

2026 年 10 月 14 日

サイバー攻撃による経済損失をどう考えるか

～一企業の被害から、マクロ的な経済損失となるリスク～

経済調査部 主席エコノミスト 前田 和馬

(Tel : 050-5473-3888)

情報漏洩を中心にサイバー攻撃による被害が国内外で目立っている。相次ぐサイバー攻撃にはAIが悪用された可能性が指摘されており、今後もこうした被害は拡大する懸念がある。サイバー攻撃による経済的な影響は主に3つ考えられる。

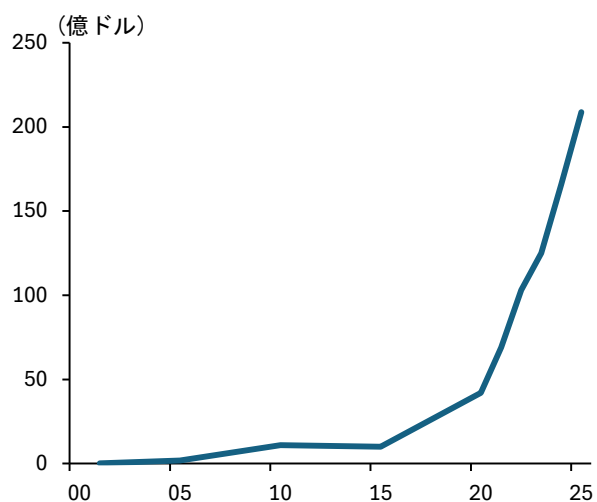
まず、被害による直接的な金銭損失であり、仮想通貨等の資産の流出、身代金の支払い、被害者への補償金支払いなどが挙げられる。FBIが被害申告ベースでまとめた「Annual Internet Crime Report 2025」によると、米国を中心としたサイバー犯罪の被害総額（個人被害も含む）は209億ドルと近年飛躍的に拡大している。なお、こうした被害は基本的に所得移転であり、生産活動を捕捉する国内総生産（GDP）に直接的な影響を与えるわけではない。

次に、サイバー攻撃を通じた企業活動への損害だ。例えば[CSISとMcAfeeによる2020年の調査](#)では、サイバー攻撃を受けた場合に業務は平均18時間中断したと指摘する。サイバー攻撃は既存顧客へのサービス提供や新たな顧客獲得活動などを抑制する懸念がある。これに加えて、企業のブランド価値を毀損し、顧客は該当サービスの利用を当面ためらうかもしれない。

サイバー攻撃による経済活動への被害が一企業に留まるのであれば、競合他社が代替的にサービスを提供する、或いはシステム復旧後に挽回生産などが生じることで、マクロ的な影響は限定される。しかし、こうした被害が「交通インフラなど代替が難しい企業」、或いは「産業内の広範な企業」に及ぶ場合、サイバー攻撃で損なわれた供給能力を補うことが難しく、マクロ経済全体の損失へと波及する。AIを通じたサイバー攻撃の頻発は、従来のミクロ的な「一企業の被害」から、マクロ的な「産業や経済全体の被害」に転じるリスクを高めている可能性がある。

最後に、サイバーセキュリティ対策の強化によるIT関連支出の増加であり、これはGDPを押し上げる可能性が高い。例えば、2000年問題（西暦が2000年になるとコンピュータが誤作動を起こすとの懸念）の際のIT対策費用は全世界で[3,000～6,000億ドル](#)と、1999年における世界GDPの0.9～1.8%に達したとみられている。一方、攻撃をうける企業の防御対策よりも、AI脅威論による開発抑制の動きが強まる場合、データセンター投資や株式市場の調整を通じて景気減速へと繋がる懸念がある。なお、米国ではトランプ政権が対中競争力の観点からAI規制に消極的であるほか、連邦議会におけるFrontier ActなどのAI規制法案も成立に至るかは不透明だ。

図表 1：全米におけるサイバー犯罪の被害総額



出所：FBI より第一ライフ資産運用経済研究所が作成

以 上