IMFBlog
INSIGHTS AND ANALYSIS ON ECONOMICS & FINANCE

サイバー攻撃への防御はグローバルであるべき

エマヌエル・コップ、リンカーン・カフェンバーガー、クリストファー・ウィルソン

2017 年 10 月 26 日

サイバーリスクには地理的な境界線がなく、世界全体が脅威にさらされている。そのため、国際機関の役割が重要となる
(solarseven/iStock by Getty Images)

金融機関を標的としたサイバー攻撃が増え、非常に高度化している。アメリカの個人情報機関 Equifax のシステムに不正侵入があったケースでは、1 億 4,300 万人分の信用情報の機密性が損なわれた。また、バングラデッシュ中央銀行は 8,100 万ドルの盗難にあった。こうした事例 2 つが注目を浴びたが、これら以外にも金融業界では最近システムへの不正侵入が発生してきている。

今日、金融機関は常にサイバーリスクに脅かされており、また、高度に相互接続した金融システムを正常に機能させる上でも、サイバー攻撃が恒常的な脅威となっている。銀行はその規模を問わず、毎日、サイバー攻撃を受けている。個々の企業を狙ったシステムへの不正侵入によって、他の金融機関や非金融機関を巻き込んだ負の連鎖反応が起こりかねず、金融システム全体を脅かすシステミックなリスクを発生させる可能性がある。これはサイバーリスクの新たな側面であり、その理解はあまり進んでいない。

IMF が最近発表したワーキングペーパーでは、情報共有の促進や、政策の調整や設計、紛争解決の支援、システミックなリスクの抑制を行う上で、国際決済銀行や金融安定理事会、IMF などの国際機関が大きな役割を果たせることが示されている。

洗練された攻撃

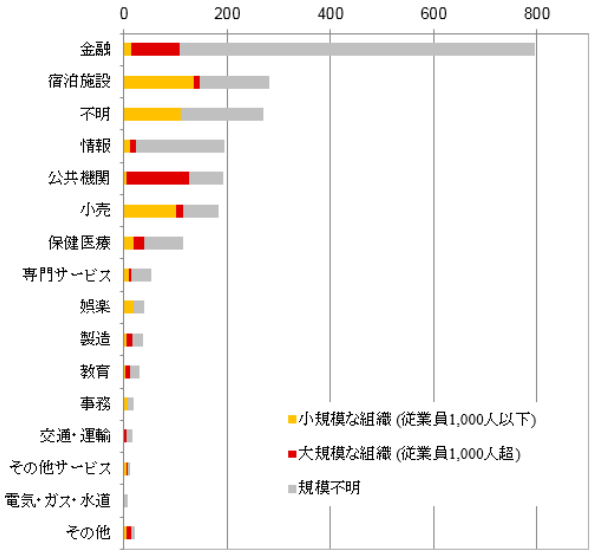
最も危険なサイバー攻撃の例としては、送金やATMを狙ったもの、銀行システムに入り込む悪質なソフトウェア、ファイルやハードウェアの破壊、内部のオペレーションを混乱させる恐喝行為が挙げられる。

しかし、現時点で存在する国内規制や業界自主規制の寄せ集めのもとでは、包括的なデータが欠けており、リスクが過小評価されている可能性が高い。

企業もまた、不確実性を助長している。というのも、企業は評判が損なわれたり、取引を失ったりすることを恐れて、サイバー事象が生じても情報公開を行わないことが多いからだ。多くの場合、システムへの不正侵入に関する情報は、数ヵ月後になって、場合によっては、数年後になってから初めて公開されている。

サイバー攻撃の標的となる金融業界
他の産業よりも多くの攻撃を金融業界は受けている。

(システムに不正侵入が発生した件数。業界別に見た2015年の数字)



[出所] Verizon。また、IMF職員による試算。

セキュリティの限界

このように広範にわたり、複雑性も高い脅威をどのように管理すれば良いのだろうか。ファイアウォールやデータ暗号化、研修や事業継続計画などのセキュリティ対策は必要であるものの高額になることもあり、通常の事業運営を困難にしてしまうこともありうる。プロダクトやプロセスの再設計によって、リスク回避を強化できる可能性もあるが、新しい手順によって脆弱性が新たに生み出されることもある。

企業は保険会社や外部のサイバーセキュリティ業者といった第三者にリスクを移転させることもできる。しかし、こうした主体間に存在する情報の非対称性や情報不足、そして一般的には、この手の経済リスクに対する経験が不足しているといった理由で、民間部門によって金融システム内のサイバーリスクが軽減される可能性が制限されてしまっている。企業はどの程度のリスクにさらされているかを過小評価しがちで、また、リスクから自分の身を守る能力やサイバー保険の対象範囲を過大に見積もりすぎる傾向にある。保険対象になるその他のリスクと比較して、サイバーリスクに対する理解は進んでおらず、結果として、保険会社は不確実性を考慮して、保険料を高めに設定している。

システミックなリスク

こうした第三者機関もハッカーの標的になる可能性がある。そして、もしサイバーセキュリティ業者や保険会社が数社しか市場に存在せず、少数の企業に集中してしまった場合、このこと自体が金融システム全体に対するシステミックなリスクの源泉となってしまう。

また、金融システム内で情報技術が集中することによっても、システミックなリスクが発生しうる。金融機関は共通のオペレーティング・システムやプログラム、クラウドサーバー、電子ネットワークのハブを使用している。銀行間取引市場や送金市場を介した接続によって、ショックはすぐに金融システム全体に拡大してしま

う。サイバー保険は人気があるため、その市場は急成長しているが、保険業界でサイバーリスクが蓄積し続けること自体がシステミックなリスクになりかねない。

サイバー攻撃によるダメージに伴ってシステミックなリスクが発生しないよう、公的部門が果たすべき役割は明確になっている。

規制の役割

各国の政府当局は、サイバー攻撃が速やかに、かつ正確に報告されるように、また、損失のデータを体系的に収集できるように、動機付けを行うべきだ。サイバー攻撃は本質的に犯罪行為であるため、銀行業の規制当局は警察など法執行機関と迅速に調整を行えるようにすべきである。そして、サイバー攻撃の脅威が変化するのに合わせて、規制当局が速やかに対応策を適宜変更できる能力と権限を持つことは不可欠である。

サイバーリスクに地理的な境界線は存在せず、脅威は世界的なものである。従って、国際機関が果たす役割が重要となる。システミックなサイバーリスクに対して協調的な対策をとることを各国政府が考慮すべき時が来ている。金融安定理事会など国際組織や G7 のような国際的な会議体がメンバーに情報を広め、国家間での政策調整を行えるように、取り組みを率先している。こうした制度や会議体は、システミックなサイバーリスクが情報面で、また、国際的な調整の面で突きつけている課題いくつかへの対策を支援する上で相応しい立場にあるように思える。

*****

エマヌエル・コップは北米課のシニアエコノミスト。アメリカ経済を担当。以前には、IMF の金融資本市場局で勤務し、ドイツやイタリア、デンマーク、コロンビアなど様々な金融部門評価プログラムを実行した。また、ポルトガルの経済調整プログラムも担当した。調査の関心分野は、マクロ金融リスク、金融の安定性と規制、投資やマクロ経済予測である。オーストリアのウィーン経済大学で金融修士号と経済学博士号を取得している。

クリストファー・ウィルソンは金融資本市場局のシニアファイナンシャルセクターエキスパート。銀行業の監督と規制の全般を専門分野にしており、特に、バーゼル III 流動性基準に関心を持ち、このテーマに関する技術支援ミッションのリーダーを務めた。IMF での勤務前には、オーストラリア健全性規制庁とイギリスの金融サービス機構に勤め、大手銀行と地方銀行の監督など銀行業の監督と規制を担当した。直近では、バーゼル III の国内導入に取り組んでいる。マッコーリー大学の経済学士号と政治・公共政策修士号を取得し、また、FINSIA から応用金融学の準修士号を得ている。

リンカーン・カフェンバーガーは IMF で情報セキュリティの専門家として勤務している。10 年にわたり、組織が直面する脅威を理解し、情報やリスクに基づく決断を行えるように支援してきた。