第７５８号

平成３０年７月１日

公益社団法人　安全保障懇話会
発行所　東京都新宿区若松町１８－３
電話　３２０２－８６３１　㈹

安全保障を考える

外交上の出来事に起因するサイバー攻撃の事例説明

サイバーディフェンス研究所 専務理事／上級分析官　名和利男

1. はじめに

報道等で伝えられている「サイバー脅威」は、テロ（政治的な目的を達成するために暴力及び破壊活動名時の手段の行使）の概念を含んだ「サイバー攻撃」と、犯罪（法によって禁じられている行為）の領域としての「サイバー犯罪」に分けることができる。安全保障、外交、危機管理の領域においては、このようなテロや犯罪の観点からサイバー脅威を解釈することが多い。

一方、IT（情報システム）の観点から眺めた「サイバー攻撃」は、”インターネットを通じて、サーバーやパソコンなどのコンピュータシステム対する破壊活動やデータを窃取、改ざんするなどの行為”であると認識されている。以前は、IT（情報システム）部門で対処、解決できる問題であった。

ところが、最近、多くの民間企業や公的団体は、コスト削減強化や生産性強化を目的としたIT（情報システム）やインターネットの利用の範囲を拡大している。最近では、基幹業務や重要データをアウトソーシングサービス（クラウドサービス等）で運用するケースが目立ち始めている。つまり、組織の業務がIT（情報システム）に大き

く依存するようになってきているため、「サイバー攻撃」は、組織内のすべての部門における問題となってきており、組織の上層部がリーダーシップをとることが強く求められてきている。

筆者は、このような状況に至るまでの背景及び要因として、次のような出来事の流れがあったと認識している。

① 先んじて規制緩和によって競争力をつけた外国企業が日本に進出或いは輸出攻勢を仕掛けてきたことにより、競争力のない国内企業が市場から追い出される。
② これに対抗するために、日本は国内の規制緩和や競争政策を促進、強化する。
③ 少子高齢化に伴い、労働力人口の減少及び労働者一人当たりの負担が増加している。
④ このような状況を打開するために、日本は国内産業が国際競争力を維持するために組織や業界の枠を超えたデータ利活用や情報通信技術を最大限に活用する推進政策である Society5.0 等を推進する。

本稿では、このような状況認識のもと、内閣法第 15 条で示されている危機管理（国民の生命、身体又は財産に重大な被害が生じ、又は生じるおそれがある緊急の事態への対処及び当該事態の発生の防止）の観点で、「サイバー攻撃」に対する対処に必要な状況認識の一助となる事例等を紹介する。

2. 緩やかなハッカー集団によるサイバー攻撃と対策

一般の社会生活の中で身近に感じるサイバー攻撃として、「インターネットを通じて特定の相手にサイバー攻撃を行う活動家（Activist）により緩やかに形成されたハッカー（Hacker）集団」（以下、Hacktivist／Hacker と Activist を組み合わせた造語）により同時多発的に行われるサイバー攻撃を紹介する。

まず、この Hacktivist が生まれた背景の一つに、インターネット利活用の浸透や SNS（ソーシャル・ネットワーキング・サービス）の発展による国や地域を超えた個人間の情報が容易になったことを理解していただきたい。次の図は、インターネットの黎明期からの変遷の中で、「攻撃側」と「サイバー脅威」の関係性に着眼した Hacktivists の特徴を示したものである。

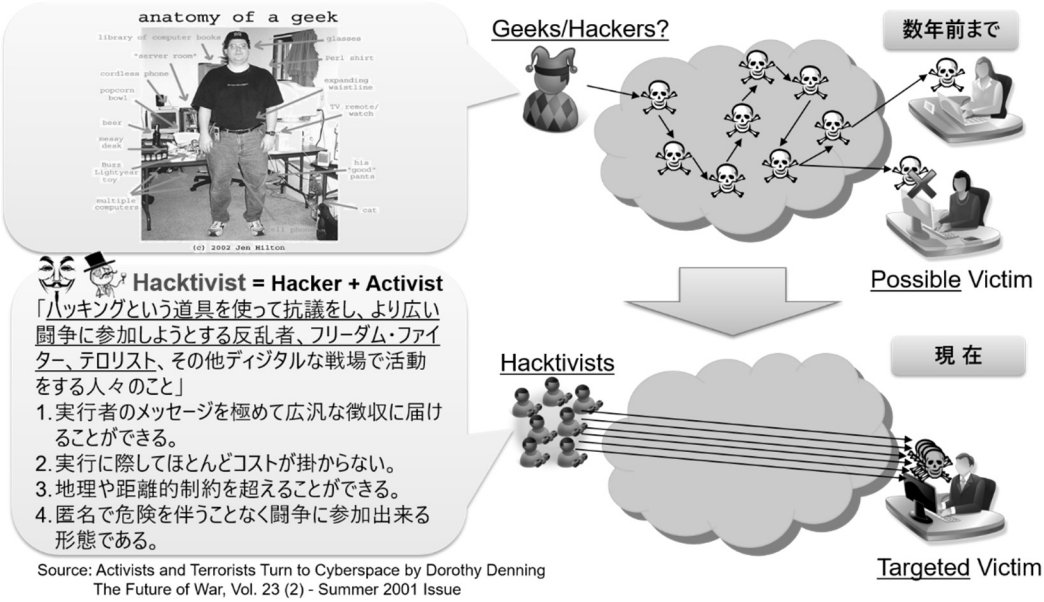


図 1　「攻撃側」と「サイバー脅威」の変化

インターネットの黎明期において、Hacker の一部に、Geek（オタク／コンピュータやインターネットについてマニアックな技術や知識を有する人）が存在していた。全体から見ると僅かであるが、自分自身で作成したコンピュータプログラムを多くの方々に「知ってもらいたい」という自己顕示欲や「使ってもらいたい」という自己承認欲が非常に強い者が、それらを強制的に実現しようと、コンピュータウィルスを作成してさまざまなコンピュータシステムにおいて、その脆弱性の悪用やユーザーの心理的な隙を突くなどの手段で動作させようとする行為をするようになってきた。

現象面では、生物学におけるウィルスの「感染」と酷似した挙動が見られるため、”コンピュータシステムへの感染”と表現されるようになった。また、僅かな者による行為であったため、そのコンピュータウィルスの数量が多かったとしても、その特徴や仕組みの種類数は限られていたため、生物学における「ワクチン」の概念と共通性のある「ウィルス対策ソフト」が開発されて積極的に利用されるようになった。「ワクチン」は、ウィルス等の病原体から製作して人体・動物体に接種することで体内にその病気に対する抗体を生じさせるものである。一方、「ウィルス対策ソフト」は、インターネット空間或いは感染したコンピュータシステムに残存するコンピュータウィルスを収集・抽出及び解析した上で、同種のものを検知・駆除する仕組みである。

インターネット黎明期から SNS が普及・浸透するまで、対処すべきコンピュータウィルスの多くは、現在のように高度で巧妙なものではなかったため、必然的にウィル

ス対策ソフトも、それほど高度なものではなかった。そのため、以前の「ウィルス対策ソフト」は、捜査機関における「指名手配」（一定の事件で逮捕状が発布されている被疑者の情報を公開し、国民全体から情報提供を受けることで被疑者の身柄確保を行うためのシステム）と類似したものであった。したがって、異なる種類のコンピュータウィルスが登場するたびに、それを検知・駆除するための「指名手配」を作成及び展開するというイタチごっこが長らく続いた。

ところが、スマートフォンの爆発的な普及やインターネット常時接続の低価格化により、インターネット上でコミュニティ形成が容易になり、個人の主張や行動が表面化しやすくなった。これにより、集団的な同調心理に流され、意識のあるなしに関係なく、一部の者により形成された特定の主義や信条に基づいた集団的活動の一時的な協調者になる者が急増した。そのような中で、昨今の貧富の格差拡大及び政府の不作為に対する不満等の高まりに関連すると見られる、特定の領域に対するサイバー攻撃が相次いで発生するようになった。このようなサイバー攻撃を仕掛けている者の中で、インターネット上で観察できている者が、前述した「Hacktivist」である。

ここで注目すべきことして、「Hacktivist」は、特定の主義や信条に基づいているため、その行動の目的を達成しようとする傾向にあることである。以前のようなコンピュータウィルスをインターネット上にばら撒くことはせず、SNS 等を駆使しながら仲間を集め、攻撃対象に何かしらの被害を発生させるための準備を秘密裏に行うことが多い。したがって、すでに対策済みであるために被害の発生が期待できない「インターネット上に広くばら撒かれたコンピュータウィルス」の利用は考えにくい。攻撃対象に対して大きな被害を多く発生させることが期待できるマルウェア（悪意のあるソフトウェア）、不正アクセス、DDoS（サービス拒否）攻撃、Doxing（組織内部の個人情報や重要と認識される内部資料の暴露）等を仕掛ける傾向がある。

このような「攻撃側」と「サイバー脅威」の変化の中で、以前までの「ウィルス対策ソフト」の有効性は低下した。これに関連して、2014 年 5 月、ウィルス対策ソフトの開発提供会社として有名な米シマンテック社の上級副社長のブライアン・ダイ氏が、Wall Street Journal 紙において、「（従来型の）ウィルス対策ソフトは死んだ」と発言[1] している。現在、諸外国において、ますます高度化及び巧妙化するマルウェアに対する

---

[1] Symantec CEO says antivirus is dead.
https://www.symantec.com/connect/forums/symantec-ceo-says-antivirus-dead

検知技術が多額な予算をもって研究開発されている。しかしながら、日本ではこの領域における予算は低調気味であるため、かなりの遅れをとっている。

Hacktivist の例として、日本に関係性のある「Anonymous」と「中国紅客連盟」を紹介する

(Anonymous)

「Anonymous」とは、創設者の中核的なメンバの活動や思想に協調するネットユーザー（特に技術者）が、インターネット上で緩やかなコミュニティとして連帯した集団である。

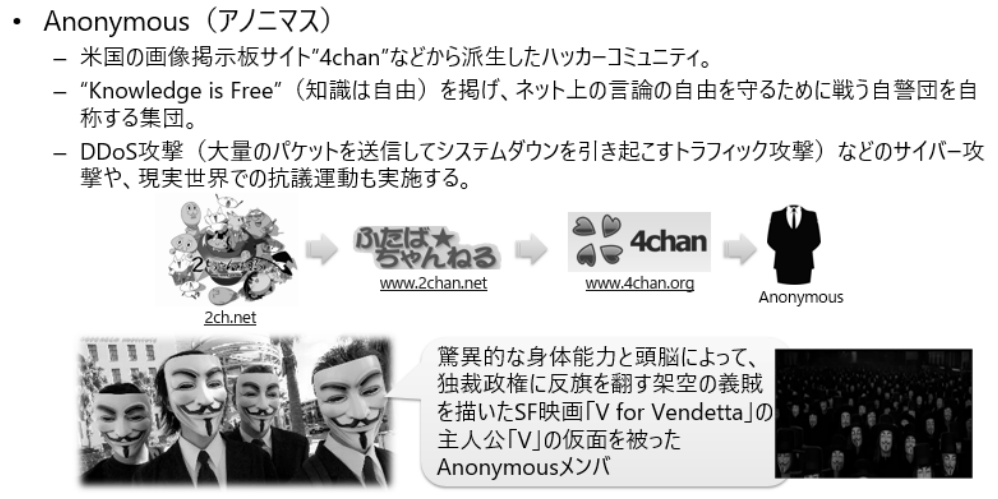


図 2　多国間で形成される Anonymous

攻撃活動の多くは、SNS でよく利用されるハッシュタグ（#）で、攻撃活動を意味する Operation の略称 Op を接頭辞として、標的を象徴するような文字列で示すような攻撃キャンペーンを仕掛けることである。例えば、次の図のように、2012 年 1 月、違法ダウンロードの温床となっていたとして、米国司法省と FBI により閉鎖された MegaUpload に関連した攻撃キャンペーンが有名である。

Anonymous A: *"Why can't I get my files from MegaUpload anymore?"*
「なぜ、私のファイルが MegaUpload から入手できなくなってしまったんだ?」
Anonymous B: *"Dude, have you had your head in the CLOUD. Don't you know the feds took down the site?"*
「おお、おまえはぼんやりしていたんだな。政府がそのサイトを断ち下げたことを知らないのか?」
Anonymous A: *"Man,*&%$ that! #OpMegaUpload! See how the feds like their own medicine.*
「畜生、#OpMegaUploadだ! 政府に当然の報いを与えよう。」

図 3　#OpMegaUpload が発案されたやり取り

構成員の全てが攻撃技術を持っているとは限らないため、簡単なツールや攻撃請負サービスを利用したDDoS攻撃を仕掛けることが多い。

派生経緯は、米国の画像掲示板サイトである「4chan」から派生したハッカーコミュニティであるとされている。これは、名前を入れずに投稿すると、その名前が自動的にAnonymousに置き換えられて表示されることに起因している。そして、その「4chan」は、閉鎖騒動となった「2ちゃんねる」の避難先として2001年8月に設立された「ふたば☆ちゃんねる」の非公式姉妹サイトになることを目的に2003年10月に設立[2]されたものである。そのため、Anonymousによる集団的行動の一部には、日本の「2ちゃんねる」で発展した文化や特性が見られている。

（中国紅客連盟）

「中国紅客連盟」とは、中国大陸に存在するHacktivistであり、世界最大のハッカー集団であるとされている。

この言葉の「紅客」は、1999年5月、米軍がユーゴスラビアの在ベオグラード中国大使館に対する誤爆事案に対して、反発心を高めたネットユーザーが名乗り始めた造語である。”紅”は、中国共産党の色であり、中国政府を援護する意味が込められている。そのため、最も活動が本格化したのは、2000年1月、大阪で開催された南京大虐殺を否定する集会に起因する「中央省庁Webサイト集中改ざん事件」、2001年4月、米国及び中国の軍用機が空中衝突した事件に起因した「米国の主要組織に対する大規模なサイバー攻撃」であるが、その過程の中で「紅客」が相互に連携し始めて、「米客連盟」を形成していった。

---

[2] ようこそ、4chanへ！
http://www.4chan.org/japanese

中国红客联盟（中国）

- 英語名
  - **H**onke **U**nion of **C**hina
- 設立日
  - 2000年12月31日
- 中核メンバ
  - **lion** ： 連盟の創設者で Web マスター、ネットワークセキュリティを担当
  - **bkbll**： 連盟の総務を担当
  - **yaya**： 連盟の会計兼人事のネットワーク管理を担当
  - **Redfreedom**： 米国に対するサイバー攻撃、非常勤の技術責任者を担当
  - **NikNanA**： 連盟の運用及びネットワーク管理担当
- 登録者数
  - ピーク時は8万人（**約65%は大学生**）
- 概要
  1. 1998年 3月 インドネシアに対するサイバー攻撃
  2. 1999年 3月 米国に対するサイバー攻撃
  3. 1999年 8月 台湾に対するサイバー攻撃
  4. 2000年 1月~2月 日本に対するサイバー攻撃
  5. 2001年 4月 米国に対するサイバー攻撃
  6. 2004年12月 解散
  7. 2005年 4月 再編
  8. 2005年 日本に対するサイバー攻撃
  9. 2010年 8月 フィリピンに対するサイバー攻撃
  10. 2010年 9月 日本に対するサイバー攻撃

- **黒客**（ヘイカー）／**駭客**（ハイカー）→「ハッカー」
- **紅客**（ホンカー）→「**愛国的なハッカー**」
- （稀に）**博客**（ポーカー）→「ブロガー」

http://www.cnhonkerarmy.com/

彼らは、特に米国や日本に対するサイバー攻撃を愛国心やナショナリズを発揮する形態の一つとして捉えた。

3. 日本が巻き込まれそうだったサイバー攻撃「OpNuke」

数多く発生する Anonymous によるサイバー攻撃の中で、執筆時点において、日本が巻き込まれそうだった OpNuke の攻撃キャンペーンを紹介する。

2018 年 2 月 22 日、ブログや SNS など複数の Web サイトで Anonymous を名乗る者が「OpNuke」の開始を宣言[3] した。

この宣言は、世界で核戦争や大量破壊兵器を製造する準備が行われていると主張しつつ、大量壊兵器の製造者とみなした核物質関連施設や原子力発電所などを標的として、サイト改ざん、内部情報流出、DDoS 攻撃を仕掛けると予告したものである。この標的リストの中に、日本の関連施設も入っていた。しかし、宣言や標的リストの多くは、以前より頻繁に行われている「OpGreenRight」という、環境問題を訴えた地球の緑を守ると主張する攻撃キャンペーンと類似しているところが多い。

---

3 https://www.cyberguerrilla.org/blog/international-call-for-anti-nuclear-operation-opnuke/

図 4　「OpNuke」開始宣言を謳ったサイトに表示されたロゴ

[ENG VERSION]
Hello citizens of the world, we are anonymous,
In a world where violence, abuses, exploitation and anything else are in the agenda. That's what you missed and to be forgotten by ways: Governments destroy us and enviroment with weapons of mass destruction, like nuclear plants and nuclear weapons.

Lately between the United States and North Korea, there have been heated quarrels, that could lead to serious consequences. It was to kill two birds with one stone and to spread fear in the world. This period increased sales of heavy weapons. Also that is uncontrolled period that can cause mass destruction of world. One step that excee the limit can cause the trouble of people. This is madness in our point of view. We think we have to show our stance against this madness.

We have right to protest this madness and disgusting destruction policy on our life and world. We are not just against nuclear weapons and nuclear plants. We are against mass destruction of our life and world. All green lands and every group what are oppose this period are under attack. Everybody is free to fight for the world, it's life and for all people, animal life. We are convinced that unity is strength.

You are welcome anybody excluded, you can inform us of any success that is of type: Defacement , Leaks, Denial Of Service ,Or other, through our pages or twitter channels. Good work and thanks for the help!
[ITA VERSION]
Salve cittadini noi siamo anonymous , In un mondo dove la violenza , soprusi , e quant'altro sono al ordine del giorno, manca solo che i nostri governi ci distruggano con armi di distruzione di massa , come le armi nucleari. Ultimamente tra gli Stati Uniti e la Korea del Nord , si sono verificati diverbi scottanti , che potrebbero portare a serie conseguenze , semplicemente per la pazzia che nutrono questi avversari. E' nostro diritto dunque , protestare e batterci contro questo schifo , non solo per queste questioni, ma perchè , le centrali nucleare sono un pericolo per l'intero mondo. Oguno è libero di battersi per la propria nazione o per quella altrui se ne avete voglia , siamo convinti che l'unione fà la forza. Siete tutti i benvenuti nessuno escluso , potete informarci di eventuali successi che sia di tipo : Defaceing , Leaks , Denial Of Service o altro, tramite le nostre

pagine twitter o canali. Buon Lavoro e grazie per l'aiuto !
More Info on Nuclear : https://ghostbin.com/paste/ec652
****
Join Us :
webchat.cyberguerrilla.org
irc,cyberguerrilla.org/6697
6dvj6v5imhny3anf.onion/6697
#OpNuke
www.cyberguerrilla.org/blog/
https://twitter.com/C_G_A_Nexus
cyberguerrilla@riseup.net
www.antisec-ita.blogspot.com
https://twitter.com/AntiSec_Italy
antisecitaly@mail2tor.com
****
– First target list :
https://en.wikipedia.org/wiki/List_of_nuclear_power_stations
– Second target list :
https://ghostbin.com/paste/n3p2d
We Are Anonymous
We Are People
We Are An Idea
Join & Expect Us.
More Shit Coming Up Stay Tuned.

図 5 「OpNuke」開始宣言を謳ったサイトに掲載されたメッセージ

「OpNuke」のメッセージにおいて第 1 標的リスト（First target list）及び第 2 標的リスト(Second target list)として日本の関連組織が多数掲載されているが、いずれも、Wikipedia に掲載されているものや過去の同様な攻撃キャンペーンで示された標的リストを使い回している印象がある。しかし、このような攻撃キャンペーンを初めて知り、賛同或いは協調する者にとっては、この標的リストに真剣に向き合うことがあるため、このメッセージ内で示されている攻撃手段であるサイト改ざん(Defacement)、内部情報流出（Leaks)、DDoS 攻撃（Denial Of Service）に対する警戒をする必要がある。

これまでの Anonymous による攻撃キャンペーンは数多く発生しているが、その大半において「賛同或いは協調する者が十分に集まらない」或いは「深刻な被害を発生させるサイバー攻撃を仕掛ける能力を有する者が参画しない」ためにサイバー攻撃そのものが発生しないケースがほとんどである。一部において、「サイバー攻撃を仕掛けたとしても小規模の Web サイトに対する短時間の DDoS 攻撃の発生」に留まる、或いは「流出済みの内部情報や個人情報を改めて拡散する」という限定的なサイバー攻撃になる。稀にではあるが、特定領域の複数組織に対する大規模なサイバー攻撃が発

生し、その一部で深刻な被害が出るケースがあり、規模が甚大であるがゆえに SNS 等のネット上のコミュニティで騒がれ、深刻な被害がネットユーザー等に影響を与えるがゆえにメディア等で報道される。

今回の「OpNuke」は、結果として SNS やメディアが注目するようなサイバー攻撃の発生は見当たらなかったため、ネットワークセキュリティを専門にする技術者の多くは、関心対象としていなかったようである。しかし、この「OpNuke」の開始宣言に至るまで経緯を観察すると、今後の外交・安全保障から派生するサイバー攻撃の予見性を向上するために役立つ観点を得ることができた。

以下、「OpNuke」の開始宣言に大きな影響を与えたえ出来事をまとめると、次の図のとおりになる。

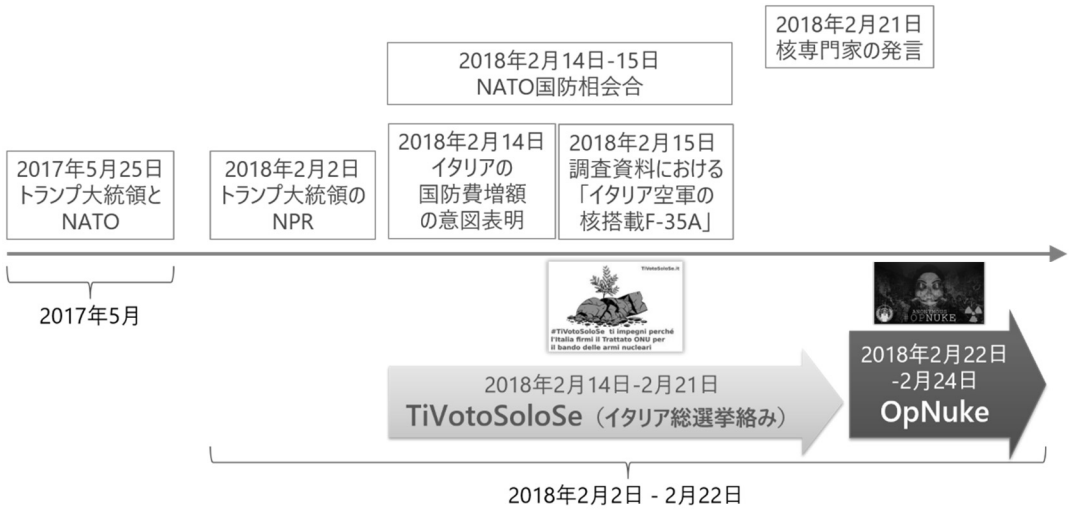


図 6　「OpNuke」の開始宣言に至るまでの出来事

（2017 年 5 月 25 日 トランプ大統領が NATO 加盟国に国防費増を要求）

2017 年 5 月 25 日、NATO 首脳会談において、米国トランプ大統領が、すべての NATO 加盟国に応分の財政負担として、国防費を国内総生産（GDP）比 2%に増やすことを求めた。この背景には、NATO 加盟国の国防予算合計のうち、米国が 70%以上を占めており、米国は GDP 比 3.5%以上の国防予算が支出している一方、ギリシャ、エストニア、英国、ルーマニア、ポーランドの 5 か国以外の NATO 加盟国は GDP 比 2%以下である。また、NATO 加盟国には、2014 年までに GDP 比 2%の国防予算の目標基準を達成するとした合意が取り交わされている。

これにより、米国から「核共有（Nuclear Sharing)」を受けている 4 か国（ドイツ、

イタリア、ベルギー、オランダ）は、いずれも国防予算の目標基準を達成していないため、米国との関係悪化に懸念を示した。この「核共有」とは、NATO において独自の核装備を持たない加盟国が核抑止力を持つために、米国から核兵器を借り受ける形で自国内に戦術核を配備している。平時は米国が管理をしているが、非常事態時に迅速に迎撃する態勢になっている。

（2018 年 2 月 2 日　トランプ大統領の核戦略指針 NPR）

2018 年 2 月 2 日、米国トランプ大統領は、新たな核戦略指針「Nuclear Posture Review[4]（NPR)」を発表した。ロシア、中国、北朝鮮が核兵器増強を進める現状に対応して、爆発力を小さくし、機動性を高めた新型核兵器の導入を明記し、破壊力の強い通常兵器（非核兵器）や大規模サイバー攻撃等に対する核兵器による報復の可能性についても言及した。前政権（オバマ大統領）の「核なき世界を目指す」から「今よりも使いやすい核兵器を持つ」方針に転換し、核兵器の役割を広げた。軍事的な抑止力を高める戦略である。

この方針転換に対して、米国科学者連盟の核情報プロジェクトのディレクター、ハンス・クリステンセン氏は「トランプ大統領に米国の核能力に関するブリーフィングが必要なのは明らかだ」と異議を唱えている。

（2018 年 2 月 14 日-15 日 NATO 国防相会合）

2018 年 2 月 14 日及び 15 日、ベルギー・ブリュッセルで NATO 加盟国による国防相会合が開催された。主に NATO 核計画、軍事費の負担、新司令部の創設などが議論された。この中で、NATO 内の委員会である核計画グループ（Nuclear Planning Group）会合も開催され、核兵器の配備、安全性・セキュリティ・残存性、関連する通信・情報システムなど、核兵器に係る政策と管理について議論がされた。

特に、イタリアのピノッティ国防相は、2024 年までに米国の（NATO 加盟各国における GDP 比国防費）2%の要求に応じる意思を持っていることを確認した。

---

4 https://www.clingendael.org/sites/default/files/2018-02/PB_Trump%27s_Nuclear_Posture_Review.pdf

（2018 年 2 月 14 日 イタリア総選挙に絡んだ国連核兵器禁止条約の批准運動）

NATO 国防相会合におけるイタリアのピノッティ国防相の発言に対して、イタリア国内において、3 月 4 日のイタリア総選挙に絡めた強い反発が相次いで発生した。

2017 年 7 月 7 日、国連において法的拘束力を持つ核軍縮関連の条約として「核兵器禁止条約」が採択されたが、米国から核共有を受けているイタリアは、これに批准していない。そこで、イタリア総選挙に絡めた形で、イタリア政府に「核兵器禁止条約」への批准を強く求めるために、「#TiVotoSoloSe」（You vote only if : あなたが投票してくれたら）というキャンペーンを開始[5] して、www.tivotosolose.it に「核兵器禁止条約」への批准を約束する候補者の名前を公表した。このような批准運動が始まったところに、NATO 国防相会合でのピノッティ国防相の発言が、ネット上で大きく取り上げられた。

図 7　TiVotoSoloSe キャンペーン活動の様子

（2018 年 2 月 15 日 核脅威イニシャティブの調査レポート）

2018 年 2 月 15 日、核脅威イニシャティブ（Nuclear Threat Initiative）が、NATO の核配備に関する調査レポート「Building a Safe, Secure, and Credible NATO Nuclear Posture」を公表[6] した。

核脅威イニシャティブ（Nuclear Threat Initiative：以下、NTI）とは、2001 年に設立された米国の非営利団体で、核、生物、放射線、化学、サイバーの領域における大量破壊兵器による致命的な攻撃や事故を防ぐために活動している。

---

[5] http://www.iltorinese.it/tivotosolose/

[6] https://www.nti.org/media/documents/NTI_NATO_RPT_Web.pdf

今回、公表された調査レポートの中で、次のようにイタリアの状況が示されている。

F-35A のデュアル対応の役割の可能性について、イタリアの国民或いは行政機関において議論されていない。現在航空機に承認されている予算には指定されていない。現在、戦闘機に対して承認されている予算は、核ミッションに適用させるために割当予算を明示していない。おそらく、ミッションにおける核の役割及びコストに関する議会の議論により、反対派が多くなるだろう

図 8 NTI の「NATO の核配備に関する調査レポート」におけるイタリアの状況

（2018 年 2 月 21 日 核専門家の発言）

2018 年 2 月 21 日、トランプ大統領の核戦略指針に対して異議を唱えた、（上述の）米国科学者連盟の核情報プロジェクトのディレクター、ハンス・クリステンセン氏が、Twitter で、「もしイタリアが防衛費の負担を改善したいのであれば、核共有を段階的に止め、戦闘機の無意味な核武装を解除し、NATO が現に利用できる通常兵器による作戦に集中すべきである」と主張[7] した。

図 9　核専門家の発言

以上のように、「OpNuke」開始宣言に至るまでには、外交・安全保障の領域における一連の出来事が積み重なったことが一因として考えられるが、イタリア国民の目線

[7] https://twitter.com/nukestrat/status/966448586132262912

から眺めると、地域特有の歴史的経緯やその時々の社会的要因に加えて、昨今の SNS の浸透による個人間の情報流通が活性化している状況が大きく影響していることが見える。また、それぞれの出来事を子細に観察していくと、必然的な結果として出現した「サイバー空間を利用した抗議活動」であると見なすこともできる。

筆者は、このような観察及びレビューは、今後のサイバー攻撃の発生見積もるために実施される OSINT（オープンソースインテリジェンス）活動に役立つものであると考えている。

4. 北朝鮮によるサイバー脅威

ここ数年、欧米各国のサイバー脅威インテリジェンスを専門とする機関が、相次いで、北朝鮮によるサイバー脅威に関するレポートを公表している。いずれのレポートも、北朝鮮のハッキング能力が高いレベルにあると評価している。

特に、2016 年 9 月、韓国軍の国防統合データセンター（DIDC）が、北朝鮮と推定されるサイバー攻撃を受け、北朝鮮首脳部の斬首作戦である「作戦計画 5015」や米軍が韓国軍に提供した北朝鮮監視資料など総ファイルサイズにして 235GB 程の軍事機密情報が流出した。このほかにも、北朝鮮と断定或いは強く推定されているサイバー攻撃は、2017 年だけでも、約 89 億円が盗み出されたバングラディッシュ中央銀行に対するサイバー攻撃や世界各国で大規模な被害を与えた WannaCry（ネットワーク経由で侵入・拡散する身代金要求型マルウェア）がある。

このような北朝鮮は、他国の情報を破壊できるサイバー能力を持つ 7 か国の一つとして認識[8] されている。7 か国とは、北朝鮮、米国、ロシア、中国、英国、イラン、フランスのことである。

以下、信頼できる機関から公表されている資料の中から、北朝鮮によるサイバー攻撃能力に関する情報を集約したものを紹介する。

（北朝鮮のプログラミング能力）

北朝鮮は、全国の若い才能を平壌〈ピョンヤン〉の金星 1・2 中学校（中・高等学校）

---

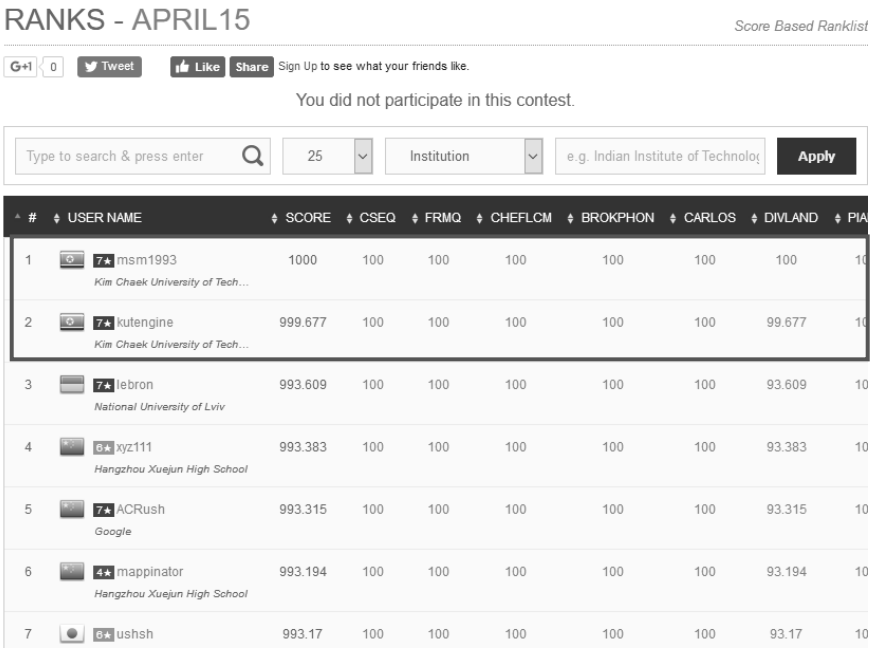
8 https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military

コンピュータ「英才班」に集め、専門ハッカーとして養成し、最優秀成績で卒業する学生には金日成（キム・イルソン）総合大学、金策工業総合大学進学とともに、親を平壌（ピョンヤン）に住むようにするという特恵を与えている。成績優秀者には、外国留学の機会を提供するなど、北朝鮮内の最上流層に近い扱いを提供している。

これらの大学には「情報科学小組」（サークルに相当）が設置されている。これは、北朝鮮の最高英才教育機関である平壌第 1 高等中学校を卒業して金日成総合大学に入学した英才らと「国際数学オリンピック」に出場し、優秀な成績を収めた学生で構成されている。「情報科学小組」の指導教官には、若く有能な教授がつき、国際的なプログラミングコンテストに出場するための準備に集中する。この準備は、非常に集中的に行われ、「情報科学小組」の学生（以下、小組生）は、過去の既出問題を中心に膨大な学習量をこなしていく。10 人前後で構成された小組生は、毎日試験を受けるため、徹夜の勉強を日常茶飯事のようにする。このような集中度の高いプロセスに耐えられない、或いは創造的思考能力が低い学生は外される。そして、指導教官は、大学内の党委員会議に、「情報科学小組」の運営状況を随時報告し、必要な支援を受けることになる。

北朝鮮の大学は、午前 8 時から授業を始め、午前に 90 分ずつ 3 時間目まで行われ、午後には講義がない。一般の学生は、午後に自習、労力動員、行事などに動員されるが、小組生は、午前の授業後に一切の動員や行事で免除される特別恩恵を受け、ひたすらプログラミングコンテストへの出場準備に集中する。そして、コンテストへの参加が確定した小組生は、すぐに講義から外され、専門訓練に入る。その期間に講義を受けなくても、大学は単位を保証するため、学年進級に問題はない。

2015 年 4 月、インドで開催される世界的なインターネットプログラムコンテストである「コードシェフ（Code Chef）」において、北朝鮮の金日成総合大学の学生が 1 位を獲得した。「コードシェフ」は、240 時間以内に提示された 10 個の問題を解いた結果の精度を評価して勝負を競う大会であり、世界のプログラマー大会と教育、イベントを主催する世界的なプログラムのコミュニティである。金日成総合大学の学生は、2013 年からこの大会に参加し、複数回 1 位を獲得し、2013 年 9 月には、「コーディング皇帝」という名声を持つ米国のグーグルチームを下し、注目を集めた。理科大学、金策工業総合大学の学生もこの大会で 1 位になった。


RANKS - APRIL15

Score Based Ranklist

Sign Up to see what your friends like.

You did not participate in this contest.

Type to search & press enter | 25 | Institution | e.g. Indian Institute of Technolo | Apply

#	USER NAME	SCORE	CSEQ	FRMQ	CHEFLCM	BROKPHON	CARLOS	DIVLAND	PIA
1	msm1993 Kim Chaek University of Tech...	1000	100	100	100	100	100	100	10
2	kutengine Kim Chaek University of Tech...	999.677	100	100	100	100	100	99.677	10
3	lebron National University of Lviv	993.609	100	100	100	100	100	93.609	10
4	xyz111 Hangzhou Xuejun High School	993.383	100	100	100	100	100	93.383	10
5	ACRush Google	993.315	100	100	100	100	100	93.315	10
6	mappinator Hangzhou Xuejun High School	993.194	100	100	100	100	100	93.194	10
7	ushsh	993.17	100	100	100	100	100	93.17	10

図 10　Code Chef（2015 年 4 月開催）の結果ランキング

2016 年 5 月、ACM 国際大学対抗プログラミングコンテスト（ACM-ICPC）において、北朝鮮の金日成総合大学（Kim Il Sung University）及び韓国 KAIST（科学技術院）が 28 位を獲得した。このコンテストは、毎年、全世界の大学生が参加し実力を競う国際コンピュータープログラミング大会で、IBM が 1977 年から後援しており、大会本部は米国ベイラー大学に置かれている。2016 年の上位大学は、1 位：サンクトペテルブルク大学（ロシア）、2 位：上海交通大学（中国）、3 位：ハーバード大学（米国）である。

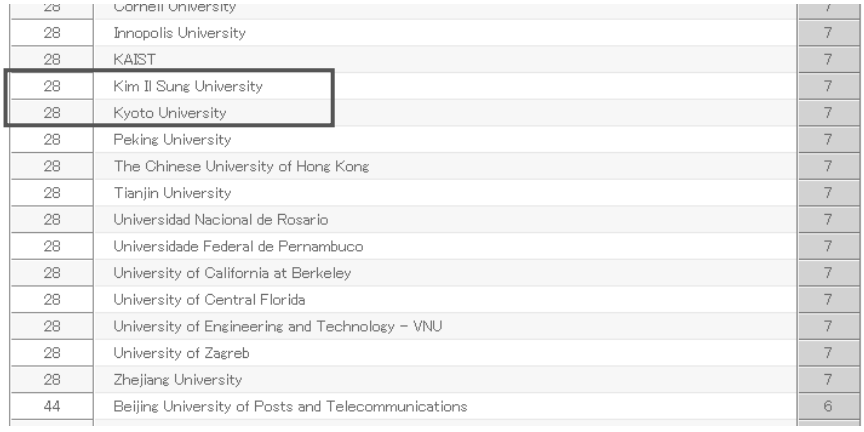

28	Cornell University
28	Innopolis University
28	KAIST
28	Kim Il Sung University
28	Kyoto University
28	Peking University
28	The Chinese University of Hong Kong
28	Tianjin University
28	Universidad Nacional de Rosario
28	Universidade Federal de Pernambuco
28	University of California at Berkeley
28	University of Central Florida
28	University of Engineering and Technology - VNU
28	University of Zagreb
28	Zhejiang University
44	Beijing University of Posts and Telecommunications

図 11　ACM-ICPC（2016 年 5 月開催）の結果ランキング

（北朝鮮のハッカー人材のキャリア）

上述の優秀な学生の多くは、総参謀部傘下の指揮自動化大学（旧・美林〈ミリム〉大学）や金策工科大学等に進学して高度な教育を受けた後、最終的に選抜された者のみが偵察総局傘下の「電子偵察局」（121 局）に配属され、ハッキングやマルウェアの拡散などの任務を遂行する。

「電子偵察局」（121 局）は、1998 年、121 小隊で始まり、2012 年、総参謀部と対外連絡部が加わり、121 局に昇格した。当初、500 人でスタートしたが、2009 年、金正日国防委員長が、ハッカー人材を拡大せよとの指示により、3000 人水準までに増加した。2015 年に 5900 人、2017 年に 8000 人規模になった。原子力発電所、金融、管制塔、通信などの国の重要施設に応じて特別な目的のハッキングの専門家を養成している。ハッキング攻撃と防御の技術を兼ね備えている米国、ロシア、中国とは異なり、攻撃に重点を置いている。しかし、北朝鮮にはハッキングを通じて失う施設が非常に少ない、サイバー防御力は弱いものと推定されている。2009 年 7 月 7 日、大規模 DDoS 攻撃により、韓国の主要なサイトを麻痺させることに成功し、ハッカー部隊の威力を発揮した。 それ以降、ハッカー養成が強化され、現在、北朝鮮のハッカー組織の中核となっている。

（北朝鮮の外貨獲得部隊「180 小隊」）

2013 年 4 月、北朝鮮の最高指導者である金正恩国務委員会委員長は、労働党中央軍事委員会拡大会議で「2018 祖国統一構想」を明らかにし、2017 年までに 5 つの核打撃力を開発するように特命を下した。同時に、5 つの重要核打撃力を開発するための予算を確保するための討議が行われ、金正恩（キム・ジョンウン）は、サイバー部隊が外貨を稼ぐことができる「最高のソフトウェア開発能力を持つサイバー要員 500 人」を選抜して外貨を稼ぐ部隊の創設を指示した。この部隊は、外貨稼ぎの経験が豊富な中央党 39 号室の下で、本格的な活動を開始した。それ以降、世界の多くの国のソフトウェアアウトソーシング開発市場に参加して大量のアプリケーションの受注を介して、大量の外貨を稼いでいる。

北朝鮮の内閣と外務省は、この部隊が外貨稼ぎのために世界各国に自由に行き来できるように査証（ビザ）を含むすべての条件を最優先で保障し、関連大使館の協力を受けている。また、この部隊の要員は、中国朝鮮族や日本人の身分で受注市場に参加して、比較的安価な応札価格で獲得する戦略で外貨稼ぎをした。

金正恩（キム・ジョンウン）は、この部隊の成果を高く評価し、自分自身の誕生日（1 月 8 日）にちなんで「180 小隊」と命名した。そして、「180 小隊」がいる限りどんな経済封鎖も怖くないとし、部隊の活動を積極的に奨励している

北朝鮮は、石炭などの鉱物取引のほか、全く予想外の領域（サイバー空間）で巨額のお金を稼いでいることに注目する必要がある。

5. おわりに

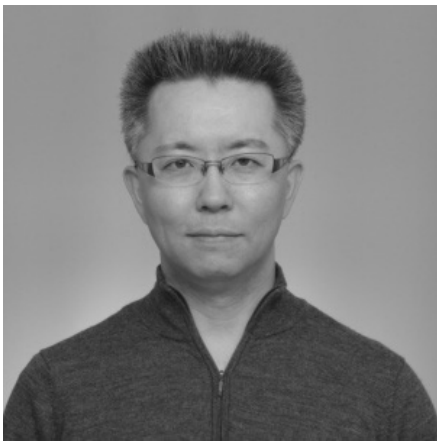
本稿では、外交・安全保障の観点からサイバー攻撃主体の変遷として「日本との関係性のある Hacktivist の実情」を紹介するとともに、「高まる核の脅威に対する抑止力の確保」に向けた取り組みに反発する市民活動がサイバー領域に拡大していること、そして国家の支援を受けたサイバー攻撃部隊の現実として「北朝鮮の 180 部隊」を説明した。

現在、サイバー空間は、国民の日常生活、社会経済活動、行政活動等のあらゆる活動に必要不可欠な頭脳・神経系となっており、サイバー空間と実空間の融合・一体化が進展している。そのため、物理空間における個人や集団が引き起こす事象が、シームレスかつダイナミックにサイバー空間に進展するケースが目立ってきている。また、徹底的な状況認識をしている国では、「大規模なサイバー攻撃」を「核兵器」と同等レベルの脅威と認識し始めている。残念ながら、我が国においては、国家としての「大規模サイバー攻撃」が、国民の生命、身体、財産に重大な被害を及ぼすという認識は緒に就いたばかりである。また、国家の意図を示すようなサイバー能力を保有する実力組織は未整備で、（予算確保ではなく）能力確保のための準備も希薄である。

サイバー空間で発生している脅威は、人間の目・耳・鼻などの感覚器官で感じ取とれないものである。そのため、他の領域の脅威に比べて自らの意志と知力で認識及び理解することが難しく、受動的な姿勢になりやすい。ところが、ここ数年、物理空間に深刻な被害を及ぼすサイバー攻撃がすでに発生している。

今すぐにも、能動的な姿勢に転換し、自らの感覚でサイバー脅威を感じ取らなければ、攻撃側と我々防御側における能力及びパフォーマンスの格差は拡大の一途を辿ることになる。このような状況になっていること、少なくとも国を守る最後の「砦と」なるすべての方々に理解していただきたい。（了）

【筆者紹介】



名和　利男（なわ　としお）

１９７１年北海道北見市生まれ

海上自衛隊において、護衛艦の COC（戦闘情報中枢）の業務に従事した後、航空自衛隊において、信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システム等のセキュリティ担当業務に従事。その後、国内ベンチャー企業のセキュリティ担当兼教育本部マネージャー、JPCERT コーディネーションセンター早期警戒グループのリーダを経て、サイバーディフェンス研究所に参加。専門分野であるインシデントハンドリングの経験と実績を活かして、CSIRT 構築及び、サイバー演習（机上演習、機能演習等）の国内第一人者として、支援サービスを提供。最近は、サイバーインテリジェンスやアクティブディフェンスに関する活動を強化中。

「安全保障を考える」に対する投稿について

（編 集 部）

「安全保障を考える」に対する会員各位の積極的なご投稿をお願い致します。

投稿される場合は原稿用紙（400字詰）10～15枚程度が適当と考えております。

なお、既に発表されているものについてはご遠慮下さい。