【資料４】

2023 年 1 月 26 日

2022 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、2022 年に、「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（第 10 版 2022 年 12 月改訂）」等を公表した（ https://www.fisc.or.jp/publication/book/005614.php ）。かかる改訂内容と、現在のチェックリストとの主な関連性を示すと、〔図表 1〕として整理できる。いずれも、チェックリスト通番の見直しを要する改訂内容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
通番 3 役職員に対する情報管理方法の周知やモニタリング等の実施により、セキュリティ管理態勢の定着を図る。	統制基準 13 セキュリティ遵守状況を確認すること	＜項番の新設＞ 5　セキュリティポリシーに沿ってサイバーセキュリティに関するリスクが管理されており、同リスクが自社のリスク許容度の範囲に収まるよう優先順位を考慮して適切に管理することが望ましい。【統 5】 6　セキュリティ遵守状況は、経営層に報告することが望ましい。
通番 10 委託業務が円滑かつ適正に遂行されるよう、必要な対策を実施する。	統制基準 21 外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること	＜一部内容の追記＞ 1　契約締結時に考慮すべき事項として、以下を追加 （17）サイバー攻撃に関する留意事項 サイバー攻撃に関するセキュリティ対策（脆弱性診断、監視等）や対応体制（インシデント発生時の対応、管理責任者等）

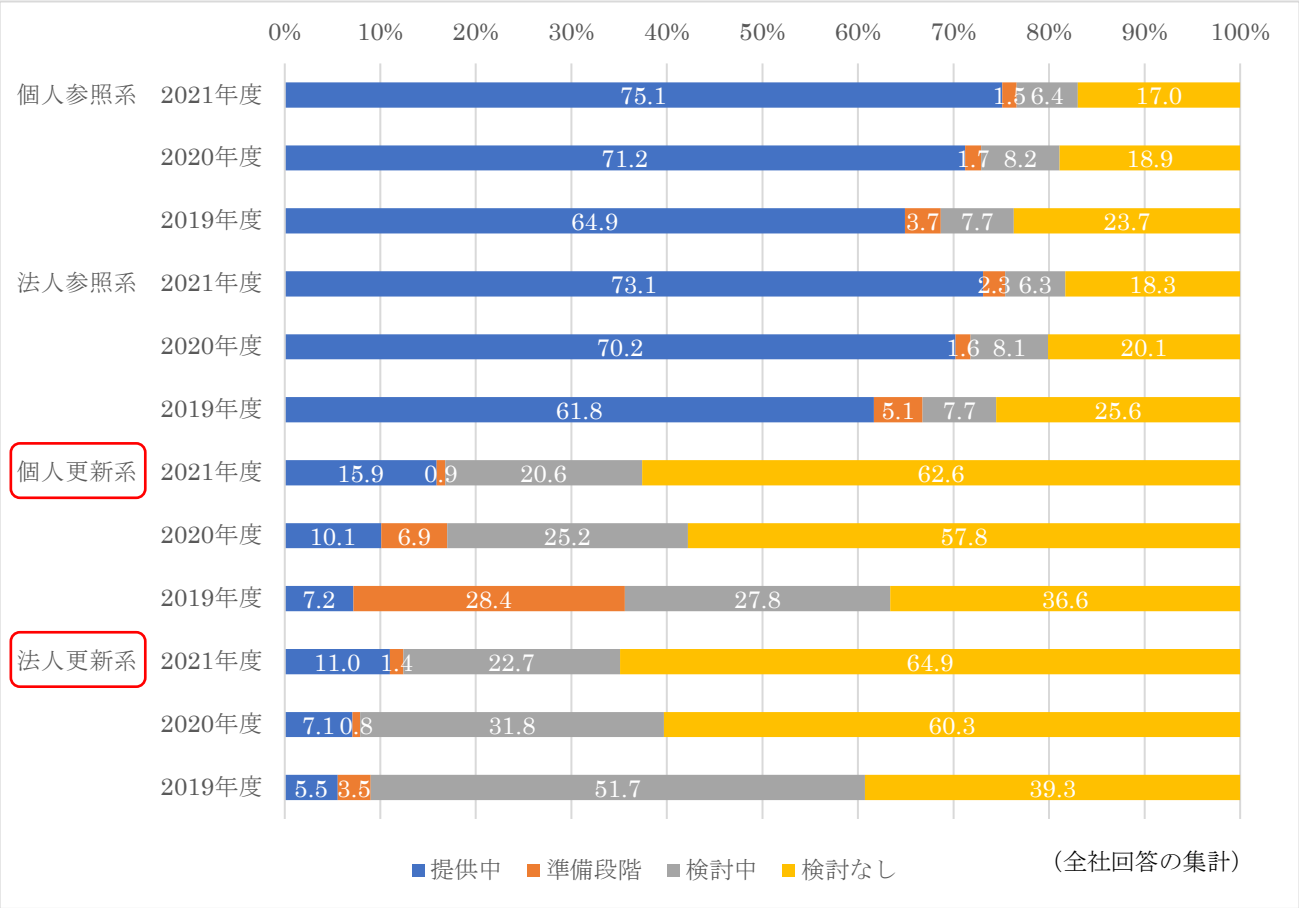
チェックリスト	安全対策基準	主な改訂内容
		2　業務継続の観点から、委託先のテレワーク環境に留意する以下の文言を追加 「なお、いずれも委託先がテレワーク環境により業務を継続することにも留意した指標とする必要がある。」 ＜項番の新設＞ 3　広域災害・感染症の流行等の影響により外部委託先が SLA どおりに委託業務を遂行できない場合の対応策についても、事前に考慮しておくことが望ましい。 具体的な対応策としては、以下の例がある。 (1) 感染症の流行により人との接触削減を求められた場合に備えたテレワークによる業務遂行 ただし、必要に応じて事前に委託先テレワーク環境の技術的安全管理措置を調査し、実現可能性を確認 (2) テレワークで委託業務を遂行できない業務整理を行い、必要に応じた委託契約の見直し
通番 11 クラウドサービス利用にあたってはクラウドサービス固有のリスクを考慮した対策を実施する。	統制基準 24 クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること	＜項番の新設＞ 7　クラウドサービスのアクセス権限に関する仕様変更や金融機関等の誤設定により、クラウド上に保管したデータが漏洩する可能性がある。このため、特定システムにおいてクラウドサービスを利用する場合、金融機関等は、クラウド事業者に対し、クラウドサービスのアクセス権限設定に関する仕様変更が事前に通知されることを確認する必要がある。また、クラウドサービスのアクセス権限設定の仕様変更や金融機関等における設定の変更時には、設定内容の妥当性を確認する必要がある。妥当性の確認においては、専門家によるシステム監査や誤設定の自動検知等の診断サービス等を利用することも有効である。 なお、通常システムにおいては、利用するサービスの内容及びリスク特性等に応じて、これらの対策を実施する必要がある。
通番 22 システムアクセス時の認証を実施する。	実務基準 16 不正アクセスの監視機能を設けること	＜一部内容の追記＞ 1　不正アクセスの監視機能を使用した対策例として、以下を追加 (8) クラウドサービスを利用している場合は、CASB(Cloud Access Security Broker)のコンセプトに基づく製品・ツール等の専用ソフトウェア等により、不正利用を自動監視または早期に検知する。

(6) 更新系 API のサービス提供状況

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。当センターが実施した「令和 4 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 15.9%（前年比＋5.8%）、 法人更新系は 11.0%（同＋3.9%）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〕）。

なお、オープン API のサービスの体制整備状況等については、別添資料「【ご参考】令和 4 年度金融機関アンケート調査結果概要」を参照されたい。

〔図表 2〕オープン API を通じたサービス提供状況



出所：FISC「令和 4 年度金融機関アンケート調査結果」

3 2022 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、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、2022 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