

Current smartcard security activities in Japan



2010.09.22-24 #11 ICC

ECSEC T.R.A.

Secretariat of ICSS-JC, the Japanese consortium

Yasuyoshi Uemura

Preface

We know that security issues are global.

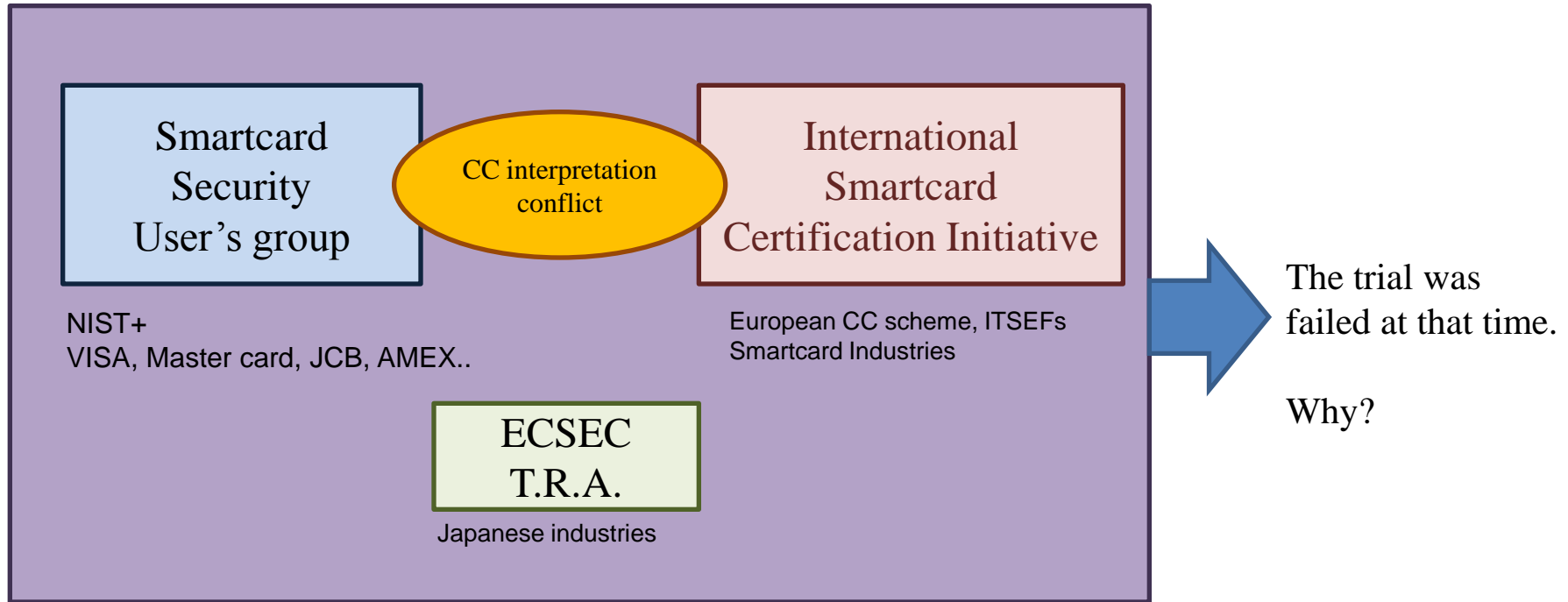
Through networks, any threat becomes global problem.

Many companies are competing their products performance, keeping their product confidential. But we all will not be able to allow a insecure product connects to global system in another country. That is why we need security assurance in same manner as another region is doing.

Since above, we are intending to contribute to CCRA.

We also know international harmonization through discussion is very important **especially in hardware security** field.

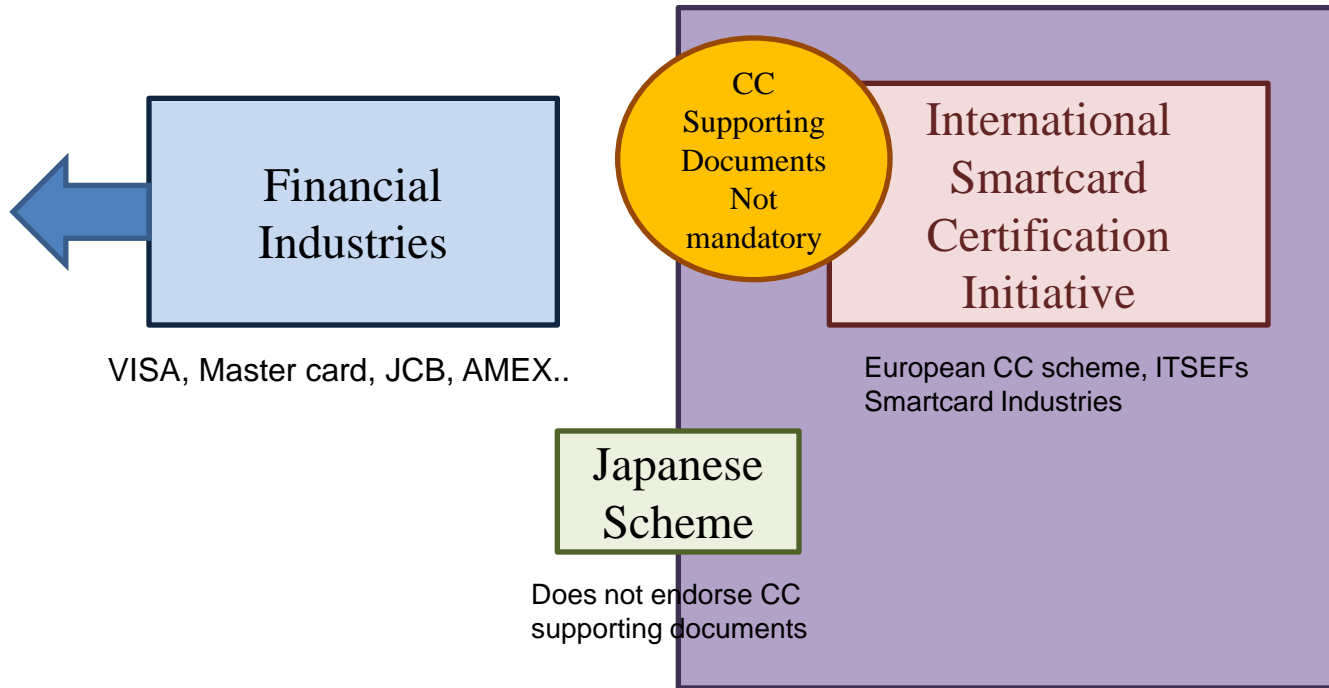
Tall tales, once upon a time



CCRA 2001-2002

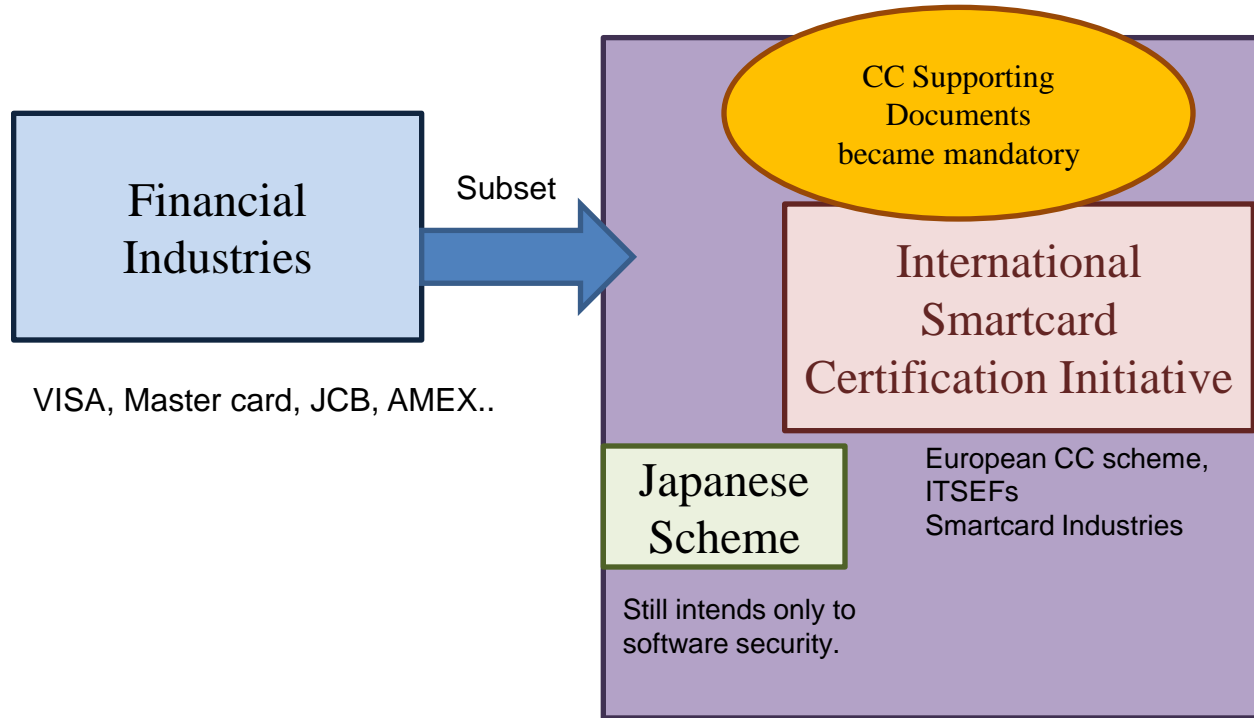
Under CCRA initiative, it was tried to build worldwide understanding for CC hardware interpretation.

CCRA 2003-



Japanese scheme denied JIL origin documents and intends only to software security. Financial industries run away from CC certification, since CC is not cost effectable. European manner became CC subset but not mandatory.

CCRA 2006-



CC supporting documents became mandatory on 2006.

The European manner took a formal position in CCRA.

Financial industries began to use a part of CC evaluation in their private scheme.

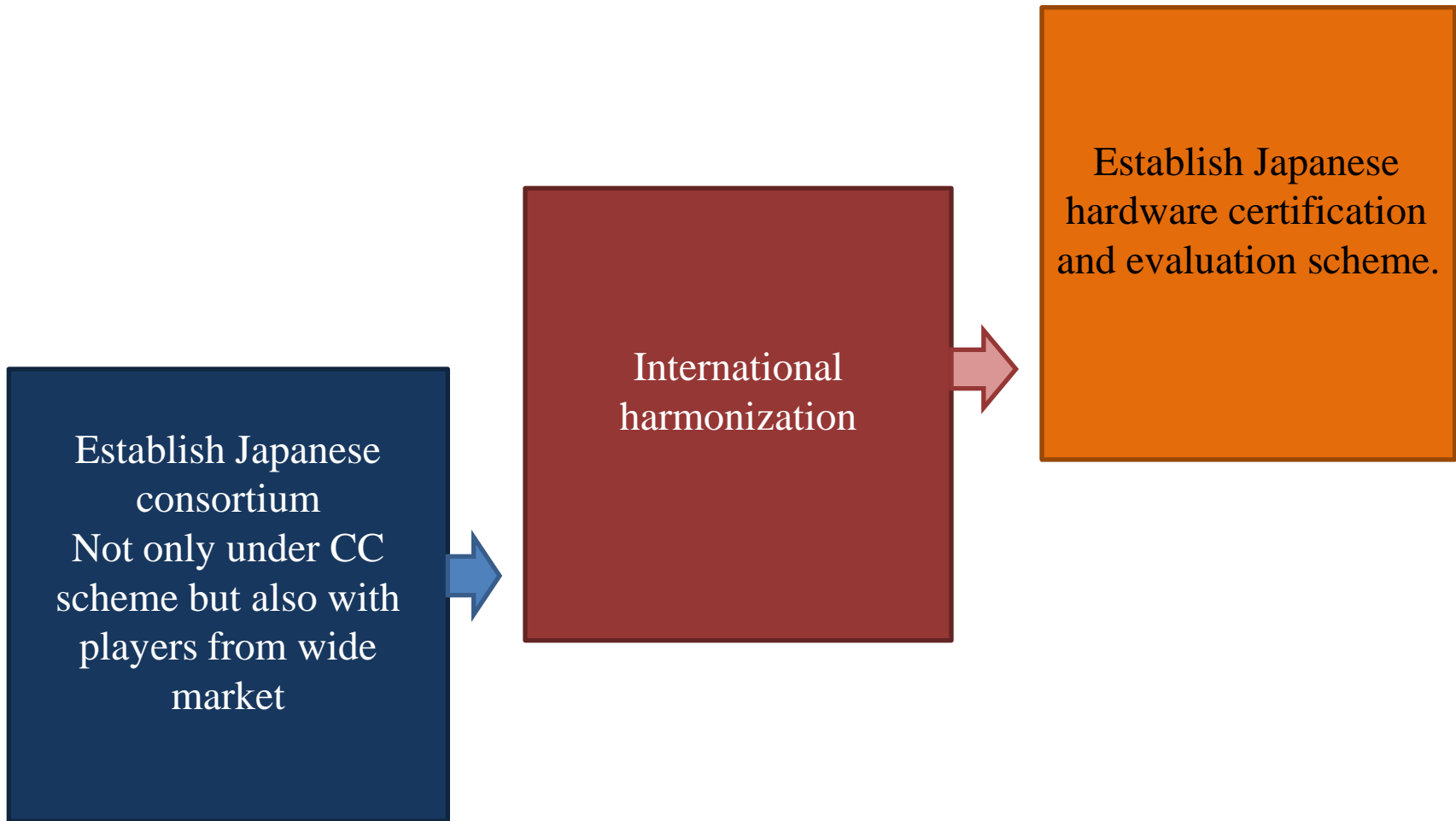
Even recognizes CC supporting documents as “mandatory”, Japanese scheme still intends only to software security.

Japanese hardware industries run into European scheme to be certified.

Back ground of Japan's activity after ten years.

- ◆ Japan has **huge market**, a number of users and vendors of IC chip and smartcard; or products of embedded IC chips.
- ◆ However, Japanese CC scheme has been intended mainly to software field during these ten years.
- ◆ Now, Japanese scheme starts to set up CC hardware security assurance for above market. Both certification and evaluation scheme now being prepared.
- ◆ In the hardware security field, **we declare to respect the manner** which has been carried by European society in CCRA during these ten years.
- ◆ Japan has no intention to act somewhat different from above manner, but intends **international harmonization**.

Japan's Strategy



The activities through
IC System Security Round Table
and ICSS Japan Consortium

IC System Security Round Table ICSS-RT



Discuss all things related to
Security Assurance of
Smart chip, Devices using smart chip,
and its application systems in Japan ,
and also international issues of this field.

Target of activity

Smart chip, Devices using smart chip,
and its application systems

Applicants; 36 entities

User of the application system, Provider of the application system, Provider of the software, Provider of the device, Provider of the chip, Evaluation facility, Certification body, National laboratory

AIST(National Laboratory)
Canon
Dai Nippon Printing
ECSEC Laboratory (ITSEF)
ECSEC T.R.A.
FeliCa Networks
Hitachi
IPA (CB)
ITSC (ITSEF)
Japan Consumer Credit Association
Japan Credit Card Association
Japan Payment Service Association
Japan Quality Assurance Organization
Japan Smartcard Solutions
JCB
JR East
JR East Mechatronics
Kyodo Printing

Lac
Maxell Seiki
Mitsubishi Electric
Mizuho IR (ITSEF)
Nippon Conlux
Nozomi
NTT Communications
NTT Data
Oki Engineering
Panasonic
Panasonic System Networks
Renesas Electronics
Seibu Holdings
Sharp
Sony
Toppan Printing
Toshiba
TUViT Japan(ITSEF)

ICSS-RT Membership, 36 entities, Sep.2010

Copyright ECSEC T.R.A. Sep 2010

ICSS-RT

Discuss all things related to Security Assurance of IC systems in Japan

- Proposing what kind of social infrastructure is needed to realize reasonable security assurance for IC systems in Japan .
- Proposing what kind of technical basis are needed for security assurance of this field in Japan.

Discuss security situation in the market

- ◆ Exchange information about real threats in the market.
- ◆ Exchange information about actual attack event and its techniques in the market.
- ◆ To modify and abstract the information about actual attack event and its techniques through the secretariat if needed.
- ◆ In put the information to ICSS-JC

Discuss the sudden and important security event in IC application systems

- ◆ Discuss how to manage the security event suddenly happened in the important social application system such as finance system or transportation system as well.
- ◆ Discussion between all stakeholders, if the event could not be resolved between specific user and vendor.
- ◆ Even if the event is happened in foreign society, if the influence will come to Japanese social system.

IC System Security Japan Consortium =ICSS-JC



Working Group in ICSS-RT

Discuss CC application in this field
as international standard of security assurance

Member

Those who has interest to **CC**
certification in the ICSS-RT
members.

ICSS-JC

- ◆ ICSS-JC stands for IC System Security- Japan Consortium, which has 13 registered member organisations as of September 2010.
- ◆ ICSS-JC has been organised on 22nd July 2009.
- ◆ Objectives include establishing the hardware evaluation scheme based on CC that will be consistent with the European scheme.

AIST(National Laboratory)

Dai Nippon Printing

ECSEC Laboratory (ITSEF)

FeliCa Networks

IPA (CB)

ITSC (ITSEF)

Mizuho IR (ITSEF)

NTT Data

Panasonic System Networks

Renesas Electronics

Sony

Toppan Printing

Toshiba

ECSEC T.R.A. [Secretariat]

ICSS-JC Membership, 14 entities, Sep.2010

Evaluation Methodology and Procedures

- ICSS-JC is intending to prepare Japanese documents for evaluation methodology and procedures under CC supporting documents adjust to international standards.
- Above are needed to keep **equivalence of CC evaluation results** between CCRA countries, especially with Europe.

Extent of security implementations

- ◆ According to information of attack examples from market, publications, and input from ICSS-RT or international society
- ◆ ICSS-JC is intending to discuss “From when, what kind of security measures should be implemented to the product for which application, against which attack techniques”.
- ◆ Above may be related to the international standard of evaluation procedure in vulnerability analysis part.
- ◆ We are not intending to do somewhat different to what other countries are doing.
- ◆ **We want to harmonize Japanese procedures to the international.**

State of art security techniques

- According to study results from the national laboratory, publications, and information from discussion between foreign countries,
- ICSS-JC is intending to share state of art security techniques in this field and discuss its application to the security evaluation and assurance.
- Each member may take the position for technical contribution and result will be brought together.

ICSS-JC Activity Report

From July 2009 to September 2010

	Meeting	Date	No. of Attendees
1 st	Regular meeting	22 nd July 2009	35
2 nd	Regular meeting	7 th October 2009	34
3 rd	Regular meeting	26 th October 2009	30
4 th	Regular meeting	6 th January 2010	28
5 th	Regular meeting	26 th January 2010	20
6 th	Regular meeting	19 th February 2010	30
7 th	Regular meeting	12 th May 2010	24
8 th	Regular meeting	2 nd June 2010	28
9 th	Regular meeting	7 th July 2010	27
10 th	Regular meeting	1 st September 2010	28

Summary of Meetings

- ◆ Confirmation of information control rules
- ◆ METI national project; “*Development for security evaluation techniques of system LSI*”
- ◆ Reviewing CC documents related to the hardware evaluation
- ◆ Availability of DPA evaluation board SASEBO as the test vehicle
- ◆ CC hardware evaluation seminar
- ◆ Discussion; Attack database
- ◆ Discussion; CC hardware evaluation procedure

METI National Project Overview

- ◆ Project name: Development for security evaluation techniques of system LSI
- ◆ Sponsor: Ministry of Economy, Trade and Industry (METI)
- ◆ General contractor: ECSEC.TRA
- ◆ Term: **December 2009 – March 2012**
- ◆ Total budget: 655 million Yen
- ◆ Objectives include;
 - ◆ **establishing hardware security certification scheme**
 - ◆ establishing a chip testing laboratory in Japan, premises with equipment, trained personnel as well
 - ◆ Research and development for hardware security evaluation techniques
 - ◆ Supporting activities for international harmonization

FPGA board SASEBO as a Test Vehicle

- ◆ Standard FPGA testing board “SASEBO-GII” developed by AIST may be provided to ICSS-JC as a common test vehicle
- ◆ Although it may not be enough for all kinds of attacking, it will be useful as a standard test vehicle for power analysis attack techniques
- ◆ The user of SASEBO may integrate original countermeasures into FPGA by their own
- ◆ Specifications are provided from the following URL
 - ◆ http://www.rcis.aist.go.jp/files/special/SASEBO/SASEBO-GII-en/SASEBO-GII_Spec_Ver1.0_English.pdf

Activity Plan Overview

- ◆ Attack Database, Reviewing New Attacks
- ◆ Guidance for Hardware Evaluation
- ◆ Protection Profiles

Attack Database

- ◆ Comprehensive information gathering and reviewing on all kinds of attack methods and countermeasures
- ◆ Discuss whether there are any attack examples or methods to be added to CC supporting documents
- ◆ Experiences from Japanese vendors
- ◆ Reproduction in Japanese testing laboratory

This activity had started to examine whether attack samples are enough in the CC supporting document.

The approach is as following.

- i. Making the data base of almost all disclosed papers related to smartcard security.
- ii. Setting them in order to attack category in CC supporting document.
- iii. Picking out “key words” from each attack category.
- iv. Retrieving each key word in the abstract of each document.
- v. Re-setting documents in order to attack category in CC supporting document, using the approach iv. result.
- vi. Rating and ranking each document according to the priority.
- vii. Examine whether any attack exists which cannot relate to explicit categories or not.
- viii. Call ICSS-JC members for any attack category or attack sample shall be added to DB or not.

Guidance for Hardware Evaluation

- ◆ Guidance for ICSS-JC members
- ◆ Same manner with JIL group countries
- ◆ How the actual CC hardware evaluation should be performed
- ◆ What shall be prepared by the sponsor before the evaluation
- ◆ How the CB and ITSEF will work together
- ◆ Understanding how the hardware products will be certified

Integrating “Vulnerability centric evaluation” to Japan being discussed through reviewing SIN092 the British working draft.

Protection Profiles

- ◆ It is important to develop PPs to expand CC hardware evaluation market in Japan
- ◆ PPs should be developed not only for chips themselves but also for smartcard systems to keep total security
- ◆ Following 3 fields of PPs are expected to be published and certified within 2 years in Japan, through METI project with ICSS-JC support
 - ◆ Composite PP for multiple application smartcard systems
 - ◆ PP for payment terminal systems
 - ◆ PP for personal identification systems using smartcards

Yasusyoshi Uemura

Executive Vice President

Electronic Commerce Security Technology Research Association

uemura@ecsec.org

Secretariat of

**IC SYSTEM SECURITY ROUND TABLE
IC SYSTEM SECURITY JAPAN
CONSORTIUM**