Bond Blog 要約版

PGIM FIXED INCOME

サイバーセキュリティ：ESG インパクトおよび信用力への影響

本稿は、PGIM フィクスト・インカムのシニア ESG アナリストである Birgit Lundem Jakobsen が 9 月 26 日に執筆したブログ “Cybersecurity: How it Affects ESG Impact and Credit Quality” の内容を PGIM ジャパン株式会社が要約したものであり、情報提供のみを目的として作成されたものです。

サイバー攻撃はますます頻発しており、その被害も増大している。こうした中、これらサイバー攻撃が ESG に及ぼす悪影響と信用力の低下を防ぐために、企業は急速なテクノロジーの進歩に後れを取らないよう努める必要がある。サイバー攻撃に関するリスクを評価する際には、業種別の分析もさることながら企業毎の検証が極めて重要となる。例えば、徹底的なサイバー衛生（自社の IT 環境を定期的に検証し、健全な状態を保持する取り組み）、強力なガバナンス、専門知識を持った取締役を有する企業は相対的にリスクへの耐性が高いと考えられる。このように、適切なボトムアップ分析によって個別企業を正しく評価することで、顧客の資産をサイバー攻撃から守ることに貢献できると PGIM フィクスト・インカムは考えている。本レポートでは、サイバーセキュリティが ESG インパクト評価と信用力に及ぼす影響について考察する。

<要旨>

- Transforma Insights によると、IoT によってインターネットに接続されたデバイス（コネクテッドデバイス）の数は 2023 年現在で 151.4 億台と過去 4 年間で倍増しており、2030 年までに更に倍増して 294 億台に達すると見込まれている。コネクテッドデバイスの増加に伴ってサイバー犯罪も急増しているが、依然として企業側の対策は不十分であり、McAfee と CICS が 2020 年に実施した調査によると、IT セキュリティに関する事故の予防/対応計画を策定していると回答した企業は 44%にとどまっている。

- 多くの企業が、サイバー犯罪の増加が示唆する戦略的リスクや、強固なサイバーセキュリティによってもたらされる戦略的機会（競争上の優位性など）を過小評価しているが、こうした認識不足が財務的に重大な影響を及ぼす可能性がある。サイバー攻撃によって、セキュリティ侵害への対応や訴訟費用などの直接的なコストが生じるほか、業務の中断、風評被害、顧客の喪失、信用力の低下、さらには格下げによる資本コストの上昇など、広範な影響が及ぶと考えられる。こうした間接的な影響は長期にわたり、定量化も困難であるが、多くの場合には総損失額の大部分を占める。

- ESG インパクトの観点からも、企業は強固なサイバーセキュリティを構築する責任を負っている。サイバー攻撃による機密性の高い個人データの漏えい、重要インフラの停止、ソーシャルメディアの操作など、社会的および環境的にも大きな損害がもたらされる可能性があり、優れたガバナンスのためには強固なサイバーセキュリティの構築が不可欠である。

- サイバーセキュリティを巡る環境は変化を続けている。個人情報の保護に関する消費者の関心は高まっており、規制当局もこれを認識している。こうした中、2023 年 7 月 26 日に米国証券取引委員会（SEC）は、サイバーセキュリティに関する新しい開示規則を採択した。これにより、12 月から上場企業は重大な事故を 4 日以内に開示する必要があるほか、サイバーセキュリティのリスク管理、戦略、ガバナンスについての重要情報の年次開示が求められる。また、AI および量子コンピューターの進歩によってより安全性の高い暗号化アルゴリズムが可能となり、サイバーセキュリティの強化に貢献できると考えられる一方、サイバー攻撃を行う側もこうしたテクノロジーを利用する可能性が高い。

サイバーセキュリティ：ESG インパクトおよび信用力への影響

- 必然的に全ての企業がサイバー攻撃の標的となり得るが、IBM のデータによると、特に製造業、金融・保険、専門サービス、消費者サービスなどが最も頻繁に標的となっている。サイバー攻撃の標的とされやすい企業の特徴として、①サイバー攻撃による事業中断が深刻な影響をもたらす、②広範あるいは機密性の高い情報を保持している、③サイバー攻撃の金銭的要求に応じる能力を有しているなどが挙げられる。

- ますます頻発するサイバー攻撃による被害が拡大する中、業種別の特性に加え、企業毎の検証がより重要となる。サイバー攻撃に対する防衛策は機微情報であるため各社は積極的な開示をしておらず、企業毎の評価は容易ではない可能性があるが、提供される企業情報の分析を通じて各社のサイバー攻撃に対する備えを確認することはできる。その際には、どのようなセキュリティー・ソフトウェアがインストールされているかだけでなく、ガバナンス、サイバー攻撃に関するリスク管理、サイバーセキュリティ体制、事故発生時の対応計画、サイバー攻撃からの防御と抑止のプロセスについても確認することが望ましい。これに加え、各社とのエンゲージメントを通して、サイバーセキュリティに対する経営陣の認識と関与を詳細に確認することができる。こうした適切な分析によって顧客の資産をサイバー攻撃から守ることに貢献できると PGIM フィクスト・インカムは考えており、あらゆる投資家にとって、投資先の信用および ESG を評価する際にはサイバーセキュリティ体制について検証することが重要であると考える。

データの出所(特に断りのない限り)：PGIM フィクスト・インカム、2023 年 9 月 26 日現在。

留意事項

本資料に記載の内容は、PGIM フィクスト・インカムが作成した ”Cybersecurity: How it Affects ESG Impact and Credit Quality” をPGIM ジャパン株式会社が要約したものです。PGIMフィクスト・インカムは、米国SEC の登録投資顧問会社であるPGIM インクの債券運用部門です。

本資料は、プロの投資家を対象としたものです。すべての投資にはリスクが伴い、当初元本を上回る損失が生じる可能性があります。

本資料は、当グループの資産運用ビジネスに関する情報提供を目的としたものであり、特定の金融商品の勧誘又は販売を目的としたものではありません。また、本案内に記載された内容等については今後変更されることもあります。

本資料に記載されている市場動向等は現時点での見解であり、事前の通知なしに変更されることがあります。また、その結果の確実性を表明するものではなく、将来の市場環境の変動等を保証するものでもありません。

本資料で言及されている個別銘柄は例示のみを目的とするものであり、特定の個別銘柄への投資を推奨するものではありません。

本資料に記載されている市場関連データ及び情報等は信頼できると判断した各種情報源から入手したものですが、その情報の正確性、確実性について当社が保証するものではありません。過去の運用実績は必ずしも将来の運用成果等を保証するものではありません。

本資料に掲載された各インデックスに関する知的財産権及びその他の一切の権利は、各インデックスの開発、算出、公表を行う各社に帰属します。

本資料は法務、会計、税務上のアドバイスあるいは投資推奨等を行うために作成されたものではありません。

PGIM ジャパン株式会社

金融商品取引業者 関東財務局長（金商）第 392 号

加入協会：一般社団法人日本投資顧問業協会、 一般社団法人投資信託協会、一般社団法人第二種金融商品取引業協会

PGIMJ102637