

サイバーリスクを金融安定の問題として捉え直す OECD 報告書が示す三つの増幅経路 ——地政学、サプライチェーン、市場ストレス

国際局国際機構課資金移転対策室 課長補佐 千田 正儀

金融市場のデジタル化は利便性を高める一方、決済・クラウド・外部委託先への共通依存を深めた。OECDの新報告書は、サイバーリスクを個社のIT障害ではなく、地政学、サプライチェーン、市場ストレスを通じて金融安定へ波及する問題として捉える。本稿では具体的な事例と図表を中心に、その含意を整理する。

1 OECD報告書の位置付け—サイバーを金融安定と経済安全保障の問題として捉える

OECDが公表した『金融市場におけるサイバーセキュリティと地政学的リスク』*1は、サイバー事案の頻度と複雑性の高まりを、金融市場の構造変化と結び付けて分析している。この報告書が重視するのは、(1) クラウドや重要ベンダーを介した第三者・サプライチェーン依存、(2) 急速なデジタル化に人材・ガバナンスが追いつかない新興・途上国の脆弱性、(3) 市場が既に不安定な時にショックが増幅されるタイミングの三点である。

金融機関は国境を越えてデータ、決済、清算、本人確認、ソフトウェアを共有する。したがって、最初の侵害が小規模な事業者であっても、代替しにくい機能を止めれば、流動性、信用供給、資産価格、投資家の信認へ波及し得る。サイバーセキュリティは技術部門の防御だけで完結せず、金融安定と経済安全保障を横断する経営・政策課題なのである。

2 地政学が攻撃の目的とタイミングを変える

地政学的緊張が高まると、サイバー攻撃は金銭獲得

だけでなく、制裁回避や越境決済の攪乱、政治的シグナルの発信、相手国の金融システムへの信頼低下にも用いられる。先のOECD報告書に掲載されている図表をみると、2017年のNotPetyaや2022年のロシアによるウクライナ侵略前後に、関係地域のサイバー事案が増えていた局面が分かる。相関があることは因果関係を意味しないが、この図表にある事案の動きを見ると攻撃の発生時期を国際情勢と切り離して評価できないことを示唆される。国家に関連する主体、組織犯罪集団、ハクティビストが同じ空間で活動し、攻撃が制裁発表や軍事的緊張と重なる場合もある。ランサムウェアのサービス化、IoT端末を使ったDDoS、正規データに悪性コードを隠す手法、価格フィードの改ざんなど、目的と技術の双方が多様化している。

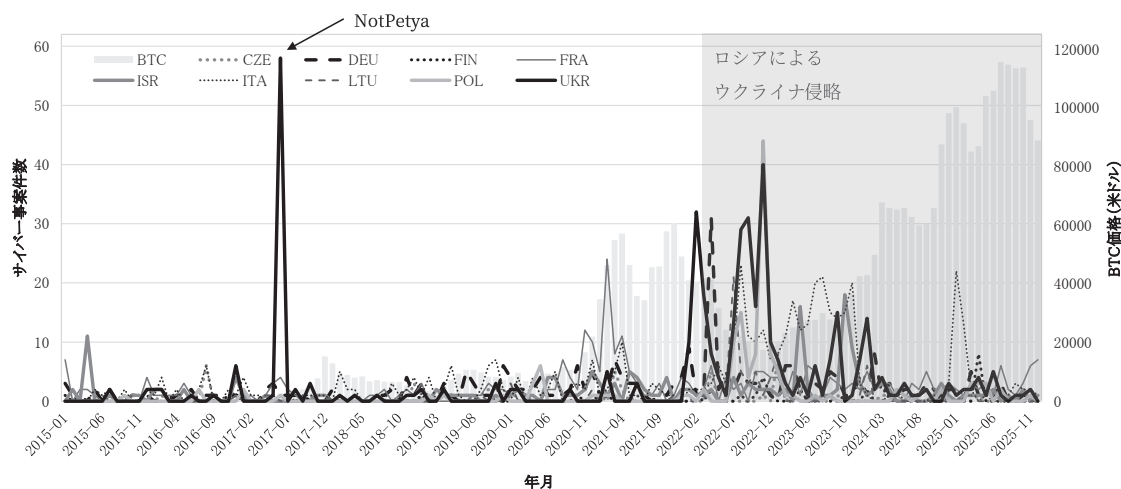
具体的な事例を見ると、サイバー事案の影響が広範に及ぶことが分かる。例えば、2016年の Bangladesh 中央銀行・SWIFT 事案では、ローカルなネットワーク防御と認証の弱点が突かれ、8,100万ドルが不正送金された。2017年のNotPetyaの事案は身代金獲得より業務破壊の色彩が強く、直接被害を受けた企業よりも取引先など間接被害企業の損失が数倍大きかった。2023年には、米国防総省付近の爆発を装った生成AIで作成したとみられる偽画像が拡散し、S&P500が一時約0.3%下落した後、虚偽と判明して反発した。この偽画像の事案は、実際の侵入がなくても、情報操作だけで市場価格が動き得ることを示している。

暗号資産を巡るサイバー攻撃は、金銭目的だけでなく、地政学的な動機も重なり得る。先のOECD報告書によれば、2024年には暗号資産プラットフォームから約22億ドルが盗まれ、2025年の大手プラットフォーム事案では約15億ドルが流出し、イーサリアムの価格が

*1) OECD 報告書『金融市場におけるサイバーセキュリティと地政学的リスク』(OECD Business and Finance Policy Papers, No.104, DOI: 10.1787/1002b1fd-en.)



図表1 地政学的緊張期のサイバー事案



注：BTC価格と、チェコ、ドイツ、フィンランド、フランス、イスラエル、イタリア、リトアニア、ポーランド、ウクライナの月次サイバー事案件数を示す。網掛けはロシアによるウクライナ侵略以降を示す。相関があることは因果関係を意味しない。
出所：OECD（2026）Figure 5を基に筆者が邦訳・再構成。

4%下落した。盗まれた資産が複数の法域やチェーンを短時間で移動すれば、制裁回避や拡散金融への利用を含め、AML/CFTによる事後追跡だけでは対応が難しい。

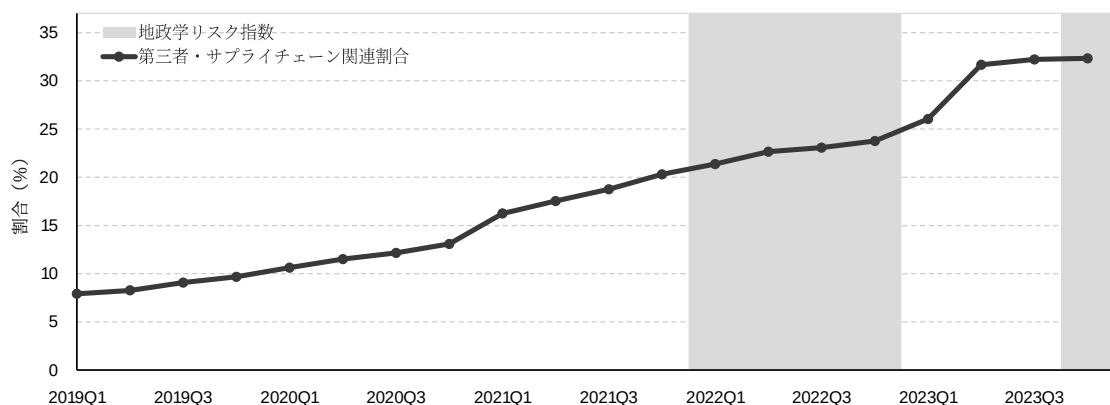
3 サプライチェーンの「弱い接続点」が共通ショックになる

金融分野のサプライチェーンとは、物流だけを指すのではなく、クラウド、データセンター、勘定系、本人確認、決済メッセージ、保管・清算などの重要なICT・サービス依存までを含めて指す言葉である。先のOECD報告書によると金融機関のサイバー事案に占める第三者・ベンダー関連の割合が2019年の約8%から2023年末には32%超へ上昇した。仮に多くの機関が同じ事業者に依存すれば、一事業者の障害が複数

機関の業務を同時に停止させ得ることにつながる。G7では中小企業向け事案が2021年初から2025年初までに14倍超へ増え、近年は銀行向け事案を上回る局面もある。攻撃者が防御の強い中核機関を正面から狙うのではなく、専門人材や投資余力の乏しい小規模事業者を入口に選んでいる可能性がある。

2024年の世界的なIT障害は悪意ある攻撃ではなかったが、集中した技術提供者の更新不具合が多数の企業・金融サービスを同時に止めることが可能であることを示した。2025年には米住宅ローン関連サービス会社への攻撃で、直接侵害されていない複数の大手銀行に関係する顧客情報が影響を受けた。重要なのは、委託先を契約時に審査するだけでなく、再委託先、代替手段、復旧目標、退出計画まで継続的に把握することである。ASEANのように中小企業が生産・物流・

図表2 金融機関のサイバー事案に占める第三者・サプライチェーン関連の割合



注：線は第三者・ベンダー関連事案の12四半期移動割合、縦帯は地政学リスク指数が上位25%となる四半期を示す。
出所：OECD（2026）Figure 7を基に筆者が邦訳・再構成。

貿易金融を支え、デジタル化が急速に進む地域では、ローカルな障害が国境を越えて実体経済と金融へ伝わりやすい。サイバー耐性は取引先選定や投資判断を左右する経済安全保障上の条件にもなりつつある。

4 市場ストレス時には同じサイバー事案でも影響が大きい

先のOECD報告書では、市場が平常時にあるかストレス下にあるか、また全サイバー事案に占める銀行向け事案の割合が低いか高いかを組み合わせ、ハイイールド債の信用リスクプレミアムを比較した。分析の結果を見ると、市場ストレスと銀行向け事案の集中が重なる区分でプレミアムが最も高いことが明らかになった。これは因果関係を証明するものではないが、流動性が乏しくリスク回避が強い局面では、業務障害が担保需要、資金繰り、信用供給への懸念を通じて市場の再評価を増幅し得ることを示す。したがって、平時の平均損失だけを基準に資本・流動性バッファを設計するのでは不十分であることが示唆される。市場ストレス、重要ベンダー障害、決済停止、偽情報の拡散が同時に起きる「複合シナリオ」を想定する必要がある。

5 実証研究が補足する二つの伝播経路

Chida, Kim and Yoshino (2026a) は、銀行部門のサイバー・ストレスが貸出・資金供給能力を徐々に弱め、その影響が3～4四半期後の長期国債価格の上

昇と上乗せ金利の低下として現れ、金融ストレスが高い時ほど大きくなる可能性を示した。また、Chida, Kim and Yoshino (2026b) は、共通のサイバー・ストレス下では、預金規模に対して店舗数が少ない銀行の取引性預金の相対的な減少幅が、店舗型銀行より少ないことを示した。ただし、これは特定の銀行モデルが絶対的に安全であることやシステム全体で預金流出が生じることを意味しない点に留意が必要である。

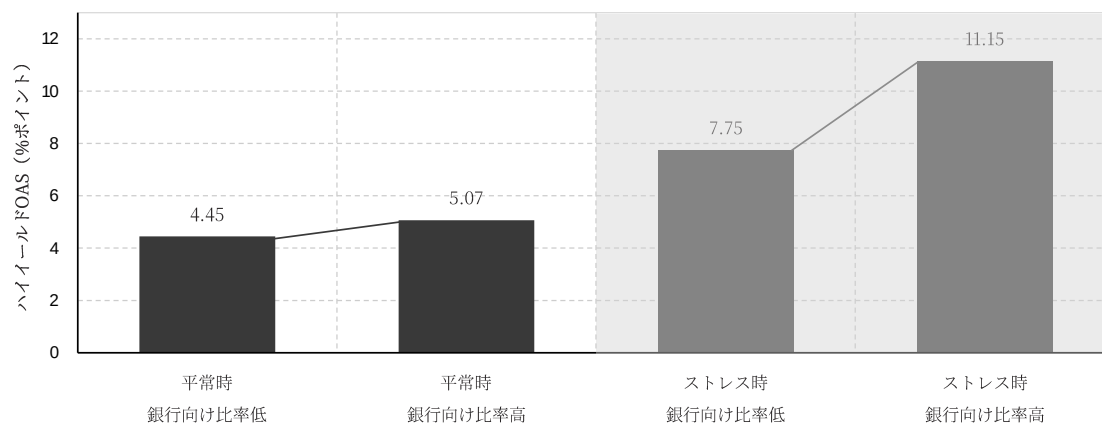
6 日本の金融機関と当局等への示唆

最後に、日本の金融機関と関係当局等に対して、以上の研究成果や考察を踏まえて四点提示したい。

第一に、サイバーリスクを盗難額や停止時間だけで測らず、決済継続、日中流動性、担保・マージン需要、取引性預金、信用供給、市場価格を一つのシナリオで点検すべきである。第二に、重要な第三者サービスを機能単位で可視化し、複数機関が同時に影響を受ける集中リスクをストレステストへ組み込む必要がある。第三に、サイバー部門、AML/CFT・制裁担当、資金繰り、広報、海外拠点が、偽情報を含む複合事案への初動を共同で訓練すべきである。特に、事実確認前の情報が市場を動かす局面を想定し、当局、取引所、金融機関が確認済み情報と未確認情報を区別して迅速に発信する手順が重要である。

第四に、地域・国際レベルの共同監視・支援の枠組みを整備することである。事案情報を集約・分析し、警戒情報、予防・防御プログラム、事案発生後の対

図表3 市場ストレスと銀行向けサイバー事案が重なる場合の信用リスクプレミアム



注：各棒はICE BofA US High Yield Index OASの区分別平均。市場ストレスはVIXが標本の80パーセンタイル以上、銀行向け比率「高」はサイバー事案に占める銀行の割合が75パーセンタイル以上の月である。記述統計であり、因果関係を示すものではない。
出所：OECD (2026) Figure A D.1 を基に筆者が邦訳・再構成。



応・復旧支援を金融機関に提供すれば、個々の銀行の重複投資を抑えつつ、専門人材を確保しにくい中小金融機関の対応力を底上げできる。OECDが提案する地域データセンターや共有分析拠点は、その具体的な基盤となり得る。ただし、共有基盤には、アクセス権、機密保持、法的保護、報告形式の共通化を明確にし、単なるデータ倉庫ではなく、早期警戒、共同演習、フォレンジック、脆弱性対応を継続的に提供する運用機能とする必要がある。サイバー攻撃を完全に防ぐことは難しい。したがって政策の目標は、侵害が起きても重要機能を維持し、波及を限定し、信認を速やかに回復できる金融システムをつくることである。地政学、サプライチェーン、市場ストレスを別々に扱わず、一体的な監視と危機対応へ接続することが求められる。

参考文献

- ・ OECD (2026) , Cybersecurity and geopolitical risks in financial markets, OECD Business and Finance Policy Papers, No.104.
- ・ Chida, M., Kim, S. and Yoshino, N. (2026a) , “Cyber risk under stress : Bank cyber shocks and systemic fragility” , Finance Research Letters, 100, 109950.
- ・ Chida, M., Kim, S. and Yoshino, N. (2026b) , “Cyber liquidity risk in the digital banking era : Evidence from transaction-deposit reallocation” , Finance Research Letters, 109, 110548.
- ・ Alba, D. (2023) , “How Fake AI Photo of a Pentagon Blast Went Viral and Briefly Spooked Stocks” , Bloomberg, 22 May 2023.

謝辞 本稿の作成に当たり、緒方国際局長、土橋優氏、草木純子氏、須田涼子氏をはじめとする国際機構課の関係者、及び高橋幸裕氏（元OECD政策アナリスト）から政策面及び実務面における有益な助言と支援をいただいた。また、本稿に関連する実証研究に関し、吉野直行氏（慶應義塾大学）及びSeohyun Kim氏（ソウル大学）から有益な示唆をいただいた。記して感謝申し上げる。

【略歴】財務省勤務。前OECD金融企業局シニアエコノミスト。金融市場、デジタル金融、サイバーリスク、アジアの金融改革に関する政策分析・国際協力に従事。ロンドンスクールオブエコノミクスにて修士号。

注：図表1～3はOECD（2026）の原図・データを基に筆者が邦訳・再構成した。本稿の見解は筆者個人のものであり、筆者の所属機関の公式見解を示すものではない。