北朝鮮のサイバー攻撃とＧＰＳ妨害 2012

2012 年 12 月

軍事アナリスト　西村　金一

北朝鮮では､2011 年 12 月に金正日総書記が死去し､その後金正恩がその後継者となった。国家の指導者が交代してからも、北朝鮮軍は、核兵器や弾道ミサイルの開発を継続するとともに、旧式兵器を近代化するための努力を行っている。また、これらと並行して軍事的対応策を検討し、新たな作戦戦略の運用に努めている。これはイラク戦争やアフガン戦争における精密誘導兵器の威力に大きな衝撃を受けたからである。

特に力を入れているのが比較的経費が少なくて効果が大きいサイバー攻撃や GPS 機能妨害である。2009 年頃から韓国政府機関等へのサイバー攻撃や韓国北西部において GPS 等への妨害を始め、2012 年まで毎年実施し、妨害の頻度や規模も拡大している。

北朝鮮によるとみられるこれらの攻撃はこれまで比較的低レベルにあったが、2011～2012 年からは影響が出ている。北朝鮮は近年、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ていることから、今後も規模を拡大し、高度なサイバーテロや GPS 機能の妨害を行ってくることが予想される。

１　北朝鮮によるサイバー攻撃

（１）北朝鮮サイバー攻撃の現状

韓国でウィルス対策ソフトを主に研究する「安哲秀研究所」によると、2009 年 7 月、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を受けた。内部の情報を盗まれた形跡はなかったが、何千台ものコンピューターがウィルス攻撃と膨大な量のアクセスにより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かあるいは北朝鮮軍が介在していることに言及した。さらに、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[1]。

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り混乱が起きた。経済的な損失は莫大であった。

---

[1] 「韓国で大規模ハッカー攻撃政府機関や在韓米軍狙う　甚大な被害、北関与か」『共同通信』2011.03.04

捜査の結果、サイバー攻撃ツールは、北朝鮮発信源の「DDoS」として知られる基本的なツールであり[2]、感染原因は、北朝鮮のサイバー部隊がばらまいたハッキング攻撃用のウィルスが、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[3]。ウィ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[4]している。

2012 年 6 月、韓国中央日報の新聞製作電算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」(Hacked By Iaone) とのメッセージが表示され、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、北朝鮮ある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[5]。

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つけず、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。これらは、単純なハッキングあるいは DDos 攻撃ではなく、深刻なクラッキング水準に到達したものと評価されている[6]。

（2）北朝鮮サイバー攻撃の能力

美林大学卒業の脱北者は「北朝鮮は 1986 年、美林大学（現・自動化大学）を平壌に設立し、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していた。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[7]。

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 1000 人規模のサイバー攻撃組織を保有している」[8]と評価している。

脱北者団体「NK 知識人連帯」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 3000 人に増加させた」とも報告している。

北朝鮮は要員要請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

---

[2] Giles Turnbull “North Korea Accused of Cyber Terror”　May 3, 2011

[3] 「北のサイバー攻撃活発化　軍事政治両面で韓国狙う」『朝鮮日報日本語版』2011.5.8

[4] “Suspected North Korean cyberattack on a bank raises fears for S. Korea” allies washingtonpost.com/world　Aug 7, 2011

[5] 「韓国報道機関のサーバーを攻撃…北朝鮮のテロ？」『韓国中央日報』2012.06.11

[6] 「報道機関サイバー攻撃＞ＤＤｏＳとは次元が違う悪意的手法＝韓国」『韓国中央日報』2012.06.15

[7] 「CIA 顔負けの北朝鮮ハッカー部隊」『朝鮮日報日本語版』2011.05.04

[8] 同上

5,500 万台、中国が 6 番目で 1,500 万台、北朝鮮は 230 番目でわずか 3 台のみである。

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、これらと並行して韓国国内で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。

（３）北朝鮮サイバー攻撃の評価

北朝鮮の昨年までのサイバー攻撃ツールは、「DDoS」の基本的なものであり、攻撃目標に侵入してサーバーから情報を盗み破壊するレベルには至っていなかった。だが 2012 年にクラッキングのレベルに達したものとみられている。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、また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みまたサーバーを破壊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、2012 年 7 月 3 日付けの韓国紙東亜日報によると、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。

２　北朝鮮によるＧＰＳ（衛星利用測位システム）機能妨害

（１）北朝鮮による妨害の状況

近代戦においては、GPS が兵器及び敵の位置を正確に測定することにより、戦場を無人化するなど戦争形態を大きく変化させている。例えば無人偵察機が自己位置と敵の位置を正確に測定し、目標に移動し、指示された目標を映す。その映像をもとに、戦場から遠く離れた射撃指揮所にいる担当将校が、目標を選定・射撃を判断し、射撃の実行を命ずることができる。パイロットが戦場にいる必要がなくなってきつつあるのである。北朝鮮は、イラク戦争やアフガン戦争を見て正確なミサイル攻撃や無人機による攻撃に衝撃を受けた。その一方で、これらの近代的な戦いにおいて、如何に戦うかを研究したことが伝えられている。正確なミサイル攻撃や無人機による攻撃は、ミサイルや無人機の自己位置と目標の位置を正確に測定することが必要になる。位置を測定して、位置を決定する兵器に使用されるのが GPS である。

そのため、北朝鮮軍は GPS の機能を妨害することを軍事戦略として選定し、妨害兵器を製造、実際に韓国の GPS 装置を妨害しその効果を確認しつつ開発している模様である。

2010 年 10 月、金泰栄国防相（当時）は韓国西部の黄海で同８月に軍や漁船が使う GPS に障害が生じたことについて、北朝鮮が電波による GPS 機能妨害を行ったとの見方を示した。

2011 年 3 月、韓国政府や軍関係者は、軍事境界線に近い北朝鮮の開城や海州の軍部隊及び金剛山から妨害電波が、5～10 分間隔で発せられ、ソウルや仁川など韓国北西部で携帯電話の GPS の機能が一時使用できなくなる事態になったと述べた。

2012 年 4 から 5 月にかけて、韓国国土海洋省は、仁川国際空港とソウルの金浦空港を発着する民間航空機約 670 機及び黄海の船舶約 120 隻が利用する衛星利用測位システム（ＧＰＳ）に、障害が発生したことを発表した[9]。

具体的事例では、12 年 4 月 29 日に仁川空港に着陸しようとしたジンエアー機の対地接近警報装置（GPWS）が誤作動を起こし、突然警報が作動した。また、同年 5 月 10 日、ソウル近郊の仁川で、無人ヘリコプター１機が試験飛行中に制御不能となって墜落した。韓国軍は北朝鮮の妨害電波によって発生している衛星利用測位システム(GPS)障害が原因の可能性があるとみている。韓国 KBS によると、北朝鮮の妨害により、韓国軍の武器システムに損失は与えなかったものの、事実上韓国の国産武器の 7 割は妨害電波への対抗能力が弱まっている。

韓国は、電波発信源の標定と信号分析の結果、発信位置は北朝鮮の開城であると特定している。また、韓国政府は 2012 年 5 月、国際電気通信連合(ITU)や国際民間航空機関(ICAO)などを通じ、北朝鮮に対して GPS 妨害について抗議する方針を示した。

（２）北朝鮮電子戦部隊の能力

韓国の国会国防委員会報告「北朝鮮の電子戦攻撃・かく乱武器」(2011 年 9 月）には、「北朝鮮が最近独自に開発している新型の電子戦攻撃装備の中に、妨害できる距離が 100 キロ以上に達する GPS かく乱装置が含まれていることを把握した」また「北朝鮮は 2000 年代前半にロシアから入手した車載型の電波妨害装置（妨害可能な距離は 50‐100 キロ）を軍事境界線（MDL）付近の 2‐3 カ所に配置し、GPS への電波妨害（ジャミング）に使用してきた」と記されている。

2011 年 5 月北朝鮮軍の電子戦部隊で勤務した経験があるチャン・セユル氏は、「北朝鮮軍には、総参謀部直属で電子戦を担当する 2 個旅団（約 1200 人）がある。各軍団でも、中隊または大隊規模の「自動化部」という電子戦組織を編制している」、「電子戦 2 個旅団は、それぞれ平安南道祥原と南浦に配置している」ことを明らかにした[10]。高麗大学・情報保護大学院の李東勲（イ・ドンフン）教授は、「2012 年 6 月の北朝鮮による GPS 妨害は、電子偵察局のサイバー戦指導局（121 局）が実行部隊である」と主張している[11]。

新たな電波妨害兵器について韓国国防部は、「朝鮮が電波妨害装置の他、強力な電磁波を放射してコンピューターなどの電子機器を無力化できる電磁パルス（EMP）弾を、今後開発する可能性がある」という見積もりを示している。

---

[9] 「韓国で大規模ＧＰＳ障害、北朝鮮から妨害電波か」『共同通信』2012.5.2、「北朝鮮の攻撃か　黄海で１２２隻にＧＰＳ障害」『聯合通信』2012.05.04

[10] 「CIA 顔負けの北朝鮮ハッカー部隊」『朝鮮日報日本語版』2011.05.04

[11] 「「韓国ＧＰＳ障害は北朝鮮・電子偵察局の犯行」『聯合ニュース』2012.06.07

北朝鮮の GPS 妨害に対処するために、韓国外交通商省報道官は、北朝鮮から発信された電波によって韓国北西部で GPS の受信に障害が発生した問題について、他国の無線通信に有害な混信を生じさせないよう求めた国際電気通信連合(ITU)憲章に違反する「国際法上の不法行為」であると指摘した。また、北朝鮮の電波妨害の効果は、商用 GPS を利用する武器システムや航法システムに若干影響があったが、レーダーや慣性航法装置（INS）など代替装備を運用することにより、妨害を無力化することができたと説明した。

（３）北朝鮮 GPS 妨害の評価

北朝鮮軍は現段階では、GPS への妨害により衛星利用測位システムに障害を受けてはいるものの重大な被害を与えてはいない。北朝鮮は、今後研究をさらに進め、GPS への妨害を確実に実施できる兵器を製造する可能性がある。兵器製造において、北朝鮮のみの技術では限界があると思われることから、ロシアや中国から非公式に技術協力を求めることが予想される。