第四章　テロリストの情報戦争（ＩＷ）と日米協力

川上　高司

１．ビン・ラディンの情報戦争

2001年の9.11同時多発テロは、テロリスト・グループが周知にアメリカに仕掛けた情報戦争(Information Warfare: IW)、中でも指揮統制戦と経済統制戦であった。テロリストは、民間航空機をハイジャックし、自爆テロを３箇所に仕掛けた。第一の目標は「経済」の中枢である世界貿易センター、第二の目標は「軍事」の中枢である国防総省、第三の目標は「政治」の中枢であるホワイトハウスといった政治および経済の中枢部を狙った「指揮統制戦」をしかけたのである。したがって、9.11テロ事件の手段は自爆テロという原始的な非対称戦であるが「情報戦」あるいは「指揮統制戦」の効果を熟知した相手であったと推測でき、この点、アメリカ政府も震撼したのは間違いないと考えられる。

テロの手段	テロの具体的目標	テロの目的	情報戦の種類	成功度
民間機ハイジャック１機目	世界貿易センター	経済の中心地	経済情報戦	◎
〃　　２機目	国防総省	軍事の中心地	指揮統制戦	△
〃　　３機目	ホワイトハウス	政治の中心地	指揮統制戦	×

その主犯格とされるオサマ・ビン・ラディンが、9.11同時多発テロまで指名手配犯の重要テロリストとしてラップトップ型コンピュータを衛星送信路でリンクし、複雑に暗号化されたメッセージによって、国境を越えて世界的地下組織と通信を行っていたことは周知の事実である(注1)。さらに、イスラム過激派のテロリストのためのテロに関する情報には全体で11巻、7000頁の「ジハード百科事典」があり、CD-ROM化されている。99年ヨルダンのアンマン空港を爆破しようとした容疑者の自宅から押収された。内容はタバコや歯磨きチューブに爆薬をしかける方法から、大きな橋の爆破方法や生物化学兵器の原材料となる細菌薬品の入手方法を豊富な図表入りで説明している。このうちビデオカメラに爆弾をしかける手口は北部同盟のマスード氏の暗殺に使われた。また、大きな心理的効果が期待できる標的として、自由の女神像やエッフェル塔をあげている。さらに、原発、高層ビル駅などを狙えば大損害を与えられると指摘している。この「教則本」はビン・ラディンに献呈されたとされる(注2)。

さらに、ブッシュ大統領が９月20日に上下両院合同会議の演説でアフガニスタンを拠点とするテロ組織「アルカーイダ」とその指導者ビン・ラディンがテロリストの背後に存在するとの演説を行った直後から(注3)、ビン・ラディンは情報戦争と心理戦争(Psychological　Warfare)を仕掛

けてきた。要は、ビン・ラディンは今回の戦争は「イスラム教」対「キリスト教」の戦いであり、世界中のイスラム教徒へ結束してアメリカへ立ち向かうように呼びかけたのである。つまり、ハンチントンの言う「文明の衝突」へと文明間の紛争へとその対立軸をもっていこうとしたわけである。これに対してブッシュ大統領は、あくまでも「テロ」対「民主主義」の戦いであり、テロは「バックル・デモクラテイア(民主主義による平和)」への挑戦であるとした。これは、もし今回の戦争が「文明の衝突」となれば、アメリカ国内にいる600万人を超えるイスラム教徒(注4)を敵に回す可能性もあった。そうなれば、アメリカ国家の分裂という可能性もでてくる。したがって、ブッシュ大統領は当初から「国民の団結」を訴え(注5)、テロの民主主義への挑戦ということを強調する必要があった。これは緻密に計算された情報戦争であった。

それに加えて、アメリカ国内では本土防衛の焦点として、継続して起こる可能性のあるテロの攻撃は、最大の効果をあげるために従来のテロリズムに加えて「情報戦争」が組み合わせて行われることが強く予測され、すなわちサイバー上のテロ（サイバー・テロ）の脅威が強く指摘されている(注6)。また、リビッキによれば、現時点で重要な意味を持つ情報戦争は、 指揮統制戦(C2W：Command and Control Warfare)、 情報基盤戦(Intelligence-Based Warfare)、 電子戦(Electric Warfare)、 心理戦(Psychological Warfare)であるとしている(注7)。このうちサイバー・テロはいずれもかかわってくる。

本稿では、サイバー・テロの位置づけを広義の情報戦(IW)と狭義の戦略情報戦(SIW：Strategic Information War)から行うと同時に、わが国の取り組みに関して論じる。

２．情報戦争とは

米陸軍は、情報戦争を「敵の情報収集と、情報を活用する機能を阻止・搾取・低下させる一方で、敵のこの種の行動に対して味方を防護し、敵の情報作戦を味方にとって都合のよいように利用するあらゆる活動」と定義している。

米国国防大学(National Defense University)は情報戦（IW）の教育を行い、そこではInformation Warfareで実施される可能性がある７つの形態― 指揮統制戦(C2W：Command and Control Warfare)、 情報基盤戦(IBW：Intelligence-Based Warfare)、 電子戦(Electric Warfare)、 心理戦(Psychological Warfare)、 ハッカー戦、 経済情報戦(Economic Information Warfare)、情報活動(economic espionage)、 サイバー戦(Cyber Warfare)―をあげ、その各々の形態で情報の防御、操作(Manipulation)、低落化(Degradation)、拒絶(Denial)活動を行うものとしている。

「指揮統制戦(C2W：Command and Control Warfare)」は、米陸軍の定義によればIWの一つの要点であり、敵側の指揮命令(Command and Control)系統を切断することである。C2WはNATO(北大西洋条約機構)が採用したエア・ランド・バトル戦術でも重視されており、また湾岸戦争の際、物量的に優位なイラク軍が能力を有効に発揮できなかった原因の一つである。指揮中

枢の人間を攻撃すること自体は、戦史の中で（例えば、織田信長が今川義元を破った「桶狭間の戦い」のように）古くから有効性を示してきた。通信系統の切断もこの範疇に属するが、その有効性は相手側の軍がどの程度自立的であるか、すなわち中枢が機能を停止した際に、どの程度柔軟な継戦能力をもっているかにかかっている。

「情報基盤戦(IBW：Intelligence-Based Warfare)」とは、敵の指揮統制系の情報システムから敵の作戦計画・位置などを入手することを目的とした情報戦の形態であり、攻撃的情報戦と防衛的情報戦にわけられる。前者は、戦闘空間における敵陣営の配置や動きを各種のセンサーにより把握することであり、防衛的情報基盤戦は、隠蔽やステルスの適用などにより、敵の情報システムを欺くような戦いをいう（注8）。

「電子戦(EW：Electric Warfare)」は（注9）、敵の電磁波利用を妨害することを目的とした情報戦の形態であり、情報伝達に関する物理的基礎を弱める戦いをいう。従来は、センサーや通信機能の探知・妨害が主であったが、今後は、情報システムのネットワーク上にある各種情報の搾取や偽情報の入力などが予想される。また、EWにはレーダー使用と対抗手段の発達（注10）、暗号化および通信傍受と暗号解読とがある（注11）。また、無線の傍受と暗号解読の電子戦では、デジタル技術進展に伴い暗号・複合化を行うパーソナルコンピューター(PC)上でのソフトウェア進歩が顕著である。そしてPCベースを暗号利用に一般化しているため、安全保障機関の暗号解読作業に大影響を与えかねない。例えば、外交通信や軍用通信に原理的解読不可能なPC暗号が利用されるようになると予想される（注12）。

「心理戦（Psychological Warfare)」とは、敵を扇動し、第三者の支持を得ることを目的とした情報戦の形態である。心理戦には、相手方の国民の意思に働きかけるもの(Counter-will)や、軍の士気に作用するもの(Counter-force)がある。先の9.11テロをビン・ラディンは「文明の衝突」論議にもっていこうとした。国境を越えた情報の流入が、人々の心理面を通じて、閉鎖的な社会体制の変化に影響を与えた例として、西側の衛星放送やVOA(Voice of America)、BBC(英国放送協会)などの聴取が、旧ソ連・東欧圏の解体に繋がる市民の活動を作り出した、という観測がある。また、CNN(ケーブル・ニュース・ネットワーク)が、国際社会のアジェンダの設定に大きな役割を果たすようになった、という主張もよく聞かれる（注13）。また、近年の情報システムの発展によるインターネットの急速な普及により、インターネットを心理戦の手段として活用することが有効と考えられている。

「ハッカー戦(Hacker Warfare)」とは、敵の情報システムを混乱させることを目的とした情報戦の形態であり、コンピュータ・システムへの攻撃である。攻撃者はどこのサイトにいるか不明であり、一般的にはどのサイトにもいるように見える。また、その攻撃意図は、システム全体的な機能麻痺から断続的な閉鎖、ランダム・データ・エラー、情報の無差別窃盗、サービスの窃盗、システムの不正監視（情報収集）、誤情報の導入などの範囲まで及ぶ。攻撃の道具としてウ

イルス (注14)、論理爆弾 (注15)、スニファーなどがある。

「経済情報戦(Economic Information Warfare)」は、コンピュータや欺瞞情報などの手段により、一国の経済基盤（エネルギー資源、真水資源、通信施設）に対して攻撃を行うことである。先進国の進んだ科学技術や競争相手の企業秘密、また米国の軍事技術や軍民両用技術を、合法・非合法の手段で、とりわけコンピューター・ネットワークにより取得する経済スパイ活動が活発化している。この対抗手段のためクリントン大統領は、1996年10月、外国の機関が関与する企業秘密の不法な取得、および同様の国内犯罪を処罰する際の法的な根拠となる「経済スパイ法(EEA：Economic Espionage ACT of 1996)」を定めた (注16) (注17)。American Society for Industrial Securityが発表した96年３月の見積もりによれば、米国の産業が産業スパイと企業秘密の不法な取得によって被る被害は、毎年20億ドルにのぼっている (注18)。Computer Security Instituteの1998年３月の調査結果で、520の企業・組織のうち、64%がセキュリティーの侵害を報告した。これは96年の数字に比べて、16%の増加になっている (注19)。

「サイバー戦(Cyber Warfare)」とは、物理的な情報インフラのうち、軍事用のシステムを攻撃するものを「サイバー・ウォーフェア」、ある国家全体の情報インフラに対する攻撃を「戦略情報戦(SIW)」と呼ぶ。後者は、コンピュータ、通信システム、データベース、メディアを通じて国家に対して行われる連携の取れた組織的攻撃をいう。1997年に、赤組が北朝鮮を装い、1900のウェッブ・サイトで入手可能なハッキングツールを使って、アメリカの送電系統の大部分を停止させ、太平洋軍司令部の指揮・統制システムを混乱させた (注20)。このようにサイバー・テロリストによるSIWが問題となっているし、現実のものとなってきている。

３．サイバー・テロリストの戦略情報戦(ＳＩＷ)

(1) ワーテルローの戦い

問題は、テロリスト・グループが戦略情報戦として組織的にサイバー・テロを行うことにある。1998年２月には、イスラエル在住の犯罪ハッカー (注21) の指示で、カリフォルニアから２人の若者が国防総省のシステムとNASA、さらにある核兵器研究所に攻撃を仕掛け、湾岸での部隊配備を混乱させた。ハームレ国防副長官は、米国の防護システムに対する過去に探知された中では「最も組織化された攻撃」だと述べた。

このようにサイバー・テロリストたちは、サイバーという兵器を駆使することにより、

特殊なソフトウェアで電話回線をパンクさせる、　航空管制機能や船舶および鉄道のコンピュータを混乱させり、　主要な金融機関や病院、その他の緊急用施設が使っているソフトウェアを混乱させる、　遠隔操作によって薬品工場の薬剤調合を変える、　ガス輸送管路の圧力を変化させてガス管を破損させる、　証券取引所の妨害をすること、などが可能である (注22)。

このようなSIWの脅威に関してクルッフォとジョージェリーは、「ワーテルローの戦い」になぞらえる。つまり、ワーテルローでは技術、計画、そして注意深い実行が、世界の政治、軍事、経済の秩序の変更を目標とする長期計画の一部として用いられた。敵対者は優位性を確保するため、その本当の目的と標的が明らかになる数ヶ月間、計画によっては数年間、秘密裏に攻撃することによって、情報戦争の成果を増大させ得る。秘密攻撃には、作戦の開始前、中、後に利用できる重要な情報資源を特定する事を目指した偵察任務も含まれる。そのような攻撃は単発ではなく、注意深く調整され、何週間、何ヶ月にもわたって展開される可能性が高い、一連の作戦から構成される。情報戦争はその標的が攻撃にさらされている事すら知られない場合に最も効果をあげるので、敵は明白に敵対的作戦を展開する前にできる限り地盤を固めるために、何ヶ月、何年間も続く作戦において最初は秘密裏に攻撃する。心得た敵対者ならば、その国が最も弱い領域を標的とし、最大の効果をあげるために統合された、従来の軍事行動、特殊作戦、テロリズム、外交的主導権と情報戦争活動とを組み合わせると考えられる(注23)。

(2) SIWの攻撃形態

さらに、SIW攻撃は、標的とされた組織の内部もしくは外部からなされる。この区別は重要であり、異なった攻撃源に対しては異なった防御法が要求される。例えば、システムの「外部攻撃」に対する防御には、暗号化、特に国家機密にかかわるシステムの物理的隔離、ネットワーク上の指定されたエリアから部外者を締め出すファイアウォールのように、より優れた防御方法や保護手段の構築が含まれる。また、スパイや不満を持った従業員からの「内部攻撃」に対しては、より厳格な職員のセキュリティーやオペレーティングの手続きが講じられる。

攻撃源	攻撃形態	戦術目標
内　　部	データ攻撃	利己的搾取
外　　部	ソフトウェア攻撃	欺瞞
	ハッキング	妨害またはサービス拒否
	物理的攻撃	破壊

また、SIWの攻撃形態は、データ攻撃、ソフトウェア攻撃、ハッキング、物理的攻撃の４つに分類できる(注24)。「データ攻撃」は、システムの不調をきたしたり、騙して許可されていないアクションや反応をさせるようにデータを挿入するものである。その攻撃形態は、例えば、単に人を惑わすプロパガンダや、偽情報工作、ファイルの破壊、センサー電波通信妨害などをとる。そのアプローチは、入力情報やシステム内の信号となるような入力情報を

操作することにより、情報資料システムやその資源を無力化したり欺こうとしたりするものである。「ソフトウェア攻撃」の形態は、「コンピュータ・ウィルス」や、ひとたびインストールされると敵対勢力に対してシステムへの継続的なアクセスを許してしまう「トラップドア」がある。「ハッキング」は破壊、使用拒否、資源の窃盗、価値あるデータの窃盗、秘密裏の監視、その他の害悪をもたらすことを目的として、情報資料システムのコントロールを強奪することである。「物理的攻撃」は、システムのオペレーションに最も影響を与える直接的かつ効果的方法で、情報システムの入力装置に過負荷を与えたり、爆撃、軍事攻撃などを行ったりする伝統的な破壊攻撃手段である。

さらに、SIWの戦術目的に関しては、「利己的搾取」「欺瞞」「妨害またはサービス拒否」「破壊」に分類できる。このうち、「利己的搾取」の場合、攻撃側の主要目的は、標的、もしくは標的に接続されている資源、例えば信頼されている経路を経て、情報を抜き取ることである。「欺瞞」の場合、攻撃側は相手が継続してオペレーションすることを許すが、相手が収集したり、生成したり、実行したり、分析したりする情報を操作する。「妨害またはサービス拒否」の場合、攻撃側は標的を破壊はしないが、一定期間オペレーションができないようにしたりして、信頼性を損なわせる。「破壊」の場合、攻撃側は標的それ自体か、それが機能するために必要なシステムを破壊することによりオペレーション不能にする。

(3) SIW脅威の分類

SIWの脅威は、「自然災害、過誤、不慮の帰結」「非組織的、緩やかなIW脅威」「戦術的IW」「戦略的IW」の４つに分類できる (注25)。「自然災害、過誤、不慮の帰結」には、天候、地震、火災、流星、その他自然災害、Y2K問題、オペレーターの人為的突発事故、設計や生産の不具合、不可抗力などがあり、システムに対する最も基本的な脅威である。中でも自然災害は被害が甚大にある可能性があり、留意せねばならないのは、敵対者が攻撃を偽装するための隠れ蓑として自然災害を利用するかもしれないことである。敵対者はまた、その時の混乱と災害に乗じて攻撃できるわけであり、国家が最も脆弱な状況にあるので絶好のチャンスである。「非組織的、緩やかなIW脅威」にはハッカー、愉快犯、ギャング、単独の犯罪者、組織的犯罪者、不満を持った従業員によるものがある。この場合、敵対者がアマチュアのハッカーを取り込んだり、支援したりして自らの指令を実行させる可能性もある。あるいは、敵対者はハッカーを陽動作戦に用いて、同時進行で破壊的な攻撃をしかける可能性も否定できない。「戦術的IW」には欺瞞作戦、電子戦(EW)、電子対策(ECM)、軍事作戦でのステルス、軍備管理のカモフラージュ、隠蔽及び欺瞞(CC&D)、産業スパイ行為、組織犯罪、潜在的敵の排除目的の限定的攻撃などがある。このIWでは技術と計画が限定・洗練されたものとなる。例えば、ECMの運用には、敵の防空レーダー、電波妨害あるいは信号

遮蔽の発生可能な装置、装備を効果的に使用するための操作技術についての深い知識が必要である。戦術的IWの計画、実行はチャレンジングなものであり、その目的は通常限られている。

自然災害、過誤、不慮の帰結	非組織的、緩やかなIW脅威	戦術的IW	戦略的IW
天候、地震、火災、流星、その他自然災害、Y2K問題、オペレーターの人為的突発事故、設計や生産の不具合、不可抗力	ハッカー、愉快犯、ギャング、単独の犯罪者、組織的犯罪者、不満を持った従業員	欺瞞作戦、電子戦(EW)、電子対策(ECM)、軍事作戦でのステルス、軍備管理のカモフラージュ、隠蔽及び欺瞞(CC&D)、産業スパイ行為、組織犯罪、潜在的敵の排除目的の限定的攻撃	拡大されたテロリスト攻撃、組織犯罪、産業スパイ、組織化された戦略目標をもったITオペレーション

(4)「戦略的IW(SIW)」

SIWには、拡大されたテロリスト攻撃、組織犯罪、産業スパイ、組織化された戦略目標をもったITオペレーションがあるが、この中でもサイバー・テロリストによるSIWが問題となっていて、最も重大な脅威となっている。対処法が非常に困難である。

戦略戦争の概念は、産業革命の時代にまでさかのぼる。軍事力は工業の能力に依存していたので、戦略家は、敵の工場、都市、物流拠点を攻撃するほうが戦場で敵軍をうち破るよりも、しばしば効果的であることを導き出した。南北戦争中にウィリアム・シャーマン将軍が率いた南部を縦断する進撃は、戦略戦争の初期の例であった。シャーマン将軍は南部連合軍を追跡するよりも敵の戦争遂行に不可欠な経済基盤を破壊した。後に、戦略家はこの「戦略戦争」の概念を発展させた。例えばJ.F.C.フラーやリデル・ハートは未来の軍隊は後方を直接攻撃するために敵の防衛戦を乗り越える手段を持つようになるだろうと主張した。ジュリオ・ドーエ、ビリー・ミッチェル、ヒュー・トレンチャードのような空軍のパイオニアは新しく発明された航空機を、前線を飛び越えて工業標的を直接攻撃する手段として使用することを提案した。また、バーナード・ブロディ、ハーマン・カーン、アルバート・ウォールシュテッターは、敵国の中枢を真っ先に素早く直接攻撃する核兵器の能力が従来の軍隊を時代遅れにしてしまうことを論じたときに、戦略戦争は核兵器と関連付けられた。つまり、SIWは決定的勝利を収めるために敵の情報インフラを直接狙うことを目標とする。伝統的なテロリストの攻撃は、限定的な目的を持ち、敵に物質的な損害をもたらすことと同じくらい世論を形成することを意図している。SIWの目的は、敵国の大量破壊兵器開発のためのプロ

グラムを妨害したりするなど、目標に対する攻撃が敵の適応力や抵抗能力の体系的破壊を引き起こし得るという理由からなのである（注26）。

SIWの目的は、グローバルな権力構造、ある地域の市場もしくは軍事力のバランス、あるいは何らかの国際的提携の安定性を崩すことですらあり得る。

SIWは、単発の攻撃ではなく一連の軍事行動から成る。すなわちSIWを仕掛ける敵は一連の個別行動による攻撃を展開すると考えられる。攻撃側は目標のシステムの最も脆弱な場所を標的とし、そのそれぞれに対して最も効果的な手法を使用することができる。また、そのような軍事行動においては攻撃側が段階的に襲撃を実行することが可能である（注27）。

その意味で、湾岸戦争は通常戦争では米国の軍事力をうち負かすことはできないという重要な教訓を米国の潜在敵国は学んだ（注28）。したがって、そうした潜在敵国はSIWを用いることによって米国の強大さを相殺し、自らの勝算を増大させ得る（注29）。しかも、SIW遂行能力にかかるコストも極めて低く、実行に必要な技術や専門知識は容易に入手可能である。したがって、テロリスト組織や国を持たない民族集団、カルト宗教といった伝統的な軍事能力を保持しない非国家活動者もSIW遂行能力を容易に獲得可能となる。

この点、1996年11月の国防科学委員会(DSB)の特別専門委員会のレポートでは（注30）、2005年までにテロリストがアメリカに対してSIWを仕掛ける可能性が広範囲にあると報告している。さらに、DSBは1996年の段階でオサマ・ビン・ラディンに代表される世界的テロリストが、多くの国々や組織がアメリカを憤慨したり、妬んだりしており、原理主義者や国粋主義者は自分達の国が、アメリカの支配する文化の一部になることを恐れている、と2001年９月11日の同時多発テロのことを予測している。

SIWを仕掛けるテロリスト・グループにはメキシコのサパティスタ、タミル・イーラム解放の虎(LTTE)、センデロ・ルミノソ(輝ける道)、ヒズボラ、ハマス、トゥパク・アマル(MRTA)、デブ・ソルや、ウェブサイトを保有しているその他のテロリストがいるとされる。テロリストは、社会に対してインフラが持つ重要性を以前から理解しており、自分たちの標的リストの上位にそれを位置づけてきた（注31）。

この点、CSISのプロジェクトチームは、「Cybercrime, Cyberterrorism,Cyberwarfare」の報告書で（注32）、米軍の最も脆弱な点の一つは、商業用の情報技術やシステムおよびそのサービスに大きく依存し、将来ともその依存度を増すであろうことだと指摘している。つまり、商業用のセンサー、コンピュータ、通信システムが高性能になればなるほど、軍事用システムを維持するのは難しくなる。サイバー・テロは、ISW攻撃に脆弱になっている米軍を支えている商業用の技術やサービスを標的とする可能性があると指摘している。

４．ＳＩＷ の問題点とその対策

(1) SIWの問題点

SIW対策の問題点は大きくわけて３点あるとCSIS報告は指摘している。

第一は、「抑止」概念がSIWに適応できないことである。SIWが意図的であるのか、そのシステムの所有者、テログループ、国家、あるいは一人なのかといった行為者の特定が即座には判定、あるいは事前に予測はできない。また、行為者が特定されねば、政府は軍事的か、外交的か、あるいは法的強制措置による報復かを決定できないからである。もし、SIWの攻撃が起こったら、行為者を特定する以前に対応策を決定しておく必要があり、そのためにはシステムへの侵略がSIWとなる敷居の定義が必要である。そして、SIWの抑止を論議するとすれば、何をもって報復するのか。つまり、SIWにはSIWで報復するのか、あるいは通常兵器なのか、核兵器なのかを決めねばならない。また、SIWを抑止、あるいは報復するために、政府は積極的SIW、受動的SIW、破壊的SIW、搾取的SIWとを区別せねばならない（注33）。

第二は、SIWの行為者を特定したとして、大統領はSIW行為者へ対する支持を国民と議会から取り付けねばらないことである。行為者は無数に存在するのに加えて、その規模、背景、信念、組織が千差万別である。そのうえ、行為者はSIWの戦力を秘密裏に開発していることも加わり、SIWの脅威の発見および分析を非常に複雑にしている。米国の指導者はSIW攻撃に対する報復を承認する前に、どれほどの証拠が必要なのかについても考慮せねばならない。

第三に、商業部門が政府に取って代わり、大部分のシステムの開発、生産、購入及び操作を行うようになってきていることである。したがってサイバー・テロリストは先ず民間企業を標的とするが、政府は企業に防御システムの購入あるいは攻撃の準備を強制することはできない。さらに、サイバー・テロに対するSIW攻撃を行う場合、民間部門を目標とすべきか議論せねばならない。

(2) SIWの特徴とその対策

SIWの特徴は、第一に国家基盤に直接影響することが考えられる。つまり、エネルギー供給、通信、経済、輸送、生産などの国家基盤は、そのほとんどが情報システムにより構成されている。したがって、その全てが情報戦における攻撃の対象となる。第二は、地理的、空間的及び政治的境界線を欠くことができる点である。SIWは地理的、空間的及び政治的境界などに無関係に戦いが発生してこれらを区分することが難しい。第三は、瞬時性を持つことである。コンピュータ・ネットワークにより、地理的距離に無関係に、一瞬にして地球規模での展開が可能である。第四に、比較的低コストで遂行が可能であることである。従来の攻撃兵器のように膨大な経費を必要とせず、極端にいえばパソコン一台でSIWを実施し得る。

第五に、対象国の情報化進展の度合いによって効果が変化する点である。欧米や日本など、情報システムの発展した国家ほど、情報戦の対象となりやすく、また、大きな影響を受けやすい。

以上のSIWの特徴を考え、かつサイバー・テロリストからのSIW攻撃を考慮した場合、前述したDSBレポートではその対策として、第一に重要機能は情報戦の攻撃に直面しても運用することができるものでなければならない、第二に、重要機能を支援するために、何らかの最小限必要な基盤能力が存在しなければならない、第三に、地域防衛よりも、地点防衛、重層防衛の方が望ましい、第四に、基盤はその構成部分やシステム及びネットワークの故障に直面しても機能することができるよう設計しなければならない。構成部分、システム及びネットワークの故障に伴うリスクは、どうしても回避できないものであるから避けようとしないで、むしろ管理せねばならない、第五に、基盤は修復することができるものでなければならないと指摘している(注34)。

米国や他国のSIWへの対応はここでは触れないが、日本のSIWに対する対応に関しては、2000年７月に「日本戦略研究フォーラム」が「サイバー戦と日本の安全保障」報告書で提言を出している(注35)。その提言は、コンピュータの普及による情報化社会の進展に伴ってコンピュータ・ウィルスなどによるサイバー攻撃が新たな国家安全保障上の重大な脅威となったと指摘した上で、「わが国の重要インフラが組織的なサイバー攻撃を受け、機能が麻痺する事態も予測されるにもかかわらず、政府の対応はほとんど手つかずのままだ」と警告している。そして、「サイバー戦に備えるため、防衛庁を中心に基本方針の策定や組織、法制を整備すべきだ」としている。なお、ここでの重要な点は、SIWで一番進んでいる米国との共同研究や共同対処のために実務者レベルのワーキング・グループの設置を提唱していることである。

５．ＳＩＷ での日米協力

サイバー戦に対する日米間の協力、とりわけ日本がアメリカとの同盟を推し進める上で重要なことは以下の４点である。

第一は、日本はアメリカとの同盟国としてサイバー戦を共同して戦うため、サイバー戦に対する技術開発の努力をアメリカと同程度までせねばならない。サイバー戦に対しては米国がぬきんでて進んでいるため、実際に日米同盟国を対象としたSIW攻撃がなされた場合、日米の技術格差により日米同盟関係に齟齬が生じる可能性がある。SIWでは、同盟国の中で一国でもサイバー戦に対する防衛が脆弱な国があれば、そこが脆弱性の窓となって、他の同盟国の情報拠点や情報通信網が破壊される可能性がある。したがって、同盟関係を維持し円滑に運用していくためには、技術格差をできる限りなくし、インターオペラビリティを高める必要性がある。

第二は、秘密保護に関する技術と法律である。米国では暗号技術が国家機密に指定されているように、コンピュータ・システムの秘密保全技術は極めて重要と認識され、法律も定められている。日本がアメリカと同程度の高い暗号技術を開発し、強固な秘密保全体制を採らない限り、アメリカとの円滑な協力はできない。

第三は、サイバー戦により日本国内の空港、湾岸、電力などの重要インフラが混乱に陥りアメリカのパワー・プロジェクション能力が阻害される可能性がある点である。そのようなことがあればアメリカの当該地域でのミッションが遂行できなくなり、日本の不備が日米同盟に大きな亀裂を呼ぶ可能性がある。

第四は、憲法第九条とのかかわりである。サイバー攻撃に対するカウンターSIWが、個別的自衛権に違反しないかという問題をクリアーにせねばならない。特に、カウンターSIWの場合には時間的に瞬時にして行わねばならず、特にアメリカとの共同作戦を展開せねばならない。日米間のインターオペラビリティに大きくかかわる問題である。

したがって、サイバー・テロリストやその他の国家からのサイバー戦に備えて、日米間に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であると考えられる。

－ 注 －

1．Anthony H.Cordesman, Cyberthreats, Information Warfare, and Critical Infrastructure Protection, CSIS, 1998

2．Sunday Times, November 4, 2001.

3．"Address to a Joint Session of Congress and the American People," September 20, 2001（http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html）

4．池田智・松本利秋『早わかりアメリカ』日本実業出版社、p241.

5．9.11テロ以降、アメリカ国内ではモスクが放火されたり銃弾が打ち込まれるなど、アラブ系米国人が迫害を受ける事件が急増しており、ブッシュ大統領は国内向けに「アラブ系米国人やイスラム教徒に敬意を払うことを忘れるべきではない」と国家の分裂をふせぐ発言をしている。(放送されたブッシュ大統領からジュリアーニＮＹ市長への電話)

6．Frank J Clluffo and Curt H.Gergely, "Information Warfare and Strategic Terrorism," *Terrorism and Political Violence*, Spring 1997, pp84-94.

7．Martin Libicki, "What Is Information Warfare?" National Defense University, ACIS Paper 3, August 1995.（http://www.ndu.edu/inss/actpubs/）

８．技術的には衛星などを利用して大域的な情報を直接、兵器の運用に利用することで、オペレーター、センサーおよび兵器を同一のプラットフォームに載せるのではなく、各々の要素を分散して電子的に連係させるシステムが比較優位となりつつある。例えば戦車戦では、砲手が赤外線照準装置を使用しての徹甲弾発射は古くなり、近未来は、センサーからの情報統合で管制官による遠隔操作でミサイルを予測位置に発射することが考えられる。

９．電子戦が戦争の趨勢を決めた例は多い。例えば、第二次大戦時、英軍はドイツのエニグマ暗号を、また米軍は日本の海軍暗号をほぼ解読していた。米国は冷戦の開始と同時に、旧ソ連が外交機密の通信に用いていたベローナ暗号に取り組んだ。

10．レーダーは探査上電波を放射するためレーダー波追尾ミサイルの標的となるので、これを回避するため、レーダー波照射アンテナと受信アンテナを分離して前者を複数個置く手段がとられる。また、航空戦では通常、電子作戦機が随伴し敵側のレーダー探知を攪乱する。

11．暗号化は、電子商取引保護に必要な技術であり、優れた暗号化ソフトウェアの商業用開発が促進されている。民生用暗号技術に、公安当局の解読能力が追いつかないことから、これをテロ集団や組織犯罪が通信に利用するのではないか、と懸念されている。このためアメリカ政府は、必要な場合には公安当局が解読できるように、事前に鍵を供託するタイプの暗号(鍵供託型暗号)を提唱しているほか、56ビット以上の鍵の長さをもつ暗号ソフトウェアの輸出を禁止していた。この規制は1999年９月16日にホワイトハウスの発表した新しい政策では、ほぼ撤廃されている。

12．この点、リビッキは「暗号は、今後とも最良の数学者の関心を惹き付けるであろうが、この分野の長く輝かしい歴史にもかかわらず、暗号をめぐって生じた対立する両陣営の角逐は、近い将来、歴史的な関心以外のものではなくなるだろう」と述べる。

13．山内康英「情報化と安全保障」(『国際問題』第475号、日本国際問題研究所、1999年10月。)

14．マリシャスコード（悪意を持ったプログラム）のうち、単独では動作せず、感染したプログラムを実行することにより実行させられるプログラムのことをいう。

15．特定の条件が成立した場合に悪意を実行するプログラムで自己複製しないものである。

16．EEAの立法は、連邦捜査局(FBI)と米国の産業界が共同して推進したもので、従来、適当な法的枠組みを欠いていた産業スパイについて、FBIに刑事犯罪として訴追する機能を与えることになった。

17．NACIC(National Counterintelligence Center)が議会に提出した1997年度の報告によれば、米国の情報活動に従事する組織からの報告書を合計した結果、少なくとも23カ国が、法的に疑いのある情報収集を米国内で行っており、このうち12カ国はとりわけ活発な収集活動を続けている。

18. 1996年のDIS(Defense Investigation Service: 97年にDefense Security Serviceと改名)の報告書によれば、国外の情報機関が特に関心を示しているのは、航空工学、装甲・兵装、化学・生物、指向・運動エネルギー、エレクトロニクス、地上管制・誘導、遠隔操縦・航行、情報、情報戦争、製造および加工技術、海洋工学、材料工学、原子力、発電、センサーおよびレーザー、署名技術、宇宙工学、兵器の効果測定など18項目の技術である。
19. 被害のあったケースの72%が金銭的損失を出した。
20. Anthony H. Cordesman, Cyberthreats, Information Warfare, and Critical Infrastructure Protection, CSIS, 1998
21. アナライザーというコード名を持つ
22. Cordesman,CSIS,p.51.
23. Frank J.Clluffo and Curt H. Gergely, "Information Warfare and Strategic Terrorism," *Terrorism and Political Violence*, Spring 1997, pp84-94.
24. Cordesman,CSIS,p.72.
25. *Ibid*, p.81.
26. Roger C.Molander, Andrew S.Riddle, Peter A.Wilson, "Strategic Information Warfare: A New Face of War," Santa Monica: RAND, 1996.(http://www.rand.org./publications/MR/MR661/MR661.pdf)
27. 例えば、SIWの軍事行動の初期段階は、被攻撃側が防衛手段を講じないように、いわば休眠状態の電子スパイが前線の後方に、埋め込まれるような形で秘密裏に運ばれるかもしれない。そして軍事行動の後期段階の場面では、出来る限りの混乱とパニックを引き起こすために極めて公然と行われるかもしれない。
28. Anthony H. Cordesman and Abraham R. Wagner, "The Lessons of Modern War, vol.4," Boulder,Colo.: *Westview Press*, 1996.
29. BruceD.Berkowits, "Warfare in the Information Age," *Science and Technology*, Autumn 1995.
30. Defense Science Board, Office of the Undersecretary of Defense for Acquisition and Technology, "Information Warfare-Defense: IW-D," Washington,D.C., November 1996.
31. Robert Kupperman and Darrel Trent, *Terrorism: Threat, Reality, Response*, Stanford, Calf.: Hoover Institution Press, 1979.
32. Cordesman, CSIS, p.10.
33. Bradley Graham, "Cyberwar: A New Weapon Awaits a Set of Rules," *Washington Post*, July 8, 1998, pp.1, 10.
34. また、DSBレポートでは、SIWに対する国防総省の準備状態を改善することを意図した50

以上の措置を勧告している。勧告内容は、国防総省内に、すべての情報戦活動に関して責任を負う中核的部署を指定する、情報戦の防衛面に関する組織を作るなどの他、勧告に対する措置を実施するための経費まで含まれている。

35. 日本戦略研究フォーラム、「サイバー戦と日本の安全保障－頭脳空間における戦争にいかに備えるか－」平成12年７月18日。