２０１８年２月６日

日　本　銀　行

金融市場インフラとサイバーレジリエンス

日本銀行理事　　桑原 茂裕

（はじめに）

日本銀行の桑原でございます。本日は、ご多忙の中、決済システムフォーラムにお越しいただき、心より御礼申し上げます。

本日のフォーラムの開会にあたり、私からは、本日のテーマであるサイバーレジリエンスについて、金融、その中でも特に金融市場インフラとの関わりを中心に、お話させていただきます。

１．　情報技術革新に対する期待

近年、情報技術は目覚ましい進歩を遂げており、例えばインターネットを通じて提供されるサービスは、我々の日常生活において一層の拡がりを見せつつあります。スマートフォンを利用したネットショッピングはもちろんのこと、最近では、人間が話しかけることにより、ＡＩがニュースを読み上げたり照明や空調を操作したりすることなどが、既に現実のものとなっています。こうした情報技術革新の流れは、今後も続くものと考えられ、我々の社会インフラを支える基盤として、情報技術の果たす役割は今後ますます大きくなっていくことが予想されます。

こうした中、金融の分野でも、例えば、ビッグデータやＡＩの利用を通じて、顧客のニーズに合わせた新しい金融商品を個別に提供できるようになるなど、情報技術の発展により、これまでにない新たなサービスが生み出されつつあります。また、従来の金融業務についても、情報技術の活用を通じて、その効率化や生産性の向上が期待されています。さらに、例えば資金決済とｅコマースやシェアリングエコノミーとが結びつくことなどにより、金融がさまざまな産業と新たなネットワークを形成する動きも出はじめており、情報技術革新によって、産業構造そのものが変わっていく可能性も指摘されているところです。

２．　サイバー攻撃の脅威

このように、我々の社会インフラにおいて、それを支える情報技術の果たす役割が高まれば高まるほど、そうした社会インフラに危害を加え、我々の社会生活に重大な影響をもたらしかねないサイバー攻撃に対する脅威も、ますます大きくなってきています。

例えば、昨年５月、ランサムウェアを使った大規模なサイバー攻撃が世界中で行われ、さまざまな被害が生じたことは記憶に新しいところです。また、先月には、業者が顧客から預かっていた仮想通貨が、不正に外部に送信され流出する事件が発生しています。仮想通貨は、現時点では、専ら投資・投機の対象となっており、支払決済への利用は僅少です。しかしながら、この事件は、決済や金融サービスの安全性や安定性の確保がいかに重要であるかを、改めて人々に認識させるものとなりました。仮想通貨関連サービスの提供者は、自主的かつ積極的に、投資家へのリスクの説明や十分なセキュリティ対策を実施する必要があり、一方で、仮想通貨に投資をする人々は、法定通貨ではなく裏付け資産も持たない仮想通貨の取引に伴うリスクをしっかり認識する必要があります。

３．　サイバーレジリエンスの向上

こうしてサイバー攻撃が大きな脅威となる中、「サイバーレジリエンス」の向上に向けた取組みの重要性が、ますます高くなってきています。

（サイバーレジリエンスとは）

「サイバーレジリエンス」とは、サイバー攻撃によって生じる被害を最小限に抑え、素早く復旧し、業務を継続できるようにすることであると、一般に言われています。

サイバー攻撃に対しては、まず、セキュリティ対策を万全に行うことで被害を生じさせないことが求められます。

一方で、情報技術の進歩に併せて、サイバー攻撃の手法も日々高度化しています。このため、サイバー攻撃により被害を生じさせない対策に加えて、仮に被害が生じた場合においても、その被害を最小限に抑え、業務を継続する能力、すなわちレジリエンスを高めることも重視されるようになってきています。

（自然災害に対する業務継続との比較）

この点、サイバーレジリエンスの向上に向けた取組みは、地震、洪水、疫病といった自然災害に対する業務継続（Business Continuity）の取組みと共通するものがあります。

しかしながら一方で、サイバーレジリエンスには、自然災害とは異なる点があることにも留意が必要です。例えば、自然災害の場合には、災害が発生すると、多くの人が直ちに認識することができます。これに対して、サイバー攻撃の場合には、システムに不正侵入されて被害が発生しても、それを探知するまでに時間を要してしまう場合があり、その間にさらに被害が拡大してしまうリスクがあります。さらに、サイバー攻撃の場合には、必ず攻撃者がいることも大きな特徴です。攻撃者は、自然災害とは異なり、特定の意図を持って行動するほか、こちらの対策を前提にしつつ、それを破るような攻撃を仕掛けてくるため、ある時点で有効な対策も、時の経過とともにそれが無効化されるリスクが常に存在します。

したがって、サイバーレジリエンスを考えるにあたっては、自然災害に対する業務継続の取組みを参考にしつつも、サイバー攻撃特有の問題点、すなわち被害の早期探知が重要であることや、攻撃者との「いたちごっこ」の側面があることなどに十分留意しつつ、不断の努力を怠らず、常に最新の対策を講じていくことが求められています。

４．　金融市場インフラのサイバーレジリエンスの向上

サイバー攻撃は、すべての産業にとって脅威となりますが、金融分野にと

っては特に大きな脅威と言えます。それは、金融がすべての産業の経済基盤を支える社会インフラとしての性質を有していることに加え、金融システムは、さまざま経済主体が「信用」によって結びつくことで成り立っているため、サイバー攻撃によって一たびその「信用」が毀損されると、金融システム全体が機能しなくなるおそれがあるからです。

その中でも、金融市場インフラに対する攻撃については、特に注意が必要です。それは、金融市場インフラが、各種金融サービスを提供する際のハブとなっており、その業務が適切に運営されない場合には、金融システム全体に大きなショックを与えかねないことに加え、そうしたショックが国内のみならず、国際金融市場にも伝播していくリスクがあるからです。このため、金融市場インフラに関するサイバーレジリエンスについては、特に高い優先度と細心の注意をもって、検討・実施していくことが重要です。

こうした観点から、ＢＩＳ決済・市場インフラ委員会（ＣＰＭＩ）および証券監督者国際機構（ＩＯＳＣＯ）は、２０１６年６月に「金融市場インフラのためのサイバーレジリエンスに係るガイダンス」を公表し、国際基準である「金融市場インフラのための原則」を補完するかたちで、金融市場インフラがサイバーレジリエンスを高めるために必要な事項を明らかにしました。また、バングラデシュ中央銀行の預金が不正に海外に送金された事件等を踏まえ、ＣＰＭＩは、２０１７年９月に「大口資金決済システムにおける不正リスクの削減」と題された市中協議文書を公表し、エンドポイントセキュリティ、すなわち端末やそれにつながるネットワーク全体の安全性の強化のために関係者が取り組むべき事項を提案したうえで、今後、これを具体化するためのガイダンスの作成を進めることを表明しています。

これらの文書においては、サイバーレジリエンスは、各金融市場インフラが単独で確保できるものではなく、市場参加者なども含めた共同努力によって実現できるものとされており、金融市場インフラの幅広い関係者による協調活動が期待されるところです。

５．　中央銀行としての取組み

こうした中、日本銀行は、日銀ネットという決済システムを管理・運営しています。このため、自らが金融市場インフラの管理・運営主体として、サイバーレジリエンス対策を適切に講じていくことはもちろんのこと、それにとどまらず、中央銀行として、決済システム全体の安全性や安定性に責任を有する立場から、幅広い関係者が行っておられる金融市場インフラに関するサイバーレジリエンスの向上に向けた取組みについても、最大限サポートしていきたいと考えています。

本日は、サイバーレジリエンスの向上に向け、日々活躍しておられる方々からご講演をいただく予定となっております。本日のフォーラムが、サイバーレジリエンスの向上に向けた皆様の取組みの一助となることを願いつつ、開会の挨拶とさせていただきます。

ご清聴ありがとうございました。

以　　上