特別研究

侮れなくなった北朝鮮のサイバー戦能力

政策提言委員・軍事／情報戦略研究所長　西村金一

北朝鮮軍は現在、核兵器や弾道ミサイル開発に努力を集中させている。旧式兵器を近代化するために、韓国の半分の地域にロケット弾を打ち込むことができる300ミリ多連装砲や首都平壌を空からの攻撃から守るS-300新型防空ミサイルなどの新型兵器を導入しているものの、軍全体の近代化と軍事力増強には程遠く、特に海空軍については、韓国軍との格差は広がるばかりである。

1991年の湾岸戦争や2003年のイラク戦争では、近代兵器に熟知しているつもりであった我々でさえも、テレビ画面に映る精密誘導兵器が数百キロ離れた海域から、正確に目標の建物に命中する凄さに大きな衝撃を受けた。近代兵器を保有していない北朝鮮軍の高級将校は、画面に映ったような攻撃を自分達も受けるかも知れないという大きな不安と恐怖を受けたに違いない。北朝鮮軍は当時、軍事的対応策を速やかに検討し、新たな作戦戦略を立案、実戦に向けて試行し始めた。北朝鮮はこの時、韓国を軍事力で統一する国家目標はそのままで、膨大な近代兵器を保有する米軍には、勝つのではなく、負けない戦略に転換したのではないかと思われる。

近代的な兵器を中国やロシアから購入するには、膨大な費用が必要であり、兵器の近代化は、ほんの一部だけを達成したに過ぎなかった。そこで、近代的兵器の劣勢を補うために、比較的経費が少なくて効果が大きいサイバー戦に力を注ぎ始めた。

金正恩委員長は、「サイバー戦は、核・ミサイルと並ぶほどの軍事力であり万能の宝剣だ」と述べ、軍事情報の入手の他に、相手国の軍事機能や経済機能を混乱させ、資金の入手のために使用し始めた。

当初、北朝鮮によるこれらの攻撃は、低レベルであったことや韓国の対策により大きな被害は出ていなかった。しかし、近年、北朝鮮はサイバーテロや電波妨害を実行する組織を拡大し人員を増加させた。そして、韓国、米国国内の企業、東南アジアの銀行、日本などの原発などにサイバー攻撃をかけ、情報やお金を盗み取る成果を、それは限られたものではあるが、挙げられるようになった。

以下、①北朝鮮によるサイバー戦の変遷　②北朝鮮のサイバー戦能力と北朝鮮のネット事情　③北朝鮮サイバー戦能力の評価―の順に分析し、説明する。

但し、サイバー戦の実態については、

攻撃をする側も攻撃を受けた側も、その実態を明らかにしない。また、それらの情報の一部だけしか、明らかにされることはない。時には、誤情報や意図的に歪められた情報が流されることもある。そのため、私としても、情報収集に限界がある中で、信頼性が高い情報源から北朝鮮に関するサイバー戦について収集し、積み重ね、分析を行ったものである。

1　北朝鮮によるサイバー戦の変遷

（1）韓国へのサイバー攻撃

2009年7月、韓国でウイルス対策ソフトを主に研究する「安哲秀研究所」によると、韓国政府機関及び銀行などが大規模なハッカー攻撃を受け、サイトがアクセス不能になるなどの被害が出た。内部の情報を盗まれた形跡はなかったが、ウイルス攻撃と膨大な量のアクセスにより何千台ものコンピューターのサーバーが飽和状態となって停止し、ウェブサイトは攻撃を受けてから4日間も影響を受け続けた。韓国国家情報院は、その攻撃が周到に準備されていることや組織的であったことから、個人によって行われたものではなく、その背後に北朝鮮の某機関、或いは北朝鮮軍が介在していることに言及した。更に、韓国内部にも北朝鮮のサイバーテロを支援する者がいたことも明らかにした。

2011年3月、大統領府や国防省を含む政府機関、在韓米軍、大手ポータルサイトや都市銀行など計40のウェブサイトが大規模なハッカー攻撃を受けた。韓国警察は、経路分析などから北朝鮮が攻撃したものと特定した。

同年4月、韓国農業銀行共同組合"Nonghyup"の電算処理ネットワークシステムがダウンした。約300台のサーバーが機能停止し、数百万人の利用者が現金自動預払機での現金取り扱いができなくなったほか、送金などの支払いが滞るという混乱が起きた。捜査の結果、サイバー攻撃ツールは、北朝鮮発信源の「DDoS」攻撃（大量のメールを1つのツールに送信することにより、そのツールの機能を停止させる攻撃）として知られる基本的なツールであった。感染原因は、北朝鮮のサイバー部隊がばら撒いたハッキング攻撃用のウイルスが、農協のシステムを管理していた韓国IBM社員のパソコンに侵入したことで起こったものあり、発信源は、北朝鮮の工作機関である偵察総局が中国に設置した拠点からだと断定された。ウイルスソフトで有名なMcAfee社のGeorg Wicherski氏は、分析の結果、「これらのサイバーテロは莫大な損失を与えてはいるが単純な手段だ」と説明している。

金正恩が後継者となった翌年の2012年6月、韓国中央日報の新聞製作電子システムがサイバー攻撃を受けた。ニュースサイトに手で口元を押さえて笑う猫の写真と「イズワンがハッキングした」とのメッセージが表示（写真参照）され、閲覧できなくなった。北朝鮮軍総参謀部はサイバー攻撃前に、金正恩第1書記（当時）を侮辱する報道を行ったとして、中央日報などの韓国メディアを名指しで非難、「謝罪しなければ聖戦を実施する」と通告していた。このことから、「北朝鮮、或いは北朝鮮の指示を受けた韓国ハッカーによるサイバーテロの可能性が考えられる」と中央日報は判断している。

これらのサイバー攻撃について、「中央日報サーバーに対する攻撃は、一般的なハッキングの次元を越えた強力かつ悪意ある手法」と考えられている。また、ハッカーは、読者情報が入ったサーバーには手を付けず、新聞を制作するのに必要な情報が入ったサーバーをターゲットにした。この攻撃は、単純なハッキング或いは「DDos」攻撃ではなく、深刻なクラッキング（悪意を持って不正に侵入し、コンピューターシステムを破壊・改竄する）水準に到達したものと評価されている。

中央日報 HP がハッキングされた直後の写真

出典：中央日報日本語版 2012 年 6 月 11 日

2013 年 3 月、韓国では、ハッキングで金融機関や放送局が襲われ、コンピューター約 4 万 8,000 台が被害を受けた。韓国軍もサイバー攻撃を受け、化学物質の貯蔵所など重要情報数千件を流出させられた。この時、被害を受けた組織のサーバーにアクセスした中に中国の IP アドレス（インターネットに接続された機器が持つ番号）が特定された。

韓国国家情報院によると 2014 年 5 月から 9 月までの間、北朝鮮のハッカー集団が、韓国のネット上にゲームに偽装したウイルスを設置した。これによって 2 万台以上のスマートフォンがコンピューターウイルスに感染し、ハッキングされた。

2010 年～ 2014 年 9 月までに、韓国の公共機関へのサイバー攻撃件数は 7 万 5,473 件に達しており、その多くは外国のネット回線を介している。

2016 年 2 月、北朝鮮が韓国の大企業や公共機関、官公庁に大規模なサイバー攻撃を仕掛け、軍事情報を含む約 4 万 2 千余りの文書を不正に抜き取っていたことが分かった。攻撃を受けたのは 160 カ所余りで、抜き出された情報には、軍の情報網関連の資料や在韓米軍の F-15 戦闘機の翼の設計図、無人偵察機の部品の写真など、防衛産業に関した資料も多数含まれている。

韓国国家情報院によると、北朝鮮は同時期に、韓国政府要人数十人のスマートフォンにサイバー攻撃を仕掛け、交信内容を盗聴するとともに、連絡先やショートメールも盗み取っていた。

韓国の KBS テレビは 2017 年 5 月 3 日、北朝鮮が韓国軍の内部ネットワークにハッキングし、朝鮮戦争が全面再開された際に適用される米韓軍の最高機密の軍事作戦「作戦計画 5027」を流出させた、と伝えた。

（2）韓国以外への国へのサイバー攻撃

2013 年 11 月、脱北者団体「NK 知識人連帯」キム・ファングン代表は、北朝鮮は 11 月上旬頃から、日本の政府機関などを狙う対日サイバー部隊が本格的な活動を開始し、「サイバー戦争を日本列島まで広げろ」との上層部の指示があったことを明らかにした。その

直後、2013年12月～2014年1月にかけて、日本の高速増殖炉「もんじゅ」のデータが盗まれた。実行したのは、北朝鮮偵察総局隷下の「ユニット91」と言われている。

2014年12月、「ラザルス」と呼ばれるハッカー集団が、米国のソニー・ピクチャーズエンタテインメントに対するサイバー攻撃を行った。ソニー・ピクチャーズの個人情報、従業員の間の電子メールなどの情報が盗まれた。米連邦捜査局（FBI）が既に北朝鮮の犯行だと断定している。

2017年5月、米情報セキュリティー会社「シマンテック」の幹部は、北朝鮮がバングラデシュ中央銀行にサイバー攻撃を仕掛け、8,100万ドル（約92億円）を盗んだ疑いがあると伝えた。攻撃が起きたのは2016年2月。バングラデシュ銀行が米ニューヨーク連邦準備銀行に持つ口座から、9億5,100万ドル（約1,084億円）の不正送金が試みられた。送金の大半は阻止されたが、8,100万ドルはフィリピンの口座への送金が成功し、その後、金の行方は現在も分かっていない。この窃盗事件は、史上最大のサーバー窃盗だとも酷評されている。この事件は、2014年のソニー・ピクチャーズへのサイバー攻撃を行ったとされる「ラザルス」と呼ばれるハッカー集団と関連があるとされている。

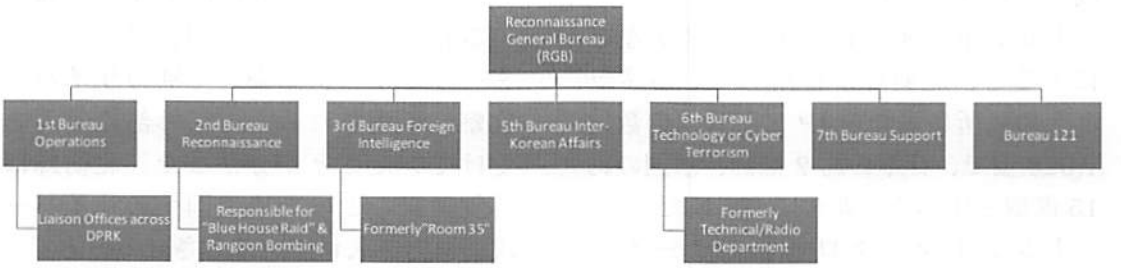
ニューヨーク・タイムズ（2017年3月）によると、2016年10月頃、北朝鮮と関係するハッカーがポーランドの複数の銀行にサイバー攻撃をかけ、世界100以上の企業・団体の口座から資金を盗もうとした。攻撃は昨年10月頃から始まり、ウイルスをポーランド金融規制当局のウェブサイトに仕込ませ、アクセスした銀行が誤ってダウンロードするのを待つ手口が使われた。「ウオーター・ホール・アタック（水飲み場型攻撃）」と呼ばれるもので、水飲み場に集まる獲物を待ち伏せする方法から名付けられたものだ。このような資金集めの攻撃部隊は、偵察総局隷下の「第180部隊」だと指摘されている。

このサイバー攻撃に使われたウイルスは、2016年10月のフィリピンの銀行への攻撃や、12月にベトナムの銀行にSWIFT経由で100万ドルの偽の送金指示があった事件でも用いられたとしている。また2017年1月には、エクアドルの銀行もSWIFT経由の送金指示で1,200万ドルを盗まれたが、ウイルスなどの詳細は分かっていない。

2017年5月、世界約150ヵ国、30万台以上に身代金要求型ウイルス（ランサムウエア）による攻撃が行われた。米シマンテックなどのセキュリティー会社は、北朝鮮の犯行ではないかという分析をしている。ハッカーはウイルスに感染したパソコンの文書や写真を暗号化し、それを解除する費用として300～600ドル相当の仮想通過ビットコインを要求した。これらの攻撃で約7万ドル（約791億円）がハッカーに渡ったが、データの復旧には全く応じていない。

2017年5月、北朝鮮の制裁決議違反を調査している国連安保理事会制裁委員会の複数の専門家委員に対し、継続的なハッキングが行われていることが判明した。このハッカーは、調査委員会の活動や組織について十分熟知している者で、北朝鮮の仕業と考えるのであるが、委員会は北朝鮮とは言及していない。

図１　偵察総局各組織と 121 局（2013 年以降）



出典：RGB organizational chart, compiled with information from The Korea Herald, 38 North, and CSIS.（2017 年 6 月 15 日）

２．北朝鮮のサイバー戦能力と北朝鮮のネット事情

（１）北朝鮮のサイバー戦能力

北朝鮮サイバー戦士の育成が進んでいる。美林（ミリム）大学卒業の脱北者は「北朝鮮は 1986 年、平壌に美林大学（自動化大学その後金一軍事大学）を設立し、本格的にサイバー戦の準備を行うとともに、フルンゼ軍事大学出身のロシア人教授 25 人を招き講義を行い、毎年 100 人から 110 人のハッカー要員を養成。鴨緑江軍事技術大学や国防大学、空軍大学、海軍大学などでも教育を実施している」と語った。

韓国軍は 2006 年の報告書で、「北朝鮮ハッカー部隊が、米軍太平洋司令部の指揮統制所を麻痺させ、米国本土のコンピューターネットワークにも被害を及ぼす能力を保有し、特に約 1,000 人規模のサイバー攻撃組織を保有している」と評価している。

前述のキム・フングァン代表は、「北朝鮮は 2010 年、偵察総局が率いるサイバー部隊、121 所を 121 局（サイバー戦指導局）に昇格させ、部隊の規模を約 3,000 人に増加させた」とも報告している。（図１参照）

韓国国防省は 2012 年に、北朝鮮は総勢約 1,700 人のハッカー専門部隊とエンジニア 4,200 人が側面支援する約 6,000 人体制になったことを明らかにした。これらの戦士が海外で活動しているのである。

（２）北朝鮮のネット事情

北朝鮮は要員養成や組織拡大を行ってはいるが、国内でのインターネット環境は、CIA THE WORLD FACEBOOK の各国インターネットホスト数比較（2010 年）によると、日本が２番目で 5,500 万台、中国が６番目で 1,500 万台、北朝鮮は 230 番目で僅か３台のみであった。

北朝鮮は要員を育成し組織を拡大しているが、国内からインターネットに自由にアクセスしてサイバーテロを実施できる環境にはない。そのため北朝鮮は、中国の丹東や大連などの中国東北部及び東南アジアに、北朝鮮サイバー攻撃組織の主な活動拠点を置きその地を発信源としてサイバーテロを実施していると見られている。ジェームズ・A・ルイス氏は "The North Korean Cyber Menace" において、韓国国内でもアウトソーシングにより北朝鮮のサイバー

テロのために働く韓国人ハッカーを養成していると報告している。

トレンドマイクロや米メディアなどによると、北朝鮮が使用しているネット上の住所に当たるIPアドレスの数は1,024個で、日本の約2億個、米国の約15億個と比べると非常に小規模だ。

トレンドマイクロ社研究チームがGeoIPとWhois情報を元にまとめた北朝鮮インターネット事情を要約すると、北朝鮮は、2013年から、合計1,024個のIPアドレスを持ち、中国のプロバイダを介してインターネットにつながっている。2017年10月1日以降は、同じIPアドレスに対してロシアのプロバイダが別経路のインターネット接続を提供している。北朝鮮が使用しているサーバーが設置されている国とIPアドレス個数は、北朝鮮の1,024個、中国の256個、チェコの8個、オランダの5個、ロシアの256個、米国の128個、ルクセンブルクの16個、不明国の8,448個で合計10,141個である。そのうち北朝鮮にあるのは1,024個だけで全体の10%、海外は90%であり、そのうち所在する国が不明なのが83%である。つまり、北朝鮮は海外、それもどの国にあるのか分からないように設定して、サーバーとIPアドレスを使用し、サイバー攻撃を仕掛けている。北朝鮮はインターネットを不正に使用し、サイバー戦実行態勢になっていると言っても過言ではない。

米国防省の議会報告によると、北朝鮮は「自国ネットワークがインターネットとほぼ切り離されていて、報復攻撃を受けるリスクが殆どない」と言及されている。だが、情報セキュリティー会社が昨年、ネットを通じて北朝鮮で送受信されている情報の流れなどを調査した結果、北朝鮮国内で使用されている相当数のパソコンが、コンピューターウイルスに感染して別のサイバー攻撃に悪用されるなど、外部の侵入を受けていたことが分かった。北朝鮮は外貨獲得などのため他国へのサイバー攻撃に力を入れているとされる一方で、セキュリティーが不十分なフリーメールサービスが公共機関で利用されていることも判明、ネット環境を巡るお粗末さや、守りの弱さが浮き彫りになった。

北朝鮮の一部在外大使館では、無料で手軽に使えるものの、IDとパスワードを盗まれると内容を覗き見される恐れがある「Gmail」や「Hot mail」などのメールサービスが利用されていることも分かった。

具体的には、北朝鮮から送信された迷惑メールの一部は、遠隔操作ウイルスに感染したパソコンから送られており、外国のハッカーなど外部から指示を受け、発信元の偽装のため"踏み台"にされていた。調査期間中だけで少なくとも約30種類以上の迷惑メールが送信されていた。中には1年以上もウイルスに感染したまま放置されていたパソコンもあった。

韓国国家保安技術研究所等によると、サイバー戦士の多くは、金策工業総合大学出身だとの情報もある。彼らは、偵察総局隷下の電子偵察局に所属しており、所在を特定されないためや追跡を避けるため、中国、マレーシア、インドネシア、カンボジアのIT企業に派遣されている。そして、平壌からの指令を受けて、その地点から韓国のサイトを攻撃している。

例えば、原発、都市ガス、変電所、

浄化場、地下鉄、鉄道関連施設などだ。韓国政府などの分析によると、過去のサイバー攻撃では、攻撃元のIPアドレスが中国にあることが確認されている。それらの拠点は、3～6人を1組とするユニットを単位として構成されている。この場合、貿易会社の海外支社や中国や東南アジア諸国との合弁会社を装っている。

そのため、米国は大量のデータを送りつけて相手のシステムを麻痺させる「DDos攻撃」などが有効と判断。2017年春から9月末にかけて実際に攻撃を行い、北朝鮮におけるネット接続の封じ込めを図ったが、思うような成果は上がらなかった。攻撃の効果が限定的だった背景には、殆どが他国である中国の回線を経由していたという北朝鮮の複雑なネット事情があるという。

更に北朝鮮は10月からロシア国営の通信事業会社からも接続サービスを受け始め、ネットインフラで中露両国から支援を得る形となった。北朝鮮からすれば、ネットインフラの依存先を複数に分散させることで、リスク低減にもつながるとみられる。

専門家の間では「これで遮断はより困難になった。接続回線が増えればサイバー攻撃の能力も向上する」との声が上がっている。

元陸上自衛隊通信学校長田中達浩氏（産経ニュース電子版）によると、北朝鮮のサイバー部隊の人員数は現在約6,800人で、約3千人態勢とされた2013年頃から倍以上に増えた。また、田中氏は「サイバー部隊が約2,900人とされる韓国の倍以上」と指摘した上で「万単位の人員がいると言われるロシアや中国より少ないが、国全体の人口を考えると金正恩がサイバー部隊を急速に強化させていることは明白だ」と分析した。

また、「北朝鮮ではサイバー部隊に入れば昇進が早い上、給与も高く、高級マンションも提供される。ハッカーを目指す若者のハングリー精神は凄まじい」と話した。

その上で、北朝鮮の現在のサイバー部隊について「実力面でいうと、米、中、露、イスラエルに続き5位（7位という情報もある）」と指摘した。

3．北朝鮮サイバー戦能力の評価

北朝鮮の2012年までのサイバー攻撃ツールは、「DDoS」の基本的なものであった。だが2013年には、攻撃目標に侵入してサーバーから情報を盗み破壊するクラッキングのレベルに達したものと見られている。これまでは韓国の民間企業だけが攻撃対象となっていた。2014年12月には、攻撃対象を米国企業に向け、コンピューターの機能を麻痺させることができることを証明した。近い将来には、韓国や日本の端末器を利用したサイバー攻撃により、これらの国が発信源となり、コンピューターから軍事情報等を盗んだり、サーバーを破壊したりしてくる可能性がある。

韓国国防省は2011年、北朝鮮のサイバーテロの動向に対して、サイバー司令部の組織と機能を強化することと、その規模を2011年現在で約500人規模のものを倍増する方針を決定するなどの対策を採っている。また、韓国政府は、6名の最精鋭ハッカーを選抜し、海外で専門教育を受けさせた後、韓国国家情報院、警察庁及び情報機関に配置するとしている。

サイバー攻撃と言えば、日本は、中国軍からの攻撃を警戒していればよかったが、これからは、中国東北部の拠点からとは言え、北朝鮮も警戒する必要性が出てきたことを改めて認識する必要がある。

北朝鮮は有事に、米国・韓国・日本に何をしてくるのか。北朝鮮が南進する時には、韓国、日本、米国の軍事施設にサイバー攻撃を行うだろう。例えば、首相官邸、軍・自衛隊の司令部などを攻撃し、指揮機能を麻痺させ、ミサイル防衛システムやイージス艦巡航ミサイルの機能を停止させる。即ち、平時には何もしないでどこかに潜んでいるハッカーが、韓国攻撃などの時には一斉に攻撃を仕掛けることになる。そうなれば、国家や軍の機能は破壊され、ストップすることになるかも知れない。

北朝鮮の核・ミサイル攻撃の脅威に対応するために、重層的なミサイル防衛や敵地攻撃能力が必要ではあるが、これと並行的に実行されることが予想されるサイバー戦への対処も怠ってはいけない。

《参考文献等》
・"North Korean Cyber Capabilities: In Brief" Every CRS Report (August 3, 2017)
・Insikt Group "North Korea Is Not Crazy" Intent is critical to comprehending North Korean cyber activity (June 15, 2017)
・http://blog.trendmicro.co.jp/archives/16218
・デイリーNK ジャパン

北朝鮮との「同化」を目指す韓国・文在寅政権 朝鮮戦争再開時、韓国軍は参戦するのか？

政策提言委員・産経新聞政治部専門委員　野口裕之

本誌が読者に届く頃、朝鮮半島情勢がどうなっているかは、北朝鮮・朝鮮労働党の金正恩委員長が核・ミサイル開発を放棄するか否かにかかっている。しかし、金氏に放棄の意志は全くない。金氏が核・ミサイル放棄を実行しない限り、筆者は朝鮮戦争再開は不可避だと、2016年晩秋から主張し続けてきた。

折しも、韓国を訪問した米国のドナルド・トランプ大統領は2017年11月7日、在韓米軍基地を訪問し、在韓米軍司令官のヴィンセント・ブルックス陸軍大将のブリーフィングを受けたが、日韓軍事筋は筆者に「軍事オプションの説明だった」と明かした。2,000名もの在沖縄海兵隊員も既に韓国に展開済みで、朝鮮半島情勢は刻々とキナ臭くなっている。