ともに挑む。ともに実る。
MIZUHO

2024 年 11 月 6 日
みずほ銀行 産業調査部

Mizuho Short Industry Focus Vol.234

安全保障の視点からみる日本産業のサイバーセキュリティ
～サプライチェーン攻撃から産業を守る～

〈要 旨〉

◆ 安全保障の視点からサイバーセキュリティが注目されている。国際情勢が不安定化する中でサイバー空間が新たな国家間対立の場として使われはじめており、基幹インフラへのサイバー攻撃を通じて相手国の社会活動を混乱させる行為や、サイバー攻撃によって政府や企業の機微情報を窃取しようとする行為が増加している。国家安全保障と企業のサイバーセキュリティは密接に繋がっており、個々の企業のサイバーセキュリティを向上させることが、国家安全保障の確立に資する。基幹インフラ企業や先端技術を保有する企業をはじめ、産業界のセキュリティレベル向上は、安全保障の観点からも要請されるところである。

◆ 近年は、サイバー攻撃の中でも標的企業に直接侵入するのではなく、標的企業の取引先等のサーバーを介して標的企業に侵入する、サプライチェーン攻撃の脅威が高まっている。2022 年には大阪の医療機関がサプライチェーン攻撃を受け 2 カ月以上にわたり診療機能に支障が生じたほか、国内大手自動車メーカーの取引先企業がサプライチェーン攻撃を受け、同社の国内全工場で生産機能が停止する事案も発生している。

◆ サプライチェーン攻撃では、サプライチェーン上の1社が攻撃を受けると、サプライチェーン全体に被害が広がるおそれがある。サプライチェーン攻撃から産業を守るためには、大企業などセキュリティ意識の高い一部の企業だけでセキュリティ施策に取り組むのではなく、中小企業を含むサプライチェーン全体のセキュリティレベルを底上げする取り組みが求められる。

◆ 大企業に比べ、中小企業におけるセキュリティ施策の推進は容易でない。IPA[1]の実施したアンケート調査によれば、中小企業は予算や人材などリソース面での制約がボトルネックとして挙げられているほか、サイバーセキュリティの専任担当を置いていない企業も多い。セキュリティ施策のうちどこから始めたらよいかわからないとの声や、そもそもサイバーセキュリティに取り組む必要性を感じていない企業も多い。

◆ 中小企業を含む産業全体のセキュリティレベル向上に向けて、①政府内司令塔機能の強化とガイドラインの体系化、②支援と拘束力の両輪による企業への働きかけ、③セキュリティ人材を有効活用する仕組みづくりの 3 点を提言する。サイバーセキュリティは必要な施策が広範に及ぶ上、その必要性に対する社会的理解の浸透が道半ばであるため、社会一体となってのセキュリティ推進は容易ではない。しかし、国家レベルでサイバー安全保障が重要になる中で、サイバーセキュリティは個々の企業のリスクマネジメントの観点で重要であることは勿論、国益・公益の観点でも必要な取り組みである。産業界としてサイバーセキュリティを協調領域として捉え、産業全体で協働して取り組む体制づくりが早急に求められる。

[1] IPA：情報処理推進機構

1. はじめに ～経済安全保障の重要性

経済安全保障は主要な経営課題の一つに

2020年代に入り日本で急速に浸透した経済安全保障の概念は、サステナビリティやDX等の潮流と同様、今や企業経営を行う上で無視することの出来ないメガトレンドとなった。冷戦終焉後の米国主導の国際秩序が不安定化してきていることや、半導体やAI等の軍民両用品（デュアルユース品）の増加を背景に、安全保障の手段として、軍事のみならず経済施策も用いようとする取り組みが、経済安全保障である。経済が安全保障の手段として使われ始めた中、その経済を構成するのは民間企業であり、企業にとっても安全保障に向き合うことが求められている。

法制定を契機に経済安全保障が社会に浸透

戦後長らく経済と安全保障の関わりが少なく、民間企業が安全保障を意識する場面が少なかった日本においても、昨今の国際情勢の変化により、経済安全保障の重要性が高まっている。2022年には日本で初めて、経済安全保障の名称を冠する法律である経済安全保障推進法が成立した。この法律の制定を契機に日本社会でも広く経済安全保障の単語が浸透するようになり、現在では新聞でも連日紙面を賑わしている。

2. サイバーセキュリティは安全保障の必要条件

新領域安全保障が重要に

従来、国家間対立は主に陸・海・空を中心とする物理空間で繰り広げられてきた。しかし近年、宇宙空間やサイバー空間等、従来みられなかった新たな領域も国家間対立の場となっている。サイバー分野では、自衛隊が2022年にサイバー防衛隊を新設したほか、警察庁も同年にサイバー警察局とサイバー特別捜査隊を発足させるなど、政府として新領域安全保障の取り組みを本格化させている。

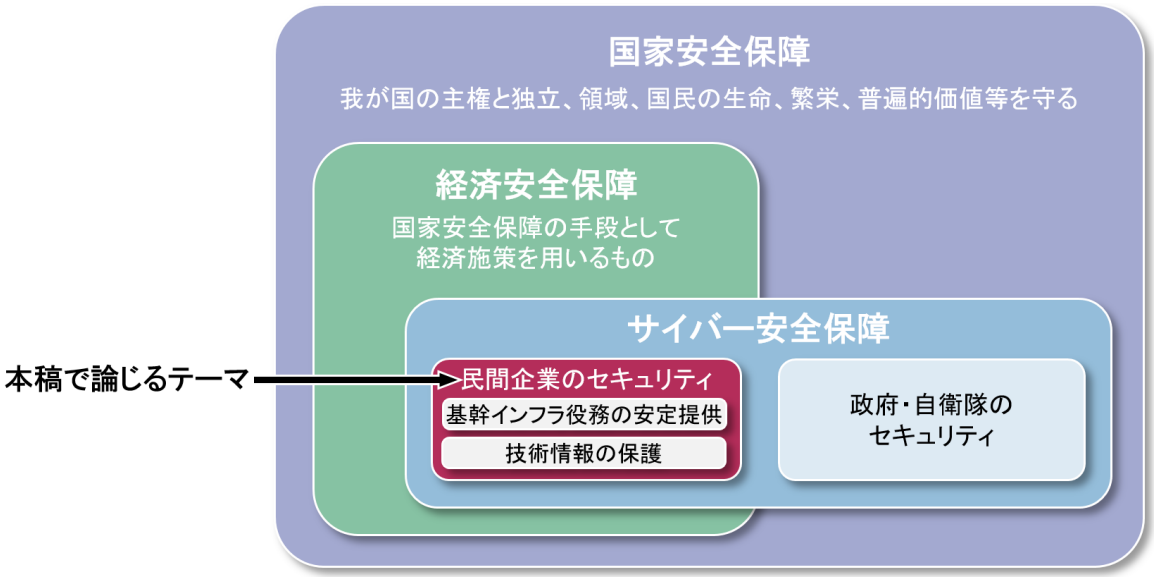
ロシア・ウクライナ戦争ではサイバー戦が展開

実際にサイバー空間が戦争に使われる事例も起きている。2022年2月に発生したロシア・ウクライナ戦争では、開戦の数カ月前から、ロシアからウクライナの政府機関、銀行、エネルギー企業等のインフラ機関にサイバー攻撃が行われ、社会活動を混乱させた後に物理的な軍事侵攻が開始されている。世界各地で戦争・対立が激化する中、サイバー攻撃から自国を守ることは安全保障を確保するために不可欠である。

サイバー安全保障のポイントは2点

サイバー空間における安全保障はサイバー安全保障と呼称される。サイバー安全保障の取り組み主体には、政府と民間企業の両方がある。このうち民間企業におけるサイバー安全保障のポイントは主に2点に整理でき、1点目は基幹インフラ役務の安定提供、2点目は技術情報の保護である（【図表1】）。

【図表1】安全保障の各概念とサイバーセキュリティの関係



（注）企業のサイバーセキュリティの目的は安全保障に限らないが、本稿では安全保障の観点に着目
（出所）国家安全保障会議「国家安全保障戦略」等より、みずほ銀行産業調査部作成

経済安全保障推進法では基幹インフラ役務の安定提供を規定

1 点目の基幹インフラ役務の安定提供は、2022 年に成立した経済安全保障推進法の 4 本柱の 1 つとして規定された。本法では、経済活動に不可欠なインフラ企業を特定社会基盤事業者として政府が予め指定し、重要設備導入時の事前審査や勧告・命令等を政府が行うこととなっている。近年は、特定国で製造されたネットワーク機器に、開発段階からバックドアと呼ばれる脆弱性が埋め込まれることで、サイバー攻撃に用いられるケースも報告されている。重要設備の審査等を行うことで、こうしたリスクを低減させることが目的である。

技術情報の保護も経済安全保障上の重要な論点

2 点目に、民間企業が有する技術情報をサイバー攻撃によって海外企業に窃取されないように保護することも大きな課題である。日本政府の経済安全保障政策は、主に「自律性の確保」および「不可欠性の確保」の 2 点を目的としている。これらの概念の詳細な解説は他の文献に譲るが、このうち「不可欠性の確保」とは、日本がグローバルサプライチェーン上のチョークポイントになることで、日本が他国にとって不可欠な国となることを目指すものである。「不可欠性の確保」には、他国対比で優れた先端技術を保有することを通じ、日本が競争力を確保することが重要である。公的機関や民間企業が有する技術情報をサイバー攻撃から守ることは、経済安全保障の観点で重要な取り組みである。

民間企業が防衛関連技術を保有する事例も増加

また近年は、軍用品と民生品の双方に活用可能なデュアルユース品の増加に伴い、防衛装備品に使われる技術情報を民間企業が保有する例も従来以上に増加しており、政府に対するサイバー攻撃に対処するだけではこれらの技術情報を守れなくなっている。実際に 2016 年～2017 年にかけて、海外のハッカー集団が、宇宙航空研究開発機構（JAXA）をはじめとする国内 200 以上の防衛・宇宙関連企業にサイバー攻撃を実行した事例がある。本事例の背景には国家および軍の関与があった可能性が高いことが警察庁により指摘[2]されており、民間企業も国家主体によるサイバー攻撃の標的になる可能性を示している。

サイバーセキュリティは個々の企業だけの問題ではない

先端技術やデュアルユース技術を有する日本企業は、防衛産業以外にも半導体産業や素材産業など枚挙に暇がない。これらの企業のセキュリティレベルを向上させて技術情報を保護することは、単に個々の企業のリスクマネジメントの問題のみならず、安全保障の観点でも要請されるところである。

サイバーセキュリティは国家安全保障と繋がっている

ここまで見てきた通り、国家安全保障と産業界のサイバーセキュリティは密接に繋がっており、企業のセキュリティレベルを向上させることが、サイバー安全保障ひいては国家安全保障の確立に寄与する。【図表 1】に記載の通り、サイバー安全保障の中には政府や自衛隊のサイバーセキュリティも含まれるが、本稿では民間産業界のサイバーセキュリティにフォーカスを当て、課題と打ち手を論じる。

3. サプライチェーン攻撃の脅威

2024 年はサイバー攻撃リスクの社会的認知が大きく高まった

2024 年 6 月に発生した出版大手 KADOKAWA グループへのランサムウェア攻撃は、ニコニコ動画をはじめ複数のサービスに大規模な障害を生じさせた。当該サービスの利用者数の多さや知名度の高さから、日本社会にサイバー攻撃のリスクを改めて知らしめた事案である。本事案の影響として KADOKAWA グループは、2024 年度決算における 84 億円の減収、調査・復旧費用等による特別損失 36 億円の計上を公表している[3]。

サプライチェーン攻撃の脅威が近年注目される

情報処理推進機構（以下、IPA）は、前年に発生した情報セキュリティ関連事案をもとに、毎年「情報セキュリティ 10 大脅威」を公表している。10 大脅威 2024 の組織部門では、1 位の「ランサムウェアによる被害」に次いで、2 位に「サプライチェーンの弱点を悪用した攻撃」がランクインしている。本項目は、2019 年に 10 大脅威の 4 位に選出されて以降、年々順位を上げ、2023 年からは 2 年連続の 2 位となっている（【図表 2】）。

[2] 警察庁「令和 3 年版警察白書」
[3] 株式会社 KADOKAWA「2025 年 3 月期 通期連結業績見通し および 第 1 四半期決算に関するお知らせ」

【図表 2】情報セキュリティ 10 大脅威 2024（組織部門）

順位	脅威	初選出年
1（1）	ランサムウェアによる被害	2016年
2（2）	サプライチェーンの弱点を悪用した攻撃	2019年
3（4）	内部不正による情報漏えい等の被害	2016年
4（3）	標的型攻撃による機密情報の窃取	2016年
5（6）	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年
6（9）	不注意による情報漏えい等の被害	2016年
7（8）	脆弱性対策情報の公開に伴う悪用増加	2016年
8（7）	ビジネスメール詐欺による金銭被害	2018年
9（5）	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年
10（10）	犯罪のビジネス化（アンダーグラウンドサービス）	2017年

（注）順位の括弧内は 2023 年版の順位
（出所）IPA「情報セキュリティ 10 大脅威 2024」（https://www.ipa.go.jp/security/10threats/10threats2024.html）より、みずほ銀行産業調査部作成

サプライチェーン攻撃はセキュリティ対策が不十分な企業を狙う

サプライチェーンの弱点を悪用するサイバー攻撃は通称、サプライチェーン攻撃と呼称される。サイバー攻撃の標的企業を直接攻撃するのではなく、標的企業と密接な関係にある子会社や取引先、委託先企業の中で、セキュリティ対策が不十分な企業に攻撃を仕掛け、侵入した企業から標的企業のシステムに侵入する手法である。

日本国内でもサプライチェーン攻撃が発生

2022 年 10 月に発生した大阪急性期・総合医療センターに対するランサムウェア攻撃[4]では、電子カルテを含む情報システムの障害により、救急診療や外来診療、手術などの診療機能に支障が生じ、診療機能の完全復旧までに 73 日を要したほか、診療制限に伴う逸失利益として十数億円が発生した[5]。本事案では、攻撃対象の病院が直接攻撃を受けたわけではなく、病院食を提供していた給食事業者の給食システムに不正アクセスが行われ、給食事業者から窃取された病院サーバーの認証情報を用いて、病院内のサーバーに侵入が行われた。本事案のような医療インフラに対する攻撃は人命に直結するおそれがあり、安全保障上の脅威といえる。

トヨタ自動車は子会社のサイバー攻撃被害により全工場が停止

2022 年 2 月には、愛知県豊田市の自動車部品メーカー・小島プレス工業が、子会社経由でサプライチェーン攻撃を受けた。社外からの受発注に関わるシステムが停止したことにより部品供給が停止し、納品先であったトヨタ自動車の国内全 14 工場の生産が約 1 日停止した。自動車産業のようにサプライチェーン構成社数の多い産業でサプライチェーン攻撃が発生すれば、影響範囲が甚大になることを示しており、製造業におけるサプライチェーン攻撃リスクを世に知らしめた事案である。

4. 大企業にとってもサプライチェーン全体を守る意義は高い

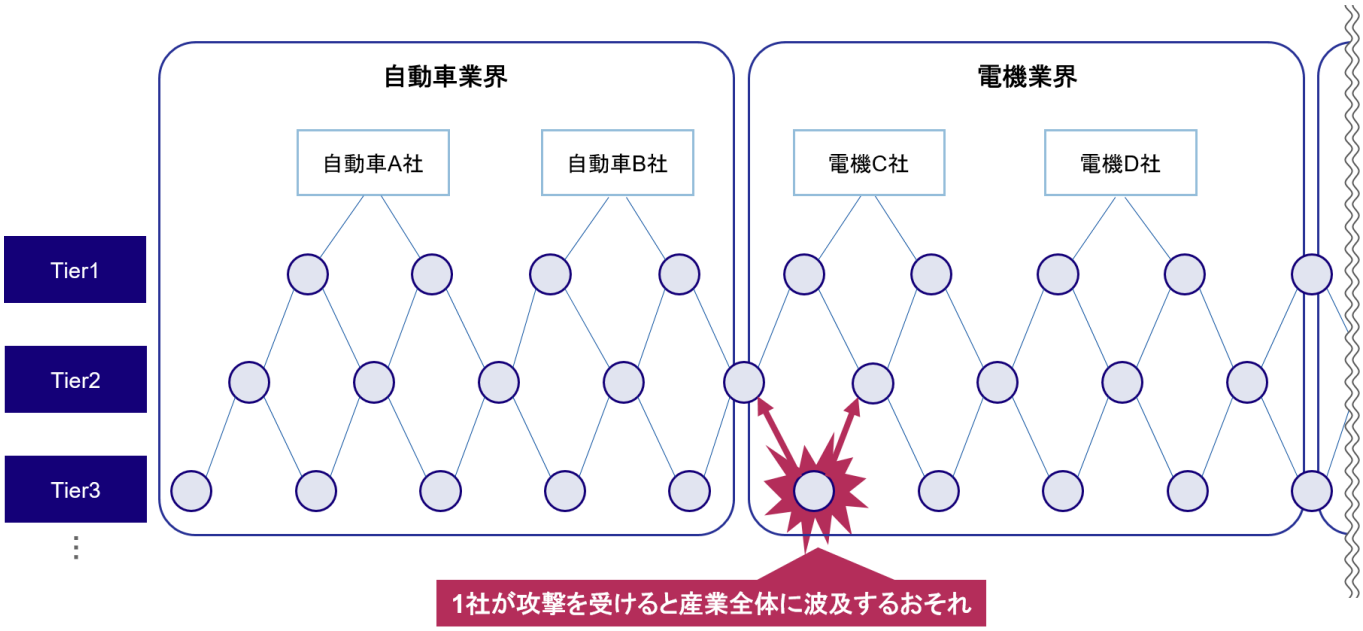
サイバーセキュリティを協調領域と捉えて産業全体で協働

ここまで見てきた通り、サプライチェーン攻撃が活発化している現在、サプライチェーン上の 1 社が攻撃を受けただけで、サプライチェーン全体に甚大な影響が出る可能性がある。前述のトヨタ自動車の事例のように、特にサプライチェーンが密接に絡み合う製造業では、1 件のサイバー攻撃がサプライチェーン全体の生産機能停止に繋がる。また、電力や水道、医療等のインフラ産業で発生すれば、1 件のサイバー攻撃がインフラ機能の停止を通じて社会機能を麻痺させるおそれがある。場合によってはインフラの停止が

[4] ランサムウェアとは、攻撃対象のデータを暗号化し、データ復元の対価として金銭を要求するコンピュータ・ウイルス。本事例ではサプライチェーン攻撃にランサムウェアが使用された。
[5] 大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会「調査報告書」

人命に直結するおそれもあり、安全保障の観点で重大な脅威といえる。こうしたサプライチェーン攻撃のリスクを踏まえ、サイバーセキュリティに感度の高い一部の大企業等だけでセキュリティ対策を進めるのではなく、子会社や委託先、取引先を含むサプライチェーン全体のセキュリティ対策に穴が出ないよう、産業全体のセキュリティレベルを底上げしていくことが重要である（【図表 3】）。

【図表 3】サプライチェーン攻撃のリスク（製造業の例）



（出所）みずほ銀行産業調査部作成

ランサムウェア攻撃の 6 割超が中小企業で発生

サプライチェーン攻撃を含むランサムウェア攻撃は、決して大企業だけが標的になっているわけではない。事実として、2024 年上半期に警察庁に報告されたランサムウェア攻撃被害のうち、6 割超は中小企業で発生している[6]。近年は大企業を中心にセキュリティ対策が進む中、中小企業を介して大企業の内部システムに侵入されるリスクも高まっており、大企業にとっても中小企業を含む取引先を守る意義は高い。また、異なる大企業が同一のサプライヤーから供給を受けていたり、別業界の企業と取引を行っているケースを考えれば、全ての産業のサプライチェーンは繋がっているといえる。業種や企業規模を問わず、サイバーセキュリティを各社の協調領域と捉え、競合関係を乗り越えて、産業全体で協働して対処することが求められる。

中小企業のサイバーセキュリティは産業全体にとって課題

中小企業に比して予算や人材に余力のある大企業では、サイバーセキュリティの専任者や専門部署を設置してセキュリティ対策に取り組む企業も多い。一方、例えば従業員数が 100 名に満たないような中小企業では予算や人材の制約から、セキュリティ対策を行う余力が限定的なケースが大宗である。中小企業のセキュリティ対策を自助努力に任せているだけでは、産業全体のセキュリティレベルの底上げは達成され得ず、サプライチェーンの至る所に弱点が存在することになりかねない。業界団体や大企業等、当事者以外のアクターが積極的に中小企業のセキュリティ対策に関与していくことも求められる。

日本企業は子会社・取引先のセキュリティ対策を把握していない

日本企業はサプライチェーンのセキュリティ対策状況の把握度合いが低いとのデータもある。NRI セキュアテクノロジーズが 2023 年に実施した調査[7]によれば、日本企業では子会社やグループ会社のセキュリティ対策状況を把握している企業は全体の 47.1%であったほか、委託先のセキュリティ対策状況については全体の 35.6%の企業しか把握しておらず、サプライチェーンのサイバーセキュリティを推進する上での課題といえる。

[6] 警察庁サイバー警察局「令和6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」
[7] NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2023」

5. 中小企業のセキュリティ課題

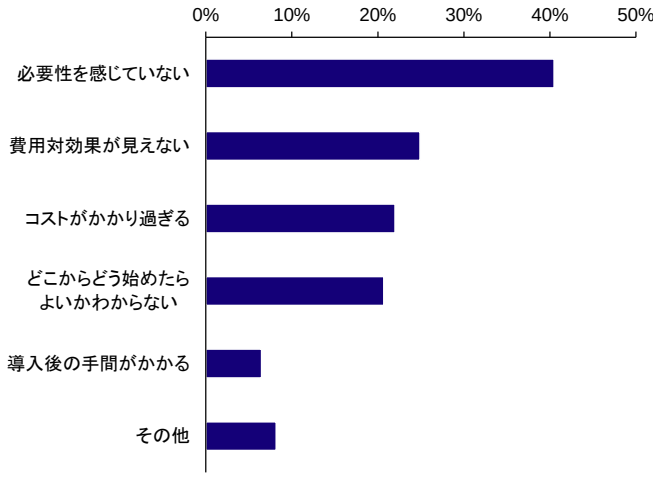
企業側の意識が最初のハードル

中小企業自身がサイバーセキュリティに取り組む制約を取り除くことも重要である。IPAが中小企業を対象に実施した調査によると、中小企業がセキュリティ投資を行わなかった理由として、コストに関する要因などが挙げられた中で、最も回答数の多かった選択肢は「必要性を感じていない」であった(【図表 4】)。「必要性を感じていない」を挙げた社数は全体の 4 割超を占め、中小企業がサイバーセキュリティに取り組む道程で最初の大きな壁となるのが、企業側の意識の問題であることが分かる。

意識の高い企業にとっては人材不足が大きな課題

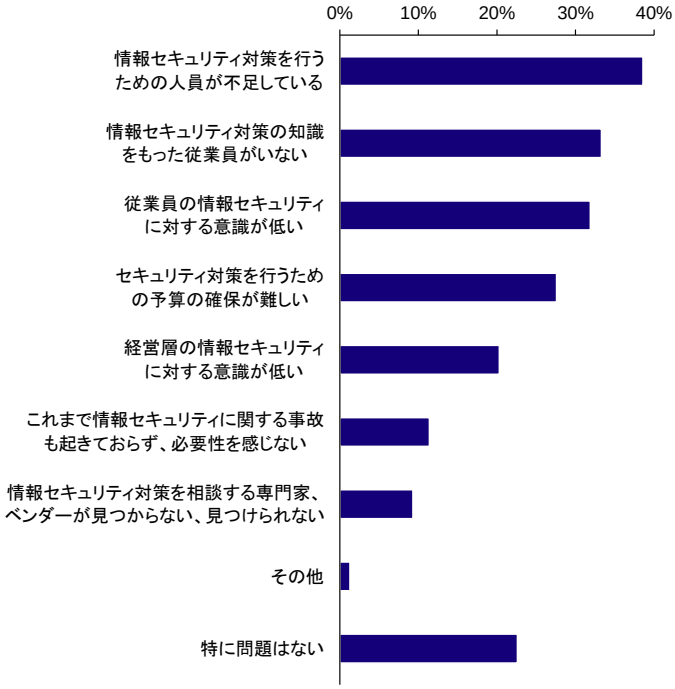
次に別の調査として、IPA が SECURITY ACTION[8]宣言事業者のみを対象に実施した調査結果をみてみると、人員不足を挙げる企業が全体の 4 割近くを占め、最多の得票となっている(【図表 5】)。同宣言事業者を対象とする本調査は、既にサイバーセキュリティに対する意識が一定程度あり、セキュリティ施策に取り組み始めた後の企業が対象のアンケートといえる。これらの調査結果を総合的に踏まえると、一般的な中小企業がサイバーセキュリティに取り組むための最初の課題は意識の低さや予算の制約が中心であり、既にセキュリティ対策に取り組み始めた中小企業が対策を高度化するための課題として、人材不足等の課題が深刻化してくるのではないかと考えられる。

【図表 4】中小企業が情報セキュリティ対策投資を行わなかった理由



(注)複数回答可
(出所)IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」より、みずほ銀行産業調査部作成

【図表 5】SECURITY ACTION 宣言事業者が情報セキュリティ対策を進める上での問題点



(注)複数回答可
(出所)IPA「2023 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」より、みずほ銀行産業調査部作成

ガイドラインの多さが、企業のとるべき施策を分かりづらくしている

中小企業全体を対象とした【図表 4】の調査結果を更に見てみると、「どこからどう始めたらよいかわからない」との選択肢にも 20%超の回答が集まっている。企業がサイバーセキュリティ施策を検討する上では、まず公的機関の刊行物を参照することが有用である。例えば国際的な基準としては ISO27001 や NIST SP800-171 等が有名である一方、日本においては、経済産業省と IPA が作成しているサイバーセキュリティ経営ガイドラインをはじめ、対象業種や企業規模に応じて、関連官庁が様々なガイドラインを公表している。国内ガイドラインの発行元は IPA や総務省のほか、厚生労働省や防衛省、金融庁等、

[8] IPA が定義するセキュリティ対策を実施した中小企業が、セキュリティに取り組んでいることを対外的に宣言する制度

各業種の所管省庁が業種別にガイドラインを発行しており、国内公的機関が発行したガイドラインの数は、筆者が確認した限りでも 20 を超える(【図表 6】)。ガイドラインが増えれば増えるほど、自社に必要なガイドラインを見落とすおそれがあるほか、自社に必要な全てのガイドラインを参照したとしても、どこから始めればよいかの判断が難しい。また、サプライヤーとして複数の業界に製品を納入している企業にとっては、複数の取引先から異なる業種ガイドラインへの準拠を求められるケースもあり対応負担が大きい。企業がどのガイドラインを参照し、何から手を付ければよいのか、政府として分かりやすく明確化することが求められる。

【図表 6】国内公的機関より発行されているガイドライン類の例

発行元	ガイドライン類の名称
経済産業省、IPA	サイバーセキュリティ経営ガイドライン
経済産業省	IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド
IPA	中小企業の情報セキュリティ対策ガイドライン
IPA	組込みシステムのセキュリティへの取組みガイド
IPA	組織における内部不正防止ガイドライン
IPA	ECサイト構築・運用セキュリティガイドライン
IPA	脆弱性対処に向けた製品開発者向けガイド
IPA	自動車の情報セキュリティへの取組みガイド
IPA、JPCERTコーディネーションセンター、 電子情報技術産業協会、ソフトウェア協会、 情報サービス産業協会、日本ネットワークセキュリティ協会	情報セキュリティ早期警戒パートナーシップガイドライン
産業サイバーセキュリティ研究会	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
クレジット取引セキュリティ対策協議会	クレジットカード・セキュリティガイドライン
総務省	テレワークセキュリティガイドライン
総務省	公衆Wi-Fi提供者向け セキュリティ対策の手引き
総務省	5G セキュリティガイドライン
総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン
総務省	スマートシティセキュリティガイドライン
総務省	クラウドサービス提供における情報セキュリティ対策ガイドライン
NICT(注)	セキュリティ導入ガイド
IoT推進コンソーシアム、総務省、経済産業省	IoTセキュリティガイドライン
厚生労働省	医療情報システムの安全管理に関するガイドライン
国土交通省	物流分野(貨物自動車運送)における情報セキュリティ確保に係る安全ガイドライン
国土交通省	物流分野(倉庫)における情報セキュリティ確保に係る安全ガイドライン
国土交通省	情報セキュリティガイドライン
文部科学省	教育情報セキュリティポリシーに関するガイドライン
防衛装備庁	防衛産業サイバーセキュリティ基準
金融庁	金融分野におけるサイバーセキュリティに関するガイドライン

(注)NICT:情報通信研究機構
(出所)各機関ウェブサイトより、みずほ銀行産業調査部作成

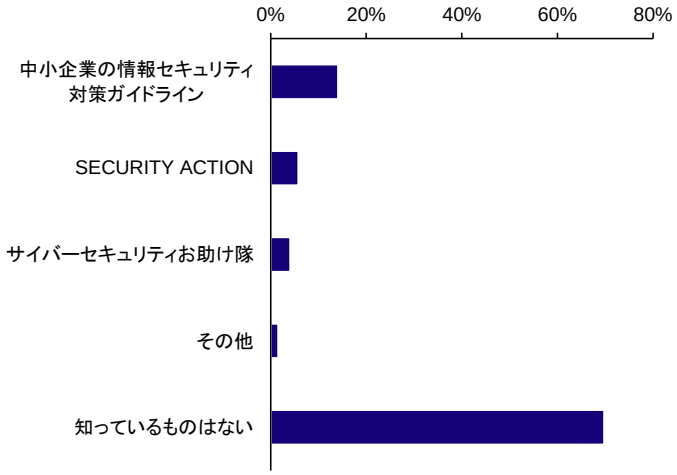
政府による予算面の支援制度は認知度の低さが課題

IPA の調査で課題に挙がった予算面の制約については、政府による支援制度が用意されている。例えば IPA が推進するサイバーセキュリティお助け隊制度は、中小企業が必要とするセキュリティ関連サービスをワンパッケージにまとめ、民間事業者から安価で提供されるサービスである。また IT 導入補助金を利用すれば、お助け隊サービスの利用料の一部が補助される。しかし、中小企業の間ではお助け隊サービスをはじめとする各種支援制度の認知度は低く、更なる普及や浸透が求められる(【図表 7】)。

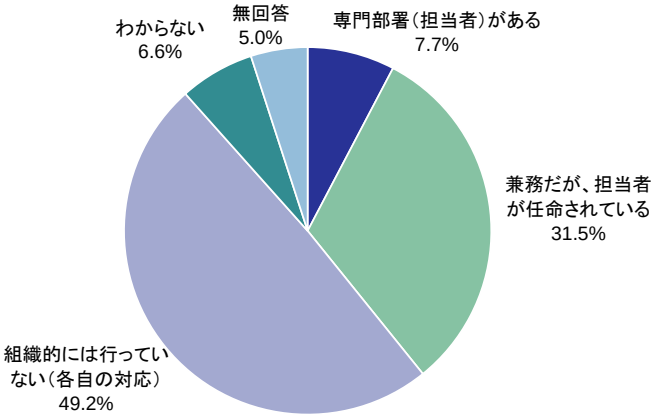
セキュリティ担当を任命していない中小企業が半数

人材面では、中小企業に専任のセキュリティ担当者を置く余力がないことが課題である。実際に中小企業のうちサイバーセキュリティの専任担当や専門部署を設置している企業は全体の 7.7%にとどまり、担当者を任命していない企業が約半数存在する(【図表 8】)。加えて、セキュリティ施策の推進には専門的な知見が求められるため、企業として専門人材を確保することも大きな課題といえよう。

【図表 7】IPA が実施する活動の認知度



【図表 8】中小企業の情報セキュリティの組織体制



（注）左図は複数回答可
（出所）両図とも、IPA「2021 年度　中小企業における情報セキュリティ対策に関する実態調査」より、みずほ銀行産業調査部作成

セキュリティ人材の増加は当面見込めず、既存人材の効率的な活用が重要

企業がサイバーセキュリティの専門人材を確保する上で社内の予算の制約をクリアする必要があることは前提として、仮に予算の制約をクリアし採用活動を行おうとしても、日本社会全体としてセキュリティ人材は著しく不足しており、人材確保は容易でない。国際的なサイバーセキュリティ団体である ISC2[9]の試算によると、日本ではセキュリティ人材の需要に対して供給が 11 万人不足しており、現在の人材数に対して日本全体で約 3 割の増員が求められている[10]。しかし、短期的に日本社会のセキュリティ人材を 11 万人も純増させることは困難である。昨今は少子化に伴い物流業や宿泊業等、あらゆる産業で人手不足が深刻化しており、限りある労働力人口から、セキュリティ分野に短期間に多くの人材を配分することは不可能である。例えば四年制大学におけるセキュリティ学科の設置数を増やすなど、セキュリティ人材を増やすための中長期的な取り組みが重要であることは論を待たないが、企業としてはセキュリティ人材の供給が当面増えない前提に立ち、既存人材を如何に効率的に活用していくかとの発想で、対応を検討していくことが重要である。

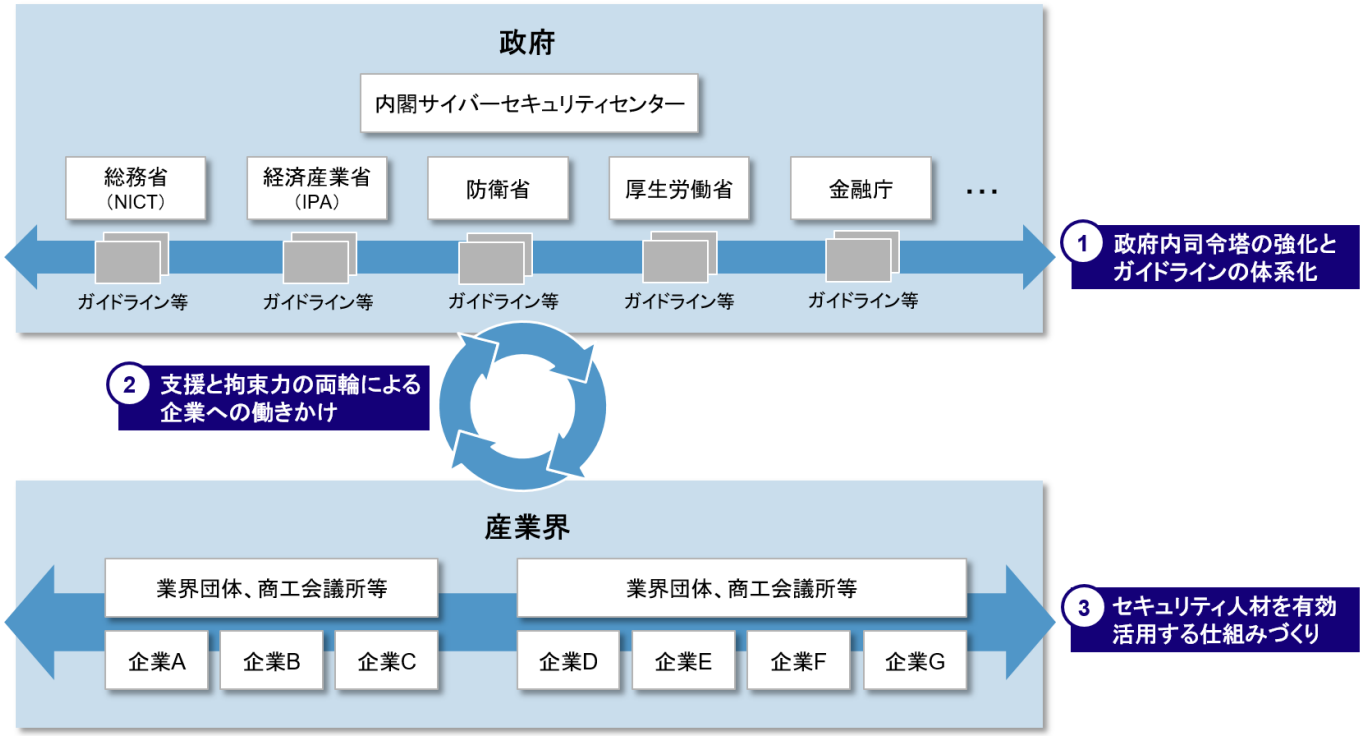
6. 官民に求められるサプライチェーンセキュリティ施策

産業界のサイバーセキュリティを官民一体で推進

5 章において、中小企業におけるセキュリティ推進のボトルネックとして、企業側の意識の問題のほか、予算や人材面にも課題があることを述べた。また政府の課題としては、ガイドラインの煩雑性や、各種支援制度の認知度の低さを挙げた。これらの課題に対して取り得る打ち手として、既に様々な有識者が各所で提示している数多くの施策があるが、本稿では、政府（官）と企業（民）それぞれの役割を踏まえ、官民に求められる施策として 3 点を提示するとともに、社会のセキュリティ推進のありたき姿を示す（【図表 9】）。

[9] ISC2：International Information System Security Certification Consortium
[10] ISC2, *CYBERSECURITY WORKFORCE STUDY 2023*

【図表 9】官民によるサイバーセキュリティ推進のありたき姿



（出所）みずほ銀行産業調査部作成

【提言①】政府内司令塔の強化とガイドラインの体系化

まず政府に求められる施策の 1 点目として、ガイドラインの体系化を挙げる。5 章に記載した通り、日本では IPA や総務省をはじめ、複数の公的機関から 20 を超えるガイドラインが公表されているなど、ガイドラインの煩雑性が課題である。業種ごとの事業特性に応じて求められる対策は異なる部分も多く、ガイドラインを完全に一元化することは不可能である。しかし、複数のガイドラインの位置づけや関係性を一覧で明確化し、企業がどれを参照すべきなのか簡単に判断できるよう、省庁横断でガイドラインを体系化することや、企業が異業種の企業のセキュリティ対策水準を評価しやすいよう、業種横断で共通の評価尺度を設けることも有用である。

NISC の発展的改組も早期に求められる

これらの施策を行うために、政府内の省庁間調整を担う司令塔機能を強化する必要もある。2022 年 12 月に閣議決定された国家安全保障戦略では、能動的サイバー防御の実現を目的に「内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する」ことが明記された。能動的サイバー防御に限らず、あらゆるサイバー安全保障政策を推進する上で、司令塔の下での省庁間連携は不可欠である。

国際規格との整合性確保も重要

またグローバルでは、ISO27001 や NIST Cyber Security Framework 等の規格が多く参照されている。例えば米国国防総省は調達の入札要件として NIST SP800-171 への準拠をサプライヤーに求めるなど、日本企業として国際規格への準拠が必要となるケースもある。国内のガイドライン間で煩雑性を解消するだけでなく、国際規格との互換性を確保したり関係性を明示することで、企業の対応コストを最小化していくことも重要である。また国際社会では各分野で標準化を巡る主導権争いがある中、日本のセキュリティ基準を国際規格としていくようなルール形成の動きをしていくことが出来れば理想的である。

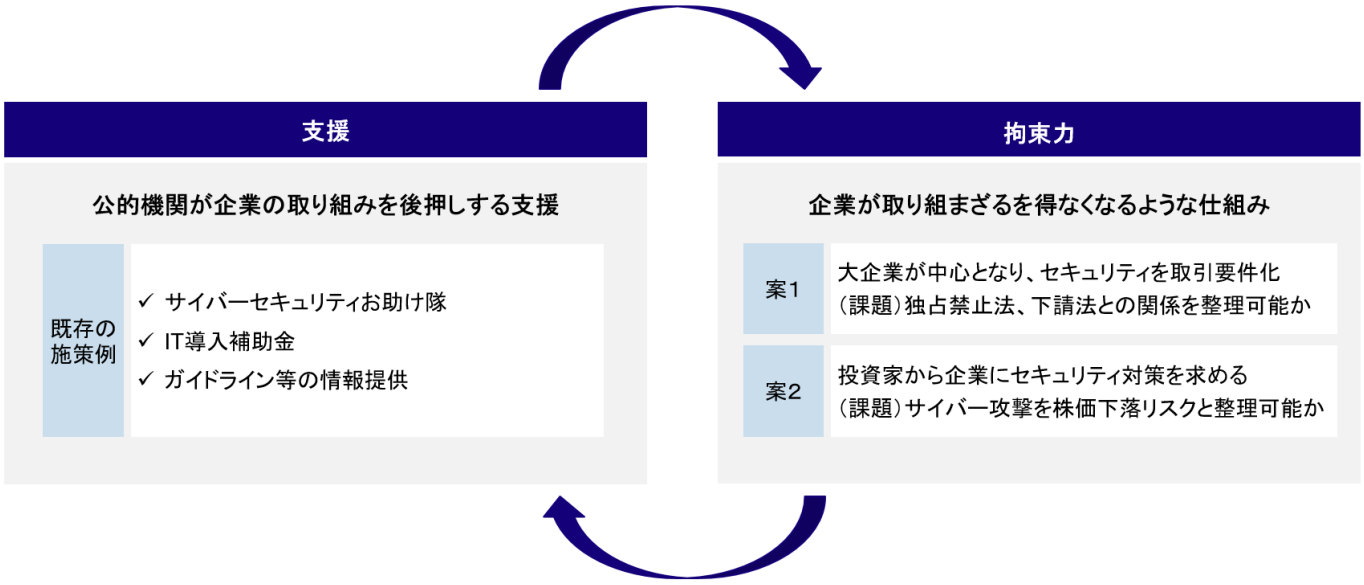
【提言②】支援と拘束力の両輪による企業への働きかけ

サプライチェーン攻撃に対してサプライチェーン全体のセキュリティ向上を実現するためには、企業規模を問わずあらゆる企業のセキュリティレベルを底上げすることが重要である。5 章で述べた通り、中小企業を中心にセキュリティ推進に対する意識面に課題があるが、JCIC[11]によれば、商工会議所の関係者がセキュリティ関連の公的支援の周知のために中小企業経営者の元に足を運んでも危機感が伝わらず、無駄足に終わることが多い

[11] JCIC：日本サイバーセキュリティ・イノベーション委員会

という[12]。企業の意識醸成に向けた関係者の地道な努力は重要であるが、企業の意識や自主性に任せているだけでは、サプライチェーンのセキュリティ確保には非常に長い時間を要することも事実である。冒頭に述べたように、サイバーセキュリティは個々の企業のリスクマネジメントの問題のみならず、安全保障という公益に基づく要請でもある。各社にセキュリティ対策を委ねるのではなく、企業がサイバーセキュリティに取り組まざるを得なくなるような社会的な仕組みを作り、支援と拘束力の両輪で、産業界全体をセキュリティ対策に巻き込んでいく必要がある(【図表 10】)。

【図表 10】支援と拘束力の両輪による企業への働きかけ



「支援」と「拘束力」の両輪で、産業界全体をセキュリティ対策に巻き込んでいく仕組みづくり

(出所)みずほ銀行産業調査部作成

大企業によるサイバーセキュリティの取引要件化が有効

セキュリティレベルの低い企業から他社に被害が拡大するというサプライチェーン攻撃の性質に鑑み、企業のセキュリティ対策の不作為は負の外部性を有すると整理出来る。一般に外部不経済を内部化する手法としては、法律に基づき規制をかける直接規制のほか、補助金や課税などの経済的手段がある。政府が直接規制をかける場合、どの程度のセキュリティ対策を一律で義務化すべきかを定める必要があるが、必要最低限とされるセキュリティ対策の水準感については社会的なコンセンサスをとることが難しい。さらに、サイバーセキュリティの分野は技術の進歩により求められる対策も日進月歩であり、規制が技術の進歩に追い付かないおそれもある。こうした前提を踏まえ、セキュリティ対策に直接規制を用いることには慎重であるべきだと考えられ、極力民間企業同士で実質的な拘束力をかけていくことが望ましい。例えば、サイバーセキュリティに対して感度の高い大企業が自社のリスク管理の一環として、取引先のセキュリティ対策を自社との取引要件に定めることは一案である。

自動車産業は産業全体のセキュリティレベル向上に取り組む

自動車産業では、業界団体である日本自動車工業会と日本自動車部品工業会が「自動車産業サイバーセキュリティガイドライン」を作成し、加盟企業に対して自己評価の実施と提出を要請している[13]。自己評価依頼を受けた企業が、自社のサプライヤーにも自己評価を展開することを通じて、業界全体としてセキュリティレベルを向上させるべく取り組んでいる。先ずはこうした動きを様々な産業に波及させていき、企業が一定のセキュリティ対策に取り組むことを日本産業全体のデファクトスタンダードとしていくことが望ましい。

12 日本サイバーセキュリティ・イノベーション委員会(JCIC)「[コラム]中小企業のサイバーセキュリティ対策 ～切れ目ないサポート制度が必要～」
13 日本自動車工業会、日本自動車部品工業会「2024 年度 経営層向け説明会 「自動車産業サイバーセキュリティガイドライン」自己評価の実施・展開のお願い」

防衛産業では防衛装備庁がセキュリティ対策を調達要件に

防衛産業では 2023 年 4 月以降、防衛装備庁が防衛関連の調達契約を対象に、サプライヤーに防衛産業サイバーセキュリティ基準への準拠を求めている。防衛産業は安全保障上の重要性が最も高い業種であるが、今やサイバー安全保障は防衛産業に限らずあらゆる業種で対応が求められる。各業界の大企業や業界団体等が中心となり、自動車産業や防衛産業の事例を参考に、業界全体を巻き込んだ取り組みを加速すべきである。

法令の兼ね合いも整理すべき論点

仮に民間企業が取引先との取引要件にセキュリティ対策を定める場合、当該要件が独占禁止法における優越的地位の濫用に抵触する懸念や、下請法上の問題がないかはクリアすべき論点である。これらの法的課題を背景に、企業間でのセキュリティ対策の要請は現状「お願い」ベースにとどまっているが、産業界のセキュリティ対策を一層加速するためには、実質的な拘束力を伴う形まで踏み込むことが必要である。政府としては、企業がセキュリティを取引要件化する場合の法令上の論点を整理し、企業の取り組みを後押しする形で指針を公表することが望まれる。

金融市場からも企業にセキュリティ対策を求めていく

脱炭素や人権などサステナビリティの分野では、投資家から企業に対する圧力が年々強まっており、企業も呼応する形で、サプライチェーンを巻き込み対応を進める構図が出来上がっている。仮に上場企業がサイバー攻撃を受けて事業継続性に影響が及べば、企業収益ひいては企業価値にも影響するおそれがあることを踏まえれば、サイバー脆弱性は企業活動の明白なリスクと捉えられるべきである。JCIC は、不正アクセス等の適時開示を行った企業において、基準日から 50 日後の株価が平均 6.3%下落することを指摘している[14]。投資家から発行体にセキュリティ対策を促していくことは、投資家と企業の双方にとり有益な取り組みである。

【提言③】セキュリティ人材を有効活用する仕組みづくり

最後に、セキュリティ人材の不足に対して産業界が一体となり取り組むことも重要である。前述の通り、短期的にセキュリティ人材の供給が急増することは見込めないため、産業界としては、現在の人材供給数が当面大きく変わらないことを前提に、効率的な人材活用を推進することが求められる。

多数の中小企業が共同で専門人材を活用する

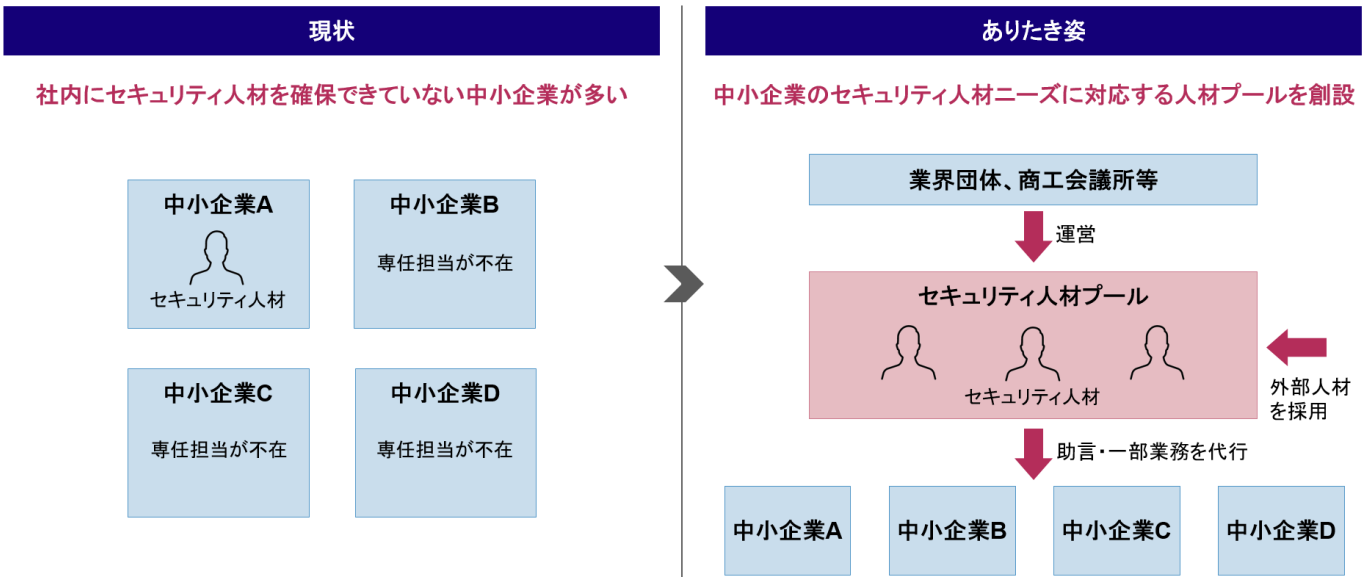
大企業ではサイバーセキュリティの専門部署や専任担当を設置する事例が増えているが、中小企業が同様の体制を作ることは難しい。5 章で示した通り、中小企業においてセキュリティの専任担当等を設置している企業は全体の 7.7%にとどまり、殆どの中小企業では、総務や IT 等、別の業務とセキュリティ業務を同一担当者が兼務していることが大宗である。他方で、特に従業員数が数名～十数名の小規模事業者をはじめ、中小企業がセキュリティの専任担当を 1 社に 1 名配置することは、中小企業の企業規模に鑑み現実的でない。このような中小企業の実情に鑑み、中小企業が自社で専門人材を雇用しなくても、低コストで専門知見にアクセス出来るような仕組みが求められる。また例えば、インシデント発生後の原因調査や報道機関対応、再発防止策の策定等を専門とするような人材が、インシデントの発生していない企業に常駐する必要性は少ない。特にこうした専門人材は 1 社で囲い込むよりも、多数の中小企業がアクセス出来る方が、人材活用の効率性は高い。

業界団体や商工会議所が「セキュリティ人材プール」を立ち上げる

セキュリティ業務のこうした特性を踏まえ、多数の中小企業が共同でセキュリティ人材を効率的に活用できるよう、業界団体や地域の商工会議所等が中心となり、セキュリティの人材プールを立ち上げることを提案したい（【図表 11】）。セキュリティ人材プールに所属する専門家が多数の中小企業に助言を行うことで、中小企業は自社単独で人材を確保するよりも、効率的にセキュリティ対策に取り組むことが可能になる。

[14] 日本サイバーセキュリティ・イノベーション委員会（JCIC）「社内のセキュリティリソースは「0.5%」以上を確保せよ ～DX with Security を実現するためのサイバーリスク数値化モデル～」

【図表 11】中小企業に対する助言や業務代行を行う「セキュリティ人材プール」構想



（出所）みずほ銀行産業調査部作成

セキュリティ業務の集約により効率化を図る

さらに、セキュリティ人材プールが助言を行うだけでなく、中小企業のセキュリティ業務の一部を代行することも一案である。企業のセキュリティ業務の全てを代行することは現実的ではないが、企業にとって委託しやすい業務からセキュリティ人材プールに委託することが出来れば、中小企業のセキュリティ業務を一層効率化できる。例えば、企業内のセキュリティガイドラインを策定する業務は、あらゆる企業に共通の業務であり、多数の企業で重複して同じ業務を行っている。特に同一業種の企業であれば、各社で策定する企業内ガイドラインも類似の内容になる可能性が高く、各社の業務をセキュリティ人材プールが代行し集約することで、業界全体のセキュリティ業務の効率化を図ることが出来る。企業内ガイドラインの策定に限らず、各社で重複して実施しているセキュリティ業務があれば、セキュリティ人材プールを受け皿として業務を委託し、集約していくべきである。

IPA は訪問支援の実証実験を実施

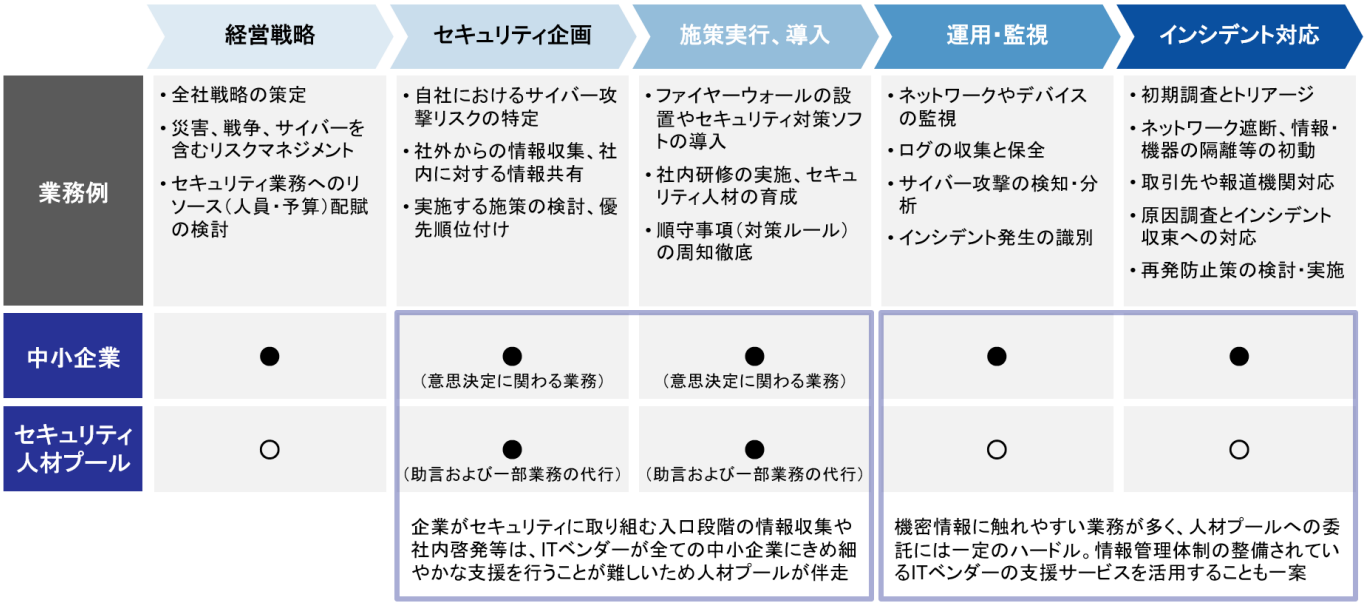
IPA は全国 3 カ所の商工会議所[15]と連携し、中小企業のセキュリティ施策を支援するための個別相談会のほか、専門家による訪問支援の実証実験を実施している[16]。今後はこうした取り組みを全国に拡大し、発展させていくことが望まれる。

セキュリティ業務の上流工程でセキュリティ人材プールを活用

セキュリティ業務の中でも、社外からの情報収集や社内研修の実施等の企画業務から、システムを 24 時間監視し不正アクセスを検知する SOC[17]や、インシデント発生後の復旧対応を担う CSIRT[18]等の下流にあたる業務まで、様々な業務が存在する（【図表 12】）。IT ベンダーはシステム導入支援のほか SOC や CSIRT 等の支援サービスを提供している一方、上流の企画業務に関しては、IT ベンダー側の収益性等の観点で全ての中小企業にきめ細やかな支援を行うことが難しい。セキュリティに取り組み始める中小企業は、上流の企画段階で「どこからどう始めたらよいかわからない」との悩みを抱えるケースも多いため、セキュリティ人材プールが企画業務に関する助言や業務の代行を行うことは有効だろう。他方、下流の運用・監視～インシデント対応にあたる業務は、前述のとおり IT ベンダーが各種支援サービスを提供していることに加え、企業の機密情報に触れやすい業務も多い。委託先にも相応の情報管理体制が求められ、業界団体の運営するセキュリティ人材プールへの委託には一定のハードルがある。係る状況を踏まえ、例えば上流の企画業務を中心にセキュリティ人材プールの支援を受けながら、運用・監視～インシデント対応業務は IT ベンダーのサービスを利用するような使い分けは一案である。尚、業務委託を通じて効率的にセキュリティ施策を推進しながら、各業務における意思決定には企業側が確り関与し、委託先への丸投げにならないようにすることも大切である。

15 大阪・名古屋・さいたまの 3 カ所
16 情報処理推進機構「「令和 6 年度セキュリティ人材活用促進実証に係る業務」に関する一般競争入札（総合評価落札方式） 入札説明書」
17 SOC：Security Operation Center
18 CSIRT：Computer Security Incident Response Team

【図表 12】セキュリティ人材プールの支援領域（一例）



（注 1）●：業務を主体的に推進する役割、○：業務を情報提供等によりサポートする役割
（注 2）本図で示す支援領域は一例であり、ユーザーとなる企業の規模や事業内容等に応じて変わり得る
（出所）みずほ銀行産業調査部作成

7. おわりに

サイバー安全保障は国家の喫緊の課題

本稿で見てきた通り、サイバーセキュリティは社会全体で取り組む必要がある半面、その必要性に対する社会的理解の浸透が道半ばであるが故に、社会一体でのセキュリティ推進は容易でない。しかし、国際情勢が目まぐるしく変化し、技術革新が急速に進む中、サイバー安全保障の確立は国家の喫緊の課題であり、早急な対応が求められる。サイバー安全保障の確立は、政府単独では達成し得ない取り組みであり、民間企業も含めて官民一体で取り組まなければ、日本の安定的な発展は見込めず、その影響は将来の企業活動にも及ぶ。

安全保障の確立が日本の持続的な発展に繋がる

企業がリスクマネジメントの観点でサイバーセキュリティに取り組むことは勿論であるが、安全保障という公益に貢献することが、将来の事業環境の予見可能性をも高めるとの視点に立ち、企業がサイバーセキュリティの取り組みを加速させることを期待したい。個々の企業の取り組みが結実し、産業全体のセキュリティ向上と安全保障の確立を通じ、日本の安定的かつ持続的な発展に繋がるよう、筆者も微力ながら貢献してまいりたい。

みずほ銀行産業調査部
総括チーム　武藤　祐貴
ird.info@mizuho-bk.co.jp

【主要参考文献】

1. 官公庁資料
   - ○ 国家安全保障会議「国家安全保障戦略」（https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf）（2022 年 12 月）
   - ○ 経済産業省「経済安全保障に関する産業・技術基盤強化アクションプラン改訂版」（https://www.meti.go.jp/policy/economy/economic_security/240515actionplan.pdf）（2024 年 5 月）
2. 書籍
   - ○ 国際文化会館地経学研究所「経済安全保障とは何か」東洋経済新報社（2024 年 5 月）
   - ○ 玉井克哉、兼原信克「経済安全保障の深層 課題克服の 12 の論点」日本経済新聞出版（2023 年 12 月）
   - ○ 笹川平和財団新領域研究会「新領域安全保障 サイバー・宇宙・無人兵器をめぐる法的課題」ウェッジ（2024 年 1 月）
   - ○ 船橋洋一「国民安全保障国家論 世界は自ら助くる者を助く」文藝春秋（2022 年 6 月）
   - ○ 兼原信克「日本人のための安全保障入門」日本経済新聞出版（2023 年 11 月）
   - ○ 喬良、王湘穂「超限戦 21 世紀の「新しい戦争」」KADOKAWA（2020 年 1 月）
   - ○ 福田敏博「図解入門 よくわかる 最新 サイバーセキュリティ対策の基本」秀和システム（2023 年 2 月）
   - ○ 淵上真一「経営層のためのサイバーセキュリティ実践入門 生成 AI、DX、コネクティビティ時代を勝ち抜くための必須スキル」プレジデント社（2024 年 2 月）
   - ○ 岩佐晃也、酒井麻里子「先読み！サイバーセキュリティ 生成 AI 時代の新たなビジネスリスク」インプレス（2024 年 4 月）
3. 記事・レポート
   - ○ 日本サイバーセキュリティ・イノベーション委員会（JCIC）「[コラム]中小企業のサイバーセキュリティ対策 ～切れ目ないサポート制度が必要～」（https://www.j-cic.com/column/SMEs-Cybersecurity.html）（2022 年 9 月）
   - ○ 日本サイバーセキュリティ・イノベーション委員会（JCIC）「社内のセキュリティリソースは「0.5%」以上を確保せよ ～DX with Security を実現するためのサイバーリスク数値化モデル～」（https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf）（2022 年 3 月）
   - ○ NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2023」（2023 年）

アンケートに
ご協力をお願いします

Mizuho Short Industry Focus／234

編集／発行　みずほ銀行産業調査部　　東京都千代田区丸の内 1-3-3　ird.info@mizuho-bk.co.jp