国際エネルギー情勢を見る目（819）　2026 年 11 月 12 日

急激に増加するサイバー攻撃：地政学リスクとエネルギー問題の観点から

一般財団法人　日本エネルギー経済研究所
顧問
小山　堅

相次ぐサイバー攻撃とそれによる被害の拡大が世界の注目を大きく集めている。特に 10 月以降になって、日本においてはサイバー攻撃に関するニュースが主要メディアのヘッドラインを飾らない日は無いほどであり、前例を見ないほどの規模でのサイバー攻撃による情報流出や被害の問題が報道され続ける事態となっている。

日本では、10 月に公表されたサイバー攻撃事案の件数が 233 件に上り、これまでの最高件数（96 件：2024 年 9 月）の 2.4 倍に達したと報道されている。また、サイバー攻撃の事案の数が増えているだけでなく、極めて大規模な情報漏洩（個人情報の流出）が発生していることも最近の重要な特徴となっている。同じく報道等によれば、公表された個人情報漏洩の件数は 10 月には 1 億 8544 万件に達し、前月の 2 倍に増加した。2026 年 10 月末までの累計での個人情報漏洩件数は 3 億 7621 万件となり、暦年で過去最高であった 2025 年の 4953 万件を既に遥かに上回る事態となっている。

また 1 事案当たりの情報漏洩件数が大型化する傾向が際立っている点も特徴である。2026 年には 1 事案当たり 1000 万件以上の情報漏洩が発生する事例が 10 件も発生した。そのうち、6 件が 10 月に集中して発生している。1000 万件以上の情報漏洩は 2012 年から 2025 年の間に 3 件しか発生しておらず、2026 年の、そして特に同年 10 月の発生状況は異例の事態といって良い。世間に名の通った大手・著名企業でも大型の情報漏洩事故が発生しており、日本全体を揺るがす社会・経済問題となっている。

サイバー攻撃の激化は日本だけでなく、世界でも重大な問題として関心を集めている。アジアでは、韓国で大手銀行も含む金融機関などがサイバー攻撃を受け、大量の個人情報流出が報告されている。台湾では金融機関がサイバー攻撃によって、不正送金などの顧客被害が発生した事例が報告された。また、欧州では、フランスを始めベルギー、スウェーデン、オランダ、ドイツなど各国で、スーパーマーケットの冷凍庫・冷蔵庫がサイバー攻撃によって温度が上昇し、食品廃棄を迫られる事態が発生、世界の耳目を集めた。フランスでは、血液バンクの冷蔵設備がサイバー攻撃を受けた事例も報告されている。

サイバー攻撃とそれによる被害の急激な増加の背景には、様々な要因が指摘されているものの、最近の問題の重要な特徴として、生成 AI を活用したサイバー攻撃が行われることで、攻撃の巧妙性が大きく高まり、また攻撃の速度と頻度が従来では考えられなかったレベルにまで強化されている可能性も指摘されるようになっている。日々の暮らしと経済活動の電化・DX 化が進展し、インターネット接続があらゆる分野に広がり、インターネットセキュリティ上の脆弱性が現実に存在する中、情報化の進展そのものが新たなサイバーセキュリティ上の深刻なリスク要因になっている、ということもできるだろう。

サイバー攻撃には、経済的な目的を持つものが多いということは夙に知られた事実である。顧客情報の公表などを脅迫材料としたり、重要データ等の利用再開やシステム停止の解除の引換を条件としたりする、「取引」の要求が行われるケースもあるとされる。また、サイバー攻撃によって違法に入手した個人情報がいわゆる「ダークウェブ」などで販売され、晒される場合もあるとされる。もちろん、攻撃対象への甚大な被害を発生させること、そのものが目的の場合もあろう。

しかし、サイバー攻撃にはもう一つ別の側面もある。軍事作戦の実行と共に、あるいはそれに先立って、敵方の社会・経済に打撃を与え、混乱・攪乱を発生させ、安定を損ね、戦争遂行能力を削ぐ、という軍事的・地政学的な戦略性を持った攻撃という面である。

実際、2022 年 2 月に始まったロシアによるウクライナ侵攻にあたっては、それに先立って、ウクライナの政府機関、メディア、基幹インフラ、IT 分野などに対するサイバー攻撃が実施され、その攻撃件数が大幅に増加した、とされている。電力などのエネルギーインフラも国家運営にとっては極めて重要であり、サイバー攻撃によって機能低下・麻痺が発生すれば、重大な影響を及ぼすことになる（なお、実際に 2015 年 12 月にはロシアによると目されるサイバー攻撃によってウクライナでは大規模な停電が発生した）。ロシアによるウクライナへのサイバー攻撃は引き続き実施されているものと見られるが、ウクライナ戦争が継続する中、電力などエネルギーインフラへの攻撃は、ミサイルやドローンなどによる直接的軍事攻撃に移ることになった。いずれにせよ、重要なエネルギーインフラは、戦時における通常の軍事攻撃及びサイバー攻撃の対象となりうるものであることが示されたともいえるだろう。

2026 年の中東における戦争においてもサイバー攻撃が関係当事国の双方において用いられた可能性は否定できないのではないか。もちろん、実際にミサイルやドローンなどを使った直接的な軍事攻撃が主体となれば、攻撃による被害はより激しく、かつ目に見える形で損傷・打撃が顕在化することになり、サイバー攻撃の影響は相対的に「見えにくくなる」という面がある。なお、本年夏以降には、米国、英国などにおいて発生したサイバー攻撃（あるいはその可能性がある事案）の背後にイランが存在したのではとの指摘も現れている。また前述した冷蔵・冷凍設備へのサイバー攻撃に対して、フランス政府がイランによるものと断定し、イランがそれを否定する、という一幕も見られた。

このように、軍事衝突や地政学リスク事象の発生にはサイバー攻撃が様々な形で関連するケースが多くみられている。今後、日本を取り巻く東アジアにおいても、様々な地政学リスクが存在するだけに、サイバー攻撃も含め、多様なリスク・脅威の存在可能性に対して、社会・経済の安定を保つため、予断を持たずに十分な備えを持つことが求められて行くことになろう。

電化が進み、インターネットへの接続が進む社会では、電力安定供給の確保はエネルギー安全保障の中でもこれまで以上に重要性を増していく。また、再生可能エネルギーの大幅な拡大という現実にも即した電力安定供給が重要になり、サイバーセキュリティ確保もその観点からの検討が重要になって行こう。これらの新情勢に対応した電力安定供給確保とサイバー問題の関わりに焦点を当てた最新分析の一つとして、弊所「IEEJ アウトルック 2027」の重要パートの一つとして発表した「再生可能エネルギー発電の安全保障問題」（永富悠、2026 年 10 月）の要旨の一部を抜粋してこの小論のまとめとしたい。

“エネルギー消費に占める電力の比率（電化率）が高まると見込まれる中、電力利用設備に対するサイバー攻撃への対応が重要となる。屋根置き太陽光発電や蓄電池など小規模分散型設備（DER）への対策が課題となる。個別の発電所だけでなく、分散型設備を含めた電力系統全体を視野に入れた対策が必要である。”

“特に、太陽光発電設備等に設置されるパワーコンディショナ（PCS）や、蓄電池、家電などに広く使われるインバータは、通信機能やクラウド接続を通じて不正アクセスや遠隔操作の対象となり得る。また、インバータは、太陽光発電モジュールや蓄電池セルと同様に製造能力が特定国に集中しており、供給集中のリスクとサイバーリスクが同時に顕在化する可能性がある。”

以上

お問い合わせ：report@tky.ieej.or.jp