オープン・イノベーションの推進とセキュリティ確保の両立を目指して

FinTechが世界的規模で加速し、日本においても今後多岐にわたるFinTechの出現が予想される一方で、情報セキュリティに関する課題が指摘されている。このような状況の下、2017年6月に公益財団法人金融情報システムセンターは報告書をまとめ、FinTechにおける安全対策の在り方に関する提言を行った。

多岐にわたるFinTechの出現に向けて必要となる安全対策

近年、金融機関、業界団体及び監督当局において、FinTechと総称されるITを活用した革新的な金融サービスへの取組みが、急速に活発化している。この結果、今後、多岐にわたるFinTechの出現が予想されているが、金融審議会は、今後の情報セキュリティに関する課題として、例えば「従来のように、サービスを提供する側が情報セキュリティ対策の責任を担い、外部とのネットワークを遮断することで情報セキュリティを構築するという手法では、十分な対策が講じられないおそれがある」と指摘している[1)]。また、情報セキュリティに留意したうえで金融機関におけるシステムのAPI[2)]公開について、官民連携して検討する方針も示されている[3)]。したがって、銀行法等の法整備や金融機関等の動向と歩調をあわせて、FinTechに関する安全対策の在り方をあらかじめ検討しておくことが必要と言える。

このような状況の下、公益財団法人金融情報システムセンター（FISC）では、「金融機関におけるFinTechに関する有識者検討会」（座長：岩原紳作早稲田大学大学院教授）[4)]を2016年10月に設置した。わが国金融機関が、FinTechにおいて、システムの安全性を確保しつつも、顧客のニーズに適応しイノベーションの成果を最大限享受しうることを目指して、2017年6月まで検討を行い、同月、報告書を公表した[5)]。

FinTechにおける安全対策の在り方に関する提言

報告書にはFinTechに関する様々な論点が記載されているが、最も重要なのはFinTechにおける安全対策の在り方に関する提言である。具体的には以下の3点となる。

①イノベーションとシステムの安全性を両立させるための原則・ルールの提言
②FinTechに携わる幅広い事業者に向けた意見表明
③重要な情報システムでクラウドサービスを利用する際のリスク管理策の提言

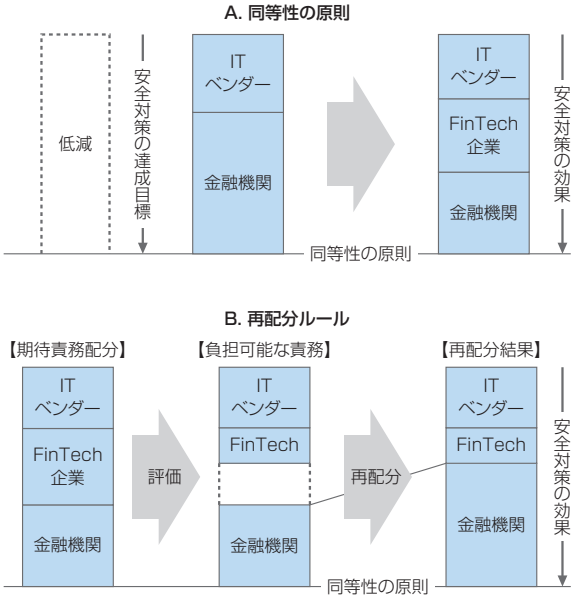
上記①について、有識者検討会においては、従来、金融機関とITベンダーの2者が安全対策を担ってきたところにFinTech企業が加わった場合、どのように安全対策の分担などを考えるべきか等の検討が行われた。その結果、「同等性の原則」、「協調の原則」、「再配分ルール」、「外部委託基準の準用ルール」の4原則・ルールが提言された。このうち「同等性の原則」とは、FinTech企業が新たに加わったとしても、安全対策の効果（総和）は従来と同等に維持されるべきとする考え方である（図表A）。金融機関等では、FinTech企業が加わることで、安全対策を以前より全体として厳しくしなければならないのではないかと考えるかもしれないが、あくまで従来と同等の安全対策を3者で分担する、ということである。また「再配分ルール」は、ベンチャーも含まれるFinTech企業では安全対策遂行能力に不足がある場合も考えられるが、その場合には金融機関等の関係者が補完することを可能とするものである。図表Bは、FinTech企業の対応不足分を金融機関が補っている場合を示している。

そもそも論であるが、FISCが発刊する安全対策基準の適用対象は金融機関であり、FinTech企業等は基準の適用対象外とされる。そこで有識者検討会は、上記②において、FinTech企業等を含む金融関連サービス

NOTE

1) 金融審議会「決済業務等の高度化に関するスタディ・グループ中間整理」18ページ。
http://www.fsa.go.jp/singi/singi_kinyu/tosin/20150428-1.html
2) Application Programming Interface
3) 金融審議会「決済業務等の高度化に関するワーキング・グループ報告～決済高度化に向けた戦略的取組み～」5ページ。
http://www.fsa.go.jp/singi/singi_kinyu/tosin/20151222-2.html
4) 「有識者検討会」とは、わが国金融機関の情報システムの安全対策推進に資することを目的としてFISC理事長の諮問機関として設置し、学識経験者や金融機関、ベンダー等の委員と官庁等のオブザーバーで構成される。検討の成果は報告書として公表するとともに、最終的にはFISC発刊の「金融機関等コンピュータシステムの安全対策基準・解説書」等に反映される。
5) FISC「金融機関におけるFinTechに関する有識者検討会報告書」。
https://www.fisc.or.jp/isolate/?id=917&c=topics&sid=354
6) FISC「API接続チェックリスト（試行版）」。
https://www.fisc.or.jp/isolate/?id=919&c=topics&sid=356

図表　「同等性の原則」と「再配分ルール」



（出所）FISC「金融機関におけるFinTechに関する有識者検討会報告書」

の提供に携わる事業者が、「適切な安全対策を実施し、金融機関や他の事業者と安全対策においても協調を促進し、ルールを形成していくことに努める」という3原則を実施することを期待する「意見表明」を行った。

また上記③では、FinTechではクラウドサービスが利用される場合が多いため、従来のクラウド基準の補足的検討が行われた。重要な情報システムでクラウドサービスが利用される場合を想定して、「統制対象クラウド拠点の把握」、「監査権等の明記」、「監査の実施（保証型監査報告書の利用）」、「監査人等モニタリング人材の配置」の4リスク管理策が提言された。

関係者による協調した取組み

FISCは、報告書の公表とほぼ同時期に、「API接続チェックリスト（試行版）」も公表した[6]。これは金融機関がAPI接続先の適格性を審査する際、両者が効率的にコミュニケーションを行うためのツールとなるものだ。

このチェックリストは、金融機関、FinTech企業、ITベンダーの実務者が検討に参画し、機密性の保持等に関して関係者が共通に確認する項目を中心に60項目を取りまとめている。金融機関が外部委託先モニタリングに使用する一般的なチェックリストとは大きく異なり、個々の「セキュリティ対応目標」に対して豊富な「手法例」を掲載し、業務特性やリスク等を勘案してその中から取捨選択できるよう工夫されている。関係者の判断により他の手法を選択することも可能としている。

また、単にチェック項目について「○」や「×」の回答を形式的に求めるのではなく、「現在の対応状況」や「今後の対応予定」という自由記入欄を用意し、関係者が協調してセキュリティ確保を行うことを促している。仮にある項目に関してAPI接続先からの回答が「×」だったとしても、その評価について金融機関は業務特性やリスク等を踏まえて総合的に判断することを求めている。

日本政府が強力に推し進めるオープン・イノベーションの推進とセキュリティ確保を両立させるためには、立場や意見の違いを乗り越え、協調して事に当たることが、金融機関を始めとしたすべての関係者に求められているのではないだろうか。

Writer's Profile

大澤 英季 Hideki Osawa
金融情報システムセンター
企画部次長
専門は内部統制、リスク管理
focus@nri.co.jp