「サイバーセキュリティと投資・金融関連制度に関する研究会」活動報告

野村資本市場研究所

2024 年 7 月

要約

1. デジタル化の進展により、サイバーリスクが企業価値のみならず、場合によっては金融資本市場、経済社会全体、そして人々の生活にも甚大な影響を及ぼすようになっており、サイバーセキュリティの重要性が増している。

2. 各国・地域では、金融資本市場のステークホルダーである金融機関、資金調達主体である企業、資金提供主体である投資家、評価機関、金融規制・監督当局、政府等が、サイバーリスクの脅威に対応すべく、様々な対応を進めてきた。具体的には、コーポレートガバナンス、情報開示、投資家行動、評価、金融商品開発、金融規制・監督、ガイドライン等の尺度から重層的な取り組みが行われている。これらは、金融資本市場、各ステークホルダーの自律的な取り組みに加え、相互に対応強化を促してきた。

3. サイバーリスクの深刻化、複雑化は刻々と進んでおり、上記の取り組みの継続は不可欠であるが、今後さらに対応を進めるべき課題もある。人材育成については、金融資本市場のみならず、社会全体で取り組みを強化することが求められる。デジタルトランスフォーメーション（DX）／人工知能（AI）の発展や地政学リスクの深刻化は、サイバーリスクの脅威として注視する必要がある。

4. 金融資本市場、金融機関、企業、投資家といった全てが自らのこととして捉え、協力・協調をしながら、不断の努力で取り組むことがサイバーリスクの軽減とともに、持続可能な社会の実現につながっていくと考えられる。

Ⅰ.「サイバーセキュリティと投資・金融関連制度に関する研究会」設立の趣旨とその目的

野村資本市場研究所は 2023 年 7 月、学識者及び実務経験者等により構成される「サイバーセキュリティと投資・金融関連制度に関する研究会」を設立した（委員会のメンバーについては「別紙 1 サイバーセキュリティと投資・金融関連制度に関する研究会 参加者」を参照）。

デジタル化の進展により、サイバーリスクが企業価値、場合によっては金融資本市場、経済社会全体、そして人々の生活にも甚大な影響を及ぼすようになっている。各国・地域では、金融資本市場に関連する切り口からも、サイバーリスクの脅威に対応すべく、コーポレートガバナンス、情報開示、評価、投資家行動、金融商品開発を始めとして様々な議論・対応が進んでいる。さらに、米国等の金融当局は、証券業界に対してサイバーリスクへの対処の厳格化に向けた取り組みを強化しており、証券市場を取り巻く規制改革の流れとも位置付けられる。日本においても、制度面も含めてしっかりと対応を進めることが、企業価値の保全・向上、金融資本市場の健全な発展において不可欠と考えられる。

以上のような問題意識から設立された本研究会は、投資や金融関連制度の観点からサイバーセキュリティに焦点を当て、諸外国の動向も踏まえた日本の現状や課題を多面的に洗い出し、ステークホルダーに求められる対応に焦点を当てて研究を進めた。2023 年 7 月から 2024 年 4 月までの 10 回に亘って、企業経営、ガバナンス、情報開示、投資、評価、金融商品、金融規制、人材育成等、幅広い観点から研究報告及び議論を行った。（取り上げた主なテーマは、別紙 2「サイバーセキュリティと投資・金融関連制度に関する研究会」を参照）。

これらのテーマにおいて検討すべき課題や議論すべき内容は多岐にわたり、かつ、その状況も日々変化していく。このため、本研究会では見解の統一や提言といった「結論」の導出を急ぐよりも、各テーマに潜在する様々な論点や課題等を浮き彫りにすることを主眼として、各専門分野の動向に基づく知見を大切にしていくことを基本とした。

Ⅱ.研究会で出された見解、知見

このようなスタンスで研究報告や議論を重ねた結果、以下をはじめ多くの見解、知見を得ることができた（議論の過程において示されたものの要約であり、本研究会における統一した見解や提言ではない）。

【世界と日本の現状】

世界では 1990 年代終盤頃から情報化社会が急速に発展する中、サイバー犯罪や攻撃による企業等への被害や社会経済全体に及ぼす影響が懸念され、サイバーセキュリティの重要性が高まっている。金融資本市場でも近年、サイバーリスクが顕在化した企業の株価が下落する等の影響が見られているほか、金融機関がサイバー攻撃を受けて決済機能が一時的に失われたりが不能になったり、顧客情報が流出するなどの被害が及ぶなど、セキュリティ対応が不可欠な状況となっている。

米国で 2021 年 5 月に起きたコロニアルパイプラインへのランサムウェア攻撃の事案もあり、企業のガバナンスにおけるサイバーセキュリティの重要性が経営者の中で浸透し始めている。研究会では、企業によってサイバーセキュリティの重要性の認識に

は差がある、投資家を含むステークホルダーの信頼を確保する上で情報開示が重要、などの意見が上がった。

【企業経営】

サイバーセキュリティを考える上では、安全保障、システム、経営者視点での環境変化を考えていくことが重要との見方が示された。さらに、昨今では新型コロナウイルス感染症の拡大等の環境変化により社会のデジタル化が進み、サイバー攻撃の脅威があらゆる産業において無縁はなくなっているとの意見も見られた。こうした中、企業の経営者はサイバーリスクに対して高い意識を持っているが、取締役のサイバーセキュリティに関する知見をさらに高めていくべきとの見解が示された。また、今後は小規模事業者のサイバーセキュリティ強化の取り組みについて底上げを図っていくべきとの意見も出された。事業会社・金融機関における組織の課題としては、人材確保、経営層の理解、予算確保等が挙げられた。

【ガバナンス】

国内企業のサイバーセキュリティのリスクへの取り組みを進める際の課題として、経営とサイバーセキュリティとの関連性についての認識を深めていくべきとの意見が出された。日本では、コーポレートガバナンス・コード、投資家と企業の対話ガイドライン等を踏まえると、ガバナンスの観点からサイバーセキュリティのテーマが十分に取り上げられてこなかったとの見方が示された。諸外国においては、データセキュリティがガバナンスの重要項目になっているとの指摘がなされると共に、ガバナンスの観点では、取締役が体制整備と情報開示を議論して決めることが目指されるべきとの意見がだされた。

【情報開示の在り方】

昨今、従来の規則の遵守や問題の発生等が焦点となる「規制当局が求める報告」に加えて、企業価値や投資判断等の要素で開示の要否が議論される「投資向けの情報開示」が進展している。投資家団体よりサイバーセキュリティをコーポレートガバナンスの論点と認識すれば、更なる議論が期待できるとの見解が示された。

ESG（環境・社会・ガバナンス）情報開示枠組みでは、発行体のサイバーセキュリティに関する開示を後押しする動きが見られており、投資家の意思決定や ESG 評価機関の分析にサイバーリスクの要素が反映され始めている。日本においても、経済産業省による投資家団体を通じた投資家の意見聴取の動きや民間企業による勉強会の開催等、サイバーセキュリティに係る投資家と企業との対話（エンゲージメント）実施に向けた機運が醸成され始めている。今後、サイバーセキュリティに関する情報開示を検討する上では、誰に何を求めるかといった目的を明確にした上で検討することが重要との指摘が行われた。

【投資家の視点】

機関投資家が、企業のサイバーセキュリティリスクや企業の講じた対策を適切に評価し、投資判断に取り込むようになれば、企業の積極的な取り組みの後押しとなりうる。研究会では、サイバーセキュリティリスクを定量化・スコア化し、ESG 投資プロセスに統合している運用会社の事例が紹介された。

そのような先進的な取り組みが始まっている一方で、サイバーセキュリティが主要な事業リスクであるという認識には企業、投資家の双方において幅があること、サイバーセキュリティに係る規制が必ずしも十分整備されておらず、サイバー事案発生時の情報開示が不足していることなどが指摘された。研究会では、投資家による日本企業に対するエンゲージメントの現場では、企業がサイバーセキュリティをトピックとして認識していないことも散見されるため、その重要性に関する経営陣の意識を高めることが必要といった意見も挙げられた。

【金融規制当局のスタンス】

金融セクターにおけるサイバー攻撃が頻発する中、金融機関におけるサイバーリスク対応に向けた取り組みを各国の金融当局や国際機関が後押ししている。日米当局は各金融機関等の業務運営全体に関連し得る施策を推進し、他方で国際機関は国際的なベースラインの底上げを目指すことに焦点を当てている。今後、各国当局、国際機関が取り組む意義がある主な分野として、金融機関におけるサイバー人材育成、リスクシェアリングの在り方、関連施策におけるサイバーリスク、が挙げられた。

中国の証券業においては、初めてのサイバーセキュリティに関するルールとして、「証券・先物業のネットワーク及び情報セキュリティ管理弁法」が 2023 年 2 月に公布された。中国当局は、同法に、証監会が主導する集中的データバックアップ制度の構築や、IT サービス提供者に対する管理監督の強化を盛り込んでいる。今後、同法に関連した取り組みの実効性が注目されるとの指摘がなされた。

【金融商品開発】

サイバーセキュリティの取り組みの選択肢として、サイバー保険が挙げられる。世界においてサイバー保険の市場規模が拡大傾向にあるとの状況が示される一方、国内企業におけるサイバーリスクに対する危機意識の低さも一部見られており、サイバー保険の普及に向けた取り組みを推進する余地があるとの見方が示された。サイバー保険の普及に向けた課題として、（1）サイバーセキュリティに対する意識等の向上、（2）企業によるサイバーセキュリティ対策のさらなる強化、（3）損害保険会社におけるサイバー保険ビジネスの持続可能性向上、が挙げられた。

【評価】

大手格付会社の S&P グローバルやムーディーズは近年、サイバーリスクに関するソリューション提供を強化すべく、サイバーセキュリティ格付会社等との連携を行っている。S&P は、格付決定プロセスにおいて、経営陣とガバナンスの要素にサイバーリスクを反映している。ムーディーズは、サイバーリスクの信用格付けへの織り込みについて具体的に発信していないが、セクター別のサイバーリスクスコアを示すヒートマップを公表している。その他、米国のセキュリティスコアカードやビットサイトは、企業のサイバーセキュリティリスクを、攻撃への脆弱性等の観点から定量的に分析し、スコアリングしている。

研究会では、これらの評価も用いてサイバーリスクを含む非財務情報を企業価値にどのようにつなげることができるかが今後の課題との指摘があった。

【人材育成】

企業がサイバーセキュリティ対策を講じるためには、優れた人材を継続的に確保できるかがカギを握ると考えられる。しかしながら、日本企業においてはサイバーセキュリティの人材不足が深刻である。ここで言う人材には、企業のリスク管理等の戦略マネジメント領域と、より実務的な技術領域の人材が含まれる。また、経営陣のコミットメントと取締役による監督の重要性を踏まえれば、経営陣等によるサイバーセキュリティの理解促進も不可欠である。

研究会では、学術機関によるサイバーセキュリティ人材の育成やカリキュラム開発の現状について、（1）経営層、（2）戦略マネジメント層、（3）実務者層・技術者層、について議論されることが多く、経営層と実務者層・技術者層の橋渡しをする人材として戦略マネジメント層の重要性が認識されていることなどが共有された。また、日本企業の実情に関して、最高情報セキュリティ責任者（CISO）でもサイバーセキュリティ分野の専門人材というよりはジェネラリストが多いが、経営層においては公認情報セキュリティマネージャー（CISM）の水準の知識は必要になるのではないか、といった指摘もあった。

Ⅲ. おわりに

本研究会ではサイバーセキュリティに関する様々な論点について議論を深めた。最後に、金融資本市場及び金融機関の観点から議論を通じて得られた知見を記したい。

金融資本市場及び金融機関は、サイバーセキュリティに関して自ら 2 つの取り組みを進めることが必要であると共に、その取り組みを促し得る存在も大切であることが見いだされた。

取り組みの 1 点目は、金融資本市場、金融機関が自律的にガバナンス体制を構築し、サイバーセキュリティ対策に取り組むことである。金融資本市場、金融機関ともに経済・社会のインフラ機能を担っており、サイバーインシデントが起きた場合、金融資本市場や経済界のみならず、人々の生活にも影響を及ぼしかねない。その意味でも市場やそのプレイヤーである金融機関にとって自身の取り組みは社会全体に対する責務という観点から重要と言える。

2 点目は、金融資本市場のステークホルダーである企業、投資家等のサイバーセキュリティへの取り組みを後押しすることである。例えば、資金調達主体である企業等に対して、企業価値を維持・保全すると共に円滑な資金調達を実現するために、サイバーセキュリティ対策の強化や適切な情報開示を促したり、金融機関が金融商品・機能等を通じて企業のサイバーセキュリティ対策を支援したりといったことが考え得る。また、資金提供主体である投資家に対して、投資パフォーマンスの向上も踏まえた調査研究情報の提供、サイバーセキュリティに関する最適なポートフォリオ構築の提案などを行うことができる。加えて、金融機関や投資家は、投資行動やエンゲージメントを通じて、企業のサイバーセキュリティ対策の強化をさらに効果的に促すことが期待される。

このように、金融資本市場、金融機関は自ら 2 つの取り組みを自律的に行うことが求められるが、これらの取り組みを促し、外部から規律を求める存在として、各種評価（信用力、ESG、サイバーセキュリティ格付け・スコア等）、金融規制・監督、政府によるガイドライン等が挙げられる。これらの存在は、自身の取り組みが適切か、そしてどの部分を強化すべきかといった点を客観的に判断するため、より良いサイバーセキュリティ対策につながり得るものと言える。

以上が研究会を通じて明らかになったことであるが、サイバーリスクの深刻化、複雑化は刻々と進んでおり、上記の取り組みの継続は不可欠であるが、残された課題もある。例えば、人材育成については、金融資本市場のみならず、社会全体で取り組みを強化することが求められる。デジタルトランスフォーメーション（DX）／人工知能（AI）の発展や地政学リスクの深刻化は、サイバーリスクの脅威として注視する必要がある。

一方、今後、さらなるサイバーセキュリティの強化を目指す上では、気候変動関連の文脈で語られる「リスクと機会」といった観点が 1 つの切り口となり得るとも考えられる。例えば、サイバーセキュリティに関連した新たな金融商品が開発されれば、金融資本市場全体のサイバーセキュリティの向上に寄与するとともに、投資機会となることも期待される。加えて、サイバーをめぐるリスクと機会に関して、企業価値にどのように影響し得るのか、実証研究をさらに進めることは、金融資本市場、投資家の観点から求められるところである。

サイバーリスクの脅威の高まりは続くと思われるが、本研究会では、金融資本市場、金融機関、企業、投資家といった全てが自らのこととして捉え、協力・協調をしながら、不断の努力で取り組むことが、サイバーリスクの軽減とともに持続可能な社会の実現につながっていくと考えている。

なお、本研究会の活動成果の詳細については、追って公表する予定である。

以上

別紙 1　サイバーセキュリティと投資・金融関連制度に関する研究会　参加者

（役職は 2024 年 3 月 31 日当時　50 音順　敬称略）

＜研究会委員＞

今川　玄	野村證券株式会社　IB ビジネス開発部　主任研究員
江夏　あかね	株式会社野村資本市場研究所 野村サステナビリティ研究センター長
門倉　朋美	株式会社野村資本市場研究所　研究員
神田　秀樹	学習院大学大学院法務研究科　教授 東京大学　名誉教授
ジェイソン・モーティマー	野村アセットマネジメント株式会社 債券サステナブル・インベストメント・ヘッド
富永　健司	株式会社野村資本市場研究所 主任研究員
野村　亜紀子	株式会社野村資本市場研究所 研究部長
藤本　正代	情報セキュリティ大学院大学　教授
丸山　満彦	PwC コンサルティング合同会社　パートナー
三井　千絵	株式会社野村総合研究所　上級研究員

＜オブザーバー＞

金融庁

経済産業省　商務情報政策局サイバーセキュリティ課

別紙 2:研究会の歩み

第 1 回（2023 年 7 月 4 日）

- 金融市場から見たサイバーセキュリティの概況

第 2 回（2023 年 8 月 29 日）

- 投資家から見たサイバーセキュリティ
- サイバーセキュリティ評価会社の見解

第 3 回（2023 年 9 月 20 日）

- セキュリティの最近の動向等
- 企業経営とサイバーセキュリティ

第 4 回（2023 年 10 月 25 日）

- 企業のサイバーセキュリティリスクとサイバー保険

第 5 回（2023 年 11 月 22 日）

- サイバーセキュリティとガバナンス

第 6 回（2023 年 12 月 13 日）

- 信用格付とサイバーリスク

第 7 回（2024 年 1 月 17 日）

- サイバーセキュリティと金融関連制度
- サイバーセキュリティと評価

第 8 回（2024 年 2 月 6 日）

- サイバーセキュリティと情報開示
- サイバーセキュリティ対策の潮流
- 米国で開催されたサイバーセキュリティに関するカンファレンスからの雑感

第 9 回（2024 年 3 月 6 日）

- サイバーセキュリティと人材
- 事業会社のサイバーセキュリティ実務
- サイバーセキュリティにおける経営層の責務

第 10 回（2024 年 4 月 19 日）

- 今後の検討課題