特別速報レポート

国際エネルギー情勢を見る目（256）　　2016 年 1 月 29 日

新情勢下におけるエネルギー安全保障とサイバーセキュリティ

一般財団法人　日本エネルギー経済研究所
常務理事　首席研究員
小山　堅

エネルギー安全保障は古くて新しい課題である。エネルギーが人間の日々の活動や経済・産業の安定的な運営にとって、そして時には軍事・戦略的な活動にとっても、欠かすことのできない重要物資である以上、エネルギー安全保障はどのような国、企業、個人にとっても重要であり続ける。エネルギー安全保障には様々な定義がありうるが、最も標準的なものとして「安定的な生活・経済・社会運営に必要な量のエネルギーを合理的な価格で確保すること」という定義がある。また、もう少しそのカバーを広げ、「必要な量と価格の確保のために、意思・政策決定の自由度を失わないこと」というポイントを付加することもできる。後者が重要なのは、いくら必要な量のエネルギーを適当な価格で手に入れることができるからといって、そのために政策的な意思決定の自由度を奪われているのではエネルギー安全保障が守られたとは言い難いからである。

これまで、エネルギー安全保障は、実際に様々な折に重大な国際・国内問題として浮上してきた。すなわち、大規模なエネルギー供給途絶が発生し、国際エネルギー価格が大幅に上昇したり、物理的なエネルギー確保に問題が生じたりするような事象が発生し、国際政治・世界経済を揺るがす問題となり、各国にとってエネルギー問題への対処が最重要課題になる事態が発生してきたのである。その典型的な例は、アラブ禁輸が契機となった第 1 次石油危機、イラン革命が引き金となった第 2 次石油危機である。また、近年ではウクライナとのガス紛争が契機となったロシア産ガスの対欧州供給途絶の発生などの例もある。

こうした実際に発生してきた問題が関係者の脳裏に強く刻み込まれてきたことが影響し、従来、エネルギー安全保障と云うと、問題を引き起こす原因・リスク事象としては、国際エネルギー市場における供給途絶や輸入してくるエネルギーの確保に関わる問題として捉えられる場合が多かった。その傾向は（日本のような）大規模な純輸入国ほど強く、従って、エネルギー安全保障対策も輸入エネルギーについての安定確保策・供給途絶対策等に重点が置かれてきたともいえる。現在でも中東情勢の不安定化やそれによる供給支障の発生、その典型的な例としての「ホルムズ海峡問題」などに関心が向けられることは多い。もちろん、現在も、そして今後とも、この種類のエネルギー安全保障に関するリスクや課題に大いに注目して行くことは重要である。しかし、エネルギー安全保障の定義からして、問題は国際市場や輸入エネルギーに関わるリスクだけを対象にすべきではない。

むしろ、東日本大震災及び福島原発事故のような事象は、国内でのエネルギー供給システムの安定に関わる問題が、実はエネルギー安全保障上の重大問題であることを明らかにした。国内における石油・電力・ガス等の重要なエネルギーインフラや供給システムに何

らかの重大問題が発生すれば、それこそエネルギー安全保障にとってクリティカルな状況が生まれる。その意味では、「水際まで」＝国際市場の安定・輸入エネルギーの安定確保と合わせて、「水際から」＝国内市場での供給システムの安定・強靭性担保、が総合的に求められるのである。

現在、国際エネルギー市場では供給過剰が眼前にあり、エネルギー価格も低位に推移している。輸入国にとって、目の前にエネルギー安全保障上の脅威が深刻に迫っているという感はもちにくい。もちろん、今の低価格がエネルギー供給投資を阻害し、将来の需給逼迫や価格高騰を準備する、あるいは産油国の不安定化を促進する、などの要因には留意しなければならない。しかし、国際市場での供給過剰・低価格状況であっても、国内供給システムに問題が発生すれば、エネルギー供給確保にとって課題が即時に生ずる可能性はある。その意味で、日本も含め、世界の主要国では国内（および国際的な面も含め）のエネルギー供給システム・インフラの安定運営に関わる問題に関心が高まっている。

その際、昨今、急速にエネルギーにとってのリスク要因として重要視されるようになっているのがサイバーセキュリティである。これまで、サイバーセキュリティは、汎用的ネットワークや IT システムに対する攻撃とそれに伴う個人および政府・企業の重要情報流出等の問題に焦点が当てられてきた。しかし、徐々にエネルギーを含め、水道・交通など重要な社会インフラに対する脅威となることが認識され、エネルギーとサイバーセキュリティを結びつけた議論が活発化している。現実に、世界ではサイバーセキュリティがエネルギー供給システムを脅かす問題が顕在化してきた。最も関心を集めた事例の一つは、2010 年に発生したイランのウラン濃縮施設の制御系システムがマルウェアに感染し遠心分離機に不具合を発生させた事件がある。その他にも、カナダ、英国、米国、トルコ等において、電力・石油施設等へのサイバー攻撃があり、電力供給に支障が発生するなどの事象が複数発生している。

こうした事態を受けて、米欧、特に米国はサイバーセキュリティとエネルギー安全保障の問題に取り組みを進めてきている。現在の社会・経済におけるエネルギー供給、中でも電力供給の安定性確保や安全保障上の重要性に鑑み、米国ではエネルギー省等が中心になって情報関連企業等とも連携し取り組みを進めている。2015 年 5 月にドイツ・ハンブルグで開催された G7 エネルギー大臣会合においても、米国等の高い関心の下でサイバーセキュリティ問題への取り組みが重要であることが政策文書にも明記された。その後、EU においても取り組み強化が進められ、本年 1 月にはエネルギー分野での対策強化を含む「ネットワークと情報セキュリティ指令：NIS 指令」が欧州議会の域内市場委員会で承認された。

今年はわが国において、5 月 26・27 日に G7 サミットが、それに先立つ 5 月 1 日にエネルギー大臣会合が開催される。世界の重要課題が議論される G7 であるが、エネルギー問題についても、新たな内外市場環境や情勢を踏まえた議論とその問題についての G7 のリーダーシップ発揮が期待される。低価格環境と中東情勢流動化の共存、アジアの重要性の一層の拡大、中国経済リスクとエネルギー市場への影響等、重要な視点は多数あるが、国際・国内重要エネルギーインフラやシステムの安定性・健全性・強靭性を保つための課題の一つとして、サイバーセキュリティ問題にも光が当てられることになろう。わが国が議長国として、これらの諸課題に対して具体的かつ建設的な議論を主導する役割を期待したい。

以上

お問い合わせ: report@tky.ieej.or.jp