資料４

API 接続チェックリスト解説書
「利用にあたっての留意事項等」の再確認

第１回 金融機関における API 接続チェックリストに関する連絡会で説明した『資料５（別紙２）ユーザーからの要望・意見について』において、チェックリスト関係者へのヒアリングの結果、チェックリストの運用面でも様々な意見を頂いた。

その中で、今後の留意すべき事項を以下にまとめるが、これらはほとんどが「API 接続チェックリスト解説書」の「３．利用にあたっての留意事項等」に明記されている内容（チェックリストへの項目追加・変更箇所の識別に関する部分は除く）であり、FISC としても、今後、チェックリストの利用方法等について、各種の機会を捉えて説明を行い、理解深耕に努めることとしたい。

- チェックリストを利用するにあたっては、API 接続先、金融機関ともに、チェックリストの目的や利用方法、確認項目毎の詳細内容を記述した「API 接続チェックリスト解説書」を必ず読み、内容をよく理解する。

- モニタリングの実施周期・方法、エビデンス提出、立入検査実施等については、リスクベースアプローチの考えに基づき、API 接続先、金融機関の双方で取り決めることが適当である。

- API 接続チェックリストは、リスクベースアプローチの考え方に基づき、現行のまま利用可能である一方、必要に応じて確認項目を追加・削除すること等も可能である。
  ただし、金融機関が API 接続チェックリストをもとに独自チェックリストを策定・利用する場合、API 接続先の対応負担を考慮し、「API 接続チェックリストとの差異」や「確認項目・手法例等の追加・変更箇所」などを識別できるようにするといった配慮を金融機関側が行うことが望ましい。

- チェックリスト（フォーマット）の利用にあたっては、次の点を踏まえ、API 接続先と金融機関との間で効率的なコミュニケーションが行えるようにする。
  - ・確認項目の「対象者」は、セキュリティ対策を実施する主体であり、「対象者」（API 接続先、金融機関、共通）がフォーマットへ記載する。
  - ・API 接続先と金融機関の双方において、自社のセキュリティ実態を正しく、できるだけ具体的に回答する。
  - ・「課題認識」欄には、現在の対応状況を踏まえ課題と認識していることを記述し、「課題への対応計画」欄には、課題認識に基づいた今後の対応計画を記述する。（課題認識欄の記述だけをもって、API 接続を不可と判断するものではない）

以上