「オープン API のあり方に関する検討会」（第４回）議事要旨

１．日　時： 平成 28 年 12 月 16 日（金）14 時 00 分 ～ 15 時 15 分
２．議　題： セキュリティ対策・利用者保護について
３．議事内容：

※ 討議対象となっている「オープン API におけるセキュリティ対策・利用者保護に関する基本的な考え方」については、取りまとめが終わった段階で公表等を行う予定です。

【全般】

- 金融機関が、特定の企業に対してとはいえ、インターネット上で API を開放するということは、ある意味でインターネット上のプロトコルの一種を銀行が提供するということと理解される。世の中に存在する様々なインターネット・プロトコルには脆弱性がある場合があり、その場合には、脆弱性を報告する仕組みが設けられている。仮に、ある金融機関が提供した API に何らかの脆弱性があった場合には、それについても通報する仕組みとなっていた方がよいと思う。

- セキュリティ対策を強化する必要性は理解しているが、その結果としてユーザビリティが低下してしまって、それが、ユーザーがインターネット・バンキングを使わないことにつながってしまっている。利便性と安全性のトレードオフの問題というものが常にあって、その間の判断をどこに置くかという議論が各企業においてなされていると思う。金融機関はできるだけ安全な方へ倒してきたという経緯があるが、そこのカルチャーが FinTech 企業の提供される UI/UX によって変わるかもしれない。金融機関のモニタリングやチェックにおいても個々のケースを踏まえて判断されることが望ましい。

【運用上の負担軽減】

- 「基本的な考え方」は、モニタリングを各銀行において行うことを前提とした枠組みであるが、例えば、API 接続先がモニタリングを受ける銀行が 200 にも、300 にもなるということだとすると、モニタリング負担が非常に大きくなるのではないかと思う。モニタリング負担の緩和という観点からは、例えばチェックリストを用意することも記載いただいているが、場合によっては、シンジケートチェックのようなかたちで、どこかの銀行が代表してチェックするような枠組みもあってもよいのではないか。

- シンジケート型のように、重複する作業を誰かが一元的に担うことで運用負荷を下げるというのはベストな解決方法だと思う。もちろん最終的な責任の所在に関する問題は常にあるため、他行の判断に完全に依拠することはでき

ないと思うが、実態としては銀行間でも横を見ながら判断されている部分もあると思うので、それを枠組みとしてもしっかりと活用することもあってよいのではないかと考えている。

- オープン API では、登場人物が金融機関と IT ベンダーの２者から、FinTech 企業を加えて３者になる。３者になっても安全対策の効果は同程度であるべきという前提のもとで、仮に FinTech 企業の実務負担が大きいということであれば、責務を金融機関、IT ベンダー、FinTech 企業の三者で再配分して、全体としてセキュリティ水準を確保する方法もある。

【API 接続連鎖の取扱い】

- FinTech 企業は､取得した情報に何か付加価値を付けて API 連鎖先に提供しているケースがほとんどだと思う。これは利用者の同意にもとづいて行われるものであるため､（銀行ではなく）FinTech 企業と FinTech 企業の連携という意識がユーザーにも十分あるのではないかと思う。

【利用者に対する補償内容・範囲】

- オープン API における利用者に対する補償内容・範囲については、インターネット・バンキングにおいて使われている申し合わせの表現を出発点に記述されており、比較的受け入れられやすいのではないか。

- 「基本的な考え方」における補償内容・範囲に関する考え方の方向性については、異論ない。法人の利用者に対する補償の要否については、個別に判断いただくということでよいと思うが、法人を一括りにするのではなく、どのような法人なら、どのような補償の範囲というようなところを、もう一段深いレベルで議論していただければと思う。

以　上