別　紙

新旧対照表（2019年９月27日）

＜解説書＞

下線部分が改訂箇所

目次	通番	改訂前	改訂後
3. 利用にあたっての留意事項等	―	各金融機関は、効率的なコミュニケーションを行う観点や、API接続先から必要以上に重要な情報を取得しないという観点から、エビデンス等の提出に代え、第三者認証や外部監査による評価の活用を積極的に検討する。	API 接続先は、第三者認証や内部統制保証報告書等を取得していなければならない訳ではない。もっとも、取得している場合には、各金融機関は、効率的なコミュニケーションを行う観点や、API接続先から必要以上に重要な情報を取得しないという観点から、エビデンス等の提出に代え、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。 例えば内部統制保証報告書等であれば、次の確認項目等で活用を検討することが考えられる（通番3、通番8、通番9、通番13、通番14、通番21、通番24、通番27、通番33 等）。
4. 用語解説	―	〈用語〉 ISAE3402 〈説明等〉 国際会計士連盟（IFAC）が定める受託業務に関する内部統制基準で、国際保証業務基準第3402号（International Standard on Assurance Engagements No.3402）の略称。	（左記を削除）
4. 用語解説	―	〈用語〉 SOC1 〈説明等〉 米国公認会計士協会（AICPA）が定める内部統制保証報告の枠組みの一つで、Service Organization Controls 1 Reportsの略称。米国保証業務基準であるSSAE16（2017年5月1日以降はSSAE18）に基づく報告書で、業務を受託した会社の財務諸表に関する内部統制評価に用いられる。	（左記を削除）
4. 用語解説	―	〈用語〉 SSAE16 〈説明等〉 米国公認会計士協会（AICPA）が定める受託業務に関する内部統制基準で、米国保証業務基準書第16号（Statement on Standards for Attestation Engagements No.16）の略称。なお、2016年4月からSSAE18に変更（SSAE16に比べ、再委託先の内部統制モニタリング等が追加）されている。	（左記を削除）
4. 用語解説	―	（右記を追加）	〈用語〉 合意された手続報告書 〈説明等〉 国際監査・保証基準審議会（IAASB）が公表している国際関連サービス基準（ISRS）4400、日本公認会計士協会が定める専門業務実務指針4400に基づく報告書で、事前に関係者間で合意された手続に関する実施結果が報告される（例えば、API接続チェックリストの確認項目の実施を対象とすることが可能）。
6. 確認項目	3	＜第三者認証の利用＞ 1. 提供するサービスや目的に合致した第三者認証を取得（注3）してセキュリティ管理態勢が整備されていることを示すことが考えられるが、第三者認証を取得していなければならない訳ではない。	＜第三者認証、内部統制保証報告書等の利用＞ 1. API接続に関するセキュリティ管理態勢を含めた第三者認証を取得、もしくは、内部統制保証報告書等を入手（注3）してセキュリティ管理態勢が整備されていることを示すことが考えられるが、第三者認証、内部統制保証報告書等を取得していなければならない訳ではない。
		（注3） ① プライバシーマーク、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の認証を取得している。 ② 内部統制保証報告書〔SOC1（SSAE16・ISAE3402）、SOC2、IT委員会実務指針7号〕や情報セキュリティ監査報告書を取得している。 ③ クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証（ISO27017）を取得している。	（注3） ① プライバシーマーク、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の認証を取得している。 ② 内部統制保証報告書（SOC2、IT委員会実務指針7号）や情報セキュリティ監査報告書を取得している。 ③ クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証（ISO27017）を取得している。 ④ 合意された手続報告書を取得している。
6. 確認項目	33	＜アプリケーションの管理＞ 1. スマートデバイスにおけるアプリケーション利用時の顧客保護のため、不正な偽アプリケーションが出回らないよう、必要な対策を実施している。（注1）	＜アプリケーションの管理＞ 1. スマートデバイスにおけるアプリケーション利用時の利用者保護のため、不正な偽アプリケーションが出回らないよう、必要な対策を実施している。（注1）
		（注1） ① アプリ作成時に電子署名を付与する。 ② スマートフォンアプリをリバースエンジニアリングされた場合に備えて、暗号化や難読化等の対策を行う。 ③ アプリ内部に個人情報を保存しない。 ④ アプリ提供サイトのパトロールを実施する。	（注1） ① アプリ作成時に電子署名を付与する。 ② スマートフォンアプリをリバースエンジニアリングされた場合に備えて、暗号化や難読化等の対策を行う。 ③ アプリ内部に個人情報を保存しない。 ④ アプリ提供サイトのパトロールを実施する。 ⑤ QRコード決済を利用する場合、QRコード決済固有のリスクに対する安全対策や利用者保護等の措置を講じる。 関連規定 FISC「安全対策基準」 実務基準 9 個別業務・サービス 実142、実143、実144

＜フォーマット＞

区分	通番	改訂前	改訂後
サービスシステムのセキュリティ機能	33	（右記を追加）	【関連規定】 FISC・安対基準 【関連規定箇所】 実142、実143、実144