サイバーセキュリティと企業価値
－投資家による評価と効果的な情報開示－

江夏　あかね

▌要　約▐

1. サイバーリスクは財務・非財務の観点から企業価値に影響を及ぼす可能性があり、企業によるサイバーセキュリティに関する情報開示がますます重要になっている。米国ではサイバーセキュリティ関連情報開示が米国証券取引委員会（SEC）により義務化されている。日本では 2024 年 3 月末時点で義務化されていないものの、政府により情報開示を推進する様々な施策も背景に、企業による取り組みが進んでいる。
2. 多くの投資家がサイバーリスクに着目し、環境・社会・ガバナンス（ESG）評価の要素の 1 つとして考慮したり、企業の経営陣とエンゲージメントを実施するケースも見られている。さらに、近年は、投資家による評価・判断を後押しすべく、金融庁による「投資家と企業の対話ガイドライン」、責任投資原則（PRI）や国際コーポレートガバナンスネットワーク（ICGN）といったグローバルな投資家団体による活動、議決権行使助言会社による議決権行使助言方針、ESG 評価機関や信用格付会社による評価、等の動きも見られている。
3. 企業が効果的にサイバーセキュリティ関連情報開示を行うための主な論点としては、（1）読み手（投資家等）が注目する論点への意識、（2）企業価値維持・保全のツールとしての位置づけ、（3）国内外における当局の動向の注視、が挙げられる。特に、読み手である各ステークホルダーが着目する論点を意識した情報開示が円滑な企業経営の一助になり得る。また、投資家に対しては、ガバナンスの論点（経営陣のコミットメント、監督体制等）を中心に企業価値に影響を及ぼす可能性がある要素をわかりやすく示すことが大切である。

野村資本市場研究所　関連論文等

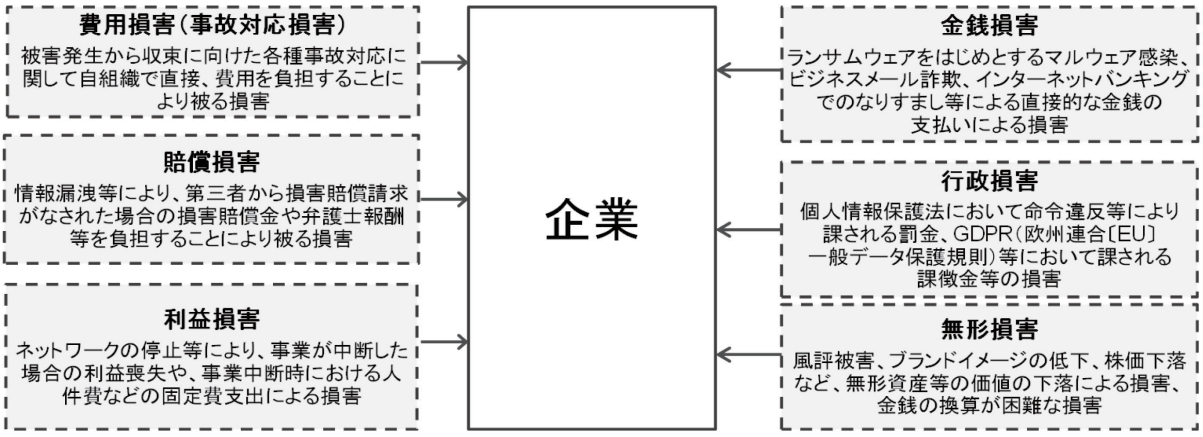
・江夏あかね「機関投資家から見たサイバーセキュリティ―サステナブルな情報化社会実現に向けた論点整理―」『野村サステナビリティクォータリー』第 3 巻第 4 号（2022 年秋号）。
・板津直孝「サイバーセキュリティに関わる SEC の開示規則案―広範囲に及ぶインシデントの懸念と情報開示―」『野村サステナビリティクォータリー』第 4 巻第 2 号（2023 年春号）。
・今川玄「サイバーリスクと信用格付―警戒強める格付会社、攻撃前でも格下げの可能性―」『野村サステナビリティクォータリー』第 3 巻第 3 号（2022 年夏号）。

Ⅰ 企業価値に影響を及ぼし得るサイバーリスクと情報開示

デジタル化の進展や地政学リスクが顕在化する中で、サイバー攻撃被害を受ける企業が増えている。サイバー攻撃は、企業にとって、事故対応や賠償等を通じた財務面への影響のみならず、風評被害等を通じて非財務面にも影響を及ぼし得る（図表 1 参照）。その意味で、サイバーリスクへの対応は、企業価値を維持・保全する上で不可欠なものである。そして、サイバーセキュリティに関する情報開示は、投資家による企業評価の観点のみならず、取引先等も含めたステークホルダーからの信認を得る上でますます重要になっている。その一方で、情報が攻撃者に対するヒントにもなりかねないため、適切な開示対応が求められる。このような中、各国政府は企業等のサイバーセキュリティ関連情報開示に対して関与・支援している。

本稿では、日米におけるサイバーセキュリティ関連情報開示の状況を概観した上で、投資家が近年、サイバーセキュリティをどのように投資判断要素としているかを紹介する。その上で、企業にとって効果的な情報開示のための論点を考察する。

図表 1　サイバー攻撃による企業に発生し得る主な損害の種類



（出所）日本ネットワークセキュリティ協会「インシデント損害額調査レポート　第 2 版」2023 年 2 月 9 日、より野村資本市場研究所作成

Ⅱ　日米におけるサイバーセキュリティ関連情報開示

以下では、企業によるサイバーセキュリティ関連情報開示に対する日米の状況を概観する。2024 年 3 月末時点で、米国では企業による情報開示が米国証券取引委員会（SEC）により義務化されているが、日本では義務化されていない。

１．日本

日本では、「企業内容等の開示に関する内閣府令」（内閣府令）が 2019 年 1 月に改正され、有価証券報告書における「事業等のリスク」に関する情報の充実が求められた[1]。その後、金融庁は 2019 年 3 月、「記述情報の開示に関する原則」を公表した[2]。同庁では同時に、原則に対応する形で各社の開示の良いポイントを示した「記述情報の開示の好事例集」を公表し始め、年度毎に更新をしている[3]。同事例集には、情報セキュリティ／サイバーセキュリティ関連の開示例も含まれている[4]。

一方、総務省でも「企業内容等の開示に関する内閣府令」の改正を受けて、サイバーセキュリティ対策の情報開示を促す方策を検討し、2019 年 6 月に「サイバーセキュリティ対策情報開示の手引き」を公表している[5]。同書は、対策の必要性、情報開示の意義や手段に加え、企業における情報開示の在り方を示している。具体的には、経済産業省と独立行政法人情報処理推進機構（IPA）による「サイバーセキュリティ経営ガイドライン Ver 2.0」で掲げられたサイバーセキュリティ経営の重要 10 項目[6]に基本的に沿った対策の実施状況に関する開示の説明のほか、5 つの開示のポイント（目的適合性、表現真正性、比較可能性、理解容易性、適時公表性）を挙げている。

さらに、2023 年 1 月 31 日付内閣府令等の改正により、「サステナビリティに関する考え方及び取組」が有価証券報告書に示すことが求められるようになった。金融庁は、サステナビリティ情報には、サイバーセキュリティ等に関する事項が含まれ得ると示した上で、

1　金融庁「『企業内容等の開示に関する内閣府令』の改正案に対するパブリックコメントの結果等について」2019 年 1 月 31 日。

2　同原則において、事業等のリスクに関して法令上記載が求められている事項として、（1）「企業の財政状態、経営成績及びキャッシュ・フローの状況等に重要な影響を与える可能性があると経営者が認識している主要なリスクについて、当該リスクが顕在化する可能性の程度や時期、当該リスクが顕在化した場合に経営成績等の状況に与える影響の内容、当該リスクへの対応策を記載するなど、具体的に記載すること」、（2）「開示に当たっては、リスクの重要性や経営方針・経営戦略等との関連性の程度を考慮して、分かりやすく記載すること」、が求められていると記された（金融庁「記述情報の開示に関する原則」2019 年 3 月 19 日）。

3　金融庁「『記述情報の開示に関する原則』及び『記述情報の開示の好事例集』の公表について」2019 年 3 月 19 日。

4　2023 年 12 月に公表された事例集では、（1）情報セキュリティの事例として伊藤忠テクノソリューションズ及び三井物産、（2）サイバーセキュリティの事例としてジェイテクト及び阿波銀行、を取り上げている（金融庁「記述情報の開示の好事例集 2023」2023 年 12 月 27 日）。

5　総務省サイバーセキュリティ統括官「サイバーセキュリティ対策情報開示の手引き」2019 年 6 月。

6　10 項目は、（1）サイバーセキュリティ対応方針策定、（2）経営層によるリスク管理体制の構築、（3）資源（予算、人員等）の確保、（4）リスクの把握と対応計画策定、（5）保護対策（防御・検知・分析）の実施、（6）PDCA の実施、（7）緊急対応体制の整備、（8）復旧体制の整備、（9）取引先・委託先やグループ単位のサイバーセキュリティ対策、（10）情報共有活動への参加（総務省サイバーセキュリティ統括官「サイバーセキュリティ対策情報開示の手引き」2019 年 6 月）。

「ガバナンス」と「リスク管理」は、すべての企業において開示が求められ、「戦略」と「指標及び目標」は、企業において重要性を判断して開示することが求められると説明している[7]。

このように、日本では、企業におけるサイバーセキュリティ情報開示は義務化されていないものの、政府により情報開示を推進する様々な施策が展開されている。このような背景の下、企業によるサイバーセキュリティ関連情報リスクの開示は浸透してきており、情報技術（IT）業界団体の日本IT団体連盟が2023年に実施した調査によると、東京証券取引所のプライム上場企業の有価証券報告書に関して、セキュリティに関するリスク事項を公開している企業は全体の93%に上っている（図表2参照）。日本では開示が義務化されていないこともあり、内容や質についてはそれぞれの会社で異なる傾向があるとみられる[8]。ただ、少なくとも大部分のプライム上場企業がサイバーリスク等について情報開示していることは、サイバーリスクが経営に及ぼす可能性について認識が進んでいることを示唆していると言える。

図表2　東京証券取引所プライム上場企業の情報開示動向

調査年（n=企業数）	有価証券報告書		コーポレートガバナンス報告書	
	記載社数	記載率	記載社数	記載率
2023（n=1,660）	1,543	93%	789	48%
2022（n=1,837）	1,712	93%	826	45%
2021（n=2,183）	1,773	81%	909	42%
2020（n=2,176）	1,603	74%	873	42%

（注）　1. 検索条件：〔上場市場 ： 東証一部 OR 東証プライム〕、〔キーワード：「システムリスク OR 情報セキュリティ OR サイバーセキュリティ OR 個人情報 OR プライバシーOR サイバー攻撃 OR 不正アクセス」を含む〕。
2. 2021年以前は東証一部。

（出所）日本IT団体連盟 サイバーセキュリティ委員会 企業評価分科会「サイバーインデックス企業調査2023」2023年12月、より野村資本市場研究所作成

２．米国

米国では、SECが2010年代以降、サイバーセキュリティ関連情報開示に関する取り組みを強化してきた経緯がある[9]。具体的には、（1）サイバーセキュリティリスク及びサイバーインシデントに関する開示のあり方に関するガイダンス[10]を公表（2011年10月）、（2）同ガイダンスの拡張、強化を目的に、解釈指針[11]を公表（2018年2月）、（3）エン

7　金融庁「記述情報の開示に関する原則（別添）－サステナビリティ情報の開示について―」2022年11月7日。
8　加藤・豊田（2023）には、製薬企業が作成した有価証券報告書（2018～2022年）における情報セキュリティに関する開示状況の分析結果がまとめられている（加藤晃・豊田雄彦「製薬企業のリスク情報開示―情報セキュリティ―」『国際医薬品情報』第1224号、国際商業出版、2023年4月24日）。
9　詳細は、江夏あかね「機関投資家から見たサイバーセキュリティ―サステナブルな情報化社会実現に向けた論点整理―」『野村サステナビリティクォータリー』第3巻第4号（2022年秋号）、を参照されたい。
10　U.S. Securities and Exchange Commission, “CF Disclosure Guidance: Topic No.2 Cybersecurity,” October 13, 2011.
11　U.S. Securities and Exchange Commission, “Commission Statement and Guidance on Public Company Cybersecurity Disclosures,” February 26, 2018.

フォースメント（民事制裁金）を実施（2021 年～）、等が挙げられる。

このような経緯もあり、SEC は 2023 年 7 月、上場会社のサイバーセキュリティに関する情報開示規則を採択した[12]（図表 3 参照）。同規則は、上場会社のサイバーリスク管理、戦略、ガバナンス、サイバーインシデントに関する開示を強化・標準化し、社会全体のサイバーセキュリティの水準の向上を図ることが目的で、2023 年 12 月 15 日以降に適用されている。

本規則は、米国企業のみならず、米国に上場している米国外の企業（FPI）も適用範囲となっており、ニューヨーク証券取引所とナスダックに上場する 5,667 社[13]がこの規則を遵守する必要がある。そのため、米国に上場する日本企業も対応に迫られている状況となっている。

図表 3　SEC による上場会社のサイバーセキュリティに関する情報開示規則の概要

年次報告 Form 10-K（外国民間発行者は 20-F） **2023 年 12 月 15 日以降適用**
・ サイバーセキュリティに関するリスクマネジメント及びストラテジーの開示 ✓ サイバーセキュリティの脅威による重大なリスクの評価、特定及び管理のためのプロセスがある場合、当該プロセスについて、合理的な投資家が理解するために十分かつ詳細な説明が必要 ✓ 以前発生したサイバーインシデントの結果を含めサイバーセキュリティの脅威に起因するリスクが、当該企業に重大な影響を及ぼしたか、または重大な影響を与える可能性が合理的に高いか否か、該当する場合にはどのように該当するか、について説明が必要
・ サイバーセキュリティに関するガバナンスの開示 ✓ サイバーセキュリティの脅威に関するリスクに対する取締役会による監視について説明が必要。加えて、監督を取締役会または下位の委員会が担当している場合は、当該委員会を特定するとともに、当該委員会に対して当該リスクが通知されるプロセスの説明が必要 ✓ サイバーセキュリティの脅威による登録会社の重大なリスクに対する評価及び管理について、経営陣の役割を説明することが必要
重要事項報告 Form 8-K（外国民間発行者は 6-K） **2023 年 12 月 18 日以降適用**
・ 開示のタイミング ✓ サイバーセキュリティインシデントが重大であると登録会社が判断した場合、4 営業日以内に Form 8-K を提出しなければならない。登録会社は、当該インシデント発見後、重要性に関する決定を不当な遅延なしに行わないとならない ✓ ただし、米国司法長官が当該サイバーセキュリティインシデントの臨時開示が国家安全保障または公共の安全に重大なリスクをもたらすと判断し、そのような決定を書面で SEC に通知した場合、原則として、Form 8-K の提出を最大 30 日間遅らせることが可能
・ 開示の内容 ✓ インシデントの性質、範囲及びタイミングの重要部分 ✓ 登録会社において生じるまたは生じる可能性のある重大な影響（財政状態及び経営成績を含む） ✓ ただし、Form 8-K の提出の時点で、当該情報が未確定または利用できない場合、当該情報が確定または利用可能となったのち、不当な遅延なしに、4 営業日以内に訂正報告書を提出する旨の開示を行うことが認められている

（出所）U.S. Securities and Exchange Commission, “Factsheet: Public Company Cybersecurity Disclosures; Final Rules,” July 26, 2023、各種資料、より野村資本市場研究所作成

[12] 詳細は、板津直孝「サイバーセキュリティに関わる SEC の開示規則案―広範囲に及ぶインシデントの懸念と情報開示―」『野村サステナビリティクォータリー』第 4 巻第 2 号（2023 年春号）、を参照されたい。

[13] 2024 年 2 月時点。国際取引所連合（WFE）の統計に基づく（World Federation of Exchanges, “Market Statistics-April 2024”）。

Ⅲ 投資家によるサイバーセキュリティ要素の評価・判断

金融資本市場では近年、サイバーリスクが顕在化した企業への株価への影響が観察されている（図表 4 参照）。サイバーリスクは、企業価値に様々な形で影響を及ぼし得る上、規制強化の動きも後押しをする形で、多くの投資家が注目している。

本章では、日本 IT 団体連盟が 2023 年 12 月に公表した日米の機関投資家を対象に実施した調査結果を概観するとともに、投資家による取組事例や、投資家による評価・判断を後押しする主な動向を紹介する。

図表 4　サイバーリスクが顕在化した企業の株価への影響に関する主な分析／事例

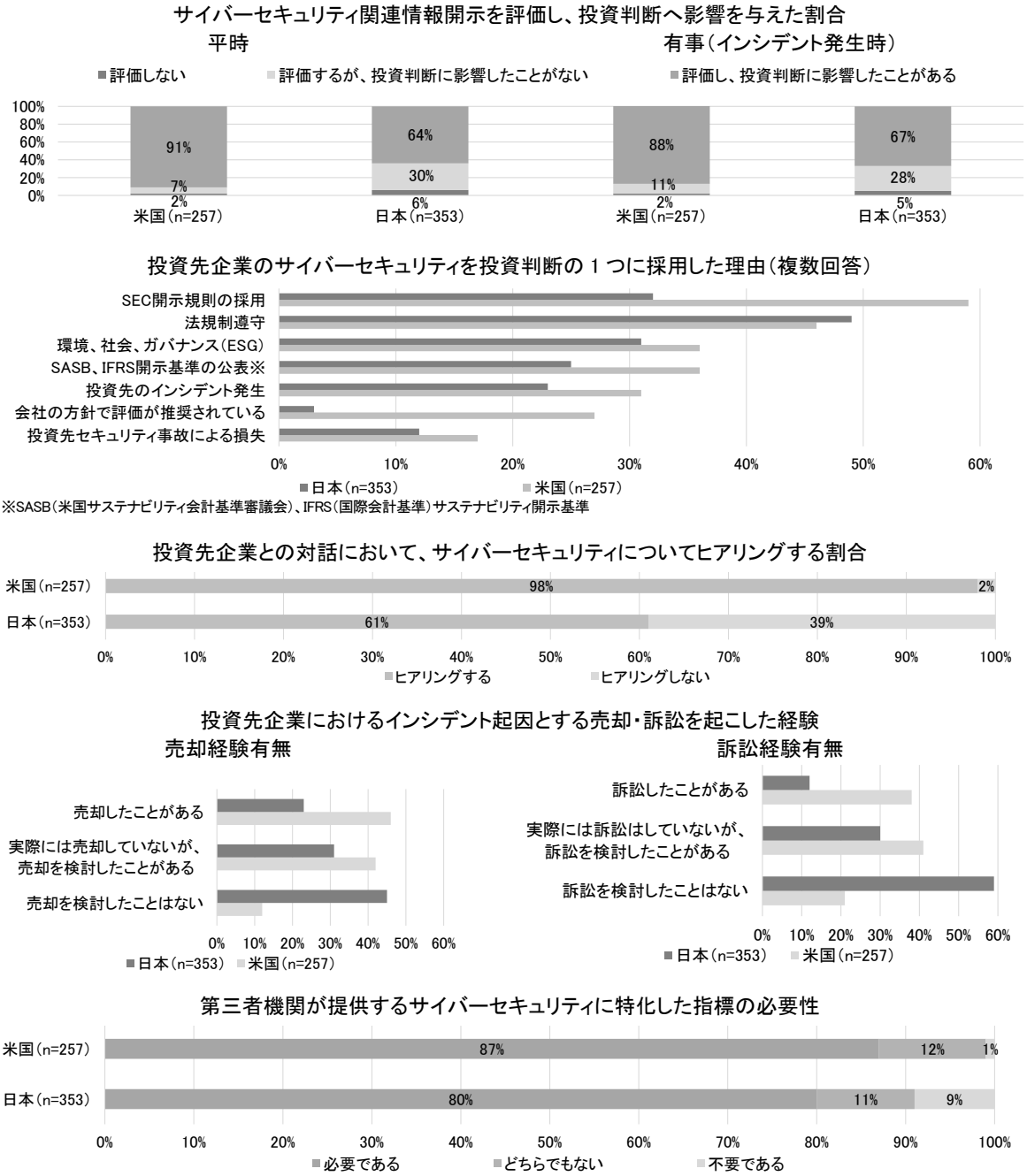
- **ニューヨーク証券取引所の上場企業のうち、データ侵害にあった企業の株価は平均で約 3.5%下落し、市場平均を下回る傾向（英国の調査会社 コンパリテックによる調査）**
- **日本国内で情報流出等の適時開示を行った企業の株価は 50 日後に平均約 6.3%下落（日本サイバーセキュリティ・イノベーション委員会〔JCIC〕の分析）**
- **株価下落のみならず、サイバー攻撃を受けた企業の株価が適切な事後対応等を背景に一旦下落したものの、その後回復、上昇（ノルウェーのアルミニウム製造・エネルギー大手ノルスクハイドロ）**

（出所）Comparitech, “How Data Breaches Affect Stock Market Share Prices,” February 9, 2021、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、鈴木乾也「運命を変える―サイバー攻撃と企業の命運―」『週刊 経団連タイムス』第 3466 号、一般社団法人日本経済団体連合会、2020 年 9 月 3 日、より野村資本市場研究所作成

１．日米投資家による取組事例

日本 IT 団体連盟による日米の機関投資家を対象に実施した調査結果では、米国投資家の約 9 割、日本の投資家の 6 割超がサイバーセキュリティ関連情報開示に基づき評価し、投資判断に影響したことがあるとの回答を得たことなどが紹介されている（図表 5 参照）。米国のほうが影響したと答えた投資家の割合が多かった背景としては、SEC による開示規制の採用に加え、実際に投資先企業のサイバーインシデントを起因した売却を経験した投資家の割合が多いことなどが背景とみられる。

図表 5　日米の機関投資家のサイバーセキュリティ関連情報開示に関する意識調査結果



（注）　日本 IT 団体連盟が 2023 年に日米投資家（日本：353 人、米国：257 人）に対して実施したサイバーセキュリティ情報開示に関する意識調査の結果。

（出所）日本 IT 団体連盟 サイバーセキュリティ委員会 企業評価分科会「サイバーインデックス企業調査 2023」2023 年 12 月、より野村資本市場研究所作成

2．投資家による取組事例

投資家による取組事例では、（1）投資先企業の環境・社会・ガバナンス（ESG）評価の要素の 1 つとして考慮（野村アセットマネジメント〔NAM〕）、（2）企業の経営陣との対話（ブラックロック）、を取り上げる。

１）事例 1：ESG 評価の要素の 1 つとして考慮（NAM）

NAM では、債券の ESG 評価において、持続可能性に加え、強靭性が重要との問題意識の下、定量評価モデルにサイバーセキュリティに関する要素を組み込んでいる[14]。具体的には、同社独自の業界別マテリアリティとサイバーセキュリティ・パフォーマンスなどのデータを統合した結果は、企業におけるガバナンス・リスクの一要素として、体系的に ESG 定量評価モデルに加味される。同モデルをベースとした最終的な発行体別のスコアは、各種のグローバル・クレジット戦略策定に活用されている。なお、同社では、サイバーセキュリティ・パフォーマンスに関するデータなどを発行体とのエンゲージメント活動にも生かすことを目指している。

２）事例 2：企業の経営陣とのエンゲージメント（ブラックロック）

ブラックロックでは、データプライバシーとセキュリティを重要リスクとみなし、経営陣とのエンゲージメントを実施している。具体的には、企業の経営陣と対話する際に、（1）重要性（マテリアリティ）の評価、（2）取締役会の監視とリソース、（3）顧客の同意とデータ処理、（4）サードパーティの管理、の要素に焦点を置いている（図表 6 参照）。

図表 6　データプライバシー及びセキュリティに関するエンゲージメントの論点（ブラックロック）

項目	内容
重要性（マテリアリティ）の評価	・企業が収集するデータの量、種類、機密性など、ビジネスモデルに基づいて、企業がデータプライバシーとセキュリティのリスクにどのように晒されているか（ユーザー対顧客、個人対企業、プライベートとパブリック、機密と非機密） ・プライバシー、データ、サイバーセキュリティに関連して、具体的に企業の財務上にどのような影響があるのか ・関連する規制対応は行われているか、または想定されているか。複数の管轄区域で営業／上場している企業の場合、複数のデータセキュリティ／プライバシー規制をどのように遵守しているか
取締役会の監視とリソース	・取締役会は、重要なプライバシー及びデータセキュリティリスクの包括的な監視と理解をどの程度効果的に維持しているか ・これらの事項は、企業の事業継続計画にどのように織り込まれているか ・サイバーリスクマネジメントにはどのようなリソースが充てられているか。また、これらがビジネスに適していると考えられる理由は何か。従業員研修に関する指標は、社内外のステークホルダーと広く共有されているか ・企業は業界のセキュリティフレームワークを使用しているか。また、そのフレームワークに対して自社をどのように評価しているか ・企業は、データセキュリティ侵害から保護するために、技術的及び組織的なセキュリティ問題をどのように特定し、対処しているか
顧客の同意とデータ処理	・顧客の信頼を維持しながら、収益機会のために顧客の個人情報を収集し、その使用と法的、規制上、及び評判上のリスクとのバランスをとるために、どのようなデータが適切かをどのように判断しているか ・顧客が自分のデータに関連する重要性とリスクをより意識するようになるにつれて、長期的に顧客が自分のデータを共有する意思が変化する可能性をどのように考慮しているか ・収集したデータが定められた目的のために使用され、逸脱がないことをどのように保証しているか ・企業がターゲティング目的でユーザーの個人情報にアルゴリズムを適用している場合、これらのアルゴリズムを（経営レベルと取締役会レベルの両方で）検証して、民族、購買力、その他の人口統計学的カテゴリに基づく、センシティブと見なされる可能性のある差別がないことを確認するためのポリシーはどのようなものか
サードパーティの管理	・データを第三者に転送する場合、企業は、転送中にデータの取り扱いが責任ある方法で行われ、企業の保護ポリシーに沿っていることをどのように保証しているか

（出所）BlackRock, “Our Approach to Data Privacy and Security: Investment Stewardship,” July 2022、より野村資本市場研究所作成

[14] 野村アセットマネジメント「責任投資レポート 2021」。

３．投資家による評価・判断を後押しする主な動向

投資家による評価・判断を後押しする主な動向については、（1）金融庁による「投資家と企業の対話ガイドライン」、（2）グローバルな投資家団体による活動、（3）議決権行使助言会社による方針、（4）ESG評価機関による評価、（5）信用格付会社による評価、を取り上げる。

１）金融庁による「投資家と企業の対話ガイドライン」における言及

日本では、2021年6月に改訂されたコーポレートガバナンス・コード自体に、用語としてのサイバーセキュリティ／サイバーリスクは含まれていない。ただし、スチュワードシップ・コード及びコーポレートガバナンス・コードの附属文書として位置付けられる「投資家と企業の対話ガイドライン」（金融庁、2021年6月改訂版）において、サイバーセキュリティ対応の必要性に関する言及がある（図表7参照）。

図表7　「投資家と企業の対話ガイドライン」におけるサイバーセキュリティに関する言及（抜粋）

1. 経営環境の変化に対応した経営判断

（略）

1－3. ESG や SDGs に対する社会的要請・関心の高まりやデジタルトランスフォーメーションの進展、サイバーセキュリティ対応の必要性、サプライチェーン全体での公正・適正な取引や国際的な経済安全保障を巡る環境変化への対応の必要性等の事業を取り巻く環境の変化が、経営戦略・経営計画等において適切に反映されているか。また、例えば、取締役会の下または経営陣の側に、サステナビリティに関する委員会を設置するなど、サステナビリティに関する取組みを全社的に検討・推進するための枠組みを整備しているか。

（略）

（注）　下線は野村資本市場研究所による。
（出所）金融庁「投資家と企業の対話ガイドライン」2021年6月11日、より野村資本市場研究所作成

ただし、20ヵ国・地域（G20）及び経済協力開発機構（OECD）が2023年9月に改訂した「G20／OECD コーポレートガバナンス原則」では、サイバーリスクは取締役会が対処すべきリスクとして特に重要であることが追記された[15]。過去の経緯に鑑みると、将来的にコーポレートガバナンス・コード自体にサイバーに関する言及が示される可能性もあり得ると考えられる[16]。

[15] 原則Ⅴ・D・2注釈（経済協力開発機構「G20／OECD コーポレートガバナンス原則2023」2024年、深見健太・金江麻耶「G20/OECD コーポレート・ガバナンス原則の改訂ポイントー約10年ぶりの改訂となった企業統治分野における唯一の国際基準ー」『金融財政事情』第74巻第38号、金融財政事情研究会、2023年10月）。

[16] 2015年6月に制定されたコーポレートガバナンス・コードの検討に当たって、金融庁と東京証券取引所が共同開催した有識者会議では、「『日本再興戦略』改訂2014」に基づきOECD原則の内容も踏まえた議論が行われ、原案が取りまとめられた経緯がある（OECD日本政府代表部「『コーポレートガバナンス・コード』策定に当たっての日本政府とOECDとの連携」）。

２）グローバルな投資家団体による活動：PRI と ICGN[17]

近年は、グローバルな投資家団体がサイバーセキュリティに関して各種活動を行っている。例えば、責任投資原則（PRI）は、（1）企業がサイバーセキュリティの問題をどの程度真剣に受け止めているかに関する調査結果[18]を発表（2018 年 7 月）、（2）機関投資家との協働エンゲージメントプロジェクト[19]を実施（2017～2019 年）、している。PRI は同プロジェクトの結果を踏まえ、エンゲージメント及び開示の期待に関する推奨事項及びそれに付随する投資家による企業への潜在的な質問を提示している[20]。

一方、国際コーポレートガバナンスネットワーク（ICGN）は、（1）投資家がサイバーリスクの監視及びサイバー関連リスクに関して企業の取締役会とエンゲージメントできるようにすることを目的とした視点レポート[21]を公表、（2）グローバル・ガバナンス原則（2021 年版）[22]においてサイバーリスク等について言及、といった取り組みをしている。特に、視点レポートでは、サイバーリスク等に関するエンゲージメントにおける実用的な質問として、（1）投資家がサイバーリスク監視に関連して取締役会に尋ねることができるもの、（2）投資家が取締役会に対して、経営陣にサイバー関連リスクの範囲を超えて尋ねるように促すためのもの、を提示している。

３）議決権行使助言会社による方針：ガバナンス体制の一環で言及

米議決権行使助言会社のグラスルイスは、2024 年議決権行使助言方針にて、株主の利益につながるガバナンス体制の一項目として、サイバーリスクの監督に関する方針を提示している（図表 8 参照）。サイバー攻撃による重大な損害が生じた場合に開示内容や監督が不十分と考えられた場合、取締役に対して反対助言を行う場合があると言及している。

図表 8　グラスルイスによるサイバーリスクの監督に関する方針の言及（抜粋）

サイバー関連の潜在的な不利益を考慮すると、サイバーリスクは全ての企業にとって重大な懸念事項であると考える。したがって、企業はこれらのリスクを可能な限り検証し、軽減することが重要であると考える。このような観点から、全ての企業に対して、サイバーセキュリティに関わる事項を監督する取締役会の役割について、明確な開示を行うことを推奨する。さらに、急速に変化を続けるこの重要な課題について、企業が取締役に対して、どのように熟知させているかを開示することは、企業がこの問題について真剣に取り組んでいるということを株主が理解する一助になると考える。

原則として、サイバー関連の問題における企業の監督や開示に基づいた助言判断は行わない。ただし、サイバー攻撃によって株主に重大な損害が生じた場合、この点に関する企業の情報開示を精査し、その開示内容や監督が不十分であると考えられる場合には、しかるべき取締役に対して反対助言を行う場合がある。

（出所）Glass Lewis, “2024 Benchmark Policy Guidelines,” 2024、より野村資本市場研究所作成

17 前掲注 9 参照。

18 Principle for Responsible Investment, “Stepping up Governance on Cyber Security,” 2018; Principle for Responsible Investment, “PRI Steps up Engagement on Cyber Security,” July 25, 2018.

19 Principle for Responsible Investment, “Engaging on Cyber Security: Results of the PRI Collaborative Engagement 2017-2019,” 2020.

20 前掲注 19 参照。

21 International Corporate Governance Network, “ICGN Viewpoint: Cyber Risk,” May 2016.

22 International Corporate Governance Network, “ICGN Global Governance Principles,” 2021.

４）ESG 評価機関による評価

世界の代表的な ESG 評価機関では、サイバーセキュリティ関連の指標を「G」（ガバナンス）に分類するケースが多いが、一部の機関では顧客・製品に関するプライバシー・情報セキュリティという観点から、「S」（社会）に分類している[23]。各評価機関による評価手法は異なるが、情報セキュリティ対策等の共通項目もある（図表 9 参照）。そして、複数の評価機関は、各産業のサイバーリスクの影響度に応じてサイバー関連の項目の総合スコアへの影響度を重みづけとして設定しており、例えば IT、金融等では重みづけが高くなる等の仕組みを導入している[24]。

図表 9　S&P グローバルによるコーポレートサステナビリティ評価（CSA）による評価項目

項目	内容
IT セキュリティ／サイバーセキュリティ・ガバナンス	サイバーセキュリティ戦略における取締役会の責任
	サイバーセキュリティを監督するための経営層の責任
IT セキュリティ／サイバーセキュリティ対策	情報セキュリティ／サイバーセキュリティに関する方針
	疑わしい事例があった場合のエスカレーションプロセス
	従業員の業績評価への反映
IT セキュリティ／サイバーセキュリティ・プロセスとインフラ	事業継続計画
	外部認証取得
	脆弱性分析
IT セキュリティ／サイバーセキュリティ侵害	インシデントと違反の件数
	保険

（出所）田原英俊「ESG 情報開示とサイバーセキュリティ」2023 年 3 月 17 日、より野村資本市場研究所作成

５）信用格付会社による評価[25]

国際的な信用格付会社は近年、サイバーリスクに関する多数の見解を公表している。そして、例えば、2017 年 9 月の米消費者信用大手エクスファクスへのサイバー攻撃に際しては、S&P グローバルやムーディーズは格付アクションを講じている[26]。

さらに、S&P グローバルが 2022 年 3 月（日本語版は同年 4 月）に公表した、サイバーリスクが事業会社の信用力分析に及ぼす影響に関するレポート[27]には、金融市場で注目が集まったようだ。同レポートでは、（1）サイバーリスクの準備状況は、

---

23 クオンクロップ「乱立する ESG 指標：情報セキュリティの見られ方」2021 年 10 月 15 日。

24 PwC「なぜ ESG 格付けにおいてサイバーセキュリティの重要性が高まっているのか」2022 年 4 月 8 日。

25 詳細は、今川玄「サイバーリスクと信用格付－警戒強める格付会社、攻撃前でも格下げの可能性－」『野村サステナビリティクォータリー』第 3 巻第 3 号（2022 年夏号）、江夏あかね「機関投資家から見たサイバーセキュリティーサステナブルな情報化社会実現に向けた論点整理－」『野村サステナビリティクォータリー』第 3 巻第 4 号（2022 年秋号）、を参照されたい。

26 エクイファクスへのサイバー攻撃では、1.4 億人超の個人情報が流出し、2017 年 9 月に訴訟・政府による調査に関連する費用の影響の大きさを踏まえて、格付けは BBB＋で据え置いたものの、アウトルックをネガティブに変更した。その後、情報流出対策の投資や事業関連投資による収益の圧迫やレバレッジの悪化により、2019 年 3 月に格付けを BBB に引き下げ、アウトルックをネガティブとした。ムーディーズは 2019 年 5 月、同社のシニア無担保債格付け（Baa1）を据え置いた上で、格付見通しを安定的からネガティブに変更している（S&P グローバル「日本の事業会社セクター：信用力の安定化を阻む新たなリスク」2022 年 4 月 20 日、Moody's, "Moody's Affirms Equifax Sr Uns at Baa1, Revise Outlook to Negative from Stable," May 17, 2019）。

27 S&P Global, "How Cyber Risk Affects Credit Analysis for Global Corporate Issuers," March 30, 2022、S&P グローバル「サイバーリスクは事業会社の信用力分析にどのように影響を与えるのか」2022 年 4 月 14 日。

同社の分析でますます重要かつ新たなリスク要因となっている、（2）サイバーリスクを軽減する戦略を自社のガバナンス体制及びリスク管理に組み込んでいない企業は、サイバー攻撃よりも前に格付けへの下方圧力に直面する可能性がある、と指摘している。

Ⅳ 企業による効果的な情報開示のための論点

本稿では、サイバーリスクが財務・非財務の観点から企業価値に影響を及ぼす可能性があり、企業によるサイバーセキュリティに関する情報開示がますます重要になっていることを概観した。米国ではサイバーセキュリティ関連情報開示が SEC により義務化されている。日本では 2024 年 3 月末時点で義務化されていないものの、政府により情報開示を推進する様々な施策も背景に、企業による取り組みが進んでいる。情報開示をする企業が増えている中で、今後は内容の拡充や質の向上を意識する企業が増えると想定される。

そして、多くの投資家がサイバーリスクに着目し、ESG 評価の要素の 1 つとして考慮したり、企業の経営陣とエンゲージメントを実施したりするケースも見られている。さらに、近年は、金融庁による「投資家と企業の対話ガイドライン」やグローバルな投資家団体による活動を始めとした投資家による評価・判断を後押しする動きもある。

このような状況を踏まえると、企業が効果的にサイバーセキュリティ関連情報開示を行うための主な論点としては、（1）読み手（投資家等）が注目する論点への意識、（2）企業価値維持・保全のツールとしての位置づけ、（3）国内外における当局の動向の注視、が挙げられる。

1 点目について、企業によるサイバーセキュリティ関連情報開示の読み手は、投資家、取引先、金融機関等、多岐にわたるステークホルダーである。各ステークホルダーが着目する論点を意識した情報開示が円滑な企業経営の一助になり得る。特に、投資家に対しては、企業価値に影響を及ぼす可能性がある要素、特に財務・非財務面で最も影響を及ぼす可能性のあるガバナンスの論点（経営陣のコミットメント、監督体制等）を中心にわかりやすく示すことがポイントと言える。

2 点目について、サイバーセキュリティ関連情報開示は、自社のサイバーセキュリティ対応を見つめ直し、価値の維持・保全に向けた取り組みを強化するプロセスと言える。情報開示は、ゴールである企業価値の維持・保全を達成するためのチェックポイントともいえる。さらに、投資家等のステークホルダーとの対話のベースとなり、客観的な視点も踏まえてさらなるサイバーセキュリティ対応の強化に向けた有意義な意見を得られる可能性もある。

3 点目について、サイバーリスクには国境がないため、国内のみならず、国外における動きにも注目することが重要である。例えば、日本では 2024 年 3 月末時点でサイバーセキュリティ関連情報開示は義務化されていないが、将来の可能性も見据えて、米国等の海外の当局の動きを注視することも大切と言える。