サイバーリスクと金融規制

淵田　康之

▌要　約▐

1. 今日の金融市場においては、金融機関の破綻リスクよりも、サイバーアタックがもたらすリスクに対する懸念の方が高まっている。
2. グローバル金融危機から 10 余年を経て、金融機関の自己資本や流動性など、財務面を中心に厳格な健全性を求める規制が整備されてきた。一方、金融サービスにおいて IT の活用がより重要となるなかで、サイバーリスクに対する金融機関や金融当局の対応がますます問われるようになっている。
3. 多くの国では、官民が協力し、サイバーインシデントに関する情報共有・分析、演習の実施などの対応は強化しつつある。米国では、重要なデータが毀損しても、別途、保管したデータにより業務を迅速に再開可能とするシェルター ド・ハーバーという仕組みを、銀行界、証券界、資産運用業界が共同で構築した。サイバーセキュリティ保険市場も、米国を中心に成長を遂げている。G7 や G20 の金融当局者のレベルでも、サイバーセキュリティへの取組みが強化されつつある。
4. 国際電気通信連合が発表する Global Cybersecurity Index において、わが国は 2014 年時点では 5 位にランクされていたが、2018 年には 14 位となった。諸外国におけるサイバーセキュリティ政策が、わが国を上回るスピードで進化していることが、この背景にある。
5. わが国の金融分野では、サイバーアタックの結果、暗号資産取引所における顧客資産の流出事件やスマホ決済サービスの不正利用事件が、相次いで生じている。資金決済分野のサイバーセキュリティは、システミックリスク防止という観点から、優先度は高い。異業種による決済ビジネス進出も活発化するなかで、現状では、銀行、資金移動業者、前払式支払手段発行者、カード会社、といった業界ごとに縦割りの政策対応が目立つ点など、改善が求められよう。

Ⅰ 一段と重要となるサイバーリスクへの対応

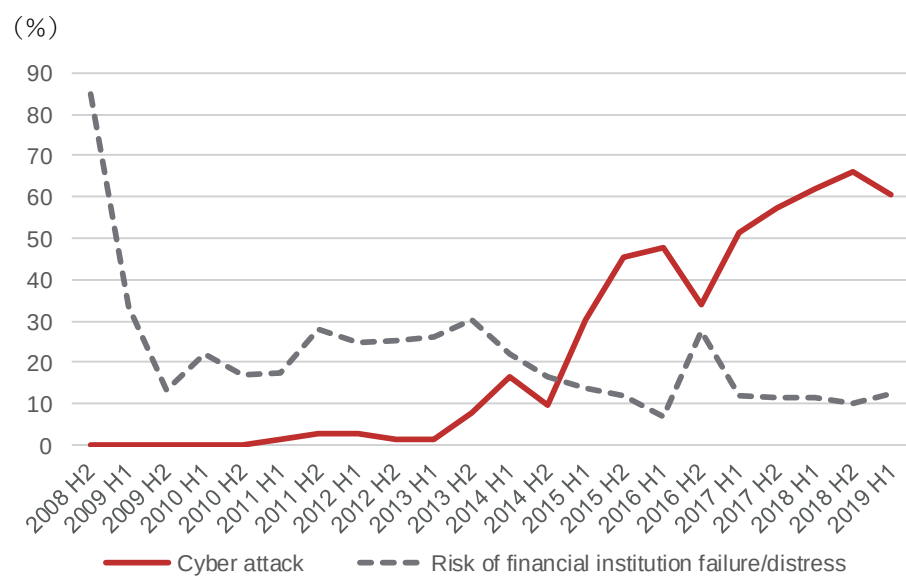
1．様変わりしたリスクの所在

金融市場において、警戒すべきリスクは何か。ひと昔前であれば、金融機関の破綻リスクであったかもしれないが、今日、サイバーアタックの方が、より警戒すべきリスクと認識されているようである。イングランド銀行が半年に 1 回公表しているシステミックリスクサーベイにおいても、英国金融システムにおける主要なリスクとして、サイバーアタックをあげる回答が、過去 5 年ほど上昇傾向にあり、金融機関の破綻リスクへの懸念を大きく上回る状況が生じているのである[1]（図表 1）。

同サーベイがスタートしたのは、グローバル金融危機が本格化しつつあった 2008 年 7 月であるが、当時は金融機関の破綻懸念一色であり、サイバーアタックを懸念する声はゼロであった。今日、金融市場におけるリスクの所在が様変わりしたのである。

同サーベイで、最近、リスクの源泉としてトップに挙げられているのは、Brexit 問題もあり「英国の政治的リスク」となっているが、サイバーアタックがこれに次ぐ位置づけとなっている。金融機関の破綻リスクを、トップに挙げた者はいない。

図表 1　英国金融システムにおける主要なリスク



（注）　市場関係者に対するサーベイ結果
（出所）Bank of England, “Systemic Risk Survey Results,” July 2019

[1] Bank of England, “Systemic Risk Survey Results”（最新は 2019 年 7 月 11 日に発表された 2019 年前半分）参照。市場関係者（2019 年上半期の場合、回答者 81 名）に対し「実現すると英国の金融システムに大きなインパクトを与えると思われるリスクを 5 つ指摘して下さい」という質問を行った結果（%）。

米国でも FRB のパウエル議長が、サイバーリスクへの対応を最重視する発言を繰り返している。就任前の議会公聴会においてもパウエル氏は、サイバーリスクが「米国の金融機関、米国経済、米国政府機関が直面する single most important risk かもしれない」と述べていた[2]。

また 2017 年 12 月、Office of Financial Research（OFR、財務省金融調査局）[3]の議会に対する年次報告書においても、米国の金融システムに対する 3 つの主要な脅威の一つとして、「サイバーセキュリティ事故に対する脆弱性」が挙げられている[4]。

OFR は従来、主として大手金融機関や大手ノンバンクの財務状況やポジション動向をウォッチすることにより、システミックリスクを警戒してきた。しかしサイバーアタックにより、2014 年 9 月に JP モルガン・チェースにおいて 7600 万世帯の顧客情報（住所、氏名、電話番号、メールアドレスなど）が流出、さらに 2017 年 9 月には、消費者信用情報会社である Equifax において 1 億 4,790 万人の個人情報（社会保障番号や運転免許証情報が含まれる）が流出する事件が生じた。こうした大規模なサイバーセキュリティ上の問題が相次いだことに対し、OFR としても、システミックリスクの観点から警鐘を鳴らす必要が生じたわけである。

2014 年の情報流出事件以後、JP モルガン・チェースは、ダイモン CEO が、毎年の株主へのレターなどにおいて、サイバーセキュリティ問題への取組みを繰り返し強調している。2019 年の株主のレターの中でも、「サイバーセキュリティ問題は、米国の金融システムにとって最大の脅威かもしれない」と述べている。

こうしたなか 2019 年 7 月には、米銀大手のキャピタル・ワンが、外部からの不正アクセスによりクレジットカード利用者など 1 億 600 万人分の個人情報が漏洩した可能性があると発表した。

今日、金融サービスはますますコンピュータ・ネットワークに依存する形で提供されるようになっているが、金融システムは、サイバーアタックの脅威に曝され続けており、決め手となる対策も見出だせていない状況にある。

２．サイバーアタックのリスクとは

イングランド銀行のサーベイや OFR 報告書は、サイバーアタックがもたらすリスクとして、システミックリスク、すなわち金融市場全体に深刻な影響が及ぶリスクに焦点を当てている。

---

[2] 2017 年 11 月 28 日の米議会上院公聴会における発言。

[3] OFR は、グローバル金融危機後、金融システムのリスクの計測や分析、各種調査を行う機関として、ドッド・フランク法によって財務省内に設置された機関。ドッド・フランク法は、米国金融におけるシステミックリスクを監視し、必要な対処をする機関として Financial Stability Oversight Council（FSOC、金融安定監督評議会）を設置したが、OFR は、FSOC の事務局機能を担っている。

[4] 他の二つは、「システム上重要な金融機関の破綻処理の障害」、「市場及び業界の構造的な変化」である。後者は、財務省証券の決済が特定の金融機関に依存する傾向が強まっていること、多数の証券市場が併存する結果、流動性の低下が懸念されること、及び LIBOR の代替指標への移行が円滑に進まない可能性があることを指している。

伝統的なシステミックリスクとは、金融恐慌時などにおいて、人々が疑心暗鬼となる結果、健全な金融機関に対しても、預金取り付け騒ぎが生じ、金融機能がマヒするような事態を指す。大規模なサイバーアタックにより預金口座の残高が奪われるような事態が頻発するようなことがあれば、人々は金融恐慌時同様の疑心暗鬼に陥る可能性がある。どの金融機関であれば大丈夫か、一般利用者は確信が持てなくなり、とりあえず資金を引き出そう、取引は控えよう、という行動が一気に拡大する恐れがある。

またサイバーアタックにより、意図した決済が実行されない場合、あるいは口座に保有していたはずの資金が流出してしまうような事態が生ずる場合、直接の損害に留まらず、当該決済や資金を前提として行われようとしていた他の経済取引が実行できなくなるなど、影響が連鎖的に拡大しかねず、問題はまさにシステミックなものとなる。

OFR の報告書も、サイバーセキュリティ問題は、金融機関への信頼を喪失させること、顧客の金融取引データの正確性を損なうこと、代替が容易にきかない重要な金融サービスが被害を受けることなどを通じて、金融の安定性にリスクをもたらすと指摘している。

このように、システミックリスクという深刻な形態にまでは至らなくとも、サイバーリスクは個々の利用者の財産や取引へのリスクがある他、利用者の個人情報や顧客企業の機密情報の漏洩リスク、さらに奪われた資金がマネーロンダリングにより犯罪組織に流れたり、テロリズム・ファイナンスに充てられたりするリスクがある。以下に示すように、これらのリスクは金融機関に対する経営リスクにもつながる。

３．金融機関経営への影響

米国における Equifax の情報漏洩の場合、会長兼 CEO が引責辞任を迫られた他、2019 年 7 月における連邦取引委員会、消費者金融保護局、州政府との和解では、最大 4 億 2,500 万ドルを消費者への補償に充てること、州に 1 億 7,500 万ドル、消費者金融保護局に 1 億ドルを支払うこと、12 億 5,000 万ドルをかけデータ保護強化プログラムを推進することとされた。

2019 年 7 月に発覚したキャピタル・ワンの情報漏洩事件の場合、流出した情報の悪用による被害はまだ報告されておらず、集団訴訟や当局による制裁の行方などは現時点では不明である。ただし同行の発表によれば、2019 年中に、顧客への通知費用、顧客のクレジット情報や ID を用いた不正が行われていないかの無料モニタリングなど顧客保護の費用、テクノロジー関連費用、法務関連費用など、1 億ドルから 1.5 億ドルの費用が発生する見込みとされる。同行はサイバーセキュリティ保険に加入しており、最大 4 億ドルまでカバーされているという。

このようなことから、金融機関におけるサイバーセキュリティ関連の支出も拡大している。2014 年に大規模な情報流出事件を起こした JP モルガン・チェースにおいては、2015 年にサイバーセキュリティ関連予算を倍増させ、年間 5 億ドルとした。2019 年の株主へのレターによれば、この金額は 6 億ドル近くとされ、サイバーセキュリティ分野には、

3,000 人以上の従業員が携わっているという。

欧州においては、GDPR（General Data Protection Regulation、一般データ保護規則）の導入にみられるように、個人情報保護政策が強化されており、サイバーアタックにより情報漏洩が生じた場合の制裁金も、無視できない規模となりうる。金融機関の例ではないが、英国の ICO （Information Commissioner's Office、情報コミッショナー事務局）[5]は、2019 年 7 月 8 日、British Airways とその親会社に対し、50 万人の顧客の情報が流出した問題で、GDPR 違反があったとして 1 億 8,339 万ポンドの罰金を科すことを発表した。この金額は、同社の 2018 年における世界売上の 1.5%に相当するとされる[6]。

Ⅱ　サイバーリスク時代の金融業者の適格性

１．健全性とサイバーセキュリティ

金融規制においては、伝統的に金融業者の資本力など財務基盤が重視されてきた。特に銀行は、決済サービスを担うことから、ある銀行の破綻が他の銀行、及びこれら銀行に口座を持つ企業などの破綻につながりかねず、経済全体の混乱、すなわちシステミックリスクにつながりかねないからである。

2007～8 年のグローバル金融危機以降、今日に至るまで、資本規制をはじめとする健全性規制は格段に強化されてきた。この間、銀行のみならず、システム上重要なノンバンクに対しても規制が強化されたこと、また金融機関をいかに破綻させないかではなく、破綻してもその影響を限定的なものとする点が重視されるようになったことなど、重要な規制アプローチの変化もあった。しかし、金融サービス事業者の破綻リスクを、システミックリスク防止の観点から、最重視するという点では、従来の延長線上にあるといって良いであろう。

しかし上記のように、金融市場関係者が、システミックリスクの源泉として金融機関の破綻よりも、サイバーアタックを重視するようになっている点、そしてサイバーアタックがもたらす金融機関への影響が、過去に比べて格段に大きなものとなっていることを踏まえると、金融規制のプライオリティも見直す必要が生じていると言えるかもしれない。

もちろん、サイバーアタックのリスクに対しても、個々の金融機関に対する健全性規制はある程度は有効である。例えば財務基盤が十分であれば、被害者への補償金や巨額の制裁金などの負担にも耐えられよう。しかし、いくら自己資本や流動性が充実していようと、サイバーアタックを防御する能力や、被害から回復する能力が優れていることを意味しない。個々の金融機関は破綻せず、また事後的に個別の損失を補償するリソースがあろうと、サイバーアタックにより決済が途絶するような事態が生じれば、経済全体に与える影響は、

[5] 英国の個人情報保護機関。独立公益法人。

[6] GDPR 違反企業に課される制裁金額は、悪質な違反の場合、2,000 万ユーロまたは前年のグローバルな売上高の 4%のいずれか大きい金額が上限とされている。

金融機関の連鎖的倒産が生じた場合と同様、甚大なものとなりうるのである。

このようなことから、今日、金融機関には一定水準以上の健全性が求められるのと同様、一定水準以上のサイバーセキュリティ能力が求められる時代となっていると言えよう。もちろん既に、各国の金融当局は、こうした認識の下、サイバーセキュリティに対する対応強化を金融機関に求めているが、いくつかの課題も指摘されている。

２．異業種の参加

イングランド銀行が 2019 年 6 月に発表した Future of Finance という報告書は、英国の金融システムの将来を展望し、イングランド銀行にとっての課題を整理したものであるが、課題の一つとして金融分野のサイバーセキュリティ問題への対応が論じられている[7]。

金融システムの中でも、特に決済分野において、サービス提供事業者の多様化が進展していることへの対応が急務とされている。従来であれば、厳格な監視下にあった銀行によって提供されていたサービスが、FinTech の台頭にみられるように、異業種によって担われる部分が拡大しているからである。

異業種の関与の形態としては、異業種が銀行の機能を代替するケースの他に、オープン API 化もあり、銀行とユーザーの間に異業種が関与する形でサービスが提供されるケースも増加している。この場合、決済が完了するまでのプロセス（ペイメント・チェーン）が長くなり、関与する業者も増加し、全体が複雑化する状況が生じている。

これら異業種は、国によって扱いは異なるが、サイバーセキュリティの分野に限らず、利用者保護の枠組みなども含め、必ずしも銀行と同様の規制・監督を受けていない場合も多い。この結果、ペイメント・チェーンが長く、複雑になっていることとも相まって、サイバーアタックへの脆弱性が増大している可能性がある。

３．金融機関の IT 能力

上記は、銀行のような厳格な規制・監督下にない異業種の台頭が、サイバーセキュリティ上の問題の源泉となりうるという観点からの懸念であるが、逆に銀行など伝統的な金融機関のサイバーセキュリティ能力が、異業種に比べて相対的に低下している恐れも指摘される。

まず FinTech の台頭に対し、レガシーシステムを抱えながら、店舗に依存した伝統的なサービス提供を続ける金融機関が、競争的に劣後しかねないという問題がある。金融サービスに求められるテクノロジーは急速に変化している。伝統的な金融機関においては、収益性が低下する結果、レガシーシステムの見直しはもちろん、サイバーセキュリティ強化のためにリソースを十分投入できなくなる懸念に直面している。

特に銀行に関しては、預貸利ザヤを重要な収益源としてきたが、低金利の継続によりこ

[7] Bank of England, “Future of Finance,” June 2019.

れが縮小し、一方、グローバル金融危機後の規制強化もあり、規制遵守コストが上昇するという問題にも直面している。これに対して、預金口座を提供しない FinTech は、より緩い規制環境下にあり、様々な事業を通じて収益を追求できる。

IT 企業のなかでも、大手のクラウドサービス提供業者は、セキュリティ分野のテクノロジーをリードする地位にあり、分散されたストレッジ施設や多重化されたバックアップ体制、DDoS（distributed denial-of-service）攻撃[8]などのサイバー攻撃に対する先端的な防御ツール、ネットワーク全体で漏れの無いよう、ソフトウェアを自動的にアップデイトする体制などを備えている。最もリソースを有する大手金融機関においても、これらクラウドサービス提供業者に匹敵するほどのサイバーデフェンス投資を実行できていないとの指摘もある[9]。

４．金融機関のクラウド活用

サイバーデフェンスへの投資という点で、クラウドサービス提供業者が大手金融機関を上回るとすれば、金融機関が個別にサイバーセキュリティ対応をするよりも、クラウドサービス提供業者と契約し、データ管理やシステム運営をクラウドに移管するというのが、一つの解となる可能性がある。

金融機関にとってクラウドサービスの採用は、FinTech との競争や協調という点でも不可欠との指摘もある[10]。顧客により良いエクスペリエンスを提供する上では、レガシーシステムへの依存を続けるのではなく、クラウドを活用することにより、先端的なサービスを迅速に導入することを検討すべきというわけである。

ただしクラウドサービスの利用が万能薬ではないことは、キャピタル・ワンの事件からも明らかである。今回、ハッカーの被害にあったのは、キャピタル・ワンがクラウド上に保管していた顧客データであった。キャピタル・ワンは、2014 年よりアマゾンのクラウドサービスを採用しており、大手米銀の中で最も早くクラウド化に踏み切った銀行の一つであった。同行は 2020 年までに、自行のデータセンターの運営を停止し、完全にクラウドに移行することを宣言している。

今回の情報漏洩の原因は、クラウドサービスそのものではなく、クラウドにアクセスするためのキャピタル・ワン側のウェブ・アプリケーションにおけるファイアーウォールの設定ミスにあったとされる。またクラウドを利用していたからこそ、情報漏洩への対処を迅速に行うことができたとされる。しかし当然のことながら、クラウドサービスは安全か

[8] ネットに接続された多数の端末や機器を活用し DOS 攻撃、すなわちウェブサービスを使用不能とする攻撃を行うもの。

[9] Bank of England (2019).

[10] Brad Carr, Daniel Pujazon and Jaime Vazquez, “Cloud Computing in the Financial Sector, Part I,” Institute of International Finance, August 2018.

という議論が生じている[11]。いずれにしても、外部のクラウドサービスを活用する場合でも、金融機関自体に一定レベル以上の IT に関する知見が備わっている必要があることは間違いない。

Ⅲ サイバーセキュリティ強化への取組み

１．情報共有・分析、演習の実施

サイバーセキュリティの強化に向けて、既に個々の金融機関による自主的な取組み、金融業界としての取組み、そして当局による取組みが展開されてきたところである。このうち、金融業界としての取組みとしては、米国に起源をもつ FS-ISAC（Financial Services Information Sharing and Analysis Center）がある。

ISAC は、クリントン政権時代、主要産業分野において、インフラへの物理的攻撃及びサイバーアタックに対抗する目的で、設立することが推奨されたものである[12]。重要なインフラの大半が民間部門によって所有・運営されていることから、政府と民間部門で情報共有を行い、協力して対処することが必要とされたのである。

ISAC は民間組織であるが、連邦政府のコンサルテーションと支援の下で、そのデザインや機能が決定された[13]。一つのモデルとされたのが、感染症対策における世界の中心的機関となっている米国疾病予防管理センター（Centers for Disease Control and Prevention）である。

1999 年、ISAC の第一号として設立されたのが、金融分野の ISAC（FS-ISAC）である。その後、米国のみならず諸外国の金融機関も参加し、今日では 50 ヵ国以上、7,000 の金融機関が会員となっている[14]。本部は米国のバージニア州に置かれているが、2017 年には、英国とシンガポールにも、拠点が開設されている。

サイバーアタックに対する演習も、各国で実施されている。個々の金融機関レベルでも、ペネトレーションテスト[15]の実施は一般的になっているが、当局も関与する形で銀行界、さらには銀行以外の業界や金融インフラも含めた演習も行われるようになっている。

---

[11] Robert McMillan, “Capital One breach casts shadow over cloud security,” *Wall Street Journal*, July 30, 2019、及び Hannah Murphy and Shannon Bond, “Capital One data breach sparks cloud security fears,” *Financial Times*, July 30, 2019 参照。

[12] 1993 年の世界貿易センタービル駐車場爆破事件や、1995 年のオクラホマシティ連邦ビル爆破テロ事件を背景に、テロ攻撃に対する米国の脆弱性が問題視されたことから、1996 年の大統領命令（“Executive Order EO 13010, Critical Infrastructure Protection,” The White House, July 15, 1996）によって「重要インフラに関する大統領委員会（President’s Commission on Critical Infrastructure、PCCIP）」が設置された。PCCIP の提言によって設立された組織の一つが ISAC（Information Sharing and Analysis Center）である。1998 年の大統領決定指令 63（“Presidential Decision Directive/NSC-63,” The White House, May 22, 1998）により、PCCIP の全ての勧告の発動が命じられた。

[13] ISAC は、当初、サイバー上の脅威への対応を目的としていたが、同時多発テロ事件を受けて、2003 年、Homeland Security Presidential Decision Directive 7 において、物理的脅威への対応を含むものとされた。

[14] FS-ISAC のホームページより。

[15] システムへの侵入を試みることで、システムに脆弱性がないかどうかテストする手法。

演習を行うことにより、新たな脆弱性が認識され、対応策を講じることが可能となる。米国では、2015 年に米国財務省が主導し、官民のサイバーセキュリティ・シミュレーション、「ハミルトン・シリーズ」が行われたが、これを契機にシェルタード・ハーバー（Sheltered Harbor）という新たな仕組みが構築された。

２．シェルタード・ハーバー

シェルタード・ハーバーは、サイバー攻撃により、バックアップ・システムも含めた障害が生じ、重要なデータが失われる、あるいは利用不能となるような事態が生じても、回復できるようにするための仕組みであり、2017 年に導入された。

「ハミルトン・シリーズ」のシミュレーションでは、サイバーアタックの結果、金融機関の機能が麻痺し、多くの顧客がパニックに陥るような事態の発生に対して、米国の金融サービス産業、ひいては米国経済は脆弱であると結論づけられたという。しかも、攻撃の対象となったのが小規模の銀行であっても、混乱はシステム全体に広がることが確認された。そこで、大手金融機関、業界団体、システム会社などにより、参加機関の顧客口座データを、日々、暗号化して保管し、問題発生時にデータ回復が可能となる仕組みの構築がスタートしたのである。ゴールドマン・サックスの Chief Operational Risk Officer の Phil Venables 氏とモルガン・スタンレーの元 Chief Operating Officer の James Rosenthal 氏が構想を主導した。

データの保管場所（Data Vault）は、個々の参加機関が所有・管理するが、自社のインフラ（バックアップ・システムを含む）とは隔離されたものとする必要がある。データは、毎日夜間に定められた標準フォーマットで改変不能の形で保管される。

バックアップ・システムを含め、重要システムが機能しなくなるようなカタストロフィ的イベントが生じた場合、データを回復し、顧客が取引を速やかに再開できるようにするための回復プラン（Resiliency Plan）を準備し、テストすることが参加機関に要求される。

シェルタード・ハーバーの運営主体は、参加金融機関におけるデータ保管体制や回復プランの策定をサポートし、必要な要件が満たされた機関に対して証明書を発行する。参加料は、金融機関の規模に応じ、年間 250 ドルから 2 万 5,000 ドルである。

シェルタード・ハーバーの運営主体には、全米銀行協会（American Bankers Association、ABA）や米国証券業金融市場協会（Securities Industry and Financial Markets Association、SIFMA）をはじめとする主要な金融関係団体が参加している。組織としては、FS-ISAC 傘下の非営利 LLC として運営されている。ゴールドマン・サックスの Venables 氏が、現在、同社の取締役会議長を務めている。

米国の全ての銀行、クレジット・ユニオン、証券会社、資産運用会社、業界団体、サービスプロバイダーが希望すれば参加できる。2019 年 3 月時点で、参加企業は全米の預金口座の 71%、リテール証券口座の 55%をカバーしている[16]。将来的には他のアセットクラ

[16] Sheltered Harbor, “Fact Sheet,” March 2019.

スや海外への展開も視野に入れている。

イングランド銀行の Future of Finance は、シェルタード・ハーバーを紹介し、同様な仕組みを英国に導入することも考えられるとしている。

３．サイバーセキュリティ保険市場の育成

サイバーリスク対策として、サイバーセキュリティ保険も注目されている。サイバーセキュリティ保険は、サイバーアタックの被害に対する経済的補償を提供するだけではなく、サイバーリスクを診断し、必要な備えを促すサービスなども併せて提供されている場合が多い。

サイバーセキュリティ保険市場は、未だ普及途上であり、サイバーアタックの被害額に対し、サイバーセキュリティ保険でカバーされている部分は、わずかとされている[17]。また全世界のサイバーセキュリティ保険市場のおよそ 9 割（収入保険料ベース）が、米国の国内リスクを対象とした契約で占められているとの推計もあり、他の地域への導入は遅れている[18]。

サイバーアタックは、被害を受けた企業が公表していない部分も多いとみられること、また今後、GDPR におけるようにサイバーアタックの結果、情報漏洩等が生じた場合のコスト負担は上昇するとみられることから、サイバーセキュリティ保険市場の潜在的ニーズは高いとみられる。

しかし現状、サイバーインシデント[19]に関する歴史的データが不十分であり、また将来のサイバーリスクの可能性についても不確実性が大きいこともあり、保険会社にとってサイバーセキュリティ保険商品の開発は容易ではない。結果、保険料も他の保険に比べて高額となっており、普及の妨げとなっている。

OECD は、各国政府はサイバーセキュリティ保険市場の育成をサイバーリスク政策の一環に位置づけるべきとしており、サイバーインシデントに関する過去からのデータの利用可能性の向上、サイバーリスクの理解促進につながるフォワードルッキングな分析、サイバーセキュリティ保険のカバレッジの明確化などの点で、政府が関与することの意義を強調している[20]。米国の州政府では、サイバーセキュリティ保険に加盟している IT 業者を、調達の際に優遇する制度の導入を検討する動きもある[21]。

---

[17] Lloyd’s, “Counting the cost: Cyber exposure decoded,” *Emerging Risks Report 2017*, July 14, 2017.

[18] https://home.kpmg/xx/en/home/insights/2018/10/lead-in-cyber-insurance-fs.html.

[19] 悪意のあるものか否かを問わず、サイバーセキュリティを脅かす、あるいはセキュリティポリシー等に違反する情報システム関連のイベント。

[20] OECD, “Enhancing the Role of Insurance in Cyber Risk Management,” November 2017.

[21] マサチューセッツ州など。
http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

４．グローバルな取組み

サイバーセキュリティの強化に向けて、個々の金融機関による自主的な取組み、金融業界としての取組み、そして当局による取組みが展開されているとしたが、近年、国を超えた取組みも本格化している。サイバーアタックには国境は無い。2017 年における WannaCry というランサムウェア[22]の被害は、世界 150 カ国、25 万台のコンピューターに及んだ[23]。ある国が脆弱性を抱えていると、金融ネットワークを通じて容易に他国にもリスクが及びかねないことを踏まえても、グローバルな対応は不可欠と言える。グローバルにビジネスを展開する金融機関にとっても、進出する海外拠点ごとに現地当局から求められるサイバーセキュリティが異なることは、不都合である。

G7 においては、2016 年の伊勢志摩サミットの際に、附属文書「サイバーに関する G7 の原則と行動（G7 Principles and Actions on Cyber）」が採択され、G7 としてサイバーセキュリティの脅威情報の共有を強化すること、及び金融、エネルギー、運輸、通信といった重要インフラのサイバーセキュリティの改善への協力にコミットすることが宣言された。

これに先立ち、2015 年には米国財務省とイングランド銀行を共同議長として G7 Cyber Expert Group（CEG）が設置され、G7 としての金融分野におけるサイバーセキュリティへの取組みがスタートしている。CEG は金融セクターのサイバーセキュリティに関して、2016 年 10 月にベストプラクティスをまとめた文書、2017 年 10 月には各組織が自らの状況を評価するための文書、2018 年 10 月には、ペネトレーションテストに関する指針とサードパーティのサイバーリスクマネジメントに関する文書を発表した[24]。これらの文書には拘束力はないものの、先進国の間でサイバーセキュリティに対する目線を合わせ、協調的なアプローチを確立していくことが目指されている。

2019 年 6 月には、初の G7 合同による危機管理演習が実施されている。G7 の金融当局（財務省、中央銀行、銀行監督当局、市場監督当局）の他、一部の民間金融機関も演習に参加した。2019 年 7 月にフランスのシャンティで開催された、7 か国財務大臣・中央銀行総裁会議では、国内及び国際的な将来の演習に向けて、今回の合同演習から教訓を得ること、また今後数年間の演習の計画を策定することが合意されている。この他、サイバーセキュリティに関する規制のあり方や、情報共有にあたって、サイバーインシデントの分類を G7 として共通化することが議論された。

G20 のレベルでは、2017 年 3 月、ドイツのバーデンバーデンにおける 20 カ国財務大臣・中央銀行総裁会議声明におき、サイバーアタック等に対し、メンバー国における金融サービスと金融機関の強靭性を向上させること、そして国境を超えた協力の第一歩として、

[22] コンピューターに感染することで、コンピューターやデータを利用できなくし、利用者に回復させたければ「身代金（ransom、ランサム）」を払うことを要求するタイプのマルウェア（悪意あるソフトウェア）。

[23] “Ransomware cyber-attack threat escalating – Europol,” BBC, 14 May 2017

[24] “G7 Fundamental Elements of Cybersecurity for the Financial Sector”、“G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector”、“G7 Fundamental Elements for Threat-led Penetration Testing”、“G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector”。

FSB に対して各国の現状調査を要請することが盛り込まれた。現状調査の結果は、2017 年 10 月に発表されている[25]。

FSB は G20 の要請を受け、サイバーセキュリティに関する用語集のとりまとめも行っている。主要な用語について、共通した理解がなければ、情報共有や協調的な対応も困難となるからである。用語集は 2018 年 11 月に公表されている。2019 年にかけては、FSB は、サイバーインシデントに対する民間金融機関の初動と回復に関する実務をサーベイし、とりまとめる作業を行っている[26]。

この他、サイバーセキュリティ保険市場育成に関しては、先述のように OECD において検討が進められており、2017 年 5 月には、7 か国財務大臣・中央銀行総裁会議（於：イタリア・バーリ）に対して、OECD として“Supporting an effective cyber insurance market”という報告書を提出した他、2018 年 2 月には、パリで国際会議も開催している。

Ⅳ わが国の現状と展望

１．相対的な地位の低下

国際連合の専門機関の一つである国際電気通信連合（International Telecommunication Union、ITU）が発表した Global Cybersecurity Index の 2018 年版において、わが国は世界 14 位にランクされている。2014 年時点では、5 位であったが、他の諸国が相次いでわが国を上回るスピードでサイバーセキュリティ対策を強化したため、わが国の相対的な地位は低下したのである（図表 2）。

Global Cybersecurity Index は、Legal（法制面の整備）、Technical（具体的施策の実行フレームワーク、技術的対応メカニズム）、Organizational（国家レベルの戦略、組織的対応）、Capacity building（研究・開発、教育・訓練）、Cooperation（国際協力、官民協力、情報共有体制）という 5 つの柱で、各国を評価している。

2014 年調査でわが国と同じく 5 位だった英国は、2018 年調査で 1 位となった。英国の場合、2015 年まで、サイバーセキュリティ対策は企業の自主性に任されていた。しかし、2016 年 10 月、“National Cyber Security Strategy 2016 to 2021”が策定され、National Cyber Security Center（NCSC）が設立された。NCSC は、重要インフラ事業者のガイダンス作成、中小企業や個人に対するアドバイス、人材育成のためのトレーニング等を実施している。また、英国へのサイバー攻撃に半自動的に対応するため、Active Cyber Defense プログラ

[25] FSB, “Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices,” October 13, 2017.

[26] 検討作業の報告が、2019 年 6 月の 20 か国財務大臣・中央銀行総裁会議（於福岡）で発表され、実際のサーベイは同年 7 月に着手されている。FSB, “Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka,” June 8-9, 2019 及び FSB, “Cyber Incident Response and Recovery, Survey of Industry Practices”参照。

図表 2　グローバル・サイバーセキュリティ・インデックス（ランキング）

2014年	2017年	2018年
1　米国	1　シンガポール	1　英国
2　カナダ	2　米国	2　米国
3　オーストラリア	3　マレーシア	3　フランス
3　マレーシア	4　オマーン	4　リトアニア
3　オマーン	5　エストニア	5　エストニア
4　ニュージーランド	6　モーリシャス	6　シンガポール
4　ノルウェー	7　オーストラリア	7　スペイン
5　ブラジル	8　ジョージア	8　マレーシア
5　エストニア	9　フランス	9　カナダ
5　ドイツ	10　カナダ	9　ノルウェー
5　インド	11　ロシア	10　オーストラリア
5　日本	12　日本	11　ルクセンブルク
5　韓国	13　ノルウェー	12　オランダ
5　英国	14　英国	13　サウジアラビア
	15　韓国	14　日本
	16　エジプト	14　モーリシャス

（注）　網掛けは、2014 年時点では日本のランク以下だった国。
（出所）ITU 資料より野村資本市場研究所作成

ムをインターネットサービス事業者と共に構築している[27]。

わが国の場合、Global Cybersecurity Index の 2017 年調査において、Organizational の柱のうち Cybersecurity metrics（ベンチマークに基づく評価の実施）の項目、Capacity building の柱のうち Incentive mechanisms（サイバーセキュリティ促進への助成）の項目、Cooperation の柱のうち Public-private partnership（官民における情報やリソースの共有）の項目、以上の 3 項目が特に低い評価を受けていた[28]。

わが国の場合、セキュリティ事故に関する報告先や報告様式等が様々であること、また諸外国のように報告義務や罰則規定が法制度化されていないこと、各組織において必要なセキュリティ情報の収集や対策の実装を自動化する仕組みが普及していないこと、などの課題も指摘されてきた[29]。

わが国でも、2014 年にサイバーセキュリティ基本法が成立し、同法に基づき 2015 年 1 月に内閣にサイバーセキュリティ戦略本部が設置され、内閣官房に内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity, NISC）が設置された。また 2018 年 12 月には、サイバーセキュリティ基本法が改正され、脅威情

[27] 一般社団法人日本サイバーセキュリティ・イノベーション委員会「諸外国におけるサイバーセキュリティの情報共有に関する調査」、2018 年 3 月 9 日参照。
[28] Leading（先進的）、Maturing（ほぼ実現）、Initiating（整備途上）の 3 段階のうち、Initiating の位置づけ。2018 年版では同分類に基づく評価の記述は無い。
[29] 一般社団法人日本サイバーセキュリティ・イノベーション委員会（2018）。

報・対策情報等の共有・分析等の円滑化を図るため、2019 年 4 月に NISC にサイバーセキュリティ協議会が発足したところである。

近年、諸外国においては、サイバーセキュリティに関する規制・監督や、個人情報の漏洩に対する報告義務や罰則が一段と強化される傾向にある[30]。グローバルに事業を行うわが国の企業は、既にこうした動きに対応を迫られているが、わが国の今後の制度を検討していく上でも、こうした潮流を踏まえる必要があろう。

２．金融分野の取組み

わが国では、従来、各金融機関のサイバーセキュリティ管理態勢について、システムリスク管理等の一環として監督・検査の対象とされてきた。しかし近年、サイバー攻撃が金融システムの安定にとって重大なリスクとなっており、個々の金融機関を超え、業界全体のサイバーセキュリティ強化が必要と認識されるようになった。このため 2014 年 8 月に、一般社団法人金融 ISAC が設立されている。

金融当局においては、上記の 2014 年に成立したサイバーセキュリティ基本法に基づき、金融を含む重要インフラ事業者[31]のサイバーセキュリティ確保のための施策が導入された。すなわち 2015 年 4 月、金融庁においては、各金融業態向けの「総合的な監督指針」、「事務ガイドライン」、「金融検査マニュアル」などが改訂された。改訂前においては、コンピューターシステムのダウンや誤作動等、システム障害への対応に重点が置かれていたが、この改訂において情報セキュリティ管理やサイバーセキュリティ管理の項目が明記され、各種の対策事例も具体的に盛り込まれたものとなった。

また 2015 年 7 月には、金融庁は「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」を公表した。同方針では、①サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、②金融機関同士の情報共有の枠組みの実効性向上、③業界横断的演習の継続的な実施、④金融分野のサイバーセキュリティ強化に向けた人材育成、⑤金融庁としての態勢構築、という 5 つの方針が掲げられている。

同取組方針の策定から 3 年が経過したが、金融庁が 2019 年 6 月に発表した「金融分野のサイバーセキュリティレポート」[32]によれば、地域銀行においては、脆弱性診断等を意識的に実施しているのは一部にとどまり、その必要性が十分浸透していないこと、信金・信組においては、業態内上位であってもリスク評価やインシデント対応といった基礎的態

[30] 2017 年 6 月に成立した中国のサイバーセキュリティ法においては、当局が事業者のサイバーセキュリティについて立ち入り調査が可能とされた。2018 年 2 月に成立したシンガポールのサイバーセキュリティ法においては、重要インフラに対してインシデントの届出義務が課された（罰則あり）。2018 年 12 月に成立したオーストラリアの Assistance and Access Act においては、政府が IT 事業者に対し暗号を解除した通信内容を提供することを要請できることとした。

[31] 重要インフラ分野として、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油の 14 分野が特定されている。

[32] 2015 年 7 月発表の取組方針は、2018 年 10 月に改訂されているが、この中で、「金融分野全体のサイバーセキュリティ対策の強化を促すために、金融分野に共通する課題等について積極的に情報発信する」とされた。本レポートは、これを受けて取りまとめられた。

勢は依然として整備途上の段階に留まり、脆弱性対応についても委託先任せとなっていること、証券会社等においても、信金・信組同様、整備途上のところが多いこと、等の問題点が指摘されている。

３．資金決済分野のサイバーセキュリティ問題

わが国では、2018 年 1 月に暗号資産（仮想通貨）交換業者におき、580 億円相当の暗号資産不正流出事件が生じた。これより規模は小さいものの、2018 年 9 月、2019 年 7 月にも同様の不正流出事件が生じている。また 2018 年 12 月と 2019 年 7 月には、大規模なキャンペーンの下でスタートしたスマホ決済サービスにおいて、セキュリティ上の不備から、不正利用が相次いで発生し、大きな注目を集めた。

暗号資産交換所は、2010 年頃からわが国に登場したが、2014 年 2 月、当時、最大規模の交換所であったマウントゴックスにおき、不正アクセスによって当時のレートで 480 億円相当のビットコインが消失し、暗号資産の払い戻しが停止するという事件が生じた。この事件を一つの背景として、2016 年 5 月に改正資金決済法が成立し、暗号資産交換業者に対する登録制が導入された経緯がある[33]。またスマホ決済サービス業者は、資金決済法上の前払式支払手段発行者として登録した上で業務を行っている[34]。

つまり、いずれも資金決済法上の登録業者として金融庁の監督下にある業者において、重大なサイバーセキュリティ上の問題が相次いで発生した形となる。もちろん、これら業者のサイバーセキュリティについても、「事務ガイドライン」などにおいて、必要な取組みが相当程度、具体的に記述されていたが、徹底されていなかった可能性がある。

先述のように、イングランド銀行の報告書は、ペイメント・チェーンへの異業種の参入について、サイバーリスクという観点から注意を喚起しているが、わが国ではまさに、金融当局として懸念すべき事態が頻発しているわけである。以下、わが国の資金決済分野のサイバーセキュリティに関する課題を整理してみよう。

[33] 資金決済法は、2009 年 6 月に成立し、2010 年 4 月に施行された。2016 年 5 月の改正により、仮想通貨交換業者に対する登録制が導入された後、2019 年 5 月の改正では「仮想通貨」を「暗号資産」に置き換えた他、暗号資産交換業者や暗号資産取引に対する規制強化が導入された。

[34] 前払式支払手段は、従来、商品券取締法や前払式証票規制法で規制されてきたが、サーバー型電子マネーを含める形で資金決済法に規定された。2016 年 5 月の資金決済法改正では、スマホなどと連動させて利用される「電子端末型プリペイドカード」、すなわち今日、前払式支払手段による「スマホ決済」と呼ばれているサービスの登場を受けた規定の改正が実現している。具体的には、従来、プリペイドカードに利用限度額などを表示する義務があったが、インターネットでの情報提供も認められた。この他、プリペイドカードの利用拡大に伴い、利用者がトラブルに巻き込まれる事案が増加したことを受けて、発行者に対して加盟店管理や苦情処理体制の整備が明確に要求された。なお LINE Pay やメルペイなど、送金機能も提供する業者は、資金決済法上の資金移動業者としても登録されている。

４．今後の課題

第一に、わが国のサイバーセキュリティ対策が、前記の Cybersecurity Index に示されるように、相対的に諸外国に遅れをとる状況にある。いうまでもなく金融取引はグローバル化しており、一国における取引の混乱は他国にも波及しかねない。海外顧客の情報流出や不正取得された資金がテロ組織に流れるような事態も、国際的問題となる。従って、主要な国々と少なくとも同等のタイミング及びレベルで、セキュリティの向上が実現していく必要がある。

第二に、サイバーセキュリティという観点から、諸外国において法規制によって求められている事項でも、わが国では自主的取組みに留まっている部分がある。例えば、前記のようにセキュリティ事故の情報共有の枠組みは整備が進みつつあるものの、諸外国におけるように、罰則規定を伴う報告義務が法制化されるには至っていない。

決済分野では、EU や中国、マレーシア、メキシコなどでは、オンラインでの決済取引の実行やセンシティブな支払いデータへのアクセスなどにおいて、多要素認証を求める Strong Customer Authentication（SCA）の導入を義務化する動きがある[35]。

これに対して、わが国においては、SCA の義務付けといった議論は進展しておらず、クレジットカード利用時の多要素認証の一形態である 3D セキュアも、普及途上の段階である。マイナンバーカードのデジタル ID としての利用も進んでいない。

前払式支払手段発行者に対する金融庁の事務ガイドラインにおいては、インターネット等を利用して非対面取引を行う場合は、「取引のリスクに見合った適切な認証方式」の導入が求められ、多要素認証も例示されている。しかし 2019 年 7 月には、ユーザー登録において多要素認証を導入していなかったスマホ決済業者（前払式支払手段発行者）のサービスで、他人による不正利用が短時間で多数発生したことは、記憶に新しい。

当該事件においては、当初、被害者からの苦情対応が適切ではなかったとの報道もある。前払式支払手段発行者に関しては、サーバー型電子マネーを巡る消費者被害が増加した際、適切な苦情処理が行われていないとして、2015 年に消費者委員会が金融庁に対して建議を行った経緯がある。これを受け、2016 年の改正資金移動法において「利用者からの苦情の適切かつ迅速な処理のために必要な措置を講じなければならない」とする規定が導入された。

このような現行のガイドラインや法律上の規定が、適切にエンフォースされていたかも再点検の必要があろう。

第三に、サイバーセキュリティ基本法における重要インフラとして「金融」と「クレジット」（クレジットカード決済のシステムを指す）が並列的に位置づけられている点に象徴されるように、決済機能の維持という観点から一貫した政策対応を講ずるのではなく、

[35] 多要素認証とは、①暗証番号やパスワードなど本人しから知らない情報、②カードやスマートフォンなど本人が所有するもの、③本人の指紋や顔などの生体情報、といった複数の要素を組み合わせて本人確認を行うこと。EU の場合、2 つ以上の要素を組み合わせて本人確認することが、2019 年 9 月から義務付けされる。淵田康之「デジタル ID 時代の世界と日本」『野村資本市場クォータリー』2019 年夏号参照。

金融庁と経済産業省が、それぞれ所管する業態に対して政策を講じる姿となっている。また同じ金融庁所管の業態においても、決済サービスに従事する業者を横断的にとらえるのではなく、専ら業態縦割りでサイバーセキュリティ体制が論じられる傾向がある。

しかし例えばスマホ決済におけるセキュリティ・インシデントは、銀行口座からの不正な資金の流出とクレジットカードの不正利用という両方の形態で生じている。スマホ決済業者、銀行、クレジットカード会社を横断的にとらえ、一貫したセキュリティ対策を講ずることが不可欠であろう。またスマホ決済業者が、一般事業会社の子会社であるような場合は、親会社も含めたセキュリティ・ガバナンスのあり方に着目する必要があると考えられる。

サイバーアタックによってユーザーに被害が生じた場合、銀行やクレジットカードを利用していた場合と、スマホ決済など新たな決済サービスを利用していた場合とでは、補償などのあり方が異なる点についても、それが合理的な差異であるか、またユーザー側に理解が行き届いているかが問われる必要があろう。前払式支払手段発行者に関しては、補償のあり方以前の問題として、苦情処理体制に問題があるとして、消費者委員会が金融庁に改善を促した経緯があることは、既述の通りである。

EU は 2007 年の段階で、銀行、クレジットカード、電子マネー、送金業者など、決済サービス提供業者全体を横断的に規制する決済サービス指令を成立させ、共通の利用者保護の枠組みを導入している。同指令の 2015 年改正時には、先述の SCA の義務化も盛り込まれた。

以上のように、わが国の金融は、サイバーセキュリティ分野で諸外国に相対的に遅れた地位にあり、法制面の整備一つとっても課題が多い。サイバーセキュリティ問題とも密接に関連するが、わが国は AML/CFT（Anti-Money Laundering and Countering the Financing of Terrorism、マネー・ローンダリング及びテロ資金供与対策）でも国際的に低い評価を受けてきた経緯がある。このような現実があるなかで、わが国は暗号資産取引やスマホ決済など、IT を活用したイノベイティブなサービスを諸外国と遜色ないスピード感で導入してきた。

グローバル金融危機は、サブプライムローンやクレジットデリバティブなど、金融・資本市場全体から見れば、ボリューム的には限定的でメインストリームとは言えない分野を発端として拡大した。これと同様に、サイバーセキュリティ問題に起因する金融のシステミックリスクも、必ずしも大手銀行のように重要インフラとして警戒されていない分野が火元になる可能性がある。こうした点にも留意し、法制面及び監視・監督体制の整備を含めた対応が求められよう。