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－

江夏　あかね

▌要　約▐

1. 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ており、サイバーセキュリティの重要性がますます高まっている。
2. 昨今のサイバーセキュリティ関連の動向を機関投資家の視点で整理すると、情報開示規制、コーポレートガバナンス・コード、環境・社会・ガバナンス（ESG）評価機関と信用格付会社の評価・見解、が主要な論点として挙げられる。グローバルな投資家団体においても、2010 年代頃から議論や取り組みが見られている。
3. 情報技術（IT）・デジタル化、デジタル・トランスフォーメーション（DX）の進展、サイバー犯罪・攻撃の複雑化・巧妙化・甚大化等を踏まえると、サイバーセキュリティ関連課題の対応に終わりを定めるのは困難と言える。そのため、サステナブルな情報化社会の実現に向け、企業、投資家、政府・規制当局を始めとした多数のステークホルダーが一丸となってサイバー関連課題に関する対応を続ける必要がある。
4. 投資家は、（1）サイバー関連の動向やリスク、潜在的な価値をしっかり見極める眼を養うこと、その上で、（2）エンゲージメントを通じて企業に適切なサイバーセキュリティ関連対応を促すこと、ができる。そして、このような取り組みを通じて、投資パフォーマンスの向上のみならず、社会全体のサイバーセキュリティ強化にもつながり得るため、大切な役割を果たすと考えられる。

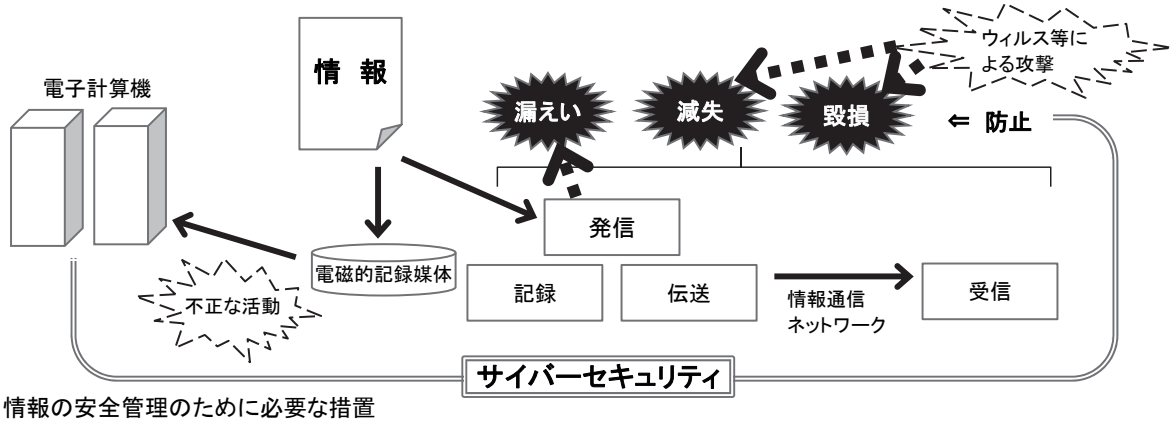
野村資本市場研究所　関連論文等

・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 情報化社会の中で重要性が増すサイバーセキュリティ

世界では、情報通信技術やサービスが 1990 年代終盤頃から急速に発展し、情報化社会、すなわち、情報の生産・収集・伝達・処理を中心として社会経済が発展していく社会[1]へと変貌を遂げている。その一方で、サイバー犯罪や攻撃が複雑化・巧妙化し、企業等に甚大な被害も及ぶとともに、社会経済全体に及ぼす影響が懸念されている[2]。そのような中、情報化社会の安全性、持続可能性を維持すべく、サイバーセキュリティの重要性がますます高まっている（図表 1 参照）。

図表 1　サイバーセキュリティ（イメージ）



・情報の安全管理のために必要な措置
・情報システム及び情報通信ネットワークの安全性及び信頼性確保のために必要な措置
（電磁的記録媒体を通じた電子計算機に対する不正な活動による被害防止のために必要な措置を含む）
・適切な維持管理

（出所）羽室英太郎『サイバーセキュリティ入門－図解×Q&A』慶應義塾大学出版会、2018 年、より野村資本市場研究所作成

サイバーセキュリティをめぐっては、主に「G」（ガバナンス）面を通じて、企業価値に影響を及ぼし得る要素との認識が広まりつつあり、金融資本市場に関連する分野でも近年、多面的な議論や取り組みが進展しつつある。しかしながら、昨今の新型コロナウイルス感染症問題により、テレワークやオンライン授業等、従来利活用が十分に進んでいなかった分野でもデジタル化が進んでいる。さらに、ウクライナ情勢等の地政学的緊張の高まりも背景としたサイバー犯罪や攻撃の甚大化の勢いに鑑みると、将来的にサイバーリスクが金融資本市場、そして投資家を予期せぬ形で脅かす事態にもなりかねないとも考えられる。

1　情報化社会には、様々な定義があるが、例えば、デジタル大辞泉では、「物や資本などにかわって知識や情報に価値が置かれ、情報の生産・収集・伝達・処理を中心として社会・経済が発展していく社会。情報社会」と定義している。（小学館『デジタル大辞泉』）

2　例えば、世界経済フォーラム（WEF）が 2022 年 1 月に公表した専門家メンバーに対するアンケート調査結果によると、発生の可能性が高いグローバルリスクの順位において、短期的（0～2 年）では 7 位、中期的（2～5 年）では 8 位にサイバーセキュリティ対策の失敗が上がっている。（World Economic Forum, “The Global Risks Report 2022 17th Edition,” 2022）

本稿では機関投資家の視点に立ってサイバーセキュリティを整理する。まずは定義や企業価値への影響を確認し、主要な論点として、情報開示規制、コーポレートガバナンス・コード、環境・社会・ガバナンス（ESG）評価機関と信用格付会社の評価・見解、グローバルな投資家団体による取り組みを概観し、今後の論点を考える。

Ⅱ　サイバーセキュリティの定義と企業価値への影響

本章では、サイバーセキュリティの定義を確認した上で、投資判断の材料となり得る要素としてサイバーをめぐる脅威と企業価値への影響を考察する。

１．サイバーセキュリティの定義及び特徴

サイバーセキュリティに関しては、様々な定義が存在するが、日本のサイバーセキュリティ基本法第 2 条に基づくと、データ、情報システム、情報通信ネットワークを安全に保つための対策を講じて、それを維持することを意味している[3]（図表 2 参照）。

図表 2　サイバーセキュリティに関する主な定義

定義主体	内容
サイバーセキュリティ基本法	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体〔以下「電磁的記録媒体」という。〕を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう（第 2 条）
経済産業省・独立行政法人情報処理推進機構	電子データの漏洩・改竄等や、期待されていた情報技術（IT）システムや制御システム等の機能が果たされないといった不具合が生じないようにすること
総務省	私たちがインターネットやコンピューターを安心して使い続けられるように、大切な情報が外部に漏れたり、ウイルスに感染してデータが壊されたり、普段使っているサービスが急に使えなくなったりしないように、必要な対策をすること（サイバーセキュリティ対策）
	情報に関して（1）機密性（ある情報へのアクセスを認められた人だけがその情報にアクセスできる状態）、（2）完全性（情報が破壊、改竄または消去されていない状態）、（3）可用性（情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態）、を確保すること
ISO／IEC TS27100：2020（サイバーセキュリティの概要を提供する規格）	サイバーセキュリティ：サイバーリスクから人々、社会、組織及び国々を守ること ・ サイバーリスク：サイバー空間内のエンティティの目的に対する不確かさの影響 ・ サイバー空間：ネットワーク、サービス、システム、人々、プロセス及び組織が相互接続されたデジタル環境にあって、デジタル環境上に存在するか、またはその中を横断するもの

（出所）経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 2.0」2017 年 11 月 16 日、総務省国民のためのサイバーセキュリティサイト「サイバーセキュリティって何？」、永宮直史 編著・特定非営利活動法人日本セキュリティ監査協会 著『ISO/IEC 27001・27002 拡張によるサイバーセキュリティ対策―ISO/IEC TS 27100：2020 の解説と ISMS 活用術―』日本規格協会、2022 年、より野村資本市場研究所作成

[3] 増島雅和・蔦大輔『事例に学ぶサイバーセキュリティ』経団連出版、2020 年。

サイバーセキュリティ基本法に基づくと、サイバーセキュリティの主な特徴として、（1）保護客体としての情報は、電磁的方式によりやり取りされるサーバや端末、記録媒体に保存されたデータに限定、（2）外部からのサイバー攻撃への対策のみならず、企業の従業員による機密性の高い情報の不正持ち出し、不正送金、天災や何らかの人為ミスによって企業の情報システムに障害が発生した場合にそれを迅速復旧するための措置等も含む、（3）サイバー攻撃はインターネットを通じたもののみならず、例えばUSBメモリ等の外部記録媒体を用いた物理的攻撃も含む、が挙げられる[4]。

他方、サイバーセキュリティの概要を提供する規格である「ISO／IEC TS27100：2020[5]」では、国や組織などの安定性と継続性の確保、財産の保全、人々の生命や健康の維持のために許容される水準以下にサイバーリスクを抑えることを目的として掲げている[6]。なお、同規格では、サイバーセキュリティと関連する概念である情報セキュリティとの関係も整理している。具体的には、情報セキュリティは情報そのものを対象としているのに対し、サイバーセキュリティは組織自身の財産等に係るリスクのみでなく、関連する組織や社会、人々を対象としていると示している。

２．サイバーをめぐる脅威と企業価値への影響

１）サイバーをめぐる脅威

サイバー攻撃は近年、多様化、高度化、巧妙化するとともに、攻撃対象は個別企業・組織のみならず、重要インフラ、政府等と広範に渡っている。そして、その被害は直接の攻撃対象のみならず、連鎖的に広がり、経済社会全体に及ぼす影響が甚大となり得る可能性が示唆されている。

例えば、総務省の情報通信白書では、サイバーセキュリティに関する問題が引き起こす経済的損失をめぐる複数の試算を紹介している[7]。同白書で取り上げられた米国のサイバーセキュリティ調査研究企業のサイバーセキュリティ・ベンチャーズでは2022年1月、世界の2021年のサイバー犯罪による損害額は6兆ドルとの試算とともに、今後5年間で毎年15%ずつ増加し、2025年には10.5兆ドルに達するとの見込みを示している[8]。同時に、サイバー犯罪は風評被害の恐れ等を背景に明らかになっていない部分が相当程度存在すると指摘している。

---

4 前掲脚注3を参照。

5 国際標準化機構（ISO）は、各国の代表的標準化機関から成る国際標準化機関で、電気・通信及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）に関する国際規格を作成している。国際電気標準会議（IEC）は、各国の代表的標準化機関から成る国際標準化機関であり、電気及び電子技術分野の国際規格を作成している。技術仕様書（TS）は、将来的に国際規格（IS）として合意される可能性がある文書と位置付けられるものである。「ISO/IEC TS27100：2020」は、ISOとIECが共同で策定したもので、「情報技術−サイバーセキュリティ−概要と概念」を提供する規格として、2020年12月に発行された。（日本産業標準調査会「ISO／IEC」、日本産業標準調査会「IEC規格の制定手順」、一般財団法人日本情報経済社会推進協会「ISO／IEC27000ファミリー規格について」2022年11月1日）

6 永宮直史 編著・特定非営利活動法人日本セキュリティ監査協会 著『ISO/IEC 27001・27002拡張によるサイバーセキュリティ対策―ISO/IEC TS 27100：2020の解説とISMS活用術―』日本規格協会、2022年。

7 総務省「令和元年版情報通信白書」2019年。

8 “2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics,” *Cybercrime Magazine*, January 19, 2022.

２）企業価値への影響

サイバーの脅威は、財務・非財務面を通じて企業価値に影響を及ぼし得る。例えば、米国証券取引委員会（SEC）が 2011 年 10 月に米国上場企業を対象に公表したサイバーリスク開示の在り方に関するガイダンスにて、サイバー攻撃に伴う企業価値への影響として、復旧・修復コスト、サイバーセキュリティ対策コストの増加、売上減少、訴訟対応、風評被害を例示している[9]。近年のセキュリティインシデントにおける金銭的被害の状況を見ると、影響額が大きいケースが散見される（図表 3 参照）。さらに、サイバー攻撃が企業の存続に大きく影響を及ぼした事例も数は多くないものの見られている（図表 4 参照）。

図表 3　金銭的被害が発生したセキュリティインシデント事例

時期	国・地域	組織	影響種別	金銭影響（億円）	概要
2021 年 11 月	日本	病院	改修費用	2	新電子カルテシステム構築費用
2021 年 8 月	日本	建設	特別損失	7.5	ランサムウェア感染の調査復旧費用
2021 年 5 月	ブラジル	食肉加工	身代金	12	ランサムウェアに感染し、身代金を支払い
2020 年 10 月	英国	航空	制裁金	27	個人情報漏洩による、欧州連合（EU）一般データ保護規則（GDPR）違反
2020 年 10 月	英国	ホテル	制裁金	25	個人情報漏洩による、EU GDPR 違反
2019 年 3 月	ノルウェー	製造業	営業停止	45	ランサムウェア感染により生産量減少
2018 年 10 月	香港	航空	時価総額	226	不正アクセスにより株価 3.8%安
2018 年 8 月	台湾	半導体	営業停止	275	ランサムウェア感染により製造が 3 日停止
2018 年 1 月	日本	暗号資産	金銭被害	580	不正アクセスにより暗号資産が流出
2017 年 12 月	米国	運輸	営業停止	440	ランサムウェア感染による大規模な影響
2017 年 8 月	デンマーク	運輸	営業停止	330	ランサムウェア感染により輸送が遅延し混乱
2017 年 6 月	ドイツ	製薬	営業停止	360	ランサムウェア感染によりネットワーク停止
2016 年 2 月	バングラデシュ	銀行	金銭被害	1,080	不正アクセスにより海外口座に不正送金
2014 年 7 月	日本	教育	特別損失	260	内部犯行による情報漏洩後、対策費に投資

（注）　ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム。
（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、より野村資本市場研究所作成

[9] U.S. Securities and Exchange Commission, “CF Disclosure Guidance: Topic No.2 Cybersecurity,” October 13, 2011.

図表 4　サイバー攻撃が企業の存続に大きく影響を及ぼした主な事例

事例	内容
アメリカン・メディカル・コレクション・エージェンシー（AMCA、米医療費回収機関）	2018 年 8 月～2019 年 3 月に行われた AMCA の支払いウェブサイトへのサイバー攻撃により、顧客である複数の医療検査サービス企業が個人情報流出等の影響を受けた。顧客が AMCA らを相手取った集団訴訟を行い、AMCA の親会社が 2019 年 6 月に連邦破産法第 11 章を適用申請した
コロニアル・パイプライン（米、石油パイプライン大手）	2021 年 5 月 7 日にランサムウェアによるサイバー攻撃を受け、全ての業務を停止。停止されたサービスは同月 12 日から再開され、同月 15 日までに供給網全体が復旧した
マウントゴックス（日本、暗号資産〔仮想通貨〕交換業者）	同社のシステムに対する不正侵入者によるハッキング行為により、顧客へのビットコインの返還が困難になり、2014 年 4 月に破産手続き開始。その後、ビットコインの価格高騰等の事情もあり、債権者の意向を踏まえて民事再生手続きに移行し、2021 年 10 月に認可決定。本事件に関して、代表者が起訴され、執行猶予付きの有罪判決が出されるとともに、海外でハッカーが逮捕された
コインチェック（日本、暗号資産〔仮想通貨〕交換業者）	2018 年 1 月に仮想通貨の流出が発生。金融庁による業務改善命令が 2 度出された後、同年 4 月にマネックスグループが完全子会社化し、経営を再建した

（出所）柴原多「オンライン上の外部攻撃と事業継続対応」『西村あさひ法律事務所 事業再生／倒産ニューズレター』2022 年 2 月 28 日、より野村資本市場研究所作成

一方、金融資本市場では、サイバーリスクが顕在化した企業の株価への影響が近年、観察されている。例えば、英国の調査会社コンパリテックの調査によると、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が見られた[10]。また、一般財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）の分析によると、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%下落した[11]。なお、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一旦低下したものの、適切な事後対応等を背景に回復し、その後上昇した事例も存在する[12]。

このような状況下、企業経営におけるサイバーセキュリティ対策の重要性が近年、高まる傾向にある。例えば、経済産業省及び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」では、「サイバーセキュリティは経営問題」と位置付けた上で、（1）経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えた場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる、（2）国内外でサプライチェーンのセキュリティ対策が高まっており、業務を請け負う企業にとって国際的なビジネスに影響をもたらす、と

[10] Comparitech, “How Data Breaches Affect Stock Market Share Prices,” February 9, 2021.

[11] 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。

[12] 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は、同社の生産管理システムが 2019 年 3 月 18 日にランサムウェアに感染し、システムでの操業ができなくなり、損害が約 3.5 億ノルウェークローネ（日本円で約 45 億円）に及んだ。同社の株価はサイバー攻撃直後に約 5%下落したものの、1 ヵ月後には約 6%上昇した。これは、同社のサイバーセキュリティ対策と事後対応（攻撃直後の手動操作への切り替えによる操業継続、政府機関の協力の下での迅速なインシデント対応、損害額の一部がサイバー保険により補填される見込み等）を、社会や株主が好意的に捉えたことが背景とされている。（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）

いった可能性を指摘している[13]。同時に、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上のみならず、情報技術（IT）を利活用して企業の収益を生み出す上でも重要な要素となると述べている。

また、日本経済団体連合会が 2022 年 10 月に公表した「経団連サイバーセキュリティ経営宣言 2.0」でも、「Society 5.0 for SDGs[14]の実現に向けた価値創造やバリューチェーンの構築、さらにはリスクマネジメントの観点から、実効あるサイバーセキュリティ対策を講じることは、いまやすべての企業にとって、経営のトッププライオリティと言っても過言ではない」との言及がある。

これらを踏まえると、サイバーセキュリティは、企業価値に様々な形で影響を及ぼし得るケースも見られるため、投資判断材料としての重要性も高まっていると考えられる。

Ⅲ サイバーセキュリティと情報開示、コーポレートガバナンス

本章では、サイバーセキュリティをめぐる動向のうち、投資家の視点に立って重要と思われる制度・仕組みの観点から、情報開示規制とコーポレートガバナンス・コードを概観する。

１．情報開示規制

企業によるサイバーセキュリティに関する情報開示は、投資家を含めたステークホルダーからの信頼を確保する上で重要である。特に投資家にとって、情報開示は、投資判断や企業との対話（エンゲージメント）を行う際の土台となる。その一方で、情報開示は場合によって攻撃者に対してヒントを与えてしまう等のデメリットもあり、企業による適切な対応が求められる[15]。本項では、企業に適切な情報開示を促す動きとして、日本に加え、米国 SEC、英国財務報告評議会（FRC）及び国際サステナビリティ基準審議会（ISSB）による取り組みを紹介する。

[13] 経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 2.0」2017 年 11 月 16 日。

[14] 日本経済団体連合会では、持続可能な開発目標（SDGs）の達成に向けて、革新技術を最大限活用することにより経済発展と社会的課題の解決を両立するコンセプトとして「Society 5.0」を提案している。（日本経済団体連合会「Society for SDGs」）

[15] 例えば、サイバーセキュリティ関連の情報開示の主なメリットとしては、（1）ステークホルダーからの信頼を確保し、取引先として競争力を高め、また投融資先としての魅力を高める、（2）経営陣、委託先、グループ会社、従業員等の意識の改革や向上、（3）攻撃者への牽制、がある。主なデメリットとしては、攻撃者に対してヒントを与えてしまいかねない、が挙げられる。（塩崎彰久他『サイバーセキュリティ法務』商事法務、2021 年）

１）日本

日本では、「企業内容等の開示に関する内閣府令」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[16]。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[17]。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[18]。例えば 2022 年 2 月に公表された「記述情報の開示の好事例集 2021」では、情報セキュリティに関するリスクについて、サイバー攻撃や新型コロナウイルス感染症の影響によるテレワークの増加への対応等の観点を含めて具体的に記載した事例を始めとして、複数の企業の実際の開示事例が紹介されている[19]。

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[20]。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、経済産業省等による「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（図表 5 参照）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。

図表 5　企業における情報開示の在り方（実施が望まれるサイバーセキュリティ対策、抜粋）

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**

（出所）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、より野村資本市場研究所作成

[16] 金融庁「『企業内容等の開示に関する内閣府令』の改正案に関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。

[17] 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）

[18] 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。

[19] 金融庁「記述情報の開示の好事例集 2021」2022 年 2 月 4 日。

[20] 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。

２）米国 SEC

米国では 2010 年代以降、企業に適切なサイバーセキュリティ関連情報開示を促すべく、SEC を中心に様々な動きが見られる。SEC の企業財務局は 2011 年 10 月、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を公表した[21]。同ガイダンスには、法的な強制力はないが、証券諸法において投資家が通常、投資判断に重要と判断するリスク及び出来事について、適時、網羅的かつ正確な情報開示を行うように設計されていることが確認されている[22]。その上で、開示要件の中にはサイバーセキュリティリスクやサイバーインシデントを明示的に言及するものは存在しないものの、リスク要因、経営者による財政状態及び経営成績の検討と分析（MD&A）、事業の状況、訴訟手続き、財務諸表開示、開示統制・手続きのうちいくつかの項目で義務付けることが可能と示された。

SEC は 2018 年 2 月、上記のガイダンスの拡張、強化を目的に、解釈指針を公表した[23]。同指針には、サイバーセキュリティ情報開示に関する方針・手続きの必要性を強調するとともに、サイバーセキュリティに関するインサイダー取引規制の適用可能性を示した[24]。

SEC は 2020 年代に入って、情報開示の強化を目指す複数の取り組みを実施している。2021 年には、サイバーセキュリティ情報開示に関するエンフォースメントとして違約金や民事制裁金が課せられる事案が相次いで発生した（図表 6 参照）。さらに、2022 年 3 月には公開企業によるサイバーセキュリティリスク管理、戦略、ガバナンス、インシデント報告に関する開示を強化し標準化するための規則の改正案を公表した[25]。同案では、従来の重大なサイバーセキュリティインシデントに関する報告に加え、サイバーセキュリティリスクを特定、管理するための方針と手順を定期的に報告するように要求している[26]（図表 7 参照）。

SEC は 2022 年末頃を目途に同開示規則の制定を目指しているが、米国企業のみな

---

[21] 本ガイダンスでは、サイバーセキュリティについて、ネットワーク、システム、コンピューター、プログラム、及びデータを攻撃、損傷、または不正アクセスから保護するために設計された技術、プロセス、及びプラクティスの集合体と定義付けている。（U.S. Securities and Exchange Commission, “CF Disclosure: Guidance Topic No.2 Cybersecurity,” October 13, 2011）

[22] 脇黒丸新太郎「サイバーセキュリティ開示をめぐる日米比較考察―開示制度の実効性を確保するガバナンス体制の視点を踏まえて―」『法学研究論集』第 56 号、明治大学大学院、2022 年 2 月 25 日。

[23] U.S. Securities and Exchange Commission, “Commission Statement and Guidance on Public Company Cybersecurity Disclosures,” February 26, 2018.

[24] 塩崎彰久他『サイバーセキュリティ法務』商事法務、2021 年。

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

[26] これらには、取締役会によるサイバーセキュリティリスクの監視、サイバーセキュリティリスクの評価と管理における経営陣の役割と専門知識、以前に報告されたサイバーセキュリティインシデントに関する最新情報の提供が含まれる。（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）

らず、米国に上場する外国企業にも適用が見込まれている[27]。さらに、米国では前述のエンフォースメント事例のみならず、2022 年 3 月 15 日に「2022 年の重要インフラに関するサイバーインシデント報告法」（CIRCIA）が制定されており、規制当局による監視が増える傾向にある[28]。このような状況の下、米国内外の金融市場、産業界では、SEC による新たなサイバーセキュリティ情報開示規則に注目が集まる傾向が見られる。

図表 6　SEC によるサイバーセキュリティ情報開示に関するエンフォースメント

事例	内容
ファースト・アメリカン（米金融機関）	同社のウェブページで顧客情報等の流出が可能であるとの脆弱性をサイバーセキュリティジャーナリストに告発されていたのにも関わらず、同社の最高情報管理責任者には伝えられていなかった。2019 年 5 月に提出した臨時報告書で不適切な開示を行ったとして、同社に改善命令及び 487,616 ドルの違約金が課された
ピアソン（英教育出版大手）	顧客アカウントの学生データと管理者のログイン認証情報の漏洩が実際起きたのにもかかわらず、2019 年 7 月に提出した半期報告書には仮想的なリスクとして表記し、実際にデータ侵害を受けた事実を開示しなかった。そのため、投資家に誤解を与えうる不十分な開示を行ったとして、同社に 100 万ドルの民事制裁金が課された

（出所）U.S. Securities and Exchange Commission, “SEC Charges Issuer With Cybersecurity Disclosure Controls Failures,” June 15, 2021; U.S. Securities and Exchange Commission, “SEC Charges Pearson plc for Misleading Investors About Cyber Breach,” August 16, 2021、脇黒丸新太郎「サイバーセキュリティ開示をめぐる日米比較考察―開示制度の実効性を確保するガバナンス体制の視点を踏まえて―」『法学研究論集』第 56 号、明治大学大学院、2022 年 2 月 25 日、より野村資本市場研究所作成

図表 7　SEC によるサイバーセキュリティ開示に関わる規則案の概要

重要なサイバーインシデントの適時開示　Form 8-K（日本を含む外国企業は 6-K）
重要と判断してから 4 営業日以内に開示
・ インシデントの概要（発見時期、進行状況、性質、影響範囲など）
・ データ窃取、改竄、変更、または不適切な利用の有無
・ 企業活動への影響
・ 問題の修復状況　など
定期報告（年次・非半期）における開示 Form 10-K、10-Q（日本を含む外国企業は 20-F）
・ 開示済みのインシデントの最新状況
・ 集約評価によって重要と判断した一連のサイバーインシデント
・ インシデントの影響（オペレーション、リスク管理、財務状況など）
・ サイバーセキュリティガバナンス（取締役会による監視）
・ サイバーセキュリティ評価プログラムの概観
・ 外部委託先におけるリスク識別の方法
・ 事業戦略、財務計画、資本配分等へ与える影響
・ 経営陣や取締役会の役割や責任、及び専門知識　など

（出所）デロイトトーマツグループ「第 3 回　サイバーインシデントに関する開示の国際動向【米国証券取引委員会（米国 SEC）のサイバーセキュリティ開示の規則案への対応準備について】」2022 年 9 月 5 日

[27] デロイトトーマツグループ「第 3 回　サイバーインシデントに関する開示の国際動向【米国証券取引委員会（米国 SEC）のサイバーセキュリティ開示の規則案への対応準備について】」2022 年 9 月 5 日。

[28] 2022 年の重要インフラに関するサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022、CIRCIA）では、重要インフラの所有者や運用者はサイバーインシデントについては 72 時間以内に、ランサムウェアの支払いについては 24 時間以内に、サイバーセキュリティ・インフラセキュリティ庁（CISA）に報告することが義務付けられた。同法律は、16 の重要インフラセクターにまたがる企業・組織がどのようなサイバーインシデントを報告すべきか定めた規則を、CISA が制定することを義務付けている。（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）

３）英国 FRC

英国 FRC は、同国のコーポレートガバナンス、企業報告、監査等を監督する機関である。事業予算や活動資金は英国政府や産業界から拠出され、ボードメンバーは英国ビジネス・イノベーション・技能大臣が任命する。本稿では、FRC におけるサイバーリスク関連情報開示の取り組みとして、（1）戦略報告書ガイダンスにおける対応、（2）財務報告ラボ（Financial Reporting Lab、後述参照）におけるサイバー、デジタル、データのリスクに関する開示プロジェクト、を紹介する。

1 点目について、英国企業はビジネスモデルに関する記述を要する戦略報告書（Strategic Report）の開示が義務付けられている[29]。FRC は 2014 年 6 月に戦略報告書のガイダンスを公表し、その後、2018 年 7 月及び 2022 年 6 月に改訂している。2018 年 7 月の改訂版より、サイバーリスクの開示に関する言及が含まれている（図表 8 参照）。

図表 8　FRC による戦略報告書のガイダンスにおけるサイバーリスクに関する言及（抜粋）

企業のリスク・プロファイルが変化した場合、多くの企業は、特定された個々のリスクが増加したのか、減少したのか、あるいは同じ重大度のままであったのかを説明する。リスク軽減は、企業が変更にどのように対応したかを示すこともできる。

例えば、近年、多くの事業者が直面するサイバーリスクは著しく増大しており、リスクの開示は、例えば、サイバー攻撃、顧客の信頼の欠如につながる機密データの損失、事業の特定の要素の操作の失敗につながる IT システムの障害など、サイバーリスクが事業にどのような影響を及ぼす可能性があるか、リスクの軽減は、事業者が増大するリスクを緩和するために実施したプロセスを、説明することができる。

（出所）Financial Reporting Council, “Guidance on the Strategic Report,” June 2022、より野村資本市場研究所訳

2 点目について、財務報告ラボは、FRC に設置された企業報告の効果を改善するための調査研究を行う機関として 2011 年に設立され、FRC から活動資金が拠出されている。同ラボのメンバーは、FRC、監査法人、投資家、企業等で構成されており、開示に関するルールや規則を定めるのではなく、投資家やアナリストも関与する形で求められる開示の在り方を調査研究、発信することが期待されている。

財務報告ラボでは 2021 年 9 月、サイバー、デジタル及びデータリスク関する開示プロジェクトを立ち上げ、企業、投資家等のステークホルダーに参加を呼び掛け、企業のプロセスの変化を踏まえた有用な開示検討を始めた[30]。そして、2022 年 8 月に研究成果となるレポートを公表した[31]。これらには、投資家向けの開示を最適にする方法の詳細のほか、実践的な例も含まれている。レポートでは、企業によるデジタルセキュリティリスクの開示は投資家のニーズを効果的に満たしていないと指摘し、多くの場合、デジタルセキュリティに関する有用な情報が限定的であり、ビジネスのより

[29] 戦略報告書では、戦略、ビジネスモデル、男女別人数（取締役、シニアマネジメント、従業員）に関する記述が義務付けられている。英国 2006 年会社法が 2013 年 8 月に改正され、アニュアルレポートの一部として、戦略報告書の作成と公開が義務付けられた。（経済産業省「英国における議論」第 6 回持続的成長に向けた長期投資（ESG・無形資産投資）研究会参考資料 1、2017 年 1 月 10 日）

[30] Financial Reporting Lab, “Call for Participants: Cyber, Digital and Data Risk,” September 2021.

[31] Financial Reporting Council, “FRC Publishes Recommendations to Improve Digital Security Disclosure,” August 3, 2022; Financial Reporting Council, “FRC Lab Report: Digital Security Risk Disclosure,” August 2022.

広い意味での戦略的方向性に、結び付いていないか、地政学的またはサイバーイベントに十分に対応していない旨が言及されている。そして、企業は、戦略、ガバナンス、リスク、イベントの側面に焦点を当てることで、開示を改善できるとしている。財務報告ラボによる本プロジェクトは、利用者である投資家も含めた様々なステークホルダーとともにまとめられたもので、ステークホルダーの意図も反映する形で企業による開示の質の向上に寄与することが期待される。

4）ISSB

ISSB とは、英国の国際会計基準財団（IFRS 財団）が国際連合気候変動枠組条約第26回締約国会議 （COP26）の開催中の2021年11月に設立を公表した審議会で、サステナビリティ開示基準の包括的なグローバルなベースラインの開発を目指している。ISSB は 2022 年 3 月にサステナビリティ開示基準（サステナビリティ関連財務情報の開示に関する全般的要求事項及び気候関連開示）の公開草案を公表し、2023 年に可能な限り早い時期に最終基準を公表することを目指している[32]。

ISSB では 2022 年 7 月に開催された会議にて、大まかに定義されたトピックとして、今後、基準化に向けて議論が行われる可能性のある 8 つのテーマ及び市場ニーズへ対応するための課題を提示したが、その中に「サイバーセキュリティ、データセキュリティ、顧客のプライバシー」が含まれている（図表 9 参照）。同発表資料には、本テーマの基準は、既存の材料をベースに構築される可能性があるとして、サステナビリティ会計基準審議会（SASB）によるデータセキュリティとデータプライバシーに関する基準を例として挙げている。ISSB によるサイバーセキュリティ等に関する基準の策定時期等は示されていないものの、サステナビリティ開示基準の存在感等に鑑みると、今後の動向が注目される。

図表 9　ISSB にて基準化が行われる可能性のあるテーマと市場ニーズへ対応するための課題（サイバーセキュリティ、データセキュリティ、顧客のプライバシー、抜粋）

- **サイバーセキュリティリスクに関する将来を見越した分析は定量化及び比較が困難であること**
- **法律や枠組みが多様であるため、規制リスクエクスポージャーを法域間で比較することは困難であること**
- **企業が、サイバーセキュリティの実務や過去の事故に関する情報を開示することをためらう可能性があること**

（出所）International Sustainability Standards Board, “AP1A: Items to be Considered in Development of Request for Information,” July 2022、経済産業省「ISSB 開示基準の審議状況について（事務局資料①）」第 10 回非財務情報開示指針研究会資料 3、2022 年 10 月、より野村資本市場研究所作成

[32] サステナビリティ基準委員会（SSBJ）「国際基準等の解説：ISSB 公開草案の『IFRS S2 号〔気候関連開示〕』（S2 基準案）について」2022 年 10 月 21 日。

２．コーポレートガバナンス・コード

一般に、コーポレートガバナンスは「会社が、株主をはじめ顧客、従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み[33]」と定義付けられている。実効的なコーポレートガバナンスの実現に資する主要な原則を取りまとめたコーポレートガバナンス・コードが適切に実践されることは、会社の持続的な成長と中長期的な企業価値の向上のための自律的な対応が図られることを通じて、会社、投資家、ひいては経済全体の発展にも寄与することになるとの考えが示されている。本項では、最近の動向として、日本に加え、国際的な動きとして、世界経済フォーラム（WEF）等、20ヵ国・地域（G20）及び経済協力開発機構（OECD）による取り組みを概観する。

１）日本

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」（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10参照）。

ただし、後述のとおり「G20／OECD コーポレートガバナンス原則」の改訂作業が進められており、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視野に入るとみられる[34]。

図表10「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

[33] 東京証券取引所「コーポレートガバナンス・コード―会社の持続的な成長と中長期的な企業価値の向上のために―」2021年6月11日。

[34] 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）WEF 等

WEFは2021年3月、全米取締役協会（NACD）、インターネット・セキュリティ・アライアンス（ISA）及びPwCと共同で「サイバーセキュリティのための取締役会ガバナンス原則」を公表した（図表 11 参照）。同原則は、企業の取締役が組織のサイバーセキュリティ戦略を策定し、サイバーリスク問題についてステークホルダーと関わる際の参考資料として位置づけられ、6つの原則で構成されている。

図表 11 「サイバーセキュリティのための取締役会ガバナンス原則」における 6 つの原則

1. サイバーセキュリティは戦略的な事業を可能にする
2. サイバーリスクの経済的要因と影響を理解する
3. サイバーリスクマネジメントをビジネスニーズに整合させる
4. サイバーセキュリティをサポートするような組織設計にする
5. 取締役ガバナンスにサイバーセキュリティの専門知識を組み込む
6. 体系的なレジリエンスと協働を推進する

（出所）World Economic Forum et al., “Principles for Board Governance of Cyber Risk,” March 2021、より野村資本市場研究所訳

３）G20 及び OECD

OECD では、コーポレートガバナンス問題を前進させるとともに、OECD 加盟国・非加盟国双方において、立法・規制上の参考になることを意図し、1999 年に「OECD コーポレートガバナンス原則」を公表している。同原則は国際的なベンチマークとして位置づけられており、これまでも改訂が行われてきた。2022 年に入って「G20／OECD コーポレートガバナンス原則」の改訂案が公表され、同年 9 月 19 日から 10 月 21 日まで意見募集が実施された[35]。

同改訂案の中には 10 の優先分野が特定されており、その中で「新しいデジタル技術の成長と新たな機会とリスク」が掲げられている[36]。デジタルに関しては、（1）デジタル技術はコーポレートガバナンス要件の監督と実施の強化を目的として利用される場合もあるが、監督当局と規制当局が関連するリスク管理に十分な注意を払う必要がある、（2）バーチャル会議の処理を担う技術ベンダーが株主の平等な参加と身元確認を可能にする公正で透明性のある株主総会の実施を支援するために必要な専門性とデータ処理能力及びデジタルセキュリティ能力を備えていることが求められる、（3）財務・非財務情報開示に含めるべき重要な情報の 1 つとして、デジタルセキュリティリスク等の予測可能なリスク要因がある、（4）取締役会が果たすべき機能の 1 つであるリスク管理の方針と手順の見直し及び評価の中に、動的で急速に変化する可能性のあるデジタルセキュリティリスクの管理も含まれ、他のリスクと同様に全体

[35] Organisation for Economic Cooperation and Development, “Public Consultation on Draft Revisions to the G20/OECD Principles of Corporate Governance,” 2022.

[36] OECD では、10 の優先分野に関する補助資料を挙げており、デジタル化とコーポレートガバナンス」と題したワーキングペーパーも含まれている。（Organisation for Economic Cooperation and Development, “Digitalisation and Corporate Governance,” OECD Corporate Governance Working Papers No. 26, 2022）

の循環的企業リスク管理の枠組みに広く統合されるべき、等が示されている。

同改訂案は2023年に最終化される予定となっており[37]、前述のとおり、日本を含めた多くの国のコーポレートガバナンス・コードにおいて将来的に参考にされる可能性があると解釈される。

Ⅳ サイバーセキュリティとESG評価、信用格付け

投資家は、投資判断に資する情報を調査・分析・評価する機能を組織内に有するとともに、組織外のツールとしてESG評価機関や信用格付会社による機能もしばしば活用する傾向にある。本章では、本稿執筆時点のESG評価機関等による評価分析手法や注目される見解を紹介する。

１．ESG評価機関による評価

ESG評価機関は、ESG課題の中で投資家の関心の高いものや、投資判断に有用な項目を特定し、企業の公開情報や個別の質問表等を活用して企業情報の収集や調査、評価を行い、機関投資家に提供している[38]。

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[39]。各評価機関による評価手法は異なるが、情報セキュリティ方針、研修等の共通項目もある（図表 12 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（図表13参照）。

[37] Organisation for Economic Cooperation and Development, “OECD Secretary-General’s Report to G20 Finance Ministers and Central Bank Governors on the Review of the G20/OECD Principles of Corporate Governance,” February 2022.

[38] 日本取引所グループによるESG評価機関・データプロバイダの説明。（日本取引所グループ「ESG評価機関等の紹介」）

[39] 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。

図表 12　主要 ESG 評価機関による評価項目と特徴

項目	内容
情報セキュリティ方針	・ S&P グローバルに買収された RobecoSAM の ESG 調査部門が提供する「SAM コーポレートサステナビリティ評価」（SAM 指標）では、「IT セキュリティ/サイバーセキュリティ施策」の項目で、従業員が情報セキュリティの重要性を認知することを目的とし、全従業員が会社の情報セキュリティ方針にアクセス可能であることを評価 ・ GRESB（Global Real Estate Sustainability Benchmark）は、企業の ESG 分野における方針有無を評価する「ESG ポリシー」の項目で、ガバナンス関連の方針として、サイバーセキュリティとデータ保護とプライバシーに関する方針が開示されていることを評価
情報セキュリティ研修	・ SAM 指標では「IT セキュリティ／サイバーセキュリティ施策」の項目で、従業員が情報セキュリティの重要性を認知することを目的とし、情報セキュリティ・サイバーセキュリティに関する意識向上のための研修を行っていることを評価 ・ ISS ESG による「ISS ESG コーポレートレーティング」（ISS 指標）では、企業が従業員向けの情報セキュリティ研修の実施とその頻度を開示していることを評価。特に、情報セキュリティに特化した従業員への強化研修や役員への特別研修が付加的に実施されている場合、最高評価を付与
情報セキュリティガバナンス	・ SAM 指標では「IT セキュリティ／サイバーセキュリティ」の項目で、サイバーセキュリティ戦略に携わる取締役・執行役が存在することを評価。特に取締役に関しては、情報セキュリティ関連のバックグラウンドの有無も評価項目に含まれる ・ ISS 指標では、「情報セキュリティリスクの監視」の項目にて、(1)情報セキュリティに携わる取締役のうち、社外取締役の割合、(2)取締役会で情報セキュリティに関する議題を取り上げる頻度、(3)情報セキュリティリスクの特定・軽減・対応を担う取締役の人数、を評価
第三者認証	・ SAM 指標は 2 つの観点（認証と監査）から評価。認証の観点からは、ISO27001（情報セキュリティマネジメントシステム〔ISMS〕に関する国際規格）や NIST（米国国立標準技術研究所）、またはそれらに準ずる第三者認証の取得を評価。監査の観点からは、外部機関による情報セキュリティ監査に加えて、模擬的サイバー攻撃を含む第三者による脆弱性分析が実施されていることを評価 ・ ISS 指標は、FedRAMP(連邦情報リスク承認管理プログラム)または SOC2（米国公認会計士協会によって定められた委託会社の内部統制・サイバーセキュリティに関する内部統制保証報告の枠組みの一部）による監査、または関連産業において ISO27001・FISMA（連邦情報セキュリティマネジメント法）・医療業界の代表者が管理する組織である HITRUST(Health Information Trust Alliance)の認証を取得していることを評価

（出所）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、より野村資本市場研究所作成

図表 13　ESG 評価機関によるサイバーセキュリティ・プライバシー保護の ESG 評価の重みづけ

MSCI		S&P Global CSA		サステイナリティクス（データプライバシーとセキュリティ）	
業界	重みづけ	業界	重みづけ	業界	リスクスコア
コミュニケーション・サービス	24.1%	インタラクティブメディア、サービス及びホームエンターテイメント	11.0%	ソフトウェア及びサービス	5.25
				保険	4.53
金融	10.1%	ソフトウェア	11.0%	銀行	4.52
IT	10.1%	IT サービス	11.0%	総合金融	4.52
業界別「プライバシー及びデータセキュリティ」の重みづけ（上位 3 業界）		業界別「情報セキュリティとシステム・アベイラビリティ」と「プライバシー保護」合計（上位 3 業界）		業界別「データ保護とセキュリティ」のリスクスコア（上位 4 業界、10 が最大のリスク）	

（出所）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、より野村資本市場研究所作成

２．信用格付会社による見解

信用格付けは、投資家が投資判断を行う際の信用リスク評価の参考として、金融・資本市場において広範に利用されており、投資家の投資判断に大きく影響を与えている[40]。本節では、S&P グローバル及びムーディーズによる動きを概観する[41]。両社は近年、サイバーリスクに関するソリューションの提供に向けてコミットメントを強めており[42]、多数の見解を公表している。

１）S&P グローバル

S&P グローバルは 2022 年 3 月（日本語版は同年 4 月）、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を公表した[43]。同レポートでは、（1）サイバーリスクの準備状況は、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、と指摘した（図表 14 参照）。同社によると、日本では 2022 年 4 月現在、サイバー攻撃によって格付けに直接影響が及んだ事例はないが、海外では 2017 年 9 月の米消費者信用大手エクイファクスへのサイバー攻撃にて同社の格付けを引き下げる等の事例が存在する[44]。

---

40 金融庁「信用格付業者向けの監督指針」2022 年 6 月。

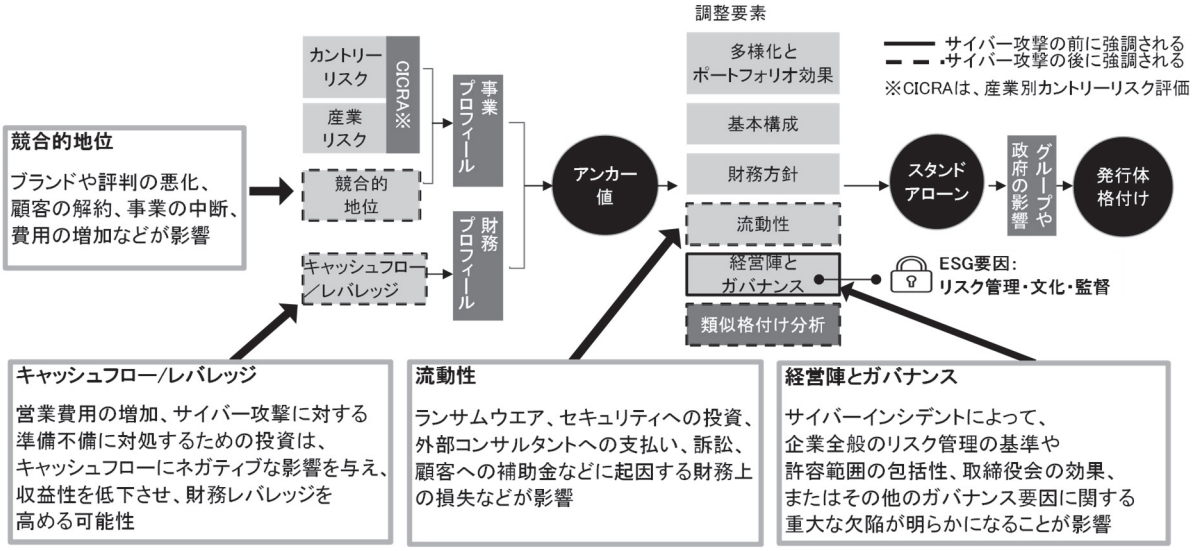
41 信用格付会社によるサイバーリスクに関する分析の詳細については、今川玄「サイバーリスクと信用格付－警戒強める格付会社、攻撃前でも格下げの可能性－」『野村サステナビリティクォータリー』第 3 巻第 3 号（2022 年夏号）も併せて参照されたい。

42 例えば、S&P グローバルは 2021 年 8 月、損害保険会社向けのソフトウェア開発会社ガイドワイヤソフトウェアとの協力関係を拡大、ムーディーズは同年 9 月、サイバーリスクの評価・分析、パフォーマンス管理ツールの提供会社ビットサイトに 2 億 5,000 万ドルを追加出資、を発表している。（S&P Global Ratings, “S&P Global Ratings Expands Cyber Risk Insights Partnership with Guidewire Software,” August 31, 2021; Moody’s, “Moody’s and Bitsight Partner to Create Integrated Cybersecurity Risk Platform,” September 13, 2021）

43 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。

44 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。（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）。

図表 14　S&P による事業会社の格付けの枠組み：サイバーリスクの織り込み方



（出所）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、より野村資本市場研究所作成

2）ムーディーズ

ムーディーズでも近年、サイバーリスクに関するレポートを複数公表している。例えば、同社が 2022 年 9 月に公表した「サイバー・ヒートマップ」と題したレポートでは、サイバーリスクについてエクスポージャーと軽減の要素に基づき分析を進め、格付付与先の 71 のセクターを 4 段階の総合サイバーリスクスコア（低い、中程度、高い、非常に高い）に分類した結果、5 つのセクターが「非常に高い」に分類されたこと等を明らかにしている（図表 15 参照）。同レポートでは、デジタル化の進展によりサイバーリスクは高まるものの、全般的な想定財務インパクトは大きくなく、今日のサイバーインシデントのほとんどが信用格付けに影響を与えるほどの重大な水準にまではなっていないと説明している。

図表 15　ムーディーズによる総合サイバーリスクスコアにおいて「非常に高い」とされたセクター

セクター	エクスポージャー			軽減		総合サイバーリスクスコア
	システム上の役割	デジタル化	境界の脆弱性	基本的なサイバー実務	想定財務インパクト	
規制及び自主規制された発電を行う公益事業	非常に高い	高い	非常に高い	高い	中程度	非常に高い
送配電力･ガス事業	非常に高い	高い	非常に高い	高い	中程度	非常に高い
規制のない公益･電力会社	非常に高い	高い	非常に高い	高い	中程度	非常に高い
上下水道事業	非常に高い	高い	非常に高い	非常に高い	中程度	非常に高い
非営利病院	高い	非常に高い	中程度	中程度	低い	非常に高い

（出所）Moody’s, “Cyber Heatmap: Risk are Rising, But Many Sectors are Boosting Defensive Capabilities,” September 28, 2022、より野村資本市場研究所作成

V グローバルな投資家団体による活動

サステナブルファイナンスやその代表的な手法としての ESG 投資をめぐっては、様々な投資家団体が存在し、投資家の観点から健全な金融資本市場の発展に向けた取り組みを続けている。本章では、代表的な団体として責任投資原則（PRI）及び国際コーポレートガバナンスネットワーク（ICGN）を取り上げ、サイバー関連の近年の活動を概観する。

1．PRI

PRI は、国際連合環境計画・金融イニシアティブ（UNEP FI）及び国際連合グローバル・コンパクトと連携した投資家イニシアティブである。本項では、主な取り組みとして、（1）大手企業のサイバーセキュリティ対応状況の分析（2018 年 7 月）、（2）機関投資家との共同エンゲージメントプロジェクト（2017～2019 年）、を紹介する。

1 点目について、PRI は 2018 年 7 月、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を発表した[45]。本調査では、サイバーセキュリティに関する 14 の調査指標を基に、100 社（地域〔欧州、米国、オーストラリア及びアジア〕、セクター〔ヘルスケア、金融、消費財、IT 及び通信〕）のサイバーセキュリティに関する情報開示を評価した（図表 16 参照）。その結果、企業によるこの分野の情報開示はしばしば投資家の期待水準を下回っており、企業が潜在的なサイバーセキュリティの侵害を特定、管理、修復するためにどのような立ち位置になるか投資家が判断することが困難であることが明らかになった。

PRI では、調査結果を踏まえて 2 点目の共同エンゲージメントプロジェクトを実施することとなった。同プロジェクトは、2017～2019 年にかけて PRI が 55 の機関投資家（運用資産残高合計 12 兆ドル強）と共同で実施したもので、上記の 5 セクターに属する 53 社に対して共同エンゲージメントが実施された[46]。成果報告書によると、サイバーセキュリティに関する 14 の指標の開示状況について 2019 年時点で、（1）調査対象企業のうち 8 割以上が開示（指標 1、2 及び 14）、（2）同 5 割以上が開示（指標 5、6、8、9 及び 13）、（3）改善が求められる分野（指標 4 及び 11）、に分類される。これらを踏まえ、PRI は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（図表 17 参照）。PRI はサイバーリスクがますます複雑化していく問題であることを踏まえ、次の取り組みとして、人工知能（AI）やイノベーションの倫理、適切なガバナンスメカニズムや規制上のギャップ等の関連テーマを探求すると示している。

[45] 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.

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

図表 16　PRI によるサイバーセキュリティに関する調査指標

指標	詳細
法務コンプライアンス	
1	会社は、サイバー及びデータ保護に関連するものを含め、全ての関連する法律を遵守することを公式にコミットしているか
ポリシー	
2	会社は、プライバシー及び／またはデータ保護ポリシーを開示しているか
3	ポリシーは第三者を含めて業務全体を明示的にカバーしているか
上級管理職と取締役会のアカウンタビリティ	
4	情報管理とサイバーセキュリティの全体的な責任を負う経営幹部または執行委員会レベルの指名された人物を特定しているか
5	取締役会または取締役会委員会はサイバーセキュリティの問題に責任を負うか
取締役会のコミュニケーション	
6	会社は、取締役会に（どのように、誰により、どのような頻度で）サイバーリスクを報告しているか
7	取締役会は、会社のサイバー／情報セキュリティ戦略に関する詳細な情報を得ているか（どのような情報が得られ、得た情報がどのように評価されるかを含む）
スキルとリソース	
8	会社は、サイバーセキュリティ、または情報セキュリティチーム、または専用予算を有していることを公表しているか
9	取締役会がサイバーセキュリティに関する業界イニシアティブに関与していること、またはサイバーセキュリティに関する社内外の専門知識にアクセスできることを示しているか
10	取締役の選任に当たって、そのようなスキルを有する人材を積極的に模索しているか
トレーニング	
11	情報またはサイバーセキュリティ要件に関するトレーニングを全従業員に提供しているか
評価	
12	会社は、情報またはサイバーセキュリティに関する方針やシステムに関する監査を行っているか
プロセスと手順	
13	会社は、インシデント管理計画（災害復旧及び事業継続を含む）を策定しているか
14	会社は、リスク評価／事業継続計画の重要部分として、情報またはサイバーセキュリティについて開示しているか

（出所）Principle for Responsible Investment, “Stepping up Governance on Cyber Security,” 2018、より野村資本市場研究所訳

図表 17　PRI によるエンゲージメント及び開示の期待に関する推奨事項

1. 取締役会の監視	
投資家が取締役会レベルでサイバーセキュリティの監督、能力、説明責任を検証することが重要である	
【潜在的な質問】	・ 組織のサイバーセキュリティを支えるガバナンス構造はどのようなものか。また、その有効性を実証できるか ・ 取締役会にサイバーセキュリティに関する専門知識はあるか ・ 取締役会で、サイバーセキュリティに関連するスキルと経験のギャップにどのように対処しているか
2. サイバーへの耐性（レジリエンス）の全体的な戦略への確実な組み込み	
投資家は、予防的及びコンプライアンス指向のサイバー防御を通じたサイバー回復力に関して、企業に戦略的方向性に関する考え方を尋ねる必要がある	
【潜在的な質問】	・ サイバーセキュリティに関する戦略的及びコンプライアンス上の優先事情は何か ・ バリューチェーン内のサイバーセキュリティに関する主な懸念事項は何か
3. 共通言語のチェック	
投資家は、方針、ベンチマーク、インセンティブの間に矛盾がないかどうか調べることで、取締役会の考えが組織全体にどのように影響しているかを見直すことが求められる	
【潜在的な質問】	・ 取締役会に報告されているサイバーセキュリティ指標の例と、それが全社的なインセンティブやベンチマークとどのように関連しているのか ・ 取締役会によるサイバーセキュリティに関する報告は、サイバーセキュリティ計画及び戦略にどのように役立っているか
4. 技術的なコントロールを超えて見る	
投資家は、投資先企業と会話する際、サイバーセキュリティに関する優先順位とサイバーセキュリティ意識の範囲に関する洞察を得られるような質問を提起することが求められる	
【潜在的な質問】	・ 経験したサイバーセキュリティ違反から何を学んだか、また、これらの学びを反映するために既存のメカニズムをどのように修正したか ・ サイバーセキュリティ保護の一環として、組織の能力をどのように強化しているか
5. 開示の期待水準の設定	
投資家は、セクター間の現状のレポーティング慣行に基づいて、開示に関して最低限と考えるものを設定することができる	
【潜在的な質問】	—（提示なし）

（出所）Principle for Responsible Investment, “Engaging on Cyber Security: Results of the PRI Collaborative Engagement 2017-2019,” 2020、より野村資本市場研究所訳

２．ICGN

ICGN は、投資家によって 1995 年に設立されたガバナンス専門家の団体である[47]。本項では、主な取り組みとして、（1）視点レポートの公表（2016 年 5 月）、（2）グローバル・ガバナンス原則（2021 年版）における言及、を紹介する。

1 点目について、ICGN は 2016 年 5 月、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を公表した[48]。同レポートでは、企業に対してサイバー関連リスクに関する経営活動をどのように監督するかについて投資家とのコミュニケーションを強化すること

[47] 日本の年金積立金管理運用独立行政法人（GPIF）を含め、45 ヵ国超の機関投資家（運用資産総額は 70 兆米ドル超）が会員で、コーポレートガバナンスと投資家のスチュワードシップの実効的な水準の向上を通じ、世界全体の効率的な市場と持続可能な経済の発展を推進することをミッションとしている。

[48] 本レポートでは、サイバー関連リスクについて、企業の目的達成や投資家の利益を阻害する可能性のある情報通信技術に関するリスクの範囲を指すと定義付けている。（International Corporate Governance Network, “ICGN Viewpoint: Cyber Risk,” May 2016）

を奨励している。一方、投資家に対して取締役会との対話においてビジネス目標を踏まえて全てのサイバー関連リスクに対してバランスの取れた監視が行われているかに焦点を当てるべきとしている。その上で、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、を示している（図表 18 参照）。

図表 18　ICGN による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

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質問
・ 取締役会内でサイバーリスクの監視はどのように整理されているか
・ サイバーリスクの監視に適切に対処するために、取締役会はどのように訓練され、教育されているか
・ 取締役会のサイバーリスクに関する議論において、(1)戦略プロセスと計画の監視、(2)リスクプログラム管理の監視、(3)リスク対応の準備、はどのように登場しているか
・ 次の問題を適切に予測することが犠牲になり、直近のサイバー関連の問題に過度に焦点を当ててしまう可能性を回避するために、取締役会の議論はどのように管理されているのか
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質問
【戦略プロセスと計画の監視】
・ 経営陣は、企業の目的、プロセス、データのうち、どれが最も戦略的であり、サイバー脅威に対して最も脆弱であるかをどのように評価するのか
・ これらのリスクを効果的に管理するために使用されるサイバーリスクセキュリティ戦略は何か
・ サイバーリスクの監視は、企業の戦略やリスク軽減とどのように統合されているか 企業情報技術の監視／ガバナンスはどのような形で行われているか。これは、取締役会によって承認された戦略及び技術投資とどのように関連しているか
【リスクプログラム管理の監視】
・ 会社は、ビジネス戦略と IT 戦略、優先順位、予算編成の整合性をどのように改善しているか。IT 予算は戦略的イニシアティブの目標に直接対応しているか
・ 会社は、運用可能で安定し、保護され、回復可能な IT システムを確保するために、どのようなプロセス・規律に沿っているか。これらのプロセスは、従業員の雇用、トレーニング、改善を容易にするために、グローバル教育や業界教育で広く活用されているか
・ 従業員は、安全なシステム相互接続などのトピックについて、企業のパートナー組織や顧客組織の担当者とトレーニングを実施しているか
・ サイバー関連リスクを管理するためのリソースが各リスク領域に比例して配分されていることを、会社はどのように把握しているか
・ 会社は、(1) デジタル化、収益化、またはビジネスを混乱させる可能性のあるあらゆるテクノロジー、(2) ビジネスモデルに触れる、あるいは触れる可能性のある技術、(3)企業の業界におけるビジネスモデルに関する指数関数的技術と技術の経済性、をどのように理解しているか
・ 会社は、どのようなサイバーリスクを管理しているのか。コンプライアンスに対するリスク、またはパフォーマンス目標の達成に対するリスクはどうか
・ サイバーリスクプログラムの有効性はどのように評価されているか
【リスク対応の準備】
・ 会社のサイバーリスク対応計画は、リスク評価で特定された「仮に」や警告の兆候にどのように完全対処しているか
・ 会社の過去 10 回の技術的問題の根本原因は何だったのか。経営陣は、これらの原因を徹底的に診断するために堅牢なアプローチを用い、それらの原因を修正するために何を行っているか。取締役会はどのように関与したか

（出所）International Corporate Governance Network, “ICGN Viewpoint: Cyber Risk,” May 2016、より野村資本市場研究所訳

2 点目のグローバル・ガバナンス原則は、主に上場企業に適用され、投資の意思決定に影響を与える可能性が最も高いコーポレートガバナンスの課題に関する期待事項を示しており、10 の原則で構成されている。2001 年に初めて策定され、その後改訂が複数回行われたが、2021 年版で原則 6（リスクの監督）の指針の中にサイバーセキュリティに関する言及が示された（図表 19 参照）。

図表 19　ICGN の「グローバル・ガバナンス原則」におけるサイバーセキュリティに関する言及（抜粋）

原則 6：リスクの監督

取締役会は、会社の主要なリスクの評価と開示を積極的に監督し、定期的に、または重大な事業上の変更があるごとに、リスク管理の手法を承認し、当該手法が効果的に機能していることを確認すべきである。

指針

（略）

6.2　包括的な方針

取締役会は、会社全体にわたり、リスクの監視に包括的な方針を採用すべきである。これには、企業のビジネスモデル、サイバーセキュリティ、サプライチェーンの回復力、業績、支払能力、流動性、評判に対する脅威が含まれる。リスクの監視は、財務資本だけでなく、人的資本と自然資本、特に国連の持続可能な開発目標で特定されたシステミックリスクを含むように拡張すべきである。これらは企業のビジネスモデルと戦略に関連している。重要なことはリスク許容度に関する取締役会の合意であり、取締役会はこれを分かりやすい用語で一般に周知させるよう努めるべきである。

（略）

（注）　下線は野村資本市場研究所による。
（出所）International Corporate Governance Network, “ICGN Global Governance Principles,” 2021、より野村資本市場研究所作成

VI 今後の論点

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ており、サイバーセキュリティの重要性がますます高まっている。

各国のサイバーセキュリティ関連の情報開示規制の流れを見ると、開示拡充の方向性は共通しているものの、米国 SEC のように情報開示に係るエンフォースメントを実施する動きや、英国 FRC の財務報告ラボのプロジェクトのように投資家も含めたステークホルダーともに有用な開示について検討するといった動きが見られる。コーポレートガバナンス・コードをめぐっては、前述のとおり、2022 年に公表された「G20／OECD コーポレートガバナンス原則」の改訂案の内容に鑑みると、将来的に日本を含めた各国の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含まれる可能性があるとみられる。

ESG評価機関と信用格付会社では、サイバーセキュリティの要素を評価・分析に織り込み始めているが、サイバー犯罪や攻撃の複雑化・巧妙化、被害の拡大等の状況に鑑みると、評価・分析項目や手法は今後も継続的に見直される可能性があり、注視が必要と言える。そして、グローバルな投資家団体による活動については、サイバーリスクが企業価値に及

ぼす影響の甚大化を踏まえると、本稿で取り上げた ICGN、PRI 以外にも企業、投資家に対してサイバーセキュリティへの対応を求める声が投資家団体等から上がる可能性がある。

IT・デジタル化、デジタル・トランスフォーメーション（DX）[49]が進む一方で、サイバー犯罪・攻撃が複雑化・巧妙化・甚大化しているため、サイバーセキュリティ関連課題対応に終わりを定めるのは困難と言える。そのため、サステナブルな情報化社会の実現に向け、企業、投資家、政府・規制当局を始めとした多数のステークホルダーが一丸となってサイバー関連課題に関する対応を続ける必要がある。

投資家は、（1）サイバー関連の動向やリスク、潜在的な価値をしっかり見極める眼を養うこと、その上で、（2）エンゲージメントを通じて企業に適切なサイバーセキュリティ関連対応を促すこと、ができる。そして、このような取り組みを通じて、投資パフォーマンスの向上のみならず、社会全体のサイバーセキュリティ強化にもつながり得るため、大切な役割を果たすと考えられる。

[49] IT 化とデジタル化はほぼ同じ意味で使われる局面が多く（ただし、イメージとしては、デジタル化の方が意味的な範囲が少し広い）、IT ツールの導入、デジタルデータ・技術の活用を指す。DX と IT 化は目的が異なる。IT 化の主な目的は業務の効率化、DX はビジネスモデルや業務の変革である。（経済産業省中小企業庁「『デジタル・トランスフォーメーション』DX とは何か？ IT 化とはどこが違うのか？」）