ブリーフィング・メモ

サイバー傭兵の動向
――サイバー攻撃代行の現状と課題――

特別研究官　小野 圭司

近年のサイバー戦の特徴に、サイバー傭兵（サイバー攻撃代行業）の台頭がある。これは情報技術（IT）の特性に合わせた、合理的な動きである。しかし彼等が必ずしも、報酬目的（経済合理的）に行動するわけではないことが問題を複雑にしている。

１．サイバー傭兵が生じる原因と特性

サイバー傭兵が生じる主な要因は、大きく２つが考えられる。１つはソフトウェア開発が、極めて知識集約的なことである。このため技術者の質の劣位を量で補うことは絶対に不可能で、小さな組織や個人でも技量次第で十分競争力を有する。IT のように技術進歩が急速な分野では、意思決定の遅れがそのまま致命的な競争力の喪失に繋がるが、この点でも機動的な意思決定が可能な小さな組織や個人は有利である。従って、技術に優れた個人が緩やかに繋がる「アノニマス(Anonymous)」のようなハクティビスト（行動主義的なハッカー集団）の結成や活躍は不思議なことではない。ハクビティストは、社会に影響を与えることを目的にコンピュータ・ネットワーク上で不正侵入やサイバー攻撃等を行っている。

もう１つは、人材供給に纏わる問題である。サイバー・セキュリティの人材は 2019 年の時点でアジアでは 260 万人、世界全体で 400 万人以上不足しており、さらにこの人数は増加傾向にある。つまり IT 技術者の不足は世界的に深刻で、それに伴いこの分野での外託化も広がりつつある。サイバー攻撃代行も、この延長線上にあると見て良い。

これらの背後には、権威や常識にとらわれず、組織の枠にも収まらないで行動する傾向が強いという、技量に優れるハッカー達の特性がある。彼等の中にはサイバー攻撃で得た報酬で豪華な生活を送り、その様子をソーシャル・ネットワーキング・サービス（SNS）で誇示することに価値を見出す者、また厳重な防護を突破して、コンピュータ・システムへの不正侵入自体を楽しむ者もいる。さらには「アノニマス」に参加するハクティビストのように、社会的・政治的正義感から無償でサイバー攻撃に加わる者も多い。このような者達がサイバー攻撃に参加する動機として、報酬以外の比重（自己顕示や達成感、正義感）が大きい場合が少なくない。

２．サイバー傭兵の現状

イランではサイバー軍の設立（2009 年）以前に、民間の IT 技術者が有志のハッカー集団を形成し、2010 年頃より米航空宇宙局（NASA）や米国の金融機関への侵入やホームページの書き換え等を行っていた。彼等はイラン政府の依頼・指示に基づいた攻撃を行うようにもなり、イランの情報部門に対してサイバー戦の訓練も提供している。米国政府も 2016 年 3 月に、イランのイスラム革命防衛隊の支援を受けたハッカーによる攻撃を受けたことを公表している。これらはいずれも構成人数が 5～10 人と小規模で、先に述べた「小さな組織や個人でも技量次第で十分競争力を有する」を体現している。

また彼等は外国関係機関の他、イラン国内外の反体制組織へのサイバー攻撃を行うなど、国内治安維持に関わる依頼もイラン政府から受けている。

2007 年 4 月 27 日に、エストニアの政府機関のサイトが DoS/DDoS 攻撃（サーバやネットワークに過大な負荷を掛け処理能力を飽和させる攻撃）を受けた。これはネットワークに繋がった端末がマルウェアに感染すると他の端末もマルウェアが複製され、設定された時期に同時攻撃を行うというものであった。明確な証拠は無いものの、この攻撃にはロシア政府関係者の関与が強く疑われている。例えばロシア下院のセルゲイ・マルコフ（Sergei Markov）は、自身の関係者がプーチン政権を支持する IT・サイバー技術者と一緒に、上記の DoS/DDoS 攻撃を行っていたこと認めている。

2008 年 8 月の南オセチア紛争では、民間人技術者が DoS/DDoS 攻撃に動員された。ロシア政府はサイバー攻撃に際して犯罪者を動員・組織したと見られているが、この犯罪者を動員して非合法的な活動を行わせるというのはソ連時代からの伝統である。例えば 2017 年にはロシア連邦保安庁（FSB）がサイバー犯罪者を使って、政府関係者や報道関係者、金融機関や交通関係の民間企業に勤める個人の情報の抜き取っていた（フィッシング）ことが明らかになった。因みに 2013 年に欧州で逮捕された、FSB に協力していたと見られるサイバー犯罪者はロシア国内に逃亡し、米国政府や国際刑事警察機構（Interpol）が引き渡しを要求したがロシア側はその要求を拒否している。

中国ではハッカー達は、国家に対して危険を及ばさない限り容認され、場合によっては国の支援を受けており、その数は数万人から 100 万人に及ぶと見られている。また四川省に拠点を置く NCPH（Network Crack Program Hacker）グループに代表される大学生のハッカー集団の中には、政府関係機関と密接な関係を有しているものがあり、サイバー攻撃の依頼・指示を受けることもある。例えば、2006 年の米国防省を含む米国政府機関への侵入は NCPH が行っている。これらハッカー集団は、中国では「サイバー民兵」や「情報専門民兵」と呼ばれており、中国政府も 2004 年の国防白書で初めてその存在を公式に認めている。

学生を基盤とするものに加えて、中国政府は民間企業を主体とするサイバー民兵も組織している。この背景には、中国でのサイバー防衛・セキュリティ需要が急速に高まっていることがある。中国のサイバー防衛の市場規模は 2003 年には 5.3 億ドル、2011 年には 28 億ドル、2016 年には 48 億ドルと順調に拡大しており、2021 年には 132 億ドルを超えるものと予測されている。このような状況下で『フィナンシャル・タイムズ』紙にも取り上げられた南昊科技公司は、ソフトウェア開発やスキャナなど電子機器の製造を手がける企業だが、中国人民解放軍のサイバー民兵としても機能し、人民解放軍のサイバー戦要員教育も請け負っている。

３．ランサムウェアとサイバー攻撃代行

最近頻発しているランサムウェアのサイバー攻撃では、開発と攻撃者の分業化・専業化が指摘されている。かつてランサムウェアの開発者は自ら攻撃を行って収益を得ていたが、ファイル暗号化型ランサムウェアが台頭した 2013 年頃からランサムウェアの需要が高まるとともに、ダークウェブ上で RaaS（Ransomware-as-a-Service）と呼ばれるサイバー攻撃の請負・代行が確認されるようになった。

RaaS とはランサムウェアの開発者が、その作成や管理などを行うためのインフラを、サイバー攻撃者向けに提供するサービスである。ランサムウェアの最大の目的は被害者

に身代金を払わせることで、RaaS では支払われた身代金は開発者とサイバー攻撃請負・代行者の間で分配する。この仕組みにより、サイバー攻撃請負・代行者はランサムウェアを開発する手間を省いて簡便に金銭目当ての攻撃を行うことができ、逆に RaaS の提供者は自分の手を汚すことなく収益を上げることができる。例としてランサムウェア「CERBER」のサイバー攻撃収入は、2016 年 7 月だけで 19 万 5,000 ドルに上り、そのうち開発者の取り分は約 40%（7 万 8,000 ドル）で、残りはランサムウェアを配布した攻撃者に分配されたと見られている。さらにこのような資金分配は、仮想通貨・暗号資産を使ってダークウェブ上で行われている可能性も指摘されている。

また 2017 年に存在が確認された「SATAN」という RaaS は、1 年以上にわたり匿名ネットワーク（The Onion Router：TOR）内の同一サイト上で稼働を続けていた。「SATAN」はサイバー攻撃請負・代行者に、Windows 上で機能するランサムウェアを提供している。「SATAN」ではランサムウェアの開発・配布に加えて、それを使ったサイバー攻撃用の暗号化ツールも提供している。

現在では、マルウェアに様々な形式の暗号化や圧縮を行って表面上のコードが異なる「亜種」を作成することで、サイバー防衛側による検出を回避することが常套化している。そして最近の電子メールを使ったサイバー攻撃では、相手による検知を避けるためにマルウェアを直接添付せず、ドロッパー（ウェブサイトからファイルをダウンロードさせるソフトウェア）を添付して、侵入が成功した場合にそのドロッパーによって最終目的のマルウェア（ランサムウェア）を侵入させることが多い。「SATAN」でも暗号化したランサムウェアのファイルはダウンロード用のサーバに置き、ドロッパーによりダウンロードさせる手法を採ることが可能となっている。因みに「SATAN」では入手した身代金の 3 割が開発者、7 割がサイバー攻撃請負・代行者の取り分となっている。サイバー攻撃請負・代行者の分配率を高くすることで、不特定のサイバー攻撃者を多数動員することが可能になると見られている。

ランサムウェアが、このような不特定多数のサイバー攻撃の請負・代行者の動員が可能である理由は、それ自体が利益（身代金）を生むためである。単なるサイバー傭兵の募集であれば、攻撃を企画する者は報酬を支払うための資金を事前に準備する必要がある。しかし資金力が無くてもソフトウェアの開発能力に優れる者は、ランサムウェアで身代金を獲ることができるので、それを前提にサイバー攻撃の請負・代行者（傭兵）を集めることも可能となる。このようにランサムウェアの普及で、サイバー傭兵の活用やサイバー攻撃代行に新しい傾向（元手は必ずしも必要ない）が生じたと言えよう。

４．ハクティビストの台頭

先に IT・サイバー技術者（ハッカー）は「権威や常識にとらわれず、組織の枠にも、はまらない」と述べた。このような彼等は、自由な情報交換と知識の共有のためには非合理的な官僚主義を忌避し、政府や体制に対する批判勢力を形成することがある。その代表的なものの 1 つが、ウィキリークス（WikiLeaks）である。

ウィキリークスは 2006 年に生まれたハクティビスト集団で、内部告発情報をインターネット上に公開しているサイトである。創設者のジュリアン・アサンジュ（Julian Assange）は元々ジャーナリストで、暗号理論にも精通したハッカーでもあった。これは単に不正や隠蔽された情報を白日の下に晒すというだけではなく、法執行では解決できない問題について社会的な関心を喚起して、司法や行政の限界を示すという社会運動

でもある。この運動がサイバー攻撃代行的なサイバー傭兵と大きく異なるのは、経済的利益（報酬）の追求が動機ではない点にある。つまり彼等は標的を攻撃して損害を与えたり、報酬を得ることを目的としておらず、主に行政機関や大企業を対象に、不正や理不尽に関する情報（多くは法で解決困難な問題に関するもの）を入手し、インターネット上で広く世の中に告発するという懲悪義賊的な社会貢献を目指していた。

近年注目を集めているハクティビスト集団に、「アノニマス」がある。これは不特定多数のハッカーが、「抽象的ではあるが誰もが賛同しやすい大義」の下に即興的に集まったものである。彼等はインターネット・チャットで会議を行い、標的に対して主にDoS/DDoS 攻撃を実行する。その中核となるハッカーの技量は相当高いと見なされるが、不特定多数のハッカーを即興的に集めることから、長期的・計画的な攻撃には向いていない。DoS/DDoS の飽和攻撃は攻撃手順を組むのも単純で、攻撃側の調整負担も軽くて済むので、アノニマスのような組織が行うサイバー攻撃に適している。

ハクティビスト集団は、往々にして付和雷同な者が集まるために、何かの切っ掛けで膨大な人数が徒党を組むことがある。そしてこうした性質を有する彼等を自らの思う方向に利用し、さらには世論の誘導・世論工作も行われている。例えば欧米のハクティビストは大体において自由主義的な反体制の政治思想を共有しているが、中国の場合には、特に 2000 年前後に活発に活動したハクティビスト集団（「中国紅客連盟」や「中国鷹派連盟」等）は愛国主義的な傾向を持ち、中国政府もその限りにおいて、外国に対するサイバー攻撃を行う彼等を泳がせていたのは先に述べたとおりである。またハクティビスト達の方も愛国心からの動きが発端ではあったものの、その活動が中国の大衆から支持され、「英雄」として祭り上げられたことも、活動の動機として大きな比重を占めていた。これは先に挙げた、サイバー攻撃に参加する報酬以外の動機（自己顕示や達成感、正義感）と軌を同じくする。

ハクティビスト集団は一般に、「不正・理不尽」を世の中に訴えて正すという漠然とした正義感を持っている。中国の愛国的集団も、外国は誤っており理不尽であると考えている。この「不正・理不尽」という判断は各ハッカーが独自に行い、その判断に賛同した者が伐異党同的に行動を起こす。逆に言うとハクティビスト集団の中でこの判断の差異が顕在化すると、集団そのものが瓦解する危険がある。実際にアノニマスも、内部では派閥争いが絶えず生じている。このため中国も習近平政権になってからは、ハクティビストへの監視・管理を強める方向に舵を切り始めたと言われている。

〈参考文献〉
・Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018)
・Eneken Tikk, Kadri Kaska, Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010)
・(ISC) ²ed., *(ISC)²Cybersecurity Workforce Study, 2019* (Clearwater, FL: (ISC) ², 2019)
・塚越健司『ハクティビズムとは何か――ハッカーと社会運動』（SB 新書、2012年）
・ジュリアン・アサンジュ『アンダー・グラウンド』〔三木直子訳〕（春秋社、2012 年）
・伊東寛『サイバー戦争論――ナショナルセキュリティの現在』（原書房、2016 年）
・小野圭司「軍産関係史とそれを巡る思想――軍産相対関係の段階的変化に関する考察」『戦史研究年報』第 21 号（2018 年3月）

防衛研究所企画部企画調整課
外　線：０３－３２６０－３０１１　専用線：８－６－２９１７１
ＦＡＸ：０３－３２６０－３０３４　防衛研究所ウェブサイト：http://www.nids.mod.go.jp/