【資料 5】

2023 年 12 月 13 日

2023 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」とする。

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を要望する具体的な意見は寄せられていない。

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、チェックリスト見直しの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している限り、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、2023 年 5 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 11 版」として公表した[1]。第 11 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
通番 1 セキュリティ管理責任の所在と対象範囲を明確にする	統制基準 4 セキュリティ管理体制を整備すること	＜一部内容の追記＞ 1　全社的にセキュリティを統括する責任者（CIO、CISO 等）を明確にし、統一的なセキュリティの統制、管理を行うことが必要である。　CIO、CISO を追記

[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
通番 2 セキュリティ管理ルールを整備する	統制基準 1 システムの安全対策に係る重要事項を定めた規定を整備すること	＜一部内容の追記＞ 1　なお、セキュリティポリシーには、個人情報の取扱い及びその法令遵守に関する内容が盛り込まれていることが必要である。 セキュリティポリシーに盛り込まれるべき内容追加
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ば望ましい　追加 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　追加
	統制基準 14 セキュリティ教育を行うこと	＜一部内容の追記＞ クラウドサービスにおけるセキュリティ教育を実施する際の参考情報を追加
	監査基準 1 システム監査体制を整備すること	＜一部追加＞ 3　クラウド利用の場合の、外部専門機関の活用を追加
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 20 外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること	＜一部内容の追記＞ 3　「機密保持契約」を「秘密保持契約」に修正
	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盟約を締結すること	1　「機密保持に関する契約」を「秘密保持契約」に修正
	統制基準 22 外部委託先の要員にルールを遵守させ、さおの遵守状況を確認すること	4　クラウド事業者の要員に対してルールの遵守情報を確認することを追加
	統制基準 23 外部委託における管理体制を整備し、委託業務の遂行状況を確認すること	3　クラウド事業者に対して業務の遂行状況を確認することを追加（項番の追加）
	監査 1 システム監査体制を整備すること	

チェックリスト	安全対策基準	主な改訂内容
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 監査基準 1 システム監査体制を整備すること	＜一部内容の追記＞ 2　外部委託契約については【統 21】を参照のこと追加 ＜項番追加＞ 3　クラウド事業者がその責任範囲において実施する安全対策についても、統制基準に沿って管理することが基本となるが、その際には実務基準を参考にしながら確認するものの､統制上の管理方法が制約される場合もあり、その場合は第三者保証による報告書等を利用するなどの方策を講ずることが考えられる。そのうち、以下の実務基準については、クラウドサービス固有で対応すべき事項や特に留意すべき事項があるため考慮が必要である。 (1)伝送データの漏えい防止策【実 4】 クラウド事業者におけるデータ伝送時のデータ保護について確認する。確認する経路としては以下の例がある。 ①仮想プライベートクラウド領域内 ②仮想プライベートクラウド領域からクラウドセンター内のアクセスポイントへの経路や、リージョン間の経路 (2)暗号鍵の保護機能【実 13】 暗号鍵を蓄積するディスク等について、物理的なアクセスからの保護や、例外的にアクセスする場合に備えたルールやモニタリング・監査の内容など、機密性の観点での保護対策を確認するとともに、完全性、可用性の観点で確認する。 (3)外部ネットワークからの不正侵入防止策【実 14】 管理インタフェースについて、クラウド事業者が講じている不正侵入防止策を確認する。 (4)不正アクセスの発生に備えた対応策、復旧策【実 19】 クラウド事業者の責任範囲への不正アクセスがクラウド利用者へ与える影響について、影響拡大防止策や、クラウド利用者への報告方法や内容、体制等が整備されていることを確認する。 (5)アクセス権限の付与、見直しの手続き【実 27】 障害事象調査等の過程で、金融機関等の資産に例外的にアクセスする必要が発生した場合に備えた手続きや体制等が明確になっていることを確認する。 (6)データファイルの授受・管理方法【実 28】 ログや設定情報、コンテンツに紐づくメタデータ（投稿者、投稿日時など）等、クラウド利用者が意図せずしてクラウドサービス上で生成されるデータについて明確に特定し、管理方法を定めているか確認する。 (7)ハードウェア・ソフトウェアの管理【実 48】 クラウド事業者が入手した OS やミドルウェアの修正情報、脆弱性情報、障害情報を金融機関等のクラウド利用

チェックリスト	安全対策基準	主な改訂内容
		者に連絡する体制やルールを整備しているか確認する。 (8)障害時・災害時の復旧手段【実 71】 クラウドサービスの提供に直結する外部委託や外部のサービスの利用の有無を確認し、クラウド事業者の障害時手順等で、委託業務が遂行できない場合の対応策が考慮されているか確認する。 (9)システムの廃棄計画・廃棄手順【実 82】 情報が読取不可能となるようにハードウェアの廃棄を行っていることを定期的に確認する。 ＜下記追加＞ 項番を 3 から 4 に変更し、「第三者保証による報告書等は、監査以外に、クラウド事業者の要員に対するルールの遵守状況、及び業務の遂行状況の確認についても利用できるが、詳細については【統 22、統 23】を参照のこと。」と参照先を追加。 ＜下記追加＞ 項番を 4 から 5 に変更し、「通常システムにおいても、定期的に監査を実施することが望ましい。」と通常システムの取扱いを追加。 ＜下記追加＞ 項番を 5 から 6 に変更し、「通常システムにおいても配置することが望ましい。」と通常システムの取扱いを追加。 ＜下記追加＞ 項番を 6 から 7 に変更し、『責任分界点については、「第 2 編Ⅱ.3.(1)クラウドサービスにおいて安全対策を決定するうえでの留意点」を参照のこと。』と参照先を追加。 ＜下記変更＞ 項番を 7 から 8 へ変更。 ＜一部追加＞ 3　クラウド利用の場合の、外部専門機関の活用を追加
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	＜項番追加＞ 4　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の確認事項を追加
通番 22 システムアクセス時の認証を実施する	実務基準 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 実務基準 8 本人確認機能を設ける	＜項番追加＞ 5　クラウド事業者に対して金融機関等で策定したセキュリティ基準の充足を確認することを追加 ＜一部変更＞ 2　確認内容を具体化及び複数の方法を組み合わせることを文中に記載

チェックリスト	安全対策基準	主な改訂内容
	こと 実務基準 16 不正アクセスの監視機能を設けること	 ＜一部追加＞ 1　侵入防御システム（IPS）を追加 　不正アクセスの監視機能を使用した対策例追加
通番 23 システムアクセスとその作業についてのログを保管し、有事の際に調査が可能なようにする	実務基準 10 アクセス履歴を管理すること	＜一部追加＞ 6　ログをバックアップすることを追加 8　クラウド関連 9　クラウド関連 参考 2 アクセス履歴
通番 33 偽アプリケーション対策を実施する	実務基準 142 ＱＲカード決済における安全対策を講ずること	＜一部変更＞ ＵＲＬの変更

3　2023 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、2023 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