金融情報システムセンター
The Center for Financial Industry Information Systems

資料３

FinTechに関するFISCの取組みについて

平成29年1月
公益財団法人 金融情報システムセンター
企画部

「金融情報システムセンター」とは

公益財団法人　金融情報システムセンター
(FISC : The Center for Financial Industry Information Systems)

FISCの概要

- 銀行、証券会社、保険会社、コンピュータメーカー、情報処理会社等の出損により大蔵大臣（当時）の許可を得て、財団法人として設立（1984年11月）。2011年４月に、内閣総理大臣の認定を受け、公益財団法人に移行。

- 金融情報システムに関する諸問題（技術、IT利活用、リスク管理、セキュリティ等）について総合的な調査研究を行うとともに、得られた知見を、「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）をはじめとする各種ガイドライン等や調査レポートとして結実し、各種刊行物やセミナーを通じて社会に還元。

- 会員　645機関（2016年9月末現在）
  都市銀行、信託銀行、外国銀行、地方銀行、第二地方銀行協会加盟行、信用金庫、信用組合、労働金庫、農林中央金庫、各都道府県信連、商工組合中央金庫、生命保険会社、損害保険会社、証券会社、銀行系カード会社、電気通信・情報通信会社、メーカー、情報システム会社　等
  ※一般社団法人FinTech協会、株式会社マネーフォワード

FISC安対基準の概要

- 金融機関等コンピュータシステムの障害発生の未然防止や発生時の影響の最小化、障害からの早期回復のための安全対策について記述したもの。1985年12月発刊後30年以上にわたり、環境変化を踏まえて改訂を重ね（最新版は第８版とその追補改訂）、金融情報システム（金融機関が行う金融業務を担う情報システム）に関する安全対策の拠りどころとして、金融機関やITベンダー等、幅広い関係者に活用されている。
- 設備基準（138項目）、運用基準（120項目）、技術基準（53項目）、合計311項目から構成。

決済高度化のためのアクションプランとFISCの関係

決済高度化官民推進会議においてフォローアップされる以下の主要事項につき、情報セキュリティ等金融情報システムの安全対策の観点から、各種の取組みを行っている。

主要事項⑬
情報セキュリティのあり方に関する検討

⇒ **FISC「FinTechに関する有識者検討会」**「FinTechに関する安全対策の在り方」について検討中。

主要事項⑧
オープンAPIのあり方に関する検討

⇒ 全銀協「オープンAPIの在り方に関する検討会」への参画※１

主要事項⑦
ブロックチェーン技術の活用等に関する検討

⇒ 全銀協「ブロックチェーン技術の活用可能性と課題に関する検討会」への参画

※１　全銀協「オープンAPIの在り方に関する検討会」で議論がされている**「API接続先チェックリスト」（仮称）**（API接続先が確保すべき安全管理措置の目安水準含む）について、FISCが制定のための事務局となる方向で、対応を検討中。

「有識者検討会」とは

FISC有識者検討会は、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に、当センターの理事長の諮問機関としてテーマに応じて設置。
これまで、「サイバー攻撃対応」「クラウド利用」等を取り上げ、検討会で取りまとめられた報告書を踏まえて、FISC安対基準の改訂が行われてきた。

「金融機関におけるFinTechに関する有識者検討会」の設置

- 我が国金融機関が、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、「FinTechに関する安全対策の在り方」を検討。
  - 座長：岩原紳作 早稲田大学大学院法務研究科教授
  - 座長代理：渕崎正弘 株式会社日本総合研究所 代表取締役社長
  - 委員：
    - 学界：安冨潔　慶應義塾大学名誉教授　國領二郎 慶應義塾大学総合政策学部教授　ほか
    - 金融界：都銀、地銀、ネット銀行、生保、損保、証券
    - 実務界：FinTech業界団体、FinTech企業、ITベンダー、クラウドベンダー　ほか
    - オブザーバー：金融庁、日銀、総務省、経産省
- 2016年10月～2017年6月に計５～６回

これまでの検討会運営状況

第一回	2016年10月5日	【論点】金融機関におけるFinTechに関する安全対策検討の在り方
第二回	2016年12月1日	【論点】FinTechに関する安対基準適用上の課題 【論点】安対基準の対象外となるFinTech業務の取扱い

検討会における主な議論

①安全対策における責務の再分配について

- FinTech業務においては、金融機関・ITベンダーに加えて、FinTech企業が、情報システムにおける安全対策の担い手となることが期待される。
- しかしながら、従来の安対基準では、情報システムの安全対策の責務を、金融機関とITベンダーが担うことを前提に策定されているため、現状では、FinTech企業に対してもITベンダーの役割を全面的に代替させることとなる可能性がある。これにより、FinTech企業の革新的な性質を損なうことが危惧される。

⇒ 金融機関は、従来の安全対策の効果を維持しつつ、安全対策の責務を、FinTech企業の安全対策遂行能力に応じて、金融機関・ITベンダー・FinTech企業の３者で再配分しうることを、明確にしてはどうか？

②外部委託基準の準用について

- FinTech企業が主導し金融機関が受動的立場となる金融関連サービスにおいて、金融機関とFinTech企業の関係は、必ずしも金融機関による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。
- 両者の関係がいかなる形態となるにせよ、FinTech業務の実質的内容をみれば、外部委託と共通する要素が見出される可能性が高く、また、従来の安対基準では外部委託の基準は完備されてきたものが存在し、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。

⇒ 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こととしてはどうか？

検討会における主な議論

③安対基準の対象外となるFinTech業務の取扱い

- 安対基準は、「金融機関が行う金融業務」を担う情報システムを対象としてきた。
- また、安対基準は、FISC会員によって策定される自主基準であり、その規範性は自主基準の策定過程に参画した当事者においてのみ生ずることとなる。
- したがって、FISCの会員でない金融機関・非金融機関が行う金融業務等は安対基準の対象外となる。
- 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。

⇒ 現在、FinTech企業やその業界団体が、FISCに入会するといった取組みが進んでいるところであるが、加えて、必ずしもFISCの会員とならない、企業や業界団体に対しても、何らかの「意見表明」を行ってはどうか？

FinTech業務全般における安全対策に関する意見表明（案）

現在、以下の「意見表明」（案）について、委員にご検討いただいているところ。
最終的には、有識者検討会報告書に盛り込み、報告書の公表等を通じて、社会的に発信していく予定。

【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」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。

FinTech業務全般における安全対策に関する意見表明（案）

（1）

金融関連サービス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安対基準をはじめとして、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。**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。※２**

※２　「API接続先チェックリスト」（仮称）策定の事務局、FinTech業界団体の自主基準策定支援等を通じて、FISCとして、整合性確保等に向けた役割を果たしていく予定。