特別速報レポート

国際エネルギー情勢を見る目（532）　　2021 年 5 月 12 日

サイバー攻撃とエネルギー安全保障

一般財団法人　日本エネルギー経済研究所
専務理事　首席研究員
小山　堅

5 月 7 日、米国最大の石油パイプラインがサイバー攻撃を受けて操業を停止した。サイバー攻撃を受けたのはコロニアル・パイプライン社で、操業停止したパイプラインは、メキシコ湾岸・テキサス州の精製基地とニューヨークなどの北東部大消費地を結ぶ全長 8,850 キロメートルに及ぶ大規模・長距離パイプラインであり、ガソリン・ディーゼル・ジェット燃料などの主要製品を輸送、米国の石油消費センターである東海岸の消費量の 45%に相当する日量 250 万バレルを供給する、米国石油製品供給の「大動脈」の一つであった。

コロニアル・パイプライン社を襲ったサイバー攻撃は、「ランサムウェア（重要データ等を暗号化して「人質」に取り身代金を要求するタイプのマルウェア）」で、攻撃に気が付いた同社が操業を全面停止した。操業再開と復旧を図る同社は、9 日には一部の小規模ラインについて部分再開し、10 日には週末までの実質的な再開・復旧を目指す方針を発表したが、現時点で先行きの予断は許されない状況となっている。

「大動脈」の操業停止を受けて、米国の燃料供給に軋みが走っている。パイプラインの操業全面停止を受けて、国内での石油製品供給地からのタンカー輸送など他の代替輸送手段の活用、海外からの製品輸入確保、現時点で市場に存在し利用可能な石油製品在庫等の活用、等で低下した供給を補う努力が続いている。そのため、サイバー攻撃後に一時的にガソリンの先物価格等が反応したが、原油価格も 11 日までじりじりと上げてはいるが、総じてここまではそれほどは激しい反応が無く、比較的落ち着いた相場展開となっていると言える。しかし、パイプラインの復旧が遅れ、供給支障が長引くようであれば、米国の石油製品需給に逼迫感が生ずる可能性は否定はできない。コロナ禍からの回復過程で、ガソリン需要を含む石油製品需要が基調として増加の方向にあり、またこれから「ドライブシーズン」入りする米国ではガソリン需要が大きく拡大する時期にあるからである。

実際、コロニアル・パイプラインによる供給に大きく依存する一部の州や地域では、ガソリン不足を懸念・危惧して、ガソリンスタンドに給油の長蛇の車列が発生、売り切れや在庫切れが実際に起こるケースも見られている。供給不足に対する懸念が発生するとパニック買いや買いだめが生じるのは「市場の常」であり、これの仮需の発生によって、供給不足がさらに悪化するという悪循環が生ずる。消費者の冷静な対応が求められると同時に、可能な限り早期のパイプライン操業復旧が今後の事態の展開の鍵を握ることになろう。

今回のサイバー攻撃に関しては、5 月 10 日に米国連邦捜査局（FBI）がロシアのハッカー集団、Darkside の犯行と断定した。Darkside はこれまでにも数多くの営利目的でのネットワーク不法侵入を実施してきたサイバー犯罪集団で、今回のサイバー攻撃について自ら声明を発して、この攻撃は「政治とは無関係で、犯行は金銭目的」であると主張している。しかし、Darkside の犯行と断定されたことでロシア（当局）の関与が関心を集めることになり、バイデン大統領は、現時点ではロシア政府・当局が関与した証拠はないものの、サイバー攻撃がロシアのハッカー集団によって、ロシアを拠点に実施された証拠がある、との趣旨の意見を表明、ロシアにも一定の責任があるとの見方を示している。ロシア政府はこのサイバー攻撃には何の関係もないという立場を示しているが、厳しさを募らせている

米ロ関係にとっての、また新しい火種になる可能性もありうる。

コロニアル・パイプラインの復旧、米国の石油製品需給や石油価格動向、サイバー攻撃主体とその責任を巡る捜査や議論による米ロ関係への影響、等が今後の注目点となるが、今回のサイバー攻撃による石油供給支障は、サイバー攻撃がエネルギー安全保障にとって極めて重大なリスク要因であることを改めて世界に印象付けた。もともと、エネルギーに関連した世界において、サイバー攻撃はこれまでも実際に発生し、多くの被害と深刻な影響を生み出す事例が見られてきた。2015 年 12 月のウクライナへのサイバー攻撃による大規模停電などがその代表事例であり、最近では、本年 4 月のイランの核関連施設へのイスラエルによるとされるサイバー攻撃による電力供給システムの停止、などもある。しかし、今回のコロニアル・パイプランへの攻撃は、米国での事件であり、欧米や日本などの先進国・高度なエネルギー消費大国で発生したサイバー攻撃による大規模で深刻な供給支障発生という顕著な事例となった。もちろん、これまでも日欧米に対しても様々なサイバー攻撃が行われ、エネルギーやインフラ関連で被害は発生している。しかし、今回の攻撃と被害の大きさはまさに先進国での初めての重大な事例として世界の耳目を集めることになった。しかも、その攻撃主体が海外の集団であり、かつ国際政治・地政学の観点で米国との対立を深めるロシアの犯罪集団が犯行に及んだ、という点も重要であった。

「経済活動や市民生活の正常な運営にとって、必要十分なエネルギーを、安定的に、合理的・手頃な価格で確保すること」と定義できるエネルギー安全保障に対しては、それを脅かす様々なリスク要因が存在している。その中で、突発的で予測不能な形で発生する様々なリスク要因を「緊急事態・偶発的リスク要因」と分類することができるが、その中身にはエネルギー開発・生産という上流から、国際・国内双方での輸送部門や一次エネルギーから最終エネルギーを製造する転換部門、さらには最終消費者までの流通・配送と最終消費機器を利用した消費に至る下流部門など、全体としてのエネルギー供給チェーンのどこかのポイントでの「事故」・「支障」の発生が重要な要素として含まれる。この「事故」「支障」を引き起こすものとして、戦争・革命など政治的事件、自然災害、異常気象などがあるが、サイバー攻撃もその一つであり、近年その重要性への関心が大きく高まっていた。

世界のエネルギーシステムは、上流・中流・下流まで極めて大規模で複雑な供給チェーンとして構築されており、その安定的な運営がエネルギー安全保障の担保そのものである。この巨大なシステムを安定的に、効率的に運営していくためには、高度な情報通信技術に依存せざるを得ない。いわば、高度な情報通信技術の活用の上にエネルギー安全保障が立脚している面がある。だからこそ、サイバー攻撃は今日の高度なエネルギーシステムの脆弱性を突き、機能不全を引き起こすことでエネルギー安全保障を脅かす重大なリスク要因となるのである。

エネルギーが市民生活や経済運営、時には国家運営そのものにとって、欠かすことのできない財であり、戦略的に重要な物資であることから、サイバー攻撃でエネルギー供給やエネルギー安全保障を脅かすことは、直接的な軍事攻撃やテロでそれを脅かすことと同等とみなすこともできる。従って、サイバー攻撃でエネルギー安全保障に深刻な打撃を与えることは、国際政治・地政学的にも非常に重大な意味を持ちうることとなりうる。先述の通り、これまで日米欧等では、サイバー攻撃が深刻なエネルギー供給不足を発生させることはあまりなかったが、今回のコロニアル・パイプラインへの攻撃と操業停止は、こうした問題はいつでも、どこでも起こりうることを改めて各国に再認識させることとなった。

本年は異常気象による電力危機が日米双方で年初に発生したが、今回はサイバー攻撃による石油供給支障が発生した。様々な新たなリスク要因にも対応できる、エネルギー安全保障政策の見直しが今後の政策議論で重要になっていくことになろう。

以上

お問い合わせ:report@tky.ieej.or.jp