情報技術の発達による新たな地球的問題：

ネットナショナリズムとサイバー攻撃

李苑暻

1.　　初めに

現代社会の人々、特に留学生たちはインターネットをよく使う。一日にも何回も情報を検索したり、メールを送ったりする。情報を探す時、 留学生たちは易しく自分の母国にあるウェブサイトに接続することができる。

インターネットが初めて登場した時、国境の意味が弱まり、国家間の対立も減少するなどのバラ色の未来を切り開くという考えもある。しかし、インターネットが世界的に普及するほど、ネットを媒介とした様々な問題も発生している。特に、世界各国で発生しているサイバー犯罪とサイバー攻撃、さらにはサイバー戦争の危険性はますます大きくなり、最近では、世界各国の主要議題として浮上している。

日本でも、企業や官公庁、団体などのデータベースのウイルス感染や情報漏洩が相次いでいる。こうした裏には国境を超えるサイバー攻撃が関連している場合が多く、日本内にもその攻撃者が海外にいる場合の対策について、 いくつかの議論が進められている。

本研究は、まず、新しい地球的な問題として浮上している国家間のサイバー攻撃が発生する理由は何なのかを把握する。続いて、日本を中心とした東アジア内でのサイバー攻撃の社会·文化的な理由、特にナショナリズム的な背景で発生するサイバー攻撃を中心に、その原因と解決策について考えてみる。

２．国境を超えるサイバー攻撃の背景

国家間のサイバー攻撃は軍事的、経済的、社会・文化的背景や目的を持って発生している。まず、軍事的な側面では、敵対関係の国々が相手国の軍事機密を盗むか、国内政治を混乱させ、軍事的な優位に立つために行っている。とりわけＩＴ先進国では、政治・経済活動や日常生活がＩＴシステムで支えられているため、そこを攻撃することで甚大な被害を与えることができる。電気や水道、金融、交通などのインフラを停止させれば簡単にパニックを引き起こすことができるし、誤作動によって施設を物理的に破壊することも不可能ではない（吉澤 2012）。

経済面では、競争的な関係の企業が相手の情報を盗んで不当な利益を得るため、国境を越えるサイバー攻撃が発生する場合がある。例えば、新製品の開発情報を盗み出し、先に

製品化して市場占有率を一変させるとか、競合社の工場の機器やシステムを感染させ、運行停止に追い込めることなどが発生している。

最後に、本研究で最も強調したいことは、国家間の社会・文化的な問題を背景としてサイバー攻撃が発生することである。軍事的、経済的な側面とは異なり、社会・文化的な理由でサイバー攻撃をする人々は、組織化された団体ではなく、個人または匿名の集団である。 2012 年 6 月末、日本音楽著作権協会（JASRAC）、財務省、最高裁判所、自民党と民主党などのホームページが相次いでサイバー攻撃にさらされた。これは国際的なハッカー集団「アノニマス」が 2012 年 6 月 20 日に成立した日本の改正著作権法が自由なインターネット利用を侵害するとして、大規模な示威行動に打って出たとみられる（日本経済新聞 2012）。また、日中韓の間では歴史認識や領土の問題で、サイバー空間で紛争が起こり、相手国の重要ホームページを攻撃する行動も定期的に行われている。このような行動は、誰が攻撃するか把握するのが非常に難しく、法の適用と予防も容易ではない。

サイバー攻撃では、攻撃元をいくらでも偽装できるため、攻撃側が圧倒的に有利となる。攻撃主体が誰かを分かること（帰属問題）が技術的に難しいことのほか、把握しても現在の政治･国際法の下では解決ができない場合が多い。最近の東アジアで展開されているサイバー空間の歪曲された右傾化とサイバー攻撃の危険性は、日中韓の関係及び安全保障まで影響を与える可能性が高まっていることから、地球的問題としての研究が必要である。

３．ネットナショナリズムと東アジアのサイバー攻撃

東アジアのナショナリズムは、西洋の帝国主義的な侵奪と共に様々な経路で形成されはじめ、国家の建設と産業の発展に中心的な原動力となった。一方、ネットナショナリズムは、サイバー空間の技術的･文化的な特殊性により、従来のナショナリズムとかなりの差が存在する。その上、インターネットでは情報の書き直しや歪めることも簡単であり、不正確または不公正な情報を短い時間内に行き渡らせることができるという危険性がある。

また、日中韓のインターネット世論が、言語圏によって分離されていることも問題である。理論的にインターネット世論は、グローバルなレベルで誰でもアクセスできるが、実際には同じ言語を使用する人の間で閉鎖的な空間を形成している。相手国の声が排除されたまま自国のインターネット利用者のみの意見が共有され、ネットナショナリズムは増幅される傾向がある。もちろん、最近機械翻訳技術が発達し、他の言語で書いているウェブ・コンテンツを閲覧することが可能となったが、このような技術もなく、一部のネット掲示板の右翼的な発言が周辺国に送信され、東アジア地域内の相互右傾化という悪循環に陥るの側面を見せている。代表的に、ネット上の他言語で書かれた韓国関連記事を翻訳して紹介する「ゲソムン（噂）ドットコム

（http://www.gesomoon.com）」というサイトがある（Kim、2011）。このサイトには、通訳者と一般利用者が海外のネット掲示板に出入りして収集された韓国関連の発言を翻訳して提供する。出所の 30%程度が日本の代表的なネット掲示板である「２ちゃんねる（http://www.2ch.net）、以下 2ch」であり、最も刺激的な内容を中心に翻訳されている。

このような現状で、サイバー空間では、東アジアの両国間あるいは 3 カ国間の争点について生産的な議論が行われることより、極端な国粋主義が繰り返したり、歪曲された情報に基づいて相手国を中傷したりすることが日常的に行う勢力が共通に表れている。このような偏った意見を持っている勢力が全体ネット利用者のうちの一部にすぎないとしても、その内容の刺激性が高いため、他のネット利用者の目を引くことが容易である。さらに、インターネット上の極端な言説が、いくつかの流動層の視覚と判断に影響を与える可能性がある。最終的に日韓・中韓・日中関係に悪影響を与える可能性があることに、その危険性を地球的な観点で考えなければならない。

日韓のネットナショナリズムに起因したサイバー攻撃として、次のような事例がある。まず、毎年の 3 月 1 日には、韓国で日帝時代の「3.1 独立運動」という反日運動をした日のため「3.1 節」という記念日なので、韓国と日本の一部のネット利用者間の DDoS 攻撃（分散型サービス不能攻撃）が引き続き発生している。DDos 攻撃とは、特定のウェブサイトに大量のリクエストを送りつけて「落とす」攻撃である。その手法は非常に簡単で、ホームページの再読み込みボタン（ F5 キー）を押すだけである。これを十数万人規模で実施することで、ホームページが応答不能になってしまう。また、2010 年には韓国の人気ネット掲示板「DCInside（http://www.dcinside.com）」で、2ch に韓国のフィギュ・アスケートのキム･ヨナ選手が審判を買収して金メダルを取ったなどの発言が多数掲載されっているということで、2ch にアクセスして F5 キーを連続で押すことと攻撃用プログラムを使用したことでサーバーへの接続障害を起こした。当時、2ch の利用者も韓国大統領府とサイバー外交団を標榜する VANK(Voluntary Agency Network of Korea）のホームページを攻撃することで仕返し、 VANK のサーバーが一時に不能になった。この攻撃は、組織化された団体ではなく、匿名の個人がサイバー空間で一時的に集まって行動したことで、参加者を把握して処罰することが不可能であり、関連法も整備されてない状態である。

４．小結：サイバー空間の平和のための東アジアの取り組み

サイバー攻撃の危険性が高くなる事態を受けて、各国は本格的な「サイバー武装」を強化している。2011 年７月、米国防総省は「サイバー空間作戦戦略」を発表し、サイバー空間を陸・海・空・宇宙に次ぐ「第５の作戦領域」と位置付けた。この戦略は、米国がサイバー攻撃を受けた場合、ミサイルなどの通常兵器で報復攻撃をすることができるということを表明している。しかし、サイバー空間という脱近代的な空間での問題を、近代的な方

法で解決しようとすることで、各国の反対にあい、その効果についても疑問が出ている。

一方、東アジアには米国と違い平和的な動きがある。一例として、日本と韓国がサイバー空間の平和のためにしている政府間の協力とインターネット・リテラシー（literacy）教育は、他国が反発を持つ余地が少なく、東アジア地域の平和にも貢献できる方法であると思う。まず、韓国のKISA（Korea Internet and Security Agency）は3.1節を控え、日韓のDDoS攻撃や不正投稿の拡散などの攻撃を防ぐために、韓国の大統領府・外交部・独島関連サイト･人気ネット掲示板などの主要なサイトの監視を強化した。また、KISAはJPCERTコーディネーションセンター（JPCERT/CC）と緊急連絡システムを稼動して、モニタリング情報を共有することで、日韓の間に発生するかもしれない事故に迅速に対応することができ、2012と2013年3月1日には、両国の主要サイトに何も問題がなかった。

最後に、日本では、インターネットの登場で、誰でも自由な発言が可能になることで、メディア・リテラシー能力が低い者同士に同調したことがネット右翼の本質であると批判する声が高まっている。このため、各国ごとにネットナショナリズムの危険性を認識し、全体的なネット利用者のインターネット・リテラシーを高める努力が必要である。

将来的には、サイバー空間で今より多くのことができるはずで、この空間をより良く活用するために適切な制度が必要である。この制度は一つの国家で作ることはできないので、国家間の協力がもっと重要になると予想される。

参考文献

川口貴久. 2013.「サイバー空間の安全保障をめぐる課題とアメリカの動向」.『日本国際問題研究所平成25年度研究プロジェクト分析レポート』

土屋大洋. 2012. 『サイバー・テロ日米vs.中国』. 東京: 文藝春秋.

吉澤亨史. 2012.「サイバー戦争、圧倒的破壊力のサイバー攻撃：出遅れた日本は格好の標的」.『エコノミスト』. 第 90 巻第 35 号. 52～53 頁

日本経済新聞. 2012.「ハッカー集団、日本標的、官庁・政党などにサイバー攻撃」6 月 28 日. 朝刊. 3 ページ

Mie, A. 2013. "NET UYOKU: Xenophobia finds fertile soil in web anonymity", *The Japan Times*, Jan 8.

Wu, X. 2007. *Chinese cyber nationalism: Evolution, characteristics, and implications*. Lanham: Lexington Books.