Japan SPOTLIGHT ECONOMY, CULTURE & HISTORY Bimonthly

ジャパン・スポットライト 2020 年 1/2 月号掲載（2020 年 3 月 10 日発行）（通巻 230 号）
英文掲載号　https://www.jef.or.jp/jspotlight/backnumber/detail/230/
エリザベス・ブロー Elizabeth Braw 氏（ロイヤル・ユナイテッドサービス研究所 上席研究員）
コラム名：Cover Story 3

（日本語仮訳版）

企業が安全保障問題で大きな役割を担う

企業はどのようにサイバー攻撃の標的になるのか

本年 1 月 3 日、米国がイランの将軍カシム・ソレイマニを殺害して直ぐに、イランは米国企業を攻撃することで報復するだろう、という警告がなされ始めた。イランが米国企業を攻撃するとしたら、それは初めてではないだろう。今日、民間セクターは益々お互いに戦争にまでは至ることなく、地政学的な権力を求めて競争する国家としての標的となっている。しかし、企業は自身を単純に犠牲として考えるべきではない。逆に、企業は国の安全保障に重要な役割を担うのだ。

6 年前、名も知れぬハッカーが世界最大のギャンブル企業、ラスベガス・サンズのコンピューターネットワークにマルウェアを挿入した。それはカジノのサーバーの 4 分の 3 を機能不全とし、それを再生するのに 4 千万米ドル以上のコストが必要となる事態だった。米国政府当局は後に、イラン政府のために働いているハッカー達がこの攻撃を実行したことを明らかにした。ラスベガス・サンズは、シェルドン・アデルソンという問題の多い実業家でイスラエルの（後にまたドナルド・トランプ大統領の）熱心な支持者である人物が所有していた。サイバー攻撃の 4 か月前に、アデルソンは公に米国はイランに原子爆弾を投下すべきとの提案を行っていた。

民間セクターが標的となった歴史

アデルソンのギャンブル帝国に対する攻撃は、国が世界の覇権を巡って競争する時に、企業が如何にして標的となるかを示す初期の例だった。何世紀もの間、民間人、後にはまたビジネスが、種族、公国、国家がお互いに戦争を起こす時に標的となってきた。このような攻撃は単純に戦争の一部だったのだ。1864 年と 1949 年の間に結ばれたジュネーブ諸条約は、後に民間人を保護するルールを導入した。しかしながら、企業は軍事的な紛争における標的であり続けた。第一次世界大戦中、例えば、フランスとイタリアの助成を得た英国の帝国海軍は、ドイツとその同盟国のために一次産品を輸送する全ての船を封鎖した。第二次世界大戦中は 12,000 以上の地雷が、米国によって日本の船の航海ルート、領海水域、あるいは港に飢餓戦略の一部として埋められた。これらの地雷は、670

の日本の商船を沈めるか、あるいは大きな被害を与えるかして、海上輸送による交易を麻痺させたと米国海軍のティモシー・マクギ―ハン司令官とダグラス・ワール司令官は米国海軍研究所の 2016 年 1 月の論文で述べている。第二次世界大戦中、英米は最小の軍事的価値しかない、ドレスデンを爆撃した。この攻撃の是非は議論を呼んだ。この攻撃は企業とその建物を瓦礫と化してしまった。ナチスドイツは強制的にドイツが占拠した国の企業の所有者（しばしばユダヤ人）から企業を収用した。

今日異なるのは、企業は戦争の宣戦布告がなされなかったとしても攻撃を受けるということだ。ヒスコックス保険会社の 2019 年のサイバー攻撃対応レポートでの報告事項について考えてみよう。昨年は、ベルギー、フランス、ドイツ、オランダ、スペイン、英国及び米国の企業の６１％が発表に先立つ 12 か月間でサイバー攻撃に晒されたと報告されている。これはその前の年の 45%から上昇している。困ったことに、サプライチェーンにおける弱い繋がりの結果、一回かそれ以上のサイバー攻撃を経験し、より高い 65%という比率が報告されている。（ヒスコックスがその報告書にサプライチェーンを含めたのは初めて）更に、企業はますます繰り返しサイバー攻撃を受けるようになっている。「この報告書で対象とされた 15 セクターの全てで 1 回以上の攻撃を受けたと報告している企業の比率が急増した。７か国全てにおいて最も標的とされたセクターは、いわゆる TMT（技術、メディア、テレコム）だった。72%の企業が一回以上の攻撃を受けたと報告しており、一年前の 53%から上昇した。政府関係機関が第 2 位で（攻撃の報告を受けた機関が全体の 71%で、前年の 55%から上昇）次は金融サービス（67%、これも前年の 57%から上昇）、とヒスコックスは報告している。

英国政府の 2019 年サイバーセキュリティ―違反サーベイによれば、企業の 32%、慈善団体の 22%が、直近 12 か月で、サイバーセキュリティ―違反か攻撃を経験したということだ。中規模企業ないし大企業は最もサイバー攻撃の影響を受けており、それぞれ 60%と 61%である。攻撃の回数は減少したが、それは攻撃が和らいだことを意味するわけではない。このサーベイの発行者である英国のデジタル・文化・メディア・スポーツ省は、一つの可能性として、「攻撃を行うものが、より狭い（といっても依然として多いが）範囲の企業に焦点を絞った攻撃をするようになるという行動に変化している。」という。

もちろん、全てのサイバー攻撃が政府に関係しているわけではないが、多くがそうである。ニューヨークのシンクタンク外交評議会は、国家に結び付いたサイバー攻撃（西欧政府に関係したサイバー攻撃を含む）のデータベースを保有している。昨年 4 月に、例えば、ドイツの巨大薬品企業バイエルは、中国政府と関連のある中国のハッカー集団「ウィキッドパンダ」（邪悪なパンダ）の攻撃を受けたと報告された。サイバーセキュリティ―企業クラウドストライクによれば、このグループの手段は、「公共セキュリティー省を含む複数の中国政府当局を顧客とする契約企業へと痕跡をたどることができた。ウィキッドパンダが標的としたのは、エンジニアリング、製造業、技術セクターといった中国の戦略的経済計画と整合的なセクターにおける高付加価値を有する組織に絞られていた。ウクライナの重要な機能を担

う水の塩素処理施設が、ロシアのために働くハッカーの標的となっていた。APT33、リファインドキットン、あるいはホルミウムといわれるイランのハッカーグループは、多くのハッカーがやるように動力プラントを単に破壊するのではなく、その作動に干渉することを行ってきた。

企業に対するその他の種類の攻撃

企業は他の方法による攻撃にもまた晒される。昨年 7 月、英国籍でスウェーデン所有の貨物船、ステナ・イムペロ号が、イラン革命軍の奇襲隊によってホルムズ海峡で拿捕された。当初イランは貨物船が国際法に違反したと主張していたが、後に拿捕は
その月の初めにイランの石油タンカーがシリアに原油を輸送した疑いで英国に拿捕されたことへの報復であると述べた。ステナ・イムペロ号の拿捕の後、保険のコストが高騰した。

民間企業の役員は、また、企業の本拠地または重要な事業を行っている国に対して敵意を持つ政府による偽情報のキャンペーンが、企業に損害を与えることについても危惧している。例えば、X 会社が拠点を置く B 国に対する A 国の偽情報のキャンペーンが成功した場合を想像してみよう。B 国政府の安定性についての誤った情報の拡散により、A 国は、例えば自国の通貨価値を高めることが出来、それによって X 会社を含む企業に甚大な損害を与えることになる。

言い換えれば、企業は、どこかの国が特に自分達に対して復讐をしようとしているのでなくても、他国ないしはその代理人によって標的とされ、被害を受けることになるのだ。自らが代表する国を弱体化させる一つのやり方として、企業が攻撃を受けるのだ。ステナ・イムペロ号は、イラン政府がこの船をあるいはスウェーデン人の所有者ステナ・ブルクに被害を与えたいがために拿捕されたのではなく、英国によるイランの貨物船の拿捕に抗議するために拿捕されたのだ。そして更にこの拿捕は、トランプ政権の反イラン・キャンペーン及びイラン核合意としての方が良く知られている合同総括行動計画（JCPOA）に対する抗議と見ることもできる。ステナ・イムペロ号の拿捕によって、イランは欲すればホルムズ海峡を国際貿易にとって危険な地域に出来ることを示したのだ。それは航海ルートに依存する企業への厳しい打撃であり、同様にそのルートに依存する多くの国に対する厳しい打撃ともなるだろう。

外国政府が標的とする企業にとっての困難

企業が国の代理人として標的とされ得るないしされているという現実は問題をもたらす。何故なら、如何なる企業も事実上国家に対して自身を守ることが出来ないからだ。例えもし稀にそのようなことが想定上出来ることがあるとしても、法律は私人が他の国に対して攻撃的行為を行うことを禁じている。これは防衛に信頼を持たせるための必要条件だ。サイバーの領域では、例えば、企業は自身を防衛することは許されているが、自身のサイバー攻撃によって反撃することは許されていない。また企業は、サイバー攻撃を企てている疑いのあ

る個人やグループの攻撃を予防的に阻止する行為も許されていない。攻撃的なサイバー行為は政府の領域であり、それには良い理由がある。それは、積極的な攻撃により、企業は外国政府との摩擦をその母国の政府が軍事的手段に踏み込むまでに増幅させてしまう可能性があるからだ。

それにもかかわらず、政府のみが国家の安全保障に責任があるという現在の仕組みは、攻撃が軍事的性格のものだけではない時代において適切なものではないことは明瞭だ。それはまた、国が特にその定義上、社会の開かれた性格のゆえに、攻撃に対して脆弱である自由民主主義国家がその社会に対する破壊行為を最小化することが出来ることは全ての人の利益である。もし、敵意を持った攻撃が繰り返され、広範な被害をもたらすなら、それはその国の現在の企業活動に被害を与えその活動に生きる国民にも被害を与えるだけではないだろう。それはまた、ビジネスを行うための安全な場所としての国の地位も傷つけることになろう。言い換えれば、企業は国の安全保障において役割を持つのである。

安全保障における企業に期待される役割

それは新しい概念のように思えるし、実際そうである。企業は第二次世界大戦を含めて以前の戦争で安全保障において役割を果たしてきた。防衛産業はその定義上、今も役割を果たしている。しかしながら、今日全ての種類の企業は安全保障において一定の役割を果たすことが出来る。実際、欧米政府は小さすぎてその市民社会全体を防衛する傘を広げることは出来ない。そしてまたそうすることは彼らの社会にとって許容できる事でもないし望ましいことでもない。

しかし企業はどの役割を担うべきなのか？冷戦の期間、北欧諸国はいわゆる「総合防衛」モデルを開発した。それは冷戦期間中の脅威が今日の自由民主主義国家に影響する脅威とは異なるとしても、今日教訓となり得るものだ。総合防衛は、第二次世界大戦中に中立国であるスウェーデンがナチスドイツの圧倒的な戦力に直面した際にスウェーデンによって創られた。スウェーデンは冷戦中にそれを更に発展させ、そしてデンマーク、ノルウェイ、フィンランドもまたそれを開発した。

総合防衛によってスウェーデン政府は、ストックホルム証券取引所、郵便サービス、電話会社、そして鉄道会社を含む極めて重要と考えられる企業との密接な関係を維持した。また更に、ボルボやサーブといった企業とも密接な関係を維持し、国が有事の際に機能を維持できるようにしたのだ。これらの企業は、K 企業として知られ、危機の間、活動を継続することを余儀なくされた。そして主要スタッフは、この活動の継続を保証するために兵役を免除された。ボルボやサーブ、また武器製造企業のボフォルスのような場合には、政府は山間の工場施設の建設に補助金を与えて外敵の襲撃からこれら企業の生産を守ろうとした。スウェーデンは、2000 年代の初めに概ね総合防衛を解除したが、現在、冷戦の時の規模程ではないが、またそのシステムを再構築しつつある。

フィンランドは、その総合防衛モデルとして、1950 年代にスウェーデンによって導入さ

れた国防研修を完全なものとした。政治、ビジネス、市民運動そして軍隊で登場しつつあるリーダー達を３週間だけの泊まり込みの安全保障研修に招待すること（その後フォローアップの研修を行う）が大いに実施された。その成果の一つは、フィンランドのビジネスエリートは安全保障に精通しそれをビジネス活動に活用していることだ。

もちろん、冷戦期間中は多くの企業が政府系の独占企業であり、その活動を自由に政府のニーズに適応させることが出来たのは役に立つことだった。しかしながら、ボルボやサーブ、またボフォルスの関与が示すように、グローバル市場で競争する私企業に国の安全保障における役割を担わせることが可能だった。確実にスウェーデン政府はビジネス幹部の愛国心に訴えることが出来たのだ。その時代には全てのスウェーデンの主要企業はスウェーデン市民によって運営されていた。それは他の国においてもほとんどの主要企業がそれぞれの国の国民によって運営されていたのと同様である。そして企業は、外国の大きな組織によって所有されることはなかった。

今日その事情は異なる。多くの国で、主要企業は究極的には外国の組織によって所有され得るのだ。例えばボルボは、中国の自動車大企業ジーリーが保有している。実際、例えもし最高経営責任者が自身の会社の本社のある国の安全保障に貢献すべきとの責任を感じたとしても、そのためのステップは外国を本拠とする会社の所有者とは相いれないかもしれない。更に、世界のビジネスは今やMBA世代が主導しており、経営と金融情勢には明るくても安全保障については少しも理解していない。いくつかの新興大企業は自国の政府と出来るだけ距離を置くことを喜ぶような感じすらある。2016年の米国大統領選挙運動の間におけるロシアとの接触について、最小限の情報以上のものを米国議会と政府に対して提供するのを拒んだフェースブックについて考えてみるといい。

同時に、自らが活動する国が、日常生活への妨害やその国の投資家の信頼度を傷つけ、引いてはその国の経済の実績を損なうような偽情報から可能な限り自由であることを維持するのは、ビジネスとしての利益にも合う。フィンランドの安全保障研修は、他の自由民主主義諸国にとって良い出発点となろう。研修は政府が新しいリーダー達（特に重要なビジネスリーダー達を含めて）に対して、国の安全保障の基礎と直面する脅威について教えることに理想的な手段を提供し、そしてその後に行われるフォローアップのための研修は政府が新しく出現した安全保障問題についての情報を提供することを可能にする。更に研修はその職業人生を通じてお互いに交流し相談しあうことになる新興リーダー達のネットワークを構築するのだ。

安全保障のための政府と民間セクターの協力

自由民主主義国家の政府はまた、企業の、特に通信、運輸、電力、食料、廃棄物といった戦略的セクターの最高経営責任者を定期協議に招待し、新しい脅威とより一般的に安全保障の現状についての最新情報を提供することをすべきだろう。もしこれらの人々が安全検査を受けられるなら、このような情報提供に極秘情報を含むこともあり得よう。政府による

定期的な安全保障の最新情報提供は、ビジネスリーダーが新聞を読んだり、リスク分析のコンサル企業のレポートを読んだりして得られる以上に包括的に自身の活動環境について考察することを可能にするだろう。

もちろんそれは、自動的に安全保障に益するやり方で意思決定を変えるようになることを意味するものではない。しかしながら、それは事業の決定を行うに際して安全保障についてのより良い理解を持つことを意味する。多くの自由民主主義国家において、今日ビジネスはMBA世代によって主導されているだけではなく、大部分が安全保障と最小限の接触しかない世代によって主導されていることを念頭に置くべきである。対照的に、1960年代と70年代の主要米国企業は、例えば、しばしば第二次世界大戦に従軍した人々によって主導され、殆ど全ての北欧のビジネスリーダーは兵役に従事したことがあるのである。

もう一つの考慮されるべきステップは、戦略的セクターの企業が安全保障を支える上で特定の役割を果たすようなインセンティブを与えることである。例えば、包括的な危機管理計画を開発する上での役割だ。今日、冷戦の終わりまで殆ど政府所有であったサービス、(主に、通信、航空、水道、電気、鉄道）は大部分民営化されてきた。今日、大部分のセクターで多くのより小さな企業は横並びでしばしば競争者として活動している。スウェーデンの冷戦期間のK企業群に似た役割を担うことに合意した企業は付加的な支出を補う政府補助金を受け取ることが出来る。また逆に、あるいは付加的に、それら企業は王国で使用される王室保証のラベルと似た特別の政府承認を付与されることがあり得よう。それはそれらの企業に「最良企業」の資格を与えることになる。

もちろん、企業の最高経営責任者は、安全保障への関与は会社にとっての純利益にはならないとなおも決断するかもしれない。実際、グローバルに活動している大企業の場合、企業が本拠を置く西欧の大国の安全保障への貢献は、その他の市場へのアクセスを妨げることもあり得るとの決断を最高経営責任者はするかもしれない。こういった、当該国の利益ではなく、如何に自社の利益になるかということだけに基づいて決断を下す自由がビジネスリーダーにあることは、自由民主主義国家の弱点の一つだ。対照的に、中国のような専制的な国では、政府は公には私企業と考えられる企業に対してすら特別の活動を命じたり、あるいは政府との密接な協力を命じたり出来る。

法制がこの問題を解決できよう。しかしながらそれは十分な手段ではない。そして、いったん新しい法律が出来ると、それに影響される者は最小限の要求を満たすだけで対応する傾向がある。従って、限定的な法制度とビジネスリーダーの関与の組み合わせが、コンサルテーションと安全保障研修によって最も生産的な推進策となり得よう。それは、企業を安定的な環境で活動させたいという経営者の欲求の上に立って、その意思決定が国と引いては企業とを裨益するのに役立つ情報を提供する政府のコンサルテーションを含むことになろう。政府が特定の企業を他に比べて有利に扱うべきでないがゆえに、そのコンサルテーションはそれぞれの戦略的セクターの中の全ての主要な企業の最高経営責任者に公開されることが重要となろう。唯一の制約は、参加企業は安全検査を受けなければいけないことだ。

企業所有法が重要な役割を果たすだろう

もう一つの点は極めて重要だ。即ち、企業の所有についての法律だ。今日、主要企業ですらしばしば独立しておらず、外国の大企業によってさえ保有されているがゆえに、またそのことが企業の役員の安全保障分野における行動の自由を制約するがゆえに、自由民主主義国家は外国人ないし企業による所有権のルールについて考察すべきだ。大抵の自由民主主義国家が戦略的企業の外国所有を制限する法律を持っているにも関わらず、そのルールは大抵防衛産業に限定され極めて寛容である。英国では、例えば、2002 年と 2018 年の間に、政府は安全保障を理由に 8 件のビジネス取引に介入しただけだった。しかしながら、規制を強めようという動きはある。2018 年に米国は、外国投資リスク審査近代化法（FIRRMA）を通じて、より厳しいルールを課した。同じ年ドイツは、戦略的企業における外国投資が政府の許可を要する株式所有の比率を 25%から 15%に引き下げた。同じく 2018 年に英国政府は、「戦略的製品」を売るビジネスにおける 25%以上の株式買収について、政府の許可を必要とする旨の提案を政府の白書で行った。英国政府はこのようなルールで毎年 200 くらいの政府への許可申請があるものと見込んでいる。

その他の自由民主主義国家においても、同様の動きが進行中ではあるが、問題はこのようなより厳しいルールが十分かどうかということだ。戦略的セクターでは、外国の企業保有を全面的に禁止すべきなのか、それともそれは西欧諸国の企業が依存するグローバル市場の活力を損なうことになるのか。中国がその域内で活動する如何なる類の外国企業にも厳しい制約を課していることを思い出す価値がある。

結論

日本からカナダまで、自由民主主義国家は市場の成功に依存している。自由で開かれら国には厄介な問題はあるが、冷戦期間中、米国は生活水準で測ればライバルであるソ連を圧倒した。1989 年には、ソビエト連邦内のロシア共和国の一人当たり GDP は現在の米ドル価値で 3,428 ドルだったが、これに対して米国は 22,857 ドルだった。日本は地政学的な攻撃とは無縁でそれより更に良く、24,813 ドルだった。

本稿で概観してきたように、問題は今日の安全保障の脅威は企業に直接的な打撃を与え得るし、また与えているということだ。本稿で取り上げた全ての提案が全ての自由民主主義国家によって採用され得るわけではない。しかしながら、それぞれの政府は緊急に単なる情報提供によるかまたはサイバー攻撃やその他の攻撃の場合に、国への被害を最小化する上で、企業が積極的役割を担うようにインセンティブを与えるかは別として、安全保障における民間セクターの関与をどうすれば可能に出来るか考えることが出来るし、またそうすべきである。

もちろん、前者が後者に情報を与える。それによって、安全保障への脅威を正しく理解した戦略的セクターの企業のリーダーは、おそらく次の四半期の営業報告だけに関心を集中

する役員がビジネスに無関係のこととして片付けるような安全保障関連の動きに、自らの企業を関与させようとするようになるだろう。方程式は一つの基本的な現実に行きつく。即ち、今日、ビジネスは過去では考えられなかったほど地政学的な攻撃の標的となっているがゆえに、ビジネスとしてもその役割を果たすことが自身の利益にもなることは疑いの余地がない。企業はまさに、そうする機会と政府への協力のための仕組みを与えられなければならない。

（了）