



The PrivacyMark® System

System, Reliability mechanism and Transparency programs



**JIPDEC**

Profile of The PrivacyMark[®] System

1. Objectives:

- to enhance consumers' awareness of personal information protection
- to provide entities with an incentive to win social trust from consumers and business partners

2. Date of Commencement : April 1, 1998

3. Promotion Body: **JIPDEC**

4. Criterion: **JIS Q 15001:2006**

Japanese Industrial
Standard

The serial number for “Personal information protection management systems – Requirements”

The PrivacyMark System has adopted **JIS Q 15001** as its assessment criterion since 1999 when the first edition was developed, **encompassing the eight principles of OECD and extracting most of the concept of the EU Directive(95/46/EC).**

The second edition was made public in 2006.

➤ Refer to page 16 - 18 for the details of the requirements

5. Accumulated Number of P-Mark Entities:**20,199** ⇒Page 2

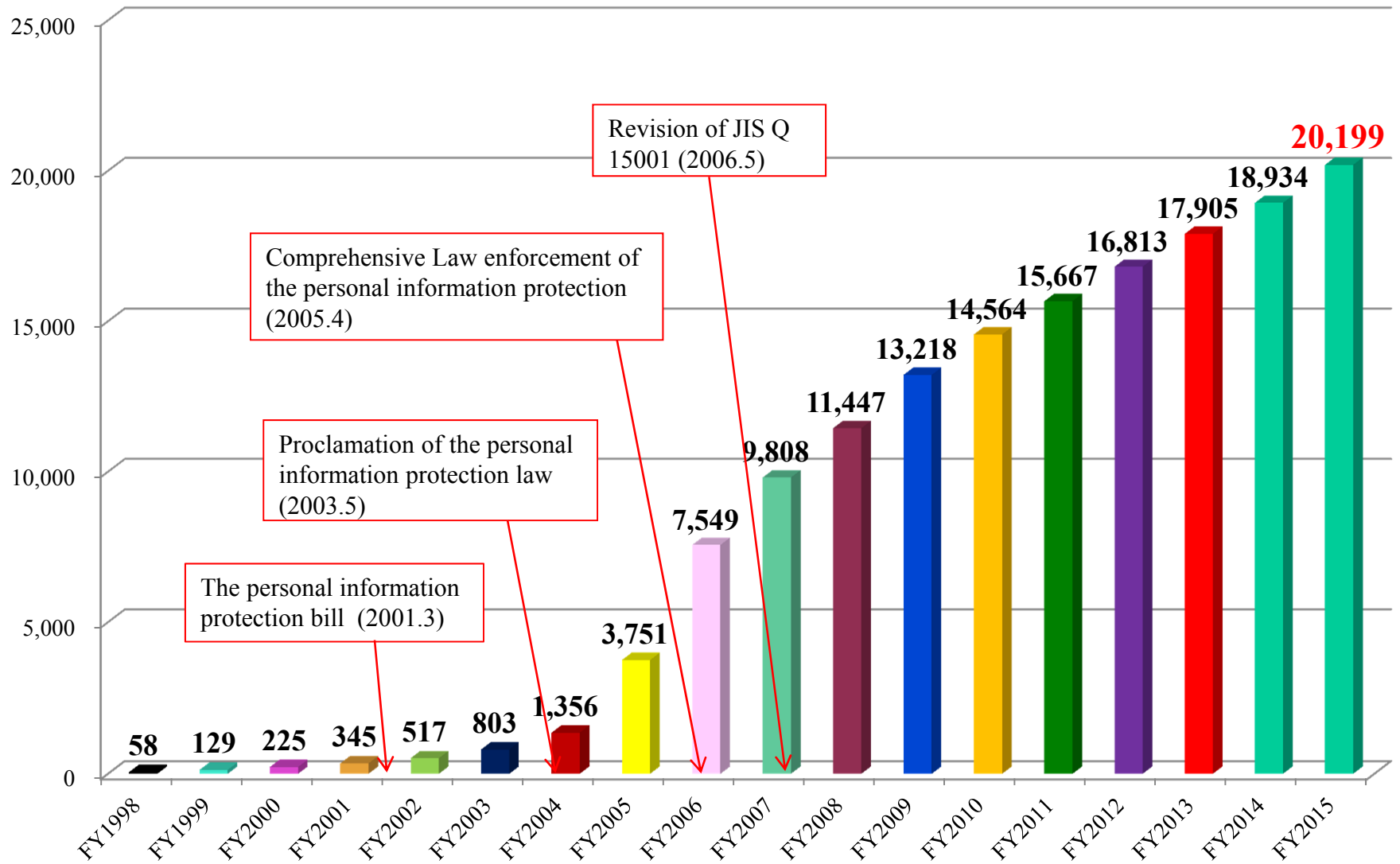
6. Number of Assessment Bodies: 18 (except Assessment Division of JIPDEC)

7. Number of Assessor Training Bodies: 3

8. Number of Assessors: 1,209 (as of Mach 31, 2015)

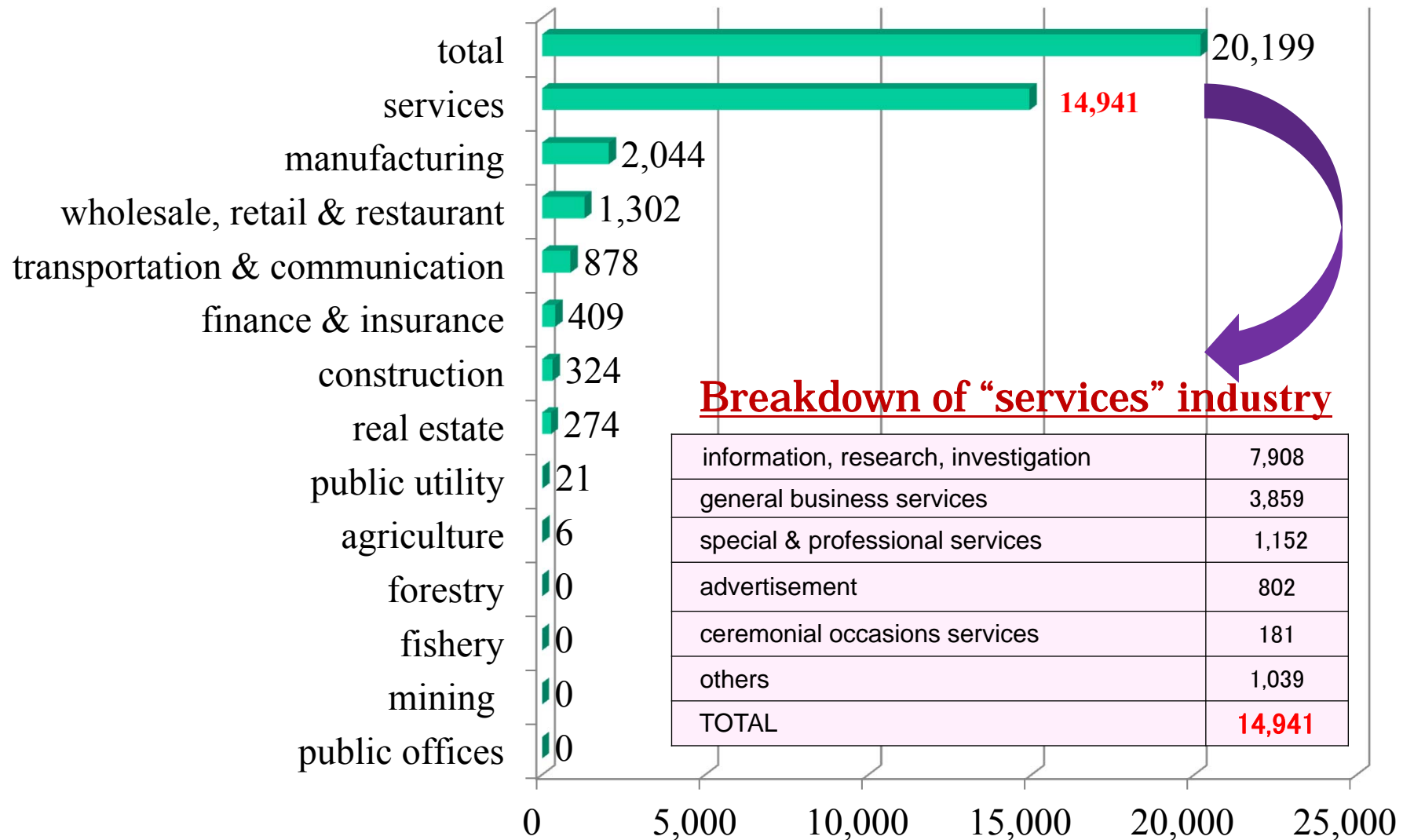
Senior Assessors: 314 Assessors: 264 Assistant Assessors: 631

The accumulated number of PrivacyMark entities



(as of March 31, 2016)

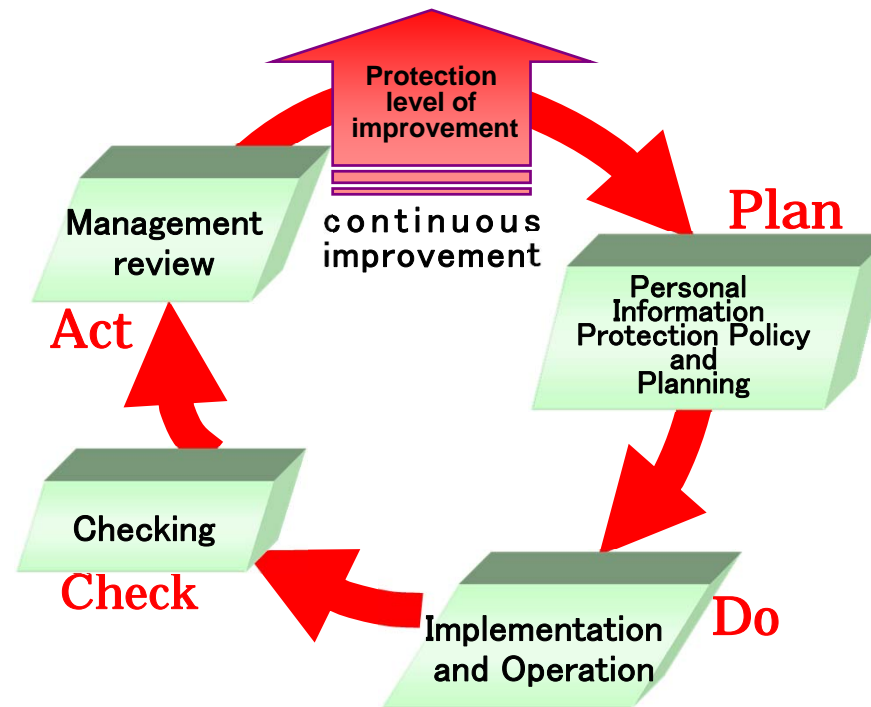
The number of PrivacyMark entities by industry



(as of March 31, 2016)

The PrivacyMark[®] System

- The concept of JISQ15001 is continuous improvement based on by “the PDCA Cycle”.



- The PrivacyMark System assesses whether or not applicants' **PMS** (Personal information protection Management System) adequately manage risks on handling of personal information.

➤ Refer to page 5 for the two stages of the assessments.

The PrivacyMark[®] System

Major Assessment Items of the PrivacyMark System

PMS Document Assessment :

Over-120 items

- It should announce its privacy policy (personal information protection policy).
- It should establish its PMS.
- It should establish the procedures to implement the PMS.
 - how to acquire, use and provide personal information
 - how to response to the inquiries from the persons concerned (disclosure, correction, deletion, etc.)
 - education, inspection, corrective and preventive action, review of PMS, etc.

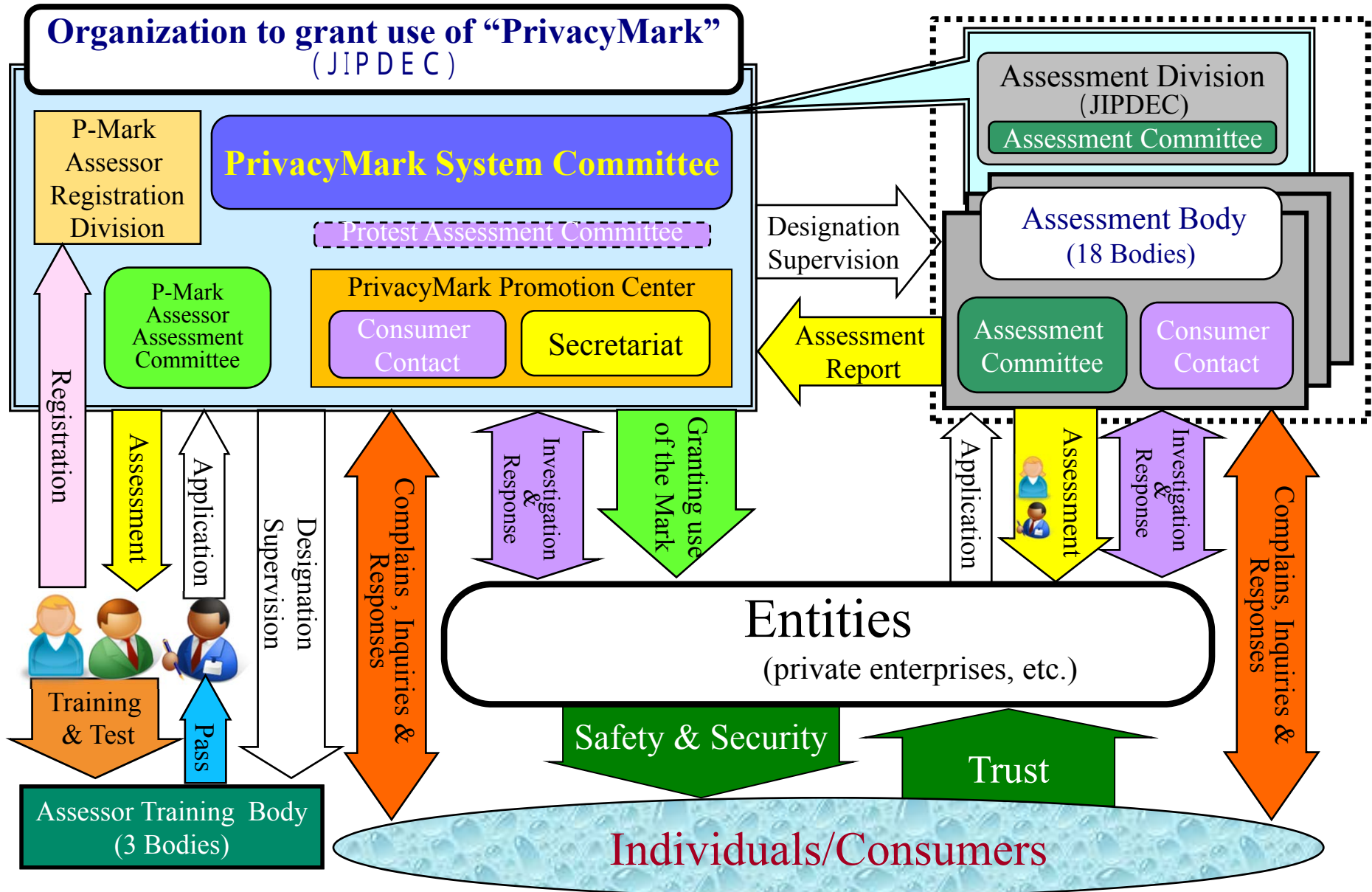
On-site Assessment :

Operations /Over-52 items

Security Safeguards / Over-41 items

- It should implement, maintain, review and correct its PMS.
- It should specify all kinds of personal information and recognize risks on the handling of the personal information.
- It should analyze the risks and take appropriate security control measures.
- It should handle the information in accordance with the procedures.
- It should provide all of managements and employees with education on the personal information protection.
- It should implement audit process.
- It should implement corrective and review process.

Organization of the PrivacyMark® System



The PrivacyMark System

(1) The PrivacyMark System Committee

■ Committee Members:

- designate experts on personal information protection from the outside
- Members(9 persons): Professors, Representatives of business groups, Representatives of consumers, Lawyers, etc.

■ Roles & Responsibilities:

- establishment and revision of rules and regulations of the System
- designation and cancellation of Assessment Body
- cancellation or suspension of the PrivacyMark entities that violated PrivacyMark System Rules and Regulations
- Operation of the System etc.

The PrivacyMark System

(2) The Assessment Body

■ JIPDEC and 18 Bodies:

- JIPDEC: Assessment Division
- 18 Bodies: 12 industry-specific bodies and 6 regional bodies
 - In principle, applicants should submit the application form to the industry-specific body to which they belong.
 - If the body is not available, it may submit the form to the specific regional body or JIPDEC.

(3) The PrivacyMark Assessment Committee

- assesses Assessor's reports on the applicants and report the results to the PrivacyMark System Committee
- Members : experts of personal information protection, professors, representatives of business groups and consumers, lawyers, etc.

(4) The PrivacyMark Assessor Training Body

- 3 Designated Bodies (as of March, 2016)
- operate a 5-day Course for new entries (Assistant Assessor) and a half-day Follow-up Course for all Assessors

The PrivacyMark System

(5) The PrivacyMark Assessor Assessment Committee

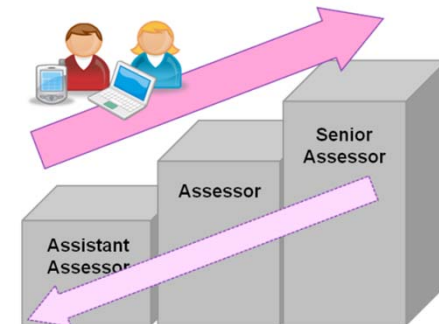
- assesses whether or not the applicants have competence for the concerned qualification
- In cases of promotion to Assessor or Senior Assessor, the applicants are required to have regulated business experiences and recommendations of Senior Assessors.
 - new entry for Assistant Assessor: required to take a 5-day course and pass the exam
 - promotion to Assessor: required to complete five assessments through OJT and receive recommendations of two or more Senior Assessors who instructed him/her
 - promotion to Senior Assessor: required to complete ten formal assessments and recommendations of two or more Senior Assessors who instruct him/her

(6) The PrivacyMark Assessor Registration Division

- operates registration of the PrivacyMark Assessors
- the number of Assessors registered

(**Totaled 1,209 Assessors** as of March 31, 2015)

Senior Assessor : 314
Assessor : 264
Assistant Assessor : 631



The PrivacyMark System

(7) The PrivacyMark Consumer Contact

- set up in JIPDEC and in each Assessment Body
- handles inquiries and complaints on personal information issues free of charge
- investigates cases and provides results with the person including entities' remedial actions, if any.
- The contact of JIPDEC is composed of four regular consultants and a part-time consultant in addition to a manager and an assistant.
- The number of the cases regarding the PrivacyMark entities handled in FY2015 was 422. (FY2014: 415cases)

(8) The Protest Assessment Committee (ad-hoc committee)

In the case of a protest or complaint about the matters below filed by any PrivacyMark entity, applicant for a PrivacyMark entity or Assessor position, person who took a course for Assessors, and consumers, the Protest Assessment Committee shall be temporarily set up in the PrivacyMark System Committee.

- on the result of new entry or renewal assessment for use of the PrivacyMark, Assessment Body, Assessor Training Body from the applicants concerned
- on the result of assessment by Assessor Training Body from the applicants
- any related complain on the System, each Body, etc. from consumers, etc.

and the like

The PrivacyMark System

(9) Judgment of Disqualification and Penalty

How are leaks of personal information and violations of the PrivacyMark Rules by a PrivacyMark entity discovered?

- 1) the concerned party(person) and/or a third party acting in good faith(consumers)
- 2) a internal “whistle-blower”/ a internal concerned employee
- 3) mass media (news)
- 4) JIPDEC

The PrivacyMark Penalty Rules: Refer to page 13 for the detail of the point process.

| Level | Penalty Category | Total Points |
|-------|--------------------------------|---------------|
| 1 | warning | 1, 2, 3, 4, 5 |
| 2 | recommendation / citation | 6, 7 |
| 3 | temporary halt of using P-mark | 8, 9 |
| 4 | termination | 10 and more |

The PrivacyMark System

The PrivacyMark Penalty calculation chart

| | Judgment matter | points |
|---|--|-------------|
| 1 | presence or absence of responsibility | 0, 1, 10 ※1 |
| 2 | contents and volume of personal information(data) | 0, 1, 2 ※2 |
| 3 | presence or absence of influence to the person concerned | 0, 1, 2 |
| 4 | presence or absence of influence to the P-mark System | 0, 1, 2, 3 |
| 5 | presence or absence of an accident within a year | 0, 1, 2, 3 |

- ※1 An inevitability reason such as an inside job is regarded absence of responsibility(zero point).
A pre-meditated crime that management commits (recognizing incompliance or illegality), what's called, an organized crime is regarded ten points.
- ※2 The case of sensitive data is regarded two points.



Total points
(See the page 12 chart.)

The PrivacyMark System

(10) Others

- **Openness**
 - **The standards and regulations are available on the PrivacyMark System web site.**
 - **The guidelines for implementation of the management system is also available on the web site**
- **Provision of information**
 - **to provide with consumers and entities with information on personal information protection and know-how of development and improvement of PMS such as free seminars and consumer-oriented or easily-understood information distributed on the web site.**

The Fee Structure of the PrivacyMark System

Since April 1, 2014 [JPY (Tax included)]

| Category | New Application | | | Renewal | | |
|-----------------------|-----------------|----------------|------------------|----------------|----------------|----------------|
| Scale | Small | Medium | Large | Small | Medium | Large |
| Application Fee | 51,429 | 51,429 | 51,429 | 51,429 | 51,429 | 51,429 |
| Screening Fee | 205,715 | 462,857 | 977,142 | 123,428 | 308,572 | 668,571 |
| Mark Registration Fee | 51,429 | 102,858 | 205,715 | 51,429 | 102,858 | 205,715 |
| Total | 308,573 | 617,144 | 1,234,286 | 226,286 | 462,859 | 925,715 |

■ The effective period of the mark use fee is for **2 years**.

■ Business scale

Large: Business operators on a scale exceeding that of medium scale business operators

Small: Business operators with a number of full-time employees of 20 or less. In the case for wholesalers, retailers (including food outlets) and services, with a number of the employees of 5 or less

Medium:

| | Manufacturers and Others | Wholesalers | Retailers | Services |
|----------------|--------------------------|---------------------|--------------------|--------------------|
| Capital | 300 million or less | 100 million or less | 50 million or less | 50 million or less |
| Persons | 300 or less | 100 or less | 50 or less | 100 or less |

NOTE: the number of the persons who belong to the entity such as employees, directors and the like

The Requirements of JISQ15001:2006

| The Criteria of the PrivacyMark System | |
|--|--|
| P | 3.1 General requirements |
| | 3.2 Personal information protection policy |
| | 3.3 Plan |
| | 3.3.1 Specification of personal information |
| | 3.3.2 Laws, guidelines and other codes stipulated by the state |
| | 3.3.3 Recognition, analysis and measures of risk, etc. |
| | 3.3.4 Resources, roles, responsibility and authority |
| | 3.3.5 Internal regulations |
| D | 3.3.6 Planning documents |
| | 3.3.7 Preparation for state of emergency |
| | 3.4 Implementation and operation |
| | 3.4.1 Operation procedures |
| | 3.4.2 Principles on acquisition, use and provision |
| | 3.4.2.1 Specification of purpose of use |
| 3.4.2.2 Appropriate acquisition | |
| 3.4.2.3 Restriction of acquisition, use and provision of specific sensitive personal information | |

The Requirements of JISQ15001:2006

The Criteria of the PrivacyMark System

| | |
|---|---|
| D | 3.4 Implementation and operation (continued) |
| | 3.4.2 Principles on acquisition, use and provision (continued) |
| | 3.4.2.4 Measures for acquiring with documents directly from the person |
| | 3.4.2.5 Measures for acquiring personal information by methods other than 3.4.2.4 |
| | 3.4.2.6 Measures concerning use |
| | 3.4.2.7 Measures when accessing the person |
| | 3.4.2.8 Measures concerning provision |
| | 3.4.3 Appropriate control |
| | 3.4.3.1 Securement of accuracy |
| | 3.4.3.2 Security control measures |
| | 3.4.3.3 Supervision of employees |
| | 3.4.3.4 Supervision of trustees |
| | 3.4.4 Rights of the person concerning personal information |
| | 3.4.4.1 Rights concerning personal information |
| | 3.4.4.2 Procedures to meet requests for disclosure and others |
| 3.4.4.3 Making the matters concerning personal information subject to disclosure widely known, etc. | |

The Requirements of JISQ15001:2006

| The Criteria of the PrivacyMark System | |
|--|--|
| D | 3.4 Implementation and operation (continued) |
| | 3.4.4 Rights of the person concerning personal information (continued) |
| | 3.4.4.4 Notification of purpose of use of personal information subject to disclosure |
| | 3.4.4.5 Disclosure of personal information subject to disclosure |
| | 3.4.4.6 Correction, addition or deletion of personal information subject to disclosure |
| | 3.4.4.7 Veto of use or provision of personal information subject to disclosure |
| | 3.4.5 Education |
| | 3.5 Personal information protection management system documents |
| | 3.5.1 Range of documents |
| | 3.5.2 Document control |
| 3.5.3 Record control | |
| 3.6 Response to complaints and consultations | |
| C | 3.7 Inspection |
| | 3.7.1 Confirmation of operations |
| | 3.7.2 Audits |
| A | 3.8 Corrective actions and preventive actions |
| | 3.9 Review by the representative of the business entity |

The PrivacyMark System

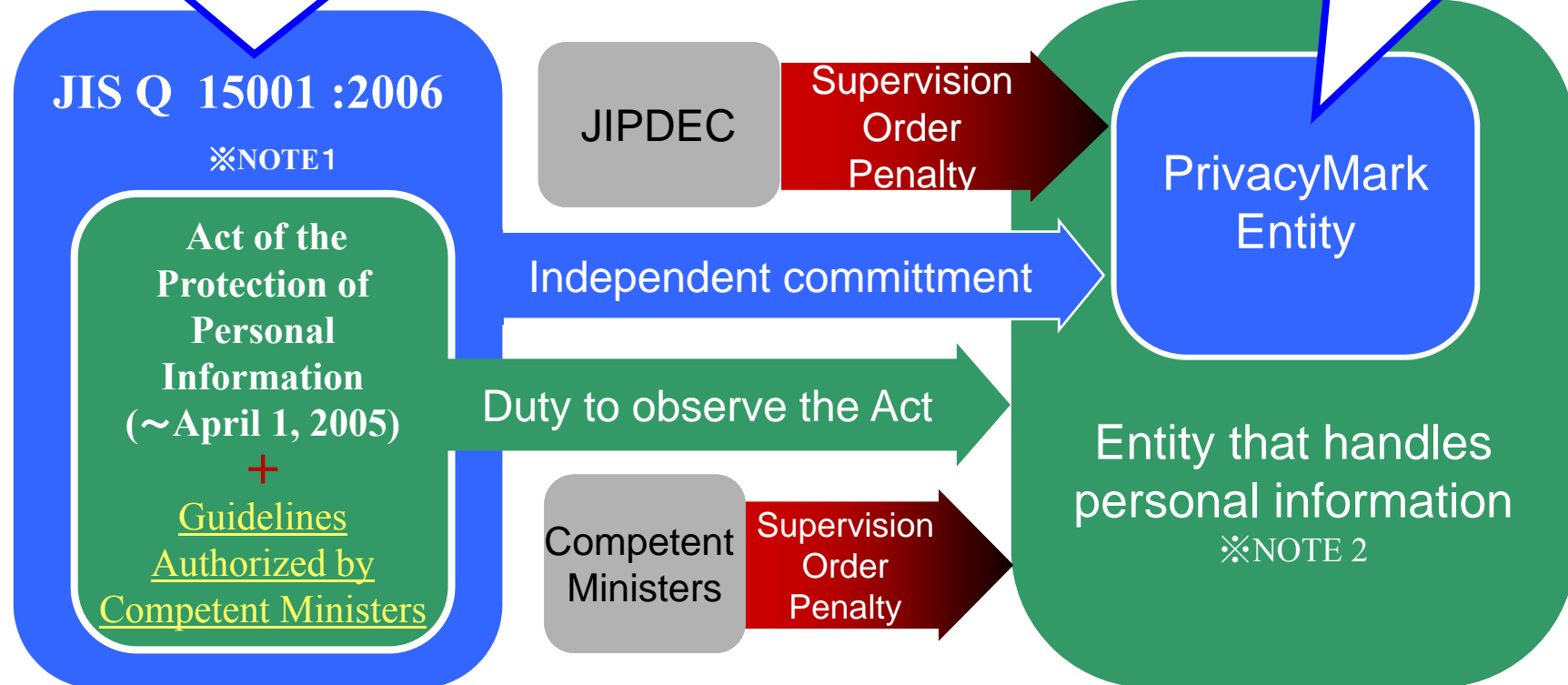
Development of the criteria for the System

| Period | Criteria of P-Mark Assessment | What happened outside the System |
|-----------------------------------|--|---|
| April 1998 ~March 1999 | Guideline pertaining to the protection of personal information processed by computer in private sector (May 1997, The Ministry of International Trade and Industry) | <ul style="list-style-type: none"> ▪ Directive 95/46/EC of the European Parliament and of the Council (October 24, 1995) |
| April 1999 ~May 2006 | JIS Q 15001:1999 "Requirements-Personal Information Protection Management System" | <ul style="list-style-type: none"> ▪ Proclamation of Act on the Protection of Personal Information (May, 2003) ▪ Complete enforcement of Act on the Protection of Personal Information (April, 2005) ▪ Announcement of Competent Ministers regarding sector guidelines for personal information protection (2005) |
| June 2006~ | JIS Q 15001:2006 "Requirements-Personal Information Protection Management System" | <ul style="list-style-type: none"> ▪ Announcement of JIS Q 15001:2006 (May 20, 2006) ▪ Modification of Sector Guidelines for personal information protection (in principle, every year) |

The Japanese Act and The PrivacyMark System

- No criterion for the number of personal information data
- No criterion of being dead or alive
- Wider protection of individual's rights than the Act
- More detailed requirements than the Act

Entity that maintains higher level of personal information protection (to observe the requirements of the Act and JIS Q 15001)



NOTE 1: JIS Q15001 is the standards based on Industrial Standardization Law in Japan.

NOTE 2: It's total number of the personal information identified that makes up personal information databases, etc. used for its business not exceeding 5,000 on any given day in the last six months.

The PrivacyMark System

PrivacyMark Promotion Center

JIPDEC

Roppongi First Building, 9-9 Roppongi 1-chome,
Minato-ku Tokyo, 106-0032 JAPAN

TEL: +81-3-5860-7563

FAX: +81-3-5573-0562

<https://privacymark.org/>