資料２－１

平成 30 年 9 月 27 日
API 接続チェックリスト ワーキンググループ

「API 接続チェックリスト原案」の検討結果

本 WG における「API 接続チェックリスト原案」の検討結果について、以下の通り報告いたします。

１．開催実績

以下の通り、全６回の会議を開催いたしました。

回数	日時	主な内容
第１回	６月 11 日（月） 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） ・「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） 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） ・「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） 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 ・「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） 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
第５回	８月 28 日（火） 15：45～18：00	・「API 接続チェックリスト原案」の内容確認
第６回	９月 11 日（火） 15：45～17：45	・「API 接続チェックリスト原案」の最終確認

（注）上記第４回と第５回の間、「API 接続チェックリスト原案」の最終案について事務局と各委員が個別に打合せを実施し、詳細検討を行いました。

２．検討結果（概要）

「API 接続チェックリスト原案」のポイントは以下の通りです。

①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（「解説書」及び「フォーマット」）に変更しました。

・「解説書」

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（セキュリティ対応目標及び説明文、手法例等）を記述したもので、チェックリストを利用するにあたって必ず読んでおくもの

・「フォーマット」

確認項目毎に現在の対応状況や課題認識等を入力できるようになっており、関係者間でコミュニケーションを行う際に利用するもの

②ユーザーの要望に対応すべく、記載内容の精緻化や類似しているものを整理統合し、60 項目あった確認項目を 43 項目に整理しました。

③「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基本的に修正を行っていませんが、連鎖接続先へのチェックに関する確認項目を追加しました。

④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しました。

⑤上記②及び③の結果、最終的に確認項目は 60 項目から 44 項目へ減少しました。

なお、確認項目に関し、必須項目と任意項目に分けるか、参照系と更新系に分けるか、レベル別にするかについても検討しました。「フォーマット」にある確認項目以外に必要なものがある場合は各金融機関にて「フォーマット」に独自の確認項目を追加し、一方で、一部の確認項目が不要な場合は各金融機関にて「フォーマット」から削除する（いわゆる「リスクベースアプローチ」の考え方を採用する）こととしたため、現時点においては区別しないとの結論となりました。

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等）取得をどのように利活用すべきか。

以上

（参考）

・検討すべき観点毎の検討結果について

【別紙１】参照

別紙１

検討すべき観点毎の検討結果について

第１回（６月７日）の有識者検討会において決定された検討すべき観点毎の検討結果は、以下の通りとなります。

１．有識者検討会における対応方針（有識者検討会第１回【資料４】２ページ）

【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。 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 【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。

２．本 WG における検討結果

（1）ユーザーからの要望への対応

項番	事項	内容
1	必須項目と任意項目の別に関するもの	・「フォーマット」にある確認項目以外に必要なものがある場合は各金融機関にて「フォーマット」に独自の確認項目を追加し、一方で、一部の確認項目が不要な場合は各金融機関にて「フォーマット」から削除する（いわゆる「リスクベースアプローチ」の考え方を採用する）こととしたため、現時点においては必須項目と任意項目に分けないことにしました。
2	類似項目に関するもの	・記載内容の精緻化や類似しているものを整理統合し、60 項目あった確認項目を 43 項目に整理しました。 ・整理統合を行った確認項目は以下の通りです。 - 通番 3、4、9（セキュリティ管理態勢の定着） →（新）通番 3 - 通番 11、12、13（外部委託管理） →（新）通番 10（外部委託）、11（クラウド） - 通番 15、16（利用者からの相談対応） →（新）通番 13 - 通番 20、21、22（コンピュータ設備管理） →（新）通番 17 - 通番 23、24（オフィスへの入室制限の実施） →（新）通番 18 - 通番 27、28、38、39 （内部からの不正アクセスの抑止） →（新）通番 21 - 通番 31、32（作業担当者による不正の防止） →（新）通番 24 - 通番 35、36、37（脆弱性対策の実施） →（新）通番 27 - 通番 44、45、46（適切な認証機能の整備） →（新）通番 32 - 通番 49、52（ログの取得） →（新）通番 35 - 通番 58、59（利用者への説明） →（新）通番 43

項番	事項	内容
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しました。 ・具体的な内容は以下の通りです。 【追加した場所】 （新）通番 9 （不正アクセスや障害等発生への態勢整備） 【追加した手法例】 ＜障害等発生時の連絡体制＞ 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。 ２．緊急時の連絡体制を定期的に見直している。
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しました。 ・具体的な内容は以下の通りです。 【追加した場所】 （新）通番 21 （情報資産への内部からの不正アクセス抑止） 【追加する手法例】 ＜顧客情報の改竄防止＞ 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。 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。 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。 ４．顧客情報の改竄防止のために必要な対策を実施している。

項番	事項	内容
5	運用面に関するもの	・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（「解説書」及び「フォーマット」）に変更しました。 ・「解説書」及び「フォーマット」の内容は以下の通りです。 -「解説書」 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（セキュリティ対応目標及び説明文、手法例等）を記述したもので、チェックリストを利用するにあたって必ず読んでおくもの -「フォーマット」 確認項目毎に現在の対応状況や課題認識等を入力できるようになっており、関係者間でコミュニケーションを行う際に利用するもの

（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になっていました。 ・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」に反映させることの要否を別途検討することにしました。

（3）前回検討時の継続検討事項への対応

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になっていました。 ・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」に反映させることの要否を別途検討することにしました。
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、対応済と判断しました。
3	理解のしやすさ	・「API 接続チェックリスト解説書」に用語解説のページを設け、理解しにくい用語に関する解説等を行うことで対応済と判断しました。
4	参照系と更新系の別	・「フォーマット」にある確認項目以外に必要なものがある場合は各金融機関にて「フォーマット」に独自の確認項目を追加し、一方で、一部の確認項目が不要な場合は各金融機関にて「フォーマット」から削除する（いわゆる「リスクベースアプローチ」の考え方を採用する）こととしたため、現時点においては参照系と更新系に分けないことにしました。
5	レベル別	・参照系と更新系の別と同様、現時点においてはレベル別にしないことにしました。

（4）API 利用に関する契約書との整合性確保

・「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基本的に修正を行っていませんが、前回検討時に想定していなかった新たな事項である「連鎖接続先へのチェック」に関する確認項目を追加しました。
・具体的な内容は以下の通りです。

【追加した場所】

（新）通番 8

【セキュリティ対応目標】

連鎖接続における安全性を確保する。

【説明】

連鎖接続先においてセキュリティ不祥事案が発生しないよう、連鎖接続先における安全性確保のための施策を実施する。

【手法例】

＜連鎖接続先の安全対策＞

1．連鎖接続先が遵守すべき安全対策の内容を踏まえた契約を締結している。
2．連鎖接続先における安全対策の実施状況を把握している。
3．連鎖接続先が決められた安全対策を実施していない場合は改善を求める等、必要な対応を実施している。

（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ます。

以上