資料２－１

# 「API 接続チェックリスト原案」の検討状況

前回（６月７日）の本検討会において承認いただきました「API 接続チェックリスト ワーキンググループ」における検討状況について、以下の通り報告いたします。

１．開催実績

| 回数 | 日時 | 主な内容 |
|---|---|---|
| 第１回 | ６月 11 日（月）<br>15：45～17：45 | ・「API 接続チェックリスト（試行版）」の活用状況等の発表（4 委員）<br>・「API 接続チェックリスト」の確定に向けた具体的な方法に関する検討 |
| 第２回 | ６月 26 日（火）<br>15：45～18：00 | ・「API 利用に関する契約書との整合性確保」に関する確認結果の発表（3 委員）<br>・「API 接続チェックリスト（試行版）」見直しに関する確認結果の発表（全委員） |
| 第３回 | ７月５日（木）<br>15：45～17：45 | ・「API 利用に関する契約書との整合性確保」及び「API 接続チェックリスト（試行版）」見直しに関する事務局案の概要説明<br>・「API 接続チェックリスト原案（事務局案）」の提示及び「API 接続チェックリスト原案」の検討 |
| 第４回 | ７月 25 日（水）<br>15：45～17：55 | ・「API 接続チェックリスト原案（事務局案修正版）」の提示及び「API 接続チェックリスト原案」の検討 |

２．全体概況

「API 接続チェックリスト原案」については、以下の方針で検討しております。

①ユーザーの要望に対応すべく、確認項目の精緻化や類似しているものを統合する。

②可用性（障害等発生時の連絡体制）及び完全性（顧客情報の改竄防止）に関する手法例を追加する。

③使いやすさを高めるとともに手法例の位置づけ等に関する誤解を避けるため、2 種類の様式（「安対基準の記載方式に倣ったもの」と「回答欄を設けた一覧表形式のもの」）に変更し、かつ、位置づけや利用方法、留意事項等に関する解説を作成する。

④「API 利用契約の条文例」（全銀協公表）との整合性はとれているため原則修正は行わないが、連鎖接続先へのチェックに関する確認項目を追加する。

⑤確認項目は基本的に全て必須項目とし、任意項目は設けない。

⑥参照系・更新系の別及びレベル別に関しては、サービス内容やリスク特性等によってチェックポイントは様々であるため、現時点においては区別して策定しない。

３．主な検討事項

以下については対応方法の詳細について、検討を継続しております。

①第三者認証（ISMS、内部統制保証報告書等）取得をどのように利活用できるか。

②銀行法に基づく法令遵守体制の整備に関する確認項目を追加すべきか。

③API 接続時だけでなく、接続後のモニタリングの際にどのように利用することができるか。

４．今後の予定

本検討会からの指示に基づき、「API 接続チェックリスト原案」の継続検討を行います。

以上

（参考）

・確認項目数の増減について

今回の見直しの結果、確認項目数は 60 から 45 となり、15 項目数分が減少する見込み。

| 対応方針（「２．全体概況」の方針毎） | 増加数 | 減少数 | 増減 |
|---|---|---|---|
| ①確認項目の精緻化や類似しているものを統合 | 0 | 16 | △16 |
| ②可用性及び完全性に関する手法例の追加 | 0 | 0 | 0 |
| ③2 種類の様式への変更及び解説の作成 | 0 | 0 | 0 |
| ④「API 利用契約の条文例」との整合性確保 | 1 | 0 | 1 |
| ⑤必須項目と任意項目の別 | － | － | － |
| ⑥参照系・更新系の別及びレベル別 | － | － | － |
| 合計 | 1 | 16 | △15 |

・検討すべき観点毎の検討状況について

【別紙１】参照

・「API 接続チェックリスト」（確定版）の維持管理方法について

【別紙２】参照（FISC 事務局提出資料）

別紙１

検討すべき観点毎の検討状況について

前回（６月７日）の本検討会において決定された検討すべき観点毎の検討状況は以下の通りとなります。

| 項番 | 観点 | 検討状況 |
|---|---|---|
| 1 | ユーザーからの要望への対応 | ・確認項目は基本的に全て必須項目とし、任意項目は設けない。<br>・セキュリティ目標と手法例の整合性等、精緻化を図る。<br>・確認項目が類似しているものは統合する。<br>・可用性及び完全性に関する手法例を追加する。<br>・「API 接続チェックリスト」は使いやすさを高めるとともに手法例の位置づけ等に関する誤解を避けるため、2 種類の様式に変更し、解説を作成する。 |
| 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 | ・「API 接続チェックリスト」の解説の中に用語解説（定義）を設け、理解しにくい用語に関する解説等を行う。<br>・サービス内容やリスク特性等によってチェックポイントは様々であるため、現時点においては参照系と更新系に区別して策定しない。レベル別についても同様とする。 |
| 4 | API 利用に関する契約書との整合性確保 | ・「API 接続チェックリスト」と「API 利用契約の条文例」の整合性は基本的にとれており、また、記載を一致させる必要はないため、原則修正は行わない。ただし、連鎖接続先に関する確認項目を新たに追加する。 |
| 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】 | （本検討会第３回に FISC 事務局より上程予定） |

【詳細内容】

1．ユーザーからの要望への対応

| 項番 | 事項 | 詳細内容 |
|---|---|---|
| 1 | 必須項目と任意項目の別に関するもの | ・現状の確認項目は基本的に全て必須項目と判断し、任意項目は設けない。<br>・新たに追加する確認項目（「連鎖接続先に対するチェック」）についても必須項目とする。 |
| 2 | 類似項目に関するもの | ・確認項目が類似しているものについては統合し、記載内容の整理を行う。<br>・統合する確認項目は以下の通り。<br>- 通番 3、4、9（セキュリティ管理態勢の整備）<br>- 通番 11、12、13（外部委託管理）<br>- 通番 20、21、22（コンピュータ設備管理）<br>- 通番 23、24（オフィスへの入室制限の実施）<br>- 通番 27、28、38、39（不正アクセスの抑止）<br>- 通番 31、32（単独作業による不正の防止）<br>- 通番 35、36、37（脆弱性対策の実施）<br>- 通番 44、45、46（適切な認証機能の整備）<br>- 通番 49、52（ログの取得）<br>- 通番 58、59（利用者への説明）<br>・上記の結果、確認項目数は 16 減少する見込み。 |
| 3 | 可用性に関するもの | ・障害等発生時の連絡体制に関する手法例を追加する。<br>・追加する内容は以下の通り。<br>【追加する場所（見直し前）】<br>通番 10（不正アクセス発生への対応態勢）<br>【追加する手法例】<br>＜障害等発生時の連絡体制＞<br>１．障害等の発生に備えて緊急時の連絡体制を決めている。<br>２．緊急時の連絡体制を定期的に見直している。 |

| 項番 | 事項 | 詳細内容 |
|---|---|---|
| 4 | 完全性に関するもの | ・顧客情報の改竄防止に関する手法例を追加する。<br>・追加する内容は以下の通り。<br>【追加する場所（見直し前)】<br>通番 27（システムや情報資産への不正アクセスの抑止）<br>【追加する手法例】<br>＜顧客情報の改竄防止＞<br>１．顧客情報の取り扱いに関する管理ルールを定めている。<br>２．顧客情報に関する管理ルールの遵守状況を把握している。<br>３．管理ルールの遵守状況に応じて、必要な改善を行っている。 |
| 5 | 運用面に関するもの | ・「API 接続チェックリスト」は使いやすさを高めるとともに、手法例の位置づけ等に関する誤解を避けるため、以下の 2 種類の様式に変更する。<br>①「API 接続チェックリスト」（A4 縦 Word 版）<br>…安対基準の記載方式を参考に、確認項目毎にセキュリティ対応目標やその解説文（主要な対応を織り込んで作成)、手法例等を記述。<br>②「フォーマット」（A3 横 Excel 版）<br>…一覧表形式で、セキュリティ対応目標と回答欄があり、ユーザーが実際にやり取りする際に使用。<br>・ユーザーが「API 接続チェックリスト」及び「API 接続チェックリスト・フォーマット」の利用にあたって誤解を生じないよう、解説を作成する。解説は「API 接続チェックリスト」（A4 縦 Word 版）の冒頭部分に記載し、利用時に必ず読まれるようにする。 |

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 | 事項 | 詳細内容 |
|---|---|---|
| 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 | ・「ユーザーからの要望への対応」に関する対応を行うことにより、左記は対応済と判断している。 |
| 3 | 理解のしやすさ | ・「API 接続チェックリスト」の解説の中に用語解説（定義）を設け、理解しにくい用語に関する解説等を行う。 |
| 4 | 参照系と更新系の別 | ・サービス内容やリスク特性等によってチェックポイントは様々であるため、現時点においては区別して策定しない。 |
| 5 | レベル別 | ・サービス内容やリスク特性等によってチェックポイントは様々であるため、現時点においてはレベル別に策定しない。 |

４．API 利用に関する契約書との整合性確保

・「API 接続チェックリスト」と「API 利用契約の条文例」の整合性は基本的にとれており、また、記載を一致させる必要はないため、原則修正は行わない。ただし、以下については、確認項目の追加を行う。

＜確認項目を新たに追加するもの＞

①「連鎖接続先（第 13 条）に対するチェック」に関する項目

（理由）前回検討時に想定していなかった新たな事項であるため。

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。

以上

別紙２

# 「API 接続チェックリスト」（確定版）の維持管理方法について

FISC 事務局

「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 事務局にて検討し、検討結果を本検討会第３回に上程することとされております（有識者検討会第１回【資料４】２ページ参照）。

しかしながら、この維持管理方法の内容は、ワーキンググループにおける「API 接続チェックリスト原案」の検討に影響を与えることが予想されたため、現時点において FISC 事務局にて想定している概要をワーキンググループ第２回において提示し、検討を行っていただきました。

なお、下記内容は、今後の有識者検討会及びワーキンググループにおける検討等を踏まえて、必要な修正を行う予定です。

【概要】

・基本的な考え方

「API 接続チェックリスト」がユーザー（金融機関及び API 接続先、IT ベンダー）にとって常に有益なものであるよう、定期的に見直しの要否を検討する。

・具体的な手続き

FISC に「API 接続チェックリスト連絡会（仮称）」を設置し、以下の事項を踏まえて年１回、チェックリストの見直しの要否を検討する。

- ユーザーの使用状況や要望
- オープン API に関するインシデント発生状況
- オープン API に関する標準化動向　等

なお、インシデント発生等に伴い、ユーザーに対して速やかに注意喚起を行うことが必要な場合は、FISC 事務局がホームページ等を通じて行う。

以上