「API 接続チェックリスト」の見直し要否に関する委員意見

資料４

１．見直し要否に関する各委員の意見

対応方針（案）の通り見直しを行わない	11 名
見直しを行う	1 名

２．チェックリストに関する見直し意見

	委員	該当箇所	修正案	修正理由	FISC 対応方針・コメント
1	－	－	回答のレベル感について、どの程度詳細記載しないといけないのかの表現例を統一して欲しい。	金融機関との調整において、セキュリティ担当部署等では「そのように定めている」という粗い回答が一次回答となることが多いが、最終的には「XXX 規程第 Y 条 X 項：○○○と規定されており、その内容は社内ポータルサイトにて提示されており、年一度の研修にて周知徹底を実施している」といった、より詳細な記載が必要となる。 回答の期待水準を相互に理解するため、より詳細な記載が求められることを、ひな形上も理解できる調整を要望したい。	【方針】現状のまま ✧　解説書 3.利用にあたっての留意事項等に、 『「フォーマット」はコミュニケーション・ツールとして活用していることを想定しているため、API 接続先と金融機関の双方において、自社のセキュリティ実態を正しく、できるだけ具体的に回答する』と明記されている。
2	－	－	各銀行が独自フォーマットでファイルを送ってくることの廃止。あえて行うのであれば、「FISC チェックリスト＋銀行独自差分」のようにして欲しい。	本要求は昨年のチェックリスト見直しにおいてもお伝えしたが、改善が見られていない。 この状況が変わらない限り、多数のフォーマットに個別回答するという、チェックリスト共通化の目的が果たされない。	【方針】現状のまま（2019 年連絡会にて検討済） ✧　昨年も同様の指摘あり、下記のように整理した。尚、当センターの今後の活動（説明会等）においても、引き続き周知に努める。 『API 接続先が金融機関ごとの独自リストに対応する負担を考慮する必要があり、チェックリストの追加・変更箇所を識別しやすくするなどの配慮が金融機関に求められる。』 2019 年 7 月 26 日開催の連絡会【資料 5（別紙 2)】

３．上記以外の意見

	委員	該当箇所	ご意見	FISC コメント
1	－	通番 20/手法例 3 通番 30/手法例 6	パスワード付き ZIP ファイルは非推奨として欲しい。 パスワード付き ZIP ファイルはウイルススキャンを実行することができず、「通番 20/手法例 3」や「通番 30/手法例 6（注 4）③」の記載と矛盾する。	✧　チェックリストにおいてパスワード付 ZIP ファイルに関する記載はなく、特に推奨もしていない。 また、各金融機関や API 接続先のセキュリティルールに依存するため、一概に非推奨にすることは難しい。
2	－	通番 21 通番 22 通番 32	パスワードの定期変更は非推奨として欲しい。 パスワードの定期変更を求めてくる金融機関があるが、米国 NIST、並びに日本の総務省において、定期的なパスワード変更は「すべきではない」「不要」とされている。	✧　昨年の連絡会においても、安全対策基準（第 9 版改訂）の改訂に伴い、対応を検討したが、予てからチェックリストにおいてパスワードの定期的な変更に関する記載はなく、見直しは不要と整理した。 2019 年 7 月 26 日開催の連絡会【資料 5（別紙 1)】

	委員	該当箇所	意見	FISC コメント
3	－	－	（チェックリストの項目見直しについて） チェックリストの項目の追加・削除の必要はない。現行のチェックリストの内容で、セキュリティ面で必要となる要素の骨格・フレームワークは整っていることと、過去の様々な利害関係の結果として決まった経緯があると理解している。 ただし、この 1 年間で各金融機関・電代業者間の API 接続契約の各場面でチェックリストが実際に活用され、金融機関・電代業者の双方に実務上有益なナレッジが蓄積しているのは事実であり、忘れないうちにその内容を共有する「別の座組み」があっても良いのではないか？と考える。	✧　昨年度も電代業協会と共催で金融機関向けの意見交換会を開催したが、今後も必要に応じ、テーマを定めて「別の座組み」を設けることは検討して行く。
4	－	－	（チェックリストのコミュニケーション・ツールとしての使い方等について） FISC チェックリストにはセキュリティ面で意識すべき内容が列挙されているが、そもそも金融機関・電代業者両者のシステム環境、アプリ・サービス環境（利用している API 基盤ベンダー）がどのようなものを利用しているのか等の技術面の情報があった方が、運用を意識した際には API 稼働後、不具合（不正）発生等の切り分け等初動がよくなるのでよいのではないかと考えている。 これはチェックリスト内に新規項目として入れる必要はないと考えているが、あえて入れるのであれば「API 接続両者のシステム・アプリ・サービス稼働環境を把握」といった形になるのではないか。	✧　左記内容は本来のチェックリストの内容に直接的に関係するものではないが、各確認項目の内容を確認する上で、必要な事項（システム環境など）は関係者間でリスクベースアプローチに基づき、取り決めることが適当であると整理している。
5	－	－	（チェックリストの審査における集合的仕組み、JDD や KPMG による AUP 他について） 現行のチェックリストの本来の目的を超えているが、今後の課題として次のような点を共有したい。 たとえば、昨今のドコモ口座問題のような問題事象について、事前に抑止する、または事後的に対処するといったことも目的に含めるならば、チェックリストによる対応方針等の概要把握だけでは、その目的の達成は当然不可能である。 契約時、開発時、試験時、運用時、などの各ステージで必要なチェックを促すような仕組みが最低限必要であると考えている。特に試験時においては、金融機関から必要なテストケースなどをご提示頂く（このケースが不正利用に対応できていることを示すもの）などは一考してもよいのではないか？ ただし、この方針をそのまま、まともに実施しようとすると、両者で工数が急増することが見込まれ、また API 接続までの時間も多く要することになるため、適切な落としどころはそれぞれの業界で、仮に可能ならば FISC の皆さん、行政意見も考慮しながら進められたらよいのではないかと考える。	✧　参考意見として伺っておく。
6	－	－	電代業者側は、API またはスクレイピング接続対応する金融機関には全てチェックリスト対応を行うことになる。仮に電代業者側から提示する内容（＝チェックリストの記載内容）は同じだとしても、それに対する個別確認・理解合わせの工数は金融機関の数だけ比例的に発生する。 この業務は必要不可欠であるので、我々としては当然対応するが、初回契約後のモニタリングも含めて両者側で意味のあり、なおかつ効率的なやり方を模索したいというのが正直なところである。	✧　チェックリストの審査における集合的仕組み、AUP 等の第三書認証の活用等については、昨年の連絡会における議論を踏まえて「第三者認証や内部統制保証報告書等の活用を積極的に検討する」として、解説書の記載を修正済。また、活用するか否かは、関係者間でリスクベースアプローチに基づき、取り決めることが適当であると整理している。