資料３

2022 年 1 月 20 日

2021 年度　API 接続チェックリスト見直し要否　対応方針

公益財団法人　金融情報システムセンター

【対応方針】API 接続チェックリストの見直しは「不要」といたしたい

金融機関・電子決済等代行業者のユーザー要望、チェックリスト関連規定（FISC「安全対策基準」、全銀協「オープン API の在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他、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、今年度の API 接続チェックリストの見直しは不要といたしたい。

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きている。

- チェックリスト関連規定
  （FISC「安全対策基準」、全銀協「オープン API の在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と意見交換を行ってきたが、これまでチェックリストの改訂を要望する具体的な意見は寄せられていない。

(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している限りでは、これまで、チェックリストの改訂を要するような情報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している限りでは、これまで、チェックリストの改訂を要するような情報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公表しているが、2020 年度の連絡会において、自主基準の内容はチェックリストの見直しを要するものではないと考えられることから、チェックリストの見直しは行わないこととした。公表後、これまで、自主基準の改訂等は公表されていない。

(5) チェックリストの関連規定等の改訂

当センターは、①昨今のテレワークの浸透と②一昨年発生した口座不正出金事案を踏まえ、2021 年 12 月「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（第 9 版令和 3 年 12 月版）」を公表した。https://www.fisc.or.jp/publication/book/005075.php

①のテレワークを踏まえた改訂内容は、チェックリストの確認項目と関連性が非常に高いとまでは言えない。また、②の口座不正出金事案を踏まえた改訂内容は、FinTech 企業等が金融機関等の顧客に対し決済サービスを提供する場合の安全対策を規定しており、今後、振込等の資金移動を伴う更新系 API サービスの提供が進み、チェックリストの見直しを検討する際の参考にすべき事項。

なお、従前よりチェックリスト通番 21 および通番 22 に関連規定として明記されている、実務基準 8、実務基準 26，実務基準 27 の主な改訂内容は〔図表 1〕の通り。

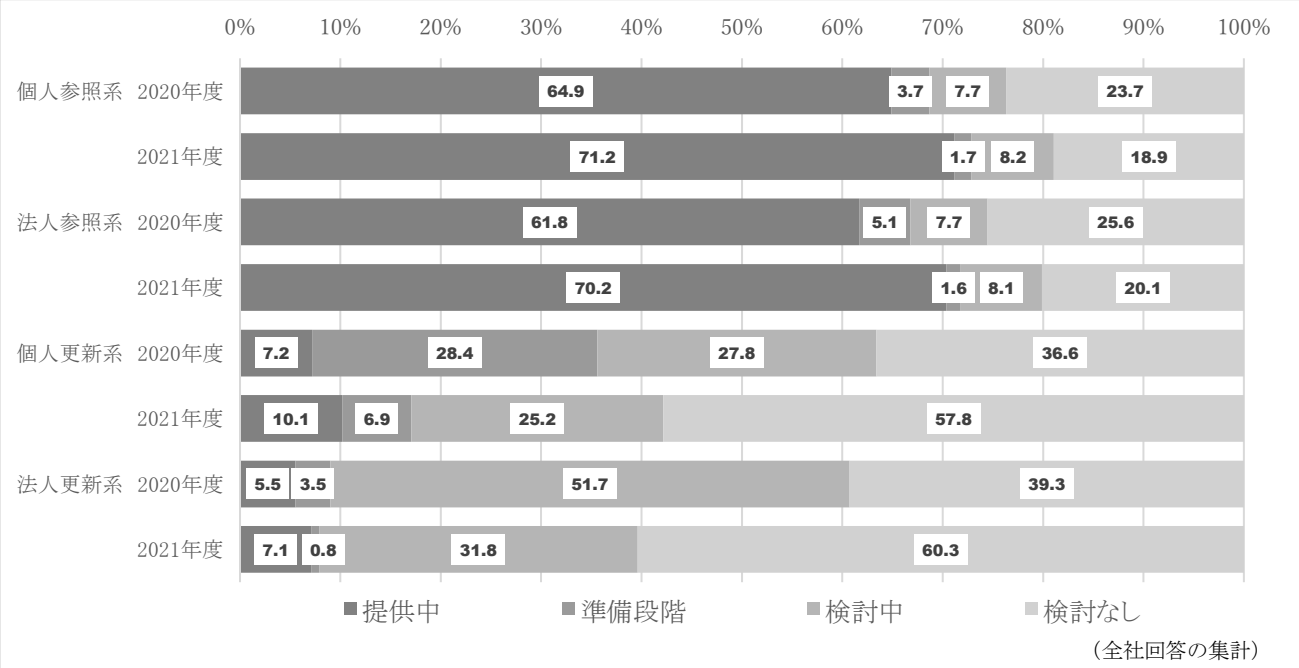
〔図表 1　チェックリストに関連規定として明記されている安全対策基準の主な改定内容〕

チェックリスト	安全対策基準	今般の主な改訂内容
通番 21 情報資産への内部からの不正アクセスを抑止する	実務基準 27 各種資源、システム権限の付与、見直し手続を明確化すること	＜一部内容の追記＞ 2（4）「アクセス権限を抹消できない場合は、当該アクセス権が設定されている ID を、管理台帳等を用いて管理し、管理者による適切な管理を実施する」との一文を追記。 2（5）「外部からアクセス可能な環境に対して管理者権限でアクセス可能とする場合は、デバイス認証やアクセス経路の権限等により限られた環境からしか使えないように設定する等の対策を行うことも検討する」との一文を追記。
通番 22 システムアクセス時の認証を実施する	実務基準 8 本人確認機能を設けること	＜一部内容の追記＞ 2「ただし、キャッシュカードの暗証番号のような組み合わせ数が僅少な情報を、記憶要素として用いる認証方式に頼る認証方法は、インターネット上での利用を避けることが望ましい」との一文を追記 4「資金移動及び注文等の取引を行う場合」との文言を追記
	実務基準 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	＜一部内容の追記＞ 3 パスワード漏洩に備えた対策として、多要素認証や多段階認証を追加。多要素認証を利用する際についても、認証要素に関して、配布時、紛失時、流出時を含めた運用管理方法を明確にし、適切な管理を行うことが望ましいとし、運用管理方法の考慮事項として以下の例を追記。 ・認証要素の配布時、適切に本人確認を行い、安全な経路で配布すること ・認証要素の紛失時や流出時に、即時に利用権限を停止すること

(6) 更新系 API

これまでの連絡会において、更新系 API のユースケースが多く発生した際には、改めてチェックリストの見直し要否を検討するとしてきたが、当センターが実施した「令和 3 年度金融機関アンケート調査結果」によれば、個人更新系のサービスを提供中と回答している金融機関は全体の 10.1%（前年比＋2.9%）、法人更新系は 7.1%（同＋1.6%）と、依然として更新系 API のサービスが広く提供されている状況とは言えない（〔図表 2〕）。

〔図表２〕オープン API の取組み状況



出所：「令和 3 年度金融機関アンケート調査結果」

3 2021 年度のチェックリスト見直し方針

既述のとおり、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、更新系 API のユースケースが広く提供されている状況にないこと等を踏まえ、2021 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