

日中韓のネットナショナリズムとサイバー攻撃

代表研究者 李 ウォンギョン 上智大学 グローバル教育センター 特別研究員

1 はじめに

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、攻撃者が海外にいる場合の対策について、色々な議論が進められている。しかし、多くの研究が軍事・経済的な側面に集中されているため、本研究は国家間の社会・文化的な問題を背景としてサイバー攻撃が発生した事例に注目したい。軍事・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行う人々は、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。そして、他の攻撃と比べても、攻撃主体が誰かを分けることが技術的に難しいこと（帰属問題）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。

本研究は、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る。そのため、第2節では先行研究を中心に、ネット上のナショナリズムの登場を説明する理論と日中韓の最近のナショナリズムの傾向を明確にする。特に、カイアニ(Caiani, 2013)のヨーロッパの事例研究を参照し、技術的な変数として提示したのが何かを把握する。本研究は権威主義を経験した日韓では、どのような右翼コミュニティが存在し、各のコミュニティはどのように連結されているかを調査する。第3節では、日中韓の主要なインターネット掲示板の内容や相互作用を中心に、過去10年間のナショナリズム的な言説の変化を比較する。右翼の言説の主題が多様化され、活動領域も広がっていたことを示す。第4節では、日韓・日中・中韓の間に発生したサイバー攻撃の体系的な事例を選び、その背景にある技術的な側面に注目した。第5節では、サイバー攻撃に対応するための各国の制度と協力動向を見ながら、共通の取り組みが協力の機会を提供する可能性もあることを示唆する。

2 理論的背景

2-1 インターネット・ナショナリズム

(1) インターネット・コミュニケーションの性格

サイバー空間 (cyber space) は1990年代から登場した新たなコミュニケーションの通路である。インターネットを媒介としたコミュニケーションの性格に関しては、いくつかの対立的な議論があり、交流の促進や仮想のコミュニティ (virtual community) の形成の可能性を予測する意見¹がある一方、むしろ帰属集団のアイデンティティや外集団への偏見が強化される集団極端化 (group polarization) 現象が発生することを予測する研究 (Sunstein, 2011) もある。本研究の第3節でも注目するネット掲示板に対しても、有益な情報を得ることができる新たなコミュニケーション空間、いわゆる「電子アゴラ」という見方がある反面、極端な意見や中傷がありふれている「葛藤の空間」という対立的な評価が存在する。DiMaggio et al. (2001) は学界を中心に、サイバー空間への評価が楽観論と悲観論の時代を超え、インターネットをベースとした人々の相互作用の特性を理解する社会科学的な研究がさらに本格化されている第三の段階に進んでいく必要性を指摘したので、本研究もその視点を採択した。

国家間の交流の側面でのサイバー空間でのコミュニケーションは、交流の主体を少数エリートから多数の

市民に、一時的・部分的な交流から日常・全面的な交流に変換するきっかけになってきた。1990年代以降のグローバル化の影響で、全体的な国際交流での国家主導の比重が縮小され、企業・自治体・教育機関・市民団体・個人など、民間交流の比重が高まってきた。さらに、インターネット・コミュニケーションはが国境を超える交流の物理的な制約をほとんど消え、交流のコストも大幅に低くなってきた。ネット上では違う言語を使う利用者同士でも、自動翻訳などの特化サイトを介して交流することもでき、その結果、電子メール・テキストメッセージ・チャットサイト・ネット電話など、様々な手段を介し、違う国籍を持っている人々が会話を交わす状況である。しかし、グローバル化と情報通信技術(ICT)の発達で領土や国民国家(nation state)など近代的な概念を弱体化させる可能性と共に、むしろ他国との異質性を浮き彫りにし、ナショナリズムを拡大させるという視点が共存している(Calhoun, 2007)。

本研究は、サイバー空間で右傾化が展開されている理由として、脱近代的な ICT の特徴に注目したい。Lew et al. (2008) はインターネット・ナショナリズムについて、個人が民族に最高の忠誠を捧げるべきと信じる近代的なナショナリズムが、サイバー空間でネットワークを利用し、言説が増幅されている特徴を強調した。この過程で、生産的な論議が行われるのではなく、矛盾的な言説が繰り返されていると主張した。Caiani (2013) はイタリア・ドイツ・フランス・スペイン・イギリス・アメリカの右翼のインターネット・コミュニティを調査し、形成の背景を政治、文化、技術の3つに分けて考察した。例えば、フランスとイタリアのように極右政党が議席を増やすことに成功した国とスペインとドイツのように変化が表していない国、権威主義的な政府を経験したイタリア・ドイツ・スペインとの経験がないイギリス・アメリカの右翼のネットコミュニティの数や連結方式を比較した。調査対象国では60~140個以上の極右性向のネットコミュニティが存在しており、社会ネットワーク分析(social network analysis: SNS)を利用して、サイト間のハイパーリンクを調査した。その結果、各サイトはコミュニケーションよりイデオロギーの伝播に集中していることが明らかになった。ネットコミュニティの展開については、36%がNeo-Naziなど排外主義的な活動に参加し、29%は極右政党への支持を表明、19%は若い世代のサブカルチャー化、7%は政治活動へ参加するように分化したと記述した。

(2) 日中間の場合

日中韓は、インターネットの使用率が高く、特にネット掲示板でのコミュニケーションが若者層の文化として活発化されているが、コミュニケーション機会の拡大が相互理解に繋がっていることではない。すなわち、日中韓の人気ネット掲示板では他国に関する意見が、ネットの匿名性を悪用して誹謗中傷になったり、排外主義的な発言が溢れることで、葛藤の側面が急速に増幅されている。

日中韓のサイバー空間での右傾化、ひいてはインターネット・ナショナリズムの登場においては、東アジア内の歴史的な葛藤や社会・経済的な問題など「近代的」な要因を通じて説明する研究が多い。高原(2006)は、日中韓で一部のネット利用者がナショナリズム的な性向を積極的に表出している背景には、経済的な不安があると見て、これを「不安型ナショナリズム」と命名した。1960~70年代のナショナリズムが高度成長期の日本に対する自負心を基に形成されたことと比べ、不安型ナショナリズムは、経済不況と社会流動化に不安を感じている若者のネット上の「趣味」として成長していたという。近藤(2007)も、バブル世代は心理的余裕を基にリベラルな性向を持っていたが、経済的な余裕がない世代はネット上でナショナリズムをサブカルチャーの形で発現させ、楽しんでいると指摘した。彼らには排外主義的なコンテンツも他のネット利用者の関心を引くことができる、一つの遊びに過ぎないと述べている。しかし、本研究は、日中韓のインターネット・ナショナリズムには ICT 本来の技術的な特徴が大きな影響を及ぼしたと仮説を立て、ナショナリズムを背景に発生したサイバー攻撃を減らすためにも日中韓が技術的な協力を中心に共通の取り組みを形成することがもっとも重要と見ている。そのため、カイアニ(Caiani, 2013)のヨーロッパの事例研究を参照し、日中韓のサイバー空間ではどのような右翼コミュニティが存在し、各のコミュニティはどのように連結されているかを調査する。日中韓の事例として、日本の「ネット右翼」、中国の「中国紅客連盟」、韓国の「反日活動家」を挙げ、ネット上で彼らが形成し始めた10年前には、社会での影響力が微小であったが、最近では活動領域が拡大され、国際関係にどれほどの影響力を及ぼしているかを検証する。また、過去10年間、各コミュニティの性格が変化した場合、その原因は何なのか分析する。

2-2 サイバー攻撃

サイバー攻撃は、一定の目的を持った Hacker や Cracker が情報通信技術を利用して計画的に国家・企業・団体・個人のコンピューターやそのシステムに不正なアクセスを行い、停止または誤作動させたり、あるいは情報を消去することで、被害を与える行為である。個人レベルのサイバー攻撃は、一応サイバー犯罪として認識されるが、政治的な動機を持っていたり、その攻撃が国境を超える場合にはサイバーテロ、さらにはサイバー戦争に拡大される可能性もある。

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）。その上、電力システムや化学工場の制御システム、交通管制システムなどの基盤施設に攻撃が行われた場合は、死傷者が出ることもある（山崎，2015）。

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、社会・文化的な理由でサイバー攻撃が発生することもある。サイバー攻撃では、攻撃者を偽装できるため、攻撃する側が圧倒的に有利であるが、特に社会・文化的な理由で攻撃する人々は、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ことが多いことから、法の適用と予防も容易ではない。

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が定期的に行われている。情報社会が加速されるとほど、市民が利用する公共施設の情報通信技術に対する依存度は大きくなり、その分、サイバー攻撃にさらされる可能性ははるかに大きくなっている。国の主要な基盤施設の運用もコンピュータ・ネットワークに依存している状況で、新たな脆弱性も増加していることである。

3 日中韓のサイバー空間での右傾化の傾向

3-1 日本の「ネット右翼」

日本のサイバー空間では、1990年代後半から反韓・反中感情を表出しており、2005年にはメディア²から「ネット右翼」と名付けられた集団が存在する。従来の右翼とは異なり、排外主義を表している「ネット右翼」は、10余年の進化を続け、ネット上のコミュニティだけではなく、オフラインでも行動する団体として成長した。特に、最近の2～3年間には、ネット右翼の存在や言説が中韓にも報道され、関心も集めている。ネット右翼が主に活動している空間としては、日本語電子掲示板サイト 2ちゃんねる（以下、2ch）³、ニコニコ動画⁴、ヤフージャパンニュース掲示板⁵、日本文化チャンネル桜⁶、過激派の Twitter アカウントなどが指摘されている（北田 2003，近藤・谷崎 2007，辻 2008）。

2ch とニコニコ動画などは、ネット右翼だけの空間ではないが、韓国では嫌韓サイトとして指摘され、サイバー攻撃の対象にもなっていた。特に 2ch は、700 種を超える様々なテーマの議論が行われている世界最大規模の掲示板である。ネット右翼が活動している代表的なコーナーは △ニュース速報+ △東アジアニュース+ △ニュース極東 △戦争・紛争 △ハングル △中国など 10ヶ所を過ぎないことで、全体の掲示板の規模に比べると微々たる水準である。各掲示板の利用者は、テーマに関する内容を投稿しているが、ネット右翼は活動拠点とした掲示板で、韓国と中国を誹謗する文章を繰り返して書き込み、いわゆる「荒らし(trolling)」を行うことで討論を妨害している。また、ヤフーニュースのコメント欄では、韓国あるいは中国関連の記事に排外主義的なコメントを作成し、他のネット利用者の目を引くことを目的にしている。

しかし、日本のネットで排外主義的な言説が多くなっているにもかかわらず、ネット右翼の数が多いことか、少数のネット右翼が作成したコメントが多いことかを判断することは容易ではない。複数の電子メールや SNS アカウ

ントを匿名で作成し、活動するネット右翼が多いため、正確な規模を把握することが技術的に難しいからである。アンケート調査に基づいた辻(2008)によると、ネット右翼は20～30代の男性が中心で、反韓・反中の意見を積極的に繰り広げる少数と、ネット右翼の投稿に対し、投票機能を利用してコメントに「そう思う」か「そう思わない」のボタンを押すことで、自分の性向を表現する多数に分けることができる。

ネット右翼の活動空間は、ウィキペディア、企業のホームページ、ホワイトハウスのホームページなどネット上で拡大されてきた。一部は、2011年8月のフジテレビ抗議デモなど、オフラインでの活動に参加するようになった。一方、他の一部は単発的に行われる活動ではなく、排外主義の勢力化として成長し、2007年1月、桜井誠を中心にしたネット右翼が集まって発足した「在日特権を許さない市民の会⁸(以下、在特会)」になっていた。在特会は、歪曲されたデータに基に、在日コリアンと中国人が、日本の優遇措置を不当に受けていると主張している。2016年6月現在、1万6千人の会員が登録した日本最大規模の右翼団体に成長し、徐々に日韓関係にもある影響力を広げている。在特会は、発足当初に2chの掲示板、右翼系のブログ、SNSなどのサイバー空間で、自分の不満と怒りを「特定アジア(韓国、北朝鮮、中国)」に表出していた。しかし、2012年からは日本国内の代表的な韓人タウンで、韓流の中心地である東京の新大久保と大阪の鶴橋をはじめ、各地でデモを実施している。2013年には、彼らの過激な発言(hate speech)と破壊行為が、韓国と中国のメディアにも詳しく報道され、日韓・日中関係の新たなリスクになっていた。

3-2 中国の「紅客連盟」

中国紅客連盟(HUC; 以下、紅客⁹)は、1999～2000年に北京大学の在大学生を中心に形成され、最近までアメリカ・台湾・日本・韓国などの政府関係のウェブサイトに一連の攻撃を仕掛けたナショナリズムを備えたハッキング・グループである。その名は、共産党の色である紅のハッカーが、無政府主義者が多い黒客(ハッカー)たちを相手に中国政府を援護して戦っていることを示唆する。

日中間では、2010年9月に尖閣諸島で中国漁船衝突事件が起きたことや2012年9～10月に日本政府が尖閣諸島の国有化を検討したことをきっかけに、紅客が日本政府機関ウェブサイトを攻撃する計画を表明していたことがある。その結果、2010年9月16～17日には警察庁のサイトに接続できなくなることを含め、大量のデータを標的に送りつけたDoS攻撃を受けた。2011年には紅客のリーダーが「日本攻撃専用DOSツール」を配布し、使用方法もブログにアップしたと言われ、日本にとってはサイバー攻撃の中で中国発の攻撃が最も脅迫的に認識されている(土屋, 2012)。

3-3 韓国の「反日活動家」と「日ベ」

韓国のサイバー空間での右翼的な過激派、特に日本に対する動きは、いくつかの「反日サイト」から観察できる。愛国を強調し、中国人を中心とした外国人に対して反感を表出する「日刊ベスト貯蔵所(以下、日ベ)¹⁰」というサイトも存在する。

韓国の社会には、日本の植民地支配の経験から由来した根強い反日感情が存在する。特に、匿名性が高いインターネットでは、反日感情が過激に表出され、ネット上の日本関連ニュースに内容とは関係ない非難のコメントを書くなど、感情的に対応する利用者が多く見られる。歴史問題や独島のような主題が登場した場合には攻撃性がより高くなり、日本を嫌悪する発言として現れることもある。日本の地震や災害に関連する記事に、嘲笑するコメントがつく場合もある。体表的な反日サイトとして2004年からは、2chを中心とした日本のウェブサイト、直接サイバー攻撃を試す集団が出現した。韓国の2chとしても知られている「デジタルカメラ・インサイド(以下、DCinside)」の「コメディ・プログラム掲示板」、「歴史掲示板」など一部の掲示板の利用者が、ネット上の「反日活動家」になり、「ネットテロ対応連合(以下、ネット対連)¹¹」を結成した。ネット対連の主な参加者は小・中学生男子であり、掲示板では日本へのサイバー攻撃を論じるポスティングを除くと、試験・成績・歴史授業などが主要話題になっていた。オフラインへの進出は、活発ではなかったが、2011年と2013年の日韓のサッカー試合中、プラカードを掛けた事件が発生したことがある。

ネット上の過激派が、全体のインターネット利用者のうち一部に過ぎないとしても、その内容の刺激性が

高いため、他のインターネット利用者の目を引くことは容易である。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野と判断に影響を与える可能性があり、最終的には日韓・中韓関係に悪影響を与える可能性を見落としてはならない。

4 サイバー攻撃の展開と情報通信技術

4-1 日中韓でのサイバー攻撃

ネット上の過激派の影響力が拡大されていた背景には、まず、ICTの発展を考えられる。過去10余年の日中韓のインターネット利用率は、表1に示しているように増加を続けていた。サイバー空間が新しい対話の場になり、国家間の対立も減少するという考えもあった。日中韓ではインターネット利用者間の対話が可能になったことから、相互理解にも肯定的な影響を及ぼすことが期待された。しかし、インターネットが普及するほど、情報通信技術(ICT)を媒介とした様々な問題も発生し、2000年代には日中韓のサイバー空間での紛争は増加してきた。

表1 日中韓のインターネット利用率：2000～2013年

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Japan	30.0	38.5	46.6	48.4	62.4	66.9	68.7	74.3	75.4	78.0	78.2	79.1	86.3	86.3
Korea	44.7	56.6	59.4	65.5	72.7	73.5	78.1	78.8	81.0	81.6	83.7	83.8	84.1	84.8
China	1.8	2.6	4.6	6.2	7.3	8.5	10.5	16.0	22.6	28.9	34.3	38.3	42.3	45.8
Hong Kong	27.8	38.7	43.1	52.2	56.4	56.9	60.8	64.8	66.7	69.4	72.0	72.2	72.9	74.2

出所: ITU, ICT Statistics Database.

例えば、日韓の交流において1990年代末から2000年代前半に至る時期は画期的な変化期と言われている。両国間の大衆文化の流入が本格化されたことと、サッカーワールドカップの共同開催など協力の経験が増えたことで、相手国に親しみを感じる人が増加したのである。それと共に、ブロードバンドの普及が急速に行われ、国境を越えるコミュニケーションの機会を大衆にも与えた。しかし、日韓のネット利用者がサイバー空間で、相手国のウェブサイトや掲示板を攻撃する事例も2001年から発見された。2002年から2008年の間には表2のように、独島－竹島・東海－日本海・慰安婦問題など歴史と領土を巡る論争が、サイバー空間に移動し、代理戦を行っていたと見られる。この時から、毎年3月1日(韓国の独立運動記念日)、2月22日(竹島の日)、8月15日(韓国の光復節)、10月25日(独島の日)など、一定な周期でサイバー攻撃が発生し始めた。

両国のサイバー攻撃が本格化され、その影響力が大きくなったことは、2010年から2012年である。この時期には、両国のネット利用者の興味の対象が、スポーツ試合の結果、相手国のコンテンツ政策、移民者への福祉などに広がってきた。2013年2月、ネット上で23人を対象として行ったアンケート調査によると、韓国の反日活動家が日本へのサイバー攻撃に参加する理由の中で最も多かったのは「楽しさ」と「ストレス解消」である。これは、サイバー攻撃のリーダー層が、「日本が先に攻撃していたから」あるいは「愛国者になりたいから」を選択したことと違っている。その他、「日本より発達していた韓国のICTを自慢するため」という応答があり、両国間の技術競争がサイバー空間で歪曲されて表していることも見せる。

表 2 日韓のサイバー空間での紛争

日時	動機	攻撃者	対象	活動計画	結果
2001年 3月1日	日本で扶桑社版「新しい歴史教科書」が検定合格	DCinside	文部省/自民党	DoS攻撃	システムの一時的障害
2002年6月	サッカーワールドカップの日韓共同開催	Enjoy Japan	Enjoy Japan	掲示板での議論と非難	-
9月	小泉首相の訪朝による拉致問題発覚	2ch	ハン・ワールド	嫌韓ヘイトスピーチの投稿	HANBoardの閉鎖
2003年6月	青山里戦闘の真偽の論争	Enjoy Japan	Enjoy Japan	掲示板での議論と非難	-
12月29日	ネット右翼による「Kの国の方式」の開設	DCinside	Kの国の方式	DoS攻撃	Kの国の方式の閉鎖
2004年1月9日	小泉首相の「竹島は日本の領土」発言	DCinside	2chとミラーサイト	DoS攻撃	システムの一時的障害
1月16日	韓国の独島記念切手発行				
2005年1月14日	島根県の条例による「竹島の日(2月22日)」の指定	DCinside	2ch/島根県	DoS攻撃	システムの一時的障害
8月5日	グーグルの「東海」表記	2ch	VANK	DoS攻撃	システムの一時的障害
2008年5月	ウィキペディアによる「独島-竹島」編集禁止	2ch DCinside	ウィキペディア	書き直し	編集禁止
8月15日	韓国の光復節	DCinside	2ch	DDoS攻撃	-
2010年	2ch、ロシアで韓国人留学生の襲撃事件を嘲笑	DCinside	2ch	DDoS攻撃	システムの障害
2月18-26日	バンクーバー五輪でのキム・ヨナの金メダルを嘲笑				
3月1日	日韓併合100周年	DCinside ネット対連			
3月2日	3.1の攻撃の打ち返し(1)	2ch	VANK/青瓦臺	DDoS攻撃	サービスの一時遅延
8月15日	3.1の攻撃の打ち返し(2)	2ch	韓国ゲームサイト	-	-
2011年3月1日	「テロ国」にならないため、攻撃されることを待ち	DCinside	2ch	-	攻撃無し
7月25日	高岡蒼佑がツイッターで「反韓流」コメント	-	-	2chでの議論と非難	8月のデモ計画
8月7日	フジテレビの本社前での放送番組が	2ch	フジテレビ	600人	
8月21日	韓国プログラムに偏重されたと抗議			5000人参加	
8月15日	TBSでの韓国選手への殴打事件 日本の国会議員の独島上陸	DCinside ネット対連	2ch TBS	DDoS攻撃	-
9月1日	フジテレビのスポンサー 「東海」と表記した鏡月社の日本販売担当	2ch	KAO サントリー社	不買運動	
2012年3月1日	「テロ国」にならないため、攻撃されることを待ち	DCinside	2ch	-	攻撃無し
3月21日	独島の広報モデルに活動した俳優キム・テヒの入国 ロート製薬がキム・テヒをモデルに起用	2ch	ロート製薬	不買運動	
5月10日	ニュージャージー州で日本人慰安婦碑が建立	2ch	ホワイトハウスhp	請願掲載	-
8月10日	李明博大統領の独島訪問	2ch	DCinside	-	-
11日	ロンドンオリンピックのサッカー日韓戦のセロモニ	DCinside	2ch	-	-

三国のサイバー空間での紛争が増えるようになったきっかけは、2ch、Baidu、DCinsideなどの国内向けのネット掲示板の内容を翻訳して紹介するサービスが登場したこと、電子翻訳機の機能が向上したことのようにICTがある。インターネット環境が整備され、コンピュータを利用した翻訳技術が発達しながら他国のウェブコンテンツの内容を閲覧することが可能になり、掲示板での排外主義的な言説が周辺国にすぐ転送され、東アジア地域内の相互右傾化という悪循環に陥る側面もある。その上、インターネット・ニュースの普及もサイバー空間での葛藤の原因になっている。インターネットニュースは、従来のメディアとは異なり、各記事をクリックする数に応じて経済的な補償が決定される。つまり、重要なニュースではなくても、ネット利用者の目を引く刺激的な内容であれば、メインの記事になれるシステムである。この過程で、ネットメディアが反日・反中・反韓感情を過度に刺激している傾向があることに注意する必要がある。

4-2 サイバーセキュリティ技術の進化と認識の変化

三国の民間レベルでのサイバー攻撃、特にナショナリズム的な背景で発生する攻撃の方法は、2000年代初には不法プログラムを利用した「サービス拒否攻撃(以下、DoS 攻撃)」が多く、特定サイトに障害を発生さ

せることを目標としていた。一方、2000年代後半からにはDoS攻撃より強力な「分散型サービス拒否攻撃(以下、DDoS攻撃)」に進化し、攻撃の対象サイトも多様化された。

例えば、現在までの日韓サイバー攻撃の中で、最も大規模として知られている事件は、2010年3月1日と2日、DCinsideと2chの間に発生した。2chのサーバーを管理していた米国のPacific Internet Exchange(PIE)によると、3月1日午前11時40分頃から、韓国を発信源とする大量のアクセスがあり、2chのサーバーの負荷が上昇された。PIE社は2chのサーバーをすべて停止させ、攻撃の発信源となったIPアドレスからの通信を遮断する措置をとったが、サーバーの回復と広告収入の減少など、約250万ドルの被害が発生したと述べた。一部のネット右翼は反撃を試み、韓国の民間外交使節団「Voluntary Agency Network of Korea: VANK」や青瓦臺(大統領官邸)サイトのアクセス速度の低下が発生した。

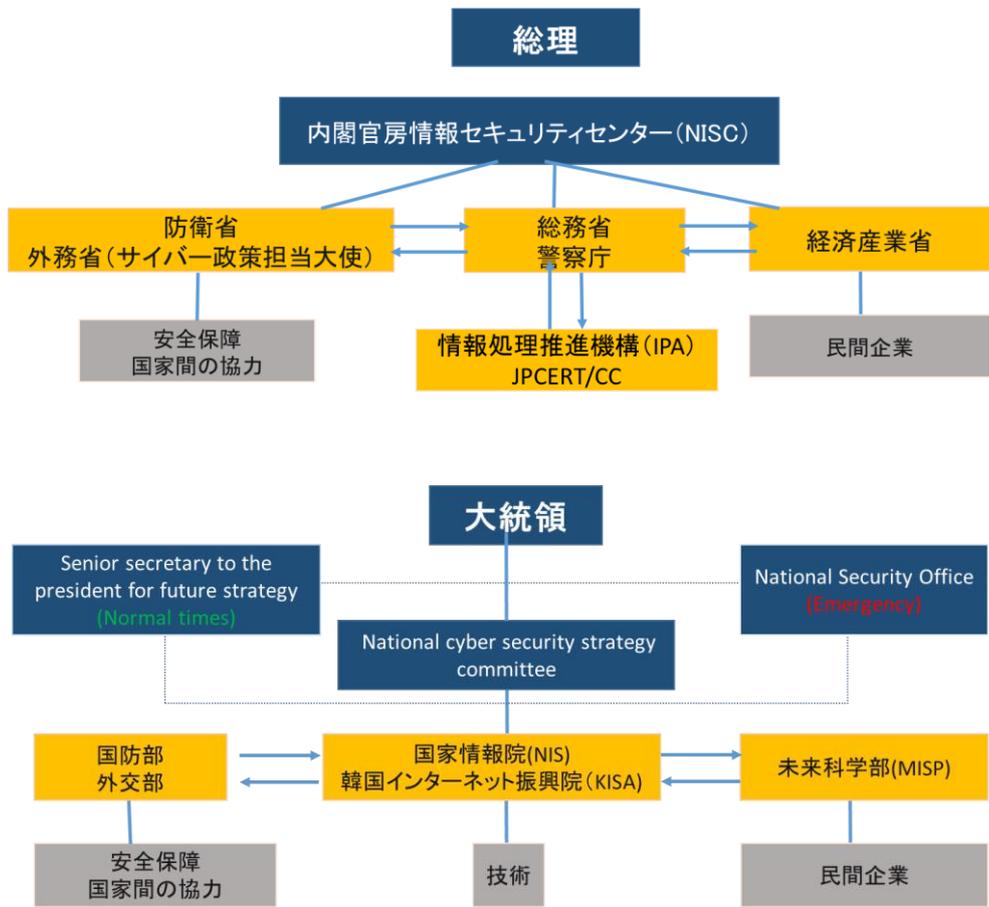
この事件は、1990年代末からの日韓の交流の増加、特にブロードバンドの普及でインターネットを媒介とした対話が急増したことの影が極大化された現象だと思われる。その時期には、多くのネット利用者がまだ「サイバー攻撃は犯罪」として認識してなかったことと、両国のサイバーセキュリティ会社や機構の対応が不十分であったこと、両国間のサイバー協力の経験が浅かったことも事態を悪化させた。それをきっかけにサイバー攻撃は犯罪という認識も両国で徐々に広まり、この以降にはネット右翼と反日活动家の双方ともに反応は冷ややかた。

5 日中韓のサイバー攻撃の関連制度

2000年代の日中韓のサイバー空間では、社会・文化的な問題、特に歴史認識や領土の問題でサイバー空間で紛争が起こり、相手国のウェブサイトやサーバーを攻撃する行為が定期的に行われていた。社会・文化的な理由でサイバー攻撃を行う個人または匿名の集団を減らすためには、技術的な工夫とともに関連制度の整備も必ず並行されなければならない。このような試みはある程度成功的であり、韓国のインターネット振興院(Korea Internet and Security Agency: KISA)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、韓国の青瓦臺・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働して、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年から2016年の3月1日には、両国の主要サイトに問題が起らなかった。

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、政府間の共同の取り組みも始まっている。一方、現在までの日中・中韓のサイバーセキュリティ分野での協力と比べると、日韓の間の協力がはるかに進んでいることが分かる。2011年以降、日韓のサイバーセキュリティ関連組織と「サイバーセキュリティ基本法」などの法律が整備され、図1のように日本と韓国のサイバー攻撃に対する取り組みが類似していることで協力が比較的容易になった。

図1 日韓のサイバーセキュリティ関連組織



2004年、日本のIPAと韓国のKISAの相互協力協定(MCA)が採決したことをはじめ、民間・機構レベルでの日韓のサイバー協力も次々に実現されていた。2011年頃からはJPCERT/CCとKISAの緊急連絡システムを稼動したことや日本ネットワークセキュリティ協会(JNSA)と韓国知識情報保安産業協会(KISIA)の共同シンポジウムを定期的に関開くようになったことなど、協力がより深くなっている。それは、日本と韓国は2009年7月などで朝鮮・中国発と思われる大規模なサイバー攻撃に共に直面したこと、ナショナリズムを背景にした2010年3月の日韓の間のサイバー攻撃などが両国と日米韓の安全保障の脅威になりかねないという危機感が高まってから実現できたと思われる。

そのように、サイバー攻撃に対応する共通の取り組みは両国あるいは三国の協力の機会を提供している側面もある。日中韓のCyber Policy Consultationなど、サイバー空間の平和のために行っている政府間の協力が国際法によるサイバー攻撃規制のための論議に繋がり、学界でも技術とコミュニケーションに関する研究やインターネット・リテラシー教育まで拡大されることができたら、東アジア地域の平和にも貢献できる機会になる可能性もある。

6 おわりに

2000年代以降、日中・日韓・中韓の間に発生したサイバー攻撃の代表的な事例を分析した結果、社会・文化的な要因の中でも、特にナショナリズムを背景として攻撃が発生したことが分かる。両国間に歴史認識や領土に関する問題が発生した時期に、インターネット掲示板を中心としたサイバー空間でも紛争が起こり、相手国のウェブサイト攻撃する行為が繰り返行われていた。サイバー空間には「ネット右翼」(日本)、「中国紅客連盟」(中国)、「反日活動家」(韓国)などの過激派コミュニティが存在し、過去10年間のネット掲示板ことの相互作用が拡大、ナショナリズム的な言説の主題も多様化され、活動領域も広がっていた。

そこには、ICTの技術的な変数が重要な影響を及ぼしたとみられる。

その反面、2012年まで増加したナショナリズム的な背景で発生するサイバー攻撃は、2013年以降は収まっている傾向がある。それは、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が、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たことにより、2010年代から政府間の共同の取り組みが始まっていたからだと推測される。サイバー攻撃に対応するための日中韓の共通の取り組みは、両国あるいは三国間における共同連携の機会を生み出すという肯定的側面がある。

日韓のネット上の右翼的な過激派は、10年前には現実での影響力が微小であったが、最近では活動領域が拡大されていることが分かる。それは、日韓がサイバー攻撃を行うことができる相手として認識させることと、両国間の世論を悪化させることとして、民間レベルおよび技術に関する両国関係にある影響を与えている。しかし、このような現象が両国間の外交関係にも影響を及ぼすようになったかを分析するためには、今後の追跡調査がさらに必要である。

【参考文献】

- Calhoun, C. (2007) Nations matter: Culture, history, and the cosmopolitan dream. London & New York: Routledge.
- Caiani, M. & Parenti, L. (2013) European and American Extreme Right Groups and the Internet. Ashgate Publishing
- Castells, M. (2010) The Rise of the Network Society. Malden, MA: Wiley-Blackwell.
- Chase, T. (2011) Nationalism and the net: Online discussion of Gogureo history in China and South Korea. *China information* 25(1): 61-82.
- Conversi, D. (2012). Irresponsible radicalisation: Diasporas, globalisation and long-distance nationalism in the digital age. *Journal of Ethnic and Migration Studies*, 38(9), 1357-1379. doi:10.1080/1369183X.2012.698204
- DiMaggio, P., Hargittai, E., Neuman, W. and Robinson, J. (2001). "Social Implications of the Internet" *Annual Review of Sociology* Vol. 27: 307-336
- Eriksen, T. H. (2006). Nations in cyberspace. Ernest Gellner Lecture, Delivered to the ASEN Conference, London School of Economics,
- Fackler, M. (2010, August 28). New dissent in Japan is loudly anti-foreign.
- Hamelink, C. J. (2000). The ethics of cyberspace. London: SAGE.
- Mie, A. (2013, January 8). Net Uyoku: Xenophobia finds fertile soil in web anonymity. *The Japan Times*.
- Oishi, Y. (2008) "A Consideration of Media-Nationalism: A Case Study of Japan after the Second World War", *Keio Communication Review*, 30: 5-17.
- Therwath, I. (2012). Cyber-hindutva: Hindu nationalism, the diaspora and the web. *Social Science Information Sur Les Sciences Sociales*, 51(4), 551-577. doi:10.1177/0539018412456782
- Sakamoto, R. (2011). "Koreans, Go Home!" Internet Nationalism in Contemporary Japan as a Digitally Mediated Subculture, *The Asia-Pacific Journal: Japan Focus* Sunstein, 2011
- Wu, X. (2007). Chinese cyber nationalism: Evolution, characteristics, and implications. Lanham: Lexington Books.
- あ川口貴久. (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』
- 金明秀. (2011). 「インターネット利用史にみられる2つの《グreshamの法則》——ハン・ワールドの体験を中心として」 <http://han.org/a/gresham>.
- 近藤瑠漫・谷崎晃編. (2007). 『ネット右翼とサブカル民主主義: マイデモクラシー症候群』. 東京: 三一書房.
- 高原基彰. (2006). 『不安型ナショナリズムの時代 : 日韓中のネット世代が憎みあう本当の理由』. 東京: 洋泉社.

- 高原 基彰. (2010). 日韓中のナショナリズムと情報社会化によるその変動の比較考察 A Comparative Study of Nationalism in Japan, Korea, China and Their Transformation Under the Transition to Information Society 情報社会学会誌 Vol.5 No.2 原著論文
- 田辺俊介, (2016). 現代日本におけるナショナリズムと政治, 時点国際比較による実証研究, 国際化と政治参加に関する研究プロジェクト,
- 土屋大洋. (2012). 『サイバー・テロ日米 vs. 中国』. 東京: 文藝春秋.
- 辻大介. (2009). 「研究室からのメディア・レポート 調査データから探る「ネット右翼」の実態」. 『ジャーナリズム』 (226), 62-69.
- 樋口直人. (2012). 『日本のエスニック・ビジネス』. 京都: 世界思想社.
- _____. (2014). 『日本型排外主義: 在特会・外国人参政権・東アジア地政学』. 名古屋: 名古屋大学出版会.
- ミレット・ニコラ. (2014). 日韓関係に対してインターネットに表れた日本のナショナリズム. 広島大学 学術情報リポジトリ. 29 期巻
- 古谷経衡. (2013). 『 ネット右翼の逆襲-「嫌韓」思想と新保守論』. 総和社.
- 安田浩一. (2012). 『ネットと愛国: 在特会の「闇」を追いかけて』. 東京: 講談社.
- 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』. 90(35), 52-53.

- 곽희양 (Kwak, H.) (2013). “일베 현상에서 한국사회를 본다.” 『경향신문』(6 월 4 일).
- 김기덕 (Kim, K.) (2011). “미디어 콘텐츠 속 한 중·일 젊은 세대의 역사문화갈등과 대안모색.” 『통일인문학논총』 52, 143-179.
- 김응기 (Kim, W.) (2013). “혐한 시위를 통해 보는 제일 코리안: 카운터(counter) 활동을 중심으로.” 재외한인학회 연례학술대회 발표논문. 서울. 12 월.
- 김종길 (Kim, J.) (2005). “사이버공론장의 분화와 속의민주주의의 조건.” 『한국사회학』 39(2), 34-68.
- 김효진 (Kim, H.) (2011). “기호로서의 혐한과 혐중: 일본 네티우익과 내셔널리즘 (嗜好としての「嫌韓」と「嫌中」-日本のネット右翼とナショナリズム; Hate korea and hate china as taste: Net right and nationalism in contemporary japan)” 『일본학연구』 33, 31-56.
- 류석진 (Lew, S.) & 조희정 (Cho, H.) (2008). “온라인 공간의 민족주의적 갈등에 대한 연구.” 『사이버커뮤니케이션 학보』 25(4), 83-119.
- 박수옥 (Park, S.) (2009). “일본의 혐한류와 미디어내셔널리즘 (Media nationalism and Hate Korea wave in Japan: 2ch and the four daily newspapers in Japan).” 『한국언론정보학보』120-147
- 이지원 (Lee, C.) (2012). “인터넷 확산 시기의 한일 온라인 커뮤니케이션과 선순환적 교류의 조건 (Rethinking cross-border online communication: A case study of Korea-Japan)” 『한림일본학』 21, 121-153.
- 황성빈 (Hwang, S.) (2014). “네티우익과 반한류, 배외주의의 여론: 주요 언론의 담론 분석을 중심으로(Xenophobic Voices in Japan: A Case Study of Anti-Korean Demonstrations by Nettouyoku and Zaitokukai).” 『일본』, 124.
- Gallup Korea. <https://panel.gallup.co.kr>

※ 韓国語文献においては、ハングルの姓名とタイトルを基に、該当文献が英語または日本語にも記録された場合、併記した。

(注書き)

¹ Rheingold (1993) は、サイバー空間で利用者が継続的に議論して形成した人間関係網を「仮想コミュニティ」と定義した。すなわち、多くの伝統的なコミュニティは、近代化の過程で弱化・解体されたが、サイバー空間での交流を通じて従来のコミュニティに比肩されるほどのコミュニケーションができるサイバー・コミュニケーションの肯定的な可能性を重視した。

² 産業経済新聞. 2005年5月9日など.

³ <http://www.2ch.net> は西村博之という日本人が創設したといわれているが、現在、ドメインはシンガポールの PACKET MONSTER 社が、サーバーは米国の Pacific Internet Exchange (PIE) 社が管理している。

⁴ <http://www.nicovideo.jp>

⁵ <http://headlines.yahoo.co.jp/cm/list>

⁶ <http://www.ch-sakura.jp>

⁷ <http://petitions.whitehouse.gov>

⁸ <http://www.zaitokukai.info>

⁹ <http://www.chinesehonker.org>, <http://www.cnhonker.net>, <http://www.redhacker.org> などのグループが中国紅客連盟を名乗る。

¹⁰ <http://www.ilbe.com/>

¹¹ <http://cafe.naver.com/thecogall> 韓国の大手ポータルサービス NAVER の掲示板を利用している。

〈発表資料〉

題名	掲載誌・学会名等	発表年月
Cyber nationalism in Japan: the Net right and its impact on the society	the 72nd Annual Meeting of the Midwest Political Science Association	2014年4月
ネットワーク時代の外交と安保	ソウル：社会評論社 図書 (ISBN 978-89-6435-731-6)	2014年7月
Cyber Nationalism in East Asia and Trilateral Relations between Korea, Japan and China	the 13th Doctoral Students Conference for Association of Pacific Rim Universities	2014年8月
日韓サイバー空間での右翼の形成とこの影響に関する研究	第59回日本国際政治学会研究大会	2014年11月
日韓のサイバー空間での紛争とその対応	第39回情報通信学会大会	2015年6月
Cyber-attacks based on nationalism: Far-right groups in Japanese and Korean cyberspace	ITS LA conference 2015	2015年10月