【資料５】

2025 年 1 月 30 日
金融情報システムセンター

2024 年度　API 接続チェックリスト見直し要否　対応方針

【対応方針】API 接続チェックリストの見直しは「不要」とする。

金融機関・電子決済等代行業者のニーズ、チェックリスト関連規程（FISC「安全対策基準」、全銀協「オープン API のあり方に関する検討会報告書」）改訂、更新系 API のサービス提供状況ほか、当センターが確認する限り、API 接続チェックリストの見直しを要するような事象は発生していないと考えられることから、API 接続チェックリストの内容は不変としたい。

1　見直しに関するルール

API 接続チェックリスト（以下、チェックリスト）の維持管理方法については、チェックリスト解説書 P2 に下記の通り規定されている。

今後の維持管理方法

FISC は、「API 接続チェックリスト」が常に有益なものであるよう、「API 接続チェックリスト連絡会」を設置し、以下の事項を踏まえて年 1 回、チェックリストの見直しについて検討する。また、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、有識者検討会等を開催し審議することとする。

(1) ユーザーの使用状況や要望
(2) オープン API に関するインシデントの発生状況
(3) オープン API に関する標準化の動向
(4) 認定電子決済等代行事業者協会の自主基準　等

なお、インシデントの発生等に伴い、金融機関及び API 接続先に対して速やかに注意喚起等を行う必要がある場合には、FISC 事務局がウェブサイト等を通じて行う。

また、過去の「API 接続チェックリスト連絡会」（以下、連絡会）において、下記事項の動向についても継続的に確認している。

- チェックリスト関連規定
  （FISC「金融機関等コンピュータシステムの安全対策基準・解説書」、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」）
- 更新系 API のサービス提供状況

2　各検討事項の評価

(1) ユーザーの使用状況や要望

昨年度連絡会の議事要旨公表以降、複数の金融機関、電子決済等代行業者等と意見交換を行ってきたなかで、チェックリストの改訂にかかる具体的なニーズは確認できていない。

一部の金融機関、電子決済等代行業者からは、更新系 API が普及した場合には、チェックリストの見直しについて検討が必要となる可能性もあるとの意見があった。

しかしながら、金融機関による更新系 API への取組みが低位である現状においては、チェックリストの更改は不要と考える。

(2) オープン API に関するインシデントの発生状況

当センターが情報収集する限り、これまで、チェックリストの改訂を要するようなインシデントの発生は確認できていない。

(3) オープン API に関する標準化の動向

当センターが情報収集する限りでは、これまで、チェックリストの改訂を要するような標準化の動向は確認できていない。

(4) 認定電子決済等代行事業者協会の自主基準

2020 年 12 月、電子決済等代行事業者協会は、会員向けの自主基準を制定しているが、その後、チェックリストの見直しを要する改訂等は行われていない。

(5) チェックリストの関連規程等の改訂

当センターは、2024 年 3 月に、「金融機関等コンピュータシステムの安全対策基準・解説書」（以下、「安全対策基準」という。）を改訂し、「第 12 版」として公表した[1]。第 12 版では、チェックリストにおける確認項目において、関連規定として敷衍されている安全対策基準の一部の基準項目が改訂されており、その内容は、〔図表 1〕のとおりである。

改訂内容を確認した結果、いずれもチェックリストの見直しを要するものではないと判断される。

〔図表 1〕チェックリストに関連規定として明記されている安全対策基準の主な改訂内容

チェックリスト	安全対策基準	主な改訂内容
-	1.安全対策基準の意義	また、政府が定める重要インフラ 14 分野の一つに金融分野が挙げられており、金融関連サービスを重要インフラとして官民が一体となり、重点的に防護することが求められている。 【下線部追加】 ・金融関連サービスを重要インフラとして防護する必要がある旨の記載を追加

[1] https://www.fisc.or.jp/publication/book/005831.php

チェックリスト	安全対策基準	主な改訂内容
-	１.安全対策基準の 意義	FinTech 企業 （脚注 1） IT を活用した新たな金融関連サービスを提供する事業者。 【下線部変更】 ・用語定義の見直しに伴う脚注の 修正
-	1.総論 (3) （脚注 21）	（脚注 21） 例えば、預金取扱金融機関における勘定系システムに対し、オープン API 等による接続が行われる場合は、当該システムはインターネットバンキングに類似するリスク特性を有していると解され、金融機関等は、FinTech 企業に対し、「データの保全」や「本人認証」に係る安全対策の実施状況や、その効果について検証を行うこととなる。 【下線部変更】 ・用語定義の見直しに伴う脚注の修正
-	3.用語の解説 (2)	外部委託先 金融機関等から業務を受託する事業者又は、金融機関等にサービスを提供する事業者。なお外部委託先には再委託先を含む。また、再委託先には再々委託先以下の階層を含む。 【下線部変更】 ・定義の記載を改善
-	3.用語の解説 (2)	金融機関 銀行等の預金取扱金融機関、信託会社、保険会社、証券会社、クレジット会社をいう。 【下線部追加】 ・金融機関の用語解説を追記
-	3.用語の解説 (2)	金融機関等 銀行等の預金取扱金融機関、信託会社、保険会社、証券会社、クレジット会社、資金移動業者、前払式支払手段発行者等をいう。 【下線部変更】 ・金融機関等の用語定義を見直し
3. 情報・セキュリティ管理態	統 14 セキュリティ教育を行うこと。	教育テーマとしては、以下の例がある。 (6)サイバーセキュリティ（コンピュータウイルスへの対応等） 【下線部変更】 ・セキュリティ意識向上のための教育テーマとして、サイバーセキュリティを追記
10. 外部委託管理	統 21 外部委託先と安全対策	【クラウド利用の場合の考慮事項】 【下線部変更・削除】

チェックリスト	安全対策基準	主な改訂内容
	に関する項目を盛り込んだ契約を締結すること。	・分かりやすい表現に見直し
10. 外部委託管理	統 22 外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。	②データセンターの入退管理ルール、機器管理ルール 【下線部変更】 ・用語の見直し
39. API セキュリティ機能利用者の利便性と、リスクに見合った利用者保護を実現する認証強度とする。	統 27 FinTech 企業がダイレクトチャネルを通じて、金融機関等の顧客に対し、金融機関等の口座と連携した金融関連サービスを提供する場合には、金融機関等は連携するサービス全体のリスクを把握し、発生する可能性がある固有のリスクを考慮した適切な安全対策を講ずること。	FinTech 企業がダイレクトチャネルを通じて、金融機関等の顧客に対し、金融機関等の口座と連携した金融関連サービスを提供する場合には、金融機関等は連携するサービス全体のリスクを把握し、発生する可能性がある固有のリスクを考慮した適切な安全対策を講ずること。 【下線部変更】 ・用語の見直し
22. システム開発・運用管理 システムアクセス時の認証を実施する。	実 1 他人に暗証番号・パスワード等を知られないための対策を講ずること。 実 8. 本人確認機能を設けること。 実 26 パスワードが他人に知られないための措置を講じておくこと。	基準番号 実 147 基準大項目 個別業務・サービス等 基準中項目 テレワーク 基準小項目 テレワークにおけるデータの保護及び通信の保護・暗号化の対策を講ずること。 【下線部変更】 ・パスワード関連基準 一覧に実 147 を追記
22. システム開発・運用管理 システムアクセス時の認証を実施する。	実 16. 不正アクセスの 監視機能を設けること。	(2)CD/ATM 等やデビットカード端末 を利用したカード取引においては、暗証番号が規定回数誤入力された場合、以後のカード取引を禁止する。 【下線部削除】 ・用語の見直し
-	実 21 コンピュータウイルス等の不正プログラムの検知対策を講ずるこ	1-(2)アクセス履歴による検知システムの運転状況監視や、稼働履歴の分析等により、運転状況の異常、重要ファイルへの不正アクセス、異常なパスワードエラー回数等を確認し、不正行為を検知する。

チェックリスト	安全対策基準	主な改訂内容
	と。	【下線部変更】 ・分かりやすい表現に見直し
21. システム開発・運用管理 情報資産への内部からの不正アクセスを抑止する。	実 27 各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	4.クラウド利用の場合、クラウドサービスにおける権限の付与や見直しの手続きを明確にするため、クラウド事業者に対して、クラウドサービスで提供される資源に対するアクセス権限付与に関する手続き及びそれに関する機能を確認することが必要である。 【下線部変更】 ・分かりやすい表現に見直し
33. サービスシステムのセキュリティ機能	実 142 QR コード決済における安全対策を講ずること。	1. ④利用者のスマートデバイスと QR コード決済アプリを紐付ける 【下線部変更】 ・用語の見直し
33. サービスシステムのセキュリティ機能	実 144 QR コード決済利用上の留意事項を顧客に注意喚起すること。	1. QR コード決済のサービス内容及び留意事項の顧客への周知方法としては、以下の例がある。(省略) (4) 店頭や ATM コーナーのポスターへの記載 【下線部変更】 ・用語の見直し
3. 情報・セキュリティ管理態勢	監 1 システム監査体制を整備すること。	5-(注 1) 金融機関等が監査法人を利用した監査を行う場合、監査の対象期間において外部委託先の会計監査に従事していない監査法人とし、また、選定した監査法人が外部委託先の SOC2、保証業務実務指針 3702 の保証業務に従事している場合には、外部委託先の保証業務に直接従事していない監査責任者を選定するなどにより、外部委託先との利益相反に疑義が生じないような外観とすることが考えられる。 5-(注 2) SOC1、SOC2、保証業務実務指針 3402「受託業務に係る内部統制の保証報告書に関する実務指針」、保証業務実務指針 3702「情報セキュリティ等に関する受託業務の Trust に係る内部統制の保証報告書に関する実務指針」等に基づく第三者保証による報告書。 【下線部変更】 ・指針の変更に伴い修正

3　2024 年度のチェックリスト見直し方針

以上のとおり、見直しのルールとして規定されている 4 項目、関連規定等にチェックリストの見直しが必要となる事項がないこと等を踏まえ、2024 年度のチェックリストの見直しは行わないこととしたい。

以　上