サイバー対応に熱心なオバマ政権

三井物産戦略研究所
研究フェロー
鈴木通彦

略歴：1969 年防衛大学校、1974 年同研究科を卒業。陸上自衛隊入隊後、陸上幕僚監部教育訓練部長、第 9 師団長を歴任。2000 年から三井物産戦略研究所研究主幹、ハーバード大学上席客員研究員などを経て、現職。

サイバー対応とネットビジネスのバランスに新戦略

オバマ政権が、増え続けるサイバー事案に対応し新たな国家戦略を打ち出した。

政府機関や民間企業へのサイバー攻撃[1]の激増が理由で、６月に出された商務省のサイバー青書は、「2011年１－３月期、ネット上に２年前の2009年同期の２倍以上、約６万7,000／日の新種の悪意あるソフトが出現した」と述べる。最近も、ソニー、Google、シティバンク、IMF、上院議員事務所が攻撃を受け、中でもソニーの7,700万件に及ぶ個人情報の流出が大問題に発展した。

これらのサイバー攻撃は、主に非国家主体によるが、ロシアによる、2007年のエストニアの赤軍兵士像破壊に対する報復のための「ウイルスをサーバ等に紛れ込ませ、機能を低下させる（分散型サービス拒否）」攻撃や、2008年のグルジア軍事攻撃とリンクした報道機関や政府機関への攻撃が出現したこともある。

また、米軍が新たに編成したサイバー司令部を2010年10月に本格運用させ、韓国が2011年４月にサイバー対応を任務とする軍を500名規模から倍増すると発表し、中国も６月に広州軍区にサイバー専門部隊が存在することを公式に認めるなど、各国ともサイバー攻撃や防御に積極的に軍を関与させ始めた。

これらを踏まえ、オバマ政権は、インターネットが冷戦後の経済にパラダイムシフトを起こしたように、今後もこの分野の技術革新がビジネスを活性化させる可能性があると、国防総省と商務省を両輪に、サイバーセキュリティに配慮しつつネットビジネスを通じて経済の活性化を図る新戦略に移行しようとしている。

日本でも、三菱重工業やIHI、川崎重工業などいくつかの有力防衛産業が「狙い撃ち型」サイバー攻撃を受けたと最近報じられた。現段階で、攻撃源は特定できていないが、フランス国防大臣やドイツのメルケル首相が2007年に中国を名指しで非難したことや今回の攻撃規模と質の高さを斟酌すれば、外国の国家、特に軍の関与も十分考えられる。

サイバー能力に対する低い自己評価と新たな戦略方向

米国のサイバーセキュリティは、1999年12月、クリントン大統領によるネットの利便性を高める電子政府化を促す覚書に端を発する。ネット化の背後には、必ず脆弱性が存在する。そこで、歴代の政権は、図表１のようにサイバーセキュリティに関するいくつかの報告書を出した。そして、オバマ政権になって、報告書の数が特に増えた。それは、ネットを経済発展の原動力にしたい考えと、米国社会が進歩すればするほどサイバー攻撃に脆弱になるというジレンマに由来する。

戦略の中核は2010年３月の「包括的サイバーセキュリティ・イニシアチブ」である。ここでは、ネット利用を促すとともに、サイバー対策の基準を作り、研究開発と教育を促し、しかし、企業や個人の防護はあくまで自主性に任せる新戦略を打ち出した。

その一方で、米国のサイバー防御力がそれほど高くなく、政府機関や米国社会のネット依存度が高い分だけ総体的にサイバー攻撃に対し脆弱で、また、基本的人権に関わるプライバシーや個人情報保護に対する国家統制が難しいとの悩みもある。

クリントン政権とブッシュ政権のサイバースペース・セキュリティ担当大統領補佐官リチャード・クラークは、2010年の著書「世界サイバー戦争」で各国のサイバー戦能力を、攻撃力、依存度および防御力で評価した。彼は、米国は攻撃力が高いものの、社会インフラを運営するに当たり、高い技術力を持ちながらもネット依存度が高いため極めて脆弱で、世界中の多くの攻撃源から米国を守るには防御力（探知、分析、緩和、そして予防する能力）も充分ではなく、総合力が低いと述べる。警鐘を鳴らす意味からか米国に手厳しいが、中枢にいた人物によるものだけにその評価は重い。防御力の低さは、その後のサイバー司令部の編成に伴う指揮の一元化や後述するような上級担当部局の設置など、クラークが提唱し続けたいくつかが具体化したことで現在は改善されつつある。

これらを踏まえ、商務省は、①インターネットプライバシーの強化、②サイバーセキュリティの改善、③知的財産の保護、および④情報の自由な流れの保証を基本原則に組み込むとともに、⑤ネット社会の脆弱性軽減や情報通信分野の革新に功績のあった企業に調達でインセンティブを付与し、⑥研究開発と国際協力を重視するという６つの新戦略を打ち出した。また、国防総省は、サイバー攻撃を受ければこれを軍事作戦、すなわち戦争行為として扱うほか、人材を確保し、技術革新を促し、国内各機関や友好国軍との連携を強化するなど、５つの戦略を公表した。これにより、オバマ政権のサイバー戦略が固まった。

図表１. 米国のサイバーセキュリティに関する報告書

時期	誰が	表題
1999年 12月	クリントン	電子政府化を促す大統領覚書（政府内指針）
2000年	クリントン	米国のサイバースペース防衛；情報システム防衛のための国家戦略
2008年 1月	ブッシュ	包括的サイバーセキュリティ・イニシアチブ
2009年 5月	オバマ	サイバースペース政策見直し；信頼性があり、復元力のある情報通信インフラの保証
2010年 3月	オバマ	包括的サイバーセキュリティ・イニシアチブ
2011年 4月	オバマ	サイバースペースにおける信頼性ある個人認証のための国家戦略
2011年 5月	オバマ	サイバースペースのための国際戦略
2011年 6月	商務省	サイバーセキュリティ、イノベーションおよびインターネット経済
2011年 7月	国防総省	サイバースペース運用のための国防総省戦略

オバマ政権のサイバー戦略の３つの特徴

オバマ政権の戦略は、総じて、ネットの利便性重視を基本に、国家組織に対するサイバー防御を強化し、民間はビジネス活性化を促しつつ自主防御に任せる方向で、その特徴は、以下の通りである。

第一に、米軍とその他の政府機関および民間などの分野に応じて規制する戦略。政権は、ビジネス発展の阻害になるので、民間に対し強い国家統制をとり得ないと考える。このため、政権は、政府機関の米軍を完全統制し、他の政府機関に対して情報公開とのバランスに配慮しつつ統制するが、民間については一定の基準内で自主規制に委ねる方向である。しかし、国家がサイバーを総合指揮する意思は強く、最高技術責任者、最高情報責任者、およびサイバーセキュリティ調整官を新たに大統領府に置いた。民間は、自主対応に委ねるが、利便性とセキュリティコストの相関が不明なため、今後の具体策が課題として残った。また、防御強化のコストが著しく高く、それにもかかわらず官民組織への侵入阻止が容易でないことから、少なくとも民間に対しては、防御よりも被害の早期復元に戦略をシフトさせる可能性も議論されている。

第二に、国際協力。政権は、「サイバースペースのための国際戦略」を出し、初めて国際協力に乗り出す意思を表明した。単独の国家が、非国家主体のサイバー攻撃を阻止することはほぼ不可能で、国際協力が欠かせない。そこで、国際協力を拒否し続けてきた米国も方向転換し、オープンで共同使用でき、安全性と信頼性が高いサイバースペースを作るため国際協力を提案するに至った。サイバーセキュリティ外国支援プランや国際基準設定委員会の設置などが具体例になりそうだ。

第三に、研究開発と教育の重視。ネット社会はビジネスを活性化する。このため最先端技術をいかにリードするかが重要になる。政権は、サイバーに関する研究開発と人材育成を重視し、そのための予算を主に国防総省と国土安全保障省に計上した。例えば、2012年国防予算の情報技術分383億ドルのうち32億ドルはサイバーセキュリティ関連である。事前探知や不正アクセス防止を狙いにする政府用新ITシステムEINSTEIN3も開発中で、さらに、中国におけるGoogleやアフリカ諸国のネット介入を契機に、国家によるWeb監視を乗り越える新通信方式の開発着手も発表された。

教育分野の代表は、サイバーセキュリティ人材発掘のための官民協同組織「米国サイバーチャレンジUSCC」である。この組織は、ITに関する知識・技能を問う競技大会や人材開発のための集中教育を行っている。国防総省主催の犯罪科学チャレンジ、空軍主催のサイバーパトリオット、非営利団体によるNetWars Capture-the-Flagなどの競技会がその例である。また、全米科学財団は政府機関に勤務を予定する学生に対する奨学金制度を打ち出した。

同じような社会構造を持ち、防御力も低い日本にとり、米国がとった分野に応じて規制する戦略、特に商務省の６つの戦略が、ネットを通じた経済発展とサイバー防御のバランスにどれほど効果を見せるか注目される。

1　新アメリカ安全保障センター（CNAS）によれば、サイバー攻撃は、重要システム、資産、情報および機能を操作、窃取、妨害、拒否、低下、あるいは破壊しようとするコンピュータ、電子情報および／またはデジタルネットワークを使用する敵対行為を、サイバー防御は、コンピュータ、電子情報および／またはデジタルネットワークを防護するため、その脆弱性を探知、分析、緩和そして予防しようとサイバー領域を通じて行う行為をいう。