資料３－１

現行のチェックリストにおける第三者認証の取扱いについて

１．昨年開催の有識者検討会で決められた継続検討事項

- 第３回オープン API に関する有識者検討会（2018 年 9 月 27 日開催）
  【資料２－１】「API 接続チェックリスト原案」の検討結果　より

> ３．今後の留意点
> 以下については、今後さらに検討を深めていくことにしました。
> ・金融機関は、API 接続先の**第三者認証**（ISMS、内部統制保証報告書）取得をどのように利活用すべきか。

２．チェックリストにおける第三者認証に関する記載内容

- 解説書（P８）
  ３．利用にあたっての留意事項等

> 各金融機関は、効率的なコミュニケーションを行う観点や API 接続先から必要以上に重要情報を取得しないという観点から、エビデンス等の提出に代え、**第三者認証**や外部監査による評価の活用を積極的に検討する。

- 解説書（P26、P27）
  ６．確認項目　【通番３】

> ＜第三者認証の利用＞
> １．提供するサービスや目的に合致した**第三者認証**を取得（注３）してセキュリティ管理態勢が整備されていることを示すことが考えられるが、**第三者認証**を取得していなければならない訳ではない。

> （注３）
> ① プライバシーマーク、ISMS（JISQ27001 等）、ITSMS（JISQ20000-1 等）の認証を取得している。
> ② 内部統制保証報告書〔SOC1（SSAE16・ISAE3402）、SOC2、IT 委員会実務指針 7 号〕や情報セキュリティ監査報告書を取得している。
> ③ クラウドセキュリティ推進協議会の CS マークや ISMS クラウドセキュリティ認証（ISO27017）を取得している。