サイバーリスク：マクロ金融安定性に対し高まる懸念

デジタル化の進展、技術進歩、地政学的な緊張の高まりを背景に、サイバー関連のインシデント、特に悪意を伴うものが、過去二十年、とりわけ 2020 年以降、非常に頻繁に発生している。主要金融機関が甚大な被害にあえば、信頼の喪失、重要なサービスの途絶、およびテクノロジーや金融面でのつながりを要因とした他の金融機関への波及により、マクロ金融の安定性が重大な脅威にさらされかねない。

本章で示すように、これまでのところサイバーインシデントは金融システムを脅かすまでには至っていないが、企業が巨額の直接的な損失を被るリスクは高まっており、被害が 25 億ドルを超過する事態も想定される。さらに、サイバーインシデントに伴う間接的な損害も大きく、被害企業が公表した直接的損額を大きく上回ることが多い。

サイバーインシデントの発生と予防に寄与する要因を理解することが、強固なサイバーセキュリティ政策や戦略を確立する上で重要である。本章の分析は、デジタル化の進展と地政学的な緊張の高まりによりサーバーインシデントのリスクが大幅に高まる一方で、サイバー関連法制の整備と企業内のサイバー関連のガバナンス強化を通じ、リスクの逓減を図りうることを示している。

金融セクターは高いサイバーリスクにさらされており、サイバーインシデント全体の五分の一近くが金融機関を対象としたものである。決済サービスや銀行カストディ業務などの重要なサービスにおいては、その寡占度の高さと代替性の低さから、金融機関におけるサイバーインシデントが特に破壊的な影響をもたらす恐れがあり、金融機関がサイバーセキュリティを強化し業務継続性を確保することの重要性が強調される。また、金融機関の業務は外部の共通 IT プロバイダーに依存しているケースが多く、ショックが同時発生し波及するリスクを高めている。

金融機関における重大なサイバーインシデントは、金融システムに対する信頼を損ない、極端な場合には市場での売り注文の殺到や銀行の取り付けが起きる可能性もある。サイバーインシデントを契機とした深刻な取り付けはこれまでのところ起こっていないが、実証分析によれば小規模な米銀行においては、サイバー攻撃を受けた後、小規模ながらある程度長期にわたり預金の流出が起きていたことが示唆されている。

グローバルな金融システムへのサイバーリスクが重大で深刻化しつつある中、政策面およびガバナンス面でこうした動向に遅れを取ってはならない。しかしながら、新興市場国と発展途上国の中央銀行と金融監督当局を対象とした調査では、サイバーセキュリティ政策の枠組みが依然として不十分なケースが多く見られる。

金融セクターのサイバーリスクへの耐性は、国家レベルでの十分なサイバーセキュリティ戦略と、適切な規制監督の枠組み、有能なサイバーセキュリティ人材、国内・国際的情報共有体制の整備を通じて強化しなければならない。サイバーリスクのモニタリングの実効性を上げるためには、サイ

バーインシデントの報告体制も強化するべきである。監督当局は、金融会社の役員に対して、サイバーセキュリティの管理と適切なリスクカルチャーの醸成、サイバー衛生の徹底、サイバートレーニング・サイバー意識の向上についての責任を課すべきである。サイバーインシデントに伴い生じうるサービスの途絶を抑制するために、金融機関はサイバーインシデントへの対応と復旧の手順を定め、テストすべきである。各国当局は有効な対応手順と危機管理の枠組みを整備する必要がある。

IMF は金融セクター評価プログラム（FSAP）と能力開発の取り組みを通じ、加盟国のサイバーセキュリティの枠組み強化を積極的に支援している。報告書全文は、こちらの英語版をご参照ください。http://IMF.org/GFSR-April2024