November 2024

National Risk Assessment -Follow-up Report

【 Digest Version 】

The Japanese version is the authoritative version, and the English version is for reference only.

- The National Public Safety Commission annually prepares and publishes the National Risk Assessment-Follow-up Report (hereinafter referred to as an “NRA-FUR”), which describes risks of misuse for ML/TF in each category of the transactions carried out by specified business operators and other matters under the Act on Prevention of Transfer of Criminal Proceeds.

- While taking into consideration the contents of the NRA-FUR, specified business operators submit STRs after having determined whether transactions are suspicious in regard to ML/TF, and also take measures for accurately performing verification at the time of transaction, and other matters.

- This document is a digest version of the NRA-FUR published in November 2024. For more details, refer to the full version of the NRA-FUR.

Table of Contents

Page number

1. Overview of NRA-FUR

Section 1. Risk Assessment Method				
Section 2. Environment Surrounding Japan				
	Geographic environment, social environment, economic environment, criminal environment			
Section 3. Analysis of Money Laundering Cases				
	1.Offenders	Boryokudan, Anonymous and fluid criminal groups, Crime groups of Foreigners in Japan		
	2.Modus Operandi	Predicate offences (thefts, frauds, etc.)		
		Major transactions misused for money laundering		
	3.Suspicious Transaction Report (STR)			
Section 4. High-risk Transactions				
	1.Transaction Types	Non-face-to-face transactions, cash transactions, cross-border transactions		
	2.Countries/Regions	Particularly high	Iran and North Korea	High / Myanmar
	3.Customer Attributes	Persons who intend to commit ML/TF		"Boryokudans" International terrorists
		Persons for whom it is difficult to conduct CDD		Non-residents, foreign PEPs, legal persons (legal persons without transparency of beneficial owners)
Section 5. Risk of Products and Services				
	Relatively higher risk than other business forms	Products and services dealt with by deposit-taking financial institutions Funds transfer services, cryptoassets Electronic payment instruments (expected to have a relatively higher risk)		
	Considered to be of risk	Insurance, investment, trust, money lending, foreign currency exchanges, financial leasing, credit cards, real estate, precious metals and stones, postal receiving services, telephone receiving services, telephone forwarding services, legal/accounting services		
	Products and services using new technologies that should be monitored closely	High-value electronically transferable prepaid payment instruments Casinos		
Section 6. Low-risk Transactions				
	Factors that Mitigate Risks	Source of funds is identified, the customer, etc., is the national government or a local public entity, the customers, etc., are limited under laws and regulations, the transaction process is supervised by the national government, etc. based on laws, etc., it is difficult to disguise the actual status of legal persons, etc. minimal or no fund-accumulation features, the transaction amount is less than the regulatory threshold, customer identification measures are secured by laws, etc.		
	Types of Low-risk Transactions			

1 Partial revision in offender classification

- ✓ “Online and telephone fraud group” have been changed to “Anonymous and fluid criminal groups,” （Analysis as offenders that engage in a wider range of fundraising activities）
- ✓ Descriptions have been added of fundraising activities such as investment /romance fraud via social media, which are seeing a sharp increase in cases

2 Deepening the analysis

- ✓ In light of the fact that shell companies or opaque companies and corporate accounts are being misused for ML, the analysis of legal persons (legal persons without transparency of beneficial owners, etc.) has been deepened

3 Introduction of international situations and cases

- ✓ From reports on cyber-related fraud (CEF) by the FATF, etc.
- ✓ The APG's typology report

4 Topics have been added and updated

- ✓ Consideration of revising FATF Recommendation 16
- ✓ International trends surrounding cryptoassets ,etc.

5 Examples have been added of STRs

- ✓ Examples of STRs of high-risk（non-face-to-face transactions, cash transactions, and cross-border transactions.）

6 Addition of “Items that the competent authorities have identified and that business operators should be aware of"

- ✓ Investigation of the operational aspects of risk mitigation measures for specified business operators

7 Readability function was added

- ✓ The table of contents was subdivided
- ✓ PDF bookmark function was added
- ✓ Charts were actively utilized ,etc.

3. Environment Surrounding Japan

✓ This section describes the geographic, social, economic and criminal environments that constitute the premise of ML/TF threats

✓ Describes only crime situation in this page

The number of recognized criminal offence cases

※The statistical date is from the year2023

- The total number of recognized criminal offence cases; 703,351

  ※Increased for the second consecutive year, returning to the pre=COVID-19 pandemic level
- The amount of damage from offences against property; Approximately 251.9 billion yen（+56.7% from the previous year）
- Looking at the breakdown of this figure, the amount of damage caused by fraud; Approximately162.6 billion yen（+ 85.4% from the previous year）

  ※ Increase in fraud damages partly due to rise in internet-based frauds

Situation of Phishing

- The number of reported phishing cases: 1,196,390 （+ 227,558 from the previous year, the highest number ever）
- Most of the phishing attacks were from offenders impersonating credit card operators and e-commerce business operators

Situation of Online Banking Fraud Cases

- The number of online banking fraud cases: 5,578
  The amount of damage: Approximately 8.73 billion yen（ both of which are the highest ever）
- The majority of victim are individuals, and by age, approximately 60% of victims are in their 40s to 60s.
- The breakdown of modus operandi: 53% were via email and 21% were via SMS
- More than 50% of the fraudulent remittance amounts were transferred to financial institution accounts of cryptoassets exchange service providers

Situation of Credit Card Fraud

- The amount of damage: 54.09 billion yen ※The worst since statistics began being collected in 1997

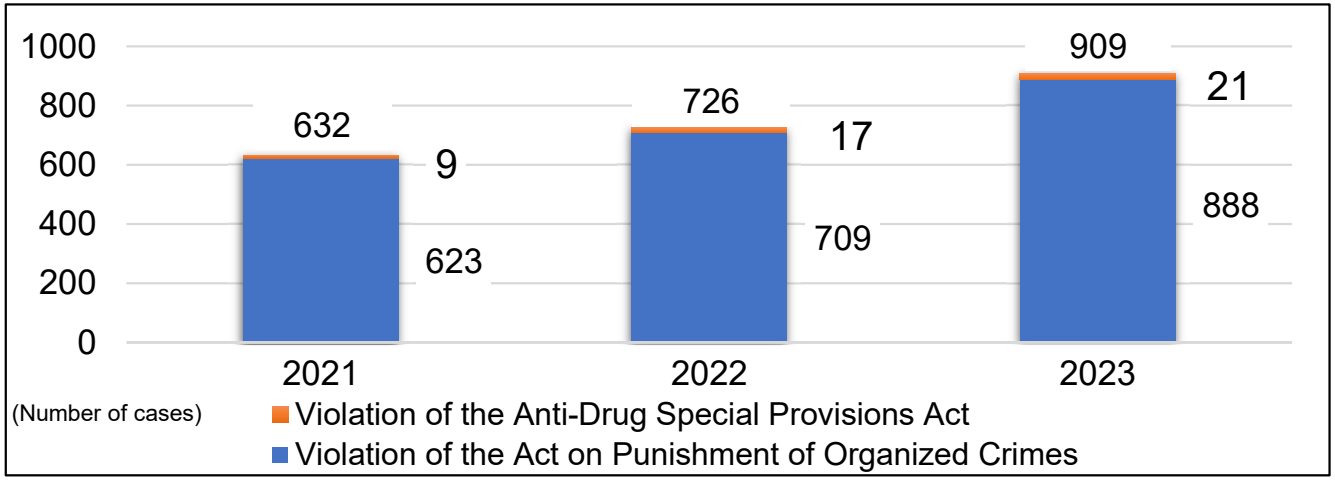
Situation of Ransomware

- The number of ransomware attack cases reported to the National Police Agency: 197 ※Remaining at a high level
- Many of them were victims of double extortion
- In many cases, criminals demanded payment in cryptoassets
- Regardless of size and industries, companies and organizations have become victims of ransomware attacks

4. Analysis of Money Laundering Cases

✓ This section analyzes the "offenders" and "predicate offences" that generate criminal proceeds, constituting the threat of ML/TF.

Number of Cleared ML Cases



Money laundering

- Money laundering refers to the concealment and receipt of proceeds obtained from certain predicate offences, as well as certain acts performed for the purpose of controlling the business management of companies, etc.
- Such acts are defined as crimes under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act

➢ An increase of 183 cases compared to the previous year

Status of Confiscation of Criminal Proceeds

			2021	2022	2023
Preservation for confiscation before prosecution					
	Act on Punishment of Organized Crimes	Number of cases	142	162	211
		Total amount of money and claims (thousand yen)	507,211	1,047,244	1,044,378
	Anti-Drug Special Provisions Act	Number of cases	24	23	20
		Total amount of money and claims (thousand yen)	32,712	25,363	45,427
Confiscation					
	Act on Punishment of Organized Crimes	Number of persons	72	76	119
		Amount (thousand yen)	217,888	205,665	353,107
	Anti-Drug Special Provisions Act	Number of persons	51	56	54
		Amount (thousand yen)	10,465	5,678	8,404
Collection of a sum of equivalent value					
	Act on Punishment of Organized Crimes	Number of persons	62	92	103
		Amount (thousand yen)	1,476,380	1,342,766	1,267,096
	Anti-Drug Special Provisions Act	Number of persons	226	223	199
		Amount (thousand yen)	854,361	860,989	394,524

➢ It is important to confiscate criminal proceeds in order to prevent them from being used to maintain and expand criminal organizations or to invest in future criminal activities

4. Analysis of Money Laundering Cases ～offender～

✓ There are various types of ML offenders, regardless of their nationality, type of crime, or whether or not they are organized

✓ mainly

Boryokudan, Anonymous and fluid criminal groups, Crime Groups of Foreigners in Japan

are picked up and analysed

※ Note that this article analyzes Anonymous and fluid criminal groups and Crime groups of foreigners in Japan as separate types of offenders, but some Crime groups of foreigners in Japan are also included in Anonymous and fluid criminal groups

Boryokudan

✓ ML by Boryokudan remains a serious threat

✓ Among cleared ML cases, 57 cases (6.3%) were related to Boryokudan gangsters【in 2023】

The characteristics of fundraising activities

- The fundraising activities by fraud have become established
- Boryokudan gangsters have been deeply involved in online and telephone fraud in leading positions
- Fundraising activities are conducted in a wide variety of areas, including finance, construction, labor dispatch, and adult entertainment businesses

An analysis of status of cleared ML cases

- By predicate offences, fraud, computer fraud, and theft were common
- Regarding criminal proceeds, the total amount (limited to those that can be monetized) was approximately 1.39 billion yen
- Compared to other offender, The cases involved receiving cash without involving any goods or services were common
- In domestic exchange transactions, nearly half of the accounts used were in the names of those closely related to Boryokudan gangsters

Anonymous and fluid criminal groups

✓ The scope of offenders has been expanded to include "Anonymous and fluid criminal groups" as offenders that engage in a wider range of fundraising activities, not limited to online and telephone fraud

Characteristics

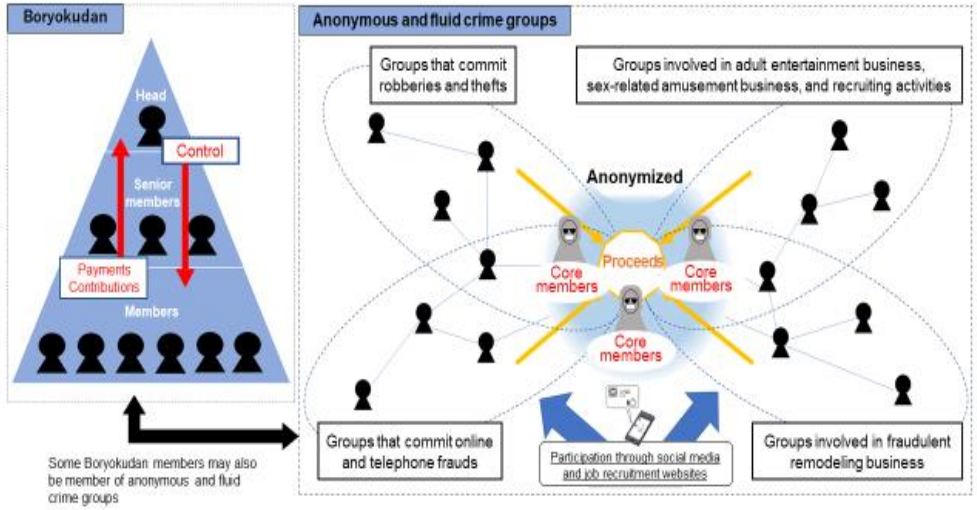
- Anonymity of core members and fluidity of crime actors
- Diverse fundraising activities and the return of criminal proceeds

Fundraising Crimes

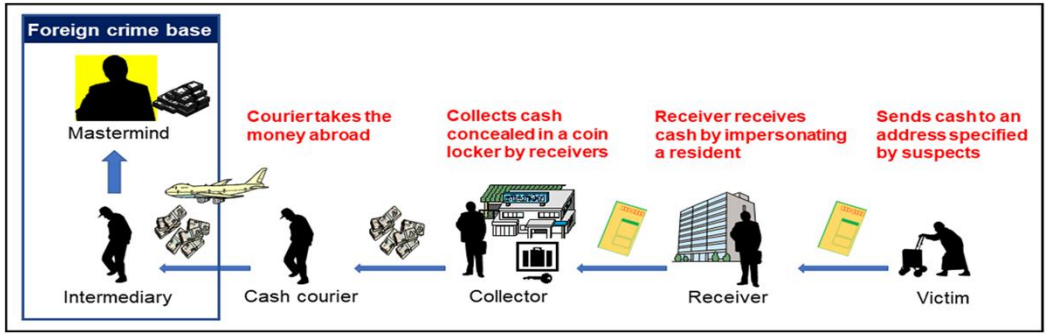
- Online and telephone fraud
- Investment /romance fraud via social media
- Armed robbery and theft (organized theft)
- Financing activities in bustling areas and nightlife spots
- Gambling offences related to online casinos
- Fraud and specified commercial transactions by malicious remodeling businesses
- Drug-related offences

Money laundering

- There have been cases of online and telephone fraud being committed from bases abroad, with criminal proceeds being transferred via foreign accounts, or by couriers to foreign countries
- The ultimate destination of criminal proceeds is core members



2023	Number of recognized cases (Number of cases)	Amount of damage (100 million yen)
Online and telephone fraud	19,038	453
Investment /romance fraud via social media	3,846	455



Crime Groups of Foreigners in Japan

- ✓ Criminal proceeds from offences in which foreigners are involved are difficult to trace because they are transferred across borders between countries with different legal and transaction systems
- ✓ There have been many cases in which domestic criminals, under instructions from instructors in foreign countries, have committed crime in an organized manner, and remitted criminal proceeds to foreign countries
- ✓ Of the cleared ML cases, 96 cases (10.6%) were committed by foreigners in Japan【In 2023】

An analysis of status of cleared ML cases committed

- ➢ By nationality, the majority of offender are from China and Vietnam（with China accounting for nearly half of the total）
- ➢ By predicate offences, fraud is the most common, followed by theft and violation of the Immigration Control and Refugee Recognition Act
- ➢ In terms of the type of transaction, domestic exchange transactions are the most common, followed by credit card transactions and prepaid payment instruments
- ➢ Among ML offences that involve the misuse of domestic exchange transactions and deposit transactions, over 50% use bank accounts under fictitious foreign names or other foreigners' names

Topic

Recent Situation Concerning Crimes Committed by Foreigners in Japan

- ● Looking at the situation regarding arrests of foreigners in Japan committing crimes, both the number of cases and the number of persons arrested in 2023 increased compared to the previous year
- ● The amount of loss from offences against property by foreigners in Japan arrested: About 3.24 billion yen (+1.34 billion yen compared to the previous year)

Vietnamese Nationals in Japan

- ➢ ML cases cleared by type of predicate offences: fraud 30.2%, theft 19.8%, violation of the Immigration Control and Refugee Recognition Act 14.6%
- ➢ Increased in intellectual crimes in recent years; many cases of mobile phone fraud at mobile phone sales agencies
- ➢ The existence of Vietnamese account trafficking organizations has also become evident, and in recent years, account trafficking by Vietnamese through social media has tended to increase in number

Chinese Nationals in Japan

- ➢ Types of Penal Code offences: theft 48.8%, intellectual crime 19.8%, and violent crimes 15.8%
- ➢ ML cases cleared by type of predicate offences: theft 41.8%, fraud 39.2%, computer fraud10.5%
- ➢ Chinese criminal organizations often form groups using regional and familial ties or by recruiting colleagues from their workplaces
- ➢ There have been instances of Chinese criminal organizations recruiting residents through social media to partake in criminal activities

Predicate Offences

- Predicate offences include offences that generate illegal proceeds and those subject to the death penalty, imprisonment with work for life or four years or longer
- Imprisonment without work offences listed in Tables 1 and 2 attached to the Act on Punishment of Organized Crimes
- Drug-related offences listed in the Anti-Drug Special Provisions Act

→ The threat of ML/TF

The size of generated criminal proceeds, relevance to ML offences, types of misused transactions, danger of fomenting organized crime, and impact on sound economic activities differ depending on the type of predicate offence

◆ Numbers of Cleared ML Cases under the Act on Punishment of Organized Crimes

Year \ Predicate offences	Fraud	Theft	Computer fraud	Violation of the Investment Act/Money Lending Business Act (Note 1)	Drug-related offences (Note 2)	Habitual gambling/ running a gambling venue for profit	Violation of the Immigration Control and Refugee Recognition Act	Violation of the Amusement Business Act	Violation of the Trademark Act (Note 3)	Document forgery offences (Note 4)	Other	Total
2021	243	217	42	26	9	12	16	14	8	4	57	648
2022	254	257	105	13	21	11	7	4	10	12	59	753
2023	334	319	160	16	22	17	6	9	9	9	54	955
Total	831	793	307	55	52	40	29	27	27	25	170	2,356

- Fraud and theft, accounted for approximately 70% of the total
- Computer fraud is on the rise

Topic

Flow of Criminal Proceeds from Cyber Enabled Fraud (CEF)

・・・FATF, Egmont Group and ICPO published a report in November 2023

Classifying CEF（Cyber Enabled Fraud）

① Business Email Compromise fraud（BEC fraud）
② Phishing fraud
③ Social media and telecommunication impersonation fraud
④ Online trading/ trading platform fraud
⑤ Online romance fraud
⑥ Employment scams

Characteristics of CEF

- CEF is a growing transnational organised crime
- CEF criminal syndicates are often well structured into distinct sub-groups with specialised areas of criminal expertise

Characteristics of money laundering

- Illicit proceeds from CEF are often transferred to foreign jurisdictions. These proceeds may then be further laundered through the financial systems of other third-party jurisdictions
- Regions that are highly cashless and digital-based are expectedly more vulnerable to the ML risks associated with this crime
- CEF-proceeds are rapidly laundered through a network of accounts
- These networks can be complex by extending across multiple borders and financial institutions, and CEF-related ML networks of accounts typically involve individuals as well as legal entities
- Individual money mules may be knowingly complicit in the laundering of funds or work unwittingly (through deception), or negligently, and may also be offered incentives or fees to handle the illicit funds
- Victims of CEF can often be tricked into acting as money mules
- The use of unhosted wallets, peer-to-peer transactions, peel chains, etc., are the preferred methods to launder cryptoassets-related CEF-proceeds, and are often used in combination

Key Focus Points When Submit STRs

※ See the full version

Major Transactions Misused for Money Laundering

- The police analyzed cleared ML/TF cases to examine what transactions were misused for ML/TF, summarizing the transactions, products and services that were misused for concealment and receipt of criminal proceeds, as well as products and services that were misused for transforming criminal proceeds obtained in the predicate offences (if any)

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Credit cards	Deposit transactions	Prepaid payment instruments (Note 1, Note 2)	Cryptoassets	Funds transfer services	Legal persons	Cross-border transaction (such as foreign exchanges)	Precious metals and stones	Financial instruments	Real estate	Foreign currency exchange	Legal/accounting professionals	Money lending	Bills and checks	Postal receiving services	Total
2021	208	72	40	40	21	9	9	16	9	2	2	0	1	1	0	0	0	430
2022	266	105	55	24	39	16	10	6	7	1	0	0	0	1	0	0	0	530
2023	311	129	51	36	40	29	21	15	11	3	3	4	2	0	2	1	1	659
Total	785	306	146	100	100	54	40	37	27	6	5	4	3	2	2	1	1	1,619

- The majority of transaction misused for ML involving products and services(domestic exchange transactions, cash transactions, deposit transactions)offered by deposit-taking financial institutions
- There are many cases where offenders have victims make payment to bank accounts opened in the name of fictitious or other parties through domestic exchange transactions, which enables prompt and secure fund transfers
- With the significant increase in fraudulent use of credit cards, the number of misuse cases has also risen
- There is an observable expansion in the misuse of various payment methods（prepaid payment instruments, cryptoassets, funds transfer services, etc.）

others There are also many ML cases without using the products and services of specified business operators
（example) Cases where mailed criminal proceeds were received under someone else's name after being left in a vacant room or a parcel box
Cases where criminal proceeds were concealed in coin lockers in online and telephone fraud

Topic **APG Yearly Typologies Report 2023**

- The Report published in December 2023 describes the ML situation and misused transactions in the Asia-Pacific region

◆Annual Reported Number of STRs by Business Type

Category \ Year	2021	2022	2023
	Number of reports	Number of reports	Number of reports
Financial institutions	495,029	542,003	661,838
Deposit-taking institutions	411,683	435,728	522,649
Banks	390,381	414,651	498,155
Shinkin banks, credit cooperative	18,461	18,520	21,636
Labour banks	318	316	397
Norinchukin banks, etc.	2,523	2,241	2,461
Insurance companies	3,458	3,939	4,575
Financial instruments business	19,718	19,032	20,550
Money lenders	35,442	45,684	63,954
Funds transfer service providers	10,499	20,271	29,232
Crypto-assets exchange service	13,540	16,550	19,344
Commodity derivatives business	388	318	846
Currency exchange operators	201	430	655
Electronic monetary claim	7	0	14
Other	93	51	19
Financial leasing operators	163	71	214
Credit card operators	34,904	41,106	45,674
Real estate brokers	4	11	18
Dealers in precious metals and stones	48	124	138
Postal receiving service providers	0	1	30
Telephone receiving service	0	0	0
Telephone forwarding service	2	1	17
Total	**530,150**	↑ **583,317**	↑ **707,929**

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators (excluding lawyers, etc. and judicial scriveners, etc.) to submit STRs to competent authorities if assets received in transactions related to specified business affairs are suspected of being criminal proceeds, or if there is suspicion of ML in connection with transactions related to specified business affairs

Examples of STR Utilization

- As awareness of AML/CFT has increased, the number of STRs has been increasing every year, and the content of these reports has also become more substantial
- In order to provide feedback to specified business operators that the reported information on suspicious transactions is being effectively used in the investigation of ML cases and their predicate offences, and to promote the understanding and efforts among specified business operators regarding STRs, the following introduces examples
- Introduced recent crime cases and trends reported by each investigative organization

【Examples of Cases in Which Investigating Authorities Other than the Prefectural Police Utilized STRs】

- Fraud case, theft case (Public Prosecutors Office)
- Cases of violation of Corporation Tax Act/Consumption Tax Act /Income Tax Act (National Tax Agency)
- Cases of smuggling of illegal drugs (Japan Customs)
- Cases of illicit trafficking of narcotics and methamphetamine (Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare)
- Understanding of the actual circumstances of poaching organizations (Japan Coast Guard)

- ✓ The following types were identified as transactions that affect the level of risk in transactions
  Non-face-to-face transactions, Cash transactions, Cross-border transactions
- ✓ They were analyzed and evaluated from
  - The perspective of inherent risks of being misused for ML/TF, typologies
  - Trends of STRs
  - Measures to mitigate risks

High risk

Non-Face-to-face Transactions

Inherent Risks of Being Misused for ML/TF

- Non-face-to-face transactions involve conducting transactions without direct face-to-face interaction with the counterparty
- There are limitations on the information available about the counterparty compared to face-to-face transactions
- Online non-face-to-face transactions have been increasing, driven by advancements in information and communication technologies and social situation
- It becomes easier for them to falsify their identity verification documents and personal identification details, impersonate others, and transfer bank or transaction accounts

Assessment of Risks

- As non-face-to-face transactions may hinder specified business operators from directly seeing customers and identification documents, the accuracy of customer identification can deteriorate
- Compared with face-to-face transactions, non-face-to-face transactions make it easier for offenders to falsify customer identification data and pretend to be a fictitious or other person by falsifying identification documents
- After identity verification has been completed, it is easier for a third party to conduct a transaction fraudulently than in face-to-face transactions

High risk

Cash Transactions

Inherent Risks of Being Misused for ML/TF

- Cash transactions are highly anonymous and they are unique in that the flow of funds is not easily traceable
- The vulnerabilities of products and services offered by specified business operators, combined with characteristics such as the liquidity of cash, can be misused for ML/TF
- In Japan, the balance of cash in circulation is high compared to other countries. the cashless payment ratio has been steadily increasing

Assessment of Risks

- Cash transactions have high liquidity and anonymity. Therefore, cash transactions may hinder the tracing of criminal proceeds
- In fact, there have been many cases where money launderers misused cash transactions

There is a risk
(Some transactions are risky)

Cross-border Transactions

Inherent Risks of Being Misused for ML/TF

- Japan conducts a large number of transactions as one of the leading international financial markets around the world
- Domestic legal and transaction systems vary from country to country, for example Nominee system, etc. Monitoring and supervision implemented in one country may not be applied in other nations
- By disguising trade transactions, criminal proceeds could be transferred
- Criminal groups committing online and telephone fraud are transferring criminal proceeds to foreign countries by transporting cash using cash couriers, transferring cryptoassets using foreign cryptoassets exchange service providers, and transferring funds via foreign accounts

Assessment of Risks

- In cross-border transactions, it is not easy to trace transferred funds compared to domestic transactions
- In fact, in some cases, ML has been conducted through cross-border transactions
- There is a risk that criminal proceeds obtained by Anonymous and fluid criminal groups and Crime groups of foreigners in Japan may be transferred back to foreign countries

High risk transactions

- ✓ Transactions related to countries and regions where proper AML/CFT measures are not implemented
- ✓ Cross-border remittances originated from large amounts of cash
- ✓ Transactions in which it is suspected that the customer is providing false information about the purpose or source of funds for a cross-border remittance

Topic ***Diversification of payment methods in cross-border transactions and consideration of revising FATF Recommendation 16 on transparency of transfers***

✓ Countries/Regions that require attention because they may influence transaction risks were identified. Then, they were analyzed and evaluated from the perspective of

- Factors that increase risks
- Measures to mitigate risks

Factors that Increase Risks

- The FATF identifies jurisdictions (countries/regions) with strategic AML/CFT deficiencies that have not made sufficient progress in addressing those deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies
- It also issues public statements that call on its member countries/regions to take AML/CFT measures in consideration of risks arising from the deficiencies, and strongly urges all countries/regions to do the same
- Those countries/regions identified as High-Risk Jurisdictions subject to a Call for Action have been published as the "blacklist"

Assessment of Risks

Very high risk	North Korea	Since February 2011, the FATF has continuously called on its members countries/regions to apply countermeasures, and has strongly urged all countries/regions to do the same, to protect the international financial system from the ongoing and substantial ML/TF risks emanating from North Korea
	Iran	The FATF requests all member countries, as well as other countries/regions, to completely terminate the temporary suspension of the countermeasures against Iran and apply the countermeasures from February 2020 in light of Iran's failure to develop internal collateral laws for executing the United Nations Convention against Transnational Organized Crime and international agreements to prevent the provision of funds for terrorism according to the FATF standards
High risk	Myanmar	Since October 2022, the FATF, considering that Myanmar has not made significant progress in addressing serious deficiencies in AML/CFT measures, has called upon member countries/regions to apply enhanced CDD measures commensurate with the risks emanating from Myanmar, and has strongly urged all countries/regions to do the same

- Transactions conducted with those countries/regions designated as the Jurisdictions under Increased Monitoring for improving the AML/CFT measures before the deficiencies pointed out by FATF are resolved are recognized to be risky
- Even if there are no direct transactions with these countries, malicious and shrewd methods may be used to redirect funds through neighboring countries/regions, so thorough measures need to be implemented, including verification at the time of transactions

Russia	During the FATF plenary meeting in February 2023, it was decided to suspend Russia's membership in the FATF. This decision was based on the conclusion that Russian Federation's actions unacceptably run counter to the core principles of the FATF, which aiming to promote security, safety, and the integrity of the global financial system and represented a gross violation of the commitment to international cooperation and mutual respect

✓ The customer attributes that affect transaction risks were identified as follows

○ Persons who intend to commit ML/TF:

Boryokudans, International terrorists(Islamic extremists,etc.)

○ Persons for whom it is difficult to conduct CDD:

Non-residents, Foreign PEPs, Legal persons (legal persons without transparency of beneficial owner)

✓ The above attributes were analyzed and evaluated from the perspective of factors that increase risks and measures to mitigate risks

High risk

Boryokudans

Inherent Risks of Being Misused for ML/TF

- Boryokudan have been committing various fund acquisition offences according to the changing times
  → the trafficking of stimulants, gambling , collection of protection money, theft, online and telephone fraud , fraud misusing public benefit programs, etc.
- It is increasingly difficult to define proceeds of crime. Boryokudan groups often conduct ML to avoid tracing of funds, taxation, and confiscation or to avoid being arrested for acquired funds
- Criminal proceeds are funds to maintain and strengthen organizations by using them as operating capital to commit further crimes or to obtain weapons. Criminal proceeds may also be used to interfere with legal businesses

Assessment of Risks

- ML is indispensable to “Boryokudans” and "Boryokudans" engage in ML
- In recent years, Boryokudan are actively engaging in activities to obtain funds in society while concealing the state of their organizations
- Anonymous and fluid criminal groups are increasing their illegal fundraising activities, such as online and telephone fraud, while coexisting and prospering with Boryokudan
  - ✓ It is necessary to examine CDD not only the direct counterparty to a transaction, but also to any substantive counterparties

High risk

International terrorists(Islamic extremists, etc.)

International Terrorism Situation

- Terrorist incidents believed to be related to Islamic extremists have occurred in various countries. As such, it can be said that the situation surrounding international terrorism remains severe
- No terrorist activity by terrorists designated by the United Nations Security Council has been confirmed in Japan
- It is therefore possible that those who are affected by extremism of ISIL and AQ affiliated organizations could commit terrorism in Japan

Characteristics of terrorist financing

- Terrorist financing ➡ Terrorist financing may be obtained through crimes or monetary assistance provided to foreign fighters by their families. It may also be obtained through activities disguised as legitimate transactions by organizations and companies
- Some transactions related to terrorist financing ➡ Some transactions related to terrorist financing may be conducted through cross-border remittances to financial institutions located in the regions under terrorist organizations' control. However, as such transactions may be smaller in value than transactions related to ML
- Money intended for terrorist financing ➡ Iraq, Syria, and Somalia, among others. in some cases, money is transferred through Turkey or other neighboring countries instead of going there directly.

Assessment of Risks

- Even when there have not been any cases of terrorist attacks or terrorist financing in a country, that fact does not immediately lead to the conclusion that the risk of terrorist financing is low
- The possibility of funds being collected in that country and being remitted abroad should not be excluded

Concerns in Japan

- ✓ Members of Islamic extremist and other terrorist groups hide themselves in communities of foreigners and misuse the communities for fundraising
- ✓ Foreign fighters engage in fundraising and other activities
- ✓ Persons who travel to conflict areas
- ✓ Terrorist financing may be provided through transactions disguised as legitimate ones conducted by Japanese organizations and companies
- ✓ Products and services provided by specified business operators (including cryptoassets transfer) may be misused without being monitored by the business operators

Topic

Risk of Abuse of Nonprofit Organizations for TF

・・・The FATF also calls its member countries to prevent nonprofit organizations from being abused by terrorists (※)

Vulnerabilities of nonprofit organizations

- They having gained societal trust, can access various funding sources
- They often handle significant amounts of cash
- Some operate in or near areas affected by terrorist acts, providing financial transaction frameworks
- There are instances where the entities raising funds for activities differ from those disbursing them, leading to a lack of transparency in fund usage

Assessment of Risks

- It should be noted that there have been no cases of nonprofit organizations being prosecuted for being exploited for terrorist financing in Japan
- limited number of nonprofit organizations conduct activities abroad

➡ It is considered that they are at a low risk of abuse

Nonprofit organizations in japan

・・・The section describe the risk assessment of nonprofit organizations conducted by the competent administrative authorities（CESNAs, Public Interest Corporation, Social Welfare Corporation, Medical Corporation, School Corporation, Religious Corporations,Other Organizations)

Nonprofit organizations an increased risk

- ✓ Nonprofit organizations operating in regions where terrorist activities are being carried out or in their vicinity
- ✓ Nonprofit organizations handling significant amounts of funds and conducting international fund transfers or cash transactions abroad
- ✓ Nonprofit organizations with unclear legal entities, such as those in a dormant state

※The FATF notes that measures to protect non-profit organizations from the misuse of terrorist financing must not hinder or prevent them from carrying out legitimate charitable activities

High risk

Non-resident Customers

Factors that Increase Risks

- Generally, the CDD measures, including identity verification and verification of assets and income, for non-residents are limited compared to those for residents
- Specified business operators may not have the knowledge needed to determine whether or not identification documents are authentic because the identification documents or supplementary documents used to verify the identity of non-residents are issued by foreign governments

Assessment of Risks

- When non-face-to-face transactions are conducted or when identification documents issued by foreign governments are used, anonymity will increase, and it is more difficult to track funds if ML/TF or the like is performed.

High risk

Foreign Politically Exposed Persons

Factors that Increase Risks

- Foreign politically exposed persons have positions and influence that can be misused for ML/TF
- Specified business operators' CDD, including verifying customer identification data and ascertaining the nature/transfer of their assets, is limited
- The strictness of laws against corruption varies from jurisdiction to jurisdiction

High risk

Legal Persons (Legal Persons without Transparency of Beneficial Owner)

Inherent Risks of Being Misused for ML/TF

- Legal persons are considered to have characteristics(Structure, Transactions, Corporation type) unique to legal persons that are different from natural persons

Vulnerabilities regarding ML/TF

- It enters the complex rights/control structure of a legal person, making the entity to which it belongs unclear and making it difficult to trace criminal proceeds
- By mixing criminal proceeds with legitimate business earnings, the source of illegal earnings can be made unclear
- By using services such as rental offices, it becomes possible to make up fictitious or exaggerated appearances of business trustworthiness, and business scale
- There is a risk that shell companies may be established in countries/regions serving as offshore financial centers and that the shell companies are misused to conceal criminal proceeds

Assessment of Risks

- Due to their unique characteristics, legal persons can easily conceal the criminal proceeds
- In fact, in recent years, there have been cases of ML that appear to deliberately exploit the unique characteristics of legal persons
  →In 2024, members of a criminal group were arrested for recruiting people to become representatives of shell company for rewards through social media, instructing them on how to set up legal persons and open legal person accounts, and laundering criminal proceeds using those accounts（managed approximately 500 shell companies and approximately 4,000 company accounts in an organized manner）
- It is extremely difficult to trace funds attributed to legal persons, especially legal persons without transparency of beneficial owners（FATF points out）

6. Risk of Products and Services

- ✓ This section assesses the risks of products and services provided by each type of specified business operators
- ✓ It also analyzes products and services using new technologies that should be monitored closely

Major Products and Services in which Risk is Recognized

- ➢ The assessment takes into account the scale of each business type and the vulnerability of each product/service, while analyzing the factors that increase the risks for each product/service provided by specified business operators, details of STRs, and measures to mitigate risks, assesses the risks of products/services

◆ The vulnerability factors that present particularly high risks regarding products and services

Vulnerability factor	Overview
Anonymity	Anonymity of source of funds through cash transactions, anonymity of non-face-to-face transactions in the Internet space, and anonymity through the creation of a fictitious appearance
Transferability	Ease of transferring funds and transferring rights (ownership, beneficiary rights, etc.) to third parties (transfer of rights holders)
Extensiveness	The geographical and attribute extensiveness of the counterparty of the transfer, including cross-border transactions
Convertibility	The convertibility of the source of funds by converting cash into other rights or goods, or by converting goods with high property value into cash
Complexity	Difficulty in tracing highly sophisticated and complex transaction types

◆ The results of the assessment of risks for each product or service provided by specified business operators

Risk level	Products and services
Transactions of relatively higher risk than other business forms	Products/services provided by deposit-taking institutions, funds transfer services, cryptoassets, and electronic payment instruments (expected to have a relatively higher risk)
Transactions considered to be of risk	Insurance, investment, trust, money lending, foreign currency exchanges, financial leasing, credit cards, real estate, precious metals and stones, postal receiving services, telephone receiving services, telephone forwarding services, and legal/accounting services

6. Risk of Products and Services

Products and Services Dealt with by Deposit-taking Institution

Relatively higher risk than other business forms

Vulnerability factor

- Anonymity
- Transferability
- Extensiveness
- Convertibility
- Complexity

- Deposit/savings accounts･･･Safe and secure fund management
- Deposit Transactions･･･Easily prepare and store funds anytime, anywhere
- Domestic Exchange Transactions･･･Allows quick and reliable transfer of funds between large numbers of people and across large distances
- Safe-Deposit Box･･･Allow safe storage of assets while maintaining confidentiality
- Bills and Checks･･･Excellent in terms of certainty of conversion into cash and ease of transport
- The situation in which accounts under the names of fictitious or other parties are being misused

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names (including suspected ones)
✓ Transactions made by numerous people ✓ Frequent transactions
✓ Transactions involving large amounts of remittances and deposits or withdrawals
✓ Transactions where sudden large deposits and withdrawals are made in accounts that normally do not move funds
✓ Transactions involving remittances, deposits, and withdrawals performed in an unnatural manner and frequency in light of the purpose of the account holders' transactions, occupations, and business contents
✓ Transactions involving deposits and withdrawals using the accounts of customers who have multiple accounts (including accounts held under different names using store names)

Insurance Dealt with by Insurance Companies, etc.

There is a risk

Vulnerability factor

- Convertibility

- Insurance products with cash accumulation features enable criminal proceeds to be converted to immediate or deferred

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Transactions in which an insurance premium is paid when a contract is concluded, and the contract is canceled soon afterward

There is a risk — Products and Services Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators

Vulnerability factor

- Extensiveness
- Convertibility
- Complexity

- They can convert proceeds into various rights such as stocks and use criminal proceeds to increase their profits
- Complex funds make it difficult to trace the origins of the funds

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

There is a risk — Trust Dealt with by Trust Companies, etc.

Vulnerability factor

- Transferability
- Complexity

- Trusts have the functions of altering the attribution, quantity, and nature of the property
- Offenders attempting ML/TF may be able to separate themselves from criminal proceeds and conceal the relationship with the proceeds if they misuse a trust

There is a risk — Money Lending Dealt with by Money Lenders, etc.

Vulnerability factor

- Anonymity
- Transferability

- Money lending by money lenders, etc., can make tracking criminal proceeds difficult
- There is a risk of misuse for generating criminal proceeds

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

Relatively higher risk than other business forms — Funds Transfer Services Dealt with by Funds Transfer Service Providers

Vulnerability factor

- Anonymity
- Transferability
- Extensiveness

- Characteristics of funds transfer services（foreign exchange transactions are performed as a business, Ease of transferring funds, Extensiveness, Anonymity）
- The existence of funds transfer service providers that offer services to remit to many countries abroad
- The existence of type I funds transfer services, which allow large amounts of foreign exchange transactions
- Substitutability from services offered by deposit-taking financial institutions
- The increase in both the annual number of remittances and the amount handled in the funds transfer business

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Transactions having unusual characteristics or conducted at an unusual frequency considering the purpose of the transactions, occupation, or business of the client, etc.
✓ Frequent remittance transactions from a large number of persons

Expected to have a relatively higher risk than other business forms — Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers

Vulnerability factor

- Anonymity
- Transferability
- Extensiveness
- Complexity

- Similar characteristics to cryptoassets（have a high degree of user anonymity and the nature of their transfers being instantaneous and cross-border）
- Given that they are more stable in value than cryptoassets
- They may be used as a means of remittance and payment in a wide range of fields in the future
- The environment surrounding electronic payment instruments could rapidly change, potentially leading to a swift change in their risk level

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

Relatively higher risk than other business forms

Cryptoassets Dealt with by Cryptoassets Exchange Service Providers

Vulnerability factor

- Anonymity
- Transferability
- Extensiveness
- Complexity

- Cryptoassets allow users to be anonymous and enable instant cross-border transfers
- Some countries have no or inadequate regulation on cryptoassets. If cryptoassets exchange service providers in these countries are abused for crimes, it is difficult to trace the transfer of such cryptoassets
- There are cases where persons who intend to commit ML/TF use cryptoasset transactions in addition to products and services handled by deposit-taking institutions
- Cryptoassets transactions are increasing globally and the environment surrounding such transactions is rapidly changing

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

Topic **International Trends in Cryptoassets**

・・・ Introducing "Targeted Update on Implementation of the FATF Standards"

- It points out the differences in regulation of cryptoassets among countries and challenges such as market changes due to the introduction of new technologies
- It is necessary to continuously pay attention to the risks of ML/TF in cryptoasset transactions

There is a risk

Foreign Currency Exchanges Dealt with by Currency Exchange Operators

Vulnerability factor

- Anonymity
- Convertibility

- Foreign currency exchange can be a part of a strategy to take the proceeds of crime abroad
- Foreign-currency exchange is usually carried out in cash
- Foreign currency exchange is highly liquid and can be possessed or transferred without information about the bearer

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Frequent transactions in a short period
✓ Transactions in which it is suspected that the customer intentionally avoided verification at the time of transactions
✓ Transactions related to currency, etc., that was a counterfeit or stolen currency or suspected like that
✓ Transactions in which it was suspected that the customer was acting on behalf of other people

There is a risk Financial Leasing Dealt with by Financial Leasing Operators

Vulnerability factor

- Transferability

➢ A lessee and a seller being able to conspire to conduct a false transaction

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Transactions related to financial leasing in which it is suspected of defrauding a financial leasing operator out of money under multiple financial leasing contracts
✓ Transactions related to financial leasing in which it is suspected that a lessee, etc., intends to defraud a financial leasing operator out of money by concluding several leasing contracts based on the same facilities

There is a risk Credit Cards Dealt with by Credit Card Operators

Vulnerability factor

- Transferability
- Convertibility

➢ They can transform criminal proceeds obtained in cash into another form of assets by utilizing the credit

➢ By using fraudulently obtained credit card information to apply for the purchase of goods and then impersonating someone else to receive them, it is possible to disguise the fact of acquiring criminal proceeds

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Transactions related to a customer who frequently purchases large amounts of cash equivalent, such as gift cards, by using credit cards

There is a risk — Real Estate Dealt with by Real Estate Brokers

Vulnerability factor

- Anonymity
- Convertibility

- Real estate has high value and can be exchanged for large amounts of cash
- It is possible for offenders to transfer criminal proceeds by, for example, paying more than the market value for a property
- Recently, there have been many cases where real estate was purchased for the purpose of preserving assets or investment
- There is a risk that crime organizations in and outside Japan, etc. have been misusing real estate transactions to change the form of criminal proceeds
- Conducting a transaction for a large amount that does not match the attributes of the customer requires a response corresponding to the risk, such as verification of the source, etc. of the purchase fund, in addition to the attributes of the customer

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

There is a risk — Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones

Vulnerability factor

- Anonymity
- Convertibility

- Precious metals and stones have high financial value, are easy to transport and exchanged with cash all over the world
- Precious metals and stones are highly anonymous because it is difficult to trace their distribution channel and location after transactions
- In particular, gold bullion are usually purchased with cash

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ The same person/company buying and selling a large amount of precious metals in a short period
✓ Transactions of frequent purchases resulting in a large amount, even if the purchase amount at the time is small
✓ Purchases or sales with high value that are not proportionate to the customer's income or assets, etc.

There is a risk Postal Receiving Services Dealt with by Postal Receiving Service Providers

Vulnerability factor

- Anonymity

- Postal receiving services are misused to provide locations for sending proceeds derived from crime, such as fraud and sales of illegal goods
- It can be difficult to identify the party committing the ML/TF or ownership of the criminal proceeds
- Postal receiving service providers neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies in their internal control systems, which may increase the risks that postal receiving services present

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names
✓ Transactions with customers who often receive large amounts of cash
✓ Transactions in which it is suspected that customers might use the service to disguise the company's actual status
✓ Transactions with a customer who plans to make contracts for a postal receiving service using multiple companies' names

There is a risk Telephone Receiving Services Dealt with by Telephone Receiving Service Providers

Vulnerability factor

- Anonymity

- Telephone receiving services have the characteristic of enabling customers to create a fictitious appearance for their business and to disguise the principal of an ML/TF operation and the ownership of criminal proceeds unclear

There is a risk — Telephone Forwarding Services Dealt with by Telephone Forwarding Service Providers

Vulnerability factor

- Anonymity

- By using telephone forwarding services, customers can give their business a false appearance and conceal the offenders committing ML/TF or the ownership of criminal proceeds
- Telephone forwarding services present a risk of being misused for ML/TF concealing the criminal proceeds obtained from online and telephone fraud, etc.
- Telephone forwarding service providers' neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies in their internal control systems, which may increase the risks that telephone forwarding services present

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

There is a risk — Legal/Accounting Services Dealt with by Legal/Accounting Professionals

Vulnerability factor

- Anonymity
- Complexity

- Legal/accounting professionals have high social credibility
- Legal/accounting professionals utilize their advanced expertise to be involved in various transaction activities
  - Acts or procedures concerning buying and selling residential lots and buildings
  - Acts or procedures concerning the establishment or merger of companies
  - Management or disposal of cash, deposits, securities, and other assets

The transactions become even more risky

✓ Transactions under anonymous or fictitious, borrowed, and false names

Products and Services Using New Technologies That Should Be Monitored Closely

High-Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers

- By international brand prepaid payment instruments
  - Services allowing deposits of tens of millions of yen are also provided
  - These international brand prepaid payment instruments, utilizing the payment infrastructure of the brand's credit cards, can be used at affiliated stores of the brand, including online, offering the same service functions as the credit cards

➡ They could be considered to have at least the same risk level from an ML/TF perspective

Risks of prepaid payment instruments

- ✓ The availability of prepaid payment instruments, including online stores, has expanded, and their forms and methods of use are diverse
- ✓ Because identity verification is not required for use, they can be considered to have a high degree of anonymity
- ✓ There have been cases where prepaid payment instruments were misused in the ML process, with an increasing trend in such incidents

Casinos

- A report published by FATF pointed out the risk of ML/TF stemming from casinos as follows
  - Casinos are a cash-intensive business, with a high volume of large cash transactions taking place very quickly
  - Casinos offer various financial services (accounts, remittance, foreign exchange, etc.)
  - In some jurisdictions, poorly regulated or unregulated for AML/CFT

Topic **Report on ML and International Organized Crime Related to Online Casinos**

- In a report published, UNODC warned that international organized crime in Southeast Asia has been rapidly developing and expanding in recent years by incorporating the latest information technology
- Among other things, the report pointed out the following matters regarding ML by criminal organizations through the misuse of online casinos
  1. Recent situations regarding casino-related ML in Southeast Asia and surrounding regions
  2. Characteristics and modus operandi of ML using online casinos

《Information》 JAFIC website, etc.

JAFIC TOP PAGE

✓ https://www.npa.go.jp/sosikihanzai/jafic/index.htm

Annual Report and National Risk Assessment Follow-up Report

➢ https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/nenzihokoku.htm

Reference cases of suspicious transactions

➢ https://www.npa.go.jp/sosikihanzai/jafic/todoke/gyosei.htm

THE WHITE PAPER

✓ https://www.npa.go.jp/publications/whitepaper/index_keisatsu.html

Statistics and other data held by the National Police Agency (Online and telephone fraud, Organized Crime, Crime Statistics, etc.)

✓ https://www.npa.go.jp/publications/statistics/index.html

JAFIC
Japan Financial Intelligence Center