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

議事２－２

# 外部委託検討会報告書の概要

平成28年10月

公益財団法人 金融情報システムセンター
企画部

©2016 FISC All rights reserved

# 「有識者検討会」とは

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設置するもので、学識経験者及び各業界団体並びに各金融機関の代表等で構成

## 過去取り扱ったテーマ

| | |
|---|---|
| サイバー攻撃対応 | 金融機関のサイバー攻撃対応の在り方について検討<br>（開催時期：2013年６月～2015年７月※途中休会あり） |
| クラウド利用 | クラウド特有の論点や適切なリスク管理・契約管理の在り方について検討<br>（開催時期：2014年４月～2014年10月） |

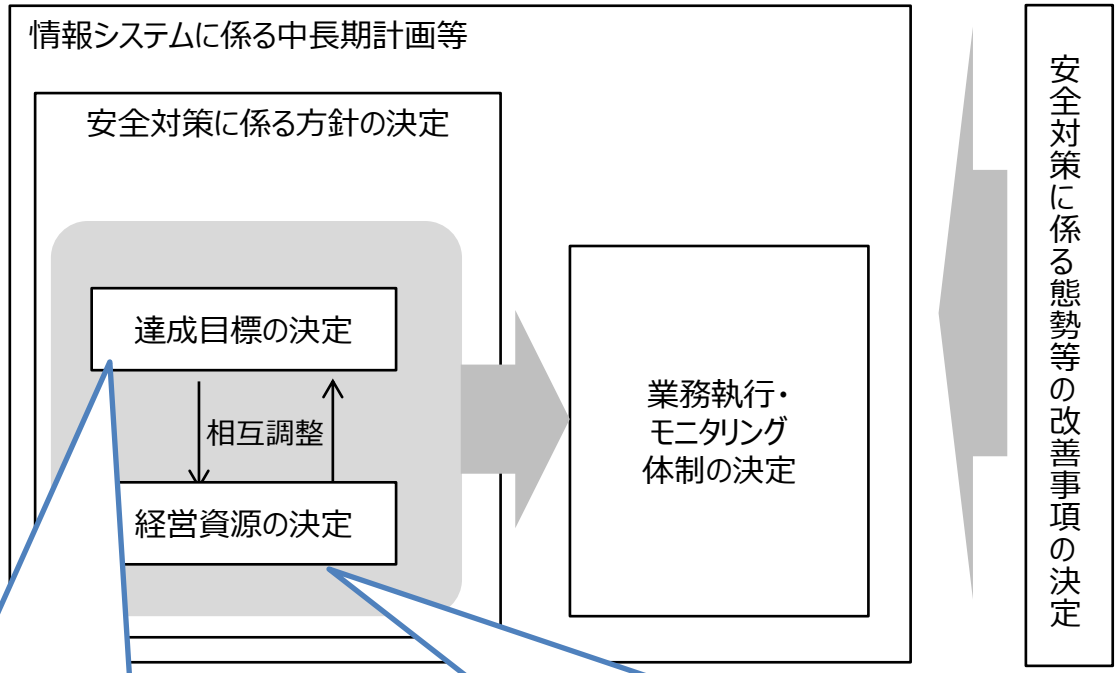
## 外部委託有識者検討会　運営体制、日程

- 平成27年10月、「金融機関における外部委託に関する有識者検討会」を開設
  - 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：
    - 学術界：國領二郎 慶應義塾大学総合政策学部教授ほか３名
    - 金融業界：都銀、地銀、外銀、信金、生保、損保、証券
    - 実務界：ベンダー等
    - オブザーバー：金融庁、日銀、総務省、経産省
- 全６回の会合を開催
  （第1回 平成28年10月23日、第2回 同12月1日、
  第3回 平成28年2月3日、第4回 同3月23日、第5回 同5月12日、第6回 同6月27日）
- 平成28年7月１日、報告書を公表（FISCホームページ（http://www.fisc.or.jp）に掲載）

©2016 FISC All rights reserved

# （1）経営層の役割と責任

経営層は「中長期計画等における安全対策に係る重要事項の決定」、
「安全対策に係る態勢等の改善事項の決定」の役割と責任を果たすことが必要である。




不備等の発生により顧客等に深刻な影響を及ぼす可能性がある情報システムには、高い達成目標を設定し、影響が金融機関等の内部に留まる情報システムに対しては、相応の達成目標を設定。

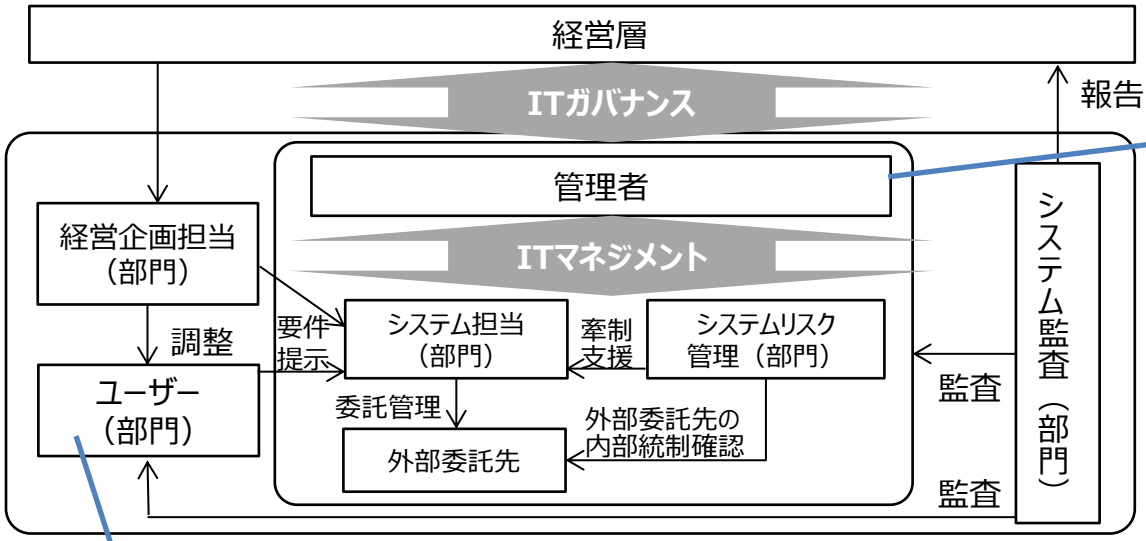
経営層は、安全対策の達成目標の決定と同時に、達成目標を実現するために必要となる経営資源の投下（費用・配分方針等）を決定する。
経営層は、経営資源が有限であることを踏まえた、達成目標を検討するとともに、リスク特性に応じた資源配分を決定することが重要。

©2016 FISC All rights reserved

# （2）ITマネジメント

ITマネジメントとは、経営層によるITガバナンスのもとで、管理者が、情報システムの執行部門（システム担当・システムリスク管理担当等）に対して、ITに関する業務執行の管理等を行うことをいう。

情報システムの安全対策に携わる関係者（例）




- 経営層は、安全対策をはじめとした情報システムに関する十分な知識・経験を有し、金融機関等の業務全般にわたる知識を有する役職員を管理者に選任する。
- 内部規程・組織体制の整備や、個々の情報システムに対する安全対策の決定及びその実効性の検証を行う。
- また、経営層に対して、ITガバナンスにおいて必要となる情報を、迅速かつ正確に提供する役割を担う。

- ビジネスモデルに対する情報システムの安全・安定に脅威となる要素の排除、コントロールを作りこむ等、システム担当やシステムリスク管理担当等と連携する。
- 管理者に対してシステム化の有用性・経営戦略への目的適合性等の説明責任、特に、効果に関する説明責任を負う。
- システム開発着手時に、システム担当に対して業務要件を提示する責任を負う。業務要件変更時は、適時適切にシステム担当に伝える。

©2016 FISC All rights reserved

# （1）新たな安全対策の在り方の必要性

**安対基準の意義**

- 安全対策基準は、金融機関の自己責任と自主性尊重を原則としつつも、その公共性と社会的責任の大きさに鑑み、個別金融機関による対応を補完するものとして、その安全性の確保を目的に、30年前にはじめて策定された。
- 業界共通のガイドラインとして金融機関等において広く浸透し、安全対策の重要性も強く認識されるに至った。

**従来の安全対策の考え方とその課題**

- 安対基準は、その適用対象を「基幹業務のオンラインコンピュータ・システム」とする一方で、それ以外の情報システムについては、安対基準を適宜取り入れる」あるいは「個別に判断する」という記載にとどまっており、大きな比率を占めるその他情報システムにおいては、不確実性を含む環境となっている。
- 過度な安全対策を招来してもやむを得ない内容となっている。

**新たな安全対策の在り方**

- 金融機関等の情報システムに求められる役割が大きく変容するなかで、30年間大きく変わらずに来た「安全対策基準の考え方」を見直すべき時期が到来している。

©2016 FISC All rights reserved

# （2）リスクベースアプローチ：海外先進諸国の動向

米英をはじめとした海外先進諸国では、一般的に「リスクベースアプローチ」と総称される考え方が、監督当局及び金融機関等における共通認識となっている。「リスクベースアプローチ」は、一般的には、リスク特性を分析した結果を、対策の優先順位等の合理的な意思決定に活用するという考え方。

## リスクベースアプローチの主な特徴

- リスクの顕在化を予防する対策に無制限に費用を投下し、リスクゼロを追求することは、合理的でないとしている。
  『経営資源が無限ではない。ゼロ停止を目指すといったアプローチすべてを実施することは不可能である。（ 英国監督当局公表文書） 』
  『ITの分野で100点満点を取ろうと思ったら、膨大なコストがかかる。特に、中小金融機関の場合は経営資源が限定されているので、ITの特定の部門で100点満点をとるよりも、それにかかるコストを他の分野に振り向けた方がよい場合がある。 （米国監督当局ヒアリング） 』

- 監督当局は、リスク区分法やリスク管理策については、必ずしも事細かく成文化しておらず、基本的に金融機関の判断に委ねている。
  『成文化すると、それが絶対的になり、本当はもっとよい方法があるかもしれないのに、それを見逃し、イノベーションが起きないという問題がある。（米国監督当局ヒアリング） 』

- そうした中でも、監督当局は、外部委託等のガイドラインにおいて、「重要な銀行機能・共有サービスや顧客に深刻な影響を及ぼす業務」等を「重要業務」とし、特段の定義をするとともに、個別の管理策を示している。

©2016 FISC All rights reserved

# （3）安全対策における基本原則

## 基本原則１

情報システムに対する安全対策の達成目標は、個々の情報システムのリスク特性に応じて、必要十分な内容で決定されるべきである。

## 基本原則２

情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較衡量したうえで、情報システム予算内での新規開発等との調整のみならず、経営資源全体も視野に入れ、企業価値の最大化を目指して、決定されるべきである。

## 基本原則３

上記原則が遵守されたうえで、妥当な意思決定等が行われ、適切に運営されている限りにおいては、安全対策は独自に決定することが可能である。

## 基本原則４

なお、金融機関等が保有する重大な外部性を有する情報システム及び機微情報を保有する情報システムにおいては、上記に加えて、その社会的・公共的な観点から、このシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されるべきである。

©2016 FISC All rights reserved

# （4）安全対策における基本原則

## システムの外部性

- 個別金融機関の決済システムにおけるシステム障害等によって、他金融機関等社会全体に経済的損失を与える可能性のある性質をいう。「外部性を有する」情報システムに関する損害額等は正確には把握できない。つまり、個別金融機関等がシステム障害等に伴い社会全体に及ぼす損失額を正確に把握し、障害を防止するためのコストを事前に算定・内部化して、安全対策の立案に的確に反映させることは困難である。
- 「外部性」には、個別金融機関の顧客は含まれない。なぜなら、顧客に対しては、相手を個別に認識し個別に対処可能であり、損失額を内部的に算定可能であるからである。

## 保有情報の機微性

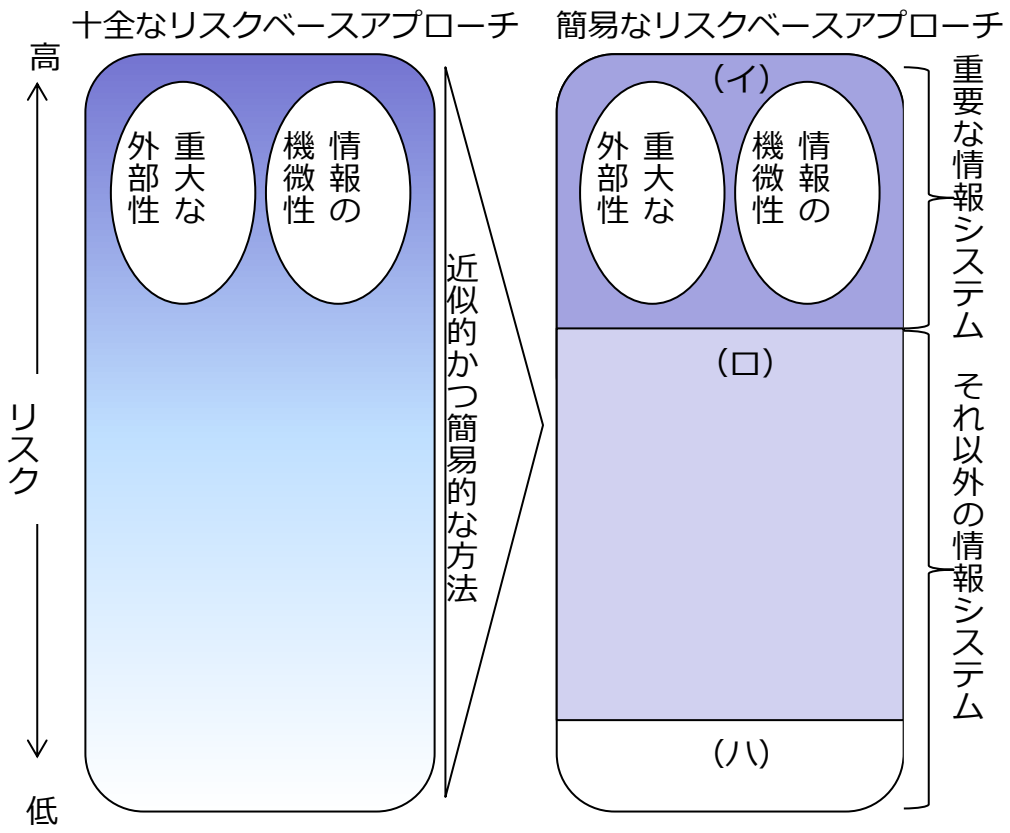
- 機微性を有する情報は、一般の個人情報と区別せず取扱うことは適当でない。仮に同一に扱われてしまった場合には、機微情報に影響されて過度な安全対策目標が設定され、資源の過剰配分が行われるおそれがある。
- 機微情報が流出した場合、経済的損失に留まらず、基本的人権の侵害といった広範な損失を被る可能性があるため、その取扱いは社会的・公共的な性質を有する。

©2016 FISC All rights reserved

# （5）リスクベースアプローチに従った安対基準適用方法

- 「十全なリスクベースアプローチ」と「簡易なリスクベースアプローチ」
  - 「重要な情報システム」には、「高い安対基準」(注１)の適用が求められる。
  - 「それ以外の情報システム」には、「必要最低限の安対基準」 (注２)の適用が必要である。なお、外部性や顧客情報を持たず、かつ内部への影響も軽微な情報システムは、安対基準の適用対象外とすることが可能である。

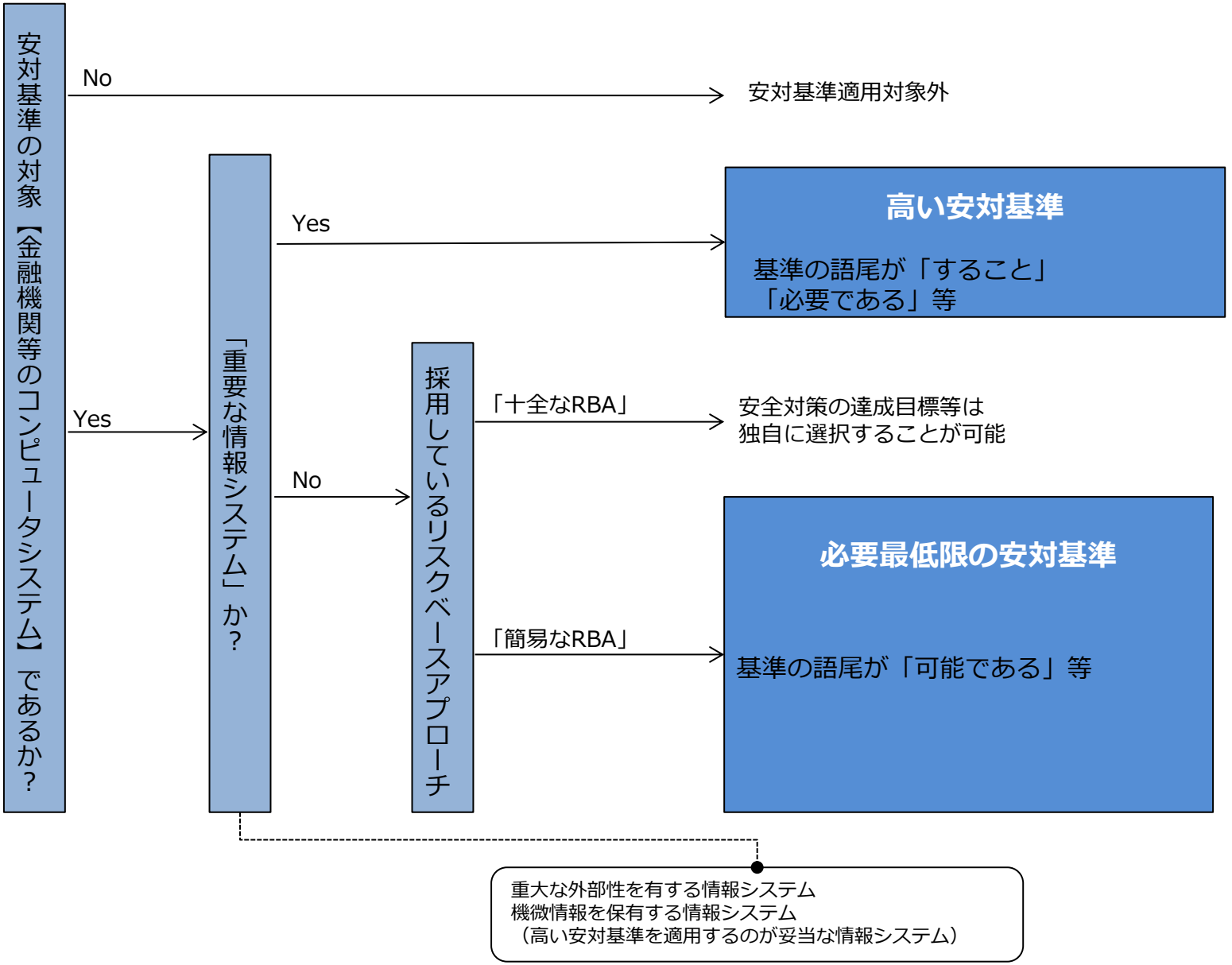
（注１）安対基準の語尾で「すること」「必要である」を対象
（注２）安対基準の語尾で「可能である」を対象




| 安対基準の適用区分 | | 安対基準の語尾 |
|---|---|---|
| 十全なリスクベースアプローチ | | 「重大な外部性」「情報の機微性」を有する情報システム等には「すること」「必要である」を適用。それ以外は独自に選定可能 |
| 簡易なリスクベースアプローチ | イ | 「すること」「必要である」 |
| | ロ | 「可能である」（「可能である」がない場合、イの基準を適用） |
| | ハ | 安対適用対象外 |

©2016 FISC All rights reserved

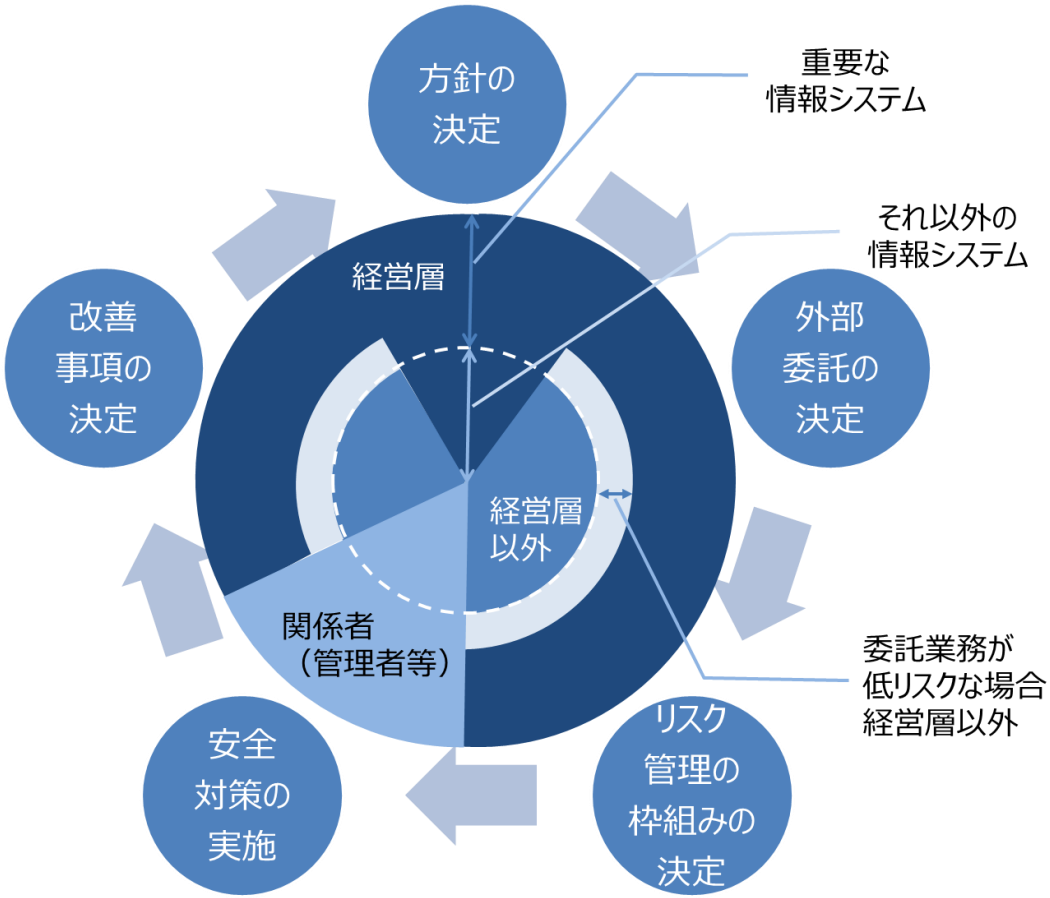
# （6）リスクベースアプローチに従った安対基準適用手順




©2016 FISC All rights reserved

# （1）外部委託における管理プロセス

外部委託におけるリスク管理の在り方を検討するにあたり、まず管理責任等を語るべく
ITガバナンスの観点から、外部委託における管理プロセスを特定し、その内容等を明らかにした。




©2016 FISC All rights reserved

# （2）再委託のリスク管理策

再委託先統制の責任は、一義的には委託先にあり、金融機関は委託先の再委託先に対する管理をチェックすることにある。
その場合、管理フェーズの中でも、再委託先選定の妥当性のチェック、及び再委託先の業務運営を委託先が適切に管理・監督しているか、の２点が特に重要である。

適切な再委託先が選定されるよう、再委託先の選定要件をあらかじめ定めること。

「重要な情報システム」が再委託される場合は、委託先が再委託先を選定することを前提とし、再委託先の事前審査を行なうこと。

「重要な情報システム」が外部委託される場合は、金融機関等による再委託先への監査権を明記すること。

| | システム種別 | 選定要件策定 | 事前審査 | 監査権の明記 | 有事対応 |
|---|---|---|---|---|---|
| 運用の外部委託 | 重要な情報システム | ○ | ○ | ○ | ○ |
| | 結果的に低リスクとなる場合 | ○ | △1 | △2 | – |
| | それ以外の情報システム | ○ | △1 | △2 | – |
| 開発の外部委託 | 重要な情報システム及びそれ以外の情報システム | ○ | △1 | △2 | – |

「重要な情報システム」が外部委託される場合は、コンティンジェンシープランは委託先や再委託先も含めて策定される必要がある。

○　リスク管理策の適用が必要
△1　委託先の再委託先に対する審査・管理プロセスの検証をもって、再委託先に対する個別の事前審査に代替させることが可能
△2　委託先との契約において再委託先への監査権を明記しないことが可能

©2016 FISC All rights reserved

# （1）今後の安対基準等改訂の考え方

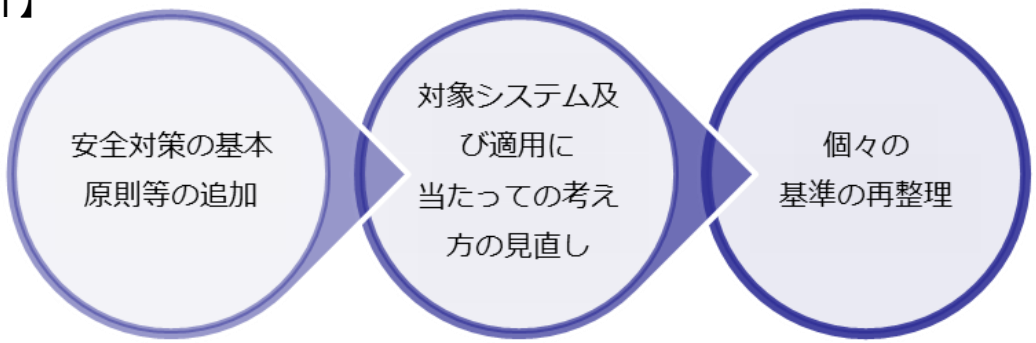
## 考慮事項

- システム更改時や新システム導入時に、変更後の安対基準等へ順次移行を図ることを可能とする。ただし、現状で既に問題を抱え、変更後の高い水準でのリスク管理策の適用が要請されている場合には、早期の移行が必要とされる。

## FinTechに関する有識者検討会（仮称）との関係

- FinTechで総称される金融サービスは、外部委託の形態で利用されることが多いと考えられる。
- 今年10月からは「FinTech」をテーマに有識者検討会の開催を予定しており、その終了後に、「外部委託」の成果とあわせて、安対基準等の改訂の検討に着手する予定。

【改訂方針】




©2016 FISC All rights reserved

議事３

金融機関における FinTech に関する安全対策検討の在り方

金融機関における FinTech に関する安全対策の在り方を検討いただくにあたり、まず、その検討の在り方について、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】

金融機関における FinTech に関する安全対策の検討は、どのように行われることが適切であるか？

【論点に係る原案の構成】

１．　検討の手順

・FinTech に関する安全対策を検討するにあたって、安対基準の適用手順に従って、どのような手順で検討することが望ましいか、明確にする。

２．安対基準の対象となる情報システムの判別基準

・検討の手順の第一として、安対基準が対象となる情報システムの範囲を明らかにしたうえで、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ものを明確にする。【論点１】

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

・検討の手順の第二として、「重要な情報システム」において利用が想定される FinTech に係るテクノロジー等について、取り上げるべき時期の考え方について明確にする。

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

・検討の手順の第三として、「重要な情報システム以外の情報システム」について、簡易なリスクベースアプローチを採用した際の安全対策の在り方とリスク管理策を検討することとなるが、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』を明確にした後に、その『検討を進めるにあたっての前提』を整理する。

・従来の安対基準で必ずしも想定されていなかった事項として、『安全対策実施上の新たな関係者となる FinTech 企業の登場』、『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』を取り上げる。【論点２】

・検討を進めるにあたっての前提として、『検討対象となる FinTech 業務のタイプ』、『FinTech 業務における安全対策実施上の関係者の基本的類型』、『本検討会において前提とすべき業務タイプ別類型』、『FinTech 業務における安全対策の検討で考慮されるべき観点』、『「オープン API」との関係』、を取り上げる。【論点３】【論点４】

【論点に係る原案】

・別紙１参照。

【FinTech 業務を担う情報システムに対する安対基準の適用手順と検討の在り方】

・別紙２参照。

【検討の進め方（案）】

・別紙３参照。

以上

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。

**論点１**

安対基準の対象外となる FinTech 業務においても、利用者保護等の社会的観点から、その情報システムにおいて、何らかの安全対策が必要であることは否めない。そのため、本検討会として、こうした直接的にはその情報システムが安対基準の対象とならない FinTech 業務に対しても、なんらかの意見表明を行う必要はあるか？

[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。

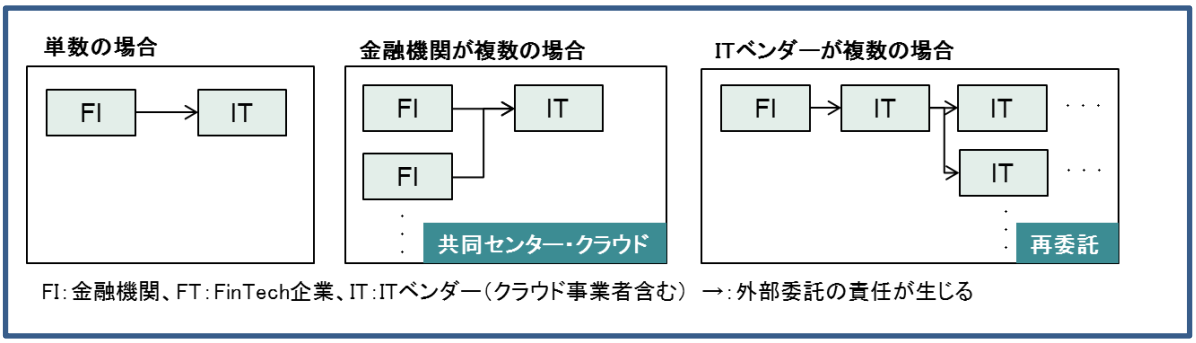
IT ベンダーが複数となる場合において、まず、金融機関の委託先が複数となる場合には、統制が直接可能であることから、固有の性質は生じず単数の場合と何ら異ならない。一方、再委託により間接的に委託先が多段階にわたり複数となる場合は、再委託先に対して金融機関による統制が及びにくくなることから、固有の性質がある類型となる（詳細は外部委託検討会報告書を参照）。

---

[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、金融機関の間に交渉があり、その結果、FinTech 企業が取得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。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に由来するものである。したがって、提供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]。

（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。

**論点２**

FinTech に関して、「必ずしも従来の安対基準で想定されていなかった事項」として検討を行う必要があるのは、これで十分か？

[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。

[12] 金融機関に管理責任があるデータとしては、例えば、顧客の取引履歴情報等がある。なお、逆に、金融機関に渡されるデータとして決済指示も考えられる。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。

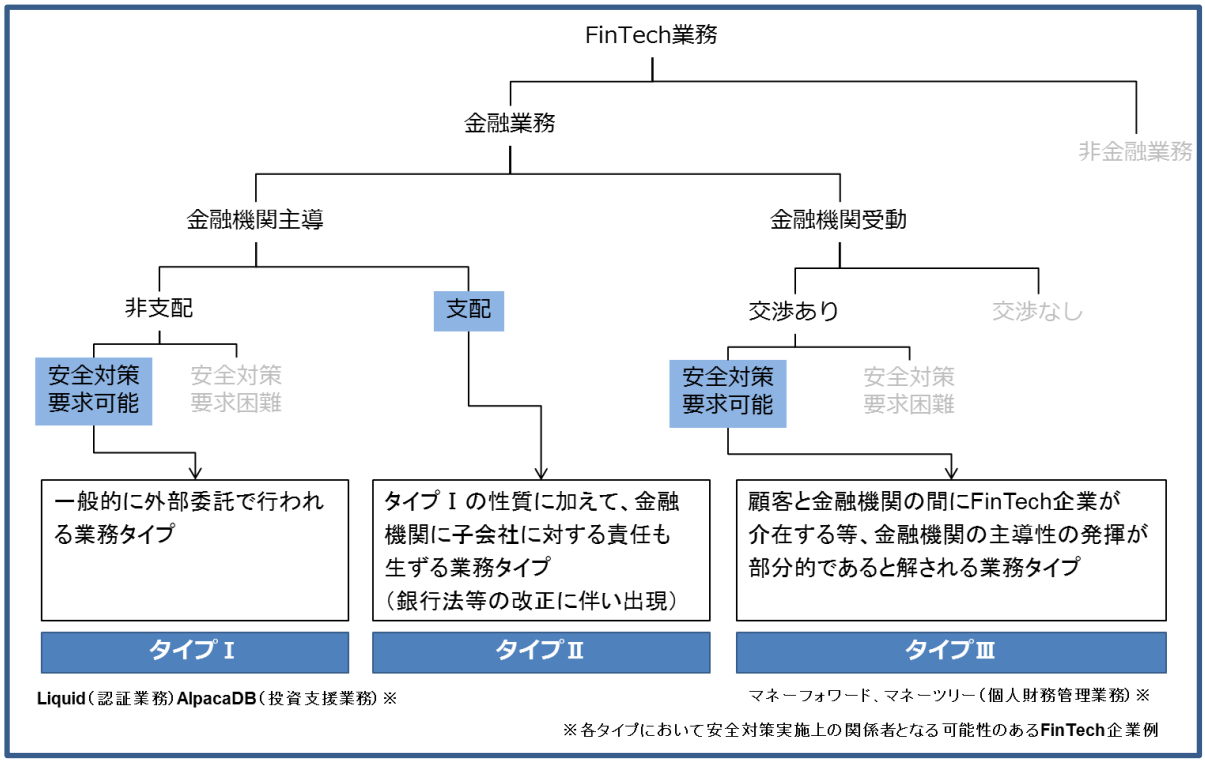
[13] FISC 外部委託検討会報告書において、機微性の程度が高い機微情報に関しては「その保護のために最上位の安全対策目標が設定されるべき」個人情報として、「本人の許諾なく機微情報が流出した場合、経済的損失にとどまらず、基本的人権の侵害といった広範な損失を被る可能性があることから、その取扱いには社会的・公共的な性質を有するもの」とされている。

（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。

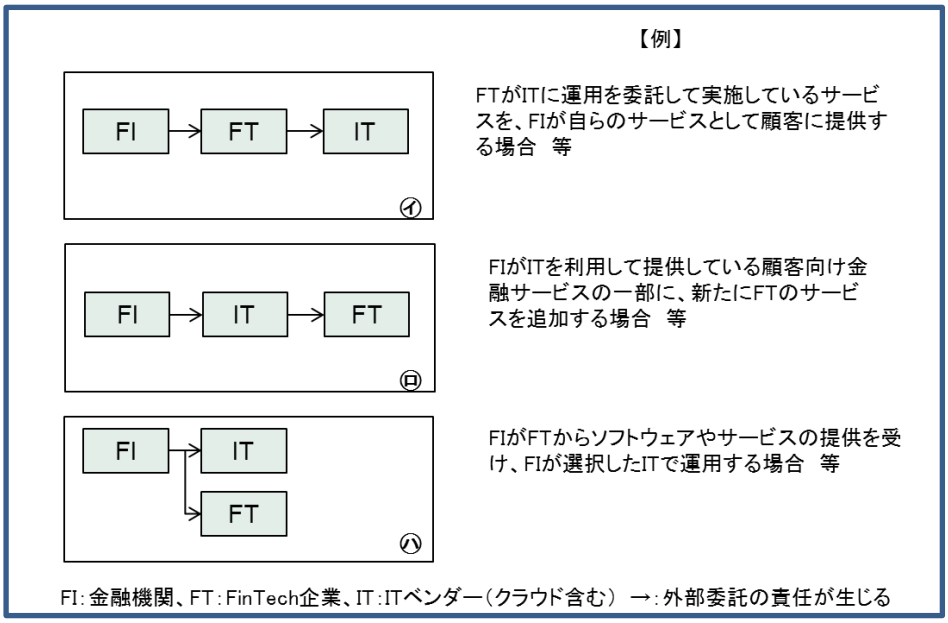
[14] 平成 28 年５月の銀行法等改正においては、あわせて「金融グループにおける経営管理の充実」のために、持株会社等が果たすべき「機能」が明確化された。また、岩原紳作『金融持株会社におけるグループガバナンス－銀行法と会社法の交錯（３）－』において「多くの金融持株会社は、（中略）子会社との間で経営管理契約を結んで経営管理のための助言・指導を行うことを定めている。」としている。

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。

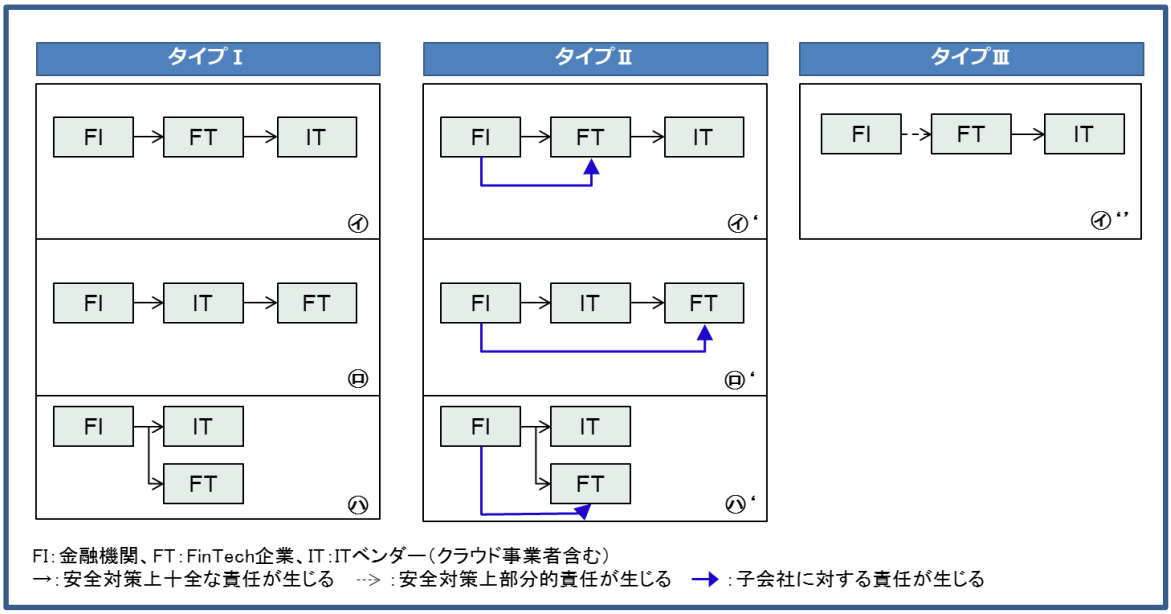
（注）今後、金融機関に部分的に安全対策上の責任が生じる場合等 FinTech に関する安全対策の在り方を検討する中で、固有の性質があるものとして、基本的類型が追加される可能性は残る。

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。

**論点３**

FinTech 業務における安全対策を検討するにあたって、前提とすべき類型は、この７類型で十分か？

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。

**論点４**

FinTech 業務における安全対策の検討にあたって考慮されるべき観点は以上で必要十分か？

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

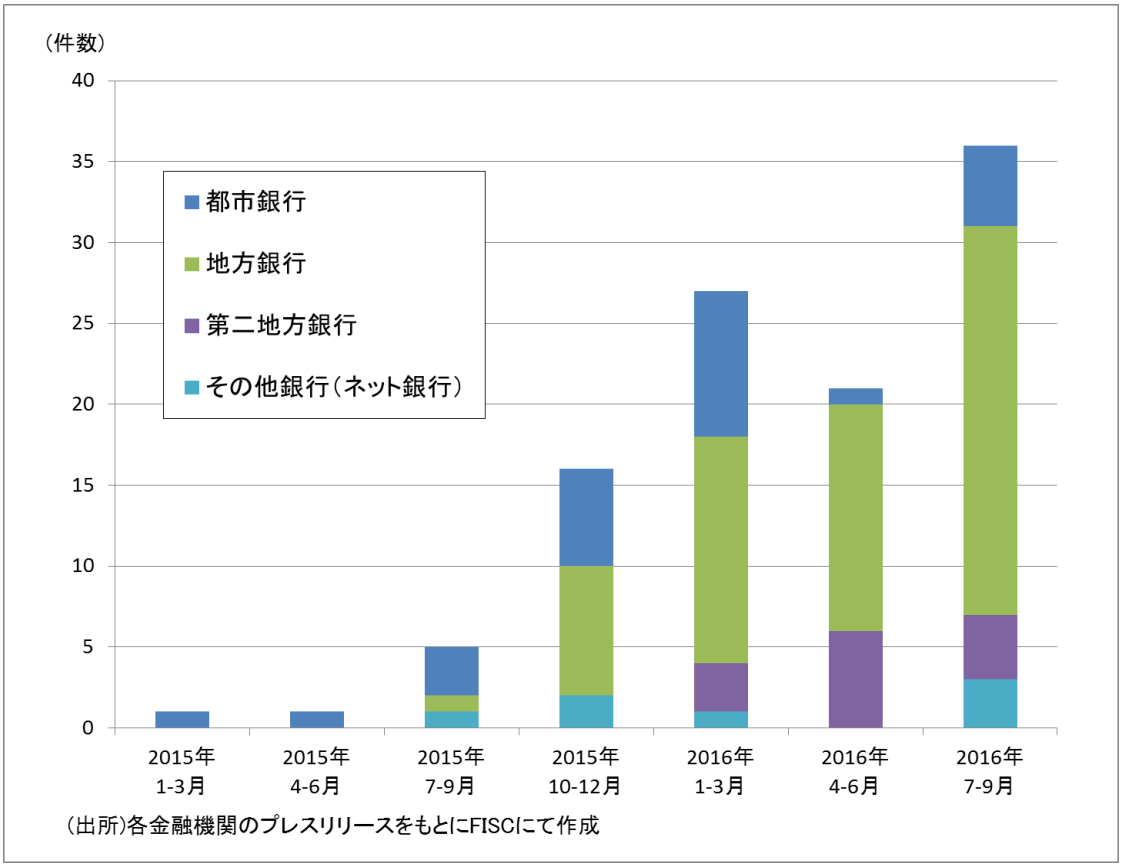
金融機関等における FinTech を巡る動向

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」<br>（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」<br>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。）

# 【別紙2】FinTech業務を担う情報システムに対する安対基準の適用手順と検討の在り方

FinTech業務を担う情報システム

## 安対基準の適用手順

**安対基準の対象【金融機関等のコンピュータシステム】であるか？**

No → 安対基準適用対象外
「電子商取引の情報システム」
「金融機関等以外の事業者が自らのサービス利用者のために行うFinTech業務」 等

Yes → **「重要な情報システム」か？**

Yes → **高い安対基準**
基準の語尾が「すること」「必要である」等

No → **採用しているリスクベースアプローチ**

「十全なRBA」 → 安全対策の達成目標等は独自に選択することが可能

「簡易なRBA」 → **必要最低限の安対基準**
基準の語尾が「可能である」等

金融業務を担う情報システムであり、かつ、金融機関等に責任が生ずる情報システム

重大な外部性を有する情報システム
機微情報を保有する情報システム
（高い安対基準を適用するのが妥当な情報システム）

## FinTechに関する検討の在り方

その情報システムが安対基準の対象とならないFinTech業務に対しても何らかの意見表明を行う必要があるか？ ***論点1***

従来の安対基準が想定していないFinTechに係るテクノロジー等（ブロックチェーン技術やAI）は、今後のユースケースの出現状況をにらみながら検討が可能となる時期を確定させる。
**本検討会に続く、来年度以降の検討会において検討を行う**

**安対基準の不確実性を低減するという観点から、FinTechに関する安全対策の在り方を検討する**

そのための前提を第一回検討会では、以下の項目で検討する。

【想定されていなかった事項】***論点2***
- 安全対策実施上の関係者となるFinTech企業の登場
- 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

【FinTech業務に従来の安対基準を適用した場合に内在する問題を検討するにあたっての前提】***論点3，4***
- 前提とすべきFinTech業務タイプ別類型
- 検討にあたって考慮されるべき観点「中立性」「有効性」
- 「オープンAPI」との関係

別紙３

**検討会の進め方（案）**

第１回を 10 月５日とし 2017 年６月頃までを目途に終了する前提。なお、今後の検討状況等次第で変更となる可能性あり。

| | |
|---|---|
| 第１回<br>10 月５日（水） | 議事１　有識者検討会規則の説明（事務局）<br>議事２　プレゼン：国内外の FinTech に関する動向（委員）<br>プレゼン：外部委託検討会報告書概要（事務局）<br>議事３　論点メモ：金融機関における FinTech に関する安全対策検討の在り方 |
| 第２回<br>12 月１日（木）<br>（予定） | 議事１　第１回検討会に対するご意見及びご回答<br>議事２　プレゼン：FinTech に関する安対基準適用上の課題（委員）<br>議事３　論点メモ：FinTech に関する安対基準適用上の課題 |
| 第３回<br>（未定） | 議事１　第２回検討会に対するご意見及びご回答<br>議事２　論点メモ：FinTech に関する安全対策の在り方 |
| 第４回<br>（未定）※ | 議事１　第３回検討会に対するご意見及びご回答<br>議事２　プレゼン：オープンＡＰＩの検討状況<br>議事３　論点メモ：オープンＡＰＩにおける安全対策の在り方 |
| 第５回<br>（未定）※ | 議事１　第４回検討会に対するご意見及びご回答<br>議事２　有識者検討会報告書ドラフト |
| 第６回<br>（未定）※ | 議事１　第５回検討会に対するご意見及びご回答 |

※　全銀協のオープン API 関する検討状況を踏まえて、開催時期を決定。

以上