出國報告(出國類別：會議)

出席 2012 年第 13 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：韓簡任技正鎮華、謝技正志昌
派赴國家：法國
出國期間：101 年 9 月 16 日至 9 月 22 日
報告日期：101 年 11 月 15 日

摘要

第 13 屆國際共同準則研討會議(ICCC, International Common Criteria Conference)自 101 年 9 月 18 至 20 日於法國的巴黎(Paris)舉行，由 ANSSI 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 66 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、中國代表進行意見交流外，亦與德國 TÜViT 就我國推動資安設備檢測現況提出說明。

目次

壹、目的

本會負責推動「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。

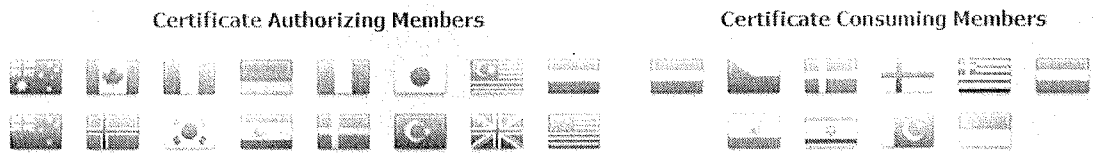
共同準則相互承認組織(Common Criteria Recognition Agreement，簡稱 CCRA)的目的為促進 CC 目標實現，讓認證/驗證機構（CB）發行 CC 證書應符合高度和一致的標準，使資訊科技產品及保護剖繪獲得 CC 認證後，使用者在購買或使用這些產品時，不需要作進一步評估。

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、巴基斯坦、新加坡等 10 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、馬來西亞等 16 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 16 日	自臺北中正機場啟程
9 月 18 日至 20 日	參加研討會
9 月 22 日	返抵國門

2012 年第 13 屆國際共同準則研討會議，在法國的巴黎(Paris)舉行，由負責法國資訊系統安全與防護的 ANSSI（Agence Nationale de la Sécurité des Systèmes d' Information）主辦，該會議除例行的開閉幕儀式、管委會報告與專題演說外，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 66 場次：

DAY 1 - TUESDAY SEPTEMBER 18

Time	Plenary – [illegible]		
09:00	Opening plenary - [illegible]		
09:30	Welcoming Address - [illegible]		
10:00	Keynote speech #1 - [illegible]		
10:30	Keynote speech #2 - [illegible] *Director of Technology Strategy, [illegible], United Kingdom*		
11:00	COFFEE BREAK - GRAND FOYER		
11:30	Panel Discussion - [illegible]		
12:00	Update from CCRA Management Committee - [illegible], *CCMC Chairman*		
12:30	Update from CCRA Development Board - David [illegible], *CCDB Chairman*		
13:00–14:00	LUNCH - RESTAURANT		
14:30	*Press Conference - Room A / Modigliani* Dag Ströman, Patrick Pailloux, Christophe Blad, Mario Figueiredo, Alicia Squires		
	Track 1 - [illegible]	Track 2 - [illegible]	Track 3 - [illegible]
14:30	French Scheme Updates [illegible], *Head of FR's CB, ANSSI, France, Scheme Updates*	Evaluation of products involving cryptography within the German CC-Scheme *Mr Adrian [illegible], Cryptography*	Minimum Site Security Requirements for the Smart Secure Device supply chain [illegible] *Secure Development*
15:00	German Scheme Updates [illegible], *Head of DE's CB, BSI, Germany, Scheme Updates*	Common criteria on crypto? *Mr Matthew [illegible], Cryptography*	Common Criteria and Secure Development: A New Proposal [illegible] *Secure Development*
15:30	Japanese Scheme Updates *Mr [illegible], Head of JP's CB, IPA, Japan, Scheme Updates*	Smartphone Applications - Common Criteria is going Mobile *Mr Jens [illegible], Mobile Security*	Virtualization and the Common Criteria [illegible] *Virtualization*
16:00	COFFEE BREAK - GRAND FOYER		
16:30	Turkish Scheme Updates *Mrs [illegible], Head of TR's CB, TSE, Turkey / Scheme Updates*	(U)SIM certification process configuration issues [illegible] *Mobile Security*	Certification of development sites of smart card manufacturers [illegible] *Secure Development*
17:00	British Scheme Updates [illegible] *Head of UK's CB, CESG, United Kingdom, Scheme Updates*	Security requirements for NFC devices [illegible] *Mobile Security*	CC compositional certification for MILS virtualization platforms [illegible] *Virtualization*
17:30	American Scheme Updates *Mr [illegible], Head of US' CB, NIAP, United States, Scheme Updates*	Overview of security evaluation of electronic travel documents [illegible] *Experiences*	Feedback on the application of ALC requirements in Open Source projects [illegible] *Secure Development*
18:00	END OF DAY 1 CONFERENCE		

DAY 2 - WEDNESDAY SEPTEMBER 19

Time	Track 1 - [illegible]	Track 2 - [illegible]	Track 3 - [illegible]
09:00	CCMB Report [illegible]	US NIAP Protection Profiles Progress and Lessons Learned [illegible] *CC and New Techniques*	Observations from an NDPP Evaluation [illegible] *Experiences*
09:30	CC Users Forum Report to the Community [illegible] *Reports from CC Communities*	Assurance Activities: Ensuring Triumph, Avoiding Tragedy [illegible] *CC and New Techniques*	NDPP - is it better? [illegible] *Experiences*
10:00	ISCI contribution to Common Criteria methodology improvement [illegible] *Reports from CC Communities*	Modular Protection Profiles [illegible] *CC and New Techniques*	Experience with OSPP Evaluations [illegible] *Experiences*
10:30	COFFEE BREAK - GRAND FOYER		
11:00	Reuse of evidences and evaluation results [illegible] *Reports from CC Communities*	CSPN to CC Evolution [illegible] *CC and New Techniques*	Certification of a loader integrated in a Secure Microcontroller: strategic stakes [illegible] *Experiences*
11:30	Progress Report from the Supply Chain Security Technical Workgroup [illegible] *Reports from CC Communities*	An Architectural Framework Approach in the Development of Technical Communities and Collaborative Protection Profiles *Mr [illegible], CC and New Techniques*	Teaching CC: lessons learned [illegible] *Experiences*
12:00	NIAP Technical Communities [illegible] *Reports from CC Communities*	Security proposal on mobile payment [illegible] *CC and New Techniques*	Technical challenges and solutions in Sony FeliCa contactless smartcard EAL6+ evaluation [illegible] *Experiences*
12:30–13:30	LUNCH - RESTAURANT		
14:00	General Purpose Operating System Protection Profile/Stepwise Refinement of Evaluation Methodology [illegible] *Reports from CC Communities*	How a revised TSFI definition can save work for both the developer and the evaluator allowing focusing on its security impact [illegible] *CC and New Techniques*	Complex Systems Security Assessment based on CC methodology [illegible] *Experiences*
14:30	Progress Report on the Enterprise Security Management Suite [illegible] *Reports from CC Communities*	Making a better standard PP [illegible] *CC and New Techniques*	CLOUD SECURITY AND COMMON CRITERIA [illegible] *New areas of application for CC Certification*
15:00	Details of new MFP-PP as a candidate for CPP [illegible] *Procurement of CC certified Products*	IT Security Evaluation in China [illegible] *CC and other Standards*	INNOVATION and the COMMON CRITERIA [illegible] *New areas of application for CC Certification*
15:30	COFFEE BREAK - GRAND FOYER		
16:00	Test Vehicle for Java Card [illegible] *CC and Tools*	To be defined	Assurance case for General Purpose Hardware [illegible] *New areas of application for CC Certification*
16:30	The Re-assessment Process within the BSI-Scheme [illegible] *Assurance Maintenance*	Commercial Product Assurance - an update *Mr [illegible], CC and other Standards*	Common Criteria for deployment of NFC solution " (Return on Experience) [illegible] *New areas of application for CC Certification*
17:00	Software Modularisation and the Common Criteria A Smartcard Developer's Perspective [illegible] *Assurance Maintenance*	ISO/IEC JTC 1/SC 27/WG 3 new Terms of Reference and progress [illegible] *CC and other Standards*	Applying Common Criteria (CC) to Service Oriented Architectures (SOA) [illegible] *New areas of application for CC Certification*
17:30	END OF DAY 2 CONFERENCE		
19:00	GALA DINNER & CERTIFICATE AWARD MUSÉE DES ARTS FORAINS, PARIS		

DAY 3 - THURSDAY SEPTEMBER 20

Time	Track 1 - [illegible]	Track 2 - [illegible]	Track 3 - [illegible]
09:00	Update from CEN TC 224 WG 17 Progress Status, Server Signing Standard and other related Protection Profiles [illegible]	Biometrics Evaluation and Testing [illegible]	CC and Smart Grid Lessons learned [illegible]
09:30	Common Criteria in 5 years time: what uses might we see? A personal view for discussion [illegible]	Security Evaluation of Communication Protocols in Common Criteria [illegible]	Legal regulations and independent vulnerability analysis [illegible]
10:00	Technical Communities Theory and Practice [illegible]	Computer Network Defense PP's [illegible]	Electronic Signature Conform to the CC Anytime, Anywhere, with any Device [illegible]
10:30	COFFEE BREAK - GRAND FOYER		
11:00	*Closing Plenary - A / Modigliani*		
	Closing Plenary "Roundup of events at the ICCC" [illegible]		
11:30	Closing Speech [illegible] *General Director, ANSSI, France*		
12:00	Conclusion words from CCMC Dag Ströman, *CCMC Chairman*		
12:30	Announcement of the 14th ICCC		
13:00–14:00	LUNCH / RESTAURANT		
14:30	END OF ICCC 2012		

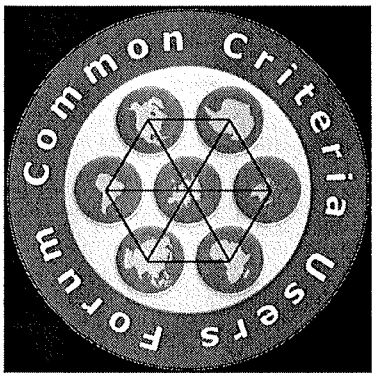
ICCC
PARIS, 18-20 SEPTEMBER
2012
INTERNATIONAL COMMON CRITERIA CONFERENCE

肆、研討會摘述

一、管委會報告

由 CCRA 管委會(Management Committee；MC)主席 Dag Ströman 先生報告，重點摘要如次：

(一) 管委會同意成立共同規範使用者論壇(Common Criteria User Forum；CCUF)，作為正式交流聯繫平台，該交流聯繫將由 DB 主席負責管理。管委會鼓勵 CC/CCRA 有關者加入 CCUF。該論壇標誌為



(二) CCRA 過去活動，在相當程度上，一直專注於發展 CC/CEM 及在體系中調和 CC/CEM 的應用。今為增加 CCRA 參與者的利益，將透過參與 CCRA 的政府機構、產品供應商和實驗室之合作，促進保護剖繪（protection profiles；PPs）的發展。目前已有一些國家將 PP 作為採購目的。為調合 CCRA 參與者應用 PP，管委會已同意適當管理 PP 的基本架構，以確保 PP 能成為公平競爭的工具。未來 CCRA 執行重點，包括：

1. 在不衝擊產品價格與時效性下，一般 ICT 市場現貨（COTS）產品的安全等級須被提昇。
2. 藉由建立技術社群(Technical Communities；TC)去發展「合作的保護剖繪(collaborative Protection Profiles；cPPs)」及相關證實文件，來增

強標準化的水平，達到合理、可比較、能複製及兼具成本效益評估的結果。

3. 理想狀況，每一技術領域由一個 TC 主導，其範疇應被明確定義，且能建議 cPPs 使用於政府採購上。TC 將由下列單位代表共同組成：

(1) 國家政府

A. 使每一 cPP 有最大接受度

B. 限制每一技術領域可提供的 cPPs 的數量

C. 分攤 cPP 發展的成本

(2) 在 cPP 範圍內的產品供應商

A. 包含最先進的技術

B. 提昇公平競爭

C. 最大化符合性產品之接受度及數量

(3) 被 CCRA 認可的 IT 安全評估場所

A. 提供實驗室間的一致性

B. 同意有效的保證行為

4. 會員國相互承認應基於 cPPs 可達到的一般水準。

5. cPPs 應為多個供應商對相似產品提供個別 STs 做優先處理。

6. 在任何可適用的時候，cPPs 應被用來代替個別的 STs。

7. STs 的應用應被保留在 cPPs 不存在或者不適用的案件，及 CCRA 相互承認應局限於 EAL 2。

8. 應將 CC 當成「功具箱」來發展 cPPs。

9. 原則上，沒有 CCRA 的相互承認是超過 cPP 等級的。超出 cPPs 評估等級者應被保留，而該等情況為：

(1) 國家的要求

(2) 個別利害關係者間的協議，諸如：

A. 國與國的雙邊協議

B. 資訊系統資深官員小組的相互承認協議(Senior Officers Group for Information Systems, Mutual Recognition Agreement SOGIS-MRA)及其他類似的協議。

10. cPPs 和/或證實文件將處理弱點分析的要求，以確保驗證產品達到預期的安全等級。

另 CCRA 發展董事會（CCRA Development Board；CCDB）將要求 CCRA 管理委員會認可每一技術領域，當 cPP 透過投票程序同意後，CCDB 接受被提出的 PP(包含證實文件)。被 CCDB 所接受或指定的 TC，負責 cPPs 及證實文件的產出及事後維護。

(三) CCv3.1 revision 4 正式發布，該與 revision 3 之主要差異，在於修正 PP 所含假設（assumption）刪除或增加的條件，以使 PP 的應用更為明確：

1. 如果處理假設的操作環境其所有安全目的（security objectives）可被評估標的（Target Of Evaluation；TOE）的安全目的置換時，該假設能被刪除。
2. 如果給予適當理由說明，新的假設為何與之前 PP 處理降低威脅及履行組織安全政策（Organizational Security Policy；OSP）無關時，該假設能被增加。

二、CC 評估的脈動

隨著行動通信服務的普及（目前估計約有 50 多億行動用戶），行動通信相關資安議題越發為世人重視，成為 CC 推動的新亮點。

(一) 在通信系統方面－以 3GPP 為例：

【現況】

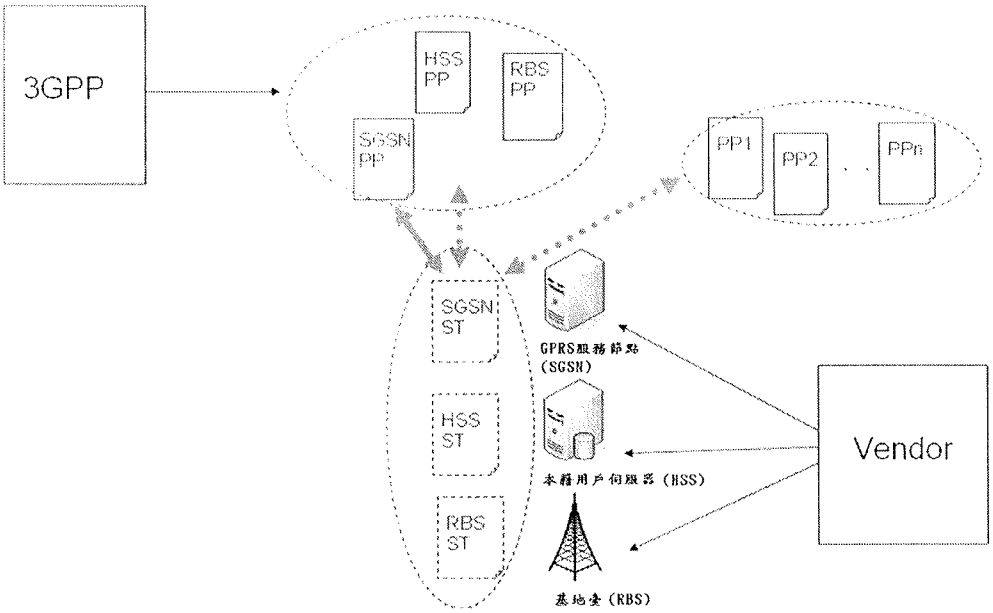
1. 有定義空中介面、IP 傳輸介面等保護機制。
2. 未定義全部的威脅情境等級。
3. 未定義網路安全的承諾規範。

【推動】

3GPP 同意分析與評估電信產品及其定義的網路功能，有關資安保證的適合性，其進行方式如次：

1. 以 CCRA 使用的方法與定義去評估適用性。

2. 與 CCRA 建立聯絡管道，以了解 CCRA 相關程序與範疇。



(二) 在通信終端應用方面－以 Smartphone 應用（Apps）為例：

評估標的（Target of Evaluation；TOE）範疇包括：

1. 安全功能

A. 資料移入（Data import）：透過 OS 以剪貼簿方式複製

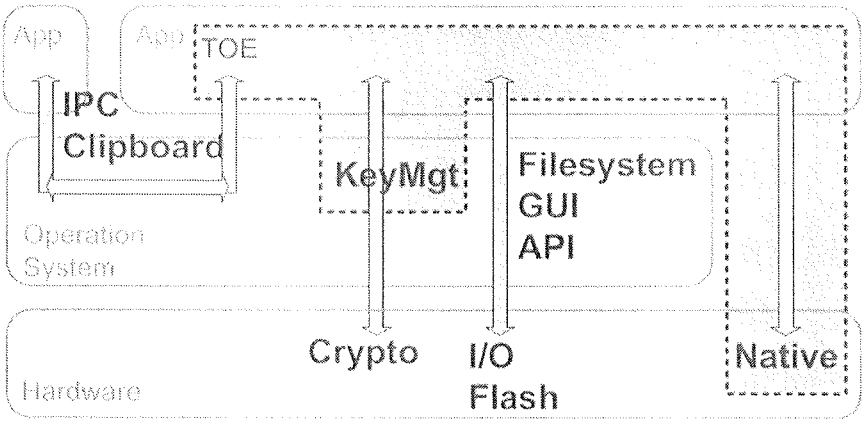
B. 密鑰管理(Key management)：經密碼演算產生密鑰由 OS 管理

C. 加密儲存（Encrypted storage）

2. 環境

A. 存取控制與隔離

B. 行動裝置的管理



三、CC 評估的改進

（一） 為降低共同準則評估工作之無效負擔，減少非必要的文件化工作。在研討會中，有與會者倡議修正 TOE 之安全功能(TOE Security Functionality；TSF)介面（interface of the TSF；TSFI）定義為：

「藉由外部實體提供資料給 TSF 的介面（means），從 TSF 接收資料的介面及從 TSF 請求服務的介面」

即攻擊者有可能存取及/或 SFR 被溯及的介面，原委臚列如次：

1. TOE 形態包括操作系統、網路設備及智慧卡或智慧卡相關設備等，但大部分的 TOE 僅包含部分有效 TSF，而非全部。
2. 若依現在 CC Part1 1 / CEM 檢測標準－包含設備所有 TSFI 或參照 CC Part 3 Annex A.2－針對潛在攻擊者可能存取的 TSFI，均有過猶不及的缺點。

若依上述定義修正，經實案檢測，確有節省時間及評估者可專注於產品安全方面之優點：

CC	影響	
	發展者	評估者
ADV_FSP	非 TSFI 介面文件化的細部要求大量減少	降低評估工作負擔
ATE	有較少的 TSFIs 去做測試	降低評估工作負擔

（二） CC 的安全評估保證等級（Evaluation Assurance Levels；EALs）考量有下述缺點，在研討會中，有與會者倡議 TC 製作較佳的標準 PP：

1.許多 CC 的評估無法確保一致性。

2.即使產品通過高階 EAL，亦存在有弱點。

有關製作標準 PP 的建議規則，分列如次：

1.每一 PP 應符合 CC 保證保護剖繪評估（Assurance Protect Profile Evaluation；APE）的要求。

2.每一 SFR 應被測試。

3.每一保證活動要求的元件或成分應明確。

4.每一保證活動應僅針對有相關的一特定評估層面。

5.每一保證活動應被客觀陳述，並確認該活動適用的投入、動作與產出。

6.每一保證活動不應要求客戶投入超出 ST 的東西。

7.每一保證活動應被設計具成本效益且有意義。

8.每一保證活動應被設計只能被 CC 測試實驗室操作，以能得出評估結論。

9.每一保證活動不應延伸 TOE 功能要求。

四、與他國交流

研討會期間，本會代表與日本及德國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資安產品驗證的發展現況，亦與中國信息安全認證中心人員進行了解。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. Matsutoshi Murata (村田松壽)

	Mr. Fumiaki Manabe (真鍋史明)
中國信息安全認證中心	魏昊主任
德國 TÜViT 實驗室	Mr. Antonius Sommer

交流內容摘述

（一） 日本驗證主管機關(IPA)代表表示，該國對中小企業（SMB）採購 IT 認證產品，提供減稅優惠之誘因，該作法可為我國目前推動資通訊產品安全驗證之參考。另為發展日本多功能事務機（Multi-Function Printer；MFP)的 PP，該國於今年 3 月成立 TC，由 MFP 供應商與政府單位組成，並規劃未來將該 PP 草案送進 CCUF 討論，以發展成 cPP，能被 CCRA 成員使用。我方對日方推動資安產品認證手法之細膩，深表欽佩，且表示我方擬以政府機關率先採購之方式，去活絡相關產品驗證之進行。

（二） 中國大陸代表表示，大陸產品認證主管機關為中國國家認證認可管理委員會（CNCA），該委員會指定中國信息安全認證中心（ISCCC）為其資訊安全產品驗證機關（certification body），並指定中國信息安全測評中心（CNITSEC）、國家保密局涉密信息系統安全保密測評中心、信息產業部計算機安全技術檢測中心等 7 資訊安全產品驗證實驗室，而部分中心有其項下授權之實驗室。大陸有防火牆、安全路由器、反垃圾郵件、網路弱點掃描等 13 種資安產品需強制驗證，且有些驗證亦分為基礎型與進階型兩類，該與我國刻正推動的資安產品驗證方式相似。

（三） 德國 TÜViT 實驗室高階主管詢問我國刻正推動之資通訊產品安全驗證相關進度，及其與我國驗證實驗室合作驗證資安產品是否被認

可等問題，經說明後，該主管甚表高興，足見該實驗室對我國資安產品市場前景的樂觀與期盼。

伍、心得與建議

此次交流活動，讓吾等了解資通設備安全檢測之趨勢與作法，其中包括 cPP 的產生、如何降低共同準則評估工作之無效負擔等，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：

一、 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。

二、 積極推動我國資通訊設備產品驗證

（一） 加強推動本會認可的資通安全設備列於政府採購共同供應契約規範

出席本次會議發現，CCRA 會員國漸有將保護剖繪規格與政府採購掛勾之趨勢，該作法頗有政府為領頭羊之意，準此，我國欲發展資安產業，可從推動政府部門採購相關產品著手，應有事半功倍之效。

（二） 持續制定能與國際接軌的資通設備檢測規範

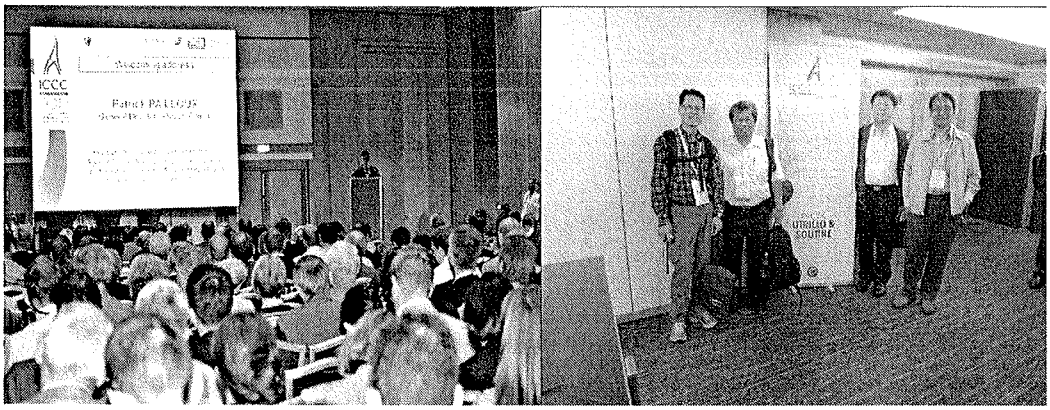
出席本次會議發現，CC 評估有朝行動相關產品之趨勢，本會雖於 100 年完成防火牆設備、入侵偵測防禦設備、防毒閘道器設備、垃圾郵件過濾設備、網頁應用防火牆、應用軟體控管系統、乙太網路交換器、路由交換器等 8 項資通設備安全檢測技術規範。惟該 8 項資通設備仍不足因應全面提升我國資通設備環境安全之所需，且為避免閉門造車，應配合國際檢測脈動，增訂其他資通設備安全檢測技術規範。

（三） 檢視現行資通設備安全檢測技術規範

出席本次會議發現，CC 新修正版本正式出爐，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，準此，對該等規範有再檢視之必要性。

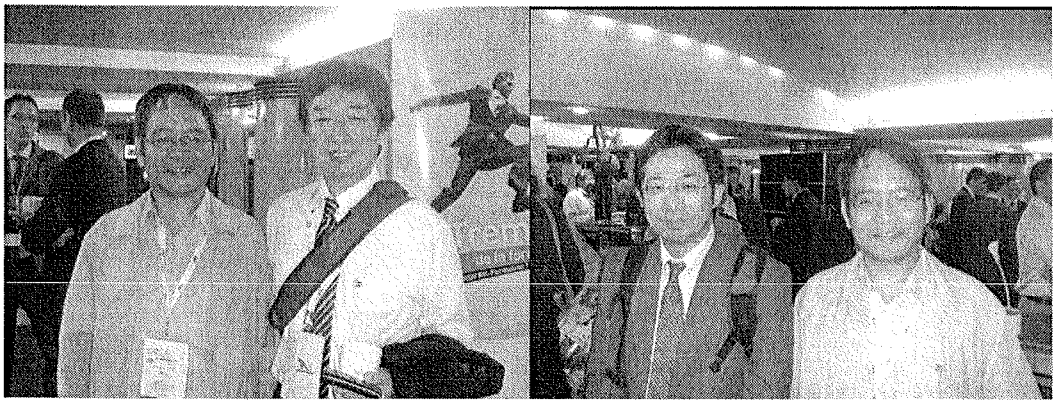
陸、照片

1_會場



▲13thICCC 會場

2_交流



▲與日方代表交流

▲與大陸代表交流　　▲與德國 TÜViT 代表交流