サイバー戦争の法的概念を超えて

高橋郁夫†
†株式会社ＩＴリサーチ・アート　〒960-8021 福島県福島市霞町７番２１号
E-mail:　†ikuo@comit.jp,

あらまし　2009 年 7 月上旬の米国、韓国に対する大規模なサイバー攻撃は、「サイバーウォー」という言葉を彷彿とさせ、国家の背景があるとも報道されている。過去のエストニア、グルジアにおける攻撃などに対する分析などもあわせて、それらの攻撃が、国際的に法的にどのように認識されているのかについて詳細に検討するのが本稿の目的である。
キーワード　サイバー戦争、サイバーテロ、通信の秘密、官民連携

Legal Analysis of Cyber Warfare

Ikuo　Takahashi†
† KK IT research Art
E-mail:　† i kuo@comit.jp

Abstract D-Dos attack against Korea and US infrastructure in July,2009 remind the term" Cyber War". Some report said that there was the shadow of state behind those attacks. Analyzing past attacks against Estonia and Georgia, the goal is to make a review of attacks and defense from legal aspect and to make suggestions toward the new legal framework.

Keyword　Cyber　War,　Cyber　Terrorism, Secrecy of Communication,

1. 議論の意義

1.1. サイバー戦争をめぐる二つの見方

楽器音響機器の販売会社であるサウンドハウスという会社は、2008 年 3 月に、同社のサーバが攻撃を受けて、クレジットカード情報が流出した可能性があるという被害に直面した。ナリタシナィジャーナルという情報誌は、「サイバー戦争の幕開け」というタイトルととも

に、当該流出に対する対応の経緯を詳細に載せるともに、海外からの攻撃に備えることが、いま必要であるとして、その対応の重要性を声高に説いている。また、1998 年には、“Cybercrime, Cyberterrorism,　Cyberwarfare, Averting an Electronic Waterloo”という報告書がでており、これによって、これらの用語が、広く認められるようになったといわれている。現代においては、すでにサイバー戦争という状況に到達しているものとして、その意識を高めるべきであるという団体もある。サイバーテロリズムという用語もよく耳にするようになってきている。その一方で、サイバーテロリズムなどが存在したということはないという論者もいる。また、「サイバーテロによって電力網を掌握したりダムのゲートを開いたり、航空管制ネットワークを則って飛行機を衝突させたりというのは、おそろしい事態だが、非現実的だ。このようなことをリモートで行うのは、とても難しい。」ということもいわれている。客観的にサイバー戦争という問題をどのように認識し、どのように考えるべきかがサイバーセキュリティの重要なテーマであるということがいえるであろう。

私たちは、インターネットにおける攻撃として、ニュースその他で、サイバー戦争ではないかと世間をさわがしたものとして種々の攻撃をあげる（韓国・米国に対する攻撃、グルジアに対する攻撃、エストニアに対する攻撃）ことができる。私たちは、対応とその法的意義を考えるまえに、これらの攻撃（（１）韓国・米国に対する大規模な D-Dos 攻撃、（２）グルジアに対するサイバー攻撃、（３）エストニアに対するサイバー攻撃）について、まず、議論の開始として簡潔にまとめておくことは、有意義である。

1.2.　具体的な攻撃・防御の実態

サイバー戦争、サイバーテロリズムについては、それらの言葉が議論される実際の紛争について具体的に論じると以下のようになる。

1.2.1. 韓国・米国に対する大規模な D-Dos 攻撃

これは、2009 年７月上旬に、青瓦台、国会、国防省、与党ハンナラ党、朝鮮日報、新韓銀行、大手ポータルサイトのネイバーなど多数のサイトが、大規模な DOS 攻撃を受けたという事案である。また、同時に、米国のホワイトハウス、FTC や国務省などのサイトへの接続も一時、不能になった。攻撃のもとについては、北朝鮮が関与しているのではないかという報道も存在した。一方で、イギリスのサイトが利用されているという分析も存在している。

1.2.2. グルジアに対するサイバー攻撃

これは、2008 年８月に、グルジアからの分離独立を目指す南オセチア自治州をめぐる軍事活動と時を同じくして、グルジアのすべてのウェブサイトが接続困難になり、サイトが書き換えられ、不正な指令が拡散されたという事件である。この具体的な事情については、以下のとおりである。

政治的状況

南オセチアは、1991 年のグルジア・オセチア紛争の際に事実上独立していたが、国際的

には、グルジアの一部として認識されていた。現在でも、国連の多数は、領土的には、一部であると認識している。１９９１年のグルジア・オセチア紛争の後も、緊張関係が続き、１９９２年には、欧州安全保障機構（ＯＳＣＥ）のもと、平和維持軍（ロシア、グルジア、オセチアからなる）が組織された。しかしながら、グルジアとロシアの援助する分離主義者との間での緊張は、高まっていった。

グルジアのＩＴ化状況

グルジアにおいて１００名あたりのインターネットユーザは、７名（エストニアは５７）であり、諸国に対して、ＩＴの進行状況はむしろ遅れているということができる。もっとも、近時は、ブロードバング化の進展により着実に利用者が増加している。地理的に、グルジアは、トルコ、アルメニア、アゼルバイジャン、ロシアの「ランドルーター」を利用するという選択肢しかない。グルジアの国際への接続状況は、役半分程度にいたっているとのことである。具体的には、３０９のグルジアのプレフィックスは、トルコとアゼルバイジャン（ロシア経由）によってルーティングされている。グルジアと西ヨーロッパとのコネクションは、当時、設置目前であった。サービスプロバイダは、コーカサス・オンラインやコーカサス・ネットワーク・ツビリシが市場の９０パーセントを占めていた。

攻撃の開始と攻撃態様・影響

２００８年８月７日、分離主義者の挑発の後、グルジア軍は、分離主義軍に対して突然の攻撃を開始した。翌日は、ロシア軍は、「海外におけるロシア人の保護」の国家的義務について、言及し、グルジア軍に対して、最初は、南オセチアで、その後、平和維持強制）peacekeeping mandate)の範囲を超えて軍事作戦を開始した。ミヘイル・サーカシヴィリ・グルジア大統領は、８月９日、戦争状態にあると宣言した[1]。

ロシアのグルジアへの進行に先立って、８月８日、グルジアの政府サイトに対してサイバー攻撃が開始され、軍事攻撃自体は、８月１２日の停戦協定によって終了したものの、サイバー攻撃は、８月いっぱいにわたっておこなわれた。

サイバー攻撃の態様としては、公共機関のウェブサイトの書き換え、およびＤＤｏＳ攻撃、指令および悪意あるソフトウエアの配布などがある。また、グルジアの政治家の電子メールエドレスのリストの配布によりスパムや標的型攻撃などもおこなわれた。

グルジア・ユナイテッド・テレコムのルーターは、使えなくなり、数日間サービスを提供できなくなった。コーカサス・ネットワーク・ツビリシは、クエリーによって、あふれてしまった。物理的にルーティングの見直しを図ったが、コーカサス・ネットワークのインフラが、紛争中の場所を通っており、物理的に断絶したことも関係して、中小のインターネットプロバイダーには、逆効果になってしまった。

グルジア・ロシア紛争においては、重要な政府のウェブサイトにたいするＤｏＳおよび

---

[1] この点については、ＥＵの報告書が客観的な立場から報告されている。
「双方の「虚構」崩す　グルジア紛争報告書　宣伝合戦も再燃」
http://sankei.jp.msn.com/world/europe/091004/erp0910042310003-c.htm

ＤＤｏＳ攻撃とそれに対する対応がきわめて、重要な意義をもったものと考えられている。というのは、その時期において国際社会に対して情報を発信し、住民に対して情報を伝達する必要があり、それかできないとなると、国際社会からの支持をとりつけることができず、また、国民の士気にも影響しえたからである。また、エストニアにおける重要インフラに対する影響までにはいたらないものの、グルジア国立銀行は、電子取引の提供を１０日間、停止した。

防御対応

グルジアにおける攻撃対応は、グルジアＣＥＲＴによってコーディネイトされた。ＣＥＲＴグルジアは、高度教育機関のコンピューター・ネットワークサポートを提供しており、サイバー攻撃に対してナショナルＣＥＲＴの役割を果たしている。攻撃直後から、攻撃をさまたげようと一時的に、ＩＰアドレスを変更して、パケットをループバックさせるものや、ホスト自体を変更してしまうものもあった。また、グルジア通信委員会の命令によりグルジアからのロシアへのアクセスは、ブロックされた。また、グルジアの主要なサーバは、米国等を根拠とするサーバに一時的に物理的に移転することとなった。ポーランドＣＥＲＴは、ＩＰデータを分析し、フランスＣＥＲＴは、ログファイルの収集に協力した。また、エストニアＣＥＲＴの情報セキュリティ専門家が、グルジアを訪問し、ノウハウと経験を提供している。

攻撃者の正体

攻撃に際して、ロシア語のブログ、会議室、ウエブサイトが、グルジアのウエブサイトを攻撃するバッチスクリプト（war.bat というファイル名もあった）を配布し、また、どのようにして、ピン・フラッド攻撃をするかという指示を配布していた。また、ＳＱＬインジェクションに対して脆弱であるサイトの情報も広まっていた。この代表的なサイトが、stopgeorgia.ru（　stopgeorgia.info）である。また、この攻撃には、ロシアのＲＢＮも関与しているのではないかという認識が一般的になっているようである。

具体的な攻撃には、ボットネットが利用されている。これらのボットネットのコントローラーは、ロシアのハーダーによってよく使われている MachBot であった。

ロシアのハッカーコミュニティが、この攻撃に関与していたことは明らかであるが、政府関係機関が関与したという認定は困難であるとされている。

1.2.3. エストニアに対する攻撃

2007 年 4 月末にエストニアが、DOS 攻撃等の大規模サイバー攻撃を受け、同国のインターネット・インフラストラクチャの一部が麻痺したという事件があった。この事件を詳細に紹介すると以下のようになる。

政治的な文脈

2007 年 4 月 26 日、27 日、エストニアの首都タリンは、ロシア系住民のグループによる暴動に見舞われた。これは、ソビエト時代の第二次世界大戦の記念碑（ブロンズソルジャー）を撤去し、移転しようというエストニア政府の決定に反対する声に呼応するものであった。

エストニアでは、ソビエト時代の記念碑等は、取り除かれていたが、民族主義的な運動は、急進化し、エストニア国旗をもっている人が襲われたりという事件が起きたりするようになった。4 月 26 日、1000 人ほどの人間が記念碑の場所に集まり、撤去にたいして抗議をした。抗議は、後に暴動化し、100 名が負傷し、1 名が志望した。また、警察は、1300 名を逮捕した。この暴動による被害は、およそ４５０万ユーロと算定されている。政府は、予定より早く記念碑の撤去をなし、４月３０日に、移転した。

エストニアの情報化の進展

エストニアの人口は、１３０万人、人口の密集度も低かったので、社会自体が、情報化を進展させることで、公共サービスを充実させてきた。インターネットバンキングは、９８パーセントにいたっているし、また、モバイルパーキングは、５０パーセントを超えている。モバイル交通チケットも一般化してきている。また、行政の電子化もきわめて進展している。４５０以上の公共機関と３万以上の起業家が、“Ｘ－ｒｏａｄ”といわれているデータ交換レイヤーを利用している。８０パーセントの自然人の収入申告が、電子的に行われた。また、世界ではじめて電子投票を利用した国家でもある。

サイバー攻撃の時系列的記述

具体的な攻撃を時系列的に記述すると以下のようになる。

感情的対応（４月２７日から２９日）

４月 27 日の遅くには、政府のウェブサイトに対する最初の攻撃が、報告されている。この段階での攻撃は、単純なものであり「サイバー暴動」というべきものであった。ロシア語の掲示板などで、特定の引数をもちいた ping コマンドの利用が、指示されたりしていた。後に、自動的に ping コマンドを発射する方法が指示されていた。これらによって単純な D-Dos 攻撃がひきおこされたのである。

主たる攻撃（４月３０日から５月１８日）

４月３０日からは、大規模なボットネットの利用によって特徴づけられる主たる攻撃が開始した。より洗練され、協調されたものであり、インターネットのフォーラムによって指令や標的リストを伝えるという手法は維持されていた。エストニアにおける代表的な固定通信サービスの会社である Elion の DNS サーバとルーターは、一時的にサービス障害をきたすに至った。これらの攻撃は、間歇的に行われ、第１波（５月４日）、第２波（５月９日－１１日）、第３波（５月１５日）、第４波（５月１８日）にわけて行われた。特に５月９日（ロシアの戦勝記念日でもある）の攻撃は、熾烈で、５８ものサイトが遮断を余儀なくされた。政府機関や銀行などのサイトが、利用不能になったりした。

攻撃手法および攻撃目標

これらの攻撃手法としては、ＤｏＳおよびＤＤｏＳ攻撃、ウェブサイト改竄、ＤＮＳサーバ攻撃、大量のスパム通信などが見受けられた。また、攻撃目標としては、主として（1）エストニアのインターネット中枢に責任ある機構のサーバ（２）政府および政治的ターゲット（３）民間部門によって提供されるサービス（４）個人的・ランダムな目標などが、

目標になっている。

攻撃元

攻撃の元は、ほとんとがエストニアの外部からのものと判断されている。そして、急激な、予測つかないトラフィックが引き起こされたのが、エストニアのウェブサイトに公表されている情報に対して外国から興味をもったというわけではないことは明かである。攻撃のもとは種々の国に渡るが、主たるものは、インターネットのフォーラムやウェブサイト[2]の指示によって国家主義的・政治的感情によりいわば煽動された大衆であった。主攻撃の第２波は、通常の市民の抗議行動の域を超えていた。中央の指令・コントロールが効いており、波状攻撃は、定刻に行われ、金銭的・知的資源を有するものと分析されている。

防御方策

サイバー攻撃については、エストニアの CERT が、技術的に対応した。また、フィンランドのＣＥＲＴは、プロバイダーへの連携や国際的協調にたいして、重要な役割を果たした。また、国際的な連携については、エストニアの防衛省が援助をしている。米国やドイツを中心にして、自国の領域から発信されたり、その領域を通過するトラフィックを制限したりした。

刑事事件としての nashi

なお、この攻撃に関して、Konstantin　Goloskokov が、Reform　Party のホームページの改竄をしたということで起訴されている。彼は、クレムリンシンパのロシア系若者のグループである Nashi の人民委員（commissar）である。

社会的な影響

この攻撃は、直接、経済的な影響を及ぼし、社会的にも広範な影響を有した。社会的な影響というのは、エストニアにおいては、政府のウェブサイトが利用不能となり、公的な電子メールアドレスを偽ったスパムメールが著しく増加したので、通常の政府との通信が不可能になったのである。近時のｅ－ガバメント政策により、従来の通信手段は大幅に削減されており、市民は連絡に困難をきたすようになった。

---

[2] ４月２８日には、ロシアのサイト（http://2ch.ru や http://forum.web-dozor.ru）でエストニアに対する攻撃を呼びかける発言が確認されている。