ECONOMY, CULTURE & HISTORY
Japan SPOTLIGHT
Bimonthly

ジャパン・スポットライト 2018 年 5/6 月号（2018 年 5 月 10 日発行）（通巻 219 号）
英文掲載号　https://www.jef.or.jp/jspotlight/backnumber/detail/219/

大澤淳氏（公益財団法人　中曽根康弘世界平和研究所　主任研究員）
コラム名：Cover Story

（日本語仮訳版）

古典的リアリズムの世界に回帰するサイバー空間

ポスト冷戦の時代が終わり、国際政治に古典的リアリズム（現実主義）が戻ってきたと言われている。古典的リアリズムの世界とは、国家が中心的なアクター（行為者）であり、その国家の生存に関わる安全保障が第一義的問題となる世界である。サイバー空間もまた、この国際政治の回帰現象と無縁ではない。

この 10 年、サイバー空間は、国家の戦略目的を達成し、意思を表示する場として国家により利用され始めている。国家が国益を実現する手段としてサイバー攻撃という方法を用い始めたのは、約 10 年前のバルト三国にさかのぼる。攻撃の実行者を隠匿し易いサイバー空間では、国家相互のリアリズム的な対立がより先鋭的な形で現れている。

国家を背景としたサイバー攻撃の増加

2007 年 4 月 27 日、北欧バルト三国の一角エストニアの政府、議会、報道機関、銀行に対して大規模な「機能妨害型」の DDoS（分散型サービス拒否）攻撃が発生した。このサイバー攻撃は、所有者が知らないうちに他人のコントロール下に置かれた「Botnet」と呼ばれる世界中に散らばった数万台のコンピュータ群からなされたものであった。さらに、同年 5 月には第 2 波のより大規模な DDoS 攻撃がエストニアを襲い、金融機関のオンラインバンキングや ATM が停止するなど、市民生活が大混乱に陥った。

攻撃のきっかけは、ソ連占領時代の赤軍兵士の像の移転をめぐる隣国ロシアとの国際紛争であった。当時、この像の移転をめぐり、エストニア国内のロシア系住民が反対し、これをロシアが支援する中で、エストニアとロシアの関係は非常に悪化していた。のちに、サイバー攻撃に使われた Botnet をコントロールしていた「マスター・コンピュータ」がロシア国内に存在し、キリル文字に対応するキーボードで操作されていたことが明らかになったことから、このサイバー攻撃の背後にはロシア政府ないし同国政府と強い繋がりのある集団がいたと見られている。

エストニアと同様にロシアとの紛争を抱える旧ソ連圏の国々では、2008 年 6 月リトアニア、2008 年 8 月ジョージア、2009 年 1 月にキルギスタンで同様の「機能妨害型」のサイバー攻撃が発生している。このうち、ジョージアでは、民族紛争が発生していた同国の南オセチアに対するロシア軍の侵攻と前後してサイバー攻撃が発生し、物理的攻撃とサイバーの

攻撃という「ハイブリッド紛争」の懸念が現実のものとなった。

ロシアの周辺国では、2015 年 12 月に、ロシアとの間で武力紛争を抱えているウクライナにおいて、国家が関与する世界初の重要インフラへのサイバー攻撃が発生した。同年 12 月 23 日、ウクライナ西部の電力会社 Prykarpattyaoblenergo の送電システムに対して、制御系のコンピュータを乗っ取るサイバー攻撃が発生し、いくつかの変電所が強制的にオフラインになった。この結果 22 万世帯で数時間にわたり停電が発生した。同様の攻撃は、2016 年 12 月にもウクライナの首都キエフで発生している。ウクライナ政府は一連の攻撃をロシアの犯行として非難を行なっている。

さらに 2017 年 6 月には、同じくウクライナをターゲットとしたマルウェア「Not-Petya」による大規模なサイバー攻撃が発生した。このマルウェアは、感染したコンピュータのハードディスクデータをすべて暗号化して使用不能にする、という極めて悪性度の強いものであった。当該マルウェアの初期感染経路がウクライナ国内で使われる会計ソフト「MeDoc」であり、ウクライナの政府機関、交通機関、重要インフラなどが集中的に感染したことから、当初はウクライナを攻撃対象とした地域限定的サイバー攻撃とみなされていた。しかし、感染を広げる能力も高かったことから、ウクライナ国内に支店網を持っていたグローバル企業が次々にこのマルウェアの犠牲となった。代表的なものでも、デンマークのマークス（海運業)、米国のモンテリーズ（食品業)、FEDEX（空運業)、英国の WPP（広告代理業）など世界有数な企業が被害にあった。

ウクライナ政府は、攻撃直後にサイバー攻撃をロシア政府が行ったと非難したが、欧米系の企業も大きな被害にあったことから、慎重に調査を続けていた米英加豪 NZ の五カ国は、Not-Petya によるサイバー攻撃がロシア政府によって実施されたことを確認し、2018 年 2 月 15 日にロシア政府を共同で非難する声明を発表している。

中東では、2010 年にイランのウラン濃縮施設の制御システムを狙ったマルウェア「Stuxnet」による攻撃が発覚している。このマルウェアは、濃縮ウランの製造に欠かせない遠心分離機を制御していたシーメンス社製の PLC（Programmable Logic Controller)を狙い、制御システムの麻痺を狙った機能破壊型の攻撃であった。2013 年には、イランからの報復攻撃が、この攻撃を実行したと報道された米国のニューヨーク州のダムに対して行われていたことが明らかになっている。イランはこれ以外にも、2012 年 8 月にサウジアラビアやカタールのエネルギー企業を狙った攻撃や 2016 年 11 月に発生したサウジアラビアの政府機関や企業を狙った攻撃に関与したと見られている。

東アジア地域もホットなサイバー戦が行われている地域である。北朝鮮からは、韓国を狙った「機能妨害型」／「機能破壊型」サイバー攻撃が断続的に発生している。2009 年 7 月には政府機関、金融機関、報道機関に対して「機能妨害型」のサイバー攻撃が発生し、2013 年 3 月には、報道機関や金融機関で感染したコンピュータのデータを消去する「機能破壊型」サイバー攻撃が発生した。2014 年には韓国水力原子力発電会社（KHNP）を狙ったサイバー攻撃が発生している。これら一連の攻撃について、韓国政府は北朝鮮の犯行として調査

報告を発表している。

北朝鮮が関与していると見られるサイバー攻撃グループは非常に能力が高いと見られ、2014 年に米国のソニー・ピクチャーズを攻撃したのをはじめ、2016 年以降バングラディッシュや他国の中央銀行・金融機関をねらった金銭目的の攻撃を盛んに行なっており、各国でも懸念が高まっている。

サイバーパンデミック WannaCry の衝撃

そのようなサイバー攻撃のニュースを毎日のように目にするようになって久しいが、2017 年 5 月、サイバーセキュリティの専門家が目を剥くようなサイバー攻撃が発生した。爆発的な感染力を持つ新種のランサムウェア「WannaCry」の出現である。このマルウェアは、感染したコンピュータのファイルを暗号化し、被害者に対して「復元したければ＄300 相当のビットコインを払え」と要求する典型的なランサムウェアであったが、その感染拡大プロセスがかつてないほど深刻なものであった。このマルウェアは、感染と同時に自身を感染させるモジュールを起動し、ネットワーク内外の他のコンピュータに感染を横展開する機能を持っていた。その結果、WannaCry の発生から 10 日足らずで、世界中 150 カ国以上で 30 万台のコンピュータが感染し、さらながサイバー・パンデミックの様相を呈したのである。

WannaCry によって、英国においては、国民保健サービス (NHS) のネットワークが感染し、患者のカルテなどが参照できなくなる事態となり、救急車の受け入れが停止し、手術が中止になるなど国民生活に大きな影響が生じた。世界的にも英国の他、フランスの自動車企業ルノー、ドイツ鉄道、スペインの通信企業テレフォニカ、ブラジルの石油企業ペトロブラスなどで感染が見つかり、ロシア内務省や中国の公安部などの本来サイバーセキュリティがしっかりしていると思われる政府機関にも感染が広がった。

日本でも、日立製作所および同社の関連グループ企業のグローバルなネットワークで感染が発生し、同社のメール送受信に不具合が生じた他、ホンダの狭山工場では感染によって操業を一時停止する被害が生じた。また、日本マクドナルドでは、WannaCry の亜種の感染が発生し、ポイントや電子マネーを利用した決済が停止する被害が生じた。

この WannaCry に関しては、後にサイバーセキュリティ企業のフォレンジック（技術痕跡分析）により、北朝鮮と関係する「Lazarus」というサイバー攻撃グループが作成に関与していることが明らかになった。医療機関に大きな被害の出た英国では、政府の国家サイバーセキュリティセンター(NCSC)が中心となって分析を行い、英国の安全保障当局者は北朝鮮のハッカーが攻撃に関与したと判断している、と英国 BBC は報じている。

この北朝鮮と関係する Lazarus は、2014 年に発生した米国のソニー・ピクチャーズ・エンターテイメントに対するサイバー攻撃や、2016 年にバングラディッシュ中央銀行からサイバー攻撃によって 8100 万ドルが詐取された SWIFT 不正送金事案を実行したと言われており、北朝鮮の国家機関とほぼ同一と見られている。

WannaCry が世界初のサイバー・パンデミックとでも言うべき感染の広がりと被害をもた

らしたのは、WannaCry が Windows のファイル共有機能 SMB の脆弱性を突いて感染を広げる機能を持っていたからであった。この脆弱性は 2016 年 9 月にマイクロソフト社から初めて公表され、脆弱性修正ツール MS17-010 が 2017 年 3 月に初めて公開されていたが、修正ツールを適用していない PC やサーバーは世界各地に散らばっており、攻撃されれば確実に感染するという致命的な脆弱性であった。

この脆弱性を利用した侵入ツールは「EternalBlue」(脆弱性を突いて任意の命令を実行)と「DoublePular」(EternalBlue によって作成されるバックドア)と呼ばれ、元々は米国国家安全保障局 (NSA) が他国のネットワークに侵入するために開発したものと言われている。この米国製と見られる強力な侵入ツールを北朝鮮が利用することができたのは、ロシア系のハッカー集団と見られる Shadow Brokers が 2017 年 4 月にツールをネット上に公開したからであった。公開からほぼ１ヶ月たらずで、この強力な侵入ツールを組み込んだサイバー攻撃が行われたことに、サイバーセキュリティ関係者の間では激震が走った。しかし、それ以上に深刻な事実は、国家級の最先端のサイバー攻撃ツールが、国家機関のみならず、民間企業も含む世界中のコンピュータに対して無作為に使われた点にある。

日本へのサイバー攻撃の激化

機能妨害や制御システムを狙ったサイバー攻撃の他にも、特定の組織・個人から機密情報を窃取することを目的とした国家が関与する標的型攻撃も増加している。日本では、2011 年に衆議院や政府機関、防衛産業を狙い、情報の窃取を目的とした大規模な標的型攻撃 (APT) が明らかになったが、同様の情報窃取を目的とした攻撃は、2005 年ごろから断続的に繰り返されてきたと見られており、2015 年 5 月には日本年金機構が保有する個人情報を狙った標的型サイバー攻撃が発生している。

日本年金機構に対するサイバー攻撃では、「Emdivi」と呼ばれるマルウェアが使用された。年金機構へのサイバー事案を調査した日本政府の NISC の報告書によれば、攻撃の第１波は 2015 年 5 月 8 日に発生し、その後の４波にわたる攻撃により、最終的に 30 台以上のコンピュータが感染し、125 万件に及ぶ個人情報が部外に流出した。同マルウェアを技術的解析したマクニカネットワークスによれば、マルウェアの作成者は中国国内で、月-金、9 時-17 時に勤務する者であると分析されており、これら一連の「情報窃取型」サイバー攻撃には、中国の関与が強く疑われている。これら中国由来の「情報窃取型」サイバー攻撃を繰り返しているサイバー攻撃グループは、2016 年以降特に日本を対象に攻勢を強めていると分析されており、今後厳重に注視していく必要がある。

民主主義を脅かす情報操作型サイバー攻撃

さらに、直近の新しいサイバー攻撃を取り巻く状況の変化として、国家間の対立を背景に、相手国内の情報操作を目的とした「情報操作型」サイバー攻撃（情報戦）が行われるようになっている。米国では 2016 年の大統領選挙中に民主党の全国委員会を標的として、ロシア

系のサイバー攻撃グループ APT28(FancyBear)や APT29(CozyBear)が情報窃取型サイバー攻撃を行い、入手した民主党の内部情報を WikiLeaks を通じて配信したとみられている。これ以外にも偽ニュースの流布、代理主体を用いたサイバー攻撃によるかく乱、サイバー窃取による機密情報の意図的な公開が行われ、大統領選挙の最終結果に大きな影響を及ぼしたと言われる。同様の「情報操作型」サイバー攻撃は、2017 年のフランス大統領選挙やドイツの総選挙でも発生しており、各国ともその対応に苦慮している。

国家を背景としたサイバー攻撃を防ぐために

これまで見てきたように、サイバー空間は、諜報活動、機能妨害、破壊行為、情報操作を目的として、国家の戦略目的を達成し、意思を表示する場として利用されている。また、感染力・破壊力の強いマルウェアが次々に出現しており、世界全体を巻き込む深刻なサイバー・パンデミックが発生する恐れも高まっている。

すでに米中間、欧米露間、米北朝鮮間では、サイバー諜報、機能妨害、破壊型攻撃が発生しつつあり、今の所「戦争」に至らないグレーゾーンにとどまっているが、より感染力・破壊力の強いマルウェアが次々に出現しており、世界全体を巻き込む深刻なサイバーパンデミックが発生する恐れも高まっている。

日本では、中国によるサイバー窃取は顕著であるが、重要インフラを狙った大規模なサイバー攻撃はまだ発生していない。しかし、国際情勢の変化や世界に蔓延するサイバー・パンデミックが発生すれば、日本の国民生活に甚大な影響が生じることが予想され、懸念が高まっている。

米国はサイバー安全保障に関して、サイバー・セキュリティの確保、重要インフラの防護といった Passive Defense では不十分と認識し、相手国への侵入と継続的な行動監視、インターネット空間の膨大な電子データの蓄積とビッグデータ分析を利用した事案後の分析・追跡を行っているとみられる。

実際 2015 年に確立された米国のサイバー安全保障戦略は、サイバー防御力を高めることによる抗たん性の確保および復元性を高めることによる「拒否的サイバー抑止」能力の向上と、サイバー反撃を含む様々な政策手段による「懲罰的サイバー抑止」能力の向上の両面からなり、国家が関与するサイバー攻撃を抑止することを中核に据えている。

従来各国のサイバー対応は、サイバーセキュリティの確保、重要インフラの防護といった受動的サイバー防御を中心に行ってきたが、攻撃グループの継続的な行動監視やビッグデータ分析を利用した攻撃対応など、より積極的サイバー防御が求められるようになっている。

（了）