Disclaimer

April 2019

The API Connection Checklist for Financial Institutions and API Connection Partners (October 2018 Edition) was originally issued in Japanese in October 2018.

This is an unofficial English translation that has not been reviewed by Council of Experts on Open API for Financial Institutions (established by FISC) or any other bodies.

If there are any errors or mistranslations in this English version, please refer to the Japanese original. Only the Japanese original is valid, and the translated texts are to be used solely as reference to understand the Checklist.

FISC does not guarantee that the English translation is accurate, reliable, and based on the latest Japanese version and is not responsible for any consequences resulting from use of the information in this English version.

Secretariat: The Center for Financial Industry Information Systems (FISC)

API Connection Checklist

for Financial Institutions and API Connection Partners

Manual

<October 2018 Edition>

October 12, 2018

Council of Experts on Open API for Financial Institutions
Working Group on API Connection Checklist for Financial Institutions
(Secretariat: The Center for Financial Industry Information Systems)

Acknowledgement

Many people have participated in the translation. The secretariat would like to thank all of the members, especially:

Mr. Masao Oumi
Senior Manager
Digital Strategy Section
Business Strategy Department, Financial Segment
NTT DATA Corporation

API Connection Checklist
for Financial Institutions and API Connection Partners

Manual

Table of contents

1. About API Connection Checklist

1.1. Objectives

An open application programming interface (open API) for financial institutions[1] refers to an API provided by financial institutions to API connection partners. The latter—API connection partners—are permitted access to financial institutions' information systems with customers' consent.[2] To ensure secure data linkage, financial institutions and their API connection partners need to check security-related matters. However, in light of the fact that both sides have multiple counterparties, it is important that this be conducted efficiently.[3]

For this reason, The Center for Financial Industry Information Systems (FISC)—with the cooperation of financial institutions, FinTech companies, IT vendors, and other relevant parties—has developed an API Connection Checklist as a tool for efficient interactive communication in API connections. It is hoped that use of this Checklist by related parties[4] will lead to more widespread use of efficient, secure API connections.

The API Connection Checklist can also be used as a communication tool for follow-up monitoring to be conducted after an API connection has been established.

[1] As used in the API Connection Checklist, "financial institutions" refers to the following types of financial institutions: banks, Shinkin Central Bank, Shinkin Banks (credit unions), The Rokinren Bank, Labour Banks (workers' credit unions), Shinkumi Federation Bank, Shinkumi Banks (credit cooperatives), The Norinchukin Bank, National Federation of Agricultural Cooperative Associations (ZEN-NOH), agricultural cooperatives, National Federation of Fisheries Cooperatives Associations, fisheries cooperatives, and Shoko Chukin Bank.

[2] The report of the Working Group on the Financial System of the Financial System Council titled "Development of Systems for Open Innovation" (issued December 27, 2016) states: "An API (application programming interface) refers to a program that enables parties outside of a bank to connect to the bank's systems and use their functions. Among these, an open API refers to an API provided by the bank to firms such as FinTech companies; those firms are permitted access to the bank's information systems with customers' consent. An open API is a technology that enables secure linkage of data with outside firms, and it is said to be one of the technologies of realizing open innovation."
https://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1.html(in Japanese only)

[3] The report of the Review Committee on Open APIs (secretariat: Japanese Bankers Association) titled "Report of Review Committee on Open APIs: Promoting Open Innovation" (issued July 13, 2017) states: "In order to reduce the screen-related workload for banks and other companies accessing APIs, it is expected that banks will establish an "API Connection Checklist" (provisional name) to use when reviewing the eligibility of third parties."
https://www.zenginkyo.or.jp/fileadmin/res/en/news/news170713.pdf

[4] In case where the existing API Connection Checklist (trial version) (issued June 28, 2017) is already in use, it is desirable that migration to the new API Connection Checklist be completed within about one year.

1.2. Future reviews and updates

To ensure that the API Connection Checklist is useful at all times, FISC will establish a liaison council to review the Checklist annually based on the facts such as those listed below. When important decisions are required, such as when making major revisions to the Checklist, a council of experts or similar body will be convened to deliberate on related matters.

- Usage of the Checklist and user needs
- Incidents occurred related to open API
- Developments in standardization of the open API
- Self-imposed rules of the Japan Association for Financial APIs

When there is a need for warning financial institutions and API connection partners swiftly, in cases such as when incidents have occurred, the FISC secretariat will do so through its Website and other means.

2. Overall structure

The API Connection Checklist consists of (1) API Connection Checklist Manual (hereinafter “Manual”) and (2) API Connection Checklist (Format) (hereinafter “Format”). Each of these is outlined below.

2.1. Manual

The Manual describes the objectives of the Checklist and how to use it, as well as details of individual items to check[5] (e.g., security objectives and examples of methods). It should be read before using the Checklist.

There are 44 items classified into the nine categories as follows.

Chapter	Category	Purpose	Nos.
1	Governance of information and security management	To check whether governance has been established at API connection partners to manage information and ensure security.	1-9
2	Outsourcing management	To check how API connection partners manage outsourcing, if they use it.	10-11
3	Cooperation between financial institutions and API connection partners	To determine the scope of responsibilities to be borne by financial institutions and API connection partners from the viewpoint of protecting users.	12-16
4	Management of computer facilities	To check whether security is ensured regarding facilities of the computer systems with which API connection partners provide services.	17
5	Management of office facilities	To check whether security is ensured regarding the offices in which there is equipment having access to the systems used by API connection partners to provide services.	18-20
6	Management of system development and operations	To check how API connection partners manage system development and operations.	21-28
7	Service-system security functions	To check the security implementation requirements of the systems used by API connection partners to provide services.	29-35
8	API security functions	To check the systems used to manage API access from the viewpoint of protecting users.	36-42
9	Security of API use	To check the accountability to users.	43-44

[5] They refer to items that financial institutions and/or API connection partners are expected to check in order to link data between them in a secure manner.

The following contents are provided for each item to check (see the table below).

(1) Category: One of the nine categories in the table above
(2) Subject party: Party that should implement security measures
(3) Sequential number
(4) Security objectives: Objectives of security measures to be implemented
(5) Description of security objectives: Details of the objectives
(6) Example methods: Examples of security measures
(7) Notes: Additional information on example methods
(8) Related rules: Passages referenced in (a) Japanese Bankers Association (JBA), “Report of Review Committee on Open APIs: Promoting Open Innovation” (issued July 13, 2017) (hereinafter “Report of Review Committee on Open APIs”) and (b) FISC, “FISC Security Guidelines on Computer Systems for Financial Institutions, 9th Edition” (hereinafter “FISC Security Guidelines”)

[Specifications of each item to check]

- The party that should implement security measures is indicated by "✓."
- If "both" is checked (✓), both the API connection partner and the financial institution should implement security measures.

(1) Category
(...)

Indicates the applicable one from the nine categories.

(2) Subject party		
API connection partner	Financial institution	Both
✓		

(3)	(4) (...)

Describes objectives of security measures to be implemented.

(5) (...)
(...)

Describes details of security objectives.

(6) Examples of methods to be adopted are as follows.

[(...)]
1. (...)
2. (...)

[(...)]
1. (...) (Note 1)
2. (...) (Note 2)

- The example methods shown just serve as illustrations.
- API connection partners and financial institutions may cooperate to choose appropriate methods for achieving security objectives in consideration of matters such as the distinctive characteristics and functional risks of the services provided by the API connection partners.

(7) (Note 1)
1) (...)
2) (...)
3) (...)

(Note 2)
1) (...)
2) (...)

Notes provide additional information on example methods.
(No description if not applicable.)

(8) Related rules	... ...

Shows the location(s) referenced in the related rules: JBA, "Report of Review Committee on Open APIs," and FISC, "FISC Security Guidelines."
(No description if not applicable.)

2.2. Format

The Format can be used to enter information such as the current status and issues recognized for each item to check. The Format is intended for use in communication between related parties.

The headings are defined below.

(1) Sequential number
(2) Category: One of the nine categories
(3) Security objectives: Objectives of security measures to be implemented
(4) Subject party: Party that should implement security measures
(5) Current status: Status of security measures that have been implemented by the subject party
(6) Issues to be addressed: Current issues to be addressed by the subject party
(7) Improvement plans: Plans with which the subject party addresses current issues
(8) Related rules: References (JBA, "Report of Review Committee on Open APIs," and FISC, "FISC Security Guidelines")
(9) Part of related rules: Part of reference in (a) JBA, "Report of Review Committee on Open APIs," and (b) FISC, "FISC Security Guidelines"

[Format entry specifications]

(1) No.	(2) Category	(3) Security objectives	(4) Subject party	(5) Current status	(6) Issues to be addressed	(7) Improvement plans	(8) Related rules	(9) Part of related rules	Notes
1	(...)	(...)						(...)	
2	(...)	(...)						(...)	
3	(...)	(...)	(...)				(...)	(...)	
4	(...)	(...)	(...)				(...)	(...)	
5	(...)	(...)	(...)				(...)	(...)	

(5) [Current status]
Describes the current status of measures implemented by the subject party vis-a-vis the security objectives.

(6) [Issues to be addressed]
Describes current issues to be addressed by the subject party.

(7) [Improvement plans]
Describes plans with which the subject party addresses current issues.

3. Notes for use

The following matters must be noted when using the Manual and the Format.

Items to check

- A wide range of items to check is provided, especially those related to maintenance of confidentiality. However, it should be noted that all items may not be covered that individual financial institutions need to check.

- The subject party for each item to check refers to the party that should implement security measures (i.e., those who should fill out the Format). There are three types of entries: API connection partners, financial institutions, and both. Items in the type "both" are implemented jointly by API connection partners and financial institutions (both parties should make entries to the Format).

- If there is a need to check items other than those contained in the Format, each financial institution may add items to check in light of matters such as the distinctive characteristics and functional risks of the services provided by an API connection partner. Similarly, if some items are considered unnecessary, each financial institution may exclude them from the Format (i.e., the so-called "risk-based approach" is employed).

- 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.

Example methods

- The example methods shown in the Manual just serve as illustrations. API connection partners and financial institutions may cooperate to choose adequate methods for achieving security objectives in consideration of matters such as the distinctive characteristics and functional risks of the services provided by the API connection partners.

Entries and decisions on API connection

- Since the Format is intended to be a communication tool, both API connection partners and financial institutions should make entries as specifically as possible and describe the state of their own security accurately.

- In the initial eligibility examination, if the API connection candidate provides the financial institution in advance with information such as that in the "Current status" field in the Format, this is likely to lessen the burden on both parties.

- It is not satisfactory for financial institutions just to receive the Format and know whether their API connection partners have implemented measures or not. Financial institutions should use the “Current status” field and others to strive to hold a close dialogue with API connection partners.

- A financial institution should determine whether or not to establish an API connection based on consideration of matters such as the distinctive characteristics and functional risks of the services provided by the API connection candidate, even if the candidate has not addressed one or more of the items to check shown on the Format.

Use in follow-up monitoring

- It would be appropriate that the API connection partner and the financial institution decide together on the frequency of follow-up monitoring. Examples of the frequency include (1) every fiscal year and (2) at the time when there has been a change in the items to check.[6]

- It would be appropriate for matters such as the methods and extent of follow-up monitoring be decided on by both the API connection partner and the financial institution together.

[6] The report of the Review Committee on Open APIs (secretariat: Japanese Bankers Association), “Report of Review Committee on Open APIs: Promoting Open Innovation” (issued July 13, 2017), states: ”Even after API access is provided, it is necessary for banks to verify the information security-related eligibility of third parties, either on a periodic or an as-needed basis.” https://www.zenginkyo.or.jp/fileadmin/res/en/news/news170713.pdf

4. Glossary

Major terms[7] used in the Checklist are described below.

Term	Page(s)	Description
API connection partner	32, 33, 37, 39, 40, 42, 78, 79, 80, 81, 84	A FinTech company orother type of business connecting with a financial institution through an API connection.
CS Mark	27	Cloud Security Mark, a mark awarded by the Cloud Information Security Promotion Alliance to cloud service provides whose cloud information security statements have been confirmed to be eligible through cloud information security auditing as specified by the Japan Information Security Audit Association (JASA).
CVSS	62	Common Vulnerability Scoring System, a general-purpose method of assessment of vulnerabilities in information systems. The method can be applied to the products of any vendors.
DBMS	68, 75	Database Management System, a system that is used to operate and manage a database and is necessary for setting it up.
DMZ	59	Demilitarized Zone, a network zone that is established in between external and internal networks, segregated by devices such as firewalls, in a network connected to the Internet or other external networks.
FTP	62	File Transfer Protocol, a protocol used to transfer files between specific computers.
IDS	59, 60	Intrusion Detection System, a system that (1) monitors communications with the outside, (2) detects attacks, intrusions, or other types of unauthorized access to internal networks or servers, and (3) notifies administrators.
IPS	59, 60	Intrusion Prevention System, a system that (1) monitors communications with the outside, (2) detects attacks, intrusions, or other types of unauthorized access to internal networks or servers, and (3) prevents them.

[7] This glossary mainly covers the major technical terms used in the example methods and notes for items to check.

Term	Page(s)	Description
ISAE 3402	27	International Standard on Assurance Engagements No.3402, a set of internal control guidelines on outsourced operations, established by the International Federation of Accountants (IFAC).
ISMS	27	Information Security Management System, a framework for ensuring security of corporate information assets.
ISMS Cloud Security Certification	27	Certification that is granted to an ISMS conforming to the JIS Q27001 standard if it has implemented certain management measures specific to the provision/use of cloud services covered by the said standard.
ISO 27017	27	An international standard of the International Organization for Standardization (ISO), establishing standards for the establishment, implementation, maintenance, and continuous improvement of ISMSs that cover provision/use of cloud services.
ITSMS	27	IT Service Management System, a framework for efficient and effective management and provision of IT services by service providers.
JC3	59, 77, 80	The Japan Cybercrime Control Center, a center intended to (1) identify, mitigate, and disable the sources of cybercrimes and other threats in cyberspace and (2) take action to prevent future cases. Experiences of industry, academics, and legal enforcement agencies are put together and analysed, and the results are shared to observe developments in cyberspace as a whole.
JIS Q 20000-1	27	A standard based on the international standard ISO 20000-1, establishing standards for planning, establishment, operation, monitoring, review, maintenance, and improvement of ITSMSs.
JIS Q 27001	27	A standard based on the international standard ISO 27001, establishing standards for establishment, implementation, maintenance, and continuous improvement of ISMSs.

Term	Page(s)	Description
JPCERT	59, 77, 80	The Japan Computer Emergency Response Team coordination center, which, from the technical viewpoint, handles the following tasks regarding computer security incidents such as intrusions and denial-of-service attacks made via the Internet: (1) receiving reports from Website operators in Japan, (2) providing support for their response to the incidents, (3) ascertaining the conditions under which they occurred, (4) analyzing the modus operandi, and (5) finding and advising countermeasures to prevent the reoccurrence of the incidents.
MTP	47	Media Transfer Protocol, a protocol for transfer of media files such as audio and video files between PCs and smartphones, digital audio players, and other devices connected by USB cables.
NFS	62	Network File System, a system for sharing files via networks.
OAuth 2.0	76, 77, 81	A set of standard specifications for API access authorization. It was formulated by the OAuth Working Group of the Internet Engineering Task Force (IETF: a standardization agency for Internet technologies) and is described in the document named Request for Comments (RFC) 6749 published by the IETF.
OS command injection	62	An attack that abuses Web application vulnerabilities to execute unauthorized OS commands.
rexec	62	A program that makes it possible to execute programs on another computer via a network.
RFS	62	Remote File System, a file system on another computer connected to a network.
rlogin	62	A program that makes it possible to log in to a remote server via a network.
rsh	62	Remote shell, a program that makes it possible to operate a shell on another computer via a network.
SMTP	62	Simple Mail Transfer Protocol, a protocol for transfer of email.

Term	Page(s)	Description
SOC1	27	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.
SOC2	27	Service Organization Controls 2 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. SOC2 reports—based on Attestation Standard Section 101 (AT101)—are used in the assessment of the internal control relevant to security, availability, processing integrity, confidentiality, and privacy at service providers to which operations are outsourced.
SQL injection	62	An attack intended to abuse Web application vulnerabilities and make unauthorized data alteration by executing Structured Query Language (SQL: a language used to operate databases) commands.
SSAE 16	27	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.
TELNET	62	Teletype Network, a protocol used to operate a device connected to a remote network via the Internet or other types of connections.
URI	77	Uniform Resource Identifier, a standard defining data formats for unique identifiers for information, services, devices, and other resources.
application site	72	A Website operated by a business such as an OS vendor and a mobile telecommunications carrier to distribute safe, secure applications.
buffer overflow	62	A system error in which data is entered in excess of the storage area secured in computer memory as a result of a program bug.

Term	Page(s)	Description
chain connection partner	32	A sub-outsourcer providing electronic payment services, pursuant to the provisions of Article 34-64, No. 9, Paragraph 3 of the Ordinance for Enforcement of the Banking Act. Cases such as (1) outsourcing of services for depositors at the second level or subsequent levels or (2) outsourcing to connected businesses at the second level or subsequent levels is regarded as sub-outsourcing of electronic payment services. Cases that do not involve outsourcing of services for depositors (even if they do involve outsourcing at the second level or subsequent levels) are not considered as those of chain connection partners.
check digits	67	Numerical values and codes assigned through pre-established calculation procedures to detect numerical errors and prevent forgery.
cloud service	37, 42	IT service based on cloud computing, which is defined by the U.S. National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Generally available in a wide range of forms, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
computer resource	44	The hardware and networks needed to operate computer systems.
confidential information	30, 64, 66, 67	Information to be treated as confidential, such as personal identification numbers, passwords, credit card numbers, and biometric authentication information.

Term	Page(s)	Description
control-target cloud bases	37	Facilities where data are effectively accessed and that should be subject to control by API connection partners. Such facilities should be identified in light of the geographical dispersion of information processing sites in cloud services. Candidates for such facilities include—but are not limited to—data centers, operation centers, headquarters, and branch offices of cloud service providers. The facilities should be identified individually by API connection partners in light of considerations such as the contents of cloud services used and the state of internal management by the cloud service providers.
executives and employees	22, 26, 27, 29, 44, 51, 53	All executives and employees of a company.
Financial ISAC	59, 77, 80	The Financial Information Sharing and Analysis Center, established to coordinate activities of financial institutions in Japan to share and analyze cyber security information and improve the level of security. Its ultimate objective is to continue to make users feel secure.
hashing	68	Converting a source data to a hash value of a fixed length (a unique text string of the same length) by calculation using a hash algorithm.
important information	46, 47, 48, 66, 67, 84	Information that may have a major impact on stakeholders if it is leaked out, such as confidential information and other types of customer information.
information assets	22, 23, 24, 26, 27, 28, 29, 30, 44, 46, 47, 48, 51, 52, 53, 56, 66, 68	A certain amount of valuable information collected by an enterprise in the process of doing business; and the equipment used to collect, process, store, and otherwise handle such information.
information security audit report	27	A report in which an auditor—from an independent, expert standpoint—expresses opinions and results of its verification or evaluation of (1) the audited organization’s governance on management of information security and (2) its controls of risks.
internal control attestation report	27	A report in which a certified public accountant or an audit firm expresses the results of and opinions on assessment of internal control at outsourced companies or other service providers.

Term	Page(s)	Description
IT Committee Practical Guidance No. 7	27	A guidance established by the Japanese Institute of Certified Public Accountants (JICPA) for auditing and other operations handled by certified public accountants, especially relating to their attestation engagements in which they verify outsourcers' internal control on security, availability, integrity, and confidentiality and prepare reports for use by their clients.
list-based attack	71	An attack that involves attempts at unauthorized login using a prepared list of sets of IDs and passwords.
mount	75	To connect an external device to a computer and make it usable.
multi-factor authentication	54	A method of authenticating user identity through combination of two or more of multiple factors such as knowledge information (e.g., a password), information in the user's possession (e.g., a one-time password), and biometric information (e.g., a fingerprint); also known as "two-factor authentication" when using two factors.
operation job	55	Processing of periodic execution of programs on a computer.
Privacy Mark	27	A registered trademark of the Japan Institute for Promotion of Digital Economy (JIPDEC). It authorizes businesses that safeguard their clients' personal information appropriately in conformity with JIS Q15001 (Personal information protection management systems—Requirements), a Japanese Industrial Standard established under the Industrial Standardization Act.
registry	47	A database that stores information on various hardware and software settings on a computer.
repository	58	A database that stores information used in application development such as system design information, programs, and data.
reverse proxy	60	A server that relays messages from external sources and performs various functions, such as data encryption and decryption and data compression, as a proxy for a specific server.
security incident	31, 56, 70, 74	A security-related incident at an organization. It could result in loss of society's trust.
shell	54, 66	A program with which users on input/output devices can input/output information to/from a computer.

Term	Page(s)	Description
social login	71	An authentication method that uses social media accounts (such as Facebook accounts) to authenticate user identity.
source code	57, 58	A text string described using languages or data formats easy for humans to understand and describe.
stateful inspection	59	A function with which (1) network status is monitored and recorded and (2) communications are permitted or blocked in light of conditions such as their contents and directions.
token	48, 54, 70, 76, 77, 81, 83, 84	A text string issued by the API provider (financial institution) to the API connection partner in an API connection. It is used for purposes such as (1) proving that user authentication has already been done and (2) limiting types of API execution.
tool-based	62	A method of using software functions instead of manual operations.
unmount	75	To make it possible to remove safely an external device connected to a computer.
user	30, 33, 40, 41, 42, 43, 55, 70, 71, 74, 75, 77, 78, 79, 82, 83, 84	A party that has concluded a usage agreement with an API connection partner, consenting to the terms of use of services provided by the API connection partner concerned.

5. List of items to check

Category	Nos.	Security objectives	Subject party
Governance of information and security management	1	Make clear who is responsible for what regarding security management.	API connection partner
	2	Establish security management rules.	API connection partner
	3	Establish firmly governance of security management through means including (1) ensuring that all executives and employees thoroughly understand information management methods and (2) doing follow-up monitoring.	API connection partner
	4	Manage information assets.	API connection partner
	5	Implement measures to prevent misconduct by executives and employees.	API connection partner
	6	Prevent leakage of information from devices and other equipment when the organization’s services are terminated or systems are disposed of.	API connection partner
	7	Implement review and countermeasures in the event of a security incident.	API connection partner
	8	Ensure security in chain connections.	API connection partner
	9	Prepare for incidents such as unauthorized access and system failures.	Both
Outsourcing management	10	Implement measures as necessary to ensure effective and proper execution of outsourced operations.	API connection partner
	11	Implement measures in light of risks specific to cloud services when using them.	API connection partner
Cooperation between financial institutions and API connection partners	12	Review and improve security measures.	Both
	13	Implement appropriate responses to requests, inquiries, and other contacts from users.	Both
	14	Prevent spread of damage to users.	Both
	15	Compensate users appropriately when needed.	Both

Category	Nos.	Security objectives	Subject party
Cooperation between financial institutions and API connection partners	16	Operate contact points for user compensation properly.	Both
Management of computer facilities	17	Implement countermeasures against information leakage from computer facilities.	API connection partner
Management of office facilities	18	Prevent entry of unauthorized persons and restrict access to important information.	API connection partner
	19	Prevent persons involved from taking information out of the premises.	API connection partner
	20	Prevent attacks such as intrusions to internal systems through infection with computer viruses.	API connection partner
Management of system development and operations	21	Prevent unauthorized access to information assets from within.	API connection partner
	22	Implement authentication on system access.	API connection partner
	23	Maintain logs of access to and use of systems to enable investigation in the event of incidents.	API connection partner
	24	Implement countermeasures to prevent misconduct by operators.	API connection partner
	25	Implement measures as necessary to prevent marked deterioration in quality when making changes to systems.	API connection partner
	26	Implement countermeasures against unauthorized access from the outside.	API connection partner
	27	Implement countermeasures against vulnerabilities in systems and networks.	API connection partner
	28	Manage confidential information taken out of the premises.	API connection partner
Service-system security functions	29	Implement management measures suited to the types and contents of data.	API connection partner

Category	Nos.	Security objectives	Subject party
Service-system security functions	30	Implement countermeasures against leakage of confidential information.	API connection partner
	31	Enable restoration of lost or damaged information.	API connection partner
	32	Develop authentication functions to protect users.	API connection partner
	33	Implement countermeasures against fake applications.	API connection partner
	34	Keep the spread of damage from unauthorized access to a minimum.	Both
	35	Enable tracing in the event of unauthorized access.	Both
API security functions	36	Implement countermeasures against leakage of confidential information related to authentication and authorization.	API connection partner
	37	Prevent unexpected usage of API.	API connection partner
	38	Ensure that user accounts are not used to establish API connection without the user's knowledge.	Financial institution
	39	Realize the strength of authentication that strikes a suitable balance between user convenience and user protection suited to the risk involved.	Financial institution
	40	Implement multilayered protection against attacks targeting vulnerabilities.	Financial institution
	41	Reduce the risk of misuse of authentication as much as possible	Financial institution
	42	Protect users through the overall strength of authentication, including the strength maintained by API connection partners.	Financial institution
Security of API use	43	Ensure accountability to users regarding their API use.	API connection partner
	44	Prevent user misconceptions and misunderstandings regarding API connections.	Financial institution

6. Items to Check

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

1	Make clear who is responsible for what regarding security management.

Appoint persons responsible for security management and define their job scope so that appropriate security measures are implemented.

Examples of methods to be adopted are as follows.

[Appointment of responsible persons]

1. A chief officer responsible for security management is appointed, and the job scope of security management is grasped.
2. Persons responsible for operations related to security management of information assets are appointed.
3. Persons responsible for information asset management are appointed in the department that handles information assets.

[Duties of chief officer and other responsible persons]

1. The chief officer responsible for security management implements various measures for information management. (Note 1)
2. Persons responsible for security management in the department that administrates API services implement various measures for information management. (Note 2)

(Note 1)

1) Approving, and familiarizing executives and employees with, (1) rules on security management of information assets and (2) criteria for selecting outsourcing companies.
2) Appointing (1) persons responsible for security management and (2) administrators of data used for identification of information-asset users.
3) Receiving reports from persons responsible for security management and giving them advice and guidance.
4) Planning education and training for security management of information assets.
5) Dealing with matters related to security management of information assets in general within the organization.

(Note 2)

1) Managing assignment and change of persons handling information assets.
2) Approving applications for use of information assets, and maintaining records of such applications.
3) Designating and changing locations for storing media that contain information assets.
4) Maintaining (1) records on settings and changes of classification of information assets and (2) those on authority to access them.
5) Understanding how information assets are handled.
6) Checking how information assets are handled by outsourcing companies.
7) Conducting education and training for security management of information assets.
8) Making reports to the chief officer for security management.
9) Dealing with matters related to security management of information assets in the department concerned.

Related rules	FISC Security Guidelines Control Guidelines 1. Internal control C4, C6, C7, C8

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

2	Establish security management rules.

Establish policies and rules on security management so that governance of security management continues to be ensured.

Examples of methods to be adopted are as follows.

[Preparation of documents related to security]

1. A basic policy and handling rules on security management of information assets are established. (Note 1)
2. Regular reviews and revisions are done with regard to rules on security management, inspection, and auditing of information assets.

[Establishment of access management rules]

1. A data manager is assigned; persons who can access customer information are specified; and a framework and rules of access management are established.

(Note 1)

1) Establishing a basic policy that includes the following.
   a. Name of organization
   b. Service office for handling inquiries and complaints on security management measures
   c. Oath of security management
   d. Oath of continuous improvement of the basic policy
   e. Oath of compliance with relevant laws and regulations
2) Establishing handling rules for each of the following data management stage.
   a. Acquisition and input
   b. Processing and use
   c. Saving and storage
   d. Transfer and transmission
   e. Erasure and disposal
   f. Response to incidents such as data leakage
3) Establishing rules on inspection and auditing of information-asset handling.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.1 Eligibility of Third Parties d FISC Security Guidelines Control Guidelines 1. Internal control C1, C12

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

3	Establish firmly governance of security management through means including (1) ensuring that all executives and employees thoroughly understand information management methods and (2) doing follow-up monitoring.

Conduct security education for executives and employees and monitor the compliance status regularly so that governance of security management is ensured across the organization.

Examples of methods to be adopted are as follows.

[Familiarization and raised awareness]

1. Executives and employees are informed and reminded of implementation of security management.

[Education and training]

1. Executives and employees are properly informed of security management measures, educated, and trained. (Note 1)

[Establishment of governance]

1. Governance as well as practice is established in accordance with handling rules on security management of information assets.
2. Information management rules are established for the services that the organization provides, and the rules are observed.

[Evidence to prove that great importance is attached to security]

1. To cultivate organization culture, executives and employees continually conduct discussions, taking into account security issues as well. Contents of the discussions are presented as evidence.
2. Security management is conducted on the basis of self-regulatory guidelines, if they are formulated by the industry association, and evidence is presented that the organization concerned got guidance and training given by the association.

[Monitoring]

1. It is regularly checked whether security management rules are observed, and practice is improved if necessary.
2. The department handling information assets establishes a self-inspection arrangement and checks whether or not rules are observed.
3. The compliance with handling rules is recorded and checked.

[Auditing]

1. There is a framework for audit that is performed by persons from the outside of the department to be audited. The audits are conducted to check whether or not rules have been correctly observed. (Note 2)

[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.

(Note 1)

1) Providing executives and employees with (1) education at the time of recruitment and (2) regular education and training for them.
2) Conducting training on handling information assets.
3) Notifying executives and employees of disciplinary actions in case of violation of working rules for security management of information assets.
4) Conducting evaluation and regular review of education and training for executives and employees.

(Note 2)

1) Appointing (1) a person responsible for audit and (2) persons performing audits, both from the outside of the department handling information assets.
2) Making auditing ready by developing an audit plan.
3) Conducting audits regularly and on an ad hoc basis.
4) Making improvements if violation of rules is found as a result of an audit.

(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)

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.1 Eligibility of Third Parties d 3.3.3 Countermeasures for Internal Unauthorized Access e FISC Security Guidelines Control Guidelines 1. Internal control C13, C14 Audit Guidelines 1. System auditing A1

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

4	Manage information assets.

Manage information assets in preparation for possible information leakage, so that in an emergency the scope of the impact is quickly grasped and appropriate measures can be taken.

Examples of methods to be adopted are as follows.

[Records of information assets]
1. Records of information assets are kept in the book. (Note 1)

(Note 1)
Examples of items to be recorded include the following.
1) Acquired item
2) Purpose of use
3) Location, method, and term of storage
4) Department in charge
5) Access control status

Related rules	JBA "Report of Review Committee on Open APIs" 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

5	Implement measures to prevent misconduct by executives and employees.

Implement measures to prevent misconduct by executives and employees so that, for example, information will not be taken out from the organization without permission.

Examples of methods to be adopted are as follows.

[Measures against misconduct by executives and employees]

1. Non-disclosure contracts are concluded with executives and employees at the time of recruitment or other occasions. (Note 1)
2. Working rules stipulate (1) executives' and employees' roles in, and responsibilities for, handling information assets and (2) disciplinary actions against executives and employees in case of violation of non-disclosure contracts.

(Note 1)

1) When concluding non-disclosure contracts (covering the duty to preserve the confidentiality of secrets learned in the course of business), the details of the contracts including the following are fully explained.
   a. Provisions of liability in case of violating non-disclosure obligations
   b. Provisions of compliance with non-disclosure obligations after the executives and employees leave the organization
2) If staff from a temporary staffing agency are engaged, their confidentiality obligations are stipulated in the contract, memorandum, or written pledge (electronic means may also be eligible).

Related rules	JBA "Report of Review Committee on Open APIs" 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access c

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

6	Prevent leakage of information from devices and other equipment when the organization’s services are terminated or systems are disposed of.

Implement measures such as erasing information stored in equipment so that information leakage is prevented after termination of the organization’s services or systems disposal.

Examples of methods to be adopted are as follows.

[Return and erasure of data on service termination]

1. It is made clear (1) whether or not data are returned when services are terminated and (2) how they are returned (if applicable). (Note 1)
2. The following is prearranged in preparation for service termination: (1) whether data are erased (and when, if applicable); (2) whether storage media are disposed of (and when, if applicable); (3) how data owned by the user are erased; and (4) whether a third party confirms that data have been entirely erased.

[Plan for disposal of information assets]

1. A plan for disposing of information assets is arranged. (Note 2)

(Note 1)

1) Completely erasing confidential information.
2) Exercising the right of audit to confirm data disposal.
3) Making clear a procedure for disposing of information systems.

(Note 2)

1) Purpose of disposal
2) Scope of data to be disposed of
3) Timing of disposal
4) Procedure of disposal
5) How to dispose of assets recorded on the balance sheet

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

7	Implement review and countermeasures in the event of a security incident.

Analyze the cause of the incident and implement necessary measures so that reoccurrence of such an incident is avoided.

Examples of methods to be adopted are as follows.

[Response to incidents]

1. Information on security incidents that occurred in the past and responses to them are recorded and stored.
2. For serious incidents, third parties evaluate (1) the validity of measures taken, (2) the extent of improvements, and (3) control processes.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.1 Eligibility of Third Parties b

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
✓		

8	Ensure security in chain connections.

Implement measures to ensure security at a chain connection partner, so that no security incidents will occur at such a connection partner.

Examples of methods to be adopted are as follows.

[Security measures at chain connection partners]

1. Contracts between API connection partners and their chain connection partners are concluded based on concrete security measures to be implemented by chain connection partners.
2. It is fully grasped what security measures are implemented at chain connection partners.
3. Necessary actions (such as seeking improvements) are taken if it is found that a chain connection partner has not implemented security measures decided jointly by the API connection partner and its chain connection partner.

Category
Governance of information and security management

Subject party		
API connection partner	Financial institution	Both
		✓

9	Prepare for incidents such as unauthorized access and system failures.

Prepare for incidents such as unauthorized access and system failures so that appropriate action can be taken in such incidents.

Examples of methods to be adopted are as follows.

[Readiness to take action in case of unauthorized access (including cases of information leakage)]

1. Necessary responses to unauthorized access are prearranged and are made clear. (Note 1)
2. Rules for communication with the counterparty’s relevant departments and in-house reporting are established. (Note 2)
3. An organizational framework is established in advance to be able to investigate the cause and influence of information leakage triggered by unauthorized access.
4. An organizational framework is established to discuss preventive measures and follow-ups.

[Preparation for communication in system failures]

1. A contact network for emergencies is established in preparation for system failures.
2. The contact network for emergencies is updated regularly.

(Note 1)

1) Making communication tools available in advance to issue the alert.
2) Prearranging how to identify users in trouble and share relevant information between the financial institution and its API connection partner.
3) Deciding in advance how to contact the persons to be involved (and also who should be contacted).
4) Confirming the scope of countermeasures for preventing the spread of damage.
5) Deciding in advance how to inform users.

(Note 2)
Examples of the persons to be contacted at a financial institution and in external organizations:

1) Operators and managers at data centers
2) System-related personnel and managers other than 1) above
3) Persons in charge in computer manufacturers and companies of facilities such as UPS
4) Managers responsible for communication with the headquarters and branch offices
5) Managers responsible for communication with external shared systems (Zengin Center, Integrated ATM System, Joint CMS, etc.)
6) PR manager
7) Responsible managers in the headquarters and branch offices
8) Managers responsible for communication with data centers
9) Persons in charge of maintenance at a manufacturer, etc.
10) Physical security companies

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.4 Handling Unauthorized Access When It Occurs c

Category
Outsourcing management

Subject party		
API connection partner	Financial institution	Both
✓		

10	Implement measures as necessary to ensure effective and proper execution of outsourced operations.

Implement necessary measures so that outsourced operations (including use of cloud services)[8] are performed efficiently and properly.

Examples of methods to be adopted are as follows.

[Selection of service providers]
1. Criteria for selecting outsourcing service providers are established.
2. Rules on outsourcing are prepared.
3. Rule-based assessment of candidate service providers are conducted. The responsible manager gives approval to the selection results.

[Conclusion of outsourcing contract]
1. Non-disclosure agreements and/or service level agreements are concluded as necessary so that outsourced operations are performed safely.

[Checking of outsourced operations]
1. It is grasped how outsourcing service providers manage their operations. (Note 1)
2. Audit of operations at outsourcing service providers is carried out.
3. Regular check of operations at outsourcing service providers is carried out.

(Note 1)
1) Holding interviews with responsible managers.
2) Receiving regular reports on the situation of outsourced operations.
3) Receiving a report on the situation of security control.
4) Receiving a report on changes in important matters related to outsourced operations at outsourcing service providers.
5) Receiving a report on incidents and crimes related to security.

[8] Outsourcing here includes not only the cases where financial institutions or API connection partners have subcontract agreements with IT vendors (typically cases of system development and system operation), but also the cases where they do not necessarily have such agreements with IT vendors (typically use of cloud services).

Related rules	FISC Security Guidelines Control Guidelines 2. External control C20, C21, C22, C23 Audit Guidelines 1. System auditing A1

Category
Outsourcing management

Subject party		
API connection partner	Financial institution	Both
✓		

11	Implement measures in light of risks specific to cloud services when using them.

Implement necessary measures in light of the matters such as contents of the organization’s own services and risks specific to cloud services, when using cloud services.

Examples of methods to be adopted are as follows.

[Selection of cloud service providers]

1. The location of control-target cloud bases (facilities of a cloud service provider that are subject to control by API connection partners) is grasped when selecting a cloud service provider (if this is considered necessary in light of service contents and risk profiles).
2. It is confirmed that control-target cloud bases are located in areas where effective control is possible.
3. When starting using cloud services, decision is made, by using a checklist or other tools, whether the service provider is eligible.

[Conclusion of contract]

1. In the contract or agreement with the cloud service provider, there are provisions of the rights to take action on control-target cloud bases (e.g., to conduct audits) so that such rights are reserved (if this is considered necessary in light of service contents and risk profiles).
2. When negotiating a contract, the explanatory paper on the services issued by the service provider (white paper) is checked.

[Check of subcontracted operations]

1. An attestation engagement report is received from the cloud service provider, and its contents are checked (if this is considered necessary in light of service contents and risk profiles).
2. The responsible manager in the organization is informed of check results regarding the attestation engagement report.
3. In conducting audits of the cloud service provider, the attestation engagement report obtained and submitted by the service provider is used in consideration of advanced technologies adopted.
4. In relation to the organization’s services, risks associated with cloud services are recognized.

Related rules	FISC Security Guidelines Control Guidelines 2. External control C24 Audit Guidelines 1. System auditing A1

Category
Cooperation between financial institutions and API connection partners

Subject party		
API connection partner	Financial institution	Both
		✓

12	Review and improve security measures.

Review and improve security measures to prevent security incidents caused by new types of modi operandi.

Examples of methods to be adopted are as follows.

[Strengthening of cooperation]

1. Cooperation between the financial institution and the API connection partner is ensured to make it possible to review, improve, and sophisticate security measures.
2. External and internal threats that the organization may face are specified, and rules to record cyber incidents are established.

Related rules	JBA "Report of Review Committee on Open APIs" 3.3 Security Principles 3.3.4 Handling Unauthorized Access When It Occurs c

Category
Cooperation between financial institutions and API connection partners

Subject party		
API connection partner	Financial institution	Both
		✓

13	Implement appropriate responses to requests, inquiries, and other contacts from users.

Respond properly, from a viewpoint of user protection, to contacts from users such as requests, inquiries, complaints, and other contacts.

Examples of methods to be adopted are as follows.

[Response to contacts from users]

1. The division of roles between the financial institution and the API connection partner and within the organizations, as well as the workflow, is prearranged for contacts from users.

[Disclosure of contact information to users]

1. Contact information is disclosed to users for their contacts.

Related rules	JBA “Report of Review Committee on Open APIs” 3.4 User Protection Principles 3.4.2 Explaining/Displaying Information and Obtaining Consent i, j

Category
Cooperation between financial institutions and API connection partners

Subject party		
API connection partner	Financial institution	Both
		✓

14	Prevent spread of damage to users.

Implement necessary measures to prevent spread of damage to users.

Examples of methods to be adopted are as follows.

[Establishment of ways to communicate to users]

1. In order to prevent spread of damage, ways to communicate with users (Note 1) are established in advance.

(Note 1)
1) E-mail
2) Telephone
3) Website
4) SNS

Related rules	JBA “Report of Review Committee on Open APIs” 3.4 User Protection Principles 3.4.4 Actively Preventing Incidence and Spread of Damages d

Category
Cooperation between financial institutions and API connection partners

Subject party		
API connection partner	Financial institution	Both
		✓

15	Compensate users appropriately when needed.

Compensate users appropriately from a viewpoint of user protection, if this is necessary.

Examples of methods to be adopted are as follows.

[Compensation for user damage]

1. Compensation/refund procedures and compensation scopes are pre-defined in preparation for the cases where unauthorized access or system failures causes some damages to users.
2. The following is confirmed: (1) whether or not there is a document that defines the scope of liabilities for incidents and the scope of compensation between the API connection partner and its cloud service provider; (2) what the name of the document (if such a document exists); and (3) whether or not a property insurance is contracted.

Related rules	JBA “Report of Review Committee on Open APIs” 3.4 User Protection Principles 3.4.5 Responsibilities Toward and Compensation of Users c

Category
Cooperation between financial institutions and API connection partners

Subject party		
API connection partner	Financial institution	Both
		✓

16	Operate contact points for user compensation properly.

Establish contact points for user compensation and operate them properly from a viewpoint of user protection.

Examples of methods to be adopted are as follows.

[Contact points for user compensation]

1. Compensation/refund procedures and scopes for user compensation are displayed on the website so that users can check them anytime; in addition, users can obtain information on contact points for compensation/refund and its procedures.

Related rules	JBA “Report of Review Committee on Open APIs” 3.4 User Protection Principles 3.4.5 Responsibilities Toward and Compensation of Users d

Category
Management of computer facilities

Subject party		
API connection partner	Financial institution	Both
✓		

17	Implement countermeasures against information leakage from computer facilities.

Implement countermeasures for preventing leakage of information assets (electronic data) from computer rooms, if such assets are stored there.

Examples of methods to be adopted are as follows. (In case of using cloud services, refer to the security objective 11.)

[Checking of physical security of computer rooms]

1. Doors fortified against destruction are installed at gateways to important physical security areas.
2. Computer rooms and racks are locked up. (Keys, cards, and/or personal identification numbers are required when entering and leaving rooms.)

[Installation of computer resources]

1. In case of installing computer resources in an office, they are installed in locked racks so that easy access to the equipment including cables is prevented.
2. Computer resources are installed in the data center.

[Control of access by executives and employees to information assets]

1. Access control measures are implemented at every stage of the life cycle of information assets: acquisition/input, processing/use, and saving/storage. (Note 1)
2. Rules on operating surveillance cameras are established: operation time, monitoring scope, and footage storage period.
3. Physical entry/exit control devices (e.g., those attached to doors and fences) working with personal authentication systems are installed.
4. Security guards are always stationed at reception.

(Note 1)

1) Implementing entry/exit control in facilities such as working places and locations of information systems to prevent misconduct by internal and external visitors in the buildings (or rooms). (Example: Storing entry/exit records)
2) Measures to prevent misconduct such as theft. (Examples: Conducting monitoring by recording with cameras or by observing operation on the spot; prohibiting persons from bringing in/out recordable media; and inspecting such media)

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e

Category
Management of office facilities

Subject party		
API connection partner	Financial institution	Both
✓		

18	Prevent entry of unauthorized persons and restrict access to important information.

Ensure control of entry into offices and system access to prevent leakage of important information obtained in the course of business.

Examples of methods to be adopted are as follows.

[Restriction of entering rooms]

1. Entry is restricted to the rooms where equipment storing important information is installed. (Note 1)

[Implementation of measures to control access to information asset]

1. Access control measures are implemented at every stage of the life cycle of information assets: acquisition/input, processing/use, saving/storage, transfer/transmission, and erasion/disposal. (Note 2)

(Note 1)

1) A procedure manual of controlling entry to/exit from important physical security areas is prepared.

(Note 2)

1) Implementation of entry/exit control in facilities such as working places and location of information systems to prevent misconduct by internal and external visitors in the buildings (or rooms).
(Example: Storing entry/exit records)
2) Measures to prevent misconduct such as theft.
(Examples: Conducting monitoring by recording with cameras or by observing operation on the spot; prohibiting persons from bringing in/out recordable media; and inspecting such media)

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e

Category
Management of office facilities

Subject party		
API connection partner	Financial institution	Both
✓		

19	Prevent persons involved from taking information out of the premises.

Implement measures to prevent persons involved from taking information out of the premises without permission.

Examples of methods to be adopted are as follows.

[Prohibition of downloading and taking out information assets]

1. Measures are implemented against the risks of information leakage from PCs by way of external storage media and smart devices (i.e., tethering). (Note 1)
2. It is recognized how information assets (electronic data) stored in systems are handled. (Note 2)
3. PCs are managed in accordance with internal rules (e.g., measures are implemented to prevent leakage and damage of information assets). (Note 3)
4. Media are stored securely. (Note 4)
5. It is restricted to download and take out information assets. (Note 5)

(Note 1)

1) Registry setting by the administrator makes it possible to restrict data downloading onto USB sticks.

2) Restriction by write-control software is implemented (including restriction of MTP transfer and tethering).

3) Physical locking of media insertion slots is implemented (a key is necessary to insert USB sticks into a PC).

4) Sealing stickers are used. (Sealing is checked, and the inventory is controlled.)

5) Monitoring is carried out to detect violation of e-mail rules, and risks are recognized and addressed with regard to wiretapping and unauthorized alteration of transmitted important information.

6) Operation rules on business e-mails are formulated.

(Note 2)

1) Downloading data onto storage media is controlled if such downloading is technically possible. (Examples of control measures include permission by system, log acquisition and ex-post audit, sealing with USB keys, and disabling of USB ports. It is important that the operator is unable to approve his/her own operation.
2) Uploading data in online storage is controlled if such uploading is allowed.* (Examples of control measures include express granting of such right and log acquisition and auditing.)
   * This measure is not applicable if there is no Internet connection or communication with the Internet is blocked by Web filtering.
3) On PCs used for performing system maintenance or handling important information (e.g., token and authentication code), it is prohibited to (1) send/receive e-mails or (2) browse Websites without the necessity of doing so for business.

(Note 3)

1) Information assets are protected by the measures listed below.
   a. Prohibition of bringing private devices such as PCs and storage media into the office; and restriction of connecting equipment.
   b. Prohibition of unauthorized software installation on PCs used for business.
2) In order to prevent leakage of information assets, the following audits or actions are performed.
   a. Prohibition of sending business information to private e-mail accounts.
   b. Audits on outgoing mails; or system controls under which the information acquired through the organization’s services cannot be sent by e-mail.

(Note 4)

1) Producing a procedure manual and establishing methods for storing media such as paper, magnetic tape, and optical media.
2) Producing a procedure manual and establishing methods for disposing of media such as paper, magnetic tape, and optical media.

(Note 5)

1) It is technically disabled to write into portable media.
2) It is prohibited to take out information to the external Internet environment without the authority.
3) It is prohibited to take out information via e-mail without the authority.
4) It is technically restricted to write into portable media.
5) It is controlled, through monitoring, to take out information to the external Internet environment without the authority.
6) It is controlled, through monitoring, to take out information via e-mail without the authority.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e FISC Security Guidelines Practice Guidelines 4. Facilities management P49

Category
Management of office facilities

Subject party		
API connection partner	Financial institution	Both
✓		

20	Prevent attacks such as intrusions to internal systems through infection with computer viruses.

Implement necessary measures to prevent virus infection and consequent system intrusion leading to leakage or alteration of information.

Examples of methods to be adopted are as follows.

[Countermeasures against computer viruses]

1. Anti-virus software is installed on PCs used for business; pattern files are updated as needed; and virus checks on portable storage media is conducted.
2. OS and applications on PCs used for business are updated to the latest versions.
3. Virus checks are conducted on e-mails, downloaded files, accessed files on servers, and terminals for operational management. (Names of anti-virus software and the frequency of pattern file updates are presented.)
4. A series of the procedures for responding to virus infection is established and is regularly reviewed.

Related rules	JBA "Report of Review Committee on Open APIs" 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

21	Prevent unauthorized access to information assets from within.

Implement measures to prevent unauthorized access from within to information assets that include customer information so that leakage and alteration of such information is avoided.

Examples of methods to be adopted are as follows.

[Access control]

1. The number of executives and employees who are given authority to access information assets is minimized, and the scope of the access authority is limited to a minimum.

[Granting of access authority according to roles and responsibilities]

1. Classification of access authority into different kinds, as well as what kind of access authority is given, is based on the roles and responsibilities of individual executives and employees. (Note 1)
2. Access control rules are established, and strict controls are implemented with regard to various user IDs to which different kinds of access authority are given. (Note 2)

[User ID management]

1. The number and scope of access authority given to executives and employees is limited to a minimum. The scope of access authority is determined properly according to data usage in different business lines.
2. Formal procedures are established for registration, change, and withdrawal of access authority.
3. In personnel changes such as transfer and retirement, corresponding procedures (e.g., deletion of user IDs) are carried out immediately after such changes.
4. Measures to ensure correct setting and strict control of access authority are carried out. (Note 3)
5. Measures such as introduction of (1) an authentication method for user access management and (2) a method to permit and authenticate connections only from specific places and equipment are in place.

[Recording and analysis of access logs]

1. Logs of access to information assets and operational status of information systems are recorded and analyzed. (Examples of access logs to be recorded include logs concerning (1) login and logoff situations, (2) unauthorized access requests, and (3) IDs made invalid by system.)

[Log check regarding usage history of operation IDs and privileged IDs]

1. It is confirmed that there are no logs indicating suspicious operations in the production environment at the development and operation departments. Such operations include (1) exceptional operations and (2) special ones only possible with unissued privileged IDs. (Note 4)
2. Logs of access in time zones with high information leakage risks, such as weekends/holidays and late night hours, are analyzed and checked. (Note 5)

[Monitoring and auditing of information systems]

1. Usage of information systems [handling electronic information assets] as well as access to information assets is monitored.
2. Monitoring conditions are checked and audited.

[Prevention of unauthorized alteration to customer information]

1. Management rules for handling of customer information are defined.
2. It is confirmed whether management rules on customer information are observed.
3. Necessary improvements are carried out if some management rules are not observed.
4. Necessary measures are carried out to prevent unauthorized alteration to customer information. (Note 6)

(Note 1)

1) It is confirmed who has access authority so that it can be specified who have accessed the leaked information.
2) Control is established to prevent access from internal unauthorized persons.

(Note 2)

1) Privileged ID (Administration authority)
    a. As a rule, privileged IDs may not be used in development and operation and are granted only to a limited number of internal members.
    b. Privileged IDs are granted by authority of the responsible person.
    c. If the scope of access authority attached to a privileged ID has been changed, the change is confirmed within the day.
2) Operation ID
    a. An operation ID is created by the operation department based on the written request from the operation department or the development department.
    b. The development department and the operation department are separated from each other to prevent misconduct.

(Note 3)

1) Roles and responsibilities of executives and employees for handling information assets at each management level are clearly defined.
2) The scope of access authority is determined according to the management classification of information assets.
3) In principle, user IDs are given to each person and are not shared.
4) It is checked regularly (1) whether there remain IDs that are no longer used due to personnel transfer and retirement and (2) whether access authority is given properly according to the roles and responsibilities of each person.
5) Internal rules are reviewed and revised as necessary.

(Note 4)

1) Access logs are recorded and stored; logs fulfilling specific conditions are detected to be made known to operators.
2) Access logs are regularly checked.

(Note 5)

1) Examples of how to check access records: Providing logs to the manager; making it possible to refer to logs without actual access in production; and making logs to be displayed on the monitoring screen in an emergency.
2) An example of checking: Logs are checked visually to detect suspicious access.

(Note 6)

1) TLS mutual authentication is carried out.
2) The signature to a request message using electronic signature technology (e.g., HTTP Signature Messages and JSON Web Signature) is verified.
3) Request messages are encrypted by using cryptographic technology (e.g., JSON Web Encryption).

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e FISC Security Guidelines Practice Guidelines 2. Common guidelines for system operations P27, P29

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

22	Implement authentication on system access.

User identity is verified when the user accesses the system so that incidents caused by unauthorized access (such as information leakage, data alteration, and system failure) are prevented.

Examples of methods to be adopted are as follows.

[Establishment of relevant rules and identification methods]

1. Internal rules are established regarding management of IDs and passwords (along with encryption keys).
2. Methods are established such as an authentication method to control user access and an arrangement for permitting and authenticating connections only from specific places and equipment. (Note 1)

[Management of IDs and passwords]

1. Misuse of an ID that is enabled by a brute-force attack to passwords is prevented. (Note 2)
2. No embedded ID that potentially leads to unauthorized access to computer systems is used. (Note 3)
3. IDs used in databases, shells, or between programs are managed separately from IDs used by people. (Note 4)
4. Passwords used at system login have a sufficient number and types of characters so that they are not guessed easily.
5. A password is applied for and issued with approval at each login, and the issued password is valid only within the applied work.

[Authentication by certificate]

1. A terminal and the person who is entitled to use it are authenticated by use of a certificate.
2. Multi-factor authentication using onetime token at login is adopted.

[Limited connection to networks]

1. Terminals are, in principle, not allowed to connect to external networks with the exception of a limited number of pre-specified networks.

(Note 1)

1) Improvement of user identification functions.
2) Improvement of functions to prevent unauthorized use of information related to user identification.
3) Measures to prevent user identification information from being revealed to anyone.

(Note 2)

1) For example, if input of a password into the information system fails a certain number of times consecutively, the ID is disabled temporarily.

(Note 3)

1) Measures are implemented to prevent the password used in programs and operation jobs from being revealed.

(Note 4)

1) Such an ID is treated as a system ID, and login using it is prohibited.

Related rules	FISC Security Guidelines Practice Guidelines 1. Information security P1, P8, P16 Practice Guidelines 2. Common guidelines for system operations P26

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

23	Maintain logs of access to and use of systems to enable investigation in the event of incidents.

Access logs are maintained so that the cause can be investigated when information leakage or system failures occurs.

Examples of methods to be adopted are as follows.

[Recording of access to information assets]
1. Information on access to information assets is recorded, stored, and analyzed. (Note 1)

[Provision of log information]
1. Records of usage, exception processing, and security incidents (along with types of logs and storage period) related to information-asset users are provided to them.

(Note 1)
1) Access to information assets as well as operational status of information systems is recorded and analyzed. (Records include those of login and logoff, unauthorized access request, and invalidation of IDs by system.)
2) Security measures for the obtained records are implemented properly so that leakage of the records is prevented.
3) With regard to the obtained records, among others, cases with high frequencies of access that occurred especially in time zones with high information leakage risks (e.g., weekends/holidays and late night hours) are analyzed carefully.

Related rules	FISC Security Guidelines Practice Guidelines 1. Information security P10

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

24	Implement countermeasures to prevent misconduct by operators.

Implement necessary measures to prevent operators from carrying out illegal acts such as bringing out information without permission.

Examples of methods to be adopted are as follows.

[Prevention of one-person operation]

1. Misconduct caused by one-person operation is prevented. Examples of the measures for this purpose include the following: (1) the entire staff in the department is automatically informed when each of them has logged into the system; and (2) details of the day’s operation are shared by department members before they log into the system.
2. Request for approval is required at each step of operation so that one-person operation is prevented at any time.
3. Approval by others is required whenever source code changes are reflected so that one-person operation is prevented.

[Prevention of unauthorized data alteration]

1. Measures are implemented to prevent unauthorized alteration by operators to the data to be displayed to customers (examples of such measures include the following: establishment of a framework for identifying the operator on duty; restriction of the contents of outputs; recording of output; and definition of storage/disposal methods).

[Third-party audit]

1. Misconduct is excluded by external audits and/or in-house inspections conducted regularly (once a year or more).

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

25	Implement measures as necessary to prevent marked deterioration in quality when making changes to systems.

Implement necessary measures to prevent quality deterioration that may occur when changes are made to computer systems.

Examples of methods to be adopted are as follows.

[Maintenance of system quality]

1. Documents such as those on design specifications, source codes, and test results are reviewed as prescribed.
2. Automated testing is carried out to prevent unanticipated deterioration in quality, when source code changes are reflected to the repository.
3. When changes are made to a computer system, the system is shut down as necessary and a quality check by keystroke verification is performed.

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

26	Implement countermeasures against unauthorized access from the outside.

Implement countermeasures against unauthorized access from outside the organization so that information leakage or data alteration is prevented.

Examples of methods to be adopted are as follows.

[Countermeasures against unauthorized access]

1. Measures are introduced to detect intrusion and unauthorized data alteration such as Intrusion Detection System (IDS), Intrusion Protection System (IPS), and Web Application Firewall (WAF). (Note 1)
2. Various preventive actions are taken against unauthorized access from the outside. (Note 2)

[Collection of cyber threat information]

1. Cyber threat information is collected routinely from manufacturers, security vendors, external bodies (such as Financials ISAC Japan, JPCERT, National Police Agency, and JC3) and is analyzed properly (examples of the viewpoints include the following: what impact is expected on the organization’s own systems; whether immediate action is necessary; whether records show that countermeasures have been implemented based on information collected in the past).

(Note 1)

1) If the organization’s Website is made open on the Internet, stateful inspection is conducted at the firewall and a WAF is in place in the DMZ.
2) If the Web server is connected with customers via a dedicated line, and stateful inspection is conducted at the firewall; secure coding of Web applications are adopted instead of a WAF in the DMZ, and countermeasures against vulnerabilities are checked by Web diagnosis.

(Note 2)

1) Limiting accessible communication routes.
2) Improving ability to prevent intrusion from external networks.
3) Improving ability to monitor network communications and detect unauthorized access (such as introducing IDS or IPS and shortening intervals between signature [pattern file] updates).
4) Improving access control implemented on the network (such as installation of security monitoring device).
5) Introducing mechanisms to prevent unauthorized access such as firewalls and a reverse proxy, tandem multiplexing of firewalls, and countermeasures against attacks to applications.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access x

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

27	Implement countermeasures against vulnerabilities in systems and networks.

Implement countermeasures against vulnerabilities in computer systems and networks so that incidents such as information leakage is prevented.

Examples of methods to be adopted are as follows.

[Implementation of countermeasures against vulnerabilities in computer systems]
1. Countermeasures against vulnerabilities (and diagnoses of them) in computer systems are carried out. (Note 1)
2. Countermeasures against vulnerabilities are carried out for servers open to the public.
3. Security diagnoses and audits are carried out. (Note 2)
4. Network equipment is maintained properly. (Note 3)
5. Software management is carried out. (Note 4)
6. Security patches are applied. (Note 5)

[Conduct of vulnerability tests and penetration tests]
1. Vulnerability testing is conducted on a continual basis. (Note 6)
2. Penetration testing is conducted on a continual basis. (Note 7)
3. Network vulnerability testing is conducted.

(Note 1)
1) Establishing security measure guidelines (such as secure coding rules).
2) Establishing rules for implementation of security diagnosis.
3) Implementing the measures at the time of development of and changes to systems.
4) Conducting diagnoses on a regular basis.
5) Taking actions based on diagnosis results.

(Note 2)
1) Regular inspections of Web applications and networks are conducted by outsourcing them to external experts.
   a. Conducting diagnoses of resistance against intrusions and DoS attacks.
   b. Checking whether the intruder is able to make an attack on other networks by using the penetrated server as a stepping-stone.
   c. Conducting Web diagnosis and platform vulnerability diagnosis.

(Note 3)

1) For computer systems connected to external networks, preventive measures against unauthorized access are implemented such as closing unnecessary ports and minimizing the number of access routes by turning off the equipment (including network equipment) that is not used constantly.
2) Provision of online services is limited to a minimum if they are processed on servers connected to the Internet, and connection methods from the outside are restricted. (Tools with which servers can be operated remotely, such as TELNET, rlogin, rsh, rexec, FTP, RFS, and NFS, are disabled. Moreover, tools other than those above, such as SMTP, are also disabled if they are unnecessary to perform expected system functions.)

(Note 4)

1) Software is properly managed to prevent unauthorized access and malware infection.
2) Non-supported OS middleware, or other types of software are not in use.

(Note 5)

1) Establishing policies on how to apply security patches to servers and administration terminals (for example, deciding the way to collect vendor release information and the time lag between the release and application of patches).
2) Whether to apply a patch is decided according to the importance of the patch, and the CVSS (Common Vulnerability Scoring System) severity level 3 (*) patches are applied without exception.
   * Threats of the CVSS severity level 3 include the following: (1) cases in which the system may be placed under complete remote control; and (2) cases in which unauthorized alteration may be made to most data. (Example of modus operandi: Optional command execution using OS command injection, SQL injection, and buffer overflow.)

(Note 6)

1) Scope of diagnosis (e.g., application and platform)
2) Diagnosis method (e.g., tool-based diagnosis, manual diagnosis, and their combination)
3) Frequency of implementation (e.g., once-a-year diagnosis by a third party and daily for automatic diagnosis by using tools)
4) Frequency of test results reporting, and action on the domains in which some countermeasures are required based on the test results

(Note 7)

1) Scope of diagnosis (e.g., system, data, people, and facility)
2) Diagnosis by a third party (i.e., external expert)
3) Frequency of implementation (e.g., once a year)
4) Frequency of test results reporting, and action on the domains in which some countermeasures are required based on the test results

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s

Category
Management of system development and operations

Subject party		
API connection partner	Financial institution	Both
✓		

28	Manage confidential information taken out of the premises.

Establish management methods and perform information management so that confidential information taken out of the premises will not leaked out.

Examples of methods to be adopted are as follows.

[Handling of information with regard to taking out, deletion, and disposal]

1. Logs are recorded and checked on a regular basis with regard to handling (i.e., taking out, erasure, and disposal) of copies of important confidential/customer data stored in portable media.
2. If disposal of data is outsourced to a third party, this is conducted properly according to the contract with the third party and in-house rules (e.g., distinction between ordinary objects and confidential information).

[Rules on handling of electronic storage media]

1. There are management rules (e.g., bookkeeping rules) on each step of the handling of electronic storage media: acquisition, activation, usage, data copy, storage, taking out, and disposal.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.3 Countermeasures for Internal Unauthorized Access e

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
✓		

29	Implement management measures suited to the types and contents of data.

Adopt data management methods suited to the types and contents of data, because impacts of data leakage depend on those factors.

Examples of methods to be adopted are as follows.

[Setting of data management level]

1. Among the data used by the organization’s own services, those that should not be disclosed can be enumerated, and the security levels required to them are defined.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access x

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
✓		

30	Implement countermeasures against leakage of confidential information.

Implement necessary measures so that confidential information does not leak out.

Examples of methods to be adopted are as follows.

[Conduct of security management measures]

1. For dealing with confidential information such as credit-card numbers and password, a mechanism for transmitting and storing the data safely is introduced. (Note 1)

[Protection and management of data]

1. When storing important data, such as personal information and those used for authentication, in computer equipment or external media, protection by encryption or password is carried out. (Note 2)
2. Passwords or personal identification numbers used by customers and all data in the random number table are hashed. (Note 3)
3. A function is in place with which temporary files are erased as soon as they became unnecessary; there is a risk that important information may leak out if such information is included in temporary unencrypted data.
4. IDs used in databases, shells, or between programs are managed separately from operation IDs.
5. The operation department permits users to refer to data or delivers data to them after confirming the approval by the manager in charge in the development department.
6. Measures to protect information assets are implemented. (Note 4)

[Encryption process]

1. Highly confidential and important information and programs based on it, such as encryption algorithms, check digit specifications, authentication specifications, and personal information masking specifications, cannot be used or referred to by persons other than those in charge of development.
2. Encryption keys are tightly managed and safely stored: the life cycle of their validity is closely managed; and even a person in the system department is unable to refer to them if the access authority is not granted to the person. In addition, the operation procedures related to creation, delivery, storage, revoking, renewal, and disposal of encryption keys are established.
3. It is understood whether or not each network is encrypted, and if some are encrypted, encryption methods (e.g., protocol and encryption type used) and its strength (e.g., encryption key length) are managed.

[Detection of unauthorized access]

1. Measures are implemented to detect a leakage of a large amount of customer information caused by system users in the organization.
2. The history of records of downloaded customer information is acquired to confirm that there is no unauthorized access (such confirmation is done by, for example, using an installed function that can check suspicious usage).
3. Login history information, such as the date, time, and situation of the last access using an ID, is provided to the owner of the ID so that misuse by a third party is detected.

[Handling of test data]

1. For customer information included in production data used for testing, procedures to change them, by for example masking them, into a format with which customers cannot be identified are established and followed. (Note 5)
2. Production data are referred to and borrowed by developers (those who use production data in the development and testing phases) under strict control and close attention is paid to prevent accidents such as information leakage, because such operation should be considered exceptional.
3. When customer data are used in the non-production environment, data items that can identify customers, My Numbers (official personal identification numbers), and credit card numbers are masked to prevent leakage of customer information.

(Note 1)

1) Encrypting the data when storing them.
2) Masking partially confidential information such as passwords and credit card numbers if they are displayed on the screen.
3) Preventing confidential information such as passwords and credit card numbers from being output to a log.
4) Conducting countermeasures against wiretapping by using encrypted communication.

(Note 2)

1) Database: Setting passwords using the function of DBMS.
2) Document file: Setting passwords applied to the document itself or storage folder.
3) Hard disk: Activating encryption functions of hard disk drives or setting passwords
4) Backup data: Activating encryption functions or setting passwords

(Note 3)

1) Hashing is recommended, and widely adopted encryption is also allowed.
2) For two-factor authentication, both factors are targeted.
3) The encryption algorithm is one of those described in the CRYPTREC Cyphers List.

(Note 4)

1) Preventive measures are taken against illegal copy or theft of accumulated data so that the contents of information assets cannot be read.
2) Preventive measures are taken against wiretapping of transmitted data so that the contents of those data cannot be read.
3) Preventive measures are taken against malicious programs such as computer viruses.
4) Measures are implemented such as password setting and encryption when data are saved and stored in electronic file formats.
5) Proper data encryption methods are adopted.

(Note 5)

1) The procedures include the following conditions.
   a. The approval authority is given to the manager responsible for security (equivalent to the department-head level).
   b. The number of persons who can access customer data is limited to a minimum.
   c. Management rules for erasing and disposing of data are established.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
✓		

31	Enable restoration of lost or damaged information.

Implement necessary measures so that lost or damaged information can be restored.

Examples of methods to be adopted are as follows.

[Making of backups]

1. Data are backed up, generation management of backup data is performed, and restorative measures are carried out.
2. In making backups, technical countermeasures and restorative procedures are prepared in preparation for system failures. (Note 1)
3. In preparation for the case where early recovery is impossible, alternative measures are prepared (e.g., provision of backup data from another site and/or conversion of data stored in different format).

(Note 1)

1) Employing countermeasures and restorative procedures in preparation for unauthorized access.
2) Employing measures in preparation for damages caused by malicious programs such as computer viruses.
3) Improving recovery functions.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
✓		

32	Develop authentication functions to protect users.

Satisfy both user convenience and security by adopting adequate authentication methods that suit types of risks.

Examples of methods to be adopted are as follows.

[Management of authentication methods]

1. The role of authentication methods used for the organization’s services is well understood. It is fully recognized what type of authentication methods is used for each of those services, if the provision of those services is critically dependent on them. (Note 1)

[Provision of authentication means]

1. Authentication means are provided to users so that they are protected adequately. (Note 2)
2. Countermeasures are introduced in preparation for possible security incidents. (Note 3)

[Review of authentication methods]

1. If there is a service function that involves authentication, it is confirmed as necessary whether the adopted authentication method is effective enough to ensure the required level of security. (Note 4)

(Note 1)

1) For important functions of the organization’s service (e.g., inquiry and payment), it is listed and fully recognized what kind of authentication information (e.g., ID/password and onetime token) users need to input for using each of such functions.

(Note 2)

1) Account lock in cases where incorrect passwords are entered a certain number of times.
2) Lower limit of the number of password characters.
   a. The password is changed only by the user or administrator on the screen without involvement of any third party (e.g., operator).
   b. If Windows is used, the password policy is that every password in use meets the complexity requirements.
3) Provision of a screen that displays login histories.
4) Two-step authentication.
5) Risk-based authentication.

(Note 3)

1) Measures to detect misuse of the authentication function (countermeasures against list-based attacks).
2) A mechanism for detecting system vulnerability.

(Note 4)

1) Recognizing the decrease in the level of security to be ensured by authentication. (A list is made that covers all authentication methods with which users can log in to use the organization's services, such as ID/password authentication and social login. It is confirmed regularly that there is no vulnerability in those methods.)

Related rules	JBA "Report of Review Committee on Open APIs" 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access m

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
✓		

33	Implement countermeasures against fake applications.

Implement necessary measures to prevent incidents such as information leakage caused by fake applications.

Examples of methods to be adopted are as follows.

[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)

(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.

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
		✓

34	Keep the spread of damage from unauthorized access to a minimum.

Implement necessary measures to minimize the spread of damage in the event of unauthorized access.

Examples of methods to be adopted are as follows.

[Prevention of spread of unauthorized access]

1. It is operationally possible to limit and discontinue the provision of services immediately after unauthorized access is detected.

Related rules	JBA “Report of Review Committee on Open APIs ” 3.3 Security Principles 3.3.4 Handling Unauthorized Access When It Occurs a

Category
Service-system security functions

Subject party		
API connection partner	Financial institution	Both
		✓

35	Enable tracing in the event of unauthorized access.

Implement measures necessary for tracing so that causes and countermeasures can be discussed in the event of unauthorized access.

Examples of methods to be adopted are as follows.

[Acquisition and storage of logs]

1. Access logs are acquired and stored to be able to (1) respond to inquiries from users about suspicious funds transfers and (2) investigate causes and discuss countermeasures in the event of unauthorized access. (Note 1)
2. Records of utilization, exception processing, and security incidents are acquired (along with types and storage periods of those logs).
3. Appropriate execution logs are stored according to the type and level of security risks of the API in use (such logs become available by, for example, introducing a firewall that always outputs execution logs).
4. An alert goes out when there appears a specific log message code registered in advance.
5. Initial response and preservation of evidence are carried out based on the guidelines published from external bodies (e.g., NPO Institute of Digital Forensics).

(Note 1)

1) The system log is acquired (*) to check the content.
   * Operation details are recorded by using OS functions or business applications.
2) Access history management is carried out by the password management system and the access record management system.
3) Others:
   a. Activation and termination of OS and middleware is recorded in the log, and is displayed on the monitoring screen.
   b. Login to/logout from OS and middleware (including the case of failure) is recorded.
   c. The date/time of use of applications by users are recorded.
   d. The following information is recorded.
      - Activation and termination of OS
      - Activation and termination of DBMS
      - Activation and termination of middleware
      - Mount and unmount of disk devices or logical volumes
      - Activation and termination of log acquisition programs
   e. Network monitoring functions (those for, for example, acquisition of access log and alarm at unauthorized access) are installed.
   f. Operators stay alert to alarming.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s 3.3.4 Handling Unauthorized Access When It Occurs b

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
✓		

36	Implement countermeasures against leakage of confidential information related to authentication and authorization.

Implement necessary measures to prevent leakage of confidential information related to authentication and authorization.

Examples of methods to be adopted are as follows.

[Proper management of tokens]
1. Proper management of tokens is implemented according to the type and level of security risks of the API in use. (Note 1)

[Specification of objects to be encrypted]
1. It is decided what should be encrypted. (Note 2)

(Note 1)
1) Tokens valid for a period longer than a certain length of time (e.g., one hour) are encrypted when saved.

(Note 2)
1) Authorization code, access tokens, and refresh tokens that are used in OAuth2.0.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access g

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
✓		

37	Prevent unexpected usage of API.

Implement necessary measures to prevent unexpected usage of API.

Examples of methods to be adopted are as follows.

[Prevention of unexpected usage of API]

1. The scope of APIs in use and the functions that can be performed by acquired tokens are understood. (Note 1)
2. Principles of avoiding unexpected usage of API are understood, and the countermeasures are implemented. (Note 2)
3. The authorization functions and API request functions are developed based on security reference issued by external bodies (e.g., Financials ISAC Japan, JPCERT, National Police Agency, and JC3).

(Note 1)

1) The framework of OAuth2.0 is understood, and the meanings of items related to it can be explained.

2) Minimum security principles that the API provider (i.e., the financial institution concerned) is required to fulfill is understood, and it can be confirmed whether they satisfy such principles.

(Note 2)

Unexpected usage of APIs includes the following.

1) Part of a URI is falsified to make it possible to access servers and acquire other company’s data illegally.

2) API requests are falsified to acquire data illegally.

3) A malicious third party (e.g., company) takes over access tokens to illegally acquire personal information held by other companies or to damage users.

4) A malicious third party hijacks communications over the Internet or wide area network (WAN) to illegally acquire personal information or to damage users.

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
	✓	

38	Ensure that user accounts are not used to establish API connection without the user’s knowledge.

Implement necessary measures to prevent user accounts from being connected to API without the user’s awareness.

Examples of methods to be adopted are as follows.

[User identification]

1. Financial institutions (1) give the access authority to their API connection partners based only on application from individual users and (2) authenticate those users when giving such rights.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access b

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
	✓	

39	Realize the strength of authentication that strikes a suitable balance between user convenience and user protection suited to the risk involved.

Adopt the authentication method strong enough to achieve the two conflicting objectives: (1) convenience of services for users provided by API connection partners; and (2) user protection suited to the risk involved in API connection.

Examples of methods to be adopted are as follows.

[User authentication according to access scope]

1. In giving access authority to their API connection partners based on application from users, financial institutions decide how they authenticate the applying users based on their attributes, the scope of the access authority to be given, and the risks involved.
2. In deciding the strength of user authentication when access authority is given, the authentication method used for Internet banking (Note 1) is referred to as a guideline. (Note 2)

[Limitation of access scope]

1. The scope of access authority granted to API connection partners is limited to what is necessary for them to provide their services.

(Note 1)

1) An ID and a password are used at login, and a onetime password at payment.
2) Additional authentication functions are provided in cases where transactions are processed by using devices different from PCs ordinarily used.

(Note 2)

1) The authentication of users for granting access authority to API connection partners is not one related to individual transactions, but one related to permission of access.
2) The strength of authentication is determined in consideration of the risk of unauthorized access; it is recognized that the strength depends on the authentication method that is applied to individual transactions initiated by instructions coming through API.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access c

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
	✓	

40	Implement multilayered protection against attacks targeting vulnerabilities.

Implement multi-layered protection to prevent information leakage caused by attacks targeting vulnerabilities.

Examples of methods to be adopted are as follows.

[Implementation of multi-layered protection]

1. Multi-layered protection against attacks targeting unknown vulnerabilities are implemented as part of the mechanism of the system as a whole. (Note 1)

[Countermeasures against known vulnerabilities]

1. The authorization functions and API functions based on security reference issued by external bodies (e.g., Financials ISAC Japan, JPCERT, National Police Agency, and JC3) are developed.

(Note 1)

1) In general, multi-layered protection comprises (1) pre-hacking measures (measures against penetration), (2) post-hacking measures (measures against data leakage), and (3) internal measures.
   a. Pre-hacking measures: Prevent computer viruses and malware penetrating into the internal network.
   b. Post-hacking measures: Detect unusual communications over the network and prevent information leakage to the outside.
   c. Internal measures: Monitor data processing on terminals and servers and address promptly in an emergency.
2) Communication with API connection partners is, in principle, carried out by server-to-server connection. On top of that, a mechanism is introduced so that parameter information used in the connection is not tapped and/or identified by a malicious third party.
3) IP addresses of API connection partners is limited, and a mechanism is introduced with which no access is permitted from other addresses.
4) API connection partners introduce client certificates, and a mechanism is introduced to authenticate connection partners by using the certificates.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access s

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
	✓	

41	Reduce the risk of misuse of authentication as much as possible.

Implement necessary measures to reduce the risk as much as possible that the authentication for connecting with API connection partners is misused by a third party.

Examples of methods to be adopted are as follows.

[Proper management of tokens]

1. A not-too-long period of validity is set on the token issued to the API connection partner. (Note 1)
2. Countermeasures are implemented against forgery and theft of tokens according to the scope of access authority.
3. A mechanism is introduced to be able to limit, discontinue, and withdraw access authority immediately after unauthorized access is detected.

[Encryption targets]

1. Encryption targets are decided. (Note 2)

(Note 1)

1) The token is valid only once.
2) The validity expires within one month or a few months at the longest.

(Note 2)

1) Authorization code, access tokens, refresh tokens that are used in OAuth2.0.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access g, m

Category
API security functions

Subject party		
API connection partner	Financial institution	Both
	✓	

42	Protect users through the overall strength of authentication, including the strength maintained by API connection partners.

From a viewpoint of user protection, financial institutions take care to ensure the overall strength of authentication including the strength maintained by their API connection partners.

Examples of methods to be adopted are as follows.

[Confirmation and ensuring of sufficient authentication strength]

1. It is confirmed that the authentication strength maintained by API connection partners is not inferior to the one by financial institutions with regard to individual payment instructions initiated by users, relayed via API, and directed to financial institutions.
2. If the authentication strength maintained by API connection partners is inferior to the one by financial institutions but this is considered to be appropriate in light of user convenience, another mechanism is used for user protection.

Related rules	JBA “Report of Review Committee on Open APIs” 3.3 Security Principles 3.3.2 Countermeasures for External Unauthorized Access m

Category
Security of API use

Subject party		
API connection partner	Financial institution	Both
✓		

43	Ensure accountability to users regarding their API use.

Explain important matters when users start utilizing the API.

Examples of methods to be adopted are as follows.

[Preventing users' misunderstanding]
1. It is explained to users what to do with tokens in the API.

[Explanation to users]
1. It is explained to users that, in the API requiring authorization, the API function may become unavailable in certain conditions.

Related rules	JBA "Report of Review Committee on Open APIs" 3.4 User Protection Principles 3.4.2 Explaining/Displaying information and Obtaining Consent d

Category
Security of API use

Subject party		
API connection partner	Financial institution	Both
	✓	

44	Prevent user misconceptions and misunderstandings regarding API connections.

Implement necessary measures to prevent users' misconceptions and misunderstandings regarding API connections.

Examples of methods to be adopted are as follows.

[Display of important information and acquisition of consent from users]

1. In the issuance of tokens, information on API connection is displayed clearly on the screen and users' consent is requested. (Note 1)

(Note 1)

1) Name of the API connection partner to which access authority is granted
2) Name of services with API linkage
3) Contents and scopes of the authority to be granted
4) Period of validity of the authority to be granted
5) How to withdraw the granted authority in part or as a whole
6) Other items requiring cautions
7) Encryption to prevent information leakage
8) Service agreement, inquiry desk, outline of security measures, and contact point in an emergency

Related rules	JBA "Report of Review Committee on Open APIs" 3.4 User Protection Principles 3.4.2 Explaining/Displaying information and Obtaining Consent c

(Appendix table)

Member List of
Council of Experts on Open API for Financial Institutions

(Honorifics omitted; listed in no particular order)
(Organizations and titles as of meetings)

Chairperson	Shinsaku Iwahara	Professor of Law Waseda Law School
Alternate Chairperson	Masahiro Fuchizaki	Representative Director, President & CEO, Japan Research Institute, Limited
Members	Kiyoshi Yasutomi	Professor emeritus, Keio University Visiting Professor of Law School and Director, Legal Education Center, Kyoto Sangyo University Attorney (Atsumi & Sakai)
	Jiro Kokuryo	Vice President/Professor of Faculty of Policy Management, Keio University
	Hiroshi Kamiyama	Attorney-at-law Patent Attorney Hibiya Park Law Offices
	Kazuhiko Tajimi	Deputy General Manager Digital Innovation Department Mizuho Financial Group, Inc.
	Yusuke Hirota	General Manager IT Management Division The Bank of Fukuoka, Ltd.
	Norifumi Yoshimoto	General Manager FinTech Business Planning Dept. SBI Sumishin Net Bank, Ltd.
	Isamu Ando	General Manager IT Business Process Planning Dept. Dai-ichi Life Insurance Company, Limited (Until July 19, 2018)
	Kiyotaka Ito	Staff General Manager Information Systems Department Meiji Yasuda Life Insurance Company (From July 20, 2018)
	Takashi Shiba	General Manager IT Strategy Planning Department Sompo Japan Nipponkoa Insurance Inc.
	Motohiro Uemura	Deputy Managing Director CIO Office Nomura Holdings, Inc.
	Mark Makdad	Director Fintech Association of Japan
	Toshio Taki	Director of Board Head of Fintech Institute Money Forward, Inc.

	Hironobu Todoroki	Head of Corporate Management, General Counsel, Liquid, Inc. Attroney at Law
	Takashi Murakami	Senior Specialist Business Development Group Planning Department Fourth Financial Sector NTT DATA Corporation
	Kenichi Fujii	Director of Financial Innovation Center Business Planning Unit Financial Information Systems Sales Management Division Hitachi, Ltd.
	Koichi Miyakawa	Senior Expert Financial Digital Innovation Technology Development Office Financial System Development Division NEC Corporation
	Akihiro Umegai	AWS Security Office of CISO Japan Amazon Web Services Japan K.K.
	Kazumi Hirose	Azure Technology Solutions Professional Intelligent Cloud Team Unit Microsoft Japan Co., Ltd.
	Yasuyuki Ogyu	Partner Deloitte Tohmatsu Consulting LLC
Observers	Sayuri Katayose	Chief Financial Inspector Head of Information Technology and Cyber System Team Risk Analysis Division Strategy Development and Management Bureau Financial Services Agency
	Chihomi Mukai	Deputy Director Banking, Payment and Insurance Regulations Office Policy and Markets Bureau Financial Services Agency (Until August 1, 2018)
	Takuhito Ogawa	Deputy Director Banking, Payment and Insurance Regulations Office Policy and Markets Bureau Financial Services Agency (From August 2, 2018 to September 26, 2018)

Yutaka Ogawa	Deputy Director Banking, Payment and Insurance Regulations Office Policy and Markets Bureau Financial Services Agency (From September 27, 2018)
Takahiro Kaku	Director Deputy Head of Computer System Risk and Business Continuity Group Examination Planning Division Financial System and Bank Examination Department Bank of Japan (Until September 26, 2018)
Takuya Okada	Director Head of Computer System Risk and Business Continuity Group Examination Planning Division Financial System and Bank Examination Department Bank of Japan (From September 27, 2018)
Toshikazu Okuya	Director Cybersecurity Division Commerce and Information Policy Bureau Ministry of Economy, Trade and Industry
Kimihiko Kimura	Counselor Office of the Director-General for Cybersecurity Ministry of Internal Affairs and Communications

(Secretariat: The Center for Financial Industry Information Systems)

Kiyoshi Hosomizo	President
Norikazu Takahashi	Exective Director
Hidekazu Shimura	Director General Planning Department
Hideki Osawa	Deputy Director Planning Department
Mitsuyoshi Miyagi	Director General General Affairs Department
Nobuo Koike	Director General Research Department
Masaaki Wada	Director General Security and Audit Research Department
Makoto Koriyama	Director Education Center

Secretariat Staff

Takahiro Arai, Takahiro Murayama, Hiroyuki Takane, Tetsuya Nakanishi, and Ryoya Inoue

Member List of
Working Group on API Connection Checklist for Financial Institutions

(Honorifics omitted; listed in no particular order)
(Organizations and titles as of meetings)

Members	Kazuhiro Nakamura	Manager e-Business Department Mizuho Bank, Ltd. (Until August 27, 2018)
	Kunihiro Ando	Manager e-Business Department Mizuho Bank, Ltd. (From August 28, 2018)
	Daisuke Mouri	Manager IT Management Division The Bank of Fukuoka, Ltd.
	Toshihiro Kubota	Leader of IT Strategy Group Sales Planning Department Keiyo Bank, Ltd.
	Tetsuo Yone	Deputy General Manager Operational Service Progress Department The Tama Shinkin Bank
	Norifumi Yoshimoto	General Manager FinTech Business Planning Dept. SBI Sumishin Net Bank, Ltd.
	Teppei Tosa	CISO & CIO freee K.K.
	Ataru Kobayashi	Integration Engineer Platform Moneytree KK.
	Takashi Ichikawa	Director of Board, CISO Money Forward, Inc.
	Masahiko Uchiyama	Project Manager Business Strategy Team Marketing Department Marketing Division Yayoi Co., Ltd.
	Takashi Murakami	Senior Specialist Business Development Group Planning Department Fourth Financial Sector NTT DATA Corporation
	Mikio Kamada	Consulting Solution Sales Representative Global Business Service Industry Solutions Banking & Financial Market IBM Japan, Ltd.

	Kei Taniuchi	Director Digital Business Division SYSTEMS UNIT 1 Fujitsu Limited
Observers	Yusuke Sano	Financial Inspector Risk Analysis Division Strategy Development and Management Bureau Financial Services Agency
	Chihomi Mukai	Deputy Director Banking, Payment and Insurance Regulations Office Policy and Markets Bureau Financial Services Agency (Until July 24, 2018)
	Takuhito Ogawa	Deputy Director Banking, Payment and Insurance Regulations Office Policy and Markets Bureau Financial Services Agency (From July 25, 2018)
	Kazuyo Ikeda	Deputy Director Banking Business Division I Supervision Bureau Financial Services Agency (Until June 25, 2018)
	Hiroaki Nagase	Financial Inspector Banking Business Division I Supervision Bureau Financial Services Agency (From June 26, 2018)
	Takahiro Kaku	Director Deputy Head of Computer System Risk and Business Continuity Group Examination Planning Division Financial System and Bank Examination Department Bank of Japan (Until August 27, 2018)
	Takuya Okada	Director Head of Computer System Risk and Business Continuity Group Examination Planning Division Financial System and Bank Examination Department Bank of Japan (From August 28, 2018)

Masafumi Miya	Director Head of Payments Innovation and FinTech Group FinTech Center Payment and Settlement Systems Department Bank of Japan (Until July 24, 2018)
Yasushi Sugayama	Director Head of Payments Innovation and FinTech Group FinTech Center Payment and Settlement Systems Department Bank of Japan (From July 25, 2018)

(Secretariat: The Center for Financial Industry Information Systems)

Norikazu Takahashi	Executive Director
Hidekazu Shimura	Director General Planning Department
Hideki Osawa	Deputy Director Planning Department

Secretariat Staff

Takahiro Arai, Takahiro Murayama, Hiroyuki Takane, Tetsuya Nakanishi, and Ryoya Inoue

API Connection Checklist
for Financial Institutions and API Connection Partners
Manual
<October 2018 Edition>

English translation based on the Japanese original published on October 12, 2018.

The Center for Financial Industry Information Systems
4th Floor, Sumitomo Irifune Bldg.
2-1-1 Irifune, Chuo-ku, Tokyo 104-0042
TEL: +81-(0)3-5542-6060 (switchboard)
FAX: +81-(0)3-5566-1052

Printed in Japan 2019