参考資料２

「API 接続チェックリスト（試行版）」 利用にあたって

１．目的

「API 接続チェックリスト（試行版）」（以下「チェックリスト」という）は、銀行と API 接続先が効率的にコミュニケーションを行うためのツールとして、「API 接続先チェックリスト ワーキンググループ」（以下「チェックリスト WG」という）において、機密性に関して共通的に確認する項目を中心に策定したものである。

（注）オープン API のあり方に関する検討会（事務局：一般社団法人全国銀行協会）「オープン API のあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」には、「複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される」と記載されている。

２．共通確認項目及び構成要素

共通確認項目は、大きく分けると以下の２つである。

（１）安全対策の遂行能力の確認

①オープン API のあり方に関する検討会が定める安全対策の遂行能力

オープン API のあり方に関する検討会報告書「セキュリティ原則」に基づき作成

②FISC 安対基準（FinTech 関連項目）の遂行能力

FinTech 検討会で提言された考え方等を踏まえて作成

③基礎的な安全対策の管理・運営能力

FISC が策定する「必要最低限の安対基準」（注）又は業界団体の自主基準

（注）「必要最低限の安対基準」は、API 接続先を含む金融関連サービスの提供に携わる事業者において、踏まえられるべき基準としても制定される。その制定までの間は、少なくとも「安全対策遂行能力のうち基礎的な部分」を踏まえて検討されることが望ましい。

（２）その他の確認

利用者保護態勢等

共通確認項目				独自確認項目
（１）安全対策関連			（２）その他	
① API 検討会が定める安全対策の遂行能力	② FISC 安対基準(FinTech 関連)の遂行能力	③ 基礎的な安全対策の管理・運営能力	利用者保護態勢等	

３．全体構成

チェックリストには 60 個の確認項目がある。

章	区分	各章の目的	項番
1	情報・セキュリティ管理態勢	API 接続先の情報・セキュリティ管理態勢について確認する。	1-10
2	外部委託管理	API 接続先が外部事業者に委託して開発する場合の管理態勢について確認する。	11-13
3	銀行・API 接続先の協力体制	利用者保護の観点から、銀行及び API 接続先における責任分界点や役割分担について確認する。	14-19
4	コンピュータ設備管理	API 接続先がサービスを提供するシステムが実装されているコンピュータ設備のセキュリティについて確認する。	20-22
5	オフィス設備管理	API 接続先がサービスを提供するシステムにアクセスする機器が設置されているオフィスのセキュリティについて確認する。	23-26
6	システム開発・運用管理	API 接続先の基本的な開発及び運用の管理態勢について確認する。	27-40
7	サービスシステムのセキュリティ機能	API 接続先が提供するサービスシステムのセキュリティ実装要件について確認する。	41-49
8	API セキュリティ機能	利用者保護の観点から、API アクセスを管理するシステムについて確認する。	50-57
9	API 利用セキュリティ	利用者への説明義務について確認する。	58-60

４．取扱方法

（１）各項目の説明

チェックリストの各項目に関する説明は、以下の通り。

通番：通し番号

区分：テーマ別分類

セキュリティ対応目標：安全対策を実施する目標

対象者：安全対策を実施する主体

手法例：安全対策の例示

現在の対応状況：対象者が現在実施している安全対策の状況を記載する

今後の対応予定：対象者が今後実施予定の安全対策について記載する

関連規定：参照先（全銀協「セキュリティ原則」又は FISC「安対基準」）

関連規定箇所：全銀協「セキュリティ原則」及び FISC「安対基準」の参照箇所

（２）使用タイミング及び用途

チェックリストの使用タイミング及び用途は、API 接続先の任意である。

なお、API 接続先が銀行との API 接続を検討する際、チェックリストの「現在の対応状況」及び「今後の対応予定」を予め記載しておくことにより、銀行が実施する API 接続先の適格性審査において、双方の対応負担が軽減されることとなる。

（３）留意事項

チェックリストを利用するにあたっては、以下について留意する必要がある。

・チェックリストは機密性に関する確認項目を中心に策定し、各銀行の独自確認項目が多くならないよう幅広に用意した。しかし、各銀行が必要とする確認項目の全てを網羅したものではない。他に必要な確認項目がある場合は、各銀行にて独自の確認項目を付加する場合がある。

・記載されている手法例はあくまで例示であり、業務特性やリスク等を勘案し各銀行にて取捨選択する。なお、各銀行の判断により、例示以外の手法を選択することを妨げるものではない。

・チェックリストはコミュニケーション・ツールとして活用することを想定している。各銀行は必要に応じて「今後の対応予定」等の欄を用いて、API 接続先から「○」又は「×」の回答を単に受けるだけではなく、API 接続先と十分に会話するよう努める。

・チェックリストの確認項目のいずれかにおいて、API 接続先の回答が「×」であったとしても、各銀行は業務特性やリスク等を踏まえて総合的に判断する。

・チェックリストは、銀行、IT ベンダー、そして大小様々な規模の API 接続先においても利用しやすく、理解しやすいものとなるよう、見直しが行われる予定である。

５．今後の予定

チェックリスト（試行版）の見直しの時期および方法については、チェックリストWGメンバーを含む関係者の意見を踏まえ、引き続きFISCにて検討を行う。

なお、チェックリストへの反映が予定されている「必要最低限の安対基準」については、その原案がFISC安全対策専門委員会において2017年10月を目途に確定される予定のため、チェックリストの見直しの時期は少なくともそれ以降となる見込みである。

以上

参考

API 接続先チェックリスト検討の経緯

１．検討メンバー

チェックリスト WG は、API 接続に携わる関係者 10 社（全銀協から銀行 3 行、FinTech 協会から FinTech 企業 3 社、IT ベンダー3 社、FISC 監査安全部 1 名）を委員とし、金融庁及び日本銀行にもオブザーバーとして参加いただいた（事務局は FISC 企画部が担当）。

（敬称略）

区分	氏名	所属・役職
銀行 （3 名）	奥野　瑞穂	株式会社みずほ銀行 e-ビジネス営業部　法人プロダクト開発チーム 調査役
	小原　彰	株式会社三井住友銀行 システム統括部　統括グループ　グループ長
	原田　一雪	株式会社三菱東京 UFJ 銀行 デジタル企画部　事業開発グループ　次長
FinTech 企業 （3 名）	土佐　鉄平	freee 株式会社 開発本部　チーフセキュリティアーキテクト
	大目　晃弘	マネーツリー株式会社 ビジネスディベロップメント　マネージャー
	内波　生一	株式会社マネーフォワード アカウントアグリゲーション本部　本部長
IT ベンダー （3 名）	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
	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 金融インダストリー・ソリューション　担当部長
	谷内　圭	富士通株式会社 金融システム事業本部　デジタルビジネス開発室 シニアマネージャー

区分	氏名	所属・役職
FISC （1 名）	亀水　宏次	公益財団法人金融情報システムセンター 監査安全部　次長
オブザーバー （4 名）	小林　侑剛	金融庁 総務企画局　企画課　信用制度参事官室　課長補佐
	市村　雅史	金融庁 検査局　総務課　システムモニタリングチーム 専門検査官
	中井　大輔	日本銀行 金融機構局　考査企画課　企画役
	宮　　将史	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

（金融情報システムセンター事務局）

常務理事		髙橋　経一
企画部	部長	小林　寿太郎
企画部	次長	藤永　章
企画部	主任研究員	大澤　英季

◆事務局スタッフ

柴田　晃宏、仲程　文徳（第 4 回まで）、三浦　哲史、田　昊

２．開催実績

回数	日時	主な内容
第１回	２月７日（火） 10 時～12 時	API 接続先チェックリスト検討の前提（FinTech 有識者検討会における議論）の内容確認
第２回	２月 20 日（月） 15 時～17 時	API チェックリスト検討のたたき台（FinTech 企業の委員による発表）等をもとに議論
第３回	３月３日（金） 15 時～17 時	API 接続先チェックリスト作成手順案（事務局案）等をもとに議論
第４回	３月 17 日（金） 15 時～17 時	同上
第５回	４月 11 日（火） 15 時～17 時	API 接続先チェックリスト（案）等をもとに議論
第６回	４月 25 日（火） 15 時～17 時	同上
第７回	５月 11 日（木） 15 時～17 時	同上
第８回	５月 25 日（木） 15 時～17 時	同上
第９回	６月６日（火） 15 時～17 時	同上
第 10 回	６月 20 日（火） 15 時～17 時	API 接続チェックリスト（試行版）の最終確認

３．検討にあたっての前提

オープン API は、FISC において開催している「金融機関における FinTech に関する有識者検討会」（以下「FinTech 検討会」という）におけるタイプⅢ（FinTech 企業が金融関連サービスを主導する形態で、金融機関の安全対策上の責任が部分的となる場合）の実現方法の１つであることから、チェックリスト WG の検討は、FinTech 検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である。すなわち、タイプⅢにおける「外部委託基準の準用ルール」及び「必要最低限の安対基準」を踏まえつつ、FinTech に関する安全対策を検討している集団の相互関係を考慮した検討が行われることが必要である。

チェックリスト WG において、FinTech 検討会におけるタイプⅢに関する提言内容と整合的な検討が行われた結果として作成されたチェックリスト等は、FinTech 検討会の提言内容の一部として取り扱われることとなる。

（参考）「金融機関における FinTech に関する有識者検討会」報告書

【資料９】API接続にあたって使用されるチェックリストに関する集合的な検討

全銀協が公表した「オープンAPIのあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理（案）】」において，「複数の銀行とAPI接続する企業等における審査対応負担を軽減する観点から，情報セキュリティ関連機関において，銀行がAPI接続先の適格性を審査する際に使用する，必須確認項目と独自確認項目からなる「API接続先チェックリスト」（仮称）を制定することが期待される」と整理された。

こうした整理を受けて，平成29年2月，FISCが事務局となり，「API接続先チェックリストワーキンググループ」（以下「チェックリストWG」という）を設置し，入口の管理フェーズで行われる統制の内容，すなわち，API接続先に対する客観的評価で使用されるチェックリスト（以下「チェックリスト」という）の共通部分に関する検討等を行っている。

オープンAPIは，FinTech検討会におけるタイプⅢの実現方法の１つであることから，チェックリストの検討は，FinTech検討会におけるタイプⅢに関する提言内容と整合的に進められることが必要である。すなわち，タイプⅢにおける「外部委託基準の準用ルール」，及び「必要最低限の安対基準」[79]を踏まえつつ，FinTechに関する安全対策を検討している集団の相互関係を意識した検討が行われることが必要である。

また，FinTech企業の負担軽減の観点から，社会的規範性をもったチェックリストが制定されることが望ましく，そのためには，金融機関，FinTech企業，ITベンダーといったAPI接続に携わる関係者が，合意形成を目指して，チェックリストの検討過程に参画することが望ましい。

チェックリストの制定に当たって，以上の集合的な検討が行われ，その結果として，成果物が取りまとめられた場合には，その成果物は，FinTech検討会の提言内容の一部として取り扱われることとなる。また，環境変化等が生じた場合にも，以上の集合的な検討が行われ，成果物の内容が継続的に見直され，実装・運用されることが期待される。

API接続に携わる関係者においては，その成果物を，有用なものとして，金融機関の実態に応じて利用し，総体的な安全性の確保とイノベーションの両立が目指されることを期待する。

[79]「必要最低限の安対基準」は，API接続先を含む金融関連サービスの提供に携わる事業者において，踏まえられるべき基準としても制定される。その制定までの間は，少なくとも「安全対策遂行能力のうち基礎的な部分」（脚注26）を踏まえて検討されることが望ましい。

４．主な議論（要旨）

チェックリストWGにおける主な議論（要旨）は、以下の通り。

・「参照系」（注 1）と「更新系」（注 2）の別は、サービスの内容が個々で、かつ、これから拡がりをみせることから、二者の区別が現段階では難しいこと、また、一律に二者のどちらがリスクが高い又は低いとは断定できない（注 3）ことから、確認項目を分けず、銀行が案件の都度、個別に判断することとする。

・チェック項目は、独自確認項目がたくさんあるよりも、できるだけ共通項目として開示する（その上で、利用する確認項目は案件の都度、銀行が決める）方が、事前にAPI接続先が安全対策を準備するのに資するとの考えから、幅広に用意する。

・チェックリストの「セキュリティ対応目標」に対し、「手法例」（注 4）を用意する。目標に対し、単に「○」又は「×」の回答だけではなく、具体的な対応状況を銀行側に伝えることができる仕組みとする。また、「現状」及び「今後の対応状況」欄も設けることにより、銀行及びAPI接続先双方の‘コミュニケーション・ツール’としての活用を期待する。

・基本的にチェックリストは銀行がAPI接続先を審査する際に使用するリストであるが、二者間の‘コミュニケーション・ツール’を目指す観点から、API 接続先から銀行に確認する項目も含める。また、銀行及びAPI接続先の双方にて確認する項目も含める。

・チェックリストは、安全対策関連の機密性に関する確認項目をほぼ網羅し、機密性に関する独自確認項目は基本的にはない想定である。また、利用者保護に関する確認項目は、関係者で合意した項目を掲載する。

・「必要最低限の安対基準」は現時点でまだ決定されていない。決定次第、API接続に関する実態等も踏まえて、チェックリストの見直しを行う予定とする。

（注 1）「参照系」とは、銀行がAPI接続先へデータを提供する場合をいう。

（注 2）「更新系」とは、銀行がAPI接続先からデータを受入れる場合をいう。

（注 3）例えば、金額 10 万円の更新系（決済指示）のリスクと、100 万人の顧客情報の漏洩が生じて 1 人 1 千円の慰労金を配布するケース（@1 千円×100 万人=10 億円）におけるリスクを比べた場合、どちらかが高いとは一概に言えないのではないか、との意見があった。

（注 4）当初、チェックリストは「最低限の目線」あるいは「松・竹・梅のようなレベル別の目線」を示す案であったが、これから多様なサービスの拡がりが見込まれる中、現実的な対応としては、複数の具体例を列挙する形式とした。また、「手法例」はあくまで例示であり、いずれかを満たせば、その確認項目のセキュリティ対応目標をクリアしていると一義的に判断できるものではない。

５．関連団体への展開

委員としてチェックリストWGに参加していない他業態の預金取扱金融機関（以下「関連団体」という）には、チェックリストの位置づけを十分ご理解いただき、参考として利用していただくことを期待する。

（注）関連団体は以下の通り。

- 一般社団法人 全国地方銀行協会
- 一般社団法人 第二地方銀行協会
- 全国信用協同組合連合会
- 農林中央金庫
- 株式会社ゆうちょ銀行
- 一般社団法人 信託協会
- 一般社団法人 全国信用金庫協会
- 労働金庫連合会
- 株式会社 商工組合中央金庫
- 一般社団法人 国際銀行協会