サイバーセキュリティ経営における取締役の責務

株式会社サイリーグホールディングス 取締役・情報セキュリティ大学院大学 客員研究員　大越いづみ

相次ぐ「サイバーセキュリティ経営」宣言

近年の地政学リスクやコロナ禍により、グローバルサプライチェーンを構築した企業は調達リスクに直面した。一方、情報システムのネットワーク化が進む中、サプライチェーンの脆弱性を狙うサイバー攻撃が増加し、セキュリティリスクが高まっている。2022年以降、米国立標準技術研究所（NIST）や全米取締役協会、日本経済団体連合会、経済産業省は相次いで「サイバーセキュリティ経営」のガイドラインや宣言を発出したが、これらは、取締役や経営層のリーダーシップや関与の不足を示唆するものである。本稿ではサプライチェーン強靭化のための「サイバーセキュリティ経営」における取締役の役割について論考する。

サプライチェーン強靭化戦略としての「多元化」

日本企業はグローバルにサプライチェーンを構築し、特に中国を中心に現地調達比率を高めてきた。しかし、地政学リスクや経済安全保障上のリスクの高まりにより、サプライチェーン強靭化は国家戦略となった。日本企業は中国への高い依存度がリスクとされ、さらにコロナ禍によるサプライチェーンの混乱により、調達先の多元化を通じた強靭化が喫緊の経営課題となった。これは経済合理性を追求してきた従来の戦略からの転換であるが、調達安定化の点から有効性は確認されている。また、コスト増を「保険」と捉える考え方もある。

一方､サイバーセキュリティ経営の観点から、多元化はサイバー攻撃の対象となる企業や拠点が増加することを意味する。サイバーセキュリティの対策が十分ではない国や地域に拡張する場合、リスクが一段と高まることになる。従って、サプライチェーン強靭化戦略では、経営レベルにおける、横断的・多角的なリスク評価に基づく意思決定を伴うことが必要となる。しかし、調査事例や先行研究は少なく、企業におけるリスク認識と取り組みの実態把握は難しい。

日本企業のリスク認識と取り組みの状況

このような課題認識から、日本企業の多元化戦略におけるリスク認識と取り組み状況を把握するために、売上規模が大きく、取引先数が多い電気機器産業の売上上位10社（2022年度）を抽出し、各社の公開情報を活用して､「マテリアリティ（経営課題)」「事業上のリスク認識」「対策としての多元化」に関する記載内容、「取引先への要請事項」の調査を行い、以下の結果を得た。

・マテリアリティおよび事業上のリスクとして「サプライチェーン」と「サイバーセキュリティ」の認識

サプライチェーン強靭化とサイバーセキュリティについて、9社がマテリアリティか事業上のリスクとして取り上げている。自社にとってサプライチェーンリスクをサイバーセキュリティよりも重要度が高いと評価する企業もある。

・サプライチェーン強靭化とサイバーセキュリティ対策の統合的な検討

この2つの項目については、いずれの企業においてもそれぞれを個別の課題として扱っている。また、サプライチェーンの多元化に言及した7社は「多元化に伴うリスク」に関する記述がなく、統合的なリスク評価が不十分であることを示唆している。

・サプライチェーンを構成する調達先・取引先に示す調達とサイバーセキュリティガイドライン

サプライチェーンに関して各社は「調達ガイドライン／方針」等を策定し情報開示しているが、サイバーセキュリティに関するガイドラインの開示は5社に留まっている。情報開示がない企業は、サイバーセキュリティ項目を含まない国際標準の行動規範「Responsible Business Alliance」をガイドラインとして採用していることが判明した。

サイバーセキュリティ経営実現のために取締役が果たすべき役割

取締役の責務としてサイバーセキュリティ経営を推進するためには、自社の取り組みの現状を踏まえた上で、経営が実行可能な項目に絞り込んで指示・監督を行い、着実に実効性を高めていくことが求められる。以下では、3つの重要な論点を考察する。

①リスク評価の適切性の注視

経営幹部および事業部門は調達の安定化を優先する傾向があり、調達の目途がつけばサプライチェーンリスクの重要度評価を下げる可能性がある。取締役はリスク評価や対策の検討の際に、最高情報セキュリティ責任者（CISO）の関与や情報技術（IT）・セキュリティ専門部門を組み込んだ横断的・統合的な体制で臨むよう指示し、適切性を監督することが重要である。

「サイバーセキュリティ統括室」や「経済安全保障統括室」を設置し、インテリジェンス機能強化、全社一元的・横断的なリスク対応を行う企業もある。また、取締役会あるいは経営会議直轄の専門委員会設置も体制強化の選択肢として考慮に入れることが大切である。

②ガイドライン採択理由の確認

サプライチェーン強靭化対策として、調達先に対するガイドラインの遵守が強化されるが、その際に国内外で策定された標準ガイドラインを採択することがある。これらは自社の規定や規範等を決める際の参考であり、取締役は、ガイドラインの採択理由、自社との適合性、項目の過不足について、確認を指示、監督する必要がある。

③情報開示の準備

今後の課題として、サイバーセキュリティ経営に関する情報開示がある。2024年6月に経済産業省より、企業情報開示のあり方に関する懇談会の中間報告が公表されたが、今後、インシデント報告に加え、リスク管理、戦略、ガバナンスに関する情報開示に備える必要がある。同時に、情報開示を求める側に対しては、開示にかかる企業側の大きな負荷を理解し、企業価値評価に必要となる情報・データを特定するとともに、情報開示の有効性の検証が進むことを期待する。

＜参考文献＞
Inoue, H. et al., “Propagation of Overseas Economic Shocks through Global Supply Chains: Firm-level evidence (Revised),” RIETI Discussion Paper Series, 22-E-062, March 2023.
Collier, Z. et al., “The Zero Trust Supply Chain: Managing Supply Chain Risk in the Absence of Trust,” *International Journal of Production Research*, Vol. 59, Issue 11, 2021.
大越いづみ・藤本正代「サプライチェーンの信頼を確保するサイバーセキュリティ経営に関する提案」情報処理学会第86回全国大会。