令和元年９月27日

公益財団法人　金融情報システムセンター

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
議事要旨

Ⅰ　開催日時

第１回　令和元年７月26日（金）15:00～17:00

第２回　令和元年８月23日（金）15:00～16:50

Ⅱ　開催場所

公益財団法人金融情報システムセンター（以下「FISC」という）会議室

Ⅲ　委員およびオブザーバー（敬称略）

座長	稲垣　光隆	FISC 理事長
委員	酒永　洋介	株式会社三井住友銀行 システム統括部 決済システムグループ長
	衛藤　高秋	株式会社常陽銀行 システム部 主任調査役
	木野　隆之	株式会社名古屋銀行 事務システム部 システム管理グループ 副業務役
	山崎　篤志	一般社団法人全国信用金庫協会 業務推進部 次長
	中川　晃一	住信 SBI ネット銀行株式会社 受信・決済事業部 副部長
	土佐　鉄平	freee 株式会社 CISO 兼 CIO
	小林　中	マネーツリー株式会社 インテグレーションチーム マネージャー
	市川　貴志	株式会社マネーフォワード 取締役執行役員 CISO
	岡部　毅	弥生株式会社 マーケティング部 ビジネス戦略チーム 担当マネジャー
	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 アドバンストフィナンシャルサービス企画担当 シニア・スペシャリスト

	鎌田　美樹夫	日本アイ・ビー・エム株式会社 グローバル・ビジネス・サービス事業部 銀行ソリューション 担当部長
	岡本　一真	富士通株式会社 金融リスクマネジメント室 マネージャー
	塚田　朗弘	アマゾン ウェブ サービス ジャパン株式会社 技術統括本部 スタートアップソリューション部 スタートアップソリューションアーキテクト、 マネージャー
	加佐見　明夫	デロイトトーマツ ディレクター
オブザーバー	佐野　佑輔	金融庁 総合政策局リスク分析総括課 金融証券検査官
	尾川　豊	金融庁 企画市場局総務課 信用制度参事官室 企画調整官
	長瀬　礼明	金融庁 監督局銀行第一課 金融証券検査官
	河本　勝也	日本銀行 金融機構局 企画役
	菅山　靖史	日本銀行 決済機構局 FinTech センター 決済高度化グループ長・企画役
FISC（事務局）	髙橋　経一	常務理事
	小池　信夫	企画部長
	荒井　孝浩	企画部 主任研究員

Ⅳ　見直し要否に関する検討結果

■ API 接続チェックリスト（以下「チェックリスト」という）の一部の見直しを行う。今回は、有識者検討会での審議を要するような大幅な見直しではないため、本連絡会で改訂を決定する。主な見直しの内容は以下のとおり。

- 第三者認証等の利活用の例示の記載
- 確認項目における注記・関連規定の追加
- 用語の追加・削除

■ 今回策定するチェックリスト改訂版の利用開始時期の考え方は以下のとおり。

- 新たに接続を開始する場合は、今回策定の改訂版を利用する。
- チェックリスト＜2018 年 10 月版＞を利用中の場合は、今後、モニタリングなどでチェックリストを利用する際に、必要に応じて改訂版の内容を踏まえたものに切り替える（切り替えが必須ではない）。

Ⅴ　議事内容

１．API 接続チェックリストに関する連絡会の運営について

事務局より、本連絡会の設立趣旨及び運営方針について以下のとおり説明が行われた。

- o 昨年度は、チェックリストの確定版を策定するために、「オープン API に関する有識者検討会」を設立し、有識者検討会のもとに具体的検討を行う会議体として「金融機関における API 接続チェックリストに関するワーキンググループ」を設置した。有識者検討会、ワーキンググループでの審議を経て、昨年 10 月に「API 接続チェックリスト＜2018 年 10 月版＞」を公表した。
- o チェックリストに関しては、常に有益なものであるよう毎年見直しの要否を検討することとしており、今回、常設の会議体として「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」を設立する。
- o 連絡会は、「見直しの要否に関する検討及び判断」、「改訂版の策定」等を行う。
- o 見直しを行うにあたり、チェックリストを大幅に見直す等、重要な判断が必要な場合は、別途有識者検討会を開催のうえ審議を行い、その結果を踏まえ改訂版を策定することとする。

２．見直し要否に関する検討について

o 第１回連絡会で、事務局より「見直しの観点①～③」及び「見直しの観点への対応方針（案)」が提示され、デロイトトーマツの委員から、第三者認証等の利活用を検討するための基礎的な事項について説明があった。

o 第１回連絡会開催後、各委員から事務局宛てに「見直し要否に関する意見」が提出された。

o 第２回連絡会で、「見直し要否に関する意見」をもとに見直しの要否の具体的検討が行われた。

■ 見直しの観点 ①

チェックリストの関連規定（FISC「安全対策基準」、全銀協「オープンAPI検討会報告書」）等における改訂事項

- パスワードの定期的な変更を求める例示を削除（安対基準）
- スマートデバイスの可搬性に伴うリスクに関する基準の見直し（安対基準）
- QR コード決済に関する基準の新設（安対基準）　　等

＜対応方針(案)＞

o チェックリストの関連規定等における改訂内容を確認したところ、チェックリストの見直しが必要となる事項は見受けられない。

＜委員意見＞

o QRコード決済のアプリとAPI接続するケースが実際にでてきている。QRコードを使用するアプリを取り扱う場合に、FISC「安全対策基準」で新設されたQRコード決済に関する基準（実務基準142，143，144）を参照するよう記載した方が良いのではないか。

＜検討結果＞

o 委員による討議の結果、確認項目【通番33】に、FISC「安全対策基準」の実務基準142，143，144を参照する旨の記載を追加することが決定された。

o 本改訂は、重要な判断が求められる内容ではないことから、有識者検討会を開催せず、本連絡会で見直しを決定することが確認された。

■ **見直しの観点 ②**

チェックリスト解説書の「今後の維持管理方法」（P2）に記載されている、見直し検討にあたり踏まえるべき事項

- 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の発生状況
- オープンAPIに関する標準化の動向
- 認定電子決済等代行事業者協会の自主基準　等

＜対応方針（案）＞

- o「ユーザーの使用状況や要望」については、その内容を把握するため本連絡会開催までに FISC がチェックリスト関係者（金融機関、FinTech 企業、IT ベンダー等）に対しヒアリングを実施。チェックリストの運用に関してさまざまな意見があったものの、見直しに関する強い要望はなく、当該事項を踏まえた見直しは行わないこととする。また、ヒアリング時に頂いた主な意見（※）を本連絡会で還元する。
- o「オープン API に関するインシデントの発生状況」については、FISC が確認した限りでは大きなインシデントの発生が見受けられず、当該事項を踏まえた見直しは行わないこととする。ただし、今後もインシデントの発生状況を注視していく。
- o「オープンAPIに関する標準化の動向」については、現在検討されている標準仕様はあるものの、確定したものがなく、当該事項を踏まえた見直しは行わないこととする。ただし、今後も標準仕様等の検討について進捗状況を注視していく。
- o「認定電子決済等代行事業者協会の自主基準」については、現在、電代業協会で検討中であるため、当該事項を踏まえた見直しは行わないこととする。ただし、今後も検討の進捗状況を注視していく。

（※）様々な意見があったチェックリストの運用面で、今後留意すべき事項をFISCでまとめ、本連絡会で還元した（詳細は「Ⅴ．議事内容 3．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」を参照）。

また、「更新系の対応に関する意見」については次のとおり整理した。

【更新系の対応に関する主な意見】

・今後の更新系APIへの対応を見据えて、更新系APIに関する内容を追加することを検討してもよいのではないか。

・更新系の項目や手法例の追加は、更新系APIの実装基準や更新系APIのサービス体制が明確になった後に検討するべきではないか。

・更新系といっても、サービスによってリスクがさまざまで、適用するサービスと併せて検討しないと具体的なリスクがわからないのではないか。

【事務局の考え方】

・更新系APIに関するサービスが広く普及している状況にはない。

・更新系への対応に関して、具体的なサービスや機能固有のリスクを踏まえた議論を行うには、ユースケースが十分ではないと認識している。

・更新系APIに関するサービスの進展を引き続きフォローしていく。

＜検討結果＞

o 委員による討議の結果、対応方針（案）のとおり、見直しの観点②に基づく見直しは行わないことが決定された。

■ **見直しの観点 ③**

昨年開催の有識者検討会・ワーキンググループで継続検討とされた事項

- 金融機関はAPI接続先の第三者認証取得をどのように利活用すべきか

＜対応方針（案）＞

o 昨年の有識者検討会、ワーキンググループでは「第三者認証の利活用」について実態に即した議論ができなかったため、本連絡会では「第三者認証の利活用」について専門的見地からの意見を踏まえ、具体的な利活用方法を検討する。

＜第三者認証・保証報告書等に関する説明（デロイトトーマツ）＞

o セキュリティに関する第三者認証・報告書は、ISMS 認証、P マーク、TRUSTe、SOC2 保証報告書等、様々なものがあるが、その普及状況やチェックリストの確認項目との一致割合から検討対象となりうる第三者認証・報告書として「ISMS 認証」,「SOC2 保証報告書」,「合意された手続報告」の３つを選定した。

o 「ISMS 認証」、「SOC2 保証報告書」を取得済みの事業者も存在するが、チェックリストの確認に活用する場合は、認証もしくは保証範囲に API 関連サービスが含まれているかを確認する必要がある。通常は対顧客向けのサービスに対して、認証もしくは保証を得ることを目的としているため、API 接続先と金融機関の接続に関する API 関連サービスは範囲に含まれていない可能性がある。

o 「ISMS 認証」は、組織の構築した ISMS が ISO/IEC27001 に基づいて適切に運用管理されているか、第三者である「ISMS 認証」機関が審査し、証明することで取得ができる。

なお、チェックリストに活用する際の留意点は次のとおり。

- チェックリストの確認項目のうち一部の確認項目は、「ISMS 認証」の範囲に含まれておらず確認できない。
- 公開されている認証文書ではどの管理策が実装されているか把握できないため、適用宣言書等により個別に確認する必要がある。ただし、適用宣言書においても、具体的にどのような内部統制が実装されているかまでは開示されていないため、個別に確認する必要がある。
- 適用宣言書等の開示には認証取得企業の同意が必要である。

o「SOC2 保証報告書」は、米国公認会計士協会が定めた規準に基づいて、独立した監査法人が作成した報告書である。Type I 報告書（時点保証報告書）、Type Ⅱ報告書（期間保証報告書）のいずれかが発行され独立監査人の保証意見が付されているが、特に TypeⅡ報告書は、監査人が必要と考えて実施した個別詳細な手続と手続ごとの評価結果も記載される。

なお、チェックリストに活用する際の留意点は次のとおり。

- 「SOC2 保証報告書」の規準には、チェックリストの確認項目に含まれていない規準もあり、チェックリストでは不要な規準も評価した上で発行される。
- チェックリストの確認項目を満たすためには、評価規準としてセキュリティ（33 規準）と可用性（3 規準）を選択する必要がある。
- 報告書には、事業者によるサービスコミットメントが記載されているが、そこにチェックリストを充足する旨が記載されていない限り、チェックリストの確認項目が全項目含まれていない可能性が高い。

o「合意された手続報告書」は、事前に合意した手続に関する実施結果を報告する業務であり、実施結果から導かれる結論の報告や保証が提供されるものではないが、依頼者（API 接続先）、実施者（監査法人）、利用者（金融機関）で手続きの内容を設定できるため、チェックリストの確認項目を過不足なく評価することができる。

なお、チェックリストに活用する際の留意点は次のとおり。

- 契約時点では合意していなかった追加利用者（他金融機関）への配布時は、業務の性質や利用制限等の事項について個別に合意書を締結する必要がある。

o前述の３つの第三者認証、保証報告書等のコストなどは、実際のケース毎に異なり一概には言えないが、相応の準備期間と取得・維持コストがかかる。傾向としては、負担が大きい順に並べると、次のような傾向と考える。

「SOC2 保証報告書」 ＞ 「合意された手続報告書」 ＞ 「ISMS 認証」

＜委員意見＞

各委員から自らの「第三者認証等の利活用に関する意見」について説明がなされた後、以下のとおり討議が行われた。

- o 第三者認証・保証報告書等がカバーしている確認項目については、効率化を考慮して、再度確認を求めないことが望ましいと考える。
- o 取得済の第三者認証や保証報告書等の対象範囲にはチェックリストの内容が含まれていない可能性があることを認識したが、チェックリストの内容を含めた第三者認証や保証報告書等をあらためて取得するAPI接続先があるか、API接続先のご意見をお伺いしたい。
- o API接続先の立場からすると、第三者認証や保証報告書等は事業上の必要性から取得することがあっても、API接続のためにチェックリストを範囲とする第三者認証や保証報告書等をコスト負担してまで取得することはないと思う。
- o 第三者認証や保証報告書等はチェックリストの確認項目を補完できる可能性があると思うが、活用方法は各々の金融機関等が必要に応じて考えることであって、チェックリストを見直すようなものではないのではないか。
- o 確認項目の中でも、特に第三者認証や保証報告書等を活用できると思われる確認項目（通番３、８、９、13、14、21、24、27、33）がある。これらの確認項目に、「第三者認証や保証報告書等を利用する」という趣旨の手法例を追加すると、コミュニケーションの効率化に繋がるのではないか。
- o 解説書の「３．利用にあたっての留意事項等」（Ｐ８）に記載されている「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。」の箇所に、利活用が想定される「保証報告書」や「合意された手続報告書」を追加した方が良いのではないか。
- o （事務局意見）第三者認証や保証報告書等を活用できると思われる確認項目については、解説書の「３．利用にあたっての留意事項等」（Ｐ８）に既に記載されている「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。」の後に、確認項目の通番をまとめて補足説明とともに記載することも考えられる。
- o 事務局意見のように、確認項目の通番をまとめて記載する方向性自体には賛同できるが、その確認項目を充足するには第三者認証や保証報告書等の取得が必須であるとの誤解が生じることのない記載内容とする必要がある。

o 取得負担を考慮すれば第三者認証や保証報告書等の利活用は難しいとも考えられるが、取得が必須でないことが容易に理解できる内容であれば、事務局意見の方向性で記載することに異論はない。

o 第三者認証や保証報告書等が実務上どのように利活用されているかといった事例は、チェックリストのユーザーにとって非常に有益な情報と考えるが、FISCとして事例を紹介する考えはあるか。

o （事務局意見）現段階で事例紹介は予定していないが、今後、チェックリスト関係者にヒアリングを実施するなかで、第三者認証や保証報告書等の利活用に関する好事例等があれば、事例紹介について検討したい。

＜検討結果＞

o 委員による討議の結果、解説書「３．利用にあたっての留意事項等」（Ｐ８）に記載されている「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。」の箇所について、第三者認証や保証報告書等の取得が必須ではないことを明確にしたうえで、第三者認証や保証報告書等を活用できると思われる確認項目（通番３、８、９、13、14、21、24、27、33）を例として記載することが決定された。

o 本改訂は、重要な判断が求められる内容ではないことから、有識者検討会を開催せず、本連絡会で見直しを決定することが確認された。

■ **事務局から提示された観点以外のもの**

委員から提案があった、第三者認証に関連する表記等の見直し

＜委員からの提案＞

o 「第三者認証」という語句には、保証報告書（例：SOC2 等）が含まれないため、「第三者認証」と分けて「保証報告書」も記載することが必要。

o 保証報告書の例としてSOC1が記載されているが、SOC1は財務報告目的の報告書であり、チェックリストでの利活用という趣旨に沿う報告書ではないため、記載しない方が良い。　等

＜検討結果＞

o 委員による討議の結果、解説書の「利用にあたっての留意事項等」および確認項目の【通番３】で、第三者認証に関連する表記等の見直しを行うことが決定された。また、表記等の見直しに伴い、用語解説として、「合意された手続報告書」の追加、「SOC1」・「SSAE16」・「ISAE3402」の削除が確認された。

o 本改訂は、重要な判断が求められる内容ではないことから、有識者検討会を開催せず、本連絡会で見直しを決定することが確認された。

３．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

ｏ本連絡会開催に先立ち、FISCがチェックリスト関係者へチェックリストの使用状況や要望などについてヒアリングを実施したところ、チェックリストの運用面で様々な意見があり、その中で、今後の留意すべき事項を以下のとおりまとめた。これらは解説書の「３．利用にあたっての留意事項等」に明記されている内容（※）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。

（※）チェックリストへの項目追加・変更箇所の識別に関する部分は除く

■ 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「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。

■ 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FISCの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、「FISCの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