世界に広がるサイバー攻撃の脅威

増大するサイバー攻撃の脅威から金融システムを守るためには、国際社会の協調が不可欠だ。

ティム・マウラー　アーサー・ネルソン

2016年2月、ハッカーがバングラデシュ中央銀行を標的とし、国際金融システムの主要電子決済通信システムであるSWIFTの脆弱性につけこんで、10億ドルを盗み取ろうとした。不正取引の大半は阻止されたものの、それでもなお1億100万ドルが紛失した。この強奪事件は、金融界に警鐘を鳴らすものとなった。金融システム全体に及ぶサイバーリスクが大幅に過小評価されてきたことを知らしめたのである。

現在では、重大なサイバー攻撃が金融安定性リスクをもたらすとの見立ては自明だ。サイバー攻撃は、発生するか否かという問題ではなく、いつ発生するかという問題なのだ。だが世界各国の政府や企業は、その脅威の封じ込めに苦心し続けている。金融システム保護の責任を誰が担うのか不明確なままだからである。懸念は高まっており、有識者は警戒を促している。国際通貨基金（IMF）前専務理事でもあるクリスティー

重大なサイバー攻撃が金融安定性リスクをもたらすとの見立ては自明だ。サイバー攻撃は、発生するか否かという問題ではなく、いつ発生するかという問題なのだ。

ヌ・ラガルド欧州中央銀行総裁は2020年2月、サイバー攻撃が深刻な金融危機の引き金になりかねないと警告している。2020年4月には金融安定理事会（FSB）が、「適切に阻止されなかった場合、重大なサイバーインシデントは重要金融インフラを含む金融システムに大混乱を招くおそれがあり、金融安定性により幅広い影響が出かねない」と注意喚起を行った。そのような事象が発生した場合の経済的コストは莫大なものとなり、一般市民の信頼も大きく損なわれる可能性がある。

現在進行中の2つの動向がこのリスクを深刻化させている。第1の動向は、国際金融システムが未曽有のデジタルトランスフォーメーションの只中にあり、新型コロナウイルスのパンデミックがそれを加速させていることだ。銀行はテクノロジー企業に対抗し、テクノロジー企業は銀行と張り合っている。その一方で、コロナ渦でオンライン金融サービスの需要は高まり、在宅勤務は定着してきた。世界各国の中央銀行はデジタル通貨や決済システム刷新を支援するか検討している。この変革の時代にあっては、単発のインシデントが簡単に信頼を毀損したり、こうしたイノベーションを頓挫させたりしかねないため、サイバーセキュリティは未だかつてなく重要になっている。

第2の動向は、悪意のある人物が現在のデジタルトランスフォーメーションを利用しており、彼らが国際金融システムや金融安定性、そして金融システムの健全性に対する信頼にもたらす脅威が増大していることだ。コロナ禍によってハッカーは新たな標的も得ることができた。国際決済銀行によれば、金融部門が経験している新型コロナウイルス関連のサイバー攻撃の割合は、医療部門に次いで2番目の大きさとなっている。

脅威の背後にいるのは誰か

今後は、より危険な攻撃とそれに続くショックが発生すると考えられる。最も心配されるのは、記録やアルゴリズムや取引などの金融データの健全性を破損させるインシデントだ。こうした攻撃は信頼をより幅広く傷つける可能性をはらむが、対抗措置として使える技術的ソリューションは現在のところ希少だ。そうした攻撃の背後にいる悪意の人物の中には、金融機関を標的にして2013年から2018年に10億ドル以上を盗み取った犯罪集団カーバナックのように大胆さを増している犯罪者だけでなく、国家や国家の支援を受けた攻撃者もいる（表参照）。例えば北朝鮮は、過去5年間に少なくとも38か国から約20億ドルを盗んでいる。

これは世界的な問題だ。高所得国におけるサイバー攻撃は大きく報道される傾向にあるが、低所得国や下位中所得国のより脆弱なターゲットに対する攻撃の増加はあまり注目されていない。しかし金融包摂の推進が最も顕著なのはそうした国々であり、飛躍的進歩によって多くの人々がモバイル決済システムのようなデジタル金融サービスを利用できるようになってきている。デジタル金融サービスは確かに金融包摂を促進させているが、その一方でハッカーに対しては格好の標的にあふれる環境を提供してもいるのだ。例えば2020年10月にウガンダ最大のモバイルマネーネットワークであるMTNとエアテルがハッキングされた際には、4日間にわたるサービス取引の大混乱が生じた。

責任の空白

国際金融システムのデジタルインフラ依存

サイバー攻撃の詳細

これらインシデントの背後には、大胆さを増している犯罪者だけでなく国家や国家の支援を受けた集団もおり、その目的や動機も多様だ。

攻撃者	動機	目的	事例
国家、国家の支援を受けた集団	地政学的 思想的	混乱 破壊 損害 窃盗 スパイ活動 金銭的利益	データの恒久的破損 特定対象の物理的損害 送電網障害 決済システム障害 不正送金 スパイ活動
サイバー犯罪者	利得の追求	窃盗 金銭的利益	現金窃盗 不正送金 認証情報窃盗
テロリスト集団、ハクティビスト、内部関係者	思想的動機 不満	混乱	情報漏洩 名誉棄損 分散型サービス拒否攻撃

出所: European Systemic Risk Board. 2020. "Systemic Cyber Risk." https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

アートワーク：iSTOCK / YOUR_PHOTO

この問題に特化した措置が講じられなければ、イノベーションや競争やパンデミックがデジタル革命を加速させる中で国際金融システムの脆弱性は増すばかりだろう。

度が高まっているにもかかわらず、システムをサイバー攻撃から守る責任の所在は明らかになっていない。その理由の一端は、非常に目まぐるしい環境の変化にある。この問題に特化した措置が講じられなければ、イノベーションや競争やパンデミックがデジタル革命を加速させる中で国際金融システムの脆弱性は増すばかりだろう。脅威をもたらす人物の多くは金銭目的だが、単に混乱や破壊を目的とする攻撃も増えている。さらに、盗み方を知った者は同時に金融システムのネットワークやオペレーションについても知ることになるため、将来的にはより深刻な混乱や破壊を招く攻撃を仕掛けたり、そうした知識や能力を他者に売ったりすることが可能になる。このようなリスク環境の急速な進化は、その他の点では成熟し統制のとれたシステムの対応力に大きな負担をかけている。

国際金融システムの保護強化は、主として組織的な課題だ。防御を固め規制を強化する努力は重要だが、増大するリスクに打ち勝つにはそれだけでは十分ではない。多くの部門とは異なり、金融サービス界の大半は技術的なソリューションを実装するためのリソースや能力に事欠いてはいない。主な課題は、協調行動の問題だ。各国の政府や金融当局や業界の垣根を越えてシステム保護を体系づけるにはどうするのが最善か、そしていかにしてそれらのリソースを効果的かつ効率的に活用するか、といった点である。

現在様々なステークホルダーや取り組みが断片化している一因は、サイバーリスクの独特さや、その進化する性質にある。種々のコミュニティが縦割りで動いており、それぞれに与えられた権限や任務を通じてこの問題に取り組んでいる。金融監督者は強靭性に、外交官は国家の行動規範に、国家安全保障当局は悪質行為の抑止に、業界幹部は業界特有のリスクよりも各企業特有のリスクに注力している。金融サービス企業とテクノロジー企業の境界がかつてないほど曖昧になる中で、セキュリティに対する責任の境界も同様にますます見えにくくなっている。

金融、国家安全保障、外交という異なる当事者間の断絶はとりわけ顕著だ。金融当局は、サイバー攻撃の脅威がもたらす独特のリスクに直面している。そのような脅威に効果的に立ち向かうためには国家安全保障当局の関与が必要だが、両者の関係は希薄なままだ。この責任の空白と、国際金融システムを保護する役割や権限が未だ不確かであることがリスクを助長している。この不確かさの一因は現在の地政学的情勢や強い不信にあり、これによって国際社会の協調が妨げられている。サイバーセキュリティに関する協力は阻まれ、断片化され、そして多くの場合は信頼し合う最小限の関係者間に限定されている。機密扱いの国家安全保障上の資本に触れるからである。複数のステークホルダーにまたがる国際的な協力は、「なくても支障はないがあると助かる」ものではなく「なくてはならない」ものだ。

国際的な戦略

サイバー攻撃の脅威から国際金融システムを効果的に守るために、カーネギー国際平和財団は2020年11月に「サイバー攻撃の脅威に対する国際金融システム保護強化のための国際戦略（International Strategy to Better Protect the Global Financial System against Cyber Threats）」と題した報告書を発表した。世界経済フォーラムと共同で作成されたこの報告書では、国際的にも、また政府機関や金融企業やテクノロジー企業の間でも、協調を促進して断片化を解消するための具体的なアクションを推奨している。

この戦略は4つの基本的考え方に基づいている。第1は、役割と責任の明確化が必要という考え方である。金融当局、法執行機関、外交官、その他の関連政府機関、業界の間で効果的な国内関係を構築できているのは、ごく少数の国だけだ。断片化している現在の状態は国際協力を妨げ、国際金融システムの集合体としての強靭性や回復力、対応能力を弱めている。

第2は、国際協調は必要火急という考え方だ。脅威の大きさと、世界中が相互に依存しているという国際金融システムの性質を考えれば、個々の政府、金融企業、テクノロジー企業は、単独行動をとっていたのでは効果的にサイバー攻撃の脅威から身を守ることができない。

第3は、断片化を解消すれば問題に取り組むキャパシティを確保できるという考え方である。金融機関の保護強化のために多くの取り組みが

進行中だが、それらの取り組みは依然として縦割りだ。その中には他と重複しているものもあり、取引コストの増加につながっている。こうした取り組みのいくつかは十分に成熟していて、共有したり、より良く連携させたり、さらに国際化したりすることが可能だ。

第4は、国際金融システムの保護は他の部門の手本になりえるという考え方である。金融システムは、地政学的緊張が高まっている時でさえも、各国が協力に明らかな共通利益を見い出せる数少ない分野のひとつだ。金融部門に注力することが出発点となって、将来的に他の部門の保護を強化するための道筋をつけられるかもしれない。

カーネギー報告書は、サイバーレジリエンス向上のためのアクションのひとつとして、金融機関におけるサイバーリスク管理を監督するための基本的枠組みをFSBが作ることを推奨している。各国政府や業界は、脅威に関する情報共有や、イスラエルのFinCERTの例に倣った金融コンピュータ緊急事態対応チーム（CERT）の設置によってセキュリティ強化を図る必要がある。

金融当局は、データやアルゴリズムを狙った攻撃に対する金融部門の強靭性向上も優先事項とすべきだ。これには、関係者が一夜のうちに安全に顧客口座データのバックアップをとることを可能にする安全な、暗号化を用いたデータ保管も含まなければならない。 サイバー攻撃を模擬した訓練を定期的に実施して脆弱な点を特定し、行動計画を作ることも必要だ。

国際規範の強化にあたっては、各国政府が国際法をサイバー空間にどのように適用していくのかを明確にし、金融システムの健全性を保護する規範を強化するようカーネギー報告書は推奨している。オーストラリア、オランダ、英国の政府は既に最初の一歩を踏み出しており、国外からのサイバー攻撃は違法な武力行使または他国に対する内政干渉とみなされる可能性があることを示す声明を出している。

サイバーレジリエンスや国際規範の強化によって、法執行措置や業界との多国間対応を通じた集団的対応を促進できる。対応には、制裁や逮捕や資産差し押さえを含めることが可能だ。

各国政府は、脅威の評価や対応の連携を支援する組織を設立してこうした取り組みを支えることができるだろう。情報収集は金融システムに対する脅威を重点のひとつとして行い、各国政府はそうした情報を同盟国や考えを同じくする国々と共有すべきである。

能力構築

カーネギー報告書で概説されている包括的戦略は、サイバーセキュリティ人材の育成や、金融部門のサイバーセキュリティ能力の増大や、デジタルトランスフォーメーションのおかげで進展した金融包摂の護持に依拠している。

コロナ禍による失業率の上昇は、有能な人材を訓練し雇用してサイバーセキュリティ人材の充実を図る重要な契機をもたらしている。金融サービス企業は、高校生向けプログラム、見習い制度、大学生向けプログラムなども含めた人材パイプライン構築の取り組みに投資すべきだ。

サイバーセキュリティ能力を構築することは、必要なところへの支援提供に注力することを意味する。IMFをはじめとする国際機関には、特に2016年のバングラデシュ事件以後、サイバーセキュリティに関する支援要請が加盟国から数多く寄せられている。G20諸国の政府や中央銀行は、IMFのような国際機関を取り組みの調整役に指定して国際的な仕組みを形成し、金融部門のサイバーセキュリティ能力を構築することができるだろう。経済協力開発機構（OECD）や国際的な金融機関は、サイバーセキュリティ能力の構築を開発支援の構成要素とし、支援を必要とする国々への支援を大幅に増やすべきである。

最後になるが、金融包摂の進展を維持していくには、金融包摂とサイバーセキュリティの結びつきを強化する必要がある。これはアフリカでは特に緊急の課題だ。アフリカ諸国の多くが金融包摂を拡大させデジタル金融サービスへと移行する中で、自国の金融部門の大きな変革を経験しているからである。アフリカにおけるサイバーセキュリティに重点的に取り組む専門家ネットワークを形成すべきだ。

政府も中央銀行も監督当局も業界もその他の関係ステークホルダーも巻き込んで、国際社会が一致団結してこの差し迫った重要課題に対処する時が来ている。上述したような考え抜かれた戦略は、言葉を実行に移す際の青写真を示すものである。FD

ティム・マウラーはカーネギー国際平和財団のサイバーポリシーイニシアティブのディレクターでテクノロジーと国際関係プログラムのシニアフェロー。**アーサー・ネルソン**はカーネギー国際平和財団のサイバーポリシーイニシアティブのリサーチアナリスト。