出國報告（出國類別：開會）

出席 2018 年第 17 屆國際共同準則研討會（ICCC 2018）

服務機關	姓名/職稱
國家通訊傳播委員會	劉邦灶 技士
財團法人電信技術中心	徐瑋辰 副工程師

派赴國家： 荷蘭阿姆斯特丹

出國期間： **107** 年 **10** 月 **29** 日至 **11** 月 **3** 日

報告日期： **108** 年 **1** 月 **22** 日

摘要

第 17 屆國際共同準則研討會議(International Common Criteria Conference, ICCC)自 10 月 30 日至 11 月 1 日於荷蘭阿姆斯特丹假希爾頓飯店舉行，由 NSCIB 主辦。本次會議有 34 個國家、200 個來自驗證機構、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組織，匯集了 342 位 ICT 系統安全領域專家參加。本次會議議題分為「共同準則的使用進展(Advance in the Use of Common Criteria)」、「符合客戶要求(Meeting Customer Requirements)」、「驗證體制與國際技術社群的發展近況(Updates from Schemes and iTCs, International Technical Communality)」與「保證(Assurance)」共 4 大類別主題，共有 64 個討論議題。此外，本次會議適逢歐盟即將推動網路安全法(EU Cybersecurity Act)案，將對 CCRA 的互相承認體系產生相當程度影響，所以有不少討論圍繞這個議題。

ICCC 是一個經驗共享的技術會議，為政府代表、安全驗證機構與實驗室及 IT 產品和系統安全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，作為我國規劃資通安全相關政策參考。

目錄

圖目錄

表目錄

壹、 目的

由於早期各國採用之標準安全政策不一，產品製造商通常需要付出高額重複驗證成本。為確保 IT 產品有一致的標準、提高評估和認證/驗證 IT 產品及安全規格之效率與成本效益，共同準則標準（Common Criteria for Information Technology Security Evaluation，CC）因應而生。目前 CC 在 2017 年 4 月公告 CC 3.1 版第 5 個修訂版，共同準則相互承認協議（Common Criteria Recognition Agreement，CCRA）有 28 個會員國相互承認 CC 驗證。

而我國近年持續推動各項設備之安全檢測規範，國家通訊傳播委員會（NCC）自 2010 年至 2013 年推動之「資通設備之安全檢測研究計畫」時，提出網路行防火牆、無線接取設備等 10 項安全檢測規範，後於 2017 年公告「智慧型手機系統內建軟體資通安全檢測技術規範」，也與經濟部共同發布 IoT 設備資安驗證標章制度。而國際間政府(如美、歐、澳、馬來西亞等)採購資通設備時，將資訊安全評估納入需求規範中，是我國政府可效法之處。

國際共同準則研討會議（International Common Criteria Conference，ICCC）是由 CCRA 會員國每年輪流主辦一次，主要目的是藉由 CCRA 各會員國之間經驗分享與交流，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通安全議題，討論如何發展更安全的資通安全基礎環境。

藉由參加 ICCC 研討會，可了解目前國際間產品安全驗證制度及資通安全防護政策近況，掌握資通安全技術發展及未來趨勢，作為我國制定資通安防護政策、強化資通安全驗證體系、提升資通安全驗證能力及完備驗證作業程序之參考。

貳、 過程

一、 共同準則相互承認協議介紹

共同準則相互承認協議（Common Criteria Recognition Agreement，CCRA）是為了實現 CC 目標，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 ICT 產品及保護剖繪（Protection Profile，PP）獲得 CC 認證後，使用者在購買或使用這些產品時，了解該產品確實符合需求。

CCRA 目前共有 28 個會員國，已申請成為「證書承認會員國」（Certificate Consuming Members，CCM），計有丹麥、奧地利、捷克共和國、希臘、匈牙利、巴基斯坦、芬蘭、以色列、衣索比亞、卡達、新加坡等共 11 個國家。目前已申請成為「證書核發會員國」（Certificate-Authorizing Members，CAM），計有加拿大、美國、法國、德國、英國、荷蘭、澳大利亞、紐西蘭、挪威、瑞典、西班牙、義大利、土耳其、日本、韓國、馬來西亞，以及印度等共 17 個國家。

證書核發會員國 CAM　　證書承認會員國 CCM

圖 1、CCRA 成員國

CAM 指具有 CC 驗證產品安全能力，並可核發驗證證書，此證書是受 CCRA 承認，而 CCM 接受 CAM 核發 CC 證書的 ICT 產品，無須再經其國內驗證機構核證。也就是說，經過 CAM 所授權核可通過 CC 驗證的產品能獲得 CCRA 會員國的認可與採用，以免除開發廠商重複送驗之不便，與降低驗證成本及提升商業競爭力。

二、 重點議題

ICCC 2018 議程有 4 大類研討會（會議議程請參考附件一）－「共同準則的使用進展」、「符合客戶要求」、「驗證體制與國際技術社群的發展近況」與「保證」。本次主要參加「驗證體制與國際技術社群的發展近況」研討會，除更新 CCRA 發展近況外，也了解美國、日本、英國、荷蘭等國家 IT 產品安全驗證體制，另

選擇政府採購納入 CC 要求研析與 CC 自動化驗證等議題參加，進一步了解 CC 推行、問題及可能解決方案。

2.2.1 CCRA 更新

CCRA管理委員會（MC）的主席Dag Ströman報告CCRA的進展。目前CCRA各委員會主席如下：

表格 1、CCRA 各委員會主席一覽表

CCRA委員會	**主席**
管理委員會(Management Committee, MC)	瑞典Dag Ströman
執行委員會(Executive Subcommittee, ES)	土耳其Tunga Gökhun
發展委員會(Development Board, DB)	西班牙David Cerezo
維護委員會(Maintenance Board, MB)	德國Susanne Pingel
	韓國Eunkyoung Yi

CCRA成員持續增中，目前有2個國家表示有興趣加入CCRA；有2個國家申請成為CCRA成員，現進行投票中；而有1個國家正在製定計劃，並申請改變成為CAM。至於CCRA成員會定期自願性進行評鑑，韓國、荷蘭與挪威在2018年已完成同行評審（Peer Review），瑞典、美國與土耳其將於2019年執行。管理委員會MC、執行委員會ES及發展委員會DB主席職位將採CAM成員義務輪替，而CCM成員也可自願擔任。未來ICCC會議規劃如下：

表格 2、ICCC 未來會議規劃

會議時間	**會議地點**
2019年第2季	尚待確定
2019年第3季	尚待確定
2020年第2季	馬來西亞
2020年第3季	西班牙

另外，歐盟網路安全法草案，其中訂定了網路安全框架（Cyber Security Framework，CSCF），讓歐盟有了一致性IT產品安全驗證體制。Dag表示，CSCF將對全球ICT產品安全市場產生重大影響，因為近一半CCRA成員為歐盟

成員國，這意味著受到CSCF將直接影響CCRA，非歐盟之CCRA成員國也可能受到影響。

歐盟CSCF推行與CCRA運作未來要如何磨合存在許多不確定因素，但可以預期這些因素具有重要意義。資訊通信技術中的資訊技術安全認證標準問題以及全球市場上的相互認可是一個非常大而復雜的問題，這需要一些時間和精力來梳理。CCRA MC將繼續監督和分析發展，並高度歡迎與歐盟委員會和ENISA建立對話。最後，主席Dag重申CCRA目標：

- 確保評估資訊技術（IT）產品和保護剖繪（PP）能有高且一致的標準，並為產品安全的信任作出重大貢獻。
- 提升通過評估、安全性高的IT產品及保護剖繪的可用性。
- 消除重複評估IT產品和保護剖繪的負擔。
- 不斷改善IT產品和保護配置文件之評估和認證/驗證程序的效率和成本效益。

2.2.2 CCDB 更新

共同準則發展委員會（Common Criteria Development Board, CCDB）主席 David Cerezo 與英國驗證體制代表 David Martin 報告近況，略述如下：

- 提升證書效力：由法國主導，工作小組持續努力中。
- iTC：引導新創iTC與相關CCDB工作小組溝通。
- 支援文件核准流程：由第一個驗證單位進行審核。
- CCMB：定期進行支援文件審查，並於CCDB會議中報告。
- 與ISO聯絡：關注ISO SC27 WG3中的標準制定工作，並討論標準的版權議題。
- CC Portal網站更新：核准一個輕巧但仍受制的資訊發布流程。

2.2.3 CCUF 更新

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

Fiona 報告近況。Fiona 首先說明 CCUF 主要任務是提供 CC 社群和 CC 各委員會、各國驗證體制代表和政策制定者之間的溝通與通信管道。而目前 CCUF 成員近 800 名，來自於 298 個不同組織，其中產品開發商占大宗（42%)，CC 檢測實驗室次之（29%)，而其中有 5%的成員並非來自於 CCRA 會員國或歐盟 SOG-IS（Senior Official Group Information Systems Security）成員。

在人才培育方面，CCUF 提供輔導及培訓新進成員，並提供介紹素材、與大學和學院合作、鼓勵新生代參與等。目前正進行的工作包含測試自動化、PP 編輯器、CC（或 ISO）新開發工具的測試等。

2.2.4 歐盟網路安全驗證框架

歐盟網路與資訊安全局（European Network and Information Security Agency，ENISA）的營運處處長 Steve Purser 以「在歐盟網路安全驗證框架（CSCF）中率先開展合作」為題，講述歐盟網路安全法案若通過，CSCF 驗證要求、CSCF 可能的特徵、問卷調查的發現與 ENISA 在其中扮演的角色。

Steve 首先提出一個概念－網路安全經濟，意即網路安全將變成經濟政策。然而，安全評估的困難之處在於不同的產品進行安全評估時，應用到的檢測工具截然不同。安全與使用情境（context）是緊密關聯的，例如，產品開發環境的安全管理與音樂 CD 的資訊安全需要截然不同的安全要求。此外，車聯網、量子電腦等新興科技發展也將會再掀起一波安全挑戰。

產品安全驗證現行是由 CC 主導，而歐盟 SOG-IS 相互承認成員（SOG-IS/MRA）是共同標準認證的主要參與者，歐盟多國及跨部門倡議聚焦於安全議題。而 ENISA 從問卷調查中得到：

- 57%（的受訪者）知道現有多個 ICT 產品安全驗證體制
- 遇到主要問題：成本、驗證時間、透明度和支援需求。
- 90%認同歐盟級的相互承認是有必要的。
- 66%認同需要自我聲明體制（Self-Declaration Schemes）。
- 物聯網（75%）和 ICS（66%）領域產品是需要驗證和標籤。
- 81%認同驗證和標籤可成為提高透明度和增強信任度的有效工具

- 66%強調需要加大力度促進特定部門的 ICT 安全驗證
- 78%認為現有歐盟委員會機構如 JRC，ENISA，ACER 可在未來歐盟的方案發揮作用。

網路風險不斷增加情勢下，ENISA 於 2018 年 5 月提出歐盟的網路安全法草案（Cybersecurity Act，CSA），授權 ENISA 成為歐盟永久機構，強化 ENISA 的權力，建立一個歐洲網路 ICT 產品安全驗證框架（即 CSCF），CSA 主要目的在於歐盟內提供網路彈性及應變能力，協調各標準提升效率，以達成符合歐盟數位單一市場（Digital Single Market）戰略核心。

歐盟 CSCF 的任務包含：

- 避免多重國家 ICT 產品安全驗證體制所造成零散和複雜。
- 促進相互承認。
- 簡化程序，以降低 IT 產品和服務的時間成本。
- 提高歐洲 ICT 產品和服務的競爭力
- 讓使用者對 ICT 產品和服務更具信心。

ENISA 在驗證方面的首要任務是依據 CSA 建立 CSCF，所以將密集進行相關活動，包含支持政策討論、與利益關係者對話、與產業建立合作關係、盤點制定歐盟 ICT 安全驗證和標籤框架、分析歐盟 ICT 安全驗證實驗室，以及促進既有體制轉移到歐盟框架並適時回應新興輕量型（lightweight）安全要求的需求。最後，Steve 表示，在安全的世界沒有一個正確的解答，而是因應不同的情境，去量身訂做合適的安全要求。

而同樣來自 ENISA 的 Matthias Intemann 則說明 CSA 現況及 CSCF 與 CC 需要磨合之處。CSA 最早在 2017 年 9 月歐盟委員會提出（EU Commission），於 2018 年經歷歐盟理事會（EU Council）和國會（EU Parliament）討論，預計於 2018 年底經歐盟國會核准通過。

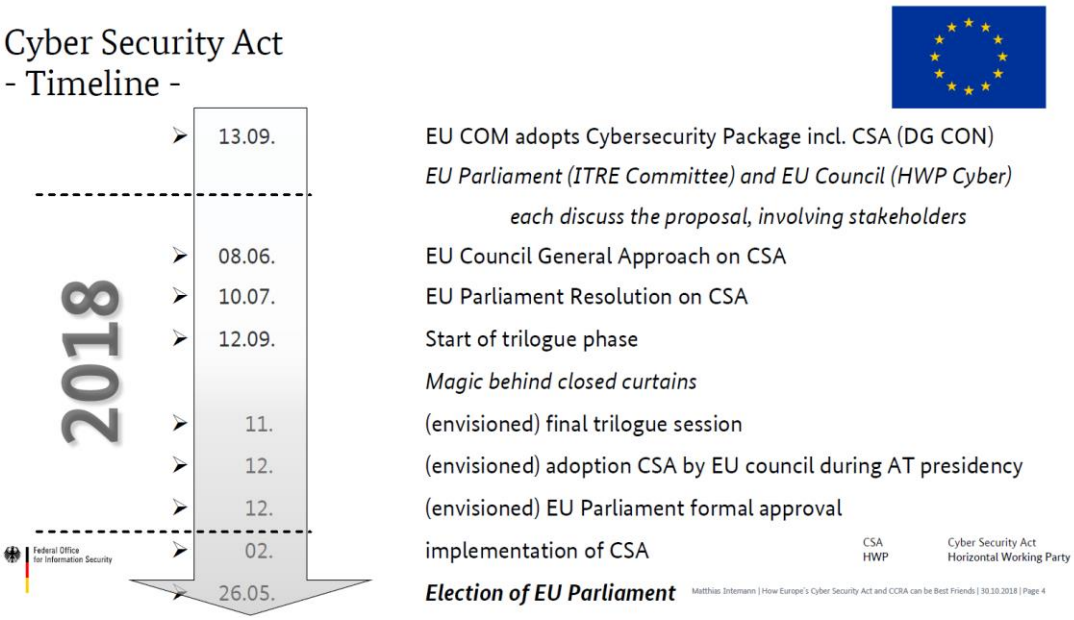


圖 2、歐盟網路安全法 CSA 草案時程

Matthias 也點出 CSA 與 CCRA 間的差異，包含了保證等級認定、相互承認方式、定期審查機制、弱點通報義務、保護剖繪運應等。因為，CCRA 有半數成員是歐盟成員國，考量 CCRA 能在歐盟順利運行，期待 CCRA 能夠進行調整。

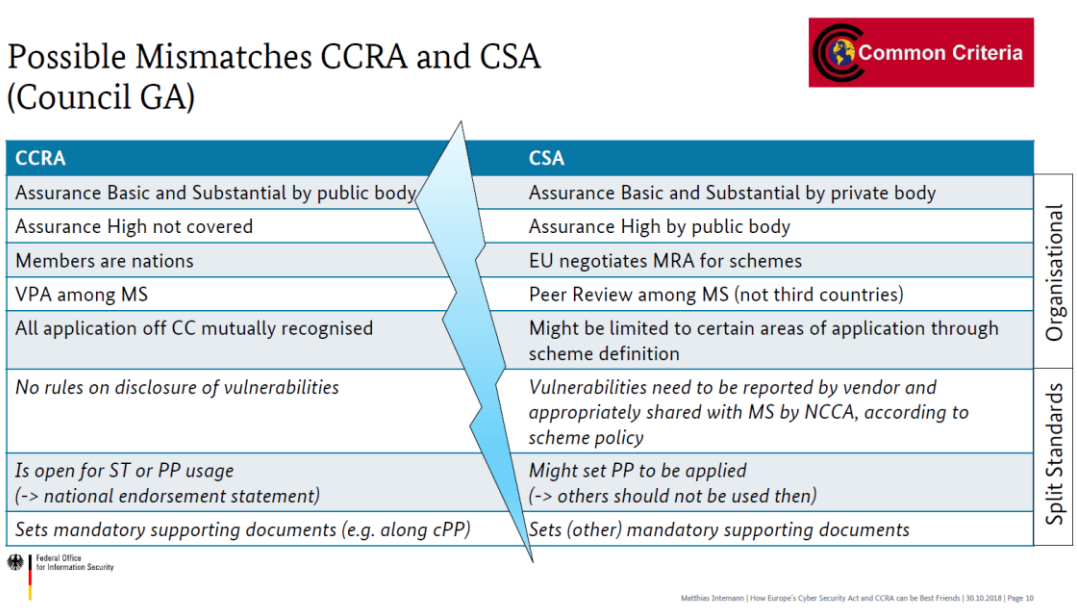


圖 3、CCRA 與歐盟 CSA 相異處

2.2.5 英國脫歐對 CC 驗證體系的影響

英國在 2016 年 6 月脫離歐盟的全民公投，以些微差距決定了英國「脫離歐盟（Brexit）」之路，這項選擇是期待英國能夠不再受歐盟法律、歐洲單一市場及若干

自由貿易協議約束，並可取回對移民政策的控制權。這對現行歐盟 SOG-IS/MRA 高度相互承認架構，及 CC 也會造成一定程度影響，而英國也需重新思考驗證體制及洽談相互承認協議 MRA。而相較 EU 正如積極推出 CSA 及 CSCF，已有了明確合理的安全驗證架構，英國目前尚未有明確架構及政策方向，講者還風趣的以大霧瀰漫景色解釋目前英國處境。

圖 4、英國處境示意圖

2.2.6 美國驗證體制更新

美國 CC 驗證機構(CB)為美國國家資訊安全保障合作組織（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（CAM），美國境內是所有會員國之中擁有檢測實驗室數量最多的國家，目前已經擁有 10 家 CC 標準檢測實驗室（包含 Acumen、atsec、Booz Allen Hamilton、CGI、COACT Inc.、CygnaCom、DXC、Gossamer、UL 與 Leidos）。

美國 NIAP 主任 Mary Baish，以「美國 CC 計劃更新」為題，講述 NIAP 的經驗與統計數字、主動參與各項活動、共同努力使用 PP 提升資訊安全、自動化工作的推展與如何透過技術社群推動共同準則等議題。

美國自 CC 標準成立以來，積極投入資源發展及通過產品驗證，根據 NIAP 統

計數據，經美國驗證符合 CC 標準產品為 158 件。而 NIAP 也積極參與如 CCRA、ISO、NATO、iTC（NW，FDE，App，DSC，USB，生物識別）等國際組織及技術社群，於 TC 中代表 50 多個技術部門。此外，NIAP 努力推動 PP 標準，參與 CCRA 的合作保護剖繪（collaborative PP）文件研擬，將美國自身制定的 PP 轉化為 cPP。

縮短 CC 測試時間是 CCRA 共同努力的目標，NIAP 正研發如何自動產生 PP 與安全目標 ST（Security Target）文件；NIAP 也對軟體應用程式及網路設備 cPP 的測試進行自動化。

美國國防部、白宮和國家安全系統皆有採購 CC 驗證通過的產品，根據 NIAP 統計，自 2017 年 9 月以來，通過 PP 評估且用於美國國家安全系統的產品成長了 17%，其中網路設備占大宗(65%)、其次為應用程式(12%)、外圍共享交換器(8%)，而其他美國政府機構正與 NIAP 合作，美國政府採購政策明確實現了對 CCRA 的承諾。最後，Mary 說明 NIAP 目前著重於為行動裝置、網路監控、隔離(separation)與資料保護等技術領域。

圖 5、美國 NIAP 著重領域

2.2.7 荷蘭驗證體制更新

荷蘭驗證方案的 Rob Huisman 以「NSCIB 與 BSPA—荷蘭 IT 安全驗證體制」為題，介紹了荷蘭國家通訊安全局（Netherlands National Communications Security Agency，NLNCSA）任務、荷蘭資訊技術安全領域的驗證體制（NSCIB）、基線安全產品評估機制（BSPA）介紹與荷蘭運行的 3 種驗證體系。

NLNCSA 透過於發展和驗證安全產品，協助荷蘭政府保護機敏資訊，監督 NSCIB 運行，而 NSCIB 是一個商業性的驗證體制，目前委由 TÜV Rheinland Nederland 公司營運。

NSCIB 目前有 64 個有效的 CC 驗證產品，其中以 IC 智慧卡（39 項）為大宗，其次分別邊界保護設備（6 項）、數位簽章（5 項）等。就產品取得 CC 保證等級分布而言，有 21 項產品為 EAL4/EAL4+，為最多數。

產品經過驗證上市時間（throughput）取決於評估標的的範圍大小和類型，也與開發人員的熟練與專業有關。以一個 EAL4 + VAN.5 而言，對於有經驗的開發廠商備齊開發者證據的狀況，約 3~5 個月可以拿到證書。從評估技術報告(ETR)草案送達 NSCIB 後，NSCIB 平均 1 個月核發證書，但也需考量與廠商的準備程度與實驗室評估過程，因此產品開發商必須承受相當程度時間和成本耗費。而基線安全產品評估（Baseline Security Product Assessment, BSPA）則是一個 NLNCSA 驗證輕量級的替代方案，提供較低的驗證時間（最久 8 周）及費用（最高 4.5 萬歐元）選項，目前適用範圍包含網路安全、網路過濾、安全訊息、媒體與檔案安全、身分識別與存取控、安全作業系統、硬體與嵌入式、智慧卡等 8 類產品。

基於政府與通用目的與其安全等級需求不同考量，NLNCSA 資訊安全驗證方案分別為 NLNCSA 國家評估、BSPA 評估與 CC 評估。NLNCSA 屬於機密等級以上使用的方案；而非機密等級則採用 CC 評估與 BSPA 評估。

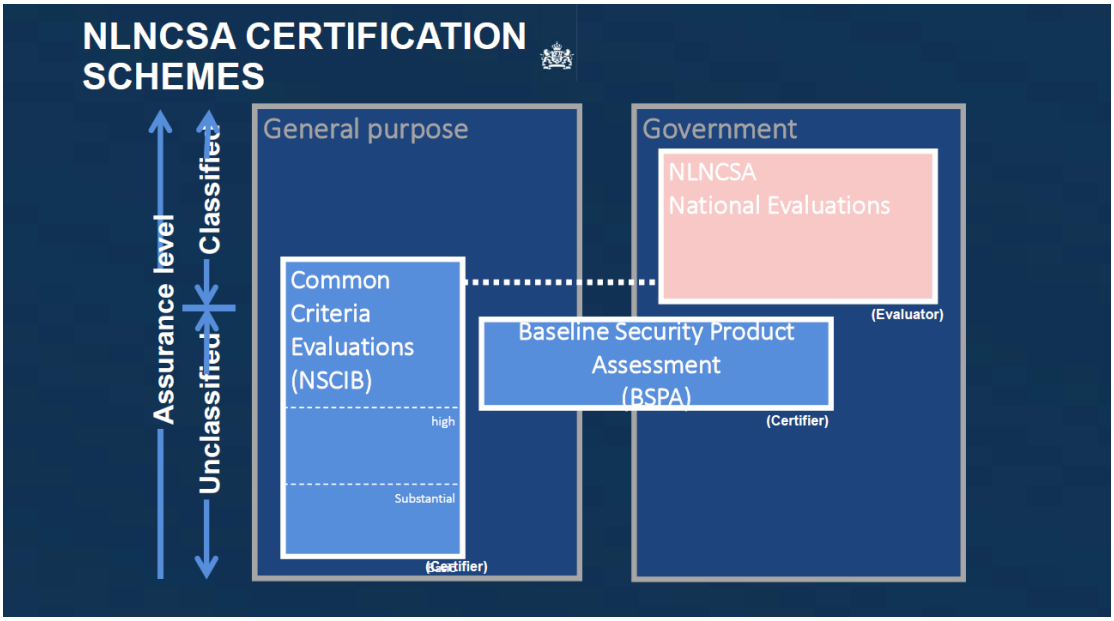


圖 6、荷蘭產品安全驗證架構

2.2.8 日本驗證體制更新

日本 IT 安全評估與驗證體制(Japan IT Security Evaluation and Certification Scheme，JISEC)代表松本人志（Hitoshi Matsumoto）介紹日本 IT 促進局（Information-technology Promotion Agency，IPA）、JISEC 及近期活動與更新。

IPA 是依據日本信息促進法於 1970 年成立，與經濟產業省（METI）進行合作，後於 2004 年重組為獨立行政法人。IPA 宗旨為促進 IT 安全和提高資訊處理系統的可靠性與發展 IT 人力資源，以實現「可靠的資訊社會」的願景。IPA 轄下設有 IT 安全中心（ISEC）的，負責收集廣泛網路安全資訊，經分析和整合資訊後，提供大眾充足有用的資訊和工具，並發展安全政策措施。

日本認證機構是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 IPA。日本於 2004 年加入 CCRA 成為授與證書會員國 CAM，目前境內有 4 家檢測實驗室。

日本 IT 產品採購政策先由 NISC 制定政府資安標準，METI 列出確保 IT 產品採購所需安全要求清單，CC 產品驗證則由 IPA 運行。而安全要求清單涵蓋了資料庫管理系統、防火牆、IDS / IPS 、多功能事務機、伺服器作業系統、智慧卡/ IC 卡等 6 大類型產品，METI 在 2018 年增加了 5 類產品，包含 USB 可

攜式存儲器、路由器、全驅動加密 HDD、行動裝置管理以及 VPN 等。

JISEC 的 CC 驗證產品以影印機為大宗（76%）、次之是 Middleware（8%），在 2017 年經過驗證產品，以 EAL2 最多（37 張）、次之為 EAL 3 和 EAL 1（各 4 張）。在 2017 年通過的產品，平均驗證所需時間為 12 個月，最久 23 個月，最快 3 個月取得證書。

另外，日本正研製新型交通卡 Suica，已取得 EAL 5+證書，可以用來搭乘火車、東京捷運、機場快捷、東京 monorail、Toei 公車等交通工具、可以用在購物時付款，也兼具有信用卡功能。此外，日本也正在計畫推出新一代護照，新版將兼容舊版護照，並採用新型安全訊息技術（PACE v2）及具有防覆寫能力。

2.2.9 馬來西亞驗證體制

馬來西亞 CC 驗證實驗室 CyberSecurity 的 Zarina Musa 以「為馬來西亞市當地場改造共同準則」為題，介紹馬來西亞 CC 評估與驗證體制（MyCC）、產業對於 CC 驗證的回饋、大馬 ICT 產品安全評估（IPSA）介紹和技術安全保證方案（TSA）的發展。

馬國網路安全機構在 2006 年（Cybersecurity Malaysia，CSM）經馬國科技創新部建置了 MyCC，而 CSM 成為 MyCC 驗證機構。MyCC 在 2007 年經 CCRA 通過成為證書承認會員國 CCP，在 2011 成為證書核發會員國 CAP。目前已有 69 項產品通過 MyCC 驗證。馬國政府藉補助鼓勵開發商取得 MyCC 驗證，並正規劃政府單位或關鍵國家基礎設施在採購 ICT 產品，需要通過 CC 驗證。

然而，國內業者對於 CC 驗證，反映耗費時間過長、費用過高，所以要求 CSM 推出一套驗證時間更短，成本更低的評估體制。因此，CSM 在 2016 年提出了一個替代方案—ICT 產品安全性評估機制（ICT Product Security Assessment，IPSA），其驗證時程較傳統 CC 驗證短，成本也更低，而且不需要重複的測試（iteration of test），測試方法參考了 CC 標準、國內標準和常見的測試方法最佳案例，， IPSA 與 CC 驗證差異對照如下表：

表格 3、馬來西亞 IPSA 與 CC 驗證比較

	CC 驗證	ICT 產品安全評估(IPSA)
專案時程	4-18 月，視評估範圍、EAL 與產品類別	1-2 月，視評估範圍而定
評估標的	ST 與 PP	客戶自行決定
測試活動	依據 CC 與 CEM 的文件審查與測試	安全功能測試與/或弱點評估
測試產出	驗證報告與 MyCC 證書	CSM 測試報告
認證效力	CCRA 國際承認	馬國國內有效

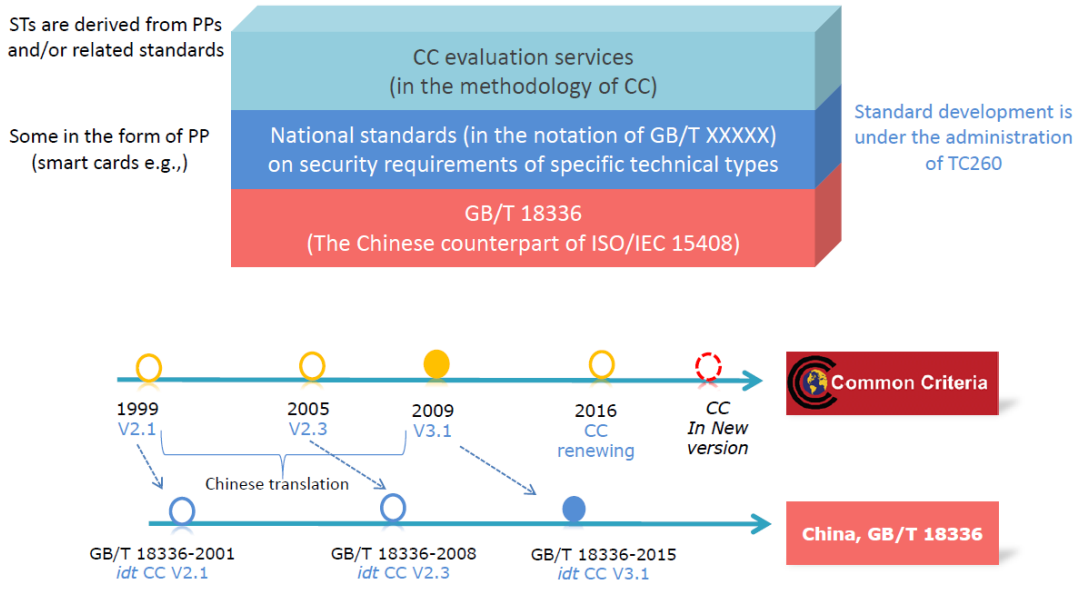
CSM 觀察到 IPSA 存在一些問題如產品安裝說明、通過與否判定，所以 CSM 在 2018 年再度提出技術安全保證機制（Technology Security Assurance, TSA），以馬國 ID 增強型生物識別讀取器作為先期試驗。目前除了前述讀取器由政府訂安全要求外，其他類型產品安全要求是經當地利害關係者達成共識而決定。TSA 每年進行 1 次維護，進行測試環境稽核。Zarina 總結表示，CC 在地化可滿足國內市場需求，但如走向國際，仍然遵循 CC 驗證體制。

2.2.10中國大陸產品安全驗證體制

中國信息安全測評中心的 Baofeng Zhang 與 Atsec 公司的白海蔚，白小姐首先聲明報告內陳述的是作者觀點，不代表相關權責單位立場。報告說明了 CC 驗證在中國大陸推展現況。

中國認證機構為中國合格評定國家認可委員會（CNAS）、驗證機構為中國網絡安全審查技術與驗證中心（CCRC）、評估實驗室則為中國信息安全測評中心和 atsec，由國家信息安全標準化技術委員會制定標準。而 CC 驗證體制在中國轉化為 GB/T 18336（與 CC 關聯及時序如下圖）。

Technical standards for CC evaluation



6

圖 7、中國驗證標準與 CC 驗證關係

目前，中國已經發布了數十個重點產品安全規格的國家標準包含了 IC 硬體韌體、讀卡機、路由器交換器、防火牆等（詳細產品類別及標準如下圖）。

National standards on specific technical types

- Dozens of security requirement focused specifications have been published as national standards
  - Some in the form of PP, using standardized security functional/assurance components
  - Others cite GB/T 18336 as a main reference, especially the security assurance framework

- IC hardware and embedded software
- Card reader
- Router
- Switcher
- Firewall
- Intrusion detection/prevention system
- Network separation system
- Operating system for Mobile terminal
- Database management system
- Security audit product
- Network vulnerability scanner
- Web application firewall
- Anti-virus gateway

Standard Number	Title
GB/T 20276-2016	Embedded software in IC card with CPU (from EAL 4+ to EAL6+)
GB/T 22186-2016	IC card chip with CPU (EAL 4+~EAL5+)
GB/T 35101-2017	Card reader(EAL4+)
GB/T 35278-2017	Mobile terminal
GB/T 33565-2017	Wireless local area network(WLAN) access system (EAL2+)
GB/T 20275-2013	Network-based intrusion detection system
GB/T 20277-2015	Network and terminal separation products
GB/T 20279-2015	Network and terminal separation products
GB/T 20281-2015	Firewall
GB/T 34976-2017	Operating system of smart mobile

7

圖 8、中國產品安全標準一覽

過去10年，中國安全產品驗證涉及了眾多領域產品如網路安全、關務、交通航運、電信、金融保險等，也包含物聯網和雲端運算等新興技術。中國自2001年起驗證了1,100多項產品，保證等級主要落在EAL2至EAL4之間（智慧卡在EAL3至EAL5+，佔1/4；其餘網路設備和其他類型產品則是在EAL1至EAL4間）。在網路設備驗證分布情形，以邊界保護設備系統為大宗，佔61%；網路相關設備系統次之，佔23%。

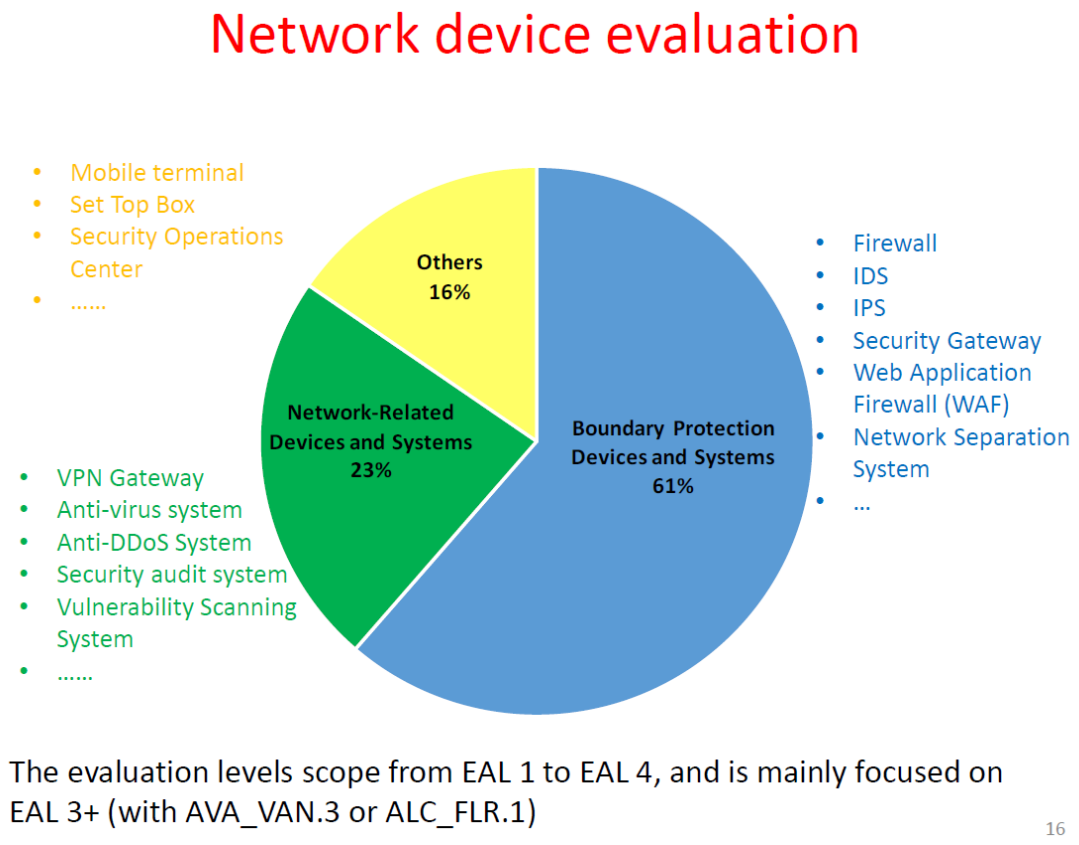


圖 9、中國網路設備安全驗證種類與分布

2.2.11俄羅斯產品安全驗證體制

俄羅斯非營利組織Echelon的Vitaly Varenitsa分享俄羅斯的CC驗證發展現狀。俄國聯邦技術和出口管制局（FSTEC）負責執行國家安全領域相關政策，並為俄國產品驗證單位。俄國自1995年成立以來政府強制要求如防火牆、存取控制系統、源碼分析、防毒軟體、IPS/IDS、可移除式儲存保護裝置、作業系統等安全設備/系統通過驗證。

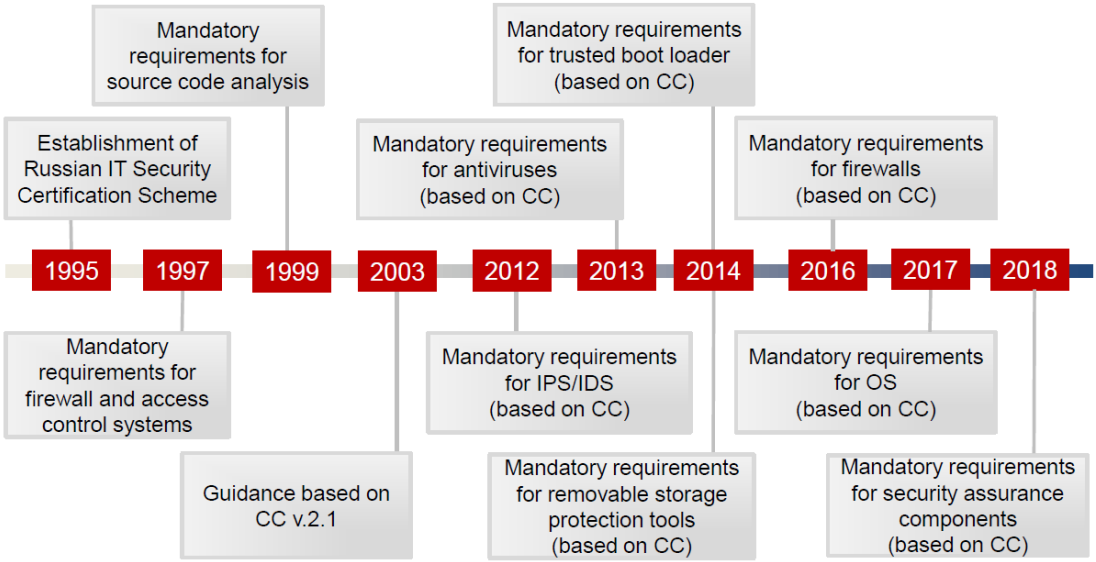


圖 10、俄國產品安全要求歷程

首先是俄國FSTEC傳統驗證體制近況，目前俄國取得認證的評估實驗室有24家、驗證機構有9家，進行安全功能評估和未宣告功能評估。驗證通過產品分布以防火牆為主（27%）、次之為內建式接取控制（23%）和接取控制系統（18%），本國與外國開發商比例為6：4。至於CC驗證部分，驗證實驗室有5家，通過驗證產品近50件，類型包含IDP/IPS、防毒程式、防火牆、作業系統等，本國與外國開發商比例為7：4。

俄國FSTEC驗證體制近期更新多了弱點分析（類似ISO/IEC TR20004:2015）、基於CC第3章的特別安全保證要求和採用軟體開發生命週期（SSDLC）。俄國驗證體制比較：

表格 4、俄國 FSTEC 與 CC 驗證比較

	FSTEC驗證程序	**CC驗證程序**
正常的檢測時間	5-6個月	3個月
需要源碼檢測	要	不用
測試標準可取得	不可	可
評估保證等級	EAL4-7	EAL1
典型資訊安全檢測工具	根據PP	根據cPP

2.2.12使用共同準則進行採購：國際採購措施

採購用於國家或敏感資訊的IT安全產品之前應先進行驗證，確保產品足以

保護此類信息。許多政府的國家機構管理及使用經驗證的產品做出了相當大的努力，而全世界都採行了各式不同措施，西班牙Jtsec的Jose Francisco Ruiz Gualda因而展開調查，並將分析IT安全產品採購的當前趨勢。

Jose蒐集了15個國家的資料。從問卷結果得知，有14個國家使用CC進行政府採購，而9個國家使用了其他標準進行採購。

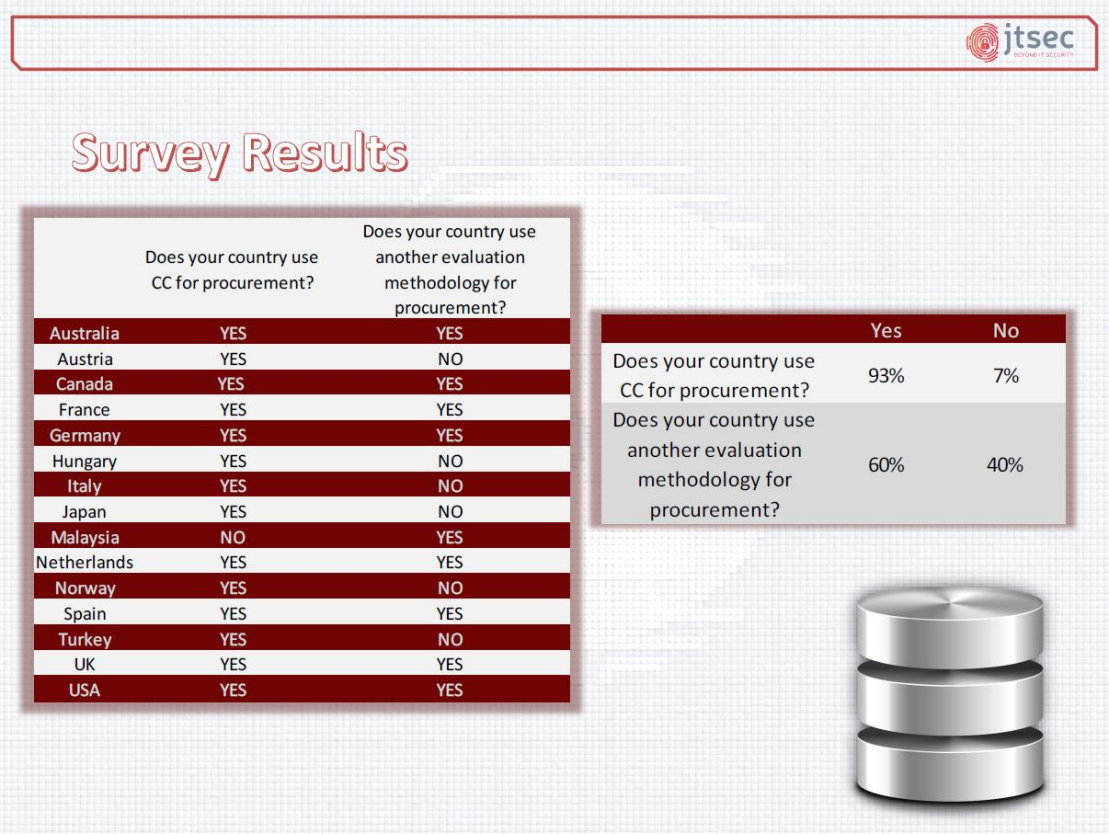


圖 11、各國政府 IT 採購政策問卷調查結果

歸納問卷調查成果，各國政府採購ICT產品政策共分成4種態樣（問卷調查整理如附件二）：

1. 使用通過驗證產品清單/型錄：美國、澳洲、西班牙
2. 法規規範採購使用 CC 標準或其標準方法：如歐盟國家、澳洲、美國
3. 採購程序中將 CC 或其他資安評估作為需求規格：如荷蘭、法國、英國、馬來西亞等
4. 不使用 CC 與其他資安評估。

Jose最後表示，CC是相當強力措施，建議全面採用，以符合市場需求；4

種採購政策中，以驗證通過產品/型錄最為簡單清楚，建議採用作為採購方式。

2.2.13 PP 開發、自動生成 ST 和支持評估活動報告的下一代工具

美國國家安全局網路安全局Jeffrey Blank和國家資訊安全保障合作組織NIAP的Robert Clemons，提出了PP與ST撰寫流程的問題與挑戰與解決方案，並現場展示PP自動化生成ST的過程。

長久以來，CC最令人詬病的是驗證時間過長，甚至超過產品的生命週期數倍，這令許多廠商卻步。另一個麻煩點就是開發文件準備。對廠商而言，PP撰寫與維護的品質與速度、撰寫ST的過程是很複雜的；對使用者而言，要瀏覽所有相關文件也是相當困難。講者表示，基本上在撰寫、更新PP過程中，有許多事不必那樣繁瑣。

講者所提出的解決方案使用XML編輯PP，實現自動化產成ST，可進行ST和PP的自動對比以及部分測試項目自動化，且利於評估的公正性考量，過程中都是開放、透明的。因PP以網頁形式表現，所以提供更加動態的體驗，使用者可依實際要求檢視PP，如希望在數分鐘內概略了解PP的安全功能要求，則可在網頁中選擇遮蔽檢測項目。目前已生成或轉換了十幾種PP文件，包括：通用作業系統、應用軟體、無線入侵檢測系統和行動裝置基礎。

參、 心得與建議

共同準則(CC) 透過 CCRA 相互承認推行了數十年，讓國際產品安全驗證有了共通標準。通過 CC 標準驗證的產品多為智慧卡、網通設備等產品，但若驗證規模較大、較複雜的，廠商可能就望之卻步，對於大多數的廠商而言，CC 驗證耗時太長，通過驗證的時程恐大於產品改版的週期、同時驗證費用所費不貲，甚至高過於驗證產品所帶來的收益。因此，各國因應此議題紛紛發展出各自國內的驗證制度，如法國的 CSPN、荷蘭的 BSPA、馬來西亞的 IPSA 等，以提高國內廠商送驗意願，進而強化產品安全能力及價值。

我國政府為完備國內產品安全相關檢測標準及制度，通傳會在 2010 年至 2013 年訂定了網路型防火牆、入侵偵測防禦系統、防毒閘道器設備等 10 項資通設備安全檢測技術規範，在 2016 年增加手機系統內建軟體資安檢測技術規範，並近期就物聯網重點設備如無線網路攝影機、無線路由器、無線接取器、MOD 及有線電視機上盒等，推出一系列資安檢測指引，而經濟部也在 2017 年制定了「行動應用 App 基本資安檢測基準」，並由通傳會和經濟部合作「物聯網資安標章」，鼓勵產業將產品送檢取得安全標章，我國政府在相關資通設備採購的規格需求也將要求有安全標章的產品，提升廠商送檢誘因，並確保我國政府所用資通設備的安全防護能力。

至於如何將國內產品推向國際，我國政府除了可透過逐一洽談雙邊，簽署相互承認 MRA 外，最快途徑莫過於加入 CCRA 了。雖我國政府先前有提出申請加入，後因外交局勢所迫而未能談成，但仍建議持續參與 CC 相關會議，透過交流與分享經驗，並提升我國能見度，以建立國際人脈，尋找加入 CCRA 契機。

肆、 附件

附件一、議程

Day 1

09:00 10:15	**Plenary Keynote Session** 09:15 Security Certification in the Age of Digital Transformation (P10b) 09:45 Spearheading Cooperation in the EU Cybersecurity Certification Framework (P10c)		
10:15 11:00	**Networking Break in Exhibits**		
11:00 13:00	**Plenary Conference Session** 11:00 CCDB Update (P11a) 11:30 CCUF Update (P11b) 11:40 CCRA Management Committee Update 12:00 Panel Discussion: The Revision of ISO/IEC 15408, 18045 and the TR22216 (P11c)		
13:00 14:00	**Lunch in Exhibit Area**		
14:00 15:30	**Track 1: Advances in the Use of Common Criteria**	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
	14:00 Track Keynote: Why I Care About the Security of Your Car (A12a) 14:30 Robustness Propagation Through Systems of Heterogeneous CC Components(A12b) 15:00 Common Criteria as Backbone of IoT Security Certification (A12c)	14:00 Introducing Secure Systems into NATO – the requirements to Common Criteria (M12a) 14:30 Continuous Mobile Application Compliance Using Government Standards(M12b) 15:00 Adopting Common Criteria Methodology and Strategies in Malaysia Critical National Information Infrastructure (CNII) (M12c)	14:00 Track Keynote: How Europe's Cyber Security Act and CCRA Can Be Best Friends(U12a) 14:30 Brexit, the EU Cyber Security Act, and Product Assurance in UK and the EU—An Update (U12b) 15:00 Cybersecurity Act: On the Route of a European Union Cybersecurity Certification System (U12c)
15:30 16:00	**Networking Break in Exhibits**		
16:00 17:30	**Track 1: Advances in the Use of Common Criteria**	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
	16:00 Why Composite Evaluations Fail(A13a)	16:00 Regulating IT Market with Common Criteria	16:00 IPSA: An Adaptation of Common Criteria for

	16:30 A Compositional Certification Methodology For a COTS-Based System(A13b) 17:00 Evaluation of Distributed Products in the CC Paradigm (A13c)	Certifications (M13a) 16:30 Using Common Criteria for Procurement: International Procurement Initiatives (M13b) 17:00 EU Cybersecurity Act: the tough part is yet to come! (M13c)	Malaysian Local Market (U13a) 16:30 Panel Discussion: The Why and How of Using CC in Private Schemes(U13b)

Day 2

	Track 1: Advances in the Use of Common Criteria	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
09:00 10:30	09:00 Introducing the Partner Program Certification Concept (A20a) 09:30 Basissicherheitszertifizierung (BSZ)—An Alternative Means to Achieve Assurance(A20b) 10:00 TEE Certification: Managing Risk for Digital Services (A20c)	09:00 Reconciling Security Vulnerabilities within the Common Criteria (M20a) 09:30 [60MIN] Hypervisor Security—Panel Discussion (M20b)	09:00 Netherlands Scheme Update (U20a) 09:30 NIAP Scheme Update (U20b) 10:00 Scheme Update of Japan (U20c)
10:30 11:00	**Networking Break in Exhibits**		
	Track 1: Advances in the Use of Common Criteria	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
11:00 12:30	11:00 Scaling Common Criteria to the Next Level (A21a) 11:30 Common? C'mon! (A21b) 12:00 Multi Assurance Evaluations for Real Products (A21c)	11:00 Connected Cars. Security Certification Schemes. (M21a) 11:30 Protection Profiles for Smart Home Appliances (M21b) 12:00 Expressing Minimum Security Requirements for Smart Meters in a Protection Profile (M21c)	11:00 The Status of IT Security Evaluation and Standards in China—A Technical Perspective (U21a) 11:30 The Russian IT Security Certification Scheme: Current Status and New Trends(U21b) 12:00 Update from ISCI WG (U21c)
12:30 13:30	**Lunch in Exhibit Area**		
	Track 1: Advances in the Use of Common Criteria	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
13:30 15:00	13:30 Working Harder: Doing Painful Things With	13:30 An Evaluation Methodology with Assurance	13:30 Common Criteria Crypto Working Group (U22a)

	cPPs (A22a) 14:00 Modular PPs: The Building Blocks of Tomorrow (A22b) 14:30 How Much Decomposition is Too Much, The Debate Between Complete PPs and PP-Configurations (A22c)	Levels for Privacy-by-Design(M22a) 14:00 [60MIN] PP v/s EAL: Where Does Security Assurance Reside? (M22b)	14:00 SOG-IS Crypto WG: Objectives, Achievements and Perspectives (U22b) 14:30 Cryptographic Module Users Forum (CMUF) Update (U22c)
15:00 15:30	**Networking Break in Exhibits**		
15:30 17:00	**Track 1: Advances in the Use of Common Criteria**	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
	15:30 Full Common Criteria Statistics Report with CC Scraper (A23a) 16:00 [60MIN] Panel Discussion: Next-Generation Tooling to Develop Protection Profiles, Automate Security Target Generation, and Support Evaluation Activity Reporting (A23b)	15:30 Verification of Cryptographic Security Functionality in NIAP CCEVS (M23a) 16:00 Ensuring Good Entropy Sources is Not a Random Act (M23b) 16:30 TLS 1.3, the Real Trusted Channel(M23c)	15:30 When cPPs Grow Up: The Challenges of Maintenance (U23a) 16:00 Towards Collaborative Protection Profiles for Biometric Systems (U23b) 16:30 Test Automation Best Practices for CC(U23c)

Day 3

09:00 10:30	**Track 1: Advances in the Use of Common Criteria**	**Track 2: Assurance**	**Track 3: Updates from Schemes and ITCs**
	09:00 Connected Cars. What About Security? (A30a) 09:30 [60MIN] Panel Discussion: Emerging Issues Between Hardware and Software Evaluations (A30b)	09:00 Frequently Updated TOEs. Is Continued Assurance Possible? (S30a) 09:30 Assurance at the Speed of Development (S30b) 10:00 Dealing with Patch Management in Common Criteria—Lessons Learned from Study Period in SC27 WG3 (S30c)	09:00 Hard Copy Device Technical Community Update (U30a) 09:30 JEDS – A Community for the Evaluation and Certification of Embedded Devices (U30b) 10:00 Reusing ALC Activities—Looking for Efficiency in CC Evaluations: A Success Story (U30c)
10:30 11:00	**Networking Break in Exhibits**		
11:00 12:30	**Track 1: Advances in the Use of Common Criteria**	**Track 2: Meeting Customer Requirements**	**Track 3: Updates from Schemes and ITCs**
	11:00 Quantum Key Distribution—A New Target for	11:00 ePassport High Assurance Evaluations in a Timely	11:00 Network Device iTC Update (U31a)

	CC Evaluation (A31a) 11:30 Guide for Evaluator in CC Evaluation: Tips and Tricks Malaysia Lab Style (A31b) 12:00 Impact of Technical Decisions on On-Going Evaluations Conforming to NDcPP (A31c)	Manner (S31a) 11:30 Hardware-Enabled AI for Embedded Security: Towards the Highest CC Evaluation Assurance Levels (S31b) 12:00 ISCI-WG1: Lean CC and High Assurance—The Java Card Pre-Compiled Evidence Project (S31c)	11:30 JTEMS—A Payment Scheme Independent Framework for POI Terminal Specific Security Evaluations Based on Common Criteria (U31b) 12:00 Status and Overview of the DSC iTC(U31c)
12:30 13:00	**Networking Break**		
13:00 14:00	**Closing Plenary Session** 13:00 Summary Panel Discussion: The EU Cybersecurity Act (P32a)		

附件二、各國政府採購 ICT 產品政策問卷調查彙整結果

資料來源：ICCC 2018 講者 Jtsec 的 Jose Francisco Ruiz Gualda

國家	採購要求CC驗證	採購要求其他驗證	具體描述
澳洲	是	是	- 澳大利亞政府系統所使用具有安全功能的產品必須通過 CC。 - 通過的產品可從澳洲評估產品清單（EPL）或 CC 網站中查詢。 - 澳大利亞國防情報局（Australian Signals Directorate）使用另一種加密產品和高保證應用的評估方法，目前由國防情報局內部完成評估。
奧地利	是	否	- 奧地利政府除歐盟有規定，一般未強制要求 CC 驗證產品。 - 奧地利沒有其他的驗證制度。 - 但常要求廠商取得 ISO 27001 認證。
加拿大	是	是	- 加拿大政府將 CC 納入為 RFP /合約要求。 - 特定類別產品需要符合相關 PP 驗證。
法國	是	是	法國政府採購要求分為 3 個等級（主要分為 CSPN 驗證與 CC 驗證）: - 初級：CSPN 驗證（輕量級） • 輕量級(Lightweight)評估，節省時間(8 週完成)

<table>
<tr><td></td><td></td><td></td><td>• 著重弱點分析與滲透測試
- 標準：EAL3+VAN.3 +FLR.3
- 強化：EAL4+VAN.5 +IMP.2+ DVS.2+FLR.3</td></tr>
<tr><td>德國</td><td>是</td><td>是</td><td>- 德國政府廣泛使用 CC 驗證產品。
- 德國有其他以 CC 為基礎的驗證評估方法，如 CC Site Certification。</td></tr>
<tr><td>匈牙利</td><td>是</td><td>否</td><td>- 匈牙利政府一般不強制要求 CC 驗證的產品，除非歐盟法規規定採用。
- 不採用其他驗證方法。</td></tr>
<tr><td>義大利</td><td>是</td><td>否</td><td>義大利政府採購常要求產品通過 CC 驗證，但沒有針對安全產品製作型錄。</td></tr>
<tr><td>日本</td><td>是</td><td>否</td><td>- 日本政府的 IT 產品採購政策是由 NISC 制定中央政府的資安標準，METI 列出確保 IT 產品採購所需安全要求清單，目前分為 11 大類：
<table>
<tr><td>1. 多功能事務機</td><td>2. 防火牆</td><td>3. IDS/IPS</td><td>4. 資料庫</td></tr>
<tr><td>5. USB</td><td>6. 智慧卡/IC</td><td>7. 全驅動加密 HDD</td><td>8. 行動裝置</td></tr>
</table></td></tr>
</table>

			9. VPN　10. 作業系統　11. 路由器 - 另外，也有標準不是強制要求項目，如日本政府推薦的加密標準。 - 日本政府在 IPA 網站公告用於日本體制的 PP 和通過驗證產品清單
馬來西亞	否	是	- 馬來西亞目前沒有使用 CC 作為政府採購要求 - 但正考慮針對關鍵基礎設施採購時，要求通過 CC 驗證。 - 馬國政府另有一個驗證制度－ICT 產品安全評估(TSA)
荷蘭	是	是	- 荷蘭政府採購政策未將 CC 列為強制要求，但一些計畫會使用 CC 驗證產品，如電子護照。 - 基線安全產品評估（BSPA）針對處理敏感但非機密資料的產品，提供輕量級驗證，也是政府採購 ICT 產品安全驗證另一種選項。 - 高機密產品：NLNCSA 國家評估
挪威	是	否	- 挪威政府除了安全法所規範的機密系統，其他沒有強制使用通過 CC 驗證產品的法規。 - 部分歐盟指令要求使用通過 CC 驗證產品。 - 其餘則由需求單位自行決定要使用何種產品。
西班	是	是	- 西班牙政府採用驗證產品型錄（CPSTIC），公共組織依據國家安全體制使用 CPSTIC。 - CPSTIC 分為合格產品及核可產品：

牙			• 合格產品（涉及敏感資訊）：高安全產品要求 CC EAL 低等級或其他 PP；中/低安全產品則要求：LINCE 評估。 • 核可產品（涉及機密資訊如國防）：要求 CC EAL 高等級。
土耳其	是	否	- 土耳其政府一般採購未使用 CC 產品清單。 - 部分政府機構有訂定 CC 相關法規，如 • 數位簽章：EAL 4 + • 電子郵件服務提供商：EAL4 + • 健康資訊軟體：EAL 2 • 新一代的收銀機財務應用軟體：符合相關 PP
英國	是	是	- 英國政府採購要求分為 CC 驗證和商用產品保證（CPA） - CPA：通過評估的安全產品獲得基礎評比（Foundation Grade）驗證，產品需要有適當商業安全作法及適用於低威脅環境。
美國	是	是	- 美國國家安全系統（NSS）所有具安全功能的 IT 產品，必須通過 CC 驗證。 - NIAP 產品符合清單（Product Compliant List）所列的產品是符合 NIAP 批准 PP 的要求。 - 美國國防部資訊網路核可產品清單（DoDIN APL） • 要求通過 DoDI 8100.04 規範 • 滿足風險管理框架（RMF）CS / IA 測試要求。

			• 要求 CC 和（可能加入）FIPS 140-2 驗證