第２章　北朝鮮のサイバー脅威評価

ブ・ヒョンウク

I. 序論

韓国政府にとって北朝鮮は最も堅牢な諜報対象の1つである。同国は主体思想を支持する盲目的な愛国主義国家であり、世界の最貧国の1つである。同国のサイバーインフラは非常に初期的なものであると考えられることから、北朝鮮では公共 Wi-Fi やクラウドサービスを利用できる環境はほとんど想定しえない。2013年に Google 社の元 CEO エリック・シュミット（Eric Schmidt）が北朝鮮への短期間の訪問から帰国した際、インターネットに接続されたコンピュータは北朝鮮に僅か数千台しかない旨を述べている。サイバー分野の観点から見ても、北朝鮮は文字どおり世界から隔絶された国家である。

しかし一方で、米韓両国に向けた北朝鮮による非常に巧妙なサイバー攻撃の開始も観測された。北朝鮮によるサイバー攻撃オペレーションは、一般に有名なウェブサイトへの単純な DDoS 攻撃や電子メールのハッキングに始まり、その後、持続的標的型攻撃（Advanced Persistent Threat: APT）[1]と呼ばれる高度技術を採用している。近年、北朝鮮ハッカーは PC プラットフォームからモバイルプラットフォームへと、その実行範囲の拡大を試みている。この傾向は有力政治家数人のスマートフォンも対象となった最近の攻撃に見られる通りである。

北朝鮮のサイバー攻撃、さらにそのインフラを目の当たりにし、多くの疑問が提された。北朝鮮のような国家がいかにしてこれほど本格的なサイバー攻撃を仕掛けることが可能なのであろうか[2]。コンピュータセキュリティ業界が自らのビジネスを

1　持続的標的型攻撃（APT）には、ネットワークへの侵入、検出の回避および長期間にわたる機密情報の窃取という複数の段階が用られる。

2　サイバーセキュリティの専門家として名高いリビッキー（Libicki）教授との電子メールでのやり取りの中で、同氏からこの疑問に対する回答があった。教授の見解は次の通りである。「北朝鮮は貧しい国家ではあるが、その国民が原始的だというわけではない（国民が飢餓に喘いでいるのは、同国指導部が国民への食糧供給の保証と別の多くの国家目標を天秤にかけ、後者を優先しているためである）。北朝鮮は核兵器開発も実施したが、これは後発開発途上国には不可能なことで

増進させるために、北朝鮮のサイバー能力・脅威レベルを誇張していると主張する懐疑論者もある。これらの疑問を踏まえた上で、北朝鮮のサイバー能力、そして現実的な脅威を正確に見極める必要性が高まりつつある。しかし、同国のサイバー能力とその目的の判断は非常に困難な作業である。北朝鮮製のマルウェアやヒューミント[3]の分析を実施してきたものの、北朝鮮で進展している詳細な現状は不明である。

本稿では、北朝鮮のサイバー能力に関する情報収集およびその客観的評価を試みる。これらの目的のため、以下のセクションにおいて、北朝鮮によるサイバー攻撃の事例分析、同国によるサイバー攻撃の脅威に関する調査結果への考察、そして同国のサイバー脅威への対応策評価を行うこととする。

II. 北朝鮮によるサイバー攻撃事例

サイバーテロおよびサイバー戦は近年における流行語となったものの、韓国のサイバーセキュリティに関する社会的言説の歴史は非常に短い。北朝鮮がサイバー攻撃を開始したのは2004年頃であるが、北朝鮮がもたらすサイバー脅威に世間が懸念を示すきっかけとなったのは、2009年の7.7 DDoS攻撃であったとする専門家もいる。7.7 DDoS以前のサイバー攻撃は、基礎技術を使用した電子メールのハッキング事案がその大半であった。

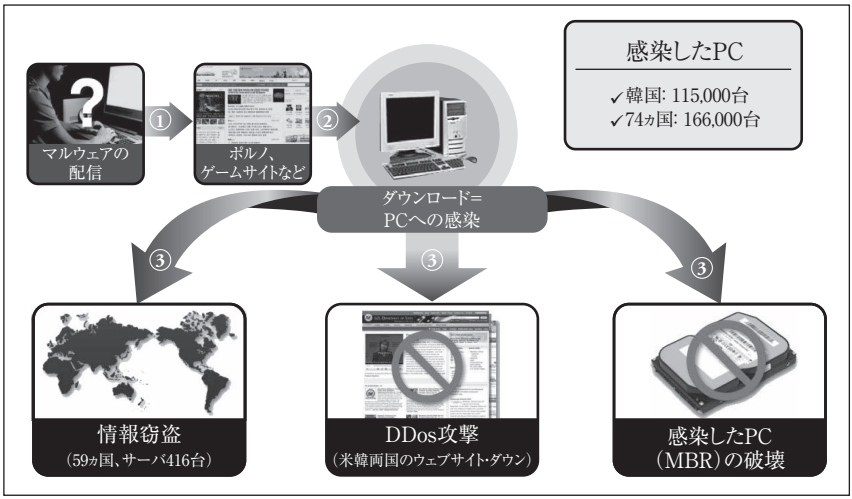
7.7 DDoS攻撃後、北朝鮮はさらに頻繁に韓国に対するサイバー攻撃を開始し、その攻撃が及ぼす影響はさらに深刻化している。かかる状況下、『月間朝鮮』（Monthly Chosun）のジャーナリスト、ベック（Baek）やその他のジャーナリストたちは、北朝鮮によるサイバー攻撃の拡大と、当時、後継者として確実視されていた金正恩の出現との間には、関連があると推論した。この議論に対しては批判の向きもあったが[4]、金正恩時代における北朝鮮からのサイバー攻撃の急増は明らかである。

ある。（北朝鮮が具備するような）サイバー能力の開発は、核兵器の開発が可能な国家の場合、何も意外なことではない。」

3　現在、韓国国内に約30,000人の北朝鮮難民がおり、中には北朝鮮のサイバー能力に関する有益な情報を提供する者もある。

4　M.リビッキー（M. Libicki）らの専門家は、北朝鮮からのサイバー活動増加が新指導者の就任

図1　7.7 DDoS サイバー攻撃



7.7 DDoS 事件以降に発生した数件の周知事案は次のとおりである。2010年7月7日、北朝鮮は韓国政府および民間セクターのウェブサイトに DDoS 攻撃を仕掛け、P2P サイト、チャットルーム、ウェブハード、および無料ワクチンプログラムのサイトを通じてマルウェアが配信された。このマルウェアに感染した PC をゾンビ PC と化すことによって、北朝鮮のハッカーは世界中の数千とも数百万台ともいわれるゾンビ PC 内のリソースの掌握を果たした。これらのハッカーがサイバー攻撃開始を決定したとき、かかるゾンビ PC が指定されたウェブサイトに大量のデータパケットを送信し、ウェブサーバの容量を氾濫させた。DDoS 攻撃が社会に深刻な被害をもたらした事例もあるが、この種のサイバー攻撃は単にウェブサイトのダウンやサイトの表面上のダメージ等、あくまでサイトに対する視覚的な損傷をもたらすに過ぎなかった。北朝鮮による DDoS 攻撃はその後、技術的精巧

に起因しているか否かについては明言し難い旨を主張している。専門家らの見解では、中国による明確なサイバー活動（特に対企業活動）の減少は例外として、その他のあらゆる場所においてサイバー活動は増加傾向を示している。つまり、この点において、北朝鮮によるサイバー攻撃の頻度は近年の傾向の一部であるように見える。しかし、その頻度は世界の他の地域でのサイバー攻撃事件の一般的傾向を著しく超えていると見られる。

さを増し、ウェブサイトをダウンさせてサーバデータを消去した事例もあるが、いずれも高度な技術が要求されるものではなかった。

2011年、北朝鮮のハッカーによりそのサイバー攻撃力の強化性が実証された。3月4日、北朝鮮は40人の韓国国民、政府、韓国軍、在韓米軍等の非公開ウェブサイトへのDDoS攻撃を開始した。約1ヵ月後、北朝鮮は韓国国内の農協インターネットバンキングシステムの機能停止を引き起こした。同銀行サーバが通信不能となり、データが消去されるに至った。この事案は2011年4月12日に発生した。同攻撃の詳細評価の後、専門家は北朝鮮ハッカーがインターネットバンキングシステムの保守専門技術者に向けてAPTを使用した可能性があったと結論付けた。北朝鮮ハッカーは多くの時間と労力を傾注することで保守技術者を特定し、同技術者のPCにマルウェアを侵入させたと見られている。この事実に気付くことなく、同技術者が定期点検のために同農協インターネットバンキングシステムに接続し、同時にマルウェアがシステムに侵入するに及んだ。これが当該事案のすべての始まりであった[5]。

悪評の高いその他のサイバー攻撃は2013年に発生している。2013年3月20日、マスターブートレコード（MBR）[6]のワイパー攻撃により、銀行、報道機関のコンピュータ32,000台がシャットダウンした。銀行には農協、新韓銀行、済州銀行が含まれ、報道機関はYTN、KBS、MBC等である。この事案は2013年の「3.20サイバーテロ」と呼称されている。この3.20サイバーテロから5日後、北朝鮮のサイバー兵士はデイリーNK（DailyNK）、自由北韓放送（Free North Korea Radio）、NKネット（NKnet）をもその攻撃対象とした。これらは北朝鮮から亡命した知識人らにより運営される一般報道機関であり、彼らはこれら報道機関を通じて北朝鮮政府の悪質性に関する情報を発信していた。北朝鮮の計画による別のサイバー攻撃は2013年6月25日に発生した事案である。これは政

5　上記の農協機関が銀行業務を正常化させるために1ヵ月を要した。（http://www.itworld.co.kr/news/73444?page=0,1; retrieved Aug 25, 2016）

6　マスターブートレコード（MBR）とは、分割された大容量記憶装置の先端にある特殊型ブートセクターを指す。

府、報道機関の16のウェブサイトに対するDDoS攻撃であり、北朝鮮ハッカーはこれらのウェブサイトのDNSサーバもその標的とした。

2014年11月、北朝鮮の動きはより大胆になり、ソニー・ピクチャーズ・エンタテインメントに対するMBRワイパー攻撃を仕掛けた。このハッキング事件により、北朝鮮のサイバー攻撃への脅威に対する非常に大きな懸念と強い反発が生じた。2014年12月、韓国の原子力発電会社である「韓国水力原子力発電会社」の情報システムへのサイバー攻撃が計画された。その攻撃目的は、データ窃取、強奪およびMBRワイパー攻撃であった。同事案は、北朝鮮にはサイバー攻撃を通して実害的な物的損害をもたらす能力を既に有しているという認識を、同国が得ようと画策した結果の行動であると考えられる。よって、これは重大事案とも見なされた[7]。

2015年には「物理的な」軍事的挑発行為は多数発生したが、北朝鮮によるサイバー攻撃に関しては比較的平穏であった。しかし、2016年に入り、北朝鮮によるサイバー脅威は再燃した。JETCO Technologyのキム・ミンホ（Min-ho Kim）によると、北朝鮮は2016年上半期中、少なくとも10回にわたるサイバー攻撃を実施している。北朝鮮は4回目の核実験後、サイバー攻撃の回数を増加させている。2016年6月末時点、韓国は平壌市内の柳京洞に攻撃サーバ16台を特定した。北朝鮮によるサイバー攻撃においてハッカーにより使用されたとみられる33のマルウェア分析が現在進行中である[8]。

北朝鮮によるサイバー攻撃事案を再検討する中で、我々の注意を引く複数のある特徴に気付くことができる。第一に、従来のセキュリティ脅威を、それとは異なる他の脅威と融合するというサイバー攻撃が北朝鮮の通常の攻撃パターンになった点である。北朝鮮ハッキング組織の精鋭らは、サイバー攻撃と4回目の核実験などの他の軍事的挑発行動を連携させるよう政府当局から指令を受けていたと考

7　この事案は韓国における原子力発電所の安全性に関する懸念拡大のきっかけにもなったことから、心理的損害をもたらしたということができる。（http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150317160750&type=det&re=; retrieved Aug 25, 2016）

8　専門家によると、北朝鮮ハッカーにより開発されたマルウェアにおいてはコマンドラインの繰り返しが見られる。多くの北朝鮮製マルウェアが「キムスキーシリーズ」（Kimsuky series）と呼称されている理由は、「キムスキー」（kimsuky）の文字がマルウェアコード内に繰り返し使用されているためである。

えられる。北朝鮮の目的は韓国国民の正常な判断力・精神力を粉砕することであり、この目標達成のため、ハッカーはデマやプロパガンダ等を拡散したのである。朴大統領に有害な内容となる電子メールが送信された事案もあった。例えば、北朝鮮ハッカーは、現韓国政府による北朝鮮の核問題に対するアプローチを批判する大量の電子メールを送信した。ハッカーはメールの信頼性を高めるため、影響力を有する学者や放送局（例えばMBCおよびSBS）から窃取したアカウントを使用しこれらのメールの送信を実行した。

第二に、北朝鮮のサイバー兵士は、北朝鮮が政治家、高位軍人数名のスマートフォンをハッキングした事案のように、その実行範囲をモバイル領域へと拡大した。サイバー兵士らはテキストメッセージ、録音通話記録、連絡先情報の窃取を試みた。第三の側面は、北朝鮮には公共交通管理システムに障害を引き起こす狙いがあったことであり、これは大混乱に陥らせる可能性があるものである。実際、ソウルの地下鉄網であるソウルメトロへのハッキング計画があり、同計画によりサイバー攻撃を起因とする運行障害を予示する不穏な兆候が国内にもたらされた。最後に、2016年における防衛関連企業へのハッキング計画である。ハッカーはF-16戦闘機の保守マニュアル、韓国のドローン関連部品の写真データ、その他の機密文書を窃取している。当局は42,600点に及ぶ文書・文献が窃取されたと推定している。これは直近の事案であり、北朝鮮ハッカーが軍事目的にその重点を置いていることを示唆するものである。

III. 北朝鮮のサイバー脅威：諸調査結果

2010年代に入り、韓国におけるセキュリティ専門家の多くがサイバー戦、サイバーテロの議論に加わった。多くの専門家がこの問題を様々な視点から捉えている。ここに示すのは重要な議論の一部である。第一に、最もよく見られる議題の一つは北朝鮮によるサイバー攻撃の目的分析である。専門家は北朝鮮のサイバー攻撃を非対称戦略の遂行と見なす傾向にある。実際、サイバー脅威は非対称戦略の別称ともなっている。この戦略により貧困国家が低コストで、富裕国家の情報通信技術（ICT）資産に危害を加える機会を得られるようになる。韓国におけ

る例のように、ある国が高度なICTネットワークで密接に繋がっている場合、その国の標的インフラへの攻撃により混乱の連鎖が引き起こされる可能性がある。

数十年間におよぶ経済的危難により、北朝鮮は特に通常兵器の領域において、韓国との軍拡競争を放棄せざるを得なかった。したがって、核開発という選択はその劣勢を補おうとする大胆な行動であり、高度なサイバー兵器開発はもうひとつの選択肢であった。我々はそれを北朝鮮による「オフセット戦略」と称することがあり[9]、サイバー活動は同戦略の重要な位置を占める。サイバー手段の利用により、北朝鮮はソウルメトロへのサイバー攻撃事案のように、ネットワーク社会に大規模な混乱を引き起こすことが可能となっている。軍事的には、北朝鮮のハッカーは米軍および韓国軍の複雑なセンサー・シューターや一体化された指令制御システム等、軍事ネットワークへの侵入を試みる可能性がある。したがって北朝鮮のサイバー兵士が侵入を果たした場合、米韓連合軍はネットワーク中心の交戦において困難な状況に直面する可能性がある。

第二は、北朝鮮はサイバー攻撃を政治的手段として採用しているという点である。ここで述べる政治的手段とは、朝鮮半島の治安情勢をグレーゾーン、すなわち、脅威が重大かつ明らかであるが、軍事的手段を取ることで、その情勢を正常化する方法がほとんど存在しない地帯へと転換し得る手段を意味する。つまり、北朝鮮はミサイル実験、核実験、遠隔の諸島地域または非武装地帯への限定的な軍事攻撃、さらにサイバーテロ等、様々な手段を採用することで朝鮮半島における政治的地勢の粉砕を試みたのである。さらに、北朝鮮は他の挑発的行為との融合を常套手段としており、これは結果的には優れた戦術的手段である。これが、筆者自身を含む専門家が複合的危機、すなわち様々な危機が混在している状況という観点から、北朝鮮によるサイバー攻撃の規則性の解析を試みている理由である。予備調査の結果は、他の挑発的行為と融合された場合、サイバーテロは、緊張状態を高めるための効果的な手段として使用でき、北朝鮮は必ずこの手法を用いると報告している（Boo and Choi、2014）。実際に北朝鮮は、軍事的挑発行動やプロ

[9] オフセットは、ある不利益な局面に対して非対称的に填補するいくつかの手段を指す。通常、オフセット戦略は形勢逆転の戦略として理解される。

パガンダの政治的影響力を強化する手段としてサイバー脅威を利用している。北朝鮮は長距離ミサイル実験や核実験等、大規模な軍事的挑発の前後にサイバー攻撃を行うのが定説であった。専門家はまた、北朝鮮への対処法に関して、韓国社会を２極論に分断するという北朝鮮の目的遂行において、同国によるサイバー手段の利用を可能にするという点でも、サイバースペースの有用性を認識している。

関心が高い別の議論として、北朝鮮のサイバー脅威の技術水準に関する評価が挙げられる。研究者や評論家らが北朝鮮の能力評価を実施し、同国と他の国々の能力の比較を試みた結果、いくつかの点が明らかになっている。北朝鮮のサイバー戦力は米国 CIA とほぼ同等であるとさえ推測する研究者がいる一方、北朝鮮のサイバー攻撃能力レベルは中程度だと思われる[10]。しかし、インターネット接続環境の不足により北朝鮮のネットワークシステムへの侵入方法が殆ど存在しないことから、その防衛能力は非常に高いと考えられる。かかるアイロニー的状況が北朝鮮のサイバー脅威を厄介な障壁としている[11]。

表１　サイバー戦力の国別比較

国名	サイバー攻撃	サイバー依存	サイバー防衛	合計
米国	8	2	1	11
ロシア	7	5	4	16
中国	5	4	6	15
イラン	4	5	3	12
北朝鮮	2	9	7	18

出典：Richard A. Clarke and Robert K. Knake, *"Cyber War: The Next Threat to National Security and What to do about it"*, ECC 2010 p.149

[10] 攻撃行為に関して言えば、北朝鮮ハッカーは非常に攻撃的である。北朝鮮のサイバー攻撃力に関する議論において、米国海軍兵学校の M. リビッキー（M. Libicki）教授は「他国の大半は、情報の窃取を目的にコンピュータに侵入するが、北朝鮮はコンピュータ自体を破壊する目的でもコンピュータシステムに侵入する」と述べている。

[11] 米国海軍兵学校のリビッキー教授によると、北朝鮮のサイバー能力はその他の多くの国々（例：スペイン、レバノン）よりも高度である。同教授の考察では、おそらく北朝鮮は多くのサイバー犯罪組織と同程度に高度なサイバー能力を有している（さらに、かかる組織は無防備な標的を攻撃することに特化している）。外部との接続がありかつ標準的な Windows 搭載システムに侵入することは、一定の能力を有するハッキング集団にとって何ら困難な作業ではない。

表 2　コールマン（Coleman）による比較結果

国名	意図性	攻撃能力	インテリジェンスレート	合計
中国	4.2	3.8	4.0	4.0
米国	4.2	3.8	4.0	4.0
ロシア	4.3	3.5	3.8	3.9
インド	4.0	3.5	3.5	3.7
イラン	4.1	3.4	3.4	3.6
北朝鮮	4.2	3.4	3.3	3.6
日本	3.9	3.3	3.5	3.6
イスラエル	4.0	3.8	3.0	3.6
韓国	3.5	3.0	3.2	3.2
パキスタン	3.9	2.7	2.6	3.1

出典：Coleman, K., The Weaponry and Strategies of Digital Conflict, in Armstead, E. L (eds.), *The Proceedings of the 5th International Conference on Information Warfare and Security*, (The Air Force Institute of Technology, Ohio; 2010). p. 498

北朝鮮のサイバー戦組織、あるいは同教育機関に関する情報は多くはないものの、同国偵察総局（GBR）が韓国に対するサイバー攻撃に深く関与している事実が確認されている。北朝鮮の亡命識者でありNKネットの議長を務める金恒光は、北朝鮮の中核となるサイバー部隊に関する情報を提供している。これによれば、1998年9月、金正日により「121部隊」が組織され、それ以降、韓国に対して30,000件を超えるサイバー攻撃が実施されている。各種ニュースソースからの報告によれば、金正日自らがサイバー戦の実行能力を強化するよう強く主張したとのことである。例えば、金正日は「20世紀の戦争は石油・銃弾に関わる交戦であったが、21世紀の戦争は諜報戦である」と述べている。専門家の考察では北朝鮮の諜報戦の概念にはサイバー戦も含まれている。これを反映し、朝鮮人民軍はネットワークの分断、インフラ破壊、敵軍の司令系統、制御システム機能停止の実行を含む「電子諜報戦」の概念の下、サイバー戦力の強化に挑んだのである。

サイバー攻撃の実施に関し、NKネットの金恒光は中国瀋陽市の北朝鮮レスト

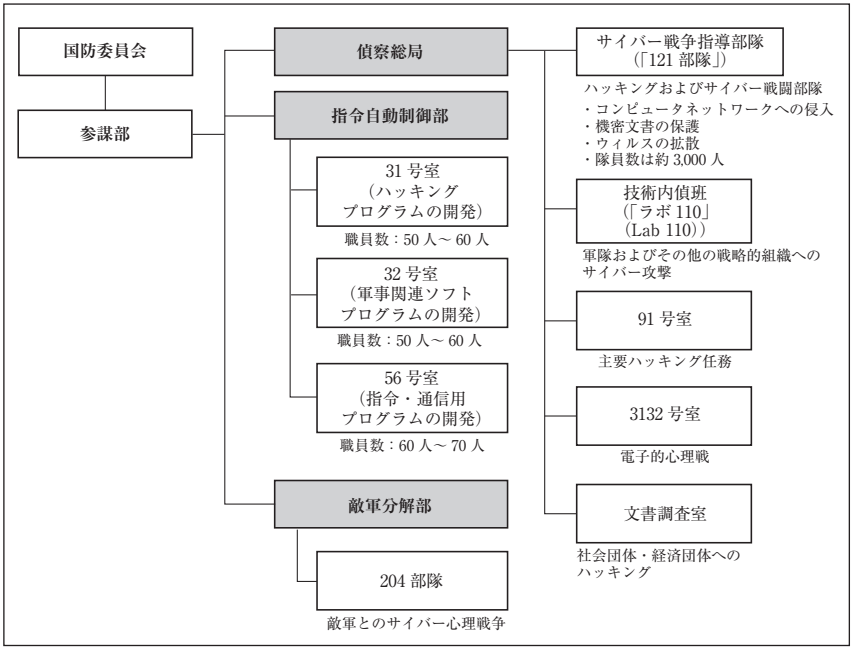
ラン「Chilsung-gak」等、中国国内に複数存在するサイバー攻撃の極秘作戦現場を指摘している。同氏によると、北朝鮮ハッカーは瀋陽市、丹東市、北京市、その他の中国国内都市にあるPCカフェでサイバー攻撃を実行し、中国聯通等、中国国内の電気通信事業者の基幹回線網に密かにジャンパを設置し、障害通信線を使用してサイバー攻撃を実行することもあったという。また、「121部隊」のサイバーテロリストの中には、国家的サイバー攻撃活動の目的のために日本、東南アジア、アフリカ、欧州諸国に渡った者までいたという。

将来のハッカー候補者を育成するため、北朝鮮政府はサイバー兵士養成を専門とした一連の教育機関を設立した。また1980年代半ば以降、プロのハッカー集団を養成することにより、自国のサイバー攻撃力を強化してきた。新たなニュースソースによると、北朝鮮はサイバー兵士を教育する目的でミリム大学、モランボン大学、その他の高等教育機関を開設している。かかる機関は朝鮮人民軍と密接な関わりを有し、毎年数百人ものプロのハッカーを教育していると見られている。彼らはトップクラスのハッカーとなり、卒業後は軍当局者としてハッキング部隊任務が課されるものと推測される。北朝鮮のサイバー戦機構に関し、図2に示した構成図作成においては、専門家による推察、脱北者の証言を援用した[12]。北朝鮮のサイバー戦組織図の解明に関し最も重要な点は、かかるハッキング部隊が国防委員会監督下の北朝鮮偵察総局（GBR）[13]の配下に置かれている点である。先に述べたとおり、韓国検察院、国家情報院はGBRの「121部隊」を多くのサイバー攻撃の主要容疑者として指名手配している。一方、北朝鮮によるサイバー兵士の推定総計人数は6,800人に達しており、さらに金恒光、その他のニュースソースによると、近い将来10,000人に達する可能性がある。

[12] 筆者自身、可能な限り多くの情報収集を行うものの、情報が限定的であるため事実とは異なる情報も存在する。しかし図2には北朝鮮のサイバー戦部隊の実体をほぼ厳密に反映させている。

[13] GBRは北朝鮮の諜報機関の1つであり、韓国に対する内偵活動を担う。

図 2　北朝鮮のサイバー戦部隊体制



出典：Boo, Hyeong-wook *et. al*.. 2013. *A Study on Future Direction of Defense Cyber Policy*. KIDA report (in Korean). p. 94

一方、近年の調査結果によれば、北朝鮮が自国のサイバー能力の行使により利益獲得にほぼ成功している事実が報告されている。韓国自由民主研究所（Korea Institute of Liberal Democracy：KILD）のユー・ドンリュル（You, Dong-ryul）博士は、北朝鮮がサイバー活動を通じて年間 10 億ドルの利益を得ていることを指摘している[14]。北朝鮮ハッカーは違法サイバー賭博サイトを開設し、プレイヤーにゲーム上のレアアイテムを販売するオンラインゲームを展開し、さらにバングラデシュ等の場合と同様、オンラインバンキングシステムを破壊するに至った。ユー博

[14] 北朝鮮の対外貿易取引額が公式では年間 100 億ドルに満たないことを考慮すると、10 億ドルという金額は同国にとって相当な金額である。ユー博士が提示した同金額はやや意外である。筆者自身を含む専門家は北朝鮮がサイバー活動によりある程度の金額を獲得しているという事実を認識していたが、同博士により提示された金額については疑問を呈した。

士によると、北朝鮮がかかる活動において多額の外貨獲得に及んでいる旨が指摘されている。

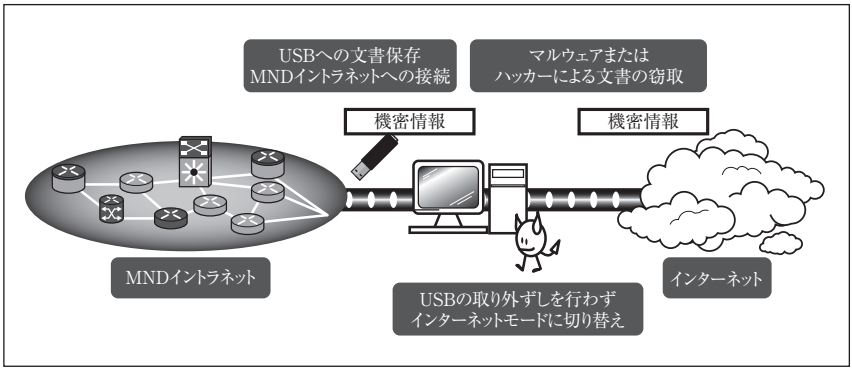
IV. 北朝鮮のサイバー脅威への対処と新たな脅威の評価

韓国は世界のIT大国として発展を続けながらも、10年以上にわたり北朝鮮によるサイバー攻撃の影響を受けてきた。韓国はサイバーセキュリティを強化してきたが、同国のネットワーク依存が強まることにより、自由化・民主化を果たした他の国々と同様、必然的にある一定の脆弱性にも晒されることとなった。ネットワークはそれ自体の脆弱性、そして敵国のサイバー攻撃能力の強化を要因として危殆化している。この2つの要因は相互に連関しており、その結果として韓国に生じる壊滅的な影響が実証されてきた。北朝鮮によるサイバー攻撃を受け、その被害が特定のウェブサイト凍結のみに留まる場合もあるが、相当額の社会的コストが発生する事件も多発している。後者の事例にはインターネットバンキングの機能停止、韓国軍からの作戦計画5027の窃取、防衛関連産業からの機密文書窃取、有力政治家のスマートフォンへのハッキング行為等が含まれている。これらの中で、作戦計画5027の窃取、すなわち作戦計画の機密情報を含む文書の抜き取りが最も予期せぬ事案であった。下図に韓国軍のイントラネットからデータ窃取が実施された仕組みを示す[15]。

---

[15] ある意味において「作戦計画5027の窃取」という表現を用いることで誤解が生じる可能性もある。作戦計画5027の機密文書全てではなく、ブリーフィングで使用される作戦計画の概要箇所（PowerPointファイル）の窃取であるためである。この事案が起きた原因はデュアルPCでのUSBメモリスティックの使用にあった。デュアルPCとは個別のオペレーティングシステムが搭載された2つのハードドライブを有するPCのことで、それぞれ韓国国防部（MND）のイントラネット用とインターネット用に使用される。したがって、使用者は必要に応じインターネット接続からMNDイントラネット接続用のコンピュータに（もしくはこの逆も然りである）再起動する必要があった。実際、デュアルPCとはハードドライブ以外のコンピュータの全コンポーネントを共有する2台のPCのことである。作戦計画5027の窃取は、ある職員がインターネット接続を使用するにあたり、システムからUSBメモリスティックを取り外さずにMNDに接続されたシステムを再起動した際に発生した。USBメモリスティックには作戦計画5027の概要資料が保存されていた。この事案以降、MNDはデュアルPCの使用を禁止した。((http://www.hani.co.kr/arti/politics/defense/394238.html retrieved Aug. 25. 2016))

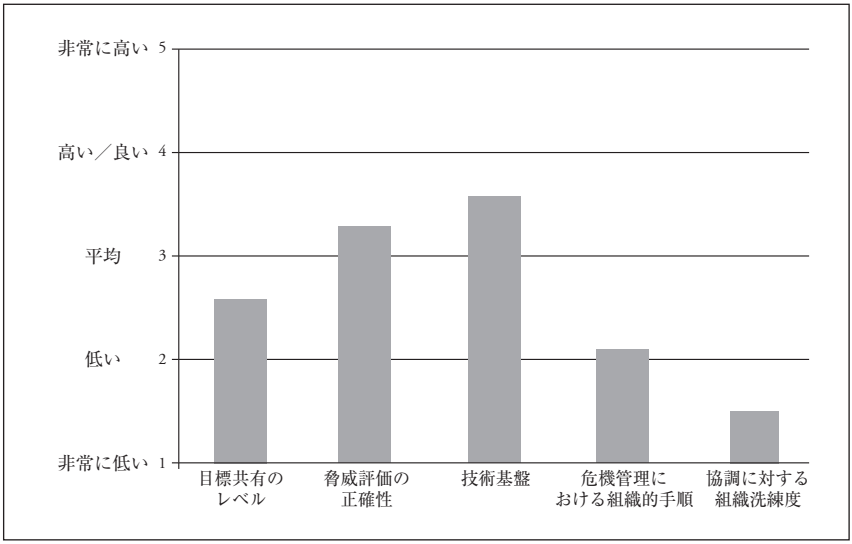
図3　作戦計画5027の抜き取り



サイバー攻撃による脅威がますます高まっている現状に対して、韓国は多面的な取組みを実施した。例えば、政府は2010年にサイバー司令部を新たに設立し、各大学のサイバーセキュリティ関連学科を国として支援し、さらに学生への啓発教育を行い、「サイバーセキュリティ・マスタープラン」を発表した。しかし、その後も専門家によりさらなる対策強化が唱えられ、北朝鮮によるサイバー攻撃に相対するための多面的アプローチが提案された。かかる状況の下、実務者と研究者はその喫緊性を示し続け、韓国における堅牢なサイバー防衛態勢の基盤構築に向けた推進力強化が図られた。しかし、政府やオピニオンリーダーらによる取組みにも関わらず、その態勢は依然として断片的かつ非常に複雑化した様態にある。また、反サイバーテロ態勢強化に資する政治的支援に一貫性が存在しておらず、国際的な連携の取組みは今次ようやく起ち上がりつつあるところである。さらに、一般市民はサイバースペースに制限や規制を課すよりもプライバシーを尊重する傾向にある。その一方で、北朝鮮はこれらの難題を超克することで、常にその目標の達成に挑んでいる。様々な要因により、北朝鮮のサイバー脅威に対抗する韓国の態勢の現状は多くの脆弱性を孕んでいるのである。2013年のブー（Boo）他による研究では反テロ態勢の現状を明らかにする試みがなされており、専門家へのデルファイ調査の結果が示されている。図4のとおり、技術基盤およ

び脅威評価の正確性に関わる評価点は概ね良好であったが、その他の要素は平均以下であると評されている。

図４　サイバー脅威に対する韓国の準備態勢に関する専門家へのデルファイ調査の結果



出典：Boo, Hyeong-wook *et. al.*. 2013. *A Study on Future Direction of Defense Cyber Policy*. KIDA report (in Korean). p. 19

技術基盤、脅威評価の正確性の評価点が比較的高位であるにも関わらず、目標共有、組織的手順、洗練度における評価点が低いことから、韓国におけるサイバー脅威対応の順応性を高めることは困難であると予示される。他方、脅威評価において不備があったと主張する専門家もある。かかる専門家は、韓国は北朝鮮によりもたらされるサイバー脅威を再評価する必要があると主張している。一般的に韓国政府による脅威評価は概して正確な評価であると認識されていることから、これは多少の意外性を有する見解である。しかし、ハン・ヒ（Han, Hee）のような研究者は、韓国 MND は北朝鮮の隠れた潜在的なサイバー戦能力に対して危機意識を持つ必要があるという議論を展開している。ハン博士は、MND

内には6,800人のハッカーを北朝鮮のサイバー脅威の総体として認識している傾向があると主張している。また、MNDによるこの認識は否定されるべきであり、MNDはその「壁」の向こう側に存在する潜在能力こそを重要視する必要があるとも述べている。北朝鮮ハッカーが数千、さらに数百万台を超えるゾンビPCを隷下にしている事実がある以上、その能力は単に北朝鮮ハッカーの人数に還元されるものではない。ハッカーは僅か数回のクリック動作によって、世界中で一斉にサイバー攻撃を仕掛けることが可能である。かかる観点から、博士は、北朝鮮のサイバー戦力に関する認識を6,800人のサイバー兵士、ゾンビPC、そしてウェブ内で裏工作を図るマルウェアの「混合体」であるという新たな見解に切り替える必要がある旨を主張している。

またハン博士は、韓国のサイバーセキュリティ政策団体は北朝鮮に欺かれているという事実を認識することが重要であると述べている。北朝鮮は初期的なサイバー技術を具備しているように自らの偽装を図っている。北朝鮮が、自らのサイバー攻撃に対処する韓国社会および軍による対抗能力を試すことを目的としていることから、まずは初期的攻撃技術を用いたサイバー攻撃を敢行したと見る専門家もある。つまり、現状において北朝鮮の目的は欺くことであり、最悪のシナリオはまだ実行されていないと論じることも可能である。実際のサイバー交戦に到る遂行オペレーションを考慮すれば、その見解は正しいと言える。サイバー兵器、マルウェアは一旦公開されると、そのアイテムからはサイバー兵器、マルウェアとしての存在価値が損失する。これはセキュリティ対策者によってこれらの解析が行われ、無効化させる対処法が発見されるためである。さらにセキュリティ対策者は、対抗手段を開発し、対策としてその提供を実施するであろう。したがって、北朝鮮にとって最も有効かつ強力なサイバー兵器は実際にはまだ使用されていないというのが当然の結論であろう。

V. 結論

在韓米軍（USFK）の司令官に就任したブルックス（Brooks）陸軍大将は、北朝鮮のサイバー脅威は世界一ではないとしても、最もよく組織化された優れた

サイバー戦力を配備している国のひとつである旨を述べている[16]。かかる戦力を使用し、北朝鮮は韓国、そして世界に向けた重大なサイバー攻撃を展開し続けている。金正恩時代においては、事実サイバー攻撃事案の増加が確認されている。その攻撃には高度な技術が運用されており、同時にサイバー作戦の目的は無作為な情報の窃取から韓国の重大インフラに対する計画的かつ巧妙に仕組まれた攻撃へ推移していると見られている。さらに北朝鮮のサイバー兵士は多くの SNS サイトに登録し、世論を操ることで、韓国社会内での意見の相違衝突を煽動しようと企てている。これは心理戦争を行う行動として捉えることもできる。また、近年、北朝鮮はサイバー能力を外貨獲得のための手段として使用し、自国に望ましい成果を得ている。

約 60年間、北朝鮮と韓国の軍拡競争は従来の兵器体系の範囲内で行われてきた。すなわち、軍部は戦車、大砲、戦闘機、駆逐艦、潜水艦等の獲得に傾注していた。しかし2010年代に入り事態は急変した。北朝鮮は核兵器やその他の WMD を開発し、これにより朝鮮半島内の軍事的均衡に変化がもたらされた。従来の兵器体系を近代化する重要性は、WMD を前にしてその存在意義を失いつつある。また、北朝鮮のもう一つの戦略的動向活動はサイバー分野で図られている。WMD、そしてサイバー兵器の開発は非対称戦略の開始と捉えられるものである。

本稿において、北朝鮮によるサイバー攻撃事案に関する分析を行い、同国のサイバー能力に関わる過去の事例研究の結果をまとめた。さらに韓国の対応、その対応の努力から習得された教訓に対する評価を行った。かかる問題に対する議論を図った上、北朝鮮のサイバー脅威に対し真摯に留意を払うべきものとの結論付けを行うことが可能となる。サイバー兵器は安価であるが、ネットワークに依存する韓国に重大な脅威をもたらすものである。最悪のシナリオはまだ実現には至っていない。したがって研究者や実務者は想定外の事態を考慮し、政府、軍部に

[16] ブルックス陸軍大将は 2016 年 4 月、連合軍司令官として指名を受けた米上院聴聞会でこれらの見解を述べた。(http://news.chosun.com/site/data/html_dir/2016/04/20/2016042002453.html ; retrieved on Aug. 25. 2016)

その分析結果を提供していくことが望まれる。

参考文献

Baek, Seung-koo. 2015. Evolving North Korean Cyber Terrorism. *Monthly Chosun*. (https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=201509100013 accessed 2016. 7. 23)

Boo, Hyeong-wook and Choi, Suon. 2014. Crisis Pattern Change and Its Implication for National Crisis Management System. *Journal of Defense Policy Studies*. Vol. 30. No. 1.

Boo, Hyeong-wook and Lee, Kang-kyu. 2012. Cyber War and Policy Suggestions for South Korean Planners. *International Journal of Korean Unification Studies*, Vol. 21, No. 2.

Boo, Hyeong-wook *et. al.*. 2013. *A Study on Future Direction of Defense Cyber Policy*. KIDA report (in Korean).

Boo, Hyeong-wook. 2013. Issues of Cyber Security and Policy Directions: Discussions for the Establishment of Defense Ministry's Cyber Policy (in Korean), *Journal of National Defense Studies*. Vol. 56, No. 2.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. ECC 2010

Coleman, K. 2010. The Weaponry and Strategies of Digital Conflict, in Armstead, E. L (eds.). *The Proceedings of the 5th International Conference on Information Warfare and Security*, (The Air Force Institute of Technology, Ohio; 2010)

Comfort, L. K. 2002. Rethinking Security: Organizational Fragility in Extreme Events. *Public Administration Review.* pp. 98-107.

Deibert, Ronald. "Militarizing Cyberspace", *Technological Review*, (Boston, MA: MIT, 2010), (http://www.technologyreview.com/notebook/419458/militarizing-cyberspace; retrieved Aug 25, 2016)

Dennis C. Blair. 2010. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence.

Han, Hee. 2016. *Cyber threat by North Korea: capability and intention*. Paper presented at The 6th RINSA-KAS Joint International Conference.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* (Santa Monica, CA: RAND)

Mahnken, Thomas G. 2011. Cyberwar and Cyber Warfare in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age Vol. II* (Washington, DC: Center for a New American Security). pp. 55-64.

Manjikian, Mary McEvoy. 2010. From Global Village to Virtual battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly.* Vol 54. Issue 2. pp. 381-401.

Nye, Joseph S. Jr. 2011. Power and National Security in Cyberspace. in Kristin M. Lord and Travis Sharp (eds.) *America's Cyber Future: Security and Prosperity in the Information Age Vol.II.* (Washington, DC: Center for a New American Security). pp. 5-23.

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke. 2011. On Cyber Warfare. *A Chatham House Report*

Singer, Peter W. and Noah Schactman. 2011. *The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive*. Brookings Institute. (http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman; retrieved Aug 25, 2016)

Thomas G. Mahnken. 2011. Cyberwar and Cyber Warfare. in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age Vol.II.* (Washington, DC: Center for a New American Security)