★ベネズエラへのサイバー攻撃は世界への警鐘＝ミシオン・ベルダド

ベネズエラのグリ水力発電所はコンピューター化され、SCADA システムとよばれるソフトウェアで制御されている。ベネズエラにたいする 2 つの全国停電作戦はこのシステムへのサイバー攻撃だったのではないかとの仮説がますます信頼度を高めていた。それだけに事件は、新しい戦争様式について重要な問題点を明らかにし、世界中に警鐘を鳴らした。

さらにベネズエラ政府は、国家電力システムの一部のインフラにたいする電磁パルス兵器による影響もあると指摘した。このもう一つの仮説も、サイバー攻撃と同様、大多数の民間メディアや米政府スポークスマン、ベネズエラ国内の反チャビス主義者たちからありえないことだと嘲りの対象にされた。

この破壊行為が世界規模で取り上げていることをみても事態は緊急性を帯びている。 ベネズエラは崩壊すると頭ごなしに説明を押し付けても、多くの人々が介入の新しい方法が出現していると判断するようになっていることは疑いの余地はない。多くの人々の中には現在の米国大統領も含まれる。

ベネズエラの電力システムへのパルス兵器による影響が検出され、政府が公に非難をした。その数日後、ホワイトハウスは、「重要な技術とインフラ」への防衛システムを強化するよう米軍科学界に促す大統領令を出した。 （米国防総省への「実存的脅威」であるロシアと中国は、この分野で独自の武器を持っている）。

ワシントンによるこの動きは、マドゥーロ大統領による非難の（根拠を）補強するものだ。新たな次元の戦争がすでに実験されてきた。これからは世界の紛争の主役である（大国の）利益のためにそれが使われることは疑いない。こうした事実は、もはや世界で常識となっており、軍事作戦の第一線で研究されているからである。

2019 年 3 月 7 日に記録されたベネズエラのグリ水力発電所へのサイバー攻撃ほど大規模なものはなかった。特に、72 時間を超えて継続した停電による人的および経済的影響についてそういえる。 将来、他の国（米国を含む）で同様の攻撃が発生した場合、ベネズエラが先例となるだろう。

米誌「フォーブズ」は、停電の原因が米国主導のサイバー攻撃であることが「非

常に現実的」であることを認めた記事を掲載した。 この記事は、(サイバー攻撃が) 社会の重要なインフラとサービスに損害を与えるため、国内の対立を加速させて政権交代を強いる際に有効な戦術であることは確実であるとしている。

一方、イランの電力網を解体するために米当局から資金提供を受けたイラン系米国人科学者の証言を我々は知っている。同様の意図を聞いたのは初めてではない。「ニトロ・ゼウス計画」は、サイバー戦争や野戦を含む様々なタイプの破壊活動によって、イランの電力システムに甚大な影響を与えることを意図していた。

さらに、毎年ダボスで開催されている「世界経済フォーラム」は、今年 2 月以来、国家や企業がハッカーによる攻撃（独立、契約または政府からの攻撃）に直面していることを警告し、「サイバー攻撃からの回復力」を強化する共通戦略を策定するようよびかけてきた。 送電網などの重要なインフラは、痛々しい波状的な影響を引き起こす可能性があるからだ。

「世界経済フォーラム」は 3 月 27 日、上記のよびかけをさらに補強するレポートを発表し、「過去 10 年間で電力セクターが重大なサイバー攻撃を経験した」と指摘した。関連する諸事件を次のように再現している。

(再現ビデオ略)

これは、サイバーセキュリティ問題にとりくむため 2018 年 5 月に「世界経済フォーラム」が創設した作業グループ「システム・オブ・サイバーレジリエンス：エレクトリック」の報告で、次のように叙述を始めている。

「冬季にフランス本土で 6 時間の停電が起きれば、一般家庭、企業および重要な機関へ総計 15 億ユーロを超える損害をもたらす可能性がある。重要な電力インフラへの十分に調整されたサイバー攻撃は、国にこの種の経済的影響を与える可能性がある。 現実的か？米国土安全保障局の関係者は 2018 年に、ハッカーが複数の米国の電力会社の制御室に侵入し、顧客への電力の流れを妨げる可能性があると公に宣言した」

作業グループによると、電力システム（国であれ企業であれ）へのサイバー攻撃の危険性は、住民だけでなく経済的地域や国家安全保障についても考えられている。ベネズエラではグリ水力発電所へのサイバー攻撃により、石油産業、製造業、サービス業への影響や貿易の麻痺、その他の国の経済循環の死活的な活動への影響により、停電の 4 日間で 9 億ドル近い損害をだした。（「世界経済フォーラム」作業グループの）報告は次のようにのべている。

「電力部門は、他の重要なインフラはもちろんのこと、サプライチェーン、電気通信、港湾などの産業、下水道施設と相互依存関係をもってお互いに強く接続されている。そしてこの相互接続性は、ニールセン米国家安全保障局長官が言ったように、増大している。長官は「ハイパーコネクティビティ（超接続性）は、あなたのリスクは私のリスクであることを意味する。最も弱い環への攻撃が私たち全員に影響を与える結果になりえる」。

ベネズエラの停電は外国（特に米国）からの新しい戦争様式による仕業だとの兆候があるだけでなく、ベネズエラの前例は、「フォーブズ」や「世界経済フォーラム」といった西側の著名組織が、世界中の諸国のライフラインや企業にたいする類似の武器による戦略攻撃がありえるとする警告に根拠を与えている。それはいささかの痕跡も残さず政治的なコストも払うことなく外国に介入する方法なのだ。

ボルトン米大統領補佐官は 2018 年 9 月の記者会見で、敵にたいする地政学的および軍事的抑止のためのサイバー空間の重要性を指摘。そのために「攻撃的なサイバー作戦を承認し、米国にたいする作戦への参加のコストは彼らが望むより高くなることを示した」と語った。

中国とトランプ政権の貿易戦争の背後に、サイバー戦争と最新世代技術の発展をめぐる戦場があることを考慮にいれるなら、サイバネティック戦略をめぐる軍拡競争はますます重視されている。

近年、さまざまな関係者が向き合うようよびかける第３次世界大戦は、この分野で準備されている。しかしベネズエラのサイバー攻撃でわれわれが目にしたのは、誰にとっても望ましくない波状効果を生み出すこの種の攻撃から、さらなる熱意をもって防御する態度だ。

米国はグリ発電所やそのほかのエネルギー拠点への破壊工作で社会的、経済的不満を醸成してグアイド政権への肩入れを強めようとしている。一方ロシアは、米国が新たに作りだした混成形態の戦争によるクーデターや軍事干渉の意図に反対している。

米政府がサイバー攻撃への守りを固めるように軍事、科学界に要請し、欧米企業と結びついた諸組織がさかんに「サイバー攻撃回復力」戦略をよびかけている。それらが明らかにしているのは、ベネズエラの電力システムにたいする多因性の攻撃は世界規模の事件であり、こうした戦争にたいする備えを欠いている諸国や企業にたいする警告であるということだ。

旧来型の干渉の形態にかわる変化にとんだ戦争と脅迫を前にして、警鐘がなっている。サイバー戦争や新しい兵器に対応する行動分野についてのより深いビジョンが構想されはじめていることは明らかである。

（了）