IMFBlog
INSIGHTS AND ANALYSIS ON ECONOMICS & FINANCE

金融セクターのサイバーリスクを試算する

クリスティーヌ・ラガルド **2018 年 6 月 22 日**

サイバー攻撃による金融機関の年間損失額は平均で総計数千億ドルに達する可能性がある
(写真: EtiAmmos/iStock by Getty Images)

サイバーリスクが金融システムにとって重大な脅威となりつつあり、IMF スタッフによるモデリングによると、サイバー攻撃によって金融機関が被る平均の年間損失額は数千億ドルに達すると算定されています。銀行の利益がむしばまれ、また金融安定性が脅かされることになりかねません。

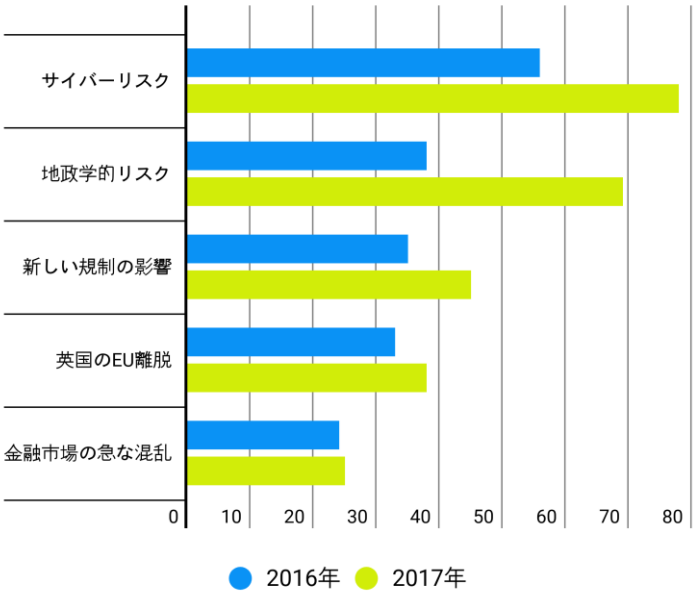
最近、サイバー攻撃が現実の脅威となったことを突きつける事例が相次いでいます。犯罪者が機密情報にアクセスするといったデータ漏えいや、仮想通貨取引所のコインチェックで 5 億ドル相当の流出が生じるなどの詐欺事件が既に起きており、標的にされた金融機関は運営不可能な状態に陥る脅威にさらされます。

これまで様々な調査を通じて、金融機関のリスク担当者や役職者が、サイバー攻撃を最大の懸念事項に挙げていることが一貫して示されてきましたが、これは驚くことではありません。例えば、下のグラフを見てみましょう。

様々な調査では、サイバー攻撃が最大のリスクとして挙げられている

リスク担当者など、金融機関の役員はサイバー攻撃の脅威が増しており、地政学的事象や新しい規制よりもサイバー攻撃がもたらすリスクの方が大きいと見ている。

(回答者に占める割合。単位は%)



出典: Depository Trust & Clearing Corp.による調査。
DTCC Systemic Risk Barometer 2017Q1として発表されている。

国際通貨基金

金融セクターの脆弱性

金融セクターは特にサイバー攻撃にさらされやすい状況にあります。資金の仲介という重要な役割があることから、金融機関は格好の標的なのです。ひとつの金融機関に対して攻撃が成功すると、高度に相互接続した金融システムを通じて瞬く間に被害が拡散してしまう恐れがあるのに、サイバー攻撃に対する耐性が低い可能性がある旧式のシステムを金融機関の多くが使い続けています。またサイバー攻撃が成功すると、

金銭的損失という重大で直接的な被害だけでなく、評判の失墜など間接的な被害も引き起こしかねません。

最近注目を集めた事例によって、サイバーリスクは国際機関をはじめとした公的セクターの検討課題として重視されるようになりました。とはいえ、サイバーリスクの定量分析はいまだ初期段階にとどまっています。特に、サイバー攻撃による損失に関するデータが不足していることと、サイバーリスクのモデリングが困難であることがネックとなっています。

最近の IMF の調査では、サイバー攻撃によって被る潜在的損失について考察するための枠組みを主に金融機関向けに提供しています。

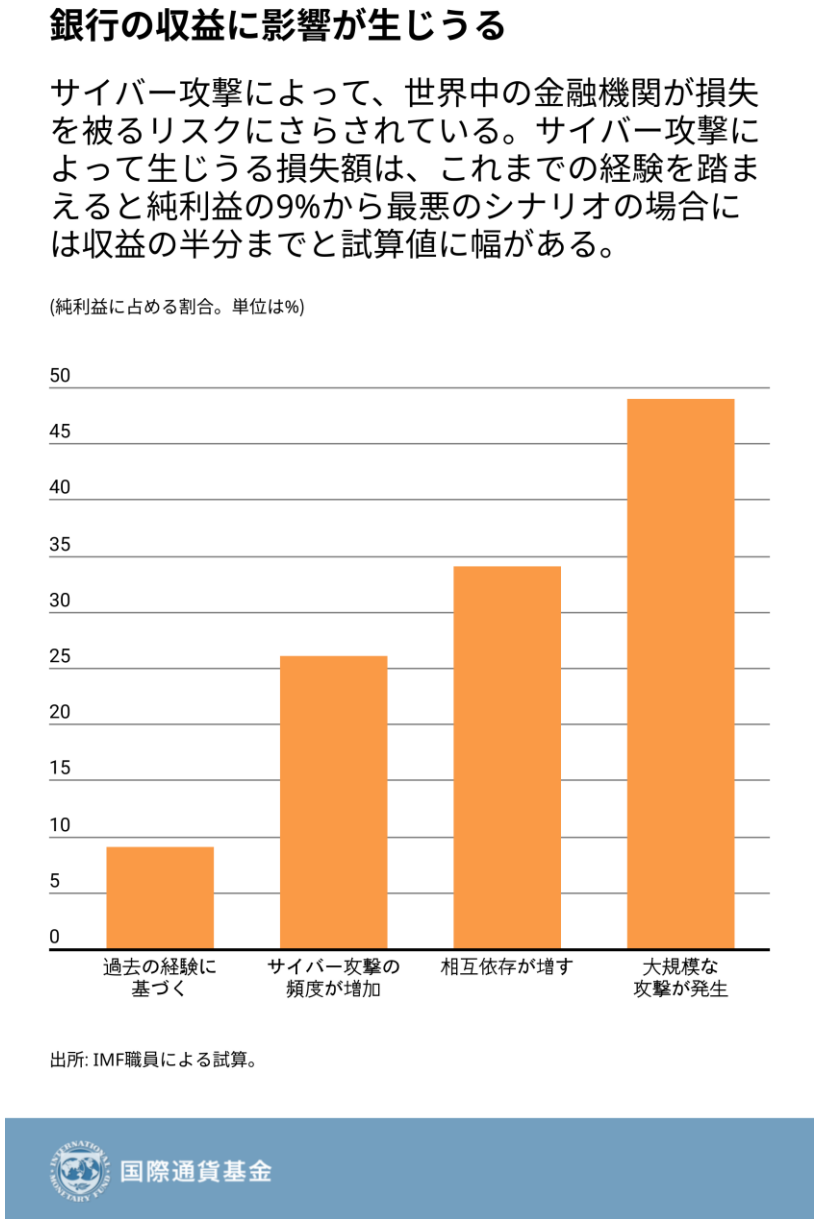
潜在的損失の算定

モデリングの枠組みでは、保険数理学の手法とオペレーショナルリスク測定の手法を活用して、サイバー攻撃による損失総額を試算しています。これには金融機関へのサイバー攻撃の頻度を推定し、また攻撃による損失の広がりを把握することが必要です。それを土台にして、サイバー攻撃による損失全体の広がりを算定する数値解析が可能になります。

IMF では、ここ最近の 50 か国におけるサイバー攻撃による損失を網羅した一連のデータを利用して、枠組みを説明しています。どのように金融機関の潜在的損失を算定するかの一例を示すものです。これ自体、困難な作業ですが、サイバーリスクに関して大きなデータギャップがあることからさらに難易度が増しています。また、金融システムに対して大規模なサイバー攻撃が成功した事例は、ありがたいことに、これまでのところありません。

この点からも、今回の私たちの検証結果はあくまで理解を助けるものとして捉えるべきでしょう。額面上では、サイバー攻撃による年平均の潜在的損失額が銀行の純利益全体の 9%近く、約 1,000 億ドルと相当な額に上る可能性が示唆されています。もっと厳しいシナリオでは、過去の実績と比較して攻撃の頻度は倍、拡散リスクも高いサイバー攻撃を想定しています。この場合、損失額は先のシナリオの 2.5 から 3.5 倍の 2,700 億ドルから 3,500 億ドルに達する可能性があります。

この枠組みは、大規模攻撃を受けた場合の最悪のリスクシナリオの検証にも活用できるでしょう。今回 IMF が収集したデータ分布を見ると、そのようなシナリオでは、下から 5%の最悪のケースにおいては、平均の潜在的損失額は銀行の純利益の半分にまで達する可能性が示され、そうなると金融セクター自体が危険にさらされることになります。



今回算定された潜在的損失額は、現在のサイバー保険市場の規模とは桁違いです。最近成長しつつあるとはいえ、サイバーリスクに対する保険市場の規模はまだ小さいままで、2017 年の全世界の保険料総計でも 30 億ドル程度に過ぎません。金融機関の多くはサイバー保険をかけてさえいないのが現状です。保険適用範囲は限定的ですし、保険会社にとっては、サイバー・エクスポージャーの不確実性、データの不足、悪影響拡散の可能性などが相まって、リスク評価を難しいものにしています。

今後に向けて

リスク評価には改善の余地が大いにあります。サイバー攻撃の頻度と影響度に関して、政府がより詳細で一貫性があり、完全なデータを収集できれば、金融セクターのリスク評価の一助となるでしょう。欧州連合の一般データ保護規則（GDPR）下で検討されているように、侵害発生時の報告義務はサイバー攻撃に対する知見を改善することになるでしょう。シナリオ分析を活用することで、サイバー攻撃がどのように拡散し得るかについて包括的な評価方法を開発し、適切な対応策を官民両面で設計するのにも役立つでしょう。

また、金融機関とインフラの耐性をどう強化していくべきか理解するためのさらなる取り組みも必要です。このような取り組みはサイバー攻撃の成功確率を下げるだけでなく、スムーズで迅速な復旧を促すためには欠かせません。また世界中の公的セクターにおいても、ここまで述べてきたリスクを監視・制御する能力を向上させる必要があります。

すなわち、サイバーリスクに対する規制・監督の枠組みを強化することが求められており、効果的な監督手法、現実に即した脆弱性評価と復旧テスト、緊急時対応計画に力が注がれるべきです。IMF は加盟国による規制や監督の枠組み強化を助けるために技術支援を行っています。

*****

クリスティーヌ・ラガルドは、国際通貨基金専務理事。1 期目の 5 年間を終了し、2016 年 7 月に 2 期目に再任命。フランス国籍。2007 年 6 月から 2011 年 7 月まで同国の財務相。また、それ以前に 2 年間、対外貿易担当相も務めた。

反トラスト法、労働法弁護士として多方面で活躍。ベーカー&マッケンジー国際法律事務所のパートナーとして活躍し、1999 年 10 月には同事務所のチェアマンに就任。2005 年 6 月にフランスで初の入閣を果たす。ラガルド氏は、政治学院と第 10 大学ロースクールで学位を取得。パリ第 10 大学ではベーカー&マッケンジー事務所勤務前の 1981 年に講義を行った経験も有する。

より詳細な経歴はこちらでご確認ください。

関連リンク:

サイバー攻撃への防御はグローバルであるべき