

サイバーセキュリティと財務パフォーマンス／ リスクとの重要な関連性

ビットサイト 投資管理パートナーシップ ディレクター ニコル・パスター・マツセク

ビットサイト (Bitsight) は、2011年に設立された、米国マサチューセッツ州ボストンに本社を置く世界的なサイバーリスク管理のソリューション及びサイバー格付けを提供する企業である。ビットサイトの使命は、顧客である組織とバリューチェーン内の取引先等の、サイバーセキュリティ・リスクに関するエクスポージャー、パフォーマンス及びレジリエンス（回復力）の効果的な管理を支援することである。ビットサイトのサイバーリスクに関するデータと脆弱性を把握する仕組みは、10年以上の経験に基づいて構築されており、企業のセキュリティパフォーマンスとデジタル・サプライチェーンのための技術的ソリューションの提供に重点を置いている。ビジネスリーダーや規制当局によるサイバーセキュリティ・リスクへの注目が高まる現況において、ビットサイトのデータは、サイバー保険の引き受け、信用リスク分析、取締役会におけるレポーティング、統合された投資フレームワークなど、コーポレートガバナンスや金融による対応での利用が拡大している。

ビットサイトのセキュリティ格付けにおいては、セキュリティイベントと構成情報といった2種類の外部から観察可能なデータを分析することを通じて、組織のサイバーセキュリティ体制を評価している。セキュリティイベントには、マルウェアの配布等が含まれる。これらは通常、外部の敵対者によるコントロールを意味する。また、構成情報には、サイバーセキュリティのベストプラクティスに関するチェックが含まれる。ビットサイトによる格付けは、侵害されたシステムの数、種類、イベント期間及び組織が攻撃を防御するために講じた手段を考慮した、独自のアルゴリズムに基づいて日々算出される。格付け評価では、リスクに関して、侵害されたシステム、攻撃防御手段、ユーザー

の行動、および公開情報に分類している。格付けプロセスでは、これらの要素のうち、侵害されたシステムと攻撃防御手段に重点を置いて評価している。分析の結果、企業は、同業他社と比較したパフォーマンスに基づいてA～Fのグレードを付与される。各グレードは、ビットサイトのカバレッジの中での企業の相対的位置付けを反映している。評価は、公平性を確保するために組織の規模に基づいて調整される。格付けに関するプラットフォームでは、世界に展開するセンサーから収集されたデータを組み込んでおり、情報が日々更新されるとともに、重要な変更が生じた場合にハイライトして表示される。このような革新的なアプローチにより、組織は、自社及びベンダーやパートナーのセキュリティパフォーマンスに関する貴重な洞察を得ることが可能になる。

ビットサイトのデータは、サイバーセキュリティ評価、脆弱性監視、内部レポート作成といった用途で、技術専門家によって広く活用されている。ビットサイトのセキュリティ格付けは、組織のサイバーセキュリティ・パフォーマンスの客観的かつ定量化可能な指標を提供することを通じて、利用者のより良い意思決定を支援している。ビットサイトは、特にサードパーティとの関係において、組織のセキュリティ体制の管理やリスク軽減に役立つツールや洞察を提供することを通じて、重要な役割を果たしている。

業務運営上のテクノロジーへの依存度が高まるにつれて、デジタルリスクと物理的リスク双方への対応の観点から、より広範なビジネスエコシステム全体におけるサイバーリスクのエクスポージャーの可視化が不可欠となっている。ビットサイトのプラットフォームとデータは、従来のセキュリティアプリケーションを超えて、より広範な統合リスク意思決定、特に



投資管理にまで活用可能となっている。

ビットサイトは、大量のサイバーリスク格付けと分析データセットを提供している。これには、最大4,000万の組織に関する日々の格付けが含まれている。これらの格付けは、マーシュ・マクレナン等が測定しているデータ侵害やランサムウェアを含むサイバーセキュリティ・インシデントとの強い相関関係が確認されている¹。実用的なサイバーリスクデータと分析は、主要な業績との相関性を証明している。投資マネージャーにとっては、ポートフォリオ内のサイバーリスクのプライシングと管理、意思決定プロセスの強化、リスクを効果的に軽減してリスク調整後のリターンを最大化することを可能としている。さらに、ビットサイトが格付けを付与するために収集するデータは外部から観察可能であり、企業による個別的な情報開示を必要としない。ビットサイトの格付けは、投資家にとっては公開情報として取り扱い可能となり、市場リスクの透明性向上に貢献すると言える。

サイバー攻撃はこれまで、投資家にとってプライシングに織り込めない不透明なリスクとして認識されていた。しかし、サイバー関連のニュースが散見され、規制強化の動きもある中、市場リーダーたちは、同要素を認識し、経営に織り込む動きが加速しているようだ。例えば、米国証券取引委員会（SEC）は2023年7月、上場会社に対して新たなサイバーセキュリティに関する開示規則を採択した²。これを通じて、「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義務が新たに課せられたほか、サイバーセキュリティ・リスク管理³、専門知識、ガバナンスのより詳細な開示が求められることとなった。本規則は、コーポレートガバナンスを強化し、取締役会と株主の両方の保護を強化することを目的としている。ビットサイトでは、このような規制動向を資本市場におけるサイバーセキュリティの重要性の高まりを示す先行指標として捉えている。また、投資の意思決定におけるサイバーリスクの織り込みがさらに加速するようになると予想している。

投資家は、以下に示すように、様々な方法でビットサイトのデータを活用している。

- ① デューデリジェンスと引受の強化：サイバーリスクを投資の意思決定に反映

- ② アルファ・シグナル：アウトパフォームの機会を特定

- ③ ポートフォリオリスク管理：リスクの高い企業を特定し、リスク軽減とエンゲージメント活動を優先

- ④ 投資管理：効果的なサイバーリスクの監視を通じた長期的な投資価値の保全・向上

ビットサイトのデータは、コーポレートガバナンスと企業パフォーマンスの低遅延（ある要求に対して応答するまでに要する時間を短縮し、できるだけ素早く反応させること）の代替指標として、またサイバーイベントの早期警告シグナルとして、独立して検証された強力な価値を有している。ソラクティブの調査によると、ビットサイトの格付けパフォーマンスの上位25%に入る企業は、ベンチマーク・インデックスのパフォーマンスを上回り、低いボラティリティでかつ1~7%の超過リターンを創出している⁴。同様に、ディリジェントによる分析によると、ビットサイトの格付けが高い企業は約4倍の株主価値を生み出していることが明らかになった⁵。ビットサイトがムーディーズ・アナリティクスと共に行った調査では、サイバーインシデントが財務パフォーマンスに与える重大な悪影響が示されており、12ヵ月間にわたって負のエクイティ・リターンが継続的に発生し、信用リスクに悪影響を及ぼしていることが明らかになった⁶。

ビットサイトは、投資管理における格付けの活用方法を拡大すべく、以下のとおり、資本市場の業界リーダーと多数のパートナーシップを築いている。

- ・ ムーディーズは2021年、ビットサイトに2.5億ドルを投資した。両社は、経営トップがデータを活用してより適したリスク判断を下すことを支援するという共通の目標を有している。ビットサイトのサイバーセキュリティ格付けと分析は、ムーディーズの包括的なリスクソリューションに統合されている。ムーディーズは、ビットサイトのデータを掲載した30以上のリサーチレポートを公表している。この中には、信用リスクに関するネガティブな内容のレポートが含まれるほか、サイバーリスクと財務パフォーマンスの関係等に焦点を当てている。



- 大手議決権行使助言サービス会社であるグラスルイスは、ビットサイトのデータを議決権に関する調査レポートに統合し、投資家に企業のサイバーリスクマネジメントに関する明確な洞察を提供している。
- S&Pグローバルは、ビットサイトと提携し、世界中の組織に関する重要なサイバーセキュリティ・インテリジェンスをアセットマネージャーに提供している。この協働は、信用格付けと同様にサイバーリスクの評価と管理に役立つサイバーセキュリティ格付けを提供し、銘柄選択とリスク管理の意思決定を促進している。
- ソラクティブは、ビットサイトのサイバーセキュリティ格付けを活用して、ソラクティブ・ビットサイト・サイバーリスク・インデックスを作成している。本インデックスは、優れたサイバーセキュリティを反映して、ビットサイトのサイバー格付けが高い企業が対象となっている。本連携によって、投資家に信頼性が高く実用的なデータを提供するとともに、投資戦略の強化に貢献している。

サイバーセキュリティ・リスクが市場のダイナミクスにますます影響を与える時代に、投資家はサイバーリスクを投資戦略に統合することの重要性を認識する必要がある。規制環境が変化し、サイバーレジリエンスと財務パフォーマンスを結びつける事象が増えていることも背景に、このようなアプローチの必要性がますます注目されている。ビットサイト等のプロバイダーからの包括的なサイバーリスクデータを活用することで、投資家は意思決定プロセスを強化し、ポートフォリオの価値を保全するとともに、顧客に対する受託者責任を果たすことが可能となる。サイバーの脅威が進化し続ける中、資本市場活動に堅牢なサイバーセキュリティ評価を組み込むことは、リスク調整後の持続的なリターンを達成するために不可欠と言える。

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 Critical Connection between Cybersecurity and Financial Performance and Risk

**Nicole Pastor Matusek, Director,
Investment Management Partnerships, Bitsight**

Bitsight, founded in the United States in 2011 and headquartered in Boston, Massachusetts, is a global cyber risk management and ratings provider. Bitsight's mission is to enable effective management of cybersecurity risk exposure, performance, and resiliency for organizations and their partners in the value chain. Built on over a decade of experience, Bitsight's cyber risk data and vulnerability insights were developed with a focus on delivering technical solutions for enterprise security performance and digital supply chains. Currently, with growing attention on cybersecurity risks from business leaders and regulators, Bitsight data is finding expanded use in corporate governance and financial applications such as cyber insurance underwriting, credit risk, corporate board reporting, and integrated investment frameworks.

Bitsight Security Ratings assess the cybersecurity posture of organizations by analyzing two types of externally observable data: security events and configuration information. Security events include behaviors such as malware distribution, among others, which typically indicate external adversary control. Configuration information involves checks on cybersecurity best practices. Bitsight ratings are calculated daily using a proprietary algorithm that considers the number and types of compromised systems, the duration of events, and diligence configurations. Ratings categorize risks into compromised systems, diligence, user behavior, and public disclosures, with compromised systems

and diligence being heavily weighted. Companies receive letter grades based on their performance relative to peers, ranging from A to F, with each grade reflecting the company's standing in Bitsight's inventory. Ratings are normalized based on the size of the organization to ensure fairness. The platform provides daily updates and highlights significant changes, incorporating data collected from globally deployed sensors. This innovative approach allows organizations to gain valuable insights into their security performance and that of their vendors and partners.

Bitsight's data is widely used by technical professionals for cybersecurity assessments, vulnerability monitoring, and internal reporting. Its security ratings provide an objective, quantifiable measure of an organization's cybersecurity performance, facilitating better decision-making. Bitsight plays a crucial role in the cybersecurity landscape by offering tools and insights that help organizations manage their security posture and mitigate risks, particularly in the context of third-party relationships.

Growing operational reliance on technology has made cybersecurity both a digital and a physical risk, making it essential to gain visibility into cyber risk exposure across the broader business ecosystem. The power of the Bitsight platform and data extends beyond traditional security applications to integrated risk decision making more broadly, particularly investment management.



Bitsight produces the largest cyber risk ratings and analytics dataset, with daily ratings on up to 40 million entities and the strongest correlation to cybersecurity incidents, including breach and ransomware, as measured by industry leaders such as Marsh McLennan¹. Actionable cyber risk data and analytics with proven correlation to key business outcomes and a relative scoring methodology enable investment managers to price and manage cyber risk within their portfolios, enhance their decisioning processes, and mitigate risks effectively to maximize risk-adjusted returns. Further, the data Bitsight collects to generate its ratings is externally observable and does not require company disclosure, representing public information for investors and contributing to greater market risk transparency.

Cyber is an unpriced and historically opaque dimension of risk for investors, but continued cyber headlines and regulatory tailwinds are driving accelerated awareness and adoption by market leaders. For example, in July 2023, the U.S. Securities and Exchange Commission (SEC) voted to adopt new cyber security requirements for publicly traded companies², creating new obligations for reporting “material” cybersecurity incidents and requiring more detailed disclosure of cybersecurity risk management³, expertise, and governance. The new rules aim to enhance corporate governance and bolster protections for both boards and shareholders. Bitsight views regulatory moves like this as a leading indicator of the growing importance of cybersecurity in capital markets that will further exert pressure on the integration of cyber risk in investment decision making.

Investors leverage Bitsight data in a variety of ways:

1. Enhanced Due Diligence & Underwriting: Price cyber risk into investment decision making
2. Alpha Signal: Identify opportunities for outperformance
3. Portfolio Risk Management: Identify

high-risk companies to prioritize risk mitigation and engagement activities

4. Investment Stewardship: Enhance and protect long-term investment value by promoting effective cyber risk oversight

Bitsight data has strong, independently verified value as a low-latency proxy for corporate governance and company performance and a downside early warning signal of adverse cyber events. Solactive Research⁴ found that companies in the top 25% of Bitsight ratings performance outperform the benchmark indices, generating excess returns of 1-7% with lower volatility. Similarly, an analysis by Diligent⁵ found that companies with advanced Bitsight ratings create nearly four times of shareholder value. Bitsight research published with Moody's Analytics⁶ illustrated the significant negative impacts of cyber incidents on financial performance, driving enduring negative equity returns experienced over a 12-month period and detrimental impact on credit risk.

Bitsight has numerous partnerships with capital markets industry leaders to facilitate the investment management use case:

- **Moody's** invested \$250 million in Bitsight in 2021. The two organizations share a common goal of helping leaders make better risk decisions with data. Bitsight's cybersecurity ratings and analytics are integrated into Moody's suite of comprehensive risk solutions. Moody's has produced over 30 research publications featuring Bitsight data, including multiple credit negative reports, further underscoring the relationship between cyber risk and financial performance.
- **Glass Lewis**, a leading proxy advisory services firm, integrates Bitsight's data into its Proxy Paper research reports, offering investors clear insights into a company's cyber risk management.
- **S&P** Global partners with Bitsight to provide asset managers with critical cybersecurity intelligence on organizations worldwide. This collaboration offers



cybersecurity ratings that help assess and manage cyber risk, similar to credit ratings, driving stock selection and risk management decisions.

- **Solactive** leverages Bitsight’s cybersecurity ratings to create the Solactive Bitsight Cyber Risk Indices. The indices focus on companies with high BitSight Security Ratings, reflecting superior cybersecurity. This partnership provides investors with reliable and actionable data to augment their investment strategies.

In an era where cybersecurity risks are increasingly influencing market dynamics, investment managers must recognize the

critical importance of integrating cyber risk into their investment strategies. The evolving regulatory landscape and the growing body of evidence linking cyber resilience to financial performance underscore the necessity of this approach. Leveraging comprehensive cyber risk data from providers like Bitsight enables investment managers to enhance their decision-making processes, protect portfolio value, and fulfill their fiduciary duties to clients. As cyber threats continue to evolve, incorporating robust cybersecurity assessments into capital market activities will be essential for achieving sustained, risk-adjusted returns.

-
- 1 Bitsight, “New Study Finds Significant Correlation Between Bitsight Analytics and Cybersecurity Incidents,” October 25, 2022.
 - 2 U.S. Securities and Exchange Commission, “17 CFR Parts 229, 232, 239, 240, and 249 [Release Nos. 33-11216; 34-97989; File No. S7-09-22] RIN 3235-AM89: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” July 26, 2023.
 - 3 Bitsight, “Cyber Risk Management: Our Solutions”.
 - 4 Solactive, “Cybersecurity as a Competitive Advantage: Introducing the Solactive BitSight Cyber Risk Indices,” October 6, 2020.
 - 5 Diligent, “Companies With Advanced Cybersecurity Performance Deliver Nearly Four Times’ Higher Shareholder Return Than Their Peers, According to Diligent and Bitsight,” March 26, 2024.
 - 6 Moody’s Analytics, “The impact of Cyber Security Management Practices on the Likelihood of Cyber Events and its Effect on Financial Risk,” September 2023.