エンゲージメントを通じたサプライチェーンのサイバー・レジリエンス強化
－エンゲージメントを効果的に実践するための新たな手法－

野村アセットマネジメント
債券サステナブル・インベストメント・ヘッド
ジェイソン・モーティマー

▌要　約▐

1. 企業は、自社およびサプライチェーン上の取引先企業のネットワークの脆弱性に起因するサイバーセキュリティ・リスクに直面している。自動車、金融、小売りの各業種において大きな注目を集めた有害事象は、サプライチェーンに対するサイバー攻撃がバリューチェーン全体にわたって業務を混乱させ、データを危険にさらし、その結果、重大な経済的損失や重要な国家機能への障害をもたらす可能性があることを示している。
2. 上流・下流の取引先企業が抱えるサード・パーティへの脆弱性を特定し、緩和するために、「サイバー・サプライチェーン・リスク管理（C-SCRM）」は不可欠であり、企業の最高情報セキュリティ責任者（CISO）、規制当局、投資家にとっても重要な関心事項となっている。
3. サイバーセキュリティに関する定量的なパフォーマンス・データを活用して、サプライチェーン全体のリスクを評価した上で、バリューチェーンの全階層において効果的なサイバーセキュリティの枠組みを確実に構築するよう企業に働きかけることが、投資家にとって選択肢となる。これは、スコープ 3（サプライチェーン）における排出量と労働者の権利が一般的にモニタリングされているのと相似形である。
4. 投資家はこのような先を見越したアプローチによって、重大なリスクを特定し、投資リターンの改善を期待できるようになる。同時に、全体的なサイバー・レジリエンスの強化や、サイバーセキュリティ・リスクに関連する社会経済的な影響への対応にもつながる。

Ⅰ はじめに

企業経営者、規制当局、投資家にとって、組織におけるサイバーセキュリティはますます重要なリスク・ファクターとなっている。最近、大きな注目を集めた自動車、金融、小売りの分野でのサイバー事故は、多くの場合、業務や財務に与える影響が対象企業一社にとどまらず、エコシステム全体にも波及し、財務面や社会経済面で深刻な意味を持つことを証明している。今日の企業には、自社の製品・サービスだけでなく、サプライチェーン上の取引先企業の製品・サービスの完全性、安全性、強靭性を確保することが求められている。社会経済のサステナビリティに貢献しつつ、この新たなリスク・ファクターを体系的に統合、評価することに関心のある投資家は、この動きに注目すべきであろう。

組織のサイバーセキュリティ・リスクは、自社のネットワークやシステム（サイバーセキュリティの境界線）の脆弱性にとどまらず、上流・下流のサプライヤー、受託業者、デジタル・サービス・プロバイダーの脆弱性にも関連する。これは「サイバー・サプライチェーン・リスク管理（C-SCRM）」と呼ばれる概念であり、企業の最高情報セキュリティ責任者（CISO）、規制当局、サイバー・リスクに敏感な取締役会にとって重要な関心事項となっている。企業には、現在の相互性の強いサプライチェーンから発生するサイバーセキュリティ・リスクを特定、評価、緩和することが求められている。

Ⅱ サイバー・サプライチェーン・リスク管理（C-SCRM）について

サイバー・サプライチェーン・リスクが実世界に影響を与えた事例として、2022年3月に日本の大手自動車メーカーが、非上場の取引先部品メーカーで発生したサイバー事故の影響で、国内 14 工場の稼働停止に追い込まれた事例が挙げられる。サイバー・サプライチェーン・リスクは、その名称から受ける印象とは裏腹に、物理的なサプライチェーンにとどまらず、企業のデジタル・サプライチェーンを構成するソフトウェアやサービスのプロバイダーにも波及している。また、別の事例を挙げると、2024 年 6 月には、自動車ディーラー向けソフトウェア・プロバイダーに対するランサムウェア攻撃の影響によって、複数の自動車メーカーが全米数百のディーラーでの販売停止を余儀なくされている。残念ながら、サイバー・サプライチェーン・リスクの脅威を完全に把握し、対策を講じることは非常に難しい。さらに、悪名高い事例として、2014 年に米国の大手小売業者が、7,000万件の顧客クレジットカード情報を失った事例が挙げられる。サード・パーティである暖房・換気・空調（HVAC）受託業者のハッキングにより、犯罪者がベンダー・ポータルを通じてこの小売業者のサーバーにアクセスしたケースである。

また、C-SCRMは銀行をはじめとする金融サービス会社にも関連するものであり、金融規制当局においても、ベンダー・サプライチェーンやデジタル・サプライチェーンの脆弱性が、最も重大なサイバーセキュリティ・リスクとして認識されている。サイバーセキュリティの評価会社であるセキュリティ・スコアカード社の最近の調査によると、欧州の大

手金融機関 240 社のうち 78%が、過去 1 年間にサード・パーティによるデータ漏洩を経験している。このうち 18%のセキュリティ・パフォーマンス・レーティングは、レーティング上位の企業と比べて漏洩リスクが 7 倍高いことを示している。

高度なサイバーセキュリティ対策を独自に備えた銀行でさえも、サプライチェーンにおけるサイバー事故がもたらす世界的な影響に直面する可能性がある。一例を挙げると、2023 年にデリバティブ取引のソフトウェア・プロバイダーに対するランサムウェア攻撃の影響によって、銀行業界は電子取引の処理をスプレッドシート上での手作業に切り替えざるを得なくなった。このハッキングは商業的な動機によるものであり、直接的な影響は限定的であったが、特に政府からの支援を受けた当事者が関与する場合には、同様の攻撃が金融市場にシステミック・リスクを引き起こす可能性があることを、世界中の金融規制当局に警告する形となった。今後は、金融セクターに属する企業にとって、サイバーセキュリティのベストプラクティスに関するサービス・パートナーの評価とエンゲージメントが、重要な課題になると予想される。

一連の事例は、サプライチェーン上流・下流の取引先企業の脆弱性が、自社に対する直接的な侵害と同様に混乱や損失を生じさせる可能性があり、サイバーセキュリティの境界線を防御するだけでは、より広範なリスクへの対応として不十分であることを示している。実際、小規模な組織は、サイバーセキュリティ・リスクを効果的に管理するためのリソースや専門性が不足する傾向にあり、ハッカーにとって、サプライチェーン上の取引先企業は攻撃しやすい魅力的な標的になることが多い。

このような状況に対応するため、米国立標準技術研究所（NIST）は、組織がサイバー・サプライチェーン・リスクをより効果的に管理するためのガイドラインを更新している。米国では、国土安全保障省や証券取引委員会をはじめとする規制当局が、このようなサイバーセキュリティの側面に対する監督を強化している。また、EU の「デジタル・オペレーション・レジリエンス法（DORA）」や米国の「国家のサイバーセキュリティ強化に関する大統領令（EO14028）」などの新しい規制では、サプライチェーン上の重要なソフトウェアのセキュリティの重要性を踏まえて、デジタル経済において企業が従うべき新たな要件が定められている。これらの要件に従うことは、単なる規制上の負担ではなく、企業やその投資家にとって、サイバー・リスクの監視と業務のレジリエンスを向上させる機会にもつながる。

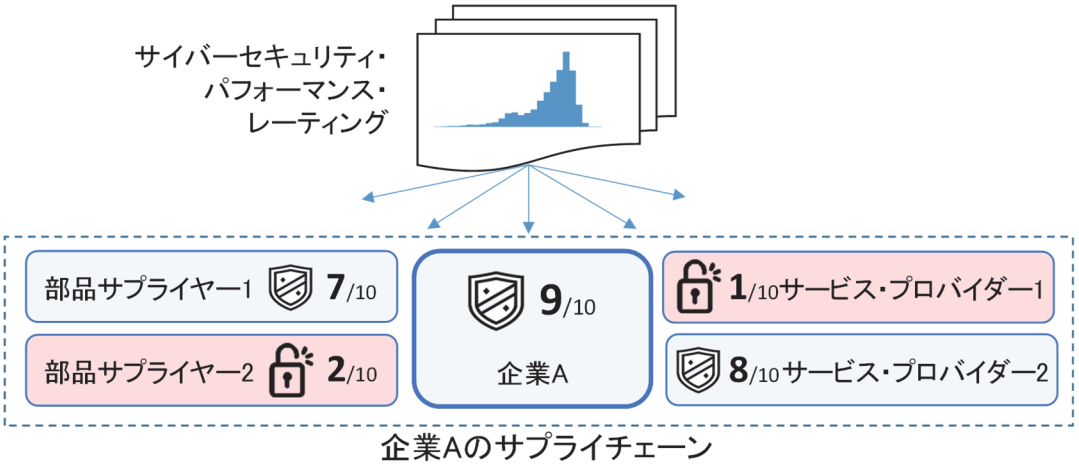
Ⅲ 投資家の C-SCRM に関するエンゲージメント戦略

サイバー・サプライチェーン・リスクは、企業自身の業務や評判に悪影響を与えるだけでなく、ビジネス、法律、財務に関連する影響を生じさせ、経済活動や基幹サービス、消費者データ保護の分野で混乱を引き起こすなど、社会経済的な悪影響を及ぼす可能性がある。このため、投資先企業を分析し、エンゲージメントに取り組む投資家にとって、サステナビリティの観点からも重要になる。しかしながら、脅威が外的な性質を有し、潜在的なリスク要因が多いことを考えると、影響を受ける企業にとって、さらには情報の非対称性に直面する外部の投資家にとって、サプライチェーン・リスクの管理は難しい問題となる。それでは、実際に投資家ができること、すべきことは何であろうか。

ここでは、サイバーセキュリティに関する定量的なパフォーマンス・データを活用することで可能になった、斬新で補完的なアプローチを 2 つ紹介する。投資家の間ではそれほど認識されていないものの、外部から観測可能なサイバー・テレメトリー・データ（遠隔技術を通じて収集されるシステムやネットワークの状態に関するデータ）を活用することで、対象組織におけるサイバーセキュリティの成熟度や、ランサムウェアおよびデータ漏洩に関する相対的なリスクを分析することが可能になった。これらのデータだけで、企業のプライベート・ネットワークにおけるサイバーセキュリティの状態を完全に把握することは不可能だが、データの偏在性、客観性、比較可能性によって、他のサステナビリティ要因にも共通するデータの開示不足という課題に対して、効果的な対策が講じられている。

投資家はサイバーセキュリティ・リスク・レーティングを活用することによって、個別企業のサイバーセキュリティ・スコアに対する分析を定量的に拡充し、既知のサプライヤーやサービス・プロバイダーのパフォーマンス（サード・パーティリスクおよびそれ以外の当事者のリスク）を反映させることができるようになった（図表 1）。例えば、「企

図表 1　サプライチェーンにおける企業のリスク評価に
サイバーセキュリティ・パフォーマンス・レーティングを統合する手法



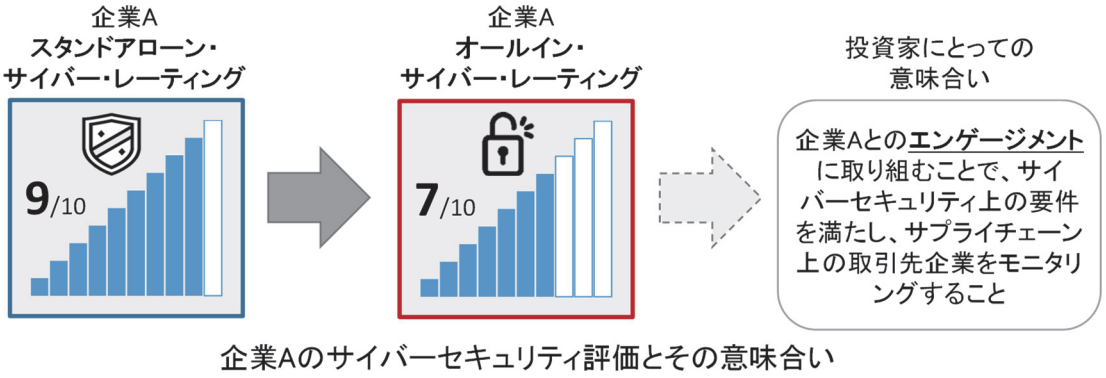
（出所）野村アセットマネジメント

業 A」が適切なサイバーセキュリティ管理を実践しているのに対して、主要な納入業者である「サプライヤーB」のパフォーマンスが見劣りするようなケースでは、より包括的に投資リスクを評価するために、「企業 A」の全体的なサイバーセキュリティ・パフォーマンス・レーティングをその分だけ下方修正するべきであろう。

ハイレベルな定量的評価は、個別組織に対する詳細な C-SCRM 分析を代替するものではないが、一般的な投資家にとってそのレベルの定性的な詳細は不要であろう。代わりに、トップダウンの相対リスクに基づく手法が、最も重要なリスクを簡易に特定するのに適している。サイバー・サプライチェーン・リスクが多くの判断材料の 1 つに過ぎないような、大規模な企業向け投資に取り組む投資家にとっては、分析の効率性とスケーラビリティは特に重要な留意点である。

企業とのサプライチェーン・リスクをテーマとするサイバーセキュリティ・エンゲージメントにおいても、相対的なリスクとスコアに基づくアプローチは有益である（図表 2）。投資家は、温室効果ガスのスコープ 3 排出量や生物多様性、人権問題といった従来のサステナブル投資に関するエンゲージメントの概念を、サプライチェーン・リスクに応用することが可能である。これらの環境や社会に関連するリスクは、サイバー・サプライチェーン・リスクと同様に、データ開示が限定的でアクセスが難しい小規模な非上場のサプライヤーに集中する傾向にあり、投資家にとっては評価とエンゲージメントが難しい問題となる。

図表 2　サイバー・サプライチェーン・リスクに関する洞察を統合し、
スコアリングの調整や建設的なエンゲージメントを目指す手法



企業Aのサイバーセキュリティ評価とその意味合い

（出所）野村アセットマネジメント

Ⅳ 結論

サステナビリティの分野においては、投資家は投資先の上場企業との間でリスク管理に関するエンゲージメントに取り組み、サプライチェーン上の取引先企業に対して、ネットゼロ目標へのコミットメントや労働基準遵守のエビデンス提供を要求する。少数派の投資家の多くは、このようなアプローチを採用することによって、議決権行使やバリュエーションの前提調整といった伝統的なエンゲージメント手法を活用しつつ、関連する指標について個別組織のパフォーマンスを分析、追跡できるようになる。

サード・パーティのサイバー・リスクについても、同じ手法を用いて対応するべきであろう。サプライチェーン上の取引先企業がサイバーセキュリティの枠組みを構築し、全階層において実践するよう、投資先企業に働きかけることである。サプライヤーは、セキュリティ対策や透明性向上を促されることで、脅威が緩和され、サイバー・レジリエンスが全体として強化される。このようなデータに基づく実践的なアプローチを通じて、サプライチェーン全体におけるサイバーセキュリティの強化を促し、リスクを管理しつつ、投資リターンの改善を図るという重要な役割を果たすことが、投資家には可能である。

〔原文 (Original)〕

Investor Engagement for Cyber Resilience in Supply Chains – A new method for integration and effective corporate engagement on cybersecurity supply chain risks –

Jason Mortimer,
Head of Sustainable Investment - Fixed Income,
Nomura Asset Management

▌Abstract ▐

1. Companies face cybersecurity risks from vulnerabilities in their own networks and those of their supply chain partners. High profile incidents in the automotive, financial, and retail sectors demonstrate that supply chains cyberattacks can disrupt operations and compromise data across the value chain, causing material financial losses and impairment to critical national functions.
2. Cybersecurity Supply Chain Risk Management (C-SCRM) is essential for identifying and mitigating third-party vulnerabilities in both upstream and downstream partners, and is now a key concern for business CISOs regulators, and investors.
3. Investors can leverage quantitative cybersecurity performance data to assess risks across supply chains, engaging with companies to ensure that effective cybersecurity frameworks are in place across all tiers of their value chain – just as Scope 3 supply chain emissions and labor right standards are commonly tracked and managed.
4. This proactive approach can identify material risks and potentially improve investment returns, while contributing to overall cyber resilience and addressing socio-economic impacts related to cybersecurity risks.

Ⅰ Introduction

Organizational cybersecurity is an increasingly prominent risk factor for business leaders, regulators, and investors. Recent high-profile cyber incidents in automotive, financial, and retail sectors demonstrate that the operational and financial impacts of cyber incidents often extend beyond a single affected company, adversely affecting entire ecosystems with severe financial and socio-economic implications. Companies are now expected to ensure the integrity, security, and resilience of their supply chain partners' products and services, as well as their own. Investors interested in systematically integrating and pricing this emerging risk factor while contributing to socio-economic sustainability should take note.

An organization’s cybersecurity risk is not limited to vulnerabilities in its own networks and systems (i.e. its cybersecurity perimeter) but also includes those of upstream and downstream suppliers, contractors, and digital service providers. This is known as Cybersecurity Supply Chain Risk Management (C-SCRM), which requires companies to identify, assess, and mitigate cybersecurity risks arising from interconnected modern supply chains, and has become a key focus for Chief Information Security Officers (CISOs), regulators, and cyber risk-aware boards.

Ⅱ Cybersecurity in Supply Chain Risk Management (C-SCRM)

Illustrating the real world impact from supply chain cyber risk, a large Japanese automobile manufacturer in March 2022 was forced to shut down production at 14 domestic plants due to a cybersecurity incident at a single unlisted parts supplier. And despite the name, cybersecurity supply chain risk extends beyond physical supply chains to include software and service providers that make up the company’s digital supply chain. In another example, several car companies were affected by a ransomware attack on an auto dealership software provider in June 2024, halting sales across hundreds of dealerships in the USA. Unfortunately, supply chain cybersecurity threats are notoriously difficult to fully map out and prepare for. In one infamous case, a large US retailer lost 70 million customers' credit card details in 2014 when criminals accessed the retailer’s servers through a vendor portal linked to a hack at a third party HVAC (heating ventilation and air conditioning) contractor.

C-SCRM is also relevant for banks and financial service firms, where vendor and digital supply chain vulnerabilities are now seen as the greatest cybersecurity risk by regulators. A recent study by cybersecurity firm SecurityScorecard found that 78% of 240 large European financial institutions experienced a third-party data breach in the past year, and that 18% of the affected firms had a security performance rating correlating with a seven-fold increased risk of data breach compared to top-rated firms.

Even well-protected banks with sophisticated cybersecurity defenses of their own can face global repercussions from cyber supply chain incidents. For instance, a ransomware attack on a software provider

for derivatives trading in 2023 forced banks to revert to manual processing of electronic trades by hand and on spreadsheets. While this specific hack was commercially motivated and direct impact was limited, this incident alerted financial regulators worldwide to the potential for similar attacks to cause systemic financial market risks, especially if state-backed actors are involved. Moving forward, evaluating and engaging service partners on cybersecurity best practices will be a major focus for financial sector companies.

These examples illustrate that vulnerabilities in upstream and downstream supply chain partners can lead to disruptions and losses just as with direct corporate breaches and that defending a company's cybersecurity perimeter alone is insufficient for addressing the broader range of risks. In fact, a company's supply chain partners often present an easier and more attractive target for hackers, as smaller organizations typically have fewer resources and expertise for managing cybersecurity risks effectively.

In response, the National Institute of Standards and Technology (NIST) has updated guidelines for organizations to manage cybersecurity supply chain risk more effectively. In the USA, regulators such as the Department of Homeland Security and the US Securities and Exchange Commission have increased their oversight on this aspect of cybersecurity. New regulations like the EU's Digital Operations Resilience Act (DORA) and the US's Executive Order 14028 "On Improving the Nation's Cybersecurity" recognize the importance of securing critical software in supply chains and establish new corporate requirements for the digital economy. Complying with these standards is not just a regulatory burden but an opportunity for companies - and their investors - to improve cyber risk oversight and operational resilience.

Ⅲ Investor Strategies for Engagement on C-SCRM

In addition to the adverse effects on the company's own operations and reputation, cybersecurity supply chain risk can have business, legal, and financial repercussions, and cause negative socio-economic impact though disruption to economic activity, critical services, and consumer data privacy. This makes such risks relevant for investors as a sustainability topic to analyze and engage with portfolio companies. However, the external nature of the threat and the high number of potential risk vectors make supply chain risk management a significant challenge for affected companies, and even more so for external investors who face greater information asymmetries. So what can or should investors do in practice?

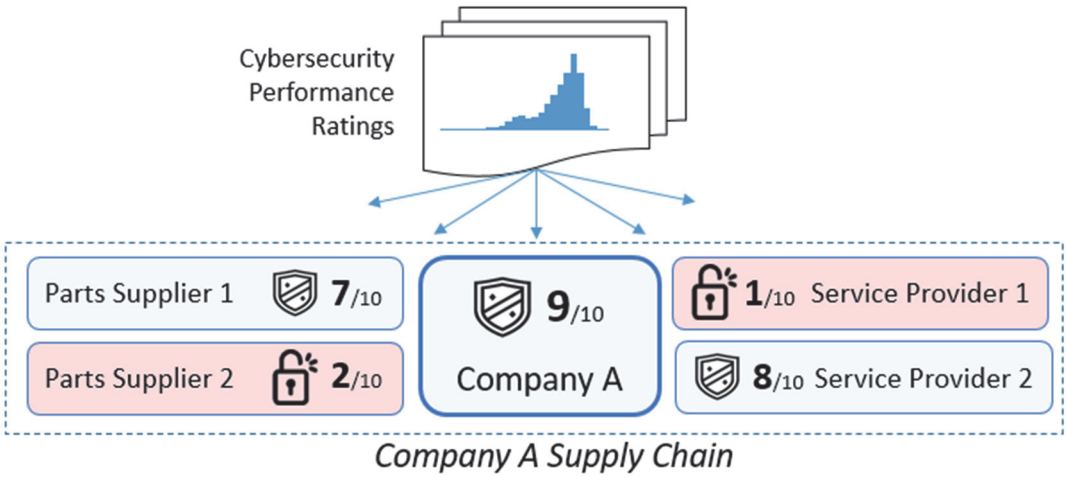
Here we present two novel and complementary approaches, enabled by the availability of quantitative cybersecurity performance data. While still relatively unknown among investors, it is possible to analyze an organization's cybersecurity maturity level and relative risk of ransomware and data breach using externally observable cyber telemetry data. Although these data alone cannot capture the complete cybersecurity posture of a company's private network, their ubiquity, objectivity, and comparability effectively addresses the challenge of insufficient data disclosures common in other sustainability factors.

Investors using these cybersecurity risk ratings can extend the quantitative analysis of an individual company's cybersecurity scores to include the performance of its known suppliers and service vendors (third-party and nth-party risks) (Figure1). For example, if "Company A" demonstrates good cybersecurity management but a key supplier, "Supplier B," has weak performance, then Company A's overall cybersecurity performance should be marked down accordingly for a more complete assessment of investment risk.

While high-level quantitative assessments are not a substitute for in-depth organization-specific C-SCRM analysis, a typical investor will not require this level of qualitative detail. Instead, a top-down, relative risk-based method is better suited for easily identifying the most critical risks. Analytical efficiency and scalability is an especially important consideration for investors considering a large universe of corporate investments where cybersecurity supply chain risk is just one of many factors for consideration.

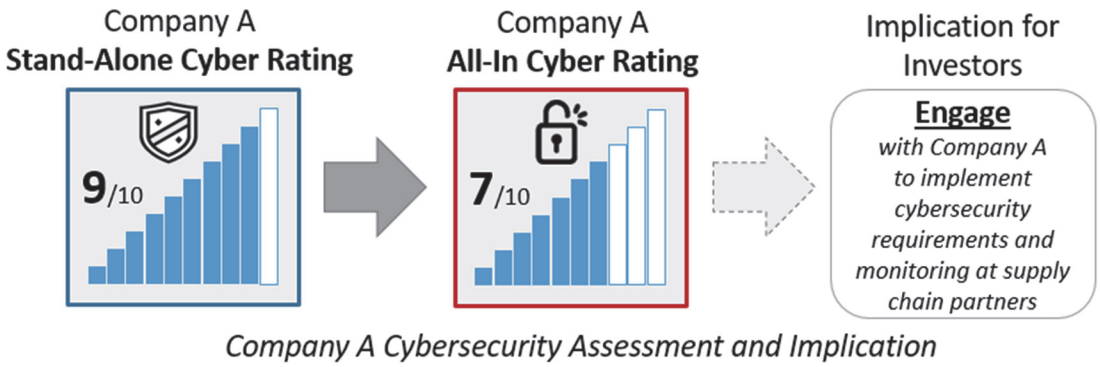
A relative risk and score-based approach can also inform corporate cybersecurity engagements for supply chain risk (Figure2). Investors can apply concepts from traditional sustainable investment engagement on supply chain risks, such as GHG Scope 3, biodiversity, and human rights. Like cyber supply chain risks, these environmental and social risks are often concentrated in smaller, non-listed suppliers where data disclosures are limited and access is difficult, making assessment and engagement a challenge for investors.

Figure 1: A method for integrating cybersecurity performance ratings for corporate risk in the supply chain



Source: Nomura Asset Management.

Figure 2: A method for integrating corporate cybersecurity supply chain risk insights to adjust scoring and target constructive engagement



Source: Nomura Asset Management.

Ⅳ Conclusion

In sustainable markets, investors engage publicly listed portfolio companies on their management of these risks, requiring supply chain partners to commit to Net Zero pledges or provide evidence of compliance with labor standards. This approach allows many minority investors to analyze and track performance for a single entity on relevant metrics, leveraging traditional engagement methods like shareholder voting and adjusting valuation assumptions.

We propose that investors use these same methods to address third-party cyber risks by engaging investee companies to ensure that cybersecurity frameworks are in place and implemented across all tiers by their supply chain partners. Through enlightened self-interest, these suppliers can be encouraged and incentivized to improve their security practices and transparency, thus mitigating shared threats and enhancing overall cyber resilience. With this practical and data-driven approach, investors can play a powerful role to incentivize better cybersecurity across supply chains, manage risk, and potentially improve investment returns.