平成30年９月25日

公益財団法人　金融情報システムセンター

第２回　金融機関におけるオープンAPIに関する有識者検討会　議事録

Ⅰ　開催日時：

平成30年８月２日（木）15:45～17:00

Ⅱ　開催場所：

FISC会議室

Ⅲ　出席者（敬称略）

座長	岩原　紳作	早稲田大学大学院法務研究科教授
座長代理	渕崎　正弘	株式会社日本総合研究所代表取締役社長
委員	落合　孝文	（代理出席）渥美坂井法律事務所・外国法共同事業 弁護士
	多治見　和彦	株式会社みずほフィナンシャルグループ デジタルイノベーション部次長
	廣田　祐介	株式会社福岡銀行 IT 管理部長
	吉本　憲文	住信 SBI ネット銀行株式会社 FinTech 事業企画部長
	伊藤　清隆	明治安田生命保険相互会社情報システム部審議役
	司波　卓	損害保険ジャパン日本興亜株式会社 IT 企画部長
	植村　元洋	野村ホールディングス株式会社 IT 統括部次長
	木村　康宏	（代理出席）一般社団法人 Fintech 協会 代表理事副会長
	瀧　俊雄	株式会社マネーフォワード取締役 Fintech 研究所長
	轟木　博信	株式会社 Liquid 経営管理部長 弁護士
	村上　隆	株式会社エヌ・ティ・ティ・データ第四金融事業本部 企画部シニア・スペシャリスト

	藤井　研一	株式会社日立製作所金融システム営業統括本部 事業企画本部金融イノベーション推進センタ担当部長
	宮川　晃一	日本電気株式会社金融システム開発本部 金融デジタルイノベーション技術開発室 シニアエキスパート
	梅谷　晃宏	アマゾンウェブサービスジャパン株式会社 セキュリティ統括本部長 CISO 担当
	廣瀬　一海	日本マイクロソフト株式会社 クラウド&ソリューション事業本部 インテリジェントクラウド統括本部 Azure Technology Solutions Professional
	荻生　泰之	デロイトトーマツコンサルティング合同会社執行役員
オブザーバー	片寄　早百合	金融庁総合政策局リスク分析総括課 IT・サイバー等システムチーム長主任統括検査官
	小川　拓人	金融庁企画市場局総務課 信用制度参事官室課長補佐
	油田　友幸	（代理出席）日本銀行金融機構局考査企画課 システム・業務継続グループ企画役
	奥家　敏和	経済産業省商務情報政策局 サイバーセキュリティ課長
	吉永　勇輝	（代理出席）総務省サイバーセキュリティ統括官付 参事官付主査
FISC(事務局)	細溝　清史	理事長
	髙橋　経一	常務理事
	宮城　充良	総務部長
	志村　秀一	企画部長
	大澤　英季	企画部次長
	小池　信夫	調査部長
	和田　昌昭	監査安全部長
	郡山　信	研修センター長

Ⅳ　議事内容

１．【議事】API接続チェックリスト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」の検討状況報告

○岩原座長　座長を務めさせていただいております岩原でございます。それでは、本日の議事を始めさせていただきます。本日は議事次第にございますように議事が１つでございまして、「API接続チェックリスト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』の検討状況報告」ということでございます。

それでは、事務局より説明をいただきたいと思います。よろしくお願いいたします。

○大澤企画部次長　それでは事務局から報告をさせていただきます。お手元に資料２－１「『API接続チェックリスト原案』の検討状況」をご用意いただけますでしょうか。こちらを使いまして、ワーキンググループの検討状況について報告をさせていただきます。

まず１番、「開催実績」についてです。

６月７日に開催した前回の検討会でワーキンググループの設置をご承認いただきまして、翌週６月11日から計４回会合を設けております。

内容をご紹介いたしますと、第１回は委員12名のうち４名の方から現状のチェックリスト（試行版）の活用状況等について自由に発表していただいて、そういった話をもとにワーキンググループとして、どのように検討していくべきかということを議論しております。

第２回に関しては、各委員が個別にさまざまな見直し等検討していただいた結果について発表をしていただきました。その中でも、全銀協様で契約書の議論も行っていただいていることもありましたので、全銀協様の契約書に関する検討会にご参加されている３名の方には、契約書に関する議論の内容も含めて検討をしていただいて、どのようにチェックリストを考えるべきか、見直していくべきかという意見を具体的に出していただきました。

そういった内容を踏まえて第３回は、事務局案を策定しまして、それをもとに具体的な中身の検討を行っております。

第３回の中で議論がいろいろありましたので、第４回では一度策定しました事務局案を修正しまして、議論を継続しております。現状の修正内容に関しましては、後ほどサンプ

ルとして幾つか見ていただこうと思いますが、従来のものに比べて相当修正をする方向で進んでおります。

続いて２番、「全体概況」をご報告いたします。

チェックリスト原案については、記載している６つの方針で検討しております。

まず１点目、現行の試行版に対してはユーザーの皆様、多くの方から多様な要望が既に出ております。そういった要望の中で、特に確認項目の精緻化や類似しているものをこの機会に一気に見直そうと考えております。

２点目、可用性及び完全性に関する手法例追加についてですが、そもそもチェックリストは機密性を意識して作成されているため、こういった可用性・完全性の面についても議論を行いまして、一旦現状としましては、手法例として「連絡体制」、「改竄防止」をつけ加えてはどうかという方向で検討しております。

３点目、チェックリストをより使いやすくするとともに、手法例の位置づけ等に関する誤解、こちらは手法例は例示ですけれども、例示ではなくやらなければいけないものという誤解が一部生まれているというご指摘もいただいておりましたので、そういったものを解消するために、チェックリストを２種類の様式、「安対基準の記載方式にならったもの」と「回答欄を設けた一覧表形式のもの」へ変更を行ってみようと考えております。かつ留意事項等を含めた解説書を作成してはどうかということで、今検討しております。

４点目、先ほど申し上げました全銀協様の契約書の議論との整合性等も確認しまして、概ね整合性はとれていると判断しておりますが、契約書の議論でありました連鎖接続先の話がチェックリストには入っていないということで、入れるべきではないかという議論をしております。

５点目、６点目はチェックリスト（試行版）を作成するときに出ていた継続検討事項ですが、５点目の必須と任意に分けるという話、６点目の参照系API、更新系APIを区分する話、あとはレベル別に区分をつけたらどうかといったところに関しては、現状ワーキンググループとしましては、それぞれの理由から５点目については任意項目を設けない、６点目に関しては区別して策定しないという方向で考えております。詳細はこの後ご説明いたします。

次のページの３番は「主な検討事項」になります。

ここに記載の３点に関しては、現状ワーキンググループとしまして、対応の詳細についてまだ決め切れていないといった点がございますので報告させていただきます。

まず１点目、第三者認証の取得です。チェックリストの中でAPI接続先が第三者認証を取得するという手法例がありますが、こういった資格を取得している場合に、チェックリストでどのように活用できるか、つまり第三者認証を取得している企業であれば、例えば確認項目の一部が省略できる、エビデンスの提出が省略できるといったところまで記載できるか、というところはまだ検討を続けなければいけないという状況です。

２点目、銀行法に基づく法令遵守体制の整備に関する確認項目の追加についてです。こちらは銀行法施行規則に定めのあります、銀行の接続基準で求められているような内容について、チェックリスト上追加すべきかということですが、これについても、まだしっかりと結論は出せていないというところです。

３点目は、API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このチェックリストを利用することができるか、ということです。当初チェックリストはAPI接続時に利用するということで想定して作成しておりましたが、実務者が集まって議論しますと、接続後の利用についての話も出ることから、接続後の利用をどのように考えてこのチェックリストを見直すべきなのかといったところです。大きくこの３点が継続検討事項となっております。

４番、「今後の予定」ですが、まだワーキンググループで検討を続けておりますので本有識者検討会からのご指示をいただいて、それを踏まえて９月上旬まで継続検討を行いたいと考えております。

なお、参考として表がございまして、あくまでも現状ですが、確認項目数が現行60ございますが、15程度減少して45になるのではないかと考えております。

以上、ワーキンググループの全体状況をご報告させていただきました。この後は今の報告した内容について、より詳細にご説明すべきところにポイントを置いて説明させていただきたいと思います。

では３ページ目の別紙１をご覧ください。こちらは前回６月７日の本有識者検討会で、チェックリストをどういった観点で見直すべきかということでご決定いただいた６項目、「ユーザーからの要望への対応」から始まって、一番下の「維持管理方法」まで、これらに関してまとめたものでございます。

まず項番１、「ユーザーからの要望への対応」については、非常に検討の内容が多くありますので、またこの後にまとめておりまして、４ページ目、５ページ目がユーザーからの要望への対応をまとめた内容となります。こちらのほうから１つずつご説明させていた

だきます。まずユーザーからの要望を前回の有識者検討会のときに５つに分けました。「必須と任意の別に関するもの」、「類似項目に関するもの」等、５番までございますので、それぞれに関して検討の状況をご説明させていただきます。

まず項番１、「必須項目と任意項目の別に関するもの」でございます。こちらに関しては、現在60あるチェックリストの中で、例えばこの番号のものは任意にしてはどうかということで幾つか事務局でたたき台を作りまして、ワーキンググループのメンバーの方に議論していただきました。ワーキンググループのメンバーからは、銀行とAPI接続先のコミュニケーションにおいて、最終的には60項目すべて必要ではないか、あえて任意項目にするものはないのではないかということになりまして、現状の60項目は必須であると一旦結論を出しております。

また、新たに今回連鎖接続先の項目を追加することを考えておりますが、これに関しても必須項目であろうと考えております。ただ、この後ご説明しますが、類似項目は整理しますので項目数は減らすということになります。

次に項番２、「類似項目に関するもの」です。こちらについては、幾つか具体的にご覧いただきたいと思います。類似項目ということで整理統合しようと考えているものをリストアップした結果を記載しております。この場では、１つ目と２つ目を具体的に見ていただこうと思います。それではお手元に資料２－５「API接続チェックリスト原案（新旧対比表）」をご用意いただけますでしょうか。こちらでどのような整理統合をしようとしているかをご説明させていただきたいと思います。

それでは２ページ目をお開きいただき、通番３をご覧ください。セキュリティ対応目標が「セキュリティ管理態勢の定着を図る」ということで、セキュリティ管理態勢の整備に関係したところでございます。こちらに関しては、通番４が通番３とかなり類似しているということで、まず通番４を通番３に取り込むことを考えております。その結果、通番４の右側のブルーの箇所（見直し後の内容）は記載が何もないということになっております。ただ、それだけではなく実際には細かく見ますと、通番３と通番４の手法例で重複している箇所がございますので、そういうところを整理しようとしています。通番３ですと一番初めに、＜周知・意識啓発の徹底＞ということで手法例が３つ書いてございます。また、通番４も＜教育・研修の実施＞ということでこちらも手法例が３つ書いております。これらに関しては通番３の右側のブルーの箇所（見直し後の内容）を見ていただきますと、＜周知・意識啓発の徹底＞のところはもともと３つ手法例が書いてありましたが、１つにま

とめ上げています。もともと通番４にありました＜教育・研修の実施＞のところも３つ手法例が書いてありましたが１つになっているという形で、通番３と通番４を合わせるだけでなくて内容の重複感を取り除いて、できるだけ必要なものだけ、シンプルなものにしようという修正を行っております。

また、通番９をご覧いただけますでしょうか。資料２－５「API接続チェックリスト原案（新旧対比表）」の４ページ目でございます。こちらは、従来第三者認証の取得ということで１つ独立した確認項目でございます。いくつもの認証の資格が列挙されており、これを見ますとAPI接続先がこういった資格をあたかも取得しなければいけない、いくつも取らなければならないと見られがちになっているという問題点があると認識しております。よって、ここは大幅に改善させようと考え、まず通番９番の右側のブルーの箇所（見直し後の内容）はなくなります。つまりこの通番９を先ほどの通番３に取り込みます。

また、通番３に戻っていただけますでしょうか。通番３の右側のブルーの箇所（見直し後の内容）の真ん中あたりに、＜第三者認証の利用＞という手法例がございます。繰り返しですが、先ほどは資格が手法例に列挙されているイメージでしたが、誤解を招かないように第三者認証の「取得」ではなくて「利用」というタイトルに変え、なおかつ手法例の文章も、「第三者認証を取得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」という内容に変えました。

そして、（注３）具体例ということで、見直し前には手法例に書いていた資格のプライバシーマーク、SOC１等を具体例として書くようにしてはどうかと考えております。

また併せてご説明いたしますと、右側のブルーの箇所（見直し後の内容）で一番左側、「セキュリティ対応目標」もこの機会に見直しを図っております。例えば、通番３ですと、従来は「セキュリティ管理態勢の定着を図る」という表記でしたけれども、右側のブルーの箇所（見直し後の内容）を見ていただきますと、「役職員に情報管理方法を周知し、セキュリティ管理態勢の定着を図る」ということで表現を補ったり、あとはその下にある解説文という従来なかったものを作りまして、このセキュリティ対応目標について少し解説するような、そして読んで理解していただきやすいような文章を作ってはどうかと考えております。

また、この表の一番右側ですが、タイトルが「用語解説候補」と書いてあります。通番３のところですと、「用語解説候補」に資格が幾つも書いております。これは後ほどご説明しますが、こういった用語の解説をしてはどうかと考えているものでございます。こう

いったさまざまな修正を行おうと考えています。

もう１つサンプルということでご説明させていただきます。資料２－５「API接続チェックリスト原案（新旧対比表）」の５ページ目、通番11の外部委託に関係したところです。もともとは通番11から通番13まで、外部委託に関係した確認項目でしたが、やはり似たようなところがあるということと、クラウドサービスの利用がある場合についても表記を工夫して書いていたつもりではあるんですが、まだきちんと整理できていないという反省等もございますので、この機会に通番11のほうは外部委託一般に関するもの、通番12はクラウドサービスを利用する場合ということで、それぞれ分けて書くことを考えております。もともとの通番13は、通番11と通番12のどちらかに取り込めばいいということで、通番13番の右側のブルーの箇所（見直し後の内容）は記載なしということで考えています。

通番11の具体的な手法例ですけれども、委託先の選定に関するもの、委託契約の締結に関するもの、あと従来ございませんでしたが、委託状況の確認に関するものと、３つに分けて整理しております。特に委託状況の確認は従来ありませんでしたが、こちらは安全対策基準の統制基準23の内容、（注１）具体例に関しても安全対策基準に書いてある内容を参考に、こういう内容がチェックリストに載っていたほうがいいのではないかということで作ったものになっております。

一方、通番12は先ほどご説明したとおり、クラウドサービスを利用する場合を意識してまとめております。こちらに関しては、安全対策基準第９版にある統制対象クラウド拠点、こういった表現等も取り込むような形で、また契約の締結に関しても安全対策基準の内容を反映させてはどうかということで、追記するような形になっております。

以上、類似項目を整理統合するという話以外も含めましたが、こういった形で現状のチェックリストを修正する方向で検討を進めております。

それでは資料２－１「『API接続チェックリスト原案』の検討状況」に戻っていただけますでしょうか。ユーザーからの要望への対応で５つありました項目のうちの項番２「類似項目に関するもの」に関して状況をご説明させていただきました。

次に項番３「可用性に関するもの」でございます。こちらに関しては、先ほど申し上げましたが、障害が発生したときの連絡体制に関する手法例が現状のチェックリストにございませんでしたので、この機会に追加してはどうかということで、手法例としては緊急時の連絡体制を決めて、定期的に見直しているというような内容を考えております。

項番４「完全性に関するもの」につきましては、顧客情報の改竄防止に関する手法例を追加してはどうかと考えておりまして、追加する手法例としては３つございます。1つ目、顧客情報の取り扱いに関する管理ルールを定め、２つ目、遵守状況を把握して、３つ目、必要な改善を行っている。こういった手法例を追加してはどうかというふうに考えております。２つとも既存に似たような項目がございますので、それらに追加する形で考えております。

最後の項番５「運用面に関するもの」についてです。こちらに関しては、チェックリストの様式を変えたらどうかということで、本日サンプルをお持ちしておりますので、サンプルをもとにご説明させていただきます。サンプルは資料２－２「『API接続チェックリスト原案』（Ａ４縦Word版）サンプル)」ともう１つありまして、資料２－３「『API接続チェックリスト原案（フォーマット)』（Ａ３横Excel版）サンプル)」の２種類になります。

まず資料２－２「『API接続チェックリスト原案』（Ａ４縦Word版）サンプル)」です。こちらを見ていただくと、すぐお気づきになる方が多いと思いますが、安全対策基準の現状のフォーマットを参考にしています。従来のチェックリストで手法例に目が行きがちなところを、新たな形式ではページの上部に「通番１」「セキュリティ管理責任の所在と対象範囲を明確にする」、その下はセキュリティ対応目標に関する簡単な解説文を記載しており、これらを中心に見るという形にフォーマットを変えたらどうかと考えております。従来からの手法例や具体例は先ほどの整理統合を踏まえた結果、残るものはページ中段からこのような形で表記すればいいのではないかと考えております。これが１つ目でございます。

そしてもう１つ、先ほどの資料２－２「『API接続チェックリスト原案』（Ａ４縦Word版）サンプル)」のほうが解説書といいますか、読み物というふうに位置づけられるのに対して、資料２－３「『API接続チェックリスト原案（フォーマット)』（Ａ３横Excel版）サンプル)」は、実際に銀行とAPI接続先の皆様がやり取りするものを想定して、このようにしたらどうかと考えています。資料２－３「『API接続チェックリスト原案（フォーマット)』（Ａ３横Excel版）サンプル)」は基本的に左側にセキュリティの対応目標のみを記載し、従来ありました手法例等はすべてカットして、ページ中央に３つの入力エリアを設けて「現在の対応状況」、「課題認識」、「課題への対応計画」といったものをそれぞれの立場で記入し、そして先方とのコミュニケーションを図っていただくために使うことを

想定しております。

１つ追加でご説明しますと、資料２－４「『API接続チェックリスト』の解説について」があったかと思います。こちらに関しては、チェックリストを正しく利用していただくために、チェックリストの位置づけ、使い方、留意事項、先ほど申し上げました用語の解説一覧等を含む内容で作成し、先ほどの資料２－２「『API接続チェックリスト原案』（Ａ４縦Word版）サンプル)」の前に配置し、一緒に合わせた形で使っていただくことを想定しております。従来の言い方ですと、安全対策基準の前説と言われるようなものを意識して、このチェックリストについても同様のものを作成してはどうかと考えております。内容だけではなく、こういった見た目、フォーマット等もこの機会に変えてよりよくしていくべきだとワーキンググループで議論しています。

それでは資料２－１「『API接続チェックリスト原案』の検討状況」のほうに戻っていただきまして、３ページ目をご覧ください。項番１「ユーザーからの要望への対応」ということで、今ご報告いたしましたさまざまな点の修正を行おうと考えております。今回ワーキンググループでは、ここに一番力を入れておりまして、有識者検討会で決定いただいた他の観点に関しても、後ほどご報告いたします。

３ページ目の項番２、「安対基準改訂への対応」でございます。これに関しては、第１回目の有識者検討会のときにも報告をさせていただきましたが、この対応に関しては、認定電子決済等代行事業者協会様の自主基準の制定と密接に絡むと考えておりますので、今回ワーキンググループとしましては、安対基準が第９版で大幅に変わったからということで、それを直接的な理由としてチェックリストの見直しは、現時点ではまだ行っておりません。協会様の話を踏まえて検討していくものと認識しております。

項番３、「前回検討時の継続検討事項への対応」でございます。こちらに関しては、お手元の資料の６ページ目にまとめておりますので、こちらをご覧ください。６ページ目の項番３、「前回検討時の継続検討事項への対応」でございます。こちらにも項番が１～５ございまして、前回の有識者検討会でお示しした５つでございます。これらに関してどういう検討をしているかといいますと、右側の詳細内容に記載しております。項番１「業界自主基準（規則）の反映」は先ほどの話と同様になります。項番２の「利用のしやすさ」に関しては、先ほど申し上げましたユーザーからの要望への対応をさまざまに行うと思っておりますので、利用のしやすさという観点はここに包含されると考えております。

項番３「理解のしやすさ」ということを意識して、先ほど申し上げました用語の解説等

を行いたいと考えております。

項番４「参照系と更新系の別」、項番５「レベル別」に関しては記載のとおり、サービス内容やリスク特性によってチェックポイントはさまざまであるのではないかということで、現時点ではそれぞれ区別して策定することをワーキンググループでは考えていないということでございます。

３ページ目に戻っていただいて、項番４「API利用に関する契約書との整合性確保」でございます。「API利用に関する契約書との整合性確保」に関しては既にご報告させていただいたとおり、全体的には整合性がとれていると考えておりまして、修正の必要はないと考えております。連鎖接続の話は、この機会にチェックリストに追加してはどうかと考えています。

ちなみに、連鎖接続に関する確認項目として追加する内容ですが、先ほど見ていただいた資料２－５「API接続チェックリスト原案（新旧比較表）」の４ページ目、通番でいうと８番と９番の間に１つ新たな項目を加えており、右側のブルーの箇所（見直し後の内容）に文字が赤くなっている手法例等がありますが、これをチェックリストに新たに追加してはどうかと考えております。セキュリティ対応目標は「連鎖接続における安全性を確保する」、対象者は「API接続先」、解説文は、「連鎖接続が行われる場合、連鎖接続先において適切な安全対策が実施される仕組みを整備する」ということで、手法例を３つ記載してはどうかと考えております。契約の締結に関係したもの、実施状況の把握に関係したもの、そして最後は、改善を求める等必要な対策を実施しているといった内容の手法例を追加してはどうかと考えております。

それでは、また資料２－１「『API接続チェックリスト原案』の検討状況」の３ページ目に戻っていただきまして、項番５「法規制への対応」でございます。銀行法等の法規制の対応ということで、これに関しては基本的には、前回でもご報告していますけれども、銀行法及び内閣府令等から要請されているチェックリストの要件はないと判断しております。

項番６「維持管理方法」に関しては、記載のとおり、次回第３回のこの有識者検討会にFISC事務局より提出させていただく予定と考えておりますが、現時点で概略だけを申し上げたいと思います。お手元の資料２－１「『API接続チェックリスト原案』の検討状況」の一番最後のページに別紙２をつけておりますので、そちらをご覧ください。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」ということでございます。

詳細は次回と思っておりますが、概要としましては基本的な考え方のところに記載してありますとおり、このチェックリストがユーザ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ということで、今考えているものとしましては、連絡会を設置して年１回見直しの要否を検討するという形を考えております。ユーザーの方々の使用状況や要望、インシデントの発生状況、それからオープンAPIに関する標準化の動向等、こういったものを踏まえてチェックリストを１年に１回、見直す必要があるのかどうか等を検討すべきと考えております。

なお、インシデント発生等に伴って、速やかに注意喚起等を行う必要がある場合は、先ほど申し上げた年１回の話とは別に、FISC事務局からホームページ等を通じて行うということを考えております。

以上、ワーキンググループにおいて検討してきた概要を報告させていただきました。追加して今後の予定ですが、ワーキンググループの次回開催は８月下旬、そして９月上旬、あと２回ほど考えております。それまでの間、つまり８月中は会議は開催せずに、各委員から出されたいろいろな見直しの意見について、個別に事務局と委員が打ち合わせを行って、まだ取り込むべきものは一体あとどのくらいあるのかということを検討し、第３回の有識者検討会に、できるだけ精度の高いものを上程させていただきたいと思っております。以上となります。

○岩原座長　大澤企画部次長、ありがとうございました。ただいま説明がございましたワーキンググループでの検討状況について、ご質問、ご意見ございませんでしょうか。多治見委員。

○多治見委員　みずほフィナンシャルグループの多治見でございます。２点確認させていただきたいことがございます。１点目は、今回作成していただいたＡ３のフォーマットでございますが、こちらは、例えば最初のページで「対象者」の欄にAPI接続先とあると、みずほからしますとFinTech企業様に「現在の対応状況」、「課題認識」、「課題への対応計画」の３行を埋めていただく形になると思います。みずほでも記入いただいた内容に対してのコメントとか質問をこちらに記載させていただいて、フィードバックをさせていただくということも、実務運用上やってきております。

このフォーマットは、何回もやり取りしていけば最終的には、３行で事足りるような形

にはなるかと思いますが、実務上運営していく中で金融機関側として、もしくは埋めるのが金融機関側であれば逆の立場になるのかもしれませんが、ディスカッションをする、意見交換をやっていくフォーマットになっているといいのではないかというのが、みずほの中でも挙がってきた意見でございます。

２点目でございますが、参照系と更新系の区別をしないということでございますけれども、みずほの中でも実際どういう運営をしているかというと、どちらかというと参照系よりも更新系のほうがよりセキュリティに気を配るということがあります。我々にとっても、設計についてより力を入れてきちんとやらないといけない、これは金融システムが崩れてしまう可能性がより高いからということでもございます。そういった点で参照系と更新系の区別をしないという形になりますと、チェックリストを通った後のFinTech企業様を平等に扱うという精神からしますと、どうしてもチェック時に保守的に見ざるを得ないことになります。ですので、比較的保守的に見るということですが、参照系しか使わないというようなAPI接続先の方からすると非常に厳しめに見られるということが実態としてでてくる可能性があります。

そういったものが新しい金融サービスの創出を妨げることになると残念なことでもあるので、その点について実際実務のお立場の方からのいろいろな意見もあるかと思いますので、後半のワーキンググループのところで、ぜひともディスカッションしていただくテーマとして挙げさせていただければと思っております。

○岩原座長　ほかによろしいでしょうか。特によろしいですか。木村委員代理。

○木村委員代理　Fintech協会の木村でございます。先ほどご指摘があった事項に近いことですが、参照・更新の別なのか、どういうレベル別なのかというところはありますが、任意と必須に分けづらいということなのかなと思います。せっかく解説文を作成されるということだったので、そういうところに参考情報として、ヒートマップみたいな形なのかわからないですが、こういうケースではこの箇所は特によく見たほうがいい、ここの箇所はそこまでよく見なくてもいいというような軽重がわかるようなものを入れていただけると、多分実務上は助かるのではないかと思いました。要らないというのは結構難しいと思うんですけれども、とはいえ軽重があるということは、解説書になら書けるのではないかと思います。

当協会のようなところですと、やはり小規模のスタートアップの企業が、どうやってチェックリスト等を使ってセキュアにやっていくかというのは非常に重要なポイントですので、そういう意味で、解説の書き方というところで、かなり救える部分があるのではないかと思います。作成は大変だと思いますけれども、軽重をうまく織り込んだような表現をご検討いただけるとありがたいと思います。

別の話として気になっているところは、私もまだ中身を全部読めてないので不要な懸念かもしれませんが、新旧比較の具体的な中身を拝見していますと、今回の大きな特徴として、対応目標の下に解説文を入れられたというところが、非常に大きな改善点と思います。ここの書きぶりは、結構気をつける必要があると思っています。この解説文のところにあまり具体的なことが書いてあると、手法例の一部を必須化しているように読んでしまう可能性が非常に強いと思っております。

せっかく目標と手法例・具体例という形で分けているので、解説文によって、一部の手法例を必須にしているように誤解されないような書き方にしていただきたいと思っております。具体的に今指摘できなくて申し訳ありませんが、一度そういった目線で解説文をワーキンググループでも検討していただけると、よりよいものになると思っております。以上でございます。

○岩原座長　瀧委員、どうぞ。

○瀧委員　マネーフォワード瀧でございます。３点ございます。１つ目は、先ほどご説明の中であった認定の協会というところで、電子決済等代行事業者協会の認定を取るタイミングはまだ先のことではあるので、認定という表現をどうすればよいかといったところを後々ご相談できればと思っています。とはいえ、秋口以降で自主規制の中身も詰めてまいります。そのときの内容の目線は、こちらのチェックリストの中で必須に近いところをベンチマークにして考えていくという側面もあると考えております。よくある事例でいうと、マネーフォワードとfreeeというのは、両方とも、数百人の社員がいる大きな会社ですが、そうではない会社にとっても有益な基準を作るということを考えたときに、やはりボトムラインというかミニマムラインの必須とは何かというところが、基準を作るテーマになりますので、コミュニケーションツールよりもう少し下限を見たものになると思っております。あとはよくある話ですが、リスクベースでアプローチできているかというこ

とがあろうかと思っています。先ほど更新と参照の区別の話がございましたけれども、同じ参照系をやるのでも、300人の会社と５人の会社では、恐らくユーザーの広さとかそういったところで差分があると思っています。やり方をまだ試行錯誤しているところですけれども、このようなひな型というよりは事例案とかそういったものを、協会としてお示しできていくとよいと思っております。特に問題というわけではないですが、例えば、資料２－５「API接続チェックリスト原案（新旧比較表）」の通番１ですと、「最高責任者を明確化し」というところがありますが、人が１人しかいないようなケースとかも考えないといけないと思っています。例えば５人で創業したイノベーティブなサービスが批准できるものであるのかという想像力が問われていると思っています。小規模の企業でも対応ができるものになっているかというところは若干気をつけていきたいと思っていまして、制度設計をやっていければと思っているというのが、１点目とほぼ２点目の軽微基準のところになろうかと思っています。

３点目は、特に不要かなという意見表明になりますが、法令遵守のポイントです。資料２－１「『API接続チェックリスト原案』の検討状況」の２ページ目の３．主な検討事項の②法令遵守体制のところは、チェックリストにおいてチェックを実施したり、それをベースにしたコミュニケーションを行うというスコープからはずれているものと考えています。これは本来であれば当局との対話であったり、あるいは契約書の中での対話といったところで吸収するべき議論と思っております。コンプライアンスの項目は、恐らく何も知らない人が３年後に見たときには、コンプライアンス対応の項目はこのチェックリストにある項目だけで十分ですかという話が出ることが容易に想像されますので、追加するべきでないという意見になります。以上３点申し上げます。

○岩原座長　ほかにいかがでしょうか。宮川委員。

○宮川委員　NECの宮川でございます。今までご質問された方の解決のヒントになればと思いまして、１点意見を申し上げたいと思います。資料２－２「『API接続チェックリスト原案』（Ａ４縦Word版）サンプル)」の解説文の部分です。やはりリスクベースアプローチというのが非常に重要な考え方なので、ここの解説の中に、なぜこれをやらないといけないかというリスクを少し記載すると、具体的な手法例を考えやすくすると思います。このままだと手法例にどうしても目がいってしまって、それをやらなければいけない

ということになります。そうではなく、これをなぜやるのかというリスクの部分を記載していただくことによって、手法例をビジネスのシーンに合わせた形で考えていただけることになるのではないかということで、意見を述べさせていただきます。以上です。

○岩原座長　ほかに何かございますか。落合委員代理。

○落合委員代理　落合でございます。資料２－５「API接続チェックリスト原案（新旧比較表）」の統合のところを拝見しまして気づいたところがございます。例えば、通番３と通番４と通番９のところを合併されるというお話の中で、プライバシーマークとかTRUSTeを取得するという手法例が通番３のところに合併されていますが、これは必ず取らないといけないという趣旨ではないということを明確化されるということだったと思います。今の文章では明確に書かれていないという感じがあります。

例えば、こういった箇所は取っていれば評価するけれども、必ず求めるものではない、といったことを書いていただいたほうが、より見直しの趣旨がわかりやすいのではないかと思いました。

また、例えば通番11では、通番12と合併されるというお話もあったと思います。クラウドの場合のほうだけを見ればいいような場合については、通番11番は必ずしも見なくてもいいですということも、今回の整理の趣旨ということで書いていただいたほうが、より読み手にとっても明確になるのではないかと思いましたので、そういったところをご検討いただければと思います。

○岩原座長　ほかに何かございますか。梅谷委員。

○梅谷委員　アマゾン梅谷です。何点かありますが、今、落合委員代理からご指摘がありましたので、私も同じ箇所に気づきましたのでそこからお話しします。

資料２－５「API接続チェックリスト原案（新旧比較表）」の１５ページ目、通番11と通番12の見方です。外部委託の整理ということで、安対基準の統制の20、21、22、23はクラウドでも共同センターでも委託するときには共通して見ましょう、統制の24はその上でクラウドに特徴的なものがあれば確認するという追加の項目になっています。今の書き方ですと、関連規定箇所をぱっと書かれたのかなと理解していますが、ここは通番12は

統制の24だけにしたほうが、さきほど落合委員代理が指摘されたことがはっきりすると思っています。通番12に関してはクラウド特有として書き、データセンターでもいいですし、ホスティングでもいいですし、何かしら外部委託に共通の要件を参照する際には、通番11を見るという書き方のほうが明確になると思います。

それから資料２－５「API接続チェックリスト原案（新旧比較表）」に関しては、いろいろ事務局の方で苦労されたのではないかと思います。以前より大分整理されてきたという印象です。

その上で、資料２－１「『API接続チェックリスト原案』の検討状況」の３．主な検討事項の③にも関連しますし、第三者認証をどう活用するかという点にも関連することになります。接続のモニタリングの際にどのようにするのかと言っていながらも、実は安対基準の監査１が関連規定箇所としてマップされています。例えば通番３の「情報セキュリティ管理態勢の定着を図る」においては、統13と監１が関連していますということでマップされています。監査の項目が入ってくるということは、今後継続してどのようにチェックするかという内容です。そうするとここは継続チェックに使えるという認識で、皆さん自然に検討されていると考えられます。そういう視点で見ていくと何点か、継続チェックで使えるところが実はあるのではないかと思っています。例えば関連規定箇所に監１が含まれるのはどこかという形で監査という観点から整理してもいいですが、もう少し何かしら整理をしたほうが皆さん使いやすくなると思っています。

それから第三者認証、クラウドが出てきてから、特にそこの話を我々ベンダー側もすることが多いですが、この性質の１つとしては、当事者同士で何がセキュアであるのか認識を合わすことがなかなか難しいという背景があり、第三者認証の話につながることが多いです。さまざまなクラウドに関連する認識やサービスや利用形態が異なるケースにおいて、第三者があなたの組織のセキュリティ体制はこうなっていて、運用がこうなっていますと、それなりの客観的な質の高さを持って示していることになりますので、よくありがちな、銀行様とFinTech企業様の間ですとか、銀行様と我々クラウドベンダーの間ですとか、あるいはクラウドベンダーとFinTech企業様の間でディスカッションが起きる中で、１つの客観的な着地点として使えるわけです。

ですからその意味で、例えばISO27001を取っている場合、あるいは27017を取っている場合は、このチェック項目はある程度よしとしましょうというマークをもうちょっと進んでやったほうが、お互いの認識の違いに基づいたあまり有益ではないディスカッション

を減らせるのではないかと思っています。

もう１点、継続的な監査と第三者認証に関係しますが、いわゆる認証認定の話と監査の話は別です。例えばSOC１、SOC２、あとCSマーク等は監査報告書という形です。認証というのは、ざっくばらんな言い方になりますが、ある一時点で態勢が整っているかといったものを見ていますが、監査というのは運用を含めて時系列で見ています。例えばAWSが出しているSOC１ですと、365日が監査対象になっています。それがちゃんと継続して運用されていましたというのを示すレポートになっていますから、ある一時点で統制がされていて、それが継続して実施できているのかという時間的な深さを持って使えるようになっています。もしこれをフルに活用していくのであれば、例えばSOC１とか日本ですと86号監査を実施している場合には、ある程度、確認するべき箇所をよしとするような記述があるといいと思います。

それから３．主な検討事項の２つ目です。先ほどマネーフォワードの瀧委員からもご意見がありましたが、安全対策基準に法令遵守とか入っていたかなという観点で私は疑問に思っています。入っていなかったのではないかと思っています。あくまでもこれはセキュリティの基準ですから、そこに法令遵守というようなピュアなコンプライアンスの内容が入ってきますと、今後運用していく上でも若干混乱が出るという印象がありまして、あまり入れるのはよろしくないという印象があります。

ただ、ワーキンググループの検討状況を私も存じ上げておりませんが、具体的なリスクが見えているがゆえにこれを入れないといけないということで、皆さんが理解できるのであれば、それはそれでいいと思っています。何となく心配なので入れておくということであれば、入れるための要求事項としては過大な内容という印象です。以上になります。

○岩原座長　ほかに何かございますか。特にございませんか。廣瀬委員。

○廣瀬委員　日本マイクロソフトの廣瀬です。先ほどの更新系・参照系のところですが、私は実務のほうも担当していますので、通番54のところは参考情報として具体例を挙げると役に立つのではないかなと思います。資料２－５「API接続チェックリスト原案（新旧対比表）」の23ページ、通番54です。APIのアクセス範囲で更新系と参照系を分けて、それぞれの接続先に対して参照系のみ更新系のみを提供するというアクセス管理手法も検討するべきだというのは、１つ参考例として記載するべきと考えます。

次に14ページの通番33です。システムの品質確保についてですが、記載項目が主に情報システム、アプリケーションやAPIを載せるサーバー群についてのものがほとんどですので、APIそのものに対するモニタリングであったりロギングといったこと、つまりAPIそのもの、システムは動作しているもののアプリケーションやAPIの可用性低下について、そして問題が発生した場合にいかに早く復元、修正を行うかということについての記載があったほうがいいと思います。品質確保というところで２点気になるところがございましたので、ご報告いたします。

○岩原座長　よろしいですか。ほかに何かご意見はございますでしょうか。木村委員代理。

○木村委員代理　先ほどチェックリストをモニタリングにどう使っていくかという話が出ていましたが、今、当社を含め幾つかのベンダーさんでも似たような感じかなと思いますが、実務上はもう実際モニタリングにも使っているということだけ、申し添えておきたいと思いました。今ですと最初に埋めたチェックリストを、定期的にやり取りをして変更がありませんか、特に重要な箇所はどうですかといったことを、実際銀行様とやり取りをして、事実上のモニタリングに使っているということは先行的に始まっております。その流れでそういったやり方を実際に推奨することになっていけば、皆安心して使えると思いました。

また、先ほどありましたコンプライアンスの話は、当方も混ぜて入れ込まないほうがよいとは思っております。これを入れていくと、また銀行様が公開されている接続基準との関係も結構難しくなってくると思っています。接続基準があまり標準化されていないというか、皆さん結構個性がある一方、大体５項目ぐらいあると４項目ぐらい内容としてはほぼ重複していて、その中にコンプライアンスと書いてあるとか、結構接続基準自体への対応も大変ですけれども、接続基準とこちらとの整理が難しくなってきてしまうと思いますので、チェックリストにはコンプライアンスの内容は入れないほうがいいということを当方も思っております。

○岩原座長　ほかに何かございますでしょうか。特にございませんでしょうか。

それでは、チェックリストを確定させる上で追加して検討すべき事項などございません

でしょうか。特にありませんか。梅谷委員。

○梅谷委員　アマゾン梅谷です。最後に１点だけ、どうしようかと私も迷いながら発言させていただきますが、例えば大手の金融機関様でAPIを作成される際に、スクラッチからオンプレとかサーバーを使って作られてやる場合と、FinTech企業様の提供するサービスやAPI、あるいはFinTech企業様間での連携のためのAPIを作成するという場合には、API環境作成のためのテクニカルな方法としての違いやコストに差がある印象です。

大手のクラウドベンダー、例えば、AWSとかマイクロソフト様もそうですし、グーグル様もそうですけれども、クラウドサービスはAPI構築を支援するためのサービスを提供しています。FinTech企業様の場合はそうしたサービスを活用してAPIを作成するケースが多くあります。その場合には、先に述べたように、オンプレ環境でサーバー構築等から実施する際に必要となると思われる内容にいまのチェックリストは近いのではないかという観点で、もしかしたら内容が重いかなという感じがしています。

例えば、アマゾンのAPI構築を支援するサービスを使ってAPIを作りたいときは今回作成しているチェックリストをどのように活用しようかと思ったのですが、AWSのAPIのサービスですとチェックリストの通番１、通番２等の内容はクラウドベンダーによってあらかじめ確認されている内容となるため、そのようなクラウドサービス側の情報をあらかじめ提供することでチェック時に使ってもらえれば、金融機関様とFinTech企業様がお互いに効率よく必要な情報を確認できるといったことも考えられます。解説書のほうでもいいのかなと思っていますが、例えばクラウドベンダーが提供するAPIを作りやすくするサービスを使う場合には、クラウドベンダーからこういう情報を取り寄せると比較的容易に確認できるといった形で、１つの方向性を示したいと思っています。具体的な文案は今持ち合わせておりませんので、解説書を検討される際に、何らか参考として提供させていただければと思っております。

○岩原座長　ほかに何かありますか。よろしいですか。いろいろご意見をいただきましてありがとうございます。いただいたご意見について事務局から何かありますでしょうか。

○志村企画部長　志村でございます。参照系・更新系という話を複数名の方から伺い

ました。それを反映していくやり方として、必ずしも通番１は参照系、通番２は更新系といった機械的なやり方ではなくて、お話にありましたが解説書で書くとか、そういうやり方もあり得るというふうに、ご意見として伺いましたが、よろしいでしょうか。

○岩原座長　よろしいですか。それではただいま事務局からいただきました対応等について特にご意見はないでしょうか。よろしいですか。

ないようでございましたら、これをもちまして、本日の議事を終了させていただきたいと思います。

次に今後の事務連絡等について、事務局の志村企画部長よりお願いいたします。

２.事務連絡

○志村企画部長　連絡事項は全部で３点ございます。まず１点目ですけれども、本日の内容に対するご意見等ございましたら、最初の議事次第の５．に書いてございますメールアドレス宛て１週間をめどで恐縮ですけれども８月９日木曜日までに電子メールでお送りいただければと思っております。

続いて２点目ですが、こちらも議事次第の６．にございますとおり、第３回検討会の開催日時のご案内でございます。次回は９月 27 日木曜日、時間は本日と同じで 15 時 45 分からを予定しております。この有識者検討会ですけれども、一応次回第３回をもって終了ということで考えてございます。

最後に３点目でございます。本検討会の議事録及び配付資料ですけれども、前回の１回目の検討会と同様、当センターのホームページにて一般に公開させていただこうと思っております。議事録は事務局で作成次第、ご発言のございました委員の方々に事前にご確認いただきますので、よろしくお願いします。配付資料は議事録に先立って１週間後程度をめどに公開していく予定でございます。以上でございます。

３．閉会

○岩原座長　それでは以上をもちまして終了させていただきたいと思いますが、何か特にご質問ございませんでしょうか。よろしいでしょうか。

それではこれにて「第２回金融機関におけるオープン API に関する有識者検討会」を終了いたします。お忙しいところをご参集いただきましてまことにありがとうございました。

以上