ガバナンス研究部会（第３０６回）議事録

日時：2024年2月16日（金）午後3時～5時
場所：WEB 会議
出席者：（計１６人）

【報告】

１　井上部会長より、●●●●氏の入会について諮ったところ、出席者全員の賛成で了承された。
２　今井部会員より、１月２０日に開催された学会理事会の報告がなされた。
３　井上部会長より、当部会ミッションの文言修正についての提案がなされ、原案通り改訂（「監査の視点も含めて」を削除）することが了承された（適用開始４月１日）。

【定例研究発表】

１　サイバーセキュリティとＩＴガバナンス（小林正一部会員）

＜概要説明＞

○　近年、サイバーセキュリティは、全社的リスクマネジメントの問題となり、経営戦略や事業継続に関する重要な問題となっている。この背景には、サイバー攻撃の高度化・巧妙化に伴い,日本国内においてもサイバーセキュリティに関する深刻な事例が発生しており、経済産業省からサイバーセキュリティ経営ガイドラインが公表されるなど取締役会としての経営責任やガバナンスが問われる時代となっている。
○　こうした時代の変化の流れの中でサイバーリスクの現状を把握し、その課題に対する経営のガバナンス対応に関しての論点を整理する。最近は大手企業に侵入するサプライチェーン攻撃のリスクや病院などのインフラに対する攻撃も多くなってきており、対岸の火事とは言っていられない状況にある。
○　サイバーセキュリティに関するリスクは、①情報セキュリティリスク②システムリスク・事業継続リスク③サプライチェーンリスク④リーガルリスク⑤レピュテーションリスクなどがある。
○　2024 年 1 月に公表された情報処理推進機構のサイバーセキュリティの 10 大脅威 2024 では、ランサムウェアによる被害が前年に続けて 1 位、サプライチェーンの弱点を悪用した攻撃が 2 位であった。まだまだランサムウェアによる被害が収まらず継続している現状がある。各企業はいざというときのためのサイバーセキュリティ対策を検討しておく必要がある。
○　東京商工リサーチの行ったウイルス感染・不正アクセスの発生推移を見ても過去最多となっており、ランサムウェアによる被害が多発している傾向にある。また、警察庁のランサムウェア被害の情勢を見ても高い水準で推移していることがわかる。被害事例は病院の電子カルテなど社会インフラにも及んでいる。政府(経済産業省)としてもこうした事態を受けてサイバーセキュリティ対策の強化を公表するなど注意喚起を促している。
○　経済産業省と情報処理推進機構は、サイバーセキュリティ経営ガイドライン(経営者が

認識すべき 3 原則と重要 10 項目)を公表し,経営としてガバナンスの対応を求めている。取締役会としては会社法の内部統制システム構築義務の中にサイバーセキュリティ対策を含んで対応することが経営課題として求められ、監査役はその運用状況をモニタリングし必要に応じ意見提言することが重要と考えられる。

＜討議・意見＞

○ 小規模な組織や個人の場合、ランサムウェアを完全に防御することは簡単ではない。実際には、メールを安易に開かないこと、セキュリティソフトを利用することに加え、必要に応じてシステムの脆弱性を調査することが対応として重要である。

○ 上場会社にとって、株主総会直前にサイバーセキュリティに関する深刻な事例が発生するなどの事態が生じることは避けなければならない。どのようなセキュリティソフトを使用し、それを適切にアップデートしているかといった情報については、取締役の義務として、開示すべきではないか。

○ 大手の監査法人の実務での対応としては、情報に優先順位をつけて、守るべき優先順位の高い情報については厳格に守られる態勢が取られているか、バックアップが確保されているかなど、適切に対応がなされているかを確認するとともに、残余のリスクについても適切に対応するように指導しており、またそのレベルを徐々に高めている。

○ 通常のサイバー攻撃に対する防御は経営者・取締役の責任と言えるが、他国からのスーパーコンピュータを使った攻撃に対する防御まで経営者・取締役の責任とするのは過剰な期待と言える。どこまで対応すべきかという法律での定めがない中で、企業としては可能な範囲で極力対応することしかないのではないか。

○ サイバー攻撃された事例では、当該企業がどのようなレベルのセキュリティ措置を取っていたのかを具体的に見る必要がある。それによって、その企業が一定の措置を取っていたか否かの判断をすることになる。

2 公共調達に人権の「保護・尊重・救済」をどのように組み込むか～「持続可能な公共調達」の実現～（古谷由紀子部会員）

＜概要説明＞

○ 一般財団法人 CSO ネットワークでは、2022 年 12 月に中谷元首相補佐官（国際人権問題担当）（当時）に「公共調達を通じた人権の保護・尊重と持続可能な社会づくり～バリューチェーンにおける責任ある企業行動・労働慣行に向けた第一次提言」を手交、2024 年 3 月に最終提言を公表予定。

○ 目的は、公共調達への「ビジネスと人権に関する指導原則（指導原則）」及び持続可能な社会に向けた施策の組入れについて提言するものであり、2020 年に日本政府が策定・公表した「『ビジネスと人権』に関する行動計画（NAP）」の中で、「人権を保護する国家の義務に関する取組み」の一つとして、「公共調達における「ビジネスと人権」関連の調達ルールの徹底」が掲げられていることにも対応するものであり、日本政府が責任ある公共調達を行うことによって、民間に責任ある企業行動を促し、市場における公正な競争環境を創出し誰一人取り残さない包摂的な社会経済の発展に寄与することを目指すものである。

○　背景として、持続可能な社会の実現には、社会、経済、環境の統合的な発展・保護が必要とされ、近年世界では、公共調達を持続可能な社会を目指す政策実現の手段として位置付けた「持続可能な公共調達」（Sustainable Public Procurement：SPP、以下、SPP）を推進する動きが広がっていることがある。SPP は、地球全体の持続可能性を高める社会的、経済的、環境的配慮を公共調達に戦略的に組入れたものであり、その社会的・経済的配慮には、女性や子ども、マイノリティや障害者などの人権の尊重のほか、児童労働、強制労働の撤廃その他労働者の権利の尊重が含まれる。

○　本提言は、この SPP の取組みの中で、国際社会が一丸となって対応することが求められているバリューチェーン上の労働・人権問題に焦点を当てて、具体的な提言とともに国内外の参考事例を紹介している。

○　本提言の内容は、
提言１：一貫した政策に基づく持続可能な公共調達（SPP）の推進
提言２：企業行動が人権や社会的経済的発展にもたらす「正」「負」の影響を考慮した「人権尊重調達枠組」の策定
提言３：政府による「救済（苦情処理）メカニズム」の提供
提言４：SPP 推進のための能力開発と体制整備、国民の権利意識の醸成

○　政府の動きとしては、2023 年 4 月に公共調達の入札説明書や契約書等において、「入札希望者/契約者は『責任あるサプライチェーン等における人権尊重のためのガイドライン』踏まえて人権尊重に取り組むよう務める」としたところ、各省庁ではこの方針に基づき対応しているようだがその全容が必ずしも明確ではない。今後、国・自治体における SPP の浸透・普及が期待される。

＜討議・意見＞

○　バリューチェーンとサプライチェーンの用語については、必ずしも統一的な認識があるわけではない。サプライチェーンの方がバリューチェーンよりも広い範囲をカバーしているという議論もあるが、バリューチェーンを販売・広告などの領域を含めたものと定義すると、バリューチェーンの方がサプライチェーンよりも広い意味を持つものと考えることができる。

○　欧米では法律によって人権尊重を担保している。わが国では法律による規律づけはなされていないが、国際的な人権尊重の考え方を踏まえると法律の有無にかかわらず、企業は人権尊重に取り組む必要がある。欧米は法律、わが国はソフトローでの対応となっているが、わが国でも法律によって規律すべきという声も強くある。

○　企業の自主性に任せておくとなかなか人権尊重を考慮した調達が進まないので、それを進める 1 つの武器として公共調達を通じた人権の保護・尊重に焦点をあてていると理解される。

○　法律の有無にかかわらず、個人の人権が尊重されない世界は今や許されないのであり、企業も適切に対応していく必要がある。

○　公共調達に関しては、受注者側の企業の意識だけではなく、むしろ発注者側の問題も大きいのではないか。予算・コストを意識した価格だけを主な判断基準とした発注をしていては、公共調達を通じた人権の保護・尊重はなかなか達成できない。

○　ソフトローでの規律づけだと、真面目な会社は対応するが、そうでない会社は対応しない。これが価格競争力に影響することから、ソフトローによる規律づけには限界がある。ハードローでの対応を模索すべきではないか。

【次回開催日】３月１５日（金）午後３時　WEB にて開催