7th ICCC

Design and Development of a Knowledge-based Tool for ST Developers Based CC V3.1

Soka University
JAPAN

Guillermo Horacio RAMIREZ CACERES **Yoshimi TESHIGAWARA**

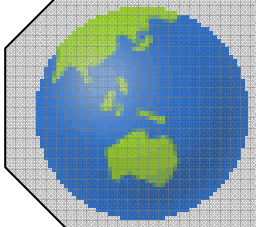
Graduate School of Engineering, Soka University, Tokyo, Japan

E-mail:{guillerm,teshiga}@soka.ac.jp

21 September 2006

Contents

- Introduction
- Research Issues
- Fundamental Research Target
- Knowledge-base Architecture
- Conclusion
- Future Works



Introduction

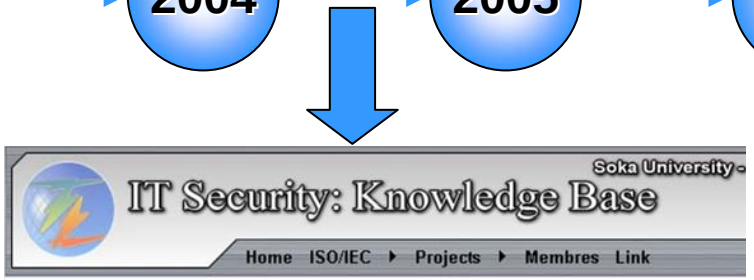
Introduction

2001 → 2002 → 2003 → 2004 → 2005 → 2006

International Standard

ISO 15446 | ISO 15408

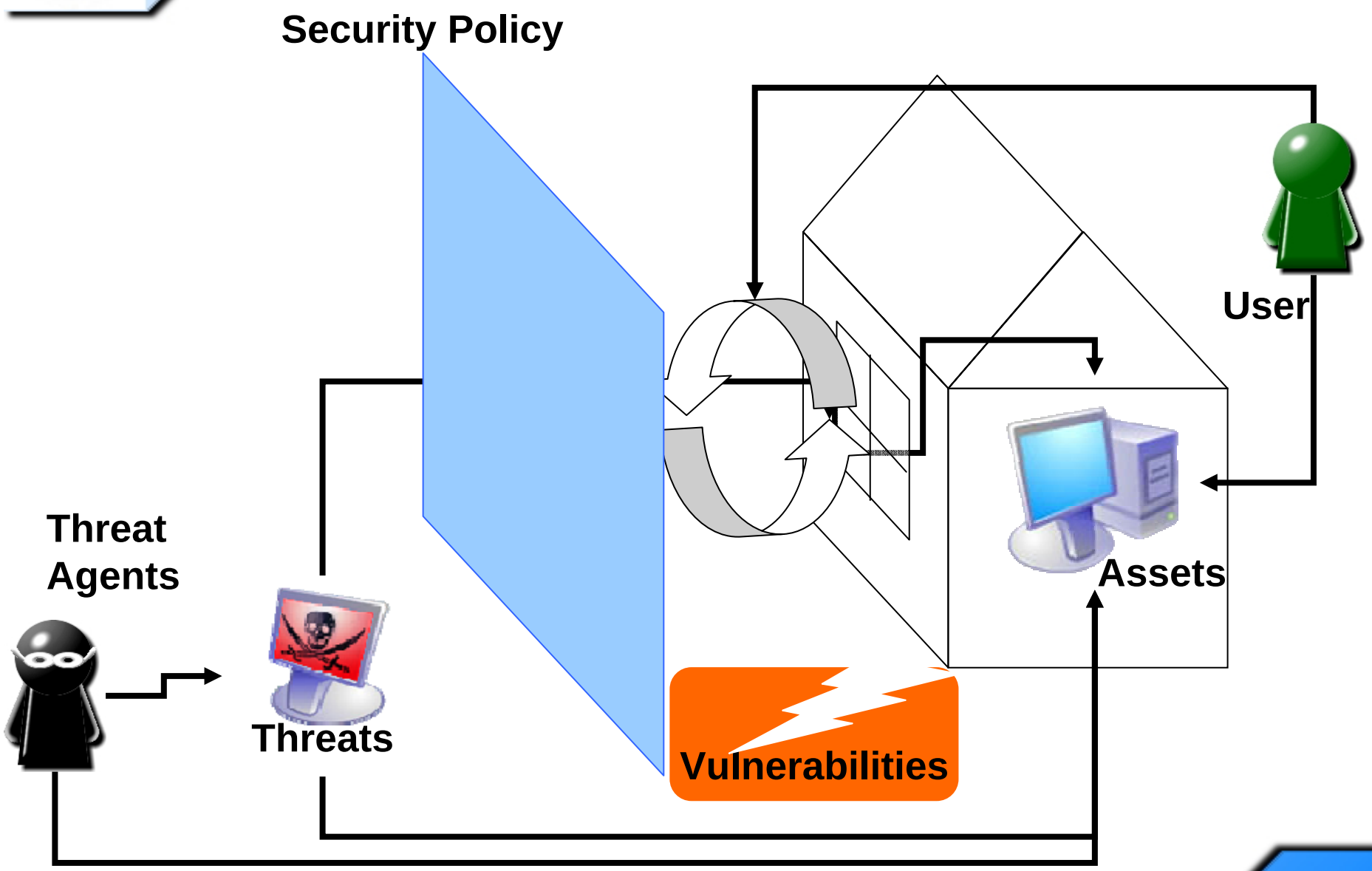
- The technical languages used with the large number of new words

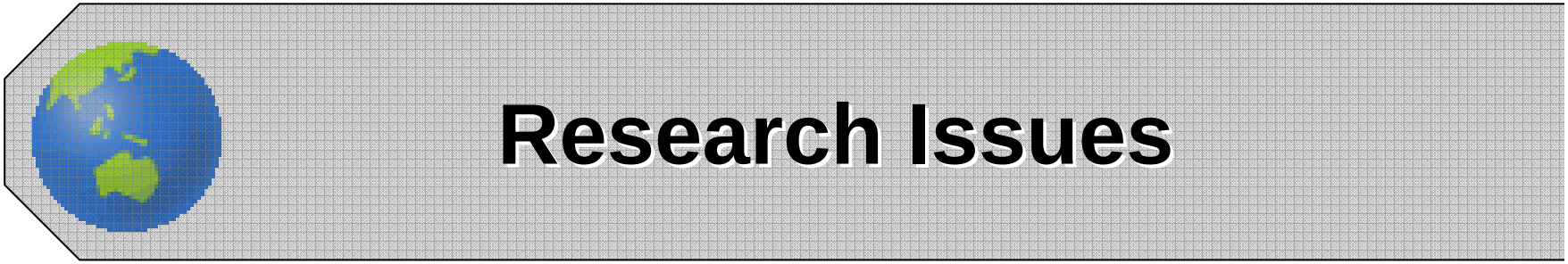


- ST developers can find the necessary information in ISO/IEC 15408
- ST Developer's knowledge shortage can be supplemented by using this tool to access the necessary information in international standards

- The new version of Knowledge base also include a self training tool.

Security Concepts




Research Issues

CC Language

Knowledge required

- ISO/IEC 15408 consists of approximately 700 pages.
- ISO/IEC TR 15446 consists of approximately 180 pages.
- The ST developer must read many times when trying to create a ST for evaluation.

Relevant experience

- The ST developer must write a document between 50 and 200 pages long.
- STs or PPs evaluated by CC are published on the Internet. and the ST developer can use this evaluated STs or PPs as references.

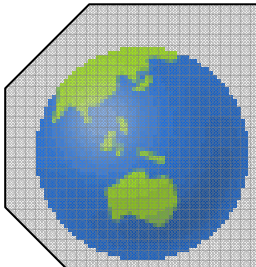
Example of CC Language

2.5 The PP and ST Development Process

The presentation of the requirements for PPs and STs in [15408-1] annexes B and C, and in [15408-3] clauses 3 to 5, might suggest that it is expected that PPs and STs are always developed in a logical 'top-down' manner, e.g. (in the case of a PP) that: (47)

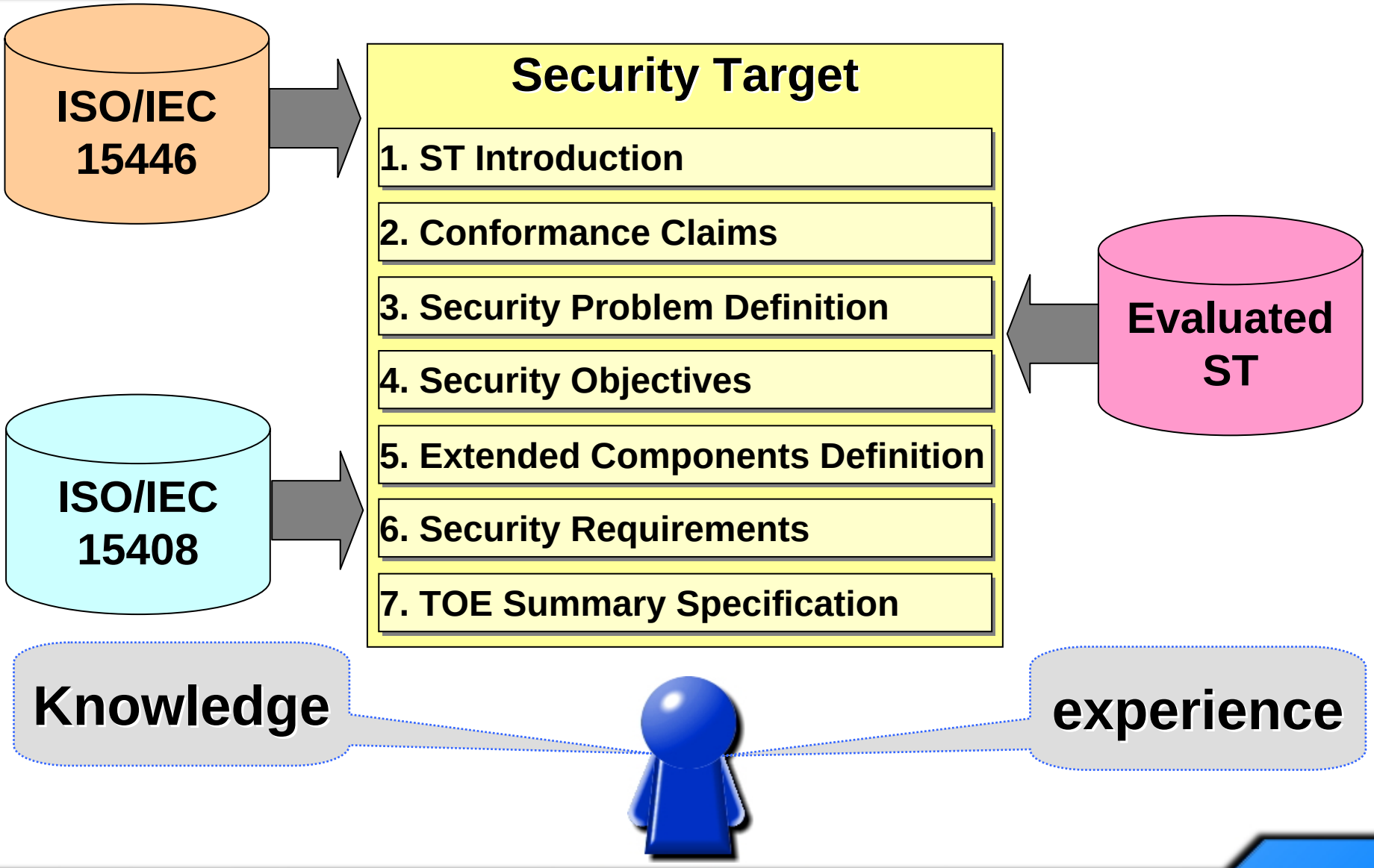
1.4.3 Usage of the PP and ST

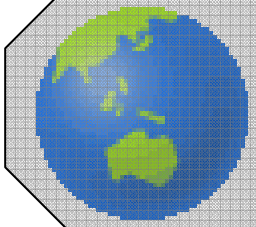
A PP may be used to define a 'standard' set of security requirements with which one or more products may claim compliance, or which systems used for a particular purpose within an organisation must comply. (See [15408-1] subclause 2.3 for the definition of the terms *product* and *system*, and also [15408-1] subclause 4.1.2 for a general discussion of the distinction between the two). A PP may apply to a particular type of TOE (e.g. operating system, database management system, smartcard, firewall, and so on), or it could apply to a set of products grouped together in a *composite* TOE (system or product). (21)



Fundamental Research Target

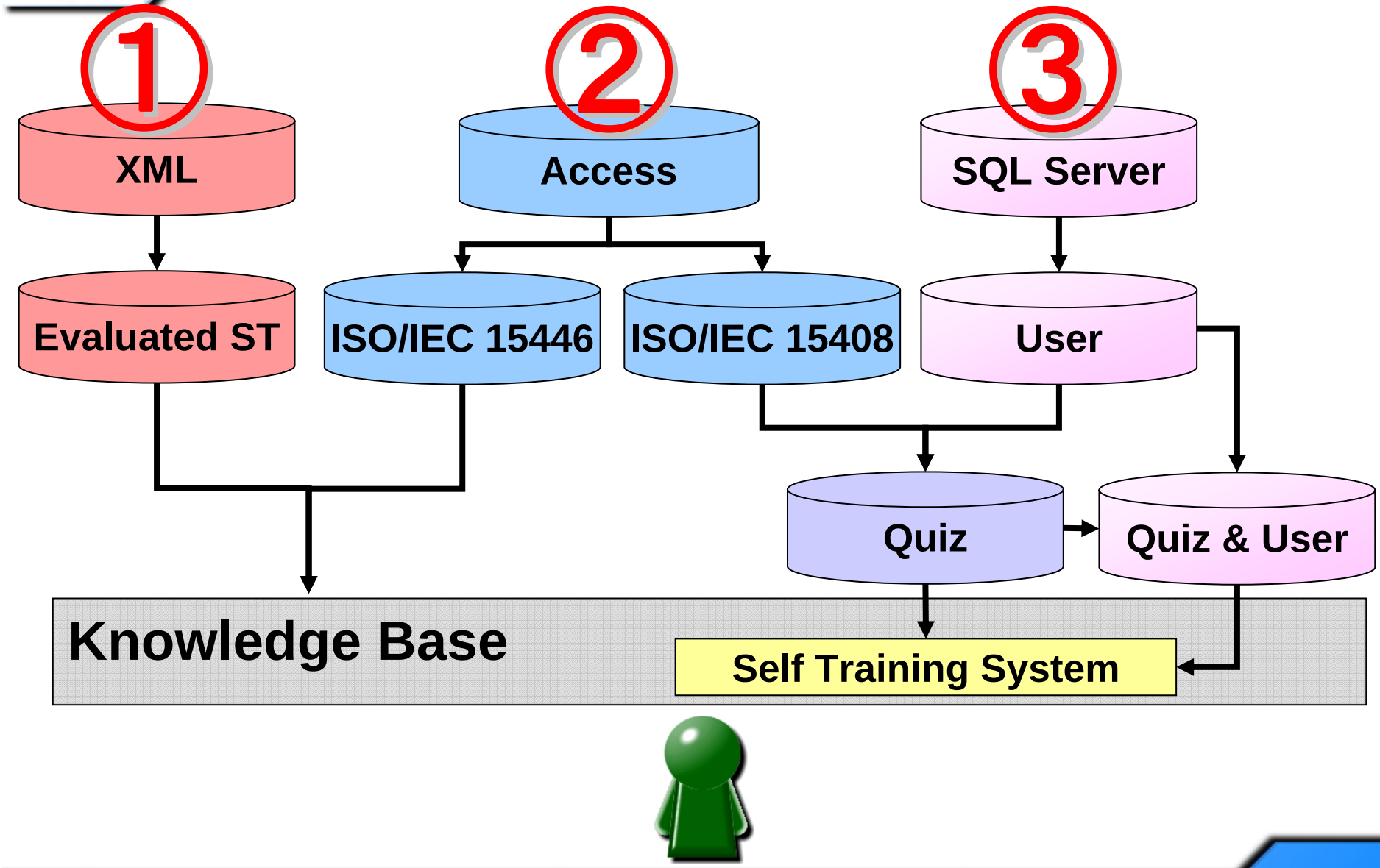
Knowledge-base

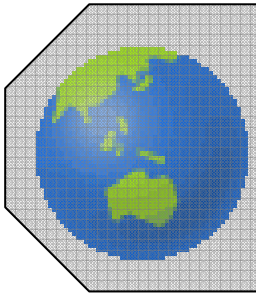




Knowledge-base Architecture

Knowledge base Architecture





Published ST Knowledge-base

①

Published ST Knowledge-base

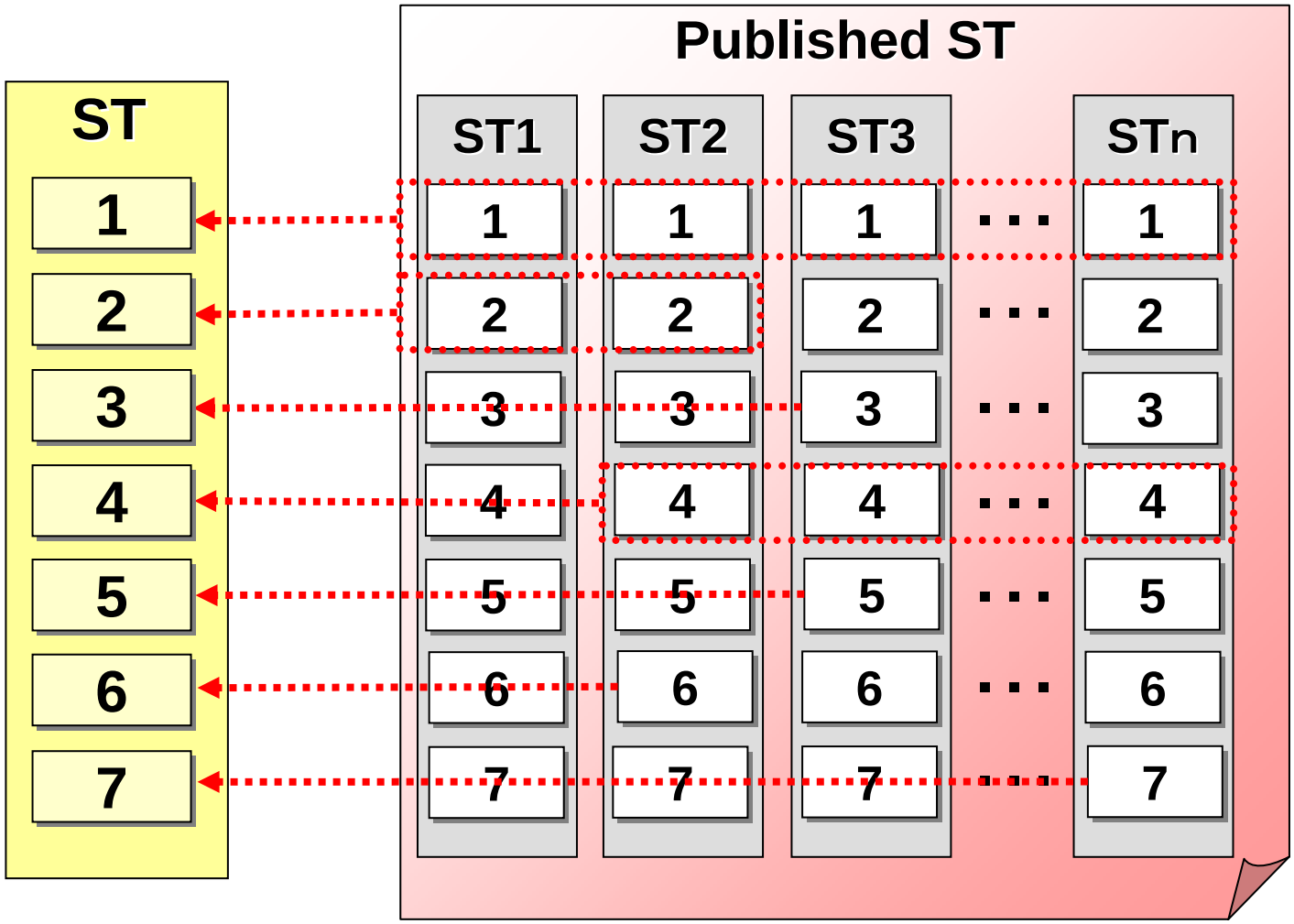
- IT products evaluated and authenticated based on CC are published on the Web Page of each country

Security_Target : テーブル

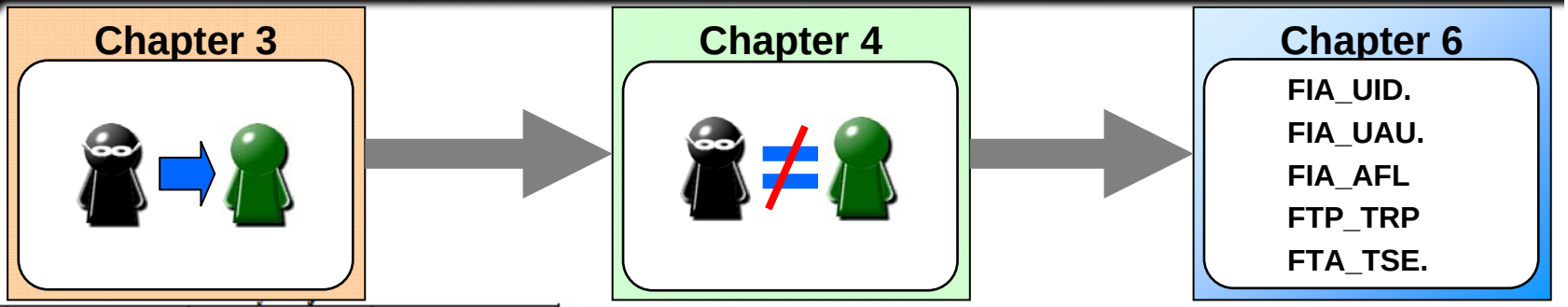
ST_Id	ST_Tipo	Product	Manufacturer	EAL	EAL_Observation	Date	Country	ST_PDF
39	Firewalls	Stonesoft StoneGate Firewall V2.0.5	Stonesoft Corporation	EAL 4	, augmented ALC_FLR.1	9/03	USA	☑
40	Firewalls	Symantec Enterprise Firewall, v8.0	Symantec Corporation	EAL 4		7/04	England	☐
41	Firewalls	Symantec Enterprise Firewall, v7.0.4 running	Symantec Corporation	EAL 4		9/03	England	☐
42	Firewalls	Symantec Enterprise Firewall, v7.0	Symantec Corporation	EAL 4		5/02	England	☐
43	Firewalls	Symantec Enterprise Firewall on the Symar	Symantec Corporation	EAL 4		3/04	England	☐
44	Firewalls	Symantec Gateway Security v2.0 5400 Serie	Symantec Corporation	EAL 4	augmented ALC_FLR.1	4/04	England	☐
45	Firewalls	TeleWall System, V 2.0 for NT 4.0	SecureLogix Corporation	EAL 2	Augmented ACM_CAP.3	0/01	Canada	☑
46	Firewalls	Watchguard LiveSecurity System w/Firebox	Watchguard Technologies	EAL 2		8/01	USA	☑
47	Guards	DragonFly Companion, V3.02, Build 129	ITT Industries	EAL 2		0/01	USA	☑
48	Guards	DragonFly Guard Model G1.2	ITT Industries	EAL 2		0/01	USA	☑
49	Guards	Owl Computing Technologies Data Diode V	Owl Computing Technologies,	EAL 2		1/02	USA	☑
50	IDS/IPS	Cisco Intrusion Detection System Appliance	Cisco Systems, Inc.	EAL 2		5/04	USA	☑
51	IDS/IPS	Cisco Intrusion Detection System Module (	Cisco Systems, Inc.	EAL 2	Augmented ALC_FLR.1	5/04	USA	☑
52	IDS/IPS	Enterasys Dragon-EAL™ Intrusion Defense	Enterasys Networks	EAL 2		9/04	USA	☑
53	IDS/IPS	IntruShield Intrusion Detection System	McAfee, Inc.	EAL 3		8/04	USA	☑
54	IDS/IPS	Intrusion, Inc. SecureNet Pro™ Intrusion Det	Intrusion, Inc. SecureNet Pro™	EAL 2		2/02	USA	☑
55	IDS/IPS	Lancope StealthWatch and StealthWatch +	Lancope, Inc.	EAL 2	Augmented ALC_FLR.2	6/04	USA	☑
56	IDS/IPS	Symantec CyberWolf, Version 2.0	Symantec Corporation	EAL 2		6/04	USA	☑
57	IDS/IPS	Symantec Manhunt Version 2.11	Symantec Corporation	EAL 3		2/03	USA	☑
58	IDS/IPS	TippingPoint UnityOne™ Version 1.2	TippingPoint Technologies, Inc	EAL 2		8/03	USA	☑
59	IDS/IPS	Top Layer Networks IDS Balancer TM Vers	Top Layer Networks	EAL 2		8/04	USA	☑
60	Miscellaneous	BKK SignCubes, Version 1.5 (BSI-DSZ-CC-	Bundsverband der Betriebskra	EAL 3	Augmented ADV_IMP.1 A	5/04	Germany	☐
61	Miscellaneous	Canon imageRUNNER 2200/2800/3300 Ser	Canon U.S.A., Inc.	EAL 3		6/04	USA	☑
62	Miscellaneous	Data-Defender V1.0	IBH-IMPEX Elektronik GmbH	EAL 1		5/02	Germany	☐
63	Miscellaneous	DEP/PCI Version 3.0	Banksys N.V.	EAL 3	Augmented ADV_FSP.2	8/03	Germany	☐
65	Miscellaneous	IBM Directory Server 5.2 (BSI-DSZ-CC-02	IBM Corporation	EAL 3		3/04	Germany	☐
66	Miscellaneous	IBM LPAR for POWER 4 for the IBM pSerie	IBM Corporation	EAL 4	Augmented ALC_FLR.1	1/04	Germany	☐
67	Miscellaneous	IBM Tivoli Access Manager for e-business	IBM Corporation	EAL 3	+	0/03	Germany	☐
68	Miscellaneous	Image Overwrite Security for Xerox WorkCe	Xerox Corporation	EAL 2		5/04	USA	☑
70	Miscellaneous	Sharp Corporation Multifunction Device with	Sharp Electronics Corporation	EAL 2		2/02	USA	☑

レコード: 1 / 169

ST evaluated and certificated by CC

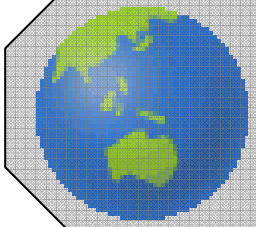


Example



	TOE				IT Environ				Non - IT Environ			
	O.ADMIN	O.DETECT	O.MONITOR	O.QUEUE	O.AUTH_ACCESS	O.ENV_ADMIN	O.SEP	O.TIME	O.INSTALL	O.PERSON	O.PHYCAL	O.HARDWRE
Assumptions												
A.LOCATE											x	
A.PROTECT									x	x	x	
A.MANAGE										x		
A.NOEVIL										x		
A.CONFIG									x	x		
A.IDENT					x							
A.SYSPRCT					x						x	
A.HARDWRE												x
A.SYSTIME								x				
Threats												
T.ACCESS_DATA					x		x				x	
T.OVRLOAD				x								
T.UNAUTH					x		x			x	x	

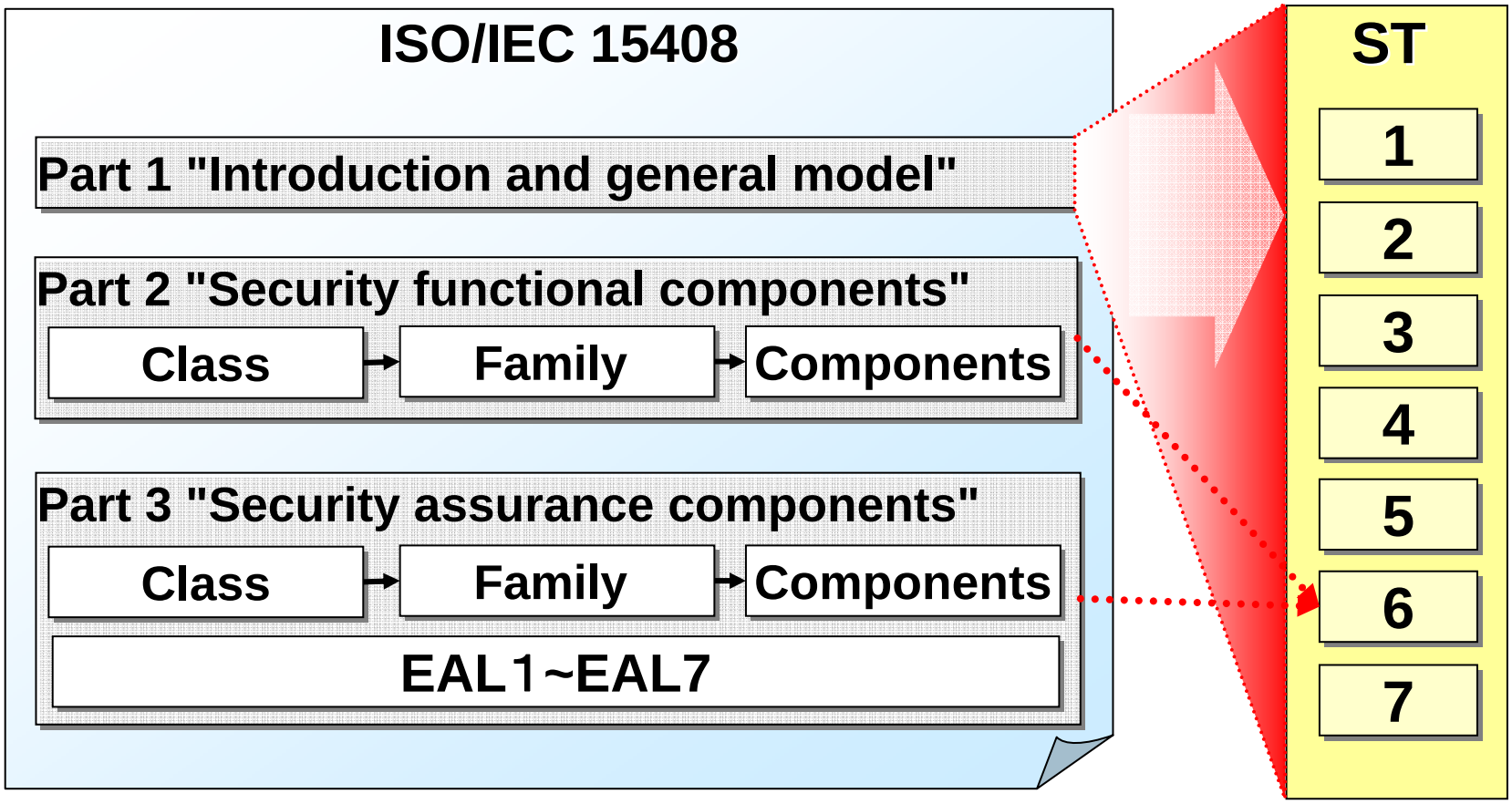
Objectives	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1a	FAU_SAR.1b	FAU_SAR.1c	FAU_SAR.3a	FAU_SAR.3b	FAU_SAR.3c	FDP_IFC.2	FDP_IFF.1	FMT_SMF.1	FPT_RVM.1	FMT_SMR.1	FIA_UID.1	FPT_SEP.1	FPT_STM.1
TOE																		
O.ADMIN	x	x	x	x	x	x		x	x	x			x		x	x		
O.DETECT											x	x	x		x	x	x	
O.MONITOR		x	x														x	x
O.QUEUE											x	x		x			x	
IT Environment																		
O.AUTH_ACCESS															x	x		
O.ENV_ADMIN							x											
O.SEP																	x	
O.TIME																		x



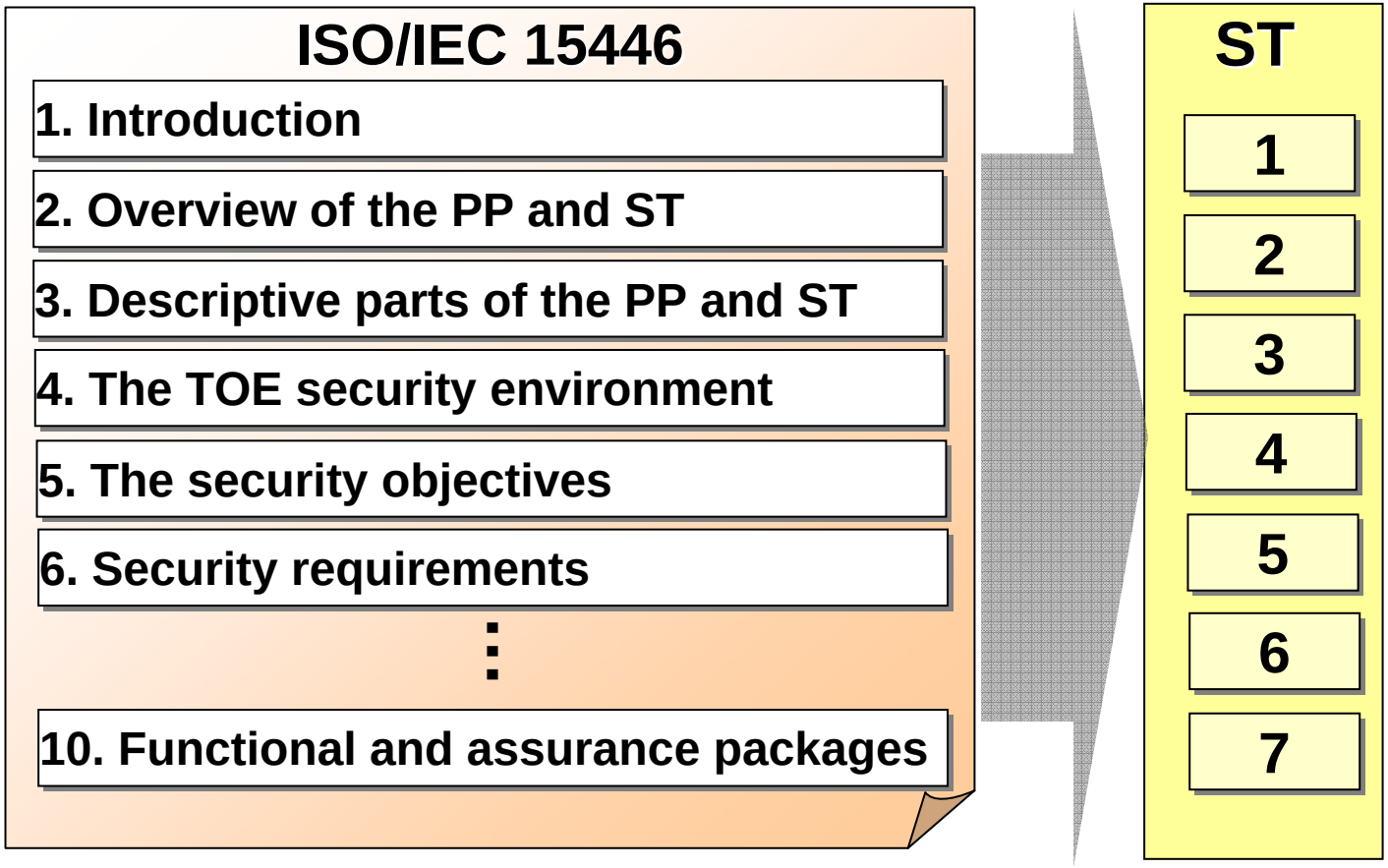
ISO/IEC 15408
ISO/IEC TR 15446

②

ISO/IEC 15408



ISO/IEC TR 15446



Security Target Contents

1. ST Introduction

2. Conformance Claims

3. Security Problem Definition
   - Threats
   - Organisational Security Policies
   - Assumptions

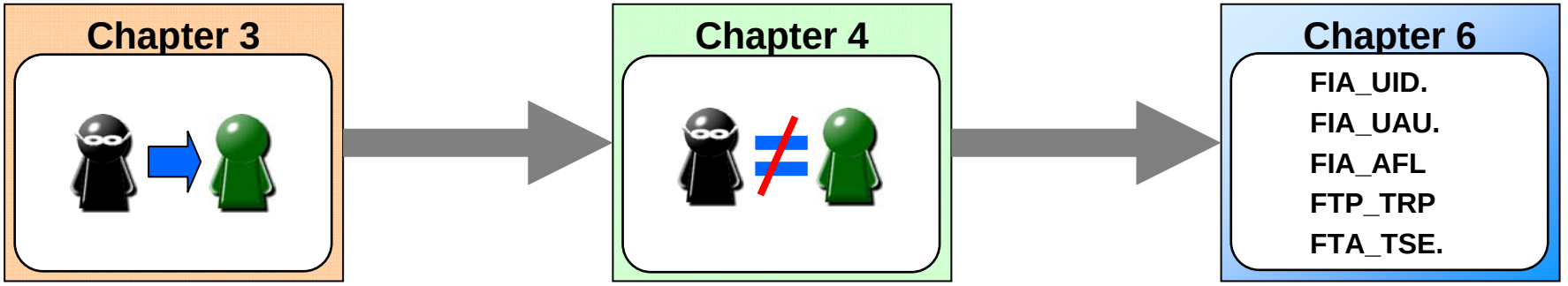
4. Security Objectives
   - Security objectives for the TOE
   - Security objectives for the operational environment

5. Extended Components Definition

6. Security Requirements
   - Security Functional Requirements
   - Security Assurance Requirements

7. TOE Summary Specification

Security Target Contents



3. Security Problem Definition

- Threats
- Organisational Security Policies
- Assumptions

4. Security Objectives

- Security objectives for the TOE
- Security objectives for the operational environment

6. Security Requirements

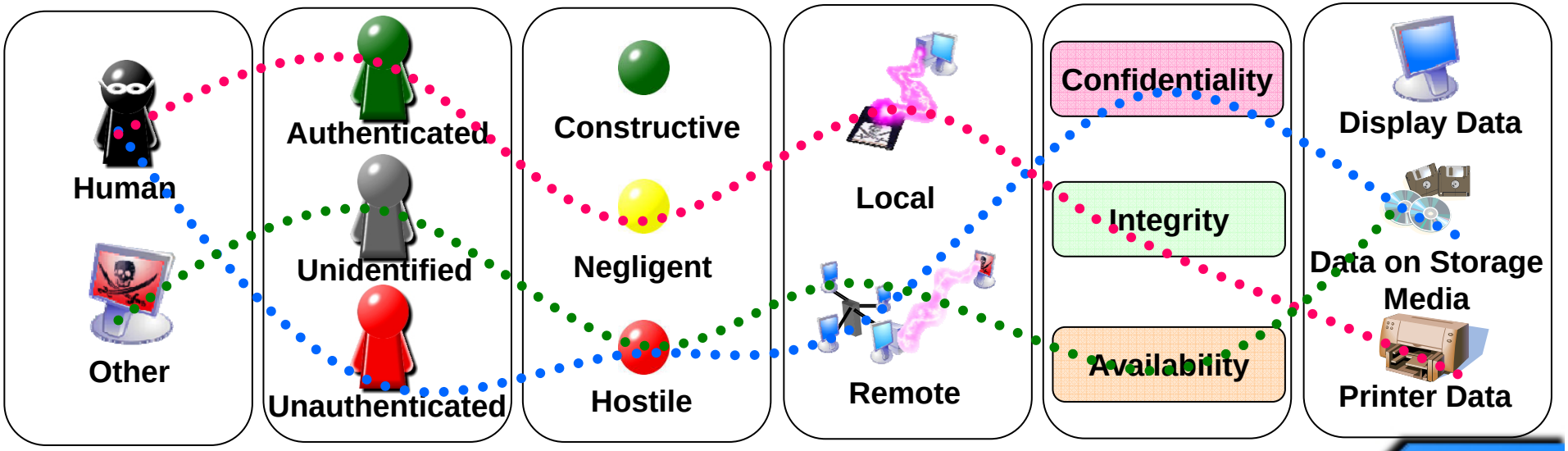
- Security Functional Requirements
- Security Assurance Requirements

Section 3

3. Security Problem Definition

Threats | **Organisational Security Policies** | **Assumptions**

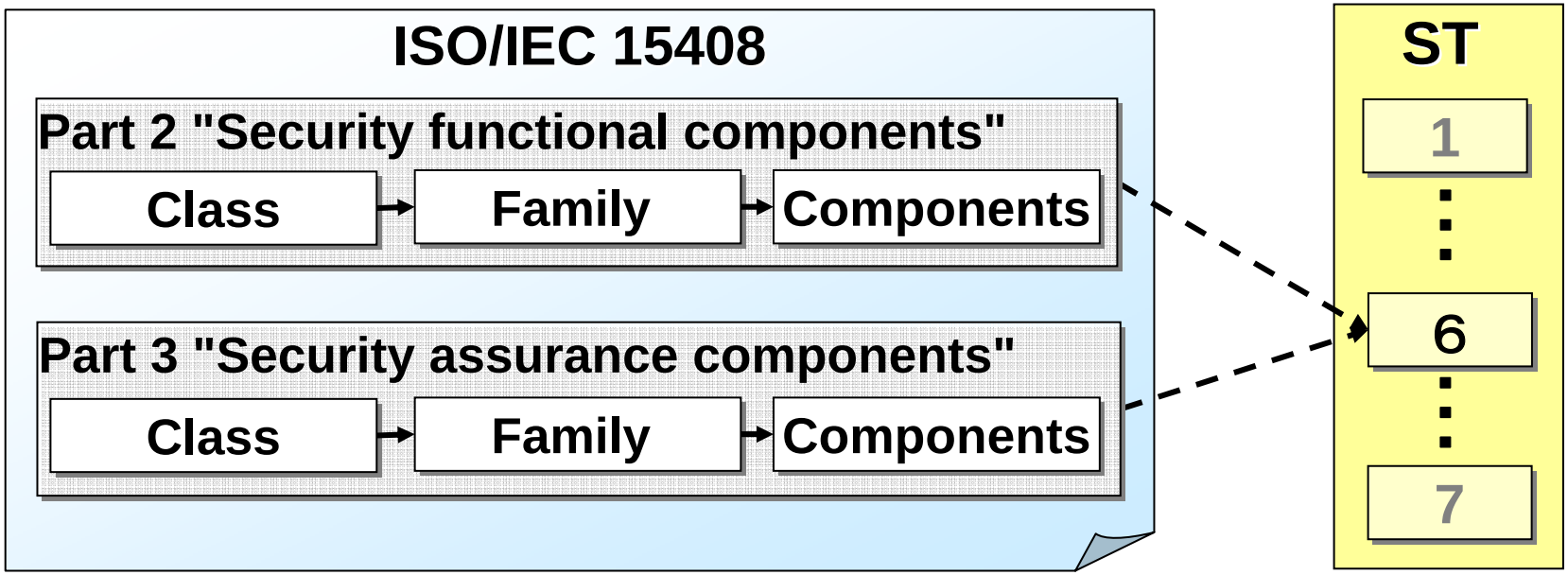
- The security problems to be addressed by the TOE
- CC does not provide a framework for risk analysis
- ST developers would be able to use a Threats Model tools



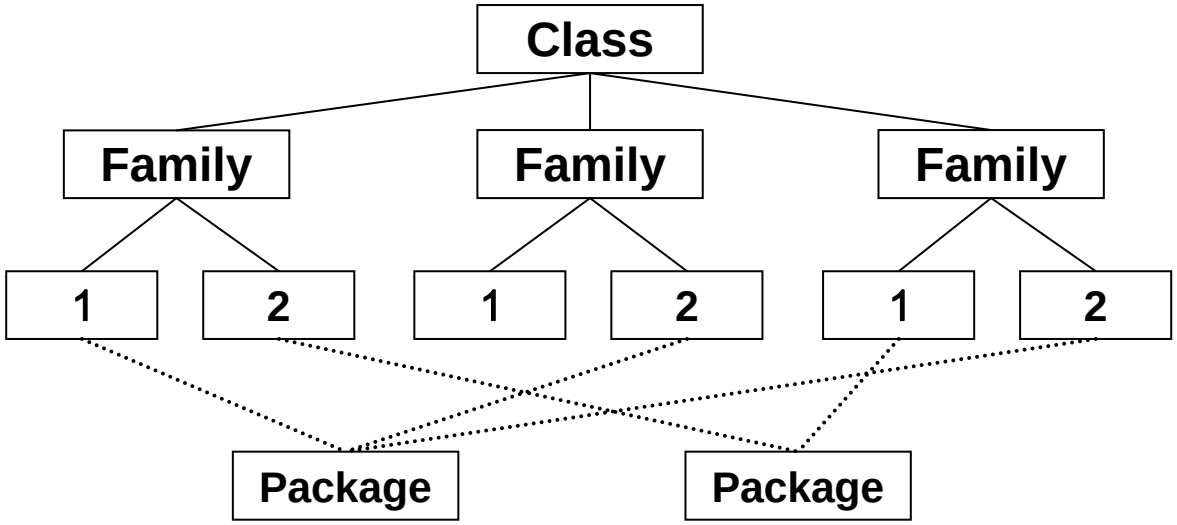
Section 6

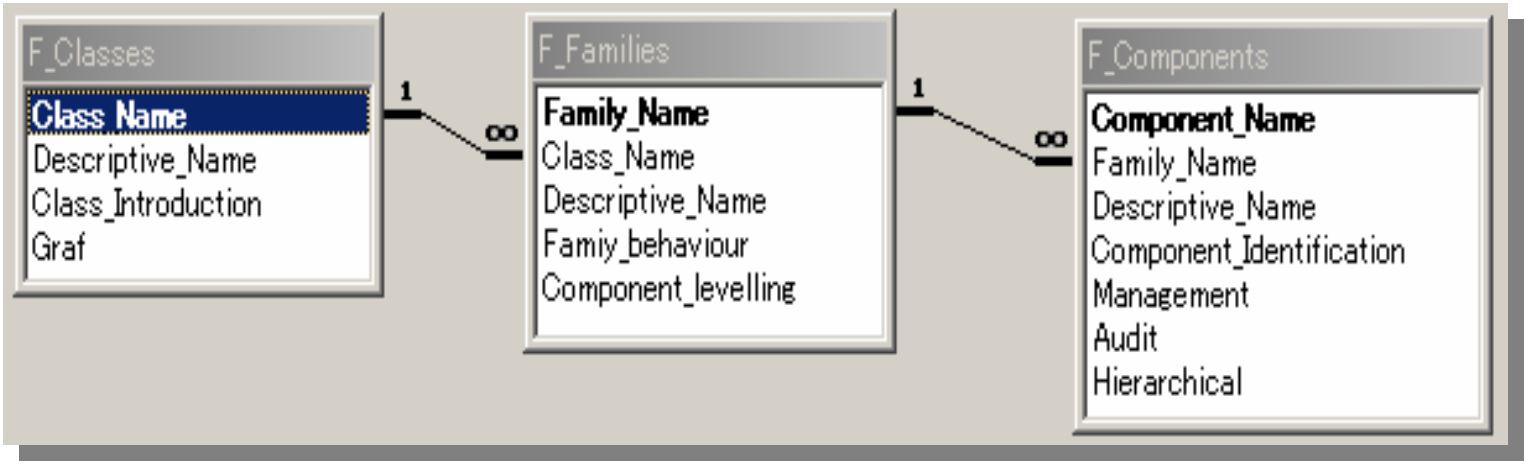
6. Security Requirements

- Security Functional Requirements
- Security Assurance Requirements

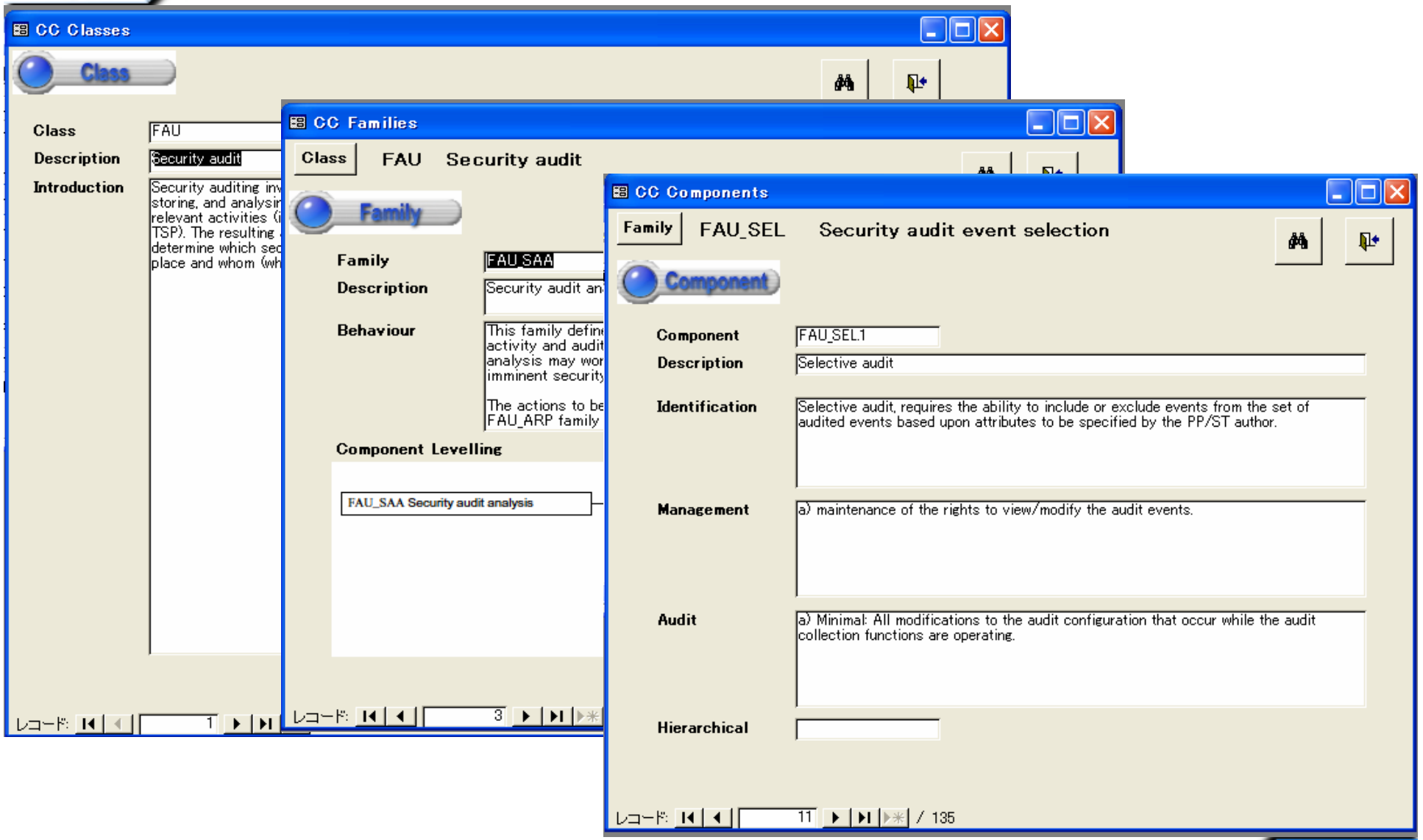


ISO/IEC 15408





ISO/IEC 15408 Knowledge-base

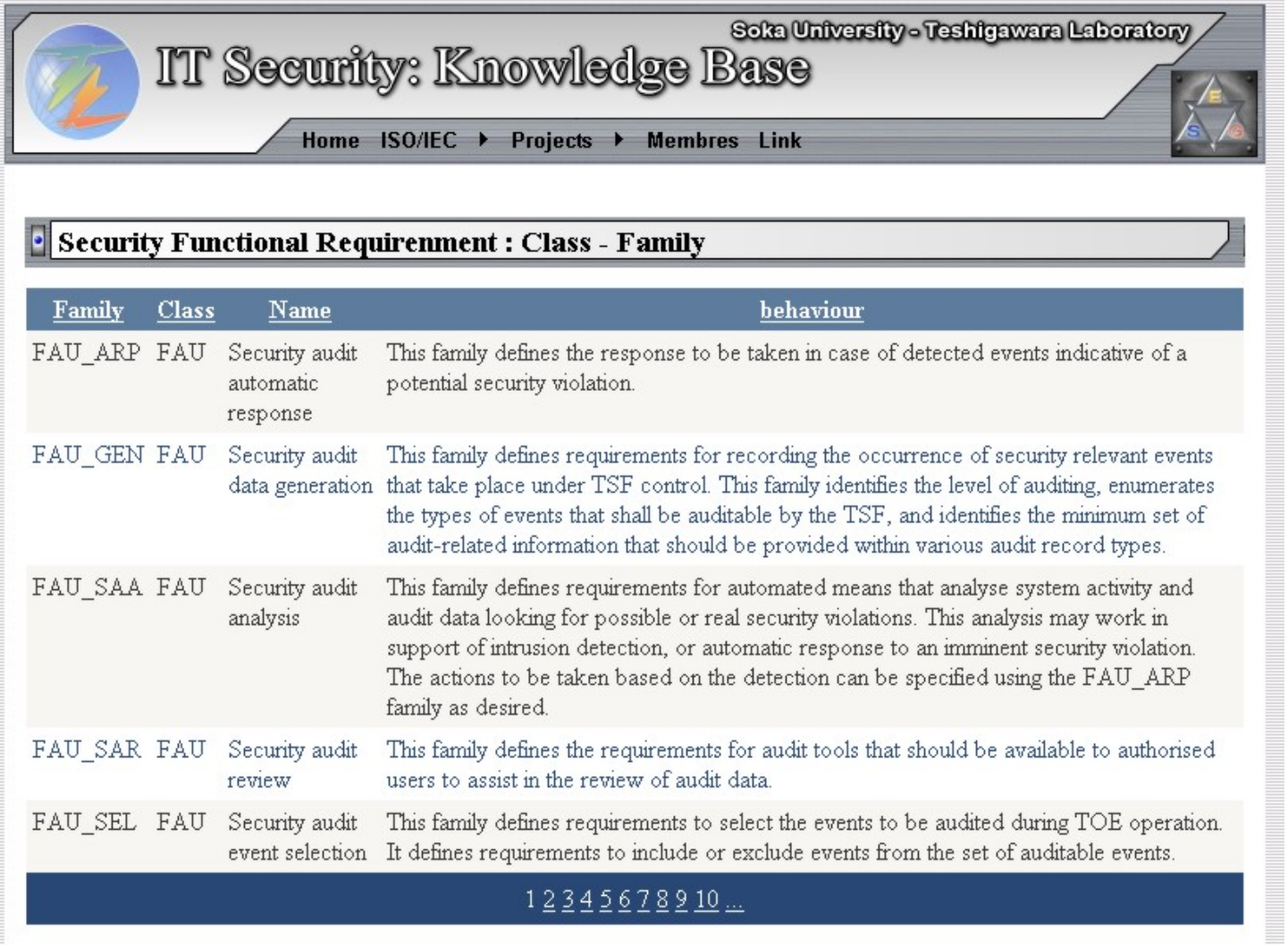


SFR : Class

Security Functional Requirenment : Class

Class	Name	Introduction
FAU	Security audit	Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities (i.e. activities controlled by the TSP). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.
FCO	Communication	This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt). These families ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.
FCS	Cryptographic support	The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software. The FCS class is composed of two families: FCS_CKM Cryptographic key management and FCS_COP Cryptographic operation. The FCS_CKM family addresses the management aspects of cryptographic keys, while the FCS_COP family is concerned with the operational use of those cryptographic keys.
FDP	User data protection	This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data. FDP is split into four groups of families (listed below) that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

SFR : Family



Family	Class	Name	behaviour
FAU_ARP	FAU	Security audit automatic response	This family defines the response to be taken in case of detected events indicative of a potential security violation.
FAU_GEN	FAU	Security audit data generation	This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.
FAU_SAA	FAU	Security audit analysis	This family defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to an imminent security violation. The actions to be taken based on the detection can be specified using the FAU_ARP family as desired.
FAU_SAR	FAU	Security audit review	This family defines the requirements for audit tools that should be available to authorised users to assist in the review of audit data.
FAU_SEL	FAU	Security audit event selection	This family defines requirements to select the events to be audited during TOE operation. It defines requirements to include or exclude events from the set of auditable events.

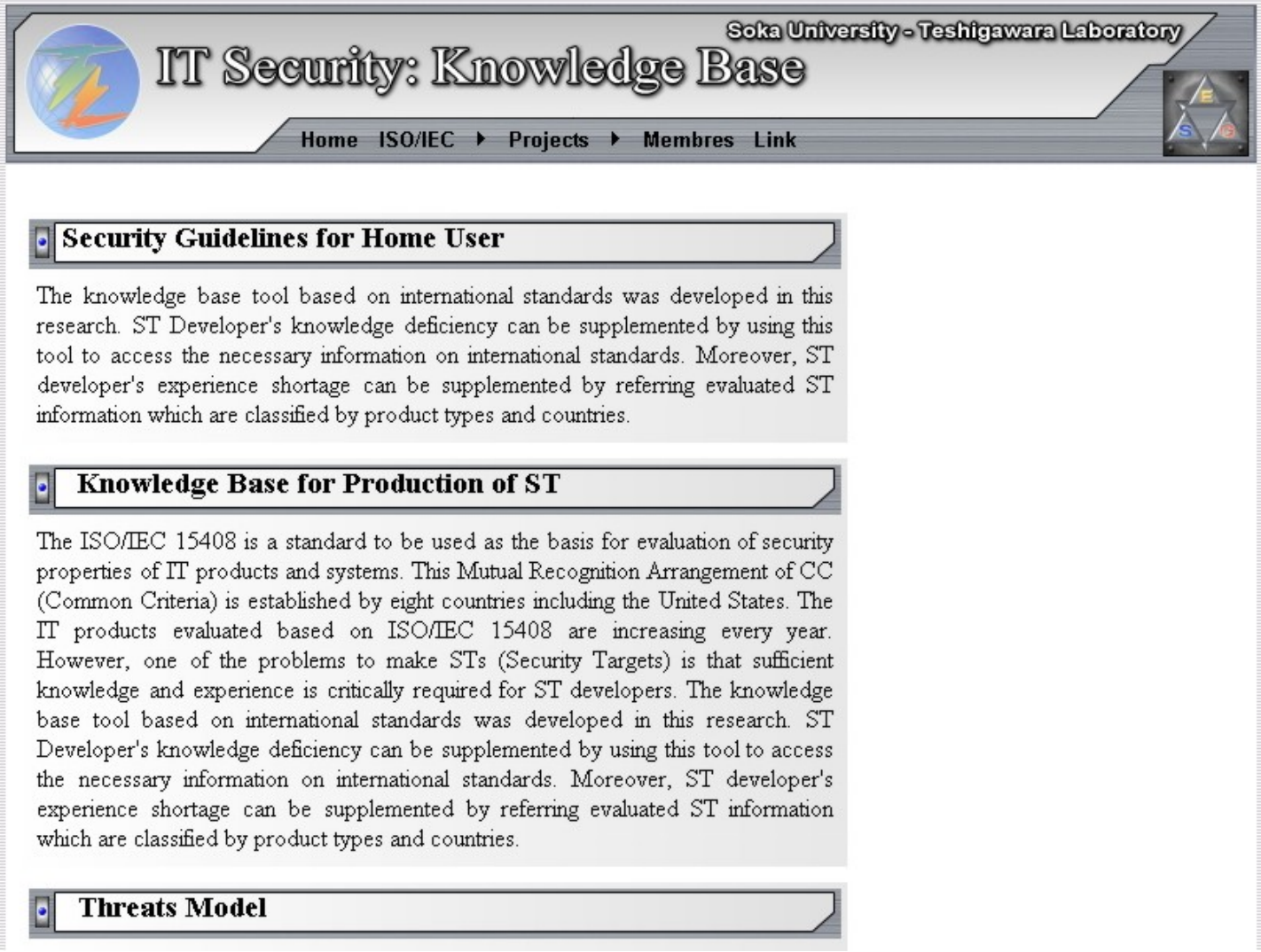
1 2 3 4 5 6 7 8 9 10 ...

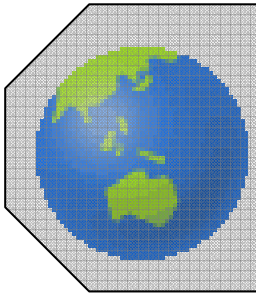
SFR : Components

Security Functional Requirenment : Class - Family - Components

Component	Family	Name	Identification	Management	Audit	Hierarchical
FAU_ARP.1	FAU_ARP	Security alarms	the TSF shall take actions in case a potential security violation is detected.	a) the management (addition, removal, or modification) of actions.	a) Minimal: Actions taken due to imminent security violations.	No other components.
FAU_GEN.1	FAU_GEN	Audit data generation	Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.			
FAU_GEN.2	FAU_GEN	User identity association	User identity association, the TSF shall associate auditable events to individual user identities.			
FAU_SAA.1	FAU_SAA	Potential violation analysis	Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.	a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.	a) Minimal: Enabling and disabling of any of the analysis echanisms; b) Minimal: Automated responses performed by the tool.	

Projects: Threats Model





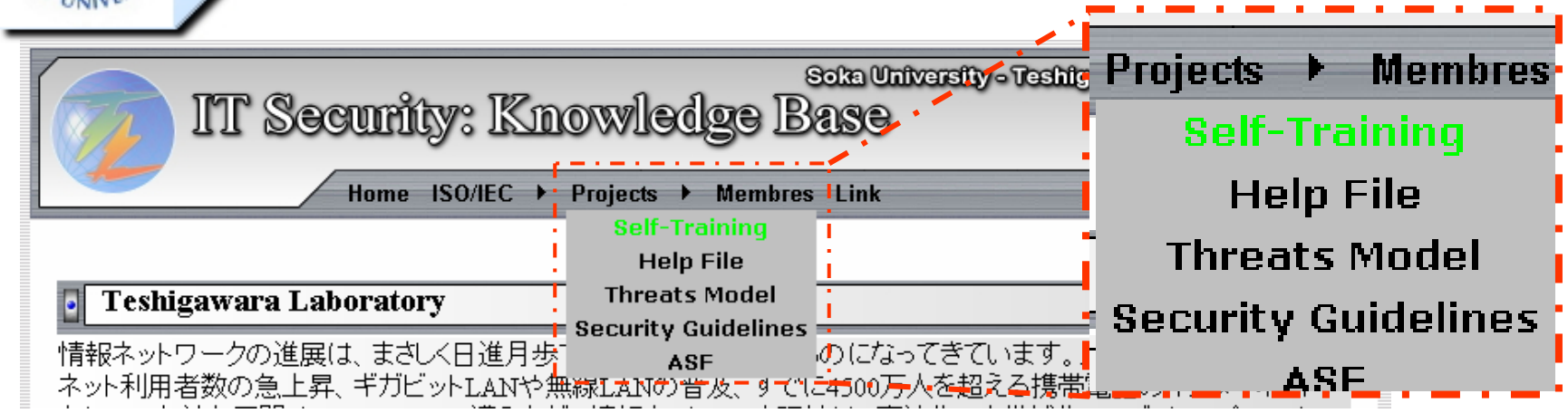
Self-Training System ③

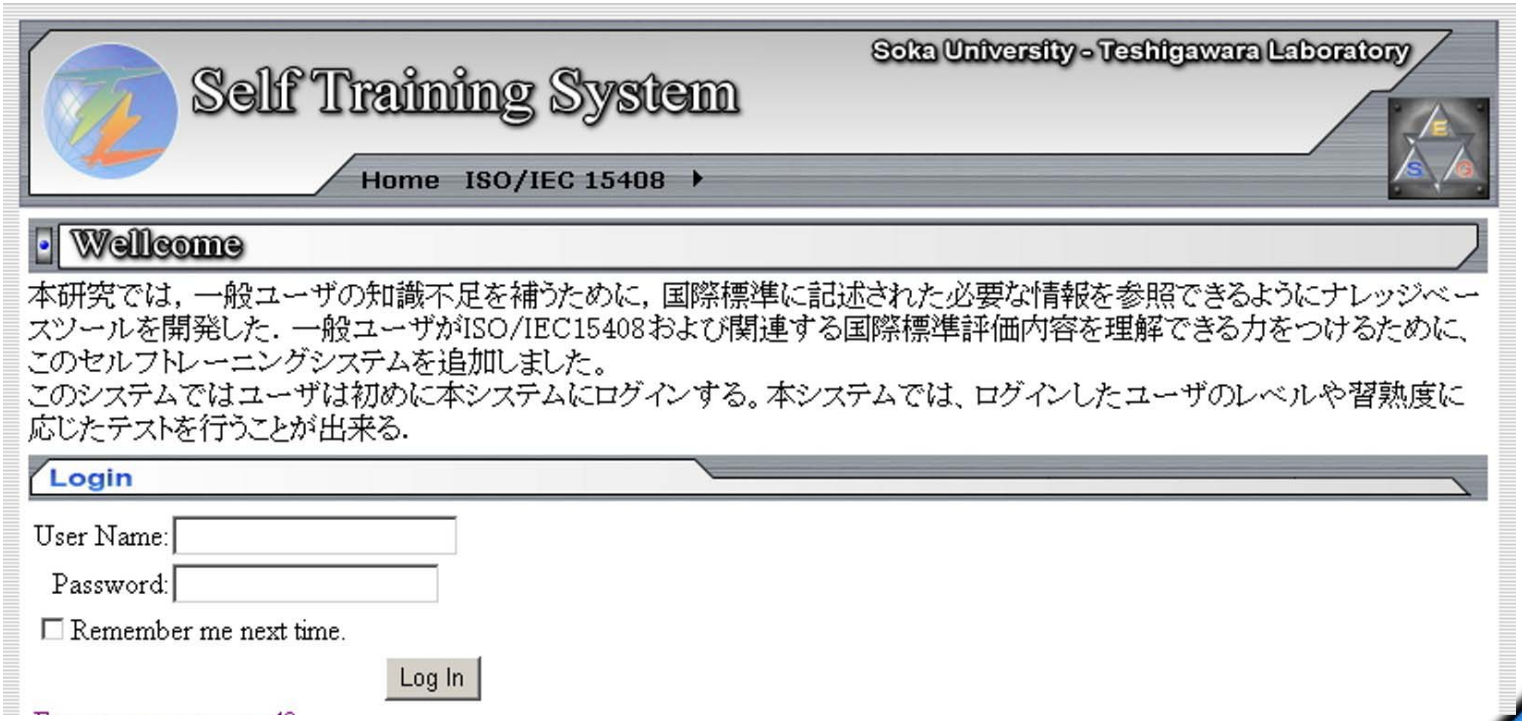
Target audience of the CC



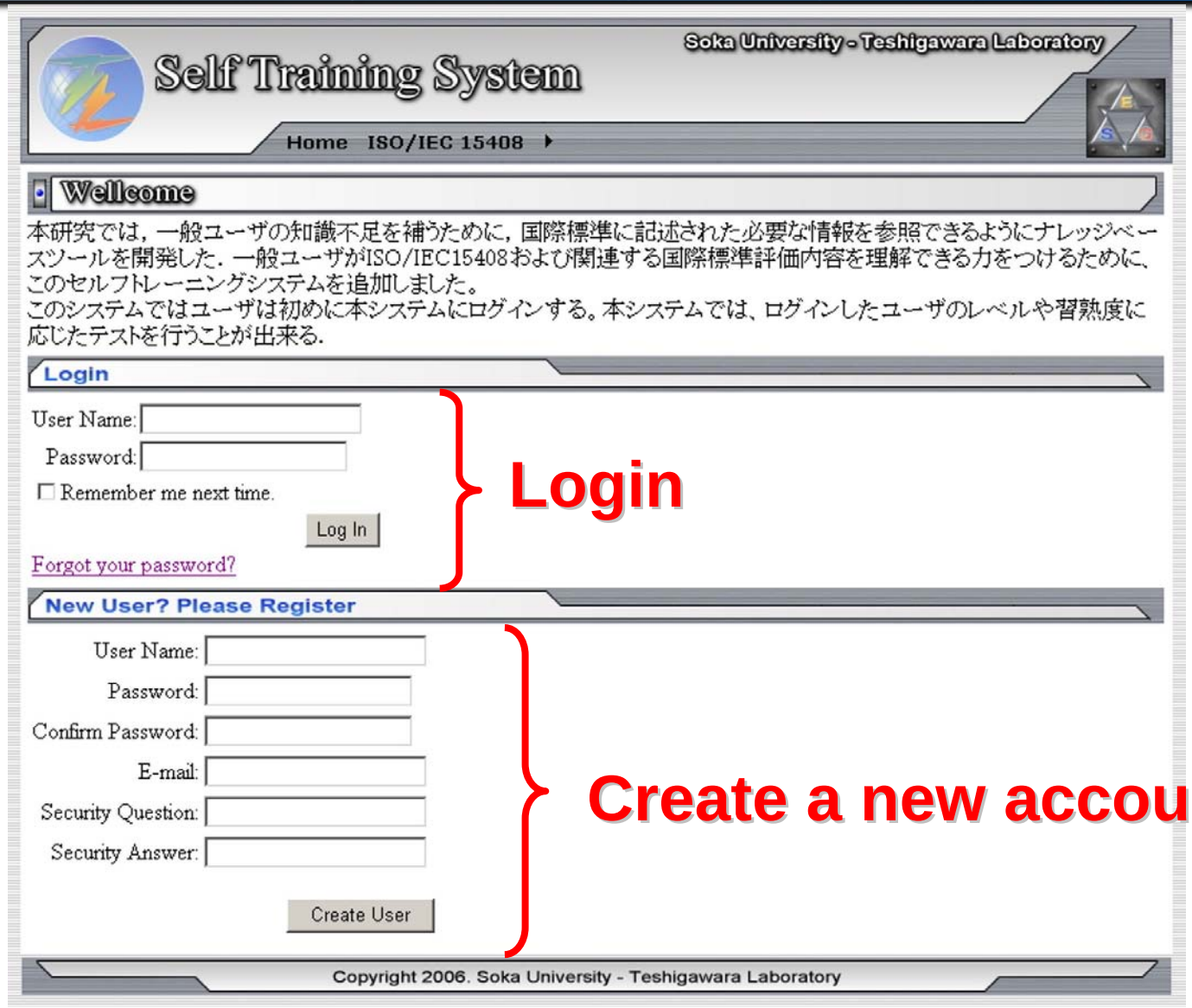
	Consumers	Developers	Evaluators
Advanced			
Intermediate			
Beginners			

Knowledge-based





Login

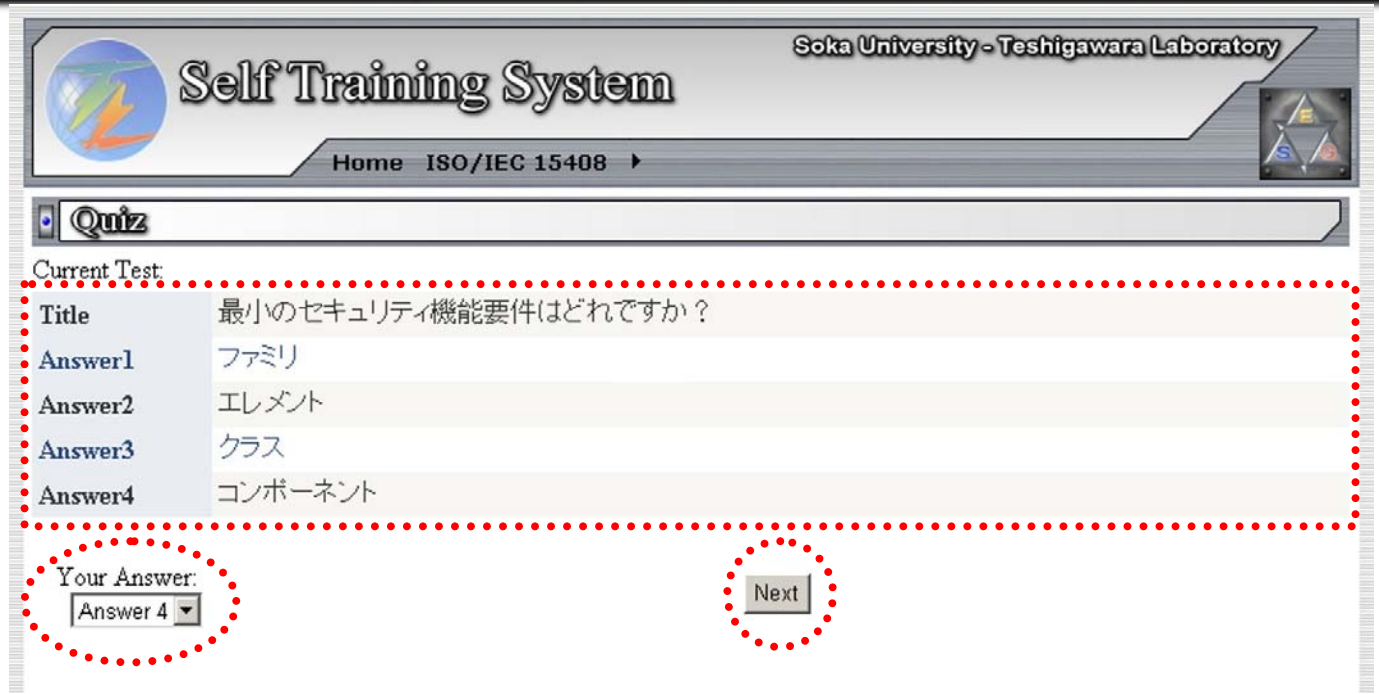

Soka University - Teshigawara Laboratory
Self Training System
Home ISO/IEC 15408
Wellcome
本研究では，一般ユーザの知識不足を補うために，国際標準に記述された必要な情報を参照できるようにナレッジベースツールを開発した．一般ユーザがISO/IEC15408および関連する国際標準評価内容を理解できる力をつけるために，このセルフトレーニングシステムを追加しました。
このシステムではユーザは初めに本システムにログインする。本システムでは、ログインしたユーザのレベルや習熟度に応じたテストを行うことが出来る.
Login
User Name:
Password:
Remember me next time.
Log In
Forgot your password?
Login
New User? Please Register
User Name:
Password:
Confirm Password:
E-mail:
Security Question:
Security Answer:
Create User
Create a new account
Copyright 2006. Soka University - Teshigawara Laboratory

Main Menu

List of available tests

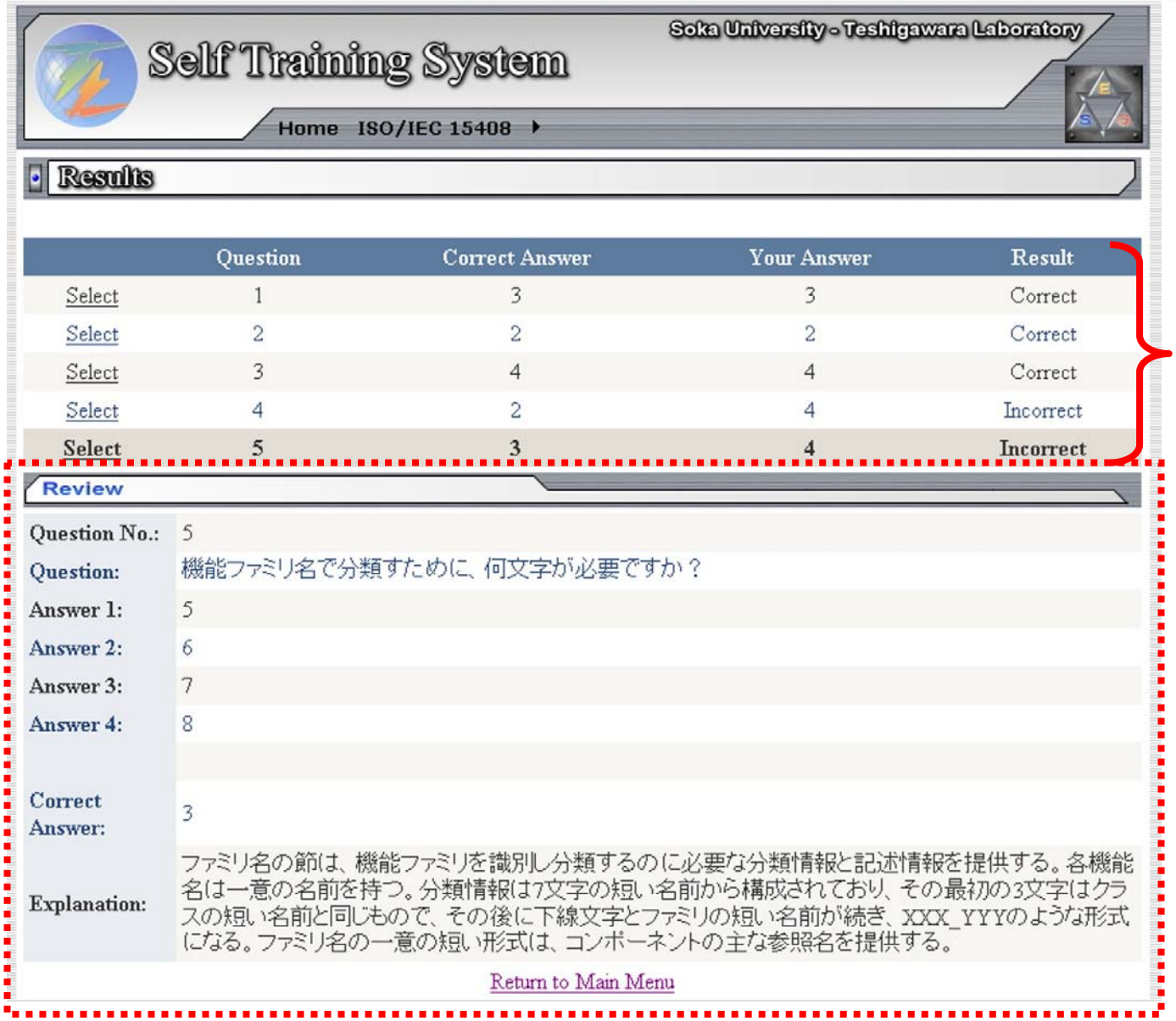
The user should be able to review the results of the tests taken in the past

Test Page



The user will see the questions and the possible answers, [1],[2],[3],[4]… they will pick one and click the next button

Results of the quiz



Knowledge Based Tool

Consumers

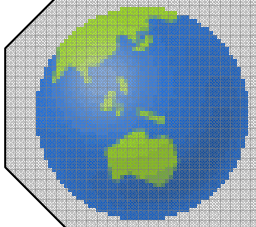
Developers

Evaluators

Security Functional Requirenment : Class - Family - Components

Component	Family	Name	Identification	Management	Audit	Hierarchical
FDP_ETC.2	FDP_ETC	Export of user data with security attributes	Export of user data with security attributes requires that the TSF enforce the appropriate SFPs using a function that accurately and unambiguously associates security attributes with the user data that is exported.	The following actions could be considered for the management functions in FMT Management: a) The additional exportation control rules could be configurable by a user in a defined role	The following events shall be auditable if FAU_GEN Security audit data generation is included in the PP/ST: A) Minimal: Successful export of information. B) Basic: All attempts to export information.	

beginners · Intermediate · Advanced



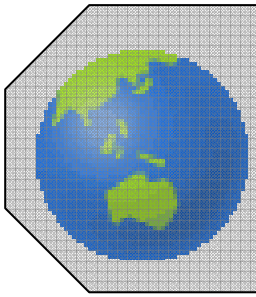
Conclusion & Future Works

Conclusion

- Design and development of a knowledge-based tool for ST developers based on CCV3.1.
- It was explained the architecture of the knowledge-based tool and showed how it can help ST developers create STs that are to be evaluated by CC.
- ST developer's **knowledge** deficiency can be supplemented by using this tool to access the necessary information on international standards.
- ST developer's relevant **experience** faced by ST developer can also be supplemented by referring to evaluated information of STs which are classified by types and countries.

Future Works

- ISO/IEC 19791 is an international standard that must be used as the basis for evaluation of operating system.
- This new standard will be included in the knowledge-based tool.



Questions & Answers

http://www.teshilab.net

Guillermo Horacio RAMIREZ CACERES **Yoshimi TESHIGAWARA**

Graduate School of Engineering, Soka University

Tokyo, Japan

E-mail:{guillerm,teshiga}@soka.ac.jp