

ITSC

Introduction to the IT Security Center

<http://www.itsc.or.jp>

An IT Society with unlimited potential

Reliable security produces success

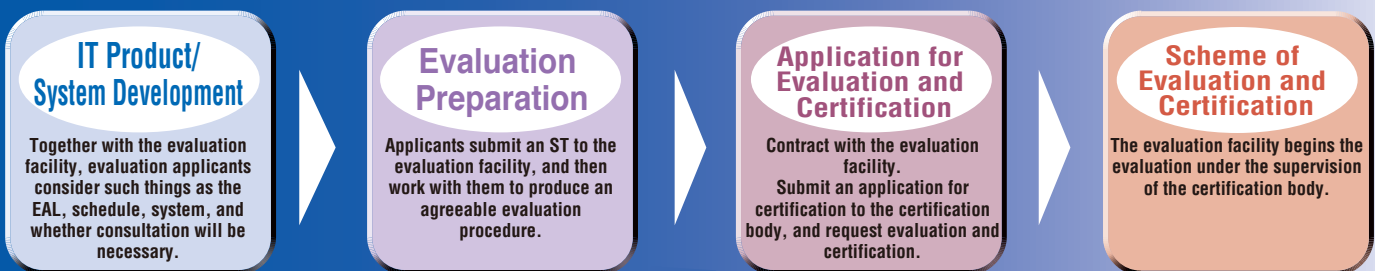
In April 2001, JEITA established the JEITA IT Security Center, building on JEITA's extensive track record of achievement in IT security.

As early as 1987, ITSC had already begun research and surveys for the Common Criteria, which became the basis of ISO/IEC 15408.

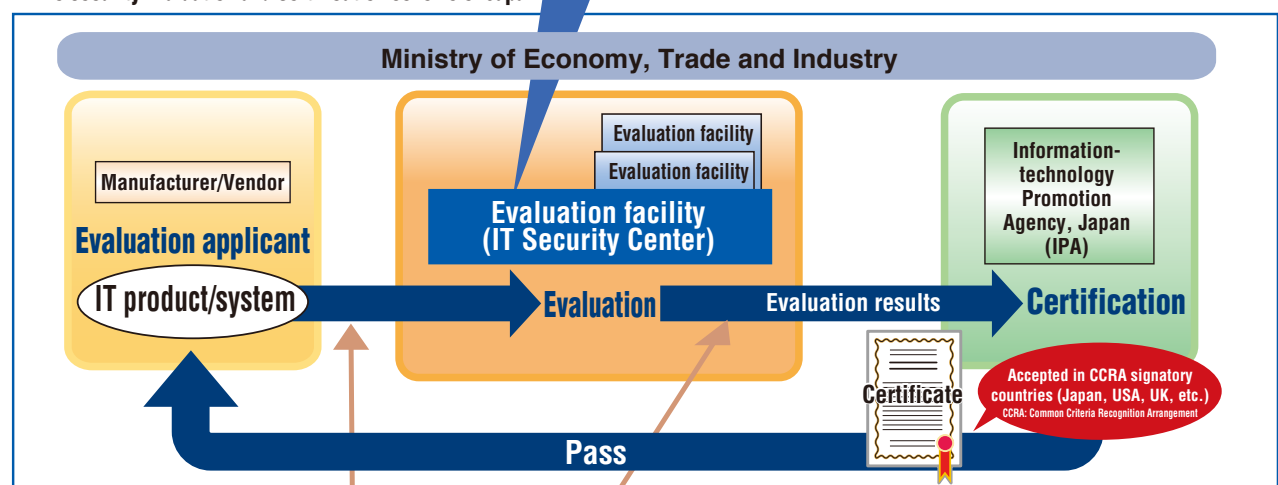
In 2007 ITSC became independent of JEITA.

The IT Security Center conducts security evaluations of IT products/systems to inspect the reliability of their security, security evaluation consultations, and security training for security engineers.

Evaluation Request Procedure



• The Security Evaluation and Certification Scheme of Japan



Security International Standard ISO/IEC15408 (Common Criteria)

Security evaluation criteria

Security target

Functional requirements

User identification and certification

Access control

Assurance requirements

Development environment

Specifications

Source code

Guidance documents

In order to effectively improve the quality of security for global IT products/systems, efforts were made to standardize IT security internationally for at least 20 years. IT security was standardized through the ISO/IEC15408 standard, which was established in 1999. ISO/IEC 15408 is a set of regulations for implementing valid security functions for all types of IT products/systems and for verifying their compliance in both hardware and software. This verification is conducted according to the security evaluation and certification scheme designated by each country, which is based on ISO/IEC15408.

In Japan, the Ministry of Economy, Trade and Industry established this scheme in April 2001. It operates based on "Evaluation," which verifies the security functions of IT products/systems, and "Certification," which confirms the evaluation results. IT Security Center is an official EAL4 Evaluation Facility.

Materials Necessary for Security Evaluation

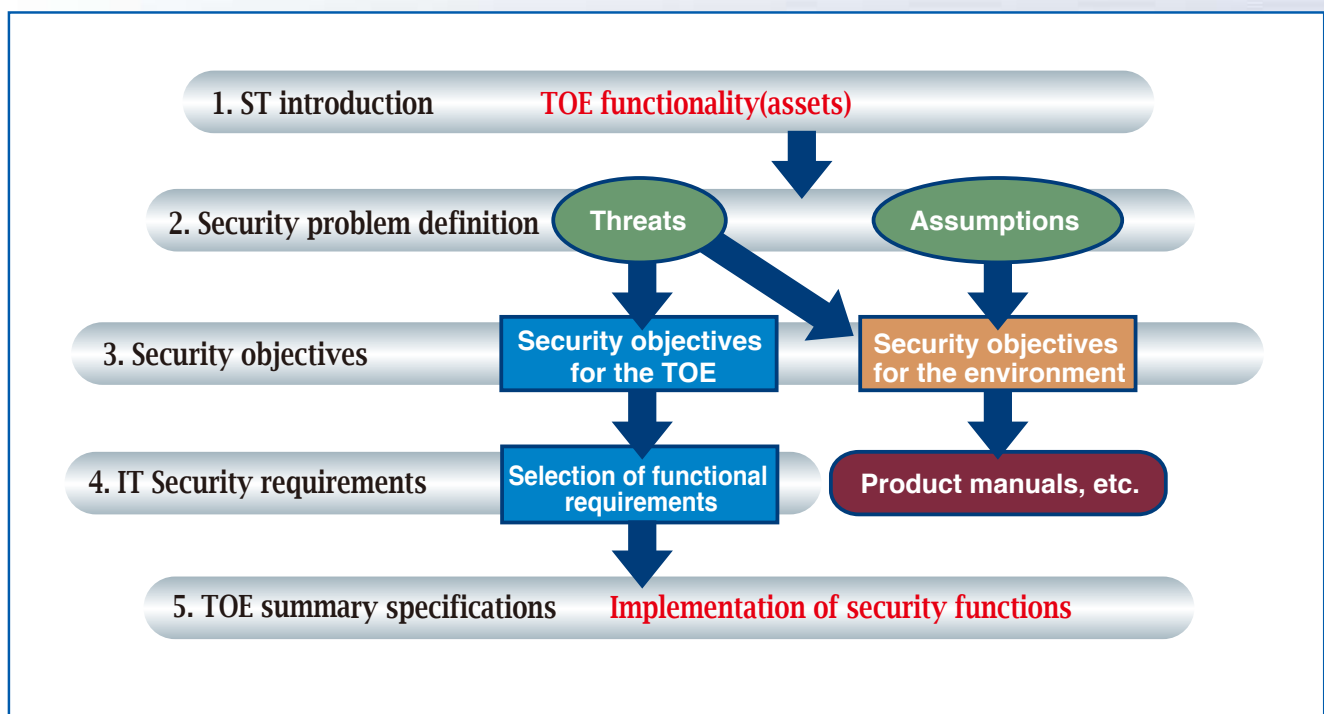
Security Target

Development related documentations

Target of Evaluation (TOE)

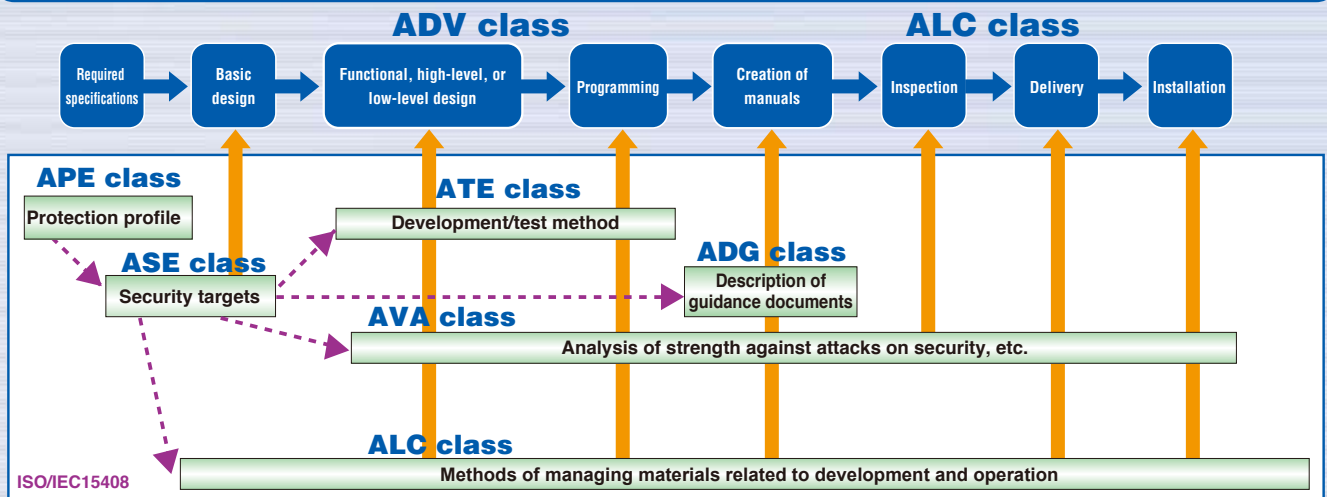
In order for IT product/system developers to receive evaluation and certification of their product's security, they must submit their IT product/system (TOE: Target of Evaluation) and its development related documentations to an evaluation facility approved by this scheme (IT Security Center, etc.) Development related documentations are largely documents that are normally created during IT product/system development, such as functional specification, test specification, and source code. However, developers may not create some documentation in usual development of IT product/system. For example, one of those is Security Target (ST).

Structure of Security Target



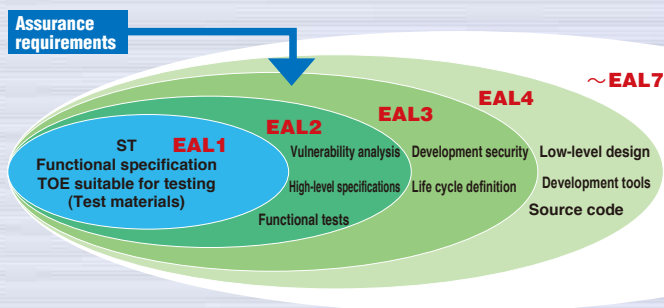
The ST is the basic design for TOE security functions and is more than just a set of specifications. It logically proves why the implemented security functions are valid. ST describes the methods of preventing assets from threats, such as modification and leaks by attackers. If these methods prove to be valid, the security functions described in the ST are considered valid.

Development through Maintenance of IT Products (Generally the same for IT Systems)



TOE security functions are evaluated to verify whether they have been developed and implemented as described in the ST. ISO/IEC15408 defines the requirements (assurance requirements) for the development and implementation methods that are specified in the ST. The TOE assurance requirements do not require a special development method. The following types of documents are required depending on the security functions specified in the ST: development documents, such as functional specifications that describe external interfaces and those implemented interfaces that divide the TOE into subsystems (high-level specifications), and documents, such as manuals (guidance documents), test specifications, and development environment regulations (configuration management).

• Evaluation Assurance Level (EAL)



Clarification of the Remaining Risk

Assurance requirements are categorized into 7 levels, EAL1 to 7 (EAL: Evaluation Assurance Level). The EAL represents how detailed the development documentation will be verified. For example, TOEs that deal with national secrets may require EAL7, which is the highest level. Normally, EAL4 is considered the highest level for business.

Family	Evidence	EAL1	EAL2	EAL3	EAL4
AGD_OPE	Operational user guidance	●	●	●	●
AGD_PRE	Preparative procedure	●	●	●	●
ADV_ARC	Architecture description		●	●	●
ADV_FSP	Functional specification	●	●	●	●
ADV_IMP	Implementation representation				●
ADV_TDS	Design of TOE		●	●	●
ALC_CMC	CM documentation	●	●	●	●
ALC_CMS	Configuration list	●	●	●	●
ALC_DEL	Delivery procedure		●	●	●
ALC_DVS	Development documentation			●	●
ALC_LCD	Life-cycle definition			●	●
ALC_TAT	Development tool and options				●
ATE_COV	Test coverage		●	●	●
ATE_DPT	Depth of testing			●	●
ATE_FUN	Test documentation		●	●	●
ATE_IND	TOE for testing	●	●	●	●
AVA_VAN	TOE for testing	●	●	●	●

Security Support for IT Society

- Provision of services by IT system developers with extensive expertise
- Personnel with experience in a broad range of specialized fields, from IT products to IT systems

Pioneering Activities for Security Evaluation in Japan

- First trial of security evaluation in Japan using Common Criteria V1.0
- Participated in establishment of the security evaluation/certification scheme in Japan



Security Evaluation (EAL1 to EAL4 and PP)

The purpose of a security evaluation is to acquire ISO/IEC15408 certification. We conduct security evaluations for IT products and systems (TOE) based on the evaluation documents provided by the customer. During a security evaluation, the Security Targets (ST) is verified first. The IT product or system is then inspected to verify that it has been developed as specified in the ST.

Security Evaluation

Security evaluation of IT products/systems

Verification of ST

The security functions of IT products and systems are verified according to the ST.

TOE(Target of Evaluation)

- Hardware/software products
 - From IT products to information processing systems
- Examples
IT products: firewalls, accounting tools, IC card products, etc.
Information processing systems: accounting systems, electronic commerce systems, etc.



Development Consulting

Support Service for Design of Security Functions

Robust security functions cannot be created by just spending money. Systematic threats analysis and effective plans for countermeasures are necessary to establish cost-effective, leak-proof security functions. We look at security from our customers' perspective and offer them optimal security function designs.

Support Service for Security Evaluation and Acquisition of Certification

For security evaluation of IT products and systems, documents must be prepared in accordance with the ST, such as design documents, test specifications, and various types of analysis documents. We provide counseling in regard to such things as the type of evaluation documents necessary to satisfy the required evaluation assurance level and the appropriate method of writing these documents. Additionally, we review evaluation documents and create Protection Profiles (PP) and Security Targets (ST) on behalf of our customers.



Training

The IT Security Center provides numerous training programs aimed at acquiring the security technology related skills that are required at different stages of development for IT products and systems, including such things as security basics, system design, production control, inspection, and evaluation.

Training Program System

Introduction to ISO/IEC15408

ST creation method

ST creation practice

Development method

Inspection/
Evaluation method

IT Security Center Training Seminars

ISO/IEC15408 Engineer Training

1. Introductory lecture
2. Lecture on ST creation techniques
3. ST creation practice (using tools)
4. Lecture on development/inspection/evaluation techniques

Achievements of ITSC

1987-	Established a "Computer Security Expert Committee," and then began a survey related to security evaluation standards.
1992	Published The Basic Requirements of Computer Security (Security function and Assurance Versions)
1998	First trial evaluation in Japan using Common Criteria V1.0 (the basis for ISO/IEC15408)
1999	Participated in creation of the JIS standard for security from the International Standard
2000	Participated in establishment of the security evaluation/certification scheme in Japan Developed the "System Protection Profile for e-government"
2001	Participated in production of the JIS-TR for CEM (Common Methodology for Information Technology Security Evaluation)
2002	Acquired authorization as an EAL3 security evaluation facility
2003	Acquired authorization as an EAL4 security evaluation facility
2007	Became independent organization from JEITA
2009	Testing laboratorie of CMVP accredited by the National Institute of Standards and Technology, National Voluntary Laboratory Accreditation Program (NVLAP) (LAB CODE: 200822-0)
2010	Testing laboratory of JCMVP accredited by the National Institute of Technology and Evaluation(NITE), and approved by the Information Tecnology Promotion Agency,Japan(IPA)

Information Technology Security Center(IT Security Center)

1-1-3 Ohtemachi, Chiyoda-ku, Tokyo 100-0004
Tel: +81-3-5218-2231 Fax:+81-3-5218-2232
E-mail: contact@itsc.or.jp
<http://www.itsc.or.jp>