国際取引法学会全国大会　グローバルコンプライアンス法制部会

【報告タイトル】

ガバナンスの観点からみるサイバーセキュリティと取締役の責任
内部統制システム構築に係る米国会社法上の義務と証券法の開示義務からの考察

報告者：神山　静香（実践女子大学）

【概要】

現代の企業経営においては、企業の事業活動による負の外部性への配慮や不確実性を伴うリスクへの対応が求められる。近年、サイバー攻撃により、国家の経済安全保障に関わる重大なインシデントが発生しており、米国では、ソフトウェアを提供する企業がサイバー攻撃の標的となり、顧客の大企業や政府機関から機密情報が流出する大規模な情報漏洩事件が発生している（サンバースト攻撃事件)。米政府機関がロシア諜報機関によるものとの声明を発表する等、地上戦とサイバー攻撃のハイブリッド戦争ともいわれる情勢を受け、サイバーセキュリティは、広範な外部性を伴う重要な事業リスク及びコンプライアンスリスクと認識されている。

2019 年、わが国では金融庁が「記述情報の開示に関する原則」を公表し、非財務情報（記述情報）開示の考え方をプリンシプルとして公表した。「事業等のリスク」として、投資家の判断に重要な影響を及ぼす可能性のある事項を具体的に記載することが求められ、2023 年、「企業内容等の開示に関する内閣府令」が改正され、有価証券報告書等に「サステナビリティに関する考え方及び取組」の記載欄が新設された。非財務情報開示の拡充・充実が図られる一方で、経営者が認識していないリスクが法定の開示事項に該当するか学説上争いがある等、非財務情報に係る虚偽記載、不記載、誤導的不記載の該当性について明確な判断基準はない。また、取締役の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれるとされるが、金融商品取引法上の非財務情報開示に係る責任と内部統制システム構築・運用に係る会社法上の取締役の善管注意義務との関係は明らかではない。本報告では、上記問題への示唆を得ることを目的として米国の判例・学説を考察する。

米国では、大規模なサイバー攻撃事件について、会社法の分野で、レッドフラッグを見落とした取締役の不作為が継続的・組織的な監視義務の懈怠や不誠実性を示すものであるとして、株主代表訴訟が提起されている。明白な実定法違反がない場合でも、取締役が内部統制システムの構築・運用監視を怠ったことでリスクが顕在化し、多様なステークホルダーに甚大な被害をもたらした場合は任務懈怠責任が成立するのか、裁判所の立場を検討したい。

証券法については、サンバースト攻撃事件では、企業のウェブサイトに掲載されたセキュリティに係る声明が重大な虚偽または誤解を招くものであるとして、1934 年証券取引所法 10 条(b)項及び規則 10b－5 に基づき、民事制裁金の支払い等を求める証券訴訟が証券取引委員会（SEC）により提起されている。いかなる場合に証券詐欺が成立するかを検討したい。