CHUBU ASSOCIATION OF CORPORATE EXECUTIVES

自分事として捉える経済安全保障

～経営者のコミットメントと外部連携の推進でできることから始めよう～

令和６年３月

中部経済同友会

安全保障から経営を考える委員会

―目次―

概要

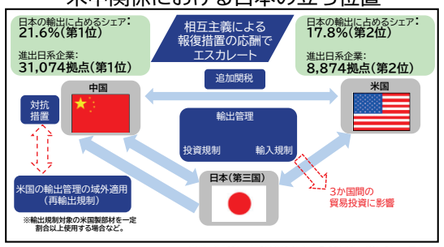
自分事として捉える経済安全保障
～経営者のコミットメントと外部連携の推進でできることから始めよう～

令和5年度
中部経済同友会
安全保障から経営を考える委員会

1 日本を取り巻く安全保障の状況と本委員会の目的

日本の立ち位置	• アメリカ、中国共に経済面での依存度が高く不可欠な2ヵ国である。 • アジアでは中国の影響力が強い国が多い。 • 米国にとって日本は重要な存在である。
現状	• 経済安全保障推進法が2023年から段階的に施行されている。 • 経営者も経済安全保障の観点で事業経営をすることが必要と認識し始めているが、「何から始めれば良いのか？」と悩まれている経営者が大半である。 • サイバー攻撃の対象は中堅・中小企業へ矛先が向いている。
本委員会の目的	• 企業規模、業種を問わず経済安全保障を経営課題として捉え、経営者自らが現状を認識し対策を講ずる契機とするため、サプライチェーン、サイバーセキュリティに焦点を当て各社の取り組みや参考事例を共有する。

米中関係における日本の立ち位置



出典：外務省・財務省資料や外国政府資料を基にジェトロ作成

資料の掲載期間が終了した為
閲覧できません

経済安全保障の要素　：企業として取組める内容　：政府主体の内容　：委員会として注力する部分

サプライチェーンの安定	貧困削減と社会的包摂	規制環境と政策の整備	経済情報の収集と分析	災害リスク管理	国内政治の安定
サイバーセキュリティ	科学技術の発展と教育	地域経済の発展と協力	エネルギー安全保障	知的財産の保護	社会的な安定と安全
産業基盤と技術力の強化	環境持続性と資源管理	インフラストラクチャーの整備	労働市場の安定と働き手の保護	外国直接投資の促進	経済政策と税制の調整
クライシスマネジメント	貿易と市場の安定	人口動態と労働力の管理	金融安定とリスク管理	国際関係と外交政策	グローバルな金融システムの安定
					軍事力と国防

出典：本委員会

2 経済安全保障の観点がなぜ経営者に必要なのか

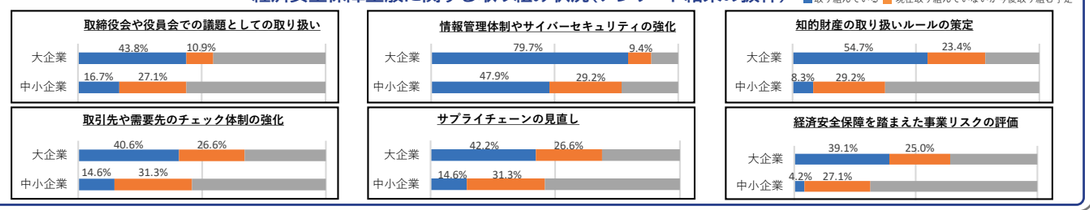
「経済安全保障推進法」が施行され、経済安全保障の時代となった。企業にとって、経済(事業)と安全保障(リスク)が重なる境目を見極め、安全保障面のリスクを排除し、事業推進していく必要がある。この見極めは、経営者にしかできない。企業経営は経済合理性だけではなく、リスク管理が今後ますます重要になる。データ保護やサイバー攻撃への対応についても、担当部署任せではなく、経営者が率先して対策を講ずる時代になったと認識するべきである。

3 本委員会の活動内容

3-1 会員へのアンケート(課題の抽出等)

経済安全保障全般	「取締役会等での議題としての取り扱い」、「取引先等のチェック体制の強化」、「知財取り扱いルールの策定」、「事業リスクの評価」等、大企業と中小企業で取り組みに大きな差がみられた。
サプライチェーンの強靭化	「材料等の調達コスト・物流コスト増大への対応」、「サプライチェーンのリスク分析・評価」、「人材の確保・育成」、「他企業との連携体制の強化」等が課題として浮かび上がった。
サイバーセキュリティ対策	「高度化・巧妙化するサイバー攻撃への対応」、「専門人材の育成」、「従業員教育の徹底」、「コスト負担の増大」等が課題として浮かび上がった。大・中小企業間での取り組み格差が大きかった。
企業(大/中小企業)間で求める事	サプライチェーンの強靭化、サイバーセキュリティ対策とも、双方から最も多かった要望は、「サイバーセキュリティ対策の共有」であった。
政府への要望	「サイバーセキュリティの強化」、「サイバーセキュリティ強靭化に関する助成金・補助金の充実」等。

経済安全保障全般に関する取り組み状況(アンケート結果の抜粋)　■取り組んでいる ■現在取り組んでいないが今後取り組む予定



※印の図表は日本経済新聞社の許諾を得て利用しています。無断複写・転載はご遠慮ください。

3-2 委員会主催講演会の有識者から学んだこと

サプライチェーン	米中対立などによる中国リスクが顕在化し、中国による経済的威圧や強国化への対応が必要となった。過度な中国依存からの脱却や持続可能なサプライチェーンの全体最適がポイントである。円安の進行によりサプライチェーンの見直しに向けた動きも加わり、企業経営の潮目が変わった。従来の経済効率優先型から、これからの経営判断はリスク対応力が重要な視点となる。
サイバーセキュリティ	サイバー攻撃から身を守るには情報共有を行い、競争ではなく協働することが重要である。 サイバー攻撃は経営課題であり、担当者任せでは限界があるため、経営者自ら関わることが重要である。

3-3 中小企業の取り組み事例の紹介と大手企業から学んだ教訓

アンケート結果から興味深い取り組みを実施している中小企業5社と本委員会会社大手3社、自動車関連大手1社の計9社に対し経済安全保障への取り組みをヒアリングした。注目すべき好事例の取り組み内容を紹介する。

中小企業の取り組み内容	
サプライチェーン対策	クラウド上でのダッシュボードにより日々の**情報共有・可視化**を実施
	調達先の分散化の促進(先物取引を導入されているケースもあり)
	クラウドシステムの導入などの**デジタル化の推進**
サイバーセキュリティ対策	重要顧客から注意喚起や事例の横展開の教育受領、**情報共有**
	大手顧客からの詳細なセキュリティチェック(2ヶ月毎の提示義務)
	セキュリティインシデント発生時の対応チーム(**CSIRT**)**を組織化**、ヒヤリハットの事例共有
	IT資産の**棚卸**、ソフトウェアの**バージョンアップ**、**バックアップ**データ取得

大手企業から学んだ教訓	
サプライチェーン対策	調達リスクマネジメントシステムの実行による**リスクの可視化**と事前の対策
	取引先との双方向での**情報共有**
サイバーセキュリティ対策	サイバー犯罪事例照会などの警察や公安調査庁などの**行政機関**や**外部機関の活用**
	セキュリティインシデント発生後の業務再開用**マニュアル整備**
	従業員向けの**教育**と標的型メール対応**訓練**の実施
	多要素認証の導入
共通	**経済安全保障室**の設置、運用
	行政や団体等の外部機関の活用(経済安全保障全般の**セミナーへの参加**による**情報収集**など)
	自社の狙われそうな技術・ノウハウの特定(**棚卸**)

4 本委員会の活動内容から得た知見

4-1 経営者に期待するマインドセット

◆ **自分事として捉える**
- 経営者自らが「**自分事**」として「日頃何をしたら良いのか」、「有事への対処法」など**危機管理意識を持ち**、サプライチェーンやサイバーセキュリティ対策への対応に**コミットメントする**こと。
- 万が一有事が発生した際には、**経営者自らが現場に立ち会い、指揮する**こと。

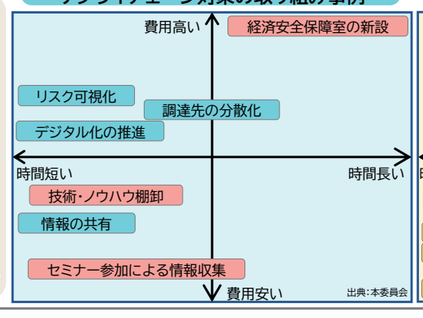
◆ **外部連携**
- 各社毎に**できることから自助努力で備えを進め、企業間の情報連携・共有する**こと。
- サイバーセキュリティ等を担う専門人材の育成、コスト負担への対応など、1社のみでは対応ができない課題は政府及び**経済・業界団体等の支援や協力を求める**こと。

4-2 全企業に求められること(委員会独自の想定)

費用をかけなくても実施できることから始め、備えることが最も重要である。

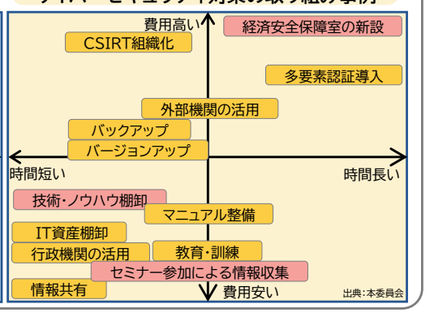
右図は、3章で取り上げた取り組み事例を実践する際、「費用」と「時間」を軸に、中小企業の視点で想定した委員会独自の図である。
今後、取り組みを検討される企業の参考となることを期待する。

サプライチェーン対策の取り組み事例



出典：本委員会

サイバーセキュリティ対策の取り組み事例



出典：本委員会

はじめに

1989 年の冷戦終結を契機に始まったグローバル資本主義は、2022 年 2 月のロシアによるウクライナ侵攻によって存続の危機を迎えている。新型コロナウイルスによるパンデミックや米中対立といった要素も加わり、世界情勢が急激に変化した結果、民主主義国家と権威主義国家の溝は深まり、新たな分断の時代に突入した。日本においては、国家及び国民の安全を害する経済活動に関連した行為を未然に防止することを目的に、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（以下、経済安全保障推進法）が 2022 年 5 月に成立している。企業は、これまでの事業戦略の抜本的な見直しを余儀なくされ、経営者には、新戦略立案に必須となる多岐に亘る経済安全保障についての深い理解と見識が求められている。

不透明感が増す社会によって安全保障上のリスクが多様化する中、外交、経済、エネルギー、食料等、世界情勢を踏まえて国家の進む道を幅広く学び、日本の立ち位置を認識することが、経済安全保障の取り組みを進める上での課題である。企業単位に目を向けると、持続的な成長を遂げ、顧客への供給責任を果たすため、サプライチェーンや製造拠点の再構築を刻々と変化する情勢や新しいルールに呼応して行うことが有用である。そのためにも、個々の企業による取り組みを活性化させることに加えて、サプライチェーン及び地域で連携した団体戦として、経済安全保障の取り組みを推進することが重要である。

当委員会で実施したアンケート結果によれば、同友会会員企業の中でも、大企業を中心に経済安全保障に対する高い意識を持ち、専門部署の設置等の取り組みを一部では始めているが、中堅・中小企業の多くが経済安全保障に対する関心を持つ半面、社内規定・方針の策定等、具体的にどういった内容から取り組みを始めればよいのか、模索していることが明らかになった。また、ロシアによるウクライナ侵攻により、企業規模を問わず 7～8 割の企業が、何らかの影響を受けていることが分かった。とりわけ輸出入における手続き増といった実務的な影響に加え、関税を含む規制強化、資材・エネルギーの仕入価格の高騰や物流コスト増加等に伴う事業活動への影響が大きいことが浮き彫りとなった。

本報告書では経済安全保障の要素のうち、製造業が多い中部圏にとって重要度・緊急度の高い経済安全保障推進法の制度に則した「サプライチェーンの安定」「サイバーセキュリティ」の 2 点に着目し、言及した。また、中小企業を主なターゲットとして、経済安全保障にこれから取り組み始める、あるいは取り組みを加速することができるような情報の提供を心掛け、取り組む意義や考える視点、具体的な取り組みについて先進的な活動を進める企業へのヒアリングなどで得られた事例を交えながら解説した。中部地区は製造業を中心に多くの企業が集積しており、これらの企業が業種や競合の垣根を越えて連携/協調することで、1 社単独では対応できない経済安全保障という難題に対して共に乗り越えることができると考える。

本報告書が経営者の皆様にとって経済安全保障にどう対峙すべきなのかを考える上でのヒントとなり、会員企業と地域経済発展の一助になれば幸いである。

令和 6 年 3 月

中部経済同友会　安全保障から経営を考える委員会

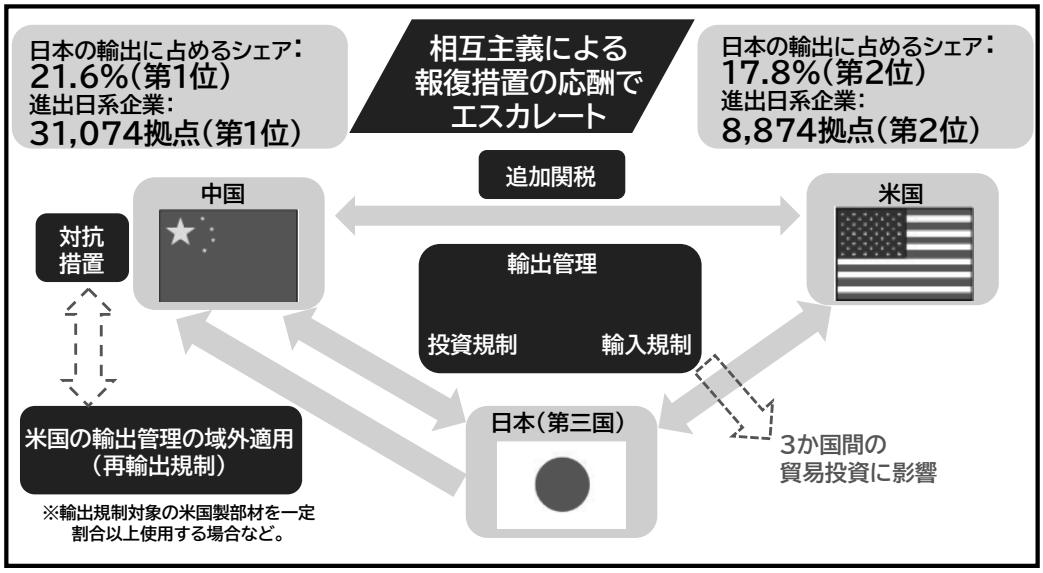
委員長　永井　淳

第１章　日本を取り巻く安全保障の状況と本委員会の目的

１．１　米中関係における日本の立ち位置

1989 年の冷戦終結を契機に、中国はグローバル化の波に乗り、急激な経済成長と軍事力の増強を続けている。その結果、トランプ米政権期に軍事とも密接に関わる先端技術をめぐり、米中の覇権争いが激化した。米国は、軍事転用の恐れがあるとして、中国通信機器大手、華為技術（以下、ファーウェイ）等への輸出規制を強めたほか、中国の知的財産侵害を理由に制裁関税をかける「貿易戦争」が、2018 年から本格化している。米中間の経済対立が常態化する中、両国のデカップリングは拡大傾向にあり、その影響は当事者だけにとどまらず、サプライチェーンの分断、国際貿易や投資の鈍化等を通じて、第三国にも及んでいる。日本企業にとっても、米国と中国は貿易投資の最大相手国であり、その動向は様々な影響を受けると考えられる。（図表 1-1）

【図表１－１】

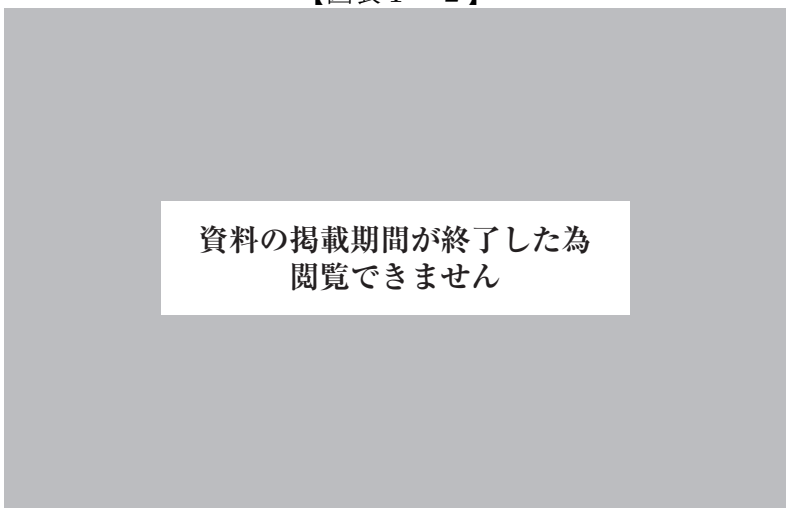


（出典：外務省・財務省資料や各国政府資料を基にジェトロ作成）

現在、日本企業による対米直接投資残高は一貫して増加傾向にあり、2022 年には約 7,752 億ドルに達し、2019 年から 4 年連続、世界最大の対米投資国となった。また、日本企業によって創出される米国における雇用創出数は、2021 年には約 96 万人に達している。研究・開発（R&D）分野への投資額も世界第 2 位の対米投資国となるなど、米国産業の生産性向上に大きく貢献している。

一方、中国は日本の最大の貿易相手国であり、中国にとっても日本は 3 番目の貿易相手国となっている。日系企業の海外拠点数も中国が第 1 位となっており、日本企業による対中投資は極めて多く、日中間の貿易・投資などの経済関係は、非常に緊密である。加えて、中国は「一帯一路」構想の推進と地域的な包括的経済連携（RCEP）協定への加盟を通じて、米国をはじめとする先進国市場への依存度を減らし、輸出市場の分散化を図っている。特に東アジア・東南アジアの国々では、経済面でも政治面でも中国から影響力を強く受けている国が多い。（図表 1-2）

【図表１－２】



（※出典：日本経済新聞（2011-01-06））

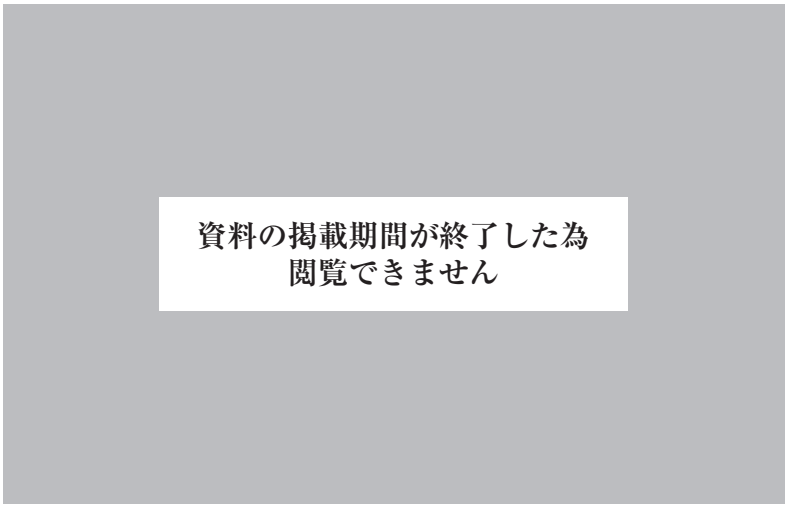
米中間での対立をきっかけに、両国で新たに導入された規制や措置は、両国それぞれで主導するルールの板挟み状態となるために、日本企業にも影響を与えている。米国政府が課す中国からの輸入品に対する最大 25%の追加関税は、日本企業が中国で生産したものにも適用されるため、日本企業にとって、生産基地としての中国の優位性が失われ、サプライチェーンのシフトが余儀なくされている。その一方で、中国政府が米国からの輸入品に課す追加関税は、日本企業が米国で作った製品にも適用され、米中による関税合戦に巻き込まれる形となっている。

さらに、米国の輸出管理規則（EAR：Export Administration Regulations）では、米国原産品および米国原産の規制対象品を組み込んだ製品や、米国原産品を製造の手段/ツールとして用いた製品を輸出する際、米国政府の許可が必要であると定めており、米国からの輸出時および輸出された国からの再輸出時にも適用される。そのため、日本企業にとっても米国製品を輸入し、部品等として組み込んだ製品を再輸出する場面で、対応が必要となる可能性がある。

１．２　現状（日本における経済安全保障政策）

前項のような情勢を踏まえ、日本は経済安全保障推進法（正式名称「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」）を 2022 年 5 月 11 日の参院本会議で可決、成立し、2023 年から段階的に施行している。この法律は、国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み制定された。安全保障の確保に関する経済施策を総合的かつ効果的に推進するため、経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本方針を策定するとともに、安全保障の確保に関する経済施策として、所要の制度が創設された。具体的には、法制上の手当てが必要な喫緊の課題に対応するため、(1)重要物資の安定的な供給の確保、(2)基幹インフラ役務の安定的な提供の確保、(3)先端的な重要技術の開発支援、(4)特許出願の非公開に関する 4 つの制度が創設された。（図表 1-3）

【図表１－３】

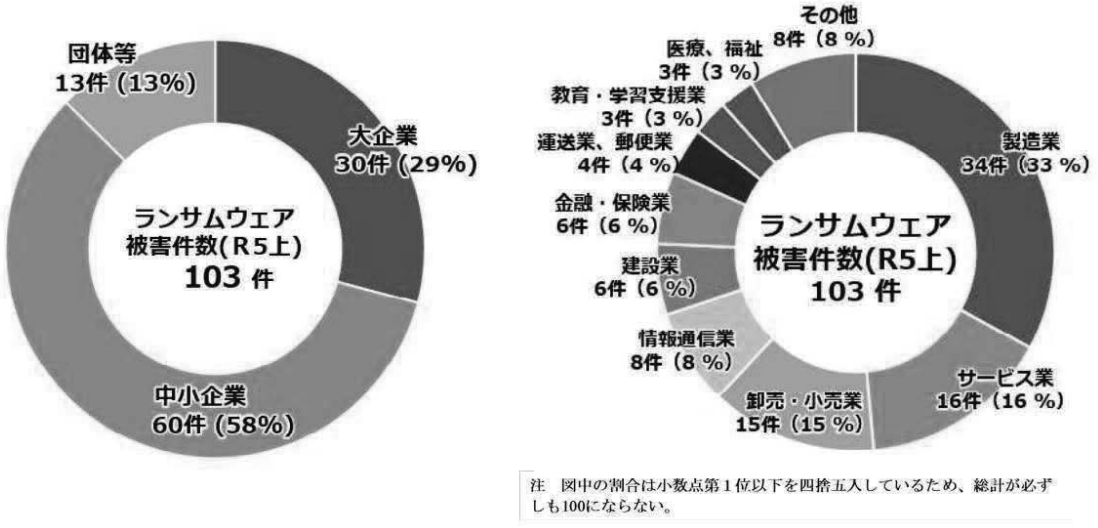


（※出典：日本経済新聞（2023-10-06））

この法律の施行により、経営者も経済安全保障を経営課題の重要ファクターの一つとして捉え、経済安全保障の観点から経営判断を行う必要に迫られているものの、企業規模により人材、金銭面での余裕がない企業にとっては「何から始めれば良いのか？」と悩まれている経営者が大半であるのが実態である。一方で、日々の経済活動において、企業規模に関わらず多くの企業がサプライチェーンにおけるリスクの脅威にさらされている。

その中でも特に、サイバー攻撃が昨今増加しており、攻撃対象が対策を施している大企業から中堅・中小企業へと矛先が向き始めている。IPA（情報処理推進機構）が毎年発行している社会的に影響が大きかったと考えられる情報セキュリティにおける事案のランキング「情報セキュリティ 10 大脅威」においても、組織（企業・団体）を対象とした脅威では、「ランサムウェアによる被害」「サプライチェーンの弱点を悪用した攻撃」が 1・2 位となっている。現在、ランサムウェアの被害の約 6 割は中小企業と言われており、業種については、製造業が最も被害を受けている。（図表 1-4）

【図表１－４】

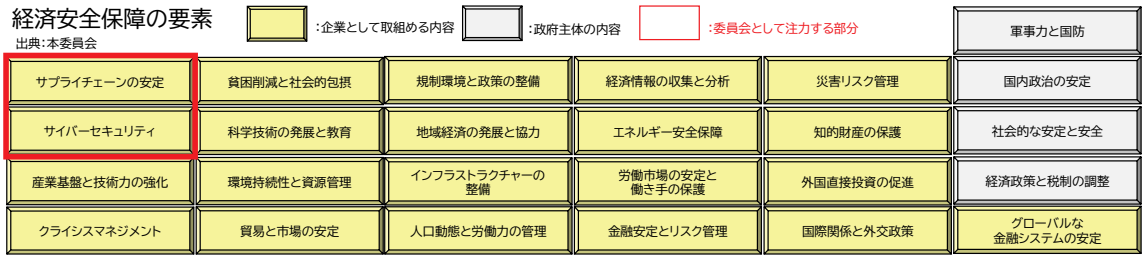


（出典：警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」）

１．３　本委員会の目的

本委員会では企業規模、業種を問わず経済安全保障を経営課題として捉え、経営者自らが現状を認識し対策を講ずる契機とするため、外交、経済、エネルギー、食料等、多数ある課題の中から、どの企業も重要度かつ緊急度が高い「サプライチェーンの安定」、「サイバーセキュリティ」に焦点を当て、各社の取り組み事例をヒアリングし、得た知見や参考事例を共有する事とした。（図表 1-5）

【図表１－５】



（出典：本委員会）

※印の図表（1-2、1-3）は、日本経済新聞社の許諾を得て利用しています。
無断複写・転載はご遠慮ください。

第２章　経済安全保障の観点がなぜ経営者に必要なのか

日本においても「経済安全保障推進法」が施行され、経済安全保障の観点から経営判断が必要な時代となった。企業にとって、経済（事業）と安全保障（リスク）が重なる境目を見極め、安全保障面のリスクを排除し、事業を推進していく必要がある。この見極めは、経営者にしかできない。企業経営は経済合理性だけではなく、リスク管理が今後ますます重要になる。

２．１　想定される企業へのリスク

これまで、「経済関係の強化とグローバル化が軍事的紛争の回避につながる」と考えられていたが、昨今、他国に経済的に依存することが、自国の安全保障の脆弱性に繋がるという議論が支配的になった。特に、日本企業においては長らくの間、地政学におけるリスクを複数ある外部環境要因の 1 つ程度に捉えていたが、これからは企業経営に強い影響を与える重要な課題であると認識する必要がある。

想定される具体的なリスクは数多くあるが、まずもって役職員生命・身体等への危険への対応が最重要であることは言うまでもない。また、通信の遮断を回避するための衛星通信を確保することが求められる。その上で、国家間の緊張や紛争が発生した国・地域での生産・販売等の企業活動への支障や原材料の高騰、サプライチェーンの混乱、サイバー攻撃を通じた活動の停止、技術情報の流出、安全保障貿易規制の強化による輸出制限の対応等が考えられる。特に、サプライチェーンにおいては、為替変動、エネルギー・原材料価格の高騰、世界的な半導体関連部品不足など企業規模を問わず影響を受けており、その中でも特に、セキュリティ対策が比較的手薄な中小企業を狙ったサイバー攻撃が昨今増加している。実際に、中小企業自体を狙うだけでなく、中小企業を踏み台として標的とする大企業への攻撃を行い、結果、重要顧客の操業を停止させてしまう事例も発生しており、サプライチェーン全体に甚大な被害をもたらす危険を抱えている。

２．２　経営者に求められる対応

後ほど第 4 章でも述べるが、この新たな分断の時代においては、経営者が安全保障の観点を持つことは事業の継続性に欠かせない。企業独自で経済安全保障に取り組むべき課題も多岐に亘っており、経営者自ら経済安全保障についての深い理解と見識が求められている。不透明感が増す社会によって経済安全保障上のリスクが多様化する中、外交、経済、エネルギー、食料等、世界情勢を踏まえて国家の進む道を幅広く学び、日本の立ち位置を認識しなければならない。

具体的な取り組みとして、各国の経済安全保障に関する最新の動向の把握、サプライチェーン上のリスク点検、社内の情報管理等、コンプライアンスとリスク管理体制の強化が求められる。また、サプライチェーンの強靭化のため、調達先の分散、国内生産体制の強化、海外生産体制の見直し等、サプライチェーンの再構築を勘案する必要もある。

特に、サプライチェーン全体に大きな影響を与えるサイバーセキュリティ対策においては、サイバー攻撃の多様化・巧妙化に伴い、経営者の更なるリーダーシップが求められている。中部地区は製造業を中心に多くの企業が集積しており、その大多数を占める中小企業による取り組みの推進が、サプライチェーンの強靭化に大きく貢献することを忘れてはならない。

第３章　本委員会の活動内容

本委員会では、報告書の取りまとめに向けて、まず会員企業の経済安全保障に関する取り組み状況や課題等を把握する目的で、会員へのアンケートを実施した。そして、アンケート調査において、他の企業の参考となる取り組みを行っている中小企業に個別にヒアリングするとともに、大手企業についてもその取り組みをヒアリングした。またその間、サプライチェーンやサイバーセキュリティを含め、企業を取り巻く経済安全保障について、その本質を理解するために、有識者を招き委員会主催の講演会を 2 回開催した。

以下、3.1 で会員へのアンケート調査の概要、3.2 で委員会主催の講演会における有識者からの学び、3.3 で企業ヒアリングを通じて得られた中小企業の取り組み事例と大手企業から学んだ教訓等について、それぞれ報告する。

３．１　会員へのアンケート（課題の抽出等）

本委員会では、2023 年 7～8 月に当会「1000 人の声プロジェクト」を通じてアンケート調査を実施した。ここでは、回答のあった 114 社からのアンケート結果について、企業規模別に分析することで、中部地区の企業における現状と課題を整理する。なお、企業規模については、中小企業庁による定義（製造業その他）に基づき、従業員数 300 人以下を中小企業、301 人以上を大企業とした。

また、本報告書では主なアンケート調査結果（図表）のみを掲載しているため、アンケート調査結果の全体については、二次元バーコードより案内の中部経済同友会サイトを参照頂きたい。

３．１．１　アンケート調査結果の主なポイント

① 経済安全保障全般に関する取り組み状況

・経済安全保障について、7 割以上の企業が「強く意識している」または「ある程度意識している」との回答であった。但し、中小企業では「強く意識している」との回答が約１割にとどまり、企業規模によって差がみられた。

・13 項目にわたる取り組み状況では、全体として、情報管理体制やサイバーセキュリティの強化に「取り組んでいる」及び「今後取り組む予定」を合わせた回答は 8 割以上と比較的多かった。一方で、取締役会等での議題としての取り扱い、専門部署や担当役員の設置、社内研修や専門人材の育成に「取り組んでいる」及び「今後取り組む予定」を合わせた回答は低調であった。さらに中小企業では、大企業と比べてその割合が低く、中でも専門人材の育成に取り組んでいるとの回答はゼロであった。

・企業の経済安全保障に向けた取り組みを推進する上での課題は、全体では「情報の適時適切な取得」「取引企業の動向把握」「自社における事業リスクの把握」という順に多かった。

② サプライチェーンの強靭化に向けた課題

・課題は、全体及び中小企業では「材料等の調達コスト、物流コスト増大への対応」「地政学リスク、自然災害の発生など予測困難なリスクに対する対応」の順に多かった。また、大企業では「BCP の策定と実行」とする回答が最も多かった。

・13 項目にわたる取り組み状況では、企業規模を問わず、いずれの項目も「実施している」

及び「今後実施する予定」を合わせた回答は 5 割以上あった。但し、中小企業では「サプライチェーンのリスク分析・評価」「人材の確保・育成」「他企業との連携体制の強化」を実施しているとの回答が 1 割に満たなかった。

・政府への要望は、企業規模を問わず「サイバーセキュリティの強化」が最も多かった。

・サプライチェーンのレジリエンスの維持・向上に向けて、中小企業から大企業、大企業から中小企業に求めることは、どちらからも「サイバーセキュリティ対策の共有」とする回答が最も多かった。

③ サイバーセキュリティ対策に向けた課題

・課題は、全体では「高度化・巧妙化するサイバー攻撃への対応」「専門人材の育成」「従業員教育の徹底」の順に多かった。また、中小企業では「コスト負担の増大」とする回答が最も多かった。

・「サイバーセキュリティ経営ガイドライン Ver3.0」について、全体では各項目とも「実施している」及び「今後実施する予定」を合わせた回答は概ね 7 割程度であった。特に大企業ではほぼ 8 割を超える回答となった。一方で、大企業と中小企業では「実施している」と回答した割合に、大きな格差がみられた。

・政府への要望は、全体では「サイバーセキュリティ強靭化に関する助成金・補助金の充実」とする回答が最も多かった。

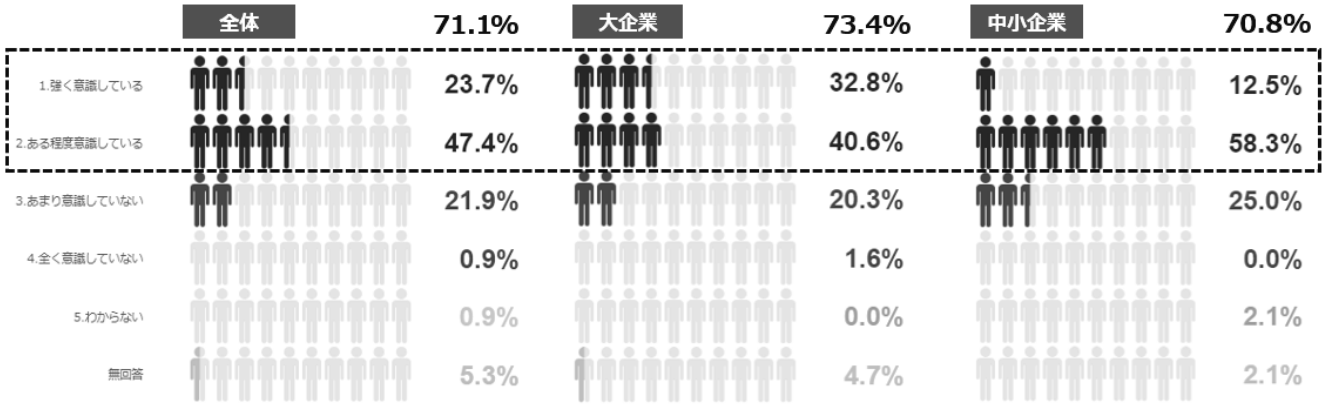
・サイバーセキュリティ対策の強化を図る上で、中小企業から大企業、大企業から中小企業に求めることは、前述のサプライチェーンと同様に「サイバーセキュリティ対策の共有」とする回答が最も多かった。今後、いかに企業間の情報連携・共有を図っていくのかが求められる。

３．１．２　経済安全保障全般に関する取り組み状況

経済安全保障に対する企業の意識について、図表 3-1 が示すように、全体でみると「強く意識している」または「ある程度意識している」とする回答が約 7 割を占めた。但し、企業規模別にみると、大企業では「強く意識している」との回答が約 3 割を占める一方、中小企業では約 1 割にとどまり、企業規模によって意識の差がみられた。

【図表３－１】

Q7. 経済安全保障について、どの程度意識していますか。（全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）

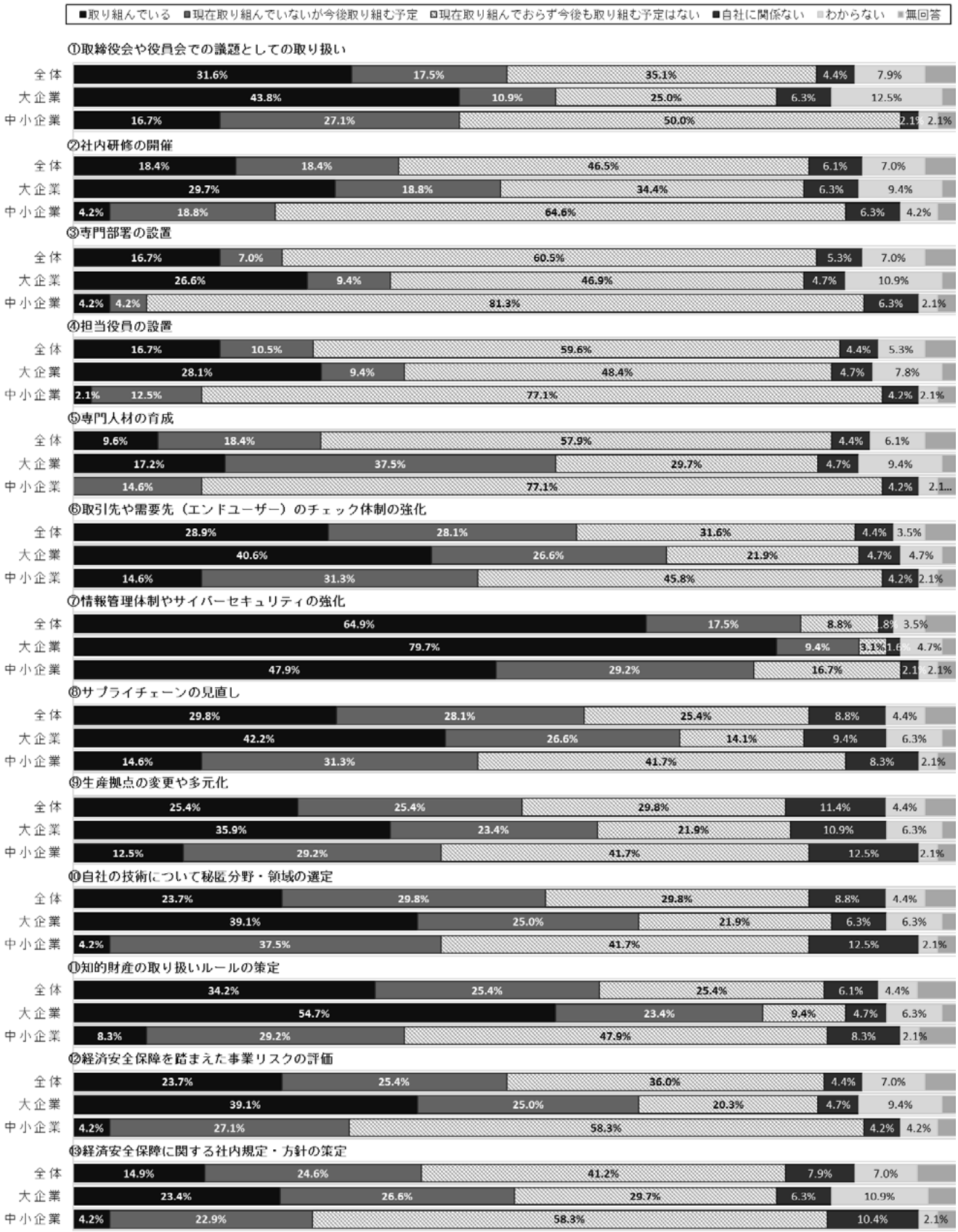


次に、経済安全保障に向けた具体的な取り組み状況について 13 項目にわたり聞いたところ、図表 3-2 が示すように、全体では、情報管理体制やサイバーセキュリティの強化に「取り組んでいる」及び「現在取り組んでいないが、今後取り組む予定」を合わせた回答は 8 割以上と比較的多かった。一方で、専門部署や担当役員の設置、社内研修や専門人材の育成、経済安全保障に関する社内規定・方針の策定に「取り組んでいる」及び「現在取り組んでいないが、今後取り組む予定」を合わせた回答は 2～3 割程度と低調であった。こうした項目を企業規模別にみると、とりわけ中小企業において「取り組んでいる」とする回答割合が低く、「取り組んでいない」とする回答が半数を占める項目も散見された。

企業の経済安全保障に向けた取り組みを推進する上での課題は、全体では「経済安全保障に関する情報の適時適切な取得」「取引企業の動向の把握」「自社における事業リスクの把握」「リソース（人員・人材教育）の不足」「海外情勢のタイムリーな把握」の順に多かった。

【図表３－２】

Q8.貴社の経済安全保障に向けた取り組み状況について教えてください（全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）。

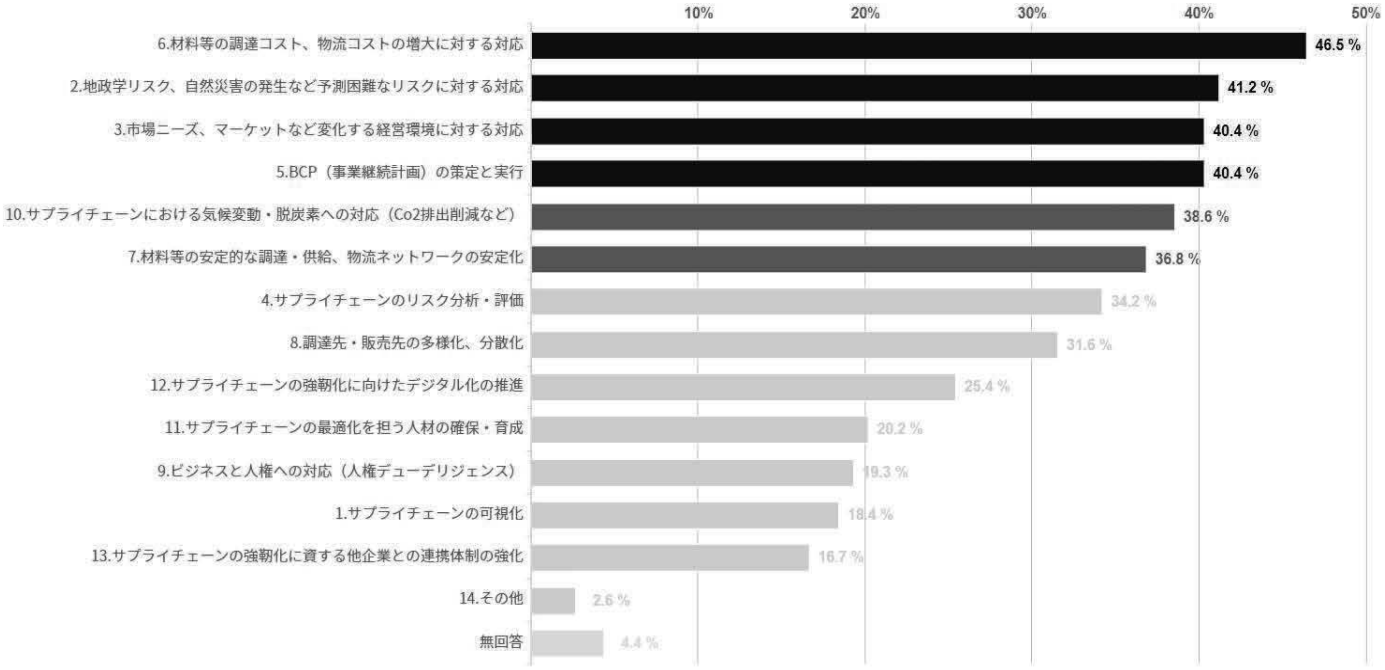


３．１．３　サプライチェーンの強靭化に向けた課題

まず、各社の抱えるサプライチェーン上の課題について聞いたところ、全体としては、図表3-3のように「材料等の調達コスト、物流コストの増大に対する対応」「地政学リスク、自然災害の発生など予測困難なリスクに対する対応」の順に多かった。企業規模別にみると、中小企業の上位は全体と同様であったが、大企業では「BCP（事業継続計画）の策定と実行」とする回答が最も多く、次いで「材料等の調達コスト、物流コストの増大に対する対応」、「サプライチェーンにおける気候変動・脱炭素への対応（CO2排出削減など）」であった。

【図表３－３】

Q12. 貴社におけるサプライチェーン上の課題は何ですか（複数回答；全体 N=114）。

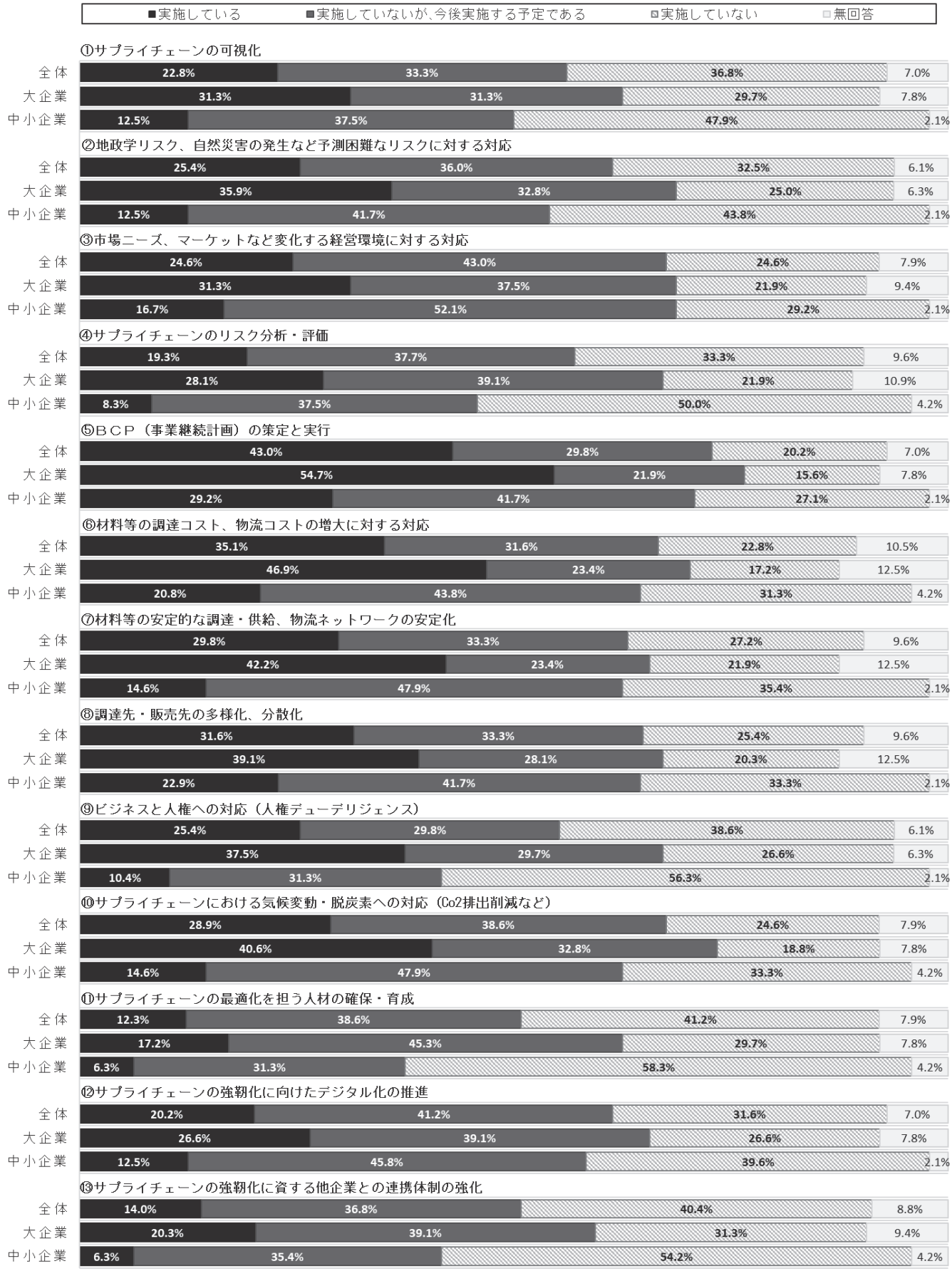


次に、サプライチェーンの強靭化に向けた具体的な取り組み状況について13項目にわたり聞いたところ、図表3-4が示すように、全体では、いずれの項目も「実施している」及び「実施していないが、今後実施する予定である」を合わせた回答が5割以上を占めた。但し、中小企業では「サプライチェーンのリスク分析・評価」「サプライチェーンの最適化を担う人材の確保・育成」「サプライチェーンの強靭化に資する他企業との連携体制の強化」について「実施している」とする回答が1割に満たなかった。また、大企業においても「サプライチェーンの最適化を担う人材の確保・育成」「サプライチェーンの強靭化に資する他企業との連携体制の強化」について「実施している」とする回答は低調であった。

なお、サプライチェーンのレジリエンス（外部のショックや変動に対して強く、迅速且つ効果的に回復できる能力）の維持・向上を図る上で、政府への要望は、全体として最も多かったのが「サイバーセキュリティの強化」であった。さらに企業規模別にみると、中小企業では「サイバーセキュリティの強化」に続き、「通貨（円）価値の安定維持」「人材投資・育成」、大企業では「国際的なルール形成における主導権確保」「資源・エネルギーの自給率向上」を求める声が多かった。

【図表３－４】

Q13.貴社はサプライチェーンの強靭化に向けて、以下の取り組みを行っていますか（全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）。

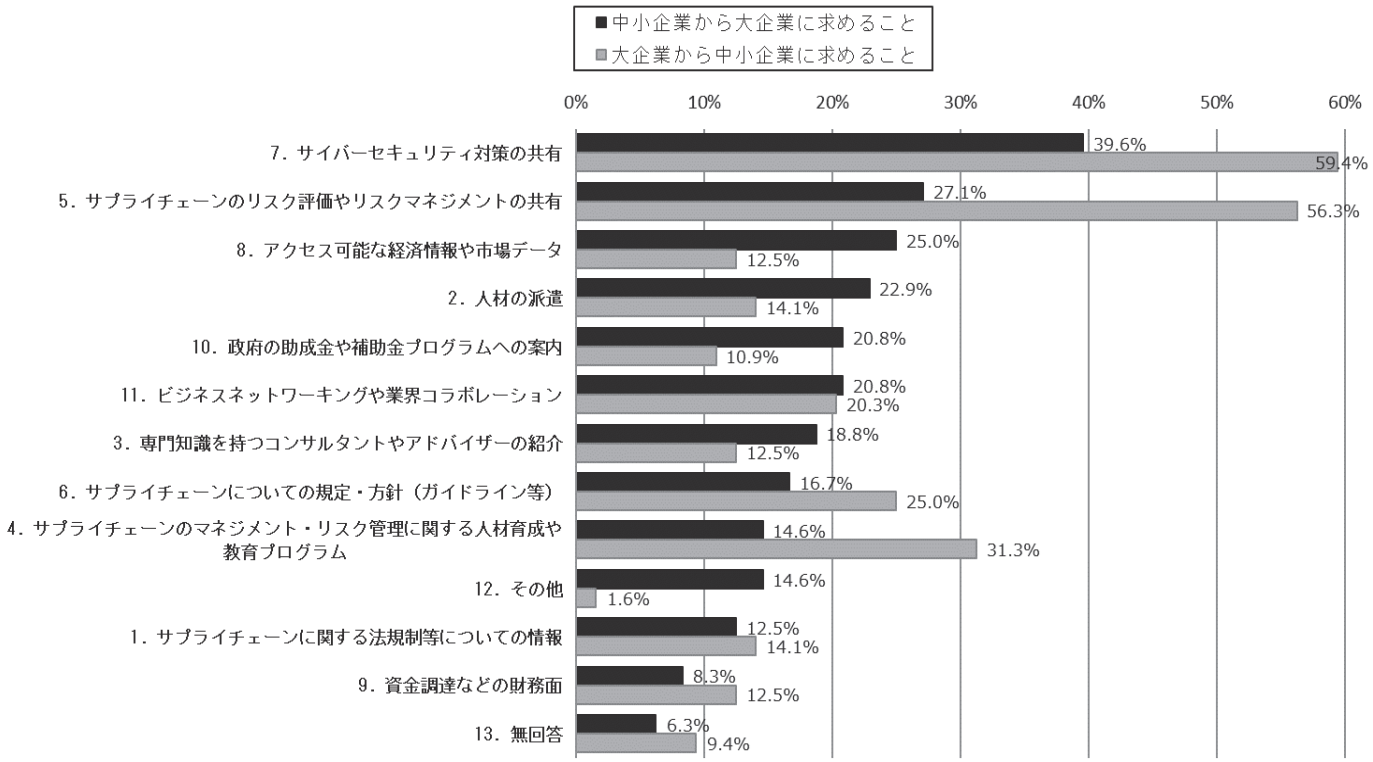


次に、サプライチェーンのレジリエンスの維持・向上のために、中小企業、大企業それぞれの立場より求める要望を聞いた。図表 3-5 が示すように、中小企業から大企業に求めることは、「サイバーセキュリティ対策の共有」「サプライチェーンのリスク評価やリスクマネジメントの共有」「アクセス可能な経済情報や市場データの共有」の順に多かった。

一方、大企業から中小企業に求めることは、「サイバーセキュリティ対策の共有」「サプライチェーンのリスク評価やリスクマネジメントの共有」「サプライチェーンのマネジメント・リスク管理に関する人材育成や教育プログラム」の順に多く、互いに共通する回答が上位を占めた。とりわけ双方よりサイバーセキュリティ対策やリスク評価、リスクマネジメント等について情報連携・共有を求める姿が明らかとなった。

【図表３－５】

Q15.中小企業、大企業それぞれの立場で回答してください（複数回答；中小企業から大企業に求めることの多い順）。＜中小企業の回答者；N=48＞貴社の属するサプライチェーンのレジリエンスの維持・向上のために、大企業に対してどんなことを求めますか。＜大企業の回答者；N=64＞貴社の属するサプライチェーンのレジリエンスの維持・向上のために、中小企業に対してどんなことを求めますか。



なお、経済産業省では、「経済安全保障上の課題への対応（民間ベストプラクティス集）―第 1 版―（2023 年 10 月）」（図表 3-6）として、企業が直面している課題等を把握する際に得られた好事例をまとめている。その中には、「サプライチェーン構造・原料調達先の可視化」（図表 3-7）や「調達先の多元化・安定化」といったサプライチェーンの強靭化に向けた事例も掲載されており、参考までに共有しておきたい。

【図表３－６】

民間ベストプラクティス集の構成

<目次>

ベストプラクティス事例	1-1	1-2	1-3	1-4	1-5	2-1	2-2	2-3	2-4
① 重点的に守るべき技術の特定	○		○	○					
② 従業員の情報管理意識の醸成	○								
③ 従業員の副業からの技術流出防止	○								
④ 重要な技術を持つ従業員の流出抑制	○								
⑤ 守るべき情報へのアクセス権の設定	○								
⑥ 原材料等のコードネーム化	○		○	○					
⑦ 重要なノウハウを持つ技術者の雇用延長		○							
⑧ 取引先企業の情報管理			○	○					
⑨ 海外工場で扱う技術・工程の制限			○		○				
⑩ 経済安全保障の観点から経営判断する体制整備						○	○	○	○
⑪ サプライチェーン構造・原料調達先の可視化						○			
⑫ 調達先との資本関係形成による安定供給確保						○			
⑬ 調達先の多元化・安定化						○	○	○	
⑭ 軍事転用防止							○		
⑮ レピュテーションリスクへの対策							○		
⑯ 契約において盛り込むべき条項							○	○	○
⑰ 適切な契約期間の設定							○		○

※目次の1-1～2-4は、これまでのヒアリングで明らかになった課題のいずれに対応するものであるかを示している。

<ヒアリングで明らかになった課題>

①技術流出リスク

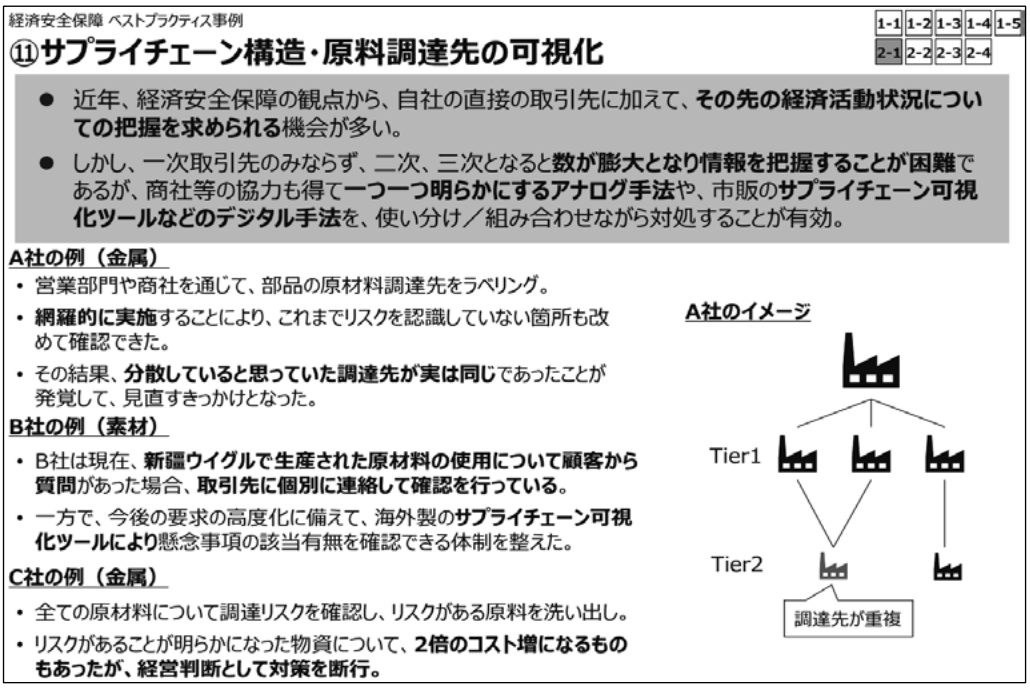
1-1. 人（現役従業員）
1-2. 人（退職者・OB）
1-3. 取引先からの要求
1-4. 共同事業等
1-5. 相手国の政策・制度

②ビジネス環境の予見性低下

2-1. 原料・部品の供給途絶
2-2. 諸外国の規制・政策
2-3. 紛争などによる経済活動混乱
2-4. 契約内容が不十分

（出典：経済産業省大臣官房安全保障室「経済安全保障上の課題への対応（民間ベストプラクティス集）-第１版-」（https://www.meti.go.jp/policy/economy/economic_security/best_practice.pdf）より抜粋）

【図表３－７】



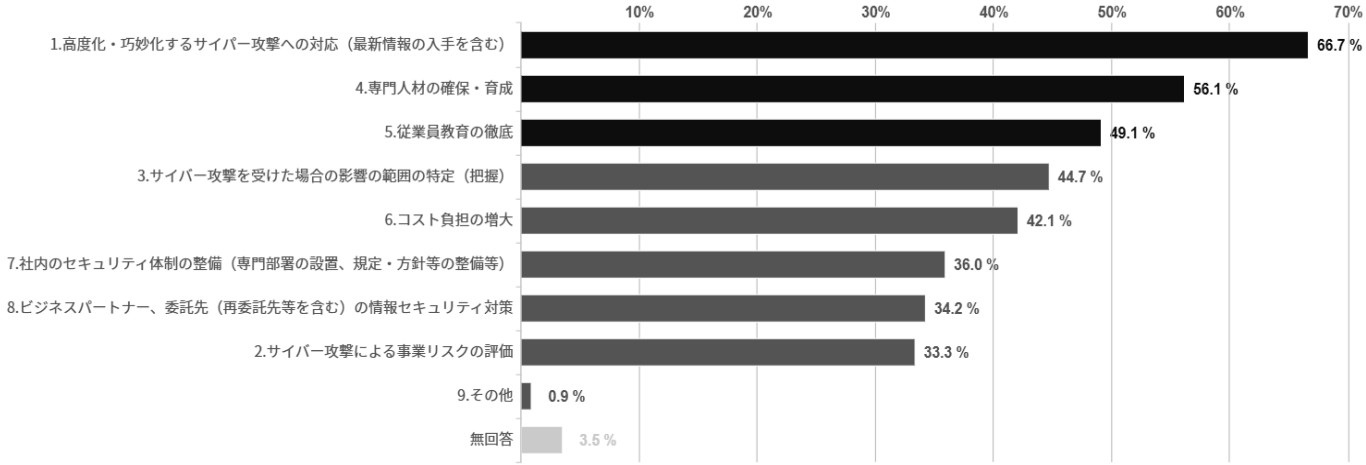
（出典：図表 3-6 と同じ）

３．１．４　サイバーセキュリティ対策に向けた課題

まず、サイバーセキュリティ対策を行う上での各社の課題について、全体では、図表 3-8 のように、「高度化・巧妙化するサイバー攻撃への対応（最新情報の入手を含む）」「専門人材の確保・育成」「従業員教育の徹底」の順に多かった。企業規模別にみると、大企業の上位は全体と同じであったが、中小企業では「コスト負担の増大」とする回答が最も多かった。サイバー攻撃が巧妙化・複雑化する一方で、企業におけるサイバーセキュリティを担う専門人材の確保や育成、対策費用に課題を感じていることが浮き彫りとなった。

【図表３－８】

Q16.貴社におけるサイバーセキュリティ対策を行う上での課題は何ですか（複数回答；全体 N=114)。



次に、経済産業省と独立行政法人情報処理推進機構で取りまとめられた「サイバーセキュリティ経営ガイドライン Ver3.0」のチェック項目の概要（図表 3-9）に基づき、それぞれの取り組み状況を聞いた。図表 3-11 が示すように、全体では「実施している」及び「実施していないが、今後実施する予定である」を合わせた回答が、いずれの項目も 7 割程度を占めた。特に大企業中心に 8 割を超える項目も多く、取り組みを推進していることが伺える。

一方で、中小企業では、「実施している」とする回答は 1～2 割程度で、「実施していないが、今後実施する予定である」を含めても 5 割前後の項目が散見され、企業規模によって取り組み状況に大きな差がみられた。

【図表３－９】

「サイバーセキュリティ経営ガイドライン Ver3.0」における「経営者が認識すべき 3 原則」及び「サイバーセキュリティ経営の重要 10 項目」（概要）

原則 1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要であることを認識している。
原則 2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要であることを認識している。
原則 3	平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要であることを認識している。
重要事項 1	サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定している。
重要事項 2	サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築している。
重要事項 3	サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討し、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組んでいる。
重要事項 4	事業に用いるデジタル環境、サービス・情報を特定し、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別している。
重要事項 5	サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築している。

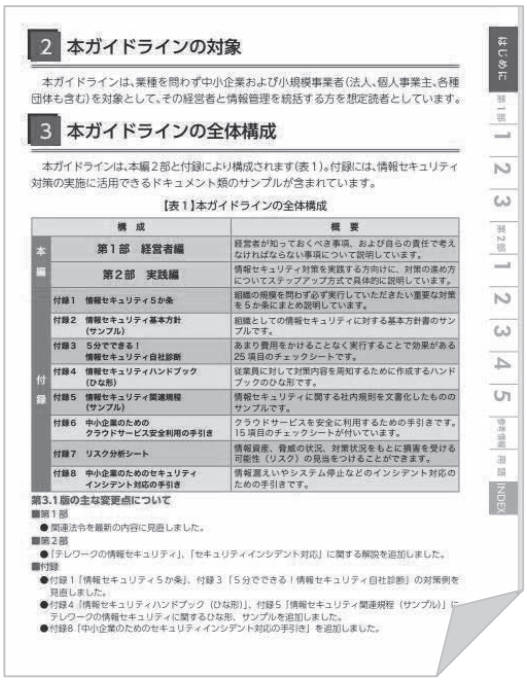
重要事項 6	リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善するため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用している。
重要事項 7	影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制を整備している。
重要事項 8	インシデントにより業務停止等に至った場合、企業経営への影響を考慮して、いつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をしている。
重要事項 9	サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況を把握している。
重要事項 10	有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをしている。

（出典:経済産業省/独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」（https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf）より作成）

なお、同ガイドラインには、付録として数十項目にわたる「サイバーセキュリティ経営チェックシート」が掲載されており、各取り組み状況を可視化するとともに、経営者が確認できるツールとなっている。また、「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集」（https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf）では、実践する際に参考となる考え方やヒント、実施手順、実践事例が示されている。

さらに、中小企業等の利用を想定した「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」（図表 3-10）では、情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針や、社内において対策を実践する際の手順や手法がまとめられているので参考にされたい。

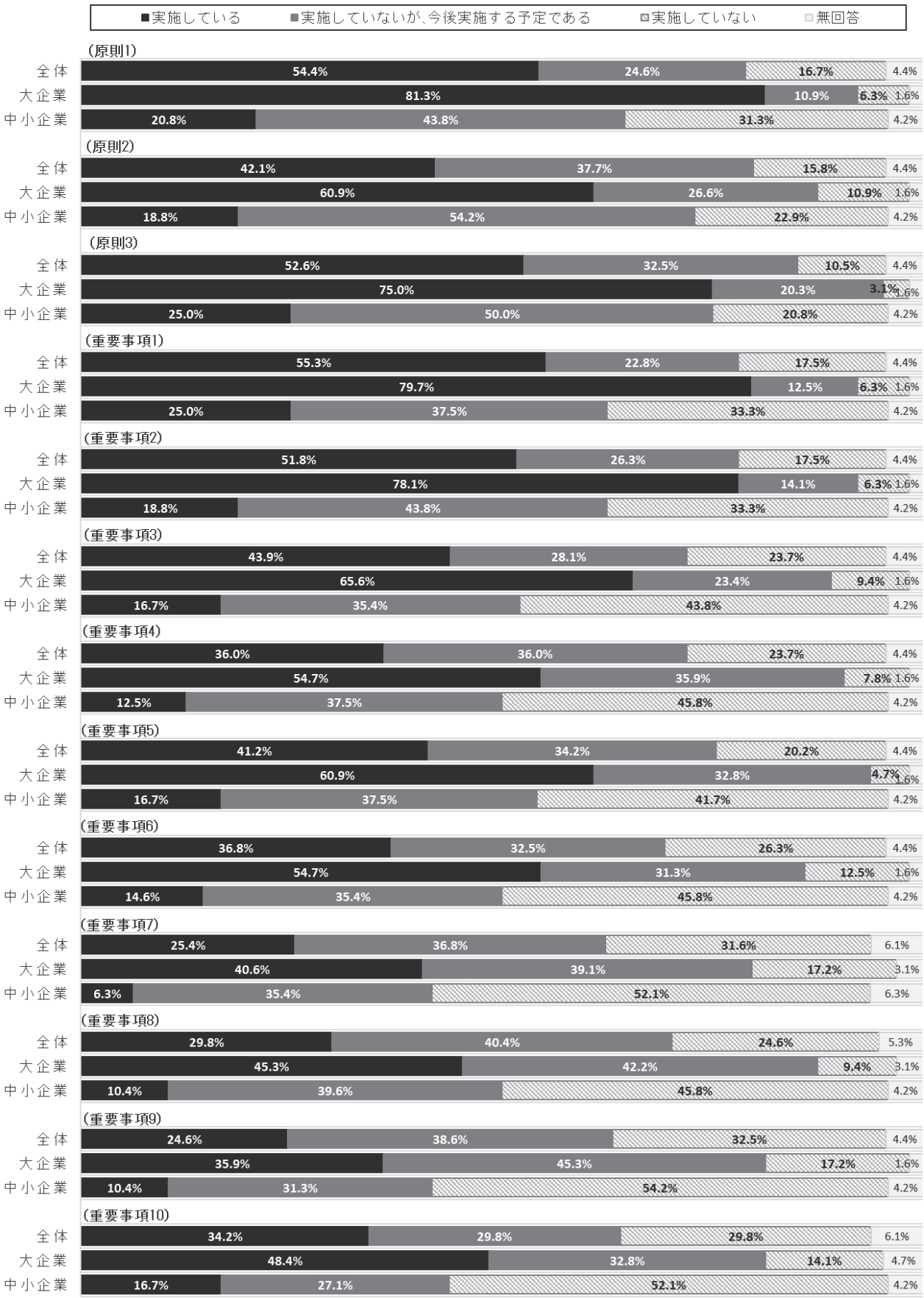
【図表３－１０】



（出典：独立行政法人情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」（https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf））

【図表３－１１】

Q17. 貴社は、経済産業省、独立行政法人情報処理推進機構がまとめた「サイバーセキュリティ経営ガイドライン Ver3.0」における「経営者が認識すべき 3 原則」「サイバーセキュリティ経営の重要 10 項目」に掲げられているチェック項目（図表 3-7）について取り組みを行っていますか（全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）。



次に、サイバーセキュリティ対策の充実を図る上で政府への要望は、全体では「サイバーセキュリティの強靭化に関する助成金・補助金の充実」「能動的サイバー防御（サイバー攻撃を受ける前に対策実行）するための情報提供」「人材投資・育成」の順に多かった。企業規模別でみると、特に中小企業では「サイバーセキュリティの強靭化に関する助成金・補助金の充実」を、大企業では「能動的サイバー防御（サイバー攻撃を受ける前に対策実行）するための情報提供」を求める声が多かった。

参考までに、政府における中小企業のサイバーセキュリティ対策促進について、図表 3-12 に掲載する。

【図表３－１２】

［１］ 中小企業のサイバーセキュリティ対策促進 2

１．背景及び課題

- サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を経由して、発注元の大企業も被害を受けている実態への取組強化が必要である。
- 他方で、そのリスクを自分事として認識していない、あるいは、何をしてよいか分からない状況にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。
- 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係にかかる懸念の払拭を更に進めていくことが必要である。

２．取組の概要

① 手法

- ✓「サイバーセキュリティお助け隊サービス」につき、サービス基準の改定による同サービスの拡充等を通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。
- ✓ こうした取組を、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携して実施し、中小企業への対策の浸透を図る。

② 取組によって期待される成果・効果

- ✓ お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。
- ✓ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）との連携により、産業界全体のサイバーセキュリティ強化が期待される。

■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 地域・中小企業のサイバーセキュリティ対策は、日本のセキュリティ対策の重要課題であるが、現状はまだ端緒に手が届き始めた段階である。当面は、政府がけん引役を務め、官民一体となって強力に推進することが必要である。
- 中小企業特有の問題（規模・費用・ノウハウの継承ほか）もあり、そうした問題へのきめ細かい具体的対応が求められる。
- 警察庁の2023年３月16日付報道発表資料「令和４年におけるサイバー空間をめぐる脅威の情勢等について」を見ると、ランサムウェア攻撃被害の53%が中小企業となっており、サプライチェーンで重要な位置を占める中小企業のサイバーセキュリティ対策は、政府だけでなく、自治体からの支援についても議論が必要である。

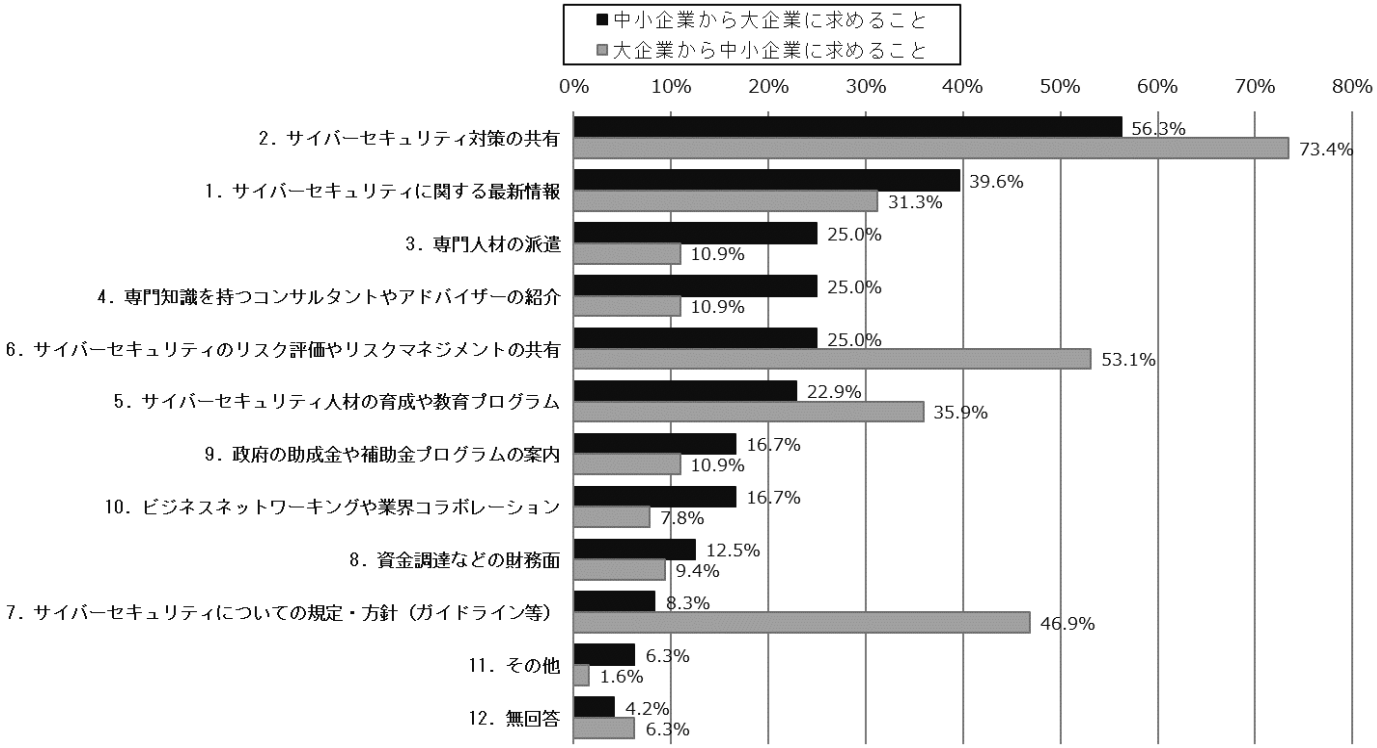
（出典：内閣サイバーセキュリティセンター「サイバーセキュリティ 2023 の概要」より抜粋）

続いて、サイバーセキュリティ対策の強化を図る上で、中小企業、大企業それぞれの立場より求める要望を聞いた。図表 3-13 が示すように中小企業から大企業に求めることは、「サイバーセキュリティ対策の共有」「サイバーセキュリティに関する最新情報」の順に多く、一方、大企業から中小企業に対して求めることは、「サイバーセキュリティ対策の共有」「サイバーセキュリティのリスク評価やリスクマネジメントの共有」「サイバーセキュリティについての規定・方針（ガイドライン等）」の順に多かった。

図表 3-5 で示したサプライチェーンと同様に、双方より「サイバーセキュリティ対策の共有」を求めており、今後、各社が対策を進めていく上で、業界やグループ企業、取引先など、企業間の情報連携・共有を図っていくことの重要性が改めて浮き彫りとなった。併せて、そうした仕組みの整備も課題といえよう。

【図表３－１３】

Q19.中小企業、大企業それぞれの立場で回答してください（複数回答；中小企業から大企業に求めることの多い順）。＜中小企業の回答者；N=48＞サイバーセキュリティ対策の強化を図る上で、大企業に対してどんなことを求めますか。＜大企業の回答者；N=64＞サイバーセキュリティ対策の強化を図る上で、取引を行っている中小企業に対してどんなことを求めますか。



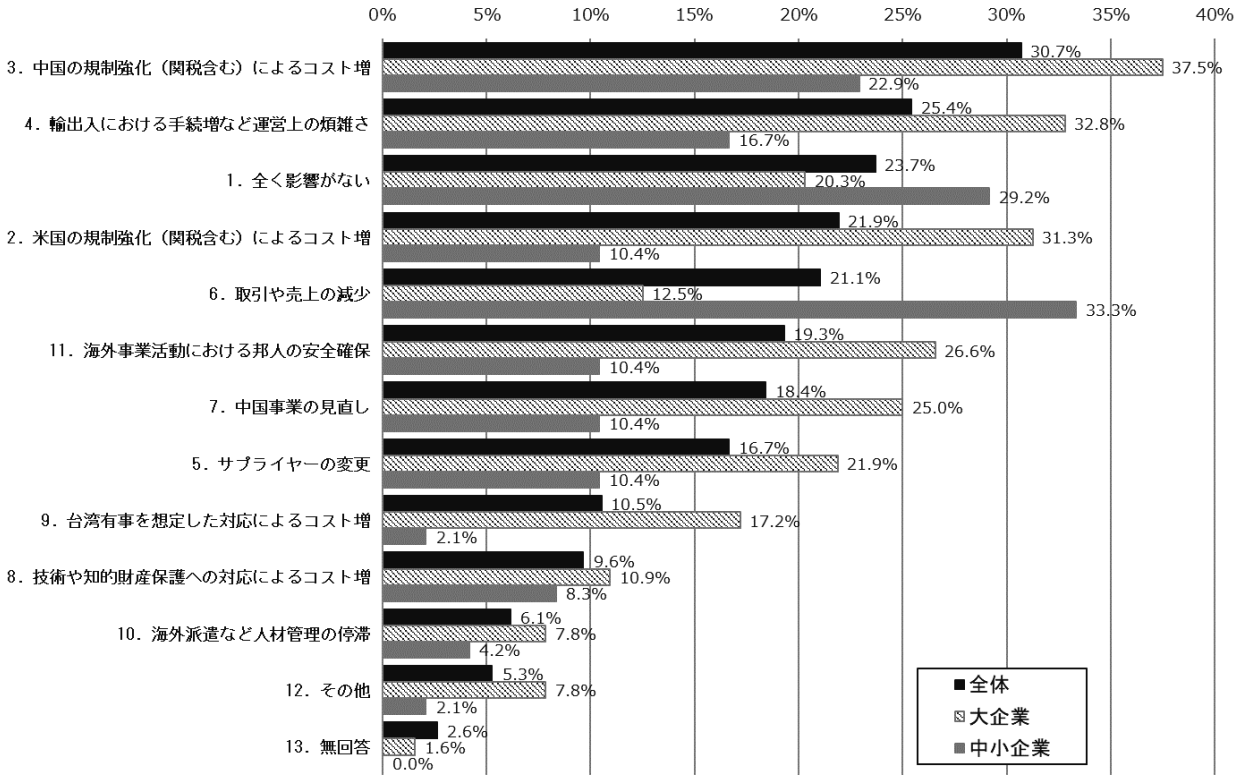
３．１．５　トピックス～米中対立、ロシアによるウクライナ侵攻の影響

今回のアンケート調査では、中部地区の会員企業の米中対立及びロシアによるウクライナ侵攻に伴う事業への影響についても調査した。

まず図表 3-14 に示したように、米中対立の影響は、全体では「中国の規制強化（関税含む）によるコスト増」「輸出入における手続増など運営上の煩雑さ」「米国の規制強化（関税含む）によるコスト増」の順に多かった。企業規模別にみると、大企業では「中国の規制強化（関税含む）によるコスト増」、中小企業では「取引や売上の減少」とする回答が最も多かった。一方で、「全く影響のない」との回答は大企業で約 2 割、中小企業で約 3 割あった。

【図表３－１４】

Q10. 米中対立の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば 2 以降より選択して下さい。なお、「全く影響がない」場合は 1 を選択してください（複数回答；全体の回答の多い順；全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）。

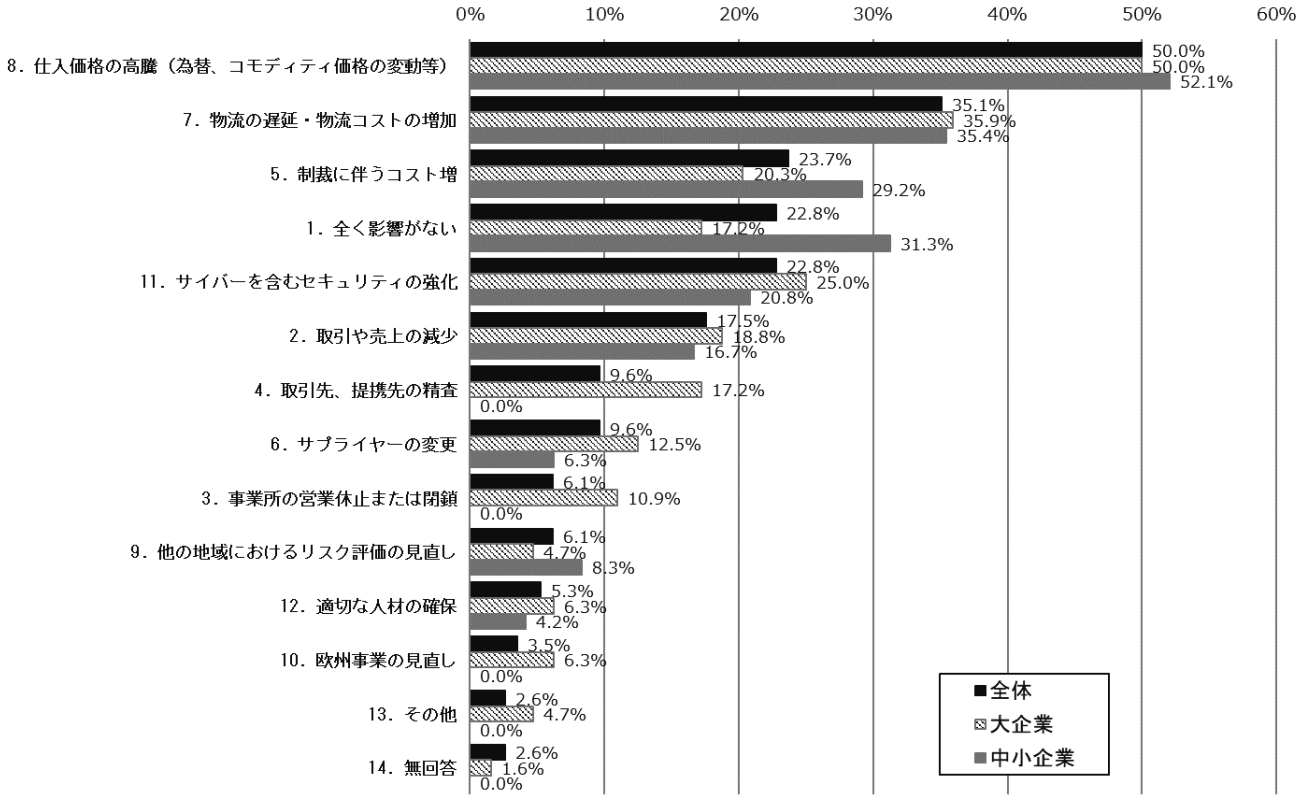


次に、図表 3-15 に示したように、ロシアによるウクライナ侵攻の影響は、企業規模を問わず「仕入価格の高騰（為替、コモディティ価格の変動等）」「物流の遅延・物流コストの増加」の順に多かった。特に「仕入価格の高騰（為替、コモディティ価格の変動等）」とする回答が他の項目を大きく上回った。一方で「全く影響のない」とする回答は、大企業で 2 割弱、中小企業で約 3 割あった。

結果として、米中対立やロシアによるウクライナ侵攻について全く影響がなったとする回答を除いた約 7～8 割の企業では、いずれかの影響を受けており、とりわけ輸出入における手続き増といった実務的な影響に加え、関税を含む規制強化、資材・エネルギーの仕入価高騰や物流コスト増加等に伴う事業活動への影響を指摘する声が浮き彫りとなった。

【図表３－１５】

Q11. ロシアによるウクライナ侵攻とこれに伴う対露制裁の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば 2 以降より選択して下さい。なお、「全く影響がない」場合は 1 を選択してください（複数回答；全体の回答の多い順；全体 N=114、大企業 N=64、中小企業 N=48、無回答 N=2）。



３．２　委員会主催講演会の有識者から学んだこと

第 1 回講演会では、中部地区のみならず、日本、世界を代表する自動車メーカーであり、全世界にサプライチェーンを有するトヨタ自動車の情報セキュリティ・トラスト部長の古田様より大企業の立場から講演を頂いた。また、第 2 回講演会では、中堅・中小企業に求められる経済安全保障について、中国とのビジネス展開を含めて、元経済産業省中部経済産業局長で明星大学経営学部教授の細川様より講演を頂いた。

① 第 1 回委員会活動

日　時：2023 年 9 月 5 日（火）13:00～14:00
講　師：トヨタ自動車株式会社　情報セキュリティ・トラスト部長　古田 朋司氏
講演テーマ：サプライチェーンを含めたサイバーセキュリティの取り組み
～経済安全保障のリスクに備えて～

＜講演内容・学んだ点＞

・サイバー攻撃は戦争や経済安全保障に深く関わる重大な問題であり、サプライチェーンを通じて自社や取引先に被害を及ぼす可能性が高い。
・サプライチェーンのセキュリティ対策には、ソフトウェアやハードウェアの更新、バックアップ、多要素認証、別ネットワークでのデータ保管などが必要であり、仕入先にも適用する必要がある。
・経営層直轄下に情報セキュリティ統括責任者（CISO）を設置し、情報セキュリティ推進会議にて報告、方向付けを行っている。また、サイバー攻撃から身を守るには情報共有し、競争ではなく協働することが重要である。
・サイバー攻撃は経営課題であり、担当者任せでは限界があるため、経営者自ら関わることが重要である。IT 予算の 15%以上を投じる企業が 3 割強にのぼることからも、サイバー攻撃への対策は優先度の高い投資である。

② 第 2 回委員会活動

日　時：2023 年 11 月 29 日（水）15:00～16:30
講　師：明星大学　経営学部　教授　細川 昌彦氏
講演テーマ：中堅・中小企業に求められる経済安全保障

＜講演内容・学んだ点＞

・従来は「経済」と「安全保障」を別々に考えれば良かったが、近年は部分的に重なり合うようになった。それが「経済安全保障」である。企業経営者としては、重なり合う部分はどこなのか、その線引きが重要となる。「経済」と「安全保障」が接近した理由は、中国による経済的威圧（他国を中国に依存させる）と強国化（他国に依存しない中国）の 2 つである。
・前者については、原発処理水の放出に伴う日本産水産物の禁輸措置などを毎年のように実施している。したがって、いかに中国依存から脱却するのかが重要となる。企業は中国への依存度を調査する必要があるが、その場合には、対象をサプライチェーン全体に広げる必要がある。
・後者については、中国は他国に依存しないよう重要産業の国産化を巧妙に進めている。

最初は中国市場へのアクセスをアピールして国内に誘致（誘致モード）し、中国企業に技術が移転したら排除（排除モード）に切り替える。また国産化政策として買収も積極化している。大手ではなく中小企業をターゲットとして、ショッピングリストを作成している。大企業の調達部門はこれまで安く仕入れることを主眼としてきたが、これからはサプライチェーンの全体最適を考えた「持続可能性」がポイントとなる。

・中国の反スパイ法の施行、サイバー攻撃など、経営を巡る環境は変化している。従来は経済効率が優先されたが、これからの経営判断はリスク対応力が重要な視点となる。

全ての企業がサイバーセキュリティ対策を適切に講じなければ、自社のみならずサプライチェーン全体に被害が及ぶことになる。サイバーセキュリティ対策は経営課題そのものであり、経営者自らが自分事化することが重要である。また、巧妙化するサイバー攻撃に対しては、自社だけでなく、他社と協働して取り組む必要がある。

近年は「経済」と「安全保障」が重なり合うようになったことから、経営者はその線引きを適切に行う必要がある。この背景には、中国による「経済的威圧」と「強国化」があるため、自社の中国への依存度を把握した上でいかに中国依存から脱却するか、中国の重要産業の国産化政策に対していかにサプライチェーン全体の持続可能性を高められるかがポイントとなる。

３．３　中小企業の取り組み事例の紹介と大手企業から学んだ教訓

本委員会では、サプライチェーンとサイバーセキュリティの分野で、経済安全保障の視点で興味深い取り組みをしている中小企業 5 社と、本委員会会社大手 3 社、自動車関連大手 1 社の計 9 社に対しヒアリングを行った。それぞれ注目すべき好事例の取り組み内容を紹介する。

【中小企業へのヒアリング】

① 加藤軽金属工業株式会社

日　程：2023 年 10 月 16 日（月）
面談者：取締役社長　加藤 大輝氏
事業内容：アルミニウムの押出形材の製造及びその加工やアルミニウムを使用した製品の組立・販売
従業員数：85 人

＜ヒアリング内容・学んだ点＞

・サプライチェーン対策として同社は LME（London Metal Exchange）より先物取引で原材料を仕入れ製品化している。3 ヶ月前に購入した価格が現在に適用される仕組みで、95%の顧客はこの制度を受け入れている。原料のアルミの調達先は世界各国で分散している（ドバイ 50%、オーストラリア 30%、ロシア 5%*、残りは自社再生アルミ）が、ロシア、ウクライナの影響は受けている。
　*2023 年後半から別調達先に切り替え
・地政学リスクの情報はエネルギー関連紙、シンクタンクや証券会社のレポートを参照している。

・グリーンアルミは一般的にはまだまだ高価なものであるものの、自社にて安価で独自に調達できるルートを確保している。しかし、案件自体が試作品製作でとどまる傾向にある。
・サイバーセキュリティに対し、実施しなければならないという意識を非常に高く持ち、社内に対するセキュリティ認知向上を図っている。

② ゼネラルヒートポンプ工業株式会社

日　程：2023 年 10 月 25 日（水）
面談者：代表取締役 柴 芳郎氏、主査 小倉 怜子氏
事業内容:各種ヒートポンプ製品の製造・販売および遠隔監視、各種エネルギー関連システム設計
従業員数：69 名（2023 年 4 月 1 日時点）

＜ヒアリング内容・学んだ点＞
・セキュリティ対策を「CSIRT*」として組織化し、拠点毎に IT に強い人材を 1 名配置することで、全社レベルでの取り組みや社員のセキュリティ意識向上を実施している。
・外部委託に頼るだけでなく「CSIRT」メンバーで、社内 IT 資産の棚卸からソフトウェアのバージョンアップ、バックアップデータの取得など、費用を最小限に抑えつつ、必要な対策を地道に実施している。
・ウイルス感染等が認められた際の初動などについて、シンプルで明瞭な手続きをマニュアル化し、社内で徹底している。
・年に 1 回開催する安全衛生大会において、「CSIRT」によるヒヤリハットの事例共有等を行うなどサイバーセキュリティに関する知見の向上を図っている。
・このセキュリティ対策の重要性をトップが理解して推進している。

＊ CSIRT：Computer Security Incident Response Team の略。
セキュリティインシデントが発生した際に対応するチームのこと。

③ エムアイシイー株式会社

日　時：2023 年 10 月 27 日（金）
面談者：代表取締役　小島 由公香氏
事業内容：IT、AI、医療機器関連ローカリゼーションサービス
従業員数：13 名、社外契約 QA パートナー：11 名
（QA＝quality assurance（品質確認、品質チェック）

＜ヒアリング内容・学んだ点＞
・サプライチェーンをより強靭化するために、クラウド上のボードを利用して、日々の情報を共有し情報の可視化を行っている。これにより、サプライチェーン間の互いのシステムをより効率良く利用する事が可能となり、自社のみでは得られない気づきも入手することが可能となっている。
・サイバーセキュリティ対策においては、大手顧客から詳細なセキュリティチェックを受けている（2 ヵ月毎のチェックシートの提示義務あり）。セキュリティのために、ホスティングやクラウドサービスを利用して、日々のデータバックアップを義務付けている。

・サイバーセキュリティに対応可能な優秀な人材や、複雑化しているセキュリティに対処可能なベンダーが、日本ではまだまだ不足しているのが現状である。海外の人材やサービスを利用する選択肢もあるが、事は簡単ではない。

④ 株式会社精器商会

日　程：2023 年 10 月 30 日（月）
面談者：専務取締役 下村 文乃氏
事業内容：機器販売、工事施工、アルミダイキャスト品・アルミ鍛造品の切削加工他
従業員数：55 名（2023 年 4 月現在）

＜ヒアリング内容・学んだ点＞

サプライチェーンにおける気候変動・脱炭素への対応（CO2 排出削減等）

・重要顧客の仕入先で構成される協力団体に所属している。その会員企業の 1 社が、パリ協定が求める水準と整合した企業が設定する温室効果ガス排出削減目標である SBT（Science Based Targets）を取得した情報を入手したことがきっかけとなり、同社でも 2022 年に取得した。
・サプライチェーン排出量の削減が SBT では求められる中、認定や今後の報告に向けては CO2 排出量の正確な数値の把握が必要になった。そのため CO2 排出量把握に向けて自社で Excel によるグラフ化を行い見える化を図った。

サプライチェーン強靭化に向けたデジタル化の推進

・重要顧客の仕入先企業の 1 社が豪雨被害により会社 PC 内に保存していたデータが水没するという事例が発生した。それをきっかけに、BCP の観点でクラウドシステムの導入を推進している。
・自社の所在地が、ハザードマップ上では水没の可能性が高いエリアとなっているため、安否確認システムを構築している。

サイバーセキュリティについて

・Teams 活用による社外で発生したサイバーセキュリティ関連の定期的な情報提供と啓蒙活動を実施している。

仲間（他企業）との連携

・1 社単独では解決が難しい課題に対し、様々な団体の繋がりを活用し、業種や業界、企業規模を超えた連携（協調）が、取り組みを加速させるために重要となる。

⑤ 株式会社三喜工作所

日　程：2023 年 11 月 20 日（月）
面談者：代表取締役 中野 喜一朗氏
事業内容：自動車部品関連、建築資材関連
従業員数：35 名（2023 年 10 月現在）

＜ヒアリング内容・学んだ点＞

BCP（事業継続計画）の策定と実行

・政府の BCP ガイドラインをもとに計画を実施しているだけでなく、自社独自の取り組みとして、雇用の確保を重視している。有事の際、復旧後に雇用が離れては生産が再開できないと考え、最低 1 年間の給与が支払えるように資金確保を常時行っている。

サイバーセキュリティの取り組みについて

・データ管理は、オフラインの PC を使用しサイバー攻撃対策を実行するだけでなく、定期的にデータはバックアップを取っている。

・重要顧客からは、情報セキュリティに対する注意喚起や事例の横展開といった教育をして頂き参考にしている。

期待する支援、課題

・情報セキュリティ分野は専門性が高く、人材の確保が困難であり、政府による専門人材の雇用サポートがあるとよい。

・１社単独ではなく、グループなどで横の繋がりを強くできればいいが、同時にトラブルの共有や競合他社への情報流出といったリスクに懸念がある。

【大手企業へのヒアリング】

① NTT コミュニケーションズ株式会社

日　程：2023 年 9 月 6 日（水）

面談者：情報セキュリティ部長 小山 覚氏

＜ヒアリング内容・学んだ点＞

ランサムウェア攻撃の備えについて

・ランサムウェア攻撃はコロナ対応のテレワーク環境から社員になりすまし侵入してくる。

・テレワーク環境が必要であれば保守契約の締結・更新を行って最新の脆弱性パッチをあてることが重要である。環境が不要であれば思い切って撤去も考慮すべきである。

・バックアップからのシステム復元は 20%ほどしか成功しなかったという統計もある。バックアップを使って業務を再開するマニュアルを作り、訓練をしておくべきである。

・ランサムウェア攻撃はサプライチェーンを狙った事案が増えている(病院、自動車、港湾で大きなニュースになったものもある)。自社を守ることがネットワークでつながった取引先を守ることにつながるということを意識すべきである。

サイバー攻撃の動向と安全保障戦略への対応について

・サイバー攻撃のパターンは大きく 3 パターン(経済産業省による分類)ある。
  - VPN 機器を狙うネットワーク貫通型攻撃
  - ランサムウェアによる二重の攻撃(データ暗号化およびデータばらまきの脅迫)
  - 海外拠点経由の攻撃(攻撃の高度化)

・海外拠点経由の攻撃は NTT コミュニケーションズもサイバー攻撃を受けた。
国家(の情報)に迫るスパイのように情報を入手するには、通信事業者や大企業への侵入が近道と知られている。セキュリティの甘い海外から侵入を試みる傾向がある。

・経済安全保障戦略の 4 本柱の一つに、基幹インフラの安全確保が挙げられており、通信

事業者が対象になっている。政府からのリスク管理措置は所管大臣が取り組みをチェックする。取り組み状況の資料の作成には自社だけでなく、委託先の契約書やマニュアルを提出することになり、相当な負担となる可能性がある。

② 株式会社みずほ銀行

日　程：2023 年 9 月 14 日（木）
面談者：経営企画部/IT・システム企画部/サイバーセキュリティ統括部/
　　コンプライアンス統括部等

＜ヒアリング内容・学んだ点＞
全体
・グローバル経済動向や国際的なリスクに対して、グループに重大な影響を及ぼすリスクを「トップリスク」と選定し、未然防止策や事後対応方針について業務計画に反映している。
・「トップリスク運営」を通じグループ内のリスクコミュニケーションが深まり、リスク認識に対する目線を統一することができている。
・同業者との情報交換等実施し、横連携を強化している。
サプライチェーンについて
・外部委託の際には、企業規模にかかわらずシステムリスクや、サイバーセキュリティリスクについて評価を行う仕組みを保有している（2 次、3 次以降、最終委託先まで外部委託先管理の対象）。
・社内外に対し、サイバーセキュリティリスク事例の共有のセミナー等を実施し、ナレッジシェアや、定期的なコミュニケーションを図っている。
サイバーセキュリティについて
・オンライン取引については「FISC 安全対策基準」等に準拠する設計標準として、多要素認証を導入している。
・情報管理については、細かな権限設定や社外への情報移送についてのモニタリング、クラウドへのデータ保管時はチェックリストを設ける等を通じ、厳格な情報管理を実践している。情報取得から廃棄までの管理について細かく手続きを制定している。
・従業員向けには、サイバー攻撃に関する事例の共有や、標的型メールへの対応訓練等を定期的また随時のタイミングで実施し、社員の情報リテラシーの向上に取り組んでいる。

③ 株式会社日立製作所

日　程：2023 年 9 月 27 日(水)
面談者：グローバル渉外統括本部経済安全保障室
　　バリュー・インテグレーション統括本部

＜ヒアリング内容・学んだ点＞
・2022 年 4 月に設立した「グローバル渉外統括本部経済安全保障室」から活動内容や注目している動向についてヒアリングした。
　また、調達部門である「バリュー・インテグレーション統括本部」から同業他社との情報

共有や調達先への情報提供についてヒアリングした。

・経済安全保障室を設立したことにより、社内外の経済安全保障に関する問合せ先が明確になるため、兼務職制であっても組織化することは検討すべきことである。
・各業界に団体活動などを通じて、経済安全保障や情報セキュリティに関して、各業界内で横連携による情報収集や議論することが重要である。
・行政や団体、あるいは弁護士事務所が開催するセミナー(無料のセミナーも多い)に参加して情報を入手することが必要である。
・入手した情報を現場まで展開することで、全社的にレベルを向上し現場の対応力をつけている。
・サプライチェーンに関しては、グループかつグローバル規模で調達BCPを構築し、「SENSE」「THINK」「ACT」の調達リスクマネジメントシステムを実行することで、リスクを可視化し事前に対策を講じている。
・企業の規模を問わず、調達先から入手した情報を全社レベルで共有することだけでなく、サプライチェーン双方向で情報共有することが重要である。

日　程：2024年1月9日(火)
面談者：情報セキュリティリスク統括本部　副統括本部長　村山 厚氏

＜ヒアリング内容・学んだ点＞
<u>サイバー攻撃事案の振り返りと得た教訓</u>

・2017年5月12日WannaCryと呼ばれるワーム型ランサムウェアが欧州の現地法人の検査機器から社内ネットワークのサーバーなどに次々と感染、グローバルで被害が発生した。
・被害範囲は、社内ネットワークに接続されている業務システムサーバー、OA用PCなど情報システム部門が管理している機器から、工場の製造･生産システムまで多岐にわたった。
・昨今、世の中の潮流(DX、働き方改革)へ対応するために、早急なサイバー対策整備が必要でありサイバー攻撃が事業へ影響を及ぼすことが明らかであることから、今まで以上に「経営」としてセキュリティを考えなければいけない状況である。
・WannaCry被害から学んだ５つのポイント。
　① セキュリティ対策範囲
　　→いろいろなモノがつながる前提で「見える化の推進」「社内 IT に加え、生産製造現場への網羅的なセキュリティ対策範囲の拡大」。
　② セキュリティパッチマネジメント
　　→「あてなくても大丈夫」から「あてなければいけない」文化への変革と適用プロセスの整備徹底。
　③ IoT/OTセキュリティ
　　→事業被害ベースでのリスク分析に基づいたセキュリティ対策の検討。
　④ サイバーBCP
　　→サイバー攻撃時のバックアップ、シナリオ、行動フロー整備及び有事の際に的確に行動をとるための訓練や演習の拡充(自然災害時BCPとの両立)。

⑤ 脅威情報分析

→継続的にプロアクティブな対策を実現するプロセス整備。

サイバーレジリエンス強化の取り組み

・サイバーセキュリティを経営課題として位置づけたセキュリティ対策を継続的かつ着実に実行することが重要である。しかし、絶対の安全はないため、有事の際には、短時間で回復できる抵抗力をつけることが必要である。
・高度化/増加するサイバー攻撃へ対処するために、社内コミュニケーションを拡充し、共感を得ること、さらには、社会全体でのセキュリティエコシステムを構築し、仲間を増やすことが必要である。
・従業員一人ひとりがセキュリティを正しく理解、共感し、自分事として捉えて行動することができる意識づくりを醸成することが必要である。

④ 自動車関連企業(東証プライム上場)

日　程：2023 年 10 月 3 日（火）
面談者：経済安全保障 専門部署

＜ヒアリング内容・学んだ点＞

経済安全保障への対応を全社で推進する時に重要なポイント

・経営トップがその重要性を認識し、発信することが肝要である。その上で、会社規模に応じて経済安全保障の担当者・委員会・組織を持つ事は 1 つの有効な手段である。

経済安全保障 専門部署について

・設置の目的は、技術流出防止とサプライチェーン対応の強化の 2 つである。
・専門部署のメンバーは、管理部門から経済安全保障に関係のある部署(法務、輸出管理、渉外など)からそれぞれ経験者を中心に組成した。
・事業部門の部長レベルを中心に兼務を発令している。それらの者が参加することで、事業活動や技術・製品開発であっても経済安全保障を念頭に置いた取り組みを推進できる。
・専門組織を立ち上げた効果として、全社的に相談先が明確になるというメリットがある。最新の政策動向から具体的な事業案件まで関連する相談は専門部署に一本化され、自社の課題が一元化できる。

セキュリティ対策について

・先ず各社で自社技術・ノウハウの整理・棚卸をして、狙われそうな技術・ノウハウを特定することから着手する。先端技術だけではなく、比較優位・独自性があるものも狙われるので注意が必要である。
・狙われそうな技術・ノウハウのセキュリティ対策は、警察や公安調査庁が最新事例を持っている。情報提供・講演実施などで協力して頂けるので活用するとよい。
・人を介しての流出が多いことから、従業員向けにセキュリティの啓蒙活動に注力している。
・セキュリティ対策について企業間の情報交換も有用である。経済団体や業界団体が情報交換の場を設置したり、集約した意見を政府へ申し入れするなどで役割を果たすと日本全体の底上げにつながるだろう。

予算や人員等のリソースに限りがある中小企業においても、経済安全保障面のリスクを理解して対策を実施している好事例が多く見られた。また、事例を紹介したどの企業も経営者自らが自社のリスクを理解し、対策を行っているということも非常に重要なポイントである。

大手企業においては、サイバーセキュリティ対策やサプライチェーンリスクの可視化を、自社内に止めずサプライチェーン全体を考慮した情報連携、情報共有をお願いしたい。中小企業を含めた取引先を守ることが、ひいてはサプライチェーン全体を守ること、自社を守ることにつながることとなる。

第４章　本委員会の活動内容から得た知見

４．１　経営者に期待するマインドセット

本章では、本委員会の活動を通じて得た知見について述べたい。まずもって重要なことは、経営者自らが危機管理意識を持ち、経済安全保障を『自分事として捉える』ことである。第 3 章にある中小企業 5 社の好事例は、社長をはじめ取締役の方が自ら紹介して下さったものである。このことからも経営者のコミットメント・経営者自らが率先垂範することの重要性がうかがえる。その上で、サプライチェーンやサイバーセキュリティ対策への対応を各社毎にできる事から自助努力で備えを進める事が肝要である。

企業毎にできることから対策を講じた上で、『外部連携』することも重要である。経済安全保障の専門部署を設置する大手企業であっても、経済安全保障の範囲は広範に及ぶだけに、自前主義だけでは立ち行かず、企業間の情報交換を通じて連携しながら対応している状況が分かった。また、サイバーセキュリティ等を担う専門人材の育成、コスト負担への対応など、個社では対応しがたい課題がアンケートから浮かび上がってきた。こういった課題解決に向けては、政府及び経済・業界団体等への支援・協力要請も必要となるだろう。

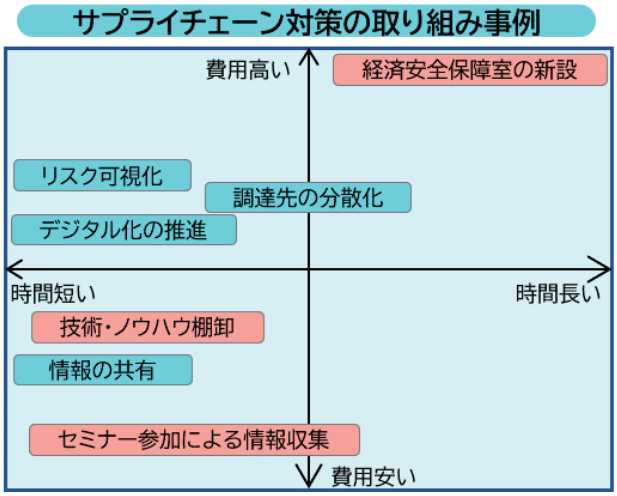
４．２　全企業に求められること（委員会独自の想定）

第 3 章で述べたサプライチェーンやサイバーセキュリティ対策への取り組み事例を実践した場合に想定される費用と時間軸を委員会独自で想定した内容が以下図である。（図表 4-1、4-2）これから取り組みを検討される企業への参考となれば幸いである。

サプライチェーンの観点では、まず手始めに、各社が比較的短時間で費用も抑制して取り組めそうなことから始めていくのはいかがだろうか。例えば、自社の「技術の棚卸」、既存取引先や時に競合となり得る同業他社との「情報の共有」から始めることを期待したい。自社の強み（競争優位性）や弱み（他社依存、調達困難等）を把握し、リスクイベント発生時に自社にどのような影響があるかを把握することは、対策の手始めとして有効かもしれない。また、取引先と双方向の密なコミュニケーションをとり、外部環境の動向を適時適切に把握し、状況によってはリスクイベント発生時に外部と連携して対応できるような体制を日頃より整えていくことを検討することも一つである。

次に、少し費用はかかるが、「リスクの可視化」「デジタル化の推進」に目を向けたい。前述した「技術の棚卸」「情報の共有」の取り組みにより把握したサプライチェーン上のリスクをクラウド上で可視化し、関係者が、サプライチェーンに関して同じ情報量を一元的に把握できるような仕組みを構築できると、より精度の高いサプライチェーン対策につながってくるだろう。これらの取り組みにより、自社のサプライチェーン上の問題点（≒リスク）を客観的に把握することができれば、将来的な自社の事業継続性の観点での予防策や BCP 対策策定につなげていくことができる。その一つの対策具体例が「調達先の分散化」であり、サプライチェーン対策として、参考にして頂けると幸いである。

【図表４－１】



青：サプライチェーン対策
ピンク：サプライチェーン・
サイバーセキュリティ
共通の対策

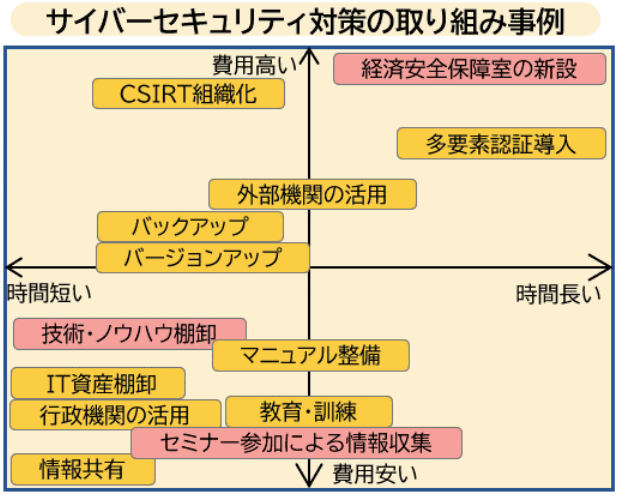
（出典：本委員会）

サイバーセキュリティの観点では、まず「情報共有」を意識すべきである。顧客や行政機関からの注意喚起や事例の収集・分析を進め、社内で適切に共有することで社員の意識醸成を図る事が必要である。これに加え、攻撃を受ける可能性のある「IT 資産棚卸」やセキュリティ事故（インシデント）発生時の対応・業務再開用の「マニュアル整備」も対策として有効である。コストをかけての「データバックアップ」や「ソフトウェアアップデート」は定常的な作業として不可欠ではあるが、実施するだけではなく、「社員教育」、マニュアルに基づく「業務再開訓練」もあわせて行い、万が一の自体にも迅速に対応できるような体制を確立することも重要である（バックアップがあってもすぐに復旧するのは困難である）。

また、パスワード盗難による社内のシステムやネットワークに侵入を試みることもあるため、「他要素認証」（例 パスワード+認証アプリ）の導入などのセキュリティツールの導入や、インシデント対応の専門チームの設立（「CSIRT＊組織化」）など、対策の専門性を高めていくこと、常に見直し続けることが期待される。

＊ CSIRT：Computer Security Incident Response Team の略。
セキュリティインシデントが発生した際に対応するチームのこと。

【図表４－２】



黄：サイバーセキュリティ対策
ピンク：サプライチェーン・
サイバーセキュリティ
共通の対策

（出典：本委員会）

「サプライチェーン」「サイバーセキュリティ」両項目共通の項目で、より高度な取り組みとして、「経済安全保障室の新設」（組織化）が挙げられる。一部の大手企業では、経済安全保障対策の一環で専門部署を新設する動きも出てきている。また、専門人材の育成・社内研修等の充実に向けた動きも見られるようになってきている。このような取り組みに至るまでには、相当のコスト（労力と時間）が必要と思われるが、外部セミナーに参加することによる主体的な情報収集等、まずはできることから少しずつ始めることが肝要である。

おわりに

経済安全保障に関し、経営者自らが率先して正しく理解するとともに、できることから自社の事業活動に落し込んでいく重要度、緊急度について本文中でも繰り返し述べており、ご理解頂けたと思うが、特に中堅・中小企業の経営者の皆様にとっては、依然としてハードルが高いと感じられているのではないだろうか。

しかし、米中対立はじめウクライナ危機、パレスチナ情勢の緊迫等、世界中で発生している国際問題は長期化する可能性が高く、地政学的な分断がもたらす世界経済への影響は日本経済にも作用し、中部経済同友会の会員企業も避けられない。先行きが見えない時代だからこそ、経営者としてリスクに立ち向かい、挑戦していく姿勢が求められる。サプライチェーンやサイバーセキュリティに限らず、幅広いリスクに対応していくため、平時からアンテナを高く張り、自分事として捉えていくことが重要である。

中部経済同友会の会員の皆様におかれては、本報告書を参考にして頂き、経営者として強力なリーダーシップのもと、経済安全保障を自分事として捉え、取り組みを加速して頂き、自社及び中部地区、日本国内の産業発展に繋げて頂ければ幸いと考える。

末筆ながら、安全保障から経営を考える委員会の活動に際し、アンケートにご協力頂いた同友会会員企業、ヒアリングなどを通じて絶大なる支援を頂いた企業のご関係者の皆様に心より感謝を申し上げる。

以　上

資料編

資料１．安全保障から経営を考える委員会　活動状況
資料２．委員会活動（講演会）の議事録
資料３．中小企業へのヒアリング議事録
資料４．大手企業へのヒアリング議事録
資料５．安全保障から経営を考える委員会　委員名簿

資料１．　安全保障から経営を考える委員会　活動状況

日付	イベント	内容・訪問先・講演者
2023.5.9	ＷＧ活動	第１回ＷＧ会議
2023.5.24	会議	第１回正副委員長会議
2023.6.5	ＷＧ活動	第２回ＷＧ会議
2023.7.10	ＷＧ活動	第３回ＷＧ会議
2023.7.24 ～ 8.18	委員会活動（アンケート）	アンケート調査
2023.8.22	ＷＧ活動	第４回ＷＧ会議
2023.9.5	委員会活動(講演会①)	トヨタ自動車株式会社 情報セキュリティ・トラスト部長 古田 朋司氏
2023.9.6	ＷＧ活動（ヒアリング）	ＮＴＴコミュニケーションズ株式会社
2023.9.6	ＷＧ活動	第５回ＷＧ会議
2023.9.12	会議	第２回正副委員長会議
2023.9.14	ＷＧ活動（ヒアリング）	株式会社みずほ銀行
2023.9.27	ＷＧ活動（ヒアリング）	株式会社日立製作所
2023.9.27	ＷＧ活動	臨時ＷＧ会議
2023.10.3	ＷＧ活動（ヒアリング）	自動車関連企業(東証プライム上場)
2023.10.16	ＷＧ活動（ヒアリング）	加藤軽金属工業株式会社
2023.10.20	ＷＧ活動	第６回ＷＧ会議
2023.10.25	ＷＧ活動（ヒアリング）	ゼネラルヒートポンプ工業株式会社
2023.10.27	ＷＧ活動（ヒアリング）	エムアイシイー株式会社
2023.10.30	ＷＧ活動（ヒアリング）	株式会社精器商会
2023.11.9	ＷＧ活動	第７回ＷＧ会議
2023.11.20	ＷＧ活動（ヒアリング）	株式会社三喜工作所
2023.11.29	委員会活動(講演会②)	明星大学 経営学部 教授 細川 昌彦氏
2023.11.30	ＷＧ活動	第８回ＷＧ会議
2023.12.14	ＷＧ活動	第９回ＷＧ会議
2023.12.18	会議	第３回正副委員長会議
2023.12.26	ＷＧ活動	第10回ＷＧ会議
2024.1.9	ＷＧ活動（ヒアリング）	株式会社日立製作所
2024.1.11	ＷＧ活動	第11回ＷＧ会議
2024.1.24	ＷＧ活動	第12回ＷＧ会議
2024.2.1	ＷＧ活動	第13回ＷＧ会議

資料２．　委員会活動（講演会）の議事録

講演会レポート《委員会活動①》

日　時：2023 年 9 月 5 日（火）13:00～14:00
行事名：安全保障から経営を考える委員会 主催講演会
講　師：トヨタ自動車株式会社　情報セキュリティ・トラスト部長　古田 朋司氏
演　題：サプライチェーンを含めたサイバーセキュリティの取り組み
～経済安全保障のリスクに備えて～

■講演内容要約

◇本日お伝えしたいこと

①戦争とサイバー攻撃の関係

敵対国は戦争へ突入前にサイバー攻撃を実施している例が多い。

②サプライチェーンのセキュリティとは？

フィジカル面とサイバー攻撃の両面が急速に進みつつあり、A）サプライチェーンを経由して自社、自社の製品・サービスが攻撃を受ける、B）サプライチェーン上の取引先がサイバー攻撃を受けて、自社の事業継続に影響するや自社の情報が漏洩する、という大きく 2 パターンに分かれる。

③サプライチェーンのセキュリティ対策とは？

利用しているソフト、アプリの構成情報の把握と脆弱性の確認等の適切なセキュリティ対策が必要で、仕入先にも適用する必要がある。

◇トヨタ自動車のセキュリティ取り組み体制

- 経営層直轄下に情報セキュリティ統括責任者（CISO）を設置し、また各分野別に役員クラスの責任者を設置している。横串部門である情報セキュリティ推進部に情報を集中させ、情報セキュリティ推進会議にて報告、方向付けを行っている。
- サイバー攻撃は全社の重点管理リスクの一つとして位置づけしている。サイバー攻撃から身を守るには情報共有し、競争ではなく協働することが何より重要である。

◇過去に被害を受けたサイバー攻撃の事例と対策

- 対策は最新のファームウェア(パッチ)を与えるなど適切なセキュリティ対策を実施しつつ、バックアップを取っておくことが肝要である。
- 業務妨害（犯罪者組織）、情報漏洩（国家支援の組織）が主な被害である。
- 経営トップ自ら対策に関わる事が重要である。

◇経済安全保障とサイバー攻撃

戦争開始前からサイバー攻撃は始まり、ハイブリッド攻撃が常識化している。

◇世の中のサイバー攻撃の状況

製造業が 3 割を占めるが、業種に限らず被害件数は倍々に増加傾向にある。

◇自動車業界へのサイバー攻撃の状況

日系製造業を見ると幅広い企業で被害が発生しており、自動車業界に限ったものではない。

◇サプライチェーンサイバー攻撃事例（仕入先での業務影響）

- 受発注・出荷システムに限らず、全 IT（社内システム）システムが停止する。元通りになるには数ヶ月を要し、その間、全てをマニュアルで処理しなくてはならないため、現場社員の負荷・心理的重圧は非常に高い。従って、経営トップ自らの積極的な関わりが重要である。
- リモート接続装置から攻撃されるケースが多い。

◇サプライチェーンセキュリティ強化の取り組み

経済産業省のサイバーセキュリティ経営ガイドライン Ver.3.0 のサイバーセキュリティ経営の「3 原則」が参考になる。

◇ご参考；仕入先へのセミナーの内容

1）緊急時の対応／連絡先方法の確認、2）標準型メールに対する社内への注意喚起、3）OS／ソフトの最新版の更新、4）リモートアクセスの脆弱性対策、5）多要素認証の導入、6）別ネットワークでのデータバックアップ、7）サーバーダウン時の生産継続

上記の内、全部は無理でも少しでも多く実施することが効果的である。

◇ご参考；取引先へのサイバー対策要求について

政府はサプライチェーン全体での対策を後押ししており、経済産業省、公正取引委員会共にそれぞれサイバー対策支援策、サイバー対策強化の重要性を提唱している。

◇サプライチェーンセキュリティ強化のゴール

トヨタグループや仕入先で知恵とノウハウを共有し、サプライチェーン全体で打たれ強い体質づくりを目指している。

◇ご参考；セキュリティ費用の目安

セキュリティ費用として、IT 予算の 15%以上を投じる企業が 3 割強にのぼる。

◇最後に

- サイバー攻撃は経営課題である。
- 担当者任せでは限界があるため、経営者自ら関わることが重要で、リスクを把握し適切なリソースの割り当てが必要である。

講演会レポート《委員会活動②》

日　時：2023 年 11 月 29 日（水）15:00～16:30
行事名：安全保障から経営を考える委員会 主催講演会
講　師：明星大学　経営学部　教授　細川 昌彦氏
演　題：中堅・中小企業に求められる経済安全保障

■講演内容要約

〇経済安全保障の時代

- 従来は政府・役所・企業にとって、「経済」と「安全保障」は別々に考えれば良かったが、近年はそれぞれが近づいて重なり合うようになった。その部分が「経済安全保障」である。重なり合う部分はどこなのか、その線引きが重要であり、企業経営者が最も意識すべきことである。
- 「経済」と「安全保障」が近づいてきた理由は、主に経済的威圧（他国を中国に依存させる）と強国化（他国に依存しない中国）の 2 つである。

〇経済的威圧

- 中国は経済力を使って、戦略的に相手国を中国に依存させようとしている。最近も原発処理水をきっかけに、日本産水産物の禁輸措置を行った。まさしく水産物を大量に日本から輸入しているという状況を利用して経済的に威圧をかけている。2016 年には韓国が北朝鮮への脅威から THAAD を配備した際には、北朝鮮ではなく中国が韓国の団体旅行客の渡航制限を行った。こうした経済的威圧を毎年行っているのが中国である。
- したがって、いかに中国依存から脱却するか、取引の分散化を図るのかが重要である。そのためには国内生産の強化、国際連携など行う必要がある。企業も自社の事業部ごとに中国への依存度を調査する必要があるが、その場合には、一次サプライヤーだけではなく、サプライチェーン全体を対象とする必要があるだろう。

〇強国化

- 中国は他国に依存することのないよう、とりわけ重要産業の国産化を進めている。この手法は巧妙に行われる。最初は中国市場へのアクセスをアピールして他国企業を国内に誘致し、自国企業との合弁企業を設立する。2､3 年後に技術が中国企業に移転し、自国で製造できるようになると締め出すようになる。戦略的な「誘致モード」から「排除モード」への転換である。
- もう一つの国産化政策として「買収」がある。大手ではなく中小企業を対象としている。中国はショッピングリストを作成しており､特に円安の今､日本企業は買収されやすい状況である。これまで大企業の調達部門は安く仕入れることが重要であったが、これからはいかに「持続可能」なサプライチェーンを構築するかがポイントである。
- 中国では「ゴールポストは動く」と言われるように、最初は「中国で生産すれば国産」として誘致を図るが、途中から「中国ブランドのみが国産」にルールを変更して外国企業は締め出すのは常套手段である。

〇反スパイ法・サイバー攻撃

- 中国では国家の安全に支障をきたすものであれば規制する。これを判断するのは共産党政権である。したがって、法律事務所に問い合わせてもあまり意味がないことに注意をしなければならない。

- 中小企業などサプライチェーンの中で脆弱な部分に攻撃を仕掛けてくる。巧妙さを増す攻撃を 100%防ぐのは不可能であり、不可能を前提に情報管理・技術管理等の対策を講じる必要がある。早期に検知し、レジリエンスを高め、被害を最小限にする（ダメージ・コントロール）こと、単なるマニュアル作成ではなく、日ごろから経営トップも含めて訓練を積んでいることが重要である。
- 2021 年にデータ安全法が施行され、海外にデータを持ち出すには政府によるチェックが必要となった。将来的には、企業は中国国外にデータを持ち出せなくなるリスクを抱えているため、経営者はどのような情報をどこに流しているのかを「データ・マッピング」により把握する必要がある。

〇まとめ

- 米中対立による中国リスクの顕在化、円安の進行などによってサプライチェーン改革に向けた動きがみられるようになり、企業経営の潮目が変わった。従来は経済効率が優先されたが、これからの経営判断はリスク対応力が重要な視点となる。

資料３． 中小企業へのヒアリング議事録

１．加藤軽金属工業株式会社

日　程：2023 年 10 月 16 日（月）
場　所：リモート形式で開催
参加者：取締役社長　加藤 大輝氏
概　要：アンケート結果からの取り組み
　　事例のヒアリング

設　立	1961 年 4 月
本　社	愛知県海部郡蟹江町西之森 三丁目 47 番地
代 表 者	加藤 大輝
年商	30 億円
資 本 金	60 百万円
従 業 員	85 人
営業品目	アルミニウムの押出形材の製造及びその加工 アルミニウムを使用した製品の組立・販売

１．具体的な取り組み内容

１）サプライチェーン強靭化

取り組み：材料等の調達コスト、物流コストの増大に対する「価格転嫁体制の構築」

材料を先物取引して製品価格に転嫁するのが業界ルールであり、ロンドン金属取引所である LME(London Metal Exchange)を通じて原材料を先物取引で調達している。3 ヶ月前に購入した原材料の価格が現在に適用される仕組みで、95%の顧客はこの制度を受け入れている。残り 5%の大口顧客は必ずしもこの制度が適用されない場合もある。

取り組み：材料等の安定的な調達・供給、物流ネットワークの安定化に対する「調達先分散化」

現在の調達先はドバイ（50%）、オーストラリア（30%）、ロシア※（5%）残りは自社の再生アルミである。ロシア、ウクライナの影響は受けている。

※2023 年後半から別調達先に切り替え

取り組み：調達先・販売先の多様化、分散化に対する
「燃料・電力価格安定調達先からの仕入れ体制構築」

来年から BRICS などのガス算出国付近からの調達を検討中である。

取り組み：サプライチェーンにおける気候変動・脱炭素に対する
「グリーンアルミ調達、リサイクルアルミ調達」

グリーンアルミは独自の安価で調達できるルートがあるものの、引き合いとしてはまだまだ低調に留まっている(グリーンアルミは価格が高価)。

国内外の比率は圧倒的に海外であり、ロシアが水力発電の精錬所を多く設けている。ロシア以外の場合、太陽光・水力発電の精錬所を有するのはドバイやオーストラリア、インドネシア等であり、今後期待が大きい。

地政学リスクの情報はエネルギー関連の業界紙、シンクタンクや証券会社のレポートを参照している。

取り組み：サプライチェーンの強靭化に資する他企業との連携体制の強化における

①「リサイクルアルミ再生・国内調達体制構築」

中小企業同士でアルミの再生炉を構築する計画がある。3K 職場で人が採用できない問題や環境問題があるので、自動化設備かつ再エネ由来の電源のみで運営予定である。

②「世界情勢を鑑みた調達体制の構築」

中国の不動産バブルがはじけるリスクに対し、調達先の複線化について情報発信している。

2）サイバーセキュリティ対策

サイバーセキュリティ対策としてはまだまだであるとの認識を持っている。防災と同じく、社内でセキュリティについての認知向上を図っている。

3）その他

・ 大手企業に求めるもの、政府に求めるもの

大手企業には、特に価格面において、世の中の変動に対する理解をしてもらいたい。政府には、世界的な情勢変化が起きた場合、原材料や燃料調達費の補填を急いでもらいたい。

・ 経済・業界団体に求めるもの

「カーボンニュートラル」で再生炉など再生モデル構築、「24 年問題」で共同配送や調達数社が同じ原材料などを共同で調達など、運用面まで支援してもらえる体制構築を希望する。

4）学んだ点

・ サプライチェーン強靭化に向け、LME を通じた先物取引による調達で価格転嫁体制を構築している。
・ 海外調達先の分散化を推進(ドバイ、オーストラリア、ロシア)している。
また、ウクライナ情勢の影響も受けており、中国の不動産バブルがはじけるリスクも懸念している。
・ サイバーセキュリティについては、社内でセキュリティの認知向上を図っている。

２．ゼネラルヒートポンプ工業株式会社

日　程：2023 年 10 月 25 日（水）
場　所：ゼネラルヒートポンプ工業株式会社
　　本社統括営業本部
面談者：代表取締役　柴 芳郎氏
　　主査　小倉 怜子氏

設　立	1984 年 11 月 6 日
本　社	愛知県名古屋市中村区
代 表 者	柴 芳郎
売　上	（非開示）
資 本 金	70 百万円
従 業 員	69 名（2023 年 4 月 1 日時点）
営業品目	各種ヒートポンプ製品の製造・販売、各種エネルギー関連システム設計

概　要：2023 年 7 月～8 月に実施したアンケート結果を踏まえ、日頃取り組まれているサイバーセキュリティに関する取り組みについて、ヒアリングを実施した。

１．IT システム環境について

- コロナ禍以前より、リモートワーク等を導入し柔軟な働き方ができる環境を整備している。
- 社員に対して会社が PC を貸与している。セキュリティの観点で、社内イントラには VPN 接続からアクセスを実施している。
- 社内メールは Microsoft365 を活用し、Teams 等で Web 会議を実施している。
- 各種ログインは ID・パスワード方式で行っており、年内に端末認証方式を導入し、セキュリティ強化をする予定である。
- 機密情報以外のデータ保管は、Sharepoint や Onedrive、Dropbox Business、OracleCloud のクラウドを利用している。

２．CSIRT（組織）について

- 2021 年度に発足した。社員数が増加したことや、デジタル庁が新設されて各種補助金の申請等の際に専門的な知見が必要になる場面が増えてきたことをうけて、組織化させた。
- 有事の際のプロジェクトとして発足ではなく、社内の IT・情報管理部門として日頃の業務として重要な機能を果たしている（全国の各拠点から 1 名ずつアサイン、現在 7 名で活動中）。
- 3 ヵ月に一度の定期的な会議体や、1 年に 1 回の安全衛生大会では、ヒヤリハットの事例共有等を行うなど、従業員向けのサイバーセキュリティに関する知見の向上の一端も担っている。
- ウイルス感染等が認められた際の初動などについては、シンプルで明瞭な手続き等を定めて社内で徹底、土日含め 24 時間体制で、何かあれば CSIRT に報告がくる仕組み作りをしている。
- CSIRT 発足後、サイバーセキュリティや情報管理の観点で、まず保有する IT 機器の数を把握する等の資産管理を手始めに行った。その後、どのようなタッチポイントでリスクがあるかなどの洗い出し・点検等を行った。
- 不定期にアクセスログの監視を実施したり、保有資産のソフトウェアのバージョンアップが適切に行われているかなどを都度確認したり、地道なフォローアップを行っている。
- その他事業継続性の観点で、システム障害時の復旧を早めるためにファイルサーバー2台をレプリケーションし、さらに災害対策で遠隔地にバックアップを行っている。

３．エムアイシイー株式会社

日　程：2023 年 10 月 27 日（金）
場　所：メールによる質疑応答
回答者：代表取締役　小島 由公香氏
概　要：会社概要、取り組み内容のご回答、質疑

設　立	1981 年
本　社	名古屋市熱田区比々野 41-1-805
代 表 者	小島 由公香
資 本 金	3,000 万円
従 業 員	13 名、社外契約 QA パートナー：11 名（QA＝quality assurance（品質確認、品質チェック）
事業内容	IT、AI、医療機器関連ローカリゼーションサービス

１．会社概要

ローカリゼーションとネーミングされているビジネスサービスの中の、UI とドキュメント及びヘルプデータの翻訳を行っている。通常の翻訳とはかなり異なり、単に翻訳するのではなく、データベースを駆使し、マクロ(CAT)を使用して、特殊な数々の翻訳処理ソフトでメモリーを判別しつつ、データ処理と翻訳処理を行う。作業の半分が AI や IT、3D 機器や医療機器などの技術翻訳、あと残りの半分が複雑なデータ処理業務である。簡単に言えば、作業のほとんどは、コンピュータのシステムエンジニアと同じフィールドの業務である。唯一システムエンジニアの作業と異なる点は、英語やフランス語、ドイツ語という他言語の翻訳が絡む点で、またこの処理は現在では「ポストエディット」という AI 処理が導入されている。

各フィールドの翻訳には、その分野の膨大な用語集を駆使する必要があり、入力上の詳細な約束ごとを厳守する必要がある。そうしないと、データベースの管理が出来なくなるためだ。別の言い方で業界内容を表現すれば、理系の PC データ処理と、文系の技術翻訳の両方が絡む業務とも言える。

クライアントはシスコシステムズ、オラクル、SAP、Google、ダッソーシステムズなどである。これらの各社が新規開発するドキュメントや、各種のシステム機能を英語から日本語に翻訳する。こうした開発は、製品やソフトが市場に出回る前に行われるため、我々の仕事には、非常に機密性が求められている。

日本の企業が上記企業のシステムやソフトを購入し導入する際、英文では解読が不便である。そのため日本語化を行うが、重複する文書も多いために、過去に訳した大量のデータベースを解析し、データベースから再活用する。この時、人工頭脳(AI)による解析が行われ、100%同じ文書なのか、ファジーマッチング率が 60%なのかがデータ上でより分けられ、100%同じ文書は、機械上で既に翻訳された状態で画面に表示される。このことはエディット作業の一貫にて、「ポストエディット」とネーミングされ、各企業のマニュアルや企業紹介文書などでは、現在こうした人工頭脳による処理が一般化されている。目下、シナリオライター達の間では、この AI による解析処理文書作成が、著作権上の大きな問題にもなっている。

データ処理に関しても、ローカリゼーションの業界では最先端の処理が行われている。面倒なデータの受送信なしで、クライアントとの間でデータ処理が行われる。具体的に説明すると、我々がクライアント企業のホストコンピュータに侵入(実際には、ユーザー名を入力して暗証番号を入れると侵入可能)すると、トラフィック(世界中に張り巡らされているデータ回線)を通して、翻訳すべき画面がモニターにアップされる。そのデータを翻訳処理し、その後またデータの送受信なく、相手のホストコンピュータに成果物を納品する、という工程が行われている。

上記は業務内容のごく一部のご紹介で、我が社の業務には、IT 系の上記クライアント同様に、最先端のデータ処理と最大限のセキュリティが求められている。

２．具体的な取り組み内容

１）経済安全保障に関する情報源

日本経済新聞、BBC news、NBC news、フィナンシャルタイムズを活用している。

２）サプライチェーンの強靭化に向けてサプライチェーンの可視化

取り組み：「クラウド上でのボードコミュニケーション」

サプライチェーンで繋がる各社が情報共有の場として、クラウド上に各社が共有して使用できるボードを作成し、業務での詳細な情報を日々アップしている。こうした情報の日々の共有が、結果として、互いのサプライチェーンの強化に繋がる(10 年前頃から実施)。サプライチェーン間のためのクラウド上への日々の情報アップは、直接利益を生み出す作業ではないため、時間をかけすぎると利益率が下がるが、自社だけでは気がつかなかったシステムの効率化や、自社が担当していない分野の仕事に関する情報が入手できる。

３）市場ニーズ、マーケットなど変化する経営環境に対する対応

取り組み：「常にネット関連の世界情報にアクセス」

世界各国の IT 関連や医療機器などの大手企業の動きをインターネット上でチェックしている。市場でどの様なニーズの仕事が、ローカライズを必要としているのかをチェックしている。

４）調達先・販売先の多様化、分散化

取り組み：「クライアントを国別に分類し受注を分散」

新しいシステムやソフトを開発している企業の本社所在地をチェックする（約 20 年前から実施)。また、我々のローカリゼーションサービス会社の仕事は、上記の大手クライアントから直接仕事を受注するのではなく、世界に点在するローカリゼーション・ベンダーから業務を受注する事が多い。その所在地も、チェックしている。

また世界に点在する現地だけではなく、そのベンダー企業のアジアオフィスや東京オフィスが存在する事があるため、こちらのオフィスもチェックしている。良かった事としては、上記行動を早くから実行したため、クライアント情報を得るコツが取得でき、企業間の合併や M&A などで調達先が変わっても、安定した受注を得る事ができている。

また、こうした世界企業の IT や 3D、医療機器などのクライアント企業で働く人材は、常に一定の企業に留まらず、ヘッドハントや自らのアクセスで報酬の良い企業に絶えず移動するため、その人材、つまり「人」と親しくなると、その「人」を通してその彼らが移動した新しい企業から仕事を得る事も多々ある。つまり、企業の「人」とのコミュニケーションは、各種情報以上に重要となる事もあり得える。

５）サプライチェーンの強靭化に向けてデジタル化の推進

取り組み：「常に最新のデータ処理にアクセス」

我が社の場合は、大手のクライアント(シスコシステムズや SAP、Google 等)が絶えず最先端のシステムやデータ処理を要求してくるため、絶えず最先端の技術を導入して業務を展開している（約 20 年前から実施)。良い点としては、常に最先端の技術に触れていることができる。

苦労している事としては、まだ開発途中のデータ処理を要求され、バグが発生したり、データ

処理工程でアクセス不能になったりするなど、思わぬタイムロスを強いられる事がある。

6）経済産業省、独立行政法人情報処理推進機構が取りまとめた「サイバーセキュリティ経営ガイドライン Ver3.0」における「経営者が認識すべき 3 原則」及び「サイバーセキュリティ経営の縦横 10 項目」に関する取り組み

（原則 3）

平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要であることを認識している。

取り組み：「クライアント側大手に対策本部あり」

大手クライアントからは常に、我が社のセキュリティチェックシステムの詳細な項目リストの提示が要求されている。また、このセキュリティチェックシステムのシートを作成し、各種のチェック項目にマーキングを入れ、2 ヵ月毎にエラーがないかの提出義務がある。

（重要項目 4）

事業に用いるデジタル環境、サービス・情報を特定し、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別している。

取り組み：「常に別データを別の場所に予備保存中」

ソフト開発会社でストレージ以上のデータ保存ができる機材を持つ企業に委託して、その機材を購入し、そのソフト開発企業のオフィスに我が社のデータのサブをキープしてもらっている（約 8 年前から実施）。現在は、クラウドが発達しドロップボックスなどのシステムも最大限活用中である。

３．今後の課題/要望

経済安全保障のフィールドは、以下の 3 つの観点がある。

1. 金融面での経済安全保障
2. 地政学的リスクでの経済安全保障（戦争、災害、気候変動等）
3. 法律上の経済安全保障（パテントなども含む）

経済安全保障は単に企業のシステムセキュリティのみではなく、常に上記の問題も絡んでくる事を認識する必要があると思う。特に日本政府が弱い点は、法律面で迅速な対応を行い、企業を側面からサポートする能力かと思う。また金融面では、世界の通貨の中で円の存在が弱まっていることは否めないため、経済安全保障を考える上で、こうした 1990 年以降の日本の金融経済の弱さ（この 30 年間、殆ど給与が上がっていないなど）も、今後より考えていく必要があると思う。

経済安全保障に関して、企業のコンピュータシステムで目下一番求められている事は、やはり「セキュリティ」項目かと思う。世界の IT 企業が、自社製品開発以外に最も力を入れて取り組んでいることは、「セキュリティ」ソフトの開発とシステムのセキュリティをコントロールする人材かと思う。日本では、この分野の人材やソフト会社がかなり不足しているのが現状ではないか。

ただし、もはやシステムや PC ソフトに国境はないため、他国のセキュリティソフトの導入など、解決策は多々あるかと思う。また人材に関しても、インド人の有能な IT 人材の活用なども考慮出来なくはないかと思うが、日本の場合は、異国人の雇用に関する言語の問題やビザや在籍に関する法律の問題もあり、事は簡単ではないだろう。経済安全保障に関して、自国のみで解決できない問題が多々

絡んでいる事実を、見逃すことは出来ないのではないだろうか。

４．学んだ点

- サプライチェーンをより強靭化するために、クラウド上のボードを利用して、日々の情報を共有し、情報の可視化を行っている。これにより、サプライチェーン間の互いのシステムをより効率良く利用する事が可能となり、自社のみでは得られない気づきも入手することが可能となっている。
- サイバーセキュリティ対策においては、大手顧客から詳細なセキュリティチェックを受けている(2 ヵ月毎のチェックシートの提出義務あり)。セキュリティのために、ホスティングやクラウドサービスを利用して、日々のデータバックアップを義務付けている。
- サイバーセキュリティに対応可能な優秀な人材や、複雑化しているセキュリティに対処可能なベンダーが、日本ではまだまだ不足しているのが現状である。海外の人材やサービスを利用する選択肢もあるが、事は簡単ではない。

４．株式会社精器商会

日　程：2023 年 10 月 30 日（月）
場　所：株式会社精器商会 本社・製造部
参加者：専務取締役　下村 文乃氏
概　要：会社概要説明、
　　取り組み内容説明、質疑

設　立	1959 年
本　社	名古屋市天白区中砂町 202
代 表 者	下村 方人
資 本 金	9,800 万円
従 業 員	55 名（2023 年 4 月現在）
事業内容	機器販売、工事施工、アルミダイキャスト品・アルミ鍛造品の切削加工 他

１．会社概要

1959 年に創業し、今年で 64 年目になる。製造部門もあるが、卸売業がメインである。主に SMC やキーエンスの空圧機器や細かなセンサーを豊田自動織機やデンソー、トヨタ紡織をはじめトヨタ系に卸している。売上のメインは、コンプレッサー関係である。お客様のご要望に何でもお答えすることをモットーに、事業を行っている。

製造機能はグループ会社の八伸工業が担い、アルミ加工等を行っている。創業以来、東大阪の企業にフランジの製造を委託していたが、コンプレッサーの生産台数が増加したことに伴い、生産能力が追い付かなくなったため、名古屋の支店として八伸工業を共同で立ち上げた。

２．具体的な取り組み内容

１）サプライチェーンにおける気候変動・脱炭素への対応

パリ協定が求める水準と整合した 5 年～10 年先を目標として企業が設定する温室効果ガス排出削減目標である SBT 認定を 2022 年に取得した。きっかけは、重要顧客の仕入先で構成される任意団体に属する会員企業が取得したという情報を聞いたことによる。認証を取得するために、CO2 排出量を細かく見える化できるツールを導入した。

現在、顧客へ製品を納品するための効率的な輸送ルートについて、顧客とともに仕入先全体で連携しながら見直しを行っている。基本的には顧客から示される方向性に全力でお応えするスタンスで取り組んでいる。

また、顧客からの燃料費の高騰分の補償費を算出するため、外注先まで含めた電気料等の使用量を細かく正確に把握することが求められており、対応している。仕入先と親会社が全員一丸となって、この局面に対応している。現状、自社だけでトラックを仕立てることが難しく、荷量的にもある程度大きなトラックで輸送しないとコスト的にも合わない。また、カンバンで 1 日に何度も納品するため、近隣の企業を巻き込みながら、顧客が仕立てたトラックで納品している。その際、顧客が提示したルートよりもベストだと思うルートを一緒に提案することもある。顧客からは、カンバンに合わせた希望の納品タイミングの要望もあり、互いにとって最適な輸送ルートを共に検証している。

２）サプライチェーンの強靭化に向けてデジタル化の推進

重要顧客の仕入先全体で、従来、紙であったカンバンを電子カンバンに変えようと、周りを巻き込みながら実施している。顧客の要望ではあるが、自社にとっても紙の保管場所を削減できるメリットがある。その結果、次の課題はデータを保管するサーバーの問題である。

2019 年に、重要顧客の仕入先企業の 1 社が、豪雨被害により会社の PC 内に保存していた CAD データが水没した影響で、顧客の工場が 1 ヶ月程製造できない状態になったことがあった。そのため、コロナ以前から BCP の観点でクラウド導入の流れがあり、以前から意識が高かった。

自社においても、東海豪雨では水没を免れることができたが、最新のハザードマップでは、津波による水没の可能性があるエリアに入っているため、BCP 対応が必須だと考えている。社員の安否確認システムの構築や非常食の備蓄などを行っている。

3）サイバーセキュリティの取り組みについて

代表者が IT 出身のため、サイバーセキュリティ対策は得意としている。また、受発注の生産管理システムが稼働してから 40 年経ち、システムの見直しを現在行っている。このタイミングに合わせ、セキュリティ面を最新のものにアップデートすることを検討している。オンプレで管理していたシステムをクラウド化し、いつでもデータが取れる状況を目指そうとしているが、一方でセキュリティ面は今までよりも深い部分までの対応が必要と考えている。サイバーセキュリティ面もアップデートしながら、業務改善を図っていくとともに、サプライチェーンを維持するためにも、生産を停めないシステムの構築が必要である。

現在、会社の PC にログインする際には、毎回認証を取っている。また、社内に IT 系に詳しい人材がいるため、Teams の機能を活用し、社員全員に向け「サイバーセキュリティ情報共有」として、実際に発生した具体的な事例を定期的に発信する自発的な啓蒙活動を行っている。

3．今後の課題/要望

- システムのクラウド化に伴い、業務の見直しも行いながら最適な仕組みを構築していきたい。
- 顧客との連携は重要と理解した上で、内容によっては、個を見た対応を行ってもらえるとよりやりやすいと感じる時もある。

4．学んだ点

- 重要顧客およびその仕入先の仲間とともに連携しながら取り組むことで、1 社単独では難しいサプライチェーンの強靭化を集団としての強みを活かして実現することができる。
- サイバーセキュリティはトップ層の強い意思により、取り組みを加速することができる。また、社員に向けて定期的な情報を発信による社員教育と意識醸成が必須である。

５．株式会社三喜工作所

日　程：2023 年 11 月 20 日（月）
場　所：リモート形式で開催
参加者：代表取締役　中野 喜一朗氏
概　要：会社概要説明、
　　取り組み内容説明、質疑

創　　業	1959 年
本　　社	愛知県あま市本郷郷中 47-1
代 表 者	中野 喜一朗
資 本 金	1,000 万円
従 業 員	35 名（2023 年 10 月現在）
事業内容	自動車部品関連、建築資材関連

１．会社概要

1959 年に有限会社三喜工作所という名前でメリヤスの問屋として創業した。その後、繊維事業から自動車部品の事業にシフトし、発展してきた。2021 年に SBTi（注 1）の認定を取得し、時代に則した取り組みを精力的に行っている。2023 年 10 月に中野 喜一朗氏が代表に就任した。社名の由来は、「お客様の喜び」「社員の喜び」「地域の喜び」というステークホルダーの三つの喜びを願う創業者の想いを表現している。所在地は、愛知県あま市で 2 拠点所有している。

経営理念として「柔軟な発想とものづくりで社会に喜びを提供する」を掲げ、ものづくりを軸に事業展開を行っている。事業方針には「安全な経営基盤」「人が触れない工程設計」「計画的な作業の遂行」の 3 点を掲げる。ここ 15 年程、無借金経営を行い、計画的な資金繰りでお客様に安心頂きながら、経営している。製造業として、変化点や不具合を起こさないことを強く意識しており、極力自働化を推進している。2008 年以降、17 時以降の残業を一切行っていない。

事業割合は、自動車部品関連事業で売上の約 85%を占めており、主な取引先はトヨタ系の 1 次サプライヤー企業となる。残り 15%は、建築資材関連の製造を行う。自動車部品の主要製品は、プラスチック部品と金属のボルトを締結する時の破損を防止するためのカラー部品、樹脂を保護しながら締結を保持するための円筒状の金属部品となる。競合先は大手が多いため、中小企業のメリットである小回りが利く点を活かしている。建築関係は、プレキャスト・プレストレストコンクリート工法で使用される金属部品となる。自社の主要工法は、冷間圧造加工、順送プレス加工、切削加工である。

今後の新たな取り組みは、①カーボンニュートラル（2030 年までに、2018 年度比で 50%の CO2 排出量の削減を目標に掲げ、推進中）、②IATF16949（注 2）の取得、③自社商品の開発（金属の端材を活用した部品の製造）の 3 つとなる。

（注 1）Science Based Targtes initiative（科学に基づく目標設定イニシアチブ）：企業と金融機関が最新の気候科学に沿って野心的な排出削減目標を設定できるようにする国際的な団体で、2030 年までに世界の排出量を半減させ、2050 年までに正味ゼロ排出量を達成することに沿って、企業の気候変動対策を加速させることに焦点を当てている。

（注 2）自動車産業に関する品質マネジメントシステムの規格

２．具体的な取り組み内容

１）サプライチェーンの可視化

製造工程は、自社でほぼすべて実施しているが、一部、表面処理と熱処理のみ、協力会社 3 社程度に依頼している。受注製品を品番別で分けたリストに、依頼する協力会社の所在地を記載し、見える化している。加えて、各社がハザードマップ上で想定されるリスクも把握しており、協力会社の所在地も考慮しながら、発注先を選定するようにしている。

自社製品の納入先での使用用途は把握できている。輸出は、すべて商社経由で納入している。

２）BCP（事業継続計画）の策定と実行

顧客企業の指導・協力のもと、政府の BCP ガイドラインを参考にしながら作成し、計画を実施している。「事業継続力強化計画」の認定を受けると、補助金の加点の支援が受けられる。

自社独自の取り組みとして、雇用の確保を最も重視している。有事の際、復旧後に雇用が離れては生産が再開できないと考え、最低 1 年間の給与が支払えるよう資金確保を常時行っている。

３）材料等の調達コスト、物流コストの増大に対する対応

昨今の材料費の増加分は、顧客にすべて認めて頂いている。扱っている金属の価格変動が激しいため、3～6 ヶ月スパンで定期的に市況のベースを顧客と定め、それに基づきすべての製品の材料単価を変動して頂いている。原材料は、複数のエリアの仕入先から、すべて自社調達している。

顧客への納品は一昨年前から、すべて自社便に変更し、原価低減に繋がっている。ただし、2024 年問題に備え、運搬作業者の雇用の確保が課題である。

４）サイバーセキュリティの取り組みについて

IPA（独立行政法人情報処理推進機構）が発行している情報セキュリティの方針設定を活用し、運用を進めている。社内では、紙媒体も使用しており、まだ対応途中が実態である。現状、目の行き届く範囲のため、トップ自らがすべての管理を行っている。データの管理は、情報流出の防止もありオフラインの PC で実施し、定期的にバックアップを取っている。重要顧客からは、情報セキュリティに対する注意喚起や事例の横展開といった教育を行って頂いている。

今後、IoT への設備投資も予定しており、情報セキュリティに関するランニングコストの確保や安全性の確保が課題と認識している。そういった専門人材の確保が中小規模の企業の課題だと考えている。突発性の高い仕事のため、常駐できる人材を雇用する必要がある。

５）カーボンニュートラルの取り組み

2021 年に SBTi の認定を取得したきっかけは、重要顧客の協力会での横の繋がりであった。もともと、中部経済産業局が主導して SBT 目標の設定を進めた企業が愛知県内に数社あり、その内の 1 社が重要顧客の協力会に所属する企業であった。その企業から、こういった認定があるという情報を聞き、自社でも取り組むことを決めた。比較的早くスタートが切れたと認識している。

３．今後の課題/要望

- 情報セキュリティ関係の知識は専門性が高いので、人材の確保ができないことが課題である。政府による専門人材の雇用のサポートがあるとよい。
- 1 社単独ではなく、グループなどで横の繋がりを強くできればいいが、同時にトラブルの共有や競合他社への情報流出といったリスクに懸念がある。

４．学んだ点

- 企業間同士の課題や情報共有を通じて経営層が率先してあるべき姿を思い描き、各取り組みの重要性を理解し推進することで、早い対策を講じることができる。
- セキュリティ人材の確保は中小企業の課題であるが、秘匿性が高い情報等を取り扱うため、副業・兼業等による手当てではハードルが高く、自社独自で確保せざるを得ない。そのため、サイバーセキュリティ人材の育成や政府による支援が急務といえよう。

資料４． 大手企業へのヒアリング議事録

１．NTT コミュニケーションズ株式会社

日　程：2023 年 9 月 6 日（水）
場　所：大手町プレイス ウェストタワー
参加者：情報セキュリティ部長　小山 覚氏

設　立	1999 年
本　社	東京都千代田区
代 表 者	丸岡 亨
売　上	(非開示)
資 本 金	2,309 億円
従 業 員	9,300 人(NTT Com グループ:17,800 人)
営業品目	国内電気通信事業における県間通話サービス、国際通信事業、ソリューション事業、及びそれに関する事業等

概　要：「ランサムウェア攻撃の備えについて」および「サイバー攻撃の動向と安全保障戦略への対応」についての紹介およびディスカッション。

１．ランサムウェア攻撃の備えについて

＜統計から学ぶ教訓＞

- 警察庁が令和 4 年の統計を発表している。令和 4 年は、企業規模・業種問わずランサムウェア攻撃を受けている。
- ランサムウェア攻撃はテレワーク環境を狙っている。テレワーク用の VPN 機器やリモートデスクトップからの侵入が 80%以上となっている。テレワークが減り、使わなくなったテレワーク環境には注意すべきである。コスト面から VPN 機器の保守契約をしないケースがある。セキュリティ対策が更新されず、攻撃を受けてしまうことになる。
- ランサムウェア攻撃にあうと、業務が停止する。長引くと半年にもわたり影響が出ることもある。自社だけではなく、取引先や業界にも波及してしまう。
- 身代金を払っても、復旧してくれるとは限らない。バックアップを取っていても復旧できないことが多い。(統計では 80%が復元できなかったと回答)
- アメリカの Web サイトだが、危険度の高い機器や IP アドレスをリストアップしているサイトがある。機種名や会社の IP アドレスを検索するとセキュリティホールがあるか確認できる。バックアップだけに頼らず、ランサムウェア攻撃の入口のセキュリティ対策が必要である。

＜事例から学ぶ教訓＞

- 2021 年に徳島の病院がランサムウェアに感染し診療が止まった。翌年の 2022 年には大阪の病院がランサムウェアに感染し、こちらも診療が止まった。大阪の病院は徳島の病院と同じ VPN 機器を使っていたにも関わらず、徳島の事件があっても同じように古いセキュリティ対策となっていた。同じ業界として情報共有しておけば防げたはずである。
- 大阪の病院は給食事業者経由で感染した。従来は経営者からすると、侵入されても自社にとられる情報がないから気にしていないということだったかもしれないが、自社を守ることがネットワークでつながった取引先を守ることにつながるということを意識すべきである。
- 自動車会社の例を挙げると仕入れ先がサイバー攻撃を受けたことで、国内の全工場を停止した。こうした判断は素晴らしい。
- 東海で身近な例としては、港湾コンテナターミナル管理のシステムがランサムウェア攻撃に

あい、機能停止した。先の 2 つの病院の事件と同じ VPN 機器を使用していた。港湾機能は重要インフラであり、アメリカでは台湾有事の際に、港湾の機能を止めるという発言が下院議員から出ている。(港湾の機能停止は)経済安全保障に直結する話となる。

＜まとめ＞

- コロナ禍で導入したテレワーク環境をランサムウェア攻撃は狙っている。今やウイルスを送り込むより、テレワーク環境から社員になりすまして侵入してくる。
- 不要であれば、思い切ってテレワーク装置を撤去、あるいは必要であれば保守契約の締結・更新を行って最新の脆弱性パッチをあてることである。
- 人材がいない理由で問題を先送りするのではなく、一番時間がかかる人材育成に取り組んだ上で、経営者として今できることをバランスをとってやるべきである。
- 自社の IP アドレスのセキュリティホールを検索し、結果をベンダーに見せて対策を確実に行うことが重要である。
- クラウドサービスのセキュリティの脆弱性対策は事業者に任せて問題ない(攻撃者が上手で100％ではないが)。企業がやるべきは ID とパスワードの管理である。どれだけ言ってもわかりやすいパスワードを使ってしまうので、多要素認証を入れるべきである。攻撃者はほぼ敬遠する。
- バックアップは必要ではあるが、システムの復元は 20%ほどしか成功しないということを念頭におくことが重要である。バックアップを使って業務を再開するマニュアルを作り、訓練をしておかないとうまくいかない。
- 何より、同じ業界や地域での情報共有をしておくことが重要である。通信の競合他社同士は互いに互換性のあるサービスを提供しており、裏側で動いている仕組みも似通っているので、攻撃者からすると同じ手法が展開できる可能性がある。競合他社同士の情報共有は非常に重要である。
- サイバーセキュリティ強靭化に関する助成金・補助金について経済産業省が税金の減免措置、中小企業向けに補助金を出している制度があるはずである。クラウドサービスを使うこともトータルコストを抑える意味では考慮しても良いのではないか。

２．サイバー攻撃の動向と安全保障戦略への対応について

＜サイバー攻撃の動向＞

- ランサムウェア攻撃は、金銭目的と情報目的の 2 つに大別される。サイバー犯罪被害の金額は日本の GDP より多いと言われており、アメリカ、中国の GDP に次ぐ規模のお金が動いている。
- サイバー攻撃のパターンはいくつかあり、2020 年に多くの企業が狙われたことから経済産業省が公表している(大きく 3 パターン)。ネットワーク貫通型は VPN 機器を狙ったものである。次にランサムウェアによる二重の脅迫、データを暗号化して解除のための金銭を要求・さらにデータをばらまくといった脅迫で、これは犯罪組織による攻撃である。3 つ目は攻撃の高度化、海外拠点経由の攻撃である。NTT コミュニケーションズもサイバー攻撃を受けた。国に迫れる・スパイのように情報を盗む場合、通信事業者や大企業に侵入することが近道だとよく知っている。特にセキュリティの甘い海外から侵入しようとする傾向がある。
- アメリカの FBI のホームページではサイバー攻撃の指名手配が公開されており、軍服姿の人

が多い。日本はアメリカに侵入を試みるために攻撃者に狙われる可能性がある。

＜安全保障戦略の対応＞

- 経済安全保障戦略の 4 本柱の一つに、基幹インフラの安全確保が挙げられており、通信事業者が対象になっている。基幹インフラの安全確保の制度は来年春頃に運用開始の予定である。
- 政府からリスク管理措置の考え方が提示されており、所管大臣が取り組みをチェックすることとされている。取り組み状況の資料の作成には自社だけでなく、委託先の契約書やマニュアルも出すことになり、相当な負担となる可能性がある。
- 取り組みとして大きく 4 点が挙げられており、①悪意のコードの混入防止(対応できる企業は少なく先進的な企業から)、 ②保守点検時の安全確保(保守事業者が信用できるかどうか)、③レジリエンス強化(サービス提供を止めない)、 ④委託先管理の強化となっている。委託先管理は、意図しない変更を防止する仕組みや再委託先のサイバーセキュリティ対策の確認(今までやってない)など、非常に細かい内容に及ぶ可能性がある。アメリカ政府は IT ベンダーに要求し調査を実施しているようだが、そうした取り組みが日本でも始まる可能性がある。
- 経済安全保障の次には国家安全保障戦略あるいは懸念国有事のことまで考えておかなくてはならない。社員の安全確保は第一(日本人がいなくても事業が回るようにしておく、懸念国籍社員のヘイトクライム対策)である。次に事業の継続である。突然ライセンス停止と言われた際に対応できるかどうかである。NTT コミュニケーションズ特有だが、現地の通信事業者と連携してサービスを提供し続けられるか、海底ケーブルを切断されたときにどうなるか、切られ方によってはほかのルートに影響する。最後に重要情報の管理である。海外委託先による情報の流出や強制的に工場や事業所が接収されたときに情報ごと取られる等への対処が必要となる。
- 能動的サイバー防御は政府でも言葉の定義ができあがっていない状況である。アクティブディフェンスという軍事用語があり、反撃も辞さないという意味を持つ。これと取り違えて能動的サイバー防御についてミスリードされているところがある。能動的サイバー防御は反撃をするものではない。国の文書を見ると、懸念国のサーバー等に事前に侵入しておいてそれを停止することもあり得ると書いてある。各国が日本に対してやっていることと同じように、攻撃能力を高めて、相手国のサーバーに侵入しておいて、もしもの時にはそれをシャットダウンすることを念頭に置いている可能性はある。
- 民間企業において参考とすべきは、攻撃者の侵入シナリオでアメリカ政府が整理したものを参照すると、攻撃者は侵入できそうなところの偵察・進入用のリソース開発をする。内部に入り込まれては、もう気づくことはできない。偵察活動を能動的に察知する、セキュリティホールがないか常に確認が必要である。リソース開発では、アンダーグラウンドの情報共有サイトで自社が攻撃対象に上がっていないか確認して防御を高める。こうしたことが民間企業における能動的サイバー防御と考える。

２．株式会社みずほ銀行

日　程：2023 年 9 月 14 日（木）
場　所：リモート形式で開催
参加者：経営企画部、IT・システム企画部、
　　サイバーセキュリティ統括部、
　　コンプライアンス統括部等から延べ 10 名

発足日	2013 年 7 月 1 日
本　社	東京都千代田区
代 表 者	加藤 勝彦
売　上	－
資 本 金	1 兆 4,040 億円
従 業 員	24,652 人
営業品目	銀行事業

概　要：

経済安全保障における主な課題、グローバル経済や国内外の動向を踏まえた、各種リスクへの対策状況など中心にヒアリングを実施した。その他「サイバーセキュリティ」「サプライチェーン」の観点での個別具体的な取り組み状況等について、調査を行った。

１．経済安全保障の取り組み状況全般について

- 非常に多岐にわたって課題があり、米中規制強化の観点では、輸出入管理、投資抑制、政府調達規制や経済制裁規制といった両国の政策・法規制への対応が必要である。
- サプライチェーン強化に関しては、与信方針の見直しや人権デューデリジェンス強化等も必要である。
- 重要インフラの安全確保の面では経済安全保障推進法対応、内部管理強化、サイバーセキュリティ強化等に向けて現在対応している。
- さらに、レピュテーションリスクの再定義やサードパーティーリスク管理強化、個人情報保護対応等については横断的なテーマとして都度対応していく。
- 足元の課題としては、経済安全保障推進法対応があり、同法の「基幹インフラ役務の安定的な提供の確保に関する制度」において公表されている「特定社会基盤事業者」の指定基準を満たしており、法令対応に向けた社内体制整備に努めている。
- グローバル経済動向や国際的なリスクに対しては、グループに重大な影響を及ぼすリスクを「トップリスク」と選定し、未然防止策や事後対応方針の策定等を通じ業務計画に反映することで、リスクガバナンス強化に努めている。
- トップリスクは、外部委員や社外取締役含めたリスク委員会での多面的な議論を経て選定され、期中のリスクコントロール状況は、取締役会にも都度報告されている。
- トップリスクには「米中対立の激化と中国経済の低迷」などグローバルなテーマも含まれており、トップリスク運営を通じてグループ内のリスクコミュニケーションを深め、リスク認識に対する目線統一を図っている。

２．「サイバーセキュリティ」「サプライチェーン」に関連する個別の取り組みについて

（サプライチェーン）

- 外部への委託案件のうち、一定の基準を満たした案件は、一般的な外部委託案件よりも深度あるシステムリスク、サイバーセキュリティリスクなどの評価を行う枠組みがある。
- サプライヤー（委託先）は大手企業に限らず、国内外グローバルに取引があり、また、2 次・3 次以降、最終委託先まで含めて、委託先や委託業務遂行状況等の管理が必要である。サプライチェーン全体のリスクを踏まえた外部委託を行っている。
- 外部委託時の考え方については IT システム企画部が従業員向けの勉強会を数百人規模で

定期的に実施している。また委託先に対しても定期的にコミュニケーションをとりながら、サイバーセキュリティリスク事例の共有等のセミナーなども実施している。

- 国内外問わず、まずは各国の経済安全保障法に準ずる法令対応を行っている。
- 金融情報システムの開発・運用に係る委託先の管理体制やオフショア開発体制の見直し等が発生した際は、システム開発を行う各国のシステム担当部で、現地法に準拠したプロジェクト管理を実施し対応している。

（サイバーセキュリティ）

- オンライン取引については、多要素認証を導入している。
- 金融機関の情報システムの安全対策に関するデファクトスタンダードである「FISC 安全対策基準」等に準拠する設計標準を定め、インターネット経由の顧客取引が可能な ID については多要素認証を採用するルールとしている。
- 最近は多要素認証を潜り抜けて、認証を突破する事例も出てきているため、都度セキュリティは強化していく取り組みが必要と認識している。
- サイバーセキュリティの観点での各種対応については、業界での横連携が重要である。
- 銀行業界内外での意見交換等を定期的に行うなど横連携の機会を設けており、顧客への各種注意喚起などは他社と共同で行うことも多い。
- 顧客の個人情報保護という観点では、その他、情報管理についての細かな権限設定や情報の保管に関する細かなルールの設定を設けている。
- 社外への情報移送についてモニタリング（ログ）する仕組みや、データをクラウド保管する場合は専用のチェックリストを設けている。
- 情報取得から廃棄に至るまでの各管理段階において、必要となる各種安全措置（組織的・人的・物理的・技術的・外的環境把握）に係る手続きを定め、従業員に徹底している。
- 従業員の情報リテラシー向上も重要である。サイバー攻撃に関する事例の従業員向け共有を定期的に実施、標的型メールへの対応の訓練なども行い、全社的な取り組みも進めている。

（その他）

- 海外拠点で万が一の緊急事態が発生した場合には、危機管理室が緊急時対応の行動計画として定めている「要因別行動計画」に沿って対応することになっており、連絡ルートや指示命令系統などはあらかじめ明確になっている。
- インシデント発生時の対応プロセスについても、関連部署・役員への報告体制（ルート）についてあらかじめ定められており、その後の当局報告や再発防止策の策定までのプロセスが明確化されている。

３．株式会社日立製作所

設　立	1920 年 2 月 1 日
本　社	東京都千代田区丸の内 1-6-6
代 表 者	小島 啓二
売　上	1 兆 6,313 億円(連結:10 兆 8,811 億円)
資 本 金	4,628 億円
従 業 員	28,672 名(連結 322,525 名)
営業品目	社会イノベーション事業

日　程：2023 年 9 月 27 日(水)
　　2024 年 1 月 9 日(火)
場　所：リモート形式で開催
参加者：グローバル渉外統括本部経済安全保障室 3 名
　　バリュー・インテグレーション統括本部 4 名
　　情報セキュリティリスク統括本部　副統括本部長　村山厚氏
概　要：１．グローバル渉外統括本部経済安全保障室
　　① 設立経緯やその役割と活動内容の紹介
　　② WG メンバーからの質疑
　　２．バリュー・インテグレーション統括本部
　　① 日立調達活動の紹介(パートナーシップのあり方/サステナブル調達/日立グループとの取引)
　　② WG メンバーからの質疑
　　３．情報セキュリティリスク統括本部
　　① サイバー攻撃事案の振り返りと得た教訓
　　② サイバーレジリエンス強化の取り組み

１．グローバル渉外統括本部経済安全保障室

〇設立経緯やその役割と活動内容について

- 2019 年頃、米国が中国の見方を変えたことを契機に、経済安全保障に関連する取り組みを開始し、その後国内で経済安全保障推進法の動きがあり、2022 年 4 月に経済安全保障室を設立した。
- 主な役割としては、国内外の経済安全保障に関する法令やリスクマネジメントへの対応、経済安全保障に関する社内対応の強化である。
- 具体的には、組織横断の課題への取り組み、社外ステークホルダーの窓口としての対応、また事業部門との連携、経営部門(リスクマネジメント会議)への報告などを実施している。
- 経済安全保障室は渉外部門の中に設立したため、渉外部門内人員で構成されている。リスクマネジメント本部、輸出管理、調達、情報セキュリティ、法務、財務、営業など、それぞれ専門分野を有する各部署と連携し対応している。
- 経済安全保障推進法への対応に関して、調達部門(バリュー・インテグレーション統括本部)や関連するスタッフ部門、および事業を推進するビジネスユニットや分社会社と連携している。
- 3～4 ヵ月に 1 回、経済安全保障連絡会議で、社内各事業部門やコーポレート部門、分社会社に情報共有をしている。

〇最新情報の入手方法や注目している動向について

- 米国の法律が先行して日本の法律などへ影響を与えているため、米国の情報はワシントンの事務所などから入手している。また経団連や日本政府からの情報など、多面的に情報を入手している。

・ 米国大統領令の対外投資、先端技術や人権に関する発表に注目している。日本からの輸出に影響を与える米国の輸入制限や特定製品、CHIPS 法やインフレ抑制法、環境関係の物品、半導体にも注意を払っている。さらに、米国での補助金対象事業の対外投資規制にも注目している。

〇経済安全保障というキーワードに関して、同友会会員企業や経営者へのアドバイス

・ 各業界で横連携を行い、情報収集や議論することが重要である。従って、本委員会は非常に良い取り組みであると考えている。
・ 最近では弁護士事務所が無料のセミナーを実施しているため、参加して情報を入手することも必要である。
・ 経団連の外交委員会からの情報収集や、懸念先調査には日本政府の経済安全保障室への問い合わせも可能である。
・ また、現場の対応力として現場レベルまで知見を上げることも重要である。

２．バリュー・インテグレーション統括本部

〇日立調達活動(サステナブル調達、調達レジリエンス)の紹介

・ 調達先(調達パートナー)との協創やバリューエンジニアリングへの取り組みを実施している。
・ また、サステナブル調達という観点で、環境、人権、社会の面からガイドラインを提示し、調達パートナーに考え方を通知している。
・ 調達レジリエンスの取り組みとして、従来の災害発生時の BCP 対応に加え、地政学リスクや経済安全保障のリスク検知への対応を含めた強化を実施している。
・ 調達パートナーのサステナビリティパフォーマンス評価およびモニタリングに、第三者評価プラットフォームの EcoVadis を導入している。
・ EcoVadis を活用し「環境」「労働と人権」「倫理」「持続可能な資材調達」の 4 分野の評価項目に基づいたサステナビリティへの取り組み状況を確認しており、グローバル・グループワイドで広く調達パートナーの参加を呼び掛けている。

〇調達部門として、他社や業界での情報共有や調達先への情報提供について

・ 日立は JEITA(電子情報技術産業協会)に参加しており、サプライチェーン可視化の観点で、二次以降の調達先可視化が共通課題だと認識している。
・ 調達本部で入手した情報は、事業部門(ビジネスユニット)や分社会社の調達部門を通して調達パートナーとリスク情報を共有している。また、調達パートナーから事業部門や分社会社を通じて入手したリスクは日立グループ全体で共有するなど双方向での情報共有を実施している。
・ 調達パートナーのリスク管理、リスク検知については社内各担当部門(経済安全保障室、リスクマネジメント本部、輸出管理)との連携で対応している。
・ 調達パートナーに対して、経済安全保障に特化したものではないが、従来から情報セキュリティ全般についてのガイドラインを提示し、情報共有を図ると同時に、サプライチェーンでのセキュリティ対策を実施している。
・ 今後、経済安全保障推進法への対応を進めていく中で、調達先への様々な依頼が出て来ると考えている。

３．情報セキュリティリスク統括本部

○サイバー攻撃事案の振り返りと得た教訓

- 2017 年 5 月 12 日 WannaCry と呼ばれるワーム型ランサムウェアが欧州の現地法人の検査機器から社内ネットワークのサーバーなどに次々と感染し、グローバルで被害が発生した。
- 被害範囲は、社内ネットワークに接続されている業務システムサーバー、OA 用 PC など情報システム部門が管理している機器から、工場の製造･生産システムまで多岐にわたった。
- 昨今、世の中の潮流(DX、働き方改革)へ対応するために、早急なサイバー対策整備が必要でありサイバー攻撃が事業へ影響を及ぼすことが明らかであることから、今まで以上に「経営」としてセキュリティを考えなければいけない状況である。
- WannaCry 被害から学んだポイントとしては下記 5 点である。

① セキュリティ対策範囲

いろいろなモノがつながる前提で、見える化を推進し、IT に加え生産製造現場の機器も対象として網羅的にセキュリティ対策範囲を拡大している。

② セキュリティパッチマネジメント

セキュリティパッチをあてなくても大丈夫という考えを一掃し「あてなければいけない」文化への変革と適用プロセスの整備を推進した。

③ IoT/OT セキュリティ

IoT 機器は数も多く個々の対策が困難であるため、事業被害ベースでのリスク分析に基づいたセキュリティ対策を検討した。

④ サイバーBCP

サイバー攻撃時のバックアップ、シナリオ、行動フローを整備し、有事の際に的確に行動をとるための訓練や演習を拡充し、サイバーBCP と自然災害時の BCP を確立した。

⑤ 脅威情報分析

継続的にプロアクティブな対策を実現するプロセスを整備している。

○サイバーレジリエンス強化の取り組み

- サイバーセキュリティを経営課題として位置づけたセキュリティ対策を継続的かつ着実に実行することが重要である。しかし、絶対の安全はないため、有事の際には、短い間で回復できる抵抗力をつけることが必要である。
- 高度化/増加するサイバー攻撃へ対処するために、社内コミュニケーションを拡充し、共感を得ること、さらには、社会全体でのセキュリティエコシステムを構築し、仲間を増やすことが必要である。
- 従業員一人ひとりがセキュリティを正しく理解、共感し、自分事としてとらえて行動することができる意識づくりを醸成することが必要である。

資料５．　安全保障から経営を考える委員会　委員名簿

【委員長】

永　井　　淳	新東工業株式会社	代表取締役　社長執行役員

【副委員長】

有　村　和　信	ＮＴＴコミュニケーションズ株式会社	執行役員 東海支社長
石　川　　卓	株式会社みずほ銀行	常務執行役員 中部リージョナルグループ長兼 エリア長(中日本エリア)
上　原　充　裕	第一生命保険株式会社	常務執行役員中部営業本部長
富　永　浩　史	豊田通商株式会社	代表取締役 CSO, 極 CEO
湯　次　善　麿	株式会社日立製作所中部支社	支社長執行役員

【委員】

天　野　源　之	天野エンザイム株式会社	取締役社長
岡　部　年　彦	東海東京証券株式会社	顧問
加　藤　大　輝	加藤軽金属工業株式会社	取締役社長
黒　川　道　男	学校法人日本福祉大学	副理事長
小　島　由公香	エムアイシイー株式会社	代表取締役
小　林　永　朋	カネソウ株式会社	取締役
佐　藤　昌　孝	東海東京証券株式会社	取締役会長
柴　　芳　郎	ゼネラルヒートポンプ工業株式会社	代表取締役
下　村　方　人	株式会社精器商会	取締役社長
中　野　喜一朗	株式会社三喜工作所	代表取締役
中　村　亮　介	東朋テクノロジー株式会社	事業企画統括部長
廣　田　利　幸	豊田合成株式会社	理事
藤　原　一　朗	株式会社名古屋銀行	取締役頭取
牧　野　隆　広	株式会社ミライプロジェクト	代表取締役
盛　田　淳　夫	敷島製パン株式会社	取締役社長
吉　村　憲　雄	宝交通株式会社	取締役社長
渡　辺　　大	株式会社マイ・ポジション	代表取締役

【ワーキング・グループ】

榊　原　尚　樹	新東工業株式会社	総務部 秘書 主任担当員
太　田　美奈子	新東工業株式会社	企画部 担当員
大　沼　隼　人	ＮＴＴコミュニケーションズ株式会社	企画部門 第二グループ 担当部長
杉　山　　拓	株式会社みずほ銀行	名古屋営業部 営業第三チーム 部長代理
谷　口　智　明	株式会社第一生命経済研究所	総合調査部マクロ環境調査グループ研究理事
摩　尼　貴　晴	株式会社第一生命経済研究所	総合調査部政策調査グループ長
辻　田　翔　一	第一生命保険株式会社	中部マーケット統括部 アシスタントマネジャー
待　鳥　真由子	豊田通商株式会社	渉外部 政策渉外室 室長
木　村　智　充	株式会社日立製作所中部支社	企画部 部長

【事務局】

田　中　喜　好	中部経済同友会	専務理事・事務局長
鶴　田　　進	中部経済同友会	事務局次長兼企画部長
山　田　有　美	中部経済同友会	主任

（令和 6 年 2 月 13 日時点）