資料４

# 「API 接続チェックリスト」の確定に向けた検討方法（案）

「API 接続チェックリスト」の確定に向けた検討方法の原案を以下の通り作成したので、ご議論いただきたい。

【主論点】
「API 接続チェックリスト」に関する検討は、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．現状認識

・当センターでは、「金融機関における FinTech に関する有識者検討会」及び「API 接続先チェックリスト ワーキンググループ」を通じて、FinTech に関する安全対策の在り方を提言及び推進させてきた。

・この過程で、昨年６月に公表した「API 接続チェックリスト（試行版）」は、金融機関と API 接続先の双方において、安全対策に関する共通のコミュニケーション・ツールとして活用され始めている。

・公表後１年を機に、当該チェックリストの使用状況やユーザーからの要望、安全対策基準の全面改訂等を踏まえて、確定版を策定する。

２．検討手順

・検討の手順の第一として、考慮すべき観点を明確にする。【論点１】

・検討の手順の第二として、今回検討対象とした観点でどのように検討するかを明確にする。【論点２】

３．開催予定

本検討会は本年９月末を目途に終了する前提とするが、今後の検討状況等次第で変更となる可能性がある。

| 回数 | 日程 | 主な議題 |
|---|---|---|
| 第１回（本日） | ６月７日（木） | ・「API 接続チェックリスト」の確定に向けた検討方法 |
| 第２回 | ８月２日（木） | ・下部組織（ワーキンググループ）における検討状況の確認（ワーキンググループからの中間報告） |
| 第３回 | ９月下旬 | ・「API 接続チェックリスト」の確定及び公表 |

【論点１】
「API 接続チェックリスト」を検討するにあたり、本検討会で取り上げるべき観点及び対応方針は以下の通りで良いか？

「API 接続チェックリスト（試行版）」は、今後、金融機関及び API 接続先による利用が急速に拡大することが予想される。そうした中、早期に確定版を策定し公表することが求められることも考慮し、本検討会で取り上げる観点及び対応方針を以下の通りとする。

| 項番 | 観点 | 対応方針 |
|---|---|---|
| 1 | ユーザーからの要望への対応 | 多くのユーザーから強い要望がある事項を中心に、対応を検討する。 |
| 2 | 安対基準改訂への対応 | 確認項目のうち「基礎的な安全対策の管理・運営能力」は、安全対策の必要最低限の基準又はそれを踏まえた FinTech 業界の自主基準（規則）に基づき見直すこととしていた。<br>今後、安対基準の改訂内容を踏まえて、認定電子決済等代行事業者協会が自主基準（規則）を制定する予定である。そのため、その内容を「基礎的な安全対策の管理・運営能力」に反映させる。 |
| 3 | 前回検討時の継続検討事項への対応 | 項番 1（ユーザーからの要望への対応）に含めて、対応を検討する。 |
| 4 | API 利用に関する契約書との整合性確保 | 現在開催されている「オープン API 推進研究会」（全銀協）における検討との平仄に留意する。 |
| 5 | 法規制への対応 | 現時点においては、銀行法及び内閣府令等から要請されている事項はないものと判断している。 |
| 6 | 維持管理方法<br>【運用面】 | 今回策定する「API 接続チェックリスト」（確定版）の維持管理方法については別途 FISC にて検討し、検討結果を本検討会（第３回）に上程する。 |

（参考）
・ユーザーからの要望について
　【別紙１】参照
・安対基準の改訂内容について
　【別紙２】参照
・前回検討時の継続検討事項について
　【別紙３】参照

【論点２】
本検討会で取り上げる観点を踏まえた検討は、以下の手順で行うことでよいか？

【本検討会】（第１回：本日）
・「金融機関における API 接続チェックリストに関するワーキンググループ」（以下、「API チェックリスト WG」という）を設置する。
・「API 接続チェックリスト」を検討する観点及び対応方針を決定する。
・API チェックリスト WG に対して、「API 接続チェックリスト（試行版）」の具体的な修正案（以下、「API 接続チェックリスト原案」という）の作成を指示する。

⇩

【API チェックリスト WG】（第１回：６月 11 日～第４回：７月 25 日）
・本検討会からの指示に基づいた計画を策定する。
・「API 接続チェックリスト原案」の検討を開始する。

⇩ 状況報告

【本検討会】（第２回：８月２日）
・API チェックリスト WG 検討状況を確認し、必要に応じて追加的な指示を行う。

⇩

【API チェックリスト WG】（第５回：８月下旬～第６回：９月中旬）
・本検討会からの指示に基づく「API 接続チェックリスト原案」の継続検討を行い、完成させる。
【FISC 事務局】
・「API 接続チェックリスト」の維持管理方法（案）を検討する。

⇩ 上程

【本検討会】（第３回：９月下旬）
・「API 接続チェックリスト原案」を精査し、確定させる。
・「API 接続チェックリスト」の維持管理方法を確定させる。
・「API 接続チェックリスト」を公表する。

以上

別紙１

ユーザーからの要望について

昨年６月の「API 接続チェックリスト（試行版）」公表後、金融機関及び API 接続先、IT ベンダーから寄せられた主な要望は以下の通り。（順不同）

〇必須項目と任意項目の別に関するもの

・手法例の中から必要なものを銀行自ら取捨選択することは、実際にはできないため、必須項目かどうかを明示して欲しい。（地銀【複数先】）
・銀行は、記載されている手法例を全て確認しなければならないと考えてしまうため、必須でない項目があるならば明記して欲しい。（地銀【複数先】）
・「認証の取得」等、スタートアップ企業にとって対応が極めて難しいと思われる項目については、削除するか、任意項目であることを明記する必要がある。（API 接続先【複数先】）
・一部の銀行に対して、例示である「手法例」が「確認すべき項目」であるとの誤解を与えているのではないか。誤解が生じないよう、安対基準を参考にするなどして表示方法等を改善する必要があると思われる。（IT ベンダー）
・仮に確認項目毎に必須や任意の別を明記しても、結局、銀行は全てについて確認することになると思われる。最初から確認項目を減らすべきではないか。（IT ベンダー）

〇類似項目に関するもの

・確認項目はいずれも必要と思われるが、類似している手法例があるため、それらについては統合した方が良い。（第二地銀）
・確認項目の中には他と類似していて一つにまとめられるものがいくつもあるように思われる。API 接続先の負荷軽減の観点からも、できるだけまとめてボリュームを減らした方が良い。（ネット銀行）

〇可用性に関するもの

・API 接続先を審査する際、可用性に関する項目がないのは問題であり追加すべきである。（都市銀行）
・可用性については、各行により求める水準等が異なるため、予め手法例を用意することは必要ないかもしれない。（都市銀行）
・可用性に関しては銀行自ら考えるべき事項であり、API 接続先に求めるものではないため、追加の必要はない。（地銀【複数先】）
・万一顧客に問題が発生した場合、銀行は顧客に関係ないとは言えないため、API 接続先の可用性についても確認すべき。（地銀）
・他行が要望し、API 接続先にとって負担とならないのであれば、可用性に関する項目を追加して構わない。（ネット銀行）

・銀行が API 接続先に可用性を要求すること自体、今後の検討項目である。現段階で決定していない以上、可用性に関する項目をチェックリストに記載することは時期尚早である。（API 接続先【複数先】）

〇完全性に関するもの

・API 接続先を審査する際、完全性に関する項目がないのは問題であり追加すべきである。（都市銀行）
・今後、更新系 API が本格化することを考慮すると、API 接続先から送られてくるデータが正しいかどうかを確認する必要がある。（都市銀行）
・他行が要望し、API 接続先にとって負担とならないのであれば、完全性に関する項目を追加して構わない。（ネット銀行）
・銀行が API 接続先に完全性を要求すること自体、今後の検討項目である。現段階で決定していない以上、完全性に関する項目をチェックリストに記載することは時期尚早である。（API 接続先【複数先】）

〇運用面に関するもの

・チェックリストの使い方として、銀行が API 接続先に記入するよう提示すべきか、API 接続先が自ら記入して銀行に自主的に提出するのか分からない。（地銀）
・自由記入欄の記載は、API 接続先によって粒度が大きく異なりやり取りが煩雑となっている。API 接続先への教育や記載例の提供が必要である。（地銀【複数先】）
・API 接続先が対応できているか、できていないかを記載する欄がないと、API 接続先との接続を承認して良いかが分からず、実務上使いにくい。（地銀【複数先】）
・現在、外部委託先を３段階で評価しているため、API 接続先についても手法例毎に同様な評価を行いたい。記載は〇×△でも１、２、３でも何でもよい。（地銀）
・API 接続先のチェック結果を公開すれば各行のチェックは不足分のみ行えば良くなり、金融業界として効率的に行うことができるのではないか。（地銀）
・多くの銀行は、手法例を取捨選択せず全てについて回答するよう求めてくる。手法例はあくまで例示であり、必要に応じて取捨選択するという正しい利用方法を徹底して欲しい。（API 接続先【複数先】）
・現在、銀行が回答する確認項目の結果は API 接続先に連携されていないため、銀行の回答結果を API 接続先に提供する運用にして欲しい。（API 接続先）
・多くの銀行からは、従来から各行で使用されている外部委託に関するチェックリストにも回答するよう要求される。FISC から公表されているチェックリストとの重複項目も見受けられることから、チェックリストの一本化を強く要望する。（API 接続先【複数先】）

以上

別紙２

安対基準の改訂内容について

本年３月に公表した「安全対策基準・解説書　第９版」における、従前の「同　第８版」及び「同　第８版追補改訂」からの主な変更点は以下の通り。

| 項番 | 主な変更点 | 内容 |
|---|---|---|
| 1 | 「安全対策の考え方」の新設 | 安全対策上必要となるITガバナンス・ITマネジメントについて解説した上で、リスクベースアプローチに基づく安全対策の基本原則及び統制の拡充について、「安全対策の考え方」として新たに示した。 |
| 2 | 金融情報システムに関する分類の導入 | 金融情報システムを、「特定システム」と「通常システム」の２つに分類した。（注１） |
| 3 | 「運用基準」「技術基準」の構成変更 | 「運用基準」及び「技術基準」を、「統制基準」「実務基準」「監査基準」の３つに再編した。（注２） |
| 4 | 基準に関する分類の導入 | 金融機関等がリスク特性に応じた安全対策の目標を定めるにあたり、不確実性を低減させることを目的に「基礎基準」を設定した。（注３）<br>一方で、「基礎基準」以外の基準は、リスク特性に応じて追加・選択する「付加基準」とした。 |
| 5 | 重複した基準の統合等 | 「運用基準」のうち外部委託管理に関する基準は、クラウドサービス利用時に関する基準と重複している個所があったため、内容を整理した上で基準の統合等を行った。（注４） |

（注１）「特定システム」と「通常システム」の定義は以下の通り。

・「特定システム」とは、金融情報システムのうち、重大な外部性を有するシステム（システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性があるシステム）や機微情報（要配慮個人情報を含む）を有するシステム（機微情報の漏えい等により顧客に広範な損失を与える可能性があるシステム）のこと。

・「通常システム」とは、特定システム以外の金融情報システムのこと。

（注２）「統制基準」「実務基準」「監査基準」の概要は以下の通り。

・「統制基準」は、ITガバナンスやITマネジメントを行う上で必要な管理体制整備のための「内部の統制」及び「外部の統制」に関する基準項目から構成されている。

・「実務基準」は、金融情報システムの信頼性・安全性の向上を図るために必要となる情報セキュリティ、システム運用等に関する基準項目から構成されている。

・「監査基準」は、統制等に対する監査に関する基準項目から構成されている。

（注３）「基礎基準」の選定にあたっての考え方は以下の通り。

・「基礎基準」は、以下のいずれかに該当する基準をいう。

- 統制・監査に関する基準
- 顧客データの漏えい防止及びシステムの不正使用防止に関する基準
- コンティンジェンシープラン策定に関する基準
- システムの運行管理に最低限必要な基準

（注４）基準の統合等を行った状況は以下の通り。

| 管理フェーズ等 | 第８版・第８版追補改訂 | | 第９版 |
|---|---|---|---|
| | 外部委託管理 | クラウド利用 | |
| 利用検討時 | 【運 87】<br>【運 87-1】 | 【運 108】 | 【統 20】<br>（【運 108】を基に再構成） |
| 契約締結時 | 【運 88】 | 【運 109】 | 【統 21】<br>（【運 109】を基に再構成） |
| 運用時 | 【運 89】<br>【運 90】 | 【運 110】 | 【統 22】【統 23】<br>（【運 89】【運 90】【運 110】を基に再構成） |
| 契約終了時 | 【運 90】 | 【運 111】 | －<br>（【統 21】へ統合） |
| 監査 | 【運 91】 | 【運 112】 | 【監 1】<br>（【運 91】【運 112】を基に再構成） |
| クラウド固有 | － | | 【統 24】<br>（新設） |

以上

別紙３

前回検討時の継続検討事項について

前回検討時（2017 年２月～６月）において継続検討とされた事項は以下の通り。

| 項番 | 事項 | 内容 |
|---|---|---|
| 1 | 業界自主基準（規則）の反映 | 確認項目のうち「基礎的な安全対策の管理・運営能力」は、安全対策の必要最低限の基準又はそれを踏まえた FinTech 業界の自主基準（規則）に基づき見直すこととしていた。<br>今後、安対基準の改訂内容を踏まえて、認定電子決済等代行事業者協会が自主基準（規則）を制定する予定である。そのため、その内容を「基礎的な安全対策の管理・運営能力」に反映させる。 |
| 2 | 利用のしやすさ | 銀行、IT ベンダー、そして大小様々な規模の API 接続先にとって利用しやすいものとなるよう見直しを行う。（下記（注）参照） |
| 3 | 理解のしやすさ | 銀行、IT ベンダー、そして大小様々な規模の API 接続先にとって理解しやすいものとなるよう見直しを行う。（下記（注）参照） |
| 4 | 参照系と更新系の別 | 確認項目を参照系に関するものと更新系に関するものに分ける。 |
| 5 | レベル別 | 確認項目のなかから最低限のものを示したり、確認項目を「松・竹・梅」のようなレベル別（難易度等）で示す。 |

（注）「API 接続チェックリスト（試行版）」は、特に小規模な API 接続先に過大な負荷を強いたり、使用すること自体に賛同が得られないものになってはいけない。そのため、実態を踏まえて見直しを行う必要がある。

以上