企業のサイバーセキュリティ・パフォーマンスのグローバル・ヒートマップ

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. サイバーセキュリティは、デジタル化が進む市場において、企業のレジリエンス、国家の安全保障、経済の繁栄を実現するために不可欠な役割を果たしている。投資家の意識は高まりつつあり、技術的な専門家ではないアナリストが企業のパフォーマンスを比較、評価できるように、信用格付けに類する標準化されたサイバーセキュリティ・リスク・レーティングが実用化されている。
2. 投資家にとっては、そのような発行体固有のパフォーマンスとリスクに関する指標を、地域レベル、業種レベルで集計することによって、パフォーマンスが脆弱な分野の把握が容易になり、これまで以上に的を絞ったリスク評価と生産性の高いコーポレート・エンゲージメントが可能になる。
3. 企業のサイバーセキュリティ・パフォーマンスは地域、業種によって異なるが、明確な傾向も見受けられる。グローバル社債市場の代表的な発行体のデータを集計した結果、オーストラリア・ニュージーランド、北米、英国・アイルランドがパフォーマンス上位の地域であることがわかった。その一方で、日本とアジア太平洋地域のパフォーマンスは、先進国市場、新興国市場の比較対象国を下回った。業種別に見ると、通信、一般消費財、資本財、情報技術といった業種の企業はサイバーセキュリティ・リスクへの備えが相対的に脆弱であり、一方で金融セクターの企業は全般に備えが最も進んでいることが確認された。
4. このような違いを理解することで、投資分析においてサイバーセキュリティ・リスクの効果的な統合が促進されるとともに、リスクに関する新たな洞察と的を絞ったコーポレート・エンゲージメントの機会が投資家に提供されることになる。

Ⅰ　サイバーセキュリティ・リスクとパフォーマンスの市場俯瞰的な理解

相互関連性が強まりデジタル化が進む市場において、企業のレジリエンス、国家の安全保障、経済の繁栄を実現するために、サイバーセキュリティは不可欠な役割を果たしている。投資家にとって、オペレーショナル・リスク、財務リスク、法務リスク、風評リスクの観点から、サイバーセキュリティは重要な意味を持ち、気候などのファクターと並んで計測、管理すべき、次世代のサステナビリティのテーマとして注目されている。組織のサイバーセキュリティ成熟度とリスクの全体像を評価することによって、投資家は企業統治とリスク管理の質に関する洞察を獲得できるようになる。サイバーセキュリティは他のサステナビリティ関連のファクターと比べて、客観的な「外部」指標が一般的に分析可能であり、投資家にとってデータの開示と透明性の問題は必ずしも制約にならない。市場価格を評価する際に、信用格付けが標準化されたリスクの見方を提供するのと同様に、定量化、標準化されたサイバーセキュリティ・リスク・レーティングは、技術的な専門家ではない投資アナリストが個別企業のサイバーセキュリティ・リスクとパフォーマンスを統合し、比較するための、利便性の高い方法を提供する。

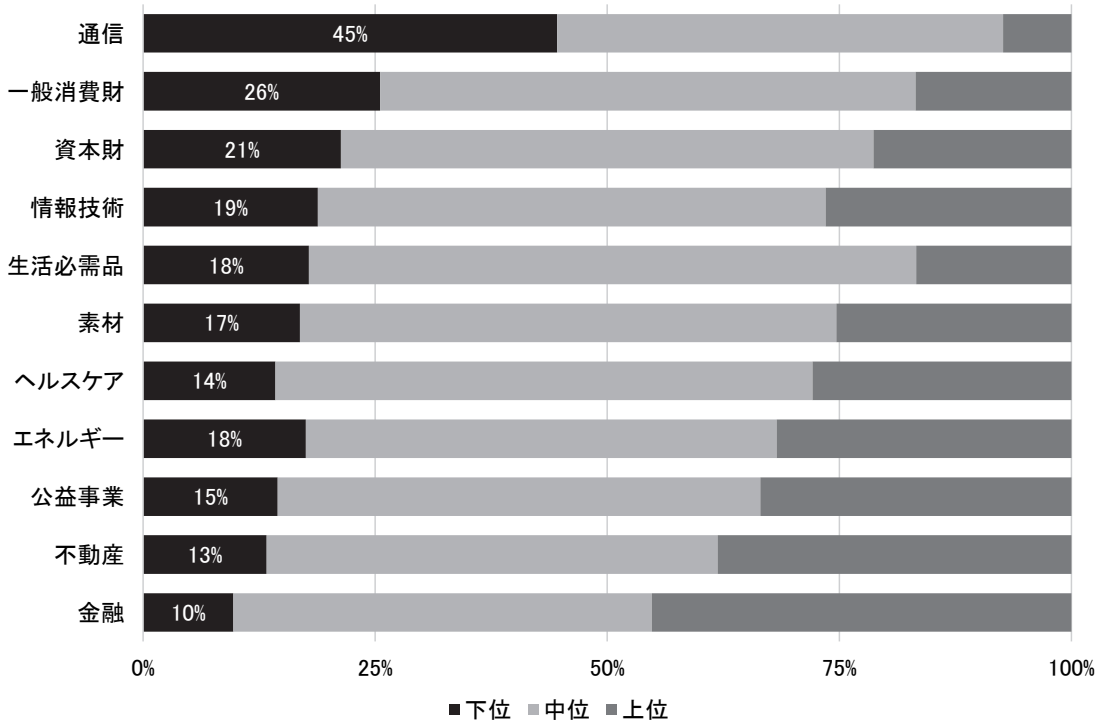
炭素排出強度や物理的気候リスクなどのサステナビリティ関連のファクターと同様に、サイバーセキュリティ・リスクの国別、業種別の分布状況は均一ではない。サイバーセキュリティ・パフォーマンスの「ヒートマップ」は、レーティング・データにアクセスのない投資家に対しても、この新しいテーマに対する意識や理解を向上させるための指針を提供する可能性を秘める。当社が行った調査は、世界の社債発行体のパフォーマンス・レーティングをボトムアップの観点から集計した上で、実世界における潜在的なリスク・エクスポージャーと相互参照することによって、投資家や企業が優先すべき地域と業種を明らかにしている。

Ⅱ　地域別・業種別グローバル・ヒートマップ

１．サイバーセキュリティ・パフォーマンス集計値（業種別）

サイバーセキュリティ・パフォーマンスのデータを業種レベルで集計したところ、技術的な要因によってレーティングが低くなりやすい通信セクターを除いて、一般消費財、資本財、情報技術の各業種のパフォーマンス・レーティングが最も低く、表面的なリスクが最も高いことが確認された（図表 1）。また、スコアを下位、中位、上位に分類する Bitsight Technologies 社のレーティング・データに注目すると、下位に分類される社債発行体（グローバル）の比率が最も高いのは、通信セクター（45%）であり、これに一般消費財セクター（26%）が続く形となった。後者には娯楽や小売といった下位業種が含まれ、消費者の個人情報やクレジットカード情報が取り扱われることも多く、ハッカーの格好の標的とされている。一方、資本財セクターについても、下位業種の航空宇宙・防衛、電気

図表 1　サイバーセキュリティ・パフォーマンス ― 企業レーティング集計値（業種別）

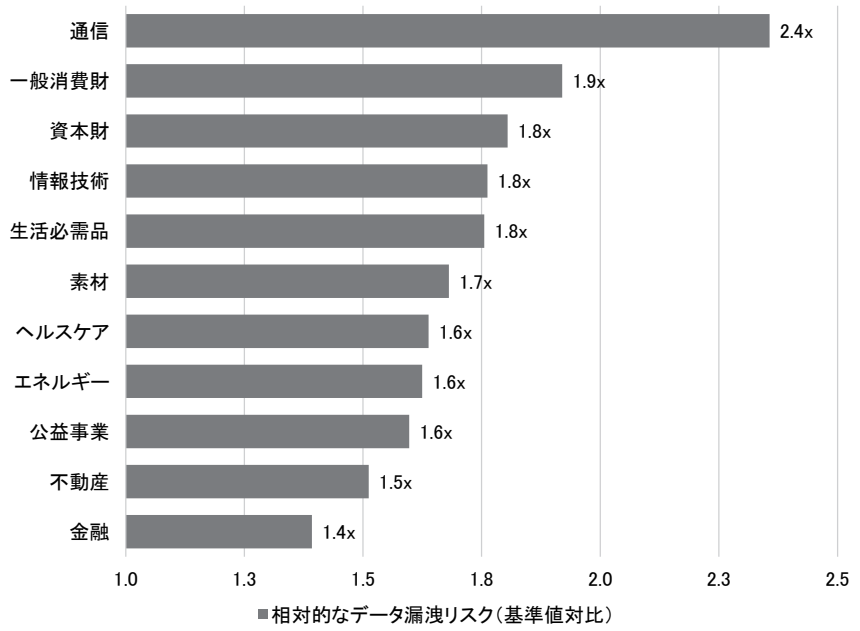


（注）　「下位」のスコアの割合が低いほど好ましい。
（出所）Bitsight Technologies 社のデータ、野村アセットマネジメントによる計算

設備、運輸、機械が重要な国家機能に貢献しているにもかかわらず、防御態勢が相対的に不十分であることから、懸念が大きい。これに対して、金融セクターは、サイバー犯罪の標的にされやすいものの、対応能力が比較的高い。銀行や機関投資家向け金融サービス企業は規制業種であり、自らのサイバー防御態勢に大規模な投資を行うケースが多いためである。

サイバーセキュリティ・パフォーマンス・スコアは実際のリスクと相関するため、企業のスコアをデータ漏洩リスクの相対的な水準に変換することが可能である（図表 2）。投資家は、相対的なリスクが特に高い業種の企業をモニタリングし、エンゲージメントに取り組むことによって、効果的な証券分析やリスク管理に資する情報を入手できる可能性がある。Bitsight Technologies 社のデータによると、通信セクターの平均的な社債発行体のデータ漏洩リスクは、低リスクの基準値よりも 2.4 倍高いことがわかった。その一方で、金融セクターでは、防御態勢と投資の水準が高いため、平均的な金融機関のリスクは基準値の 1.4 倍にとどまった。また、これらの指標は、投資家のアクティブ・オーナーシップの取り組みにおいても、的を絞ったエンゲージメントや影響度のトラッキングに関連して、有益な情報を提供する。

図表 2　サイバーセキュリティ・パフォーマンス ― 企業相対リスク集計値（業種別）



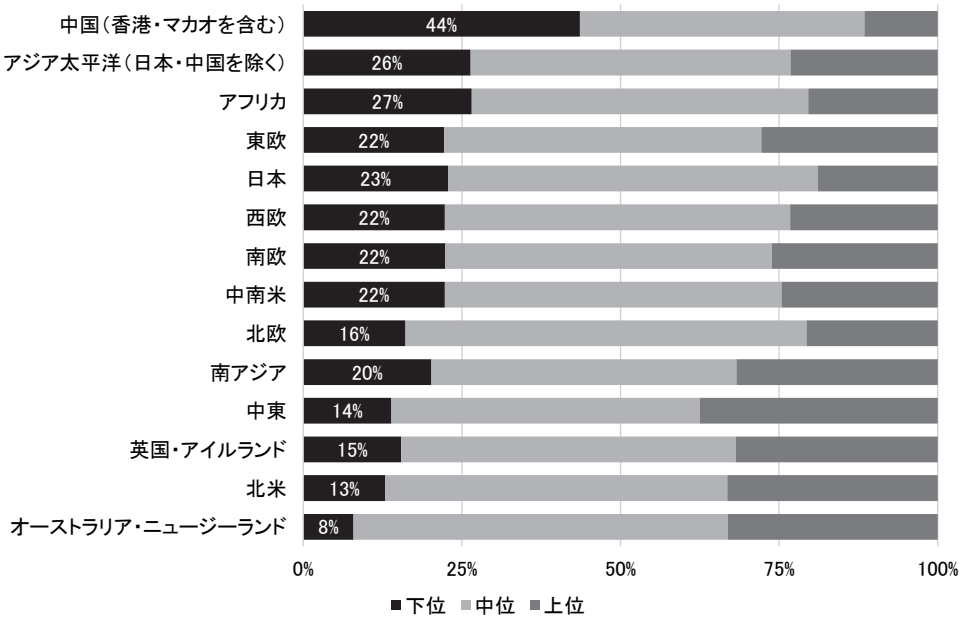
（注）　相対リスク倍率が低いほど好ましい。
（出所）Bitsight Technologies のデータ、野村アセットマネジメントによる計算

２．サイバーセキュリティ・パフォーマンス集計値（地域別）

次に、サイバーセキュリティ・パフォーマンスのデータを地域レベルで集計したところ、企業のサイバーセキュリティ対策は、一般に国民所得の水準や経済発展の度合いが高いほど改善することが確認された。ただし、いくつか留意すべき点もある。多くの場合、地域別のパフォーマンス集計値には各国の業種集中度が反映されるため、スコアの平均が良い業種（金融や不動産）や悪い業種（通信、一般消費財、情報技術）に偏るケースも考えられる。また、多国籍の組織の場合、本社や主要なマーケットが 1 つの法域に限定されていたとしても、ネットワークのプレゼンスやサイバーセキュリティ・リスクは多数の国に広がっていることがある。この点を踏まえても、地域レベルの集計結果は、市場の発展度やリスクの代替指標として、企業・インフラの強靭なサイバーセキュリティへの投資を検討する際に、どの法域において効果が高く、どの法域が相対的に遅れているかを理解する上で有益である。

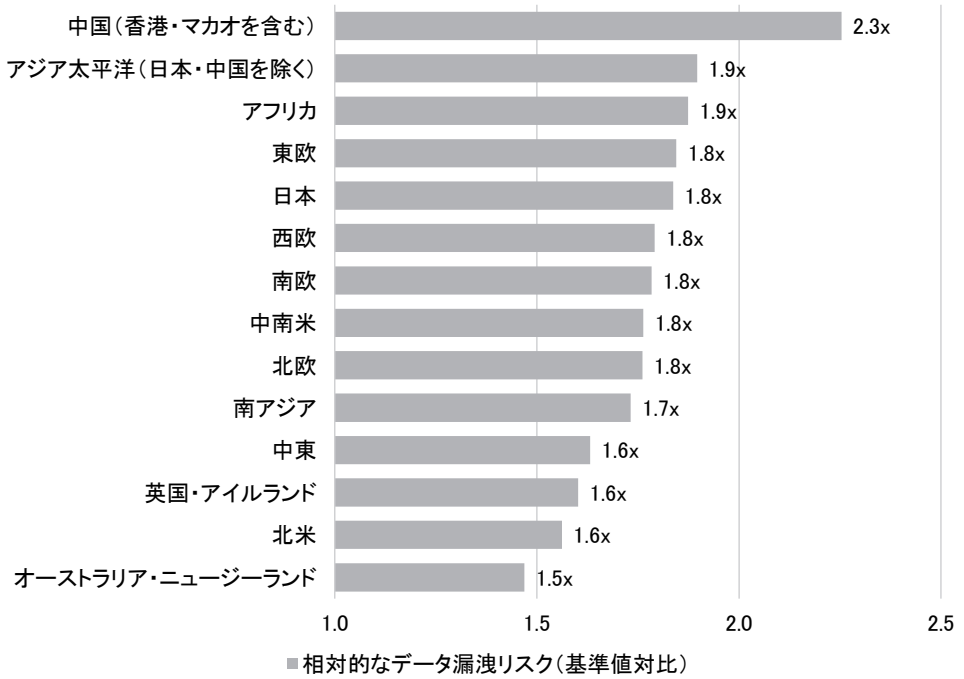
世界の社債発行体のサンプルに基づくと、サイバーセキュリティの対応力が最も高い市場は、サイバーセキュリティ政策や企業投資に対する先を見越したアプローチや、業種集中度の影響を背景に、オーストラリア・ニュージーランド、北米、英国・アイルランドであることがわかった（図表 3、図表 4）。北米地域の大半を占める米国企業は、他国の同業他社よりもレーティングは総じて高いものの、犯罪者や国家を後ろ盾とするハッカーにとって、より価値の高い標的となる可能性もある。また、サウジアラビア、アラブ首長国連邦、イスラエルを含む中東地域も、比較的高い対応力を示している。一方、欧州地域で

図表 3　サイバーセキュリティ・パフォーマンス ― 企業レーティング集計値（地域別）



（注）　「下位」のスコアの割合が低いほど好ましい。平均総合スコア順。
（出所）Bitsight Technologies 社のデータ、野村アセットマネジメントによる計算

図表 4　サイバーセキュリティ・パフォーマンス ― 企業相対リスク集計値（地域別）



（注）　相対リスク倍率が低いほど好ましい。
（出所）Bitsight Technologies 社のデータ、野村アセットマネジメントによる計算

は、北欧企業のパフォーマンスが比較的良好であるのに対して、西欧企業および南欧企業のスコアは北欧企業を下回っている。また、アジアのパフォーマンスは対象地域の中で最低の水準となった。詳細に見ると、日本のパフォーマンスは他の先進諸国よりも低く、アジア太平洋地域および中国の社債発行体の成熟度はグローバル市場で最も低いことがわかった。

Ⅲ グローバル・サイバーセキュリティ・ヒートマップ

グローバル・サイバーセキュリティ・ヒートマップは、業種別と地域別のサイバーセキュリティ・スコアを統合することによって作成される（図表 5）。通信セクターのスコアの比重を引き下げ、データが不十分な地域や業種を除外することによって、サイバーセキュリティの相対的な強靭性と改善すべき分野のグローバル・マップが浮かび上がる。具体例を挙げると、中東地域では、情報技術セクターと素材セクターの企業の対応力が、業種、地域いずれの座標軸においても比較的高いのに対して、エネルギー・セクターの企業の対応力は、他地域の同業他社に見劣りしている。また、日本の場合、他の先進国・新興国の同業他社をアウトパフォームしているのは不動産セクターと金融セクターに限られ、情報技術、エネルギー、公益事業の各セクターは、業種、地域いずれの座標軸においても、大幅にアンダーパフォームしている。一方、北米企業のパフォーマンスは、他地域の同業他社より総じて優れているものの、一般消費財セクターと資本財セクターについては、同一地域の他業種（通信など）に見劣りしている。

図表 5　グローバル・サイバーセキュリティ・ヒートマップ 2024 年

相対的なデータ漏洩リスク（基準値対比、低いほど好ましい）	業種											
地域	通信	一般消費財	資本財	情報技術	生活必需品	素材	ヘルスケア	エネルギー	公益事業	不動産	金融	平均
中国（香港・マカオを含む）	2.3	2.7	2.2	2.8	2.0	2.1		2.2	1.8	2.3	2.2	2.3
アジア太平洋（日本・中国を除く）	2.4	2.4	1.9	1.8	2.1	1.8	2.0	1.8	1.8	1.7	1.6	1.9
アフリカ	2.8		2.6		1.7	1.4	2.0			1.3	1.9	1.9
欧州（東欧）								2.0	2.6		1.3	1.8
日本	2.4	2.0	1.9	2.2	1.7	1.9	1.8	2.2	1.9	1.4	1.4	1.8
欧州（西欧）	2.4	2.1	1.9	1.7	1.8	1.9	1.6	1.9	2.0	1.3	1.4	1.8
欧州（南欧）	2.4	1.9	1.9	1.7	1.6	1.7	1.9	1.6	1.7	1.3	1.7	1.8
中南米	2.7	2.1	1.9		1.8	1.7		1.8	1.4	1.7	1.6	1.8
欧州（北欧）	2.7	1.9	1.9	1.8	1.7	1.7	1.4	1.6	1.8	1.8	1.4	1.8
南アジア	2.8	2.3	1.8	1.1	1.3	1.8	2.1	2.1	1.9		1.2	1.7
中東	3.3		1.5	1.2	1.9	1.2		2.5		1.3	1.3	1.6
欧州（英国・アイルランド）	2.1	1.8	1.7	1.5	1.8	1.5	1.6	1.6	1.5	1.2	1.4	1.6
北米	2.2	1.8	1.7	1.6	1.6	1.5	1.6	1.4	1.3	1.4	1.2	1.6
オーストラリア・ニュージーランド	2.0	1.6	1.5	1.6	1.3	1.6	1.6	1.2	1.4	1.1	1.3	1.5
平均	2.4	1.9	1.8	1.8	1.8	1.7	1.6	1.6	1.6	1.5	1.4	1.7

（注）　相対リスク倍率が低いほど好ましい。
（出所）Bitsight Technologies 社のデータ、野村アセットマネジメントによる計算

Ⅳ 結論

投資家にとって、企業のサイバーセキュリティ・パフォーマンスの指標は、市場価格に反映されない重大なリスクやアルファ創出の可能性を示唆する先行指標である。同時に、世界的に社会経済的影響を及ぼすテーマに関するコーポレート・エンゲージメントの、ユニークな機会を提供する。しかし足元では、投資プロセス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している投資家は非常に少なく、その存在を認識している投資家もほとんどいない。サステナブル投資に取り組む市場参加者が、さまざまな業種や地域の相対的な炭素排出強度を内部化するようになったのと同じように、サイバーセキュリティ・リスクを投資プロセスに効果的に統合するためには、その起源を理解する必要がある。トップダウンの観点から見ると、定量的なサイバーセキュリティ・リスク・レーティングのデータは、アクセス可能な新しいリスクの洞察を投資家に提供し、リスクの適切な統合とエンゲージメントを通じて、サイバーセキュリティを「プライシング」する方向へと市場を誘導する可能性を秘める。

〔原文 (Original)〕

Global Corporate Cybersecurity Performance Heat Map

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

▌Abstract ▐

1. Cybersecurity is vital to ensuring corporate resiliency, national security, and economic prosperity in an increasingly digitized market. Investor awareness of cybersecurity is growing, and standardized cybersecurity risk ratings, like credit ratings, are available to enable non-technical analysts to assess and compare companies' cybersecurity performance.
2. Aggregating such issuer-specific metrics of organizational cybersecurity performance and risk exposure up to the regional- and sector-level can help investors grasp where cybersecurity performance is weaker, for more focused risk assessments and productive corporate engagements.
3. Corporate cybersecurity performance varies by region and industry, but follows a discernable pattern. Based on aggregate data from companies representing global corporate debt market, the top-performing regions for cybersecurity are Australia and New Zealand, North America, and the UK and Ireland. Cybersecurity performance in Japan and Asia-Pacific to lag behind developed- and emerging market peers. By sector, companies in the Communications, Consumer Discretionary, Industrials, and Technology sectors exhibit lower cyber preparedness, while Financial sector companies tend to have the highest.
4. Understanding these variations facilitates effective integration of cybersecurity risks in investment analysis, offering investors new risk insights and opportunities for targeted corporate engagement.

Ⅰ Understanding the distribution of cybersecurity risk and performance across markets

Cybersecurity is critical for corporate resiliency, national security, and economic prosperity in an increasingly interconnected and digitized world. For investors, cybersecurity has material implications for operational, financial, legal, and reputational risks, emerging as a next-generation sustainability topic to be measured and managed alongside climate and other factors. Assessments of organizational cyber maturity and risk posture can provide investors with insights into corporate governance and the quality of risk management. Compared to other sustainability factors, cybersecurity data disclosures and transparency are not necessarily a limiting factor for investors, as objective "outside-in" measures of corporate cybersecurity are generally available for analysis. Just as credit ratings offer a standardized view of risk for market pricing, quantitative and standardized cybersecurity risk ratings provide an accessible way for non-technical investment analysts to integrate and compare the cybersecurity risk and performance of individual companies.

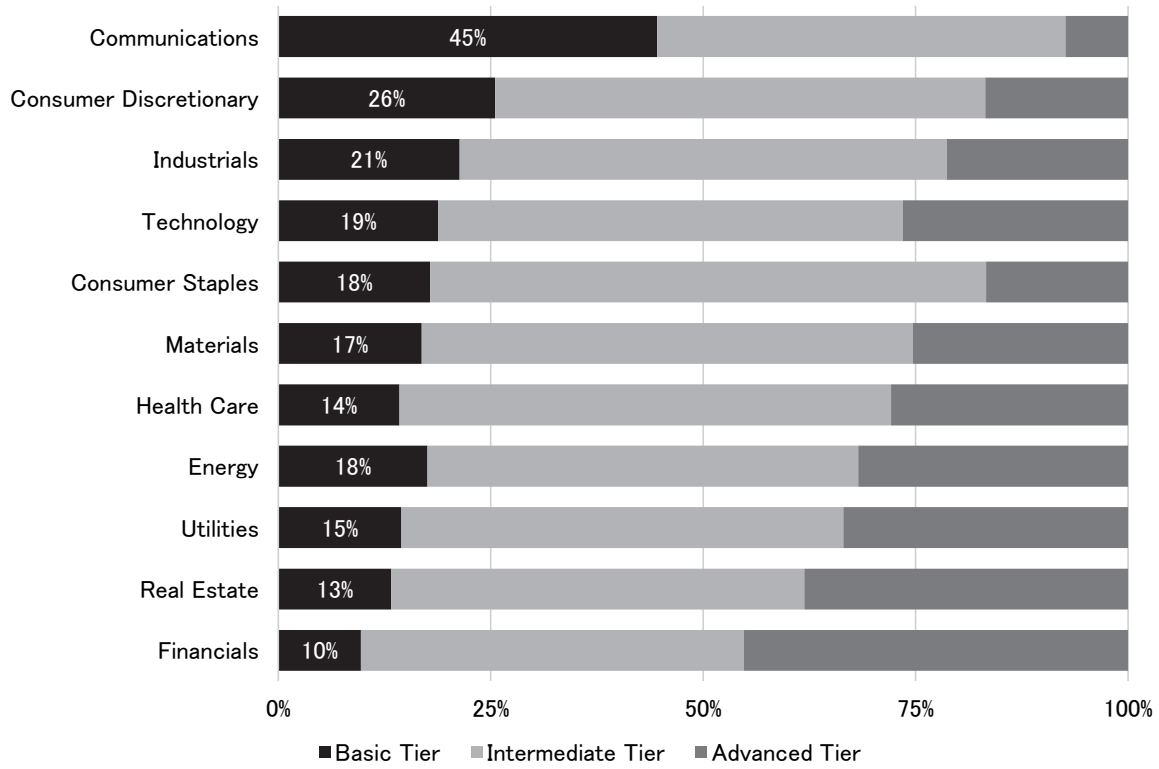
Like certain sustainability factors like carbon emissions intensity, and physical climate risk, cybersecurity risk is not equally distributed across countries and market sectors. A "heat map" of corporate cybersecurity performance can provide a guide for improving awareness and familiarity with this emerging topic, even for investors without access to cybersecurity ratings data. By aggregating bottom-up cybersecurity performance ratings at the entity level for issuers in the global corporate bond market and cross-referencing with implied real-world cyber risk exposures, our survey reveals the regions and sectors that investors and corporates should prioritize.

Ⅱ A global heat map of Cybersecurity performance by region and sector

1. Aggregate Cybersecurity Performance by Sector

Aggregating cybersecurity performance data at the sector level shows that, aside from the Communications sector—which often has low ratings due to technical factors— companies in the Consumer Discretionary, Industrials, and Information Technology sectors have the lowest cybersecurity performance ratings and the highest levels of apparent cyber risk exposure (Figure1). Based on Bitsight Technologies ratings data that categorizes scores into Basic, Intermediate, and Advanced tiers, 45% of global corporate debt issuers in the Communications sector are in the lowest tier, followed by Consumer Discretionary at 26%. This sector includes the Hospitality and Consumer Retail sub-sectors, where companies often handle private consumer data and credit card information, making them attractive targets for hackers. Industrials are another sector of concern, as the Aerospace and Defense, Electrical Equipment, Transportation, and Machinery sub-sectors contribute to national critical functions yet remain relatively under-protected. Conversely, the Financials sector, while often targeted by cyber criminals, is relatively cyber-capable, as Banks and Institutional Financial Service firms, being regulated entities, tend to invest considerably in their own cyber defenses.

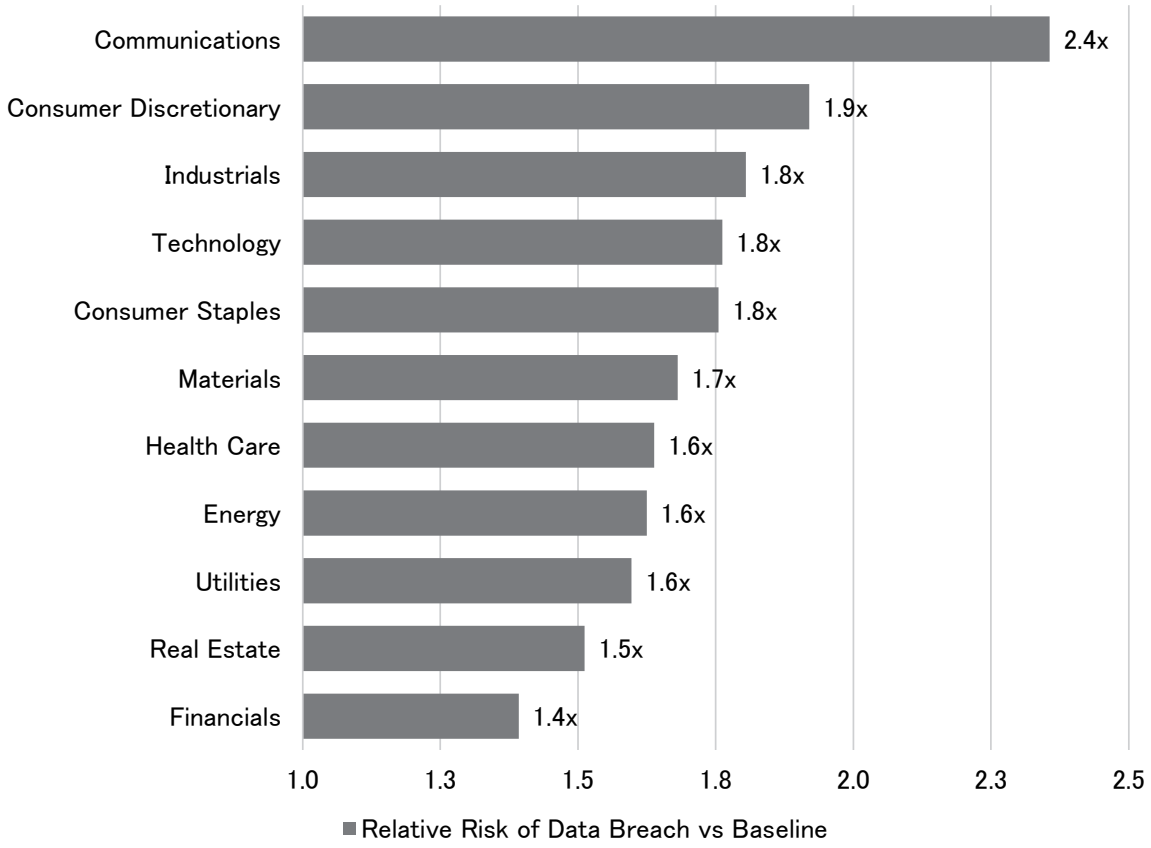
Figure 1: Cybersecurity Performance - Aggregate Corporate Ratings by Sector



Note:　Fewer “Basic” tier scores are better.
Source: Bitsight Technologies Data, Nomura Asset Management calculations.

Cybersecurity performance scores correlate with real-world risk outcomes, allowing for the translation of corporate cyber scores into relative data breach risk levels (Figure2). Monitoring and engaging corporates in the most exposed sectors regarding their relative cybersecurity risk can be an effective input for investors' securities analysis and risk management. Based on Bitsight data, the average corporate bond issuer in the Communications sector is 2.4 times more likely to experience a data breach compared to the low-risk baseline, while financial firms on average are only 1.4 times as likely, attributable to this sector’s higher levels of cyber preparedness and investment. These metrics are also useful for informing investors' active ownership efforts through targeted corporate engagement and impact tracking.

Figure 2: Cybersecurity Performance - Aggregate Corporate Relative Risk by Sector



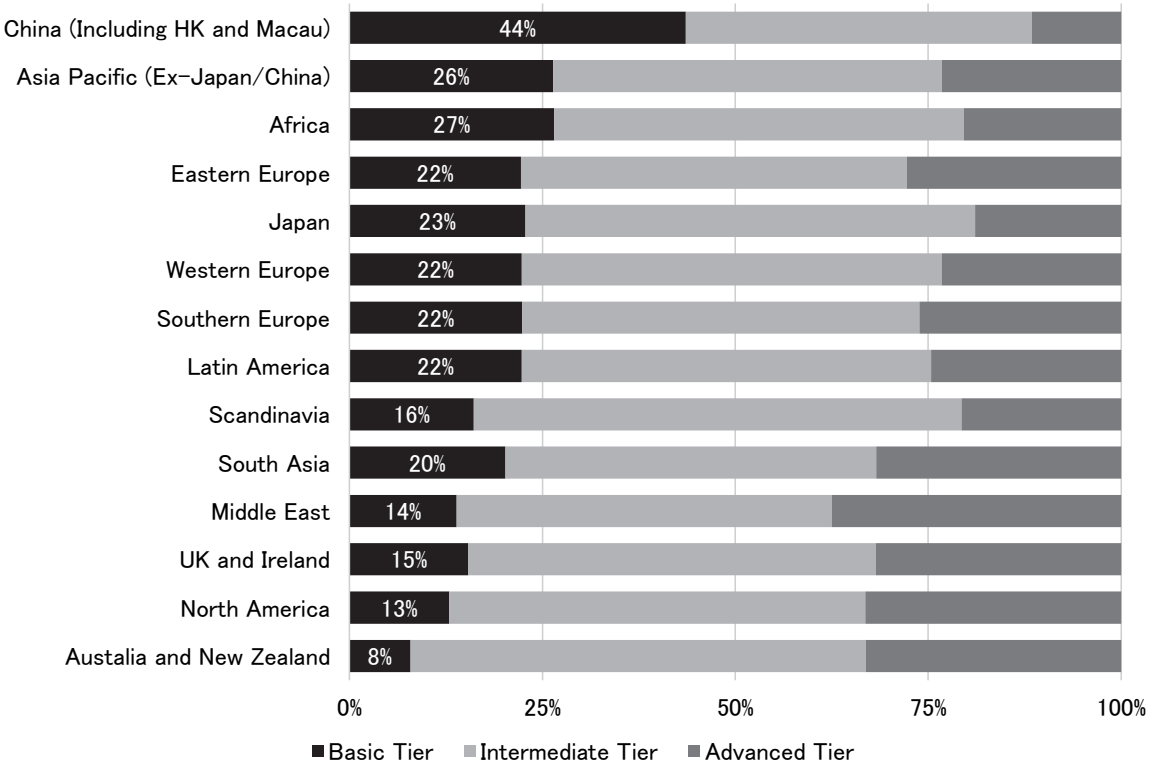
Note: Lower relative risk multiples are better.
Source: Bitsight Technologies Data, Nomura Asset Management calculations.

2. Aggregate Cybersecurity Performance by Region

Aggregating cybersecurity performance data at the regional level shows that corporate cybersecurity practices generally improve with national income levels and economic development, but some caveats apply. Regional performance aggregate scores often reflect market sector concentrations at the national level, which may be weighted toward sectors with better (Financials or Real Estate) or worse average scores (Communications, Consumer Discretionary, and Information Technology). Furthermore, in the case of multinational organizations, a company's headquarters and main market may be in one jurisdiction, while its network presence and cybersecurity risk exposures are spread across many countries. Still, regional-level results are useful for understanding which jurisdictions are more effective at investing in resilient corporate and infrastructure cybersecurity and which are relatively behind as alternative indicators of market development and risk.

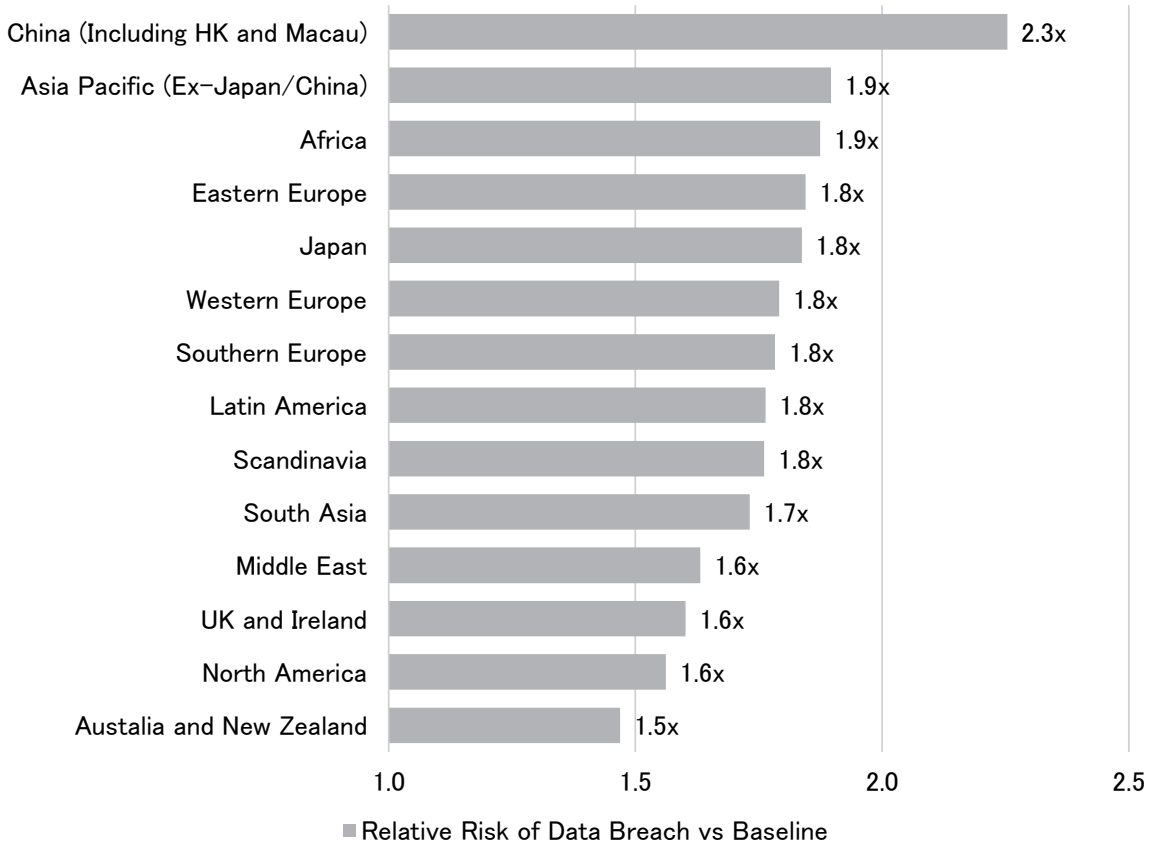
The top-performing markets for corporate cybersecurity readiness based on a sample of global bond issuers are Australia and New Zealand, North America, and the UK and Ireland, reflecting these jurisdictions' proactive approaches to cybersecurity policy and corporate investment, as well as some sector concentration elements (Figure3, Figure4). Corporates in the US, representing most of the North American region, tend to have higher cybersecurity ratings than global peers, although they may also be more high-value targets for criminals and state-backed hackers. The Middle East region, including Saudi Arabia, the UAE, and Israel, also exhibits relatively high cybersecurity readiness. Within Europe, companies in Scandinavia perform better, while Western and Southern European peers score marginally lower. Asia's cybersecurity performance is at the bottom end of the range —Japan's corporate cybersecurity underperforms compared to developed market peers, while corporate debt issuers in Asia Pacific and China exhibit the lowest levels of cyber maturity in global markets.

Figure 3: Cybersecurity Performance - Aggregate Corporate Ratings by Region



Note:　Fewer "Basic" tier scores are better. Regions sorted by overall score average.
Source: Bitsight Technologies Data, Nomura Asset Management calculations.

Figure 4: Cybersecurity Performance - Aggregate Corporate Relative Risk by Region



Note: Lower relative risk multiples are better.
Source: Bitsight Technologies Data, Nomura Asset Management calculations.

III Aggregate Cybersecurity Performance by Sector and Region – Global Cybersecurity Performance Heat Map

Integrating the sector- and regional-aggregate corporate cybersecurity score datasets produces a Global Cybersecurity Heat Map (Table1). De-emphasizing Communication sector scores and screening out region-sectors with insufficient data reveals a global map of relative cyber strength and areas for improvement. For example, Middle Eastern Technology and Materials companies exhibit relatively high levels of cyber preparedness for both their sector and region, while Middle Eastern Energy companies stand out as relatively less capable than global peers. In Japan, only Real Estate and Financials outperform global sector peers (including both developed and emerging markets), while the Japanese Technology, Energy, and Utility sectors significantly lag on both a regional and sector-peer basis. In North America, where corporate performance is generally higher than global peers, the Consumer Discretionary and Industrial sectors indicate relatively lower performance compared to other sectors in the same region (e.g., Communications).

Table 1: Global Cybersecurity Heat Map 2024

Relative Risk of Breach vs Baseline (lower is better)	Sector											
Region	Communications	Consumer Discretionary	Industrials	Technology	Consumer Staples	Materials	Health Care	Energy	Utilities	Real Estate	Financials	Average
China (Including HK and Macau)	2.3	2.7	2.2	2.8	2.0	2.1		2.2	1.8	2.3	2.2	2.3
Asia Pacific (Ex-Japan/China)	2.4	2.4	1.9	1.8	2.1	1.8	2.0	1.8	1.8	1.7	1.6	1.9
Africa	2.8		2.6		1.7	1.4	2.0			1.3	1.9	1.9
Europe (Eastern Europe)								2.0	2.6		1.3	1.8
Japan	2.4	2.0	1.9	2.2	1.7	1.9	1.8	2.2	1.9	1.4	1.4	1.8
Europe (Western Europe)	2.4	2.1	1.9	1.7	1.8	1.9	1.6	1.9	2.0	1.3	1.4	1.8
Europe (Southern Europe)	2.4	1.9	1.9	1.7	1.6	1.7	1.9	1.6	1.7	1.3	1.7	1.8
Latin America	2.7	2.1	1.9		1.8	1.7		1.8	1.4	1.7	1.6	1.8
Europe (Scandinavia)	2.7	1.9	1.9	1.8	1.7	1.7	1.4	1.6	1.8	1.8	1.4	1.8
South Asia	2.8	2.3	1.8	1.1	1.3	1.8	2.1	2.1	1.9		1.2	1.7
Middle East	3.3		1.5	1.2	1.9	1.2		2.5		1.3	1.3	1.6
Europe (UK and Ireland)	2.1	1.8	1.7	1.5	1.8	1.5	1.6	1.6	1.5	1.2	1.4	1.6
North America	2.2	1.8	1.7	1.6	1.6	1.5	1.6	1.4	1.3	1.4	1.2	1.6
Australia and New Zealand	2.0	1.6	1.5	1.6	1.3	1.6	1.6	1.2	1.4	1.1	1.3	1.5
Average	2.4	1.9	1.8	1.8	1.8	1.7	1.6	1.6	1.6	1.5	1.4	1.7

Note:　Lower relative risk multiples are better.
Source: Bitsight Technologies Data, Nomura Asset Management calculations.

IV Conclusion

Corporate cybersecurity performance measurement represents a forward indicator of material unpriced risk and potential investment alpha for investors, while presenting unique opportunities for corporate engagement on a topic with global socio-economic impact. Yet few investors are currently integrating—or are even aware of—cybersecurity performance ratings data for the investment process. Just as sustainable investment market participants have come to internalize the relative carbon emission intensities of different sectors and regions, effective integration of cybersecurity risks into investments will require an understanding of their origins. When viewed from a top-down perspective, quantitative cybersecurity risk ratings data can yield new and accessible risk insights for investors, ultimately guiding markets to “price” cybersecurity through better risk integration and engagement.