出國報告（出國類別：會議）

參加 2009 年第 10 屆
國際共同準則研討會（ICCC）報告書

服務機關：國家通訊傳播委員會
姓名職稱：謝進男　委　　員
　　陳春木　簡任技正
派赴國家：挪威
出國期間：98 年 9 月 20 日至 9 月 26 日
報告日期：98 年 12 月 25 日

摘要

第 10 屆國際共同準則研討會議(ICCC, International Common Criteria Conference)自 98 年 9 月 22 至 24 日於挪威特羅姆瑟(Tromso)舉行，共有來自 28 個國家及地區之驗證機構、檢測實驗室、資通安全領域專家、研究機構及資通設備廠商等約 300 人參加，以下世代發展趨勢、檢測技術及經驗分享等三大主軸共有 63 場發表會。

參與本次國際研討會有助於本會掌握最新資通安全相關技術標準與趨勢，俾作爲修訂相關技術規範參考，並擴展同仁視野。亦可了解他國資通安全驗證體系發展情形、檢測實驗室與驗證機構專業能力及投入驗證經驗，可作爲本會強化我國資通安全驗證體系、提升資通安全驗證能力及完備驗證作業程序之參考依據。

我國在今年的行政院 2009 年產業科技策略會議中，以建立資通訊基礎建設安全信賴機制議題，針對資通訊產品認證問題提出討論，經由該會議蒐集各界意見，由本會擬具 4 年計畫，將先進行認證體系在我國可行方式研究，後續再推動資通訊產品認證及政府機關優先採購經認證資通訊產品，逐步建立我國資通訊產品認證體系，確保我國資通訊產品安全。

目　　錄

壹、目的

共同準則(Common Criteria，亦稱 ISO/IEC 15408，簡稱 CC)爲目前國際通用的資安產品驗證標準，它於 1990 年中期整合美國 TCSEC(Trusted Computer System Evaluation Criteria)、加拿大 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)及英、德、法三國 ITSEC(Information Technology Security Evaluation Criteria)等資安標準，於 1999 年 8 月公告 2.1 版並正式運作，其後經過數次修訂，於 2006 年 9 月正式發佈 CC 3.1 版，目前 CC 4.0 也正在緊鑼密鼓的修訂和討論中，預計明年可以正式發布。CC 的目標爲確保評價的 IT 產品和保護剖繪(Protection Profile，簡稱 PP)的一致標準；要增進評估的有效性、安全性更高的 IT 產品及保護剖繪；消除 IT 產品和保護剖繪的重複評價負擔；不斷提高評估和認證/驗證處理 IT 產品及保護剖繪的效率和成本效益。

共同準則相互承認組織(Common Criteria Recognition Agreement，簡稱 CCRA)的目的爲促進 CC 目標實現，讓認證/驗證機構（CB）發行 CC 證書應符合高度和一致的標準，使資訊科技產品及保護剖繪獲得 CC 認證後，使用者在購買或使用這些產品時，不需要作進一步評估。

CCRA 目前共有 26 個會員國，已申請成爲「接受證書會員國」（Certificate-Consuming Participants，簡稱 CCP），計有奧地利、捷克共和國、丹麥、芬蘭、希臘、匈牙利、印度、以色列、馬來西亞、巴基斯坦、新加坡、土耳其等 12 個國家；已申請成爲「核發證書會員國」（Certificate-Authorizing Participants，簡稱 CAP），計有澳大利亞、紐西蘭、加拿大、法國、德國、意大利、日本、挪威、西班牙、瑞典、荷蘭、大韓民國、英國、美國等 14 個國家。CCP 指需接受 CAP 已驗證的資通產品，不必再經其國內驗證機關核證，即可在其國內市場上行銷。CAP 指該國具有驗證資安產品能力，並可核發驗證證書，憑此證書可將產品行銷至其他 25 個會員國，不必再向其輸出國重新申

請產品驗證。即通過 CC 驗證之資訊產品能獲得各國的認可與採用，以免除開發廠商重複送驗之不便。

國際共同準則研討會議(International Common Criteria Conference，簡稱 ICCC)輪流由 CCRA 會員國每年輪流主辦一次，主要目的是藉由 CCRA 各會員國間的經驗分享與交流，傳遞新的技術、威脅與弱點資訊，強化與改善 CC 標準規範，並推廣市場應用面，同時就政府與企業所關切的產品資安議題，討論如何架構更安全的資安基礎環境。

參與本次國際研討會可獲得最新國際資通安全檢測技術資訊、各國資通安全產品檢測及驗證推動現況、共同準則最新版本之制訂內容與進度等相關訊息。有助於本會掌握最新資通安全相關國際技術，俾作爲未來修訂相關技術規範參考；亦可了解他國在資通安全產品驗證體系的優缺點，檢測實驗室及驗證機構之專業能力，投入評估驗證之經驗，可作爲本會未來強化我國資通安全驗證體系、提升資通安全驗證專業能力及完備評估及驗證作業程序之參考依據。

本次研討會由本會謝委員進男、技術管理處陳簡任技正春木、財團法人電信技術中心(TTC)王資深顧問碧蓮、林副組長家弘及崔副理存得共計 5 人參加，另我國財金公司也有派代表參加。TTC 並就共同準則下世代 (The Next Generation of CC)議題，向大會提出 Challenges and Solutions of Distributed Systems Composition 論文，業經大會錄取，並受邀於本屆 ICCC 會議中進行簡報。

貳、 研討會簡介

2009 年第十屆國際共同準則會議(簡稱 ICCC 2009)係由挪威驗證機構 NSM (The Norwegian National Security Authority) and SERTIT (TheNorwegian IT Security Certification Authority)主辦。

除例行的開閉幕儀式與專題演說外，其他時段均同時安排三個子議程(Track)進行分組研討，主要議題包含下世代發展趨勢、檢測技術及經驗分享等三大主軸，共有 63 場發表會。主要議題如下：

The Next Generation of CC
Detailed Report
Evidence based Evaluations
Predictive Assurance
Skills and Interaction
Tools Support
CC in the 21st Century
CC and EU
Scheme Update
Protection of Critical Infrastructure
Tools, Techniques and Experience
E-Health and Trustworthy IT
Smart Card
E-ID
Vendors and CC
Other Topics

參、 研討會時間、地點及議程

本屆研討會於挪威(Norway)特羅姆瑟(Tromso)島舉行，自 98 年 9 月 22 日至 9 月 24 日共計 3 天，大會議程說明如下：

22 September 2009

Time	Track1 (Nord-Norge)	Track2 (Rica Hall II)	Track3 (Rica Hall I)
09:30-10:00	**Opening Plenary** (Rica Hall) **Opening Ceremony** Øistein Hanssen, Local Entertainer Berit Alette Mena, Local Entertainer **Welcoming addresses** Arild Hausberg, Mayor of Tromsø **Opening speeches** Knut Anders Moi, Deputy Director General, Ministry of Justice and the Police Kjetil Nilsen, Director General, Norwegian National Security Authority (NSM)		
10:00-10:30	**Keynote speech** **Common Criteria: A Community Focus on Improving Software Assurance** Steven B. Lipner, Senior Dir. of Security Engineering Strategy, Microsoft Corp.		
10:30-11:00	**Keynote speech** **Accelerating Achievable Assurance** Mary Ann Davidson, Chief Security Officer, Oracle Corporation		
11:00-11:30	Coffee Break		
11:30-12:30	**Panel Discussion** **The future direction of CC, and the role of industry in its development, the role of testing tools in process based assurance, and other related assurance initiatives.** **Moderator** David Martin, Scheme Director, CESG, UK **Panelists:** Steven B. Lipner, Microsoft Corporation, US Mary Ann Davidson, Oracle Corporation, US		
12:30-13:00	**Update from the CC Management Committee** Dag Ströman, Acting MC Chair		
13:00-14:30	Lunch		
14:30-15:00	**Other Topics** **Development of a Protection Profile for Biometric Systems Following ISO/IEC TR 15446** Fernandez S. Belen, Univ. Carlos III of Madrid	**E-ID** **The e-ID Card Project in Germany** Bernd Kowalski, Federal Office of Information Security	**The Next Generation of CC** **CCDB Report and overview of CC v.4 work areas** David Martin, CESG, UK
15:00-15:30	**Experiences gained from the first Site Certification Projects** Christian Krause, BSI Mr. Thomas Schröder, T-Systems GEI GmbH	**Strong Authentication based on German ID Card** Klaus Lüttich, Bremen Online Sevices	**Detailed Report** **Meaningful Reports Working Group – Status update** Bob Morey, Program Manager for the Canadian CC Scheme, Comm.Security Establishment
15:30-16:00	**Dedicated EAL: The payment terminal experience** Carolina Lavatelli, Trusted Labs	**Smart Card** **Stepping into CC v.3.1 – Supporting efficiently ADV_ARC in the smart card industry** Laurent Di Russo, NLNCSA	**Predictive Assurance** **Update on Lead Nation Project** Irmela Ruhrmann, BSI
16:00-16:30	Coffee Break		
16:30-17:00	**Fine tuning a CC evaluation in concurrence with a FIPS 140-3 validation**	**Site Certification – 1st trial: Good news and Guidelines**	**Tools Support** **Tools to verify Match-on Card**

	Javier J. Tallon, Epoche & Espri	Hans Gerd Albertsen, NXP Semiconductors Germany	**Fingerprint Verification implementation** David Cerezo, CCN
17:00-17:30	**New Crypto-Kid on the block** Sunil Trivedi, The MITRE Corp	Monitoring CC for Smart Security Devices Françoise Forge, ISCI	**Skills and Interaction** **CCDB Work Group** – Skills and Interaction David Martin, CESG UK
17:30-18:00	**Low Cost Certification Roadmap** Miguel Bañón, Epoche & Espri	**Composite evaluation of (U)SIM Applications** Carolina Lavatelli, Trusted Labs	**Vulnerability Analysis: Simplicity is the ultimate sophistication** Wouter Slegers, Your Creative Solutions
20:00-21:30	10th anniversary celebration		

23 September 2009

Time	Track1 (Nord-Norge)	Track2 (Rica Hall II)	Track3 (Rica Hall I)
09:00-09:30	**Scheme Update** Update on UK Scheme David Martin, CESG, UK Update on Japanese Scheme Hidehiro YAJIMA, IPA	**Tools, Techniques and Experience** **Formal security policy model for a system with dynamic information flow** Jens H.Rypestøl, Applica Consulting	**The Next Generation of CC** **Challenges and Solutions of Distributed Systems Composition** Tsun-Te Tsui, Telecom Technology Center
09:30-10:00	Update on Italian Scheme Massimiliano Orazi, FUB Update on US Scheme Carol Houck, NIAP, US	**Evaluation Methodology for Random Number Generator - Update of German Scheme Doc.** Wolfgang Killmann, T-Systems GEI	**Unofficial Part 4 of the CC** Lisa Vincent, SAIC Acc. Testing & Eval. Lab.
10:00-10:30	Update on US Scheme Carol Houck, NIAP, US	**Effective evaluations outside the EAL frameowrk: Vertical Assurance Packages & -Profiles** Jose E. Rico, Epoche & Espri	**An Attack Surface based Approach to Evaluation** Helmut Kurth, atsec info.sec.corp.
10:30-11:00	Coffee Break		
11:00-11:30	**CC in the 21st Century** **Appropriate Assurance: Fitting like a Glove, Not a Tent** Tony Boswell, SiVenture	**Design and Development of a Knowledge-based Tool to support ST Developers on acquisition of Cryptographic Requirements** Gillermo H.R.Caceres, Grad School of Engineering, Soka University	**How the CC intersects and compares with other security evaluation programs and what it means for the rest of us** Lachlan Turner, DOMUS IT Security Laboratory
11:30-12:00	**CC vs. ISO/IEC 27001:2005:How to use an ISO/IEC 27001:2005 Certified Information Security Management System (ISMS) in a CC Evaluation.**	**EAL6 Evaluation – Challenges in Consistency Verification between Security Policy Model and other ADV classes documents** Sun-Mi Kim, Korea Info Sec	**Enterprise Security Management Protection Profiles:An Implementation Plan** Brickman Joshua, CA Inc. and

	Jean-Yves Bernard, Thales ITSEF	Agency	Eric Winterton, Booz | Allen
12:00-12:30	**OSPP: A Flexible Approach to Operating Systems Security** Miriam Serowy, BSI	**Developer Tools and Techniques, Part I: ALC_TAT reformulation** Miguel Bañòn, Epoche & Espri	**Lessons learned while Evaluating Windows Vista and Server 2008 using the CC and alternative approaches** Michael Grimm, Microsoft Corp.
12:30-13:00	**The public domain and the CEM Attack Potential mismatch** Jose F. Ruiz, Epoche & Espri	**Developer Tools and Techniques, Part II. Application to SW: CAPEC** Robert Martin , MITRE Corporation	**Common Criteria Development Lessons from the ISMS World** Mike Nash, Gamma Secure Systems.Limited
13:00-14:30	Lunch		
14:30-15:00	**CC in the 21st Century** **Walking by the Physical borderline: Vulnerability Analysis of Hardware TOE's with Security Boxes** Marino Tapiador, CCN	**Tools, Techniques and Experience** **Optimizing ADV/AGD evidence for CC 3.1** Peter van Swieten, Brightsight BV	**The Next Generation of CC** **Making a Better PP** James Arnold, SAIC
15:00-15:30	**Public verifiability challenges CC paradigm in the context of e-voting and beyond** Roland Vogt, DFKI	**Policies vs. Threats: clarifying the Security Target** Albert Dorofeev, Sony SCE	**Incorporating user-oriented Security into CC** Robin Sharp, Technical University of Denmark
15:30-16:00	**Physical protection : Anti-tamper mechanisms in CC security evaluations** Chamorro Alvaro, Epoche & Espri	**Taking White Hats to the Laundry: How to Strengthen Testing in CC** Apostol Vasilev, atsec info. sec. corp.	**Vulnerability Analysis Taxonomy: Achieving completeness in a systematic way** Javier Jesús Tallon, Epoche & Espri, S.L
16:00-16:30	Coffee Break		
16:30-17:00	**CC Schemes Around the World: Some Lab Perspectives** Eve Pierre, SAIC	**Why source code when having binaries? Applying reverse engineering in Common Criteria evaluations below EAL4.** Trifon Giménez, Epoche & Espri, S.L	**Protection of Critical Infrastructure** **Trusting Virtual Trust** Jeremy Powell, atsec info.sec.corp.
17:00-17:30	**CC and EU** **CC within the context of the EU Privacy Seal (EuroPriSe)** Wolfgang Peter, TÜViT	**Taming the Complexity of the CC** Wouter Slegers, Your Creative Solutions	Evidence based Evaluations **Chances and Challenges** Helmut Kurth, atsec info.sec.corp
19:30-22:30	Gala Dinner Certificate Award Ceremony		

24 September 2009

Time	Track1 (Nord-Norge)	Track2 (Rica Hall II)	Track3 (Rica Hall I)
09:00-09:30	**CC and EU**	**Vendors and CC**	**Evidence based Evaluations**

	Building successful communities to interpret and apply CC Tony Boswell, SiVenture	**Sony FeliCa: Smartcard CC Evaluation Experience with Five Schemes** Hiroaki Hamada, Sony Corp.	**Semantic Techniques for the CC** Erin Connor, EWA Canada
09:30-10:00	**E-Health and Trustworthy IT** **The use of CC within the German health system** Markus Mackenbrock, BSI Germany	**Secure Software Development for Higher CC Evaluation Assurance Levels** Shanai Ardi, Dept. of Computer and Info.science, Linkøping Univ.	**Evaluation and Certification results and vulnerability analysis in USB Storage Drive Management System** Hyeon Mee Pak, KISA
10:00-10:30	**An innovative Composition Approach by the German Health Care market** Hans-Werner Blissenbach, TÜVIT and Mr. Marcel Weinand of BSI	**How much!! The cost impact of different approaches to generating deliverables** Adam O'Brien, Oracle Corp.	**A Comparison of Security Standards** Marcus Streets, Thales nCipher
10:30-11:15	Coffee Break		
11:15-12:15	**Closing Panel (Rica Hall):** **Summary of Events at the ICCC** **Summary of Events.** David Martin, Scheme Director. CESG, UK **Speech.** Kjell W. Bergan, Scheme Director, Norwegian National Security Authority (NSM) / SERTIT		
12:15-12:45	**Closing Plenary** MC Chair		
12:45-13:00	**Announcement of the 11th ICCC**		
13:15-14:45	Lunch		

肆、 研討會過程摘述

一、CC 標準部分

ICCC 2009 宣布意大利正式通過了 CCMB 考核和審查成爲最新的 CAP。全世界共有約 50 個評估實驗室，共計數百名評估師。全世界一共頒發約 1100 張 CC 證書，約 150 張 PP 證書。

CC 4.0 標準的制訂工作正在進行，共成立 Meaningful reports(由加拿大主導)、Evidence based approaches (由美國及瑞典主導)、Tools(由英國及西班牙主導)、Predictive assurance(由德國主導)、Skills and Interaction(由英國及美國主導)等 5 個專門的工作小組（Working group），並設有定期的會議和 Wiki 社區討論。在本次會議，英國的 David Martin 代表 CCDB(Common Criteria Development Board)報告總體工作和 CC 4.0 概要狀況，並就 Skills and Interaction 工作小組近期工作情況做專題講演；加拿大的 Bob Morey 代表 CCDB 報告 Meaningful Report 工作小組的近期工作情況。

二、PP 部分

PP 的開發、評估和認證被廣泛推薦和認可，來自各方的專家於專題講演介紹諸多不同產品領域中 PP 的開發、評估現狀。目前已經完成該 PP 草稿，並將提交審核和討論，計劃於 2009 年年底開始正式評估，2010 年第一季度正式發布該 PP。

從產品類型層面，很多專家在講演或討論時，皆表贊同且鼓勵針對不同產品形成產品社區論壇，加強縱向的討論和研究，特別要吸引真正的產品使用者加入討論，實現資訊安全爲使用者提供安全保證的目的。ICCC 2009 的產品主題演講，主要在智能卡、支付終端、生物技術、操作系統等領域，此外隨著 CC 廣泛發展，也衍生出了特殊領域的應用，例如德國電子身份識別、歐盟隱私保護、電子投票選舉等產品和應用領域。

三、與日本代表交流情形

利用研討會空閒時間與日本經濟產業省商業情報政策局參事官 Mr. Yasuhide Yamada (山田安秀)及驗證主管機關(IPA, Information-technology Promotion Agency, JAPAN)代表 Mr. Hidehiro Yajima、Mr. Junichi Kondo、Mr. KAI Naruki 等交流。渠等相當支持我國的申請案，雖然加入成爲 CCRA 的結論尚未定案，因爲 CC 檢測只是單純的技術議題。並建議我國應持續與各國的主管機關保持互動關係，如馬來西亞、新加坡等，以爭取對我國的支持。日本代表同時提出建議，現在情勢有利我國爭取，應繼續努力。

四、其他部分

CCRA 管理委員會(Management Committee)主席 Mats Ohlin 教授(瑞典人)於 2009 年 8 月 28 日離世，爲整個會議增添感傷的氣氛。

ICCC 2009 開始的兩個重要講演(Keynotes)分別來自於微軟(Micro Software)和甲骨文(Oracle)兩個知名產品廠商。他們作爲廠商的代表，同時以用戶者的角度，分析 CC 目前存在的不足和值得考慮的發展方向。

第二天進行的歡慶晚宴(Gala Dinner)，按照慣例頒發了各個認證機構年度內完成的認證證書。同時 IBM、微軟、甲骨文三個廠商的產品也分別獲得認證證書。共頒發了 54 個證書。

宣稱將有驚喜和秘密的 ICCC 2009 十週年慶典(The 10th anniversary)，由挪威的 SERTIT 組織安排，在 Arctic Cathedral 教堂舉辦，由特羅姆斯(Troms)的藝術學校學員演出，其表演方式在觀賞者四周出現，體驗一次不一樣的藝術饗宴。

伍、 感想及建議

一、ICCC 可獲得 CC 進展及經驗

ICCC 是整個 CC 驗證/認證體系中最重要的會議，各國驗證主管機關、驗證實驗室、安全產品業者、安全政策制定者、IT 專家、程式開發者等均會與會，參與會議可瞭解 CC 最新的發展現況、各國推動 CC 驗證情況，以及 CC 實驗室的運作情形。

二、積極加入 CCRA

早期 CC 可說是歐美各國的天下，近幾年亞洲各國(包含日本、新加坡、馬來西亞、巴基斯坦、印度與韓國)也紛紛加入 CCRA，成爲 CAP 或 CCP 的會員國。本會目前亦正積極籌畫加入 CCRA 之相關事宜，並已由財團法人電信技術中心(TTC)成立國內首座資訊安全產品檢測實驗室，可提供國內資安廠商 CC 驗證服務，及資安產品檢測的顧問服務與教育訓練。

我國在今年的行政院 2009 年產業科技策略會議中，也提出建立資通訊基礎建設安全信賴機制議題，針對資通訊產品認證問題提出討論，經由該會議，已蒐集各界意見，由本會擬具 4 年計畫，由 NICI 陳報行政院核定中。該計畫將先進行認證體系在我國可行方式研究，後續再推動資通訊產品認證及政府機關優先採購經認證資通訊產品，逐步建立我國資通訊產品認證體系，確保我國資通訊產品安全。

三、CC 的課題

CC 內容複雜與曠日費時的送驗作業是造成無法順利且迅速普及的最大原因。有鑑於此，CCRA 除將推廣宣導列爲工作重點，希望與其他資訊安全相關國際標準互相支援合作，擴大應用範圍，讓更多人了解與使用 CC。另一方面，爲了簡化安全評估作業，建立一致且明確的安全定義及規範，近年來積極進行 CC 標準的修訂改版，但是 CC 內容變動頻繁，亦引起開發廠商的普遍不耐，多位業者在本次會議中表達不滿之意，認爲此舉將會阻礙廠商產品送驗的意願。

至於 CC 是否真正符合與滿足使用者與廠商的期望與需求，近年的爭議不斷，本次會議則正式浮上檯面。資訊大廠質疑 CC 標準過於封閉及僵化，無法契合使用者需求，且驗證過程冗長，不符合經濟效益。有人認爲產品通

過驗證並非萬靈丹，只能強化對其安全功能的信心，風險管理才是規劃資訊系統架構的正途。有人則建議 CC 應多聆聽、採納使用者與廠商的心聲與意見，及時做適當的修正與調整，才能避免成爲曲高和寡的象牙塔產物。

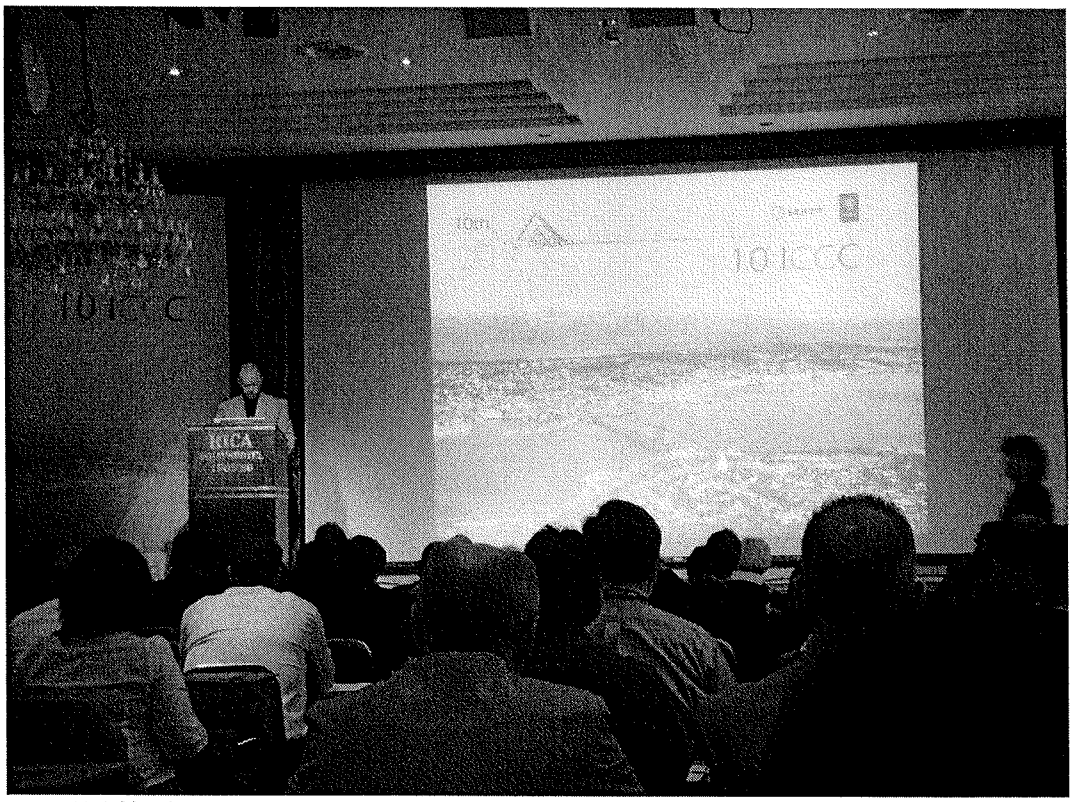
總之，如何同時維繫 CC 標準的穩定度與時效性，勢必是 CC 標準制定組織所必須審慎權衡取捨的重要課題。

四、持續參加下屆研討會，並爭取介紹我國驗證體系現況的機會

持續參加下屆研討會，並爭取投稿機會，於會議中介紹我國驗證體系及推動共同準則情形，以增加國際間了解我國在此領域所投入的努力及具體成果的機會。就目前國際現況，我國欲順利申請成爲 CCRA 會員國目標，尚須爭取各會員國的支持，爭取在 ICCC 國際研討會中介紹我國驗證體系機會，使各國了解我國推動國際共同準則情形，應是本會參加 ICCC 研討會的首要目標。

陸、 附件

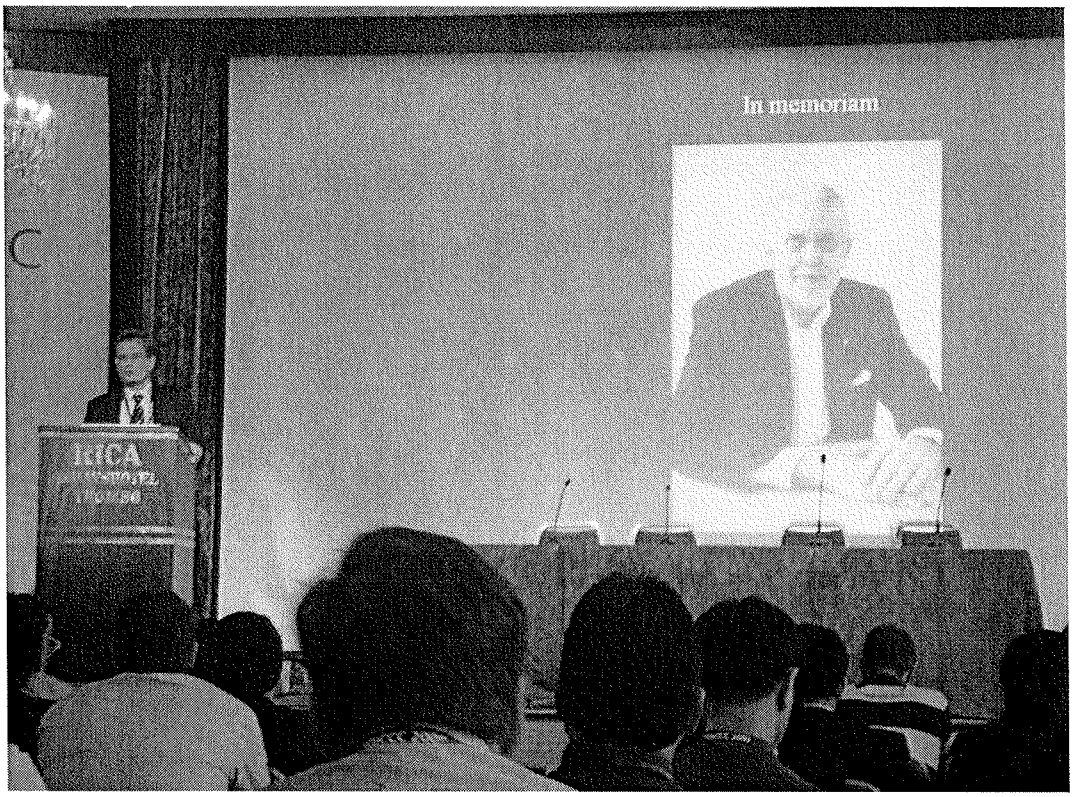
研討會會場



開幕式

論壇

開幕表演



CCRA Management Committee (MC) report 2009

TTC 發表論文