# Cybersecurity Business Opportunities and Environment in Japan

Hiromichi Nakahara

Ministry of Economy, Trade and Industry, Japan

1. Market Trend (1)General Overview

■With coming in force of "The Basic Act on Cybersecurity"(Note1), Japanese government has instituted Cybersecurity Strategic Headquarters and Cabinet Secretariat National center of Incident readiness and Strategy for Cybersecurity(NISC) in January 2015 to strengthen the system.

■In recent times, cyber attacks have become quite smart and sophisticated and run the risk of inflicting serious damage. In order to minimize the damage by cyber attacks, importance of thorough security countermeasures and monitoring services is increasing.

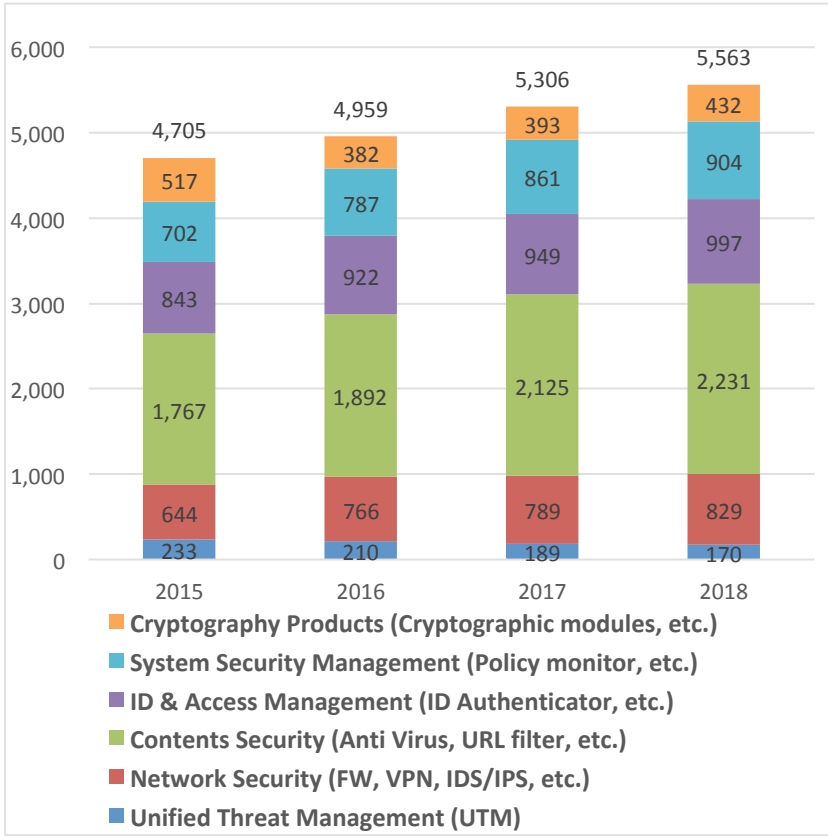2016   948.2 billion yen

2017   996.5 billion yen

2018   1045.5 billion yen （Over a trillion yen）
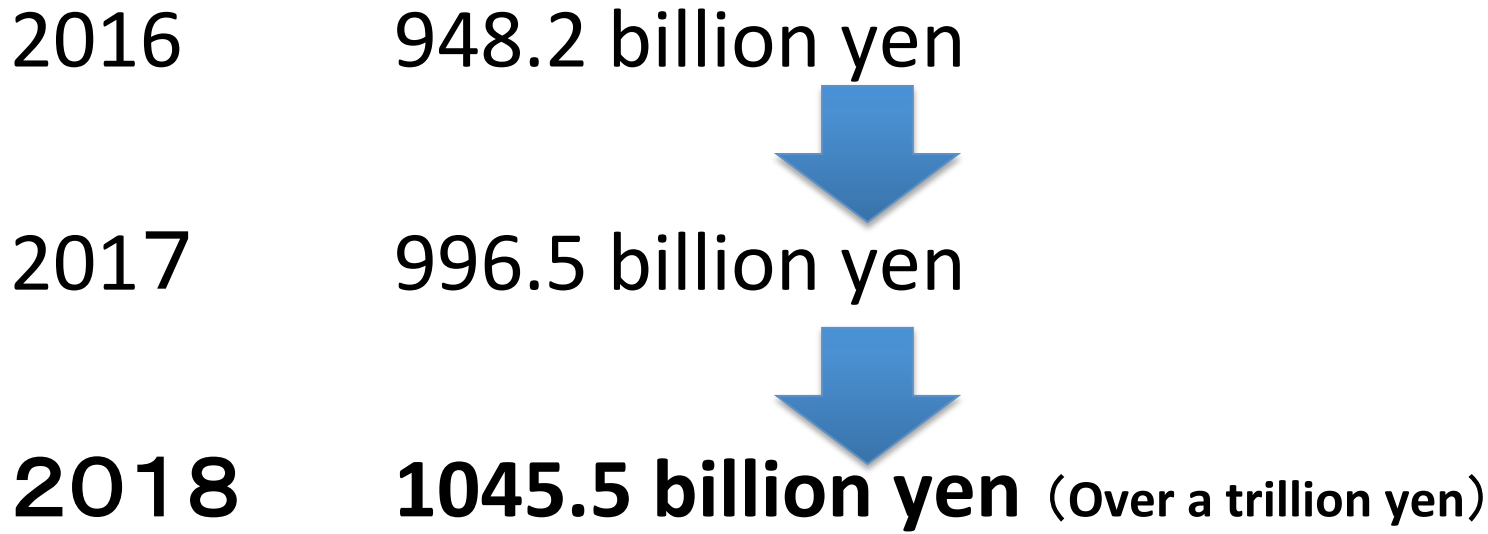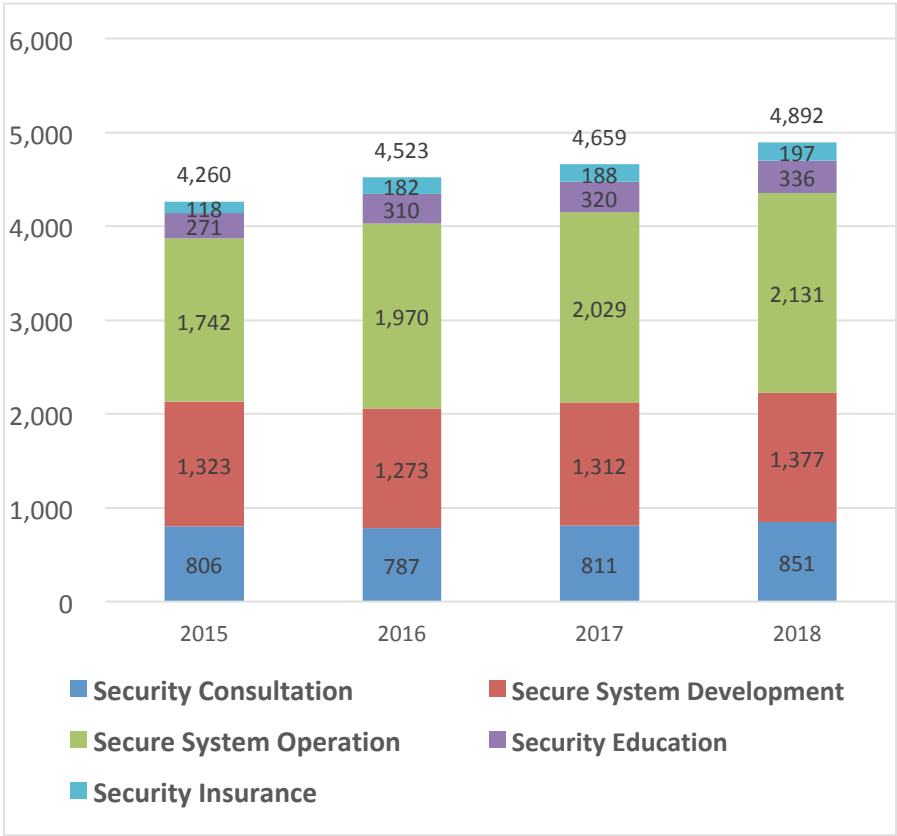
※Expectancy

[Source] Japan Network Security Association "Domestic Cyber Security Market2017's investigation report(preliminary figures)".

1. Market Trend (2) Products and Services

■ Both Products and Services Market expand.
■ The Growth of Services Market in 2018 is slightly higher than that of Products in 2018.

Products chart (left):

	2015	2016	2017	2018
Total	4,705	4,959	5,306	5,563
Cryptography Products	517	382	393	432
System Security Management	702	787	861	904
ID & Access Management	843	922	949	997
Contents Security	1,767	1,892	2,125	2,231
Network Security	644	766	789	829
Unified Threat Management (UTM)	233	210	189	170

- **Cryptography Products (Cryptographic modules, etc.)**
- **System Security Management (Policy monitor, etc.)**
- **ID & Access Management (ID Authenticator, etc.)**
- **Contents Security (Anti Virus, URL filter, etc.)**
- **Network Security (FW, VPN, IDS/IPS, etc.)**
- **Unified Threat Management (UTM)**

Services chart (right):

	2015	2016	2017	2018
Total	4,260	4,523	4,659	4,892
Security Insurance	118	182	188	197
Security Education	271	310	320	336
Secure System Operation	1,742	1,970	2,029	2,131
Secure System Development	1,323	1,273	1,312	1,377
Security Consultation	806	787	811	851

- **Security Consultation**
- **Secure System Development**
- **Secure System Operation**
- **Security Education**
- **Security Insurance**

Changes of scale in the market of
Domestic Cyber Security <u>Products</u>

Changes of scale in the market of
Domestic Cyber Security <u>Services</u>

【Source】Japan Network Security Association "Domestic Cyber Security Market2017's investigation report(preliminary figures)".
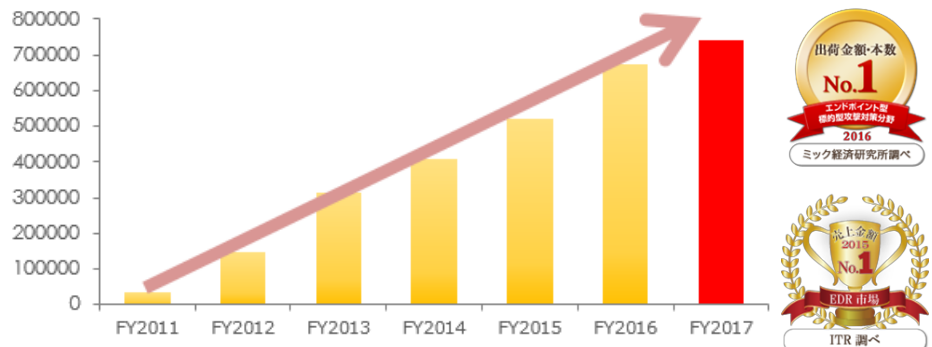
2. Japanese Major Players (1) Companies

■Japanese companies pursue development and expansion of services using advanced technology. (Examples)

Next Generation Endpoint Protection
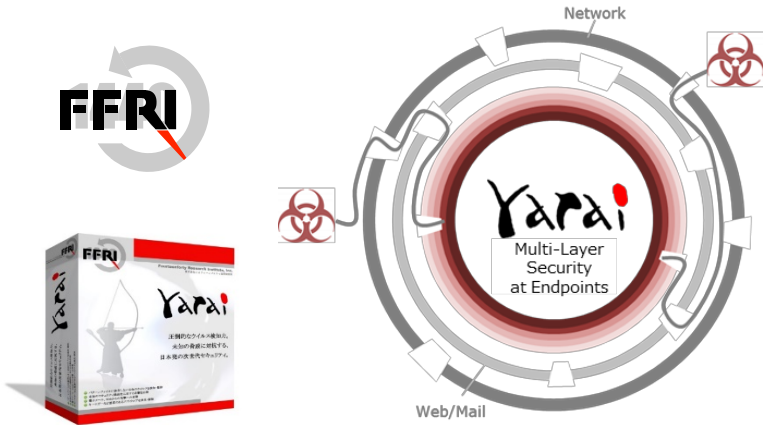
FFRI In-house Study | Strong Trend in Installation Licenses

*Sources : MIC Research Institute, "Status and Future Prospects of Information Security Solutions Market 2016
[External Attack Protection Solutions Edition]"
: ITR, "ITR Market View: Information Leakage Countermeasure Market 2016"

Name of company	Core Business in this field	Net sales (M yen)	Note
NEC Corporation	• It will deploy services such as "Security-integrated management and response solutions" where devices like servers and PCs connected to internal network will be centralized control in real time and "Threat and vulnerability information management solutions" that instantly provides information on and method to deal with cyber attack. • In February 2017 it started Security Consulting service for corporates.	2,665,000 2,844,447	FY March, 2017, Consolidated FY March2018
Internet Initiative Japan Inc.	• It will implement technical validation that will dynamically change the monitoring level of security on cloud and control unauthorized communication. It expanded the scope of validation to office network and devices in October 2017 and started demonstration experiment. It plans to offer full-range security as network service solution by the latter half of 2018.	157.790 176,040	FY March, 2017, Consolidated FY March 2018
LAC Co., Ltd.	• As the leading Japanese company in the field of cyber security, it will expand the service offerings utilizing state-of-the art technologies in security domain against cyber attacks that will target global events like Tokyo Olympics and Paralympics 2020 by re-building "JSOC" security monitoring center, building CSITR and providing support for its operation, enhancement of specialists capable to carry out security diagnosis service etc. • Registered as METI Information Security Audit Company.	37,109 38,432	FY March, 2017, Consolidated FY March2018

[Source] JETRO "Market report: Business Opportunities related to the Olympics and the Paralympics" March 2018, Website of each companies, Press release materials.
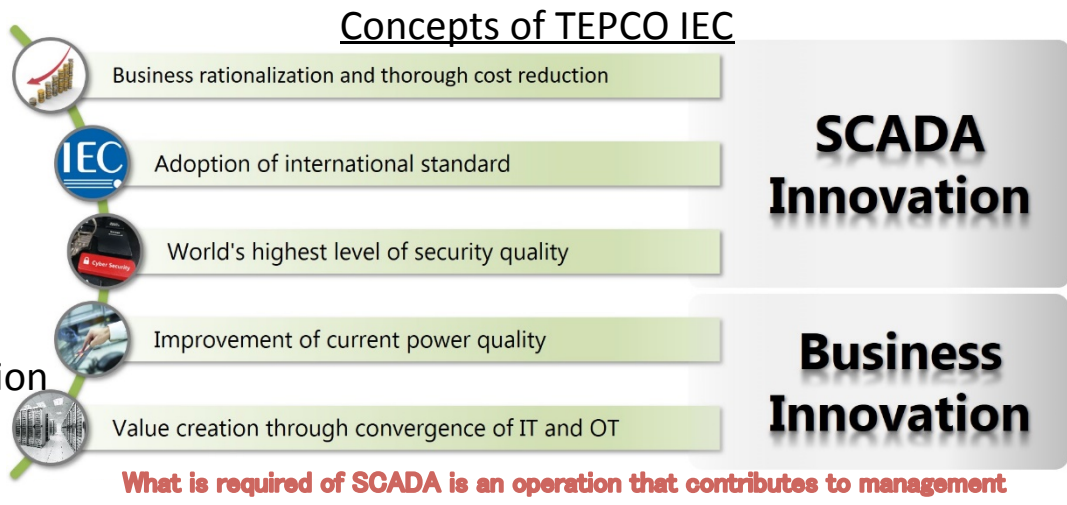
2. Japanese Major Players (1) Companies

■Japanese companies pursue development and expansion of services using advanced technology. (Examples)
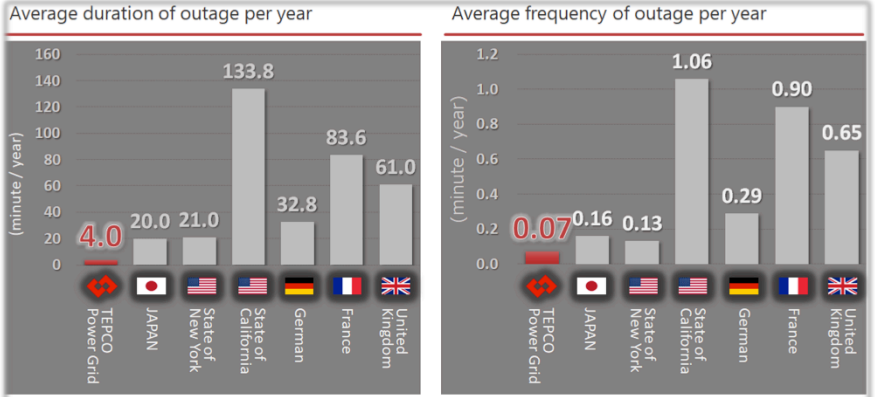
◆ In Industrial Control System, or "Ooperation Technology", Infrastructure Industry also enters into Cyber security Market and promotes overseas business expansion.
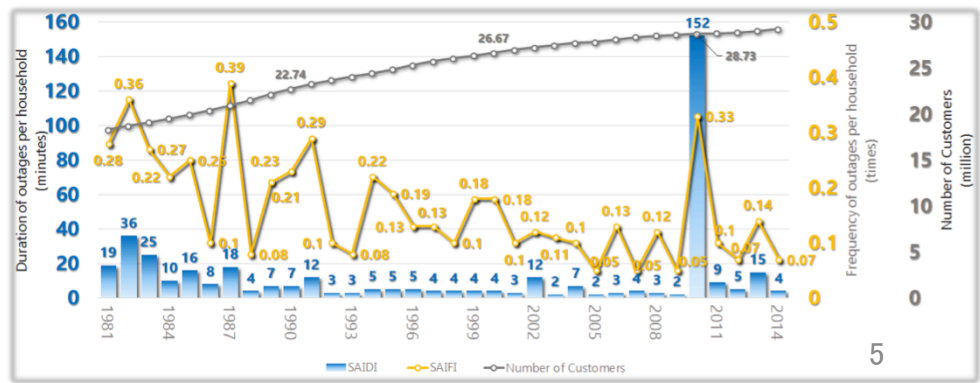
Ex) TEPCO IEC
-TEPCO IEC is a design and operation consulting company for power control systems, established in 2017.
-Putting emphasis on SCADA(Supervisory Control And Data Acquisition).
-Promoting overseas expansion in cooperation with McAfee, NTT Data and so on.

Concepts of TEPCO IEC

Business rationalization and thorough cost reduction

IEC — Adoption of international standard

World's highest level of security quality

SCADA Innovation

Improvement of current power quality

Value creation through convergence of IT and OT

Business Innovation

What is required of SCADA is an operation that contributes to management

World-class high power quality

Average duration of outage per year (minute / year)

Location	Value
TEPCO Power Grid	4.0
JAPAN	20.0
State of New York	21.0
State of California	133.8
German	32.8
France	83.6
United Kingdom	61.0

Average frequency of outage per year (minute / year)

Location	Value
TEPCO Power Grid	0.07
JAPAN	0.16
State of New York	0.13
State of California	1.06
German	0.29
France	0.90
United Kingdom	0.65

In the world

In the TEPCO

5

2. Japanese Major Players (2)International Collaboration

IPA CoE Global Training in Core Resource Development Program (France and UK)

Training in France

- September 17–18, 2018, 18 trainees from Japan visited universities and research laboratories in France to attend training to get better understanding of global standards and advanced level initiatives in cybersecurity and to have opportunities of networking with the local top level organizations and professionals.

Training at a French laboratory

Training in UK

- December 3–4, 2018, 33 trainees from Japan visited UK to attend training by government organizations and representatives of auto and finance industries as well as start-up companies in cybersecurity.

Training by auto industry cybersecurity professionals（UK）

Note: Contents in this page were provided by IPA.

3. Situation of Major Overseas Companies Entering the Market

- Examples of entry of security related foreign companies in the Japanese market.
- In recent years, entry of companies that possess information security technologies using AI has increased to provide safe guard against cyberattacks. They include Israeli companies that are armed with advanced technical competence.

Name of Overseas company	Home country	Timing for entry in Japan (launch of products)	Conditions of entry to Japanese Market
Darktrace	UK	2015	• It was established in 2013. It markets "Enterprise Immune System" that detects threat in real time based on machine learning and mathematical theory developed at the Cambridge University and offers countermeasures against cyber attack utilizing self learning technology.
Votiro,Inc.	Israel	2015	• It was established by the alumnus of Israel's intelligence agency. • It offers the software "Secure Data Sanitization" that provides protection against e-mail based virus infection. It is drawing attention for its 'harmless' defense technology that eliminates the part that is likely to be affected by virus and delivers only the required data.
Cybereason Inc.	US	2016	• It offers solution "Cybereason" developed by the members who were involved in cyber security at the intelligence forces of Israel army. Putting to use the combat experience of the founders cultivated on the forefront of cyber attack, it continuously monitors the activities unique to cyber attacks. It can immediately detect illegal behavior even if it is unknown malware. • Its Japan subsidiary was established in 2016.
Fireglass, Inc.	Israel	2017	• It was launched in Japan from June 2017. When browsing an external site from a PC in the company, it offers solution where relay server establishes access in place of PC. Thus, even if it accesses a site infected by virus, PC of the person browsing is not affected and is cut off by the relay server.

[Source] JETRO "Market report: Business Opportunities related to the Olympics and the Paralympics" March 2018

4. Government Support for Market Expansion

(1) Tax system for encouraging IoT investment with security

- When a company invest for IoT systems (e.g., robots) for improving the productivity, they can earn the corporate tax reduction from around 30% up to around 25%.

- As a prerequisite for having this tax reduction, the corporation should implement certain security measures.

  → Encourage security investment

<Case>

If a company submit a business plan for investing to a smart factory with certain security measures which can improve productivity, the corporate tax will be reduced up to 5%.

Source: Mistubishi Electric HP

Corporate tax amount

About 30%

↓

Up to about 25%

4. Government Support for Market Expansion (2)Regulatory Sandbox

1. New Regulatory Sandbox framework in Japan

- The Government of Japan (GOJ) introduced this framework on June 6, 2018 as one of the mechanisms for regulatory reform to facilitate realization of innovative technologies and business models in Japan.

- The framework does not limit the area of regulations, but covers those on financial services, healthcare industry, mobility and transportation.

- Companies, including overseas companies, can
  - apply to conduct "demonstrations" under this new framework and
  - test the possibilities of using innovative technologies such as AI, IoT or block chains for future business,

especially when they cannot start businesses due to existing Japanese regulations.

Overview of the process for regulatory reform

In cases where
- you would like to conduct business activities which utilize new technologies or new business models,
- but they conflict with existing Japanese regulations, because they do not assume such new technologies:

→ You can apply to conduct operations not as business activities but as "demonstrations" with limited time periods and participants.

→ Data collected through the demonstrations will be utilized in deliberation for regulatory reform, which will facilitate the creation of such innovative business activities with new technologies and new business models.

Contact: GoJ's Regulatory Sandbox Team at Japan Economic Revitalization Bureau, which works as the single window of the GoJ （Government of Japan）
http://www.kantei.go.jp/jp/singi/keizaisaisei/regulatorysandbox.html
E-mail: Shingijutsu_sb@cas.go.jp
Tel: +81 3－3581-0769

If you are of an overseas company or a foreign-affiliated company in Japan, you can consult the ''Invest Japan Hotline" of JETRO before consulting the GoJ's Regulatory Sandbox Team.
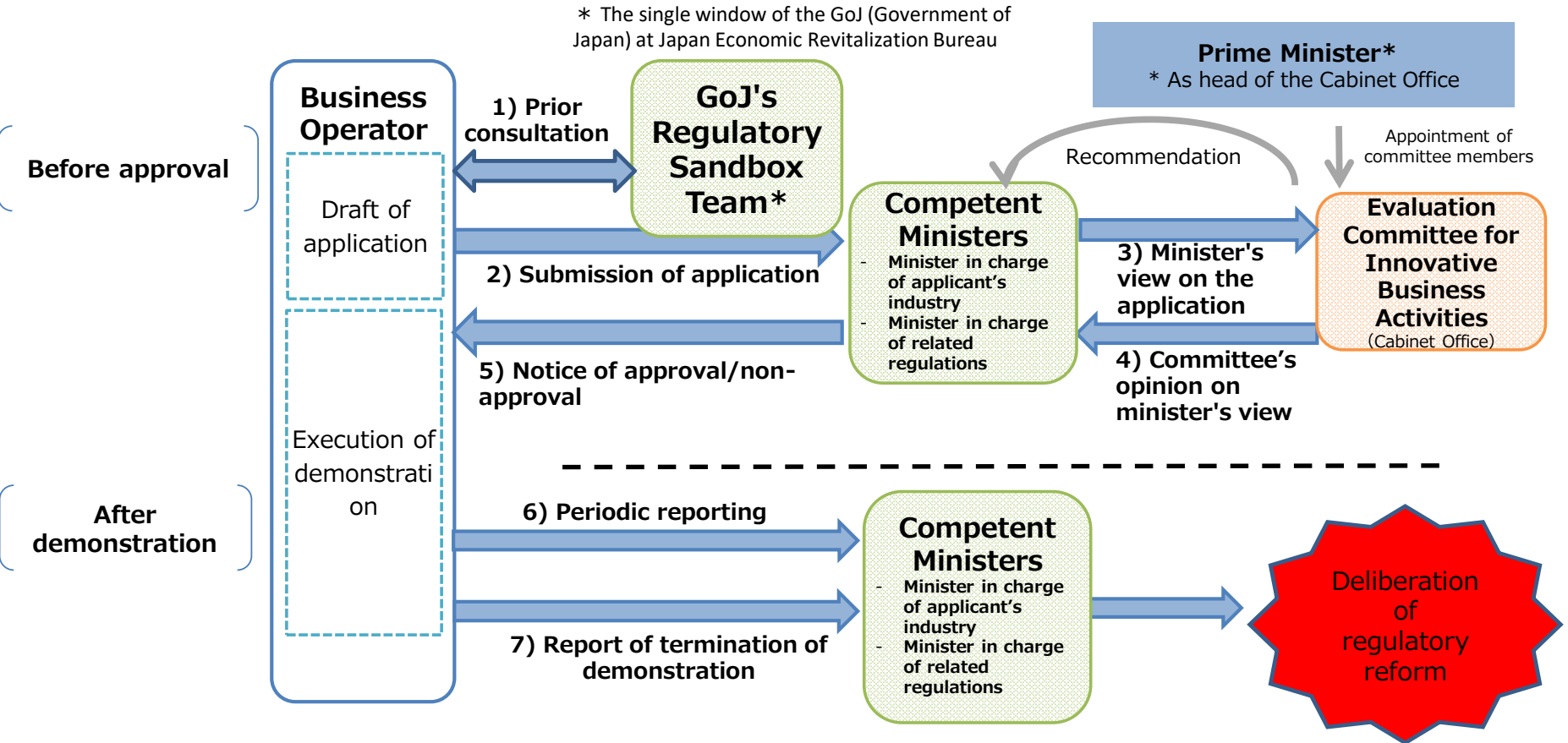https://www.jetro.go.jp/en/invest/hotline.html
E-mail: Please send by "Inquiry Form"
Tel: +81 3-3582-4684

2. Process under Regulatory Sandbox (RS) framework

＊ The single window of the GoJ (Government of Japan) at Japan Economic Revitalization Bureau

Prime Minister*
* As head of the Cabinet Office

Before approval

Business Operator

Draft of application

1) Prior consultation

GoJ's Regulatory Sandbox Team*

Recommendation

Appointment of committee members

Competent Ministers
- Minister in charge of applicant's industry
- Minister in charge of related regulations

2) Submission of application

Evaluation Committee for Innovative Business Activities
(Cabinet Office)

3) Minister's view on the application

5) Notice of approval/non-approval

4) Committee's opinion on minister's view

Execution of demonstration

After demonstration

6) Periodic reporting

7) Report of termination of demonstration

Competent Ministers
- Minister in charge of applicant's industry
- Minister in charge of related regulations

Deliberation of regulatory reform

10

4. Government Support for Market Expansion (2)Regulatory Sandbox

3. Support when using "Regulatory Sandbox" framework

Business
Operator

1.Consultation

2.Support

JETRO

3.Consultation
On proposals

4. support

GoJ's Regulatory
Sandbox Team

5.Application

opinion from
the Evaluation Committee

Competent
Minister

6.Screening
and
Decision

7. Approval

8. Support

Demonstration

9. Review the regulations
where necessary
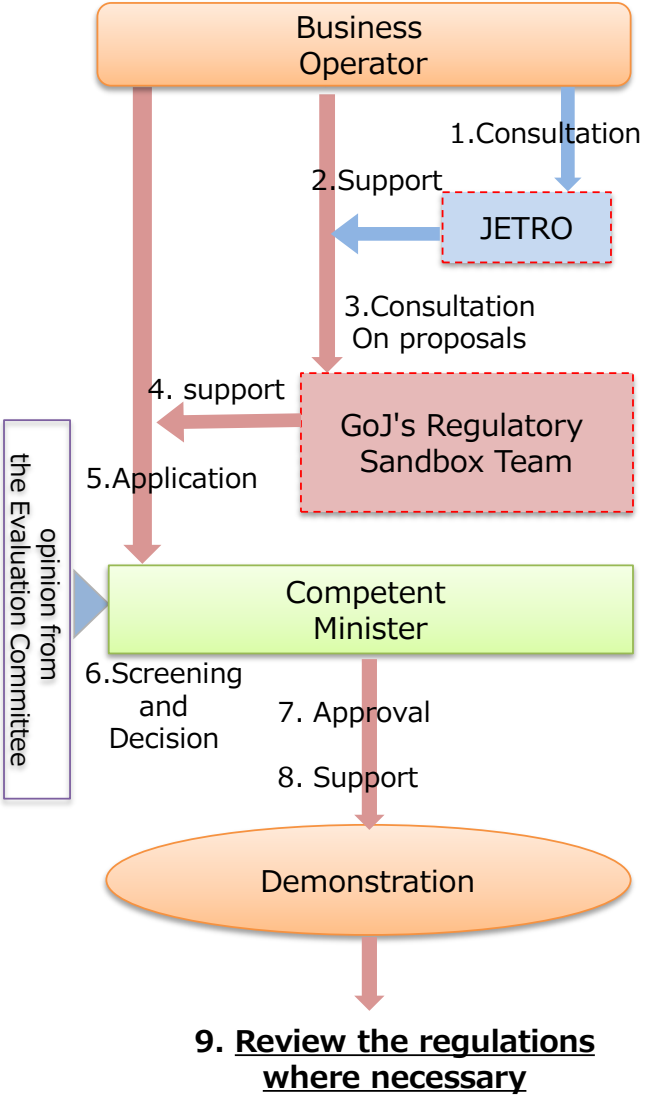
1. If you are of an overseas company or a foreign-affiliated company in Japan, you can consult JETRO before consulting the GoJ's Regulatory Sandbox Team.

2. JETRO will support you to consult the GoJ's Regulatory Sandbox Team.

3,4,5. GoJ's Regulatory Sandbox Team works as the single window of the GoJ(Government of Japan)
   - to provide consultation for private businesses, and
   - to exchange views with regulators, when appropriate,
   on the proposals to be made under the Regulatory Sandbox framework.

6,7. Screening and decision making by the competent minister referring to the opinion from the evaluation committee.

8. After the approval, provide information and advice from the competent minister necessary for the smooth and secure implementation of the demonstration

9. Competent minister will review the regulations where necessary by using the demonstration data.

11