出國報告(出國類別：會議)

出席 2015 年第 16 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：李技正福懿

派赴國家：英國
出國期間：104 年 9 月 21 日至 9 月 26 日
報告日期：104 年 12 月 15 日

摘要

第 16 屆國際共同準則研討會議(ICCC, International Common Criteria Conference)，於英國倫敦舉行，由英國通訊電子安全部(Communications-Electronics Security Group, CESG)主辦。共有來自 25 個會員國及其它國家官方及地區之驗證機構、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 350 人參加，本會議分三個組別(Tracks)，三天共 54 場小型研討會；內容包含了各國共同準則(Common Criteria，CC)認證機制更新介紹、符合客戶要求介紹及 CC 發展探討之探討等三大類別主題。

ICCC 是一個經驗共享的技術會議，為所有官方代表、負責 IT 產品和系統的安全性方面的專業人士安排互相接觸的機會，參加本次國際研討會有助於本會掌握最新資通安全相關技術的發展趨勢，並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。

目次

壹、目的 1
貳、研討會紀要 1
一、CCRA 組織 1
二、研討會參與者 2
參、研討會議程 3
肆、研討會摘述 7
一、CCRA 各組織報告摘要 7
二、各國 CC 發展現況 10
三、CC 評估趨勢 14
伍、心得與建議 18
一、持續參加 ICCC 及其外圍組織技術會議 18
二、研討會多元模式促進多方交流 18
三、積極推動我國資通訊設備產品驗證 18
陸、會場照片 20

壹、目的

本會負責推動「資通設備之安全檢測研究計畫」，研訂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，設備廠商可對應國際市場上的 IT 產品，以避免重新評估，進而促進我國資通產業發展。

資訊技術安全評估共同準則(也稱 Common Criteria，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、荷蘭 ITSEC(Information Technology Security Evaluation Criteria)等資安標準，於 1994 年公告共同準則 1.0 版，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，並且在 2012 年 9 月公告 CC 3.1 版第 4 個修訂版。

CC 的目標為確保評估的 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；消除重複評估 IT 產品和保護剖繪的負擔；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。

共同準則相互承認協議 (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。

CCRA 管理委員會提出了一份願景聲明，給予 CC 和 CCRA 應用的未來方向，共同準則相互承認協議(CC)和其配套文件-資訊技術安全評估共同方法(Common

Methodology for Information Technology Security Evaluation，簡稱 CEM)是國際協議的技術基本，CCRA 是確保產品由獨立合格的實驗室進行評估，以確保實現其特定安全性能在一定的程度之上及有一定的保證。使用在 CC 認證過程的配套文件，定義了應用於特定技術的認證的標準和評估方法。一個被評估產品的安全性認證，基於評估的結果可以出具一些證書授權計畫，而這些證書是被 CCRA 所有簽署的會員國所承認。

ICCC 是一個經驗共享的技術會議，為所有官方代表、負責 IT 產品和系統的安全性方面的專業人士安排互相接觸的特別機會，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。

貳、研討會紀要

一、CCRA 組織

為了發展 CC 標準、提升各國探討 CC 標準協同溝通，以及強化 CC 評估領域技術，基於 CCRA 宗旨成立各工作小組(Work group)及技術社群(Technical Communities)等組織。

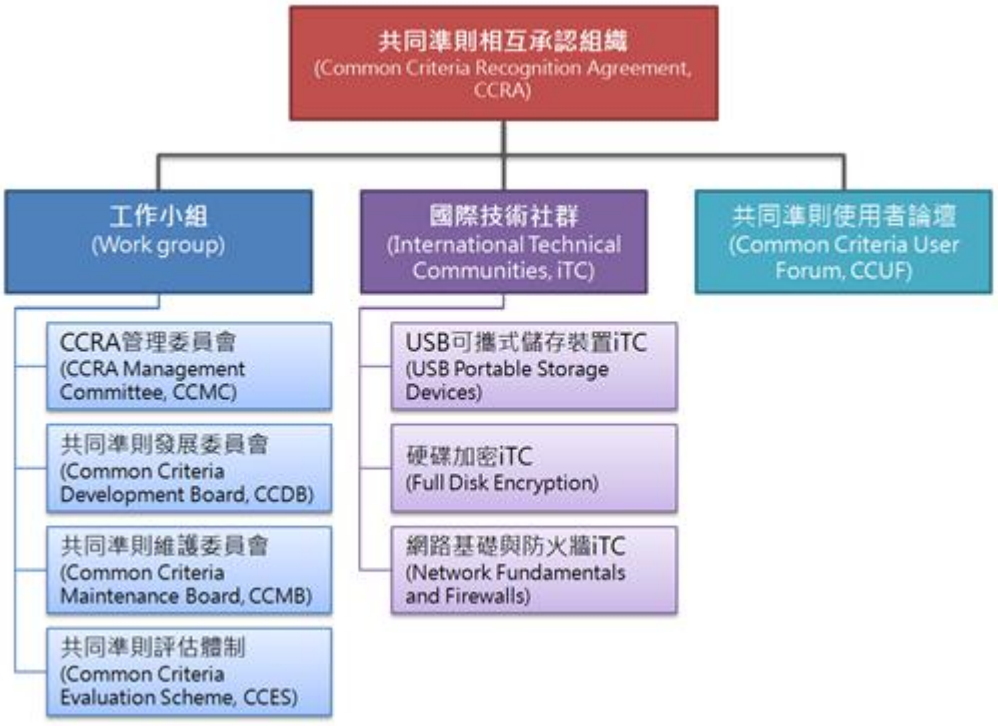

圖 1　CCRA 組織架構

CCRA 現有 25 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、以色列、巴基斯坦等 8 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、馬來西亞、印度等 17 個國家。

圖 2　CCRA 接受證書會員國及核發證書會員國

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。

二、研討會參與者

國際共同準則研討會議(ICCC)是世界共同準則社群之年度會議，並且亦為提給予各國政府機構、私人企業及非營利組織之間的對話的重要論壇。在這重要國際盛會，來自 25 個國家與匯集近 350 位 ICT 系統安全領域之參與者。參與研討會之參與者包括驗證機關、評估實驗室、研究人員、政策制定者與產品開發人員等。從 ICCC 官網資料顯示，主要參與 ICCC 參與者主要集中在產品開發商(19%)、驗證機關(14%)與 IT 分析與安全專家(14%)。

參、研討會議程

2015 年第 16 屆國際共同準則研討會議，2015 年 9 月 22 日至 2015 年 9 月 24 日在英國舉行，由英國政府通訊電子安全部(CESG)主辦，該會議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「Track 1: 符合客戶需求」、「Track 2: 促進 CC 運用」與「Track 3: CC 體制與 iTC 近況」，共計有 54 場次，議程如下：:

表 1：2015 年第 16 屆國際共同準則研討會議議程

	Track 1: 符合客戶需求 (Meeting Customer Requirements)	**Track 2: 促進 CC 運用 (Advances in the Use of Common Criteria)**	**Track 3: : CC 體制與 iTC 近況 (Updates from Schemes and iTCs)**
第一天	CC-evaulated products - An end-user's perspective (James Donndelinger, The Aerospace Corporation)	UL Keynote Address (Andy Brown, UL)	Turkish Common Criteria Certification Scheme – 2015 (Mustafa Yilmaz, Turkish Standards Institution)
	International collaboration, its practice and discussions in development of Protection Profile for Hardcopy Device (MFP PP) (Matsutoshi Murata, Japan IPA)	Equivalency and PP-based Common Criteria evaluations (Ken Elliot, The Aerospace Corp)	Japanese Scheme update (Yutaka Hayami, Japan IPA)
	Protection Profiles: Market Penetration and Lessons for the Next CC (Julian Straw, Primasec Ltd)	ISCI WG1 Methodology 2014/15 Report (John Boggie, NXP Semiconductors)	UK Scheme Update (Richard Manning, CESG)

	Track 1: 符合客戶需求 (Meeting Customer Requirements)	Track 2: 促進 CC 運用 (Advances in the Use of Common Criteria)	Track 3: : CC 體制與 iTC 近況 (Updates from Schemes and iTCs)
	Improving cPP development with end-users (Quang Trinh, Cisco Systems, Inc.)	CC Evaluation of Cryptography in Japanese Scheme with Japan – CMVP (Kenji Yamaya, ECSEC Laboratory Inc. Evaluation Centre)	Medium and higher assurance evaluations in the European context (Julie Chuzel, ANSSI, Joachim Weber, BSI, Rob Huisman, NLNCSA)
	Government agency, industry and security expert in a collaborative approach to deploying Evaluation scheme (Quang-Huy Nguyen & Boutheina Chetali, Trusted Labs)	Cryptography and Common Criteria - Establishing a representative list of internationally acceptable approved security functions in ISO/IEC 19790 (Sonu Shankar, Cisco)	Update on the US Common Criteria Scheme (NIAP) (Janine Pedersen, NIAP)
	Learning from each other and our mistakes (Alicia Squires, Cisco, Ed Morris, Gossamer Security Solutions)	The need for a common international cryptographic standard (Amy W. Nicewick, Corsec)	Common Criteria Users Forum (CCUF) Update (Matt Keller, Corsec)
第二天	Harder than you thought: Updating the Hardcopy Device Protection Profile (Brian Smithson, Ricoh Americas)	Adopting well-proven testing methods for cost-efficiency in Common Criteria testing (Jorge Luengo Garcia, Epoche and Espri)	The Network International Technical Community (Mark Jackson, Cisco)
	Mind the (assurance) gap (Richard West, Cisco Systems, Inc)	Remote testing as an alternative in CC evaluation (Jorge Luengo Garcia, Epoche and Espri)	Full Drive Encryption - iTC Progression and Status Report (Mike Grimm, Microsoft)

	Track 1: 符合客戶需求 (Meeting Customer Requirements)	Track 2: 促進 CC 運用 (Advances in the Use of Common Criteria)	Track 3: : CC 體制與 iTC 近況 (Updates from Schemes and iTCs)
	Exact PP conformance in the age of optional requirements (Justin Fisher, Booz Allen Hamilton)	Fail-secure Common Criteria - Preparing the Common Criteria for IT security's worst enemy (Michael Scheibel, TUViT)	Estimation of measurement of uncertainty on qualitative evaluations according to ISO/IEC 17025: An experimental study (Mehmet CAKIR, BEAM Teknoloji Corp.)
	Using Common Criteria evaluations to improve healthcare cyber security (Margie Zuk, MITRE & David Kleidermacher)	Developing the security functional requirements of mobile devices for the Korean government (Daewon Jung, National Security Research Institute)	NIAP: Around the Evaluation in 90 Days (Noel Richards, NIAP CCEVS)
	Something Old, Something New, Something Borrowed, Something ... (Wouter Slegers, Your Creative Solutions)	Is CC ready to lead the future of mobile Security? (Jose Francisco Ruiz Gualda, Applus Laboratories)	Community action: A Call to Arms (Tony Boswell, DNV GL & Ken Dill, Cisco)
	PP goals - are we on target? (James Arnold and Tammy Compton, Gossamer Security Solutions)	Will Common Criteria be the solution for certifying trustworthy "Things" in the "Internet Of Things (IoT)" ecosystem? (Roland Atoui, Oracle)	18 years of Common Criteria Certifications - Evaluation trends from a global perspective (Tyrone Stodart, Oracle)
	The challenge of methodically opening smart tamper envelope technologies. UNSETH project (Miguel Banon, Epoche and Espri)	Evaluating the revised CCRA - one year on (Wolfgang Killmann, T-Systems GEI GmbH)	Secure software development in the Russian IT Security Certification Scheme (Gil Bernabeu, GlobalPlatform, Inc.)
	BEATing attacks on Biometric Systems (Alain Merle, BEAT)	Progress on MSSR (Werner Gutau, Infineon Technologies)	The Development of Common Criteria in China (Yuanyuan Yang)

	Track 1: 符合客戶需求 (Meeting Customer Requirements)	Track 2: 促進 CC 運用 (Advances in the Use of Common Criteria)	Track 3: : CC 體制與 iTC 近況 (Updates from Schemes and iTCs)
	Evaluating in a time of rapid technical advances (Greg Lague and Kim Braun, EWA-Canada)	Clarification of CC Concepts (Wolfgang Killmann, T-Systems GEI GmbH)	Explaining GlobalPlatform's modular approach to its TEE Protection Profile (Gil Bernabeu, GlobalPlatform, Inc.)
第三天	Secured Memory: A New Solution, a New Evaluation Approach, a New Challenge (Miguel Jose Hernandez Vidal, Applus and Rachel Menda-Shabat, Winbond Technology Ltd.)	Vulnerability analysis for collaborative protection profiles (Ken Elliot, The Aerospace Corp)	Matching Common Criteria evaluations with the pace of development (David Grawrock, Intel Corporation)
	Non-Interfering Composed Evaluation or How to Exchange Components without Re-Evaluation (Igor Furgel, T-Systems GEI GmbH & Kevin Mueller, Airbus)	Reducing Evaluation Redundancy: Site Audit Results Re-Use (Peter Van Swieten, Brightsight)	Testing the network device: The lessons from the Korean government (Kyuho Hwang & Hawon Kim, National Security Research Institute)
	ISCI-WG1: The updated ETR_COMP template and methodology (Monique Bakker, Brightsight /Sertit)	Don't be afraid of the Entropy Bogeyman (Ed Morris, Gossamer Security Solutions)	Testing of mobile virtualization systems: The lesson from the Korean government (Miri Joo & Young Mi Park, National Security Research Institute)

肆、研討會摘述

一、CCRA 各組織報告摘要

(一) 共同準則發展委員會(Common Criteria Development Board, CCDB)：

CCMC 主要管理 CCRA 關於技術方面議題，包含共同準則及共同準則方法論(CEM)維護，以及對國際技術社群(International Technical Communality, iTC)發展合作保護剖繪(collaborative Protection Profile, cPP)監督之責。

CCDB 主席在會中提及重點如下：

1. CC 與 CEM 標準審查與更新：為與 ISO/IEC 組織共同校對 CC 標準(即 ISO/IEC 15408)與 CEM 標準(即 ISO/IEC 18045)，並且作小幅度標準內容修訂，在 2015 年 10 月 CCRA 與 SC27WG3 單位討論後，即將公告 CC 與 CEM 第 3.1 版第 5 次修訂(Release 5)，在正式改版之前會遵循改版程序向大眾徵求修訂與建議(徵詢期間 6 個月)，結果建議徵詢後預計 12 個月後提出草稿版本，並且在後續訂定版本轉換相關程序。
2. CC 標準支援文件(supporting document)審查：針對評估 iTC 擬訂適切評估支援文件，並且在 CCDB 進行審查與核准後公告在 CCRA 官網上。
3. CCRA 官網持續維護：為因應 CC 與 CEM 即將修訂版次，將會提供相關網頁資訊在官網上，並且為了評估 iTC 單位，亦會提供 iTC 重大變更及相關時程以供相關人士參閱使用。

(二) iTC/cPP 新候選名單：除原有三大 iTC 之外，將針對生物辨識(Biometrics)安全、作業系統平台上之應用系統安全、加密(encryption)安全、行動裝置安全規劃建立新 iTC 單位並致力發展相關 cPP。

(三) CCRA 管理委員會(CCRA Management Committee, CCMC)：

CCMC 主要管理整個共同準則相互承認組織(CCRA)，確保參與 CCRA 會

員會依據共同準則協議規定並保障 CCRA 整體運作。CCMC 在本屆 ICCC 研討會中提及重點如下：

1. CCRA 會員國異動：目前現有 8 個接受證書會員國(CCM)之中，已有 1 個接受證書會員國決定申請進入核發證書會員國(CAM)，目前待等資格受審中。此外，新加坡資訊通信發展管理局(IDA) 自願終止取消接受證書會員國資格，並已於今年 6 月 19 日在 CCRA 官網上已公告新加坡為非接受證書會員國成員之一。
2. 2014 與 2015 各國體制自願性評鑑：各國體制自願性定期評鑑對於相互承認體系而言是相當重要基石，必須基於各國強健及遵循規範共同準則體制才能提供可信賴之共同準則規範評估結果。在 2014 與 2015 年共針對三個會員(包含英國、美國與土耳其)完成體制自願性評鑑，並皆已通過評鑑。
4. CCRA 會員參與 2015 年 09 月 22 日第 16 屆政府間半導體會議(Governments/ Authorities Meeting on Semiconductors, GAMS)，該會議來自國際間半導體產業溝通論壇，亦即半導體產業重要政府間國際會議，今年參與討論成員包含美國、歐盟、日本、韓國、中國大陸與臺灣。在 GAMS 會議中討論針對半導體產品之密碼認證及證書之商業實務探討，並與各國討論各自加密標準與許可認證規範討論。

(四) 國際技術社群(International Technical Communality, iTC)

iTC 是經由 CCDB 成立並經 CCMC 核可的組織單位，並且彙集認(驗)證機構、實驗室、廠商及專家學者之技術團隊，iTC 主要致力於特定技術領域以制定 cPP，進而支持 CCRA 宗旨與促進資通安全產品公平競爭。至目前為止已成立三個 iTC，包含如下：

表 2： iTC 國際技術社群彙整表

iTC 名稱	參與 iTC 國家
USB 可攜式儲存裝置 iTC(USB Portable Storage Device iTC)	共有 12 個，包含澳州、加拿大、德國、芬蘭、丹麥、日本、荷蘭、新加坡、瑞典、土耳其、英國與美國。
硬碟加密(Full Disk Encryption) iTC	共有 10 個，包含澳州、加拿大、印度、日本、挪威、韓國、瑞典、土耳其、英國與美國。
網路基礎暨防火牆(Network Fundamentals and Firewalls) iTC	共有 10 個，包含澳州、加拿大、印度、日本、挪威、韓國、瑞典、土耳其、英國與美國。

(五) 共同準則使用者論壇(Common Criteria User Forum, CCUF)

共同準則使用者論壇(CCUF)源自於共同準則廠商論壇(Common Criteria Vendor Forum, CCVF)，因應各界參與需求，將廠商擴展為各界均可參與論壇，CCUF 於 2010 年正式成立，CCUF 使命主要是提供 CC 社群和 CC 各委員會、各國家體制代表和政策制定者之間的溝通與通信管道。目前 CCUF 現況如下：

1. CCUF 管理委員會由七位成員組成，包含業界思科 Cisco(Alicia Squires)、理光 Ricoh(Brian Smithson)、Ark Infosec(Lachlan Turner)、Corsec(Matt Keller)、Epoche & Espri(Miguel Bañón)、微軟 Microsoft(Mike Grimm) ，以及甲骨文 Oracle(Petra Manche)。
2. 目前會員人數共 700 位，會員類型分佈主要是以廠商(44%)、實驗室(22%)、CC 體制成員(14%)為主，其次為政府單位(5%)與學術委員(3%)，其他則是一般使用者、供應商、標準組織等。
3. 會員國籍分佈於 29 個國家中，其中為非 CCRA 會員國國家共 5 個包含中國大陸、俄國、泰國、瑞士與南非；CCUF 會員以美國(42%)、日本(13%)及韓國(7%)會員國籍占為最多數，其次為加拿大(6%)、英

國(5%)、土耳其(5%)、法國(4%)。

4. 2014 年 10 月~2015 年 09 月 CCUF 共舉辦 3 次專題討論會，CCUF 提供多個 iTC 及 TC 之間可以相互合作平台，並且定期每月舉辦成員討論會以符合規劃進度，預計將更新 CCUF 指導文件及更新 CCUF FAQ 資訊。

二、各國 CC 發展現況

（一）英國 CC 驗證體制現況

1. 英國 CC 標準驗證機構(CB)為通訊電子安全部(CESG)，是 CC 標準創始國之一所以在 1991 年就成為授與證書會員國，目前共有 3 家 CC 標準檢測實驗室(分別為 CGI、SiVenture 與 UL)。
2. 截至目前為止英國共發佈 43 張證書，產品類型分別為 IC 類產品(15 個)、網路裝置(8 個)、其他設備類(7 個)、存取控管(6 個)、保護裝置(4 個)、作業系統(3 個)。
3. 英國現行致力於針對客戶回饋建議進行 CC 及相關 IT 驗證體系改善，並且積極推行商業產品保證(Commercial Product Assurance, CPA)驗證標準，同時與專家學者合作推行 cPP。

（二）歐洲相互承認協議(SOGIS MRA)

SOGIS 是歐盟組織下委員會，不同於 CCRA 僅相互承認於 EAL4+，歐洲相互承認協議(SOGIS MRA)相互承認範圍由 EAL1 至 EAL7。SOGIS MRA 相互承認國家目前共有 10 個國家，包含英國、法國、德國、希臘、義大利、挪威、西班牙、瑞典、芬蘭與奧地利。

(三) 土耳其 CC 驗證體制現況

1. 土耳其 CC 標準驗證機構(CB)為土耳其標準局(Turkish Standards Institution, TSE)之資訊科技檢測與認證部(Information Technology Test and Certification Department)負責，並於 2008 年受 CCRA 核准為授與證書會員

國。

2. 從 2008/12 至 2015/09 統計共已發佈 42 張證書，其中包含 34 張產品認可證書及 8 張保護剖繪通過認可證書。並且目前正在檢測產品共有 32 件，以及仍在檢測中保護剖繪共有 11 件。
3. 土耳其除了實作 CC 評估體系外，針對 IT 認證服務範圍相當多元，包含場址認證(Site certification)、密碼模組與密碼演算驗證計畫(TS ISO/IEC 19790)、IT 電子紀錄管理(TS 13298)、IT 軟體套件品質要求與檢測(TS ISO/IEC 25051)、軟體生命週期(TS ISO/IEC 12207)與系統生命週期認證(TS ISO/IEC 15288)、人力資源系統認證(TS ISO/IEC 9241-151)等。

（四） 日本 CC 驗證體制現況

1. 日本 CC 標準認證機構(AB)為日本獨立行政法人製品評價技術基盤機構(National Institute of Technology and Evaluation, NITE)，驗證機構(CB)為資訊處理推進機構(INFORMATION-TECHNOLOGY PROMOTION AGENCY, IPA)，於 2004 年受 CCRA 核准為授與證書會員國，並且目前日本境內共有 5 家檢測實驗室，主要可分為軟體檢測實驗室(日本資訊技術安全中心評估部 ITSEC、ECSEC、日本瑞穗銀行股份有限公司 Mizuho IR 與德國漢德實驗室)與硬體檢測實驗室(Brightsight BV 與 ECSEC)。
2. 從 2014 年度統計共已發佈 45 張證書，其中主要集中於多功能印表機、其次為 MFP 相關軟體與產品、智慧卡 IC 晶片、儲存裝置等。並且在 2014 年度共有 5 件是維護驗證。產品申請驗證主要集中在 EAL3 驗證。
3. 在 2015 年度針對日本 CC 體制要求文件特別要求產品檢測評估符合評估工作計畫書期程控管，即檢測實驗室在檢測案件成立會交付給驗證機構產品整個檢測評估預估時程之評估工作計畫書(Evaluation Work Plan)。當驗證機構發現檢測實驗室沒有依據評估工作計畫書延後交付超過 3 個月將會向檢測實驗室提出警告通知，並須請檢測實驗室回覆延誤理由。
4. 依據日本政府於 2013 年正式通過「My number」全名為「社會保障與納

稅人識別號碼制度」法案，並預定在 2015 年 10 月以後開始分發記載國民姓名、住址、個人編號等相關資訊的「通知卡」，日本民眾可至相關單位申辦「個人編號卡（即 My number 卡）」。日本個人編號卡已由 JISEC 通過 EAL4+等級共同準則標準認證，並且能抵抗侵入性和非侵入式篡改攻擊。

（五）中國大陸 IT 安全驗證體制

1. 中國大陸為保護消費者人身與動植物安全及保護國家安全，已於 2001 年 12 月 7 日共同發布中國大陸強制認證(China Compulsory Certification，3C)之強制性產品驗證制度。針對資訊安全相關產品之驗證機關由中國信息安全測評中心(China Information Technology Security Evaluation Center, CNITSEC)擔任，目前中國大陸境內已有 15 間由驗證機關授權及認可之檢測實驗室。
2. 中國大陸針對資訊產品最先採用《計算機信息系統安全保護等級劃分準則(GB17859)》標準進行檢測評估，該標準將產品分為五個等級，包含第一級用戶自主保護級、第二級系統審計保護、第三級安全標記保護、第四級結構化保護，以及第五級存取驗證保護。不同等級之安全要求，包含自主存取控制(discretionary access control)、身分認證(Identity authentication)、資料完整性(data integrity)、物件再使用(Object reuse)、稽核(audit)、強制存取控管(mandatory access control)與安全標記(sensitivity label)各有不同要求。
3. 中國大陸為非 CCRA 會員國，並且依據歷年參與 ICCC 研討會經驗，中國大陸仍指派人員參與研討會，以獲得關於 CC 標準之發展及技術新知。CC 標準(v2.1)在 1999 年公告後，中國大陸參照 CC 標準與 ISO/IEC 15408:2005 標準發展屬於中國資訊技術安全功能產品之檢測標準《信息技術－安全技術－信息技術安全性評估準則(GB/T 18336)》。此外，亦發展類似於保護剖繪(PP)功能之標準，包含《資訊安全技術－網路交換器

(EAL3)安全要求(GB/T 21050-2007)》與《資訊安全技術－智慧卡嵌入式軟體(EAL4+)安全要求(GB/T 20276-2006)》。

4. 中國大陸送測資訊安全產品包含防火牆、入侵監測、存取安全、網路隔離、VPN、智慧卡、安全管理等。
5. 中國大陸現行積極發展檢測工具，包含智慧行動終端漏洞檢測工具、工業控制系統協定測試軟體、Web 應用安全檢測平台、硬體分離組件安全檢測平台等。

（六）美國 CC 驗證體制

1. 美國 CC 標準驗證機構(CB)為美國國家資訊保證合作組織(National Information Assurance Partnership, NIAP)，是 CC 標準創始國之一，所以在 1991 年就成為授與證書會員國，美國境內是所有會員國之中擁有檢測實驗數最多國家，目前共有 10 家 CC 標準檢測實驗室(包含 Acumen、atsec、Booz Allen Hamilton、CGI、COACT Inc.、Computer Sciences Corporation、CygnaCom、Gossamer、InfoGard 與 Leidos)。
2. 美國從 CC 標準成立以來就積極投入資源發展及通過產品驗證，從 CCRA 官網統計通過 CC 標準產品為 116 件並已發展超過 30 件保護剖繪，以及共有 96 項產品已遵循保護剖繪進行產製與驗證。同時，美國也積極參與現行 CCRA 所要推廣 cPP 之發展。
3. 未來美國將致力探討主要技術領域包含行動裝置、網路設備/防火牆、作業系統、應用軟體、無線網路、虛擬化與硬碟加密。主要持續努力項目包含參與技術委員會及 CCUF 論壇。

（七）俄國 IT 安全認證體制

1. 俄國並無加入 CCRA，但俄國自 1995 年起建置俄國 IT 安全認證體制(IT Security Certification Scheme)，並且由俄國技術暨出口管制聯邦服務中心(Federal Service for Technical and Export Control, FSTEC)擔任 IT 安全認證體系重要窗口。目前俄國境內共有 41 家檢測實驗室及 9 家驗證機構。

2. 俄國境內 IT 安全驗證體制均有依據 CC 標準改版而轉換為國內核可標準(CC v3.1 即 GOST R ISO/IEC 15408-2012/2013)及評估方法論(CEM v3.1 即 GOST R ISO/IEC 18045-2013)，讓各檢測實驗室與驗證機構予以遵循及採用。
3. 截至目前為止俄國 IT 安全認證體制共發佈近 260 張證書，產品類型分別為防火牆(35%)、存取控制系統(15%)、嵌入式存取控制(17%)、軟體(13%)、網路系統(6%)、作業系統(5%)與其他(9%)。通過認證產品之中近 6 成為俄國境內廠商，近 4 成為非俄國廠品開發商；而非俄國廠商開發商統計，主要通過產品廠商為思科 Cisco(58%)、微軟(7%)、Juniper(6%)與甲骨文(5%)。
4. 俄國現行已核准四份保護剖繪，包含入侵防護系統/入侵偵測系統保護剖繪(2012 年)、防毒軟體保護剖繪(2013 年)、可信賴引導裝載器(trusted boot loader) 保護剖繪(2014 年)與可移除儲存保護工具保護剖繪(2014 年)。目前仍在發展中保護剖繪包含防火牆、作業系統與資料庫管理系統保護剖繪。
5. 俄國針對軟體安全日益重視，已發佈《軟體安全發展一般要求》草稿版，標準內針對軟體發展進行控制，包含資訊安全威脅控管、源始碼靜態/動態分析、源始碼審查及滲透測試等。

三、CC 評估趨勢

(一)行動裝置安全議題

1. 由韓國國家安全研究院(NSRI) Keunwoo Rhee 先生主講「Developing the Security Functional Requirements of Mobile Devices for the Korean Government」主題中報告摘要如下：
   (1) 韓國在 2013 年公告行動裝置安全管理產品要求，並且在 2014 起至 2015 年止已共有 7 件採用 MDM 系統產品通過韓國驗證機構 ITSCC

認可。

(2) 為了解決行動裝置安全議題，韓國從 2014 年 8 月起集合產官學各單位針對行動裝置安全議題進行討論，並列出行動裝置安全功能要求，包含資料保護、身分認證、安全管理、存取控管、可信賴路徑，以及延伸定義組件平台與應用管理保護。此外，亦商討是否採納密碼加密支援、IPSec VPN、額外使用者認證機制及 Wi-Fi 連線性功能。

2. 由 Applus+實驗室 José Francisco Ruiz Gualda 先生主講「Is Common Criteria ready to lead the future of mobile security ?」主題報告重點如下：

(1) 行動裝置是現行新市場，針對新市場範疇將包含新使用方法、新產品、新玩家，甚而新技術解決方法。現有包含身分證、信用卡、交通卡、健保卡、資訊書法等，未來都有可能整合至行動裝置上，行動裝置安全議題不容忽視。演講者針對行動安全提出技術解決方案即推薦採用可信賴執行環境(Trusted Execution Environment, TEE)規格方案，TEE 是在不安全的作業環境下，建構獨立且可信賴的執行環境，以解決行動裝置之軟體執行安全性問題。

(2) 演講者說明現有解決方案包含主要三大類架構，包含安全元件基礎(Security element-based)架構、雲端基礎(Cloud-based)架構與可信賴執行環境基礎(TEE-based)架構。

3. 由韓國國家安全研究院(NSRI) MIRI JOO 先生主講「Testing of Mobile Virtualization Systems : The lesson from the Korean Government」主題中報告重點如下：

(1) 因應自帶設備(BYOD)風潮，員工或使用者自行購買行動裝置，公司可能負擔部份費用，使用者可以使用自行挑選設備，公司可以降低成本及有效使用 IT 系統，但行動裝置用於公司用途，可能引起高資料外洩風險並且設備可能入侵而帶給組織資安災難，有鑑於此，建議採用行動虛擬化(Mobile Virtualization)方案解決。

(2) 行動虛擬化具備有兩大特色：分割(Separation)，將行動裝置分割為私人使用區域與辦公使用區域。隔離(Isolation)，兩個分割區域不會相互影響或存取到對方資源。

(3) 行動虛擬化主要可以採用以下其中一種技術建置：超級監督者(hypervisor)，1 台行動裝置、1 個超級監督者及 2 個或多個作業系統環境；容器(Containers)技術，1 台行動裝置、1 個作業系統及容器機制。

(4) 針對行動虛擬化需要以下安全功能要求：行動虛擬化設備要有虛擬化區域保護要求、資料保護、設備與 App 控管、身分認證、自我測試、安全稽核日誌管理、資料傳輸保護；行動虛擬化伺服器要有身分認證、安全管理、安全政策管理、交談管理、安全稽核日誌管理、資料傳輸保護。

(5) 未來將針對行動裝置作業系統、行動虛擬化弱點分析，以及雲端虛擬化議題作探討。

(二)密碼安全議題

1. 由日本 ECSEC 實驗室 Kenji Yamaya 先生主講「CC Evaluation of Cryptography in Japanese Scheme with JCMVP」報告摘要如下：

(1) 有鑑於 CC 標準 Part 2 中提及資通安全產品可能包含加密支援安全功能，故檢測實驗室須針對密碼演算法進行檢測。各項密碼檢測須依賴檢測實驗室，為確保 CC 標準檢測保證，日本在 2008 年針對密碼演算法驗證成立日本密碼模組驗證計畫(Japan cryptographic module validation Program, JCMVP)，該計畫類似於美國 CAVP 機制。

(2) 日本提供 JCATT 可作為 CC 標準評估檢測之用，目前使用於晶片與智慧卡檢測，未來規劃可用於事務機設備、網通設備及 USB 設備之用。

2. 由 Corsec 安全公司 Amy Nicewick 女士主講「Common Criteria and a Mutually-Recognized International Cryptographic Standard」報告摘要如下：

(1) 產品製造商需要尋求多種不同的加密驗證或加密評論及實作後，並且在不同國家銷售。目前遭遇因境即各國在境內投入人力密碼領域成本、境內檢測實驗室自行檢測及專用檢測平台，以及眾說紛紜密碼演算法清單，各國中無使用一套共同密碼演算法驗證標準，對廠商而言即是增加產品成本。

(2) 以 CCRA 組織會員國而言，各國對於資通安全產品之密碼驗證標準不一，如美國及加拿大採用 FIPS 140-2、英國採用 CAPS/CPA/FIPS 140-2、日本韓國西班牙採用 ISO/IEC 19790、德國荷蘭鈕西蘭澳洲採用政府審查方式檢查、挪威採用基於 FIPS 140-2 標準之政府審核。

(3) 密碼安全已採用於現行 PP 或 cPP 之中，包含硬碟 PP、密碼模組 PP、加密儲存裝置 PP、IP 加密 PP、數位簽章 PP 與金鑰管理系統 PP。此外，CCUF/CCDB 密碼工作小組已開始 ISO/IEC 組織之 JTC1 SC27 WG3 密切合作。

(4) FIPS 140-2 標準可算是密碼驗證國際標準，但仍缺少國際相互承認機制並且僅有美國對該標準維護。然而 ISO/IEC 19790 雖然是國際間採用標準，但是缺少類似 CCRA 組織之中心授權機構，並且僅有有限經濟利益提供資源。有鑑於此，希望推展國際密碼計畫，以許可 cPP 制作者提供共用及可信賴密碼檢測，以及各國皆可信賴由 cPP 所需密碼演算並購意採購通過核可產品。

伍、心得與建議

此次參與研討會，可以了解資通設備安全檢測之趨勢與作法，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，透過參與，了解各國在 CC 標準努力及著重要點，包含 CCMC 對未來策略方向、iTC 與 cPP 熱烈宣導、行動裝置及雲端等技術議題研討等。經過此次研討會相關建議下：

一、 持續參加 ICCC 及其外圍組織技術會議

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。我國雖囿於政治因素，未能成為 CCRA 會員，但透過各國專家學者對於 CC 標準發展及技術分享，能得知不同往年技術導向及寶貴知識資料。確保我方能確實掌握 CC 標準發展趨勢及相關技術動向。

二、 研討會多元模式促進多方交流

研討會舉辦模式包含專題演講、座談會、議題分享、資安展覽等方式。專題演講提供特別來賓及專家對於 CC 標準及資安技術知識進行分享；而三場座談會分別邀請官方與業界以共同探討 cPP 對使用者需求度、業界對 CC 標準看法與 CC 未來資安挑戰議題，開放式座談讓各方意見得以交流，達到集思廣益之效。而議題分享透過三大議題主軸，讓有與會者挑選興趣主題，各個專家學者於與會中相互切磋。並且資安展覽更能展示廠商推銷商品，促進商業媒合與交流，可以得知近期技術導向。

三、 積極推動我國資通訊設備產品驗證

（一） 持續制定能與國際接軌的資通設備檢測規範

本會雖於 100 年至 101 年陸續完成「網路型防火牆」、「無線區網路路由

器」、「無線接取設備」、「入侵偵測防禦系統」、「防毒閘道器設備」、「網路型垃圾郵件過濾設備」、「網頁應用防火牆」、「應用軟體控管系統」、「乙太網路交換器」、「路由交換器」等 10 項資通設備安全檢測技術規範。惟該 10 項資通設備仍不足因應全面提升我國資通設備環境安全之所需，104 年檢討增加 4 項新增資通設備安全檢測之項目。105 年將新增手機系統內建軟體資安檢測技術，及建置基站資安檢測環境規劃研究，為避免閉門造車，應配合國際檢測脈動，以增訂其他資通設備安全檢測技術規範。

（二） 檢視現行資通設備安全檢測技術規範

出席本次會議發現，CCRA 刻正修正新契約內容版本，並由合法核准的國際技術社群發展出新的合作保護剖繪，考量本會所訂資通設備安全檢測技術規範有關書面審查部分，係參照 CC 設計，因此，往後對該等規範有再檢視之必要性，以作為修正檢測方向之參考依據。

陸、會場照片

▲與 CCDB 主席合影

▲與新加坡 CSA 代表合影

▲會場照片

▲座談會照片

▲座談會照片

▲座談會照片