〔提言〕

企業発信の総合安全保障

～その一歩が日本の抑止力に繋がる～

2019 年 3 月

サイバー適塾第 17 期

安全保障グループ

はじめに

まもなく「平成」の時代が終わろうとしている。この平成の 30 年間は、まさに大災害に見舞われた時代であった。1991 年（平成 3 年）の雲仙普賢岳の大噴火、1995 年（平成 7 年）の阪神淡路大震災、2004 年（平成 16 年）の新潟県中越地震、そして 2011 年（平成 23 年）に発生した東日本大震災は、未曽有の大津波で多くの人命が失われただけでなく、福島第 1 原発事故という想定外の被害をもたらし、日本の安全神話を大きく揺るがすこととなった。

そして昨年 2018 年（平成 30 年）もまた多くの災害に見舞われた年であった。6 月の大阪北部地震、7 月の西日本豪雨災害を始め、9 月に上陸した台風 21 号による被害は、関西空港連絡橋の損傷に伴う交通インフラの封鎖により、物流の停滞、インバウンド需要の減少という形で関西経済に大きな影を落とし、自治体や企業の事業継続計画（BCP）の在り方が問われることとなった。

一方で、「平成」は従来の「戦争」からは遠ざかった時代であったと言われている。太平洋戦争を経験した「昭和」の時代とは異なり、日本の国土が武力戦争の惨禍に巻き込まれることはなかった。これは国民の平和への願いとその努力から導き出された賜物であると言えるが、安全保障上のリスクから完全に遠ざかったと言えるのであろうか。

この 30 年の間、国際情勢は目まぐるしく変化し続け、世界各地では多くの紛争や武力衝突が起きた。日本近海においても、竹島や尖閣諸島、北方領土といった国境付近における係争は続いており、自衛隊によるスクランブル発進も多発するなど、日本を取り巻く安全保障環境は一層厳しさを増している。また 1995 年（平成 7 年）の地下鉄サリン事件、2001 年（平成 13 年）にはアメリカ同時多発テロが発生し、国家間の軍事的衝突だけでは語れないリスクが顕在している。特に高度に IT 化が進んだ社会においてはサイバー攻撃という脅威も高まっている。その意味でも、「日本は平和」とは言い難く、常にリスクと隣り合わせの状況と言わざるを得ない。

このような状況を踏まえ、来たる時代をどのように生きていかねばならないのか。本論では、我が国がおかれている安全保障の現状を踏まえ、特に企業経営の視点から安全保障上のリスクを分析した上で、今後の日本の「総合安全保障」の取組みにおいて、企業が果たすべき役割について考察していくこととする。

第１章　日本を取り巻く安全保障環境

第１節　米中覇権争いによる緊張の高まり

（１）覇権挑戦期の到来

アテネの歴史家トゥキディデスは、新興国が覇権国に取って変わろうとする時、国際関係に構造的なストレスが生じ、それが戦争の発生要因になると述べている。近年、米国が世界の覇権国として確固たる地位を築いているが、近代史以降の歴史をみると、覇権国は 16 世紀のスペイン・ポルトガル、18～19 世紀のイギリス、そして 20 世紀の米国へと交代している。このことから、21 世紀に覇権国が交代する可能性もあり、現在は米国に代わって中国が世界の覇権を握ろうとしている「覇権挑戦期」にあると言える。

2018 年 9 月 30 日、中国が軍事拠点化を進める南シナ海の南沙（スプラトリー）諸島周辺で、中国海軍の駆逐艦が米国のイージス駆逐艦「ディケーター」にわずか約 40 メートルの距離まで異常接近した。これに対し同年 10 月 4 日、ワシントンで演説したペンス副大統領は、中国海軍の異常接近について「我々は脅しには屈しない。身を引くことはない」と言い放ち、徹底的に中国の行動を批判した。そして、知的財産の侵害、選挙干渉、さらにウイグル族の弾圧まであらゆる問題を列挙し、中国の非難を続けた。ニューヨークタイムズは、この一連の流れを「新冷戦の号砲」と評した。

（２）中国の台頭

近年、中国の経済成長はめまぐるしく、2030 年頃には米国を抜き、GDP 世界第 1 位になると予測されている。国防費は 1980 年代末以降 GDP 比 2%程度を維持しており、GDP の 2 桁成長が約 30 年続いたことに伴い増加、米国に次ぐ世界 2 位となっている【図 1】。

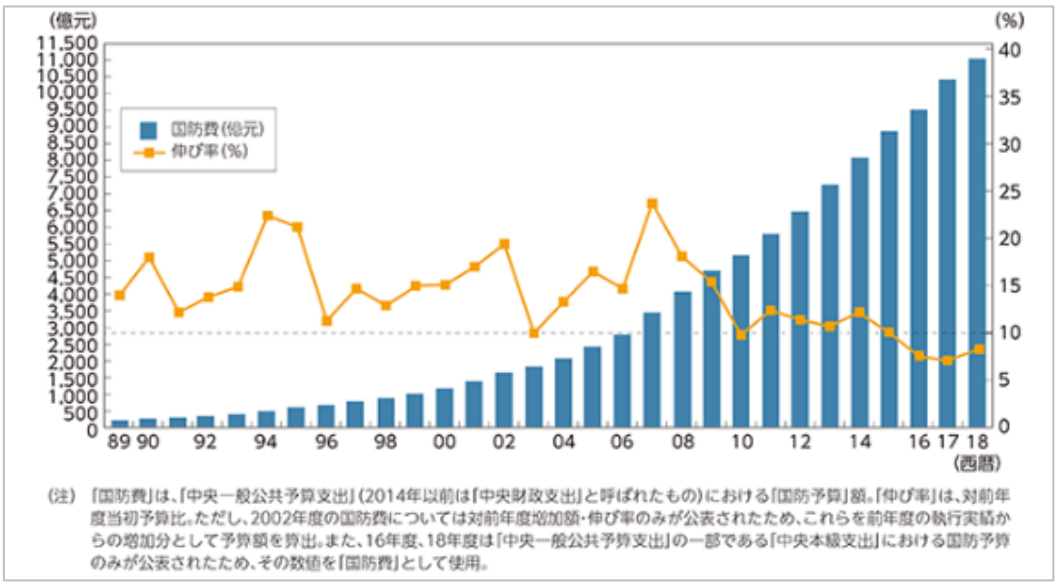


図１：【出典】平成 30 年版防衛白書

中国は豊かな経済力、軍事力を背景に、自国と主張する境界線は「九段線」に示される通り、南シナ海のほぼ全域に及んでいる【図 2】。南沙諸島、西沙（パラセル）諸島の領有権をめぐっては、 現在も中国と ASEAN 諸国間で主張が対立している。さらに、南沙諸島等への中国の影響力拡大に対しては、米国が「航行の自由」作戦を実施し、国際法に基づきすべての国が自由に海・空域を利用できることを主張している。

図 2：【出典】日本経済新聞（2016 年 6 月 30 日）

また東シナ海の尖閣諸島は、第二次世界大戦後に米国支配下となり、19 世紀から領有権を主張した日本に 1970 年代初めに返還されたが、中国も同時期にこの諸島の領有権を主張しはじめ、同海域での緊張を高めている。尖閣諸島のわずか 170km 西に位置し、南シナ海、東シナ海のどちらにも面している台湾は、自国の一部であると主張する中国と長年に渡って対立している。

昨年の国内視察で台湾の政府機関関係者に伺ったところ、2018 年の統一地方選挙で独立主義を貫く民進党が親中派の国民党に惨敗したことにより、中国との統一への機運が高まっている。地政学の観点から今後中国が台湾を吸収する事態になれば、尖閣諸島、沖縄が危機に晒されることは必至だろうと懸念されていた【図 3】。

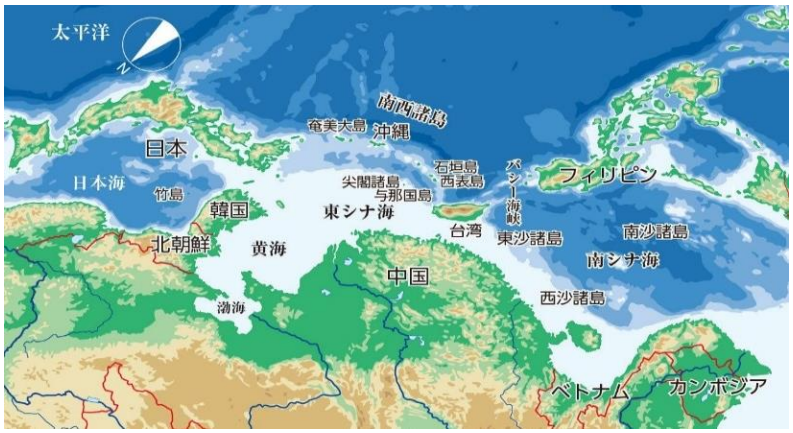


図 3：【出典】東洋経済オンライン（2015 年 5 月 26 日）

また、中国は現代版シルクロード経済圏構想として「一帯一路」を推し進めている。「一帯」とは、中国西部から中央アジアを経由してヨーロッパへと続く「シルクロード経済ベルト」を指し、「一路」とは中国沿岸部から東南アジア、スリランカ、アラビア半島の沿岸部、アフリカ東岸を結ぶ「21 世紀海上シルクロード」を指している。中国は、これらの地域に道路、港湾、発電所、パイプライン、通信設備等インフラ投資を皮切りとして、金融、製造、電子商取引、貿易、テクノロジー等各種アウトバウンド投資を積極的に進め、当該経済圏における産業活性化と高度化を図っていくことを強力に推進している。

一方、「自由で開かれたインド太平洋」構想は日本が提唱したもので、インド洋と太平洋で日米豪印が連携し、自由貿易とインフラ整備を通じて一帯の経済発展を図ると共に、海洋を中心とした安全保障協力を推進する構想である。

「一帯一路」構想と「自由で開かれたインド太平洋」構想は二つの地域秩序構想であり、その一部は競合関係にあるといえる【図 4】。

図 4:【出典】産経ニュース（2018 年 1 月 11 日）

我々が海外視察で訪問したマレーシアにおいても、中国資本による建設ラッシュが起きているが、政権交代を契機に中国の貸し付けによるインフラ整備の計画が見直されるなど、中国による「債務の罠」を警戒する動きがみられる【図 5】。

中国が運営権を握った主な海外の港湾			
1	ベルギー	セーブルージュ港	17年9月、港湾運営会社を買収
2	ジブチ	ジブチ港	17年8月、初の海運基地の運用開始
3	スリランカ	ハンバントタ港	17年7月、99年間の運営権取得
4	アラブ首長国連邦（UAE）	ハリファ港	16年、埠頭の35年間の利用権取得
5	パキスタン	グワダル港	15年、42年間の用地使用権取得
6	オーストラリア	ダーウィン港	15年、99年間の運営権取得
7	ギリシャ	ピレウス港	09年、埠頭の35年間の利用権取得 16年、港湾全体の運営権取得
8	ミャンマー	チャウピュー地区	大型港や工業団地の整備に協力
9	オマーン	ドゥクム港	工業団地の整備に協力
10	アルジェリア	ティパサ地区	大型港の整備に協力

図 5:【出典】日本経済新聞（2018 年 2 月 24 日）

（３）サイバー空間における米中間の攻防

サイバー空間においても米中は熾烈な主導権争いを繰り広げている。米国のトーマス・ドニロン米国家安全保障担当大統領補佐官は 2013 年 3 月、中国からの産業スパイ活動は、国家安全保障に関わる機密情報だけでなく企業秘密情報や知的財産の窃取も含まれていることを明らかにした。また産業スパイ活動で得た情報を中国企業へ横流しすることで、米国企業の優位性や競争力が失われることへの懸念も示している。

対して中国政府はたびたび自国をハッカー攻撃の最大の被害国と言及し、その主な警戒対象を米国としており、スノーデン事件（2013 年）によって米国の国家安全保障局（NSA）が世界中で実施していた情報窃取の対象に中国の情報通信企業や高等教育機関も含まれていたことが暴露され、米国に対する不信感を更に募らせている。

（４）宇宙空間での米中間の覇権争い

ペンス副大統領は 2018 年 8 月 9 日に国防総省で行った演説で中国やロシアの脅威に言及し、「米宇宙軍を創設すべき時が来た」と強調、「米宇宙軍省を 2020 年までに創設することを目指し、直ちに提言を実行に移すための行動に出る」と表明した。

さらに宇宙軍設立に向けた措置として、次の 4 点について演説で言及した。1 つ目は統合戦闘軍としての宇宙軍を設置すること、2 つ目は宇宙に特化した軍種横断の専門集団としての宇宙作戦部隊を設置すること、3 つ目はイノベーションと実験、将来技術の構築に注力する宇宙開発庁を設置すること、4 つ目は、宇宙軍創設に向けた作業を監督、同軍創設時に長官となる宇宙担当の国防次官補を新設することである。

対して中国も習近平指導部の大号令のもとで 2050 年までに世界をリードする「宇宙強国」になるという目標を掲げ、宇宙開発を国家の重要事業と位置付け、実績を上げ始めている。月探査に本格参入して十数年の中国が、2019 年 1 月 3 日半世紀を超える歴史を持つ米ロ両国に先んじて月の裏側への無人月探査機「嫦娥（じょうが）4 号」の着陸を成功させた。月の裏側は未解明な点が多く、将来の資源開発等で優位に立つ思惑があるとされ、宇宙開発でも米国との主導権争いが始まっている。中国の宇宙開発には軍が深く関与しほとんど情報は開示されておらず、軍事利用についても各国からの懸念が高まっている。

第２節　米中覇権争いが及ぼす日本経済への影響

米中貿易戦争の根底には、先端産業をめぐる熾烈な主導権争いがある。米国は、中国が合法・非合法を問わず、先端技術を獲得することで、経済的にも軍事的にも覇権を握ろうとしているとして警戒を強めている。

2017 年 1 月に発足したトランプ政権では、当初は貿易政策での強硬姿勢は懸念されたほどではなかったが、2018 年に入ると保護貿易主義的な政策実行に力を入れ始めた。これは、トランプ大統領が同年 11 月の中間選挙、さらには 2020 年の大統領選挙での再選も視野に入れ、選挙公約を実現することで国民からの支持を高める戦略でもあった。

現在、米国と中国の貿易摩擦がエスカレートしており、米国は 2018 年 7 月、知的財産や

技術移転等に関する中国の政策が米国に不利益を及ぼしているとして、中国からの 340 億ドル相当の輸入品に 25%の制裁関税を適用した。中国はこれに対抗して、同額の米国からの輸入品に同率の追加関税を適用し、それ以降も双方が譲らず報復関税の応酬となっている【図 6】。

図 6:米中の制裁関税と報復関税

トランプ大統領と習近平国家主席は、2018 年 12 月 1 日に首脳会談を開き、両国の間で激化した貿易摩擦について協議した結果、米国が関税を引き上げる制裁措置を 2019 年 3 月 1 日まで見送った。その後、中国による知的財産権の侵害やサイバー攻撃、そして技術移転の強制等の問題について両国で協議を行うことで合意したものの、協議の期限までに進展がなければ、関税を引き上げる制裁措置を発動する構えを崩していない。

現在、多くの米国企業が中国国内で生産活動を行っており、中国の関税率引き上げによって、そうした米国企業が中国企業から調達する部品や材料のコストが高まれば、生産活動、収益環境への打撃となる。また、米中貿易戦争で中国の内需が悪化すれば、米国企業も大きな打撃を受ける。中国人の反米感情が高まると、米国企業の製品に対する広範囲な不買運動へと発展する可能性もある。

このような米中の争いが、グローバル化された世界経済にも影響を及ぼしている。産業界においては分業を通じた効率化のメリットを活かすため、1 つの製品を作る際にそれを構成する部品の製造やいくつかの製造段階を異なる国・地域にまたがって行う、グローバル・バリューチェーンが大きく広がっており、海外で活動する日本企業数は約 2.5 万社に達している（経済産業省「海外事業活動基本調査」2016 年度実績）。過去 20 年のうちに、その数は約 2 倍に増加し、増加数のうちアジア地域が約 9 割、その約 6 割を中国（香港含む）が占めている。米国との貿易戦争で中国経済が打撃を受ければ、アジアの他国で製品を作り、中国で販売している多くの日本企業が甚大な被害を受ける可能性は否めない。その証左として、2019 年年明けの東京株式市場は大幅に下落し、2 万円の大台を割り込むなど米中関係の悪化が日本経済にも影響していると言われている。

IMF（国際通貨基金）はトランプ政権による追加関税が与える世界経済への悪影響を試算し 2018 年 7 月 18 日に公表した。上述した対中関税に加えて、検討中の輸入車への 25%の

追加関税が発動されるという前提において試算された結果、世界の GDP は 2 年間で 0.5%程度押し下げられる。また、国別の影響を見ると、主要国の中で最も大きな影響を受けるのは、制裁関税を仕掛けた米国自身であり GDP は 0.8%押し下げられる。中国を含むアジア新興国は 0.7%、中南米は 0.6%、ユーロ圏は 0.3%、日本では 0.6%の押し下げ効果となり、我が国においても景気後退の引き金となる可能性は大きい。米中貿易戦争がエスカレートすれば、世界経済へさらに大きな打撃を与え、日本が景気後退に陥るリスクも大きくなる。

このように覇権国である米中の争いが熾烈を極め、日本経済や企業に対しても大きな影響を及ぼしており、民間企業がどのようなことをリスクとして認識し、備えておくべきなのか、次章以降で我々の考えを述べる。

第２章　企業経営における安全保障上のリスクと影響

第１節　企業を取り巻く安全保障上のリスク

（１）企業におけるリスク認識の現状

「はじめに」で触れたように、平成の時代において日本人は地震や洪水等の大災害を数多く経験した。また、自然災害以外にも、新型インフルエンザの流行や地下鉄サリン事件等、想定外の事象も経験した。そのようなリスクが多く存在する環境では、事業の継続を目的とした取り組みの必要性が高まるとともに、平時からその必要性を認識することが求められている。

日本政府は、日本における事業継続の取り組みの在り方の指針として、「事業継続ガイドライン第一版」を 2005 年 8 月に公表した。その後、新型インフルエンザや東日本大震災等から得られた教訓や、平時からの取り組み、継続的な改善の重要性等を踏まえ、2013 年 8 月に「事業継続ガイドライン第三版」を公表している。

本ガイドラインでは、「経営者は、事業継続マネジメント（BCM）を通じて企業価値を高める体制を構築し、競争力を高め、取引や利益等の拡大を目指すことが必要である。」と説明されている。また、平時から「事業継続に必要な取り組みを定期的及び必要な場合に実施して経営環境の変化に応じて発展的に改善していくこと」や、「危機的事象の発生によって事業が中断または中断の可能性がある際に発動される緊急時の対応を計画すること（BCP）」の重要性も記載されている。

本ガイドラインの中で発生頻度や経営への影響度を軸に危機的事象をマッピングする際の例が示されている。【図 7】。

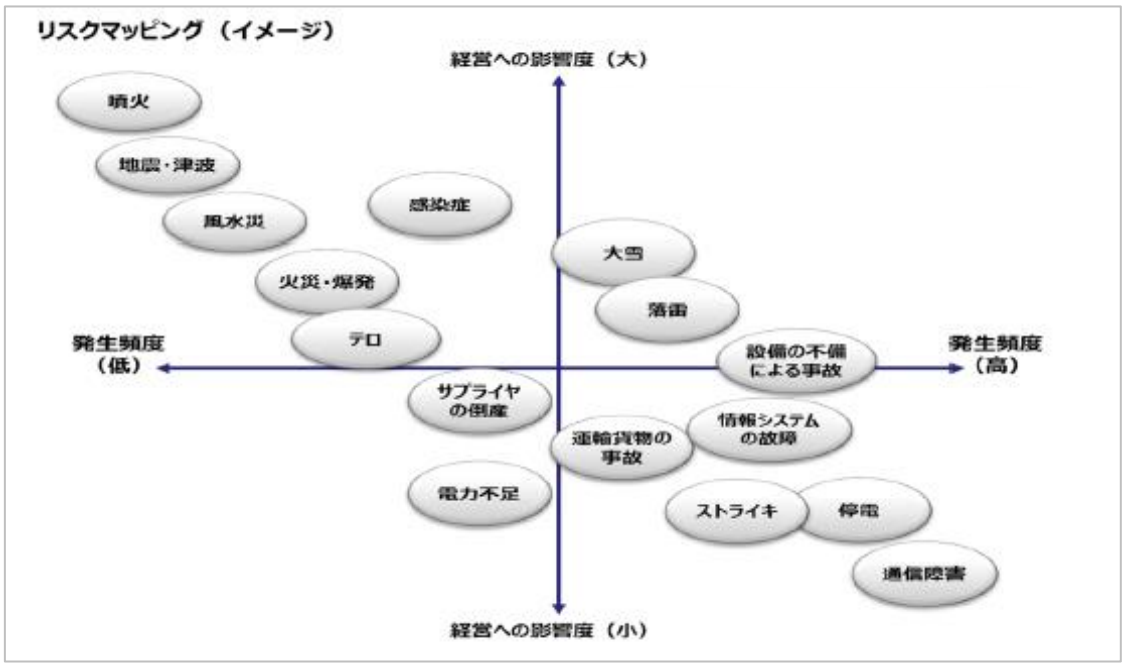


図 7:【出典】事業継続ガイドライン第三版（内閣府/2014 年 7 月）

災害や感染症等、我々が経験してきたリスクが数多くマッピングされているが、前章で触れた世界情勢の大きな変化に関連するものはほとんど触れられていない。中国の台頭に伴う東シナ海における緊張の高まりと比例する形で、2017 年における自衛隊のスクランブル発進の回数は過去最高を記録し、1 日あたり平均 3 回にものぼる【図 8】。

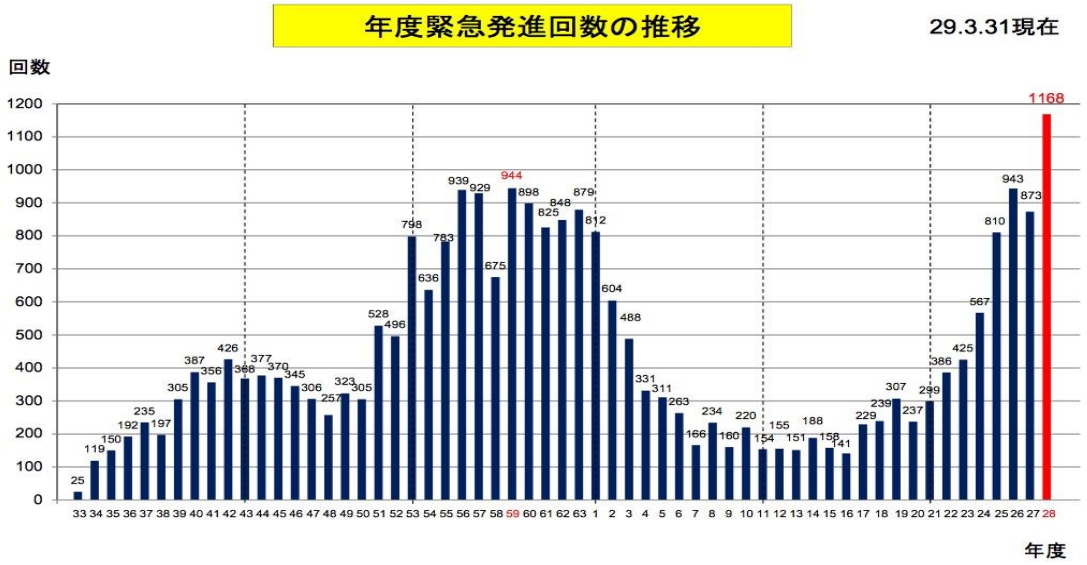


図 8:【出典】統合幕僚監部　報道発表資料（2017 年 4 月 13 日）

また、国立研究開発法人情報通信研究機構によると、2017 年に観測されたサイバー攻撃関連の通信は、2005 年の観測と比較すると約 500 倍のデータ量に達しており、サイバー空間への防衛に対する意識の重要性を裏付けるデータとなっている【図 9】。

年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125

図 9:【出典】 NICTER 観測レポート 2017 国立研究開発法人　情報通信研究機構　（2018 年 2 月 27 日）

これらを踏まえると、サイバー攻撃や武力攻撃に関連する災害に企業が巻き込まれる可能性は否定できないのではないか。サイバー攻撃は発生頻度が高く、企業が巻き込まれて被

害が発生する可能性は高い。一方、武力攻撃は発生頻度が限りなく少ないと想定されるものの、サイバー攻撃よりも被害は甚大となることが予想され、想定すべきリスクとしてマッピングするべきである。

（２）以降、サイバー攻撃や武力攻撃災害に関する企業の認識レベルについて、アンケート調査結果等を踏まえて論じていく。

（２）企業におけるリスク（サイバー攻撃、武力攻撃災害）への備えの現状

企業の経営活動に際し、何をリスクと定義づけ、それに対してどのような備えを行っているのかをサイバー適塾の会員企業を対象に調査した。

【アンケート結果】回答社数 21 社

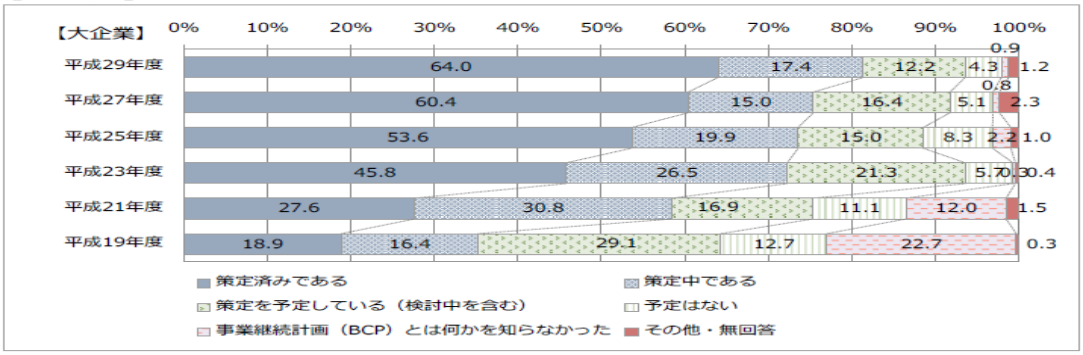
①BCP 策定について：策定している　（約 86%）
策定中である　（約 14%）
②想定される災害について（複数回答）：
・自然災害（地震・風水害・噴火等）　（100%）
・火災　（約 76%）
・事故　（約 57%）
・情報セキュリティ上のリスク（情報漏えい、システム障害、サイバー攻撃）　（約 57%）
・感染症（インフルエンザ等）　（約 67%）
・戦争やテロ、自社の不祥事　（約 48%）
・他国からのミサイル攻撃　（約 33%）
③従業員に対する BCP 対応の教育について：
・教育を行っている　（約 81%）
〈実施方法〉
・マニュアル配布による教育　（約 71%）
・e ラーニング等（ビデオ視聴含む）　（約 48%）

以上の結果より、BCP 策定は自然災害や火災、事故等の事象をリスクと想定し、対応スキルの習得は専らマニュアル、ビデオ視聴等による教育であることが明らかとなった。

また、2017 年度企業の事業継続及び防災の取り組みに関する実態調査（内閣府）によると、BCP を策定している（または策定中の）大企業は 8 割強、中堅企業は 5 割弱であり、大企業と比べて中堅企業の BCP 策定率は低いことがわかる【図 10】。

※大企業：資本金 10 億円以上かつ常用雇用者数 50 人超等、中堅企業：資本金 10 億円未満かつ常用雇用者数 50 人超等

【大企業】



【中堅企業】

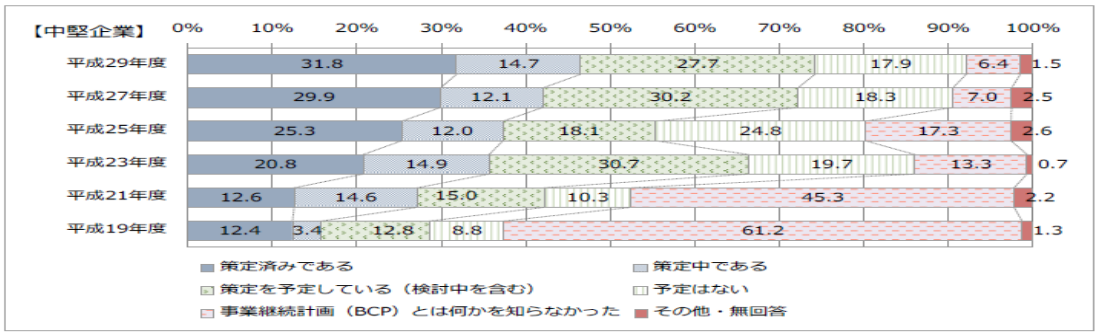


図 10:【出典】平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査（内閣府／2018 年 3 月）

大企業が想定するリスクについては、地震（約 98%）、火災・爆発（約 68%）、新型インフルエンザ等の感染症（約 69%）、通信（インターネット・電話）の途絶（約 61%、サイバー攻撃によるものを含む）が主要なものであり、テロ・紛争（約 34%）、他国からのミサイル攻撃（約 26%）をリスクとして想定する意識は低い【図 11】。

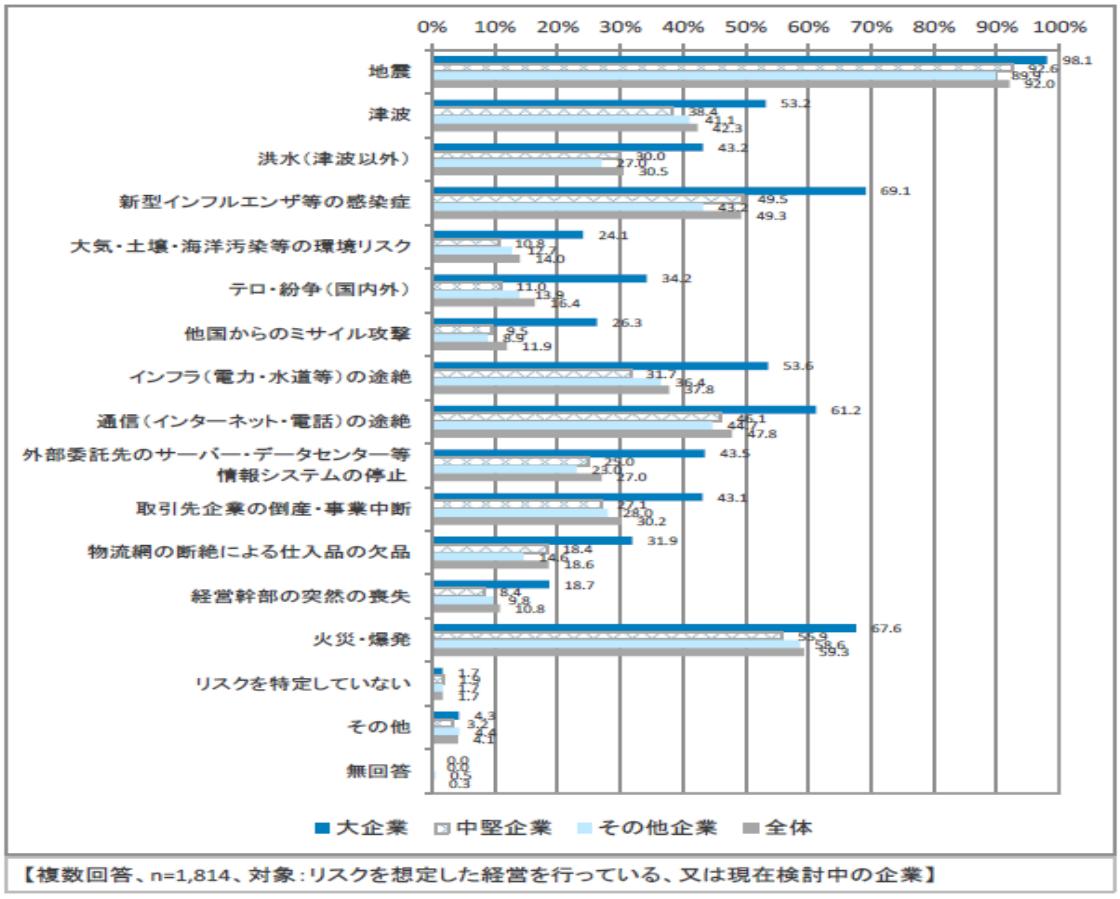


図 11:【出典】平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査（内閣府／2018 年 3 月）

サイバー適塾会員企業への調査及び内閣府調査における大企業の回答と、中堅企業の回答から、BCP 策定とリスク定義について、全体的にテロやミサイル攻撃である武力攻撃への備えや意識が希薄であることがわかる。

これらの結果を踏まえ、サイバー攻撃や武力攻撃への対策の現状とその課題について次章より把握していく。

第２節　サイバー攻撃対策

（１）「サイバーセキュリティ」の定義

サイバーセキュリティは、2014 年に成立し 2015 年に施行された「サイバーセキュリティ基本法」第 2 条の中で定義されている。なお、2015 年に日本年金機構が不正プログラムの一つであるマルウェアに感染、情報漏洩が発生した問題を受けて、「サイバーセキュリティ基本法」はその後一部を改正。2016 年 4 月 15 日、参議院本会議で「改正サイバーセキュリティ基本法」および「情報処理促進法」が賛成多数で可決、成立した。

「サイバーセキュリティ基本法」第 2 条のポイント
- ·サイバーセキュリティとは、サイバー攻撃に対する防御行為であること。
- ·何を防御するのかについては、情報データを防御すること。
- ·どこを防御するのかについては、IoT デバイスとネットワークを防御すること。

上記のポイントを踏まえると、「セキュリティが保たれている」ということは、情報データを防御するために、IoT デバイスやネットワークを安全かつ信頼できる状態に維持管理することを意味する。

（２）「サイバーセキュリティ」上のリスクが拡大した背景

パソコンやスマートフォンの普及に伴い、様々な産業をまたがった社会インフラにおいて、あらゆるモノがインターネットに繋がる IoT が急速な広がりを見せており、利便性が増している。その一方で、「セキュリティが保たれている」という状態を実現することが非常に難しい時代となっている【図 12】。

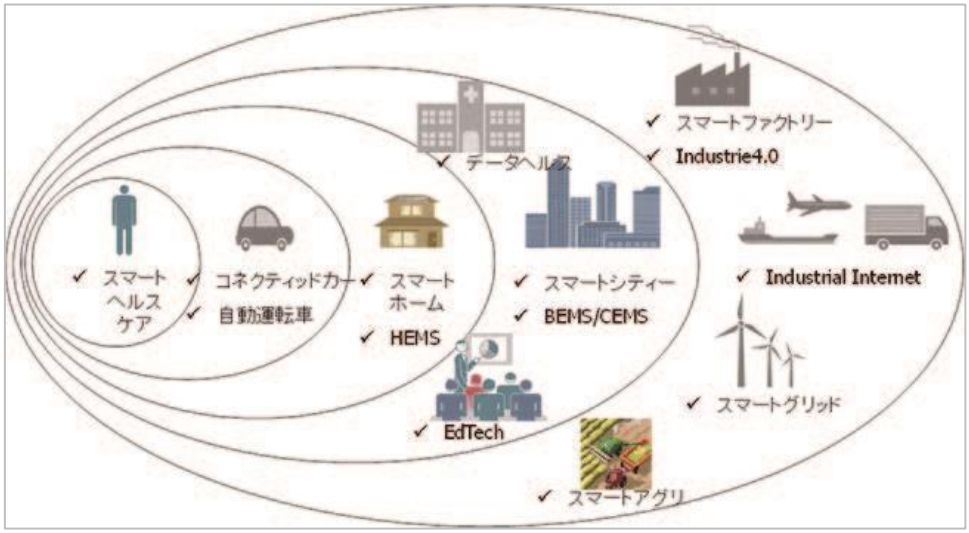


図 12:【出典】MRI トレンドレビュー　IoT が拓く未来社会（2015 年 12 月 10 日）

世界の IoT デバイス台数の推移は 2013 年以降右肩上がりで伸び続け、2020 年には 300 億台の大台に乗る見通しであり、サイバー攻撃対象の範囲・台数も今後さらに拡大すると考えられる【図 13】。

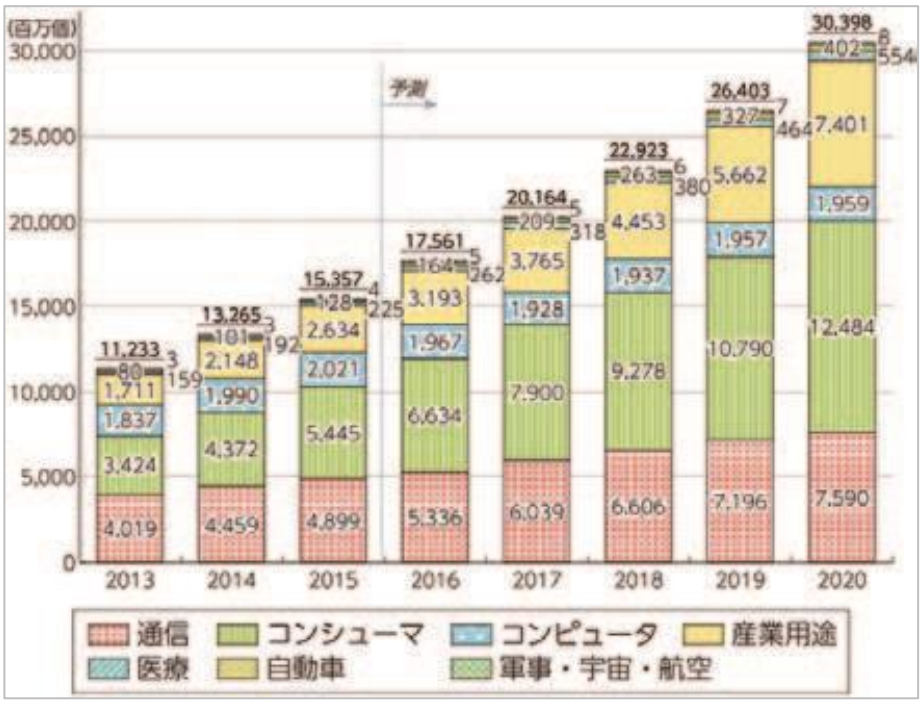


図 13:【出典】平成 28 年版情報通信白書(総務省／ 2016 年 8 月 8 日)

（３）サイバー攻撃の種類

サイバー攻撃は世界各地で続発しており、日本国内においても、機密情報の搾取や特定ターゲットの機能不全を目的とした攻撃が発生している。

サイバーセキュリティを担保するためには、「機密性（Confidentiality)」「完全性（Integrity)」「可用性（Availability)」の３つを維持することが重要である。サイバー攻撃は、情報の機密性（C）に対しては標的型メール攻撃等による情報窃取、完全性（I）に対しては Web サイトやプログラムの改ざん、可用性（A）に対して DDoS 攻撃（Distributed Denial of Service attack）やランサムウェア等による麻痺・破壊型の手法を取る【図 14】。

攻撃の種類	攻撃事例
①窃取型（C型）	「2011年衆議院サーバーハッキング事件」(2011) 何者かが、衆議院のサーバーに侵入し、約1ヶ月間にわたり不正アクセスをした。これにより、国会議員・秘書・事務局職員ら約2,600名以上のID・パスワードが流出し、流出したデータは中国国内のIPアドレスに送信されていた。 「日本年金機構情報漏えい事件」(2015) 何者かが、大量のコンピューターウイルスメールを年金機構の複数の職員に送信。それを開封した職員の端末から不正アクセスを許してしまったことによりシステムサーバーから約125万件の個人情報が流出した。
②改ざん型（I型）	「高松空港サイト改ざん事件」(2016) 何者かが、高松空港のWebサイトに不正アクセスし、時刻表ページに外部サイトへ誘導するための不正なコードを埋め込んだ。 「長野県河川水位情報サイト改ざん事件」(2017) 何者かが、長野県が運営する、雨量や河川の水位情報を提供しているWebサイトに不正にアクセスし、同サイトを閲覧するとマルウェアに感染するよう改ざんした。
③麻痺･破壊型（A型）	「2012年アノニマス日本攻撃事件」(2012) ハッカーの国際的ネットワークであるアノニマスが、同年に国会で可決された違法ダウンロード刑事罰化への対抗を目的に、財務省、自由民主党、民主党（当時）、日本音楽著作権協会などの公式ホームページに対してサイバー攻撃を行い、サーバーをダウンさせた。 「ランサムウェア Wanna Cry」(2017) 何者かが作成し全世界に展開したランサムウェアWanna Cryへの感染により、自動車メーカー・電機メーカー等、様々な業界で被害が拡大した。

図 14:国内で発生した主なサイバー攻撃事例

【出典】東京海上日動「TALISMAN」2018 年 11 月

（4）「サイバーセキュリティ」上の備えに対する課題

サイバー攻撃は、高度化・巧妙化し続け、前述の通り情報流出事故や機能不全等の被害は増える一方である。日本でも国家としてサイバーセキュリティの防衛策を強化する動きがあり、企業にも対策を講じる責任が求められている。しかしながら、先述したアンケート結果によると、企業ではサイバー攻撃に対する備えや対策がまだまだ不十分であると言わざるをえない。サイバーセキュリティ上のリスクに対する企業の備えが十分に整備されない課題は何か。以下にその主な内容を挙げる。

一つ目は、サイバーセキュリティに対する専門人材が不足していることが挙げられる。経済産業省が 2016 年に実施した調査結果によると、現在の情報セキュリティの人材不足は 13 万 2,060 人に及んでいる。企業においても、約半数が情報セキュリティ人材の不足を感じていると回答しており、必要人数を確保できていると回答したのは 26%にすぎない。さらに、日本で東京五輪が開催される 2020 年には、情報セキュリティ人材の不足数が 19 万 3,010 人まで増加する見込みである。

二つ目は、サイバーセキュリティに対する費用の問題が挙げられる。ひとたび情報流出が起きれば、企業イメージや事業そのものにとって深刻な影響を受けるが、事業効率を上げる IT 投資のように、企業は情報セキュリティに対して資金を投入していない。サイバーセキュリティの強化によって事業継続を確保することは、企業価値向上にもつながり、市場等か

らの信頼性が高まる。したがって、サイバーセキュリティの強化に費用を投入することは企業にとって「投資」をすることになるが、そのような意識をもった経営層はまだまだ少ない【図 15】。

サイバー攻撃は企業が直面するリスクでありながら、その対応策には企業間でも温度差があり、十分とは言えない状況にある。サイバーセキュリティの強化のためには経営層の意識改革が急務であるが、特に中小企業ではコスト面での圧迫、人材不足が顕著であり、個々の会社での対応が困難な現状にある。一方、すでにサイバーセキュリティ上の備えを行っている企業についても、サイバー攻撃手法の専門性が高まる中、継続的な専門技術者の確保が懸念される【図 15】。

このように、増大するサイバーセキュリティ上の問題に対して、個々の企業で対応力を高めていくことには限界がある。各企業が共通の経営課題として認識し、企業間が連携して対策を講じることが有効な手段だと考える。

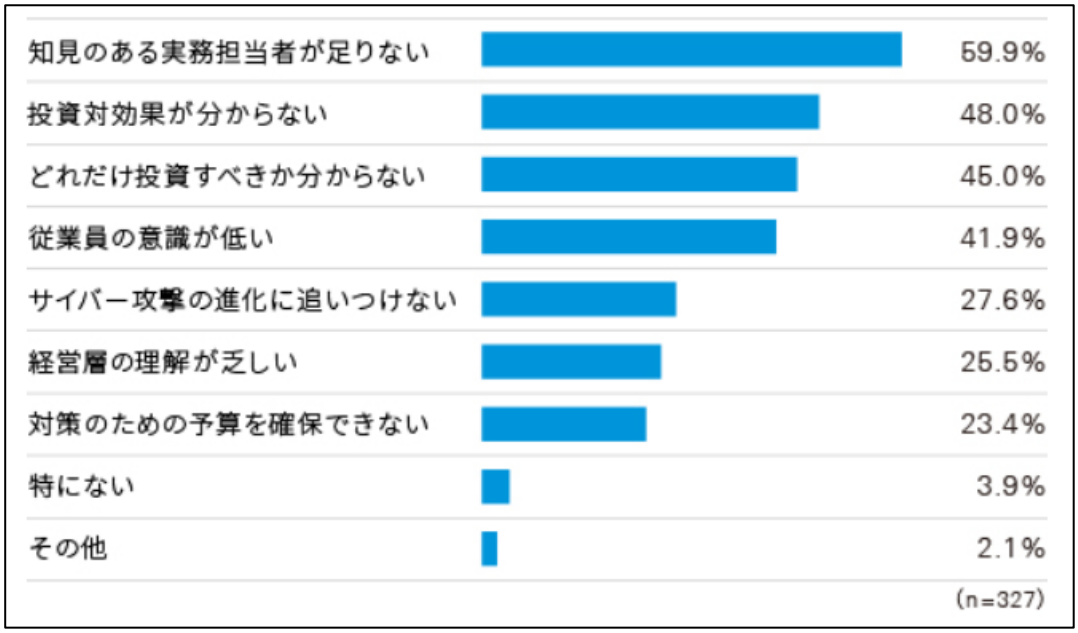


図 15：サイバーセキュリティ対策に取り組む上での課題
【出典】KPMG サイバーセキュリティサーベイ 2018

第３節　武力攻撃対策

（１）「武力攻撃災害」の定義

「武力攻撃災害」とは、『武力攻撃事態等における国民の保護のための措置に関する法律（国民保護法）』（2004 年法律制定）によれば、「武力攻撃により直接又は間接に生ずる人の死亡又は負傷、火事、爆発、放射性物質の放出その他の人的又は物的災害」と定義付けられている。なお、武力攻撃が発生した事態又は武力攻撃が発生する明白な危険が切迫していると認められるに至った事態を「武力攻撃事態」、武力攻撃事態には至っていないが、事態が緊迫し武力攻撃が予測されるに至った事態を「武力攻撃予測事態」といい、両者を合わせて

「武力攻撃事態等」と定義される。(『武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（事態対処法)』

この「武力攻撃事態」は次の４つの類型に分類されている。(『国民の保護に関する基本指針』より）

①着上陸侵攻
②弾道ミサイル攻撃
③ゲリラ・特殊部隊による攻撃
④航空攻撃

また、『武力攻撃の手段に準ずる手段を用いて多数の人を殺傷する行為が発生した事態または当該行為が発生する明白な危険が切迫していると認められるに至った事態』のことを「緊急対処事態」として定めている。いわゆるテロもこの中に含まれており、「攻撃対象施設等による分類」と「攻撃手段による分類」で区分し、国家として緊急に対処することが必要であることを明記している。

①攻撃対象施設等による分類

・危険性を内在する物質を有する施設等に対する攻撃が行われる事態
（原子力事業所・石油コンビナート・可燃性ガス貯蔵施設等の爆破、危険物積載船等への攻撃）
・多数の人が集合する施設及び大量輸送機関等に対する攻撃が行われる事態
（大規模集客施設、ターミナル駅等の爆破）

②攻撃手段による分類

・多数の人を殺傷する特性を有する物質等による攻撃が行われる事態
（ダーティボム等の爆発、生物剤・化学剤の大量散布）
・破壊の手段として交通機関を用いた攻撃等が行われる事態
（航空機等による自爆テロ）

（２）「武力攻撃災害」がもたらす影響

先述の「武力攻撃事態」と「緊急対処事態」から被る影響は以下の通りである。

(2)-1　武力攻撃事態

①着上陸侵攻

船舶により上陸する場合は沿岸部侵攻目標となりやすく、港湾設備が占領・破壊され、船舶や倉庫への被害を伴い物流網に甚大な被害が出る他、沿岸地域に居住する住民の退避等が発生する。

航空機による侵攻の場合は沿岸部に近い空港が攻撃目標となりやすく、国内の他空港も封鎖されることにより、航空ネットワークが寸断され物流・交通への影響が深刻化する。

いずれの場合も、影響が広範囲にわたるとともに、期間が比較的長期に及ぶことが想定される。

① 弾道ミサイル攻撃

発射された段階での攻撃目標の特定が極めて困難で、短時間での着弾が予想されるため、退避行動に繋げることが難しく、陸上、特に都市部に着弾した場合は被害が甚大となる。また、弾頭の種類（通常弾頭かNBC弾頭か）を着弾前に特定するのが困難であり、弾頭の種類に応じて、被害の様相や対応が大きく異なってくる。

③ゲリラ・特殊部隊による攻撃

被害は比較的狭い範囲に限定されるものの、突発的に発生するため事前の警戒が難しく、攻撃目標となる設備（原子力事業所、生活関連等施設等）の種類によっては、大きな被害が生ずる恐れがある。

④航空攻撃

弾道ミサイル攻撃に比べ、レーダー等によりその兆候を察知しやすいものの、予め攻撃目標を特定することが困難であり、防衛関連施設の他、都市部の主要な施設やライフラインのインフラ施設が目標となることが多く、住民への直接的な被害に加え、社会インフラの破壊により長期的に国民生活、企業の経済活動に大きく支障する事態を招く。

このように①から④のような直接的な軍事攻撃が行われた場合、被害規模は非常に大きなものとなる。例えば、1990年8月2日のイラクによるクウェート侵攻をきっかけに勃発した湾岸戦争においては、クウェート・イラク両国に甚大な被害を生じさせた。イラク軍によるクウェート侵攻後、多国籍軍に押されたイラク軍は焦土作戦の一環として石油設備を放火・破壊をした。そのため、約6百万バレル/日の石油が流出し消火活動だけでも15億USドルの経費がかかっている。イラク占領下及び戦争中におけるクウェート国内への被害額については、「国連補償委員会」によれば総額524億ドルの賠償額が明示されており、石油関連施設のみならず、社会インフラ全体に大きな被害が出る結果となった。

一方、イラク側についても、多国籍軍による空爆、地上戦の展開により、物的被害のみならず一般市民を巻き込んだ大きな犠牲を生み出すこととなった。カーネギーメロン大学ベス・オズボーン・ダポンテ(Beth Osborne Daponte)の調査によれば、空爆により3,500人が、同戦争全体としては10万人以上の一般市民の犠牲者が出たとされている。

(2)-2 緊急対処事態

①攻撃対象施設等による分類に基づく影響

・危険性を内在する物質を有する施設等に対する攻撃が行われる事態

原子力事業所等が破壊された場合、大量の放射性物質等が放出され、周辺住民が被ばくするとともに、汚染された飲食物を摂取した住民が被ばくする可能性があり、被害が長期化する。

石油コンビナート、可燃性ガス貯蔵施設等が爆破された場合、爆発・火災の発生により周辺住民に被害が発生するとともに、その施設からエネルギー資源の供給

が寸断されることにより、供給の減少に伴う資源価格の高騰を引き起こし社会経済活動への影響が深刻化する。

また、石油の危険物積載船等への攻撃に関しても、危険物の拡散により沿岸住民への被害が発生するとともに、港湾や航路の閉塞、海洋資源の汚染を引き起こし、社会経済活動の沈滞を招きかねない。

・多数の人が集合する施設及び大量輸送機関等に対する攻撃が行われる事態

大規模集客施設、ターミナル駅等において爆破が行われた場合、爆破自体による人的被害が発生する上、爆破の影響により施設が崩壊した場合、被害が多大なものとなる。

②攻撃手段による分類に基づく影響

・多数の人を殺傷する特性を有する物質等による攻撃が行われる事態

ダーティボム等の爆発により、爆弾の破片や飛び散った物体による被害、熱や炎による被害等が発生し、多量の放射線を浴びることにより体内の細胞機能に影響が出てガン等の発症率が上昇してしまう恐れがある。

生物剤・化学剤の大量散布は、人に知られることなく散布することが可能であり、感染した人々が移動することにより二次感染が起こって広域的に被害が拡大する恐れがある。またサリン等の化学剤は地形・気象等の影響を受けて、風下方向に拡散し被害を甚大にする恐れがある。

・破壊の手段として交通機関を用いた攻撃等が行われる事態

航空機等による自爆テロにより、搭乗している乗客・乗員はもちろんのこと、爆発・火災等の発生により攻撃目標近辺の住民に被害が発生するとともに、建物やライフライン等の被災に伴い、社会経済活動に支障が出るリスクがある。

これら①、②はまさにテロ攻撃として世界各地で発生している。国際的シンクタンクである経済平和研究所（IEP）の発表【図 16】によると、全世界におけるテロ攻撃による経済的影響は 2017 年において 520 億ドルと試算されている。2001 年の 9.11 米同時多発テロ以降、テロによる経済損失は 2003 年までは減少傾向であったが、2003 年にイラク戦争が勃発した後は増加傾向となり 2007 年には 410 億ドルとなった。その後過激派組織イスラム国（IS）によるテロ攻撃の多発により 2014 年には 1040 億ドルまでに達しており、テロ攻撃による被害の甚大さがうかがえる。

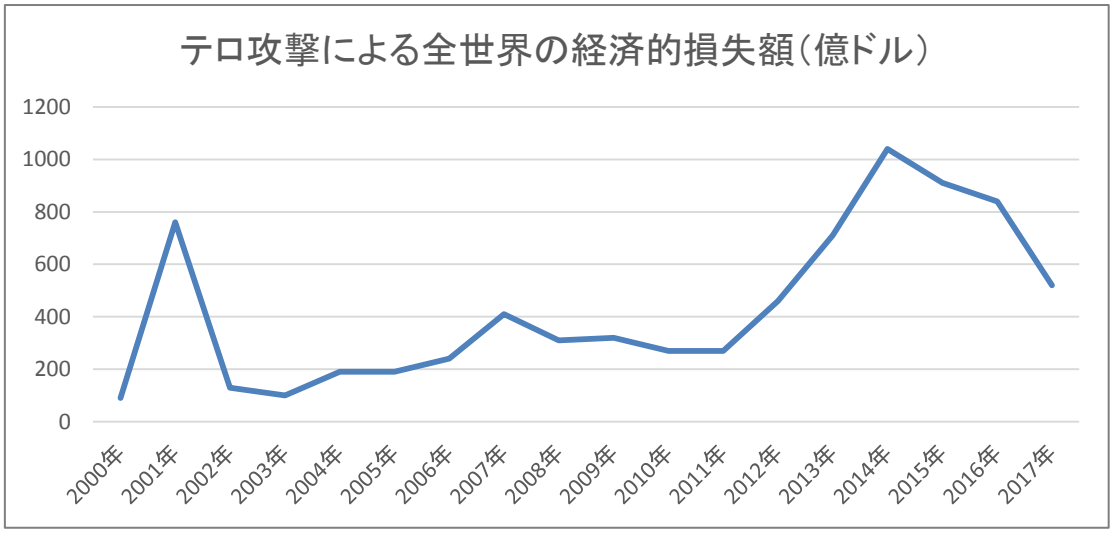


図 16:【出典】経済平和研究所（Institute for Economics and. Peace）発表を元に作成

（３）企業におけるリスクへの備えの課題

地震や津波、台風等々、度重なる災害により、各企業における自然災害に対する備え、所謂 BCP 策定は進んできた一方、武力攻撃災害に対する意識や備えは希薄である。

武力攻撃災害に備えるための企業の課題は何か、以下三点、主な課題を挙げる。

一つは、武力攻撃災害に対する企業経営者、従業員の被災に対するイメージ・想像力が希薄であり、真の危機感が醸成されていないことである。着上陸侵攻や弾道ミサイル、大規模テロ等の事態について、日本では起こるはずがないとの希望的観測に加え、企業における武力攻撃災害対応は限られており、国や地方公共団体が何とかしてくれるとの他人依存的な認識が根底にあるため、企業における備えは進まない。

一方、世界に目を向けると、スウェーデンでは自然災害等の危機や戦争等に対する防衛は全国民が関与すべきものであるとされており、「民間防衛」の意識が高い。イギリスにおいても 2004 年にテロ、ミサイル攻撃や自然災害、伝染病など多様な緊急事態に対する包括的な民間防衛の枠組みの構築を目的とした民間緊急事態法が制定されている。また、スイスでは戦争の危機に対してフォーカスした準備や心構えについて、国民へ広く周知されている。日本でも有事や災害時に召集できる予備自衛官制度が設けられているが、他国と比較すると現役自衛官に対する予備自衛官の比率が極めて低いことがわかる【図 17】。

	日本	米国	イギリス	ドイツ	韓国
現役 (a)	24.0万	143万	21.3万	28.5万	69万
予備役 (b)	4.7万	124万	27.3万	35.9万	450万
比率(b/a)	19.5%	86.7%	128.2%	126.0%	652.1%

図 17:【出典】Biz Style 予備自衛官等制度～企業の社会貢献のひとつのあり方～

二つ目は、不確実な武力攻撃災害リスクに対し、多大なコストと時間を投入するほど、経営資源に余裕がないのが実態である。特に中小企業においては、大企業に比べ BCP 策定率は

大幅に低く、その理由の多くは策定のための人材が確保できないとの理由であり【図 18】、武力攻撃災害リスクに備えるには程遠い状況である。

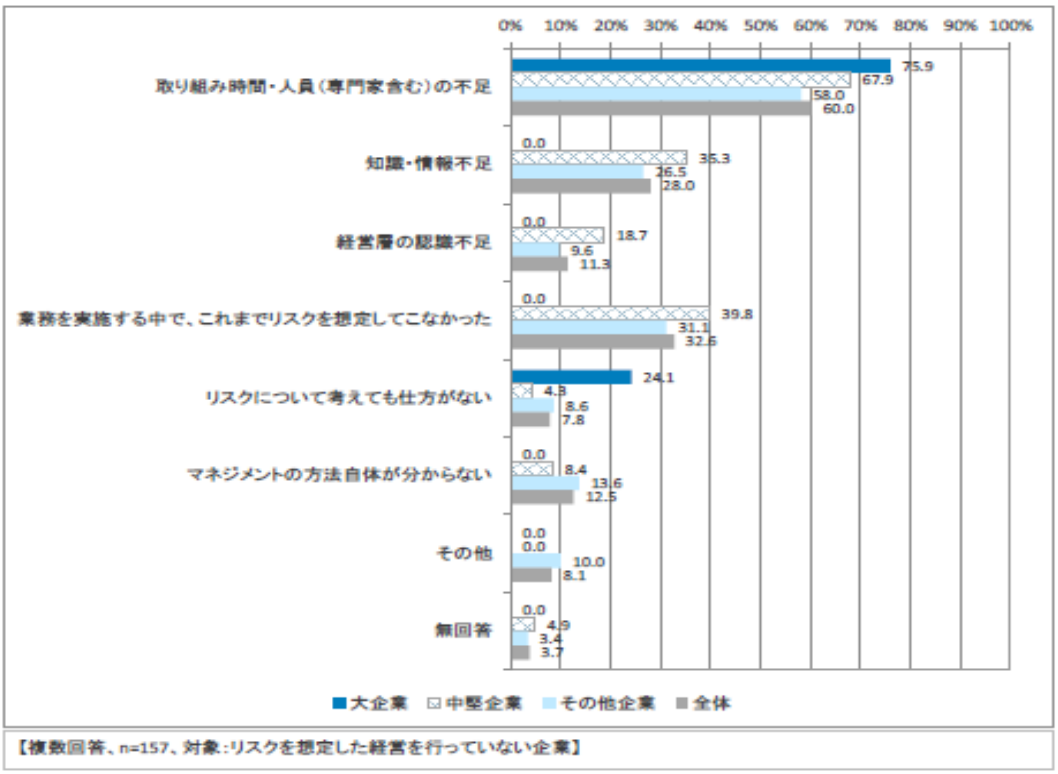


図 18:【出典】平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査（内閣府）

三つ目は、武力攻撃災害に備えるインセンティブが無いことである。企業に対する法令や規制もなく、国からの具体的な要請もないため、経営者にとって、武力攻撃災害に備えることが企業存続に必要不可欠であるとの認識は低い。更に、武力攻撃災害に備えることが企業イメージの向上に繋がるとの指標もないため、能動的な備えには繋がらない。

これまで述べてきた通り、「サイバー攻撃」と「武力攻撃災害」のいずれのケースにおいても、攻撃目標となった特定の箇所だけが被害を受けるものではなく、影響が広範囲に及び長期化する可能性が高い。特に高度にネットワーク化された現代社会においては、エネルギーや水資源といった生活の根底となるものの維持に加え、情報・通信インフラの維持が重要な課題となってくるため、これらの復旧が遅れた場合は、社会・経済全体の復旧活動に大きく支障をきたすこととなる。これは国民生活のみならず、企業の経済活動にも大きな影響を与えるものであり、企業経営においてもこれらへの備えと、発生時の迅速な復旧活動が重要となってくるが、一企業の自助努力には限界がある。特定の企業が「自分ゴト化」して取り組むだけでは実効性に乏しく、業界さらには社会全体で「みんなゴト化」して取り組まねばならない課題であると考える。

次章においては、この課題解決へ向けた我々の提言を示す。

第３章　提言

米国が「世界の警察」としての役割から一歩引き始めたのと時を同じくし、中国はアジアへの軍事支配を拡大させたことにより、世界は今「覇権挑戦期」の真っただ中にあると言える。我々日本人は、安全保障に対して真剣に向き合うことを長きにわたり回避してきたと言わざるを得ないが、安全保障上の「想定外のこと」がいつでも起こりうる時代に入っていることを強く認識しなければならない。そして、平和を希求する未来志向の「安全保障」意識の醸成に向けた一歩を踏み出さなければならない。特に企業経営においてはビジネスがグローバル化しており、安全保障上のリスク管理も不可欠である。本提言が実現し、民間企業の安全保障に対する意識変化を起こすことで、個々人の意識改革へと拡がり、ひいては日本を守る安全保障上の抑止力として機能することを期待する。

第１節　提言１　企業における安全保障リテラシーの向上

前章で述べた通り、国際情勢が緊迫化する一方、国民の安全保障の意識レベルは依然低いままである。10 頁で述べたアンケート結果からも読み取れるように、企業が巻き込まれる可能性の高いサイバー攻撃は、身近なリスクとして捉えやすいが、武力攻撃災害のリスクについては「自分ゴト化」がされにくい。そもそも安全保障や武力攻撃という事柄について触れること自体に抵抗感を感じる風潮が日本国内には根強く、議論することすらタブー視されがちである。我々塾生も半年程前までは安全保障に対する意識は希薄で、企業人が考えたところで無意味であり、仮に武力攻撃災害が起こったとしても、最後は国が何とかしてくれるだろうとの考えから無関心であった。ところが、サイバー適塾 17 期安全保障グループにおける約半年間の活動を通じて、メンバー各自の安全保障に対する意識は向上した。意識向上の要因は座学だけではなく、国内および海外視察を踏まえた自らの体験によるところが大きい。国防を担う自衛隊の方々や報道関係者、台湾・米国政府関係機関の生の声や施設見学等、自らの目で見て、聞いて、体験したことが安全保障に対する意識変革に繋がったのだと身を持って感じた。そこで、安全保障に対する意識醸成の第一歩として、机上での学びではなく、体感型の意識改革から始めていきたいと考える。また、これまでにない切り口として、地震や台風といった自然災害のみならず、サイバー攻撃や武力攻撃災害などの安全保障上のリスクにおいても防災・減災という枠組みの中で捉えることにより、身近なリスクとして感度を高めていくことができると考え、企業人の防災を含めた安全保障リテラシーを向上すべく、我々塾生が主体となって活動する以下のプログラムを提言する【図 19】。

なお、本プログラムはリスク対策の司令塔である「企業経営者」「リスク管理担当者」を対象として進めていくが、企業内での浸透状況を踏まえつつ、最終的には「一般社員」全体への意識改革、行動変容につなげていく内容としており、行動主体を我々企業人としている。

提言 1 についてはサイバー適塾 17 期安全保障グループの塾生の力で実行可能な現実味のある提言を強く意識しており、企業人目線で安全保障を捉え、国に対して求めるだけの提言ではないところに、従来のものとは一線を画している。

（１）疑似体感プログラムによる意識改革【感じる】

防災意識を高めるためには、災害発生時、自らにどのような危機が降りかかるのかをイメージすることが肝要であるが、全国各地には様々な災害による被害想定の展示や、3D シアター、体感型防災施設などが複数あり、防災への関心を高める工夫がなされている。例えば東京消防庁では昨年 4 月、災害を疑似体験できる国内初の VR 防災体験車の運用を開始しており、その反響は大きく、東京都民の防災意識は向上している。現在は自然災害に係る疑似体験施設が中心となっているが、VR を活用すれば武力攻撃災害においても疑似体験は可能であり、実際に災害を体感できる機会を与えることで危機意識の醸成に繋げることができる。

また、サイバー攻撃の脅威についても体感プログラムはあり、簡単なサイバー攻撃の体験や、現状の脅威と対策の重要性を認識するワークショップをマイクロソフト社等の民間企業が主催している。このようなプログラムを通じて、攻撃側の視点に立った自社のシステムの脆弱性を認知し、その対策の重要性に対する理解を深めていく。更に、日進月歩の IT 技術に対するリスクについて、一社単独による備えには限界があることを示し、リスクの極小化へ向けた企業間連携の必要性について考える機会を与える。

（２）防災関連機関との交流【理解する】

自然災害や事件、事故、サイバー攻撃等の有事の際、消防や警察、自衛隊、医療関係機関等は重要な役割を果たしているが、企業は防災関連機関の活動内容についてどこまで理解できているだろうか。ここまで備えておけば、あとは各機関が何とかしてくれると、他人事として捉えていないだろうか。災害が起きた際、人的・物的被害を最小限に食い止めるためには、各機関との連携は必要不可欠であり、平時からその役割や活動について理解しておくことが重要である。そこで、災害に対する危機意識や備えについて、より現実的な理解を深めるため、机上で学ぶのではなく、各機関に従事している方々との交流を図る場を設け、身を持って学ぶ機会が必要と考える。災害の最前線に立つ方々と日頃から気軽に交流し、相互理解を通じて、自然災害のみならず、武力攻撃災害やサイバー攻撃を含めたあらゆる災害について、より現実的な危機意識や備えを学ぶ機会を創出する。これは、企業側の危機意識や備えが向上するだけではなく、各機関に従事する方々にとっても企業の防災レベルを把握できる場となるため、官民のより補完的な関係の構築により、防災認識の齟齬を回避でき、被害の極小化に繋げることができる。

（３）各機関との合同訓練を通じた BCP の有効性の検証【見直す】

上述のように各機関との交流で、企業は平時からどのような対策をしておくべきか、災害発生時にどのように動くべきかを学び、今までの視点では気づかなかったリスクとその対策の洗い出しにより、まさに「想定外」のリスクを「想定内」にすることが可能になる。

災害の発生を想定し、リスクを洗い出すとともにその対策を具体化させて自社の BCP に反映させていくことが重要であり、その対策が有効に機能するかを定期的に検証する必要

がある。また大規模な災害を想定した場合には、自社単独の検証ではなく、各機関との定期的な合同訓練を通じて防災に関する最新の情報を入手し、より実効性の高い BCP へと更新していくことができる。

（４）実体験プログラム【行動する】

大地震など大規模災害の発生時においては、都道府県知事からの要請により自衛隊の災害派遣が行われることがある。要請主体は都道府県知事ではあるものの、実際の救援活動を円滑化させるために企業の立場としてどのような連携ができるかを、最寄りの自衛隊と確認しておくことが重要である。自衛隊には有事や大規模災害時に召集され、自衛官として自衛隊の活動の後方支援や基地警備等を担う予備自衛官という制度がある。しかし、【図 17】の通り他国に比較するとその比率は低く、認知度も低いのが現状である。一方、安全保障に対する国民意識の高い国は総じて国防関係者との距離が近いと国内視察で伺った。国防を担う現役自衛官や予備自衛官を身近な存在として捉えてもらえるよう、気軽に交流できる場を設け、安全保障に対するタブー視を払拭し、大胆な意識改革を図っていくため、予備自衛官の任務をより深く認知できる短期間のプログラムを企画する。

＜予備自衛官体験プログラム（３日間）＞

（１日目）コンセプト：『自分を守る』（防災）

【目的】危機管理意識の醸成、危機対応力の向上

【内容】机上：災害時の心構え、避難方法等（『自衛隊防災Ｂｏｏｋ』より）

体験：災害時の避難方法、防災テクニックの実演

交流：現役自衛官との意見交換

（２日目）コンセプト：『仲間を守る』（救援）

【目的】災害時救援活動のスキル向上、予備自衛官制度への理解醸成

【内容】机上：大規模災害発生時の対応、救命救急スキルの取得

体験：自衛隊災害派遣時の業務体験（後方支援等）

（３日目）コンセプト：『国を守る』（国防）

【目的】日本の安全保障体制の状況、自衛隊活動への理解促進

【内容】机上：日本の安全保障及び自衛隊活動の現状

体験：野外演習訓練視察、装備品見学

交流：現役自衛官との意見交換

予備自衛官制度が充実、発展していくためには企業の理解と協力も必要である。雇用者が一定期間従事することは、企業にとっては負担となるが、これは一種の企業の社会的責任（CSR）と考えることもできるのではないか。企業が環境問題に取り組むように、日本の防衛に協力することもまた社会貢献の一つだと言える。

そのためにはまず予備自衛官制度そのものがより広く社会に認知される必要があると考

え、実体験プログラムをそのきっかけとする。

（５）企業における安全保障意識の醸成プログラム【高める】

貿易・直接投資・国際金融等の企業活動を促進する前提は、世界や地域が安定していることであり、その環境を作りだすのが安全保障政策である。領土・権益・国民の安全を守り、地域を安定させる安全保障政策なくして、企業活動に従事することはできない。グローバルにビジネス展開するためには、国際政治学・安全保障論の理解が不可欠であり、企業人として身につけるべき必要な知識を習得できるカリキュラムを提供する。

＜習得すべき知識＞

１.現在の安全保障体制に至った歴史的背景を知る。

世界とその中の日本に存在する様々な諸課題についての歴史的な経緯を理解する。

２.安全保障のグローバル・スタンダードを知る。

現在の国の安全保障体制は、安保法制の整備等で徐々に実用性を高めているが、世界の標準的な水準と比較すると、制度面、予備面共に制約が厳しく、現在の安全保障体制が必ずしも十分ではない。世界第６位の海洋面積を守り、また同盟国や先進国の一員としての責務を果たし、安定した経済活動を続けていくための策を以下の視点で考察する。

短期的視点:世界標準に比べて足らざる点を洗い出し、対応策を考える。

長期的視点:標準的な水準に近づけるための抜本策を考える。

３.将来の課題を見据える。

水や食料問題などの地球全体が直面する長期的課題についても「広義の安全保障」として捉える。

図 19：安全保障リテラシー向上プログラム

第２節　提言２　関西防災連合の設立（連携）

関西には様々な業種の有力企業が存在し、財界活動を通じた情報交換の場も多く、企業が連携しやすい環境が整っている。このビジネス風土を活かし、安全保障分野も含めたあらゆる災害に備えるための企業間連携機関「関西防災連合」（以下「関防連」という）を設立し、防災における一企業の自助努力の限界を補完しながら、地域全体の防災力及び安全保障における抑止力の向上を図っていく仕組みづくりを提言したい【図 20】。

（１）設立目的

関防連の設立目的は安全保障分野を含めた関西全体の防災力向上である。自然災害のみならず、各企業が自助努力では到底カバーできない武力攻撃やサイバー攻撃等、あらゆるリスクに対する備えについて関防連を通じて学び、企業それぞれのリスクマネジメントが向上することで、結果として関西全体の総合安全保障における抑止力が高まることを目指すものである。

（２）活動内容

①安全保障リテラシー向上プログラム（提言 1）の企画運営

常に内容の見直しを行い、最新の知見を盛り込んだ「充実・発展型」のプログラムを

実施する。特に本章第１節（３）「関係機関合同訓練プログラム」の実施結果を点検・評価し、ノウハウを蓄積する。リスク毎の関係機関の動きを整理し、官民の補完的役割の強化を図る。

②防災推進企業認定制度の運営（提言３にて後述）

防災推進企業認定制度の運営管理、普及を行う。主な内容は、認定企業を拡げるため、啓発パンフレットの作成、配布を行うとともに、企業にとって魅力ある認定制度になるよう、認定要件の適宜見直しを行い、その価値の向上に努める。

③防災関連機関・参加企業間の連携

関防連参加企業、防災関係機関との連携を密にし、体制整備を行う。大規模災害への備えに万全を期するため、関防連間で相互に応援する仕組みを構築、充実させる。また、関防連参加企業が、効果的な災害対応ができるように、平時から防災関係機関との情報共有を図り連携体制を確保する。そして活動範囲を関西エリアや日本国内のみにとどめず、国外の経済団体との積極的な交流を実現し、海外の安全保障意識を学び共有する機会を提供する。

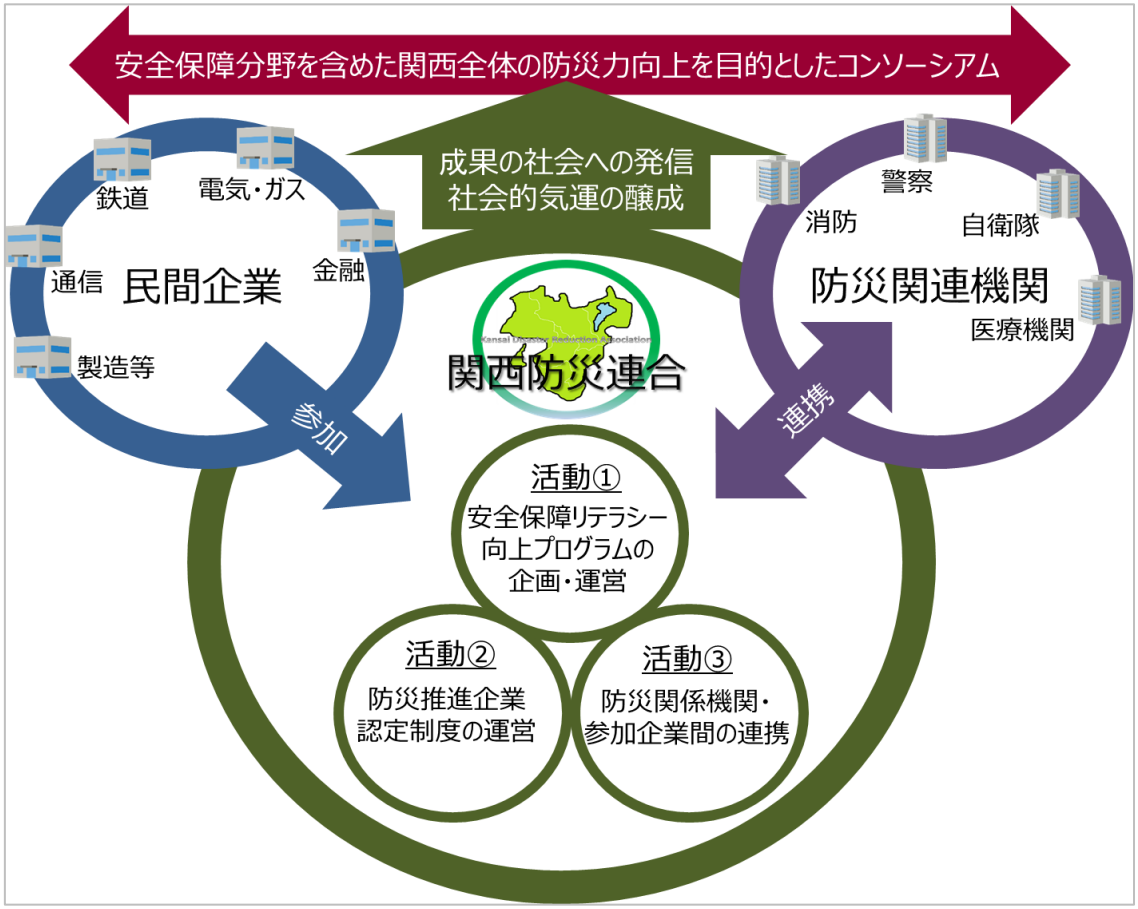


図 20：関防連イメージ

（３）参加企業のメリット

①低コストでの BCP 対策の立案およびリスク対策レベル向上

参加企業の BCP 策定に関する情報共有を行うことにより、これから BCP を立案する企業や対策内容の見直しを検討する企業は情報収集や策定ノウハウに関するコストを軽減することができる。

②セキュリティ専門人材の育成およびスキル向上

関防連が企画、実施する安全保障リテラシー向上プログラム（提言 1）を受講することにより、価値ある発想・行動を引き起こす基になる素養を高めることで危機管理意識の高い人材創出及び個々のスキル向上を実現する。

③会員企業間の新規取引拡大

会員企業が提供するリスク管理に役立つ商品やサービスをデータベース化し、ビジネスマッチングを行う。提供した会社が営業活動を行うことを可能とし、会員企業が相互に防災力を高めつつ、ビジネス面でのメリットに繋げる。

④会員企業間における連帯感の醸成

共通の連携ロゴマークを設定し名刺に連携マークを入れる等、会員企業における統一的・横断的な取組みを展開することで、平時より各社役員、社員の連帯感を醸成し、被災時の相互扶助を実現する【図 21】。

図 21:関防連ロゴマーク

（４）設立に向けた展開

まず災害時のインフラ連携、サイバー攻撃によるインシデント共有等テーマごとにワークショップを開催し、共通の課題や理念によって関係性を構築しやすいメンバー

で運営を行う。それを土台として、情報交換や相互理解等、できることから連携をはじめ、必要な時に必要なメンバーだけが集まるなど、その連携が継続しやすい環境を整える。また、連携が形骸化しないように、テーマごとに幹事となる企業を選定し、その有効性を確認しつつ、組織化を検討していく。

第３節　提言３　国による企業へのサポート

課題でも述べた通り、民間企業にとってサイバー攻撃や武力攻撃災害に備えるための国からのサポートが乏しい。企業の性質を理解し、能動的な備えに繋げるため国によるインセンティブが必要であると考え、その道筋となる防災推進企業認定制度の導入を提言する。

（１）企業価値向上に繋がる防災推進企業認定制度の導入

前述の通り、企業が社会的責任の観点から環境問題に取り組むように、日本の安全保障に協力することもまた社会貢献の一つだと言える。しかし、安全保障への取組みはCSR活動とは異なり、積極的に取組む必要性を認識しがたい。そこで、一定の要件を満たせば「防災推進企業」と認定される制度を設け、認定されることが企業のメリットにつながる仕組みを国として取り入れることを提言したい。

防災推進企業認定制度の概要は以下のとおりである。

（２）認定要件

①～③のいずれかを満たせば認定する。

① 災害避難場所を設け、誰でも利用可能であること

1997年（平成9年）から始まった「子ども110番の家」制度では、児童等の年少者が不審者等に声を掛けられるなどして身の危険を感じたときに、地域住民の自主的な協力の下で保護する運動である。同様に、自然災害や武力攻撃災害の発生に備えて、災害避難場所を確保している場合に企業を認定する。自然災害に関しては、津波による被害が予測される沿岸地域における高所避難場所や自宅が被災して帰宅できない場合に、一定期間、避難生活を送るための場所等が該当する。一方、武力攻撃災害に対しては、核ミサイルや大陸間弾道ミサイルに備えたシェルターや紛争発生時に避難生活を送るための場所等が該当する。

② 予備自衛官が一定割合在籍していること

災害および防衛の面から、有事の際に駐屯地の警備や、通訳・補給等の後方支援の任務等につく予備自衛官が一定割合在籍している場合に認定する。

③ 防災対策に活用される寄付金制度の創設

自治体によっては寄附金の「使い道」を寄附者が指定できる「ふるさと納税」のように、企業が納付する税金の使い道を一部指定できるようにし、防災対策に活用され

る税金を一定割合納付している場合に認定する。利用用途の例としては、「災害対応避難場所の設置」「災害支援物資の購入」「自衛隊活動支援」等が挙げられる。

（3）認定取得の企業メリット

防災推進企業認定制度が効果的に機能するには国に頼るだけでなく、民間企業も防災推進の重要性を理解・認識して活動し、官民の両輪で取組まなければいけない。その結果「防災推進企業」と認定されることが、企業の社会的責任を果たすことに繋がり、結果として企業価値が向上し、優秀な人材の獲得にもつながる等、企業活動に好循環をもたらすことが最大のメリットである。

ただ一方で、企業は利益の追求も必要であることから、認定取得企業に対する補助金や減税等の優遇措置の検討も国に提言していきたい。

おわりに

沖縄を訪れた高校生が次のような感想文を残していた。

> 「戦争反対!!」では戦争はなくなりません。
> それを言ったら殺人だって同じです。いくら「殺人反対」と叫んだところで、その存在は人間である限りなくなりません。
> 「戦争反対!!」というスローガンが何の意味を持つのでしょうか。残念ながら人間同士の争いはなくなりません。国同士も然りです。一国の一撃が戦争を開始させるのです。
> 「何故戦争に至ったのか、それを再発させないために必要な仕組みは何か」の考察が貧弱に思えてなりません。
> 日本人よ目を覚ましなさい。
> あなたたちの政治、経済への無知、無学がまた戦争を呼び起こすのだ。
>
> （一部抜粋）

真摯に安全保障の問題に対峙しなければならないと衝撃を受けた瞬間であった。

今、世界情勢は大きな変革期にある。1951 年、吉田茂首相は日米安保条約を結び、防衛を米国に頼り、復興を急ぐ道を選んだ。だが、その吉田首相も晩年、こう書き残している。「いつまでも他国の力を当てにすることは疑問である」。米軍に依存していては同盟を維持できないと見抜いていた。同盟が当たり前の時代は終わろうとしている。

明治維新から 150 年が過ぎ、当時を振り返ると、日本は小さい国ではあったが大志を抱き、貧しい国ではあったが自立心を失わず、遅れた国ではあったが進取の精神に充ち溢れていた。翻って、今の日本はどうだろうか。

米国が「世界の警察」ではなくなった今、日本は、「開かれたインド太平洋構想（FOIP）」の提唱国として、東南アジア及び ASEAN 諸国においてリーダー的役割を担う責任がある。

まずは、サイバー適塾 17 期安全保障グループ塾生が、「リアル」な現実を直視し続け「自分ゴト」（個社毎の対応）から「みんなゴト」へと企業間のみならず官民の連携を図る中で、現実認識の輪を拡げ、「有事の際に稲むらに火を灯せるリーダー」となることで、その第一歩を踏み出していきたい。なぜなら、武力攻撃であれ、自然災害であれ、第一対応者は国民だからである。防災・危機管理に関しては官（行政）が一方的にサービスを供給し、民（企業・住民）はサービスの受け手である、という認識はまだまだ根強いように思われる。国民一人一人に自助の精神が無ければ、自らの安全すら確保することはできない。

自助の精神を高めるためには、平時から危機管理能力の維持・向上が不可欠であり、自然災害のみならず、武力攻撃災害においても「リアリティー」を持つことが重要となる。「リアリティー」を持ち、世界に目を向ければ、日本の安全保障体制の脆弱さにも気づくはずである。ただ、いたずらに軍事力を強化するのではなく、侵略する側が「たとえテロが成功し

ても、武力には決して屈しそうもない」と思わせるほどの心理的に強固な国を作れば、十分な抑止力となる。

本提言が、民間企業の安全保障に対する意識変革を起こし、個々人にも浸透させていくことで、ひいては日本全体の防衛力、抑止力強化に繋がることを期待する。

【参考文献等】

１．書籍及びレポート

五百旗頭　真	『戦後日本外交史（第三補訂版)』 有斐閣 2014 年
木内　登英	『トランプ貿易戦争　日本を揺るがす米中衝突』 日本経済新聞出版社 2018 年
グレアム・アリソン	『米中戦争前夜』ダイヤモンド社 2017 年
高坂　正堯	『国際政治　恐怖と希望』 中公新書 1966 年
高坂　正堯	『国際政治』 中央公論社 1966 年
高橋　洋一	『日中貿易戦争で日本は果実を得る』 悟空出版 2018 年
高橋　洋一	『世界基準の安保論がすっきりわかる本』すばる舎 2016 年
野中　郁次郎	『野中郁次郎　ナレッジ・フォーラム講義録』東京経済新聞社 2018 年
橋本　明子	『日本の長い戦後』 みすず書房 2017 年
森本　敏	『図説　ゼロからわかる日本の安全保障』　実務教育出版 2016 年
簑原　俊洋	『ゼロ年代日本の重大論点―外交・安全保障で読み解く』 柏書房 2011 年
簑原　俊洋	『「戦争」で読む日米関係 100 年 日露戦争から対テロ戦争まで』 朝日新聞出版 2012 年
湯浅　博	『中国が支配する世界』飛鳥新社 2018 年
沖縄県編	『沖縄から伝えたい。米軍基地の話。Q&A　Book』2018 年
防衛省編	『日本の防衛 - 防衛白書』2018 年
防衛省編	『平成 31 年以降に係る防衛計画の大綱について』2018 年
防衛研究所編	『中国安全保障レポート』2018 年

２．参照 URL

- 図表１：防衛省『平成 30 年版防衛白書
- 』(2018 年 9 月 28 日) http://www.mod.go.jp/j/publication/wp/wp2018/html/n12302000.html#zuhyo01020301 (2019 年 2 月 12 日閲覧)
- 図表 2：日本経済新聞『中国の主権認定焦点　南シナ海問題』(2016 年 6 月 30 日) https://www.nikkei.com/article/DGXLASGM29H88_Z20C16A6FF1000/ (2019 年 1 月 28 日閲覧)
- 図表３：東洋経済オンライン『「逆さ地図」で見る、中国にとって邪魔な日本』(2015 年 5 月 26 日)　https://toyokeizai.net/articles/-/70361 (2019 年 1 月 28 日閲覧)
- 図表４：産経ニュース『紅い浸入　一帯一路の陰で（上)』(2018 年 1 月 11 日) https://www.sankei.com/world/news/180111/wor1801110014-n3.html (2019 年 1 月 28 日閲覧)
- 図表５：日本経済新聞『中国、海洋強国へ着々　海外港湾 30 カ所に』(2018 年 2 月 24 日)　https://www.nikkei.com/article/DGXMZO27366670U8A220C1MM8000/ (2019 年 1 月 28 日閲覧)

- 図表７：内閣府『事業継続ガイドライン第三版』(2014 年 7 月)
  http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03_ex.pdf (2019 年 2 月 1 日閲覧)
- 図表８：統合幕僚監部　報道発表資料『JOINT STAFF PRESS RELEASE』(2017 年 4 月 13 日)　http://www.mod.go.jp/js/Press/press2017/press_pdf/p20170413_01.pdf (2019 年 2 月 1 日閲覧)
- 図表９：国立研究開発法人情報通信研究機構『NICTER 観測レポート 2017』(2018 年 2 月 27 日)　https://www.nict.go.jp/press/2018/02/27-1.html (2019 年 2 月 1 日閲覧)
- 図表１０：内閣府『平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査』(2018 年 3 月)　http://www.bousai.go.jp/kyoiku/kigyou/pdf/h30_bcp_report.pdf (2019 年 1 月 30 日閲覧)
- 図表１１：内閣府『平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査』(2018 年 3 月)　http://www.bousai.go.jp/kyoiku/kigyou/pdf/h30_bcp_report.pdf (2019 年 1 月 30 日閲覧)
- 図表１２：株式会社三菱総合研究所『MRI トレンドレビュー　IoT が拓く未来社会』(2015 年 12 月 10 日)　https://www.mri.co.jp/opinion/column/trend/trend_20151210.html (2019 年 2 月 1 日閲覧)
- 図表１３：総務省『平成 28 年版情報通信白書』(2016 年 8 月 8 日)
  http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc121100.html (2019 年 1 月 28 日閲覧)
  図表１４：東京海上日動「TALISMAN」(2018 年 11 月)
  https://info.glasiaous.com/offering/talisman2 (2019 年 1 月 30 日閲覧)
- 図表１５：KPMG コンサルティング株式会社『サイバーセキュリティサーベイ 2018』(2018 年 9 月 26 日)　https://home.kpmg/jp/ja/home/media/press-releases/2018/09/cyber-security-survey2018.html (2019 年 1 月 28 日閲覧)
- 図表１６：経済平和研究所『Institute for Economics and. Peace』
  http://economicsandpeace.org/reports/ (2019 年 2 月 12 日閲覧)
- 図表１７：Biz Style『予備自衛官等制度～企業の社会貢献のひとつのあり方～』(2015 年 2 月 20 日)　http://vl-fcbiz.jp/article/ac072/a002738.html (2019 年 1 月 30 日閲覧)
- 図表１８：内閣府『平成 29 年度企業の事業継続及び防災の取り組みに関する実態調査』(2018 年 3 月)　http://www.bousai.go.jp/kyoiku/kigyou/pdf/h30_bcp_report.pdf (2019 年 2 月 12 日閲覧)

以上

【サイバー適塾　第 17 期　安全保障グループ　名簿】

［塾生］

［リーダー］	神野　靖子	日本生命保険相互会社
［サブリーダー］	井上　順夫	株式会社カウネット
	井作　康晴	大阪ガス株式会社
	上村　佳世	丸一鋼管株式会社
	岡野　宏俊	株式会社三井住友銀行
	岡本　太孝	株式会社ＮＴＴドコモ
	河畑　和宏	日本電通株式会社
	小寺　弘倫	西日本旅客鉄道株式会社
	中村　昇太郎	三菱商事株式会社
	野呂　真嗣	鹿島建設株式会社
	牧　剛史	富士通株式会社
	向　洋平	鴻池運輸株式会社
［担任講師］	簔原　俊洋	神戸大学大学院法学研究科　教授
［事務局］	山本　陽生	サイバー適塾運営協議会