Attachment

Old and New Comparison Chart (September 27, 2019)

〈Manual〉

The underlined part is the revised part

Table of contents	Nos.	Before revision	After revision
3. Notes for use	-	To enable efficient communication and ensure that only necessary information is collected from API connection partners, each financial institution may utilize third-party certification or external auditing instead of collecting evidence directly from API connection partners.	API connection partners don't have to obtain third-party certification or internal control attestation report. If API connection partners have acquired it, to enable efficient communication and ensure that only necessary information is collected from API connection partners, each financial institution may utilize third-party certification or internal control attestation report, etc. instead of collecting evidence directly from API connection partners. For example, if it is an internal control attestation report, etc., it is possible to consider the following items to check: Nos. 3, 8, 9, 13, 14, 21, 24, 27, 33, etc..
4. Glossary	-	<Term> ISAE3402 <Description> International Standard on Assurance Engagements No.3402, a set of internal control guidelines on outsourced operations, established by the International Federation of Accountants (IFAC).	(Delete the items on the left)
4. Glossary	-	<Term> SOC1 <Description> Service Organization Controls 1 Reports, a framework for attestation reports on internal control established by the American Institute of Certified Public Accountants (AICPA), or reports based on that framework. SOC1 reports—based on SSAE 16 (superseded by SSAE 18 since May 1, 2017) —are used in the assessment of the internal control at service providers to which operations relevant to user entities' financial statements are outsourced.	(Delete the items on the left)
4. Glossary	-	<Term> SSAE16 <Description> Statement on Standards for Attestation Engagements No. 16, a set of internal control guidelines for service providers' outsourced operations, established by the American Institute of Certified Public Accountants (AICPA). SSAE 16 was superseded by SSAE 18 (which adds to SSAE 16 standards in subjects such as monitoring of internal control of sub-outsourcers) beginning in April 2016.	(Delete the items on the left)
4. Glossary	-	(Added the items on the right)	〈Term> report on applying agreed upon procedures 〈Description> Report on applying agreed upon procedures is based on the International Service Standards (ISRS) 4400 published by the International Auditing and Assurance Standards Board (IAASB) and the Professional Practice Guidelines 4400 established by the Japan Certified Public Accountants Association. It describes the implementation result of the procedures agreed between the parties concerned. For example, items to check in the API connection checklist can be set agreed upon procedures.
6. Items to check	3	[Use of third party certification] 1. A third party certification (Note 3) that meets the nature and purposes of the services that the organization provides may be obtained as a means to prove that governance of security has been established. However, such a certification is not essential.	[Use of third party certification] 1. A third party certification or internal control attestation report (Note 3) that includes security management system for API connection may be obtained as a means to prove that governance of security has been established. However, such it is not essential.
		(Note 3) 1) Certifications of Privacy Mark, ISMS (JIS Q 27001, etc.), and ITSMS (JIS Q 20000-1, etc.) 2) Internal control attestation reports (those based on SOC1 [SSAE 16 and ISAE 3402], SOC2, or IT Committee Practical Guideline No. 7); and information security audit reports 3) CS Mark of the JASA-Cloud Information Security Promotion Alliance; and the ISMS Cloud Security Certification (ISO 27017)	(Note 3) 1) Certifications of Privacy Mark, ISMS (JIS Q 27001, etc.), and ITSMS (JIS Q 20000-1, etc.) 2) Internal control attestation reports (those based on SOC2 or IT Committee Practical Guideline No. 7); and information security audit reports 3) CS Mark of the JASA-Cloud Information Security Promotion Alliance; and the ISMS Cloud Security Certification (ISO 27017) 4) Report on applying agreed upon procedures
6. Items to check	33	[Management of applications] 1. Necessary measures are implemented to prevent distribution of illegal fake applications so that customers using applications on smart devises are protected. (Note 1)	[Management of applications] 1. Necessary measures are implemented to prevent distribution of illegal fake applications so that users using applications on smart devises are protected. (Note 1)
		(Note 1) 1) Electronic signature is given when applications are developed. 2) Implementing countermeasures such as encryption and obfuscation in preparation for the possibility that a smartphone application is reverse engineered. 3) Never saving personal information inside applications. 4) Patrolling application sites.	(Note 1) 1) Electronic signature is given when applications are developed. 2) Implementing countermeasures such as encryption and obfuscation in preparation for the possibility that a smartphone application is reverse engineered. 3) Never saving personal information inside applications. 4) Patrolling application sites. 5) When using QR code payment, take measures such as security measures and user protection for risks inherent in QR code payment. Related rules FISC Security Guidelines Practice Guidelines 9. Individual operations and services P142, P143, P144

〈Format〉

Category	Nos.	Before revision	After revision
Service-system security functions	33	(Added the items on the right)	【Related rules】 FISC Security Guidelines 【Part of related rules】 P142, P143, P144