# 信用力評価とサイバーセキュリティ
## －リスクへの備えがガバナンス評価を通じて格付に影響－

野村證券 IB ビジネス開発部
（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 客員研究員）
今川　玄

▌要　約▐

1. 信用格付においてサイバーリスクの影響が拡大しつつある。外資系格付会社の大手 2 社である S&P グローバル・レーティング（以下、S&P）、Moody's は従前からサイバーリスクについて言及していたが、ロシアによるウクライナ侵攻や米中対立といった地政学リスクの高まりがより鮮明になって以降、格付評価上のサイバーリスクに関する発信を大きく増やしている。S&P は 2022 年 3 月に格付手法を見直し、サイバー攻撃を受ける前であってもサイバーリスクへの備えが不十分な場合は格付に下押し圧力がかかることを示した。また Moody's もサイバー攻撃が格付に影響を与える要因・経路を明確化し、信用力評価におけるサイバーセキュリティの重要性を改めて指摘した。
2. 両社に共通しているのはサイバーセキュリティの取り組みは企業の一部の部門・部署が担うものではなく、経営陣が直接責任を持って対応すべきガバナンスの問題と捉えている点である。ガバナンス評価は格付評価の根幹を成す要素であり、特に外資系格付会社は重視している。S&P の格付手法の見直しでは、サイバーリスクを「経営陣とガバナンス」の評価項目に組み入れている。
3. サイバー攻撃に伴う格付アクション（格下げ、格付見通しの引き下げ、格下げ方向での見直し）はこれまでのところ少数にとどまっている。格付を取得する企業の多くは規模が大きく財務耐久力も相応にあり、サイバー攻撃による事業上・財務上の影響を吸収する余力が高かったためとされている。しかし、地政学リスクの一層の高まり、デジタル化の進展、生成人工知能（AI）や量子コンピューターといった新技術の出現等によって、サイバーリスクの格付へのネガティブな影響が拡大・深化することを S&P、Moody's ともに予測している。一方、日系格付会社からは 2024 年 10 月末時点で、格付評価上のサイバーリスクに関する言及はほぼなく、今後の発信・情報提供が待たれる。

# Ⅰ　サイバーリスクの拡大と信用格付における位置付けの明確化

サイバーセキュリティは信用力評価においても影響が拡大しつつある。サイバーリスクの脅威とそれへの備えについては日々報道で目にする。以前からサイバーセキュリティの重要性は広く一般に指摘されていたが、米中対立やロシアによるウクライナ侵攻によって、また 2024 年 11 月の米大統領選挙等もあり、サイバーリスクへの警戒は加速度的に強まっている。S&P グローバル・レーティング（以下、S&P）、Moody's といった外資系格付会社においても特にウクライナ侵攻以降、サイバーリスクに関する発信が増えており、格付評価への影響や織り込み方（格付手法）についても明確化が進みつつある。

S&P は 2022 年 3 月 30 日にサイバーリスクの信用格付への織り込み方についてレポート「How Cyber Risk Affects Credit Analysis For Global Corporate Issuers）」[1]を公表し、このなかで従来の評価軸であったサイバー攻撃後の収益・財務等への影響の分析から大きく踏み込んで、サイバー攻撃前であってもサイバーリスクへの備えが十分でない場合には格付への下押し圧力が強まる（＝格下げの可能性が高まる）と格付手法の事実上の転換とも受け止め得る考え方を導入した。

Moody's も 2024 年 6 月 4 日付のレポート「Cyber Risk-Global Not all cyberattacks are created equal」においてサイバー攻撃に関連した格付アクションの事例を示しつつ、サイバーリスクが格付に影響を与えるプロセスを整理して説明している。

S&P、Moody's いずれにも共通しているのはサイバーリスクへの備えと対処は当該企業の一部の部門・部署が責任を負うレベルのものではなく、経営陣が責任を負って向き合う事項であり、格付評価の根幹を成すコーポレートガバナンスの在り方と実効性に直結すると捉えている点である。

# Ⅱ　S&P：サイバーリスクの格付上の評価と格付アクション

## １．カバナンス評価への組み込み

S&P は 2022 年 4 月 14 日付の前掲邦訳レポート（以下、同レポート）でサイバー攻撃による格付への直接的な影響について「これまでのところ、サイバーインシデントに直面したほとんどの事業会社は、十分な財務的なバッファを持っていたため、格付けへの影響は限定的だった」としたうえで、「サイバーリスクが増大する脅威を示していることから、今後数年間で格付けへの大きな下方圧力になる可能性が高い」[2]と指摘し、サイバーリスクに起因した格下げが中期的に高い頻度で起こるとの見通しを示唆した。

また、「サイバーリスクは、ハッカーの目標、動機、能力（企業が所有する資産や重要

[1] 同社邦訳レポートは、「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。

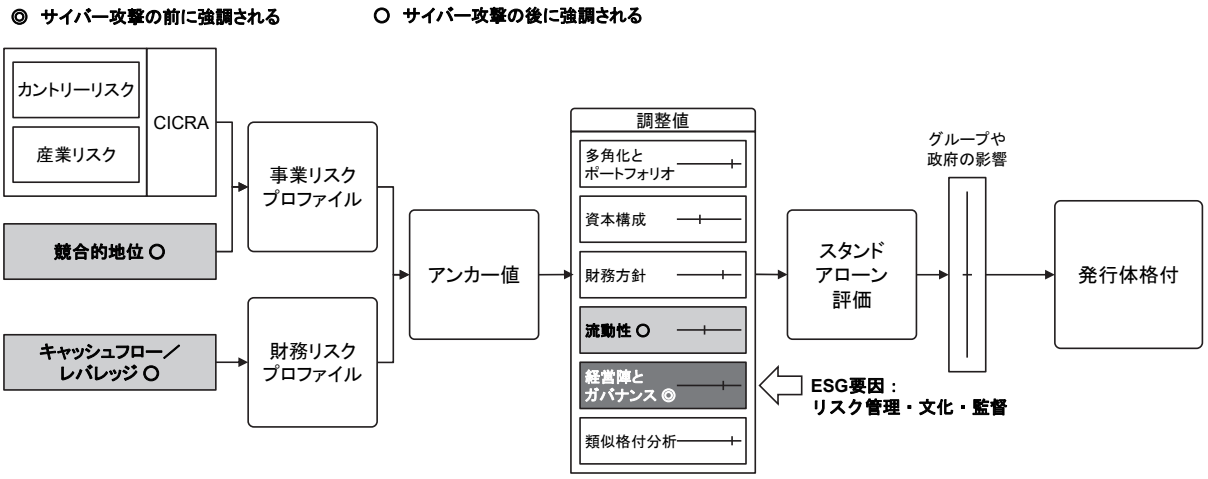
[2] 原文は we believe cyber risk represents a growing threat and will likely pose greater downside risks on credit ratings over the coming years と記されている。

なインフラに対する重要性によって決定される可能性が高い）と、企業・組織のサイバーリスクへの準備状況の組み合わせによって発生する」と前置きし、「事業会社がガバナンス体制にサイバーリスク軽減戦略を組み込んでいないと S&P が判断する場合、同じ競合的地位にある同業他社よりも格付けが低くなる可能性がある」と説明した。従来は同じような事業基盤、規模、収益力、レバレッジの会社であればほぼ同じ格付が付いていたものが、今後はサイバーリスクへの備えの評価次第で格付に差の付く可能性があるとしている。

注目すべきはサイバーリスクへの取り組みをガバナンス体制に組み込んでいるかどうかを分析の起点にしていることだ。サイバーリスク軽減戦略を企業の一部門の担当としてではなく、トップを含めた経営陣の明確なコミットの下で機能しているかどうか、その実効性を評価すると述べている。この考え方は同レポートで示された事業会社の格付規準の枠組みに示されている（図表 1）。

S&P の格付決定プロセスにおける「経営陣とガバナンス」[3]の評価はその内容次第で格付を 2 ノッチ以上引き下げる要因となる。経営陣とガバナンスは 8 つの経営陣に関する評価項目と 7 つのガバナンスに関する評価項目で構成されており、サイバーリスクへの備えは通常、経営陣の評価項目の一つである「リスク管理基準とリスク許容範囲の包括性」で勘案するとしている。

図表 1　S&P の格付決定プロセスにおけるサイバーリスクの織り込み




（注）　CICRA は、産業別カントリーリスク評価（Corporate Industry and Country Risk Assessment）の略称。
（出所）S&P グローバル・レーティング「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、8 頁より野村證券作成

[3] S&P の事業会社の格付決定プロセスにおける「経営陣とガバナンス」の評価は、同社の信用格付における ESG 評価においては広く「ガバナンス要因」として分析される。ガバナンス要因は①ガバナンス構造、②リスク管理・文化・監督監視、③透明性と報告、④その他のガバナンス要因、に分類され、サイバーリスクへの準備状況は②リスク管理・文化・監督の中で評価される。信用格付における ESG 評価については、S&P「一般格付け規準：信用格付けにおける環境・社会・ガバナンス（ESG）の原則」2021 年 10 月 20 日を参照。

## ２．サイバーリスクへの備えの評価

S&P はサイバーリスクへの備えの評価に際して、米国立標準技術研究所（National Institute of Standards and Technology, NIST）の評価の枠組み（図表 2）を活用するとしている。S&P は「ほとんどの事業会社が、NIST の 5 つの中核的なフレームワーク機能のそれぞれに対応するために、適切なレベルのサイバー防衛を整備することを期待している」という。

図表 2 に関して、「サイバーリスクへの準備状況を評価する場合、S&P は、正式に文書化されたサイバーセキュリティ戦略が存在するかどうか、また、事業会社が定期的にその有効性と成熟度を測定しているかどうかの理解を試みる。（中略）サイバーセキュリティの最終的な責任者は誰か、どのように事業会社がサイバーセキュリティに予算を割り当てているか、取締役会のサイバー専門家の力を借りているか、適切なレベルのサイバー保険に加入しているか、システミックリスクから生じる例外を方針で考慮しているかどうかを理解しようとする」と説明している。

図表 2　サイバーリスクへの準備状況の評価

| サイバーリスクへの準備状況の評価 |
| --- |
| **I. サイバーリスクの識別**<br>事業会社は自社の外部環境を理解しており、主要なリスクに対処するサイバーセキュリティ戦略を導入している。同戦略に基づき、より広範な ERM（Enterprise Risk Management）の枠組みの一部として戦略を管理しテストするためのリソースを割り当てる。事業会社は、自社の物理的な資産、デジタル資産、第三者への依存度を熟知しており、リスク許容度を設定し、取締役会の説明責任も新たに設置した。 |
| **II. 資産の防護**<br>これには、ファイアウォール、ウイルス対策、スタッフの研修といったサイバー衛生対策の実施が含まれる。事業会社は、定期的にシステム・アクセス監査や、金銭支払いに関する管理を行う。 |
| **III. サイバー攻撃の検知**<br>システムを監視し、潜在的な脅威を検出するためのツールとプロセスを確立している。 |
| **IV. 対応と被害の抑制**<br>サイバー攻撃の影響を抑え軽減するためにインシデント対応計画が規定され、頻繁にテストされている。関連する利害関係者と連絡を取っている。そこで得られた教訓を生かすためにインシデントを分析している。 |
| **V. 復旧**<br>バックアップからのデータの復旧、システムの再構築、その他の方法によるシステムへのアクセスの回復、主要な利害関係者への連絡、リスク管理方針・手法へ教訓として反映している。 |

（出所）S&P グローバル・レーティング「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、7 頁より野村證券作成

## ３．サイバー攻撃に関連した格付アクション

S&P が 2024 年 10 月末時点で、サイバー攻撃が起こる前に備えが不十分だとしてネガティブな格付アクションを起こした事例は確認できていないものの、サイバー攻撃が関連した格付アクションは出始めている。

例えば、ネットワーク、システム管理ソフトを提供する米国のソーラーウィンズ・ホールディングスの事例（図表 3-1）ではマルウェアの感染が顧客にも深刻な被害が広がる可能性を理由に「B+」から「B」に引き下げた。格付の検討事項としては「競合的地位」と「キャッシュフロー／レバレッジ」の悪化を挙げている（検討事項については図表 4 参照）。

図表 3-1　S&P　サイバー攻撃に伴う格付アクションの事例

**ソーラーウィンズ・ホールディングス**

- 長期格付／アウトルック：「B+／安定的」
- セクター：テクノロジー・ソフトウェア
- サイバー攻撃の種類：マルウェア
- 格付の検討事項：競合的地位、キャッシュフロー／レバレッジ

■ ソーラーウィンズ・ホールディングスは 2020 年 12 月 14 日に、同社の監視ソフト「オリオン」製品が、脆弱性（訳注：Vulnerability。システムやプログラムなどの技術的な欠陥のこと）を注入するマルウェア「サンバースト」に感染し、オリオンが動作するサーバーが侵害されたことを報告した。脆弱性は、2020 年 3 月から 6 月にかけてリリースされた同製品のアップデート時に注入された。同製品は同社の総売上高の 45%を占めた。同社の 30 万社以上の顧客のうち、3 万 3,000 社がオリオン製品の保守管理を実施する顧客だった。同社は、この脆弱性を含むバージョンのオリオンをインストールした顧客は 1 万 8,000 社未満と見積もっていた。

■ S&P は 2020 年 12 月 22 日に、ソーラーウィンズの格付「B+」を引き下げ方向の「クレジット・ウォッチ」に指定した。新たな情報により、感染の影響を受けた顧客が深刻な被害を受ける可能性があることが判明したためである。特に、新規販売や既存の顧客基盤の縮小に対するリスクの高まりを指摘した。

■ 2021 年 4 月には、ソーラーウィンズの格付をサイバーインシデントを主因に B に引き下げた。アウトルックは「安定的」とした。同社は同インシデントを適切に管理し、積極的なコミュニケーションによって復旧と修復を円滑に進めたが、2021 年は収益が伸び悩み、費用が増加し、収益性が低下した。この時点で S&P では、同社の顧客が同社のソフトウェアを更新する比率は、サンバーストに感染する前の 90%台前半から 80%台前半に低下し、また、セキュリティ対策を強化するための年間費用が最大 2,500 万ドルになると予想していた。傘下のマネージド・サービス事業を手掛ける米 N エイブルの分社化もあり、同社の S&P による調整後総有利子負債の対 EBITDA（利払前・税引前・減価償却前利益）倍率は 6 倍超に上昇した。約 2 年後、更新率はサンバースト感染前の過去最高の水準にまで上昇したものの、純新規事業への感染の影響が長引いており、同社の成長は引き続き逆風下にある。今回のマルウェアへの感染は、信用力に影響を与える ESG 要因の中で、引き続き非常の大きなマイナスの社会的要因であり、S&P による同社の競争力の評価と業績予想を押し下げている。

（注）　表冒頭の格付「B+」は 2024 年 10 月 10 日時点。
（出所）S&P グローバル・レーティング「事業会社セクターにおけるサイバーリスクの見通し：サイバー脅威の潜在的影響は増しつつある」2022 年 12 月 8 日、7-8 頁より野村證券作成

一方、外貨両替を手掛ける英国のトラベレックス・ホールディングスはマルウェアに感染し、オンラインサービスのオフライン化の措置を取った。これを受けて S&P は同社の格付「B-」を格下げ方向のクレジット・ウォッチに指定し、同社の評判とブランドへの悪影響が及ぶ可能性を理由にガバナンスと内部統制について懸念を発信した。その後、さらに「経営陣とガバナンス」の評価を引き下げ、段階的に格下げを実施し、最終的には 2020 年 8 月、「全面的な債務不履行（D）」との判断に至った（図表 3-2）。

図表 3-2　S&P　サイバー攻撃に伴う格付アクションの事例

**トラベレックス・ホールディングス**

- 格付：なし
- セクター：旅行、レジャー
- サイバー攻撃の種類：マルウェア
- 格付の検討事項：競合的地位、キャッシュフロー／レバレッジ、流動性、経営陣とガバナンス

■ トラベレックス・ホールディングスは 2020 年 1 月 2 日に、マルウェアに感染し、オンラインサービスに障害が発生したため、システムのオフライン化を余儀なくされたと報告した。マルウェアは主に同社のオンラインサービス部門に影響を与え、予防措置として執られたシステムのオフライン化は結果的に、英テスコ、英セインズベリーズ、英 HSBC、英ヴァージン・マネーを含む同社の顧客のオンラインサービスに影響した。顧客とのサービスに関する契約条件の違反に加え、このマルウェア感染による風評被害は、同社の市場地位と業務委託契約を更新する能力に影響する可能性があった。

■ S&P は 2020 年 1 月 9 日に、トラベレックスの格付（B-）を引き下げ方向の「クレジット・ウォッチ」に指定した。その時点でマルウェア感染による混乱の全容は明らかになっていなかったが、S&P は、同混乱は、トラベレックスの評判とブランドに影響を与えると判断し、同社のガバナンスと内部統制の強さと妥当性について懸念を提起した。サイバー攻撃の解決までに要した時間と同攻撃に関する報道によって受けた風評被害に基づき、同社の経営陣とガバナンスの評価を、「やや弱い」から「弱い」に変更した。同社の単体ベースでの高レバレッジの資本構成と格付の余裕度が低下していたことが、サイバー攻撃の規模と影響の範囲と重なって、同社の単体ベースの信用力が問われることとなった。

■ S&P は 2020 年 3 月 4 日に、ランサムウェア攻撃の連鎖効果と、新型コロナウイルス感染症による取引量の減少により、2020 年第 1 四半期の EBITDA が 2,500 万ポンド減少したことに基づき、トラベレックスを「CCC」に格下げした。同社は段階的かつ管理されたプログラムにより顧客向けシステムをすべて復旧させ、2020 年の残りの期間中のマルウェアによる影響を軽減した。同社はサイバー保険により復旧費用の一部を回収した。しかし、保険金の支払いのタイミングやサイバー攻撃の規制上の影響は、S&P による「CCC」への格下げ時点では明確でなかった。また、S&P はコロナ禍の混乱とそれが通期業績に与える影響により、同社が資本構成を持続することが極めて困難になる可能性があるとの見解を示した。

（注）　表冒頭の格付（なし）は 2024 年 10 月 10 日時点。
（出所）S&P グローバル・レーティング事業会社セクターにおけるサイバーリスクの見通し：サイバー脅威の潜在的影響は増しつつある」2022 年 12 月 8 日、9 頁より野村證券作成

図表 4　S&P　サイバー攻撃が格付に与える影響

| | |
|---|---|
| **競合的地位** | サイバーインシデントは、ブランドや評判の悪化、顧客の解約、事業の中断、または収益性に影響を与える費用の増加により、事業会社の競合的地位を害する可能性がある |
| **流動性** | ランサムウェア、セキュリティへの投資、外部コンサルタントへの支払い、訴訟、顧客への補助金などに起因する財務上の損失により、事業会社の流動性がネガティブな影響を受ける可能性がある |
| **キャッシュフロー／レバレッジ** | レバレッジ:営業費用の増加、またはサイバー攻撃に対する準備不備に対処するための投資は、キャッシュフローにネガティブな影響を与え、収益性を低下させ、財務レバレッジを高める可能性がある |
| **経営陣とガバナンス** | サイバーインシデントによって、企業全般のリスク管理の基準や許容範囲の包括性、取締役会の効果、またはその他のガバナンス要因に関する重大な欠陥が明らかになることによって、経営陣とガバナンス評価や ESG クレジット・インジケーターのネガティブな見直しにつながる可能性がある |

（出所）S&P グローバル・レーティング「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、8 頁より野村證券作成

# Ⅲ Moody's：サイバーリスクの格付上の評価と格付アクション

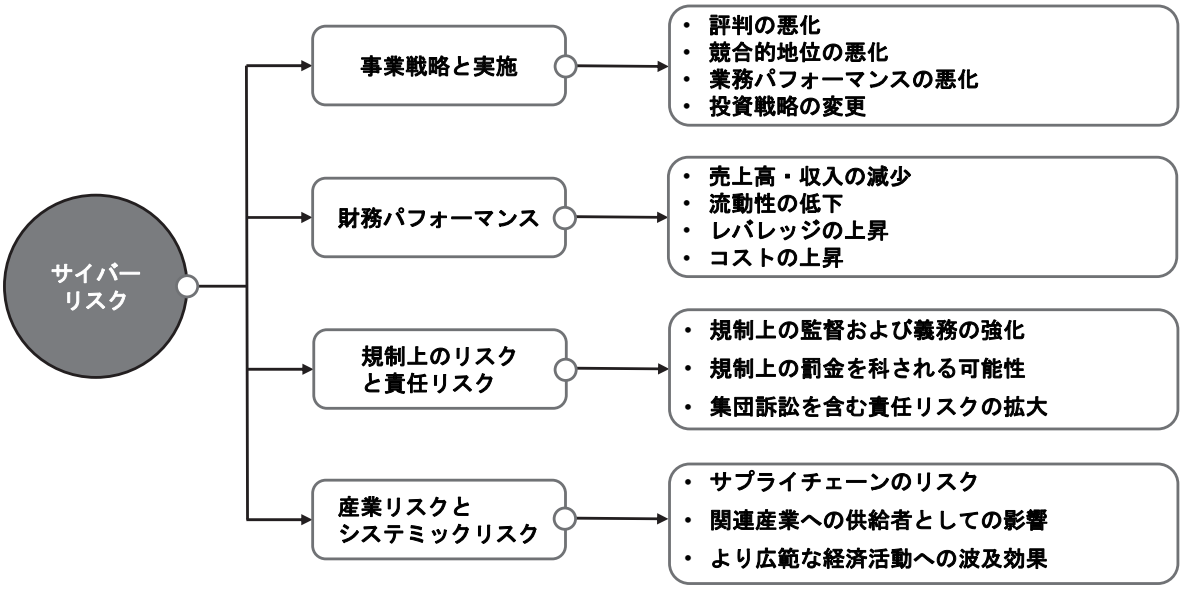
## １．格付に影響を与える経路

Moody's は、前述の 2024 年 6 月 4 日付のレポート（「Cyber Risk-Global Not all cyberattacks are created equal」、以下、同レポート）で、最初にサイバーリスクに関連した格付見直しがあった 2014 年以来、10 の発行体に対して 19 件の格付アクションを実施したとしている。サイバー攻撃がこの 10 年で劇的に増加したにもかかわらず格付アクションが少ない理由として、格付先は総じて規模の大きい企業が多く、サイバーリスクへの比較的充実した備えがあり攻撃による被害を吸収するだけの財務余力が大きい点を挙げている。ただし「サイバー攻撃の深刻さが増し、コストが上昇し、デジタル化が進展し、生成人工知能（AI）や量子コンピューターといった新しい技術が出現する中で、格付に悪影響を及ぼす可能性は高まっている」（同レポート）と見ている。

サイバーリスクが格付に影響を与える要因・経路について、Moody's は「事業戦略と実施」「財務パフォーマンス」「規制上のリスクと責任リスク」「産業リスクとシステミックリスク」の 4 つに分類している。分類ごとにさらに要因を分けて分析する手法を取っているが、各要因・経路を通じて、収入減少と資金流出の一方もしくは両方が起きて財務パフォーマンスが悪化し、格付にネガティブな影響を与えるとしている（図表 5）。

サイバーリスクへの備えはコストがかかるが、適切な備えへの投資は攻撃を受けた際の被害をより小さく、期間をより短く抑えるのに寄与し、結果的に投資額を上回る経済効果を引き出すことができるため、格付評価上ポジティブと位置付けている。また「サイバーセキュリティチームが実施する技術的対策はサイバーリスクへの露出を減少させるために重要だが、サイバーリスクは企業のリスクであり、組織の上級リーダーシップの関与が必要である。Moody's の 2020 年のサイバー調査への回答では、サイバー管理者と経営陣との

図表 5　Moody's　サイバーリスクが格付に影響を与える経路




（出所）Moody's, "Cyber Risk-Global  Not all cyberattacks are created equal," June 6, 2024, p.3、より野村證券作成

間の緊密な報告構造などより堅牢なガバナンスが、サイバーセキュリティへの予算やリソースの配分の増加と相関関係があることが示された」（同レポート）と明記し、サイバーセキュリティの向上には強固なガバナンスが前提になる点を強調している。

## 3．サイバー攻撃に関連した格付アクション

図表 6 は Moody's が 2020 年以降に実施したサイバー攻撃に関連した格付アクションである。事業リスク・財務リスクが比較的高い低格付先（≒サイバー攻撃に対して比較的脆弱と考えられる企業）に加えて、投資適格級の発行体（Capital Region Medical Center、以下、CRMC、格下げ前の格付は「Baa2」）も含まれている。CRMC の事例では「Baa2」（BBB フラット相当）から「Ba2」（BB フラット相当）の投機的水準に 3 ノッチも引き下げられているが、格付アクションの要因はサイバー攻撃だけでなく、情報技術（IT）導入費用の発生や主要契約先の支払不履行、さらに労務費や供給コストの上昇が同時に重なったことが影響したと Moody's はリリース[4]で指摘している。なお、一般的には Moody's、S&P の BBB 格は日系格付に置き換えると A 格～AA 格に、BB 格は BBB 格～A 格に相当する。

Moody's が同レポートで指摘する格付アクションの中には格下げ、格付見通しのネガティブへの変更、格下げ方向での見直しといった格付そのものの下方修正以外に、格付評価上の ESG スコアの引き下げも含まれている（T-Mobile USA、Atlas Purchaser）。格付そのものの見直しには至っていないが、ESG スコアの引き下げも格付評価上はネガティブな要素である。

[4] Moody's, "Moody's downgrades Capital Region Medical Center (MO) to Ba2; outlook negative," December 12, 2022.

図表 6　Moody's　サイバー攻撃に伴う格付アクションの事例（2020 年以降）

| 企業名 | サイバーインシデント発生時期 | サイバーインシデントの内容 | 格付アクションの時期 | 格付アクション | 格付アクションまでの期間 | 格付に影響したその他の要因 |
|---|---|---|---|---|---|---|
| **SolarWinds** | 2019 年 9 月<br>- 2020 年 12 月 | IT 管理ソフトを提供する SolarWinds はサプライチェーンにサイバー攻撃を受けた。犯人は同社の Orion ソフトウェアに悪意のある更新を実施した。この更新を顧客がダウンロードすると、犯人は顧客のネットワークにバックドアアクセスすることができ、被害は政府機関やフォーチュン 500 の企業に及んだ。 | 2020 年 12 月 | B1 を格下げ方向で見直し、その後 Ba1/安定的で維持 | 4 日 | |
| **DTI ("Epiq Global")** | 2020 年 2 月 | 2020 年 2 月、法務サービス会社の Epiq Global はランサムウェア攻撃を受け、数週間の間、特定のシステムをオフラインにせざるを得なくなった。 | 2020 年 3 月 | B3 から Caa2 に格下げし、格下げ方向での見直しを継続 | 1 ヵ月 | コロナ禍による経済低迷 |
| | | | 2020 年 6 月 | Caa2を維持、格付見通しはネガティブ | 4 ヵ月 | |
| **Ultimate Kronos Group** | 2021 年 12 月 | 2021 年 12 月 11 日、労務管理、給与、人事サービスを提供する UKG, Inc.は Kronos プライベートクラウドに影響を与えるランサムウェア攻撃を受けた。その結果、UKG の顧客の多くが従業員の労働時間の確認、給与の支払い、その他の人事関連機能を実行できなった。 | 2021 年 12 月 | B2 を維持、格付見通しを安定的からネガティブに変更 | 11 日 | 非常に競争の厳しい人材管理および給与関連サービスの市場 |
| **Capital Region Medical Center** | 2021 年 12 月 | 2021 年 12 月 17 日、CRMC（米国ミズーリ州）はランサムウェア攻撃を受け、メールや患者登録システムを含むいくつかのシステムがオフラインになった。 | 2022 年 9 月 | Baa2 を格下げ方向で見直し | 9 ヵ月 | |
| | | | 2022 年 12 月 | Baa2 から Ba2 に格下げ、格付見通しはネガティブ | 1 年 | |
| **T-Mobile USA, Inc.** | 2022 年 11 月 | T-Mobile は 2023 年 1 月 5 日に、悪意のある第三者が外部のアプリケーション・プログラミング・インターフェース（API）を介して、約 3700 万のアクティブなポストペイドとプリペイド顧客アカウントのデータに不正アクセスしたことを発表した。 | 2023 年 1 月 | 信用格付上の ESG スコアの S（5 段階評価）について S-3 から S-4 に引き下げ | 2 ヵ月 | T-Mobile はこの事件に至るまでの数年間に少なくとも 6 件のサイバーセキュリティ・インシデントを認識していた（2022 年、2021 年、2019 年、2018 年にそれぞれ 1 件、2020 年には 2 件発生） |
| **Atlas Purchaser, Inc. ("Alvaria")** | 2023 年 2 月 | 2023 年 2 月 22 日、Alvaria, Inc. はランサムウェア攻撃に関連するデータ侵害の通知を提出した。この事件により、無許可の第三者が消費者の名前、社会保障番号、パスポート番号、財務口座情報、健康保険情報、税金関連情報にアクセスすることができた。 | 2023 年 11 月 | 信用格付上の ESG スコアの S（5 段階評価）について S-3 から S-4 に引き下げ | 9 ヵ月 | |

（出所）Moody's, "Cyber Risk – Global　Not all cyberattacks are created equal," June 4, 2024、より野村證券作成

## Ⅳ 結び

S&P、Moody’s ともにサイバーセキュリティに関するソリューソンの提供と併行して、信用格付評価におけるサイバーリスクの位置付けの明確化、関連レポートの発信を進めている。今のところサイバー攻撃に起因する格下げ数は多くないものの、地政学リスクの高まり、デジタル化の進展、生成 AI の加速度的な発展等を背景に、両社ともに格付への影響が拡大・深化することを想定している。本稿では企業価値を構成する一方の要素であるクレジットの観点に焦点を当てたが、サイバー攻撃への備えの緩さがキャッシュフロー、損益の悪化に繋がり得る点は当然ながら株主価値にも結び付く。

本稿において、日本の格付会社の動向について触れなかったのは、格付投資情報センター（R&I）、日本格付研究所（JCR）のいずれからも格付評価におけるサイバーリスクに関する言及が 2024 年 10 月末時点でほぼ皆無だったためである。Moody’s、S&P と比べて企業規模、人員等の制約が大きい点は理解した上で、国内社債市場で最も利用されている日系格付が遅行指標にとどまらないためにも、洞察のある発信を期待したい。