サイバーリスクと企業価値
―今、投資家に求められることは―

野村総合研究所 上級研究員
三井　千絵

▌要　約▐

1. サイバーリスクが企業価値に与える影響がここ数年高まっている。コロナ禍により事業や業務がオンライン化したことも、そのリスクを高めている。日常的に人材や予算を適切に割り当て、必要なトレーニングを行うといった取り組みはもとより、事業が停止し、社会や経済にダメージを与え、顧客データの流出などが起きた場合でも、経営者が適切に判断や対処を行えるよう常日ごろから備えることは、被害を最小限にし、企業価値の毀損の食い止めにつながるだろう。
2. 投資家は、投資先企業の経営者がサイバーリスクに対してどのように取り組んでいるか、どのようなガバナンス体制を構築しているかを知り、必要に応じてその情報を投資先選定基準に用いたり、エンゲージメントを行うことで運用資産を守るべきといえる。米国や英国ではそのような投資家の判断を支えるための、企業開示の整備も始まっている。しかし先行して取り組む国のレギュレーターや、投資家団体等の関係者の中には「この問題は投資家も経営者もさらなる知識が必要」と感じている人もあるようだ。
3. 今後、サイバーリスクをめぐる知識の共有や、対話のプラクティスをはじめとした市場全体での取り組みが求められると言える。

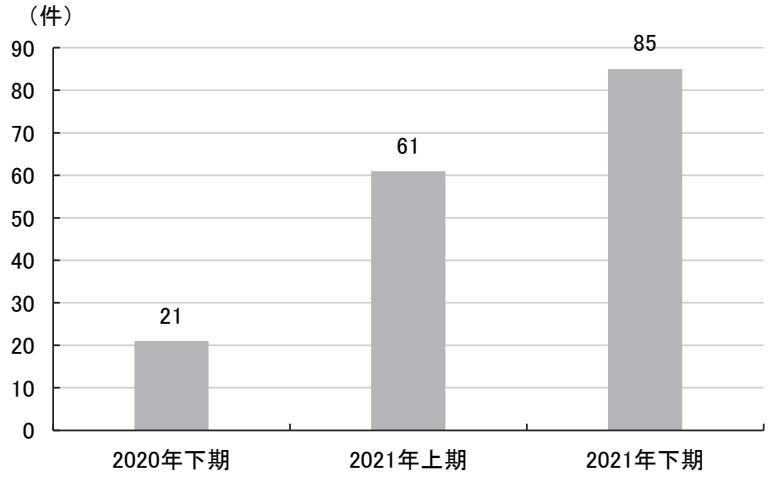
Ⅰ 増えるサイバー攻撃とその被害

企業のサイバー関連のリスクは増加の一途をたどっている。警視庁が 2022 年 4 月に公表した報告書[1]によると、特にランサムウエアによる被害が足元で急増している（図表 1 参照）。ただし、これは日本のみの傾向ではなく、2021 年 12 月に「ランサムウエアに関する G7 高級実務者会合」が開催されるなど、グローバルな対策が喫緊の課題となっている。サイバー攻撃にあった企業は、サービスやプロダクトラインが止められたり、それに伴って顧客の信頼を失ったり、サプライヤーへ迷惑をかけたり、あるいはやむにやまれず身代金を支払うといった様々なダメージを受ける。

監査法人は、顧客企業がサイバー攻撃にあうと、攻撃の種類にもよるが財務諸表の作成に関する問題により、その状況を把握することがある。EY 新日本監査法人は、サイバー攻撃を受けた企業のケースをまとめており、2022 年の監査の状況を踏まえた投資家向け勉強会で「企業がサイバー攻撃を受ける数はここ数年増加し、業務停止に発展するだけでなく、財務諸表の作成遅延となったケースも内外でみられる。また関連は明らかでないものの、その数はロシアのウクライナ侵攻後さらに増加している」と解説した。

これは、投資家にとってサイバー攻撃は、当該企業自身の問題、たとえばサービスや業務が中断されたり、顧客情報が流出したりといった事象だけでなく、決算情報が不正確になる危険性や開示の遅延という形で、アナリスト業務等に直接影響を及ぼす可能性があることを示している。

図表 1　企業・団体等におけるランサムウエア被害の報告件数の推移



（出所）警視庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について」
2022 年 4 月 7 日

[1] 警視庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」2022 年 4 月 7 日。

Ⅱ サイバーリスクと投資家

サイバーリスクは比較的新しいリスクで、「我々が口を出せる分野ではない」と考える機関投資家が未だ少なくない。企業の経営者側も、「IT 担当者ではなく経営者の責任」という認識は途上であるようだ。経済産業省及び独立行政法人情報処理推進機構（IPA）が 2017 年から発行している「サイバーセキュリティ経営ガイドライン」では、サイバー攻撃から企業を守る観点で必須の情報をまとめているが、「経営者が認識する必要のある『3 原則』」や「特に第一章は経営者にわかるよう記載をした」といった表現が続き、“経営者にわかるよう”苦心をしている様子が感じられる。しかしサイバー攻撃などが発生した時の、事業や経営に対する影響は年々大きくなっている。前章でも触れたが、業務やサービスの停止だけではなく、取引先や顧客情報が流出すれば、サプライチェーン全体に影響が及ぶ。そしてコロナ禍でますます業務やサービスのオンライン化が進んだこともあり、リスクも影響も以前より大きくなっている。

2021 年 5 月、米国の石油パイプラインがサイバー攻撃を受けて操業を停止し[2]、東海岸の社会経済活動に大規模な影響を与えた。この「操業停止」のような、自社の事業と社会に大きな影響を与える決断は、IT 担当者ではなく経営者が行うことになる。そのため経営者は少なくとも、サイバー攻撃が起きた時、迅速に情報を掌握すると共に、適切な指示を出し、株主、顧客、影響を受けるすべてのステークホルダーに速やかに説明を行う必要がある。もしそれを適切に行うことができなければ、企業価値の毀損も大きくなり、投資家もより大きな損失を被ることとなるだろう。

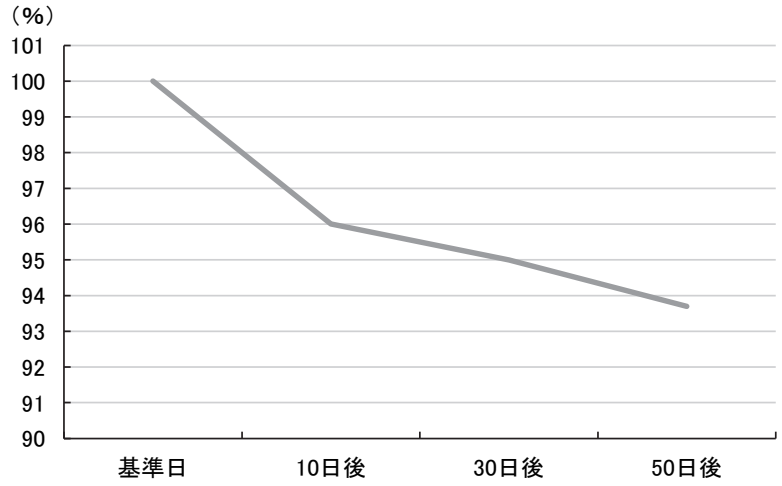
そうなると、経営者や投資家が意識するべきサイバーリスクへの対応とは、特定のソフトウエアを導入したとか、システム構成をどのようにしているかということではなく、当該企業のガバナンス、例えばスタッフには必要な投資・教育を行っているか、リソース配分は十分か、適切な監視が行えているかといった日常的なことから、何かあった時の報告、意思決定、迅速な説明ができる組織構成になっているかどうか、といったことになるだろう。重要なのは、経営者が問題をどれだけ理解しているかという点であり、経営者自身の意識やナレッジ、必要な知識を収集する活動をしているかといったことを点検することは、今や投資家としては必須のことではないだろうか。

一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）は、2022 年 3 月 17 日に発表したレポート[3]で、不正アクセス等の適時開示を行った企業の株価は、開示日の 10 日前からの 50 日間の平均で 6.3%下落していることを報告し、「セキュリティ対策の未整備な状態は、損害賠償や善管注意義務違反に問われる恐れもある」との見解を示した。実際、海外では、サービス停止に追い込まれた事例や、訴訟になり和解金として数

2 「大抵の人が知らない「サイバー攻撃」驚愕の新事情－重要インフラが狙われる？積極防衛が必要な理由－」『東洋経済 ONLINE』、東洋経済新報社、2021 年 8 月 9 日。

3 一般社団法人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―」2022 年 3 月。

図表 2　不正アクセス等の適時開示後の株価推移（サンプル 47 社）



（注）　調査対象は、証券取引所へ不正アクセス等の「適時開示」を行った 47 社。2014 年 7 月以降の適時開示企業を対象。開示日より 10 日前を 100%（基準値）とした。日経平均株価の変動値は調整済み。
（出所）一般社団法人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－」2022 年 3 月

億円～数百億円支払ったなど、大きな収益上の損失を被った事例も報告されている。しかし気候変動リスクと同様、サイバーリスクについても、経営者がリスクの所在とその影響を把握し、必要な予防措置にリソースを割き、発生時は速やかに対処を行う体制を整えていれば、企業価値の毀損を食い止めることにつながるだろう。

Ⅲ　サイバーリスクのエンゲージメント

サイバー攻撃が企業価値に与える影響がより大きくなっているのであれば、企業が必要な対応をとっているかどうかを投資先選定の条件に加えたり、あるいはまだ対応を行っていない場合は経営者にそれを求めたりすることは、顧客の資金を預かるアセット・マネージャーにとって考慮するべき点と言える。

2010 年代半ば頃は、気候変動リスクについても、投資家側からは「我々はサイエンティストではないので、企業から技術的なことを言われても判断できない」という悲鳴が聞かれた。その後様々な評価フレームワークや評価用データが整備され、投資家の判断を支えるようになった。もちろん企業の気候変動リスクをどのように投資家は考慮すべきか、どこまで専門的なことを理解すべきか、何をどのように経営者に求めるのが投資家の責任か、といったことは未だに議論の途上だ。その上気候変動と違って、その対応の有無や対応自体を隠したいと企業が考えがちなサイバーセキュリティについては、エンゲージメントの話題にとりあげるだけでも、投資家にはハードルが高いだろう。

しかし一部の投資家はその重要性を認識し、エンゲージメントの取り組みを始めている。JP モルガンアセットマネジメントは 2022 年 4 月に発行した 2021 年版の「Investment Stewardship Report[4]」の中で、その年にエンゲージメントで見られた様々なトピックとして、サイバーセキュリティについての考察を、2 つの投資先企業へのエンゲージメント事例とともに数ページに渡って説明している。まず、「サイバーセキュリティのリスクは常に存在し、ほぼすべての企業にとって重要なリスクである」と述べ、調査会社 Gartner による 2021 年の調査[5]を引用し、回答企業全体のうち約 88%の取締役は、既にサイバーセキュリティをビジネスリスクと見なしていることと、その割合は 5 年前に比べ約 3 割増加していることを紹介した。そのように多くの企業が事業リスクだと考える背景として、事業のオンライン化が進んでいることも原因の一つと分析している。パンデミック以降における各国共通の背景と言える。続けて、欧州連合（EU）で 2018 年に導入された一般データ保護規則（GDPR）によって課徴金を課せられるケースや、2020 年に施行されたカリフォルニア州消費者プライバシー法、2021 年に施行された中国のデータセキュリティ法を紹介し、これらの影響に注目する必要性を説いている。そしてサイバーセキュリティとデータ保護は、今後のビジネスリスクの中でもより重要なものになるとし、取締役会のガバナンスが一層求められると指摘した。

またサプライチェーンのリスクについても触れ、実際に 2021 年に問題が発生したケースとして、米国最大級の小売業者 Kroger への大規模データ侵害のケースを挙げた。本レポートのエンゲージメント活動を報告するセクションでは、いくつかの企業とのやりとりが記載されているが、サイバーセキュリティについてのエンゲージメントは、ダイバーシティと並び投資先企業が着実な変化を見せた（つまり、エンゲージメントとして成果があった）点であると評していた。

筆者が日本株（日本株を含むグローバル）に投資をしている、あるいはカバーしている国内外の投資家・アナリストに取り組みをヒアリングしたところ、全体の約 3 分の 2 は既にエンゲージメントでサイバーセキュリティについて話題に出したことがあると答えた。話題に出してないケースにおいて、理由の半分は「企業は十分に対応しているようだったから」ということだった。話題に出したケースでは全員が「ビジネスリスク」として話をしたと回答、そのほかの観点としては「財務リスク」「風評（レピュテーション）・リスク」、「ガバナンスの欠如」が続き、人材面の対応の問題を挙げたというケースもあった。回答に協力した全員がサイバーリスクは今後もますます重要になると感じていた。サイバーリスクに関して企業のなかで誰が責任を持つべきと考えるか、という問いには、最高経営責任者（CEO）、IT 系執行役員、取締役で回答が割れたが、IT マネージャーと答えた人はいなかった。一方、インタビューを依頼しても、このテーマへの回答に応じた人の数は多くなく、国内の投資家の中にはやはり「投資家が口を出すべき分野ではない」という反応もみられた。

4 J.P. Morgan Asset Management, “2021 Investment Stewardship Report,” April 1, 2022.
5 Gartner, "Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk," November 18, 2021.

Ⅳ レギュレーターの取り組み 1　米国証券取引委員会（SEC）

海外では、レギュレーターがサイバーリスクに関する企業開示の強化に取り組む国も出てきている。

米国 SEC は 2022 年 3 月 9 日、上場企業を対象としたサイバーセキュリティリスクのマネジメント、戦略、ガバナンス、そしてインシデントの開示に関わる改訂案を発表した[6]。ゲイリー・ゲンスラーSEC 委員長は「サイバーセキュリティは上場企業がますます対処しなければならない新たなリスクとなっている。投資家は企業がこれら増大するリスクをどのように管理しているかについて、もっと知りたいと思っている。多くの上場企業はすでにこれに関する開示を行っているが、これらの情報は一貫性があり、比較可能で、意思決定に役立つような開示である必要がある」とその発表文で述べた。

同案では、まず年次報告書において、サイバーリスクを特定し、それを管理するための方針と手続き、取締役会における監督、評価や手続きの実施における経営者の役割、財務に与える影響、専門知識についての開示が求められている。またインシデントについては、情報の機密性などを損なうインシデント、つまり外部からの攻撃だけでなく従業員が誤って情報を公開した場合なども含み、それが発生してから 4 日以内に Form 8-K（株価に影響を与える可能性のある重要事項に関する報告）による開示を求めている。後者については、米国内の業界団体である情報技術産業協議会（ITI）等から厳しすぎるという声があがり、セーフハーバー規定を盛り込むことを求める意見が送られた。Form 10-K（年次報告書）で開示を求めている内容は、何らかのリスクについて経営者に対応を求める際、基本的に必要となるようなものばかりだが、投資家団体からは急速な開示の要件化がボイラープレート（定型文言）化を招かないか懸念する声も聞かれた。また、責任投資原則（PRI）事務局は 2022 年 4 月、コメントレター[7]を発表し、その中で PRI の過去のサイバーセキュリティ開示に対する取り組み（後述）に触れ、ガバナンスの開示を重視する SEC の改訂案を歓迎する旨を明らかにした。その上で追加的に、サイバーセキュリティに関する経営陣とスタッフへの研修の種類や範囲の開示を要求した。また詳細として、ポリシーや手続きについて、事業がグローバルに展開している場合は、米国内だけではなくグローバルな開示を行うことを求めるべきとした。

Ⅴ レギュレーターの取り組み 2　英国財務報告協議会（FRC）

英国では、国家サイバーセキュリティーセンター（NCSC）がサイバーセキュリティについて取組ガイダンスなどを提供するほか、企業開示とガバナンスを監督する FRC も、サイバーリスク関連の開示とガバナンスのベストプラクティス作りの取り組みをはじめて

6 U.S. Securities and Exchange Commission, “SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies,” March 9, 2022.

7 Principles for Responsible Investment, “Consultation Response- US Securities and Exchange Commission: Cybersecurity Risk Management, Strategy Governance, and Incident Disclosure; RIN 3235-AM89,” April 2022.

いる[8]。FRC には、開示関係者で集い意見を交換しあうことでベストプラクティスを生み出す「Lab」というプロジェクトがある。過去にも気候変動や従業員（workforce）に関する開示など様々なテーマを取り上げてきたが、2021 年からサイバーセキュリティについて取り上げ、2022 年 8 月にレポートを発行した[9]。FRC Lab の取り組みでは、サイバーセキュリティのみに注目をするのではなく、デジタルシステム、プロセス、データなどを広範にカバーした議論を行った。そこではまず、「データやシステムの扱い、サイバーセキュリティへの対処はビジネスの持続性、レジリエンス、価値創造の基盤に大きな影響を与えるようになってきた」、「これらについてより詳細に投資家に開示することは、企業の持続性やレジリエンスの能力の評価に役立つ」、と取り組みの意義を説明している。また FRC はこれまでコーポレートガバナンスの議論で、従業員や顧客、サプライヤーなどステークホルダーへの考慮に関する開示を求めてきたが、サイバーセキュリティのリスクはサプライチェーンに及ぶため、コーポレートガバナンスの観点からも開示は当然のことであるとしている。つまり、サイバーセキュリティリスク要因は広範な ESG の議論に関係している、と FRC は述べている。一方サイバーリスクの開示の話をすると多くの企業は「それを開示すれば『犯人』に知らせることにもなり、サイバーアタックのリスクが増える」と心配する、と企業の状況への配慮を窺わせる記載もある。詳細については、①ストラテジー、②ガバナンス、③リスク、④インシデントが起きた時、という各項目において、投資家は何を知りたいか、企業は何を開示すべきかを表にしてまとめている。

英国らしい特徴としては、開示すべき項目それぞれに、監査委員会（Audit Committee）は役割を果たしているか（開示が必要な点について、それを経営者に指摘しているか）が、挙げられている点である。まず、ビジネスモデルや戦略において価値を生み出す部分に、デジタルシステムやサイバーセキュリティがどの程度影響を与えているのか、あるいは、デジタル資産やデータ資産に対し、企業が戦略を持っているかを説明する重要性を述べ、実際の企業開示の例をあげている。ガバナンスで説明すべき点としては、体制や報告の仕組みだけでなくカルチャーとして従業員教育も上げている。そしてインシデントの報告については、NCSC が発行している EU GDPR の要件も含むガイダンスを紹介している。

FRC は「今やパーソナル・コンピュータ（PC）を使っていない会社は無い。サイバーリスクは全ての会社の問題といえる」と考えている。「レギュレーターの役割は、このリスクについて企業を目覚めさせる必要があるということだと思っている。仮にサイバー攻撃によってビジネスが止まったらと考えれば、これはビジネスリスクであることがわかる。そしてカルチャーであり、ガバナンスであり、ポリシーの問題だ。これらは投資家にとって必要な情報だと考えている。しかしその開示がボイラープレートの繰り返しにならないよう、FRC は現時点ではあまり具体的に開示項目を挙げることはしていない。ただこの情報を年次報告書に記載するよう求めている」と述べながら、一方で投資家側もこの情報に、

[8] Financial Reporting Council, “Digital Security Risk Disclosure.” （https://www.frc.org.uk/investors/frc-lab/digital-security-risk-disclosure#publications、2022 年 10 月 31 日閲覧）

[9] Financial Reporting Council, “FRC Lab Report: Digital Security Risk Disclosure,” August 2022.

まだあまり慣れていない、と言う。エンゲージメントで質問をし、企業が答えても何が正しい答えなのかわからない、というケースがあるそうだ。日本の投資家からも「サイバー対策を実施しているかと尋ねて、実施していると答えられたらその後どうしていいかわからない」という声がよく聞かれる。今後、業界レベルで教育機会の提供、たとえば投資判断を助けるデータや評価フレーム作成の取り組みも必要となってくるだろう。

VI PRIの共同エンゲージメントの試み

グローバルな投資家団体である PRI では、サイバーセキュリティに関するコレクティブ・エンゲージメントのプロジェクトを2017年から2019年の3年間実施した。これはひとつの「実験」で、FRC Lab の活動と似ているが、投資家が集まり、投資先企業のサイバーリスクへの対応力がどのようなガバナンスのもと行われているか、投資家が理解するための開示の提言を作成するためのプロジェクトだった[10]。

実験にはグローバルに 55 社の機関投資家が集い、53 社のグローバル企業に対しエンゲージメントを行った。日本の運用会社の参加はなかった。「当時GDPR等が発出され、金融機関はこの問題に力を入れて取り組む必要があると言われていた。しかし取り組みを通して認識したのは、結局今の時代はどの企業もこの問題に取り組まなければならない、ということだった」とPRIの担当者は感じている。実際、顧客情報を管理したり、決済システムと接続したりするのは小売業も皆同じである。そしてやはりコロナ禍が、どの業種企業にも等しく自社のビジネスのオンライン化を進めさせた。PRI の担当者は「まずは企業ごとに、その企業を知っている人をリーダーとし、イニシャル・レターを送った。最初はサイバーセキュリティのことを尋ねるには、会社との信頼関係が必要だった。企業の中には非常によく取り組みを行っているのに、全くそのことを開示していないこともあった。主な理由は『何かを開示したらサイバー攻撃のターゲットにされるのではないか』という不安があるからだ。しかし、開示がなければエンゲージメントにならない」と取り組みについて説明した。

そうして作られた提言が求めている開示とは、決して技術的なことではない。まずリーガル・コンプライアンス、企業はGDPRなどがデータプロテクションについて求める対応をどれだけ行っているか。次にポリシー、そして上級のマネジメントや取締役の説明責任、取締役のコミュニケーション、取締役は企業の状況を把握しているか。次にスキルとリソース、例えばどれくらい予算を割り当てているか、経験のあるスタッフを配置しているか、そしてトレーニング、評価、プロセスと手続きとなっている。

「この問題は投資家でも、すごく考える人と、そうでもない人がいる。やはり投資家も企業もある程度のサイバーの知識が必要だと思う」とPRIの担当者は感じている。そして前述の SEC へのコメントレターでは、「取り組みは歓迎するが、あまり細かい開示を義

[10] Principles for Responsible Investment, “Engaging on Cyber Security: Results of the PRI Collaborative Engagement 2017-2019,” April 22, 2020.

務化しない方が良い。一方で、経営者も従業員もどのように必要な知識やスキルを習得しているかについての情報は開示した方が良いと答えた」と述べた。

Ⅶ サイバーリスク、まずは取締役・投資家等関係者が理解を深めることの必要性

企業にとっても投資家にとっても、気候変動、人権と開示すべきこと・エンゲージメントすべきことが次から次へと押し寄せて「もう沢山だ」という思いはあるだろう。また経営者や投資家には、IT を理解し難いもの、専門家だけが扱うもの、とみている風潮があり、サイバーリスクに関する課題は、聞く方も答える方も躊躇する、それがここ数年までよく聞かれたことだ。しかしパンデミックの影響もあり、様々な産業がデジタル化、オンライン化といった DX（デジタルトランスフォーメーション）対応を求められており、取締役会にも新たなリスクの認識や対応、スキルが必要になった。そして GDPR などデータ管理の法的規制と、ロシアによるウクライナ侵攻以降、増えているサイバー攻撃によって、そのリスクもますます大きくなった。データやサイバーリスクについて必要な対応を行わなければ、法的リスクも高まっている。これらは投資家にとっては、攻撃をうけてサービスや製品の出荷を止める判断に迫られた時、また顧客やサプライヤーに与える影響を速やかに判断し、被害を最小限に食い止める対策を示さなければならなくなった時、経営者の対応力によって企業価値に与えるインパクトが異なってくるわけで、投資先選定やエンゲージメントで積極的に考慮する必要があるだろう。

日本の独立系運用会社でアクティブ運用を行うあるファンドマネージャーは、筆者に対し、「私は特にサイバーセキュリティについて聞こう、と思ったわけではないが、企業の事業について聞いていくと、自然とその話になることがある。私にとっては事業に関わる重要なコンテンツの 1 つであり、特別なものではない」と述べた。これが本来の在り方かもしれない。しかし、サイバーリスクについて考えるにあたっては、日々新たな攻撃や、リスクの可能性などが現れるため、それらの情報についていくだけでも困難だろう。「だからある程度の基礎的な、必要な情報開示のフレームをレギュレーターが示すことはありがたいのだと思う」と前述のファンドマネージャーは述べた。開示項目がただ用意されてもこの問題は簡単には解決しないだろう。まずは FRC や PRI の取り組みのように関係者で議論をし、リスクや必要な対応について共通の認識を持っていくこと、それが第一歩なのかもしれない。