要　約

IT（情報技術）革命の積極的な側面が強調されるなか、コンピューターを用いた情報通信ネットワークの脆弱性とそれに対する依存度を高める社会の陥穽を突いたサイバー・テロやハイテク犯罪など、新しいタイプの脅威は着実に個人や組織、国家の安全保障にとっての重要な挑戦となりつつある。物理的な空間での不正行為と異なり、「サイバー空間」でのそれに対し、われわれは予防・検知・対策のすべての面で発想の転換と新しい危機管理体制の整備を進めていく必要がある。そこで本委託研究は、IT革命がさまざまなレベルで人々の社会に及ぼすことになる影響を「安全保障」という観点から捉え直し、その脅威の実態や対応策の現状と今後のあり方について考えることを目的とする。

言うまでもなく、IT革命はきわめて技術集約的な動きではあるが、本研究では、そうした技術の側面―すなわち、高度技術を用いた攻撃に対する高度技術による防衛という側面―のみに議論を限定せず、「IT革命と安全保障」をとりまく政治、軍事、経済、社会の諸側面まで検討していく。特にわが国の安全保障という観点からの議論に着目するが、その場合も、サイバー空間での不正行為が頻発する政治・軍事的な背景や技術・経済面での相互依存の現状、さらには社会・文明的な意味についても掘り下げていきたい。また、ITの技術的な発展は、「情報空間」の拡大をもたらすものである。ついては、問題は変化する情報空間における情報の収集・分析・活用の方法とも密接に結び付く。そして、これは、サイバー空間における攻撃に対する安全保障・危機管理の体制に関する議論を超え、より広い情報空間での外交の展開についても考察することにもつながるだろう。

第一章は、この委託研究全体の総論として、まず初めにサイバー空間における安全保障上の脅威の実態――大別して「サイバー空間によって結び付けられたコンピューター端末そのものの機能撹乱・破壊」と「サイバー空間を流通する情報自体への不正アクセスを狙ったもの」の二つ――について整理する。次にこれらの脅威に対する危機管理と安全保障のあり方や今後の方向性を打ち出す。その際に、サイバー空間を利用した不正行為に対する安全保障・危機管理においては、従来のリアリスト的な手段（ハード・パワー重視の発想）や技術集約的な対処やネットにおけるレッセフェール（自由放任）型の対応では不十分であることから、これらの対応を整備した上で、さらに　ネットに「法の支配」を導入する国内体制や国際協力の推進、　攻撃をむしろ前提とした「結果管理」として波及の阻止やバックアップ体制の強化などリダンダントな体制の構築、ネットからの隔絶による情報の保護、などを提言する。本章ならびに本研究全体を通じて、抑止

と対処を前提とした従来型の安全保障・危機管理観を転換し、非対称の主体間で、合理的な計算に基づく抑止も効きようがない状況で、サイバー空間の悪用は必ず起こる（あるいは、すでに日常化している）「そこにある明白な危機」であるとの認識から、多角的な対応をとる必要性が強調される。

各論に入り、第二章（岡田論文）ではハッカーの概念や歴史をたどりながら情報通信ネットワークに対する脅威の実態を整理した。ハッカーの概念についてはインターネット黎明期から様々な区分がなされているが、広く共通して認識された表現は存在しない。基本的には「工学的な技術の習熟度合いであり、常に技術に対し情熱的である技術を有した人物を指す」と考えられている。それら延長線上に「技術と熱意を、悪意もって利用する、もしくは結果的に悪意であると判断される行為を行う人物」を称したクラッカーと呼ばれる層があり、彼らが悪意を持って環境を利用した場合には、武器としてのコンピューターおよびネットワークの利用が起こりうる。
こうした脅威に対抗する側の状況として、本章では、米国における重要インフラ施設保護対策の日本への適用可能性についてふれ、さらには危機管理のための高度な手段として注目されている国際通信傍受網エシュロンに関し、その実効性と諸課題について論じ、さらに、政府規制と民間の自主規制のバランスをとる適切なレベルの政策が必要であることを提言する。

第三章（加藤論文）ではサイバー攻撃の脅威をいかに理解すべきかについて論じている。サイバー脅威には、例えば、ウィルス、サービス拒否攻撃、セキュリティー・ホール攻撃、ロジック爆弾、エミュレートなどがあるが、その脅威は時として誇張されすぎるきらいがある。確かに、コンピューターが麻痺したり、データが信頼できなくなることによる影響は計り知れないが、ファイアウォールやワクチンを利用するなど適切な防護措置さえ施されていれば、対応可能な程度にダメージを押さえることは十分に可能、と指摘する。また、サイバー攻撃で物理的被害を出すにはさまざまな問題があり、容易ではない。他方、被害を復旧するには準備を十分にしておけば比較的容易である。さらに、軍事的脅威としてのサイバー攻撃には、ヒューマン・インテリジェンスを主体にした従来の情報活動が重要である。我が国としては、インサイダー協力者を防ぎ、ダメージコントロールである結果管理を行うことで被害を限定できる。つまり、サイバー攻撃対策を考える上で求められることは、決して油断することなく、かつ過度に恐れないこと、と本章は強調する。

第四章（川上論文）では、サイバー攻撃が高度化し、例えば、昨年の米同時多発テロ事件のような非対称テロが将来、サイバー・テロと組み合わさったならばどうなるか、テロリスト・グループが「戦略情報戦(SIW)」として組織的に、かつ、一連の個別行動として攻撃を行う場合の問

題を指摘する。攻撃側は目標のシステムの最も脆弱な場所を標的とし、それぞれに対して最も効果的な手法を使用する。サイバー・テロは、　国家基盤に直接影響し、　地理的、空間的及び政治的境界線がなく、　瞬時性を持ち、　低コストで遂行可能、という特徴をもつ。ここでの問題点は、　「抑止」概念が適応できないこと、　行為者の特定が難しいこと、　カウンターSIW攻撃の支持を国民から取り付けねばならないこと、　軍事部門が商業部門へアウト・ソーシングしていること、が指摘できる。サイバー・テロに対して、　攻撃があっても重要機能は運用できねばならない、　重要機能支援のため最小限必要な基盤能力が存在する、　地域防衛より、地点防衛、重層防衛が重要、　基盤は構成部分やシステム・ネットワークの故障でも機能するよう設計しなければならない、　基盤は修復できねばならない、といえる。そこで、本章は、サイバー・テロを戦うえで日米協力は不可欠である、と主張する。こうした日米協力を推進するため、日本は、　サイバー戦に備えて技術開発を行い、　秘密保護に関する技術開発と法整備をし、　サイバー戦で日本国内の重要インフラが混乱に陥り米軍の投影能力が阻害されないようにして、憲法第９条とのかかわりをクリアーにせねばならない。最後に本章は、サイバー戦に備えて、日米間実務者レベルのワーキング・グループを設置し、その共同研究や共同対処を検討すべきことを提案する。

第五章（高橋論文）は、経済と技術の観点から、アジアにおけるIT革命のなかの日本の位置を見極め、成長著しい他の国々の動向を分析する。実のところ、アジア経済のリーダーを自認してきた日本は曲がり角に来ており、特に、技術革新のテンポの早いIT分野では、アジアの二番手に転落しようとしている。これに対し、1990年代後半から著しく台頭してきたのが、インドと中国である。

インドのソフトウェア産業は、米国シリコンバレーの「下請け」に近い形でスタートし、当初は労働集約的な単純工程に甘んじていた。しかし、インド人エンジニアは短期間に急速なキャッチアップを果たし、米国のITブームとＹ２K問題による需要拡大の追い風にも乗って自立し、現在では世界第２位のソフトウェア輸出大国に成長した。とくにIT革命の震源地であるシリコンバレーでのインド人の存在感は大きく、米印のリンケージはかつての「下請け」から「相互依存」へと深まり、さらには両者が切っても切れない「コミットメント」の段階へと発展している。

中国のソフトウェア産業は、80年代の政府主導の産業政策に端を発する。政府の研究機関や大学が株主となって企業を設立し、研究者に経営者の役割をもたせる「一院二体制」と呼ばれる独特のシステムで発展してきた。その中心である北京の「中関村」は、やはりシリコンバレーと人的･技術的に深く結ばれている。

マレーシアは、世界最先端の情報通信産業を誘致・育成し、産業構造高度化と先進国入りへの切り札にしようというマルチメディア・スーパーコリドー(MSC)計画を実行中だ。2020年まで

の先進国入りを目標とするマレーシアが、情報通信産業を核として産業構造高度化をめざす計画がMSCである。マハティール首相の強力なリーダーシップの具体化である。

第六章（矢澤論文）では、ネットワーク社会化と紛争形態の変化を社会学的見地から考察した。1990年代初頭以降盛んになったアメリカにおける「ITと安全保障」に関する議論の流れをトレースしてみると、一つの基調として、サイバーウォーからネットウォーへの変化という議論が浮かび上がってくる。それは、IT革命によって可能になった新たなサイバースペースを他から切り離して論じていた段階が終わりを告げ、サイバースペースを情報社会、知識社会、ネットワーク社会の成立というより広い文脈の中に位置付け、それと関係付けながら論ずる段階に入ってきたことを意味する。サイバースペースという新たな空間は、情報社会、ネットワーク社会の成立という根底的な社会変動の統合的な部分であることがはっきりしてきた、と本章は分析する。

新しい社会の成立・展開に伴って、新しい戦争、紛争の形態・様式が登場してきたのであるから、当然それに対峙する安全保障も新たな展開を要請されることになった。1990年代初頭以降の安全保障の展開は、「ハードな安全保障からソフトな安全保障へ」という形で定式化されている。それは今日における紛争が、その主体、形態、その領域等において、従来のそれと著しく異なるものになっていることを意味する。紛争の主体は、官僚制的組織、国家、正規軍などからネットワーク組織へ、形態はswarmingを中心とするものに、紛争の領域は、グローバルな精神共同体、情報を構造化する知識の領域を中心とするものに広がっている。従来国民国家は、監視を通じて、情報、知識をコントロールすることによって社会秩序を維持することを行ってきた。しかしこの国民国家の従来のやり方は、危機に瀕している。今日国民国家もネットワーク国家、ネットワークやコミュニケーションに依拠しない限り安全保障の機能・目的を果たすことができない。先の変化は、そうした事態を正確に体現したものに他ならない。

以上の文脈において、現代の紛争、戦争の意味が探求されることが重要である。戦争は、インスタント戦争として、その意味を大きく変容させている。ネットワークウォーの実態も、その文脈で正確に把握することができる。ここから本章は、紛争、戦争の実態を踏まえて、今日の安全保障の本質を指摘しておくとすれば、テクノロジー一辺倒で監視国家を作り上げる方向ではなく、テクノロジーと人間のコンビネーションを考えた安全保障であろう、と指摘する。人間とテクノロジーが両輪としてある安全保障、高度なテクノロジーによって人間が排除されない安全保障、という視点の重要性を本章は強調する。

本報告書では、最後に、情報セキュリティーの諸問題について、主に政策や外交、法的側面から、当該分野に造詣の深い方々による講演内容を収録した。これらの講演は、研究会の活動の一環として実施されたものである。

日本では現在、IT革命の技術的成果のみに目が行き、それを支える法整備、管理、監査、情報セキュリティー、倫理などのインフラ整備が追いついていないといえる。経済団体連合会の上田正尚氏は、我が国は情報セキュリティーに対する意識が低く、省庁の対応を見てもその考え方や対策の手法に大きな差があり、欧米のような国家安全保障的観点からの統一した取り組みがないことが問題だと指摘する。また、情報化社会の秩序維持のための法制度づくりやビジネスの面でも、欧米に遅れをとっている状況がある。技術革新が加速度的に進むために、どの時点でそれを規制する法を定めるかは法的保護とのバランスが難しいが、早急な対策が不可欠であることが論じられた。

また、防衛庁防衛研究所の橋本靖明氏には、法的側面から、サイバー・テロを国際法の枠組みとの関連において分析していただいた。サイバー・テロの特徴には、実行者及びその意図、行為の対象が多様で区別がつきにくく、結果として莫大な損害が出ることが挙げられる。国際社会はこのようなテロ、サイバー犯罪、サイバー攻撃などに対して国際的に取り締まりを強化していく方向にあり、我が国もその流れを追っている。ここでは、無秩序なサイバー空間のなかにあって、それら全てを同時並行的に捉え、制度と技術の両面から対応する必要性を説きつつ、米国同時多発テロ事件を例にとり、テロに対抗する手段としての「自衛権」についても考察した。