2012 年 3 月 31 日
キヤノングローバル戦略研究所
外交・安全保障グループ

第 10 回 PAC 政策シミュレーション
「サイバー戦争は本当に起きるのか」

1. 政策シミュレーションの概要

・実施日時：2012 年 3 月 3 日（土）―4 日（日）
・参加者：学者、ジャーナリスト、現役官僚を含む約 30 名

2. シナリオの想定

想定日時は 201X年 3 月 3 日。

過去数日、日本近隣で軍事的緊張が高まっている。A 国では昨年の総統選挙に勝利したものの、深刻な党内対立を抱える与党大統領が 2 日夜に緊急特別声明を発表し、「我々A に住む人々は大陸 B から完全に独立した別個の民族国家であり、国名を「A 共和国」に改称するための国民投票を 8 月 1 日に行う、と述べた。

これに対し、B 外務省報道官は「A は B の核心的利益であり、我々は昨日の A 当局の声明を強烈に糾弾する。B 政府と軍は A 当局による B 統一に逆行する全ての企てを軍事力を含むあらゆる手段を用いて完全に殲滅するだろう。これは A 当局に対する最大限かつ最後の警告であり、これに従わなかった場合の全ての責任は A 当局が負うべきである」と述べ、強く反発した。

近隣地域では、同日、2012 年に当選したものの強固な党内基盤を持たない C の大統領が演説を行い、「D の新総書記就任以来、3 度にわたり発生した軍事的挑発行為を強く非難する。C 軍は警戒態勢を最高度に上げるとともに、国境周辺に配備されている 6 個師団と在 C 米軍 1 個師団による緊急合同演習を 3 月 15 日から実施する」と発表した。

これに対し、D は今朝 7 時の定時ニュースで「D 軍は今回の米国と C の傀儡政権との軍事行動を D に対する宣戦布告とみなす。万一、軍事行動が開始された場合は、直ちに反撃を行う。我々の自衛権に基づく反撃は激烈かつ圧倒的なものであり、C の首都は火の海となり、敵側に耐え難い結果をもたらすであろう」とする D 外務省スポークスマンの特別声明を報じている。

3. シミュレーションの流れ

①3 月 3 日（土）10 時 30 分ごろシミュレーション開始。冒頭、在日米軍の作戦運用に関する高度の機密資料がインターネット上に漏洩したため、日本政府はその処理に忙殺された。続いて、地球的規模で GPS システムに不具合が生じ始め、その後更に、重要な米軍基地のある沖縄と三沢で原因不明の大停電が起きた。

②B、D 両国は秘密裏に連携を取りながら、計 10 回の作戦（攻撃・軍事行動）を開始した。これに対し、日本政府と米国及び C は適宜連携しつつ、共同または単独で、各作戦に対する対応策を決定・実施し、それぞれメディアを通じて対外的に発表した。

③本シミュレーション中ゲームコントローラーは、これら B、D による作戦の内容とそれに対する日米 C による防衛策の具体的内容を吟味の上、作戦の成否を判断し参加者に結果を通報した。その結果、今回はまずサイバー攻撃により米国の証券・金融システムがダウンし、その後衛星通信網が不通となった。

④続いて、D 特殊部隊が C の米国大使館を攻撃する一方、日本近海に某国海軍大艦隊が集結した。更に、B、D は大規模な合同軍事訓練を実施し、米海軍艦船に対し近隣の海域から離れるよう要求するなど地域の緊張が極度に高まった。

⑤これらすべてが 24 時間以内に発生した。インターネット上の通信は大幅に制限され、国民

経済にも深刻な影響が生じ始めた。日本外務省は B に住む在留邦人に対し退避を勧告するとともに、日米 C 間の連携を高めるための一連の措置をとった。

⑥日本政府はこうした状況を「武力攻撃予測事態」と認定し、陸海空自衛隊が召集された。また、周辺事態法に基づく「基本計画」の作成も検討された。しかし、サイバー攻撃を「武力攻撃」と解釈し、国際法上の「自衛権」を行使すべきか否かといった点につき日本政府内では十分な議論が行われなかった。

⑦3 月 4 日午前 10 時過ぎ終了。

4. シミュレーションの評価

2012 年 3 月 3-4 日、当研究所は都内において第 10 回政策シミュレーションを実施した。本シミュレーションは、近未来（201X 年）に東アジア地域において、サイバー戦を伴う緊急事態が発生するとの想定の下、サイバー戦専門家の協力を得て、チャタムハウスルールにより実施された。

同シミュレーションには学者、ジャーナリスト、現役官僚を含む約 30 名が参加し、首相官邸以下 6 つの日本関係省庁、4 カ国（A-D）の外国政府及びメディア・チームに分かれ 24 時間にわたり、サイバー戦を含む様々な政治・軍事行動、関連交渉・報道などが極めてリアルに再現された。

今回の政策シミュレーションでは、東アジア地域において起こり得る緊急事態の際、サイバー空間を利用した攻撃が実施される可能性が高いことが改めて認識された。特に、重要な教訓として以下の 3 点が挙げられる。

①サイバー戦は明確な軍事目的を持った作戦計画の初期段階であることが多い。サイバー攻撃が国際法上の「武力攻撃」に該当し、国家による自衛権発動の対象となる可能性を真剣に検討する必要がある。

②サイバー戦は長期の周到な準備がなければ実行できず、外部のサイバー攻撃根拠地・発生源に対し直ちにかつ正確に反撃することは事実上不可能である。サイバー戦は既に日々戦われており、国家戦略の確立と予算増額、人材育成を早急に進める必要がある。

③サイバー戦では攻撃と被害の発生をリアルタイムで認識することが難しい。当然、政策決定者の意思決定モードを平時から有事に切り替えるタイミングも遅れる。サイバー戦専門の情報分析能力を強化して、有事対応への移行を迅速化する必要がある。

5. 専門家の評価

最後に、ゲームコントローラーの一員として本政策シミュレーションを監督したサイバー戦専門家より、以下のような講評があった。

①多くの参加者が「平時のプロセス」を踏襲する傾向が強かったため、必ずしも現実的でない対応が多々見られた。現実世界では、外国からのサイバー攻撃に対し適用可能な法律が十分整備されていないため、効果的な措置をとることは非常に難しい。

また、今回は世界のインターネット通信接続から日本を遮断することが決定されたが、実際にはこうした接続遮断により、インターネットへの依存が高い先進国の経済活動が事実上麻痺していた可能性は極めて高い。

更に、特定のサイバー攻撃はそれが発生した時点で既にその目的を達成しており、その特定の攻撃源に反撃を加えることは技術的に極めて難しい。これらの脅威に対応するためには、十分な予算と人材を確保した中長期的な取り組みが肝要である。

②多くの参加者が敵国の意図や企図を見誤るケースも少なくなかった。敵国の攻撃意図を早い段階で見出すことが出来ない場合には、対応が総花的となり、その実効性は薄れる傾向にある。

他方、敵の意図を予測することは決して不可能ではなく、国家レベルのサイバー戦のストーリーを分析することで、サイバー戦の防衛能力を高めることは可能である。

（了）