「オープン API のあり方に関する検討会」（第５回）議事要旨

１．日　時： 平成 28 年 12 月 21 日（水）14 時 00 分 ～ 16 時 00 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：

※ 第５回討議およびその後の委員からのコメントを踏まえた「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方」の中間的な整理（案）は、添付ファイルをご参照。

【全般】

- 「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方」（以下「基本的な考え方」という。）は、事務局、銀行界および FinTech 業界が大変な苦労をされて取りまとめられたと思っており、敬意を表したい。ルールというと、すぐにイノベーションを阻害するのではないかという話になるが、共通の理解に至ったことは、非常によかったと感じている。他方、やはり、技術というものは日々変わっていくであろうし、また、実務を進めていく中で、場合によっては、今回の案の中では考えが及んでいなかったことが出てくることもあろうかと思う。そうした点については、銀行界と FinTech 業界との間で、今後も継続的に見直し、あるいは議論を重ねていけるようにしてはどうか。

- 「基本的な考え方」は、これまでの議論が十分に反映されていると考えており、賛同したい。どちらか一方のスタンダードに合わせるというのではなく、これからもお互いに見習い合いながらベストプラクティスを模索し、Win-Win-Win の関係を構築していくことが重要だと考えている。

- FinTech 各社から、運用面での効率化に関する要望があった。確かに１対１の関係でなく、マルチバンクで接続するパターンを考えた場合には、効率化を検討する必要が出てくると思う。効率化の方法は、実務的には様々な方法が考えられる。可能な範囲で契約書のひな型を共有させていただくことや、業務フローや障害の連絡方法などについて既存の接続銀行と定めているやり方を踏まえて検討していくなど、様々な方法があると思う。そうした点は、個別に連携する際に是非可能な範囲で共有をさせていただければと思う。

- 事務局が取りまとめられた「基本的な考え方」の案については、違和感ない。情報セキュリティ機関に今後期待されると記載されている箇所がいくつかあると思うので、これらについては、対応を検討していく。

【API 接続連鎖の取扱い】

- 相当論点が集約されてきたと感じる。「API 接続先の API 接続先」を「API 連鎖接続先」と呼んで取扱いを定めているが、API 接続先の API 接続先といっても、様々なものが考えられる。セキュリティ対策・利用者保護の枠組みの対象かどうかはっきりさせるためにも、「API 連鎖接続先」の定義を追記しておいた方がよいのではないかと思う。

- 米国と日本の API 連鎖はやや異なる点がある。ユーザーから見たインフォームドコンセントの観点では、日本は、米国の事例に比べれば、相当程度、一次連鎖先にユーザーの意識がある。難しいのは、(API 接続していること自体は同じであるため) このケースと、米国のように二次連鎖先の方が色濃く見えるようなケースとをどう区別するかということだと思う。

- API 連鎖接続先の取扱いについては、様々なバリエーションがあると伺った。「基本的な考え方」の中でも、対お客さまとの関係でどうしても伝えておかなければならないルールと、お客さまとの関係ではないが、システムとして必ず守っていただく必要があるルールの２通りがあると思う。特に前者については、API 連鎖接続先にもしっかりと守っていただけなければ、この原則が骨抜きになってしまうような性格のものだと思う。そういった視点で、API 連鎖接続先の取扱いや定義を整理していけばよいのではないか。

【認証水準】

- 生体認証や端末認証も「同水準以上の強度」であれば認められるという表現が出てくるが、セキュリティの強度は、なかなか一次元で測れるものではないため、ある認証方式と別の認証方式でどちらが強いか、弱いかについては、一般論としては何とも言えないのではないか。

- アメリカの地銀では、たいてい Touch ID で口座の中身までは閲覧できるようになっており、振込を行う場合にだけ追加的な認証を行うことが一般的。銀行のインターネットバンキングにおいても、参照系と更新系とでは、リスクベースで異なる認証が行われていると理解しており、日本の銀行でも最近、端末の認証情報を利用して、アプリ開いたらすぐに中身が見えるものも登場している。こうした趨勢に合わせて今後議論をアップデートしていくということではないかと思う。

【今後の対応】

- 消費者としてお願いしたいのは、スクレイピングから早く API に移行を促さなければいけないということである。移行を促していくためには、スクレイピングの方が利用者にとって楽だとか負担が小さいというようなことがあってはいけなくて、オープン API も品質がよく、ストレスも同等位でお願いし

たいと思う。
私もスマホを日々使っているが、出てくる言葉にはカタカナが多く、全然意味が分からず、止まってそれ以上、操作しないということが多々ある。銀行もリスクの説明をしっかりされたいとは思うが、消費者が全部リスクを理解することは難しく、また、スマホやタブレットはそのような情報の提供にそぐわないため、できれば、「これは絶対にやってはいけません」というところを前面に出していただいて、私達に教えていただければと思う。

以　　上