

サイバーセキュリティがマクロ経済にもたらすリスクと機会¹

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マクロ経済に関するリスクであると同時に、持続可能な成功とデジタルトランスフォーメーションを可能にする基盤でもある。サイバーセキュリティの強靱性は、デジタルトランスフォーメーションを通じて堅固で持続可能な成長を実現するために不可欠である。デジタル化には、生産性とイノベーションを促進する一方で、デジタル攻撃の対象領域を広げる側面がある。その結果、システム、データの完全性、市場の信頼を損なうサイバーインシデントに伴う経済被害が増加することとなる。サイバーリスクは価格に織り込まれていない負の外部性である。企業は、サイバーインシデントの社会・経済コストを内部化していないため、サイバーレジリエンスへの投資が過小となっている。また投資家は、企業のサイバーリスクへの対応を評価するための透明性の高いデータをこれまで入手できていなかった。
2. サイバーセキュリティ対応に関する規制を、技術的な側面に限定して構築するのは実践的ではなく、政策当局は、的を絞った開示要件の策定、責任の明確化、市場メカニズムの推進などの措置を、総合的に実施することに注力すべきである。サイバーセキュリティの分野にサステナビリティ分析を応用することで、インセンティブの整合化、サイバー対策および人材育成への投資促進、デジタルサービスに対する信頼の維持が可能になる。
3. 世界各国のサイバーセキュリティ対応を定量的に評価する指標においては、各業種のパフォーマンスが示されると同時に、日本が抱えるサイバーセキュリティ上の課題が浮き彫りになった。投資家は「アウトサイド・イン（外部）」のサイバーセキュリティリスク・レーティング（CRR）を活用することによって、企業のサイバー対策の健全性を比較した上で、資本配分にサイバーリスク指標を反映することが可能になる。本稿では、このボトムアップ・データを用いて、企業のサイバー対策の健全性に関するグローバル・ヒートマップを作成し、地域・業種に関する洞察を提供する。日本では、エネルギー、テクノロジー、公益事業、素材の各業種が、国際平均を顕著に下回っている。投資分析に定量的なサイバーセキュリティ指標を取り入れることで、織り込まれていない重要なリスクを可視化し、エンゲージメントの判断に活用するとともに、市場におけるサイバーセキュリティのより適切なプライシングに寄与することが可能となる。

¹ 本稿は、Asian Development Bank, “Harnessing Digital Transformation for Good Asian Development Policy Report 2025,” May 2025 への寄稿論文を基に作成した。

I サイバーセキュリティ：持続可能な成長に向けたマクロ経済のリスクと機会

デジタル化が進む経済において、持続可能で強靱かつ包摂的な発展を実現するには、サイバーセキュリティの強化が不可欠である。日本をはじめとする諸国では、金融、通信、医療、公益事業、物流、公共サービスなどの業種における生産性の向上やイノベーションの促進という形で、デジタルトランスフォーメーションの恩恵を享受する大きな機会が存在している。その一方で、デジタル化は、ネットワーク・サービスの指数関数的な成長に伴い、サイバー犯罪者やハッカーが重要システムの攻撃・妨害の標的とする対象領域（デジタルアタック・サーフェス）が拡大する。このため、社会全体でサイバーセキュリティ対策を強化・改善することによって、デジタルサービスへのアクセスと信頼性を維持することは、デジタル経済そのものの包摂的で持続可能な発展に不可欠である。

現代のデジタル経済において、サイバーセキュリティはあらゆる分野そして事業体に影響するため、政策当局、規制当局、市場参加者にとって一段と重要な検討課題となっている。世界銀行の分析によると、2024年にサイバーインシデントが直接的、間接的にもたらした損失は、世界の国内総生産（GDP）の0.21%から9.1%に達した²。米国のヘルスケアおよびエネルギー・セクターや日本の食品・飲料サプライチェーンで発生し、重要なセクターに障害をもたらした最近のサイバー攻撃が証明したように、1件のインシデントであっても連鎖的なシステム障害を引き起こし、数億人に影響する可能性がある。

企業に対するサイバー攻撃の影響は、最近ではマクロ経済レベルでも顕在化している。英国では、2025年に大手自動車メーカーがサイバー攻撃を受け、国全体の自動車生産が28.6%落ち込んだため、イングランド銀行は第3四半期のGDP見通しの下方修正を余儀なくされている³。また、サイバーセキュリティは先進国に限られた問題ではない。コスタリカでは、2022年にランサムウェア攻撃によって行政サービスが長期間停止状態に陥り、国家非常事態宣言が発せられ、GDPの約2.4%相当の損失が発生したと推計されている⁴。

II サイバーセキュリティ：持続可能で強靱な成長と発展を支える基盤

特に新興国市場では、サイバーセキュリティは持続可能で包摂的な経済成長を促進する重要なイネーブラーとなる可能性を秘めるが、安全で信頼性の高いデジタルのシステムとネットワークを構築するために、政府にはより一層の取り組みが求められる。世界銀行の調査では、重大なサイバーインシデントの発生率（開示ベース）を上位25%から下位25%へ引き下げることに成功した新興国は、国民1人当たりGDPを10年間で1.5%押し上げる可能性があること、また、サイバーセキュリティに対する政策上のコミットメント

² Estefania Vergara Cobos and Salcen Cakir, “A Review of the Economic Costs of Cyber Incidents,” World Bank Group, 2024.

³ “A hack impacting Jaguar Land Rover was so bad that it hurt the U.K.’s GDP, Bank of England says,” *NBC News*, November 11, 2025.

⁴ Estefania Vergara Cobos, *Cybersecurity Economics for Emerging Markets*, World Bank, 2024.

が強い国ほど、デジタル化産業の成長が速いことが示されている⁵。デジタル・デバイドの問題に対応しつつ、こうした成長機会を実現することは、接続環境、通信技術、デジタルサービスへの手頃なアクセスの拡大といった単純なものではなく、社会全体におけるサイバーセキュリティの全面的な推進を通じて、誰もがアクセスできる状態を確保し、維持することが必要になる。

Ⅲ サイバーセキュリティ：市場の失敗と負の外部性

サイバー犯罪者や脅威アクターには、ハッキング行為から得られるリターンの最大化を狙って、防御が最も脆弱なネットワークを標的にする傾向がみられる。つまり、社会全体のサイバーセキュリティの強さとは、システム内で最も弱い部分の強度に他ならないということである。したがって、政策当局や規制当局にとって重要な課題は、市場参加者全体に求める基準を厳格化することで、サイバーセキュリティ対策の改善をいかに効果的に促進するかという点である。この課題に対応するには、サイバーセキュリティの問題を、本質的に負の外部性や市場の失敗として捉えることが重要である。

対策が講じられていないサイバーリスクは、サイバーセキュリティのインシデント発生につながる可能性がある。定義上、サイバーセキュリティ関連の損失は、オペレーショナル、ファイナンシャル、そして風評に関する損害の影響を直接受ける企業の内部コストと、データやシステムの完全性、サービスの安定稼働、信頼などに関する社会全体の外部コストに分けられる。個々の企業は自らのサイバーリスクを管理する責任を負うが、対策が講じられていないサイバーリスクから生じる外部コスト全体の責任を負う必要がないため、リスクを過小評価し、その結果、サイバーセキュリティへの投資は不十分になる傾向がある。このため、「緩和策が講じられていない炭素排出」の場合と同様に、「対策が講じられていないサイバーリスク」も価格に織り込まれていない負の外部性を意味しており、この場合、影響が及ぶのは環境ではなく社会経済である。

最高経営責任者をはじめとする企業の経営陣は、企業向けリスク調査においてサイバーセキュリティを最上位の懸念事項として常に挙げているにもかかわらず、投資家サイドでは、企業のサイバーリスク対応を比較評価するための基本的な情報すら不足していることが珍しくない⁶。透明性や情報開示が不足すると、市場の効率性は低下する。投資家が企業のサイバーセキュリティに関するリスクとパフォーマンスを容易に評価できず、その情報を投資判断や資金配分に反映できないからである。市場価格や調達コストという形で市場からのシグナルを得られなければ、企業は包括的なサイバーリスクの削減やサイバー保険への加入、サイバー担当スタッフの育成に投資するインセンティブを失う。炭素リスクの場合と同様に、対策が講じられていないサイバーリスクは市場の失敗を招き、その結果、リスク対応は最適なものではなくなり、企業や社会全体のコストは増大してしまう。

⁵ Estefania Vergara Cobos, *Cybersecurity Economics for Emerging Markets*, World Bank, 2024.

⁶ Allianz, "Allianz risk barometer: A cyber event is the top global business risk for 2024," January 16, 2024. PwC, "From threat to opportunity PwC's Global Risk Survey 2023," World Economic Forum, "Global Risks Report 2024," January 10, 2024.

IV 今後の方向性：サイバーセキュリティ強化に向けた政策と市場メカニズムの活用

一般に、企業のサイバーセキュリティを技術的なパフォーマンス基準の義務付けによって規制することは、実践的ではない。リスクの対象となるデータやデジタルネットワークのインフラは大部分が民間所有であり、自主的なベストプラクティスに頼らざるをえない状況にあるうえ、組織構造、業種、サイバーセキュリティのリスク許容度、時間軸が多様であるために、サイバーリスクを画一的に管理する方法が存在しないからである。このため、政策当局は、直接的な技術的規制のみによって民間のサイバーリスクを削減することに消極的であった。もっとも、重大な侵害の通知の義務付けといった開示基準の改良や、データ保護を促進し法的責任を明確化する措置の推進を通じて、サイバーセキュリティのパフォーマンス基準を向上させることは可能であろう。

対策が講じられていないサイバーリスクがもたらす負の外部性を、情報に精通したリスク回避的な投資家の自己利益を媒介として、市場メカニズムに基づき実効的に抑制する先行事例は、サステナブル投資の分野に見出すことができる。例えば、投資家は、重大なサイバーリスクについて開示情報やパフォーマンスデータが入手できれば、より適切な投資判断や資金配分、リスク評価を行う目的で、リスクを体系的に計測・統合できるようになる⁷。このように、サイバーセキュリティに関する的を絞った情報開示の要請や、リスク管理の不備に対する罰則規定の強化などの形で、市場メカニズムが確立・促進されるようになれば、企業経営者がサイバーセキュリティの分野で経済合理性の高い投資を行う動機付けとなり、結果として企業全体のサイバーセキュリティ水準の向上につながることを期待される。カーボンプライシングのケースと同様に、サイバーリスクのプライシングは、サイバーセキュリティに関する市場の失敗に対する効率的かつ効果的な市場ベースの処方箋となりうるが、それを実現するには、政策当局による規制対応が不可欠である。

V サイバーセキュリティの業種別分析—世界及び日本のヒートマップ

投資先企業の業務運営、財務管理、法的義務、社会的評価に関わるリスクの観点から、サイバーセキュリティは投資家にとって重要な意味を持つ要素であり、気候などの要因と並んで計測・管理すべき、次世代のサステナビリティ関連のテーマとして浮上している。また、投資家の立場では、サイバーセキュリティに関する企業組織の成熟度やリスク管理体制を評価することで、企業統治やリスク管理の質についての新たな洞察を得ることが期待される。実際、サイバーセキュリティの技術的専門家が通常用いる、企業のサイバーセキュリティに関する客観的な「アウトサイド・イン（外部）」指標は、一般に投資分析にも応用可能である。

信用格付けが市場の価格評価において標準化されたリスク評価を提供するのと同様に、標準化された定量的なサイバーセキュリティリスク・レーティング（CRR）は、非技術系

⁷ Jason Mortimer, “Why Cybersecurity is the Biggest Hidden ESG Risk,” March 2023.

の投資アナリストが個別企業のサイバーセキュリティに関するリスクとパフォーマンスを統合・比較するための、利用しやすい手段を提供する。内部システムへのアクセスを有したとしても、組織のサイバーリスクを完全に信頼できる形で計測する方法は存在しないが、外部からのパフォーマンス評価は、情報が全くない場合と比べて、ほぼ確実に有益である。

サステナビリティの分野における炭素排出強度や物理的気候リスクといった特定のファクターと同様に、サイバーリスクにも国や業種によってばらつきが見られる。企業のサイバーセキュリティ・パフォーマンスを可視化する「ヒートマップ」は、レーティング情報を入力できない投資家にとっても、この新しいテーマへの認識を高め、理解を深めるための指針になりうる。我々の調査では、代表的な企業サンプルを対象に、ボトムアップの観点から事業体レベルでパフォーマンス・レーティングを統合した結果、投資家や政策当局がパフォーマンスの改善において優先すべき地域と日本の業種が明らかになった。

VI サイバーセキュリティ・パフォーマンスの地域・業種別グローバル・ヒートマップ

ここでは、世界のサイバーセキュリティ・ハイジーンの水準をボトムアップの観点から分析するため、地域、国、業種別に企業レベルのハイジーン・スコアを統合した、新しいヒートマップを作成した（図表1および図表2参照）。66の国・地域の5,000を超える公募債発行体について、独自のCRRスコアを用いて個別に分析を行い、業種別に統合を試みた。また、CRR業種スコアの構造的な差異を補正するため、国ごとに業種平均スコアを等加重して単純平均のパフォーマンス・スコアを算出し、さらに地域単位で集計している。

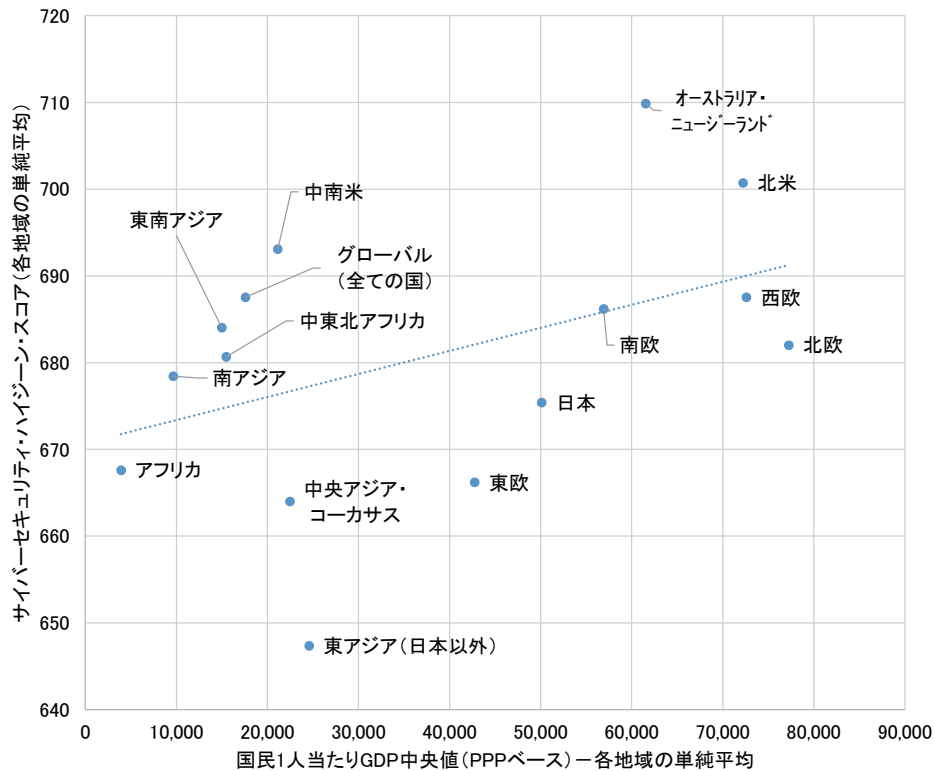
図表1 企業のサイバーセキュリティ・ハイジーン（平均）の地域及び業種別ヒートマップ

地域	セクター												国民1人 当たり GDP中央 値(PPP ベース)
	通信	一般消費財	生活必需品	エネルギー	金融	ヘルス ケア	資本財	素材	不動産	テクノロジー	公益事業	単純平均	
オーストラリア・ニュージーランド	667	699	722	730	727	699	712	701	736	700	716	710	61,533
北米	651	684	695	716	730	700	691	706	719	695	722	701	72,210
中南米	611	654	684	681	695	763	687	688	689	760	711	693	21,121
西欧	639	669	680	684	718	698	686	686	727	694	682	688	72,603
南欧	631	670	697	695	701	674	674	703	725	688	691	686	56,921
東南アジア	661	628	674	686	724	692	672	697	688	715	688	684	14,974
北欧	606	670	690	699	715	714	679	687	681	678	683	682	77,237
中東北アフリカ	556	650	672	628	723	680	689	729	720	730	710	681	15,466
南アジア	598	641	720	656	719	657	678	685	693	740	677	678	9,657
日本	635	670	686	651	719	682	670	677	719	650	672	675	50,106
アフリカ	618	630	692	660	678	665	634	717	727	703	620	668	3,919
東欧	640	550	683	667	703	640	745	730	690	660	620	666	42,756
中央アジア・コーカサス	593	665	680	665	664	647	642	695	703	697	654	664	22,470
東アジア(日本以外)	613	629	634	650	664	642	656	658	639	666	671	647	24,569
グローバル(全ての国)	636	672	686	697	714	695	681	692	706	685	699	688	17,597

(注) GDP=国内総生産、PPP=購買力平価

(出所) Bitsight Technologies のデータ、著者による計算

図表2 国民1人当たりGDP中央値とサイバーセキュリティ・スコアとの比較



(出所) Bitsight Technologies のデータ、著者による計算

上記のデータからは、オーストラリア、ニュージーランドと北米ではサイバーセキュリティが比較的強固であるのに対して、東アジア地域と日本は企業のサイバーセキュリティ・ハイジーンにおいて、地域別・所得水準別にみても、世界平均と比べても、大きく見劣りする状況が確認された。東アジア地域がこのように意外なほど見劣りする主な要因は、中国と韓国の企業のCRRが低いことであり⁸、2024年のITU（国際電気通信連合）グローバル・サイバーセキュリティ・インデックス⁹で示されたサステナビリティ政策コミットメント・スコアの高さと、ビジネスの現場で観察されるサイバーセキュリティの実践状況との間に、ギャップが存在している様子がうかがえる。これに対して、東南アジア地域と南アジア地域のパフォーマンスは比較的優秀であり、両地域に属するインドやマレーシアなどの国は主導的な役割を果たし、2024年のITUグローバル・サイバーセキュリティ・インデックスで示されたコミットメント・スコアの高さを裏付けている。

⁸ 中国全体のCRRスコアの低さを部分的に説明する特有の要因が、いくつか考えられる。第1に、中国政府は外部からの国内ウェブサイト閲覧を制限する国家的なファイアウォールを運用しているため、CRRのスコアリング・アルゴリズムの観測可能なデータポイントの数がその分少ないことが挙げられる。第2に、各事業者について、重要なネットワーク資産（適切に保守されている可能性が高い）のファイアウォール内外の比率が、CRRの定量スコアにバイアスを与える可能性がある。さらに、データサンプルに含まれる中国企業の規模が、平均的には比較的大きい点が挙げられる。大規模な組織ほどIPアドレスの数が多いため、全体の攻撃サーフェスが広がりやすく、スコアと負の相関を示す傾向がみられるからである。

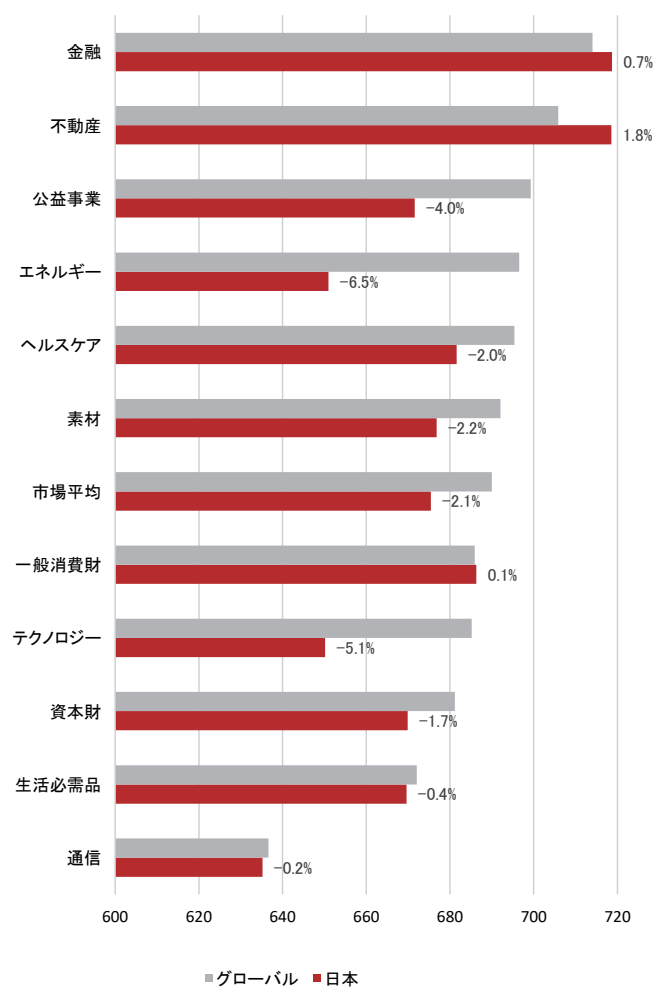
⁹ ITU, “Global Cybersecurity Index.”

VII 日本と世界の業種別サイバーセキュリティ

日本企業の業種別サイバーセキュリティ・パフォーマンスは、先進国・新興国のいずれの基準と比べても見劣りする。日本では、調査対象のほとんどの国と同様に、金融セクターと不動産セクターのサイバーセキュリティ・ハイジーンが最も高い傾向がある。金融セクターに関しては、サイバー犯罪の標的になりやすいものの、規制が厳格な業種であり、効果的なサイバーセキュリティ対策や担当スタッフの育成に必要な投資資源が比較的充実していることがその理由である。その一方で、通信セクターの CRR スコアは低い傾向がある。この業種に属する企業は、自社データと顧客データの通信が混在するネットワークやクラウドサービスを運用することが多く、こうした混在ネットワークは CRR のアルゴリズムで正確に解析するのが難しいため、業種固有の問題となっている。

規制当局や投資家にとって懸念されるのは、日本企業のパフォーマンスがほとんどの関連業種において、国際平均を下回る傾向を示していることである（図表 3）。なかでも、

図表 3 日本の業種別サイバーセキュリティリスク・レーティング（平均）



（出所） Bitsight Technologies のデータ、著者による計算

エネルギー（-6.5%）、テクノロジー（-5.1%）、公益事業（-4%）、素材（-2.2%）の各業種が、大きくアンダーパフォームしている。付言すると、これらの多くの業種は重要インフラであり、サイバー犯罪者の標的になりやすいため、日本企業にとって、アタックサーフェスの管理体制の構造的な改善や、ハイジーンの向上が極めて重要な課題となっている。

VIII 結論

企業のサイバーセキュリティ・パフォーマンス指標は、対策が講じられていない重大なリスクを示す先行指標であると同時に、投資家にとってはアルファ獲得の好機ともなりうる。また、グローバルな社会・経済的影響力を有するテーマに関連して、企業とのエンゲージメントにおいてユニークな機会を提供する。それにもかかわらず、現在、投資プロセスにパフォーマンス・レーティングのデータを取り入れている投資家、さらには、その存在を認識している投資家は非常に少ない。サステナブル投資の市場参加者が、各業種・地域の炭素排出強度を内部に取り入れるようになった状況と同様に、投資プロセスにサイバーリスクの観点を効果的に導入するためには、その起源を理解することが必要になる。トップダウンの観点からみると、定量的な CRR のデータは、実用的なリスクに関する新しい知見を投資家に提供するものである。最終的には、より適切なリスクの統合や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」する方向に市場を誘導することも可能である。

本内容は参考和訳であり、原文（Original）と内容に差異がある場合は、原文が優先されます。

〔原文 (Original)〕

The Macroeconomic Risk and Opportunity of Cybersecurity¹

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

■ Abstract ■

1. Cybersecurity is a macroeconomic risk and enabler of sustainable growth and digital transformation: Robust cybersecurity is essential for resilient and sustainable growth through digital transformation. Digitalization drives productivity and innovation but expands the digital attack surface. This increases the economic harm from cyber incidents that disrupt systems, data integrity, and market trust. Cyber risk is an unpriced negative externality: firms underinvest in cyber resilience because they do not internalize the full set of socio-economic costs of cyber incidents, and investors have lacked transparent data to price corporate cyber preparedness.
2. Because regulation of cybersecurity performance with technical mandates alone is impractical, policy makers should focus on a combination of targeted disclosure requirements, clarified liabilities, and promotion of market-based mechanisms. Applying sustainability analysis to cybersecurity can align incentives, encourage investment in cyber controls and workforce development, and preserve trust in digital services.
3. Quantitative measures of global cybersecurity show industry sector performance and reveal Japan's cybersecurity challenge: "Outside-in" cybersecurity risk ratings (CRR) enable investors to compare firms' relative cyber hygiene and incorporate cyber risk indicators into capital allocations. We present a global heat map of corporate cybersecurity from this bottoms-up data with insights into regional and sectoral cyber hygiene performance. In Japan, the energy, technology, utility, and materials sectors exhibit notable performance gaps versus global averages. Integrating quantitative cybersecurity metrics into investment analysis can reveal material, unpriced risks, inform engagement, and help markets better "price" cybersecurity.

¹ This paper is based on relevant research contributions to Asian Development Bank, "Harnessing Digital Transformation for Good Asian Development Policy Report 2025," May 2025.

I Cybersecurity as a macroeconomic risk and opportunity for sustainable growth

Improving Cybersecurity is critical to achieving sustainable, resilient, and inclusive development for an increasingly digitized economy. The opportunities for countries like Japan to benefit from the digital transformation -- through productivity improvement and innovation in finance, communications, health, utilities, logistics, and public service sectors -- is significant. But digitalization also brings risk, as the exponential growth in networked services increases the “digital attack surface” that cyber criminals and hackers can exploit for damaging and disrupting these critical systems. Preserving access and trust in digitally enabled services through robust improved cybersecurity practices across society is therefore crucial to inclusive and sustainable development of the digital economy itself.

Cybersecurity affects nearly every aspect and operating entity in modern digital economies, and so is an increasingly material issue for policy makers, regulators, and market participants to consider. According to World Bank analysis, the direct and indirect losses from cybersecurity incidents reached 0.21% to 9.1% of world GDP (Gross Domestic Product) in 2024². Even a single incident can cause cascading system failures that affect hundreds of millions of people, as recent cyberattacks on healthcare and energy in the United States and food and beverage supply chains in Japan that caused outages in critical sectors have shown.

The impact of corporate cyberattacks is now even showing up at the macroeconomic level, as a cyberattack on a UK automotive company in 2025 led the Bank of England to downgrade 3rd quarter GDP expectations due an overall 28.6% collapse in car manufacturing³. And cybersecurity is not just a developed economy issue – a 2022 ransomware attack in Costa Rica caused prolonged government service outages, a national emergency declaration, and an estimated 2.4% loss of GDP⁴.

II Cybersecurity as a factor for sustainable and resilient growth and development

Cybersecurity can be a key enabler for sustainable and inclusive growth, especially in emerging markets, but countries must do more to develop secure and trustworthy digital systems and networks. World Bank research shows that developing economies that reduce their rate of major disclosed cyber incidents from the top to the bottom quartile of countries could increase GDP per capita by 1.5% over a decade, and that digitalized industry growth is faster in countries with stronger policy commitment to cybersecurity⁵. Achieving these growth opportunities while addressing the digital divide is not as simple

² Estefania Vergara Cobos and Salcen Cakir, “A Review of the Economic Costs of Cyber Incidents,” World Bank Group, 2024.

³ “A hack impacting Jaguar Land Rover was so bad that it hurt the U.K.’s GDP, Bank of England says,” *NBC News*, November 11, 2025.

⁴ Estefania Vergara Cobos, *Cybersecurity Economics for Emerging Markets*, World Bank, 2024.

⁵ Estefania Vergara Cobos, *Cybersecurity Economics for Emerging Markets*, World Bank, 2024.

as expanding affordable access to connectivity, communications technology, and digital services. It also requires securing and maintaining that access for all through the holistic promotion of cybersecurity in society.

III Cybersecurity as a market failure and negative externality

Cybercriminals and malicious actors tend to target the least protected networks to maximize the payoff ratio from their hacking efforts. This means that cybersecurity in society is only as strong as the weakest link in the system. A primary question for policy makers and regulators then is how to effectively drive improvement in cybersecurity practices by raising standards for firms across the market. To address this challenge, it is important to understand the challenge of cybersecurity as fundamentally a negative externality and market failure.

Unmitigated cybersecurity risks can lead to cybersecurity incidents. By definition, these cybersecurity losses are allocated between internalized costs to directly affected firms from operational, financial, and reputational damages, and externalized costs to society at large from damage to data and systems integrity, service availability, and trust, etc. Individual firms are responsible for managing their own cybersecurity risk, but tend to undervalue and thus underinvest in cybersecurity because they do not have to account for the full set of externalized costs that arise from their own unmitigated cyber risk. Thus as with unmitigated carbon emissions, unmitigated cybersecurity risk represents an unpriced negative externality, but with socio-economic rather than environmental impact.

For their part, investors typically lack even basic information on relative corporate cybersecurity preparedness, even as corporate managers and CEOs (Chief Executive Officers) consistently rank cybersecurity as their top concern in corporate risk surveys⁶. The lack of transparency and disclosure makes markets less efficient, as investors cannot easily evaluate the relative cybersecurity risk and performance of companies, or reflect it in their investment decisions and capital allocations. Without a market signal from corporate valuations and funding costs, firms are dis-incentivized from investing in comprehensive cyber risk mitigations, cyber insurance, and cyber workforce development. As with carbon risks, unpriced cyber risk leads to a market failure, resulting in sub-optimal cybersecurity preparedness and higher overall costs to firms and society at large.

⁶ Allianz, “Allianz risk barometer: A cyber event is the top global business risk for 2024,” January 16, 2024. PwC, “From threat to opportunity PwC’s Global Risk Survey 2023,” World Economic Forum, “Global Risks Report 2024,” January 10, 2024.

IV The way forward: Leverage policy and market mechanisms to strengthen cybersecurity

Regulating corporate cybersecurity by mandating technical performance standards is generally impractical. This is because most at-risk data and digital network infrastructure is privately owned and relies on voluntary application of best practices, while there is no one-size fits-all approach for managing cybersecurity risks across different organizational structures, industry sectors, cybersecurity risk appetites, and over time. As a result, policymakers have been reluctant to mitigate private sector cybersecurity risks through direct technical regulation alone. However cybersecurity performance standards can be improved through better disclosure standards such as mandating material breach notifications, and advancing measures that promote data protection and clarify legal liabilities.

The sustainable investment market provides a precedent for introducing market forces to, in effect, regulate the negative externalities from unmitigated cyber risk through the self-interest of informed and risk-adverse investors. For example, if investors have access to material cybersecurity risk disclosures and performance data, then they can begin to systematically measure and integrate these risks for better investment decisions, capital allocations, and risk pricing⁷. Establishing and encouraging these market mechanisms, such as with targeted cybersecurity disclosures and greater legal penalties for cybersecurity risk mismanagement, may then encourage firm managers to make more economically rational cybersecurity investments and raise the standards of corporate cybersecurity overall. As with carbon pricing, cybersecurity risk pricing may be an efficient and effective market-based solution to the market failure of cybersecurity, but it requires enabling regulatory action from policy makers to make it a reality.

V Analysis of industry sector cybersecurity – Global and Japan Heatmaps

For investors, cybersecurity has material implications for operational, financial, legal, and reputational risks at investee firms, and is 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 also provide investors with novel insight into corporate governance and the quality of risk management. In fact, objective “outside-in” measures of corporate cybersecurity typically used by technical cybersecurity experts are also generally applicable for investment analysis.

Just as credit ratings offer a standardized view of risk for market pricing, quantitative and standardized cybersecurity risk ratings (CRR) provide an accessible way for non-technical investment analysts to integrate and compare the cybersecurity risk and performance of individual companies. While there is no perfectly reliable way to measure organizational cyber risk even with internal systems access,

⁷ Jason Mortimer, “Why Cybersecurity is the Biggest Hidden ESG Risk,” March 2023.

externally observed measures of cybersecurity performance are almost always better than having no information at all.

Like certain sustainability factors like carbon emissions intensity and physical climate risk, cybersecurity risk is not equally distributed across countries and industry 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 a representative sample of corporate entities, our survey reveals the regions and sectors in Japan that investors and policy makers should prioritize for cybersecurity performance improvement.

VI A global heat map of cybersecurity performance by region and industry sector

To analyze bottom-up cybersecurity hygiene levels around the world, we created a novel heat map of aggregate firm-level cybersecurity hygiene scores across global regions, countries, and industry sectors (Table 1, Figure 1). More than 5,000 public debt-issuing entities in 66 countries and regions were individually analyzed using proprietary CRR scores, and aggregated by industry sector. To correct for structural differences in CRR sector scores, industry average scores were equally weighted into a simple average cybersecurity performance score for each country, with further aggregation by region.

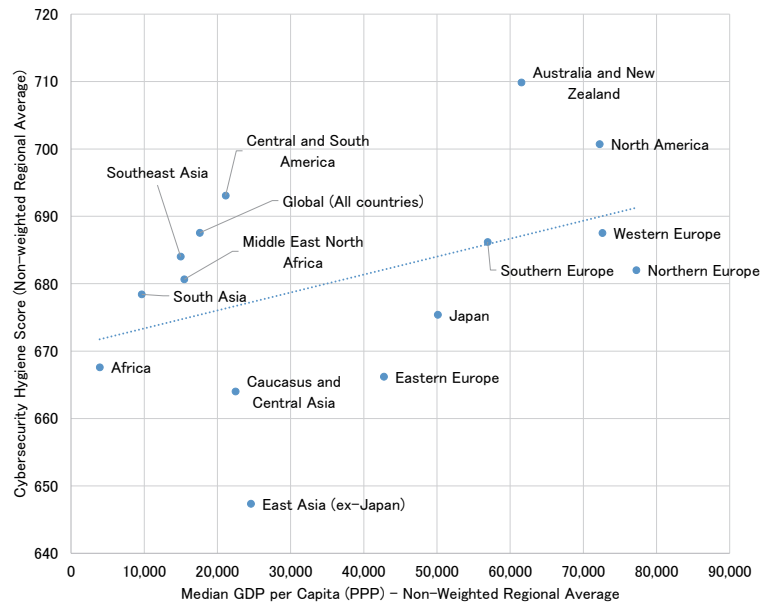
Table 1: Heat Map of Average Corporate Cybersecurity Hygiene, by Region and Sector

Region \ Sector	Sector											Simple Average	Median GDP Per Capita (PPP)
	Communi- cations	Consumer Discretionary	Consumer Staples	Energy	Financials	Health Care	Industrials	Materials	Real Estate	Technology	Utilities		
Australia and New Zealand	667	699	722	730	727	699	712	701	736	700	716	710	61,533
North America	651	684	695	716	730	700	691	706	719	695	722	701	72,210
Central and South America	611	654	684	681	695	763	687	688	689	760	711	693	21,121
Western Europe	639	669	680	684	718	698	686	686	727	694	682	688	72,603
Southern Europe	631	670	697	695	701	674	674	703	725	688	691	686	56,921
Southeast Asia	661	628	674	686	724	692	672	697	688	715	688	684	14,974
Northern Europe	606	670	690	699	715	714	679	687	681	678	683	682	77,237
Middle East North Africa	556	650	672	628	723	680	689	729	720	730	710	681	15,466
South Asia	598	641	720	656	719	657	678	685	693	740	677	678	9,657
Japan	635	670	686	651	719	682	670	677	719	650	672	675	50,106
Africa	618	630	692	660	678	665	634	717	727	703	620	668	3,919
Eastern Europe	640	550	683	667	703	640	745	730	690	660	620	666	42,756
Caucasus and Central Asia	593	665	680	665	664	647	642	695	703	697	654	664	22,470
East Asia (ex-Japan)	613	629	634	650	664	642	656	658	639	666	671	647	24,569
Global (All countries)	636	672	686	697	714	695	681	692	706	685	699	688	17,597

Note: GDP = gross domestic product, PPP = purchasing power parity.

Source: Bitsight Technologies data, author calculations.

Figure 1: Median GDP per Capita (PPP) vs Average Cybersecurity Score



Source: Bitsight Technologies data, author calculations.

These data show that while Australia and New Zealand and North America are relatively strong in cybersecurity, the East Asian region and Japan significantly underperforms other regional, global, and income-level peers for corporate cybersecurity hygiene. In East Asia, this surprising underperformance is attributable primarily to weak CRR for firms in the PRC (People's Republic of China)⁸ and the ROK (Republic of Korea), indicating a gap between these country's high cybersecurity policy commitment scores in the 2024 ITU (International Telecommunication Union) Cybersecurity Index⁹ versus actual apparent on-the-ground corporate cybersecurity practices. On the other hand, the Southeast Asian and South Asian regions are relative outperformers, with several countries in these sub regions, such as India and Malaysia, demonstrating relative leadership and validating these country's high scores for cybersecurity commitment in the ITU 2024 Global Cybersecurity Index.

VII Japanese industry sector-level cybersecurity relative to global performance

Focusing on Japan, cybersecurity performance by industry sector reveals relative underperformance versus global standards, including developed and emerging economies. In Japan as with most countries in the sample, finance sector and real estate firms tend to exhibit the highest degree of cybersecurity

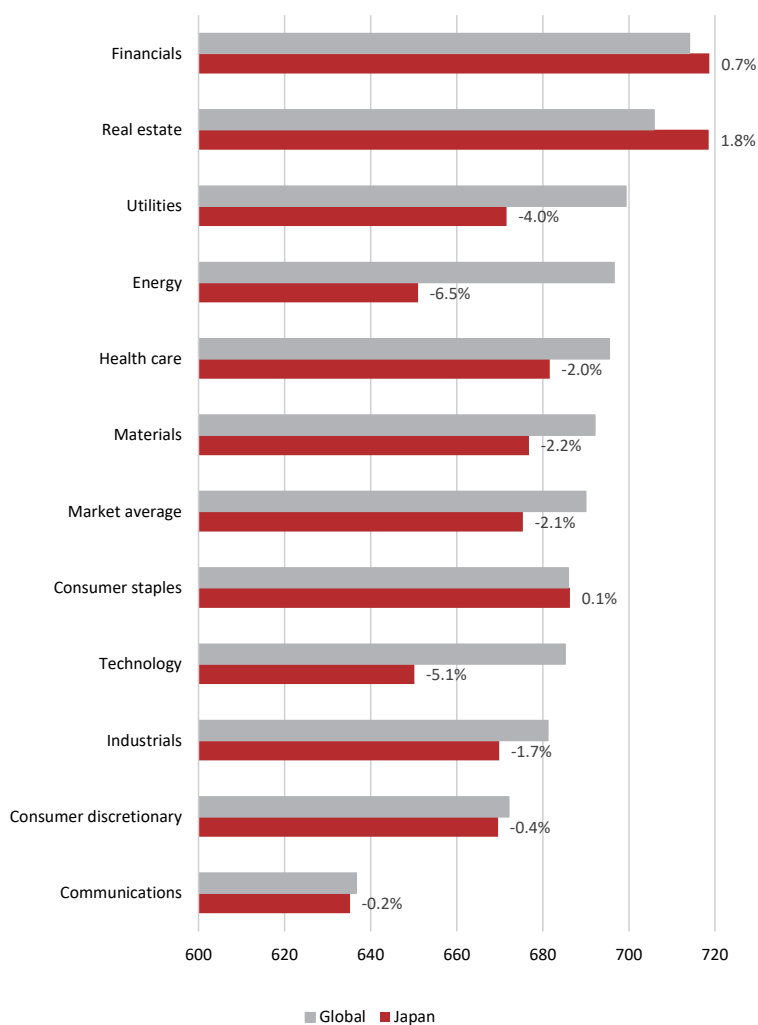
⁸ Several unique factors that may partially explain the PRC's low aggregate CRR scores. First, the country operates a national firewall which limits the visibility of domestic Chinese websites to outside users, and thus reduces the number of observable data points to the CRR scoring algorithm. Second, the relative proportion of an organization's critical network assets (which are more likely to be well maintained) outside or inside of the firewall can bias the entity's CRR quantitative score. Finally, the average size of Chinese firms in the data sample is relatively large, which tends to correlate negatively with scores since larger organizations tend to have more IP addresses and, therefore, larger overall attack surfaces.

⁹ ITU, "Global Cybersecurity Index."

hygiene. This is because even though the finance sector is a frequent target of cybercriminals, it is highly regulated and generally has the resources to invest in effective cybersecurity controls and cyber workforce development. In the same way, Japanese CRR scores for the communications sector tend to be low because these firms often operate networks and cloud-based services that mix corporate and client data traffic, which reflects a sector-specific issue as these mixed networks are difficult for CRR algorithms to parse accurately.

Of concern to regulators and investors however, corporate cybersecurity performance in Japan tends to be below the global average for almost every relevant industry (Figure 2). Among sectors, Japanese underperformance is greatest in among companies in the energy (-6.5%), technology (-5.1%), utility (-4%), and material (-2.2%) sectors. Incidentally, many of these sectors function as critical infrastructure and are commonly targeted by cybercriminals, making systematic improvements in cybersecurity attack surface management and improvement in cybersecurity hygiene a critical task for Japanese corporates.

Figure 2: Japan average Cybersecurity Risk Ratings by Industry Sector



Source: Bitsight Technologies data, author calculations.

VIII Conclusion

Corporate cybersecurity performance measurement represents a forward indicator of material unpriced risk and potential investment alpha for investors. It also presents a unique opportunity 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.