出國報告(出國類別：考察)

「資通設備之安全檢測研究計畫」參訪設備認證機關及檢測實驗室

服務機關：國家通訊傳播委員會
姓名職稱：羅副處長金賢、陳簡任技正春木、
韓鎮華科長
派赴國家：日本
出國期間：100 年 6 月 27 日至 6 月 29 日
報告日期：100 年 8 月 22 日

摘要

為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。通傳會於 2011 年 6 月 27 日至 29 日派員至日本，拜會獨立行政法人情報處理推進機構（IPA）及資訊技術安全中心（ITSC）2 個單位，實地觀摩、學習日方如何推動資通設備安全檢測，以為我日後相關施政的參考。

目次

壹、目的.....1

貳、參訪機關.....2

一、獨立行政法人情報處理推進機構（IPA；Information-technology Promotion Agency）.....2

二、資訊技術安全中心（ITSC；Information Technology Security Center）.....2

參、過程.....3

肆、參訪紀要.....4

一、拜會 IPA.....4

二、拜會 ITSC.....7

伍、心得與建議.....8

（一）制定符合我國需求的資通設備安全驗證等級.....8

（二）制定能與國際標準接軌的資通設備檢測規範.....8

（三）制定合理可接受的資通設備檢測費用與時程.....8

（四）制定能篩檢把關的檢測實驗室相關管理辦法.....9

陸、照片.....10

壹、目的

為推動「國家資通訊安全發展方案」，使我國的資通環境更能面對複雜多變的資通安全威脅，行政院於 2009 年 8 月 18 日至 20 日舉辦『塑造資安文化、推升資安產值』產業科技策略會議（Strategy Review Board，SRB）」。行政院科技顧問組於該策略會議所達成的共識與策略基礎上，協同相關部會規劃完成「行政院『塑造資安文化、推升資安產值』產業科技策略會議關鍵推動方案」，並由各主責部會在施政措施上予以落實。通傳會（NCC；National Communications Commission）依前開方案之行動計畫 3-1（2010 年至 2013 年），負責推動「資通設備之安全檢測研究計畫」，即在兼顧「政府需要」、「產業發展」及「建立檢測能量」原則下，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。

考量日本向為資通訊設備先驅，且不遺餘力地執行資訊安全政策，他山之石可以攻玉，實地觀摩、學習日本如何推動資通設備安全檢測，以作為我日後相關施政的參考，確有其必要性。此次活動，拜會獨立行政法人情報處理推進機構及資訊技術安全中心 2 個單位。

貳、參訪機關

一、獨立行政法人情報處理推進機構（Information-technology Promotion Agency；IPA）

前稱「情報處理振興事業協會」，係 1970 年 10 月 1 日基於「情報處理推動」相關法律（1970 年 5 月 22 日制定，第 90 號法律）設立之社團法人，復依 2002 年 12 月 11 日通過修正頒布之第 144 號法律，於 2004 年 1 月 5 日改組，成為具有管理功能的機構，目前有 10 個部門及中心，包括 IT 安全中心（約有 100 名研究員及職員）、軟體工程中心等，是日本經濟產業省的外圍組織，負責推展與 IT 有關的國家戰略。其主要業務包括 IT 安全、軟體工程、IT 人才培育及開放軟體等，並受理信息病毒、不當存取及脆弱性關聯情報等申報，與 JPCERT/CC 合作，公開這些情報調查、研究及緊急對策等訊息。每年會在全國 10 個地方實施情報安全研討會。

二、資訊技術安全中心（Information Technology Security Center；ITSC）

1987 年即開始研究以共同準則(Common Criteria；CC）為主之評估技術，是 CCRA 在日本第一個正式認可之評估實驗室（2002 年），目前有 15 位評估員，隸屬日本電子情報技術產業協會（ Japan Electronics and Information Technology Industries Association；JEITA）成員，並於 2009 年被認可為 FIPS 測試實驗室。業務範圍包括 IT 產品之 EAL1~EAL4 及 PP 安全評估、提供密碼模組與演算測試服務。

參、過程

6 月 27 日　　自臺北中正機場啟程

6 月 28 日　　拜會 獨立行政法人情報處理推進機構
拜會 資訊技術安全中心

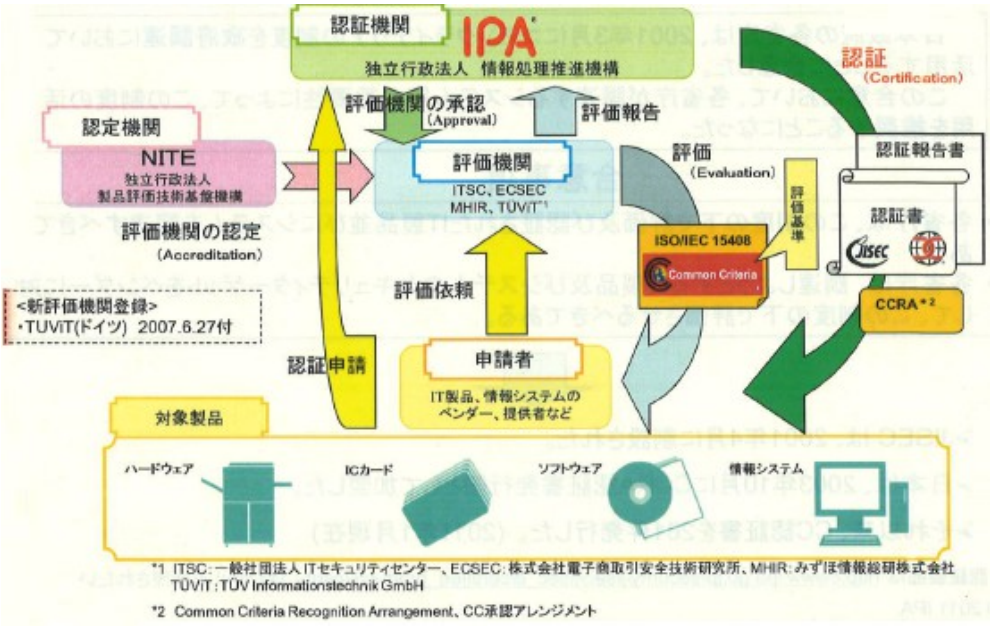
6 月 29 日　　返抵國門

肆、參訪紀要

一、拜會 IPA

由理事 仲田 雄作、センター長 矢島 秀浩及主任 村田 松寿等人全程接見，村田 松寿向我方簡報有關 IPA 運作概況，隨後，雙方進行意見交流，會談內容略整如次：

（1） 日本中央部會於 2001 年 3 月協議「對於政府採購 IT 產品及系統，建議採用經 CC 評估與驗證者」，該國於 2003 年加入 CCRA，成為授與證書會員國(Certificate Authorizing Participant；CAP)。其發證程序如下：



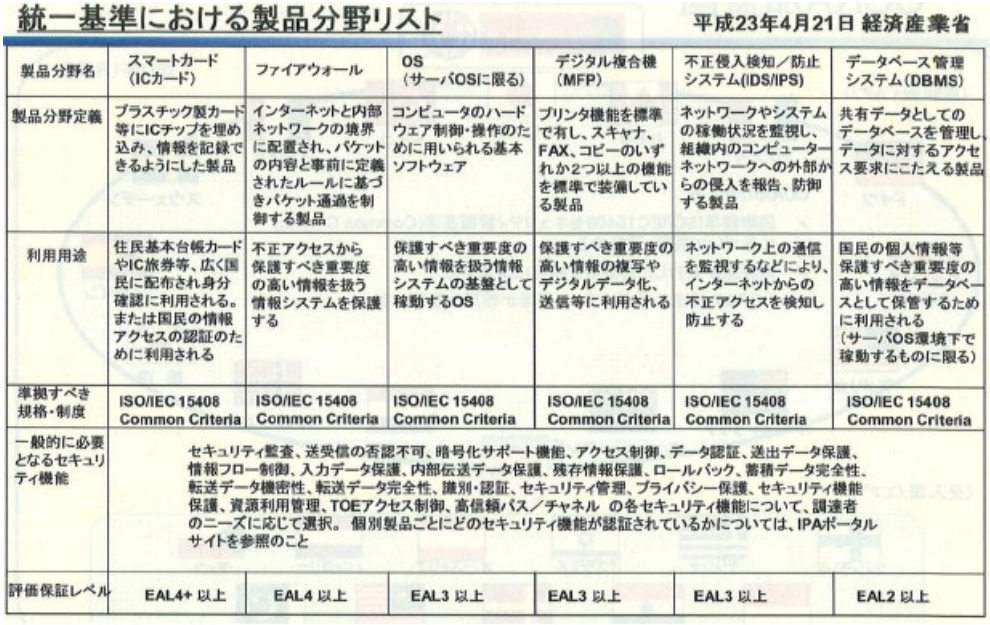
註：CC 驗證報告書若不公開，該證書之 logo 只能使用「 」而不具「 」。

（2） 日本認證產品以事務機（Multi-Function Printer；MFP）為最大量（約占 67%），產品驗證等級則以 EAL3 為大宗（約占 59%）。

（3） 日本對近 50 個軟體發展具重要安全須求之政府系統（諸如，貿易

統計系統、護照申請檢查系統等）完成安全標的（ST）之評估與確認。

（4） 2011 年 4 月 11 日，基於政府採購安全政策，日方公告 IT 安全測量標準產品目錄表，內容包括智慧卡、防火牆、伺服器 OS、事務機 、IDS/IPS 及 DATABASE（DBMS）之一般安全功能、認證等級等要求：



統一基準における製品分野リスト　　平成23年4月21日 経済産業省

製品分野名	スマートカード（ICカード）	ファイアウォール	OS（サーバOSに限る）	デジタル複合機（MFP）	不正侵入検知／防止システム(IDS/IPS)	データベース管理システム(DBMS)
製品分野定義	プラスチック製カード等にICチップを埋め込み、情報を記録できるようにした製品	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア	プリンタ機能を標準で有し、スキャナ、FAX、コピーのいずれか2つ以上の機能を標準で装備している製品	ネットワークやシステムの稼働状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品	共有データとしてのデータベースを管理し、データに対するアクセス要求にこたえる製品
利用用途	住民基本台帳カードやIC旅券等、広く国民に配布され身分確認に利用される。または国民の情報アクセスの認証のために利用される	不正アクセスから保護すべき重要度の高い情報を扱う情報システムを保護する	保護すべき重要度の高い情報を扱う情報システムの基盤として稼動するOS	保護すべき重要度の高い情報の複写やデジタルデータ化、送信等に利用される	ネットワーク上の通信を監視するなどにより、インターネットからの不正アクセスを検知し防止する	国民の個人情報等保護すべき重要度の高い情報をデータベースとして保管するために利用される（サーバOS環境下で稼動するものに限る）
準拠すべき規格・制度	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria
一般的に必要となるセキュリティ機能	セキュリティ監査、送受信の否認不可、暗号化サポート機能、アクセス制御、データ認証、送出データ保護、情報フロー制御、入力データ保護、内部伝送データ保護、残存情報保護、ロールバック、蓄積データ完全性、転送データ機密性、転送データ完全性、識別・認証、セキュリティ管理、プライバシー保護、セキュリティ機能保護、資源利用管理、TOEアクセス制御、高信頼パス／チャネル の各セキュリティ機能について、調達者のニーズに応じて選択。個別製品ごとにどのセキュリティ機能が認証されているかについては、IPAポータルサイトを参照のこと					
評価保証レベル	EAL4+ 以上	EAL4 以上	EAL3 以上	EAL3 以上	EAL3 以上	EAL2 以上

（5） 日本政府為鼓勵業者加速引進 IT 產品認證，提供減稅優惠，方式有二：經認證之產品其稅可減 7%或以全部營收之 7 成繳稅；2010 至 2011 年該國重點輔導對象為中小企業（SMB）。

（6） 由於日本與大陸貿易非常密切，對大陸進口的電信設備，並無特別有安全限制上之處理。

（7） 日方完成資訊安全措施（Information Security Measures；ISM）自我評估工具，產業可藉由問答方式（共 25 題，主要出自 ISO/IEC 27001：2005 所定義之安全控制項目），了解自身於 ISM Benchmark 相對應之強弱位置，以改善其企業之資安管理。

（8） 日本 CC 實驗室或驗證機構相關收費規定

相關資料 i

申請型態		費用（含稅）
驗證	PP	399,000 円
	EAL1	514,500 円
	EAL2	672,000 円
	EAL3	787,500 円
	EAL4	997,500 円
	EAL5	1,081,500 円
	EAL6 以上	要相談
ST 確認		378,000 円
保證持續		3,700 円
驗證英文版		3,700 円
變更驗證或確認資訊		3,700 円
補發驗證報告書或確認報告書		3,300 円
變更驗證報告書或確認報告書記載事項		3,300 円

（9） 日方邀請我方參加今年 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。

二、拜會 ITSC

由部長代理 北澤 直人、副部長 倉本 康史及理事 宇賀村 直紀負責接待，倉本 康史先就該實驗室經營現況做簡報，雙方復對資通訊產品驗證問題進行意見交流，會談內容略整如次：

（1） ITSC 做 CC 評估驗證之量為全日之冠（約占 47%）。

（2） 由於產品驗證時間長、價格不菲，中小企業（SMB）申請認證比例不高，通常上市公司才會提出產品認證。

（3） 廠商送驗產品若通不過檢測時，廠商可提出相關修正；成功修正耗時最長者，達 2 年。

（4） 金融海嘯發生時，幾僅剩日本強項－事務機（MFP）提出驗證，目前其他產品驗證有漸增加之態勢。

（5） 當驗證有疑義時，IPA 會指示、評估到完全一致。

（6） 每一驗證 case 通常以 3 人一組（1 主驗 2 幫手）來做檢測，該頗有傳承之意味。其訓練評估員之方式有三：

1.電子學習課程

2.在工作中學習

3.技術會議交流

（7） ITSC 所做驗證等級只到 EAL4，EAL5 以上雖可試行，但不能發證。除晶片外，EAL5 以上產品均具機敏性。

伍、心得與建議

此次交流活動，讓吾等了解到日本在資通設備安全檢測之作法，其中包括設備檢測分級、稅減鼓勵業者加速引進 IT 產品認證等，均值得我方借鏡學習。相關建議如下：

（一）制定符合我國需求的資通設備安全驗證等級

由於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等級，一味移植於我國，恐造成水土不服，治絲益棼。準此，應先檢視我國現況，了解政府資通設備安全檢測預期目標為何，方去訂定相關驗證等級，以挈其領，達其效。

（二）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國際共同準則承認協定(CCRA；Common Criteria Recognition Arrangement)組織，因此，除研提適於我國之短中長期資通安全檢測設備類別、項目及檢測技術規範外，亦須考量將前開內容適當加入與國際接軌之具體作法及對應配套措施，較為妥適。

（三）制定合理可接受的資通設備檢測費用與時程

共同準則(Common Criteria；亦稱 ISO/IEC 15408)雖為國際通用的資安產品驗證標準，但因該驗證時間較長，一般可達 18 個月，且動輒千萬，所費不貲，造成在實務推動上，有其瓶頸，業者接受度不如預期。準此，為利我國發展資安產業得以順遂，得考量免除非必要之檢測項目，縮短驗證時程並降低費用。

（四）制定能篩檢把關的檢測實驗室相關管理辦法

囿於政府人力不足，為使我國資通設備安全能維持一定水平，藉由第三方檢測機構（實驗室）的角色對資通設備產業進行安全檢測的工作，就益顯重要。準此，如何避免實驗室良莠不齊，由實驗室相關管理辦法篩檢

把關，應為可行，即其內容至少須包含實驗室執行之檢測範圍、具備之檢測能力等項，供主管機關據以認可。

陸、照片

照片 1

▲訪問 IPA

照片 2

▲訪問 ITSC