

出國報告 (出國類別：會議)

參加 2010 年第 11 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：魏學文 委員

派赴國家：土耳其

出國期間：99 年 9 月 19 日至 9 月 25 日

報告日期：99 年 12 月 17 日

## 摘要

第 11 屆國際共同準則研討會議 (ICCC, International Common Criteria Conference) 自 99 年 9 月 21 至 23 日於土耳其的安托利亞 (Antalya) 舉行，本屆會議由土耳其標準局主辦。共有來自 26 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，本會議共分三個 tracks，三天共 24 個 sessions；內容包含了 CC 發展、各國 CC 架構、CC 和其它標準之比較、新 PP 之探討等各種主題。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，俾作為修訂相關技術規範參考，並擴展個人對於 CC 的深入了解與資安視野。參加此會議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，可作為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。

此外，本次會議除了和日本、馬來西亞等國進行意見交流外，亦順利和 CCRA 的 MC 主席會面，並持續爭取我國加入 CCRA 會員之機會。

## 目 錄

壹、 目的 .....	1
貳、 研討會簡介 .....	3
參、 研討會時間、地點及議程 .....	4
肆、 研討會過程摘述 .....	7
伍、 感想及建議 .....	9
陸、 附件 .....	10

## 圖目錄

圖 1.1 CCRA 會員國統計 .....	1
圖 6.1 ICCC2010 註冊現場 .....	10
圖 6.2 ICCC2010 大會會場 .....	10

## 表目錄

表 2.1 會議議題 .....	3
------------------	---

## 壹、 目的

共同準則(Common Criteria, 亦稱 ISO/IEC 15408, 簡稱 CC)為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, 預計可於近期中發布。CC 的目標為確保評價的 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)的目的為促進 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。



圖 1.1 CCRA 會員國統計

CCRA 目前共有 26 個會員國, 已申請成為「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

其等 12 個國家；已申請成為「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 ICC) 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, 俾作為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, 可作為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。

## 貳、 研討會簡介

2010 年第十一屆國際共同準則會議(簡稱 ICCC 2010)係由土耳其驗證機構 TSI 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，主要議題包含經驗分享、CC 發展趨勢、PP 與 CC 共具之新規範探討等議題，共有 24 場技術會議。主要議題如下：

表 2.1 會議議題

A1	Reports from CC Communities	
A2	Experiences	
A3	Experiences	
A4	Experiences	
A5	Experiences	
A6	Experiences	
A7	CC Developments	CC & Tools
A8	CC Developments	
B1	CC & new techniques	
B2	CC Developments	Biometrics
B3	Scheme Update	
B4	Scheme Update	
B5	Smart card and hardware security	
B6	Smart card and hardware security	
B7	CC & new techniques	CC and other standards
B8	CC and other standards	
C1	Cryptography	
C2	CC & Tools	
C3	Protection Profiles	
C4	Protection Profiles	
C5	Protection Profiles	
C6	CC and other standards	
C7	Reports from CC Communities	
C8	CC & Tools	

## 參、研討會時間、地點及議程

本屆研討會於土耳其(Turkey)安托利亞(Antalya)市舉行，自 99 年 9 月 21 日至 9 月 23 日共計 3 天，大會詳細議程說明如下：



September 21, 2010, Tuesday

Time			
09:00-09:30	<b>11. ICC Conference</b> <b>Opening Ceremony</b>  <b>Tahir Büyükhelvacigil</b> President of Turkish Standards Institution  <b>Mr. Dag Ströman</b> Chair of CCRA Management Committee  <b>Nihat ERGÜN</b> Minister of Industry and Trade		
09:30-11:00	<b>11. ICC Conference</b> <b>Opening Plenary Session</b>  <b>Prof. Dr. Nüket Yetis, TÜBİTAK President</b> Chairperson of the Session  <b>Keynote Speakers</b>  <i>Common Criteria: Meeting: the Needs of a Global Market?</i> <b>Steven B. Lipner</b> Senior Director of Security Engineering Strategy, Trustworthy Computing Security, Microsoft Corporation  <i>Common Criteria – An Industry Perspective: Relevance, Reform and a Call to Action</i> <b>Gene Keeling</b> Director, Global Certification Team Global Government Solutions Group Cisco		
11:00-11:30	Coffee Break		
Time			
11:30-12:00	<b>Update from the CC Management Committee</b> Dag Ströman, Acting MC Chair		
Time Panel Session			
12:00-13:00	<b>Meeting the user needs - the power of protection profiles and technical communities</b>  This panel session will include members of established technical communities and those setting up a new technical community. The panel will debate a range of questions regarding the use of Protection Profiles and Supporting Documents to express end user requirements, the value of end user participation in the development of these, how greater involvement can be encouraged, general lessons learned, etc. The chair of the panel welcomes suggestions for additional questions.		
13:00-14:30	Lunch		
Time	A1- Reports from CC Communities	B1- CC & new techniques	C1- Cryptography
14:30-16:00	ID:151-JTEMS - a community for the evaluation of payment terminals <i>Sandro Amedola, Federal Office for Information Security (BSI), Germany</i>  ID:70-GESTE: a Consortium fully supporting the CC adoption by payment terminals industry <i>Nathalie FEYT, THALES CEACI ITSEF, France</i>  ID:48-Monitoring Common Criteria for Smart Cards and related Devices <i>Alain BOUDOU, ISCI WG1, France</i>	ID:91-A practical approach to using CC Part 2 <i>Dirk-Jan Out, Brightsight, Netherlands</i>  ID: 101-The GP Composition Model - Maximizing the Efficiency of Security Certifications <i>Sarra MESTIRI, Oberthur Technology, France</i>  ID: 111-Lessons Learned From a Composed TOE Evaluation <i>Eric Winterton, Booz Allen Hamilton, USA</i>	ID:158-Evaluation of cryptographic Implementation in the German Scheme <i>Berndt Kowalski, German Federal Office for Information Security (BSI), GERMANY</i>  ID:112-Crypto-Tech: End User Nightmares <i>Ahmad Dahari Jarno, CyberSecurity, Malaysia</i>  ID: 119- Assembling the Crypto Pieces In The Common Criteria Jigsaw Puzzle <i>Marino Tapiator, Spanish Certification Body (CCN), Spain</i>
16:00-16:30	Coffee Break		

Time	A2- Experiences	B2- CC Developments	C2- CC & Tools
16:30-18:00	<p><b>ID 3-CC promotion activity to new area -Japanese experience-</b> <i>Hidehiro Yajima, IPA, Japan</i></p> <p><b>ID:46-How do you ensure evaluators are competent?</b> <i>Zarina Musa, CyberSecurity, Malaysia</i></p> <p><b>ID:159-The New NIAP Protection Profile</b> <i>Shaun Gilmore, NIAP, USA</i></p> <p><b>ID: 31- Plan for Common Criteria requirements during the Secure Software</b> <i>Reeny Sondhi, EMC, USA</i></p>	<p><b>ID:25-CC evaluations driven by the Vulnerability Analysis</b> <i>Jose Emilio Rico, EPOCHE &amp; ESPRI S.L., Spain</i></p> <p><b>ID:88-Return of the evaluation Investment. An economic analysis of different EALs and evaluation scenarios.</b> <i>Miguel Bañón, EPOCHE &amp; ESPRI S.L.,Spain</i></p> <p><b>B2- Biometrics</b></p> <p><b>ID:36-Security Evaluation of Biometric Systems In Common Criteria</b> <i>Belen Fernandez-Saavedra, TestingLab, University Carlos III of Madrid, Spain</i></p> <p><b>ID: 157 Biometric Spoof Detection In context of Common Criteria</b> <i>Frank Grefrath, Federal Office for Information Security (BSI), Germany</i></p>	<p><b>ID: 65- TL SET: A tool for supporting PP and ST Edition</b> <i>Roland ATOUI, Trusted Labs, France</i></p> <p><b>ID: 86- Security Tools for CC Testing</b> <i>Quang Trinh, SAIC Accredited Testing &amp; Evaluation Laboratories, USA</i></p> <p><b>ID: 104-Use of Semantic Techniques for CC Evaluation</b> <i>Mark Gauvreau, EWA-Canada, Canada</i></p> <p><b>ID: 15- Using tools to generate design evidence for CC evaluations</b> <i>Peter Swieten, Brightsight, Netherlands</i></p>
19:30	Welcome Cocktail		

## September 22, 2010, Wednesday

Time	A3- Experiences	B3- Scheme Update	C3- Protection Profiles
09:00-10:30	<p><b>ID: 135-MYSEA: An Approach to Building High Assurance Composite System for Cloud Computing</b> <i>Thuy D. Nguyen, Science, Naval Postgraduate School Monterey, USA</i></p> <p><b>ID: 143-The Certification of the Parts Is not The Certification of the Whole. SDR Challenge</b> <i>David Cerezo, Spanish Certification Body (CCN), Spain</i></p> <p><b>ID: 69- Learning from CC Certified Products</b> <i>Tsun-Te Tsui, Telecom Technology Center, Taiwan</i></p>	<p><b>ID: 27- KOREA Domestic IT Security Evaluation Scheme – Devise a Fast Evaluation Scheme</b> <i>HyeonMee Pak, Korea Internet &amp; Security Agency, Korea</i></p> <p><b>ID: 90- New trend of Common Criteria Certification In Japan</b> <i>Matsutosh Murata, Information Technology Promotion Agency (IPA), Japan</i></p> <p><b>ID:160- Fostering More Confidence In Commercial Technologies</b> <i>Chris Salter, NSA, USA</i></p>	<p><b>ID: 17- Enterprise Security Management Protection Profiles, A Global Threat Survey</b> <i>Joshua Brickman, CA Technologies, USA</i></p> <p><b>ID: 28- Improving the Flexibility and Applicability of Protection Profiles</b> <i>Helmut Kurth, Atsec Information Security Corp., Germany</i></p> <p><b>ID: 35- Protection Profile for Digital watermark system</b> <i>HyunJung Lee, Dongho Won, Seungjoo Kim,SungkyunKwan University, Korea</i></p>
10:30-11:00	Coffee Break		

Time	A4- Experiences	B4- Scheme Update	C4- Protection Profiles
11:00-12:30	<p><b>ID: 56-About the necessity of formulating more accurately what semiformal language means</b> <i>Franck ELLERO, THALES CEACI ITSEF, France</i></p> <p><b>ID:58-Realistic User Expectations of Assurance Levels</b> <i>Tony Boswell, SiVenture, UK</i></p> <p><b>ID:64-Using the Common Criteria In Practice</b> <i>Michael Nash, Gamma Secure Systems Ltd, UK</i></p>	<p><b>ID: 95 -UK Scheme Update</b> <i>David Martin, CESG, UK</i></p> <p><b>ID: 156-German CCRA Certification Scheme.</b> <i>Gereon Killian, Federal Office for Information Security (BSI), Germany</i></p> <p><b>ID: 72- US Policy Update</b> <i>Carol Houck, NIAP, USA</i></p>	<p><b>ID: 152-Operating System Protection Profile Modularity and Flexibility using the Common Criteria</b> <i>Intemann Matthias, Federal Office for Information Security (BSI), Germany</i></p> <p><b>ID: 51- Protection Profile for Operating System</b> <i>William Penny, IBM, USA</i></p> <p><b>ID: 83- The Protection Profile Paradox</b> <i>Patti Spicer, CSC, USA</i></p>

12:30-14:00 Lunch

Time	A5- Experiences	B5-Smart card and hardware security	C5- Protection Profiles
14:00-15:30	<p><b>ID: 117-Security Target In the crossfire of precision and readability</b> <i>Franck ELLERO, THALES CEACI ITSEF, France</i></p> <p><b>ID: 105-ATE activity In limited evaluation workload.</b> <i>Nicolas Lokiec, THALES, France</i></p> <p><b>ID: 146-The evaluation over a composite TOE with conformity with Java Card Protection Profile version 1.0 and Global Platform specification.</b> <i>Guillem Ernest Malagarriga Vilella,</i></p>	<p><b>ID: 2- Contact-less DPA smart cards must be considered under vulnerability assessment (AVA_VAN)</b> <i>Monique Bakker, Brightsight, Netherlands</i></p> <p><b>ID: 18- How helpful can be the security assessment of TOE associated tools during a Common Criteria evaluation.</b> <i>Emilie Faugeron, Thales CEACI ITSEF, France</i></p> <p><b>ID: 59- Current smartcard security activities In Japan</b> <i>Yasuyoshi Uemura, Electronic Commerce Security T.R.A., Japan</i></p>	<p><b>ID: 108- The application of ISO/IEC TR 15446:2004 In the process of compliation of Chinese national standard "GB/T 20279-2006"</b> <i>Zhen Lu, The Third Research Institute of Ministry of Public Security, P. R. China</i></p> <p><b>ID: 153-Vehicle Unit and Tachograph Cards PP</b> <i>Osman Kocar, Federal Office for Information Security (BSI), Germany</i></p> <p><b>ID: 155-Protection Profiles for Secure Signature-Creation Devices as European Standards</b> <i>Susanne Pingel, Federal Office for Information Security (BSI), Germany</i></p>

15:30-16:00 Coffee Break



Time	A6- Experiences	B6- Smart card and hardware security	C6- CC and other standards
16:00-18:00	<p><b>ID: 20- CC approaches to the certification of the components of a system when the system certification is not possible</b> Vittorio Bagini, Fondazione Ugo Bordoni and OCSI, Italy</p> <p><b>ID: 125-Expertise-based certification alternative</b> Thomas Bousson, Sogeti, France</p> <p><b>ID: 53- A Method for Determining Evaluation Assurance Levels for TOEs</b> Erkut Beydagli, TUBITAK UEKAE OKTEM, Turkey</p> <p><b>ID: 84- Evaluated Configuration In Practice</b> Shaun Lee, Oracle, USA</p>	<p><b>ID: 94- An Alternative Approach for Attack Potential Calculations of Smartcards</b> Betül Soysal, TUBITAK/UEKAE, Turkey</p> <p><b>ID: 78- How we keep on improving smart card security development, following CC requirements</b> Naohisa Ichihara, NTTDATA Corporation, Japan</p> <p><b>ID: 107- Guidance for Side-Channel-Analysis of Elliptic Curve Cryptography Implementation</b> Wolfgang Killman, T-systems, Germany</p> <p><b>ID: 54- Unravel smartcard composition requirements</b> Monique Bakker, Brightsight, Netherlands</p>	<p><b>ID: 41- FIPS 140 &amp; CC – How do they get along?</b> Erin Connor, EWA-Canada, Canada</p> <p><b>ID: 14- A Threat Modelling for Security Specification of Security Evaluation by CC and ISO/IEC TR 19791</b> Guillermo Ramirez Horacio Caceres, Faculty of Engineering, Soka University, Japan</p> <p><b>ID:30- Common Criteria's place in the security market</b> Wouter Slegers, Your Creative Solutions, Netherlands</p> <p><b>ID:97-FIPS and the Common Criteria: finding the least common denominator</b> Eugene Polulyakh, Aspect Labs Common Criteria Lab, US</p>
20:00	Gala Dinner		

## September 23, 2010, Thursday

Time	A7- CC Developments	B7- CC & new techniques	C7- Reports from CC Communities
09:00-10:30	<p><b>ID: 99-Improving EAL4+ evaluation efficiency: How to use the JIL-document "Collection of developer evidence"</b> Sophie Laborde, THALES CEACI ITSEF, France</p> <p><b>ID: 154-Lead Nation Project "Predictive Assurance"</b> Irmela Ruhmann, Federal Office for Information Security (BSI), Germany</p> <p><b>A7- CC &amp; Tools</b></p> <p><b>ID:113- Patterns-based development of IT security evaluation evidences</b> Bialas Andrzej, Institute of Innovative Tech., EMAG, Katowice, Poland</p>	<p><b>ID:89- Cloud and the Common Criteria</b> Sunil Trivedi, The MITRE Corporation, USA</p> <p><b>ID:60 -Recent Developments of Turkish eID Project</b> Oktay ADALIER, TUBITAK UEKAE, Turkey</p> <p><b>B7- CC and other standards</b></p> <p><b>ID:110-Establishing a Continuous Secure Development Environment</b> Mehmet Çakir, Miron Software, Turkey</p>	<p><b>ID:98-Streamlining Medium Assurance</b> Rob Huissmann, NLNCSA, Ministry of the Interior and Kingdom Relations, Netherlands</p> <p><b>ID:136- Enterprise Firewall Protection Profile Development Plan and Status Update</b> Tom Price (Cisco Systems, Inc.,USA) and Jane Medefesser (Juniper, USA)</p> <p><b>ID:76-Evaluating a watermelon: mitigating the threats through the operational environment</b> Jose Francisco Ruiz Gualda, EPOCHE &amp; ESPRI S.L., Spain</p>
10:30-11:00	Coffee Break		

Time	A8- CC Developments	B8- CC and other standards	C8- CC & Tools
11:00-13:00	<p><b>ID: 19- Building CC Technical Communities - A Progress Report</b> David Martin, CESG, UK</p> <p><b>ID: 148-A comparison of Common Criteria to matured ISO standards to create a more harmonized comprehensive structure covering any type of modularity, size, complexity and security of IT products</b> Ömer Anil Ardic, TSE, Turkey</p> <p><b>ID: 87- Why Isn't there reuse of certification results?</b> Scott Shorter, Cisco Systems, USA</p> <p><b>ID: 132-Becoming a CNAS Laboratory</b> Yi Mao, Atsec Information Security Corporation, USA</p>	<p><b>ID: 38- Cloud Computing: Anticipate Immediate Evaluation Needs and Extend International Mutual Recognition</b> Michael Grimm, Microsoft Corp, USA</p> <p><b>ID: 61- Common Criteria &amp; ECSS: Best Integration of a Common Criteria evaluation in a space product development process compliant with the ECSS (European Cooperation for Space Standardization) system</b> Thomas BEN, Thales CEACI ITSEF, France</p> <p><b>ID: 77- Side Channel Attacks: CC, FIPS PUB 140-2, EMV and PCI points of view</b> Ortega Chamorro Alvaro, EPOCHE &amp; ESPRI S.L., Spain</p> <p><b>ID: 26- Protection Profiles as a Governmental Tool</b> Anders Staaf, Combitech AB, Sweden</p>	<p><b>ID: 12- Model Driven Security Accreditation of Agile Systems</b> Rudolf Schreiner, Object Security Ltd., UK</p> <p><b>ID: 67- Overflowing attack potential: scoring defence-in-depth</b> Javier Tallón Guerri, EPOCHE &amp; ESPRI S.L., Spain</p> <p><b>ID: 7- Supporting CC evaluations using XML</b> Nils Tekampe, TÜVIT GmbH, Germany</p> <p><b>ID:100-Duality of the virtualization technology and its impact in CC evaluations</b> Trifón Giménez Vázquez, Epoche &amp; Espri, Spain</p>
13:00-14:00	Lunch		

Time	Closing Panel
14:30-16:00	<p><b>ID: 81- Common Criteria Development - CCDB Report</b> David Martin, CESG, UK Summary of Events at 11. ICCS David Martin, Scheme Director</p> <p>Closing Speech by Turkish Delegate</p> <p>Closing Plenary MC Chair</p>
16:00-16:15	Announcement of the 12th ICCS
16:00-16:30	Coffee Break

## 肆、 研討會過程摘述

### 一、 CC 標準部分

CC 4.0 標準的制訂工作正在進行中，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)亦循例作總體工作報告。

### 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 PP 之提出，主要仍集中在智能卡、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。電信核心網路之資安重要性日益重要，從產品之 PP 是否擴展至系統 PP 本研討會議亦開始有所討論。

### 三、 與日本、馬來西亞代表交流情形

我國通訊技術中心(TTC)長期以來也一直持續參與 ICCC 的會議並發表論文，此次在 TTC 同仁的協助下，也順利和日本及馬來西亞的驗證主管機關代表進行非正式會談與交換意見。日本與馬來西亞兩國待我們相當友善，對於我國持續加入 CCRA 會員的努力也十分了解，亦願意持續予以協助，日本代表甚更進一步建議我們爭取 MC 會議報告的機會。另外，我們和日本代表會談中亦針對電信核心網路之 PP 必要性拋出議題，希望能藉由亞洲國家之協力合作提出符合共通準則之電信核心設備(例如 core network、交換機、基地台等)之 protection profiles(PP)，目前初步亦獲得日本之認同，預定可於近期內開始交換意見，進行可行性之深入討論。

由於 CCRA 中的東南亞國家會員對我國相對友善，建議應利用此優勢，積極參與 AISEC 次級組織，及早建立我國在此圈內之參與地位，以免未來重複 CCRA 之相同困境。

#### 四、 與 CCRA 管理委員會主席交流情形

本次會議經由 Mr. Murray 之協助，順利和 CCRA 的主席 Mr. Dag Stroman 碰面，並有一個 30 分鐘之會議(9/23 11:00~11:30 @ SIDE room of Porto Bello Hotel)。參與 CCRA 之困難度極高，唯相對 Mr. Dag Stroman 對我們尚稱友好，並有部分國家對我們非常支持。是否持續推動，值得我們進行深入分析。

在此 30 分鐘討論中，我們首先針對我國在 ICT 領域之傑出表現作一簡要報告，並表達我國參與 CCRA 事務之必要性。CCRA MA 主席亦委婉表示我國家參加 CCRA 會牽涉到各國多方面的考量。另由於主席已有更換，故無法確定我國上次入會之申請是否持續處理。為了爭取時效，我們亦建議是否可以重提入會申請，唯主席提示如重提入會申請應具和上次入會申請有主客觀之條件產生變化。此外，我們亦爭取在 CCRA 的 MC 會議提出報告之機會，藉此爭取各國的支持，此部分主席同意會代為轉達我們的要求。

## 伍、 感想及建議

1. 共通準則關係到資通訊安全認證之全球性需求，並且此標準和 ISO、歐洲 FIPS 等標準亦有對齊，加入參與國家愈來愈多，主要工業國亦多已加入。因此，我國如能取得 CCIR 組織之會員，對於國內資通訊產業將有很大助益，雖然目前加入阻力仍大(需要所有會員國同意才可加入)，惟仍值得國內相關單位投入耕耘。
2. 綜觀國外各國負責制定推動資安認證單位(CB)大都相當於國內三級單位，例如日本是 Information Tech Promotion Agency(IPA)；韓國是 Korea Internet and Security Agency；美國是 National Security Agency；德國是 Federal Office for Information Security；土耳其是標準局等，相對於我國組織層級較高但缺少專責負責之技術單位。
3. 依 ICCC 會議 CB 部分之參與會議人員而言，大都為各國技術單位之高階事務人員，建議我國亦應多爭取由技術層級人員與會，爭取發聲的機會。
4. ICCC 之會議 track 數較少，通常只有 3 個 track，相當每個 track 參加人員皆有 100 人左右，且此會議之 presentation 時間也較長(約 30 分鐘)。相對之下是一個很好發聲的機會，建議未來參與此會議之人員(包含 CB 和 LAB)皆應以發表論文為主。
5. 經過前人多年努力，在此領域，我國在亞洲地區國家普遍皆已得到強力支持，例如日本、馬來西亞等。
6. NCC 參與國際事務之機會與日俱增，目前我們參與之國際活動都是 1 至 2 人，散彈打鳥之方式，甚難突破與發揮成效。建議：
  - (1)參與國際事務之經費應全面檢討。
  - (2)應檢討本會目前參與國際組織之規劃，集中火力於較易突破的地方。
7. 電信核心網路為國家重要的基礎設施(infrastructure)，由於國內電信網路重要軟硬體設備大都由國外進入，其安全需要更加注意。

陸、 附件：研討會會場



圖 6.1 ICCC2010 註冊現場



圖 6.2 ICCC2010 大會會場