に及ぼす影響やＩＴ障害を予防する方策等について、域内各国で協調しつつ検討を行うとともに、実際に障害が発生した場合の共同対応体制などを地域全体で検討する必要がある。そこで、アジア地域において地域内の検討の場である「アジア情報セキュリティ会議（仮称）」の設置を目指すこととする。

② 情報セキュリティに係る新しい諸権利に係る検討及び議論への貢献

新しい政策領域である情報セキュリティ分野は、自由なＩＴ利用との関係や、ＩＴ利用に起因する脅威によって被害を受けた者の救済等の観点から、グローバルに新たな権利概念を生み出す可能性を内包している。こうした新たな諸権利について、バランスの良い適切な内容で、グローバルなコンセンサスが実現されるよう、十分な検討を国内で行うとともに、国際的なフォーラム等における議論への貢献を行う。なお、新しい諸権利に関する議論を通じ、情報セキュリティへの意識・機運が国際的に向上する可能性があることも視野に入れるべきである。

具体的には、例えば、（１）情報セキュリティの観点から、安心・安全な経済活動を行う権利、（２）情報セキュリティの観点から安心・安全な物品やサービスを利用する権利、（３）サイバー攻撃等、ＩＴに起因する脅威によって被害を受けた際の救済に関する権利、等が挙げられる。

（１）は国際展開する企業等がグローバルな経済活動を推進するに際して、情報セキュリティの観点から、安心・安全な事業環境で活動を行える権利、（２）は

消費者が安心・安全な物品の購入やサービスの提供を受ける権利、（３）は社会的・経済的に重要なビジネスインフラ等が、サイバー攻撃等、ＩＴに起因する脅威によって被害を受けた際にグローバルな対応を通じた救済を主張できる権利である。

③ サイバー攻撃等、ＩＴに起因する脅威への対応のための取組みの推進（リスクのないＩＣＴ（ICT Risk - Free）構想）

ＩＴが世界各国のあらゆる国民生活・社会経済活動に利用・活用されつつある現在、ＩＴに起因する脅威が当該国・地域の安心・安全に大きな影響を与える可能性が増してきている。このような中で、各国政府機関や重要インフラ、企業や個人を、意図的な攻撃や非意図的な要素に起因するＩＴ障害のリスクから解放することは、グローバルなＩＴ安心利用環境を実現し、ＩＴを利活用した国民生活・社会経済活動の質を大きく向上させることにつながる。したがって、できるだけ多くの国の関係機関の間で緊密・迅速な連携を取って、ＩＴに起因するリスク・脅威への対応を進めるべきである。

また、サイバー空間では国境を越えた犯罪が起こりやすい一方で、各国の制度の相違などから犯罪の追跡可能性に限界がある。したがって、より効果的な対応を進めていくべきである。

こうしたことも踏まえ、サイバー攻撃等ＩＴに起因するリスク・脅威に関しては、主要なＩＴ先進国のハイレベル等で問題意識を共有した上で、適切に対処していくべく議論に積極的に参加・貢献するとともに、実際に問題が生じた際には、各国と協力しながら適切な対応をとるよう引き続き議論を進めることとする。なお、こうした議論においては、経済関係に限らず安全保障の分野でもかけがえのないパートナーである米国との十分な検討、緊密な連携を行うべきである。このため、現在定期的に開催している「サイバーセキュリティ日米会合」のような協力推進の場を十分に活用していくことが必要である。

また、犯罪対策については、各国の捜査機関間の捜査協力や情報共有を始めとする国際的な連携の更なる強化を目指し、引き続き G8 や ICPO 等における議論を進展させる必要があると考えられる。

④ 情報セキュリティに係るグローバルなルールや標準の形成への貢献

情報セキュリティは取組みが比較的新しい分野であるため、今後、制度面や技術面等において、グローバルなルールや標準の形成が進む可能性が高い。具体的には、ＩＴ基盤の各構成要素に係る技術、グローバルに展開する企業の情報セキ

ュリティマネジメント体制の構築に係るガバナンス、一定規模以上の企業や政府に課される調達等に関する基準やガイドラインが例として挙げられる。現に、こうしたルールや標準の形成の動きはグローバルに見られ始めており、２００２年に OECD 理事会の勧告として採択された「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[13]」は、情報システム及びネットワークを保護する手段として、すべての参加者の間にセキュリティ文化を普及させること等を目的として制定され、加盟各国のみならず諸外国において、情報セキュリティ対策を行う上での規範的な文書として位置づけられつつある。

こうしたことを踏まえると、我が国が情報セキュリティ分野の協調・貢献を進めるにあたっては、グローバルなルールや標準の形成に対して何を行いうるのか、またどのような取組みを進めると貢献度が大きいのかなど、国内的に十分に検討を行い、その後、グローバルに取組みを進めていくことが必要である。

このため、第一に、我が国の情報セキュリティに係る取組みの優れた点、問題点を十分に把握することが不可欠である。そこで、これらの諸点を客観的に把握するべく国内的に検討を行う機会を設ける必要がある。同時に、情報環境、文化が各国によって異なる点についても配慮することが不可欠である。また、このような機会に限らず、我が国の情報セキュリティに関する取組みにおいてベストプラクティスと言えるような取組ルール等の明確化を図ることが望ましい。

第二には、①にもあるように国際的なフォーラム等での議論に積極的に参加し、貢献を行っていくことが必要である。グローバルなルールや標準の形成に向けた議論は、積極的な行動を取らずに受動的に取り組んでいる間に、例えば情報環境、文化、情報セキュリティ水準等の異なるアジア域内におけるＩＴ安心利用環境の実現の観点から適切とは言えない内容や水準のルール、標準が確立してしまう可能性が存在する。その場合、我が国に限らず、各国の政府や企業、個人等の活動にグローバルにマイナスの影響を生じさせることがありうる。したがって、我が国の情報セキュリティの取組みにおいて、グローバル、地域単位、国レベルに比較しても優れているものがあるのであれば、積極的にこれらを紹介し、提案を行う。また、こうした取組みは、国際機関の場での議論にとどまらず、例えば「サイバーセキュリティ日米会合」など、二国間の会合などの機会にも適宜行うべきである。

[13] http://www.oecd.org/dataoecd/16/22/15582260.pdf

⑤ 様々な国際フォーラム等における提案や議論への積極的な参加

情報セキュリティ分野は、脅威情報をはじめ、必要な情報を適時適切に入手することが極めて重要な分野である。情報源は、国籍を問わず、幅広い方がより的確な判断につながることから、例えば、情報セキュリティ上の監視・警戒ネットワークなどの既存のグローバルな取組みについても、より積極的に参加・関与するべきである。

また、各国が関与する国際フォーラム等では、情報セキュリティ問題への対応に関し、我が国の国内政策にも影響を及ぼしうるグローバルな流れが決まる可能性が常にあり、どのような社会問題に絡めて、どのような文脈で情報セキュリティに係る案件が議論されているか、世界的な潮流から取り残されないように大きな流れを把握することが最低限必要である。

内閣官房情報セキュリティセンター（NISC）は、前述のように、国際フォーラム等に参加するとともに、横断的な情報セキュリティ問題に関する我が国としてのＰＯＣの機能を諸外国との間においても明確化し、グローバルな存在感を高めてきたところである。しかし、取組みは依然として第一歩目に過ぎず、グローバルなＩＴ安心利用環境の実現に向けて我が国が強力に国際協調・貢献を進めるためには、今後、こうした国際フォーラム等における提案や議論への参加を、さらに積極的に行うことが必要である。こうした努力を通じてこそ、はじめて必要な情報が各国から入手しやすくなり、議論の流れが把握できるようになるとともに、我が国に関係の深い情報セキュリティ問題の発生をはじめ、各国との連携が必要な場合に、適切な協力を各国に求められるような関係を構築できると考えられる。例えば、情報セキュリティに係る経済的な側面を主として扱う APEC-TEL や、事案対処や脆弱性情報のハンドリング等を扱う組織によるフォーラムである FIRST、重要情報インフラ保護問題について、各国の窓口（ＰＯＣ）リスト作成や、ベストプラクティスの交換に取り組む Meridian Conference 等の多国間フォーラムが存在するが、情報セキュリティ問題の対応の検討や、実際の問題の発生時に緊密な連携が取れるよう、この種の会合に参加して日本のＰＯＣを明確化しつつ、同時に国内関係者の間での情報交換・共有を円滑に行えるような取組みを進めるべきである。

さらに、今後は、こうした国際協調・貢献の一環として、多国間のフォーラムの開催場所として積極的に手を挙げるなど、我が国が多国間のフォーラムを主導すべく努力を行うことも重要な課題である。

また、情報セキュリティに係る政策について多国間で議論を行うに際しては、たとえ我が国の提案がグローバルなＩＴ安心利用環境の実現の観点から望ましい

ものであったとしても、我が国単独で合意形成や議論を進めることは不可能である。したがって、国際フォーラム等に積極的に参加することなどを通じ、協調・連携を組めるパートナー国を見つけることも肝要である。

用語集

- APEC : Asia-Pacific Economic Cooperation アジア太平洋経済協力会議
- APEC-TEL : APEC Telecommunications Working Group
  アジア太平洋経済協力会議−電気通信ワーキンググループ
- APCERT : Asia Pacific CERT
  アジア太平洋地域における CERT(Computer Emergency Response Team)
- ASEAN : Association of South East Asian Nations 東南アジア諸国連合
- CERT-CC : Computer Emergency Response Team - Coordination Center
  コンピュータ緊急対応チーム
- ERIA : Economic Research Institute for ASEAN and East Asia
  東アジア・アセアン経済研究センター
- FIRST : Forum for Incident Response and Security Teams
  企業、政府機関、大学などの CSIRT によって構成される国際的なフォーラム
- ICPO : International Criminal Police Organization 国際刑事警察機構
- IGF : Internet Governance Forum インターネットガバナンスフォーラム
- ISO : International Organization for Standardization　国際標準化機構
- ITU : International Telecommunication Union　国際電気通信連合
- IWWN : International Watch and Warning Network
  国際監視警告ネットワーク
- Meridian　重要情報インフラ保護に関するポリシーレベルでの協力に関するディスカッションが行われる国際会合
- OECD : Organization for Economic Co-operation and Development
  経済協力開発機構