第三者認証の利活用に関する委員意見

資料３－２

1．第三者認証の利活用に関する各委員の意見

	意見
	・総論として賛成です。また、デロイトトーマツ様のご提供いただいた資料のように、カバーできる共通項目だけでも活用することができるのではないかと認識しております。
	・デロイトトーマツ様のお話、大変参考になりました。FISC APIチェックリストを対としたSOC2保証報告書までFinTech企業側で対応できれば申し分ないですが、相応費用がかかるため 第三者認証の利用については各Fintech企業の判断に委ねざるを得ないかと考えます。 ・なお、こういった第三者認証の制度があることについて、電子決済代行業協会やFintech協会等の場を通じて各企業あてに紹介された方がよいと思います。
	・第三者認証をどのように利活用できるか具体的な実践事例は有益だと考えるので、今後実践事例を収集してFISC調査レポートなどで取り上げてはどうか。
	・トーマツ様より紹介頂いた第三者認証はいずれも、API接続チェックリストの項目確認を一定程度補完できる可能性のあるものであると理解したが、活用の方法としてはあくまで 各金融機関が各第三者認証の特徴を正しく理解し、各金融機関が各々のリスク認識を踏まえ、必要に応じて各金融機関のチェックリスト項目に独自項目として加える、程度に留める べきで、共通フォーマットとしてのチェックリストへの項目追加・改訂を検討する程のものではないと思料します。
	・審査負担の軽減の観点から、第三者認証の利用により省略できるチェックリスト項目を検討することは有益である。 ・また、将来的には、FISCチェックリストをベースに統一基準を策定し、独自の第三者認証制度を創設することも考えられるのではないか。
	・まず、時間や作業効率の向上という点で活用に賛成です。その際、第三者認証、保証型監査等によって内容の対象や時点、強度に差があると思われます。 例えば、SOC 1/2 は一年といった長い点で運用が評価されるのに対し、認証はある時点でのスナップショットの評価であったりし得ます。それを受けて、例えば SOC 1/2 を取得している 場合はこの項目は OK（または手法例に入れる？）とする、ISO27001 で評価済みの場合はOK とするなど、追加情報が与えられると金融機関・API接続先双方にメリットがあるかと考えます。
	・デロイトトーマツ社の説明を聞く限りにおいては、第三者認証を活用してAPI接続チェックリストの項目を効率的に確認することは、API接続先の認証取得に係る負担等を考慮すると 現実的ではないと考える。 ・なお、金融機関とAPI接続先との効率的な確認の観点からは、例えば、API接続先が一定のセキュリティ水準を確保していることを認定電子決済等代行事業者協会が確認し、このこと を金融機関が同協会に確認するといったスキームを確立することが考えられる。
	・活用は難しいと思料
	・弊社としては、SOC2レポート等を取得した際は、有効に活用したいと考えている。 特に運用面に関してはチェックシートによる質問、回答より細かく確認できる部分もあると考えており、金融機関、API接続先双方にメリットがあると考えている。 ・なお、第三者認証に関して現時点ではチェックリストの見直しをかける必要はないと考えている。
	・チェックリストの信頼性を担保する目的で、第三者認証の利活用を検討することに関しては問題ないと考えます。 ただし、保証を得るための対価（ランニングコストとしてどの程度の費用がかかるか？）についての検討は必須と考えます。（そのコストが最終的に利用者に転嫁されるため。） 仮に、各電代業者が第三者認証機関（監査法人等）と契約するようなスキームで、かつ、第三者認証が必須というような仕組みにしてしまった場合、新規参入事業者に対する実質的 な参入障壁となりかねないことを懸念いたします。端的に言うと、SOC2やISMSによる保証は、銀行APIといった、誰でも利用する可能性のあるサービス、かつ、利用ユーザーにとって、 その利用料金が「無料」または「廉価」と考えているサービスについては、あまりFITしないのではないかと考えています。
	・当行ではAPI接続チェックリストによる接続先が１先であることから第三者認証の利活用に関して可否に関して判断しにくい状況です。 ・利活用する際の負担軽減の為に利活用に適した第三者認証に関する情報を開示していただけるようお願いします。
	・API接続チェックリストはオフサイトモニタリングを前提としているので、外部認証での充足項目に関しては再度確認を求めないことが運用上望ましいと考える。 ・ISMS認証（ISO27001）ではAPIチェックリストの全ての項目を網羅していないため下記2種類の運用方法が検討できる。 ① ISMS認証（ISO27001）取得企業 適用範囲の定義書および適用宣言書を開示していただいた上で次の対応が検討できる。 （1） 適用宣言書で対応していると宣言している内容についてはAPIチェックリストの確認不要（但し、宣言内容次第では追加のヒアリングが必要） （2） ISO27001でカバーできていない箇所のみAPIチェックリストの内容を回答 ② SOC2レポート、合意された手続き報告書作成企業 SOC2レポートまたはAPIチェックリストの内容を網羅した合意された手続き報告書を開示されるのであれば、APIチェックリストでの確認は不要。 ・併せて、各認証によるチェックリスト充足項目は、監査法人トーマツ案に認識相違ない。 ・一方で、APIチェックリストを省略するために合意された手続報告書を準備するFintech企業がいるのかどうか委員のご意見を伺いたい。
	・この前のデロイト様のお話を伺う限り、第三者認証がFISC API接続チェックリストの完全な網羅性が担保できないのであれば、チェックリストに合致する項目についてのエビデンスに 止めるべきではないか。
	・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な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、第三者認証や保証 報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても、できる限り重要項目を限定し、API接続先の管理態勢 や対策を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。

第三者認証の利活用に関する委員意見

2. チェックリストの見直し内容

	解説書 or フォーマット	ページ	現行（修正前）	修正案（修正後）	修正理由（コメント）	備考
	解説書	8	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な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。	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。	第三者認証（評価、手続き等）については、合意された手続きの実施も視野に含めたほうが良いと考えます。	日本公認会計士協会　専門業務実務指針4400「合意された手続業務に関する実務指針」
	解説書	13	無し	合意された手続報告書	国際監査・保証審議会が公表する基準であるISRS4400,日本公認会計士協会が定める専門業務実務指針4400に基づく報告書である。 本チェックリストにおける活用方法としては、業務依頼者（API接続先）と利用者（金融機関）との間で、API接続先のセキュリティ管理態勢等について、監査法人等に実施させる一定の手続きを予め合意し、監査法人等にその手続を実施させる。監査法人等は、保証の提供は行わず、手続き実施結果を事実に即して報告する等、活用が可能である。	日本公認会計士協会　専門業務実務指針4400「合意された手続業務に関する実務指針」
	解説書	27	無し	＜外部機関による報告書の活用＞ 当該項目については、第三者報告書を取得して、管理態勢が整備、運用されていることを示すことが考えられるが、第三者報告を取得していなければならない訳ではない。 ＜第三者認証の利用＞の下に、＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、セキュリティ管理態勢が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先のセキュリティ管理態勢を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	33	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、連鎖接続先の管理態勢が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先の連鎖接続先の管理態勢を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	34	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、不正アクセスや障害の管理態勢が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先の不正アクセスや障害管理態勢を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	41	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、利用者保護態勢が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先の利用者保護の態勢を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	42	無し	同上	同上	

第三者認証の利活用に関する委員意見

	解説書 or フォーマット	ページ	現行（修正前）	修正案（修正後）	修正理由（コメント）	備考
	解説書	52	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、内部からの不正アクセス対策が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先の内部不正アクセス対策を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	58	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、内部作業者の不正行為対策が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先の内部不正行為対策を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	62	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、システムやネットワークの脆弱性対策が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先のシステムやネットワークの脆弱性対策を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	
	解説書	73	無し	＜金融機関への情報提供＞を追加し、「本項目については、保証報告書や合意された手続報告書によって、偽アプリケーション対策が整備されていることを金融機関に示すことが考えられるが、必須の取組みではない。」	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な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、第三者認証や保証報告書、合意された手続報告書の依頼、外部監査による評価の活用を積極的に検討する。とされていますが、金融機関としても少なくとも、API接続先における偽アプリケーション対策を把握し、何らかのトラブルが発生し、リスク管理を問われた場合の対応を準備する必要があると考えます。	