平成 29 年２月２日
公益財団法人　金融情報システムセンター

第３回　金融機関における FinTech に関する有識者検討会　議事次第

Ⅰ　日時
平成 29 年２月２日（木）　15:45～17:45

Ⅱ　場所
FISC 会議室

Ⅲ　議事次第

１．	15:45	開会
２．		事務連絡等
３．	15:50	【議事１】第２回 FinTech 有識者検討会に対するご意見及びご回答
４．	16:10	【議事２】プレゼン（一般社団法人全国銀行協会） 「オープン API のあり方に関する全銀協の検討状況」
５．	16:25	【議事３】API接続先チェックリスト（仮称）ワーキンググループの設置
６．	16:40	【議事４】論点メモ 「クラウドサービス利用時のリスク管理策に関する補足的検討」
７．	17:35	事務連絡
８．	17:45	閉会

Ⅳ　資料

【資料１】	第３回 FinTech 有識者検討会　座席表
【議事１】	第２回 FinTech 有識者検討会に対するご意見及びご回答
（参考資料１）	安対基準の対象外となる FinTech 業務の取扱い （第２回【議事４】別紙１の修正案）
（参考資料２）	金融機関における FinTech に関する安全対策検討の在り方 （第１回【議事３】別紙１の修正案）
（参考資料３）	FinTech に関する安対基準適用上の課題 （第２回【議事３】別紙１の修正案）
【議事２】	プレゼン資料「オープン API のあり方に関する全銀協の検討状況」
（参考資料４）	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【中間的な整理(案)】
【議事３】	API 接続先チェックリスト（仮称）ワーキンググループの設置
【議事４】	論点メモ「クラウドサービス利用時のリスク管理策に関する補足的検討」

Ⅴ　連絡事項
ご意見等あれば、電子メール＜fintech@fisc.or.jp＞にお送りください。
（送付期限　２月９日(木)　17 時）

Ⅵ　次回の開催予定
第４回　金融機関における FinTech に関する有識者検討会
（予定）平成 29 年３月 23 日（木）15:45～17:45　FISC 会議室

以上

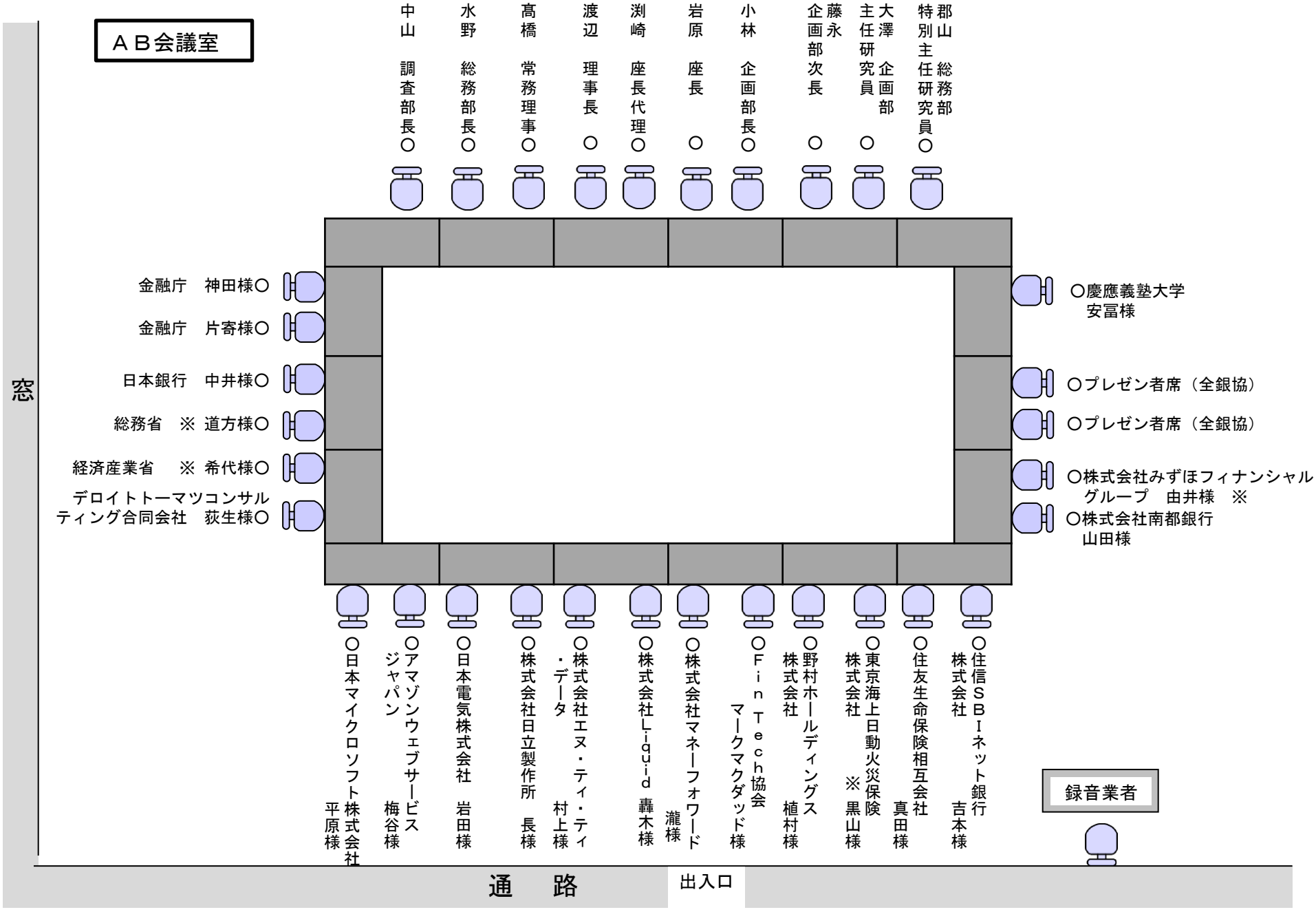
【資料１】

第３回金融機関におけるFinTechに関する有識者検討会　座席表

平成29年２月２日

※代理出席

ＡＢ会議室



議事１　第２回 FinTech 有識者検討会に対するご意見およびご回答

No	対象箇所	検討会後に頂いたご意見	事務局回答	ご意見元
1	議事１ 「第１回FinTech有識者検討会に対するご意見及びご回答」	スクレイピングはセキュリティ上の改善があるべき技術という認識はコンセンサスがあるものかと思います。しかし、こちらが昨今急に（禁止的な文脈を含めて）リスクが高くなったとする判断は、不確実性をもたらすものと考えております。 順当な技術的理解のもとに、議論が行われていくことを望んでおります。	ご指摘を踏まえ、本検討会第１回の議事「金融機関におけるFinTechに関する安全対策検討の在り方」別紙１脚注11に以下のとおり補足いたします。 ＜補足＞ なお、これは、スクリーンスクレイピングが採用されていることをもって直ちに問題がある訳ではなく、本来的には金融機関と交渉なく顧客に関するデータが取得されることが問題である点に留意が必要である。	株式会社マネーフォワード瀧様
2	議事３ 「FinTechに関する安対基準適用上の課題」	現状、全国銀行協会での「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」の素案では、API接続先企業の事前審査につき、ある程度汎用的なチェックリストを作る試みへの言及があります。これは個別の企業にとっても対応負荷を下げる良い取り組みと考えております。 Fintechの領域ごとにテンプレートは異なっていくものと考えておりますが、タイプⅢでは多数の金融機関にサービス提供するようなケースが多いため、テンプレートを作成していくような動きを促進できる表現を加えて頂くことを検討していただきたく存じます。	ご指摘もふまえ、本検討会第２回の議事「安対基準の対象外となるFinTech業務の取扱い」別紙１に「４．社会的に合意されたルールの形成に向けたFISCの役割」として補足いたします。	株式会社マネーフォワード瀧様

議事１　（参考資料１）　第２回【議事４】別紙１の修正案

別紙１

安対基準の対象外となる FinTech 業務の取扱い

１．安対基準における従来の対象の取扱い

安対基準の対象となる情報システムは、金融業務を担う情報システムであり、かつ、その安全対策について金融機関等に責任が生じる情報システムである。これは、簡単に言えば、「金融機関が行う金融業務」を担う情報システムである。したがって、「金融機関が行う非金融業務」、「非金融機関が行う金融業務」、もしくは「非金融機関が行う非金融業務」、を担う情報システムは、安対基準の直接的な対象とはならない。

ただし、「金融機関が行う非金融業務」を担う情報システムについては、同一金融機関の運営する情報システムであり、かつ、「安全対策に係る方針」のもとで、共通する安全対策も多いと想定されることから、金融業務の性質を前提とした安対基準をそのまま全面的に「適用」することは適切でないとしても、安対基準のうち非金融業務を担う情報システムの安全対策においても有益な部分については「参考」とする、すなわち、金融機関の業務の実態に即して適宜取り入れることが望ましい、という考え方に立っている。

一方、「非金融機関の行う金融業務」（例えば非金融機関が行う資金決済法上の前払い式支払手段や資金移動といった業務）は、「金融機関の行う金融業務」と機能的に類似する部分があり、安対基準の安全対策が部分的に有益となることは否定できないにしても、以下の経緯から、その業務を担う情報システムは対象とされていないとするのが、従来からの考え方である。

・安対基準は、FISC 会員によって策定される自主基準である。一般的に、自主基準とは、「国家等によって明確に規定され、裁判所などを通じて強制的に執行される法律」（ハードロー）と異なり、「私的な取決めや申し合わせ」（ソフトロー）[1]の一種であり、その社会的規範性は、自主基準の策定過程に明示的に参画した当事者においてのみ生ずるものと解される。安対基準はその会員である金融情報システムを担う当事者[2]の中でも金融機関を中心に策定されており、その策定過程[3]に「金融業務を行う非金融機関」の業界代表等は、必ずしも明示的に参画していない。そのため、そうした非金融機関を、一方的に安対基準の適用対象とすることには無理がある。

・安対基準は、金融庁の検査マニュアル等において言及されることにより、FISC 会員の枠を超えて、金融庁監督下の金融機関が、事実上適用対象とされているが、その範囲を超えて、金融庁監督下に無い非金融機関まで適用対象とすることには無理がある。

---

1 ソフトローとハードローの説明については、中山信弘編集代表『ソフトローの基礎理論』中の第３部第１章瀬下博之『ソフトローとハードロー』から引用。

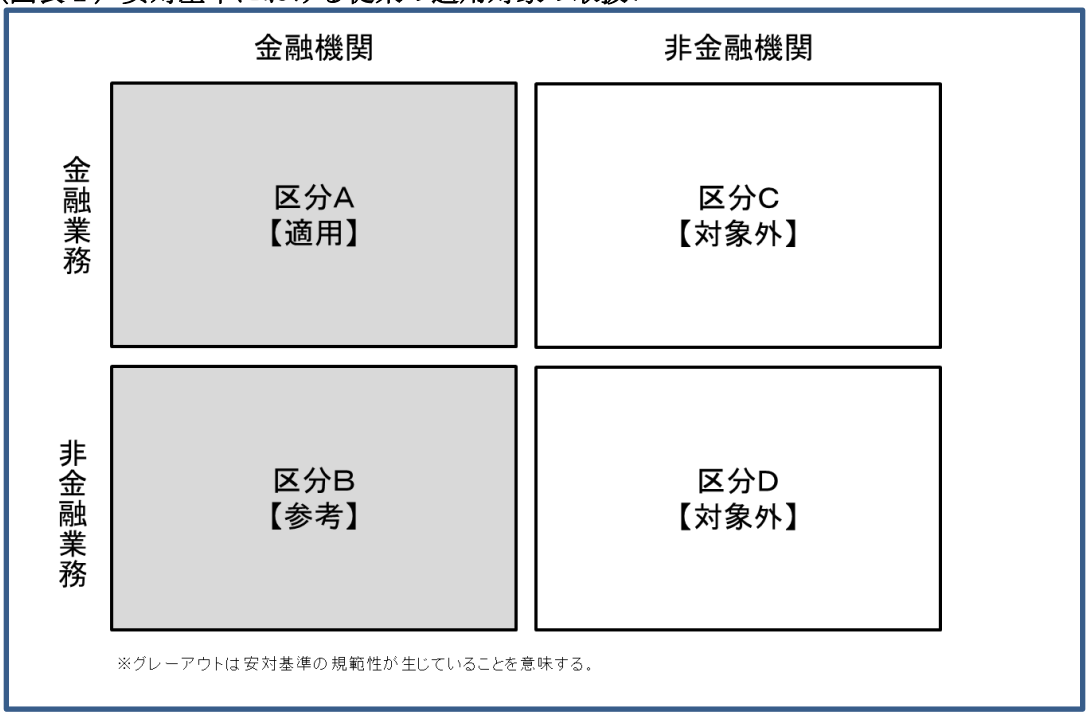
2 平成 28 年９月末現在、FISC 会員数 645 社のうち金融機関は 543 社と、その 84%を占める。

3 安対基準は FISC 会員代表者を中心に構成される安全対策専門委員会とその下部組織である安全対策基準改訂に関する検討部会で検討を行った後、会員への意見募集を経て策定される。

なお、「非金融機関の非金融業務」を担う情報システムは、安対基準の対象と考えられたことはない。

以上の考え方を図表にすると以下のとおり。

（図表１）安対基準における従来の適用対象の取扱い



２．安対基準の対象外となる FinTech 業務の取扱いの方向性

FinTech と総称される金融関連サービスは多岐にわたるとともに、今後も新しいテクノロジーあるいは新しいビジネスモデルの登場が予想される中では、そうした状況を踏まえて、FinTech 業務の安対基準における取扱いについて、本検討会において、あらかじめ整理しておくことが期待されている。

一般的に、金融機関と非金融機関は、業法等の法規制に基づいて主体が特定され、比較的対象が明確であるのに対して、FinTech と総称される金融関連サービスにおいては、金融業務と非金融業務の境界が比較的曖昧となるという特徴があるとされている[4]ことから、例えばその機能面に着目して、個別具体的に業務を特定することで、金融業務と非金融業務の区分の境界を明確にするというアプローチが考えられる。

しかしながら、このアプローチにおいても、多岐にわたるサービスが登場する中で、あらかじめ業務を個々に特定することは困難であり、また、仮に境界が明確にできたとしても、業務の機能面では大差が無いにも関わらず、安対基準上の取扱が異なることとなり、

4 例えば、増島雅和／堀天子編著『FinTech の法律』において、「FinTech による業界構造や事業モデルの変化は、金融の業態間の壁を融解するだけでなく、金融と非金融の間の壁をも溶かすことにつながる。」とされている。

その FinTech 業務の取扱いの適切性に疑義が生ずることが危惧される。

本来、利用者の立場に立てば、金融業務であるか否かは一義的な問題ではなく、また、金融機関と非金融機関のいずれが行う場合においても、FinTech 業務全体において、シームレスに一体不可分な形で、適切な安全対策が実施されることが期待されている、と考えられる。

したがって、こうした社会的期待に応えるためには、まず、我が国の金融機関が、従来からその業務において培ってきた社会的な信頼と、類似の信頼を FinTech 業務においても得ることが有益である。特に、情報システムにおける社会的信頼が形成されるにあたっては、社会的に合意されたルールである安対基準が役割として担ってきた一面があることから、多様な FinTech 業務の実態を所与の前提としたうえで、金融機関と非金融機関に関わらず、それらの業務の担い手において、如何に安対基準の社会的規範性が生じることが可能か、という観点から、整理することが有益である。

（1）区分 B の取扱いの方向性

まず、本区分においては、従来から安対基準は「参考」という形で言及されてきており、金融機関の実態においても、セキュリティポリシーやセキュリティスタンダードにおいて、安対基準等の FISC のガイドラインが取り入れられ、金融業務と非金融業務に対して、一体的に安全対策が実施されているケースが多い[5]。

したがって、FinTech 業務のうち、非金融業務とみなされる業務があった場合においても、FinTech に関する安対基準が整備されれば、従来どおり、これらの基準を「参考」として、安全対策が実施されることとなり、特段新たに検討すべき問題はない。

（2）区分 C・D の取扱いの方向性

本区分は、FinTech 業務のうち非金融機関が行う金融業務としては、例えば、FinTech 企業が主導する個人財務管理業務等の金融関連サービスや、米国で行われている P2P レンディング等がこれに含まれる。

本区分で安対基準における取扱いを検討するにあたっては、行政による制度変更を前提としないで考えるとすれば、非金融機関においても、安対基準の規範性が及んでいることが、利用者から安全対策上の信頼を得るためにも、期待される。

こうした規範性を生ずるには、次のふたつの方法が考えられる。

---

[5] 安対基準の「Ⅰ．安全対策基準の考え方」において、「全社で統一された情報の取扱いがなされるよう、セキュリティポリシーの策定が必要となっている。」とされている。また、「各金融機関等は、コンピュータシステムの利用状況、直面するリスクの種類と大きさ、保護すべき情報の重要性や、自社の規模・特性に応じたセキュリティスタンダード（自社の安対基準）を、自社のセキュリティポリシー（基本方針）に準拠しつつ、本基準を参考の上で策定し、実施することが必要である。」とされている。

①直接的に規範性が生ずる方法

非金融機関である FinTech 企業が個別に FISC の会員となり、安対基準の策定過程に明示的に参画するとともに、FinTech の観点からその基準策定に貢献するとともに、安対基準を遵守する。

②間接的に規範性が生ずる方法

FinTech 企業の業界団体が FISC 会員となり、業界団体が代表して、安対基準の策定過程に明示的に参画するとともに、FinTech 業界の観点からその基準策定に貢献する。また、安対基準と整合的な FinTech 業界の自主基準を策定し、業界団体の会員がそれを遵守する。

まず①については、既に、FISC の会員となっている FinTech 企業があり、今後、安対基準の策定過程に参画することが期待できる。また、②については、既に、FISC 会員となっている業界団体があり、本検討会にも委員として検討に参画いただいているところである。さらに、この業界団体においては、安全対策に関する自主基準の策定が予定されており、安対基準を参考としながら、業界団体の特性に応じた観点も反映させつつ、検討が進められている状況にある。

こうした取り組みが進み、安対基準の規範性が、FISC の会員となった FinTech 企業や業界団体に及ぶことができれば、その結果として、金融機関と非金融機関に関わらず、FinTech と総称される金融関連サービス全般において、シームレスに一体不可分な形で、適切な安全対策が実施されることが期待できる。

ただし、業界団体の自主基準が安対基準と整合的な内容となるか否かは、最終的にその業界団体の検討に委ねられることとなるとともに、必ずしも FISC の会員とならない FinTech 企業や業界団体も存在しうることから、そうしたことを踏まえて、本検討会として、何らかの意見表明を行うことが妥当である。

３．FinTech 業務における安全対策に関する意見表明

以上のことを踏まえて、FinTech 業務全般における安全対策に関して、以下の意見表明を行う。

【意見表明】

「金融機関における FinTech に関する有識者検討会」は、FinTech 業務を実施するのが金融機関であるか否かに関わらず、FinTech 業務を担う情報システムにおける安全対策の在り方について、高い関心を持っている。そうしたことから、FinTech 業務に携わる事業者においては、本検討会が策定する以下の「金融関連サービスの提供に携わる事業者を対象とした原則[6]」を踏まえたうえで、適切な安全対策が実施されることを期待する。

（１）金融関連サービスの提供に携わる事業者は、その利用者が安心してサービスを利用できることを目指し、自らが管理責任を負う情報システムに対して、適切な安全対策を実施する。

（２）金融関連サービスの提供に携わる事業者は、安全対策の実施にあたっては、イノベーションの成果が利用者の利便性向上に資するよう留意するとともに、金融機関とその他事業者がそれぞれ独自の優位性を活かせることを目指し、安全対策においても協調が促進されるよう留意する。

（３）金融関連サービスの提供に携わる事業者は、互いに協調して安全対策を実施するに際し、FISC 安対基準を含め、安全対策に関して社会的に合意されたルールが形成されるよう努める。

（１）

金融関連サービスの提供に携わる事業者として、金融機関や IT ベンダーに留まらず、FinTech 企業等多岐にわたる事業者が想定される。そうした事業者は、企業価値の最大化のためにも、金融関連サービスにおいては、何より利用者が安心して利用できることが重要であり、そのためには、サービスの提供に必要となる情報システムに対して、何ら安全対策を実施しない、ということは適切ではない。

（２）

FinTech に見られるとおり、金融関連サービスにおけるイノベーションには目覚ましいも

[6] FISC『外部委託検討会報告書』において提言された「安全対策における基本原則」が、主に FISC 会員を対象とした基本原則であるのに対して、「金融関連サービスの提供に携わる事業者を対象とした原則」は、「安全対策における基本原則」をもとにしつつ、より幅広く金融関連サービスの提供に携わる事業者全般を対象とした原則である。

のがあり、特に革新的なユーザー体験の提供などを通じて利用者の利便性向上に資することから、その利用が進んでいる状況にある。したがって、安全対策の実施にあたっては、イノベーションを阻害することが無いよう留意されるべきである。

また、金融機関において、オープンイノベーションが進められる中で、金融関連サービスの提供に、従来以上に複数の事業者が、多段階にわたり重層的に携わることも予想される。このように、事業者の関係が複雑になる中においても、複数の事業者が協調してサービスに携わることで、相互の優位性を取り込むことが可能となる。したがって、安全対策においても、互いに協調して取り組まれるべきである。

（３）

金融情報システムの安全対策については、金融機関等による自主基準である公益財団法人金融情報システムセンター「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」（以下「安対基準」という）をはじめとして、社会的に合意されたルールが存在する。例えば安対基準においては、その策定過程に、金融業務や情報システムに係る業界の代表者等専門的・技術的知見を有する関係者が携わるとともに、金融情報システムの安全対策に責任を負い、安全対策の実施を現場で担う関係者が自主的に参画していることに特徴がある。【参考１参照】

金融関連サービスに携わる事業者においては、社会的に合意されたルールが形成されるよう努めるとともに、こうしたルールと整合する安全対策が実施されることが望ましい。

４．社会的に合意されたルールの形成に向けた FISC の役割

従来、金融情報システムの主たる関係者は、金融機関等と IT ベンダーからなり、ほぼ FISC の会員となっていることから、安対基準に、金融情報システムの担い手の意向や特性を十分に反映することが可能である。その結果、金融情報システムにおいて必要となる安全対策については、安対基準で概ね確認することができる。

しかしながら、今後、オープンイノベーションの進展に伴い、従来以上に複数の事業者が金融関連サービスの提供に携わることが予想される中で、必ずしも、FISC の会員とならない事業者も想定され、その場合には、安対基準に全ての事業者の意向や特性を十分に反映することが容易ではなくなることが予想される。

また、各事業者が、自らのために独自に自主基準を策定することが考えられるが、仮に安対基準と何ら関係なく自主基準が策定されれば、金融関連サービスであるにもかかわらず、異なるルールが適用・運用されることとなる。

以上の、今後発生が予想される問題に対しては、FISC としても社会的な役割を果たしていくことが必要である。例えば、金融関連サービスの提供に携わる事業者の業界団体において、独自の自主基準が検討されていれば、FISC は、その検討に参画し、社会的に合意されたルール形成に向けて必要となる支援を行い、基準相互の整合性が確保されるよう努め

ていく[7]。

社会的に合意されたルールの形成にあたっては、FISC が策定を予定している「必要最低限の安対基準」に着目することが有益である。金融業務を担う情報システムにおいて最低限実施されるべき基準として策定される「必要最低限の安対基準」は、FISC 会員に限らず、金融関連サービスの提供に携わる事業者においても、踏まえられるべき基準であると考えられる。

以上

[7] 既に行われている自主基準策定の取組みとして、銀行業界においては、全国銀行協会が事務局として、「オープン API のあり方に関する検討会」が設置され、銀行業界の意向や特性を反映させた独自基準に関する検討が進められている。FISC は、その検討会に参画するとともに、そこで言及されている「API 接続先チェックリスト」（仮称）の制定に関して、事務局として支援を行っている。また、FinTech 企業の業界団体である FinTech 協会においても、協会の自主基準策定作業が進められているが、FISC はその検討に参画し、安対基準の解説等の支援も行っている。

参考１

金融機械化財団[8]（仮称）設立趣意書（抜粋）

昭和 59 年 9 月

趣　　旨

金融システムの機械化は、近年急速な展開を見せていますが、これは将来、金融機関の経営、金融業界とその他の業界との関係、ひいては我が国信用秩序に対して大きくかつ複雑な影響を与えることが予想されます。

特に、金融システムは、あらゆる経済部門の活動に必ず伴う資金決済の機能を有しており、また、金融機関と金融機関以外の第三者との間をオンラインで結ぶ第三次オンラインシステムの構築が急速に進みつつあることにかんがみれば、金融機械化システムの円滑な発展を図るため、安全性確保の問題も含め金融システムの機械化全般に関する諸問題を早急に解決し、これを着実に実行していくことが必要であると考えられます。

こうした問題については関係する業界が多岐にわたっているので、検討を行うに際しては、金融機関、保険会社、証券会社、ハード・ソフトメーカー、電気通信事業者、中央銀行、行政当局等の関係者の協力が不可欠であると考えられます。すなわち、これら関係者の十分な意思疎通の下に、知識、経験、情報等を集約することにより、安全性確保のための諸施策を推進するとともに、的確な企画・立案、開発、実施などを進めていく必要があると思われます。

このような見地から、金融機械化システムに係る諸問題を効率的かつ弾力的に処理していくことを目的として、上記関係者の参加する民間出資の第三者的中立機関を創設し、民間活力発揮のため環境整備を図っていくことが適当であると考えます。

各位には、上記の趣旨にご賛同いただき、なにぶんのご協力を賜わるようお願い申しあげる次第であります。

事業内容

（１）　金融機械化システムに係る金融取引、法律関係、投資、受益者負担、国際関係等に関する企画、調査及び研究。

（２）　金融機械化システムに係る障害・犯罪発生状況の把握・開示、安全基準の策定等による安全対策の推進。

（３）　金融機械化システムに係る共同事業の調査・研究、金融機械化システムに係る斡旋・媒介、システム監査、研修・セミナー・広報等の実施。

（下線は FISC にて付す）

[8] 「金融機械化財団」とは FISC の設立準備段階の呼称。昭和 58 年９月大蔵省銀行局長の私的懇談会として設置された「金融機械化懇談会」の報告書「金融機械化システムの安全対策」において「ある程度公的な性格を持った中立的な機関ないしは組織の創設」「金融機関、メーカー、行政当局等の専門的・技術的知識を有する関係者が参加する場」が提言されたことを受けて、昭和 59 年９月「金融機械化財団（仮称）設立準備室」が設置された。その後、正式な組織名称を「金融情報システムセンター」とし、金融機関や IT ベンダー等からの 40 名の出向職員とプロパー職員をあわせて総勢約 50 名で、昭和 59 年 11 月から、業務が開始された。なお、３０年以上を経た現在も、当時と同程度の出向職員 39 名を含む総勢 54 名（平成 28 年 11 月１日現在）で運営されている。

議事１（参考資料２） 第１回【議事３】別紙１の修正案

別紙１

金融機関における FinTech に関する安全対策検討の在り方

近年、金融機関、業界団体および監督当局等において、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[1]。

こうした取り組みの活発化の結果として、今後、多岐にわたる FinTech の出現が、予想される中、FISC においても、金融機関等の動きと歩調をあわせて、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期待されている。

１． 検討の手順

まず、FinTech と総称される金融サービスに係る諸業務（以下、「FinTech 業務」という）は多岐にわたることから、そうした業務を担う情報システムが、安対基準[2]の対象となるかどうか（あるいは対象とすべきかどうか）、その判別を行うための基準が必要となる。

次に、安対基準の対象となる FinTech 業務を担う情報システムに安対基準を適用するにあたって、どのような付加的検討がなされるべきか、を検討することが必要となる。

FinTech 業務を担う情報システムが、重大な外部性を有する情報システムおよび機微情報を保有する情報システム等（以下「重要な情報システム」という）に該当する場合は、安全対策における基本原則に従って、社会的・公共的観点から、その安全対策の達成目標の設定にあたっては、「高い安対基準」の適用を求めることとなる。そのため、重要な情報システムで使用される FinTech に係るテクノロジー等が、これまで安対基準で前提とされていない新たな性質を有している場合には、それを「高い安対基準」に反映する必要がある。

一方、FinTech 業務を担う情報システムが、重要な情報システム以外の情報システム（以下「一般の情報システム」という）である場合は、十全なリスクベースアプローチを採用する金融機関においては、独自にその安全対策の達成目標を設定することが可能となることから、本検討会において、達成目標等について、特段の検討は不要である。

簡易なリスクベースアプローチを採用した金融機関においては、一般の情報システムに対しては、「必要最低限の安対基準」が定められていれば、それを安全対策の達成目標として設定することとなるが、それが明確でない場合は、「高い安対基準」を適用せざるをえない。「必要最低限の安対基準」の前提となる簡易なリスク管理策については、これまでの有識者検討会において「クラウドサービス利用」、「外部委託」について、それぞれの安全対策の在り方を踏まえて提言が行われており、一律に「高い安対基準」が適用されることが無いよう取組みが進んでいるところであるが、FinTech 業務を担う情報システムにおいても、そうした簡易なリスク管理策について検討を行い、安対基準の不確実性を低減する必要が

[1] 2016 年第３四半期の金融機関による FinTech に関するプレスリリースが、対前年同期比で約 7 倍に増加している。また、金融庁においても、金融審議会『金融制度ワーキング・グループ』をはじめとして、FinTech を取り上げた検討が複数行われている。さらに、全国銀行協会においても、FinTech に関連した研究会が開始されている。

[2] FISC『金融機関等のコンピュータシステムの安全対策基準・解説書』の略。ここでは、現行の第８版及び第８版追補改訂だけでなく、「金融機関における外部委託に関する有識者検討会」（以下「外部委託検討会」という）の成果も含むものとして使用する。

ある。

そのために、まず、従来の安対基準で必ずしも想定されていなかった事項を明らかにするとともに、検討するにあたっての前提を整理する。そのうえで、FinTech に関する安全対策の在り方およびそのリスク管理策について、検討することとしたい。

２．安対基準の対象となる情報システムの判別基準

安対基準は、３０年以上前に策定されたその初版から一貫して「金融機関等[3]のコンピュータシステム」をその対象としてきた。「金融機関等のコンピュータシステム」とは、すなわち、金融業務を担う情報システムであり、かつ、その安全対策について金融機関等に責任が生じる情報システムのことをいう。

したがって、FinTech 業務を担う情報システムのうち、安対基準の対象となるのは、その FinTech 業務が金融業務であり、かつ、その安全対策について金融機関等に責任が生ずる情報システムである。

金融業務とは、金融機関等の業法等に基づいて、金融機関等が顧客に対して提供する金融サービスに係る業務である。したがって、顧客に対して提供するサービスであっても、例えば、商品等の売買を目的とする電子商取引業務を担う情報システムは、金融サービスに係る業務を担う情報システムとは解されないことから、安対基準の対象とはならない。また、金融機関等の内部のみで利用される情報システム（例：人事給与システム、経営情報システム等）は、安対基準の対象とはならない[4]。

一方、金融機関等以外の事業者が、金融機関等あるいは金融機関等の顧客と何ら関係なく、自らのサービス利用者のために行う FinTech 業務は、金融機関等に何ら安全対策上の責任が生じないことから、その情報システムは安対基準の対象とはならない。

---

[3] FISC 安対基準では初版（昭和 60 年 12 月）以来「金融、保険、証券、クレジット等金融業務を営む業界の各社」と表記されている。

[4] FISC 安対基準初版では「本基準は金融機関等が顧客に提供するサービスに関連するシステムを前提にしている。しかしながら、金融機関等の内部のみに利用されるシステムについても、安全対策上参考となる部分について、本基準を適宜取り入れることとする。」とされており、現在まで、その考え方が基本的には踏襲されている。

３．重要な情報システムで利用される FinTech に係るテクノロジー等の取扱い

重要な情報システムでの利用が想定される FinTech に係るテクノロジー等として、ブロックチェーン技術や AI[5]が考えられる。

検討にあたっては、これらの要素技術は、それを用いた業務の事例（ユースケース）は幅広いと考えられることから、それぞれのユースケースに応じた技術的特性に着目して、検討を進める必要がある。

もっとも、現状では、重要な情報システムにおけるユースケースが出現していないことから、直ちに検討を行うのではなく、今後のユースケースの出現状況等をにらみながら、検討が可能となる時期を確定させていくこととする。

[5] 人工知能。Artificial Inteligence の略。

４．FinTech に関する安全対策の在り方を検討するにあたっての前提

FinTech に関する安全対策の在り方およびリスク管理策を検討するにあたって、まず、従来の安対基準で必ずしも想定されていなかった事項を明らかにしたうえで、検討を進めるにあたっての前提を整理することが望ましい。

（１）従来の安対基準で必ずしも想定されていなかった事項

①安全対策実施上の新たな関係者となる FinTech 企業の登場

安対基準では、金融情報システムにおける安全対策実施上の関係者として、金融機関に加えて、情報システムの開発・運用といった技術的役割を担う委託先である IT ベンダー[6]の２者を念頭におき、策定されてきた。

しかしながら、FinTech 業務を担う企業は、IT ベンダーと類似の技術的な性質を有するとともに、金融関連サービスといったビジネスモデルの企画実施等を行う業務的な性質もあわせて有しており、こうした技術的な性質と業務的な性質[7]を同時に有する関係者は、従来の安対基準では、必ずしも明確に想定されてはいなかった。

したがって、安対基準を FinTech 業務に適用した場合に内在する問題を明らかにするにあたっては、金融機関、IT ベンダーに FinTech 企業を加えた３者関係を整理する必要がある。これにより、新たに登場した FinTech 企業等が果たすべき安全対策上の役割を検討していく。

なお、３者関係の整理にあたっては、２者関係の基本的類型の考え方（※）を参考とすることが有益である。

（※）２者関係の基本的類型の考え方

金融機関が複数となる場合において、安全対策上固有の性質が生ずるものとして対象とされた類型には、ⅰ）共同センターとⅱ）クラウドサービスがある。ⅰ）共同センターは、安全対策等の資源が効率化でき、その効果が複数の金融機関におよぶ（共同性）一方で、単一の金融機関の場合と同程度に迅速かつ円滑な意思決定が常に可能か不確実性が残るという問題（時間性の問題）を含む。ⅱ）クラウドサービスは、共同性を性質として有する一方で、共同委託者が互いに独立しており相互の合意をとる必要が無いものの、安全対策上データの所在地把握等の統制方法に固有の留意が必要となる。

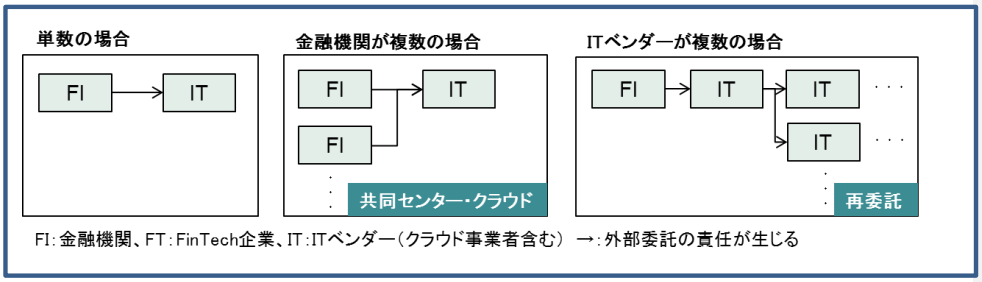
IT ベンダーが複数となる場合において、まず、金融機関の委託先が複数となる場合には、統制が直接可能であることから、固有の性質は生じず単数の場合と何ら異ならない。一方、再委託により間接的に委託先が多段階にわたり複数となる場合は、再委託先に対して金融機関による統制が及びにくくなることから、固有の性質がある類型となる（詳細は外部委託検討会報告書を参照）。

---

[6] 安対基準においては、「IT ベンダー」だけでなく、「ベンダー」「コンピュータメーカー」等の用語が使用されているが、ここではそうした技術的性質を有する当事者を「IT ベンダー」と総称する。なお、IT ベンダーには「クラウド事業者」も含むものとして使用する。

[7] 外部委託検討会報告書においては、業務的性質を有する関係者の安全対策における主な役割と責任として、Ⅱ IT ガバナンスと IT マネジメント 2.(3)「ユーザーの役割と責任」において、「①安全対策に配慮したビジネスモデルの企画」「②投資効果の達成」「③業務要件の提示」が挙げられている。

（図表１） ２者関係の基本的類型



②金融機関が必ずしも主導的立場とならない業務形態の登場

安対基準では、金融機関が、自らの顧客に対して提供する金融サービスに係る業務を担う情報システムにおいては、金融機関に安全対策上の責任が存することを前提としてきた[8]。これは、金融機関の顧客に対して提供される金融サービスに関して、金融機関がその全てを主導して決定する中においては、当然の帰結である。

一方で、FinTech を巡っては、近年、顧客と金融機関の間に介在する FinTech 企業が登場している[9]。その中には、金融機関のサービスを利用するために必要となる ID やパスワード等を顧客から提供され、それによって、自ら金融機関から顧客に関するデータを取得し、かつ、取得したデータに独自の価値を付加した後、顧客に対して直接的に金融関連サービスを提供している業者がある。このような FinTech 企業のサービスは、金融機関から取得するデータをサービスの源泉として利用しながらも、金融機関が顧客に対して提供するサービスでは得られなかった革新的なユーザー体験等を付加していること等が顧客から評価され、その利用が進んでいる状況にある[10]。

このような FinTech 企業が顧客に対して直接的に提供するサービスは、FinTech 企業がその全てを主導して決定し、金融機関と何ら交渉を行うことなく、一方的に金融機関から顧客に関するデータを取得することが可能な場合がある。このように、金融機関が完全に受動的立場となる場合は、金融機関には何ら統制の手段等が無いことから、金融機関において顧客に対する安全対策上の責任は生じないと解される。したがって、たとえ、金融機関の顧客に対して提供される金融関連サービスであっても、安対基準の対象

[8] 安対基準では、【運 90-1】において、「外部委託」とは異なる「サービス利用」に関する基準があるが、この中で、この外部委託と異なる基準が必要な理由として「各金融機関が、外部委託の管理と全く同様に、サービスの提供元を複数の中から選定することや、独自にリスク管理を行うことは難しく、また非効率な場合が多い。」とされている。これは、主導性や効率性の観点から、各金融機関が負担する安全対策上の責任の程度を一般の外部委託と比して、限定的に解すべきとしたものである。ただし、その対象は「金融機関相互のシステム・ネットワーク」に限定されており、今回検討が必要となる顧客に対する業務を対象とする基準ではない。

[9] 顧客と金融機関の間に介在する FinTech 企業の中には、本文でとりあげた以外にも、店舗や金利等金融機関がホームページ等を通じて一般的に広く公開しているデータ（オープンデータ）を利用する業者や、顧客の金融機関に対する決済指示を仲介する業者等も考えられる。

[10] 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」第２回（平成 27 年９月 15 日）では、「銀行等と利用者の間に立って、両者を介在するサービスを提供する者（いわゆる中間的業者）が拡大している。」としている。

とならないと解するのが妥当である[11]。

他方で、顧客に対して、直接的には FinTech 企業がサービスを提供するものの、FinTech 企業と金融機関の間に交渉があり、その結果、金融機関が FinTech 企業に提供するデータに関して、金融機関が決定を行うことが可能な場合がある。また、金融機関が FinTech 企業から受け入れるデータに関しても、金融機関が決定を行うことが可能な場合も考えられる。こうした、金融機関において、顧客に関するデータ[12]の提供または受け入れに関して決定権が存する場合は、金融機関が部分的にせよ主導性を発揮しているものと考えられることから、金融機関に何らかの安全対策上の責任が生じていると解するのが妥当である。

したがって、FinTech 企業が提供するサービスにおいて、情報システムにおける安全対策上の責任が、金融機関に部分的に生じる場合についても、安対基準の対象として、その安全対策の在り方を検討する必要がある。

なお、こうした金融機関の安全対策上の部分責任は、顧客の許諾があるとはしながらも、もともと金融機関に管理責任が存する顧客に関するデータを、第三者に提供すること、または、第三者から受け入れたデータに従い顧客に関するデータへ更新を行うこと、に由来するものである。したがって、提供または受け入れに関するデータのリスク特性に着目し、それに応じて、安全対策の在り方を考えることとなる。その際には、リスクベースアプローチを踏まえると、データの提供に関しては、データのリスク特性のひとつである機微性の程度のほか、データの量等にも着目することが適切である。機微性の程度とは、万一データが FinTech 企業によって、本人の許諾した範囲を超えて利用された場合、あるいは一方的に外部に流出した場合等に、顧客が被ると想定される損失の程度のことをいう[13]。また、データの受け入れに関しては、受け入れたデータに従って行うデータへの更新の規模のほか、FinTech 企業から受け入れたデータが顧客の指示に基づくものであることを、FinTech 企業が適切に確認しているかといった、FinTech 企業による顧客の本人確認方法に着目することが適切である。

（注）現在、監督当局において、顧客と金融機関の間に介在する FinTech 企業に関連した検討が進められており、その検討結果も、考慮していくことが必要である。

削除: が取得

削除: に管理責任がある

削除: なお、逆に、

削除: に渡される

削除: も

削除: 決済指示データがそもそも誤っていれば、顧客は損失を被る可能性があるが、金融機関はデータの生成に何ら関与しないことから、金融機関に安全対策上の責任は生じないと考えるのが妥当である。

11 英国の「Open Banking Standard」（2016 年２月８日）では、こういった「スクリーンスクレイピング」と称されるデータ取得方法の問題として「ウェブサイト側でアクセスをコントロールしたり規制することができない。」「何か問題が発生しても、利用者は問題解決の手段がなく、銀行に頼ることもできない。」等が挙げられている。なお、これはスクリーンスクレイピングが採用されていることをもって、ただちに問題がある訳ではなく、本来的には金融機関と交渉なくデータが取得されることが問題である点に留意が必要である。

12 金融機関が FinTech 企業に提供するデータとしては、例えば、顧客の取引履歴情報等がある。また、金融機関が FinTech 企業から受け入れるデータとしては、例えば、決済指示が考えられる。

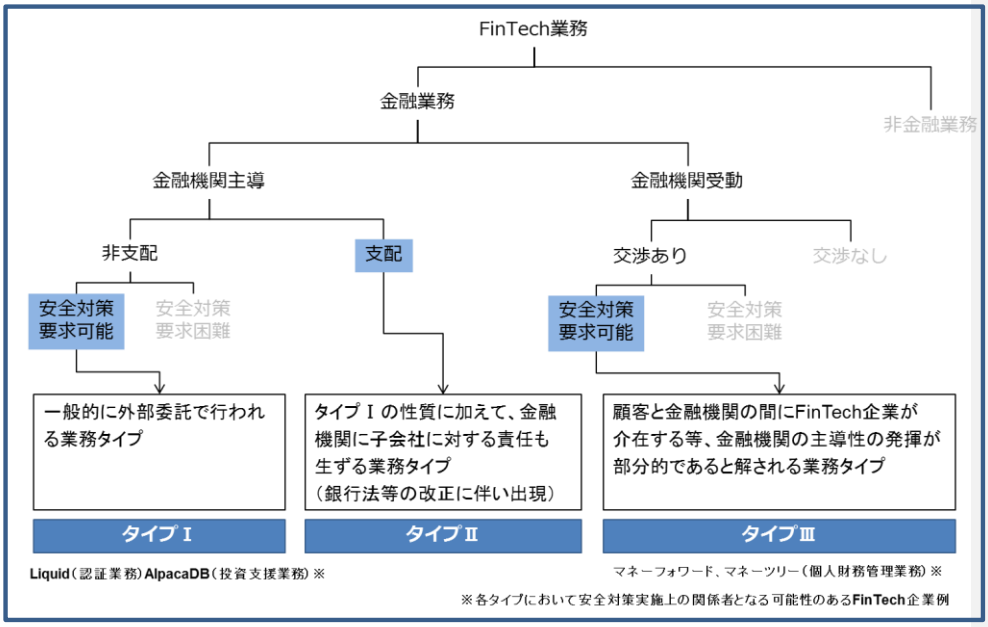
13 FISC 外部委託検討会報告書において、機微性の程度が高い機微情報に関しては「その保護のために最上位の安全対策目標が設定されるべき」個人情報として、「本人の許諾なく機微情報が流出した場合、経済的損失にとどまらず、基本的人権の侵害といった広範な損失を被る可能性があることから、その取扱いには社会的・公共的な性質を有するもの」とされている。

（２）検討を進めるにあたっての前提

①検討対象となる FinTech 業務のタイプ

前述の「安対基準の対象となる情報システムの判別基準」および「金融機関が必ずしも主導的立場とならない業務形態」にもとづくと、本検討会の検討対象となる FinTech 業務を以下の３タイプに分類可能となる。

（図表２）安対基準の対象とすべき FinTech 業務のタイプ



タイプⅠが、従来の安対基準で「外部委託」として捉えられていた基本的なタイプに該当する。タイプⅡは、先般、平成 28 年５月の銀行法等の改正によって、金融機関が FinTech 企業を子会社とした場合に、安全対策上の責任に加えて、子会社に対する責任[14]も生ずることから、安全対策上の責任の在り方を検討するにあたっては区別している。タイプⅢは、タイプⅠ、Ⅱと異なり、金融機関の安全対策上の責任が部分的となることから区別している。

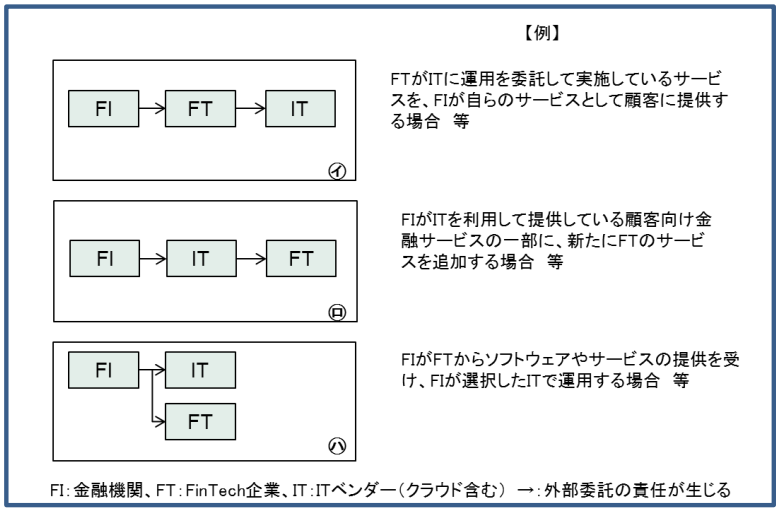
[14] 平成 28 年５月の銀行法等改正においては、あわせて「金融グループにおける経営管理の充実」のために、持株会社等が果たすべき「機能」が明確化された。また、岩原紳作『金融持株会社におけるグループガバナンス－銀行法と会社法の交錯（３）－』において「多くの金融持株会社は、（中略）子会社との間で経営管理契約を結んで経営管理のための助言・指導を行うことを定めている。」としている。

②FinTech 業務における安全対策実施上の関係者の基本的類型

金融機関が、FinTech 企業と FinTech 業務を実施するにあたっては、当然のことながら情報システムが必要であるが、金融機関や FinTech 企業においては、そのために必要となる情報システムの開発や運用といった資源を外部から調達すること、すなわち IT ベンダーに外部委託することが一般的であると考えられる。特に、業務を開始したばかりの FinTech 企業においては、IT ベンダーの中でも、クラウド事業者に委託することが多いと言われている[15]。そのため、あらためて、金融機関と FinTech 企業といった２者関係を整理することは行わず、金融機関と FinTech 企業、IT ベンダーといった３者の関係性を整理する[16]。

その場合、まず、３者がいずれも単数である場合については、金融機関は常に委託元となることから、残り２者の組み合わせに応じて、以下の類型が検討すべき類型として考えられる。

（図表３） ３者が単数の場合に考えられる類型



次に、以上の類型において、３者のいずれかが複数となる場合について、取り上げるべき基本的類型があるかどうかを整理する。まず、IT ベンダーが複数となる場合は、２

[15] 日本銀行金融システムレポート別冊シリーズ「IT の進歩がもたらす金融サービスの新たな可能性とサイバーセキュリティ」（2016 年３月）によれば、FinTech が、金融機関がこれまで提供してきた金融サービスと異なる点のひとつとして「クラウドサービスやオープンソース・ソフトウェアのように社外の資産・サービスを積極的に活用することは、準備期間を短縮し、機動的にサービスを提供できる強みにもなっている。」としている。また、FISC『金融機関におけるクラウド利用に関する有識者検討会報告書』によれば、クラウドは、スモールスタートに適する拡張性や柔軟性や、新技術導入スピードが速く、また、モバイル端末や SNS（ソーシャル・ネットワーキング・サービス）等との親和性が高いといった利便性や機能の向上、等のメリットを有しているとされている。

[16] なお、FinTech 企業の業務的性質と技術的性質が内部的に峻別可能であれば、２者関係に還元可能とする考え方も理論的にはありうるが、FinTech 企業の内部的な実態は多様であり、明確にその性質を峻別することは難しいものと考える。

者関係の基本的類型の考え方を前提にすれば、新たな類型を想定することは不要と考えられる。すなわち、金融機関の委託先である IT ベンダーが複数となる場合は、金融機関による直接の統制が可能であることから、固有の性質は生じない。一方、IT ベンダーまたは FT 企業を通じて複数の IT ベンダーに再委託を行った場合は、固有の性質がある類型として、既に外部委託検討会において包括的に検討済みであることから、本検討会において個別の検討は不要と考えられる。

次に、FinTech 企業が複数となる場合は、FinTech 企業の業務的性質に着目すると、金融機関あるいは IT ベンダーが複数の FinTech 企業に対して個々の業務的役割を決定していると考えられることから、共同性のような固有の性質が生じることはない。また、FinTech 企業の技術的性質に着目すると、IT ベンダーが複数の場合と何ら異ならない。したがって、FinTech 企業が複数となる場合においても、個別の検討は不要と考えられる。

最後に、金融機関が複数となる場合は、既に２者関係の基本的類型の考え方で整理された共同性の性質以外に固有の性質はないと考えられる。

以上のことから、３者が複数となる場合は、いずれも検討は不要と考えられる。

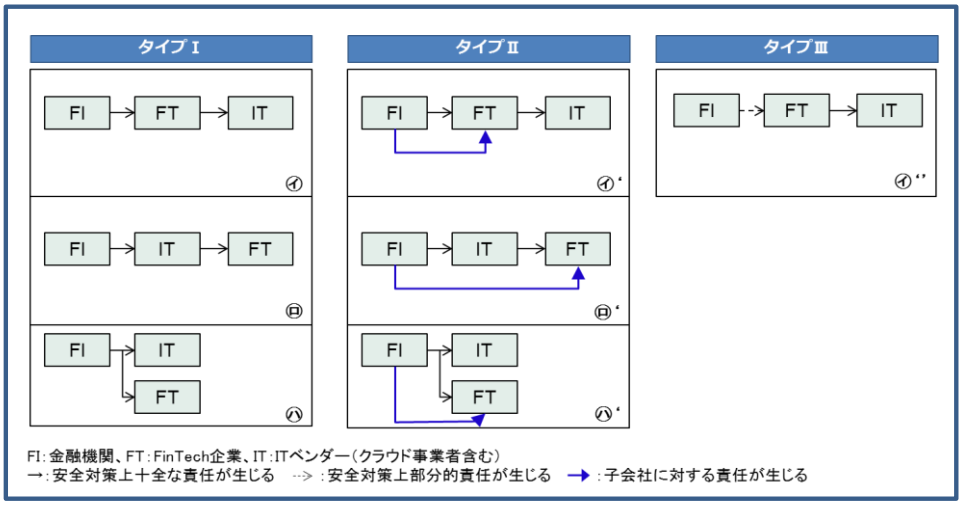
（注）今後、金融機関に部分的に安全対策上の責任が生じる場合等 FinTech に関する安全対策の在り方を検討する中で、固有の性質があるものとして、基本的類型が追加される可能性は残る。

しかしながら、３者関係における基本的類型の特定が、従来の安対基準を FinTech 業務に適用した場合に内在する問題を析出することを目的としていることに鑑みれば、現段階で、基本的類型の理論的正当性を議論するよりも、検討が必要であることが明らかな類型から、内在する問題の検討を進めるのが適切である。今後、新たな類型を取り上げることの必要性が明らかになれば、その際にあらためて立ち返って検討を行うこととする。

③本検討会において前提とすべき業務タイプ別類型

以上の「検討対象となる FinTech 業務のタイプ」および「FinTech 業務における３者関係の基本的類型」を総合すると、本検討において前提とすべき、FinTech 業務のタイプ別の類型は以下のとおりとなる。

（図表４）FinTech 業務において安全対策実施上の関係者のタイプ別類型



タイプⅠは、基本的類型である３類型である。タイプⅡはタイプⅠの３類型をもとに子会社に対する責任が付加されることで派生する３類型である。タイプⅢは、安全対策上の責任関係はタイプⅠの金融機関が FinTech 企業に委託する類型と類似であるが、その安全対策上の責任が部分的となることから派生する１類型となる。

以上から、この７類型について、従来の安対基準を適用した場合に内在する問題の有無について、具体的な検討を行っていく。

④FinTech 業務における安全対策の検討で考慮されるべき観点

問題の所在を明らかにするにあたり、そもそもどういう観点で問題を捉えるか、あらかじめ共有しておくことは有益である。

まず、本検討会の設立趣旨として、「我が国金融機関が、システムの安全性を確保しつつ、イノベーションの成果を享受することを目指していく」という観点が、考慮されるべきである。

そのうえで、FinTech 業務を実施するにあたって、様々な類型が展開されることが想定される中で、例えば、安対基準が特定の類型の採用にあたり抑制的な効果をもたらすことがないよう留意することが必要である。安対基準は情報システムを対象とした安全対策の基準であり、それ自体が、金融機関が様々に行うであろうビジネスモデルの多様性を損なうようなことがあってはならない。仮に、特定の類型の採用に抑制的となる歪みがあるのであれば、問題として取り上げることが必要である。(安対基準の中立性)

一方で、金融機関に安全対策上の責任が生じる限りにおいては、その責任を果たすために、安全対策の実施にあたっては、その実現能力、すなわち、外部委託される場合は委託先や再委託先への統制能力が、十全に確保されることが必要となる。しかしながら、多岐にわたる FinTech 業務の類型においては、金融機関がその安全対策上の責任を果たすために必要となる統制能力が必ずしも十全に機能するとは限らない場合があるのであれば、問題として取り上げる必要がある。(安対基準の有効性)

次に、以上の、安対基準の中立性および有効性といった観点は、必ずしも両立するものとは限らないことから、いずれの観点を優先させるべきか、あらかじめ、検討しておくことも考えられる。

仮に、中立性を優先させた場合には、多様なビジネスモデルを損なうことはなく、イノベーションの成果を享受し企業価値の最大化の実現に寄与することとなるものの、金融機関が顧客に対する安全対策上の責任を必ずしも果たせないこととなる懸念が生ずる。一方で、有効性を優先させた場合には、FinTech 企業や IT ベンダーに固有の負担を求める、あるいはそのビジネスの自由度を制約することが想定され、結果として FinTech 企業の革新性を損なうこととなる懸念が生ずる。

こうした中立性と有効性がトレードオフとなる問題は、多様な状況で発生すると考えられることから、あらかじめそのいずれを優先すると判断することは難しく、個々の状況に応じてケースバイケースで判断せざるをえないものと考えられる。

特に、簡易なリスクベースアプローチでは、従来の安対基準を適用した際に生じるであろう個々の問題が明らかになった後に、中立性と有効性のいずれを優先させることが簡易なリスク管理策を策定するにあたって妥当か、を検討するのが適切であろう。

⑤「オープン API」との関係

「オープン API」においては、金融機関が API を公開し、FinTech 企業等が同 API を利用して自社サービスと金融サービスを連携させる方法がとられる。

オープン API には様々な類型が考えられるが、一般的には、「金融機関が主導的立場とならない業務形態」（タイプⅢ）である場合が多い。

かかるオープン API におけるセキュリティの考え方については、平成 27 年 12 月に公表された金融審議会・決済業務等のあり方に関するワーキング・グループ報告書において、銀行界に対して「セキュリティ等の観点から、オープン API のあり方を検討するための作業部会等を設置」の上、「平成 28 年度（2016 年度）中を目途に、報告をとりまとめ」ることが提言されているところであり、同提言を受けて、今後、全銀協を事務局、金融機関・IT 関連企業・金融行政当局等をメンバーとする検討会が設置される予定となっている[17]。

同検討会には FISC もメンバーとして参加する予定であり、本検討会としては、全銀協を事務局として行われる検討会での議論を参考にしつつ、検討を行うこととしたい。

以上

[17] http://www.fsa.go.jp/singi/kessai_kanmin/siryou/20160608/04.pdf

参考

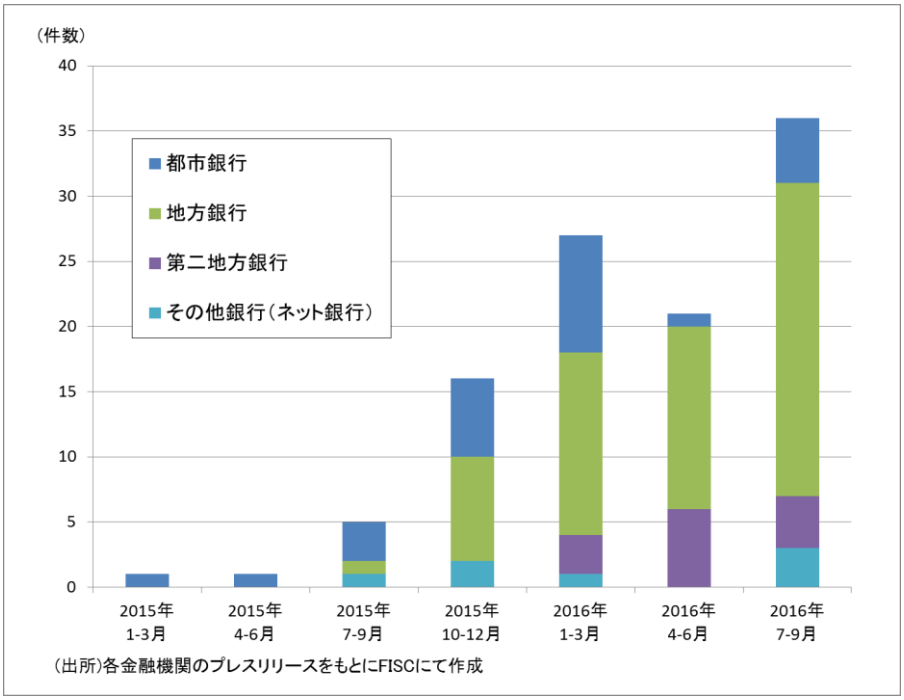
金融機関等における FinTech を巡る動向

１．国内金融機関の動向

2015 年から、都市銀行・地方銀行を中心として、国内金融機関の「FinTech」をキーワードとしたプレスリリースが急増している。主な内容は以下のとおり。

【2015 年 1-月】都市銀行が FinTech コンテストを開催
【2015 年 7-月】地方銀行のプレスリリースが増加
（FinTech 推進部署を設置　等）
【2016 年 1-月】都市銀行・地方銀行が新しい技術の実証実験開始
地方銀行が FinTech 企業と業務提携

（図表）国内金融機関の FinTech に関連するプレスリリースの件数



（出所）各金融機関のプレスリリースをもとにFISCにて作成

２．官公庁等の FinTech の定義例

「日本再興戦略 2016」（2016 年 6 月 2 日閣議決定）
近年、FinTech と呼ばれる金融・IT 融合の動きが進展しており、金融業・市場に変革をもたらしつつある。
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」 （2015 年 12 月 22 日）
FinTech とは、金融（Finance）と技術（Technology）を掛け合わせた造語であり、主に、IT を活用した革新的な金融サービス事業を指す。特に、近年は、海外を中心に、IT ベンチャー企業が、IT 技術を生かして、伝統的な銀行等が提供していない金融サービスを提供する動きが活発化している。
経済産業省「産業・金融・ＩＴ融合に関する研究会（FinTech 研究会）について」 第一回配布資料（2015 年 10 月 6 日）
近年、フィンテック（FinTech）と呼ばれる IT を活用して革新的な金融サービスを提供するベンチャー企業が現れ、流通など伝統的な金融業以外の企業が新たな金融サービスを提供する動きが、世界中で見られる。
日本銀行「決済システムレポート」（2016 年 3 月）
FinTech とは、金融（Finance）と技術（Technology）を組み合わせた言葉であり、近年、急速に注目を集めている。この FinTech の定義は必ずしも明確に定められている訳ではなく、話者によって、その意味が異なることも多いが、一般には、情報通信技術など新しい技術を取り込んだ、新たな形態の金融サービスや、あるいは、そうした金融サービスを積極的に提供 していこうとする動きを指すことが多い。

３．日本の監督当局等の動向

（１）銀行法等の改正

本年５月に銀行法等が改正され、「銀行業の高度化若しくは利用者の利便の向上に資する業務又はこれに資すると見込まれる業務を営む会社」に対して、金融機関（あるいは金融グループ）が、当局の個別認可を得て出資し子会社とすることが可能となった。これにより、金融機関（あるいは金融グループ）が FinTech に取り組むにあたり、FinTech 企業を子会社とする事例が、今後出現してくることが予想される。

（２）金融制度ワーキング・グループの開始

本年７月 28 日に、金融審議会「金融制度ワーキング・グループ」（第１回）が開催され、中間的業者に対する規制のあり方が論点として取り上げられている[18]。多様な出現形態を持つ FinTech において、銀行が必ずしも主導的な立場をとらない場合についても検討が着手されている。

（３）全国銀行協会の取組み

全国銀行協会では、本年８月４日に「オープン API のあり方に関する研究会」「ブロックチェーン技術の活用可能性と課題に関する研究会」が開催され、FinTech による金融革新の推進に関して、各銀行に対するアンケート結果を踏まえて、銀行業界としての検討が開始された。（FISC も両研究会に参加）

全国銀行協会のアンケートの中には、「FISC の金融機関等コンピュータシステムの安全対策基準等にて、銀行として取り組むべき安全対策等を示していただくことで、対策等の標準化が図られるとともに、検討時間、対応コストの削減が期待できる」といった、FISC に関するコメントも寄せられている。

（４）金融審議会における決済業務等の高度化に関する報告

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」報告（2015 年４月公表）および「決済業務等の高度化に関するワーキング・グループ」報告（2015 年 12 月公表）において、情報セキュリティに関する課題等について以下のとおり報告されている。

「決済業務等の高度化に関するスタディ・グループ」報告

第４章情報システムの安定性と情報セキュリティ　２．情報セキュリティ

（２）今後の課題

銀行における情報セキュリティについては、これまで、基本的に、外部接続先を主

[18]中間的業者を「銀行の代理業者」又は「銀行の外部委託先」として捉える規制が、業の実態と適合的といえるか、という議論がある。

として金融業界内に限定することによって、セキュリティ侵害のリスクを低下させるとともに、万一問題が発生した場合の損失・責任については、基本的にサービス提供者側が負担することにより対応されてきた。

他方、IT の発展等を背景に、ネットバンキングやモバイル送金などの例に見られるように、決済のインターフェイスは、銀行の外部へと拡大し、同時に、決済を中心とした銀行業務のアンバンドリング化が進行する中で多様なプレーヤーが決済情報のプロセスに組み込まれるようになっている。

こうした中にあっては、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。

こうしたことを踏まえると、今後、ネットワークのオープン化に対応した情報セキュリティ対策を講じることが更に重要である。このため、当面、例えば、以下のような課題について、検討を進める必要があると考えられる。

・ 銀行のネットバンキングなどについては、監督指針や FISC の安全対策基準の整備等の取組みが行われてきたが、多様なプレーヤーが決済情報のプロセスに組み込まれる中にあっては、銀行のみならず、多様なプレーヤーにおける情報セキュリティ対策の向上が重要である。こうした観点からは、多様なプレーヤーが対応の拠り所とできる準則や業界における情報セキュリティ基準の設定、その実効性の確保のための方策が重要である。

・ オープン化されたネットワークにおいて有効な情報セキュリティ対策を講じるためには、銀行その他の多様なプレーヤーと利用者が、それぞれ一定の責任を持って対策を講じることが必要である。そのためには、問題が生じた場合の責任・損失分担について、必要に応じ、一定の合理的なルールが形成されていくことが期待される。

・ 金融機関の外部も含め、オープンなネットワーク全体としてセキュリティ水準を向上させるためには、サービスを提供する側のみならずサービスを利用する側の情報セキュリティ対策が重要である。こうした観点からは、利用者のリテラシー向上も含め、利便性を考慮しつつも、幅広い関係者が情報セキュリティ対策を推進していくための方策が重要である。

「決済業務等の高度化に関するワーキング・グループ」報告

第６章　決済高度化に向けた継続的取組み

決済業務等の高度化は、これまで述べてきた方向性に沿って、着実に行動に移していく必要がある。同時に、決済を巡る環境や決済サービスの変化・発展の可能性を踏まえれば、本報告書で述べた基本的な方向性を踏まえ、継続的に戦略的な取組みを実行していくことも必要である。

そのためには、決済高度化に向けた取組みの進捗状況をフォローアップするととも

に、海外の動向や決済高度化に関連するイノベーションの状況等も踏まえながら、継続的に課題と行動を特定し、それらを官民挙げて実行に移していくことが必要であり、金融庁にはそのための体制の整備に向けた取組みが期待される。また、その際には、決済システムの安定性や情報セキュリティの確保という課題についても適切な対応がとられていくよう、留意していくことが重要である。

４．海外先進諸国の動向

（１）米国

2016 年３月末、米国通貨監督庁（OCC,Office of the Comptroller of the Currency）が、『連邦銀行システムにおける「責任ある革新」を支援する：OCC の考え方』という文書を公開し、広く意見を求めた。

その中において、まず、国法銀行は、１５０年以上前から革新の担い手であり、FinTech において伝統的な銀行業務のやり方が破壊されようとしている中でも、国法銀行が金融革新において優位性を有しており、引き続き国力の源泉であることが期待されている。

・*リンカーン大統領が１８６３年に国法銀行システムを創設して以来今日まで、イノベーション（革新）は、国法銀行システムの代表的な特徴である。特にこの１０年間、その革新精神に基づいて、国法銀行および連邦貯蓄組合は、顧客のニーズの変化に対応すべく、商品、サービスやテクノロジーを開発導入してきている。*

・*銀行が革新を続ける一方で、金融テクノロジー、いわゆる FinTech において、急速かつ劇的な進歩が起こっており、伝統的な銀行業務のやり方が「破壊」されようとしている。連邦銀行システムのその他の健全性規制当局と同様に、我々も国法銀行と連邦貯蓄組合が、こうした環境の中でも、力強く成長し、消費者、事業者、地域共同体に対して、活力をもって金融サービスを提供する役割を果たし続けることを望んでいる。*

そのために、OCC が、連邦認可金融機関において、「責任ある革新」が進められるように、それを支援する監督規制のフレームワークの準備を進めているとし、８つの原則を表明している。

1.「責任ある革新」を支援する
2.OCC 内部に「責任ある革新」を受け入れる文化を醸成する
3.OCC の経験と技能を駆使する
4.金融サービスへの公正なアクセスが提供され、消費者が公正に取扱われるような「責任ある革新」を奨励する
5.効果的なリスク管理による、安全・健全な金融機関経営を促す
6.規模に関わらず全ての金融機関が事業戦略に「責任ある革新」を盛り込むよう奨励する
7.公式な「アウトリーチ（当局が現場に赴くこと）」を通して継続的な対話を促進する
8.他の監督当局と協力する

また、国法銀行と FinTech 企業の関係としては、それぞれの優位性を活かし、互いにコラボレーションしていくことを推奨している。

・*銀行とノンバンクイノベーターは、それぞれ独自の優位性を活かし、互いにコラボレーションすれば、利益を得ることが可能である。戦略的で思慮深いコラボレーションを通じて、銀行は、最新テクノロジーへのアクセス手段を手に入れ、ノンバンクイノベーターは、潤沢な資金や巨大な顧客基盤を手に入れることができるのだ。*

さらに、効果的なリスク管理が、必要条件とされている。

・*「革新」は、リスクから自由ではないが、適切に管理されている限りにおいては、リスクは進歩を妨げるものではない。実際に、効果的なリスク管理は、「責任ある革新」の必要条件である。銀行や当局は、リスクと革新の最適なバランスを心得なければならない。*
・*金融危機から学んだとおり、革新であれば何でも良いわけではない。(中略) OCC は、安全性、健全性、法令遵守、顧客の権利保護を堅持しうる「革新」を支援するものである。*

（2）英国

英国金融行為規制機構（FCA,Financial Conduct Authority）は、2014 年 10 月から「Project Innovate」を開始、自らイノベーションを涵養することで、金融サービスにおける効果的な競争を促すことを目的としている。この取組みの一環として、革新的なアイデアを実際の人々に対して試行するため“監督規制のサンドボックス”の実施計画を 2015 年 12 月に公表した。

一方で、英国財務省の要請により 2015 年９月に「the Open Banking Working Group」が設立され、英国銀行業における API のオープン標準推進に向けた検討が開始された。その検討の成果として、2016 年２月８日に「Open Banking Standard」が公表された。この報告書には、英国において Open Banking Standard を推進するための詳細なフレームワークが記載されているが、これは、英国がこの分野の国際的なリーダーシップを獲得し、世紀を超えて、経済・産業の勝者であり続けることを目指した、取り組みであるとされている。

・*仮にこの分野で英国が国際的なリーダーシップを獲得できれば、他の多くの業界を先導することともなるであろう。すなわち、こうして強固なデータインフラが構築されることは、<u>今日の英国経済にとって重要であるだけでなく、今後一世紀以上に亘って、英国が経済界・産業界の勝者であり続けるためにも重要である</u>。*

（斜体部は FISC にて意訳。下線は FISC にて付す。）

議事１（参考資料３） 第２回【議事３】別紙１の修正案

別紙１

FinTech に関する安対基準適用上の課題

１．検討にあたっての前提

金融機関における FinTech に関する安全対策の在り方を検討するにあたっては、まず、FinTech 業務を担う情報システムに、従来の安対基準を適用した場合に内在する問題の有無を検討した後に、FinTech に関する安全対策の在り方およびそのリスク管理策を検討し、従来の安対基準に調整を行っていく。

検討にあたって、以下のとおり、付加的に踏まえておくことが有益な事項がある。

（１）目標とすべき安全対策の効果の程度

安対基準の対象となる FinTech 業務を担う情報システムについて、その安全対策の在り方を検討するにあたっては、金融機関と IT ベンダーに FinTech 企業を加えた３者関係を前提として検討することとなるが、どの程度の安全対策の効果を目標として検討を行うべきか、明確にしておくことは有益である。

これについては、顧客の立場に立てば、安全対策上の関係者が変わろうと、安全対策の効果が同程度で確保されることが期待されていると考えられる。したがって、FinTech 企業という新たな関係者が登場する場合であっても、その安全対策の効果は、従来の安対基準において実現される２者関係における安全対策の効果と比較して、同程度となるよう留意することが重要である（以下「同等性の原則」という）。

また、２者と３者で同程度の安全対策の効果の実現を目指す場合、中立性および有効性といった観点から、従来の安対基準に対する調整は必要十分な範囲に留めることが重要である。すなわち、その調整によって、金融機関および IT ベンダー等の負担が必要な範囲を超えて増加することが無いよう留意することが重要である。

（２）安対基準における検討対象領域

従来の安対基準には、「コンピュータシステムが収容される建物、設備」を対象とした設備基準および「ハードウェア、ソフトウェア等」を対象とした技術基準のようにモノを対象とした基準と、開発・運用管理体制等を対象とした運用基準のようにヒトを対象とした基準があり、いずれの基準を主に検討の対象とするか、明確にしておくことは有益である。

モノを対象とする設備基準や技術基準については、今後、多岐にわたる FinTech の出現が予想される中では、個別具体的な技術を前提として安全対策を特定することは困難であり、また、FinTech を巡る環境が変化する中、個々の安全対策を確定的に設定することも適切ではない。そのため、設備基準や技術基準に関しては、金融機関において、個々の FinTech 業務のリスク特性に応じた安全対策が独自に決定され、「安全対策における基本原則[1]」にしたがって IT ガバナンスが行われていれば十分であると考える。

一方、ヒトを対象とする運用基準は、多岐にわたる FinTech の出現に際しても、その

[1] FISC『外部委託検討会報告書』で提言された、リスクベースアプローチを踏まえた４原則のこと。

多種多様な技術等に左右されることなく適用可能なものと考えられることから、本検討においては、こうした運用基準を主として対象とすることが適切である。

また、FinTech 業務は金融機関の FinTech 企業に対する外部委託という形態で実現される場合があることから、運用基準の中でも、外部委託に関する基準を主な対象として検討することが適切である。

（3）簡易なリスク管理策の性質

簡易なリスク管理策の検討にあたっては、その性質をあらかじめ明らかにしておくことが有益である。

簡易なリスク管理策は、まず重要な情報システムに対する統制が設定されていることを前提として、その統制を、一般の情報システムに対しては、緩和することで導出されるものである。また、その反面、安対基準においては「必要最低限の基準[2]」と表現されるとおり、「最低限ここまでは実施しておくべき」という拘束性も有している。

そのため、簡易なリスク管理策の設定が不適切であると、中立性や有効性を損なうのみならず、恒常的に、過度な安全対策あるいは不十分な安全対策を招来することとなることから、その検討にあたっては、FinTech 企業をはじめとする関係者が、安全対策に取り組むにあたり、個々の情報システムの現場で直面している問題認識が正しく反映されるよう留意するとともに、慎重に検討が行われることが重要である。

（4）クラウドサービスの利用に関する安対基準の取扱い

FinTech 企業においては、IT ベンダーの中でも、クラウド事業者に情報システムの運用を委託することが多いと言われていることから、外部委託に関する安対基準において、「クラウドサービスの利用」に関する安対基準が、どのように位置づけられるか、整理しておくことが有益である。

まず、安対基準においては、クラウドサービスは外部委託の一形態として捉えられている[3]。さらに、「クラウドサービスの利用」に関する安対基準は、今後、クラウドサービス固有の内容等を除いたうえで外部委託全般の基準として参考としていくこととなっている[4]。こうした安対基準の改訂は、外部委託検討会及び本検討会の成果も踏まえて行われることとなっている[5]ため、現時点では、こうした整理が行われた後の外部委託の安対基準（クラウドサービスを含む）として、確定的なものは存在しないことに留意が必要

---

2 FISC『外部委託検討会報告書』において、「必要最低限の安対基準の意義」について「比較的低リスクな情報システムに対する安全対策として「簡易なリスク管理策」の通称で示され、安対基準の中では「可能である」と表記上区分されている基準と類似の性質を有する。」としている。また、「安全対策の不確実性を低減するという目的の範囲内で定められるべきものである。」としている。

3安対基準の運用基準「（XIV）クラウドサービスの利用」において、「クラウドサービスの利用にあたって、（中略）外部委託管理の考え方に沿って、適切なリスク管理を行うことが必要である。」としている。また、FISC「外部委託検討会報告書」５．外部委託の概念において、クラウドは外部委託の範囲に含まれるものとして整理されている。

4 FISC『外部委託検討会報告書』脚注 31 において、「クラウドサービスの基準のうち外部委託全般に適用可能なものは参考とすべきであり、一方クラウド固有として考えられる基準は外部委託一般の基準にはしない、という整理を行う必要がある。」としている。

5 FISC『外部委託検討会報告書』において、「安対基準等の改訂は、FinTech 検討会の終了を待って、外部委託及び FinTech の両検討会の成果を踏まえて、行うこととする。」としている。

である。

そのため、本検討会において、検討を行うのに必要な範囲で、暫定的に従来の安対基準のうち外部委託に関する基準の概要を整理することが必要である。

次に、「クラウドサービスの利用」に関する安対基準の前提となった FISC「金融機関におけるクラウド利用に関する有識者検討会」（以下「クラウド検討会」という）報告書は、その後続の検討会である外部委託検討会報告書で提言された「重要な情報システムの意義」等を踏まえていないため、クラウド検討会報告書のリスク管理策が、外部委託報告書で提言された「重要な情報システム」においても適切であるか、不確実性が残る現状にある。

簡易なリスク管理策が、重要な情報システムに対する管理策をもとに、その統制の程度を緩和することで導出されることに鑑みれば、こうした事情にも留意することが望ましい。

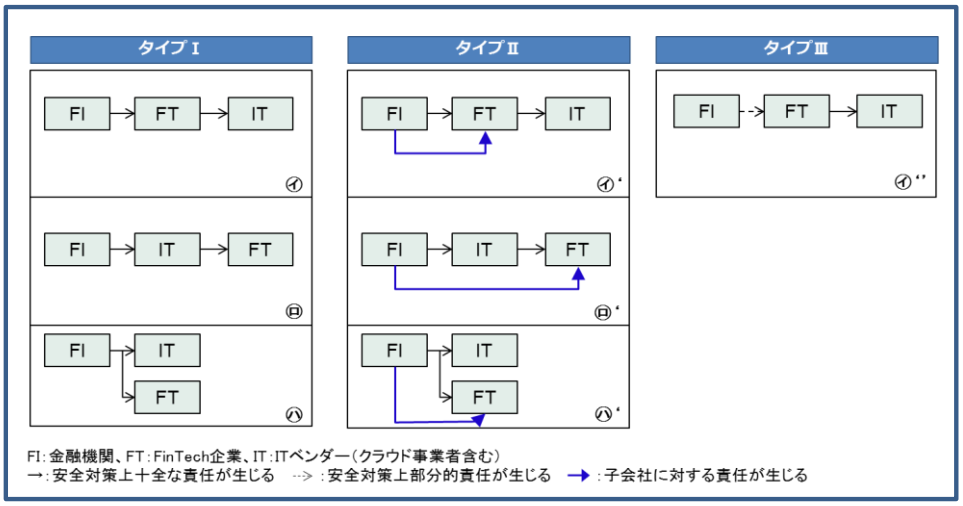
なお、以上の留意事項を解決するため、本検討会において、クラウドサービスを利用する場合の管理策について、外部委託検討会報告書の成果を踏まえて、補足的な検討を行うことが考えられる。こうした補足的検討をあらかじめ行っておけば、重要な情報システムでクラウドサービスを利用した FinTech のユースケース（ブロックチェーン・AI 等）が登場した際にも、その前提が整理されていることとなり、有益である。

２．　従来の安対基準に基づく関係者の責務

（１）関係者の責務

まず、内在する問題を検討するにあたり、「従来の安対基準の概要（外部委託関連）」を、金融機関と IT ベンダーの２者関係をもとに、３者関係（以下のタイプⅠが前提）に置き直して、整理を行った。【参考１参照】

（図表１）FinTech 業務において安全対策実施上の関係者のタイプ別類型



整理にあたっては安全対策実施上の関係者それぞれの責務を以下のとおり分類している。

- 外部委託利用時の金融機関の責務　　・・【責務Ａ】
- 一次委託先の責務　　・・【責務Ｂ】
  - 金融機関の一次委託先として負う責務・・【責務Ｂ－１】
  - 金融機関の再委託先に対する責務　　・・【責務Ｂ－２】
- 金融機関の再委託先として負う責務　・・【責務Ｃ】

関係者が以上の責務を適切に果たすことで、外部委託における安全対策の効果が実現できるものと期待されるが、その中でも、内在する問題は新たな関係者となる FinTech 企業において、具体的に認識されることから、FinTech 企業の責務に着目し、㋑㋺㋩のタイプ別類型で整理すると、次のとおりとなる。

【㋑の類型】

【責務Ｂ－１】金融機関の一次委託先として負う主な責務		注
a.利用検討時	金融機関が客観的評価を実施するために必要とする情報を、金融機関に提供する責務	3
	金融機関にデータの所在に関する情報を提供する責務	7
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関と締結する責務	11
	金融機関による再委託先への監査権を明記する責務	14
	金融機関が再委託先の事前審査を行うことに対応する責務	25
d.運用時	金融機関からデータ管理を受託する場合、漏洩防止策を講じる責務	28
	記憶装置の故障等により、機器・部品を交換する場合には、データ消去を含めた十分な管理を行う責務	29
	金融機関からの日常的監視を受忍する責務	30
	金融機関からシステムに関する総合的な監査・評価を受忍する責務	31
【責務Ｂ－２】金融機関の再委託先に対する主な責務		注
a.利用検討時	金融機関の再委託先を客観的に評価する責務 【簡】公開情報や業界における評判や実績等による評価でも可能	3
	データの所在を把握する責務 【簡】データの所在の把握について省略することも可能	7
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関の再委託先と締結する責務	11
	金融機関による再委託先への監査権を明記する責務 【簡】監査権を明記しないことが可能	14
	再委託先に対して適切な事前審査を行う責務	25
d.運用時	再委託先に金融機関のデータ管理を委託する場合、漏洩防止策を実施させる責務	28
	記憶装置の故障等により、機器・部品を交換する場合には、データ消去を含めた十分な管理を行わせる責務 【簡】消去・破壊プロセスの実効性を検証することで代替可能	29
	再委託先を日常的に監視する責務	30
	再委託先に対してシステムに関する総合的な監査・評価を行う責務 【簡】第三者認証等を活用することで代替可能	31

【㋒の類型】

【責務Ｃ】金融機関の再委託先として負う主な責務		注
a.利用検討時	IT ベンダーが客観的評価を実施するために必要となる情報を、IT ベンダーに提供する責務	3
b.契約締結時	機密保護や安全な業務の遂行等を契約として、IT ベンダーと締結する責務	11
	金融機関による監査権を明記する責務	14
d.運用時	IT ベンダーからの日常的監視を受忍する責務	30
	IT ベンダーからシステムに関する総合的な監査・評価を受忍する責務	31

【㋑の類型】

【責務Ｂ－１】金融機関の一次委託先として負う主な責務		注
a.利用検討時	金融機関が客観的評価を実施するために必要とする情報を、金融機関に提供する責務	3
b.契約締結時	機密保護や安全な作業の遂行等を契約として、金融機関と締結する責務	11
d.運用時	金融機関からの日常的監視を受忍する責務	30
	金融機関からシステムに関する総合的な監査・評価を受忍する責務	31

【簡】…既に策定されている簡易なリスク管理策　　注　…参考１の通番を記載

（２）内在する問題へのアプローチ

従来の安対基準（外部委託関連）を FinTech 業務に適用した場合に内在する問題を検討するにあたっては、以下のアプローチで、タイプ別に検討を行う。

- タイプⅠの場合、従来の安対基準を適用することで、問題が生じることはないか。
- タイプⅢの場合、そもそも従来の安対基準を適用することが、妥当であるか。

なお、タイプⅡについては、タイプⅠに異なる責任が付加される類型であることから、個別に検討を行う。

３．タイプⅠにおいて内在する問題と安全対策の在り方

タイプⅠにおいて、FinTech 企業は、【責務Ｂ】あるいは【責務Ｃ】を担うこととなるものの、そもそも、従来の安対基準では、金融機関と IT ベンダーの２者を念頭に置き策定されてきたことから、【責務Ｂ】あるいは【責務Ｃ】は、IT ベンダーが担うシステム運用を主な対象とし、IT ベンダーの安全対策遂行能力を念頭において策定されてきたものである。

したがって、【責務Ｂ】あるいは【責務Ｃ】を、FinTech 企業が担う場合には、FinTech 企業の安全対策遂行能力（保有する経営資源等）と比して、バランスを欠いたものとなっていないか、という問題が内在している。

そのため、FinTech 企業に対して、IT ベンダーに求めてきたものと同様の安対基準の適用を、形式的に求めた場合、安全対策遂行能力が IT ベンダーと同程度でない FinTech 企業においては、安全対策負担を過大とし、その負担を回避するインセンティブが生じることとなる。すなわち、その結果として、FinTech 企業のビジネスモデルの選択に、歪みを与える可能性がある（中立性の観点）。あるいは、FinTech 企業が、過大な安全対策負担になんとか応えようとした場合、その結果として、内部の経営資源を安全対策に優先的に配分することとなり、そのイノベーションを損なう可能性がある（イノベーションの成果を享受するという観点）。

一方で、FinTech 企業が加わる３者関係の場合であっても、その安全対策の効果は、従来の２者関係における安全対策の効果と比較して、同程度とすべきという考え方（同等性の原則）に立てば、単に、金融機関が、FinTech 企業の負担を、その安全対策遂行能力に見合う程度で十分として残存リスクを受容する、あるいは、FinTech 企業の安全対策遂行能力に合わせて、簡易なリスク管理策を調整することでは、本質的な問題は解決しない（有効性の観点）。

そもそも、金融機関は、企業価値の最大化を目指して、FinTech 企業の革新的な性質を自らの業務で利用すべく外部委託を行うのであって、必ずしも FinTech 企業に IT ベンダーの役割を全面的に代替させるために外部委託を行う訳ではない。

したがって、まず、金融機関は、FinTech 企業の安全対策遂行能力を確認したうえで、仮に FinTech 企業の能力を超える過大な責務があれば、その部分については、金融機関や IT ベンダーが分担することで、FinTech 企業の革新性を損なわずに安全対策の効果を達成できるよう配慮して、取り組んでいけば良いものと考えられる。

すなわち、この問題を解決するには、２者関係を念頭に置いた従来の安対基準において求められる責務の総体を維持しつつ、その責務を、３者の各類型における役割や３者の安全対策遂行能力（保有する経営資源等）に応じて、合理的に再配分しうることを、明示的にリスク管理策として認めることが適当と考える。

金融機関、IT ベンダーおよび FinTech 企業は、３者の合意の上、従来の安対基準における外部委託の責務を、３者で再配分[6]することが可能である[7]。
再配分にあたっては、「同等性の原則」にしたがって、必要な範囲を超えて関係者の負担が増加することがないよう留意する必要がある[8]。

削除: タイプⅠの安全対策の在り方としては、

削除: タイプⅠにおいて、

[6] 例えば、３者契約により、金融機関が、FinTech 企業に代わって、IT ベンダーを統制する【責務Ｂ－２】の一部を担うことで、金融機関自らが IT ベンダーに統制を行うこと等が考えられる。

[7] FinTech 企業の規模や業態は多様であることから、責務の再配分の分担内容をあらかじめ確定的に定めることは適切ではない。金融機関は、外部委託を行う FinTech 企業や IT ベンダーの実態に応じて、合理的に、その分担内容を、区々に決定すれば十分である。あるいは、分担内容の見直しありきではなく、FinTech 企業がその安全対策上の責務を果たせるように、金融機関が支援を行うことも考えられる。

[8] なお、これは「重要な情報システム」あるいは、タイプⅠ以外の類型においても妥当な考え方である。

削除: 合理的

４．タイプⅢにおいて内在する問題と安全対策の在り方

（１）金融機関の安全対策上の責任

タイプⅢは、FinTech 企業が金融関連サービスを主導する形態であり、金融機関と FinTech 企業の関係は、必ずしも外部委託と特徴づけられる形態に留まらない多様な形態を取りうるものと考えられる。また、監督当局における検討が進み、何らかの立法がなされた場合、金融機関と FinTech 企業の関係に、新たな要素が加わることも予想される。そのため、タイプⅢでは、金融機関と FinTech 企業の関係が、外部委託に留まらない幅広い形態になった場合でも柔軟に対応しうるような、安全対策の在り方を検討する必要がある。

これについては、金融機関と FinTech 企業の関係がいかなる形態となるにせよ、金融機関の立場から FinTech 業務の実質的な内容をみれば、外部委託と共通する要素が見出される可能性が高い。他方で、従来の安対基準において、外部委託に関する基準は、環境変化等に応じて見直され、完備されてきたのに対して、それ以外の形態については、必ずしも明示的な基準は存在していない。したがって、タイプⅢにおける安全対策の在り方として、基本的には外部委託の基準を「準用」することとし、それでは対応できない個別の事情がある場合に、必要に応じて修正を行うとすることが、妥当である。

外部委託基準の準用を考えるにあたっては、そもそも、外部委託の基準には、利用検討時・運用時等の管理フェーズにおける客観的評価・モニタリングの実施等、統制の方法に関する基準と、データ漏洩対策としての暗号化の実施等、統制の内容に関する基準があることに留意が必要である。

したがって、準用にあたっては、まず、統制の方法に関しては、金融機関に何らかの安全対策上の責任が生じる限りにおいては、外部委託と同様に実施されるべきものと考えられる。

タイプⅢにおける金融機関の関心項目例（【責務Ａ】から統制の方法を抜粋）		注
a.利用検討時	客観的評価の実施	3
	FinTech 企業は、金融機関が有する安全対策上の管理責任と同等の責任を果たし得るか。あるいは、金融機関が FinTech 企業に求める管理責任を果たし得るか。例えば、FinTech 企業は、安全対策において必要となる安全対策遂行能力（保有する経営資源等）を有しているか。	
b.契約締結時	安全対策を盛り込んだ契約の締結	11
	FinTech 企業は、金融機関と安全対策を盛り込んだ契約を締結するか。また、FinTech 企業は、IT ベンダーと安全対策を盛り込んだ契約を締結しているか。 （例えば、データ漏洩時の通知や損害賠償等の取決め等）	
d.運用時	日常的監視	30
	FinTech 企業は、金融機関に対して、安全対策の実行状況を報告することが可能か。	

削除: そうしてタイプⅢに外部委託の基準を準用する場合には、FinTech 企業が主導する金融関連サービスにおいては、金融機関の主導性の発揮は顧客に関するデータの提供に留まるものであることから、その主導性発揮の範囲内で責任を果たすこととなる。その場合、金融機関の関心は、例えば、以下の項目に集中することになる。

削除: .

削除: 金融機関から提供を受けた顧客に関するデータを管理するにあたり、

削除: データの保全に係る

削除: データの保全に係る

削除: データの保全に係る

	システム監査体制の整備	31
	FinTech 企業は、監査・評価を受忍するか。	

注　…参考１の通番を記載

一方で、統制の内容に関しては、安全対策上の責任が生じる部分についてのみ実施されれば十分と考えられる。金融関連サービスを FinTech 企業が主導する場合においては、金融機関の安全対策上の部分責任は、顧客に関するデータの提供または受け入れに由来することから、金融機関の統制の内容は、FinTech 企業が提供したデータを適切に管理しているか、または、FinTech 企業から受け入れたデータが顧客の指示に基づくものであることを、FinTech 企業が適切に確認しているか、という部分に関するものとなる。

以上のとおり、タイプⅢにおいて、金融機関が FinTech 企業へデータを提供する、またはデータを受入れる際に負う責務は、顧客に関するデータの保全、または本人確認に係る部分に限定されると解されることから、この部分について、FinTech 企業において有効な統制が確保され、安全対策の効果が実現されれば、金融機関のリスク管理策としては十分と考えられる。

なお、タイプⅢにおいて、顧客に関するデータの保全または本人確認に係る部分以外の項目（例えば、システムの安定稼働等）については、金融機関の関心の外であり、金融機関の立場からは、特段の統制の必要は生じない。但し、金融機関の関心外となった結果、全体として統制の程度が低下し、データの保全または本人確認に係る安全対策の効果が得られない、すなわち、「同等性の原則」が遵守されない可能性がある場合は、金融機関は、FinTech 企業に対して、何らかの付加的な統制を講ずる必要があることに留意が必要である。

タイプⅢにおいて、金融機関は、従来の外部委託の基準を準用するとともに、金融機関の責務の中で、自らが提供する顧客に関するデータの保全または本人確認に係る責務を担う、とすることが可能である。
なお、安全対策の効果に関して、「同等性の原則」にしたがって、必要な範囲で、追加的な安全対策を実施する場合があることに留意する必要がある。

（２）FinTech 企業に残る安全対策上の責任

タイプⅢにおいては、FinTech 企業は、情報システムの運用をクラウド事業者をはじめとした IT ベンダーに委託して実施することが、一般的である。したがって、外部委託の基準の準用という観点では、FinTech 企業は、金融機関から求められる責務と一体不可分な形で、【責務Ａ】の一部（およびそれから派生する【責務Ｂ】の一部）を担うことが、社会的には期待される。

さらに、FinTech 企業は、自らが主導して金融関連サービスを提供していることから、外部委託にとどまらず、サービス全般において、適切な安全対策を実施することが、社

削除: データの保全に係る

削除: す

削除: 【責務Ａ】の中でも、

削除: データの保全に関する

会的には期待されている。

したがって、安対基準の対象外となる FinTech 企業において、例えば、安対基準と整合的に FinTech 業界の自主的基準が策定されること等を通じて、なんらかの安全対策に関する取り組みが進められることが期待される。

（３）金融機関に責任が生じない場合の取扱い

FinTech 企業が主導し、かつ、金融機関と何ら交渉を行うことなく、一方的に金融機関から顧客に関するデータを取得するような金融関連サービスにおいては、金融機関には安全対策上の責任は生じないと解することとなる。

しかしながら、顧客の立場に立てば、こうした金融関連サービスを利用した場合には、何か問題が発生しても金融機関に頼ることができない、といった事態となることから、金融機関は、自らの顧客に対して、「一方的に金融機関から顧客に関するデータを取得するような金融関連サービス」を利用する場合の留意事項について、あらかじめ、注意喚起を行っておくことが望ましい。

５．関係者間の協調

上記検討から明らかなように、FinTech 業務における適切な安全対策の実施には、金融機関、IT ベンダーおよび FinTech 企業の３者が、密接に協調することが不可欠であり、これを欠いた場合には、利用者に不測の損害をもたらす惧れがある。

こうした協調の最も中心的な部分は、利用検討時やインシデント発生時等、それぞれの管理フェーズにおいて、金融機関に対して情報が適切に開示されることにあるが、他方で、これを FinTech 企業に対して必要な範囲を超えて求めれば、FinTech 企業に過度な負担を強いることとなり、そのイノベーションを損なうことにもなりかねない。

したがって、安全対策に係る情報開示が協調して適切に行われるよう、あらかじめ３者間で、合意をしておくことが望ましい。

また、協調を実現する手段として、外部委託先評価時に使用されるチェックリスト[9]を活用することが望ましい。そのためには、例えば、従来使用しているチェックリストを、協調を促すための情報共有手段としても位置付け、簡素化も含め内容を見直すことが考えられる。

以上

[9] 従来の安対基準においては、外部委託の利用検討時に「外部委託先を客観的に評価すること」とされており、実際の評価にあたって、金融機関は、システムリスクを含む外部委託全般に係るリスクを評価する汎用的なチェックリストを利用するのが一般的である。利用にあたっては、例えば、チェックリストを外部委託先に手交し自己チェックを依頼した後に、自己チェック結果に基づいてヒヤリングを行う等の方法が取られる。

議事２

オープンAPIのあり方に関する全銀協の検討状況

2017年2月2日

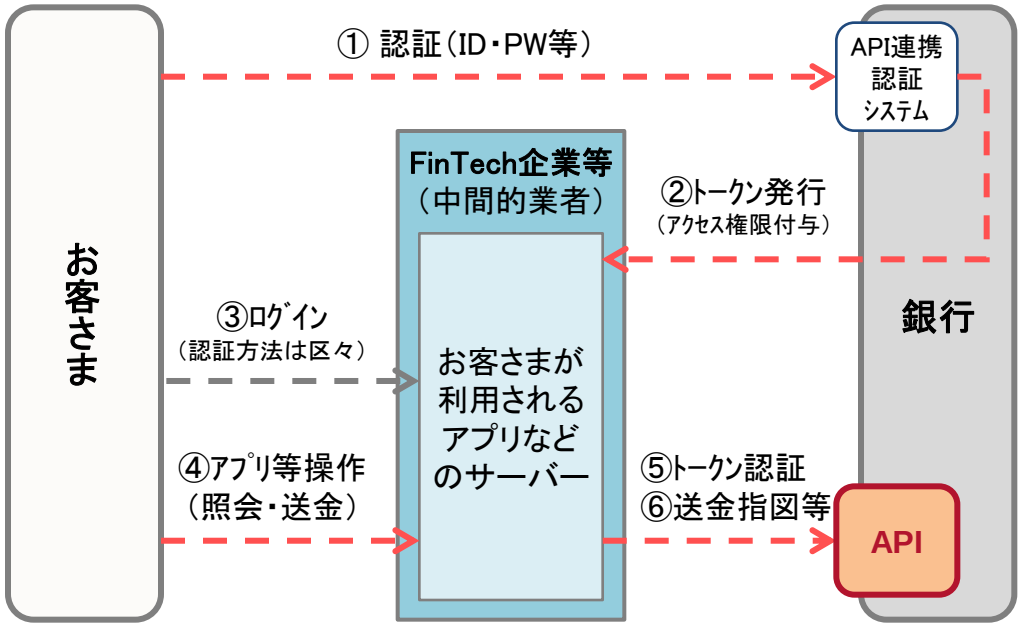
一般社団法人全国銀行協会

目次

“オープンAPI”とは

- 明確な定義はないが、一般に「API（Application Programming Interface）とは、あるアプリケーションの機能や管理するデータなどを他のアプリケーションから呼び出して利用するための接続仕様等」を指し、このうち、サードパーティ（外部企業等）からアクセス可能なAPIが「オープンAPI」と呼ばれている[1]。

APIの基本的な仕組み（OAuth2.0）



（注1）図表は実装する通信・業務フローをごく簡略化したイメージ。
（注2）なお、データ通信はインターネット回線を通じて行われることが一般的。

オープンAPIの類型（Openness）[1]

Public	• 登録すれば誰でもアクセス可能なAPI（一般的には公開情報のデータ連携に利用）	“Open” API
Acquaintance	• 一定の利用規約や契約の下で誰でもアクセス可能なAPI	
Member	• 資格要件などが定められたコミュニティに属するメンバーのみがアクセス可能なAPI	
Partner	• 相手方（パートナー）とのバイラテラルの合意に基づいてアクセスを可能とするAPI	
Private	• グループ内のエンティティのみがアクセス可能なAPI	“Closed” API

[1] Euro Banking Association “Understanding the business relevance of Open APIs and Open Banking for banks”, May 2016

金融API、銀行APIの例

- APIは様々な業種・企業において活用されているが（例：Google Maps API）、金融サービス、銀行サービスの提供に利用されるAPIは、特に「金融（Financial）API」、「銀行（Banking）API」と呼ばれる。
- APIは、外部企業等に付与する権限範囲に応じて、参照・照会系、更新・実行系に大別される。

参照・照会系API

- 株価・為替相場情報照会
- 店舗・ATM所在地
- 金利・手数料照会
- 店頭混雑状況照会
- 匿名加工・分析情報
- ポイント照会
- カード請求額照会
- 口座情報照会
- 口座残高照会
- 入出金明細照会
- KYC・AML関連情報
- 営業秘密データ　　、等
  （通常、Private APIのみ）

低 ↑ 機密性・秘匿性 ↓ 高

更新・実行系API

- 来店予約
- ローンシミュレーション
- 口座開設(*)
- 諸届（住所変更等）(*)
- 株式売買指図(*)
- 投信購入指図(*)
- 保険商品購入指図(*)
- 資金移動(*)
  - 振込・振替指図
  - 口座振替（引落）、等

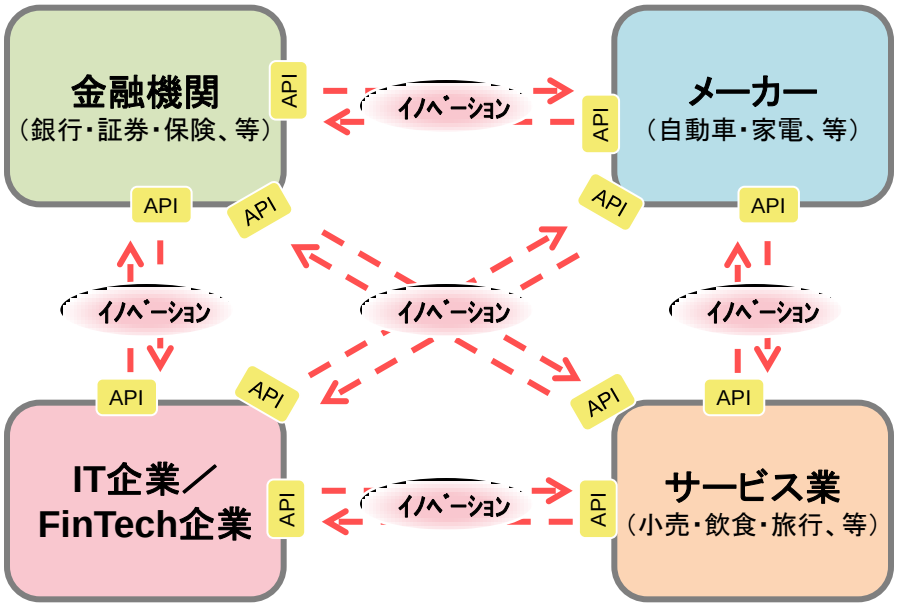
（*）登録・免許が必要となる可能性のある指図を含む。

（注）上記は、考え得る例として記載しているものであり、必ずしも実装例があるとは限らない。

オープンAPIの意義

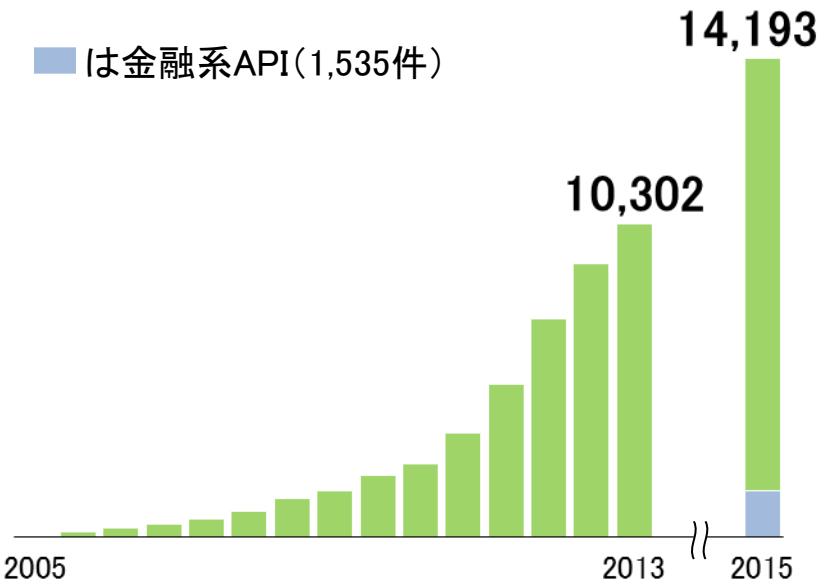
- ITの進展が金融業のあり方を大きく変容させていくことが見込まれる中で、オープンイノベーションは、今後の金融機関における基本的な戦略の一つ。
- オープンAPIは、外部企業とのセキュアなデータ連携を可能とする技術であるが、単なるデータ連携上の意義を超えて、外部企業等と金融機関が協働して、それぞれの保有する情報やサービスを組み合わせ、あるいはお互いに知恵を絞り、この「オープンイノベーション」を実現していくためのキーテクノロジーの一つと位置づけられる。
- こうした企業間の連携・協働を通じて形成される生態系は、「APIエコシステム」あるいは「APIエコノミー」と呼ばれる。

APIエコシステム、APIエコノミーの概念図



（出所） 三井住友フィナンシャルグループ （SMFG）

APIを通じて公開されている機能数の推移（グローバル）



（出所） ProgrammableWeb

金融機関の主な取組事例　わが国では協働・連携が諸外国と比較して進展

銀行名		主な取組内容	フェーズ		
			実験	参照系	更新系
日本	都市銀行A	• 2016年10月、大手ｸﾗｳﾄﾞ会計業者、大手PFM業者との法人に関する残高照会、入出金明細照会のAPI連携ｻｰﾋﾞｽを開始。今春を目途に振込に関するAPI連携の開始も目指す。	●	●	今春
	都市銀行B	• 2016年3-4月、銀行APIを活用した本邦初のﾊｯｶｿﾝｲﾍﾞﾝﾄを開催。参加者に対してﾘﾃｰﾙ向け、法人向けに、認証、残高照会、入出金明細、振込、来店予約などの幅広いﾃﾞﾓAPIを公開（=αプログラム）。 • 2016年5-6月、本番対応の前提となるβ版銀行APIを、参加者と共に最終化を実施（=βプログラム）。今春以降、振込機能を含むAPIを順次公開し、一定の審査を経たFintech企業が幅広く利用可能なAPI連携ｻｰﾋﾞｽの開始を目指す。	●	今春	今春
	都市銀行C	• 2016年7-10月、持株会社ｸﾞﾙｰﾌﾟﾍﾞｰｽでﾊｯｶｿﾝ形式のｲﾍﾞﾝﾄを開催。書類選考を経た参加企業等に対して、銀行ｻｰﾋﾞｽやｸﾚｼﾞｯﾄｶｰﾄﾞに関するﾌﾟﾛﾄﾀｲﾌﾟ金融APIを20種類以上公開。 • 2016年10月、ITﾍﾞﾝﾀﾞｰと連携し、今春を目途に、一定の審査を経たFinTech企業が幅広く利用可能な、法人に関する振込機能を含むAPI連携ｻｰﾋﾞｽの提供を目指すと発表。	●	今春	今春
	地方銀行D	• 2016年4月、大手PFM業者との残高照会、入出金明細照会のAPI連携を開始。	●	●	
	地方銀行E	• 2016年5月、大手PFM業者とのAPI連携に向けた業務提携を発表。	●		
	ﾈｯﾄ専業銀行F	• 2016年3月、大手PFM業者との残高照会、入出金明細照会のAPI連携を開始。 • 2016年8月、大手ｸﾗｳﾄﾞ会計業者との残高照会、入出金明細照会のAPI連携を開始。今春を目途に振込に関するAPI連携の開始も目指す。	●	●	今春
欧州	仏大手銀行X	• 2012年1月、APIを開始し、ｻｰﾄﾞﾊﾟｰﾃｨが開発した銀行ｱﾌﾟﾘを掲載するｱﾌﾟﾘｽﾄｱを開設。現在、46種類のｱﾌﾟﾘをｻｲﾄ上で公開・提供中。 ※ ｱﾌﾟﾘ公開は同行のｾｷｭﾘﾃｨ審査を経る必要あり。	●	●	●
	ｽﾍﾟｲﾝ大手銀行Y	• 2013年にﾊｯｶｿﾝ用APIを公開。現在ではｱﾌﾟﾘ開発者用のﾌﾟﾗｯﾄﾌｫｰﾑを設置。ｻｲﾄ上で、①ｶｰﾄﾞの購入履歴ﾃﾞｰﾀ、利用履歴ﾃﾞｰﾀへのｱｸｾｽ、②送金、③顧客の口座情報へのｱｸｾｽ等、6つのﾃｽﾄAPIを公開。※APIｱｸｾｽは承認制	●		
	独ﾈｯﾄ専業銀行Z	• 2009年設立のｲﾝﾀｰﾈｯﾄ専業銀行。預金・送金等の銀行ｻｰﾋﾞｽを、APIを通じて外部に提供し、ｻｰﾄﾞﾊﾟｰﾃｨによるｱﾌﾟﾘ開発を促すﾋﾞｼﾞﾈｽﾓﾃﾞﾙを採用。	●	●	●
米国	大手銀行L	• 2016年6月、ｸﾗｳﾄﾞ会計事業者と提携し、APIを通じて顧客情報を暗号化して同社に提供することで、同行の中小企業顧客が、より高いｾｷｭﾘﾃｨ環境下でｿﾌﾄｳｪｱを利用可能とするｻｰﾋﾞｽを提供開始。	●	●	
	大手銀行M	• 2014年9月、ﾓﾊﾞｲﾙ・ﾊﾞﾝｷﾝｸﾞの分野でFinTechを活用したｱｲﾃﾞｱを発掘するｱｸｾﾗﾚｰﾀ・ﾌﾟﾛｸﾞﾗﾑをｸﾞﾛｰﾊﾞﾙﾍﾞｰｽで開催 。一次審査通過者に対して同行のｻﾝﾌﾟﾙAPIを公開し、実用化が可能なｱｲﾃﾞｱを同行のｻｰﾋﾞｽに取込み。	●		
	中堅銀行N	• 2016年3月、開発者用ｵｰﾌﾟﾝAPIﾌﾟﾗｯﾄﾌｫｰﾑを試験導入。①複数要素認証、②Rewards（ﾘﾜｰﾄﾞ・ﾎﾟｲﾝﾄ残高照会）、③Credit Offers（年収等の基本情報を入力することでｸﾚｼﾞｯﾄｶｰﾄﾞをﾚｺﾒﾝﾄﾞする機能）、の3つのAPIを試験公開。	●		

（資料）プレスリリース、各種報道、ウェブサイト等に基づき作成
（注）内容の正確性について保証するものではない。また、全ての事例を網羅的に記載したものでもない。

オープンAPIの活用促進、円滑化に向けた全銀協の取組み

金融審・決済高度化WG報告書（2015年12月）

2. 金融・ITイノベーションに向けた新たな取組み

（中略）海外では、銀行システムの接続仕様を公表するオープンAPI の動きが進んでいる。銀行等による決済サービス等の向上、特に、銀行の決済システム等をプラットフォームとしてノンバンク・プレーヤーが利便性の高いサービスを提供していくことを促すため、我が国においても、金融機関・IT関係企業・金融行政当局等の参加を得て、セキュリティ等の観点から、オープンAPIのあり方を検討するための作業部会等を設置（平成28年度（2016年度）中を目途に、報告をとりまとめ）。

政府・日本再興戦略2016（2016年6月）

① FinTech による金融革新の推進

（中略）さらに、安価で急がない国際送金（ロー・バリュー送金）を実現する新たな仕組みの提供、情報セキュリティに留意しつつ銀行システムと連携した多様な金融サービスの創出を可能とする銀行システムの API（接続口）の公開及びブロックチェーン技術などの新たな金融技術の活用について、官民連携して検討していく。

2016年10月、全銀協に、銀行界、IT事業者、FinTech企業、学者、弁護士、消費者団体、金融庁等の関係者をﾒﾝﾊﾞｰとする「オープンAPIのあり方に関する検討会」を設置

「オープンAPIのあり方に関する検討会」の概要

2016年10月21日公表

目的

- 金融機関とFinTech企業等との連携や金融サービスの高度化に向けたツールとして、銀行システムへの接続仕様を外部事業者等に公開する"オープンAPI"への注目が高まっている。わが国銀行界においても、現在、多数の銀行がオープンAPIの活用可能性について検討を開始している状況。(全銀協アンケートによれば、48%の銀行が活用を検討中)
- 諸外国では、英国"Open Banking Standard"をはじめ、API仕様の標準化に関する検討、APIの活用を促進していく上での課題への対応(セキュリティ、利用者保護)、必要な法整備について、官民連携した取組みが進展。
- こうした動向を踏まえ、本検討会では、わが国の金融サービスの高度化、利用者利便性等の向上を実現するためのオープンAPI活用促進に向けた、官民連携のイニシアティブを取纏める。

メンバー

【メンバー】

増田　正治	(株)三井住友銀行執行役員システム統括部長
亀田　浩樹	(株)三菱東京UFJ銀行執行役員システム本部長兼システム企画部長
加藤　昌彦	(株)みずほフィナンシャルグループIT・システムグループ専門役員
梅原　弘充	(株)静岡銀行理事経営企画部長
佐々木　勉	(株)北洋銀行チャネル開発部フィンテック推進室長
吉本　憲文	住信SBIネット銀行(株)FinTech事業企画部長
佐畑　大輔	(株)NTTデータ eービジネス営業統括部長
羽川　茂雄	日本IBM(株)GBS事業本部 銀行FM金融第一インダストリーソリューション部長
丸山　弘毅	FinTech協会代表理事／(株)インフキュリオン・グループ代表取締役
Mark Makdad	FinTech協会理事／マネーツリー(株)営業部長
瀧　俊雄	一般社団法人金融革新同友会FINOVATORS／(株)マネーフォワード取締役兼Fintech研究所長
増島　雅和	森・濱田松本法律事務所パートナー弁護士
森下　哲朗	上智大学法科大学院教授
小出　篤	学習院大学法学部教授
松尾　元信	金融庁総務企画局参事官
小林　寿太郎	金融情報システムセンター企画部長
永沢　裕美子	Foster Forum良質な金融商品を育てる会事務局長

【オブザーバー】

岩下　直行	日本銀行決済機構局審議役FinTechセンター長
鎌田　沢一郎	日本証券業協会政策本部参与
中野　征治	日本クレジットカード協会／ユーシーカード(株)事業開発部長

【事務局】
一般社団法人全国銀行協会

※ 2016年10月21日現在・敬称略

（参考）主な検討事項

（※）詳細については、検討・議論を進める過程で適宜見直し。

オープンAPIにおけるセキュリティ対策及び利用者保護の基本的な考え方

Ⅰ. 背景

Ⅱ. 基本的な考え方

Ⅲ. オープンAPIの主なリスク

1. セキュリティ上の脅威とリスク

(1) API接続先への外部からの不正ｱｸｾｽに起因して生じるﾘｽｸ
(2) 銀行への外部からの不正ｱｸｾｽに起因して生じるﾘｽｸ
(3) 銀行、API接続先、利用者の間の通信に起因して生じるﾘｽｸ
(4) 内部の役職員の不正により生じるﾘｽｸ

2. API接続先のサービスに関連する利用者保護上のリスク

(1) API接続先に起因するﾘｽｸ
(2) ｲﾝﾀｰﾈｯﾄを利用した取引特有のﾘｽｸ
(3) 銀行又はAPI接続先のｼｽﾃﾑに起因するﾘｽｸ

Ⅳ. セキュリティ原則

(1) API接続先の適格性
(2) 外部からの不正ｱｸｾｽ対策
(3) 内部からの不正ｱｸｾｽ対策
(4) 不正ｱｸｾｽ発生時の対応
(5) ｾｷｭﾘﾃｨ対策の継続的な改善・見直し、高度化

Ⅴ. 利用者保護原則

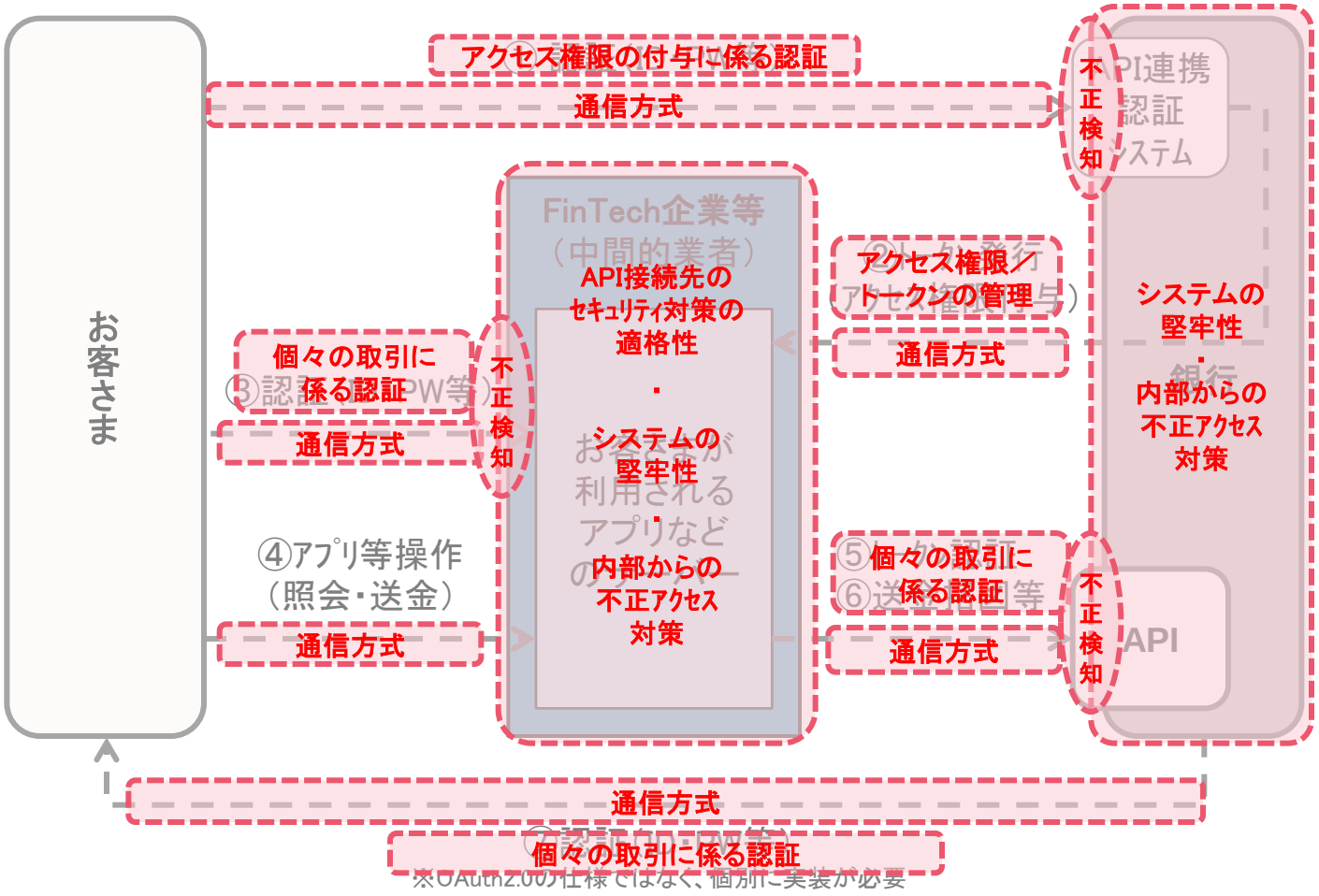
(1) API接続先の適格性
(2) 説明・表示、同意取得
(3) 不正ｱｸｾｽの未然防止
(4) 被害発生・拡大の未然防止
(5) 利用者に対する責任・補償

Ⅵ. その他

※詳細については別添の「中間的な整理（案）」をご参照。

（参考1）「セキュリティ原則」の俯瞰図

はセキュリティ対策の該当箇所



（参考2）「利用者保護原則」の俯瞰図

(1)	API接続先の適格性	利用者保護に欠ける事業者とのAPI接続の防止
(2)	説明・表示、同意取得	サービス内容等を十分に理解せずに利用することを防止
(3)	不正アクセスの未然防止	パスワード等の適切な管理を要請
	セキュリティ対策	銀行、API接続先双方でのセキュリティ対策の実施 … 前頁参照
(4)	被害発生・拡大の未然防止	速やかな機能の制限・停止
(5)	利用者に対する責任・補償	速やかな被害回復、補償等


JBA
JAPANESE
BANKERS
ASSOCIATION
一般社団法人
全国銀行協会

議事２（参考資料１）

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
【 中間的な整理(案) 】

2017年1月20日
オープンAPIのあり方に関する検討会

2017 年 1 月 20 日
オープン API のあり方に関する検討会
（事務局：一般社団法人全国銀行協会）

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

※ なお、セキュリティ原則及び利用者保護原則は、現時点の関係法令に基づいて整理したものであり、関係法令の改正等が行われた場合には当該法令に準拠した対応等が必要になることに留意すること。

Ⅰ. 背景

- 近年、金融機関と FinTech 企業等との連携を通じた金融サービスの高度化に向けたツールとして、銀行システムへの接続仕様を他の事業者等に公開する“オープン API[1]”への注目が高まっている。わが国銀行界においても、現在、多数の銀行がオープン API の活用可能性について検討を開始しているところ。
- 諸外国においては、英国“Open Banking Standard”をはじめ、API 仕様の標準化に関する検討、API の活用を促進していく上での課題への対応、利用者保護を図りつつオープン API を推進していくために必要な法整備について、官民連携した取組みが進展している。
- こうした状況を踏まえ、当検討会は、わが国金融サービスの高度化、利用者利便の向上等を実現するためのオープン API 活用促進に向けた、官民連携のイニシアティブの一環として、銀行分野のオープン API（バンキング 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を取り纏めた。
- 本文書に記載した原則は、銀行界、IT 事業者、FinTech 企業、学者、弁護士、消費者団体、金融庁等の幅広い関係者をメンバーとして議論した結果としての「規範」と位置付けられるものであり、当検討会は、オープン API に取り組む関係者において本原則が十分に尊重されることを期待する。

Ⅱ. 基本的な考え方

- IT の進展が金融業のあり方を大きく変容させていくことが見込まれる中で、オープン・イノベーションは、今後の金融機関における基本的な戦略の一つである。
- オープン API は、他の事業者等とのオープンネットワーク上でのセキュアなデータ連携を可能とする技術であるが、単なるデータ連携上の意義

[1] 明確な定義はないが、一般に API（Application Programming Interface）とは、「あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様等」を指し、このうち、サードパーティ（他の企業等）からアクセス可能な API が「オープン API」と呼ばれている。

を超えて、他の事業者等と金融機関が協働して、それぞれの保有する情報やサービスを組み合わせ、あるいはお互いに知恵を絞り、オープン・イノベーションを実現していくためのキー・テクノロジーの一つと位置づけられる。

- 金融分野におけるオープン API の活用は、現在、世界的にみても初期的な段階にあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者保護は、オープン API を活用したサービスに対する利用者の信頼を確保し、オープン API の普及、活用促進・円滑化を図る上で、重要な論点である。
- オープン API では、利用者からの申請・同意に基づいて行われるとはいえ、銀行が保有する秘匿性の高い顧客情報が FinTech 企業等の他の事業者等（以下、「API 接続先」）に提供され当該 API 接続先において蓄積・保存されるほか、銀行が決済指図等を利用者ではなく API 接続先を経由して受け取ることになる。それゆえ、オープン API に取り組むにあたっては、関係者において十分なセキュリティ対策、利用者保護が図られることが必要となる。
- 他方、API 接続先に対して、銀行と同水準のセキュリティ対策、利用者保護策を徒に求めれば、API 接続先と銀行の協働・連携による利便性の高い革新的なサービスの提供や金融サービスの高度化、イノベーションに向けた取組みが阻害され、利用者がテクノロジーの進展の恩恵を受ける機会を失うおそれがある。
- こうした認識の下、当検討会では、API の機能[2]や連携するデータの種類・秘匿性等に応じたリスクベース・アプローチに基づいて、利用者利便と利用者保護のバランスを踏まえた、銀行分野のオープン API（バンキング 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を取り纏めた。
- 取り纏めにあたっては、イノベーションを阻害しないよう留意するとともに、銀行、API 接続先双方に対して対応水準の目安を示すことで、銀行による API 接続先に対する過度に保守的なセキュリティ対策の要求や、セキュリティ上の懸念から生じる銀行側のオープン API への取組みに対する躊躇といった課題を解消し、銀行と FinTech 企業等の協調・連携の円滑化に資するものとすることを意識した。
- なお、上述の通り、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、さまざまなビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本文書では、様々なビジネスモデルやサービスに共通すると思われる主なリスクに対応したセキュリティ対策及び利用者保護策に焦点をあてて取り纏めている。
- 具体的なセキュリティ対策及び利用者保護策については、各銀行のポリシーや、個別のビジネス、各サービスのリスク、API 接続先の態様等に応じて個々に判断されるものであり、利用者保護の観点から、関係当事者において本文書の趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本文書では挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。
- 以下では、オープン API において想定される主なリスクを整理した上で、セキュリティ原則及び利用者保護原則を示す[3、4]。

[2] 例えば、更新系 API において、決済指図上限が定められていない場合、不正送金によって利用者に大きな損害が生じる可能性がある。

[3] 以下では、API 接続先が銀行の銀行代理業者又は外部委託先に該当しない場合について記載。銀行代理業者又は外部委託先に該当する場合は、銀行法に基づく利

Ⅲ．オープン API の主なリスク

・　オープン API では、金融機関のシステムに新たな通信路を設けて他の企業等を経由した新たなサービスを利用者（預金者）に提供することになるため、当該通信路を悪用したデータの漏洩・改竄や不正取引等が生じるリスクがある。これらオープン API において想定される主なリスクを列挙すれば、以下の通り。

１．セキュリティ上の脅威とリスク

(1) API 接続先への外部からの不正アクセスに起因して生じるリスク

・　API 接続先のログイン ID／パスワード等が何らかの原因で漏洩し、第三者によって、API 接続先が不正にアクセスされるリスク
・　API 接続先のシステムが第三者から攻撃を受けて、API 接続先のサービス機能の停止や、API 接続先からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

(2) 銀行への外部からの不正アクセスに起因して生じるリスク

・　トークン[5]の発行を管理する銀行側の API 連携システムが第三者によって不正に認証され、トークンが不正に取得されるリスク
・　トークンの流出や偽造等により、銀行からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

(3) 銀行、API 接続先、利用者の間の通信に起因して生じるリスク

・　ルータ等の通信経路へのハッキング、無線通信等の傍受等により、情報流出、情報改竄／消失、不正送金等が発生するリスク
・　API 接続先のプログラム不備等により、銀行のシステムがダウンするリスク
・　銀行のオープン API の通信路に不必要に大量のデータが送信され、銀行側システムの負荷が増加し、他の銀行サービスにも影響が生じるリスク

(4) 内部の役職員の不正により生じるリスク

・　内部の役職員が、利用者の情報を不正に利用（転売、私的利用を含む）するリスク

用者保護規定が適用されることに留意。

[4]　なお、セキュリティ原則及び利用者保護原則の各規定の語尾の趣旨は以下の通り。
- 「しなければならない」：　社会規範として強く求められる対応を意味する。
- 「必要である」：　銀行及び API 接続先がオープン API を活用するにあたってのベストプラクティスとして期待される対応を意味する。
- 「努めなければならない」：　その状態になるよう努力が期待される対応を意味する。
- 「考えられる」：　銀行又は API 接続先が任意に選択可能な対応を意味する。
- 「期待される」：　対象となる機関や団体に対する当検討会の期待を意味する。

[5]　OAuth2.0 において、銀行と他の企業等のアプリケーションを連携するための認証情報を保持した「許可証」。（以下同じ）

・　内部の役職員が、トークンを不正に使用して、口座残高情報の不正取得や不正決済指図を行うリスク

２．API 接続先のサービスに関連する利用者保護上のリスク

(1) API 接続先に起因するリスク

・　API 接続先の事業内容や社会的信用に疑義があり、API を利用したサービスによって、利用者に被害や混乱が生じるリスク
・　API 接続先の利用者保護態勢、経済的信用、資力等に疑義があり、利用者が十分な保護を受けられないリスク
・　API 接続先が利用者との緊急時の連絡方法を有しておらず、十分な顧客保護対応ができないリスク

(2) インターネットを利用した取引特有のリスク

・　利用者が、誰に何の権限を与えているのか、それにどのようなリスクがあるのか、API 接続先に取得される情報の利用目的は何かなどについて、十分に理解しないまま、API を活用したサービスを利用するリスク
・　トラブルが発生した場合に、利用者がどこに問い合わせたら良いかわからなくなるリスク
・　十分な説明、表示を尽くしても、利用者がよく読まずに手続きを行うリスク

(3) 銀行又は API 接続先のシステムに起因するリスク

・　API 接続先のシステムにおいて不具合、バグ等が発生し、銀行から提供された情報が正しく表示されないリスク
・　API 接続先と銀行間の通信経路に起因する障害により、利用者・API 接続先と銀行の間に取引の齟齬が発生するリスク

Ⅳ．セキュリティ原則

(1) API 接続先の適格性

（事前審査）

・　銀行は、他の事業者等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である[6]。
・　セキュリティに関連した適格性の審査にあたっては、少なくとも以下の点について API 接続先に確認することが必要である[7]。
　- セキュリティ原則の充足状況
　- 過去に発生したセキュリティ関連の不祥事案と改善状況

[6] 情報セキュリティ以外の適格性については、「Ⅴ.利用者保護原則」の「(1)API 接続先の適格性」を参照。
[7] API 接続先が ASP やクラウドサービスを利用している場合には、API 接続先から必要な開示が行われる必要があることに留意する。

- 利用者の属性や取引のリスクに応じた、継続的なセキュリティ対策の高度化に向けた態勢やリソースの有無

・ 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。

・ なお、API 接続先が任意に定めたセキュリティポリシーやセキュリティ関連文書、API 接続先が取得した情報セキュリティ関連の認証（ISO27001、TRUSTe、等）は、上記の適格性の審査にあたっての参考になると考えられる。

・ 複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される[8]。

・ なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や、銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる[9]。

（モニタリング）

・ 銀行は、API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的に又は必要に応じて確認することが必要である[10]。

・ モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、個別に判断されると考えられる。

・ 銀行は、API 接続にあたって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、必要に応じた立入検査等、情報セキュリティ対策の大幅な変更を行う場合の対応、等）を予め取り決めておくことが必要である。

・ 銀行は、API 接続先の情報セキュリティに関連した適格性に懸念があると判断した場合には、API 接続先に対して改善を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[11]。

・ なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる[12]。

[8] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。
[9] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。
[10] API 接続先が定期的な情報セキュリティ関連の外部監査を受けている場合には、それらの結果を活用すること等も考えられる。
[11] 但し、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。
[12] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

(2) 外部からの不正アクセス対策

- 以下は、アクセス権限の認可に OAuth2.0[13]、認証プロトコルに OpenID Connect1.0[14]を実装するシステムを前提とした記載。なお、同等の又はより強固な認可・認証が可能な他のプロトコル（新たなテクノロジーを含む）の採用を妨げるものではない[15]。

（アクセス権限の付与に係る認証）

- 銀行は、公表情報又は匿名加工情報を提供する場合を除き、API 接続先に対するアクセス権限の付与（OAuth2.0 においては「認可」と呼ばれる）を利用者の申請に基づき行うこととし、その際、利用者の本人認証を行わなければならない。
- 認証方式は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度とすることが必要である[16]。例えば、決済指図の権限を付与する場合には、残高・入出金明細を取得する権限を付与する場合と比較してより強固な認証方式とする等。
- 認証方式の選択にあたっては、当該銀行において採用されている他のオープンネットワークを利用した取引チャネル（例：インターネット・バンキング）の認証方式の水準が一つの目安となり得るが、以下の点にも留意が必要である。
  - 個々の取引に係る認証ではなく、アクセス権限の認可に係る認証であること
  - API を通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不正アクセスリスクに応じた認証強度とする必要があること
- 当該銀行において採用されている他のオープンネットワークを利用した取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には（例：インターネット・バンキング契約のない利用者を対象として暗証番号認証を許容する場合等）、不正アクセスリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。例えば、店頭手続・郵送確認等を併用する、資金移動上限を少額に制限する、トークンの有効期限を短期とする、不正使用発生時の補償を予め定める、等。
- その他の留意点については、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-8／Ⅱ-3-5：インターネット・バンキング）や「預金等受入金融機関に係る検査マニュアル」（別紙２-Ⅲ-1-(5)インターネットを利用した取引の管理）、金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準」、全銀協の「インターネット・バンキングにおいて留意すべき事項について」等を参考にすることが考えられる。

（アクセス権限／トークンの管理）

- 銀行は、API 接続先に付与するアクセス権限（OAuth2.0 においては「トークン」が発行される）の管理について、以下の点に留意することが必要である。

[13] アクセス権限の認可を行うためのシステムフローに関する規格。一般向けに公開されており、API 開発者は誰でも参照することが可能。IETF（Internet Engineering Task Force：インターネットで利用される技術の標準化を策定する組織）が管理・運営。
[14] 複数の API 接続先を利用する場合に、１つの ID で認証を実現できるようにする仕組みのこと。
[15] 仕様の標準化に関連する論点については、本年度内を目途とする報告書の取り纏めまでに考え方を整理する予定。
[16] 各銀行の判断に基づき、利用者保護の観点から、強固な認証方式を一律に採用することも妨げない。

- 付与するアクセス権限は、API 接続先が提供するサービスに必要な範囲に限定すること
  （利用者からの申請／同意があったとしても、不必要なアクセス権限を API 接続先に付与しないこと）
- API 接続先に発行するトークンには、利用者属性やアクセス権限の内容とそのリスク、利用者の利便性等を踏まえた適切な有効期限を設定すること
- トークンには暗号化や接続元の制限等の十分な強度の偽造・盗用対策を講じること
- 不正アクセス等を検知、または発生した場合に速やかにアクセス権限の制限、停止、取消が可能な仕組みとすること

・ 銀行は、アクセス権限やトークンを管理するシステムに堅牢なセキュリティ対策を講じなければならない。また、API 接続先に対しても、トークンの適切な管理とセキュリティ対策を求めなければならない。

（個々の取引に係る認証）

・ 利用者からの個々の取引指図（残高・入出金明細取得指図、決済指図、等）は、利用者が API 接続先のシステムにアクセスする際に API 接続先において行われる認証[17]と、銀行が個々の取引指図を API 接続先から受け付ける際に銀行において行われる認証の、二段階の認証を経て処理される。

・ 利用者保護や不正アクセス／情報流出防止の観点からは、上記いずれの認証方式とも、利用者の口座保有銀行において採用されている他のオープンネットワークを利用した取引チャネルにおける個々の取引に係る指図の認証方式と同水準以上の強度とすることが原則であると考えられる。

・ 例えば、法人利用者の口座保有銀行のインターネット・バンキングにおいて残高・入出金明細の確認に可変式パスワードや電子証明書等の固定式の ID・パスワードのみに頼らない認証方式が採用されている場合、API 接続先、銀行の双方において同水準以上の強度の認証方式を採用することが原則となる[18]。

・ 他方で、強固な認証方式の中には利用者に手続負担が大きいものや API 接続先の対応に大きな投資が必要なものもあるため、原則的な考え方を一律に適用すれば、利用者利便の大幅な低下や、利便性の高いサービスのフィージビリティが確保できなくなるおそれがあると考えられる。

・ このため、他の利用者保護策や不正アクセス／情報流出対策を組み合わせることで、利用者利便を確保しつつ、個人・法人等の利用者の属性や認証する取引のリスク等に見合った利用者保護の徹底を図っていくことも考えられる。組み合わせる他の利用者保護策や不正アクセス／情報流出対策としては、例えば以下の対策が考えられる。

（例）
- 資金移動指図に係る銀行側の認証方式をトークン認証に加えて帯域外認証も組合せ、その都度利用者を銀行側で直接認証する
- 生体認証や端末認証、複数経路認証等、一定の認証強度を確保しつつ、利便性が確保される認証方式を採用する
- 資金移動が行われた場合には、銀行又は API 接続先から利用者に対して電子メール等で通知する

[17] 但し、API 接続先が NFC（Near field radio communication：近距離無線通信）技術を用いた物理媒体による決済サービスを提供する場合等については、API 接続先における個々の取引に係る認証は、物理媒体の所持・使用を以て行われることがある。
[18] 逆に、例えば、API 接続先の認証強度がインターネット・バンキング等と比較して劣後する場合、認証強度が脆弱な API 接続先が集中的に狙われて情報流出等が発生するリスクが高まることになる。

- 利用者がアクセス可能な端末をセキュリティが確保された特定の端末や特定の種類の端末に限定する
- 利用者と API 接続先間又は API 接続先と銀行間あるいはその両方の通信方式を閉域ネットワークとする
- トークンの有効期限を短期に設定する（例えば、１回限りとする、１ヵ月から数カ月で失効させる等）
- 提供する情報の範囲や期間を制限する
- 資金移動上限を少額に制限する（例えば、１回あたりの資金移動上限を X 円、かつ簡易な認証方式に基づく資金移動の累積上限を Y 円とする）
- 資金移動先口座を強固な認証手続によって登録された口座に限定する
- 資金移動先口座を同一銀行内の本人口座に限定する
- サービスを利用可能な利用者の属性を制限する（例えば、一定の属性要件を満たす個人に限る、法人に限る、系列企業や従業員に限る、等）
- 不正送金、情報漏洩が発生した場合に銀行又は API 接続先が利用者に対して被害額を補償する [19]
- 利便性が高まる半面、認証強度が低下することによるリスクについて利用者の十分な理解と同意を得た上でサービスを提供する
- 銀行が利用者からの決済指図を API 接続先を経由せずに直接受け付ける [20]

- なお、上記の例を組み合わせれば即座に認証強度を引き下げることが可能になるわけではなく、採用する認証方式と上記の利用者保護策を組み合わせた後においても、個人・法人等の利用者の属性や認証する取引のリスクに見合った利用者保護が十分に確保されることが必要である。

（通信方式）

- 通信方式としてオープンネットワークを使用する場合、第三者による盗取等を防止する観点から、TLS を使用して保護することが必要である。

（システムの堅牢性）

- 銀行は、顧客情報について、商慣習又は信義則に基づく私法上の義務として守秘義務を負うほか、銀行法（13 条の 3 の 2：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／II-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル」（別紙２）、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」、全国銀行個人情報保護協議会が定める「個人情報保護指針」・「個人データの安全管理措置等に関する指針」等に基づき、顧客の利益が不当に害されることのないよう、当該業務に関する情報を適正に管理し、かつ、当該業務の実施状況を適切に監視するための体制の整備その他必要な措置を講じることが求められている。また、態勢が不十分な場合は、銀行法に基づく業務改善命令等の対象となる。

- 銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API では、外部委託と

[19] 但し、資金移動上限を定めない場合、被害は補償されても、反社会的勢力等に巨額の資金が盗取される可能性がある点には留意が必要。
[20] 現在、W3C（World Wide Web Consortium：ウェブ上で使用される各種技術の標準化を推進する非営利団体）において標準仕様の検討が進められている Payment Request API では、決済指図が API 接続先のサーバを経由せず、利用者の使用端末から直接銀行に送信される仕組みが検討されている。

異なり、銀行から API 接続先への情報提供は利用者からの申請／同意に基づくものであることや高い堅牢性が求められる銀行システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。

- API 接続先が確保すべき安全管理措置の水準は、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。
- API 接続先が確保すべき安全管理措置の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。但し、最低限、以下の措置については API 接続先においても必要である。
  - ウィルス対策ソフトの導入
  - 機密性の高い情報（例：API 接続先のログインパスワードやクライアント証明書、トークン、等）の暗号化
  - ファイアーウォール等のサイバー攻撃に対する多層防御の導入
  - サーバ変更監視（改ざん検知）、ネットワーク監視
  - 公開サーバ脆弱性対策
  - API 実行ログ（ユーザー、操作、結果、等）取得、保管
  - 情報喪失等に備えたバックアップ等の対策
- なお、API 接続先に、顧客の同意を得て銀行が提供する個人情報（個人データ）の個人情報保護法上の取扱は、個別のスキームに応じて個々に判断されるべきものではあるが、原則的には銀行は API 接続先に対して、個人情報委託先の監督義務（同法第 22 条）を負っていないと解するのが適当と考えられる。

（不正検知・監視機能）

- 不正検知・監視機能は、不正アクセス被害の発生やその拡大を未然に防止する上で重要な機能の一つである。
- 銀行については、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」において、データ改竄、不正アクセス、不正な取引、異常取引の検知・監視等に関する枠組みが定められている。
- 但し、オープン API においては、利用者の IP アドレスや認証失敗回数等の不正検知に活用される情報を銀行が直接入手できなくなるため、取引のリスクに応じて、銀行が必要とする場合には、API 接続先から銀行に不正検知に必要な情報が提供される仕組みを構築することが必要である。
- API 接続先についても、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、情報セキュリティ関連機関において、不正検知・監視機能の要否やその水準等についての考え方や留意点の整理が行われることが期待される。

(3) 内部からの不正アクセス対策

- 外部からの不正アクセス対策は、内部からの不正アクセスに対して効果を発揮しない場合がある。それゆえ、銀行、API 接続先の双方において内部からの不正アクセス対策が講じられることが必要である。

（銀行における内部不正対策）

- 銀行については、銀行法（13 条の３の２：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／Ⅱ-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル」（別紙２）、金融情報システムセンター（FISC）が定める「金融機関等コンピュータシステムの安全対策基準」等において、内部からの不正アクセス防止に関する枠組みが定められている。また、態勢が不十分な場合は、銀行法に基づく業務改善命令等の対象となる。

（API 接続先における内部不正対策）

- 銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出（役職員による私的な閲覧・利用、転売を含む）防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API は、銀行システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。
- API 接続先が確保すべき内部不正アクセス対策の水準は、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。
- API 接続先が確保すべき内部不正アクセス対策の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。但し、最低限、以下の措置については API 接続先においても必要である。
  - 役職員に対するシステムアクセス権限の適切な設定・運用
  - アクセスログの記録保存、定期的な査閲
  - 役職員に対する教育・研修の実施
  - サーバルームの監視、認証、入退出管理 [21]
  - 重要な機密情報・顧客情報の媒体（USB）等へのデータのコピー制限、禁止
  - 重要な機密情報・顧客情報のデータの持出、削除、廃棄管理

(4) 不正アクセス発生時の対応

（システム設計・仕様）

- 銀行及び API 接続先は、不正アクセスが判明した場合に被害発生やその拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことができるシステム設計・仕様としなければならない。

[21] クラウドサービスを利用している場合においては、安全対策基準「クラウドサービスの利用」に定めるところに拠る。

・ 銀行及び API 接続先は、不審な資金移動等についての利用者からの照会への対応や、不正アクセス発生時の原因調査、必要な対策の検討を行うため、適切なアクセスログの記録及び保存を行わなければならない。

（情報連携、対策協議）

・ 不正アクセス発生時には、速やかに銀行と API 接続先の間で情報連携を行うとともに、原因調査や必要な対策の協議等を協力して行っていくことが必要である[22]。必要な対応については、銀行と API 接続先との間で予め取り決めて明確化しておくことが必要である。

(5) セキュリティ対策の継続的な改善・見直し、高度化

・ サイバー攻撃やサイバー犯罪の手口は年々巧妙化している上、オープン API を活用した金融サービスの提供は世界的にみても現状、初期段階にある。そのため、銀行及び API 接続先は、自社のみならず他社での不正アクセス事例等を踏まえ、セキュリティ対策の継続的な改善・見直し、高度化を図っていくことが必要である。

・ セキュリティ対策の改善・見直し、高度化に向けては、銀行及び API 接続先は、協力して取り組むことが重要と考えられる。

Ⅴ. 利用者保護原則

(1) API 接続先の適格性

（事前審査）

・ 銀行は、他の事業者等との API 接続に先立ち、利用者保護等の観点から、API 接続先の適格性を審査することが必要である[23]。

・ 適格性の審査にあたっては、少なくとも以下の点について API 接続先に確認することが必要である。
  - グループ会社を含めた事業内容、兼業内容
  - 反社会的勢力との関係の有無を含む社会的信用、組織ガバナンス
  - 法令遵守態勢
  - 利用者保護態勢[24]
  - 利用者保護原則の充足状況
  - 過去に発生した利用者保護関連の不祥事案と改善状況
  - 利用者の属性や取引のリスクに応じた、継続的な利用者保護策の高度化に向けた態勢やリソースの有無

[22] その他の不正アクセス発生時の対応については、「Ⅴ.利用者保護原則」の「(4)被害発生・拡大の未然防止」を参照。
[23] 情報セキュリティ関連の適格性については、「Ⅳ.セキュリティ原則」の「(1)API 接続先の適格性」を参照。
[24] 特に顧客情報の適切な取扱・管理態勢や、取得情報の利用目的の適切性、利用約款の適切性（過度な免責規定等、利用者保護に著しく欠ける条項の有無）、について確認する。

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が定めた社内規定等は、上記の適格性の審査にあたっての参考になると考えられる。
- 複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される [25]。
- なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や、銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる [26]。

（モニタリング）

- 銀行は、API 接続先の適格性について、API 接続後も定期的に又は必要に応じて確認することが必要である。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、個別に判断されると考えられる。
- 銀行は、API 接続にあたって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、API 接続先に提出を求める情報、API 接続先が大幅な態勢見直しや業務停止等を行う場合の対応、等）を予め取り決めておくことが必要である。
- 銀行は、API 接続先の利用者保護態勢等に関する適格性に懸念があると判断した場合には API 接続先に対して改善を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない [27]。
- なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる [28]。

（その他の留意点）

- API 接続先において API 接続を通じて提供する金融サービスに関して利用者保護に欠ける不祥事案等が発生した場合、銀行と API 接続先との関

[25] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。
[26] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。
[27] 但し、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。
[28] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

係、利用者からの見え方等によっては、銀行側も社会的な批判を浴びる等のレピュテーションリスクが生じる可能性に留意が必要である。

- API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ銀行側も自行サービスの提供を取り止めて、預金者に対して API 接続先のサービスの利用を推奨する場合は、形式上、銀行と API 接続先の間に外部委託契約が締結されていなくとも、その実態において同視され、銀行法に基づく外部委託規制の対象となる可能性があることに留意が必要である。
- API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ利用者の大部分が当該 API 接続先のサービスの利用に依拠する場合は、API 接続先のシステム障害や業務停止等によって、利用者が金融サービスを利用できなくなり、混乱が生じるおそれがあることに留意が必要である。
- 事前の取決めにおいて、API 接続先における障害等によって銀行の業務に影響が生じるおそれがある場合には、ただちに銀行に連絡するよう定めておくことが必要である。なお、その他の障害等の報告要否やタイミングについても、予め取り決めておく必要があることに留意する。
- API 接続先もしくは銀行の都合によるサービス停止を行う際は、一定期間の事前通知期間を設定することが必要である。

(2) 説明・表示、同意取得

（重要な情報の表示、同意取得）

- インターネットを利用した取引は、基本的に画面に表示される情報に基づいて利用者の判断・同意が行われ、また、必要な情報を表示しても、利用者が十分に確認せずに、手続きを進める可能性がある。
- そのため、銀行及び API 接続先は、利用者の判断・同意に必要な情報を単に提供・表示するに止まらず、わかりやすく画面表示するとともに、誤認・誤解を招く表現を避け、また、利用者に重要な判断・同意を求めるものについては注意喚起プロセスを設けることや、利用者のシステム操作による同意を求めること等、利用者保護に十分配慮した表示方法、画面構成とすることに努めなければならない。
- 銀行は、トークン発行にあたって、少なくとも以下の点について、わかりやすく画面表示の上、利用者の同意を求めることが必要である。
  - アクセス権限を付与する API 接続先の名称
  - API 連携するサービス等の名称
  - 付与する権限の内容・範囲
  - 付与する権限の有効期限[29]
  - 付与した権限の削除、解除方法
  - その他注意喚起が必要な事項
- API 接続先は、サービス提供にあたって、少なくとも以下の点について、わかりやすく画面表示の上、利用者の同意を求めることが必要である。
  - 個人情報保護法に基づく取得した情報の利用目的、共有範囲（第三者提供の有無）
  - 取得した情報の削除に関する事項

[29] リフレッシュトークンを発行する場合には同トークンによって延長される最大の有効期限。

- サービス利用上の制限
- その他注意喚起が必要な事項

（リスク等に関する表示）

- API 接続先は、提供するサービスに関して生じる主なリスクの適切な表示に努めなければならない。
- API 接続先は、サービス提供時間帯又は停止時間帯、休日・休業等のサービス提供上の制約について適切な表示に努めなければならない。

（利用者の誤認防止）

- 以下の点については、特に利用者の誤認や誤解が生じるおそれがあることに留意し、適切に表示することに努めなければならない。
  - API 接続先が提供するサービスは銀行が提供するサービスとは異なること
  - 銀行と API 接続先の関係、それぞれの役割（特に API 接続先が銀行代理業者又は銀行の外部委託先でないこと）
  - 決済指図取引と他のサービスの区別
  - 銀行と API 接続先の画面の区別
- なお、銀行は、API 接続先が虚偽又は意図的に誤認を招く表示を行っていることが判明した場合には、API 接続先に対して是正を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消、関係当局への通報等の必要な措置を講じなければならない。

（その他の表示）

- 銀行及び API 接続先は、利用者からの相談・照会、苦情、問合せがあった場合の役割分担、業務フロー等を、予め取り決めておくことが必要である。
- 銀行及び API 接続先は、上記の取決め内容を踏まえ、利用者からの相談・照会、苦情、問合せに対応するための連絡先を表示することが必要である。
- API 接続先は、商号、代表者、住所、連絡先等について表示することが必要である。
- API 接続先は、電磁的方法による決算公示を選択している場合、会社法に基づく決算公告についても表示することが必要である。

(3) 不正アクセスの未然防止

- API 接続先は、不正アクセスを未然に防止する観点から、例えば以下の点について、利用者に注意喚起することに努めなければならない。
  - API 接続先のログインパスワード等は、銀行サービスに利用しているパスワード等と異なるものを設定すること
  - API 接続先のログインパスワード等は、類推されやすいものを避けること、適切な管理に努め第三者に貸与、開示しないこと、定期的に変更すること
  - セキュリティ対策ソフトを導入すること
- API 接続先は、利用者に対して、API 接続先のパスワード等の紛失、漏洩や不正アクセスの懸念がある場合には、ただちに API 接続先に対して連絡するよう求めておくことが必要である。

(4) 被害発生・拡大の未然防止

（初動対応）

- 銀行又は API 接続先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことが必要である。
- 銀行と API 接続先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、一方で API に関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を銀行と API 接続先間において予め取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。
- API 接続先が複数の銀行と接続している場合において、他の銀行においても同様の事案が発生するおそれがある場合には、API 接続先は、当該他の銀行に対してもただちに連絡し、被害拡大を未然に防止することに努めなければならない。

（利用者への連絡）

- 被害が発生した利用者への連絡や、被害が広範な利用者に及ぶ可能性がある場合に利用者にただちに十分な注意喚起（例えば、ただちにパスワード等の変更を求める等）ができるよう、API 接続先は、利用者との連絡手段を予め確保しておくことが必要である。
- 利用者に届出・登録を求める連絡手段の範囲については、提供するサービスの内容や取引のリスクに応じて、個別に判断されると考えられる。
- 銀行は、API 接続先が利用者との十分な連絡手段を予め確保することができない場合、被害発生時に、銀行が API 接続先に代わって利用者に対し連絡、注意喚起する必要が生じる可能性に留意することが必要である。

(5) 利用者に対する責任・補償 [30]

- オープン API では、取引指図の処理・実行に API 接続先と銀行の双方が関与するため、情報流出や不正送金、システム上の不具合等により利用者に損害が発生した場合、利用者に対する責任の所在や、対応窓口・主体等が不明確になるおそれがある。
- 当事者の民事上の最終的な損害賠償責任を司法の判断に委ねた場合、速やかな被害回復、補償等が図られず、利用者保護に欠けるおそれがある [31]。

（当事者間における事前の取決め）

- 銀行及び API 接続先は、利用者に対して速やかな被害回復、補償等を図る観点から、不正アクセスや情報流出、不正送金、システム上の不具合

[30] 2016 年 12 月 27 日付で公表された金融審議会・金融制度ワーキンググループ報告書では、「金融機関は（中略）業者との間で締結する契約において顧客に生じた損失の分担を定め、公表することとする」（報告書８頁参照）とされており、当該記述を踏まえ、本節は、利用者の保護を適切に確保していくための銀行及び API 接続先と顧客との間の損失分担ルールのあり方について検討したもの。

[31] なお、本節における記述は、API 接続先及び銀行が利用者保護の観点から自主的に行うことが期待される取組みであり、それぞれの利用者に対する最終的な法的責任を加重又は軽減するものではない。

等が発生した場合の対応窓口や、利用者に損害が生じた場合の補償・返金方法（含む、その主体）[32]、補償範囲について、予め取り決めておかなければならない[33]。なお、利用者に対して双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行ってはならない[34]。

- API 接続先及び銀行は、予め取り決めた利用者に対する補償・返金方法とその補償範囲（免責事由も含む）について、API 接続先及び銀行は、ウェブサイト等において利用者が常時確認できるよう表示するとともに、API 接続先が利用者と利用契約を締結する際にわかりやすく画面表示する等により、利用者が補償・返金を求める際の対応窓口やその方法について十分認識できるよう努めなければならない。

（補償内容・範囲に関する考え方）

- API を利用したサービスによる預金等の不正な払戻しについて、銀行及び API 接続先に過失がない場合でも、利用者が個人であって利用者自身の責任によらずに被害に遭われた場合については、上記事前の取決めに基づいて銀行又は API 接続先から補償を行うことが必要である。なお、利用者に重大な過失又は過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担にすることも含め、個別に判断されることが必要である。
- 法人の利用者については、個人の利用者と比較して、セキュリティ対策等への対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、サービス提供者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人の利用者に対する補償については、利用者が行っていたセキュリティ対策や不正利用被害の防止に関する状況、法人の属性やセキュリティ対策への対応力等の点を考慮して、個別に判断されることが必要である。
- 銀行及び API 接続先は、API を活用したサービスの形態や利用者の属性等に鑑みて、上記と異なる補償内容・範囲とすることに合理的な理由がある場合であって、かつ利用者に不測の損害が生じないよう、かかる補償内容・範囲について利用者に適切に説明又は表示した場合に限り、補償内容・範囲を個別に定めることができる。

（API 接続先が補償・返金責任を負う場合の留意点）

- 銀行と API 接続先との間の取決めに基づき API 接続先が利用者に対して補償・返金責任を負う場合、銀行は、API 接続先の利用者に対する補償・返金に係る態勢や資力等が利用者保護に欠けるおそれがないかに留意の上、API 接続の是非を判断するとともに、それらの状況について定期的に又は必要に応じて確認することが必要である。
- 銀行は、API 接続先の補償・返金の態勢や資力等が利用者保護に欠けるおそれがあると判断した場合、API 接続先に対して態勢の見直しや責任財産の充実、責任保険への加入を求め、API 接続先においてそれが困難な場合は API 接続しない（あるいは接続の停止又は取消を検討する）等の

[32] 利用者への補償・返金後の、銀行と API 接続先の間の内部分担（求償）についても、別途予め取り決めておくことが望ましい。
[33] 銀行及び API 接続先が利用者に対して連帯して責任を負うこととする場合でも、利用者からみて対応窓口・主体等がわかりにくくなるおそれがあることから、任意の一次的な補償・返金方法（含む、その主体）等について、予め取り決めておくことが望ましい。
[34] その前提として、銀行は、API 接続先の利用約款について、消費者契約法等を踏まえ、不相当に API 接続先の責任を限定する条項が定められていないかを精査することが必要である。

対応を行うことが必要である。

- API 接続先の利用約款等において API 接続先の免責事由が過大に定められている等（例えば、過失責任も負わない等[35]）、実質的に利用者に対する補償・返金責任が果たされないおそれがある場合、消費者契約法等を踏まえ、見直しを求めることが必要である。

Ⅵ. その他

（公表情報の取扱）

- 店舗・ATM の所在地等、銀行のウェブサイト等においてログイン等の手続きを要さずに取得可能な公表情報（以下、「公表情報」）を API 接続先に提供する場合は、上述の記載にかかわらず、以下の取扱とすることが考えられる。
  - 銀行と API 接続先との通信経路において改竄が行われることを防止する観点から、銀行と API 接続先との通信方式は、セキュリティ原則「(2) 外部からの不正アクセス対策」に定める通信方式に拠るものとする。
  - API 接続先は、システム上の不具合や外部又は内部からの攻撃による改竄等によって、銀行に利用者からの問い合わせが行われる可能性のある事態が発生した場合には、ただちに関係銀行に対し連絡するよう努めなければならない。
  - 銀行は、API の利用約款等において、不具合発生時等の責任について予め定めておくことが望ましい。
  - 銀行は、公表情報を提供する API のアクセス量を銀行側でコントロールできない場合には、システムキャパシティの超過が原因で不具合が発生するリスクに留意するものとする。

（API 接続先の API 接続先の取扱）

- 銀行は、API 接続先との間で「API 接続先の API 接続先」（以下、「API 連鎖接続先[36]」）の取扱について予め取り決めておくことが必要である。
- これには、例えば、API 接続先と同様に取扱う（銀行が API 連鎖接続先と直接契約を締結）、API の連鎖接続について銀行の承諾又は銀行への事前通知を条件とする、連鎖接続を許容する条件を双方協議の上予め定める、API 接続先の責任と管理の下で連鎖接続を許容する等、様々な方法が考えられる[37]。
- いずれの方法による場合であっても、API 連鎖接続先において、本原則の趣旨を踏まえて、十分なセキュリティ対策と利用者保護が図られていることが重要である。

[35] なお、事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項や、当該事業者、その代表者又はその使用する者の故意又は重大な過失による事業者の債務不履行により消費者に生じた損害を賠償する責任の一部を免除する条項等は、消費者契約法（第８条乃至第１０条）に基づきそもそも無効とされる。

[36] 銀行に対する API 接続先からの取引指図が、API 接続先と API 接続する他の事業者等の取引指図に基づいて行われる場合における、当該他の事業者等をいう。

[37] API 連鎖接続先の取扱は、例えば、取引のリスクに応じて参照系 API と更新系 API との間や、API 連鎖接続先が API 接続先と同一グループに属するか否かによって異なる取扱とすることも考えられる。

・　なお、API 接続先が有する自社の情報を同接続先の API を通じて他の事業者等に提供することは、API の連鎖には該当しないが、個人情報保護法等に基づき適切な利用者保護が図られる必要があることに留意する。

（業界・企業横断的なセキュリティ対策に関する取組み）

・　関係者においては、業界・企業横断的な不正アクセス事案やセキュリティ関連対策の情報共有の枠組みについて、セキュリティ関連団体等との連携を含め、引き続き検討していくことが期待される。

・　関係者においては、本原則を必要に応じて見直し・改訂していくことが必要である。なお、事務局における改訂要否の検討等の参考とするため、本原則についてご意見がある方は、末尾に掲示した意見提出先までご連絡いただきたい。

（バンキング API 以外の API における本原則の活用）

・　当検討会は、銀行以外の事業者がオープン API を提供する場合においても、本文書で定めたセキュリティ原則・利用者保護原則が、当該事業者におけるセキュリティ対策、利用者保護態勢を整備する上で、参考になることを期待する。

以　上

【本原則に対する意見提出先】

open-api＠zenginkyo.or.jp
（事務局：一般社団法人　全国銀行協会）

議事３

API 接続先チェックリスト（仮称）ワーキンググループの設置

一般社団法人全国銀行協会が取り纏めを行っている「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【中間的な整理（案）】」において、複数の銀行と API 接続する企業等における審査対応負担を軽減することを目的に、「API 接続先チェックリスト（仮称）」（銀行が API 接続先の適格性審査等を行う際に使用）の制定が期待されている。

これを受けて、以下の通り、FISC が事務局となり、当該リストおよび維持管理方法等の原案を作成することを目的としたワーキンググループを運営することを予定している。

オープン API は、「金融機関における FinTech に関する有識者検討会」におけるタイプⅢの実現形態の一つであることから、ワーキンググループでは、タイプⅢのサブルール等の議論を踏まえて検討が行われることとなる。したがって、サブルール等の議論が適切に反映されているかどうかを、本検討会において都度検証いただくこととしたい。

また、以上のことから、ワーキンググループの成果物は、本検討会の提言事項の一つとしたい。

１．委員

（別紙参照）

２．運営方針

・「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【中間的な整理（案）】」（一般社団法人全国銀行協会、2017 年 1 月 20 日）の「Ⅳ．セキュリティ原則」を踏まえた議論を行う。
・「API 接続先チェックリスト（仮称）」および当該リストの維持管理方法等の検討にあたっては、最初に FISC から原案等を提示した上で検討を進める予定。
・検討状況については、「金融機関における FinTech に関する有識者検討会」に都度報告する。
・成果物については、「金融機関における FinTech に関する有識者検討会」に上程する（本検討会の報告書の一部として掲載し、公表する予定）。

３．開催予定

・検討期間は 2017 年 2 月上旬～6 月末の約 5 ヶ月間、初回は 2 月 7 日（火）10 時～12 時（FISC 会議室）に開催予定（第 2 回は 2 月 20 日（月）15 時～17 時の予定）。
・隔週開催を想定しているが、検討状況や関係者との調整等により柔軟に対応する。

以　上

別紙

API 接続先チェックリスト（仮称）ワーキンググループ
委員名簿

（敬称略）

区分	氏名	所属・役職
銀行 （3 名）	奥野　瑞穂	株式会社みずほ銀行 e-ビジネス営業部　調査役
	小原　彰	株式会社三井住友銀行 システム統括部　統括グループ　グループ長
	原田　一雪	株式会社三菱東京 UFJ 銀行 デジタルイノベーション推進部　次長
FinTech 企業 （3 名）	土佐　鉄平	freee 株式会社 開発本部　チーフセキュリティアーキテクト
	大目　晃弘	マネーツリー株式会社 事業開発部　ビジネスデベロプメントマネージャー
	内波　生一	株式会社マネーフォワード アカウントアグリゲーション本部　本部長
IT ベンダー （3 名）	村上　隆	株式会社エヌ・ティ・ティ・データ 第四金融事業本部　企画部　シニア・スペシャリスト
	鎌田　美樹夫	日本アイ・ビー・エム株式会社 グローバル・ビジネス・サービス事業部　金融インダストリー・ソリューション　担当部長
	谷内　圭	富士通株式会社 金融システム事業本部　デジタルビジネス開発室　シニアマネージャー
FISC （1 名）	亀水　宏次	公益財団法人金融情報システムセンター 監査安全部　次長
オブザーバー （3 名）	小林　侑剛	金融庁 総務企画局　企画課　信用制度参事官室　課長補佐
	市村　雅史	金融庁 検査局　総務課　専門検査官
	中井　大輔	日本銀行 金融機構局　考査企画課　企画役

（事務局：公益財団法人金融情報システムセンター　企画部）

以　上

議事４

クラウドサービス利用時のリスク管理策に関する補足的検討

金融機関がクラウドサービスを利用する際のリスク管理策に関する補足的な検討にあたり、以下のとおり、その論点を明確にするとともに、それを踏まえた原案を別紙のとおり作成したので、ご議論いただきたい。

【主論点】

FinTech 業務をはじめとして、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、従来のクラウドサービス利用時のリスク管理策に対して、どのような補足を行うことが必要となるか？

【論点に係る原案の構成】

１．補足的な検討の観点

・重要な情報システムでクラウドサービスを利用する場合を想定した、補足的検討が有益であること、そのために、クラウドサービス固有の性質を特定することが有益であることを明確にする。
・また、英国を中心とした海外先進諸国のクラウドサービス利用に係るガイドラインの特徴を明確にする。

２．クラウドサービス固有の性質

・外部委託の一形態としてのクラウドサービスの位置づけを明確にする。そのうえで、安全対策上特定が必要となるクラウドサービス固有の性質として、「匿名の共同性」「情報処理の広域性」「技術の先進性」を明確にし、補足的検討が必要な観点を明確にする。

３．リスク管理策に関する補足

・主に重要な情報システムでクラウドサービスを利用する場合を想定して、客観的評価を実施する際の留意事項、データアクセス拠点の所在地の把握、監査権の明記、監査の実施、監査人等モニタリング人材の配置といったリスク管理策について補足を提案する。

【論点に係る原案】

・別紙１参照。

以上

別紙１

クラウドサービス利用時のリスク管理策に関する補足的検討

１．補足的な検討の観点

「金融機関におけるクラウド利用に関する有識者検討会」（以下「クラウド検討会」という）報告書、およびそれを踏まえて安対基準第８版追補改訂において策定されたクラウドに関する基準（以下「クラウド基準」という）に関して、以下の観点から、補足的な検討を行うことが有益である。

（１）クラウド基準策定後の状況の反映

クラウド基準策定後、金融機関におけるクラウドの利用が進む[1]とともに、金融機関のFinTechへの取組みも急速に活発化する中で、FinTech業務ではクラウドサービスが利用される場合が多いことから、今後、クラウドサービスの利用が益々進展していくことが予想される。一方で、外部委託検討会が行われ、「重要な情報システム」の意義が明確化される等、クラウド検討会で提言されたリスクベースアプローチの議論が更に深められてきた。そうしたクラウド基準策定後の状況を踏まえて、クラウド基準が「重要な情報システム」に適用される場合（FinTechのユースケースとしてはブロックチェーン・AI等）を想定し、クラウド基準の実効性を更に高める観点から、クラウド基準をより明確化すべき点が無いか等、補足的な検討を行うことが有益である。また、補足すべきリスク管理策の観点を明らかにするためには、クラウドサービス固有の性質を特定することが有益である[2]。

（２）海外先進諸国の動向

クラウド検討会の前後で、海外先進諸国において、クラウドサービス利用に係るガイドラインの策定[3]が進んでいることから、海外先進諸国のガイドラインを参考とすることが有益である。

海外先進諸国におけるガイドラインでは、我が国のクラウド基準と共通する点が多いが、特に特徴的なのは以下の点である。

・金融機関は、外部委託された業務に関連するデータに、実効的なアクセスが可能となるよう要求されている。ここでいう「データ」には、金融機関のデータ、顧客のデータ、取引履歴データだけでなく、システムや手続きに関するデータも含まれる[4]とされ、その範囲を狭めようとすることは適切でないとされている。また、そうした考え方に基づいて、アクセスの対象となる事業拠点に関しては、本社や事務センタ

[1] クラウド検討会直前の平成25年度、クラウドを利用している金融機関等は26.6%であったのに対して、平成27年度には、36.5%と増加している。詳細は【参考】を参照。

[2] クラウドサービス固有の性質を特定することは、今後、クラウド基準を外部委託全般に適用可能なものとクラウド固有のものとに整理する際にも有益である。詳細は、外部委託報告書脚注31を参照。

[3] 米国・英国・星国ではクラウドサービス利用に係るガイドラインがあるが、ここでは、特に2016年7月に制定された英国の「Guidance for firms outsourcing to the 'cloud' and other third-party IT services」をもとに、特徴を言及している。

[4] 例えば、要員の身元調査手続き、システム監査証跡等も含まれるとされている。

ーを含み幅広く解される一方で、必ずしもデータセンターへのアクセスが必要とならない場合もあり得るとされている。さらに、管轄権については、データアクセスの実効性を高める観点から、クラウド事業者との契約は、国内法の管轄下にあることをデファクトとしている。これらは、クラウドサービスの利用において、一般的に金融機関の統制の程度が低くなることを踏まえて、統制上必要となるデータへのアクセスに焦点を当てて、明示的に要求されているものと解される。

・要求事項を設定する目的を、「金融機関が、外部委託先を利用することに伴うオペレーショナルリスクを、適切に特定し、管理するよう促すこと」にあるとし、そのうえで、「金融機関にオペレーショナルリスクが増大することがないよう」求められている。要求事項の多くは、リスク管理、監督といった一般的な統制の方法に関する事項が中心となっており、設備等技術といった統制の内容に関する言及はほとんどない。これは、外部委託の有無に関わらず、統制水準は同一に維持すべき（安全対策の効果は同等であるべき）という基本的な考え方を明確に示す一方で、それらが十分に理解されていれば、金融機関の特性や規模等で様々にとりうる個々の技術的なリスク低減策は、一義的には金融機関に委ねられるべきである、としているものと解される。

以上のことを踏まえ、まず、クラウドサービス固有の性質を詳述し、「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中心に、補足的な検討を行う。

２．クラウドサービス固有の性質

クラウド検討会では、クラウドサービスは「外部委託の一形態として扱うことが適当」であるとされた。ここでいう外部委託とは、システム資源の調達先を表した言葉であり、その一形態であるクラウドサービスは、システム資源の調達の観点から、その性質を整理することが妥当である。

そもそも、システム資源の調達について、安対基準が策定された当初に遡れば、調達形態は現在ほど多様ではなく、例えば、建物・電源・空調・水冷等の設備一式、業務アプリケーションの開発や情報システムの運用要員等は、基本的には金融機関が自前で用意するのが一般的であり、外部から調達するのは、せいぜいホストコンピュータやテープ装置等のハードウェアや、オペレーティングシステムやデータベースシステム等の基本ソフトウェア、そして一部の開発運用要員程度であった[5]。

その後、コスト削減や先進技術の利用等を目的に、情報システムの運用に係る資源をまとめて外部から調達する、いわゆるアウトソーシングが徐々に進展した結果、今や勘定系基幹システムにおいて、金融機関の 90%以上が外部委託を利用している現状にある。同時

[5] そのため、安全対策における統制にあたっては、金融機関の内部が主な対象となることから、安対基準の初版では基準全 113 項目のうち、外部委託に関する項目は２項目となっていた。

に、これによって、金融機関は、統制の重点を内部から外部にシフトさせる必要が生じるとともに、統制の重点がシフトする中においても、安全対策の効果は、自前で調達する場合と同等に維持すべく、付加的な安全対策を実施することが必要となった[6]。

このようなシステム資源の調達方法とそれに伴う統制の重点の変化の途上で、クラウドサービスが登場した。クラウドサービスは、システム資源の調達において、従来の外部委託と比べて、利用者のニーズに応じた柔軟な調達が可能[7]となることから、金融機関が多岐にわたる FinTech に取り組む中で、利用が一層進展していくものと予想される。

同時に、金融機関にとっては、統制の対象としてのクラウドサービスの位置づけが、従来にも増して高まることが予想され、近年のクラウドサービスの状況を踏まえ、その固有の性質を以下のとおり整理し、補足的検討が必要な観点を明らかにする。

（1）匿名の共同性

クラウドサービスは、複数の事業者が、単一のクラウド事業者に委託する形態として共同性という性質を有する一方で、利用者間で何らコミュニケーションが無いという匿名の共同性を有する。

そのため、安全対策を決定する主な役割は、個々の利用者ではなくサービス全体に責任を負うクラウド事業者に帰属することとなり、例えば、個々の利用者からの個別の監査要求や、個別の改善要望の実現に対して、消極的となる傾向があるとともに、監査において必要となるデータセンターへの立入については、セキュリティ上の問題を惹起するとして、受け入れを拒否することとなる。したがって、クラウドサービスは、同様に共同性を有する形態である共同センターと比較して、金融機関による統制が十全に機能せず、リスク評価やリスク低減策を適切に実施できない、という問題が内在している。

一般の情報システムにおいては、金融機関がリスクに応じて統制の程度を決定すれば十分であるが、重要な情報システムにおいては、インシデント発生時の社会的影響が甚大であり、特に有事において、金融機関には、従来の重要な情報システムの外部委託と同程度に、クラウド事業者に対する統制能力を十全に発揮することが必要となる[8]。統制の検討にあたっては、外部委託検討会報告書で提言された「共同センター[9]」において行

---

[6] 最新の安対基準第８版追補改訂においては、外部委託に関する基準は 11 項目に増加した（うちクラウドサービスの基準は５項目）。なお、統制の重点が内部から外部へシフトしていく実態を、安対基準の構成等に、適切に反映していくことが、今後の安対基準改訂において必要となると考えられる。

[7] 柔軟な調達の特徴として、費用の経済性・調達の即時性・調達手続きの容易性・システム管理の効率性が考えられる。「費用の経済性」とは、情報処理の規模が大きいことから、規模の利益が働き相対的に低廉に利用できる余地があることをいう。「調達の即時性」とは、利用を決定してから実際のサービスインまでの時間が相対的に短いことをいう。「調達手続きの容易性」とは、例えば、システムの利用要件をインターネットから簡単に設定できること等をいう。「システム管理の効率性」とは、例えば、ハードウェア個々の管理が不要となること等をいう。また、安全対策面の特徴として、金融機関と比べて、セキュリティ投資額が大きい点（毎年数十億円を投下しているクラウドベンダーもある）、情報処理が広域に行われることでサービス継続性が高い点、が指摘されることがある。

[8] クラウド基準では、平時における統制能力の発揮を想定し、運用時のモニタリングにおいては、実効的かつ効率的な統制手法として、第三者監査の利用を選択肢として提言されるとともに、平成 28 年５月のシステム監査指針の改訂では、「クラウドサービス監査のポイント」として、第三者監査人を利用した共同監査方式について、そのプロセスや考慮点まで踏み込んだ具体的な提言がされている。

[9] 共同センターは複数の金融機関が共同で重要な情報システムの運用等を委託する形態であり、安全対策の効果が複数の利用者に及ぶ共同性という性質を有する点でクラウドサービスと同じ性質を有する。

われている統制の観点を踏まえてリスク管理策を検討することが考えられる。

以上から、重要な情報システムに関する補足的検討にあたっては、共同性という性質に関しては、共同センターに適用されるリスク管理策[10]を参考としつつ、匿名性という性質に伴う、統制の低下を補完するためのリスク管理策について明確化を行うことが適当である[11]。

（２）情報処理の広域性

クラウドサービスでは、利用者が広域に及ぶことから、情報処理拠点を含む事業拠点も、複数の国にまたがり広域に及ぶ。そのため、利用者は、事業拠点の大半が国内を中心とする従来の外部委託とは異なり、例えば、インシデント発生時に復旧や原因究明のために必要となるデータは、どこの事業拠点へ行けばアクセス可能か、その所在地をあらかじめ知っておきたい、という要望を持つことになる。また、復旧や原因究明とその後の再発防止策が実効的に行われることを担保するために、データにアクセス可能な事業拠点に対する監査権を契約書に明記したい、あるいは事業拠点に対して自国の法令が及ぶようにしたい、という要望を持つこととなる。

一般の情報システムにおいては、インシデント発生時は金融機関が個別に対処すればよく、統制の程度はリスクに応じて金融機関が決定すれば十分であるが、重要な情報システムにおいては、インシデント発生時の社会的影響が甚大であるため、データにアクセス可能な事業拠点という観点でもリスク管理策を検討することが必要となる。

以上から、重要な情報システムに関する補足的検討にあたっては、インシデント発生時の復旧や原因究明等統制上必要となるデータへのアクセス可能な事業拠点に関して、リスク管理策の明確化を行うことが適当である[12]。

（３）技術の先進性

クラウドサービスでは、複数の利用者で効率的な資源の利用を可能とする仮想化技術や、利用者以外によるデータ閲覧・処理等を不可能とするデータの秘匿性を高める技術等、特にソフトウェアにおいて技術の進展が著しい。そのため、設備やハードウェアといった物理的な安全対策による効果が、ソフトウェア技術によっても同等程度に達成可能となる場合がある[13]とともに、ソフトウェア技術自体も、旧来の技術を塗り替える、より実効的な技術が次々と登場する場合がある。したがって、設備基準や技術基準といっ

---

10 外部委託検討会報告書では、「共同センターにおけるリスク管理の在り方」として、特に、有事対応における時間性の問題を取り上げている。クラウドサービスでは、利用者間でコミュニケーションが無いことから、ある意味利用者の意思統一という問題は生じないものの、クラウド事業者は利用者全体への影響を考慮するため、対応に時間を要する可能性がある。したがって、有事対応における時間性の問題は、クラウドサービスの利用においても問題となることから、外部委託検討会報告書で提言された「共同センター固有の IT ガバナンス（リスク管理策の在り方）」は参考となる。

11 統制能力の向上策のひとつとして監査があるが、クラウド基準では監査に関して、「システム監査やモニタリングを実施することが必要である」とされており、また、監査権については、「立入監査等を実施する権利を明記すること」を「契約に明記することが望ましい」とされている。

12 クラウド基準では、所在地を確認すべき「データ」には、金融機関のデータが想定されている。そのうえで、業務の継続性の観点から所在地把握が必要とされている。また、管轄権については、「紛争が生じた際にどの国の法律が適用されるのか（中略）十分に配慮する必要がある。」とされている。

13 例えば、同等性の原則の立場に立てば、データの暗号化や複数データセンターへのデータの分散配置によって安全対策の効果が高まれば、個々のデータセンターの物理的な安全対策を従来ほど強く求めなくてもよくなる場合もあり得る。

た技術的な安全対策を、あらかじめ一意に特定しておくことが、必ずしも適切ではないことが生じうる。

そうした中、従来の安対基準では、運用基準・設備基準・技術基準相互の取扱いの考え方が、必ずしも明確に示されていないため、例えば、クラウド事業者選定時の客観的評価において、評価事項に設備基準や技術基準が字義通りに利用される、といった不確実性が残る現状にある。その結果、全体の安全対策の効果からみれば、金融機関として個別に統制を行うまでもない部分にまで形式的に統制が行われ、過度な安全対策を招来することが危惧される。

また、採用技術が先進的であるがゆえに、監査人はあらかじめクラウドサービスの採用技術等の詳細について十分に知悉しておく必要が生じるものの、金融機関が内部に保有する IT 要員やシステム監査要員が限られている場合、必ずしも実効的な監査が行えないことが危惧される。

一般の情報システムにおいては、安対基準の取扱いが明確化されれば、そのうえでリスクに応じて金融機関が決定すれば十分であるが、重要な情報システムにおいては、監査を行うことを前提としつつ、実効性を確保するという観点でも、検討することが必要となる。

以上から、補足的検討にあたっては、設備基準や技術基準といった技術的な安対基準の取扱について明確化したうえで、重要な情報システムにおいては、人材面等監査に関するリスク管理策の明確化を行うことが適切である[14]。

３．リスク管理策に関する補足

以上を踏まえて、クラウドサービス利用時のリスク管理策について、以下の補足を提案する。

（１）客観的評価を実施する際の留意事項

クラウド基準では、金融機関は、クラウド事業者の選定時において、「クラウド事業者の資質・業務遂行能力に関する情報や、クラウド事業者の内部統制やリスク管理に関する状況等をもとに評価を行うことが必要である。」とされているが、これは、客観的評価を実施する際の評価事項に、安対基準の設備基準や技術基準を含めることを必ずしも意味しないことに留意が必要である、としてはどうか。

（２）データアクセス拠点の把握

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関は、クラウド事業者の選定時において、統制上必要となるデータ（以下「必要データ」という）へのアクセスが可能となる情報処理拠点等、実質的な統制を行うにあたり対象となる事業

[14] クラウド基準では、監査の実効性を高めるために、「委託元金融機関の立入監査等が実効的でない場合などには、第三者監査により代替することも可能である」とされている。また、「既にクラウド事業者が受検している監査結果の内容を検証し、疑問点や不足する監査項目を中心にクラウド事業者に対する実地検証を行うことが有効である」とされている。

拠点（以下「統制対象クラウド拠点」という）について把握しておくこと、としてはどうか。

また、統制の実効性を担保するため、統制対象クラウド拠点は、原則として、国内に所在すること、としてはどうか。それが不可能な場合は、契約において、金融機関が、必要データに実効的にアクセスできる手段を手当てすること、としてはどうか。

（３）監査権の明記

「重要な情報システム」でクラウドサービスを利用する場合は、その社会的・公共的な性質に鑑み、金融機関が、統制対象クラウド拠点に対して監査が可能となるよう、業務委託契約に明記すること、としてはどうか。

（４）監査の実施

監査にあたっては、技術が先進的であることから、クラウド事業者が自ら監査人に委託して行った保証型監査の報告書を利用することが望ましい、としてはどうか。また、その場合、統制が十全かつ実効的に機能するよう、安対基準と整合的に検証が行われている報告書を利用することが望ましい、としてはどうか。

「重要な情報システム」でクラウドサービスを利用する場合は、統制が十全かつ実効的に機能するよう、定期的に監査を実施すること、としてはどうか。

（５）監査人等モニタリング人材の配置

「重要な情報システム」でクラウドサービスを利用する場合は、金融機関の経営層は、クラウドサービスの採用技術が先進的であることを認識したうえで、クラウド事業者に対する監査等モニタリングを実効的に実施するために必要となる能力を有した人材を配置すること、としてはどうか。また、こうした人材を金融機関内部で育成することが容易でない場合は、専門性を有する第三者監査人等を利用することが望ましい、としてはどうか。

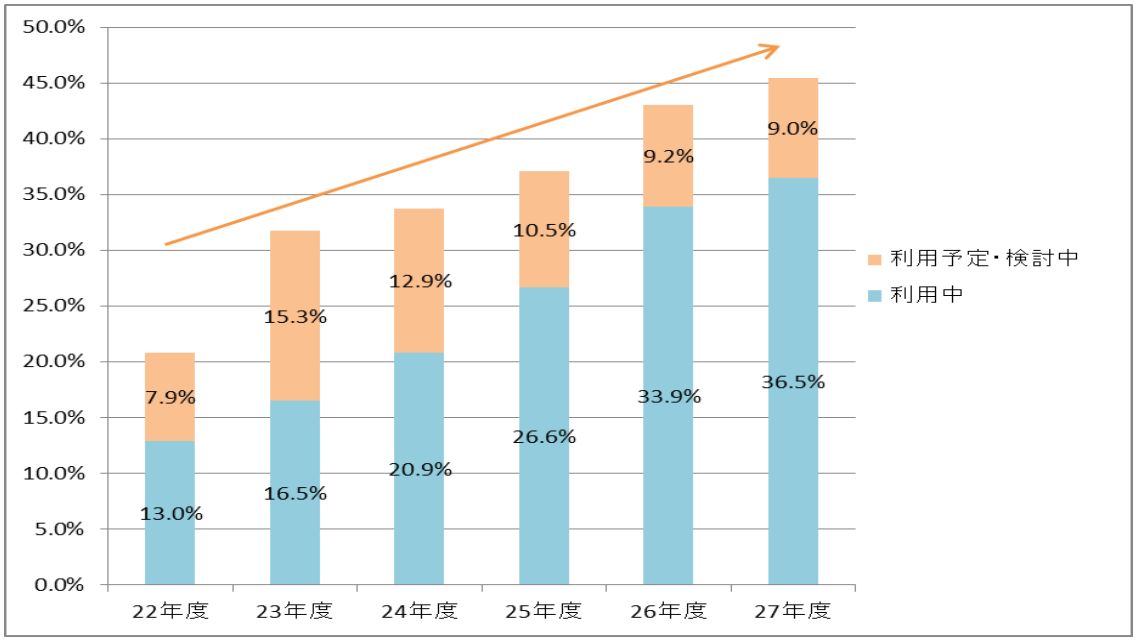
以上

参考

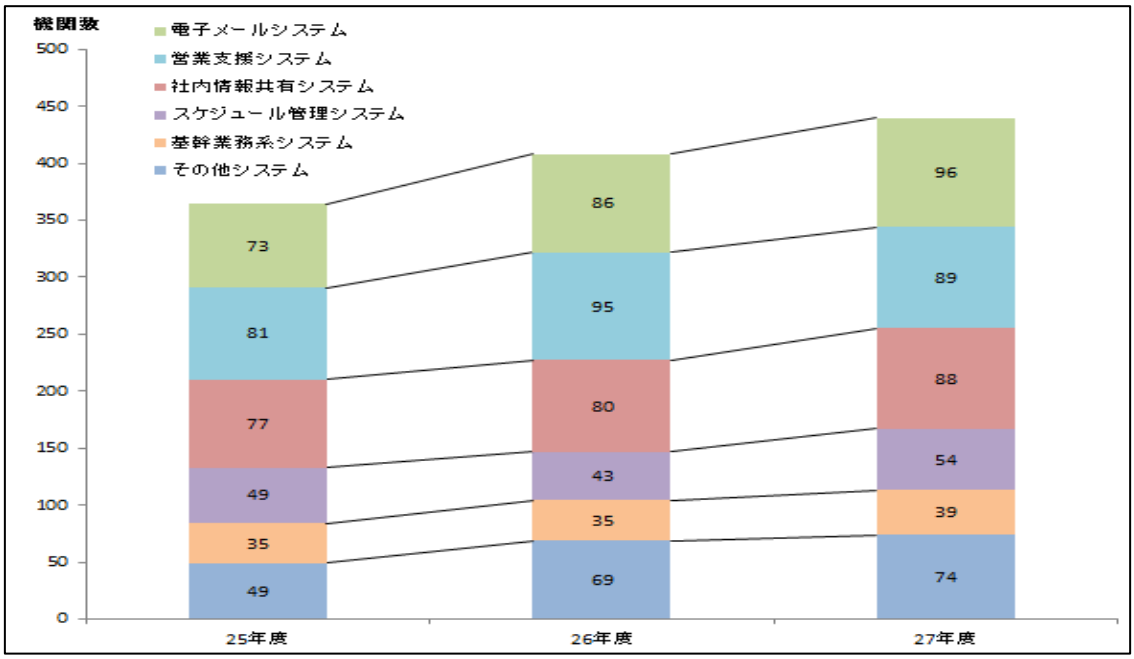
クラウドの利用状況

金融機関等のクラウドサービス利用は、平成 27 年度では、約半数の金融機関等がクラウドの利用あるいは利用の検討を行っているとともに、特定のシステムに偏ることなく、年々増加している状況にある。

（図表１）　クラウドの利用推移



（図表２）　クラウドの利用環境



（出所：FISC 金融機関アンケート調査結果）