

金融・経済指標とセキュリティインシデントとの連関性に関する分析

An Analysis of the Relationship between Financial & Economic Indicators and Security Incidents

村上誠樹 暗号・認証分科会 情報セキュリティ大学院大学

1. 研究背景・課題

金融サービスは経済活動を支える重要なインフラの一つであり、サービスが大きく滞れば金融機関のみならず社会全体に深刻な影響を及ぼす。したがって、従来の対策が通用しなくなる可能性をあらかじめ想定しておくことが求められる。

一方で、技術の進歩によって新たな外的リスクが顕在化した場合、関係者はセキュリティ投資の妥当性を明示しつつ実施する必要がある。しかし、想定されていなかったリスク要因では、定量的な指標が不足し、費用対効果を正確に算出しづらいという課題がある。

たとえば量子コンピュータの実用化が進めば、RSAなどの素因数分解型暗号の解読リスクが高まり、金融サービス全体に波及的な影響を及ぼす可能性が指摘されている。こうした状況を受け、金融機関では耐量子計算機暗号(PQC)への移行検討が始まっている。

2. 目標とする成果

社会インフラとして機能する金融サービスが大きく滞った場合をシミュレートし、その波及効果を定量的に示すことで、セキュリティ投資に関する意思決定の参考指標を提供することを目指す。

3. これまでの成果

2024年度

- 企業が将来的にクリプト・インベントリー(台帳)を整備し、PQCへの移行を行う必要性が高まると想定し、関連する研究事例を調査。
- 米国立標準技術研究所(NIST)によるPQC標準化プロジェクトの動向を情報収集。
- 定量的評価手法を検討する過程で、**産業連関表**(総務省)を用いたマクロ経済的なサイバー被害評価の先行研究に着目。
- 金融インフラの停止がもたらす影響を幅広く捉えるには、業界や企業といった個別要素に加え、数年単位のマクロ指標を用いて動向を把握できるデータが不可欠と判断。**資金循環統計**(日本銀行)に注目し、このデータを活用する研究事例を調査。

4. 今後の取り組み計画

2025年度

- 既往研究の「実サイバー被害事例を取り入れた定量評価手法」や「波及効果モデルの構築方法」を参考にしつつ、実際には金融機関で事故が起きにくく観測データが限定的であるという課題を踏まえ、資金循環統計を中心に据えたモデルを構築する。
- 資金循環統計を活用した研究研究で示されるデータ取り扱いの手法をベースに、金融資産フローが大きく滞るケースを想定し、その波及効果を分析する。
- モデル上の仮定がどの程度妥当かを検証し、セキュリティ投資や緊急時の対応指針を提示することで、金融機関が合理的な意思決定を行うための根拠を提供することを目指す。