出國報告(出國類別：會議)

出席 2011 年第 12 屆國際共同準則（ICCC）研討會

服務機關：國家通訊傳播委員會
姓名職稱：陳簡任技正春木、韓鎮華科長
派赴國家：馬來西亞
出國期間：100 年 9 月 26 日至 9 月 30 日
報告日期：100 年 11 月 21 日

摘要

第 12 屆國際共同準則研討會議(ICCC, International Common Criteria Conference)自 100 年 9 月 27 至 29 日於馬來西亞的八打靈(Petaling Jaya)舉行，由 CyberSecurity Malaysia 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 200 人參加，本會議共分三個 tracks，三天共 67 個 sessions；內容包含了各國共同準則(Common Criteria，亦稱 ISO/IEC 15408，簡稱 CC)架構、CC 和其它標準之比較、新 PP 之探討等各種主題。

參加案關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，並擴展個人對於 CC 的深入了解與資安視野。且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，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。

本次會議除了和日本、馬來西亞等國進行意見交流外，亦和中國代表與德國 TÜViT 交換有關我國資安設備檢測現況與規劃之意見。

目次

壹、目的

本會刻正負責推動「資通設備之安全檢測研究計畫」，研擬適合我國的資通設備檢測要求，包括安全檢測技術規範、檢測技術標準、設備採購參考指引等配套措施，並規劃短中長期資通設備安全檢測與國際接軌的策略方向，以期滿足政府機關(構)對於資通設備採購及使用的安全需求，進而促進我國資通產業發展。

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。

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。

他山之石可以攻玉，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，俾作為訂定相

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，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，確有其必要性

貳、研討會紀要

CCRA 目前共有 26 個會員國，已申請成為「接受證書會員國」（Certificate Consuming Members，簡稱 CCM），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、新加坡等 11 個國家；已申請成為「核發證書會員國」（Certificate-Authorizing Members，簡稱 CAM），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、土耳其等 15 個國家。

CCM 指需接受 CAM 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。CAM 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、研討會議程

9 月 26 日　　自臺北中正機場啟程

9 月 27 日至 29 日　　參加研討會

9 月 30 日　　返抵國門

2011 年第 12 屆國際共同準則研討會議，在馬來西亞的八打靈 (Petaling Jaya；吉隆坡衛星城市)舉行，由 CyberSecurity Malaysia 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 Tracks 進行分組研討，議題如下，包含經驗分享、CC 發展趨勢、PP 與 CC 規範探討等，共計有 67 場次：

September 27, 2011, Tuesday		
TRACK A *(Citrine Ballroom)* CC Formalities	**TRACK B *(Jasmine Junior Ballroom)* Technical Use of CC**	**TRACK C *(Maple Junior Ballroom)* Management Views/ Application Aspects**
Planning for Assurance Maintenance and EWA-Canada Experience Mark Gauvreau, *EWA-Canada*	**Building CC Technical Communities - A Progress Report** David Martin, *CESG, UK*	**The criteria of development site security for CC evaluations** Naruki Kai, *Information-technology Promotion Agency (IPA), Japan*
Multi-Assurance ST: Different assurance levels within a Protection Profile/Security Target (how a PP/ST can better meet the real life) Dr. Igor Furgel, *T-Systems International , Germany*	**Common Criteria methodology for Smart Cards and Security Devices: An overview of the ISCI achievements** Alain Boudou, *Eurosmart- ISCI*	**New Directions for the Common Criteria: Implications of Supply Chain and Cloud Computing** Michael Grimm, *Microsoft Corp., US*
The TOE: What's in? What's out? What does it mean? James Arnold, *SAIC Accredited Testing & Evaluation Lab, US*	**Update from ISCI-WG1 of the JIL-document "Collection of developer evidence"** Sophie Laborde, *ISCI-WG1/ Thales Communications & Security, France*	**Assuring a Hardware TrustZone** Tony Boswell, *SiVenture, UK* Simon Moore, *ARM, UK*
An Update on the NIAP Evolution Carol Houck, *NIAP/CCEVS (National Information Assurance Partnership/US Common Criteria Evaluation & Validation Scheme)*	**The EU Project ASSERT4SOA (Advanced Security Service cERTificate for SOA): Objectives, approach, and status (after one year)** Massimiliano Orazi, *Fondazione Ugo Bordoni, Italy*	**Process Improvement for Common Criteria Evaluation in Malaysian context** Siti Fatimah Abidin, *CyberSecurity Malaysia*
Turkish Common Criteria Certification Scheme from 2003 to 2011 Mariye Umay Akkaya, *TSE Turkish Scheme*	**ICSS-JC activity update: two draft PPs for contactless e-money system** Yasuyoshi Uemura, *IC System Security Japan Consortium (ICSS-JC), Japan*	**Chinese general techniques requirements for important information systems** Dr Haohao Song, *The Third Research Institute of Ministry of Public Security, Shanghai, P. R. China*
UK Scheme Update David Martin, *CESG UK Scheme*		
Japanese Scheme Update - Enforcement utilizing certified products for procurement in Japanese Government Kenjiro Sasaoka, *Information-technology Promotion Agency (IPA), Japan*	**The New NIAP Protection Profile and Extended Module** Kenneth B. Elliott, *The Aerospace Corporation, US*	**Fighting the bean-counters** Gerald Krummeck, *atsec information security GmbH, Germany*

September 28, 2011, Wednesday		
TRACK A *(Citrine Ballroom)* CC Formalities	**TRACK B *(Jasmine Junior Ballroom)* Technical Use of CC**	**TRACK C *(Maple Junior Ballroom)* Management Views/ Application Aspects**
Reduced Reporting: Pilot Results Rob Huisman, *NLNCSA, Ministry of Interior and Kingdom Relations, Netherlands* Dirk-Jan Out, *Brightsight BV, Netherlands*	**Hardcopy Device Protection Profiles Community Update 2011** Brian Smithson, *Ricoh Americas Corporation, US*	**Integrating requirements into a Protection Profiles: Lessons learned from machine-readable travel documents (MRTD) PP consolidation** Dr. Jens Oberender, *SRC Security Research & Consulting GmbH, Germany*
Better Use of CC with Lower Assurance Levels Tony Boswell, *SiVenture, UK*	**Developing European Protection Profiles for Digital Signatures** Marcus Streets, *WG17 / ETSI / Thales e-Security*	**Secure Content Automation Protocol (SCAP): how it is increasingly used to automate enterprise security management activities** Sean Barnum, *The MITRE Corporation, US*
Product Assurance in the UK - Common Criteria, Commercial Product Assurance and CESG Claims Tested Mark - is there any convergence? Simon Milford, *SiVenture, UK*	**Enterprise Security Management Protection Profiles Community Update 2011** Eric Winterton, *Booz Allen Hamilton, US*	**Leveraging Automation Protocols in CC evaluated Products** Erin Connor, *EWA-Canada*
Beyond the CC certificate: how to continue to assess the security assurance in operational systems? Christophe Blad, *OPPIDA, France*	**Security Requirements for Network Devices Protection Profile Review** James Arnold, *SAIC Accredited Testing & Evaluation Lab, US*	**Assurance Activities Test Model** Quang Trinh, *SAIC Accredited Testing & Evaluation Laboratories, US*
Mechanism to provide assurance statements from general purpose hardware David Grawrock, *Intel Corporation, US*	**Protection Profile packages to minimize combinatory complexity for industries developing mobile transactions** Claire Loiseaux, *Trusted Labs, France*	**Certifying Trust** Gene Keeling, *Cisco Systems, Inc., US*
Extending Common Criteria beyond vendor assurance Jennifer Gilbert, *CISCO Systems, Inc., US* Nithya Rachamadugu, *Cynacom Solution (CCTL), US*	**Web Application: Is it suitable for CC evaluation?** Norahana Salimin, *CyberSecurity Malaysia*	**Evaluating Third-Party Code: How Can It Be Trusted?** Courtney Cavness, *atsec information security corporation, US*
Test vehicle - tool to assess candidate ITSEFs' competency Takayuki Tobita, *Information-technology Promotion Agency (IPA), Japan*	**ARC in Practice: Common Structured Approach for the Creating and Assessment of ADV_ARC Aspect** Dr. Igor Furgel, *T-Systems International GmbH, Germany*	**Harmonizing Common Criteria and Formal Risk Analysis Methodologies: Security Target Construction through Risk Analysis** Dr. Jorge López Hernández-Ardieta, *Indra Sistemas S.A., Spain* David Vara Cuesta, *Indra Sistemas S.A., Spain*
CC SVAT: Common Criteria Software Vulnerability Analysis Toolkit Dr. Stan Kladko, *Aspect Labs, US*	**Developing a Formal Security Policy Model for a Smart Card EAL6 Evaluation** Karin Greimel, *NXP Semiconductors Austria GmbH Styria*	**Evaluation evidence production: How far can we go?** Miguel Bañón, *Epoche and Espri, Spain*
Using Threat Modeling within the Evaluation Process in a Common Criteria Evaluation Facility Alexander Findeisen, *SRC Security Research and Consulting GmbH, Germany* Dr. Bertolt Krüger, *SRC Security Research and Consulting GmbH, Germany*	**An Access Control Model for Applications on Mobile Devices using Common Criteria Certifications** Helmut Kurth, *atsec information security corporation, US* Trang Huynh, *atsec information security corporation, US*	**Criteria or Test Specifications?** Denise Cater, *IconSecurity Ltd, UK*
Refining Software Vulnerability Analysis in the Common Criteria Sean Barnum, *The MITRE Corporation, US*	**A Research on Security Vulnerabilities and Establishment of Test Procedures for IPv6-based IT Security Products** Woong-Sang Kim, *Korea Internet & Security Agency (KISA), Korea*	**TOE Security Functional Requirements, in light of attack potentials of different EAL – A Case study** Subhendu Das, *STQC IT Services, India*
From FIPS 140-2 to CC Dr. Yi Mao, *atsec information security corporation, US*	**How can ADV_ARC be used to reduce evaluation effort?** Monique Bakker, *Brightsight BV, Netherland* Peter van Swieten, *Brightsight BV, Netherland*	**Quantifying the strength of security functions in vulnerability assessment** Hongsong Shi, *China Information Technology Security Evaluation Center (CNITSEC)*
HSM Protection profile: How to CC-evaluate a HSM to meet FIPS requirements Sebastián Muñoz, *Realia Technologies S.L.* Jose Emilio Rico, *Epoche & Espri S.L*	**Penetration Test Methodology on Information-Security Product utilizing the Virtualization technology** JungDae, Kim, *Korea Security Evaluation Laboratory Co. Ltd., Korea* Byong-ki, Park, *Korea Security Evaluation Laboratory Co. Ltd., Korea*	**CC Certification from IT to ICT** Yang Cui, *HUAWEI Technologies Co. Ltd., P.R. China* Xin Wang, *HUAWEI Technologies Co. Ltd., P.R. China*
September 29, 2011, Thursday		
TRACK A *(Citrine Ballroom)* CC Formalities	**TRACK B *(Jasmine Junior Ballroom)* Technical Use of CC**	**TRACK C *(Maple Junior Ballroom)* Management Views/ Application Aspects**
Integration of Common Criteria Evaluation activities into the system engineering process Alexander Haferland, *Bundesdruckerei GmbH, Germany*	**Evaluating memory protection of smartcards and similar devices** Wolfgang Killmann, *T-Systems, Germany*	**Common Criteria and Smart Grid technologies** Eugene Polulyakh, *BKP Security, Inc. (parent company of Aspect Labs), US*
Korea Scheme for ISO 17025 Proficiency Testing in CC Evaluation Facilities Hyun-Jung Lee, *Sungkyunkwan University, Korea* Dong Ho Won, *Sungkyunkwan University, Korea*	**Human decisions, for high quality reproducible DPA** Monique Bakker, *Brightsight BV, Netherlands*	**CC Convergence with Safety standards in Aeroutics & Space industries** Michael Dulucq, *Serma Technologies, France*
Comparative study between the Chinese standards and the Common Criteria (CC) Dr. Yi Mao, *atsec information security corporation, US*	**Automatized Fault Attack Emulation for Penetration Testing** Armin Krieg, *Institute for Technical Informatics, Graz University of Technology, Austria*	**Protection Profile for the Gateway of a Smart Metering System Combining privacy protection with security for the grid** Dr Helge Kreutzmann, *BSI, Germany*
The Open Group's Trusted Technology Forum: Developing open standards for a more trusted global supply chain Joshua Brickman, *CA Technologies, US*	**Java Card testing strategy** Ismael Kane, *Applus LGAI Technological Center*	**CC and Industrial Security: Smart Meter Systems are just the beginning** Markus Bartsch, *TÜViT GmbH, Germany*

肆、研討會摘述

一、CC 評估程序

（1） 共同準則雖為國際通用的資安產品驗證標準，但因該驗證時程較長，有其執行上之瓶頸。諸如，造成廠商檢測成本過高、過時的弱點判斷與評估結果不符市場現況所需等等。因此，如何減少評估時程，為本次研討會重要討論議題，相關意見略整如次：

1.計畫管理部分

(1) 重新指派關鍵計畫給其他適合之評估員

2.客戶合作部分

(1) 廠商提供內部諮詢者

(2) 廠商讓評估員與研製者直接溝通

(3) 在服務協議中，明定研製者有提供關鍵資訊之義務

3.產品技術、發展與測試方法部分

(1) 屬利基技術（niche technology）者，包括智慧卡、生物特徵辨識等，在評估期間需要廣泛探究最新發展。

(2) 評估要與產品發展同步，追蹤廠商進度，每 2 周去確保沒有落後該計畫。

(3) 實驗室對尚未遭遇之產品型態，應加強發展其測試計畫相關部分。

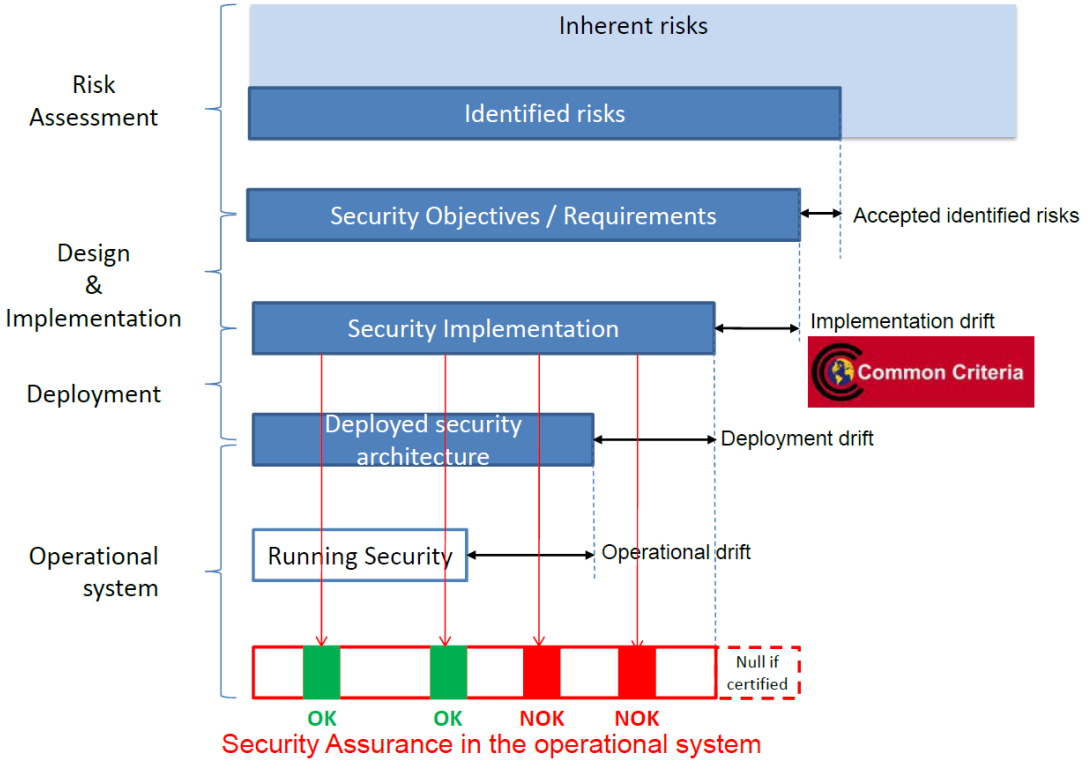
(4) 為每一產品形態，應發展其測試計畫範本。

(5) 以表單格式（內容涵蓋 ASE, AGD, ADV, ATE）記錄產品評估結果。

4.評估者專業度部分

(1) 雇用與評估主題相關之專家，以適時提供產品技術知識。

（2） 由於 CC 之安全評估目前僅專注於產品生命週期之設計與施作，而營運之布建與使用則屬系統規格之範疇，顯非僅產品個自通過安全評估，就足以因應實務情境，諸如，在布建系統安全架構中，囿於環境限制，未臻原先安全施作標準，是以，業經 CC 驗證之產品，於系統實際運作中，常不能達到預期之安全特性。



為解決 CC 在裝置及運作上之安全漂移，應在運用系統中，施以：

(1) 定義測量方式之要求

Are the [Properties] of the [Security requirement realization] as [expected]?

- [Security requirement realization]
  - The concerned security requirement: SFRs, security objectives for the operational environment
  - The supporting element: the TOE / subsystems of the TOE /

elements of TOE operational environment (operating system, database, administrators, premises,…)

- The type of element: physical / social / cyber

- [Properties]

- The temporal property: Configuration / Execution

- The specificity: Generic (TOE guidance) / Specific (deployment specific)

- [expected]

- The reference permitting to interpret the collected data

(2) 收集基本測量

(3) 使用相關參考詮釋基本測量

(4) 對測量做評估保證

(5) 關聯與聚集測量

(6) 顯示結果

二、與他國交流

研討會期間，本會代表與德國、馬來西亞及日本驗證機關代表進行洽談，以交流資安產品推動經驗，建立良好互信關係。另針對中國大陸目前的發展現況，亦與中國信息安全認證中心人員進行討論，對於目前中國大陸的進展亦有進一步的了解。會議期間之交流單位與人員，如下表：

單位	人員
日本驗證主管機關(IPA)	Mr. Yasuhide Yamada (山田安秀)
日本 IT Security Center	Mr. Naoki Ugamura (宇賀村直紀)
德國 TÜViT 實驗室	Mr. Antonius Sommer
馬來西亞 CyberSecurity（驗證單位	Ms. Zaharah Binti Zulkifli

屬科學、技術及創新部項下機構）	
中國信息安全產品檢測中心	宋好好博士

交流內容摘述

（1） 日本驗證主管機關(IPA)代表表示，對於我國目前尚未加入 CCRA 國際組織感到相當遺憾，因 CC 檢測只是單純技術議題。其提出建議，邀請我方參加今年 11 月預訂在印度舉辦之「亞洲 IT 安全評估與驗證論壇（Asian IT Security Evaluation and Certification Forum）」，除可合作、交換有關 IT 安全評估與驗證資訊外，並可增加我國成為 CCRA 會員之機會。但我方表示，囿於出國預算其他運用考量，予以婉謝。

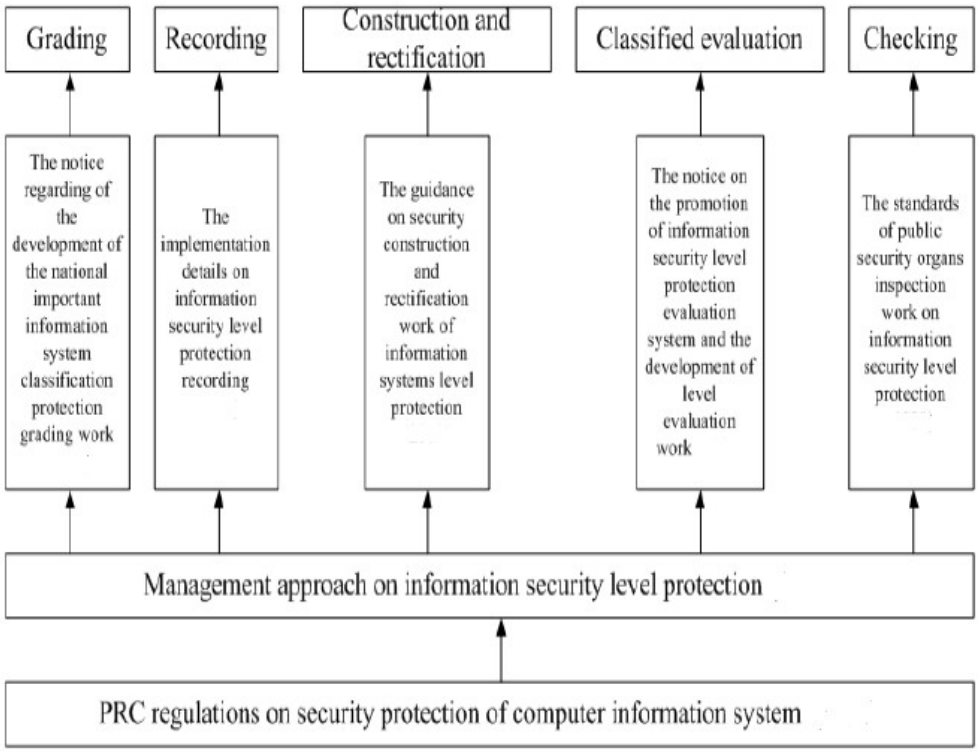
（2） 日本 ITSC 實驗室高階主管表示，由於其政府於今年施行 IT 產品採購安全政策，並公告 IT 安全測量標準產品目錄表，因此，該實驗室產品檢測數量較以往明顯上升。我方亦表示，我國刻正訂定資通設備安全檢測技術規範，將來若能如日本一樣，由政府機關帶動相關產品之採購，據信，對推展我國資安產業，應有事半功倍之效。

（3） 德國 TÜViT 實驗室高階主管表示，對於我國刻正推動之資通訊產品安全驗證非常有興趣，詳詢相關規劃內容，及為何不採國外驗證測報等等，經我方說明相關考量（包括制定符合我國國情之驗證方式、我國尚非 CCRA 會員國等因素）後，獲其認同，願意成為我國資安產品驗證實驗室。

（4） 馬來西亞 CyberSecurity 實驗室代表表示，對 CC 產品檢測時間過於冗長，有何看法。我方表示，因為資安產品生命週期不長，產品檢測時間長，除造成檢測費用偏高，中小企業廠商受測意願不高

外，亦會造成其適用性之困擾。為縮短檢測時間，我國目前規劃資安產品驗證分為「基礎等級」與「進階等級」二類，驗證時間以不超過 2 個月為限。馬方聽後，表示很有興趣想知道我方如何做到，囿於資料未備完整，無法詳細說明，雙方留下電子郵件信箱位址，以為進一步交流。

（5） 中國大陸代表表示，中國雖非 CCRA 會員國，但其產品驗證標準大多參酌 ISO/IEC15408 翻譯而成，並將資訊安全系統分級保護，以合其國情需要，作法如次：



有關該國所稱重要資訊系統，係指涉有國家機密、地方行政區域（縣、市）層級以上之政府重要網站及官方資訊系統，暨交通、電力、銀行等資訊系統。並且依機敏性不同，將該等系統之一般驗證技術，分為第一級（First Level）與第二級（Second Level），對應不同之 CC EAL（Evaluation Assurance Level）：

Level of general techniques requirements	First Level	Second Level
EAL Level	Between EAL4 and EAL5	Between EAL6 and EAL7

伍、心得與建議

此次交流活動，讓吾等了解到各國在資通設備安全檢測之作法，其中包括設備檢測分級方式、如何建構 CC 產品後市場管理模式等，均值得我方借鏡學習。推展資訊技術安全產品驗證業務是國際趨勢，加入 CCRA 對我國資安產品進軍國際市場扮演關鍵角色。然鑑於我國在國際舞台上非為聯合國會員之一，每每在國際組織社會裏，因為國籍身分遭受排拒。此種外交困境，相關建議如下：

1、 持續參加 CCRA 及其外圍組織會議

參加 CCRA 及其外圍組織會議，可和資通訊產品安全檢測先進國家交流 IT 最新安全評估與驗證資訊，讓我國相關技術能與國際接軌。今我國雖囿於政治因素，未能成為 CCRA 會員，但經過多年努力，已與亞洲諸國（日本、馬來西亞等）代表建立良好情誼。據信，只要持續耕耘，俟適當時機，該等國家應可站出，替我國說明「台灣與中國是兩不同政治實體」，支持我國能以加入世貿易組織(WTO)成功的模式加入，即以台澎金馬關稅獨立領域的身分加入並可增加我國成為 CCRA 會員之機會。準此，持續參加 CCRA 及其外圍組織會議有其必要性。

2、 積極推動我國資通訊設備產品驗證

（1） 制定符合我國需求的資通設備安全驗證方法

出席本次會議發現，今之各國莫不為降低 CC 產品檢測時間，積極努力，雖其等作法不盡相同，然而該趨勢確與我國刻正規劃之資通設備安全驗證方向一致，惟考量各國資通設備製造廠商之市場規模、研發與製造能力，並不相同，若將某些國家的資通設備安全驗證方法，全盤移植於我國，恐造成水土不服，事倍功半。準此，應先檢視我國與他國現況之差異性，暨確定短中長期目標為

何，復參酌環境相近之國家作法，截長補短，方訂定我相關驗證方法，較為妥適。

（2） 制定能與國際標準接軌的資通設備檢測規範

目前我國尚待申請加入 CCRA 組織，相關檢測能與國際規範接軌是重要考量因素之一，準此，在研提我國之資通安全檢測設備類別、項目及檢測技術規範時，亦須參酌國際作法及對應配套措施，較為妥適。

陸、照片

照片 1

▲12thICCC 會場

照片 2

▲與日方代表交換意見

照片 3

▲與德國 TÜViT 代表交換意見　　▲與馬方代表交換意見