【平成 29 年度航空研究センターシンポジウム】

航空研究センターは、平成 30 年３月 22 日（木）、「航空防衛戦略と先進技術の連携強化を目指して」と題して、公開シンポジウムを開催した。シンポジウムには、慶應義塾大学土屋教授、同じく山口准教授、国際地政学研究所上級研究員奥山氏の御参加を得て、先進技術について様々なテーマで意見交換を実施した。今回、各先生方の了解を得て、発表の内容を掲載することとした。

【平成 29 年度航空研究センターシンポジウム：発表 1】

サイバー

土屋　大洋

はじめに

皆さんこんにちは、慶應義塾大学の土屋です。本日はお招きくださりありがとうございます。私からはサイバーセキュリティを巡る話をしたいと思います。

1　サイバー戦の前触れとしての湾岸戦争

まず、1991 年の湾岸戦争のときの話を紹介したいと思います。1990 年、イラクが南隣にあるクェートに対して侵攻するということがありました。翌年の開戦の際に多国籍軍が組織されました。そのときに名を上げたのがノーマン・シュワルツコフ米中央軍司令官とコリン・パウエル統合参謀本部議長です。そして、隠れたプレイヤーが国家安全保障局（NSA）でした。NSA はアメリカ最大のインテリジェンス機関で、その時の長官はほとんど知られていませんが、ウィリアム・ステュードマンという人でした。彼は、湾岸戦争に際して、統合インテリジェンスセンターを組織しました。その中心人物が、マイク・マッコーネルでした。この人は、この時の功績が認められて、このすぐ後に NSA の長官に抜擢され、後のジョージ・W・ブッシュ政権の時には国家情報長官（DNI）に就任しました。湾岸戦争時、マッコーネルの分析官たちはイラクのサダム・フセイ

ンの指揮統制ネットワークに深く侵入しました。サイバーセキュリティは、2007 年のエストニアに対する分散型サービス拒否（DDoS）攻撃をその嚆矢（こうし）とするとされていますが、既に湾岸戦争時に米軍はサイバー攻撃で大きな作戦を行っていたのです。

イラクは首都バクダッドから南部のバスラにかけて光ケーブルのネットワークを敷設していました。イラク軍はこれを指揮統制用に使用していました。この光ファイバーの敷設の一部を西側諸国の通信事業者が手伝っていたため、米軍はこの通信事業者に連絡し、どこに光ファイバーが敷設されているのか、光ファイバーの接続点がどこにあるかを確認しました。

そして、開戦劈頭にその接続点への爆撃を行ったのです。その結果、イラクの指揮系統は混乱しました。当然のことながら、イラクはこの光ファイバーの使用をあきらめてマイクロウェーブ波、つまり無線通信で指揮を執ろうとしました。この動きは NSA も予測しており、このマイクロウェーブ波を人工衛星で傍受しました。その結果、サダム・フセインがどのように部隊を展開しようとしているのかが手に取るように分かりました。それで米軍は被害を最小限に抑えることができましたし、イラク側の被害はどんどん大きくなっていきました。やがて、サダム・フセイン側は無線が傍受されていることに気が付きました。そこでイラク軍はバイクによる伝令派遣により命令を伝達しようとしました。当然これはうまくいかず、イラク軍が敗れることになった一つの要因であったと言われています。この事例は対指揮制御戦争の最初のキャンペーンであり、将来のサイバー戦の前触れでした。

２　インターネットの普及と米国同時多発テロ

1991 年の湾岸戦争の 2 年後、1993 年頃に私はインターネットを使用し始めました。当時は、「モザイク」というブラウザを使用していました。これによってインターネットが一般に普及していきます。そして 1998 年にグーグルという会社が設立されました。皆さんが今でも使用している

グーグルという検索エンジンで有名な会社です。この会社を作った二人は大学院生だったのですが、技術を持っている人達でした。彼らは「世界中の情報を整理し、世界中の人がアクセスできるようにする」をモットーとしました。それは今のグーグルにも引き継がれています。彼らはこのモットーの下で検索エンジンを作成しました。グーグルの技術は、例えばグーグルマップやグーグルアースなどで、世界中の衛星写真を見ることができるようになるなど、安全保障にも大きな影響を与えるようになりました。

インターネットはこの後、急速に普及しましたが、サイバーセキュリティという面で大きなインパクトを与えたのが、2001 年 9 月 11 日に発生した米国同時多発テロ事件でした。この時私は丁度アメリカで生活をしていたのですが、報道を見ていて、テロリスト達がどうやってインターネットを使っていたのかということに興味を持ちました。彼らは航空券やホテルを予約する際にインターネットを使用しました。そして中東にいる仲間たちと連絡を取るのにも電子メールを使用していました。その時の電子メールが傍受されています。そこに書かれていたのは、「試合が始まろうとしている」「明日がゼロアワーだ」といったメッセージでした。これを NSA は傍受することができていました。アラビア語の平文だったので翻訳したのですが、それは 9.11 のテロの後だと言われています。しかし、テロ実施前に翻訳されていたとして、その内容からワールド・トレード・センターに飛行機で突っ込むということが分かったでしょうか。多分、分からなかっただろうと思います。

これをきっかけとして NSA が実施する傍受のやり方が変わります。つまり、傍受する対象がコンテンツからメタデータへと変化したのです。例えば、1 分間の電話を傍受したとして、その内容を解析するには 1 分間以上かかります。電子メールを開くことができたとしても、そこに記載されている内容が先ほど紹介したようなものであれば何を意味するのか分かりません。それよりも重要なのは、誰と誰がいつどれだけ連絡をしたのかということです。メタデータというのは、通話番号・通話時間・

IP アドレスその他の付帯する情報です。例えば、ある人が誰と電話しているのか、その人はテロリスト仲間なのか、それとも会社の同僚なのか、それが重要です。そこで交わされている内容は隠語が使われているかもしれないし暗号化されているのかもしれない。それよりも誰と誰が繋がっていて、ネットワークを形成しているのかが重要であると認識されるようになりました。もちろん、このような傍受はプライバシーの侵害に当たる恐れがあります。理由無くしてその人の通信を監視するということは難しいということです。しかし、9.11 後に NSA 長官になりサイバー軍の司令官を兼任するようになったキース・アレクサンダーはこう言ったそうです。「藁の中から一本の針を探し出すのは無理だ。それよりも藁全体を取り込んでしまえ。記録してしまえ。そしてそれにタグ付けをして保存しておけ」と。

３　サイバースペースの 3D（DEEP、DARK、DIRTY）化

（１）ダークウェブの存在

IoT（Internet of Things）とよく言われるように色々なデバイスがネットワークに繋がっていきます。そこに脆弱性も潜んでいます。その脆弱性を悪用しようという悪い人たちも増えているのが現状です。そしてソーシャルメディアもたくさん使われるようになってきています。そして、このソーシャルメディアのメッセージの中に悪いメッセージが隠されています。テロリストたちはソーシャルメディアを使って作戦を行うようになっています。その意味で私は 3D 化といっています。つまりインターネット、サイバースペースというものは深く（DEEP）なり、暗く（DARK）なり、汚く（DIRTY）なっているのです。どんどん私たちが知っていたようなインターネットではなくなってきているのです。

今メディアでよく使われるようになってきているのはダークウェブという言葉です。先ほど紹介したグーグルの二人は世界中の情報を整理し、我々が普通に使用できるようにすると言っていましたが、実態としては、氷山の海上に出ている部分、表層の部分しかグーグルは取り扱うことが

できません。この割合ですが、色々な統計データが出ていて、少ないものであれば全体の 4%、大きなものでも 40%となっています。つまり、世界中の大半のデータについて、グーグルは取り扱うことができないのです。この取り扱えない情報とは、自衛隊の中の情報や大学の中のネットワーク、あるいは企業のイントラネットの中のデータ等がそれに当たります。このような場所にはグーグルは入っていくことができない、つまり検索やアクセスすることができないのです。そしてこの一般人がアクセスできない領域、ディープウェブのさらに深いところ、つまりダークウェブでサイバー攻撃などが計画されているわけです。ここには悪の組織のショッピング・サイトがあり、例えば麻薬販売やサイバー攻撃の請負、果てには殺人の依頼まで受けています。そういうサイトがダークウェブの中に存在しています。

（2）アトリビューション（帰属性）の問題

そのような状況の中で、表側の世界の人間にとって問題となるのがアトリビューション（帰属性）の問題です。サイバー攻撃やサイバー犯罪を実際は誰が実行したのかということです。これを突き止めることができなければ我々はサイバー戦争に負けてしまいます。2012 年 10 月に米ニューヨーク・タイムズ紙が中国の温家宝首相が不正蓄財しているのではないかという記事を掲載しました。その直後からニューヨーク・タイムズに対してサイバー攻撃が行われました。ニューヨーク・タイムズは反撃を行います。「サイバー攻撃の発信源は上海にあるこのビルであり、そのビルの中には人民解放軍の 61398 部隊というのが入っている」と報道しました。アメリカは更に反撃を続け、2014 年 5 月にアメリカ司法長官が突然記者会見を開き、先ほど出てきた 61398 部隊所属の 5 人の中国人をサイバー犯罪の実行者と特定したと発表しました。一般にサイバー攻撃は誰がやったのかが分からないと言われていますが、本気になれば、ここまで分かるのだという一例を示したのです。

2014 年 11 月にはソニー・ピクチャーズがサイバー攻撃を受けました。従業員たちがある日、社内のパソコンを立ち上げるとパソコンが正常に

起動しなくなっていました。原因は、「インタビュー」という映画だと言われています。金正恩が見たら怒るだろうという内容です。この映画を作製したためにソニー・ピクチャーズが攻撃されたのだと言われました。すぐに米連邦捜査局（FBI）は北朝鮮がサイバー攻撃の主犯であると、アトリビューションを行ったのです。この時に出された声明をよく見ると、他の米国政府機関との密接な関係によりアトリビューションの特定を実施したとなっています。この文面は何を言っているのかを関係者に聞いたところ、米国政府機関とはNSAを指していると言われました。その時のNSAの長官は、マイク・ロジャース海軍大将でした。彼は、マルウェアが北朝鮮を離れ、カリフォルニアのソニー・ピクチャーズに至るまでの経路を全て把握していると言っています。

2016年の8月にはグシファー2.0というサイトが立ち上げられ、ここではヒラリー・クリントンのメールが暴露されました。同時にフェイクニュースが盛んにソーシャルメディアで発信されるようになりました。これはロシアが発信しているのではないかと言われました。フェイクニュースの拠点と言われているのが、サンクトペテルブルクのインターネット・リサーチ・エージェンシー（IRA）です。もちろん一つだけではありません。しかし、ここからソーシャルメディアにフェイクニュースを流し、2016年のアメリカ大統領選に干渉しようとしたのではないかと言われています。

2017年12月にロシアに行く機会があって、IRAを見に行きました。グーグルマップに出ている写真と同じような写真を撮ることができました。ただし、一箇所だけ違うところがありました。それは窓いっぱいの張り紙でした。通訳に聞いたところ、リース募集中ということでした。つまり、フェイクニュースのことが報道された後、逃げ出したのではないかとその時は思いました。帰国後、IRAはもう退去していると言ったところ、日本のテレビ局から連絡があり、あの張り紙はフェイクで現在もIRAはあの場所にいるということでした。つまり、あの張り紙もフェイクニュースだったのです。このIRAが選挙に介入してきたことは、ほ

ぼ真っ黒です。しかし、このIRAにロシアのプーチン大統領や、ロシア政府が命令を出したという証拠は現時点ではありません。この最後のパスが繋がらないため、アトリビューションが明確にできないのですが、アメリカ政府はほぼプーチン大統領が命令したと考え、ロシア政府を非難しています。バラック・オバマ大統領は、大統領選が始まる1年前から気付いていたといわれています。ただ、自分が介入することにより大統領選の結果が変わってしまうことを恐れて何も言わなかったと言われています。

しかし、アトリビューションはそれほど難しくはなくなってきているのかもしれません。2017年5月にはワナクライというマルウェアが世界中で猛威を振るいました。150カ国30万件もの被害が出たとの報道もありました。最初の報道では、犯人は北朝鮮であるということでしたが、あまりに攻撃のレベルが低いので、私は北朝鮮ではないのではないかと考えていました。しかし、日本政府も協力した結果、2017年12月にアメリカ政府は、攻撃が北朝鮮によって行われたと発表しました。

（3）クロス・ドメインの重要性とアメリカの対応

こうした報道があってから、アメリカもサイバー攻撃に対する対処の態度が変わってきました。つまり、それまではアメリカは、自身がサイバー攻撃を行っていると明確に言うことは無かったのです。それは「アメリカがサイバー攻撃をした」という発表が引き金となってアメリカに対するサイバー攻撃を誘発することを恐れていたからです。ところが、2016年3月にアシュトン・カーター国防長官は、アメリカがイスラム国に対してサイバー攻撃を行っていると講演会の中で表明しました。イスラム国のオペレーションを妨害する目的でサイバー攻撃を行ったということです。そして、トランプ大統領は、サイバー軍を戦略軍の隷下から統合軍の一つに格上げすると発表しました。そして2017年12月には北朝鮮に対するサイバー攻撃実施についても明言するようになって来ています。その最前線にいたのが太平洋軍司令官であるハリー・ハリス大将です。彼はクロス・ドメイン（多次元横断）ということを何度も言って

います。陸、海、空、宇宙、サイバースペースというドメイン（領域）を横断して戦闘が行われるということです。そしてアジア太平洋でクロス・ドメインがとても重要であり、喫緊の課題であると言っています。今日は航空自衛隊のイベントですが、彼が陸軍のイベントで言ったことを引用したいと思います。「陸軍が船を沈める、陸軍が宇宙の衛星を無力化する、陸軍が空軍のミサイルを打ち落とす、陸軍がサイバー軍の指揮統制を発揮する。こういったことがこれから起こる。陸軍は、それに対応するようにしなければならない。」これから、人工知能（AI）対 AI、ボット対ボットの戦いも始まるかもしれません。ボットとは、インターネットの中の用語でロボットを略したものです。

４　オリンピックとサイバー攻撃の脅威

我々の今の懸念は東京オリンピック・パラリンピックです。2012 年にオリンピックを開催したロンドンに行って聞いてみると、18 カ月前までには準備を終えていたそうです。逆算すれば、2019 年の 1 月までには準備を終える必要があります。もう 1 年を切っているのです。オリンピック開催時にサイバー攻撃を受けたとき、何が起こるのか色々懸念されています。ロンドンはどうやって凌いだのか。これまでも何度も出てきた NSA とイギリス側のカウンターパートである政府通信本部（GCHQ）がインテリジェンスを共有することにより乗り切ったと言われています。何故そのようなことをしたのでしょうか。それはアトリビューションと抑止です。ハッカーにとってお前がやったのだろうと名指しされるのはとても不名誉なことで、アトリビューション能力が向上することにより、サイバー攻撃を行う側はとてもやりにくくなります。深刻なケースにおいてアトリビューションができるのは国家だけだろうと言われています。

問題は、我々にカウンターパートがいるかどうかということです。NSA や GCHQ に対抗できるような能力を持った組織が日本にはあるのでしょうか。現状としてはありません。強いて言えば、自衛隊の情報本部がそれに当たるのかもしれませんし、自衛隊にもそのような能力があ

ればいいなと思います。これも憲法問題で、憲法の 21 条に通信の秘密が規定されていて、日本政府はこれを厳守してきました。時代が変わった中で、現行法制下で何ができるのか検討すべきでしょう。

東京オリンピックをどのように乗り越えていくのか。冬季オリンピックを開催した韓国の平昌が良い例ではないかと思います。平昌におけるサイバー攻撃はそれほど騒がれませんでした。しかし、開会式の最中にサーバーがダウンしたという事例がありました。このため、チケットが印刷できないという騒ぎになりました。当初、これは北朝鮮がやったのではないかと言われていましたが、北朝鮮はオリンピック期間中、非常に融和的な態度をとっていました。実はこうしたサイバー攻撃はロシアがやっていて、北朝鮮がやったように見せかけたのではないかと報道されています。どうしてこのような攻撃経路が分かるのか。それを監視する体制がアメリカにはあるからです。

このアメリカのシグナル・インテリジェンス（SIGINT）、サイバーシギント能力を中国は真似しようとしています。中国はデジタル・レーニン主義という言葉を使うようになってきています。もともとのレーニン主義は人民を監視することですが、そのデジタル版を中国で始めたということでデジタル毛沢東主義とは呼ばれていません。中国には 13 億もの人を解析するビッグデータ解析が必要になってきており、それを活用して統治を行おうとしています。

まとめ

まとめますと、デジタル通信技術による指揮統制や敵のネットワークを攻撃することの重要性が増してきています。そしてサイバー空間は 3D 化してきており、深くなって、暗くなって、汚くなってきています。これをどうするのかが課題です。これを解決する一つの要素としてアトリビューションというのがあります。先ほど幹部学校の 2 階で鈴木貫太郎元首相の「制空」という扁額（へんがく）を見ましたが、もちろん制空権は重要です。しかし、これからの時代においては「制脳権」が重要になると思います。

つまり脳の中身をどのように把握し相手の脳の中をどうコントロールしていくのか。こういうことが課題になる時代だと思います。