２０１８年４月
日本銀行決済機構局

第18回決済システムフォーラムの議事の概要

2018年2月6日開催（於：日本銀行本店）

日本銀行は本年２月、「決済システムフォーラム」の第18回会合を開催した。

金融のグローバル化や情報技術革新、さらに、インターネットやスマートフォンなど金融サービスにアクセスする媒体の多様化といった環境変化の下、金融インフラへのサイバー攻撃にいかに対処し、インフラの機能不全や情報流出などをどのように防ぐかといったサイバーセキュリティの問題に、世界的な関心が高まっている。

このような情勢を踏まえ、今回の決済システムフォーラムでは、サイバーセキュリティやサイバー攻撃耐性（サイバーレジリエンス）の問題に焦点を当てた。このフォーラムには、サイバーセキュリティに関わる幅広い主体が集まり、下記の議事次第に沿って議論が進められた（参加企業・団体は別添を参照）。

具体的には、①最近のサイバー攻撃の特徴、②サイバー攻撃への対処法、③サイバーセキュリティに必要な人材をいかに確保するか、④サイバーセキュリティの確保と情報の活用をいかに両立させるか、⑤サイバー攻撃に関する情報の共有をどのように進めるか、等について活発な議論が行われた。

以下では、当日の議論の概要を紹介する。

【議事次第】

１．開会挨拶
２．サイバー攻撃・侵害事件の動向
　「攻撃者の動向を踏まえた2018年セキュリティ予測」
３．サイバーレジリエンスに関する国際的な議論
　「決済インフラのサイバーリスクに関する国際的な議論」
４．国内の議論
（１）「サイバーセキュリティへの取組み」
（２）「Society5.0実現に向けたサイバーセキュリティの強化を求める」
５．パネルディスカッション

概　要

１．開会挨拶（日本銀行理事　桑原）

「金融市場インフラとサイバーレジリエンス」[1]

２．サイバー攻撃・侵害事件の動向
「攻撃者の動向を踏まえた 2018 年セキュリティ予測」
（ファイア・アイ執行役副社長 岩間氏）

近年、国家支援型のサイバー攻撃が増加している。今後もこの傾向は変わらないとみており、特に今年はアジアの一部からの攻撃が一層活発化する見込み。

また、その攻撃手法は年々高度化しており、国家間の諜報活動に使用されていた高度な手法が一般の攻撃者の間にも広まっている。これに伴い、攻撃を検知すること自体が困難化している。

攻撃対象については、企業が保有する AI などの最先端技術や重要インフラの情報に対する偵察活動が確認されている。加えて、一部の中央銀行や仮想通貨の交換を行うサイトを狙った攻撃も観測されているところ。

先行き、EU の一般データ保護規則において情報侵害の報告義務に違反した際に罰金等の制裁が科されることとなった場合には、ランサムウェア等を利用し、侵害の事実を隠ぺいする代わりに金銭を要求するような攻撃が増加する可能性がある。また、急速に普及しているクラウドサービスへの攻撃が増加する可能性があるほか、IoT に関しては、スマート家電等の普及が進む中、脆弱性を狙った攻撃が増加する可能性がある。仮想通貨を扱う業者についても、一般の金融機関等に比べてセキュリティが脆弱であるためターゲットになり易く、仮想通貨を狙った攻撃は増加の一途を辿るとみている。

サイバー攻撃への対応方針としては、当たり前の対策をきちんと実行することに尽きる。例えば、OS の更新情報が出た場合、必ずアップデートを行うといった基本的な対応を行うだけで、リスクを格段に低下させることが出来る。そのうえで、自社の組織に即した追加的な対応を検討すべき。

---

[1] http://www.boj.or.jp/announcements/press/koen_2018/ko180206a.htm/

３．サイバーレジリエンスに関する国際的な議論

「決済インフラのサイバーリスクに関する国際的な議論」

（日本銀行決済機構局参事役 浜野）

国際的な議論では、決済インフラのサイバーリスクは、オペレーショナルリスクの一場面と位置づけられるのが一般的であるが、サイバー攻撃の特殊性から、通常のオペレーショナルリスクとは異なる配慮が必要となり得る。2012年にCPMI/IOSCOが公表した「金融市場インフラのための原則（FMI原則）」の原則17（オペレーショナルリスク）は、オペレーショナルリスクの要因の一つとしてサイバー攻撃に明示的に言及し、「枢要なITシステムについては、障害発生から2時間以内の復旧を可能とすること」を求めている。原則17を中心に、サイバーレジリエンスの観点から、FMI原則を補完するものとして2016年に「サイバーレジリエンスガイダンス」が公表されており、FMI原則の解釈・運用にあたっては同ガイダンスを踏まえる必要がある。同ガイダンスを踏まえた個別金融市場インフラにおけるFMI原則の実施状況などは、今後、CPMI/IOSCOによる実施モニタリングの対象となり得る。

CPMI では、大口資金決済システムについて、ユーザーを含めたエコシステム全体のセキュリティ確保が重要との問題意識に基づき、エンドポイントセキュリティに関する取組みが進められている。CPMI の下に、日本銀行を含む主要中銀によるタスクフォースが設置され、2017 年 9 月にエンドポイントセキュリティの強化に向けた「基本戦略（strategy）」に関する市中協議文書を公表。現在、市中コメントを踏まえた最終報告書の策定に着手している。

SWIFT では、2016 年に発生したバングラデシュ中銀における不正送金事件以降、日本銀行を含む主要国中銀の国際協調オーバーサイトの枠組みのもと、ユーザーセキュリティの強化が進められている。SWIFT は 2016 年 5 月から全ユーザーのセキュリティ水準の引き上げを企図した取組み（CSP：Customer Security Programme）を実施しており、2017 年に、ユーザーに求める最低水準を取りまとめた「Customer Security Controls Framework」を配布し、ユーザーに対し、自己査定を行ったうえで、昨年末までに SWIFT に報告するよう求めている。主要国中銀は、国際協調オーバーサイトの一環として、CSP の適切性につき確認を行ってきており、今後、その結果の分析などを踏まえ、対応が不十分な点などが確認された場合には、国際協調オーバーサイトの枠組みの下で対応が議論されていくこととなると考えられる。

サイバーセキュリティ、サイバーレジリエンスに関する国際的な議論は、グローバル金融危機後に本格化、バングラデシュ中銀における不正送金事件等を契機に大きく進展したが、サイバー攻撃の傾向の変化やIT技術の進展等に伴い、決済インフラに求められる対応事項や要求水準も変化し得る。決済インフラやそのユーザーは、国際基準等に照らして、間断なく必要な対応を検討・実施する必要があり、中央銀行としても、同対応を支援していく所存。

４．国内の議論

（１）「サイバーセキュリティへの取組み」

（金融情報システムセンター＜FISC＞監査安全部長 和田氏）

サイバー攻撃の手口は、多様化、ビジネス化、国際化に加え、分業化が進んでおり、完全に防御することが難しくなっている。このため、防御が破られた場合に備え、攻撃の早期検知、被害の拡大防止等、経営判断を含めた早期対応が行える態勢といったサイバーレジリエンス態勢の構築が重要と言える。

FISCでは、2013年より、サイバー攻撃対応に関する有識者検討会を開始。2015年には安全対策基準にサイバー攻撃への態勢整備に関する事項を追加したほか、2017年には、サイバー攻撃に対する早期検知や被害拡大防止を企図したコンティンジェンシープラン策定のための手引書の改定といった取組みを進めてきた。

金融庁においても、2015年に、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を公表。官民が一体となって取組みを進める重要性や、サイバーセキュリティの確保に向けた対話を積み重ねていく方針が示された。この取組方針により、各金融機関の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が行われるようになり、金融レポート（平成28事務年度）では、①経営層の関与が希薄、②侵入される前提の下での対策が遅滞、③他の金融機関との共助体制が不十分、といった課題が指摘されている。

こうした課題を踏まえ、FISCでは2017年度より、サイバー攻撃対応態勢の強化に向けた「サイバーセキュリティ意見交換会」を開始。また、金融機関等におけるIT人材の確保・育成計画のための手引書を作成している。

2018年度についても、中小金融機関を主なターゲットとした「サイバーセキュリティワークショップ」を開催予定であるほか、サイバーセキュリティ人材の確保・育成に関し、金融機関における取組みの具体例をレポート等でFISC会

員に紹介する予定。この点、情報処理推進機構（IPA）が公表している「情報セキュリティ 10 大脅威　2018」で「セキュリティ人材の不足」が初めてランクインし、各金融機関でも重要な課題となっているため、FISC としてもサポートしていきたい。

サイバー攻撃の高度化・巧妙化に伴い、被害件数・被害規模が拡大する中、自らの組織の態勢を把握し、対策を適切に実施していくことが益々必要となっている。FISC としては、各金融機関の皆様に還元できるよう支援活動等を行っていきたい。

（２）「Society5.0 実現に向けたサイバーセキュリティの強化を求める」
（日本経済団体連合会サイバーセキュリティに関する懇談会座長　梶浦氏）

過去数年にわたり、経団連の情報通信委員会では、デジタルエコノミーの普及やデータの利活用等に関する検討とともに、サイバーセキュリティの重要性が議論されてきた。そうした中、サイバーセキュリティに対するリスクの急速な高まりを背景に、銀行や保険会社を含む 30 社でサイバーセキュリティに関する議論を開始。ウクライナでのサイバー攻撃による大規模停電やバングラデシュ中銀における不正送金事件に伴い、重要インフラのサイバーセキュリティへの危機感が高まる中、2015 年、2016 年の二度にわたり、サイバーセキュリティ対策の強化を提言してきた。

2017 年には、経団連の憲法にあたる企業行動憲章を改定し、サイバー攻撃対策を行う旨を明言。また、Society5.0 の時代、すなわちあらゆるモノが情報ネットワークで繋がり、データを活用することで、より効率的に付加価値を生み出していく社会の実現に向けて、三度目の提言を行った。提言では、サイバーセキュリティ対策は、価値創造のための重要な投資であり、サイバーセキュリティ耐性が企業の競争力になるとの視点を打ち出している。同時に、サイバー攻撃は自然災害同様に避けられないものであり、サイバーセキュリティは危機管理であるとの視点も示している。

実際の取組みを進めるうえでは、①企業が主体的に対策を行う「自助」、②組織や業界を超えて助け合う「共助」、③政府の情報提供や支援による「公助」、④国境を越えた「国際連携」、といった順序で対応することが重要。

また、取り組むべき事項としては、①セキュリティ人材の育成、IT ベンダー

への偏在の是正、キャリアパスの提供、②サイバー攻撃やサイバーセキュリティに関する情報共有、③サイバー攻撃の高度化等にあわせた技術対策、④官民におけるサイバーセキュリティ関連投資の促進が挙げられる。②については、自社の社会的信用が低下するとの懸念が情報漏えい事例の共有の妨げとなっており、被害企業を責めがちな日本の風潮を変えていく必要がある。④については、目先の収益への貢献が見込み難いサイバーセキュリティ投資の拡大には経営者の意識改革が必要であり、その呼び水としては、政府による税制優遇や補助金拡大といった施策があってもよいと考えられる。

さらに、政府のサイバーセキュリティに関する組織をみると、現状では各省庁等に情報関連政策や予算が散在しているため、司令塔としての内閣サイバーセキュリティセンター（NISC）の強化や、サイバーセキュリティ政策を一元的に所管する機関の創設が求められる。一方、事業会社に目を向けると、最高情報責任者（CIO）に加え、最高情報セキュリティ責任者（CISO）の必要性が認識されているほか、取引先を含めたサプライチェーン全体のサイバーセキュリティの確保が重要となってきている。

法制面をみると、現在は、サイバーセキュリティ人材の教育の一環として悪意のあるウイルスやマルウエア等を作成すると違法となってしまう。同様に、学界においても、攻撃に関する研究を行うことは倫理に反するとの声がある。攻撃手法に関する知見がないと防御を行うことは難しいため、人材育成や防御に関する研究の進展を妨げる懸念があり、何らかの対応が必要。

経団連としては、提言を行うだけでなく自ら行動を起こすべく、経営者に向けたセミナーの開催や周知広報活動、世界経済フォーラムへの参画、国際会議への参加等、取組みを進めていく所存。

５．パネルディスカッション

（１）サイバーセキュリティ人材の不足

（日本銀行決済機構局局長　山岡）

皆さんのプレゼンテーションはいずれも、「サイバーセキュリティ人材の不足」を指摘していたのが印象的であった。また、最近のコインチェック社の事例でも、この点が話題を集めたことは記憶に新しい。

では、日本においてそうしたサイバーセキュリティ人材が不足している原因

はどこにあるのか。①人材を養成する教育システム等の問題か。②人材が偏在しているのか。あるいは、③そうした人材を組織内で十分処遇できないこと等によるインセンティブの問題があるのか。もちろん、現実には複雑な要因が絡み合っていることと思うが、皆さんのご見解を賜りたい。

（経済団体連合会　梶浦氏）

人材不足は、①IT ベンダー等への偏在、②給与体系（キャリアデベロップメント）での処遇不足、③人材育成プロセスの欠如、といった多くの要因が影響。例えば、給与体系に関して、米国では優秀な専門家に経営者と同等以上の処遇が用意されるが、日本では同様の処遇は難しい。人材育成についても、米国のように軍の専門家が民間で活躍することは稀であるほか、イスラエルのように小学生の頃から特別な教育を行う制度もなく、日本の教育機関では実践的な教育は出来ない。

（金融情報システムセンター　和田氏）

金融機関が求める人材は、経営者が必要な経営判断を行えるように、サイバーセキュリティ関連情報を咀嚼・提供できる橋渡し役を担える人材であり、業務知識を持ったうえで IT ベンダー等の専門家と対話できる人材。そのような人材を確保するうえでは、業務知識や経営的センスをもつ人材に対し、IT リテラシーを高める教育を行うことが考えられる。

（ファイア・アイ　岩間氏）

人材が IT ベンダー等に偏在していることが大きな要因。米国では、IT ベンダーに限らず、各企業にサイバーセキュリティ人材がいる。日本でも、雇用の流動化が進めば、必要な人材を必要な場面で確保することができ、処遇の改善も進むと思われる。

（２）攻撃者のタイプやその目的

（日本銀行　山岡）

皆さんのプレゼンテーションでは、最近のサイバー攻撃の特徴についても紹介されていた。これに関連し、金融市場インフラにサイバー攻撃を仕掛ける攻撃者は、①金銭等の経済的利益の獲得を目的とすることが多いのか、それとも②インフラの破壊自体を目的とする事例も多いのだろうか。仮に後者のタイプ

の攻撃が高度な形で行われれば、大きな脅威となるかもしれない。

（経済団体連合会　梶浦氏）

ただ金融市場インフラを破壊したいという攻撃者は、通常は単独犯であり、さほど大きな脅威となり得ないように思う。もっとも、国家的な関与がある場合は、その規模や継続性等を鑑みると、深刻な問題を引き起こす懸念がある。

（ファイア・アイ　岩間氏）

攻撃者の目的は、①国家主導の諜報活動、②金銭等の欲得、③愉快犯、④破壊活動、と多様。日本については、米国とのつながりが強いため、米国で確認された攻撃が少し遅れてみられる傾向があるほか、企業の知的財産や高い技術力を狙った新興国等からの攻撃が多いことが特徴。

（３）サイバーセキュリティと情報の利活用のバランス

（みずほ銀行　貞広氏）

サイバーセキュリティ等の「守り」の側面だけを唱えても、片手落ちなのではないかと感じる。つまり、第４次産業革命と呼ばれる IT 革命により、情報の利活用を含めた IT サービスの拡大等、「攻め」の取組みが一層必要ではないか。

（経済団体連合会　梶浦氏）

全く同感。経団連の取組みは、IT 技術の活用による効率化・高付加価値化・高速化を一層図ることが中心にあり、それを支えるものとして、サイバーセキュリティが必要、との考えに基づく。

（ファイア・アイ　岩間氏）

日本では、「攻め」の取組みを担える IT ネットワーク技術者は比較的多いが、セキュリティの専門家は少数に止まるという印象。

（４）被害情報の共有

（日本銀行　山岡）

各国の事例を見ると、サイバー攻撃の被害者は、レピュテーション等への配慮から、攻撃を受けたことに関する情報や経験の共有に必ずしも積極的でない

事例もあるように思う。サイバー攻撃の被害に関する情報の共有を進める上で、有効と考えられる方策があるかどうか、ご見解を賜りたい。

（経済団体連合会　梶浦氏）

経営者の姿勢が重要。経営幹部が被害状況等を的確に把握できる態勢があることが前提だが、サイバー攻撃により被害を受け、その被害情報を積極的に共有した実際の事例をみても、最後は経営者の「被害情報を共有すべし」との強い意志が重要だったように思う。

（金融情報システムセンター　和田氏）

民間金融機関等で構成され、自由活発な情報交換が行われている金融 ISAC の活用が考えられる。

（ファイア・アイ　岩間氏）

被害企業が責められる風潮が情報共有を妨げているとの指摘があったが、被害を受けた事実ではなく、もっと早く公表できたのに隠蔽しようとしていたのではないか、という企業の姿勢が責められているのではないか。被害情報や自社の取組みを積極的に公表したことで、世間から評価された事例もある。可能な限り早期に多くの情報を公表するといった企業の姿勢が重要。

（５）怠りがち・見落としがちなセキュリティ対策

（日本銀行　山岡）

皆さんがさまざまな実例を見ている中で、「本当は比較的容易に実施できる有効なサイバーセキュリティ対策なのだが、実務においてとかく怠りがち、ないし見落としがち」といった対策があれば、お尋ねしておきたい。

（ファイア・アイ　岩間氏）

システム管理者等は、安定稼働しているシステムに変更を加えること、つまりパッチの適用等を避けたがる傾向があり、そこが攻撃の隙となり得る。面倒だと思わずに、必要なセキュリティ対策に取り組むことが重要。

（金融情報システムセンター　和田氏）

一度作成したセキュリティマニュアルの見直しを怠りがち。運用や外部環境

の変化を捉え、どのタイミングで、どのようにマニュアルの見直しを行うか、見直しの手順も決めておくことが重要。

（経済団体連合会　梶浦氏）

小規模事業者では、セキュリティ対策を IT ベンダーに外部委託する事例が多いが、外部環境の変化に、契約内容が追い付いていない事例が見受けられる。外部委託の際には、契約期間中であっても、その契約内容等について、必要な修正を行うことが重要。

以　　上

（別　添）

参加企業・団体（50 音順）

所属機関名	
オーストラリア・コモンウェルス銀行	東京手形交換所
外国為替円決済制度	日本経済団体連合会
金融情報システムセンター	日本証券業協会
金融庁	日本証券クリアリング機構
クリアストリーム・バンキング・ジャパン	日本取引所グループ
ゴールドマン・サックス証券	日本マルチペイメントネットワーク運営機構
CLS	ニューヨークメロン信託銀行
CD センター	農林中央金庫
JP モルガン・チェース銀行	野村證券
シティグループ証券	ファイア・アイ
シティバンク、エヌ・エイ	ほふりクリアリング
証券保管振替機構	香港上海銀行
スタンダードチャータード銀行	みずほ銀行
全銀電子債権ネットワーク	みずほ証券
全国銀行協会	三井住友銀行
全国銀行資金決済ネットワーク	三井住友信託銀行
大和証券	三菱東京 UFJ 銀行
短期金融市場取引活性化研究会	三菱 UFJ モルガン・スタンレー証券
DTCC データ・レポジトリー・ジャパン	モルガンスタンレーMUFG 証券
ドイツ証券	ユーロクリア・バンク
東京金融取引所	りそな銀行