平成 28 年 12 月 1 日
公益財団法人　金融情報システムセンター

第２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 28 年 12 月 1 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１回 FinTech 有識者検討会に対するご意見及びご回答
４．	16:00	【議事２】プレゼン 「FinTech ベンチャーのセキュリティ維持・向上に向けた当協会の取組み」（一般社団法人 FinTech 協会 理事 Mark Makdad 委員）
５．	16:15	【議事３】論点メモ 「FinTech に関する安対基準適用上の課題」
６．	16:55	【議事４】論点メモ 「安対基準の対象外となる FinTech 業務の取扱い」
７．	17:35	事務連絡
８．	17:45	閉会

Ⅳ　資料

【資料１】	第２回 FinTech 有識者検討会　座席表
【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
【議事２】	発表資料「FinTech ベンチャーのセキュリティ維持・向上に向けた当協会の取組み」
【議事３】	論点メモ「FinTech に関する安対基準適用上の課題」
【議事４】	論点メモ「安対基準の対象外となる FinTech 業務の取扱い」

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　12 月８日(木)　17 時）

Ⅵ　次回の開催予定

第３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２月２日（木）15:45～17:45　FISC 会議室

以上

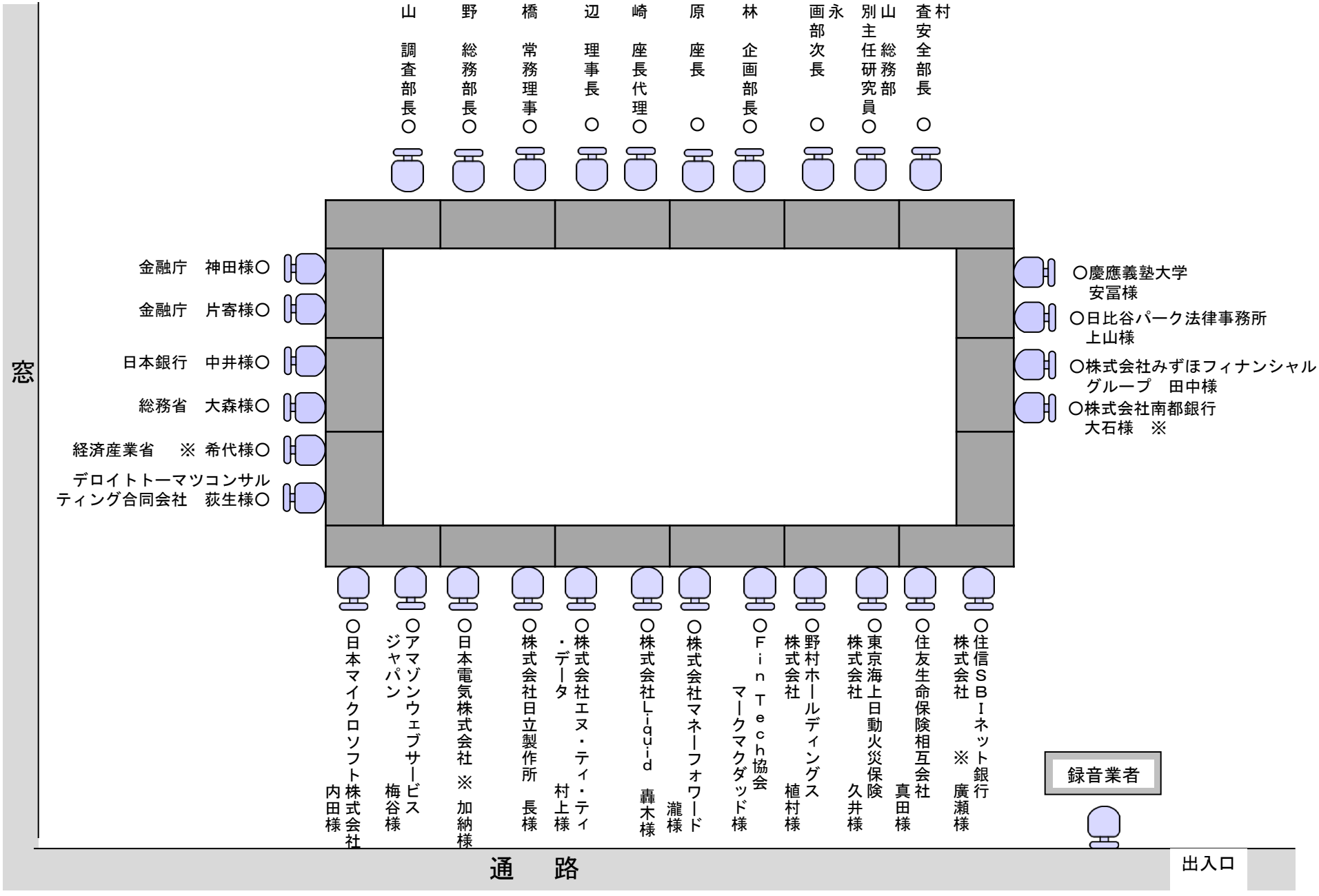
【資料１】

第２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28年12月1日

※代理出席

ＡＢ会議室



【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

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３ 論点１ （別紙１Ｐ．２）	●論点１：安対基準の適用先について 現在、安対基準の適用先として想定しているのは、金融検査マニュアルに基づく監督が行われる銀行、保険会社を中心に、「金融、保険、証券、クレジット等金融業務を営む業界の各社」とされている。 昨今、FinTech の発展に伴い、法的な枠組みとビジネスの実態に乖離が生じうることが明らかになっている。たとえば決済においては、金額に差異はあるが資金決済法に基づく資金移動業者と銀行が同様のサービスを提供しているほか、資金決済法に基づく仮想通貨事業者は FX に類似するサービスを提供している。また、店舗はカード会社(アクワイアラ)からも決済代行業者からもカード決済機能の提供をうけることができる。このように、現在では業態間の垣根が低くなり、同等のサービスが法的根拠の異なる事業者から提供されている。安対基準の趣旨に照らし合わせれば、顧客がうける便益やリスクが同様であれば、根拠法の違いによらず等しくシステムリスクへの手当てがなされるべきであるため、安対基準の適用先も幅広くカバーされるべきと考えられる。	ご意見を踏まえ、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」として、原案を作成していますのでご確認ください。	デロイトトーマツ 荻生様
2	議事３ 論点２ （別紙１Ｐ．６）	●論点２：金融機関の主導性の判断について 論点２では、「①検討対象となる FinTech 業務のタイプ」として、金融機関の関与が主導的か受動的か、および金融機関の支配の有無に応じて、３つのタイプに類型化している。特に FinTech に特徴的なサービスとして、金融サービスの提供主体が FinTech 企業であり金融機関が従属的にデータ等を提供する形態が登場していることから、タイプⅢが設けられている。 ここで、タイプⅠ－Ⅲで安対基準の内容が同一の場合、事業がいずれに分類されるかは問題とならない。しかし、タイプⅠ－Ⅲで安対基準の内容が異なる場合、事業者の判断を支援するため分類の考え方や基準を示すことが妥当ではないか。 たとえば、米国 P2P レンディング大手の Lending Club は、自社サイトで借り手を募集するがローンの組成は Issuing Bank と呼ばれる提携銀行が実行している。この場合、顧客接点は FinTech 企業であるためタイプⅢと解されるが、一方でローン組成に関わるコンプライアンス等は全て銀行の責任で行っているため、タイプⅠとする余地もある。	ご意見を踏まえ、今後のユースケースの出現状況等をみながら、対応の要否を検討させていただきます。	デロイトトーマツ 荻生様

【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

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
		【ご参考】 Lending Club 上場申請書類(Form S1) https://www.sec.gov/Archives/edgar/data/1409970/000119312514323136/d766811ds1.htm		
3	議事３ 論点３ （別紙１Ｐ．10）	●論点３：外部委託の責任について 論点３では、金融機関、FinTech 企業、IT ベンダーの３社の関係を外部委託の責任が生じる関係に応じて、㋑㋺㋩の３つに類型化している。その背景には、「金融機関は常に委託元となる」ことがある。 論点１とも関係するが、特に決済分野では受委託の関係が複雑になる。たとえば、決済代行業はアクワイアラに対し加盟店開拓・管理の責務を負っている一方、アクワイアラは決済代行業者に対して売上金の送金等カード決済機能を提供する責務を負っている。このように、決済では関係者が相互に役割を担っていることから、「金融機関は常に委託元」とは解しきれないケースがあることに留意するべきである。	（No1 の回答と同じ）	デロイトトーマツ 荻生様
4	議事３ ４．（１）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 （別紙１Ｐ．５）	「金融機関が完全に受動的立場となる場合は、金融機関には何らの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」の考え方に異論はない。 しかしながら、FinTech 企業のサービスにおいて、万一事故が発生し、顧客から金融機関に対して、FinTech 企業のサービスの利用にあたっての注意喚起が十分でなかった、といった安全対策上の部分責任が問われる可能性が否定できないのであれば、金融機関として講じるべき対策についても、要否を含めて議論してもよいのではないか。	いただいたご意見を踏まえて、本検討会第２回の議事「FinTech に関する安対基準適用上の課題」「金融機関に責任が生じない場合の取扱い」において、金融機関として講じるべき対策について、原案を作成していますのでご確認ください。	南都銀行 山田様
5	議事３ ４．（２） （図表２）安対基準の対象とすべき FinTech 業務のタイプ （別紙１Ｐ．７）	FinTech 業務の「金融業務」「非金融業務」の分類基準について検討いただきたい。 （理由） FinTech の登場によって、金融業務と非金融業務の垣根が曖昧になっており、具体的な分類について検討しておく必要があるため。	金融業務と非金融業務の区分を明確にすることは困難であり、また、適切でもないと考えます。その理由の詳細については、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」の中で記載しておりますのでご確認ください。	南都銀行 山田様

【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

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
6	議事３ ４．（２） （図表２）安対基準の対象とすべき FinTech 業務のタイプ （別紙１Ｐ．７）	分類方法については、FinTech 業務を、まず、金融機関「主導」「受動」で分類した後に「金融業務」「非金融業務」で分類する方が望ましいと考える。 （理由） 金融機関等のコンピュータシステムは、金融業務を担うか否かにかかわらず安全対策について社会的責任を負っているため、金融機関側の考え方としては当該システムについて金融機関の関わり方が優先されるべきであるため。	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いることから、まず「金融業務」「非金融業務」で分類することが妥当であると考えます。従いまして、原案のとおりとさせていただきます。	南都銀行 山田様
7	議事３ 論点１ （別紙１Ｐ．２）	別紙１（図表 2）における「金融機関受動」-「交渉なし」のモデルは安対基準の対象外ですが、顧客の ID・パスワード・追加認証情報等を保持してスクレイピングを行っており、顧客保護の観点からリスクが高いと考えられます。 「スクレイピング」に関する規制（PSD2 では違法とみなされるケースあり、米国では認可制）について、安対対象外の FinTech 業務への意見表明（論点１）の中で言及する必要があると思われます。	いただいたご意見を踏まえて、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」の中で意見表明の原案を作成していますのでご確認ください。	みずほ FG 田中様

【議事2】

FinTechベンチャーのセキュリティ維持・向上に向けた当協会の取組み

～自主的なセキュリティガイドライン策定の基本方針ご紹介とFISCへのご要望～

一般社団法人FinTech協会

理事　マーク マクダッド（マネーツリー株式会社）

（2016年12月 1日）

協会の前身 “FinTech Meetup”

FINTECH ASSOCIATION

FINTECH MEETUP

情報交換およびネットワーキングが可能なミートアップで、第１回の20名から約**150名ほど**集まるイベントとなった

#01 2014/10/16 カジュアルミートアップイベント

#02 2014/11/26 テーマ ：「英国FinTech 事情」（協賛 英国大使館）
Creative / Digital Specialist Adviser：Mr. Mark Leaver

#03 2015/02/05 テーマ ：「決済イノベーション」
Infcurion代表取締役 丸山 弘毅
「国内ペイメントカード市場の現状と今後の動向」
Kraken Bitcoin Exchange日本市場最高責任者 宮口礼子様
「ビットコイン業界とその可能性」

#04 2015/04/09 テーマ ：「起業家とのQ&A」
ウェブペイ(株) 久保 渓様、(株)お金のデザイン 北澤 直様 、
クラウドクレジット(株) 杉山 智行様、
(株)コインパス 妹尾賢俊様、 (株) Finatext 林 良太様

#05 2015/07/16 テーマ ：「VCから見た日本FinTech」
Fidelity Growth Partners 日本代表 Mr. Milstein David NTTドコモ江藤様・NTTドコモベンチャーズ北様

#06 2015/09/30 テーマ① 「FinTechエコシステム」
日本IBM API Economy兼FinTechアドバイザー Rasmus Ekman
テーマ②「Fintech協会発足の発表」
（祝辞）金融庁総務企画局 企画課 企画官 神田 潤一様

協会概要

名称	一般社団法人FinTech協会（英： FinTech Association Japan）	
設立日	平成27年9月24日	
住所	東京都港区北青山3-12-7　秋月ビル6F	
代表理事	丸山 弘毅	（株式会社インフキュリオン・グループ 代表取締役）
	工藤 博樹	（メリービズ株式会社 代表取締役）
理事	星川 高志	（クラウドキャスト株式会社 代表取締役）
	鷹取 真一	（株式会社Kyash 代表取締社長）
	北澤 直	（株式会社お金のデザイン 取締役ＣＯＯ）
	マクダッド マーク	（マネーツリー株式会社 取締役）
	木村 康宏	（freee株式会社 執行役員社会インフラ企画部長）
	堀 天子	（森・濱田松本法律事務所 パートナー）
	志織フレミングナタリー	（ペイオニア・ジャパン株式会社 代表取締役）
	荻野 調	（財産ネット株式会社 代表取締役）
	依田 寛史	（boku カントリーマネージャー）
監事	藤武 寛之	（リンクパートナーズ法律事務所 弁護士）

日本のFinTechベンチャー企業及びFinTech生態系の成長を支援し、個人及び法人により便利で役に立つ金融サービスの提供を目指す。グローバルなFinTech情報を日本で発信しながら、日本からのFinTech企業がグローバルステージで活躍できるように海外に発信する。オープンな組織にし、一般企業及び関係者のご協力を得て視野の広い活発な活動にしていきます。

会員構成

50社以上のベンチャー会員

PFM･会計、決済、資産運用、仮想通貨、セキュリティなど幅広い業種のFinTechベンチャーが参加

100社以上の法人会員

銀行･信金、クレジットカード、生･損保、証券･投信、ITベンダー、通信･メディア･印刷、コンサル･法律･会計など金融とITに関わる各分野有力企業が参加

参照：https://fintechjapan.org/members

直近の活動

- 一般向けのイベント
  - FinTech人材マッチングイベント
  - 10月29日に１周年イベントを開催し150人強のネットワーキング

- 会員分科会 （下記は一部）
  - コンプライアンス分科会： 中間的事業者、銀行代理業務
  - API・セキュリティ分科会： FinTechセキュリティ、オープンAPI
  - PFM・会計分科会： 電子レシート

- コンフェレンス開催
  - FinTech Japan 2016： 12月1日～2日@ベルサール渋谷
  - 500人程度のFinTechイベント、国内・海外のFinTechリーダーを招く
  - http://fj2016.fintechjapan.org/

- 官公庁及び民間団体と情報連携
  - 経済産業省、金融庁、全銀協、FISC、日本銀行など

FinTechベンチャーの セキュリティの課題

FINTECH ASSOCIATION

起業の悩み

- 金融サービス事業者としてどのようにセキュリティ管理態勢を整備していくか、他業種出身者には必ずしも分かり易くない。
- 多忙なベンチャー経営者、担当者が起業時のクイックリファレンスとして利用できる書籍やガイド等はあまりない。
- 起業後に「最初からこうしておけば良かった」と感じる失敗や反省を後進の起業家が参照可能なものとし、イノベーションの促進に寄与したい。苦労を水泡に帰したくない。

金融機関との協業の悩み

- チェックリストの項目が銀行毎にばらばらでコミュニケーションコストが高い。
- 銀行ごとの独自仕様が入り込んでしまうケースあり、ベンチャーのワークスタイルや業務実態と乖離のある条項が含まれているケースがある。

起業の悩み

様々な公的ガイドラインが有るものの、FinTechベンチャーが起業の際に参考とするには各々一長一短があり、FinTech協会としてセキュリティガイドラインを策定することとした。

- ISMS/ISO27001

  PDCAサイクルを求めるものであり、少人数組織で具体的対策の指針を求めるFinTechベンチャーの第一段階としてのニーズには必ずしもマッチせず、金融サービスにも特化していない。

- PCIDSS

  具体的対策が示され分かり易いものの、カード情報の不正利用防止が主眼であり、対象領域は必ずしもマッチしない。

- FISC安全対策基準

  金融機関のための基準であり、セキュリティの考え方等が解説され有益であるものの、クイックリファレンスとしてはやや重厚長大な面がある。

金融機関との協業の悩み

大企業である金融機関と少人数組織のベンチャーとの統制環境のギャップを橋渡しすることも、FinTech協会のセキュリティガイドラインに求められる役割であると考えられる。

- 独自仕様の例

  OAuth2のあるフローで、標準仕様ではGETメソッドを使って処理するように仕様が策定されているにも関わらず、POSTメソッドで実装されている。

- Fintech企業のワークスタイルからの乖離の例

  リモートワークの事実上の禁止
  →VPN等による安全確保を前提として容認されるべき。

- 事業・業務実態との乖離の例

  顧客データ削除を必須とする規定
  →機械学習によるサービス向上のために残す必要がある。

  性悪説に立った単独作業抑止の項目
  →数百人～数千人規模の外部委託業者と同じレベルの単独作業抑止まで求めることは合理的ではない。

FinTech協会　会員の意見

分科会、アンケート、関係者ヒアリング等により明確になった、セキュリティガイドラインに関する要件は次の通り。

ガイドラインの構成

a.多忙なベンチャー経営者、担当者向けに適度な分量とする。

b.起業時のクイックリファレンスとして有益なものとしたい。

リスクベースアプローチ

c.リスクベースアプローチにより作成すべき。

d.情報管理に加え、可用性と完全性の観点も必要。

e.FinTechはスマートデバイスが肝。

金融機関との協業

f.金融機関担当者とのリスクに関するコミュニケーションが上手くいかないことがある。

（前出：3頁参照）

g.金融サービスである以上、一定水準のセキュリティ確保は必須。

1)概念編（クイックリファレンス）と基準項目編（ガイドライン）に分けて編集する。 [a/b]

2)クラウド利用を前提とすること、少人数組織で運営すること等FinTechベンチャーのリスクに応じて記載内容を定める。[a/c/d/e]

3)FISC安対基準（現行）の内容を取捨選択のうえ取込み、FinTechベンチャーとしてリスクや優先度が低い項目以外はもれの無いよう、事後検証可能とする。 [d/g]

4)スマートデバイスのセキュリティ管理をはじめ、FinTechとしてリスクの高い領域はFISC安対基準（現行）以上に踏み込む。
(FISCに定めが無くても採り上げる) [e]

5)想定する（軽減を狙う）リスクおよび具体的対策事例を明示する。 [f]

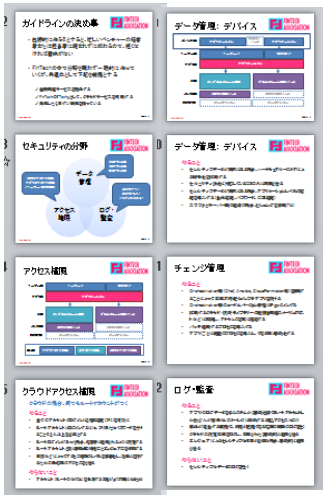
6)リスク管理上有効な新技術については、FICS安対で定める対策との関連を解説する。 [c]

ガイドラインの構成

1)「概念編」と「基準項目編」による構成

FISC「金融機関等のシステム監査指針」を参考に、チェックポイント部分とクイックリファレンス部分の２本立てとする。

金融機関等のシステム監査指針		当協会のガイドライン
「第１部 フレームワーク」	⇒	「概念編」
「第２部 チェックポイント集」	⇒	「基準項目編」



リスク評価の考え方など

概念編

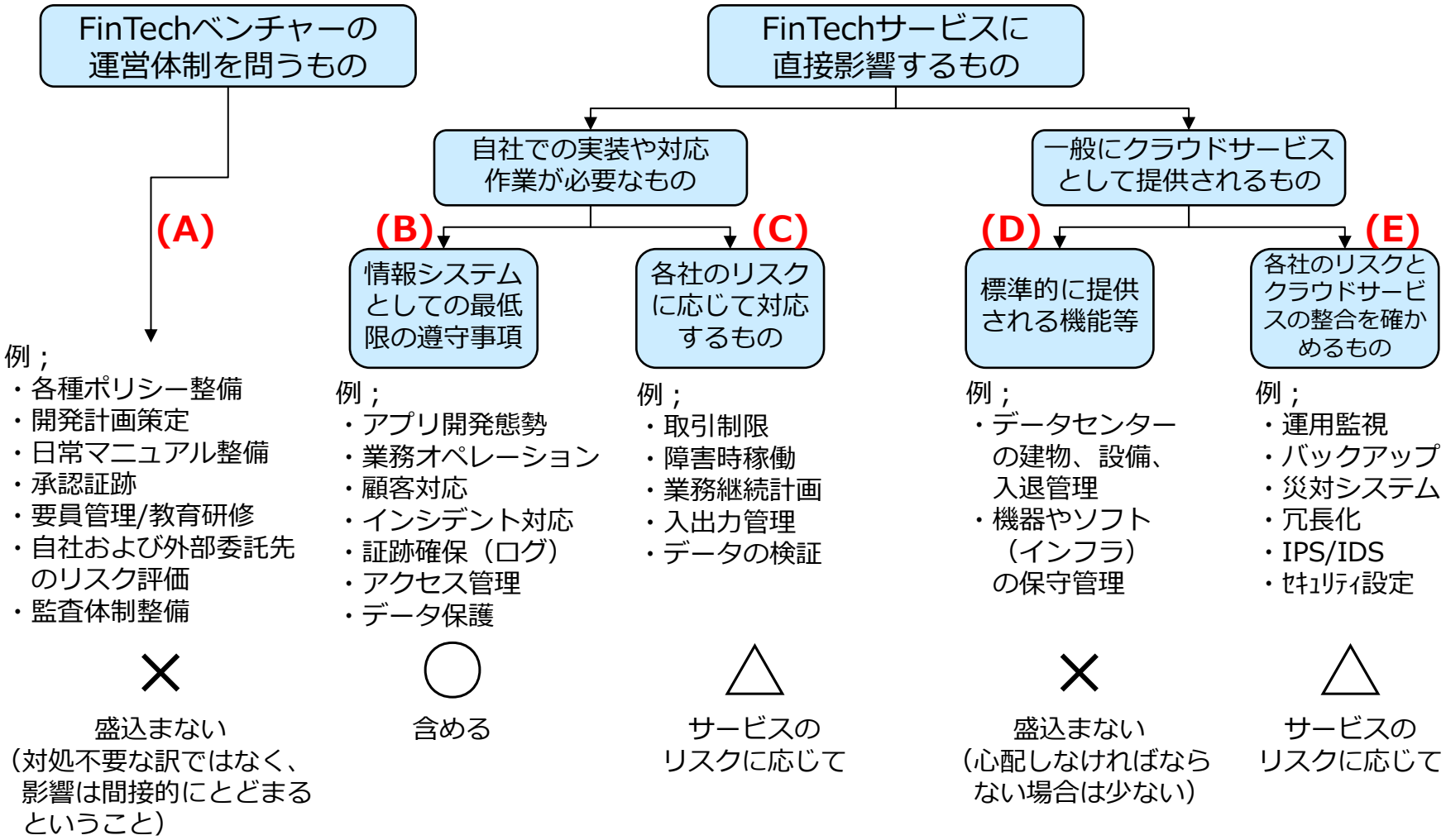
リスクに応じて実際に遵守する基準項目

チェックポイント編

ガイドラインの構成

2)チェックポイント項目の特性と対応方針

FISC安対基準等公的なガイドライン等で対象とされる項目について、各々の特性に応じたFinTechとしての優先順位など、対応方針を次の通りとする。



ガイドラインの構成

3)ガイドライン項目の章立て

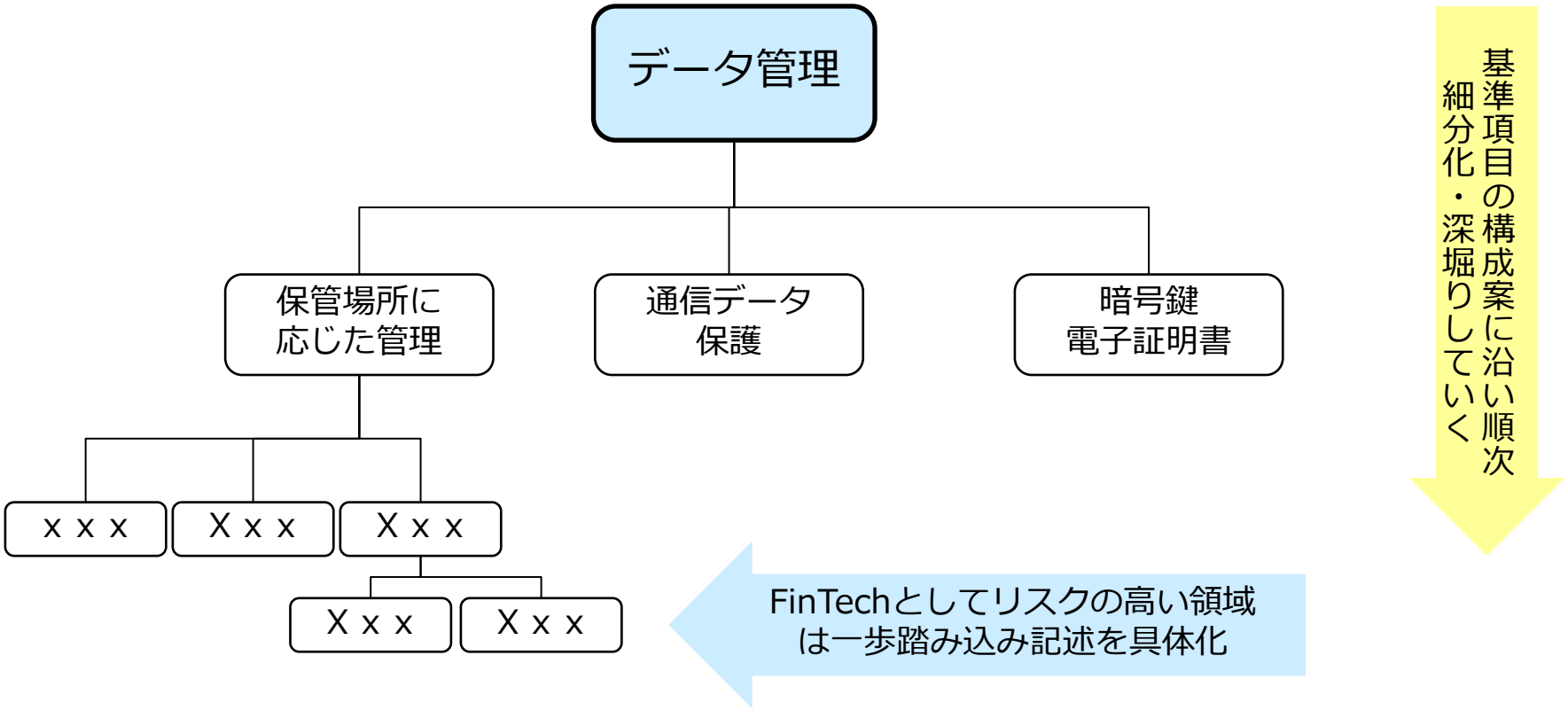
2)の方針に従うとともに、FISC安全対策基準の内容を参考にもれのないよう留意し、次のような章立てとする。

データ管理 (機密保護)	・保管場所に応じたデータ管理（クラウド/自社機器/顧客デバイス） ・通信データ保護　・暗号鍵と電子証明書
アクセス管理 ログ取得	・OS/基盤/アプリ権限管理　・ログ取得と監査　・顧客認証
運用管理・ 監視	・稼働監視　・業務管理（入出力管理）　・顧客対応（問合せ） ・インシデント管理　・障害対応　・BCP
構成管理	・冗長化/障害対策　・災害対策 ・マルウェア対策/パッチ　・サイバー防衛(DNSｷｬｯｼｭﾎﾟｲｽﾞﾆﾝｸﾞ他)
企画/開発/ 変更管理	・品質管理　・変更管理　・セキュアプログラミング

ガイドラインの構成

4)FinTechの性質に応じたリスクの取込み

スマートデバイス関連やアプリケーション層のセキュリティをはじめとした**FinTechとしてリスクが高い領域**については、一歩踏み込み記述の具体化を　目指す。



ガイドラインの構成

5)想定リスクや対策事例の明示

【サービス内容によらず、必須とする項目】

基準項目	想定リスク	適用例	対策事例（該当ある場合は悪例も）
ルートアカウントの目的外使用や悪用を牽制する。	特定の者が単独で使用でき、使用状況もチェックされない場合は目的外使用や悪用の誘因となる。	全ての場合	・2要素認証を導入し、各要素を別の者が保有することにより、単独使用を不可とする。 ・単独使用を可能としておく場合は、使用状況（ログオン/オフ日時、アカウント名、使用コマンド等）を使用者以外の管理者へ都度通知（警告）し、検証可能とする。 ・通知（警告）はメール送付の他、使用状況リストを出力する方法がある。この場合、当該リストはルート権限者による変更不可なものとし、改ざんを防止する。

【サービス内容により適用を選択する項目】

基準項目	想定リスク	適用例	対策事例（該当ある場合は悪例も）
入力したデータの正確性を件数と合計金額の一致により確認する。	誤入力により値が不正確となる。	紙面の読取り等人手が介在し正確性の担保を慎重に行う必要性が高い場合	・入力前の帳票の件数と合計金額を算出し、入力後のものと比較して一致していることを確認する。 ・予め、件数と合計金額を算出、表示する機能を実装しておく。

なお、サイバー防衛やセキュアプログラミング関連の項目は、公的ガイド*等を参照する方式も検討する。

＊ IPA<独)情報処理推進機構>各種ガイド、OWASP TOP10、SANS CWE TOP25など

ガイドラインの構成

6)新技術の活用によるリスク管理

- ✓ 次のような新技術を活用することにより、負荷軽減と同時にFISC安対基準の趣旨と同等のリスク管理が可能である。しかしながら、FISC安対基準はその字義通りにのみ解釈され、管理手法や技術が趣旨に則っているのか検討されないまま不適とされてしまう恐れがある。
- ✓ ガイドラインにおいてこのような新技術を解説し、リスクコミュニケーションの向上を図ることによって、FinTechを含めた金融システム全体の有効化と効率化に寄与していくことを目指す。
- ✓ 現時点で具体的に想定する事例は下記の２例。
- ✓ 原則として対策の一事例としての記載を想定するが、イミュータブルインフラの例など影響範囲が大きい場合は、個別テーマとして代替可能な基準項目を明示する方法も検討する。

エンベロープ暗号化 [envelop]

- ➢ データ鍵自体を暗号化して保存
- ➢ 意図されたデータ受信者に対してのみ、平文化されたデータ鍵が与えられるとともに、当該平文鍵を速やかに削除する
- ➢ 煩雑な鍵管理プロセスを省略できる

イミュータブルインフラ [imutable]

- ➢ 一度セットアップされたインフラ（サーバ）は変更しない
- ➢ 変更したい場合は、クラウド上に新規インスタンスとして作成する
- ➢ 作業を新規インスタンスへの切替に集約することにより、変更権限の管理を簡素化できる

課題認識

ここまでの内容をセキュリティガイドラインのベースとしてガイドライン策定を目指していくが、環境の変化等に応じて策定後も適時の内容見直しが求められ、当面は次の２点を課題と捉える。

- FISC安全対策基準の改訂内容および当検討会の議論
- 全国銀行協会主催の「オープンAPIのあり方に関する検討会」の議論

FISCへの要望

- 改訂される安全対策基準において、当協会のガイドラインへの言及をいただくとともに、安対基準の一部として組込みや連携*を検討いただくなど、当協会のセキュリティへの取組みの認知向上へのご助力をお願いしたい。

  * 業界団体等が策定するガイドラインに対するFISCの基準書等における言及、FISC基準書等における相当箇所の明示、あるいはFintech企業が実施すべき安全対策の目安となる基準等の公表などを想定。

- 当協会のAPI・セキュリティ分科会（前記）でのご講演など、FinTechベンチャーによる安全対策の理解促進活動へのご支援、ご助言をこれまで同様にお願いしたい。

- 金融制度ワーキンググループにおける論点②「中間的業者に係る環境整備」も踏まえ、FinTechが全て金融機関の外部委託に該当するとの誤解を招かないよう、当検討会の議論を整理、推進願いたい。

作業スケジュール

分類	項目	2016				2017			
		9	10	11	12	1	2	3	4
対関係機関	金融庁、全銀協への情報共有と議論				随時実施				
	FISC新安全対策基準（FinTech）有識者検討会議		2016.10～2017.6　月次程度で開催 協会内の協議内容を随時発信　*1						
協会内活動	理事会							★ 制定決議*2	
	分科会での報告と協議	★ 基本方針説明と合意		★ 作業進捗と協議状況を各分科会で報告		★		★ 最終案説明と合意*2	
	準備会による協議 関係者と事務局の相対相談等				有識者、協力者等関係者を招集、または相対で協議・相談				
	既存FISC安対項目の取込方針策定（取捨選択）		有識者、協力者と事務局で協議し検討						
	ガイドライン記述作業				事務局主体で継続作業				

協会として機関決定

*1 FISC有識者会議の最終成果と協会ガイドラインの位置付け整理は今後の課題とする。
*2 FISC他関係各機関の議論の状況によっては協会ガイドライン完成が後倒しとなる可能性もある。

議事３

FinTech に関する安対基準適用上の課題

金融機関における FinTech に関する安対基準適用上の課題について、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 に関して、従来の安対基準を適用した場合に内在する問題に対して、どのようなリスク管理策を策定することが適切か？

【論点に係る原案の構成】

１．検討にあたっての前提

・検討にあたって、付加的に踏まえておくことが有益な事項を明確にする。

・具体的には、「目標とすべき安全対策の効果の程度」「安対基準における検討対象領域」「簡易なリスク管理策の性質」「クラウドサービスの利用に関する安対基準の取扱い」を取り上げる。

２．　従来の安対基準に基づく関係者の責務

・従来の安対基準をもとに、３者それぞれの関係者の責務を整理するとともに、問題に対するアプローチを明確にする。

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の場合に、内在する問題および安全対策の在り方を明確にし、リスク管理策を提案する。

４．タイプⅢにおいて内在する問題と安全対策の在り方

・タイプⅢの場合に、内在する問題および安全対策の在り方を明確にし、リスク管理策を提案する。

５．関係者間の協調

・上記安全対策の検討において、関係者間の協調が重要であることを明確にする。

【論点に係る原案】

・別紙１参照。

以上

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。

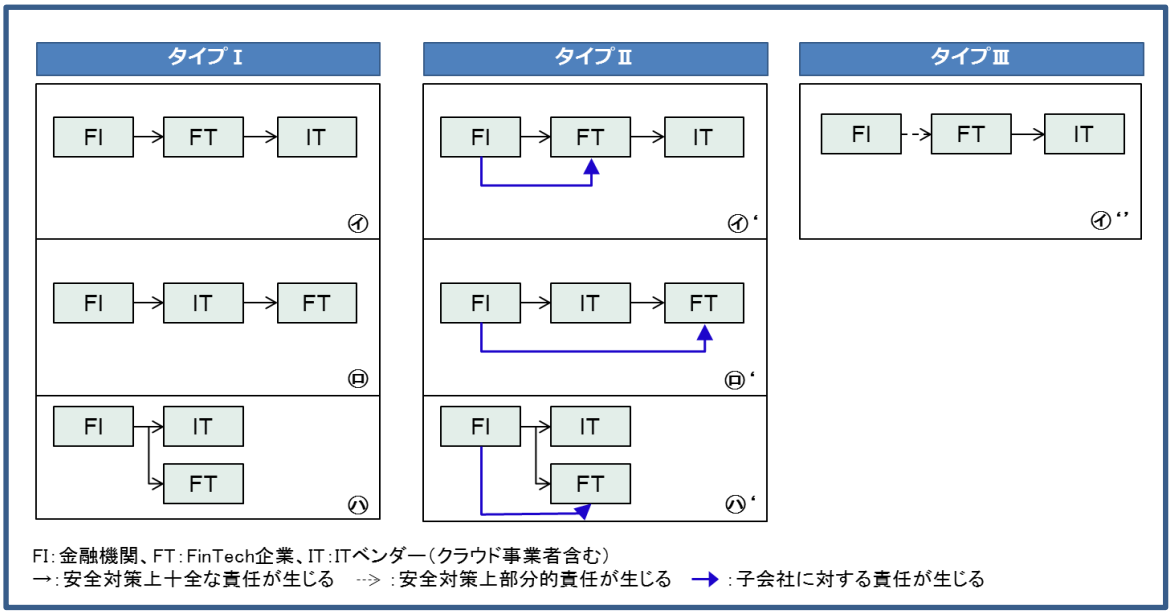
なお、以上の留意事項を解決するため、本検討会において、クラウドサービスを利用する場合の管理策について、外部委託検討会報告書の成果を踏まえて、補足的な検討を行うことが考えられる。こうした補足的検討をあらかじめ行っておけば、重要な情報システムでクラウドサービスを利用した FinTech のユースケース（ブロックチェーン・AI 等）が登場した際にも、その前提が整理されていることとなり、有益である。

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、タイプⅠの安全対策の在り方としては、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。

タイプⅠにおいて、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]。

[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」においても合理的な考え方である。

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。

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。

タイプⅢにおける金融機関の関心項目例（【責務Ａ】から抜粋）		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、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。	
	データの所在の把握	7
	FinTech 企業は、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、その具体的な所在地を把握しているか。例えば、IT ベンダーに対して、所在地に関する情報の提供を求めているか。	
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、金融機関とデータの保全に係る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 ベンダーとデータの保全に係る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）	

	監査権の明記	14
	FinTech 企業は、金融機関によるデータの保全に係る監査権を認めるか。また、再委託先との契約で、金融機関による監査権を明記しているか。	
	再委託先の事前審査の明確化	25
	FinTech 企業は、データの管理を IT ベンダーへ再委託する場合、金融機関による事前審査に、対応するか。	
d.運用時	データ管理委託時の漏洩防止策の実施	28
	FinTech 企業は、IT ベンダーに対して、データの漏洩防止策を実施させているか。	
	日常的監視	30
	FinTech 企業は、金融機関に対して、データの保全に係る状況を報告することが可能か。	
	システム監査体制の整備	31
	FinTech 企業は、データの保全に係る監査・評価を受忍するか。	

注　…参考１の通番を記載

以上のとおり、タイプⅢにおいて、金融機関が FinTech 企業へデータ提供する際に負う責務は、【責務Ａ】の中でも、顧客に関するデータの保全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に係る責務を担う、とすることが可能である。
なお、データの保全に関する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も、適切な安全対策を実施することも、社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 企業においても、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。

以上

【議事3 - 参考1】

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
a.利用検討時	1	委託目的と範囲の明確化	必要	運87 1. 2.	外部委託を行う場合は、事前に目的や範囲等を明確にすること。	－	－	－
			必要	運108 1. 2.				
	2	選定手続きの明確化	必要	運87-1 1.	外部委託先を選定するにあたっては、選定手続きを明確にすること。 （再委託先の選定要件をあらかじめ定めることを含む）	－	－	－
			必要	運108 1.				
			必要	外部委託有識者検討会 Ⅳ.4.(1)				
	3	客観的評価の実施	必要	運87-1 2.	外部委託先を客観的に評価すること。 なお、当該業務に求められるリスク管理レベルを検討のうえ、その実現が可能な外部委託先を選定すること。 その際、外部委託先の資質・業務遂行能力に関する情報や、外部委託先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。	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がある。	金融機関の再委託先を客観的に評価する責務がある。	一次委託先が客観的評価を実施するために必要とする情報を、一次委託先に提供する責務がある。
			必要	運108 3.				
	4	機密保持契約の事前締結	望ましい	運108 3.	評価にあたっては、必要に応じ機密保持契約を事前に締結することが望ましい。	－	－	－
	5	（委託業務の重要度が高くない場合） 公開情報や評判、実績等による客観的評価の実施	可能	運108 3.	金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合は、公開情報や業界における評判や実績等による客観的な評価を行うことも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、金融機関の再委託先の公開情報や業界における評判や実績等により、客観的な評価を行うことも可能である。	－
	6	契約中断・終了に伴う移行作業の事前把握	望ましい	運108 3.(11)	外部委託契約の中断・終了に伴うシステム移行作業(移行データの抽出方法と実際の移行作業内容)については、サービス利用前に把握することが望ましい。	－	－	－

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	7	データの所在の把握	必要	運1084.	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)を把握する必要がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)について、金融機関に情報を提供する責務がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)を把握する責務がある。	高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)について、一次委託先に情報提供する責務がある。
			必要	運1084.	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する必要がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、金融機関等がデータセンターの立地状況等を見極める観点から、金融機関に詳細な所在地まで情報提供する責務がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する責務がある。	勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、一次委託先等がデータセンターの立地状況等を見極める観点から、一次委託先に詳細な所在地まで情報提供する責務がある。
			必要	運1084.	インシデント発生時にデータセンターへの立入が必要になる場合や立入監査を行う際には、具体的な所在地を把握する必要がある。	インシデント発生時に金融機関がデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を金融機関に情報提供する責務がある。	インシデント発生時にデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を把握する責務がある。	インシデント発生時に一次委託先がデータセンターへ立ち入る必要がある場合や立入監査を行う際には、具体的な所在地を一次委託先に情報提供する責務がある。
		（委託業務の重要度が高くない場合）データの所在の把握の必要性	可能	運1084.	金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、データの所在地に関する情報の把握について省略することも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、データの所在地に関する情報の把握について省略することも可能である。	－
	8	他国で係争が発生することを想定して評価すべきリスク	必要	運1085.	外部委託先との間で係争が生じた場合の準拠法やこれを取り扱う裁判所に関する取決めが他国である場合に、外部委託先の選定にあたってリスクを評価すること。	－	－	－
	9	責任者による事業者決定の承認	必要	運87-13.	委託業者の決定には、最終的には責任者の承認を得ること。	－	－	－
			必要	運1086.				

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	10	（パッケージ導入の場合） 評価体制の整備及び運営・管理体制の明確化	必要	運87-14.	外部委託先が所有するアプリケーション、サービス等の導入に際しては、【運72、運73】も参照のこと。	パッケージを導入する場合、金融機関がパッケージの評価等を行うために必要とする情報を、金融機関に提供する責務がある。	パッケージを導入する場合、パッケージの有効性、信頼性、生産性等を評価する体制を整備する責務がある。 また、パッケージの運用・管理体制を明確にする責務がある。	パッケージを導入する場合、一次委託先がパッケージの評価等を行うために必要とする情報を、一次委託先に提供する責務がある。
			望ましい	運1087.	パッケージを導入する場合は、必要に応じて【運72、運73】を参照すること。			
b.契約締結時	11	安全対策を盛り込んだ委託契約の締結	必要	運881.	外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として外部委託先と締結すること。	金融機関が外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として、金融機関と締結する責務がある。	外部委託した業務が安全に遂行されるために、機密保護や安全な業務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がある。	一次委託先が外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として、一次委託先と締結する責務がある。
			必要	運1091.				
	12	事業者からの情報開示	必要（注2）	運1091.(9)	金融機関とクラウド事業者が協議のうえ、必要な情報をクラウド事業者が提供することを契約上明記すること。	金融機関が必要とする情報の提供について、金融機関との契約上明記する責務がある。	金融機関の再委託先と協議のうえ、必要な情報を金融機関の再委託先が提供することを契約上明記する責務がある。	一次委託先が必要とする情報の提供について、一次委託先との契約上明記する責務がある。
			必要（注2）	運1091.(9)	開示請求の対象情報の機密性が高い場合には、両者の間で機密保持契約を締結したうえで提供すること。	開示請求の対象情報の機密性が高い場合には、両者（金融機関と一次委託先）の間で機密保持契約を締結したうえで提供する責務がある。	開示請求の対象情報の機密性が高い場合には、両者（一次委託先と金融機関の再委託先）の間で機密保持契約を締結したうえで提供する責務がある。	開示請求の対象情報の機密性が高い場合には、両者（一次委託先と金融機関の再委託先）の間で機密保持契約を締結したうえで提供する責務がある。
			必要（注2）	運1091.(9)	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくはクラウド事業者側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを契約やSLAに明記すること。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを金融機関との契約やSLAに明記する責務がある。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを金融機関の再委託先との契約やSLAに明記する責務がある。	リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくは金融機関の再委託先の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、一次委託先からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを一次委託先との契約やSLAに明記する責務がある。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
		（委託業務の重要度が高くない場合） 事業者からの詳細かつ厳格な情報開示	可能	運109 1.(9)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合には、外部委託先に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断した場合は、金融機関の再委託先に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。	－
	13	（複数事業者へ委託する場合） 事業者間の相互調整機能を担う事業者の事前決定	必要 （注2）	運109 1.(10)	障害発生時等の迅速な対応のため、委託元金融機関の管理能力を踏まえ、委託元金融機関・外部委託先間での責任関係を明確にし、一元的な窓口機能や外部委託先間の相互調整機能を担う事業者をあらかじめ決めておくこと。 なお、この役割を委託元金融機関が担える場合においては、外部委託先側の相互調整機能を担う事業者は必要ではない。	－	－	－
		（委託業務の重要度が高くない場合） 調整機能役の事業者設置の必要性	可能	運109 1.(10)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合、かつリスク分析の結果として、障害発生時の影響範囲が限定的である、もしくは復旧自体が遅れてもその影響が軽微であると判断し得る場合は、相互調整を担う事業者を置かないことも可能である。	－	－	－

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	14	委託先への監査権の明記	必要	運88 4.(15)	外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し契約を締結することが必要である。	金融機関が外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、金融機関と契約を締結する責務がある。	外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(金融機関の再委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、金融機関の再委託先と契約を締結する責務がある。	一次委託先が外部に委託する業務の種類や範囲に応じて、安全対策上、監査の権利(外部委託先を監査する権利あるいは外部の専門機関により監査を実施する権利等)を考慮し、一次委託先と契約を締結する責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(2)	「重要な情報システム」が外部委託される場合は、委託先との委託契約の締結に当たっては、再委託先をチェックする仕組みを担保するため、金融機関等による再委託先への監査権を明記すること。	「重要な情報システム」を受託する場合は、金融機関との委託契約の締結に当たっては、金融機関の再委託先をチェックする仕組みを担保するため、金融機関等による再委託先への監査権を明記する責務がある。	「重要な情報システム」を金融機関の再委託先に外部委託する場合は、金融機関の再委託先との委託契約の締結に当たっては、金融機関の再委託先をチェックする仕組みを担保するため、金融機関等による再委託先への監査権を明記する責務がある。	「重要な情報システム」を受託する場合は、一次委託先との委託契約の締結に当たっては、金融機関の再委託先をチェックする仕組みを担保するため、金融機関等による再委託先への監査権を明記する責務がある。
			可能	外部委託有識者検討会 Ⅳ.4.(2)	監査に当たっては、みずからが実施する以外にも適切な監査人に監査を委託することも可能である。	－	監査に当たっては、みずからが実施する以外にも適切な監査人に監査を委託することも可能である。	－
			可能	外部委託有識者検討会 Ⅳ.4.(2)	「重要な情報システム」以外の情報システムが外部委託される場合は、委託先との委託契約の締結に当たっては、金融機関等による再委託先への監査権を明記しないことが可能である。	－	金融機関が「重要な情報システム」以外の情報システムを外部委託し、かつ金融機関の再委託先への監査権を明記しない場合は、金融機関の再委託先との委託契約の締結に当たって、金融機関等による再委託先への監査権を明記しないことが可能である。	－
			可能	外部委託有識者検討会 Ⅳ.4.(2)	「重要な情報システム」が外部委託される場合でも、委託業務が細分化され再委託先に委託された結果、その再委託業務のリスクが十分に低いと判断しうる場合には、上記の簡易な手続きで代替することが可能である。	－	金融機関が「重要な情報システム」を外部委託し、かつ再委託業務のリスクが十分低いと判断し、簡易な手続きで代替した場合は、その再委託業務のリスクが十分に低いと判断しうる場合には、上記の簡易な手続きで代替することが可能である。	－
	15	立入監査等の権利の明記	必要（注2）	運109 1.(12)	業務委託契約に、委託元金融機関等の立入監査等を実施する権利を明記すること。	金融機関との業務委託契約に、金融機関等の立入監査等を実施する権利を明記する責務がある。	金融機関の再委託先との業務委託契約に、一次委託先が再委託先に立入監査等を実施する権利を明記する責務がある。	一次委託先との業務委託契約に、一次委託先等の立入監査等を実施する権利を明記する責務がある。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	16	立入監査等の代替手段の明記	必要（注2）	運109 1.(12)	委託元金融機関が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とすること。	金融機関等が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替可能である。	一次委託先が金融機関の再委託先に直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とする責務がある。	一次委託先等が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替可能である。
	17	立入監査等の権利行使の明記	必要（注2）	運109 1.(12)	クラウド技術に関する重要な脆弱性が判明した場合、クラウド事業者における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、委託元金融機関への影響を確認するため、臨時の第三者監査を行うことが可能となっていること。	クラウド技術に関する重要な脆弱性が判明した場合、金融機関の再委託先における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、金融機関等への影響を確認するため、臨時の第三者監査の実施が可能となっている責務がある。	クラウド技術に関する重要な脆弱性が判明した場合、金融機関の再委託先における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、金融機関等への影響を確認するため、臨時の第三者監査を行うことが可能となっている責務がある。	クラウド技術に関する重要な脆弱性が判明した場合、自社における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、一次委託先等への影響を確認するため、臨時の第三者監査の実施が可能となっている責務がある。
		（立入監査等の実施が限定されている場合） 立入監査等の権利行使の条件の認識共有	可能	運109 1.(12)	立入監査等に代替する第三者監査が行われない、または依拠できないと判断される場合に限定して立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、委託元金融機関とクラウド事業者の両者が認識を共有することも可能である。	－	立入監査等に代替する第三者監査が行われない、または依拠できないと金融機関が判断した場合に限定して、立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、一次委託先と金融機関の再委託先の両者が認識を共有することが可能である。	－
	18	立入監査等の受入対応費用の明記	必要（注2）	運109 1.(12)	立入監査を受けるクラウド事業者側の受入対応の費用については、委託元金融機関、クラウド事業者側のいずれが負担するか、あらかじめ両者で協議しておくこと。	立入監査を受ける一次委託先側の受入対応の費用については、金融機関、一次委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。	立入監査を受ける金融機関の再委託先側の受入対応の費用については、一次委託先、金融機関の再委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。	立入監査を受ける金融機関の再委託先の受入対応の費用については、一次委託先、金融機関の再委託先側のいずれが負担するか、あらかじめ両者で協議しておく責務がある。
	19	再委託先への立入監査権の明記	必要（注2）	運109 1.(12)	再委託する業務が重要な場合、再委託先等に対して、委託元金融機関とクラウド事業者間の契約に、金融機関による再委託先への立入監査を実施する権利を明記すること。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、金融機関と一次委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、一次委託先と金融機関の再委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。	金融機関が再委託する業務が重要な場合、金融機関の再委託先等に対して、一次委託先と金融機関の再委託先間の契約に、金融機関による再委託先への立入監査を実施する権利を明記する責務がある。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	20	立入監査等の指摘事項の扱いの明記	必要（注2）	運109 1.(12)	立入監査等により判明した指摘事項については、対応の是非を含め、委託元金融機関とクラウド事業者の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にすること。	立入監査等により判明した指摘事項については、対応の是非を含め、金融機関と一次委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。	立入監査等により判明した指摘事項については、対応の是非を含め、一次委託先と金融機関の再委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。	立入監査等により判明した指摘事項については、対応の是非を含め、一次委託先と金融機関の再委託先の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にする責務がある。
	21	金融監督当局の検査等の明記	必要（注2）	運109 1.(13)	当局の立入り検査等の円滑な実施を担保するため、委託元金融機関と外部委託先との間の契約に、外部委託先の当局検査等への協力義務を明記すること。	当局の立入り検査等の円滑な実施を担保するため、金融機関と一次委託先との間の契約に、一次委託先の当局検査等への協力義務を明記する責務がある。	当局の立入り検査等の円滑な実施を担保するため、一次委託先と金融機関の再委託先との間の契約に、金融機関の再委託先の当局検査等への協力義務を明記する責務がある。	当局の立入り検査等の円滑な実施を担保するため、一次委託先と金融機関の再委託先との間の契約に、一次委託先の当局検査等への協力義務を明記する責務がある。
			必要（注2）	運109 1.(13)	業務委託の再委託先(再々委託先を含む)に対しても、金融機関と元請け事業者との間の契約に、当局検査等への協力義務を明記すること。	業務委託の再委託先(再々委託先を含む)に対しても、金融機関と一次委託先との間の契約に、当局検査等への協力義務を明記する責務がある。	業務委託の再委託先(再々委託先を含む)に対しても、一次委託先と金融機関の再委託先との間の契約に、当局検査等への協力義務を明記する責務がある。	業務委託の再委託先(再々委託先を含む)に対しても、一次委託先と金融機関の再委託先との間の契約に、当局検査等への協力義務を明記する責務がある。
			必要（注2）	運109 1.(13)	当局検査等の指摘事項については、速やかに改善を図る旨の条項を契約に明記すること。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、金融機関と一次委託先との間の契約に明記する責務がある。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、一次委託先と金融機関の再委託先との間の契約に明記する責務がある。	当局検査等の指摘事項については、速やかに改善を図る旨の条項を、一次委託先と金融機関の再委託先との間の契約に明記する責務がある。
			必要（注2）	運109 1.(14)	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、クラウド事業者が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、委託元金融機関自ら、もしくは委託元金融機関が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記すること。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、金融機関自ら、もしくは金融機関が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると一次委託先が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、一次委託先自ら、もしくは一次委託先が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。	情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、金融機関の再委託先が情報提供に応じない、提供しても迅速性に問題があると一次委託先が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、一次委託先自ら、もしくは一次委託先が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記する責務がある。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	22	インシデント発生時の立入調査の明記	必要（注2）	運109 1.(14)	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、契約締結時に合意を得ること。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、金融機関との契約締結時に合意を得る責務がある。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、金融機関の再委託先との契約締結時に合意を得る責務がある。	調査時に収集の対象となる証跡の範囲及び抽出ツールの開発・検証のために必要となる費用負担について、一次委託先との契約締結時に合意を得る責務がある。
			必要（注2）	運109 1.(14)	クラウド事業者の経営不安が発生した場合、委託元金融機関自らもしくは委託元金融機関が指定する専門業者が、必要に応じ、クラウド事業者施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことを認めるよう契約に明記すること。	金融機関の再委託先の経営不安が発生した場合、金融機関自らもしくは金融機関が指定する専門業者が、必要に応じ、金融機関の再委託先施設に立ち入り、顧客データや関連著作物・成果物を保全することに協力することを契約に明記する責務がある。	金融機関の再委託先の経営不安が発生した場合、一次委託先自らもしくは一次委託先が指定する専門業者が、必要に応じ、金融機関の再委託先施設に立ち入り、顧客データや関連著作物・成果物の保全を行うことを認めるよう契約に明記する責務がある。	自社の経営不安が発生した場合、一次委託先自らもしくは一次委託先が指定する専門業者が、必要に応じ、自社施設に立ち入り、顧客データや関連著作物・成果物を保全することに協力することを契約に明記する責務がある。
	23	（海外でのデータ保管時の場合） 日本語サポート及び障害対応窓口設置の明確化	必要（注2）	運109 1.(16)	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、外部委託先の日本法人等の障害対応窓口設置を明確にすること。	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、一次委託先の日本法人等の障害対応窓口の設置に関する情報を、金融機関に提供する責務がある。	一次委託先における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、金融機関の再委託先の日本法人等の障害対応窓口設置を明確にすること。	金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、一次委託先の日本法人等の障害対応窓口の設置に関する情報を、一次委託先に提供する責務がある。
	24	トレーサビリティ確保の準備	必要（注2）	運109 1.(17)	万一障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備すること。	万一障害や情報漏洩等のインシデントが発生した際には、金融機関からの求めに応じて、トレーサビリティ確保のための方策を準備する責務がある。	万一障害や情報漏洩等のインシデントが発生した際には、金融機関からの求めに応じて、トレーサビリティ確保のための方策を金融機関の再委託先に準備させる責務がある。	万一障害や情報漏洩等のインシデントが発生した際には、一次委託先からの求めに応じて、トレーサビリティ確保のための方策を準備する責務がある。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	25	再委託先の事前審査の明確化	必要（注2）	運109 1.(11)	外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、委託業務を再委託する場合、再委託先に対する適切な事前審査を行うこと。 勘定系システムや機密性の高い顧客データを保管するシステム等、特に重要な業務を再委託する場合には、金融機関等自らが事前審査をすること。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、金融機関が委託業務を再委託する場合、金融機関の再委託先に対する適切な事前審査を行うことに対応する責務がある。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、一次委託先が金融機関の再委託先に業務委託する場合、再委託先に対する適切な事前審査を行う責務がある。	金融機関が外部委託の状況を把握し、不適切な再委託先が介在することを排除するため、金融機関が委託業務を再委託する場合、一次委託先が金融機関の再委託先に対する適切な事前審査を行うことに対応する責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(1)				
		（「重要な情報システム」以外の情報システムの再委託の場合） 再委託先の事前審査の代替	可能	外部委託有識者検討会 Ⅳ.4.(1)	「重要な情報システム」以外の情報システムの再委託に際しては、委託先の再委託先に対する審査・管理プロセスが金融機関等のそれと同等かそれ以上実効的であるとみなされる場合には、金融機関等が、あらかじめ委託先の審査・管理プロセスの整備・運用状況の適切性検証することで、そうした検証結果の確認をもって、個別の再委託先の事前審査に代替させることが可能である。	－	－	－
		（委託業務の重要度が高くない場合） 再委託先の事前審査の簡易化	可能	運109 1.(11)	金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、再委託先における委託元金融機関による事前の審査や日常のモニタリング等のリスク管理を簡易化することも可能である。	－	－	－
		サービスレベルの合意	望ましい	運88 5.	SLAの締結やSLOの確認により、サービスレベルについて合意することが望ましい。	SLAの締結やSLOの確認により、サービスレベルについて、金融機関と合意する責務がある。	SLAの締結やSLOの確認により、サービスレベルについて、金融機関の再委託先と合意する責務がある。	SLAの締結やSLOの確認により、サービスレベルについて、一次委託先と合意する責務がある。
			望ましい	運109 2.				

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	26	（委託業務の重要度が高くない場合） SLA締結の省略	可能	運1093.	金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、クラウド事業者が提示する標準的なSLAを締結することや一般的な契約の締結のみを行い、SLAの締結を省略することも可能である。	－	金融機関等において委託する業務の重要度が高くないと判断し、かつ金融機関の再委託先が提示する標準的なSLAを締結することや一般的な契約の締結のみを行い、SLAの締結を省略した場合は、金融機関の再委託先が提示する標準的なSLAを締結することや一般的な契約の締結のみを行い、SLAの締結を省略することも可能である。	－
	27	代替サービスや他への移行の事前準備	望ましい	運1094.	サービスレベル合意の違反のほか、クラウド事業者や金融機関の方針変更によってクラウド事業者との契約の続行が困難になるような場合でも、業務の継続を可能とするため、事前に代替のクラウドサービスや一般のアウトソーシングに移行する、もしくはオンプレミスの環境に移行することができるような対策を講ずることが望ましい。	－	－	－
		（委託業務の重要度が高くない場合） 外部委託先の協力を前提としないシステム移行準備	可能	運1094.	金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、外部委託先の協力を前提とせず、別の外部委託先に移行するための準備をあらかじめ行っておくことをもって代替することが可能である。	－	－	－
c.開発時		開発の外部委託については、「必要最低限の安対基準」の適用対象とすることが可能 （注3）						

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
d.運用時	28	データ管理委託時の漏洩防止策の実施	必要	運1101.	外部委託先にデータ管理を委託する場合、漏洩防止策を講ずること。	金融機関からデータ管理を受託する場合、金融機関からの求めに応じて、漏洩防止策を講じる責務がある。	金融機関の再委託先にデータ管理を委託する場合、金融機関からの求めに応じて、金融機関の再委託先に、漏洩防止策を実施させる責務がある。	一次委託先からデータ管理を受託する場合、一次委託先からの求めに応じて、漏洩防止策を講じる責務がある。
		蓄積・伝送データの暗号化の実施	必要	運1101.(1)	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じること。 なお、仕様上の制約から暗号化が不可能な部分(平文で処理される部分)でのデータ覗き見リスクを把握するため、暗号化の仕様を把握し、自社のリスク管理のポリシーに合致しているかどうか判断する必要がある。	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じる責務がある。 なお、金融機関がリスク管理のポリシーに合致しているかどうかを判断するため、金融機関に暗号化の仕様に関する情報を提供する責務がある。	機密性の高い個人データ等が含まれているデータについては、金融機関の再委託先に対して暗号化等の管理策を求める責務がある。 なお、仕様上の制約から暗号化が不可能な部分(平文で処理される部分)でのデータ覗き見リスクを把握するため、暗号化の仕様を把握し、自社のリスク管理のポリシーに合致しているかどうか判断する責務がある。	機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じる責務がある。 なお、一次委託先がリスク管理のポリシーに合致しているかどうかを判断するため、一次委託先に暗号化の仕様に関する情報を提供する責務がある。
		暗号鍵の管理主体の適切性確認	必要	運1101.(2)	クラウド事業者に暗号鍵の管理を委ねる場合には、その管理策の概要を十分に把握し、自社のリスク管理ポリシーに合致していることを判断する必要がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、金融機関がその管理策の概要を十分に把握し、リスク管理のポリシーに合致しているかどうかを判断するため、金融機関に暗号化の仕様に関する情報を提供する責務がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、その管理策の概要を十分に把握し、自社のリスク管理ポリシーに合致していることを判断する責務がある。	金融機関の再委託先に暗号鍵の管理を委ねる場合には、一次委託先がその管理策の概要を十分に把握し、リスク管理のポリシーに合致しているかどうかを判断するため、一次委託先に暗号化の仕様に関する情報を提供する責務がある。
		暗号化の代替策の実施	必要	運1101.(3)	元データとトークンを金融機関側で持ち、クラウド環境下にあるデータを無作為な乱数に置き換え、実質的に無意味化するとしたトークン化技術を利用することが可能である。 ただし、トークン化を管理策として採用する場合には、金融機関におけるトークンマッピング(対応表)の管理についても相応の管理策が必要となる。	－	－	－

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	29	記憶装置等の障害・交換におけるデータ消去の実施	必要	運110 2.	外部委託先の記憶装置の故障等により、機器・部品を交換する場合には、交換対象の記憶装置等の機器・部品に金融機関等やその顧客の情報等の機密性の高いデータが残存している可能性があるため、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う必要がある。	一次委託先の記憶装置の故障等により、機器・部品を交換する場合には、金融機関からの求めに応じて、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う責務がある。	金融機関の再委託先の記憶装置の故障等により、機器・部品を交換する場合には、金融機関からの求めに応じて、金融機関の再委託先に、これらの記憶装置等に対して、データ消去を含めた十分な管理を行わせる責務がある。	金融機関の再委託先の記憶装置の故障等により、機器・部品を交換する場合には、一次委託先からの求めに応じて、これらの記憶装置等に対して、データ消去を含めた十分な管理を行う責務がある。
		記憶装置等の障害・交換時の消去証明書代替策	可能	運110 2.	契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、クラウド事業者に対して情報提出要請や監査等の方法で消去・破壊プロセスの実効性を検証することで代替することも可能である。	－	契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、金融機関の再委託先に対して情報提出要請や監査等の方法で消去・破壊プロセスの実効性を検証することで代替可能である。	－
		（重要なデータを扱わない場合） データ消去・破壊の必要性	可能	運110 2.	外部委託先で重要なデータを扱わない場合は、記憶装置等の交換に際し、データの消去・破壊を実施しないことも可能である。	－	－	－
	30	委託業務の日常的監視	必要	運89 1. 2. 3.	外部委託業務を円滑かつ適正に運営する観点から、委託先の業務範囲や責任、委託先要員の遵守すべきルールを明確にし、日常的に監視する必要がある。	金融機関からの日常的監視を受忍する責務がある。	外部委託業務を円滑かつ適正に運営する観点から、金融機関の再委託先の業務範囲や責任、要員が遵守すべきルールを明確にし、日常的に監視する責務がある。	一次委託先からの日常的監視を受忍する責務がある。
			必要	運90 1. 2. 3.				
			必要	運112 1. 2.				

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
	31	システム監査体制の整備	必要	運91 1. 2. 3. 4. 5. 6.	外部委託業務に関するコンピューターシステムの運用、開発・変更等において、有効性、効率性、信頼性、遵守性、および安全性を確保するため、独立した監査人がコンピューターシステムの総合的な監査・評価を行い、経営層に監査結果を報告する体制を整備する必要がある。	受託業務に関するコンピューターシステムの運用、開発・変更等において、独立した監査人が実施するコンピューターシステムの総合的な監査・評価を受忍する責務がある。	外部委託業務に関するコンピューターシステムの運用、開発・変更等において、有効性、効率性、信頼性、遵守性、および安全性を確保するため、独立した監査人がコンピューターシステムの総合的な監査・評価を行う責務がある。	受託業務に関するコンピューターシステムの運用、開発・変更等において、独立した監査人が実施するコンピューターシステムの総合的な監査・評価を受忍する責務がある。
		立入監査の実施	必要	運112 2.	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、クラウド事業者のオフィスやデータセンターへの立入監査・モニタリング等により実地で確認することが必要である。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、自社のオフィスやデータセンターへの金融機関による立入監査・モニタリング等により実地で確認を受忍する責務がある。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、金融機関の再委託先のオフィスやデータセンターへの立入監査・モニタリング等により実地で確認する責務がある。	情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、自社のオフィスやデータセンターへ立入監査・モニタリング等により実地で確認を受忍する責務がある。
		第三者監査の実施	可能	運112 3.	外部委託先に対する実地調査(オンサイトモニタリング)が有効ではない場合などに、第三者監査で代替することが可能である。	–	金融機関の再委託先に対する実地調査(オンサイトモニタリング)が有効ではない場合などに、第三者監査で代替することが可能である。	–
			必要	外部委託有識者検討会 脚注40 （注4）	第三者から見た際に、クラウド事業者との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。	第三者から見た際に、金融機関からの求めに応じて、金融機関との利益相反に疑義が生じるような外観を呈していない監査法人を選定する責務がある。	第三者から見た際に、金融機関からの求めに応じて、金融機関の再委託先に、金融機関の再委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定させる責務がある。	第三者から見た際に、一次委託先からの求めに応じて、一次委託先との利益相反に疑義が生じるような外観を呈していない監査法人を選定する責務がある。
		（委託業務の重要度が高くない場合） 費用対効果を踏まえた管理策の実施	可能	運112 4.	外部委託業務の重要度が高くない場合は、費用対効果を踏まえ、立入監査の代わりに、第三者認証等を活用することが可能である。	–	金融機関等が外部委託業務の重要度が高くないと判断する場合は、金融機関の再委託先への委託業務について、費用対効果を踏まえ、立入監査の代わりに、第三者認証等を活用することが可能である。	–

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
e.終了時	32	契約終了時の機密保護・プライバシー保護・不正防止対策の実施	必要	運111 1.	外部委託契約を終了する場合、データ漏洩防止のため、機密保護、プライバシー保護及び不正防止のための対策を講じる必要がある。	外部委託契約を終了する場合、金融機関からの求めに応じて、機密保護、プライバシー保護及び不正防止のための対策を講じる責務がある。	外部委託契約を終了する場合、金融機関からの求めに応じて、金融機関の再委託先に、機密保護、プライバシー保護及び不正防止のための対策を実施させる責務がある。	外部委託契約を終了する場合、一次委託先からの求めに応じて、機密保護、プライバシー保護及び不正防止のための対策を講じる責務がある。
		データ消去方法の種類	必要	運111 2.	データ消去にあたっては、物理的消去と論理的消去が考えられる。 なお、将来的なハードウェア更改・撤去時に物理的消去を行うことが望ましい。 （注）論理的消去の実施のみでも可	データ消去にあたっては、金融機関からの求めに応じて、論理的消去を実施する責務がある。	データ消去にあたっては、金融機関からの求めに応じて、金融機関の再委託先に、論理的消去を実施させる責務がある。	データ消去にあたっては、一次委託先からの求めに応じて、論理的消去を実施する責務がある。
		消去証明書等の受領	望ましい	運111 3.	外部委託先がデータを消去する場合、消去証明書を受領することが望ましい。	データを消去する場合、金融機関に消去証明書を提出する責務がある。	金融機関の再委託先がデータを消去する場合、消去証明書を受領する責務がある。	データを消去する場合、一次委託先に消去証明書を提出する責務がある。
		消去証明書の代替手段の実施	可能	運111 3.	外部委託先が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。	－	金融機関の再委託先が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。	－
		（機密情報を扱わない業務委託の場合） データ消去プロセスの簡略化等	可能	運111 4.	顧客データ等の機密情報を扱わない業務を外部委託先に委ねる場合は、契約終了時のデータ消去プロセスを簡略化または不要とすることも考えられ、消去証明書を不要とすることも可能である。	－	－	－

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

従来の安全対策基準の概要（外部委託関連）

管理フェーズ	通番	テーマ	統制の強度	安対基準の項番等	外部委託利用時の金融機関の責務（責務A）（注1）	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）
f.インシデント発生時	33	（重要システムの場合）再委託先を含めた有事対応	必要	外部委託有識者検討会 Ⅳ.4.(3)	「重要な情報システム」が外部委託される場合は、CPは委託先や再委託先も含めて策定される必要がある。	「重要な情報システム」を金融機関から受託する場合は、自社のCPは金融機関や金融機関の再委託先も含めて策定する責務がある。	「重要な情報システム」を金融機関の再委託先に外部委託する場合は、金融機関の再委託先のCPは金融機関や一次委託先も含めて策定させる責務がある。	「重要な情報システム」を一次委託先から受託する場合は、自社のCPは金融機関や一次委託先も含めて策定する責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(3)	委託先等でCPを個別に用意する場合は、各金融機関等のCPと完全に整合し相互補完的な内容とすること。	金融機関等でCPを個別に用意する場合は、自社のCPと完全に整合し相互補完的な内容とする責務がある。	金融機関の再委託先等でCPを個別に用意する場合は、各一次委託先等のCPと完全に整合し相互補完的な内容とさせる責務がある。	一次委託先等でCPを個別に用意する場合は、自社のCPと完全に整合し相互補完的な内容とする責務がある。
			必要	外部委託有識者検討会 Ⅳ.4.(3)	金融機関等は、平時は、委託先等とのCPに基づき、委託先及び再委託先と共同で、定期的に訓練を実施すること。	平時は、金融機関等とのCPに基づき、金融機関及び金融機関の再委託先と共同で、定期的に訓練を実施する責務がある。	平時は、金融機関の再委託先等とのCPに基づき、金融機関及び金融機関の再委託先と共同で、定期的に訓練に参加させる責務がある。	平時は、一次委託先等とのCPに基づき、金融機関及び一次委託先と共同で、定期的に訓練を実施する責務がある。
		リスク管理の実施（注5）		運90-1				

（注1）「外部委託利用時の金融機関の責務（責務A）」
FISC「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（第8版）」・「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（第8版追補改訂）」・「金融機関における外部委託に関する有識者検討会　報告書」に記載された内容から該当箇所を転載

（注2）「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（第8版追補改訂）」22ページ
『クラウド報告書』において契約書に明記することが「必要である」と記載されている項目は、オンプレミスや共同センターといった外部委託でも関連性があると思われる項目であることから、今回は「実施することが望ましい」という内容の記載に留めることとした。

（注3）「金融機関における外部委託に関する有識者検討会　報告書」43ページ
「重要な情報システム」の開発の外部委託（開発時だけでなく、利用検討時、契約締結時、終了時も含まれる）においても、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「必要最低限の安対基準」の適用対象とすることが可能である。

（注4）「金融機関における外部委託に関する有識者検討会　報告書」45ページ　脚注40
FISC『金融機関等のシステム監査指針（改訂第3版追補）』「第1部　第Ⅲ章　5. クラウドサービス監査のポイント（1）クラウド事業者に対する第三者監査人を利用した共同監査の検討」において、監査人の選定として、「顧客に対して責任を負う金融機関として、第三者から見た際に、クラウド事業者との利益相反に疑義が生じるような外観を呈していない監査法人を選定することが必要である。そのために、委託元金融機関は、共同監査の対象機関において、クラウド事業者の会計監査に従事していない監査法人を選定することが必要である。また、クラウド事業者のSOC2、IT7号の保証業務に従事している監査法人を選定する場合には、クラウド事業者のSOC2、IT7号の保証業務に従事していない監査責任者を選定することが必要である。」とされている。

（注5）「第1回金融機関におけるFinTechに関する有識者検討会 【議事3】 別紙1」5ページ　脚注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。

【注記】
本資料は、「FinTechに関する有識者検討会」向けの検討資料として、当検討会事務局にて作成したものとなります。
従って、安全対策基準の改訂を目的として作成した資料ではありません。（安全対策基準の改訂は、別途、専門委員会で検討が行われます）

議事４

安対基準の対象外となる FinTech 業務の取扱い

安対基準の対象外となる FinTech 業務の取扱いについて、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】

安対基準の対象外となる FinTech 業務に関して、どのような意見を表明することが適切であるか？

【論点に係る原案の構成】

１．安対基準における従来の対象の取扱い

・安対基準が、その対象とする情報システムを、従来はどのように取り扱ってきたか、について明確にする。

２．安対基準の対象外となる FinTech 業務の取扱いの方向性

・安対基準の対象外となる FinTech 業務に関して、社会的観点から望まれる、その取扱いの方向性を明確にする。

３．FinTech 業務における安全対策に関する意見表明

・安対基準の対象であるか否かに関わらず、FinTech 業務全般における安全対策に関して、表明すべき意見を明確にする。

【論点に係る原案】

・別紙１参照。

以上

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。

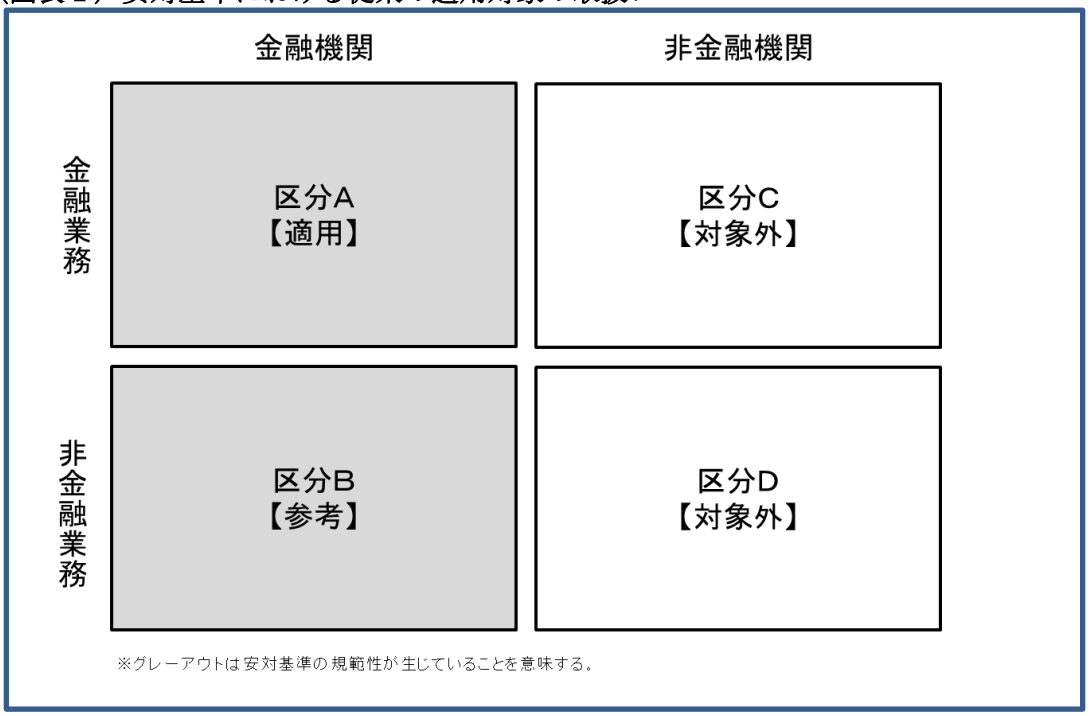
2 平成 28 年９月末現在、FISC 会員数 645 社のうち金融機関は 543 社と、その 84%を占める。

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。

以上

参考１

金融機械化財団[7]（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）

[7] 「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。