ISSN 1994-9766

NCC NEWS 10月號

NATIONAL COMMUNICATIONS COMMISSION • 第10卷 第6期 • 中華民國105年10月出刊

http://www.ncc.gov.tw

頭條故事・防制電信詐騙執行情形

人物專訪・推動國家資安政策　發展資通訊資安防護
—專訪財團法人電信技術中心董事長李漢銘博士

專欄話題・談誘捕技術的前世與今生

・行動寬頻基站資安管理方針

・智慧型手機系統內建軟體資安檢測規劃現況

NCC NEWS
中華民國105年10月出刊
第10卷 第6期

目 錄 CONTENTS

出 版 機 關 國家通訊傳播委員會
發 行 人 詹婷怡
編 輯 委 員 翁柏宗、何吉森、洪貞玲
郭文忠、陳憶寧、陳耀祥
編 輯 顧 問 陳國龍、鄭泉泙
總 編 輯 王德威
副 總 編 輯 紀效正
執 行 編 輯 黃睿迪、劉秀惠、林淑娟
電 話 886-2-3343-8798
地 址 10052 臺北市仁愛路一段50號
網 址 www.ncc.gov.tw
美 術 編 輯 奧得設計顧問股份有限公司
電 話 886-2-2365-0908

展售處
國家書店 - 松江門市
104 臺北市中山區松江路209號1樓
電話：886-2-2518-0207
五南文化廣場
臺中市中區綠川東街32號3樓
電話：886-4-2221-0237

中華郵政臺北雜誌第1102 號
執照登記為雜誌交寄
歡迎線上閱讀並下載本刊
網址：www.ncc.gov.tw

GPN：2009600628
ISSN：1994-9766
定價新臺幣：100 元
創刊日期：96.4.28

著作權所有 本刊圖文非經同意不得轉載

886+攔阻 破解詐欺遊戲

防制電信詐騙執行情形

吳政昇

壹、前言

今（105）年初馬來西亞、非洲肯亞及烏干達等國家陸續破獲國際詐騙集團，歹徒成員包含大陸及臺灣人士，究其緣由係因原本藏身臺灣之詐騙集團，在國內警政單位採取有效防制措施並強力取締後，詐騙成員改弦易轍，陣地轉移至管理相對鬆散之東南亞及非洲，詐騙對象也以警覺性較低的大陸民眾為主。

電信自由化後，國內各項電信網路建設更加普及、電信服務更顯便利、費用更為低廉，雖然奠定國內經濟發展基礎，同時增進民眾電信使用效益，卻也讓國內詐騙集團藉此對國人進行電信詐騙。因民眾受害之案件數及規模逐漸擴大，引發各界關注，政府遂採取多項防制措施並大力掃蕩，並廣泛地向社會大眾宣傳詐騙型態、檢舉管道與防詐對策，終於有效遏止詐騙危害。

為協助警政單位防制電信詐騙，遏止歹徒利用電信服務進行詐騙，國家通訊傳播委員會（以下簡稱本會）參與多項跨部會防制電信犯罪工作平臺及配合警政單位研析對策，並積極督導電信業者配合警政單位發送反詐騙宣導簡訊及採取防制措施，藉由相關具體作為協助打擊犯罪強化社會治安、防制電信詐騙保障民眾財產。

貳、電信詐騙態樣手法

綜觀古今中外，詐騙可謂無所不在，從早期金光黨、刮刮樂等傳統詐騙，到後來電信詐騙手法多以簡訊、電話、網路電話等方式詐騙。隨著網路時代民眾生活形態與交易方式改變，歹徒逐漸結合駭客盜用民眾網路交易個資，並利用新興網路工具，例如行動APP、通訊軟體、社群網站等方式進行詐騙，態樣隨著時代與時俱進，手法隨著科技不斷翻新。面臨詐騙技術與手法的不斷翻新，政府也必須要有新的思維，以科學的方法有效因應防制。慣常詐騙態樣與手法綜整如下：

一、假交易真詐財：歹徒設立空殼公司或利用人頭，以網路或電話進行假交易真詐財，詐取被害人財物。

二、刮刮樂中獎通知：歹徒假冒某公司或活動單位，通知被害人幸運獲得刮刮樂獎金或抽獎活動財物，例如：特獎獎金、免費旅遊行程或機票等，但如要領獎者，必須先匯出財物總值某百分比之稅費，始能拿到中獎之財物。

三、假冒親朋熟友：歹徒假冒（或結合猜猜我是誰）被害人之親友、同學、同事、客戶等關係，再編造各種名義向被害人借款、請求被害人支付款項存入特定銀行帳戶。

四、假冒檢警執法人員或金融機構人員：歹徒假冒檢警、法院執法人員或郵局銀行金融機構人員，謊稱被害人涉入某刑事案件或詐騙案件，需將被害

人財產轉入公務特殊帳戶予以凍結保全。歹徒同時會以偵查不得公開為由，威脅恐嚇被害人不許告知第三者。

五、盜用MSN或LINE帳號：歹徒先盜取民眾MSN或LINE帳號，再以盜用的帳號上線聯絡被害人，讓被害人誤以為是其朋友，伺機取得被害人聯絡電話或相關個資後，再進行各種網路詐騙或電信小額付費交易詐騙。

六、手機簡訊連結惡意程式：歹徒假藉各種名義寄送夾帶惡意程式連結之簡訊，民眾於不知情下點觸連結、下載並安裝惡意程式，致使手機中毒或遭歹徒操控，歹徒進而假冒被害人進行電信小額付費交易。

七、ATM解除分期付款：歹徒竊取民眾網路交易資料，假冒網路交易或商家之客服人員，佯稱該筆網路交易設定錯誤，商請被害人利用網路銀行或前往ATM操作取消設定。或請民眾購買遊戲點數回沖解除分期付款。

八、其他：假交友詐財、假綁架詐財、假求職詐財等等。

參、防制電信詐騙執行措施

本會為通訊傳播事業之監理機關，職掌通訊傳播之政策訂定、事業監理及資源管理。有關協助防制電信犯罪事宜，本會一向本於依法行政並在技術可行之前提，積極配合並協助警調機關。過往不僅協助擬訂「通訊保障及監察法」、及其施行細則，協助警調通訊監察分工，更配合修訂各項通信業務之管理規則及系統技術審驗規範相關條文，從技術面要求業者電信系統須具備防制電話詐騙相關基本功能，再從業務面強化業者電信營運須落實防制電信詐欺相關管理措施及配合犯罪調查需要提供通信紀錄。本會配合防制電信詐騙相關重要措施分述如后：

一、修訂電信業務系統網路技術規範，加強電信設備防制詐騙電話功能：鑒於次世代網路（Next generation networking, NGN）為電信業者提供國際交換、長話交換、市內交換及網路電話服務之網路趨勢，本會於100年完成修訂8種電信業務之系統網路審驗技術規範，並於103年完成訂定行動寬頻（4G）系統審驗技術規範，明訂國際、行動、市內／E.164網路交換機須具備防制電話詐騙之特定功能。其中防制國際詐騙電話之重點包含：國際交換機處理國際來話主叫號碼字首含本國國碼（886）應透傳送、國際交換機至少阻斷50組國際來話主叫號碼、用戶可選用拒接國際來話服務等功能。

二、境外話務顯示886國碼，手機顯示「+」號，方便民眾區別境外電話：鑒於詐騙集團慣用竄改國際電話顯號（來電號碼），使民眾誤信該國際來話係為國內電話號碼，本會於98年間即積極配合警政單位研議，並督導電信業者，將境外電話於國內傳送時，必須完整保留「886」國碼，讓民眾無論市話或手機受話時能清楚辨識該通話務係由境外（國際）來話，尤其於民眾手機受話顯示「＋」號，以利民眾辨識來電係屬境外電話。

三、國際話務設定攔阻名單，降低境外電話詐騙：詐騙集團為躲避警政單位追緝，逐步集團化、專業分工與國際化，持續由境外機房撥打國際（網路）電話傳送國內進行詐騙，本會配合警政單位研議，並督導中華電信股份有限公司、台灣固網股份有限公司、新世紀資通股份有限公司及亞太電信股份有限公司等固定通信業者，配合內政部警政署刑事警察局（以下簡稱刑事局）提供之國際話務白名單，設定國際話務攔阻（斷）措施，降低境外電話進入國內詐騙。103年攔阻260萬通，104年攔阻959萬通，105年8月止攔阻639萬通。

四、國際話務改接NGN網路，提升境外攔阻名單效能：為利國際來話顯號「886」國碼、並提升白名單攔阻措施之效能，本會督導中華電信股份有限公司、台灣固網股份有限公司、新世紀資通股份有限公司及亞太電信股份有限公司等固定通信業者建置NGN網路，並將國際話務改接至NGN，以配合刑事局提供之詐騙電話話務量較多之來源國，將國際話務進線路由優先改接至NGN網路執行白名單攔阻。

五、發送反詐騙宣導簡訊，提升民眾防範詐騙認知：為利警政單位教導社會大眾認識電信詐騙相關態樣、手法，並宣導防範電信詐騙之相關策略及舉報途徑，本會督導中華電信股份有限公司、遠傳電信股份有限公司、台灣大哥大股份有限公司、亞太電信股份有限公司及台灣之星電信股份有限公司（前為威寶電信）等電信業者配合刑事局發送反詐騙宣導簡訊給持有行動門號之電信用戶，103年發送6,054萬則，104年發送6,469萬則，105年9月止發送4,113萬則。

六、增訂電信事業資安管理專章，提升用戶個資安全：

依刑事局資料，解除分期付款詐騙案於104年度大肆橫行，詐欺集團先竊取網路交易個資，再以電話指示被害人到ATM操作匯款，可見網路平臺業者或電子商務服務平臺業者，因系統資安漏洞造成客戶個人資料遭竊取，淪為詐騙集團伺機進行詐騙之潛在對象。本會為強化電信服務提供者（電信業者）之系統資通訊安全，分別於103年8月22日修訂公佈第二類電信事業管理規則、104年11月13日修訂公布固定通信業務管理規則，增訂資通安全管理專章，課予電信事業經營者必須建立資通安全防護及偵測設施，定期進行滲透測試、弱點掃描及修補作業，並通過ISO/IEC 27001國際標準及主管機關公告之電信事業資通安全管理手冊ISO/IEC 27011增項稽核表之資通安全管理驗證。本會亦刻正修訂行動通信、第三代行動通信、行動寬頻等業務管理規則之資安專章，強化電信業者網路資通安全，避免用戶個資遭竊取。

肆、防制電信小額付費詐騙執行措施與成效

電信小額付費詐騙為103年新興之詐騙手法，詐騙集團假藉各種名義大量寄送夾帶惡意程式連結之簡訊，民眾於不知情下點觸連結、下載並安裝惡意程式致使手機中毒，歹徒再操控並冒名進行小額付費交易。

為遏止此類新興詐騙案件，本會積極邀集刑事局研訂對策、督導電信業者配合採行防制措施，包含：電信小額付費功能預設關閉、民眾臨櫃辦理服務開通、交易須經雙向簡訊認證、使用者自行設定專屬「安全碼」、電信業者網頁宣導詐騙態樣及防範措施、電信小額付費帳單與電信服務費用帳單分立等措施，終於有效遏止詐騙危害擴大。

依刑事局資料，手機惡意簡訊連結進行電信小額付費詐騙案件由103年6月最高468件，大幅下降至104年12月7件，105年7月6件，案件數量資料如圖1。

伍、結語

蔡總統於520就職典禮演說，特別強調新政府必須要作的幾件事，其中之一就是「強化社會治安網」。行政院林院長也在治安會報強調，「政府存在最重要的目的，就是要保障人民的生命財產和生活權利的尊嚴」、「國內治安有兩大隱憂，必需要面對而且快速改善，一個是毒品的問題，另一個是詐欺的問題」

隨著時代發展與新興科技應用，行動通信網路頻寬與品質愈加提升（2G、3G→4G），智慧行動裝置手機平板使用愈發便利，電信詐騙態樣與手法將因新技術應用而不斷演進。為有效阻絕詐騙集團利用電信服務平臺進行詐騙之犯罪管道，本會將要求電信業者強化電信服務資安措施，並輔以行政檢查督導電信業者落實執行。

本會也將配合刑事局及法務部調查局等機關，持續召開防制電信詐欺或防制網路犯罪相關技術諮詢會議，督導電信業者採取防制措施，透過部會跨域治理及公私部門聯繫協力，研析防制詐騙有效作為，因時制宜防堵新型態詐騙，消弭歹徒詐騙歪風，保障民眾財產安全。

（作者為基礎設施事務處技正）

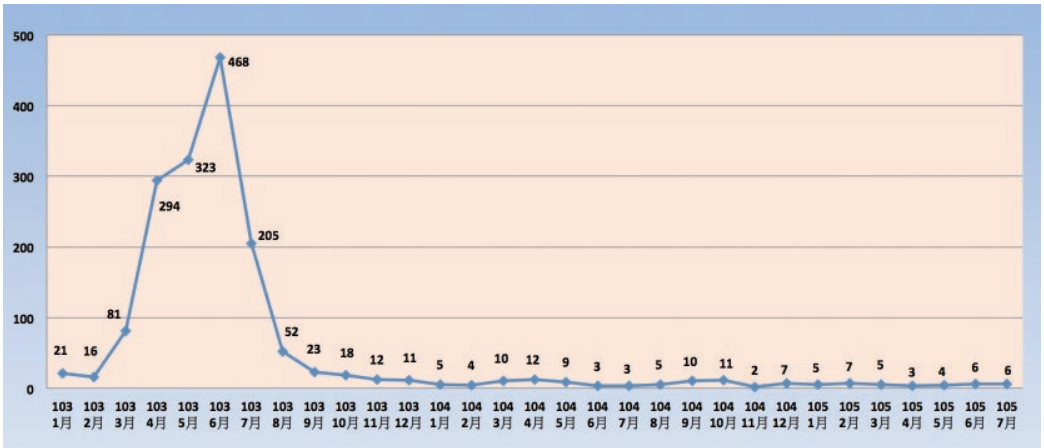

圖1 電信小額付費詐騙案件數量
資料來源：刑事局

資安即國安 4方針創三贏

推動國家資安政策　發展資通訊資安防護

—專訪財團法人電信技術中心董事長李漢銘博士

今（105）年7月，第一銀行盜領案爆發，震驚全國，許多民眾不禁擔憂：連日常生活經常使用的提款機都會被駭客入侵，個人資訊安全的問題是否更沒有保障？

事實上，數位時代的來臨，資通訊科技的發達，帶動了經濟成長，同時也提升民眾的生活品質，但，面對全球複雜多變化的資通訊科技環境，民眾、企業以及政府更必須正視日益嚴重的資安威脅議題，並提出有效措施及減緩風險的方案，這樣才能讓科技豐富我們的人生，但不至於癱瘓我們的生活。

本期NCC NEWS即採訪財團法人電信技術中心董事長李漢銘博士，李博士同時也是臺灣科大資工系特聘教授及中央研究院資訊所研究員，更是業界的資安權威專家，協助政府擬訂國家的資安政策，李董事長針對我國國家資安政策發展，以及未來願景，分享他的觀察與看法。

國家資安政策發展歷程與重點

《NCC NEWS》問（以下簡稱N）：李董事長過去對於國家資通安全政策發展歷程參與詳盡，針對臺灣資通訊安全政策的發展歷程，能否做一些簡要說明。

李漢銘董事長答（以下簡稱李）：所謂的國家資安政策，主要目的在強化我國資通訊環境安全與維護國人資通訊安全權益，並且透過國際交流合作獲得資通訊安全技能與知識，以增加我國資通訊安全能量。

而行政院則於民國90年1月特設「國家資通安全會報」，重大國家資安政策則從90年起至105年開始展開4期、每期4年之國家資安政策發展，針對各階段完成資安的成果，在下一個階段延續並強化前期工作項目，以提升資安完備程度。至於各期計畫與願景則如圖1所示。

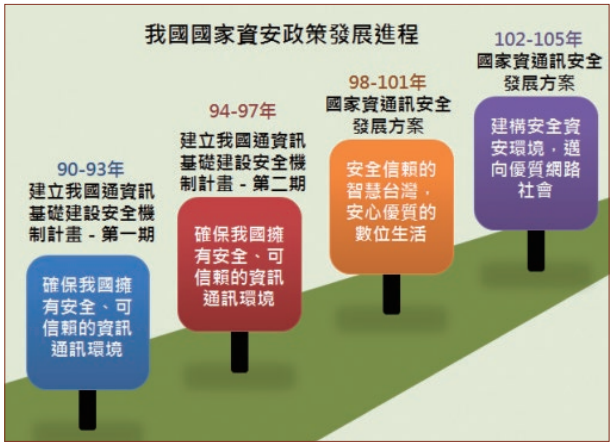

圖1 我國國家資安政策發展進程

事實上，國內規劃資安政策起步算是比較慢，從

表1的彙整表我們可以看出：第一、二期主要願景為確保我國擁有安全、可信賴的資訊通訊環境，並將資安概念慢慢加入到民間企業及政府各部會中，而國家資通安全防護管理平臺（NSOC）也是到民國92年才規劃發包，第二期則正式建立完成。

回憶當時，業者對於資通安全防護管理平臺概念並不完整，不知道怎麼做，政府各部會對於資安概念也相當薄弱，許多基礎建設中都沒有資安的規劃，而此時數位生活及智慧家庭的發展又更進一步，也因此，第三期資安政策的願景在於建構安全信賴的智慧臺灣，提供民眾安心優質的數位生活，並針對關鍵資訊基礎建設防護（CIIP）進行規劃，希望透過基礎建設的強化，讓民眾在使用智慧家庭的相關設備時，能夠更安心。

至於資安政策的第四期，重點工作在於進行資安健診跟稽核，但執行至今發現資訊人力在政府各單位都嫌不足，有嚴重斷層的現象發生，因此，目前也正在討論資訊人才的跨部會調配使用機制，希望能藉此解決人力不足的困境。

回顧資安政策的發展，雖有4期，但總共也才發展15～16年的光陰，並不算完整，自第一銀行ATM事件發生後，由於深切影響到民生生活，資安議題在社會上越顯發酵，相信未來的重要性會越來越大。

資安政策應首重人才培養與產業發展

N：請問李董事長對於國家資安政策未來發展的期許與建議。此外，智慧臺灣的概念是以寬頻網路建設為基礎，進行各種包括智慧家庭、智慧城市等應用，加上臺灣是個島嶼，因應對岸不同的政治環

表1 我國國家資安政策發展彙整表

期別	願景	政策目標、行動方案	主要工作項目
建立我國通資訊基礎建設安全機制計畫-第一期（90-93年）	確保我國擁有安全、可信賴的資訊通訊環境	7大目標及10項執行要點，各目標如下： ・積極防衛資通設施，維護國家運行體制。 ・建立資通安全優勢，提升國家競爭力量。 ・堅實資通安全建設，健全網路社群發展。 ・主動偵測安全威脅，降低實質危害因素。 ・建構安全通報體系，強化事前預警機制。 ・保障民眾隱私權益，促進網路多元發展。 ・增強執法專業能力，有效遏止網路犯罪。	・資訊安全管理系統（ISMS）稽核管理 ・建立資通安全危機事件通報及預警機制 ・資安責任等級分級 ・執法機關偵防能力，建立跨國及區域性合作機制 ・資安演練 ・2003開始發包，宏碁得標，開始規劃國家資通安全防護管理平臺（NSOC）
建立我國通資訊基礎建設安全機制計畫-第二期（94-97年）	確保我國擁有安全、可信賴的資訊通訊環境	4大目標、13項重要措施及33個行動方案，各目標如下： ・提升通報應變時效 ・健全資安防護能力 ・深化資安認知及教育 ・促進國際交流合作	・政府機關資訊安全長責任制度（CISO） ・國家資通安全防護管理平臺（NSOC），建置完成 ・強化資安內稽 ・資安關鍵指標 實體隔離
國家資通訊安全發展方案（98-101年）	安全信賴的智慧臺灣，安心優質的數位生活	4大政策目標、11項重要措施及30個行動方案，各政策目標如下： ・強化整體回應能力，提供可信賴的資訊服務 ・優質化企業競爭力，建構資安文化發展環境	・鞏固關鍵資訊基礎設施防護（CIIP） ・強化緊急應變與復原能力 ・強化電子商務資訊安全 ・厚植資安產業競爭力 ・培育全民資安素養 資訊系統分類分級
國家資通訊安全發展方案（102-105年）	建構安全資安環境，邁向優質網路社會	4大策略目標、規劃20項執行策略及52個行動方案，各策略目標如下： ・強化國家資安政策，建立安全資安環境 ・完備資安防護管理，分享多元資安情報 ・奠基資安技術能量，整合科技實務應用 ・擴大資安人才培育，加強國際資安交流	・建構政府資安專案管理機制 ・推升資安產業能量及推動資安領航計畫 ・加強資安防護二線服務及資安健診服務 ・培訓資安專業人才及國際交流合作 ・發展資安關鍵指標評核基準

境，寬頻網路除了是經濟基礎設施，也是對外的通訊網路，李董事長對於網路資通安全政策上期許建議又是為何？

李：新政府上任後，相當重視資安議題，並將國家資訊安全視為國安的重要環節。因此，8月27～28日由行政院及國安會共同舉辦擴大資安會議，以「資安即國安」為主體討論相關策略。

在兩天會議中，針對「資安即國安機制與策略」、「國家層級資安團隊發展策略」及「國防資安產業發展策略」三大議題，與會人士互相討論及分享看法。以「資安即國安機制與策略」來說，臺灣多年來資安層級偏低，新政府將資安層級提高，因此8月1日行政院資安處掛牌上路，藉此原設定為三級的資安層級，提高到二級。

而「國家層級資安團隊發展策略」部分，則是希望能效法其他國家，組織一定規模的資通電軍，讓國安更健全，也讓資安人才有另外一個出路；至於在「國防資安產業發展策略」方面，則討論如何建構資安產業，畢竟資安人才短缺，有產業才有人才，兩者息息相關，如何發展資安產業刻不容緩。

此外，資安政策首要應建立防護機制，包括國防安全、社會安全、民眾使用服務等安全，尤其是關鍵基礎設施的防護最為重要，需要首波建構起來，防護機制一旦建構，則可創造許多需求，產業也能依勢配合需求發展，進而創造出人才需求。

談到人才，其實我們最擔心的還是需求創造出來了，但資安人才培育卻跟不上，據觀察，過去社會觀念對人才從事資安領域的支持度不高，認為「駭客」是一種負面形象，因此全臺灣沒有資安科系、資安研究所，甚至教職比例也不高。所幸在李德財院士的大力推動下，94年成立臺灣資安研究中心（TWISC），才逐漸培養出學校人力，展望未來，若產業對資安人力有大幅需求，依舊會發生不足狀況，因此，如何同步發展產業、增加人才供給，將是未來政策重點。

尤其是近年來物聯網概念逐漸盛行，所有包括智慧電表、監控設備等各式數位載體都有被入侵的風險，所以人力需求激增，在國外，資安人才的待遇與國內相比高出許多，若國內培養出資安高手，產業腳步卻未跟上，這些人就會被國外企業挖角，如何讓人才根留臺灣，讓國內資安產業發展更健全，刻不容緩。

扮演智庫 推動通訊傳播產業發展

N：李博士於105年接任TTC董事長至今，對於TTC未來發展願景與展望為何？而目前在「資安即國安」的政策下，TTC除了延續此政策與使命，是否還有其他想法可以分享。

李：接任TTC董事長後，將落實TTC原本四個發展目標，包括擔任NCC（國家通訊傳播委員會）的智庫、建立國家級資通訊檢測實驗室、數位匯流服務，以及協助南部資通訊產業發展，並配合NCC未來發展，協助執行未來相關任務。

我認為在此四大目標之下，或許可以進行微幅度調整，例如：南部不一定只限南部，中南部的資通訊發展皆可納入此範圍，TTC也將配合NCC角色的轉變，與NCC合作，推動資安防護產業的發展。至於國家級資通訊檢測實驗室的建立，則可以電信為核心，一來不會跟其他業者與法人衝突，二來也能專心深度地把這塊領域的資安工作做好，並擴充到NCC相關主管業務，例如有線電視，藉此強化與其他法人之間的合作，共同做好國內資安工作。

TTC基礎發展很好，也有幸請到在南部有產業推動經驗的林根煌教授擔任執行長，我們兩位將互相搭配，將外部資源帶入TTC，也為TTC訂定了四大發展方針，包括：

1.協助NCC訂定補助方法，推動科專運作制度化。

2.積極爭取相關科技預算，深化中心發展。

3.配合新業務擴充員額，精實人才能量。

4.優化激勵措施，提升同仁工作價值。

而這些努力，我們也逐漸看到中央部會及地方政府的初步正面回應，我和執行長也將持續期勉中心同仁，群策群力、貢獻專業智慧，實現「符合社會期待、創造中心成長及滿足自我實現」之三贏目標。

攻防糾葛16年

談誘捕技術的前世與今生

蔡一郎

前言

誘捕系統（Honeypot）與誘捕網路（Honeynet）在資訊安全領域的技術發展已超過16年，成立於1999年的The Honeynet Project以誘捕技術研究為主的非營利組織，結合了全球資安研究人員，共同投入網路安全資訊收集與威脅偵測系統的發展，累積至今已有相當豐碩的成果，目前全球共有55個分會，分別於各個國家進行資訊安全與誘捕技術的推動，從低互動式的誘捕系統、高互動式的誘捕系統、誘捕網路，到沙箱分析以及情資的統計與分析平臺，透過全球有志於發展誘捕技術的專家與研究人員，分別進行各種系統與平臺的研發，而每年都有新的誘捕系統發表，透過自由軟體的方式，提供給需要的使用者可以自行建置符合需求的誘捕系統。

誘捕技術起源於如何設計與模擬一個系統或網路的架構，而該系統希望可以用於偵測特定的弱點、特定的服務以及針對攻擊者所發起的行為，如何透過所設計好的環境，進行資料的收集與掌握，因此配合誘捕系統與誘捕網路的偵測機制，對於目前重大的系統弱點或是經常被運用進行攻擊的應用服務弱點，都能夠利用誘捕系統所模擬出來的環境，等待來自網路上的可疑攻擊，收集相關的資料以提供做為後續的分析使用。目前在The Honeynet Project的網站（http://honeynet.org/）上經常會發布目前最新的工具與相關的研究成果。

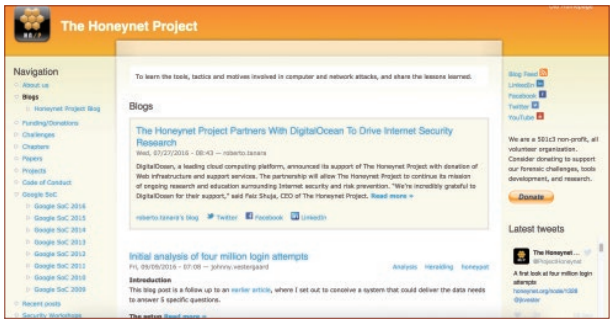

圖1 The Honeynet Project官方網站

每年由不同分會接手主辦的全球年會，有來自各個不同國家的分會成員與資安研究人員齊聚一堂，針對最新的資訊安全議題進行技術上的交流，以今年（2016）的年會主軸，主要在於因應資訊服務環境以及應用程式的多樣化，規劃了物聯網、智慧城市資安威脅以及新型誘捕系統的發佈，希望透過年會的參與討論，聚焦於改

善現在的誘捕技術，以提升在目前資通訊與應用程式運作環境中的偵測能量，而各分會的成員主要由資安產業的研究人員，以及各國家對於資訊安全事件應變的組織來組成。

圖2 The Honeynet Project Annual Workshop 2016

誘捕系統的種類與部署

誘捕系統的種類相當的多，針對不同的系統或是應用服務，大多有可以採用的誘捕系統，用來偵測網路上的異常行為，或是針對誘捕系統所進行的攻擊，透過誘捕系統上的日誌收集，我們可以掌握攻擊者對於誘捕系統所進行的攻擊手法，例如：發動攻擊的對象、下達的指令等，這些資訊都有助於我們可以進一步的瞭解攻擊者的目的以及所採用的攻擊手法，後續以做為資安防禦上的參考。

目前由The Honeynet Project所發展出來的相關誘捕技術，可以分成3個不同的面向，分別是「誘捕系統（Honeypot）」、「惡意程式分析（Malware Analysis）」以及「工具（Tools）」，其中最重要的就屬誘捕系統的發展，在不同的誘捕系統中又可以細分為「高互動式」、「中互動式」以及「低互動式」，不同的互動程度代表者當誘捕系統遭受到來自網路上的攻擊時，系統本身將會提供回應程度，以低互動式的誘捕系統而言，當接收到來自網路上的攻擊時，大多的依據所設定好的條件進行回應，同時進行資料的收集，因為採用的是系統、應用服務以及弱點模擬的方式，因此大多是針對特定的系統與應用程式漏洞進行偵測，如果超出預設的環境範圍，低互動式的誘捕系統能夠掌握的資訊將會受到限制，反之如果為高互動式的誘捕系統，採用的是擬真或是真實系統環境的部署方式，對於誘捕系統的管理以及所建置的應用服務，在安全上的考量將會比採用低互動式的誘捕系統來得嚴謹，因為如果在安全的設備或是系統本身出現問題時，將可能讓誘捕系統轉而成為攻擊者進行攻擊時的跳板，而衍生新的資訊安全問題。

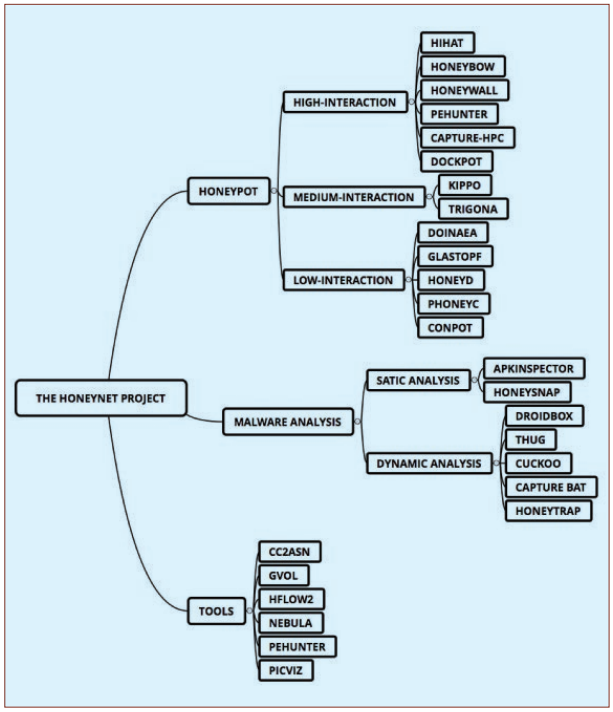

圖3 The Honeynet Project所發展的工具

除了各種不同類型的誘捕系統之外，其中以惡意程式的分析工具或是沙箱測試（Sandbox）的工具最為實用，透過誘捕系統對於網路攻擊威脅的資訊收集，其中不乏可以掌握惡意程式的散播，以目前造成絕大多數的資訊安全事件而言，惡意程式的威脅仍然是資安事件發生的主要原因之一，大多數的資訊安全事件，都與惡意程式的散播與對於系統的影響有關，因為配合誘捕系統進行惡意程式樣本的收集，之後便可進一步的使用惡意程式分析的工具，針對惡意程式進行細節的分析，以掌握更多有用的資訊，例如：惡意程式中繼站的位址等；針對惡意程式的分析，主要可以分成「靜態分析（Static Analysis）」以及「動態分析（Dynamic Analysis）」兩大類型，其中以靜態分析而

言，大多採用APKInspector以及Honeysnap之類的工具軟體，針對惡意程式本身進行程式結構以及運作流程的分析，大多數的情況在進行靜態分析時，就有機會可以找出隱藏在程式中的惡意程式碼，也可以進一步瞭解這些惡意程式所造成的影響範圍，例如：對於系統的影響、攻擊的弱點等，這些都有助於對於惡意程式的行為，有更進一步的掌握。

針對惡意程式所進行的靜態分析工作，常常需要耗費許多的人力與時間，因此除了使用靜態分析的方式進行惡意程式的分析之外，多數的情況下，我們亦可以利用動態分析的方式，進行惡意程式的分析，收集與分析惡意程式在觸發與執行的過程，對於系統、網路通訊、檔案系統等方面的影響；惡意程式樣本的分析，目前大多以Cuckoo Sandbox（https://www.cuckoosandbox.org/）進行動態的分析，在時間效益上較佳，可以在5到10分鐘的時間內，就可以完成一個惡意程式樣本的分析，再由所產生的報告，瞭解該樣本的行為屬性，以及對於系統所造成的影響。

在建置誘捕系統之後進行資料分析，主要以誘捕系統所產生的系統日誌為主，從所記錄下來的日誌內容，我們可以知道攻擊者的來源位址，攻擊的弱點與漏洞，攻擊的目標，如應用服務的種類或使用的通訊埠，利用統計分析的方式，就能夠掌握攻擊者可能的來源、採用的攻擊手法，以及攻擊目標等相關的資訊，以做為資安預警資訊的來源；以目前而言有幾種常見的資料分析方式，如果所建置的誘捕系統數量不多，大多數能夠收集到的資料量應該可以透過統計的方式，以攻擊來源的IP位址、受攻擊的目標位址、通訊埠等資訊進行統計，將排序在前面的攻擊來源納入威脅來源的名單，以建立後續追蹤的目標，另外也針對進行的攻擊手法進行分析，以確定防禦的機制，例如：針對應用服務進行的攻擊手法，大多與應用層的通訊協定以及對應的應用服務有關，例如：網站伺服器的組態設定或是使用存在弱點的軟體版本，這些都是可能造成攻擊者在發展攻擊的過程中，能夠利用這些已知的問題，對於受攻擊的目標造成實質的影響。

在部署誘捕系統或是誘捕網路時，針對特定的需求，可以選擇想要使用的誘捕系統進行架構，不過目前已有發展出具備多種誘捕系統的整合平臺，可以同時具備多種誘捕系統，其中以HoneyDrive以及T-Pot最為實用，將多種常用的誘捕系統整合在單一個作業系統之中；首先以HoneyDrive為例，目前HoneyDrive已發展到第三版，相較先前的版本，不論在系統界面以及相容性而言，都已相當的穩定，對初學者而言，可以減少建置誘捕系統時，需要處理將多個誘捕系統建置在單一運作環境時，所需要解決的套件版本間的相容性問題，也可以加速誘捕系統的建置，利用所提供的管理平臺，就可以知道目前所有啟用的誘捕系統，當時的狀態以及針對所收集到的日誌紀錄進行相關的分析。

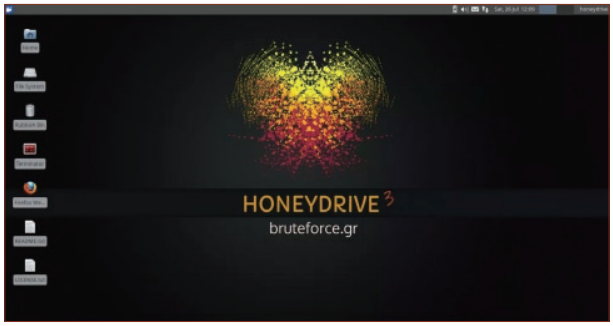

圖4 HoneyDrive

目前第三版的HonyeDiver，預先安裝了Kippo、Dionaea、Amun、Glastopf、Wordpot、Conpot、Thug以及PhoneyC，涵蓋了目前我們在系統上常用的網路應用服務，同時可以針對這些常用的服務進行網路攻擊資訊的收集工作；網路上發布的版本以OVA的檔案格式提供，在使用上建議可以直接將HoneyDrive建置在虛擬主機的環境中，除了部署上的便利之外，也可以有效的利用現有的資源，快速的建置誘捕系統。目前預先安裝好的誘捕系統，參數的設定上多採用預設值，建議可以依實際的部署情況進行變更與調整，如果所使用的環境屬於多網段（多網卡）的環境，在設定網路的組態時，必須特定留意網路組態的正確性，避免因為設定上的錯誤而影響到資料的收集來源。

除了HoneyDrive之外，目前T-Pot（http://dtag-dev-sec.github.io/）也是許多資安研究人員會使用的整合套件，其中也是預先安裝了多種誘捕系統，包括了

glastopf、kippo、honeytrap、dionaea誘捕系統，以及suricata網路安全入侵偵測／防禦系統、ELK資料分析平臺等工具，透過整合的架構提供使用者從資料的偵測收集到分析應用的平臺。

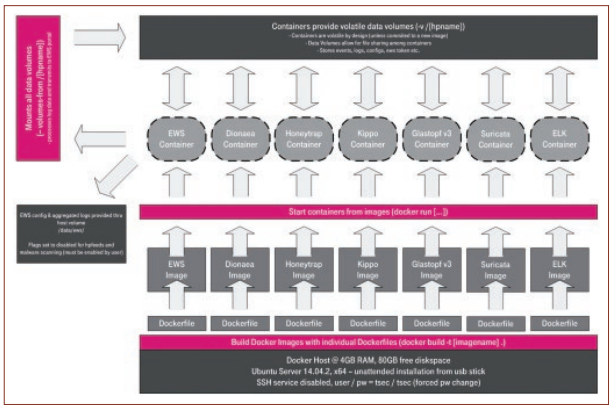

圖5 T-Pot架構圖

因為T-Pot採用最新的Docker技術進行建置，在系統維運管理上相對較為容易，也可以依據本身在部署上的需求，進行個別誘捕系統的環境設定，再由整合的日誌系統與搜尋界面，提供使用者可以快速的發現由誘捕系統所偵測到的攻擊行為，也可以配合系統偵測的結果，發展出資安設備可以使用的防禦規則，以提供進一步關於資安防禦機制的建立。

如果不採用T-Pot的系統架構，也可以直接選擇使用由Docker所提供的環境，目前The Honeynet Project在Docker的社群（https://hub.docker.com/u/honeynet/）上，已提供了多種誘捕系統的檔案，可以提供給使用者直接下載並安裝到Docker的環境中，開始後立即可以使用誘捕系統所提供的功能，目前絕大多數常見的誘捕系統，在這都已提供了相關的檔案可供下載使用。

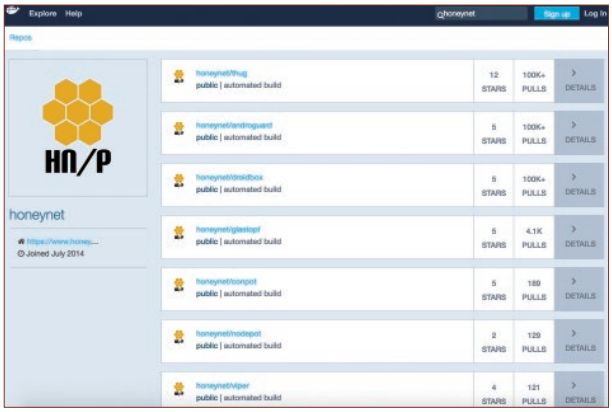

圖6 Honeynet Project在Docker上的資源

誘捕系統在臺灣的發展

自從2008年臺灣正式成立臺灣分會，並加入The Honeynet Project組織成為正式的成員，就透過分會每年辦理的大型臺灣誘捕技術會議（HoneyCon），以及針對誘捕技術相關議題進行學研分享，在臺灣進行誘捕技術的推動，並協助有興趣建置誘捕系統的研究人員相關的建置經驗，今年（2016）已是第八年在臺灣辦理HoneyCon，除了介紹最新的誘捕技術之外，也邀請來自國外的The Honeynet Project分會成員以及資安研究人員與專家，共同針對最新的資安議題進行分享，也提供給國內的與會人員，掌握全球最新誘捕技術與資安發展趨勢的機會。

圖7 HoneyCon 2016

在HoneyCon的舉辦期間，針對資安的技術也同步辦理了多場次的實作課程，透過實務的課程與演練，可以提供學員能夠在短時間之內，掌握誘捕系統的建置與部署技巧，以及對於資安工具的使用經驗，可以提升國內資訊從事人員對於資安技術的精進。

目前在國內許多大專院校以及資安的研究人員，也部署了許多的誘捕系統，而部署的方式與應用，主要依據不同的需求而定，其中以部署在資安設備之外以及對外服務的應用服務伺服器網段最多，但亦不乏將誘捕系統部署於企業內部網路的情況，因此針對不同的需求，誘捕技術都可以配合當時的網路環境，發揮出不同的應用，不過在規劃與部署的階段，需要確定部署誘捕系統的目的與需求，才能夠在選擇誘捕系統時，找到符合需求的誘捕系統，也可能配合部署環境的網路組態進行偵測機制的調整。

惡意程式的分析屬於資安專業的領域，資安的研究人員以往想要取得惡意程式的樣本與相關的分析報告，往往需要花費許多時間，而所取得的惡意程式也可能存在其它的資安問題，這對於從事資安研究而言是一個需要解決的問題，國家高速網路與計算中心（http://www.nchc.org.tw），在2013年正式發佈了國內第一個公開使用的「惡意程式知識庫」（https://owl.nchc.org.tw/），並於2016年進行改版，以提供更多樣化的功能，包括了惡意程式的分類、樣本的搜尋等，利用惡意程式知識庫所提供的資料，資安研究人員可以針對有興趣的樣本進行分析，並且利用本身所建立的測試環境，進行靜態分析或是動態分析，對於惡意程式所衍生的行為，可以提供完成分析的報告，而目前惡意程式知識庫主要的樣本來源，主要於國內所部署的誘捕系統，以及來自於國際間資安組織的交流，透過國際間的合作，讓臺灣成為全球資安偵測網路的一員，有效的掌握網際網路的資安威脅，以及惡意程式的發展趨勢。

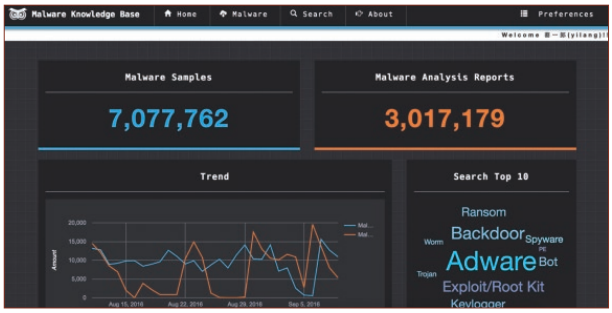

圖8 惡意程式知識庫

目前惡意程式知識庫每天新增的惡意程式超過1萬個，由此可知目前許多的資訊安全的威脅，由惡意程式所引發的仍然是主要的來源之一，例如：利用惡意程式所組成的殭屍網路，針對特定的目標發展分散式的阻斷服務攻擊，就是一個相當典型的網路攻擊手法。

結語

長久以來誘捕技術是資安研究人員與資安產業發展網路安全行為特徵時，經常選擇使用的資訊技術，除了可以提供高度彈性的部署方式之外，由The Honeynet Project多年來所發展出來的工具軟體，隨著時代的演進，目前已相當的完整，不論是採用傳統實機部署的方式，或是透過雲端服務平臺進行架設，也可利用最新的容器（container）技術，使用像Docker之類的資訊技術進行誘捕系統的部署，都能夠發揮各個不同誘捕系統所能夠提供的功能；目前誘捕系統已經從早期的攻擊日誌收集與分析，發展到惡意程式的誘捕與網路封包的側錄，對於資安研究而言，提供了更完整且多樣化的資料，可以針對不同的研究議題進行更多的分析，對於發覺新型態的網路攻擊手法而言，將會有更多樣化的可行性，能夠讓我們發掘可能潛在其中的網路攻擊行為，而不同的攻擊手法對於誘捕系統也會產生不同的結果；而目前誘捕系統也發展出高互動式的架構，透過網路上的互動以及擬真出來的場景，能夠掌握更完整的資料，將會有助於後續針對網路攻擊手法的研究以及資訊安全事件應變時，需要提供的佐證資料，目前許多的單位已將誘捕系統與對外的資安防禦架構進行整合，將誘捕系統所發現的攻擊來源，配合網路設備所產生的Netflow資料以及應用服務伺服器所留存的系統日誌，進行多參數的交叉比對，除了可以確認攻擊者的攻擊手法是否成功之外，也可以針對攻擊者對於企業或是組織內的系統影響範圍，進行更全面的比對分析，往往我們可以透過擴大比對惡意攻擊來源位址的方式，發現其它的受害主機，或是曾經遭受相同來源攻擊的紀錄，這些資訊對於強化資安防禦的整體成效而言，是相當重要而有價值的情資。

（作者為臺灣雲端安全聯盟理事長）

標準5細則 隱私不外洩

行動寬頻基站資安管理方針

許博堯

一、前言

電信網路為國家資訊化的重要基礎設施，行動寬頻網路扮演電信網路中的重要構件，隨著行動寬頻網路持續演進、用戶與資訊訊務量不斷增長，安全威脅日益成為行動寬頻網路的重要課題，欲解決這些安全威脅，國際間已有不同電信與資訊安全組織持續推動行動寬頻資安標準，考量通信環境不斷變化與演進需求，各組織依據設備製造、業者環境、使用者等面向，設計周延、合宜的行動寬頻資安標準，以促進行動寬頻服務發展，並同時兼顧資訊安全。

二、國際標準

（一）NIST SP 800-53

美國聯邦資訊安全管理法（Federal Information Security Management Act, FISMA）定義了一個廣泛的框架來保護政府資訊、運作與財產，以及面對天然及人為威脅。在FISMA實施以來，由美國國家標準和技術研究院（National Institute of Standards and Technology, NIST）擬訂相關的安全控制措施，其中包括聯邦資訊系統與組織之安全控制建議書SP 800-53（Recommended Security Controls for Federal Information Systems and Organizations），該建議書為資訊安全風險管理框架的重要構件，透過安全控制措施選擇和程序化的概念，協助規定資訊系統安全控制措施，為安全管理者、安全服務提供者、安全技術開發人員、系統開發人員、系統實施人員和系統評估人員提供指導原則。SP 800-53 將安全控制區分18個家族，各家族皆具備相關安全功能的控制措施，共205項安全控制措施。18個家族均指定一個二字元識別碼，同時區分為管理、運作與技術三類別之安全控制措施。其中，管理類別著重資訊系統安全與風險管理；運作類別著重操作人員的實行，技術類別著重資訊系統所包含硬體、軟體或韌體的運行。如表1說明。

（二）ISO/IEC 27001:2013

ISO/IEC 27000系列為國際間受到認可的資訊安全管理標準，也是通傳會（國家通訊傳播委員會）建議電信業者實施資通安全管理作業之參照標準，ISO/IEC 27001:2013標準提供建立、實作、維持及持續改善資訊安全管理系統，其中組織全景、領導、規劃、支援、運作、績效評估、改善為落實資訊安全管理系統的主要標準，分別透過規劃、執行、查核與行動（Plan-Do-Check-Action, PDCA）進行活動確保可靠度目標達成，並進而促使品質持續改善；附錄A羅列14項控制領域（A5~A18，如圖一說明）、35項目標、114項控制措施，各控制領域之控制措施皆可以提供企業實行資訊安全管理系統之參考依據。

表1 安全控制識別碼與家族名稱

識別碼	家族	類別
AC	存取控制（Access Control）	技術
AT	認知與訓練（Awareness and Training）	運行
AU	稽核與責任（Audit and Accountability）	技術
CA	安全評估與授權（Security Assessment and Authorization）	管理
CM	組態管理（Configuration Management）	運行
CP	應變計畫（Contingency Planning）	運行
IA	鑑別與認證（Identification and Authentication）	技術
IR	事件回應（Incident Response）	運行
MA	維護（Maintenance）	運行
MP	媒體保護（Media Protection）	運行
PE	實體與環境保護（Physical and Environmental Protection）	運行
PL	規劃（Planning）	管理
PS	人員安全（Personnel Security）	運行
RA	風險評估（Risk Assessment）	管理
SA	系統與服務取得（System and Services Acquisition）	管理
SC	系統與通訊保護（System and Communications Protection）	技術
SI	系統與資訊完整性（System and Information Integrity）	運行
PM	計畫管理（Program Management）	管理

資料來源：本研究整理

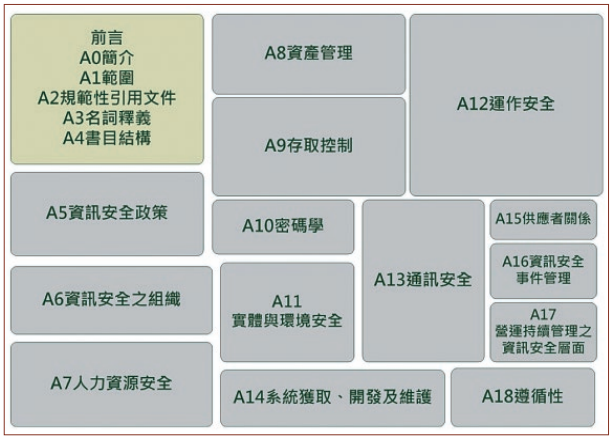

圖1 ISO 27001:2013控制措施
資料來源：本研究整理

三、國際標準適用分析

基於前述兩標準適用基站之控制措施，為評估與基站相關重要資產，即透過控制措施欲保護之對象，將基站重要資產區分為物理與資訊資產，物理資產涵蓋基站硬體設施與相關環境，以基站硬體設施安全防護為主；資訊資產涵蓋基站內部資訊，包括軟韌體、設定組態、金鑰、用戶層資料、控制層資料等，以基站系統安全防護為主。初步可歸納5項保護基站物理與資訊資產實行細則，分別為實體與環境安全、存取控制、系統與通信、維運管理、稽核紀錄，如圖2說明，5項實行細則將匯集兩標準控制措施之異同控制措施，以研擬基站資安管理方針。

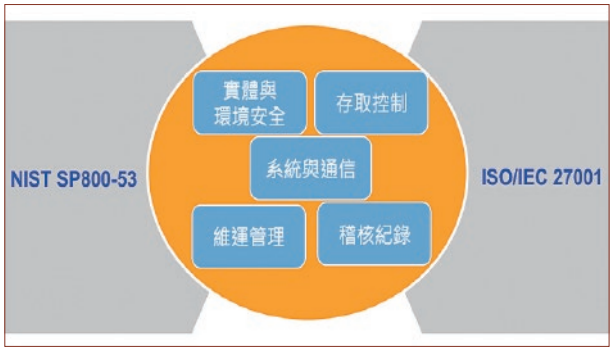

圖2 實行細則
資料來源：本研究整理

四、基站資安管理方針

各管理方針與控制措施係以ISO 27001:2013附錄A控制措施與NIST SP 800-53控制措施為基礎，並依據「ITU-T X.805通信系統安全框架」，以及3GPP規定之基站安全要求，歸納基站安全管理方針，管理方針係為原則性方法，闡明基站管理與安全性控制的策略。施行單位可依據基站系統特性與環境在符合管理方針的前提下，實施適當之控制措施，同時也得考量自身安全目標，考慮設置其它控制措施。

（一）實體與環境安全

為保護基站設施的實體與環境安全，除透過環境保護措施外，軟硬體外在的防護措施也有實施必要性，以降低發生資訊安全事件的機率。實體與環境為基站安全首要防線，再縝密的處理程序及規範，若無法確實落實實體及環境安全，則無法發揮保護作用，因此，此部分管理措施的落實與否，實為基站資安管理之基石。

1.比較分析

在實體與環境安全方面，分析兩標準適用於基站的控制措施，可再細分區域安全與實體控制、環境安全兩部分，區域安全與實體控制以實體控制為主，環境安全以設備安置保護為主。兩標準在此實施細則上大同小異，NIST SP 800-53將防範外部及環境威脅細分多種控制措施，例如防水、防火、斷電處理、纜線保護等。

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
區域安全與實體控制	· A11.1.1實體安全週界 · A11.1.3保全之辦公室、房間及設施 · A11.1.5於保全區域之工作 · A11.1.2實體進入控制措施 · A11.2.2支援之公用服務事業	· PE-2實體存取權限 · PE-3實體存取控制 · PE-4傳輸媒體的存取控制 · PE-6實體存取的監控 · CM-5存取限制更動
環境安全	· A11.1.4防範外部及環境威脅 · A11.2.1設備安置及保護 · A11.2.3佈纜安全	· PE-9電力設備與纜線 · PE-10緊急斷電 · PE-11緊急備用電源 · PE-12緊急照明 · PE-13防火 · PE-14溫濕度控制 · PE-15防水

2.管理方針建議

（1）區域安全與實體控制

· 擬訂基站實體安全與環境控制程序，並依規定施行實體安全與環境控制措施，同時進行人員認知訓練；

· 以基站設施所在區域為基礎，設置必要的管制，避免基站相關設施遭受未經授權的實體存取；

· 定期評估實體安全控制的有效性；

· 考量變更與過去的事件，檢視與更新實體安全的政策與措施。

（2）環境安全

· 宜檢查及評估可能影響基站運作之環境因素，例如火災、水、電力供應、溫濕度等，並建置相應之環境控制；

· 電力與通信纜線應予適當保護，以防範竊聽、干擾或損壞。

（二）存取控制

擬訂並維持適當的存取控制程序，鑑別（Identify）基站系統的存取行為，只有已授權、程序、裝置與經授權活動能使用基站系統與網路，降低資訊或檔案遭竊取的威脅，任何對基站系統存取的人員與行為，皆須訂定相關規範與機制，防止外部人員存取使用，同時降低內部洩露的可能。

1.比較分析

在存取控制方面，分析兩標準適用於基站的控制措施，可再細分存取管理與遠端存取兩部分，存取管理以身分鑑別為主，除身分鑑別外，也包含身分與存取管理，NIST SP 800-53 SC-41特別條列設備端口與I/O的限制存取，即管理基站系統的邏輯與實體存取介面。遠端存取說明遠端存取基站系統的控制措施，NIST SP 800-53 SC-10網路斷開連結也適用於基站遠端存取管理，針對逾時的遠端連線，應終止其通信會話，且結束相關的網路連結。

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
存取管理	· A9.1.1存取控制政策 · A9.2.1使用者註冊及註銷 · A9.2.2使用者存取權限之配置 · A9.2.4使用者之秘密鑑別資訊的管理 · A9.2.5使用者存取權限之審查 · A9.2.6存取權限之移除或調整 · A9.3.1秘密鑑別資訊之使用 · A9.4.1資訊存取限制 · A9.4.2保全登入程序 · A9.4.3通行碼管理系統 · A9.4.4具特殊權限公用程式之使用 · A9.4.5對程式源碼之存取限制	· AC-1存取控制政策與步驟 · AC-2帳號管理 · AC-3進行存取控制 · AC-5職責分工 · AC-6最小權限 · AC-7失敗的登錄測試 · AC-10並行會話控制 · AC-11會話鎖定 · AC-12會話終止 · IA-1識別認證策略與程序 · IA-2識別與認證 · IA-3設備識別與認證 · IA-4識別碼管理 · IA-9服務識別與認證 · CM-5存取限制更動 · CM-7最小功能 · SC-41端口與I/O存取
遠端存取	· A6.2.2遠距工作	· AC-17遠端存取 · SC-10網路斷開連結

2.管理方針建議

（1）存取管理

· 擬訂基站系統的存取程序，包含角色、權限、分配與取消存取程序，確保在符合程序下存取基站系統，同時進行人員認知訓練；

· 使用者與基站系統使用唯一ID，存取服務或系統前須經過認證；

・實施基站系統的邏輯存取控制，僅允許經授權使用；

・監控基站系統之存取情形；

・評估基站系統存取控制程序的有效性，並定期檢查存取控制措施的有效性。

（2）遠端存取管理

・擬訂遠端存取安全程序，依規定實行遠端存取措施，同時進行人員認知訓練。

（三）維運管理

為確保正確以及安全的操作基站設施與系統，降低各種可能的風險與損害，維護基站系統與通信作業之完整性及可用性，必須設立系統與通信維運之管理措施。

1.比較分析

在維運管理方面，分析兩標準適用於基站的控制措施，可再細分運作管理與設備維護兩部分，運作管理以基站系統操作安全性為目的，ISO 27001 A12.1.2變更管理涵蓋影響資訊安全之組織、營運過程、資訊處理設施及系統的變更，與NIST SP 800-53 CM-3、CM-6一致，此外NIST SP 800-53 CM-10軟體使用限制可呼應3GPP安全要求：基站應使用經授權的資料或軟體要求。設備維護說明基站系統維護作業，NIST SP 800-53 細分MA-3維護工具、MA-4遠端維護與MA-5維護人員的控制措施。

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
運作管理	・A11.2.5財產之攜出 ・A11.2.7設備汰除或再使用保全 ・A12.1.1文件化運作程序 ・A12.1.2變更管理 ・A12.4.4鐘訊同步	・PE-16攜出入與拆卸 ・CM-3組態（Configuration）更動控制 ・CM-6組態設定 ・CM-10軟體使用限制 ・CM-11由使用者安裝的軟體
設備維護	・A12.1.1文件化運作程序 ・A11.2.4設備維護 ・A6.2.2遠距工作	・MA-1系統維護策略與程序 ・MA-2受控制之維護 ・MA-3維護工具 ・MA-4遠端維護 ・MA-5維護人員

2.管理方針建議

（1）運作管理

・擬訂基站系統運作程序，並進行人員認知訓練，確保在符合程序下操作與管理基站系統；

・基站相關設備、資訊或軟體未經授權禁止更動；

・含有儲存媒體之基站設備組件，於汰除前或再使用前應查證，確保任何機密性、敏感性的資料及有版權的軟體已經被移除；

・建立基站系統變更程序，並依據程序進行變更。

（2）設備維護

・擬訂基站系統維護程序，並進行人員認知訓練，確保在符合程序下維護基站系統；

・建立遠端維護與診斷之認證機制。

（四）稽核紀錄

為掌握基站系統活動全貌，應規劃符合情理的稽核原則與措施，使合法使用者為其作業行為負責，對於未經授權活動加以偵測與追縱，降低安全威脅、改善安全作業。

1.比較分析

在稽核紀錄方面，分析兩標準適用於基站的控制措施，ISO 27001:2013於A12.4存錄及監視中說明如何紀錄事件與產生證據，另於A12.7.1資訊系統稽核控制措施說明稽核活動應最小程度影響營運過程。NIST SP 800-53則於AU家族中詳細說明稽核作業，包括策略及程序、內容、回應、分析與報告、同時也強調不可否認性，即使用者操作的責任，以及稽核存底保護的相關措施。

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
稽核紀錄（Log）	・A12.4.1事件存錄 ・A12.4.2日誌資訊之保護 ・A12.4.3管理者及操作者日誌 ・A12.7.1資訊系統稽核控制措施	・AU-1稽核與問責策略及程序 ・AU-2稽核事件 ・AU-3稽核紀錄內容 ・AU-4稽核儲存容量 ・AU-5稽核處理失敗回應 ・AU-6稽核監控、分析與報告 ・AU-7稽核摘要與產生報告 ・AU-8時間戳記 ・AU-9稽核資訊保護 ・AU-10不可否認性 ・AU-11稽核儲存

2.管理方針建議

・擬訂基站系統稽核措施，確保在符合程序下進行基站系統稽核措施，同時進行人員認知訓練；

・稽核紀錄應包括事件類型、起因、結果等說明；

・保護稽核紀錄應避免未經授權存取、修改與刪除。

（五）系統與通信保護

為保護基站系統處理、使用及傳輸時的機密性與完整性，應藉由安全防護控制措施，確保有效使用系統安全檢測及防護技術，保護資訊之機密性、鑑別性及/或完整性。

為確保對基站系統及其中資訊之保護，降低各種可能的風險與損害，維護基站系統與通信功能之完整性及可用性，應設立通信安全之管理措施。

1.比較分析

在系統與通信保護方面，分析兩標準適用於基站的控制措施，可再細分系統保護、通信保護、密碼保護三部分，分別說明如下：

- 系統保護以基站系統安全性為目的，皆強調脆弱性掃描與惡意程式碼的重要性，NIST SP800-53 SC-5特別說明阻斷服務保護，基站系統應具備阻斷服務保護的控制措施，以確保基站系統與通信功能可用性。
- 通信保護以傳輸保密性與完整性為目的，適用於基站系統提供的通信功能與遠端連線功能，NIST SP 800-53 SC-11信任路徑適用於基站系統的通信鏈路建立，包括S1、X2或是遠端連線，而NIST SP 800-53 SC-31隱藏通道分析則適用基站系統應檢測是否有不明的通信鏈路。
- 密碼保護為基站系統具備之加密功能，適用於基站的身分認證機制以及通信保密與完整性機制，也包括金鑰管理，就基站系統而言，應以符合3GPP標準為基準，即具備3GPP規定之加密演算法與憑證技術，例如EIA-1、EIA-2、EIA-3。

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
系統保護	· A12.6.1技術脆弱性管理 · A12.2.1防範惡意軟體控制措施	· RA-5脆弱性掃描 · SC-5阻斷服務保護 · SI-2弱點修補 · SI-3惡意程式碼防護
通信保護	· A13.1.1網路控制措施	· SC-8傳輸保密性與完整性 · SC-11信任路徑 · SC-31隱藏通道分析
密碼保護	· A10.1密碼式控制措施	· SC-12加密金鑰建立與管理 · SC-13密碼保護 · SC-17公鑰基礎設施憑證

2.管理方針建議

（1）系統保護

- 擬訂系統與通信保護程序，包括系統保護、通信保護、密碼保護，並依據程序規定實施系統與通信保護措施，同時進行人員認知訓練；
- 建立基站系統脆弱性評估機制，取得基站系統中之脆弱性資訊，並採行適當改善措施；
- 基站系統應採行適當之防護措施，防範惡意軟體、阻斷服務攻擊等安全威脅。

（2）通信保護

- 基站系統與通信鏈路應具備3GPP規定之通信保護功能，確保資訊傳輸保密性與完整性。

（3）密碼保護

- 基站系統應具備3GPP規定之資訊加密功能；
- 基站系統應具備3GPP規定之金鑰管理功能，包括金鑰生成、使用、保護及生命週期管理。

五、結語

基站資安管理方針可為基站設備與系統之安全防護提供指引，進而確保電信業者機密資訊與其客戶個人隱私不外洩，然而再嚴謹的管理方針，仍應透過管理程序、落實各項控制措施、人員認知訓練，降低基站安全風險。此外，若以資訊安全標準觀之，最終仍需電信業者透過制度面的PDCA（Plan、Do、Check、Action）循環管理，持續改善與調整，才能完善基站設備與系統之安全防護。

（作者為財團法人電信技術中心副工程師）

資安檢測353 手機安全不鬆散

智慧型手機系統內建軟體資安檢測規劃現況

基礎設施事務處

一、前言

資策會FIND公布於104年7月調查結果顯示，國內12歲以上使用智慧型手機或平板電腦者已達到1,604萬人，約每4人便有3人為行動裝置使用者。其中智慧型手機普及率約73.4%，推估約1,525萬用戶，平板電腦普及率約32%，預估約有665萬使用人口，同時擁有兩種裝置的用戶比率則是28.2%，國人平均每天花197分鐘使用智慧型手機，顯示各類行動裝置在客戶生活中已是重要的一部分。愛立信（ERICSSON）於105年8月發表最新行動趨勢報告，報告中預計智慧型手機的使用者數量將在105年Q3超越基本型手機。到了2021年，智慧型手機用戶數量更會從目前的34億成長到63億，如果預測全球人口到2020年將會達到76億左右，代表屆時將會是幾乎人手一支智慧型手機的景況。

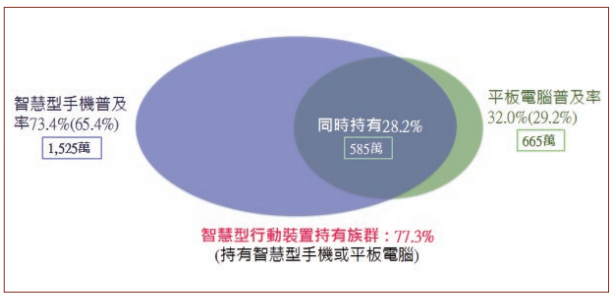

圖1 2015H1臺灣行動族群樣貌
資料來源：資策會Find

行動裝置的普及，為人們的生活帶來許多便利以及樂趣；然而隨之產生的安全議題也逐漸浮上檯面，資安廠商賽門鐵克旗下諾頓於105年6月份發表的「諾頓行動生活調查報告」[1]中發現81%受訪臺灣民眾經歷來自行動裝置的威脅，損失總金額高達新臺幣296億元。行動裝置成為現代生活中不可或缺的一部分，超過半數以上擁有行動裝置的臺灣民眾同時擁有智慧型手機及平板電腦，並傾向使用智慧型手機或平板電腦多於電腦上網。智慧型手機、平板電腦這類型行動裝置，正改變我們的生活習慣、改變這整個世界！

是以，行動裝置的安全已成為保護機敏資料的重要議題，原本專注於電腦的惡意軟體攻擊已移轉到手機及應用程式上，攻擊主要可分為以下4大種類[2]：

- 作業系統攻擊（OS Attacks）
- 手機應用系統攻擊（Mobile App Attacks）
- 通訊網路攻擊（Communication Network Attacks）
- 惡意軟體攻擊（Malware Attacks）

二、NCC重視手機系統內建軟體安全

智慧型手機基於高度可攜性與便利性，有效提升生產力與工作效率，但隨之而來，使用者也必須面對智慧型手機所帶來的資安威脅。有鑒於此，行政院國家資

通安全會報於103年6月24日第26次會議決議，參考各國手機管制機制及協調我國相關政府機關分工，由經濟部主管手機與電腦之應用軟體基本資安規範，另智慧型手機屬電信法第42條規定之電信終端設備，其出廠時已內建之軟體基本資安規範，則由國家通訊傳播委員會（以下簡稱本會）主管。為配合前述會議決議，本會參考國際標準及歐美等國作法，對於智慧型手機系統內建軟體資通安全檢測之安全等級、各等級包含之檢測細項，及各檢測細項之檢測條件、檢測方法與判定標準等事項具體規範，訂定「智慧型手機系統內建軟體資通安全檢測技術規範」草案（以下簡稱「本規範」），作為智慧型手機製造商、電信業者、我國代理商及資通安全檢測實驗室辦理檢測之依據。

本規範適用於智慧型手機系統及其系統內建軟體，以確保其符合出廠階段資訊安全要求，但不包含使用者於內建軟體中自行下載之附加服務或內容。然而資通安全本質為風險控管概念，智慧型手機系統內建軟體經檢測通過後，並不能保證受測後之智慧型手機於使用時不會被惡意破解或遭到駭客攻擊，使用者應搭配良好的使用習慣，並隨時提高資安警覺，才能降低資安問題所帶來的風險與影響程度。

三、智慧型手機系統內建軟體資通安全檢測技術規範草案概述

本規範主要檢測智慧型手機系統內建軟體資通安全，所有智慧型手機不分作業系統（包含Android、iOS或Windows作業系統）皆可進行檢測，智慧型手機之製造商、電信業者或我國代理商皆可申請智慧型手機系統內建軟體資通安全檢測及審驗。

（一）內建軟體屬性

智慧型手機系統內建軟體（以下簡稱內建軟體）指智慧型手機製造商或電信業者於出廠或銷售時已預設安裝之應用軟體，包含首次連結網路後自動安裝之應用軟體，於本規範中區分為出廠預載軟體、銷售商加載軟體及無圖示軟體3種屬性，如圖2。

（二）檢測層別與項目

依據國際間對智慧型手機安全之分層概念，將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層5個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別分別訂定檢測項目。

圖2 內建軟體屬性
資料來源：本會整理

表1 檢測層別與安全性說明

檢測層別	安全性說明
資料層（Information/Data）	資料之安全性主要包含資料的傳送、儲存或使用等相關安全，並應確保使用者資料避免遭系統內建軟體未經授權之蒐集、分享、使用、刪除、竄改及儲存。
應用程式層（APPs）	應用程式之安全性主要包含程式信任來源、執行授權等相關安全，並應確保內建軟體避免未經授權存取系統資源。
通訊協定層（Protocol）	通訊協定之安全性主要包含無線傳輸技術及通訊協定等相關安全，並應確保使用者對資料之傳輸、周邊設備之連接的可控管性。
作業系統層（Operating System）	作業系統之安全性主要包含作業系統相關服務與身分辨識等相關安全，並應確保作業系統對系統資源之保護、提醒，並讓使用者於知情的狀況下進行更新。
硬體層（Hardware）	硬體之安全性主要包含金鑰與演算模組等安全，並應確保金鑰管理、存放之保護，及演算法之安全強度符合國際規範，並讓使用者於知情的狀況下進行更新。

表2 檢測項目及安全需求說明

層別	檢測項目	安全需求
資料層(D)	1.資料使用授權	手機系統內建軟體對敏感性資料進行存取前，應取得使用者同意。
	2.資料儲存保護	手機系統內建軟體應將敏感性資料儲存於作業系統保護區域，並提供資料加密功能，以避免敏感性資料遭不正當方式存取。
	3.資料遺失保護	手機系統應提供資料保護與備份功能，以避免資料外洩和防止資料損失。
應用程式層(A)	1.程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
	2.程式信任來源	手機系統內建軟體應確認付費功能機制與資料來源的安全。

層別	檢測項目	安全需求
應用程式層(A)	3.程式執行授權	手機系統內建軟體所執行的行為，應取得使用者同意，並與其宣告之內容相符。
	4.程式執行安全	手機系統內建軟體應具備惡意字串輸入時的處理能力。
通訊協定層(P)	1.協定使用授權	手機與外部設備進行連接時，應給予使用者相對應的提示，並提供開啟及關閉無線傳輸技術之功能。
	2.協定傳輸保護	手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法，並避免可能的傳輸攻擊。
	3.協定執行安全	手機系統應具備通訊協定內容的錯誤處理能力。
作業系統層(O)	1.系統操作授權	手機系統所執行的行為，應取得使用者同意，必要時並提供風險提示。
	2.系統身分辨識	手機系統應提供安全的身分辨識及保護機制。
	3.系統執行安全	手機系統應具備程式執行期的記憶體保護機制，並提供安全回報之管道。
硬體層(H)	1.金鑰管理保護	手機之金鑰管理，應符合金鑰使用及管理標準。
	2.演算法強度要求	手機實作之加密、解密及簽章演算法，應符合金鑰演算法標準與初始化向量要求。

（三）安全等級

為配合不同安全需求，本規範將智慧型手機系統內建軟體資通安全等級區分為初級、中級及高級3種，初級為智慧型手機基本隱私保護之最低要求。中級除須符合初級之所有檢測細項外，並增加資料進階保護之檢測細項。高級則為確保智慧型手機之核心底層不會被竄改或不正當地擷取資訊，除須符合初級與中級之所有檢測細項外，並增加手機設計相關安全性文件審查之檢測細項。所有智慧型手機均應通過初級檢測項目之檢測細項，然中級與高級部分則採自願性檢測。

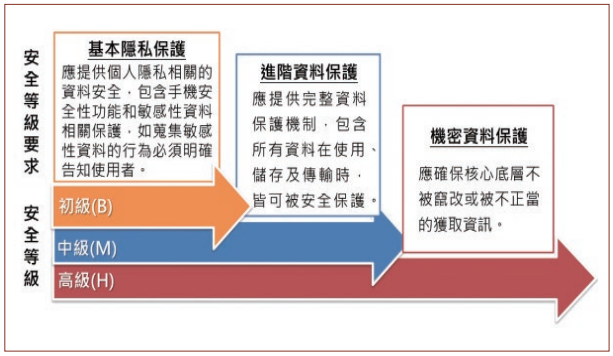

圖3 資通安全等級之要求
資料來源：本會整理

為求檢測規範可適用於各作業平臺，並且將檢測時間與檢測費用等成本建置於合理之範圍內，從目前進行實測的手機檢視，將安全等級初級者設定為基礎資料傳輸，並且適合各作業平臺，部分無法適用於各作業平臺及無圖示軟體之檢測細項，則納入中級之選測項目中，送測單位可自由選擇是否進行檢測。而於檢測編碼上，則由（+）標示為選擇檢測項目。茲將檢測層別、安全等級及檢測項目數量與必測選測項目彙整如表3。

表3 檢測層別、安全等級及檢測項目數量彙整

檢測項目數量		安全等級					
		初級		中級		高級	
		必測	選測	必測	選測	必測	選測
層別	資料層（Information/Data, D）	5	-	0	3	0	-
	應用程式層（Application, A）	6	-	3	2	0	-
	通訊協定層（Protocol, P）	4	-	3	-	0	-
	作業系統層（Operation, O）	6	-	2	-	3	-
	硬體層（Hardware, H）	0	-	0	-	6	-
總計	初級（B）	21個					
	中級（M）	34個；含5(+)					
	高級（H）	43個；含5(+)					

註：(+)為選擇檢測項目數

（四）檢測流程

檢測實驗室係指經本會依「智慧型手機系統內建軟體資通安全檢測實驗室管理作業要點」，或依「智慧型手機系統內建軟體資通安全檢測實驗室試辦認可計畫」認可具檢測能力之實驗室。檢測實驗室應依本規範所說明之適用範圍及檢測項目，對申請者檢附之相關資料及智慧型手機樣品進行書面審查與實機測試，相關檢測流程如圖4。

圖4 檢測流程圖
資料來源：本會整理

四、如何安全的使用智慧型手機

隨著4G、雲端運算、大數據發展成熟，智慧型行動裝置功能升級以及虛擬實境（Virtual Reality，VR）、擴增實境（Augmented Reality，AR）技術持續開發，其多元化應用逐步滲透至各領域。由於智慧型行動裝置硬體規格已經難有進步空間，透過VR於遊戲、娛樂的應用，強調互動行銷、遊戲特色，將可改善用戶體驗，甚至促使消費者購買更高階行動裝置，雖有報告指出到了2021年，預估物聯網裝置的總數量將會達到160億個，物聯網裝置的總數量會超越智慧型手機，各式各樣物聯網裝置如連網的汽車、消費型電子產品、智慧型手表、機器設備等將有顯著的成長，然而智慧型手機仍將會是消費者最常隨身攜帶使用的連網裝置。

因此面對新的資安威脅，使用者不得不慎，以下針對智慧型手機潛在風險，及近年重大手機安全事件說明，並提供使用者正確使用智慧型手機方式與觀念，進一步彙整國內外正確使用智慧型手機之參考指引供使用者參考使用。

（一）手機使用習慣之潛在風險：手機中毒徵兆

在臺灣智慧型手機已成為人們生活必需品，然而在享受行動裝置便利有趣的同時，民眾於手機資安防護意識卻非常薄弱，防毒大廠卡巴斯基的實驗室研究發現，Android木馬病毒可透過藍芽或Wifi快速傳播，不僅回傳手機的相關資訊，更會自動傳送簡訊至手機所有聯絡人，然而這類型病毒卻是看不到、刪不掉，因此許多民眾手機中毒卻渾然不知。

其實手機中毒仍有跡可循，當手機出現下列幾點徵兆，民眾便可懷疑手機是否感染病毒，盡快尋求專業援助，降低受害可能性。

- 使用效能無故變差
- 電池壽命突然變短
- 莫名其妙通話中斷
- 電信費用突然暴增
- 出現自動下載軟體

（二）手機資安事件與犯罪手法：常見手機詐騙手法

手機的方便性已與民眾的生活密不可分，行動網路已成為人人生活中的必需品，手機快速上網更是多數民眾嚮往，傳輸速度快，各裝置間同步連結、資料傳輸方便，但卻衍生更多個人資料安全問題。

對於有心人士而言，竊取資料盜賣是門穩賺不賠的生意，資料量越大獲取價金越高，因此在現代人手一機的社會中，手機犯罪手法不斷推陳出新，目的便是為了竊取個人資料，多變的手機犯罪手法，不外乎可區分為3種媒介：連結網址、APPs及Wifi連線，在此提供3種媒介常見的攻擊手法，提醒使用者注意。

表4 常見攻擊手法彙整表

攻擊媒介與方法	攻擊管道	結果
連結網址 ・含有惡意程式或網站的連結被點選 ・社交工程 ・釣魚網站 勒索軟體	・透過簡訊、通訊軟體（Line或what's APP等）誘發使用者點選惡意連結 ・民眾上網點選惡意連結	・小額付費下載惡意程式 ・自動加密手機內資料要求付費解密
APPs 含有惡意程式之APPs直接或間接被下載	從未知來源下載APPs	・自動傳送惡意簡訊給朋友造成小額付費或使朋友遭受詐騙 ・竊取手機內個人資料造成資料外洩
Wi-Fi 偽裝正常免費Wi-Fi吸引民眾連結	透過免費提供的誘因吸引民眾連結惡意Wi-Fi	・竊取姓名、密碼 ・獲得手機控制權

資料來源：本會整理

綜合上述的攻擊媒介，其實不外乎可區分為4種詐騙型態：結合社群網站與社交工程進行手機簡訊詐騙、網路釣魚惡意連結、勒索軟體綁架手機重要資料、偽冒惡意APPs軟體下載。

1. 結合社群網站與社交工程進行手機簡訊詐騙

手機簡訊認證碼小額付款詐騙事件，不僅是最傳統的簡訊詐騙外，過往的MSN（現在改為Skype）等即時通訊、許多社群網站（如Facebook），以及通訊APP軟體（如Line、What's APP等）皆常出現此類型詐騙手法，駭客假冒手機使用者的親朋好友的方式要求使用者點選具吸引力的連結（例如投票網站、影片等），進而造成社交攻擊事件，手機無意間遭受木馬程式攻擊，或是騙取手機簡訊認證碼，進行網路小額扣款付費的交易行為，輕則損失幾千元，重則被當成拍賣網站的人頭帳戶。

2. 網路釣魚惡意連結

現今的手機功能已等同一般電腦，該有的功能幾乎都有，然而因使用者介面關係，手機瀏覽器所提供的資訊卻無法像電腦一樣能完整呈現，例如顯示SSL資訊的功能常因手機螢幕大小限制而難以完整呈現，許多網站該跳出警示訊息要求使用者進行驗證時，手機版網頁為求畫面簡約性通常會跳過此步驟，行動版瀏覽器所提供的資訊往往不足以讓使用者判斷該網站是否有潛在的危險。

3. 勒索軟體綁架手機重要資料

大部分的勒索軟體是透過釣魚網站入侵，大多經由特定的網址來散布，內容不外乎使用引起好奇心之字眼，引導使用者點選網址或免費廣告（內含惡意連結）。勒索軟體顧名思義屬於勒索行為，當使用者受到勒索軟體攻擊，該軟體會自動加密鎖住手機或儲存資料，並要求使用者特定期間內支付相當費用，否則將永遠無法使用手機或資料。

4. 偽冒惡意APPs軟體下載

手機APPs商店裡有琳瑯滿目的免費APPs供民眾下載，然而這之中包含許多含有惡意程式的APPs，魚目混珠難以分辨。當使用者不知APPs的真實性，下載到含有惡意程式的APPs時，最容易造成下列2種情況，讓使用者難以察覺。

・直接或間接幫使用者安裝廣告或不想安裝的APPs。

・隱身在正常的APPs中。

（三）正確使用手機小撇步

網路上的詐騙方式很多種，所有的詐騙方法不外乎皆是運用民眾好奇心與求一時的方便心態進行攻擊，以下提供幾個正確使用手機的小撇步，避免手機對話紀錄、照片、密碼等隱私資料外洩，以保障個人隱私。

・僅從信賴的來源下載APPs

・下載APPs前必須停看聽

・要了解每支APP要取得哪些權限，要求之權限是否合理

・檢查定位設定

・點選網址請三思

・別把個資用通訊軟體傳出去

・即時更新作業系統

・避免資訊自動儲存

・當心免費無線上網熱點

・手機使用複雜密碼與設定遠端可刪除資料

（四）正確使用手機方式與注意事項-手機操作十大步驟

美國聯邦通信委員會對於智慧型手機之使用，分別針對Android、iOS及Windows phone作業系統，擬訂安全操作的十大步驟，摘述如後：

・設定手機的個人識別碼及通行碼（Set PINs and passwords.）

・請不要修改你的智慧型手機的安全設定（Do not modify your smartphone's security settings.）

・請備份並保護你的資料（Backup and secure your data.）

・僅從信任之來源安裝apps（Only install apps from trusted sources.）

・請在安裝APPs前確認並明瞭軟體所要求的授權（Understand app permissions before accepting them.）

・請安裝或啟用允許遠端定位及刪除資料之安全程式（Install security apps that enable remote location and wiping.）

・請更新系統或軟體之更新程式（Accept updates and patches to your smartphone's software.）

・請謹慎使用開放的無線網路（Be smart on open Wi-Fi networks.）

・請在捐贈、轉售或回收你的舊智慧型手機之前，應將資料刪除（Wipe data on your old phone before you donate, resell, or recycle it.）

・向警察機關或電信公司回報遭竊之手機（Report a stolen smartphone.）

（五）建議使用者如何安全使用智慧型手機

多數國家均在協助使用者的立場，藉由正確的設定智慧型行動裝置之相關安全機制，達到初期對於智慧型行動裝置基本使用安全之保護，因此歸納前述所有關於保護使用者資料安全之相關指引，將其彙整10項使用者指引（表5），以期防範資訊安全問題於未然。

五、結語

手機內建軟體資訊安全，不僅需要手機商、APP軟體開發商共同重視，更需要使用者具備良好的使用習慣，將可能造成的危害風險降到最低。期望透過「智慧型手機系統內建軟體資通安全檢測技術規範」之檢測機制，確保手機內建軟體之安全性，藉由政府、民間與使用者個人的共同努力，據以強化我國行動裝置資通安全，保護民眾個資與隱私。

表5 使用者指引參考表

項次	項目	說明
1	設定PIN碼、行動裝置密碼與多重身分驗證機制（例如：指紋辨識）。	避免行動裝置因送修或失竊而遭到未授權的存取內部資訊。
2	定期檢查並安裝原廠提供之更新與修補程式。	藉由原廠提供的修補機制，提升行動裝置安全性。
3	不移除行動裝置預設的安全機制。	不應對行動裝置進行「破解」、「越獄」或「取得root權限」，卸除行動裝置預設安全機制。
4	僅從受信任的來源安裝應用程式。	避免安裝來源不明的程式造成安全威脅，應從正式的官方管道取得Apps。如：Apple APP Store, BlackBerry World or Google Play。
5	不使用之行動裝置應刪除所有儲存之資料並恢復出廠預設值。	當不使用的行動裝置要移轉他人使用、廢棄、捐贈、轉賣、送修前，應刪除所有行動裝置上之資料，並恢復出廠預設值。
6	應透過建立信任安全的連線與機制傳送機敏資料。	使用點對點的安全通道（例如:SSL/TLS、HTTPS）與金鑰加密機制，對欲傳送之機敏資料（如：網路銀行之帳號、密碼）加以保護。
7	所有介面在不使用的狀況下應關閉，並避免建立不信任連線。	防止不經意的狀況下，在公共場合主動連線或被不明連線。例如：藍芽的探索模式應於使用後立即關閉，並盡可能避免使用。以及不連線到公共場合中不明的無線基地臺（或無線熱點）。
8	特別留意軟體蒐集使用者資料之要求。	在行動裝置軟體提示並要求時，應注意盡可能避免不必要之資訊之上傳。例如：不任意依據軟體指示上傳通訊錄資訊。
9	不任意相信並點選可疑的郵件或簡訊所提供之連結位址。	對不明簡訊內容應提高警覺，以防範簡訊詐騙與避免遭受安裝惡意程式之威脅。
10	對於任何應用程式執行過程所產生的錯誤代碼應加以求證。	可能是惡意程式欲繞過系統防禦機制所導致，應對不明訊息代碼向原始供應商進一步求證。

資料來源：本會整理

1 105年5月於臺灣地區抽樣訪問1001個16歲以上擁有智慧型電話或平板電腦的行動裝置成年用戶的線上調查，由Morar Consulting調查公司調查和分析，總體樣本的誤差範圍為正負3.0%。

2 https://www.checkmarx.com/2013/11/29/10-challenges-of-mobile-security/

災防成敗2大關鍵 合作與通報

淺談我國災害防救體系

■ 簡秀峯

我國災害防救體系的建構法源來自於災害防救法，而災害防救法則係於89年7月19日由總統公布，並自公布日起施行。該法主要分為總則、災害防救組織、災害防救計畫、災害預防、災害應變措施、災害復原重建、罰則等7個章節，共計有52個條文。

對於災害防救法定義的災害，其第一章總則明訂包含風災、水災、震災（含土壤液化）、旱災、寒害、土石流災害、火災、爆炸、公用氣體與油料管線、輸電線路災害、礦災、空難、海難、陸上交通事故、森林火災、毒性化學物質災害、生物病原災害、動植物疫災、輻射災害、工業管線災害等災害。而上述災害的中央災害防救業務主管機關分別為如下：

一、風災、震災（含土壤液化）、火災、爆炸災害：內政部。

二、水災、旱災、礦災、工業管線災害、公用氣體與油料管線、輸電線路災害：經濟部。

三、寒害、土石流災害、森林火災、動植物疫災：行政院農業委員會。

四、空難、海難、陸上交通事故：交通部。

五、毒性化學物質災害：行政院環境保護署。

六、生物病原災害：衛生福利部。

七、輻射災害：行政院原子能委員會。

八、其他災害：依法律規定或由中央災害防救會報指定之中央災害防救業務主管機關。

我國災防體系係採分層負責（如圖1、圖2），整體災害防救之基本方針，由行政院成立中央災害防救會報及災防委員會負責，其工作如下：

一、中央災害防救會報

（一）決定災害防救之基本方針。

（二）核定災害防救基本計畫及中央災害防救業務主管機關之災害防救業務計畫。

（三）核定重要災害防救政策與措施。

（四）核定全國緊急災害之應變措施。

（五）督導、考核中央及直轄市、縣（市）災害防救相關事項。

（六）其他依法令所規定事項。

二、中央災防委員會

（一）執行中央災害防救會報核定之災害防救政策、推動重大災害防救任務及措施。

（二）規劃災害防救基本方針。

（三）擬訂災害防救基本計畫。

（四）審查中央災害防救業務主管機關之災害防救業務計畫。

（五）協調各災害防救業務計畫或地區災害防救計畫間牴觸無法解決事項。

（六）協調金融機構就災區民眾所需重建資金事項。

（七）督導、考核、協調各級政府災害防救相關事項及應變措施。

（八）其他法令規定事項。

同時災害防救法依災害種類，明定中央災害防救業務主管機關，中央災害防救業務主管機關負責工作如下：

一、中央及直轄市、縣（市）政府與公共事業執行災害防救工作等相關事項之指揮、督導及協調。

二、災害防救業務計畫訂定與修正之研擬及執行。

三、災害防救工作之支援、處理。

四、非屬地方行政轄區之災害防救相關業務之執行、協調，及違反本法案件之處理。

五、災害區域涉及海域、跨越二以上直轄市、縣（市）行政區，或災情重大且直轄市、縣（市）政府無法因應時之協調及處理。

災害防救法除了明定中央單位災防任務外，對於直轄市、縣（市）、鄉（鎮、市）之亦明定相關災害防救會報單位，其任務分工分別如下：

一、直轄市、縣(市)災害防救會報，其任務如下：

（一）核定各該直轄市、縣（市）地區災害防救計畫。

（二）核定重要災害防救措施及對策。

（三）核定轄區內災害之緊急應變措施。

（四）督導、考核轄區內災害防救相關事項。

（五）其他依法令規定事項。

二、鄉(鎮、市)災害防救會報，其任務如下：

（一）核定各該鄉（鎮、市）地區災害防救計畫。

（二）核定重要災害防救措施及對策。

（三）推動疏散收容安置、災情通報、災後緊急搶通、環境清理等災害緊急應變及整備措施。

（四）推動社區災害防救事宜。

（五）其他依法令規定事項。

我國整體災防體系係採分層負責，由行政院成立中央災害防救會報及災防委員會負責災害防救之基本方針，地方則由直轄市、縣（市）、鄉（鎮、市）各自垂直成立相關災害防救會報單位負責災防相關業務，另依災害種類由不同中央單位負責災害防救業務計畫，並督導所屬公共事業辦理災防業務。

災害防救工作著重於事前防救規劃、演練、災害應變、災後重建。對於防救規劃，各分層負責單位皆須提出相關計畫，中央災防委員會負責研訂災害防救基本計畫，並由中央災害防救會報核定。另中央災害防救業務主管機關、公共事業則須災害防救基本計畫研訂災害防救業務計畫，然後分別由中央災防委員會、中央災害防救業務主管機關核定；而直轄市、縣（市）災害防救會報執行單位應依災害防救基本計畫、相關災害防救業務計畫及地區災害潛勢特性，擬訂地區災害防救計畫，經各該災害防救會報核定後實施，並報中央災害防救會報備查。鄉（鎮、市）公所應依上級災害防救計畫及地區災害潛勢特性，擬訂地區災害防救計畫，經各該災害防救會報核定後實施，並報所屬上級災害防救會報備查。

關於災防演習，災害防救法明定各級政府及相關公共事業，應實施災害防救訓練及演習。另對於災害應變措施，各級政府可依災害程度成立災害應變中心，同時各級政府應依權責實施下列事項：

一、災害警報之發布、傳遞、應變戒備、人員疏散、搶救、避難之勸告、災情蒐集及損失查報。

二、警戒區域劃設、交通管制、秩序維持及犯罪防治。

三、消防、防汛及其他應變措施。

四、受災民眾臨時收容、社會救助及弱勢族群特殊保護措施。

五、受災兒童及少年、學生之應急照顧。

六、危險物品設施及設備之應變處理。

七、傳染病防治、廢棄物處理、環境消毒、食品衛生檢驗及其他衛生事項。

八、搜救、緊急醫療救護及運送。

九、協助相驗、處理罹難者屍體、遺物。

十、民生物資與飲用水之供應及分配。

十一、水利、農業設施等災害防備及搶修。

十二、鐵路、道路、橋樑、大眾運輸、航空站、港埠、公用氣體與油料管線、輸電線路、電信、自來水及農漁業等公共設施之搶修。

十三、危險建築物之緊急評估。

十四、漂流物、沈沒品及其他救出物品之保管、處理。

十五、災害應變過程完整記錄。

十六、其他災害應變及防止擴大事項。

鑒於電信、傳播事業係屬災害防救法所定之公共事業，隸屬國內整體災防體系一環，而國家通訊傳播委員會（以下簡稱本會）負責電信、傳播事業之監理工作。換言之，本會負有督導電信、傳播事業災防業務之責，不論電信、傳播事業災防演練督導、災害防救業務

計畫核定、災害應變、災後復建及災損通報，皆係本會災防重點工作。災害防救工作成功與否仰賴各單位通力合作，跨部會合作或是縱向連繫通報支援，不論是在災前預防、災害應變或是災後重建階段，都是決定災害損失降低或擴大的重要關鍵因素。

（作者為基礎設施事務處技正）

▶ 參考資料

1. 災害防救法
2. 中央災害防救會報網頁http://www.cdprc.ey.gov.tw/cp.aspx?n=AB16E464A4CA3650&s=97ED16B8B0435D35

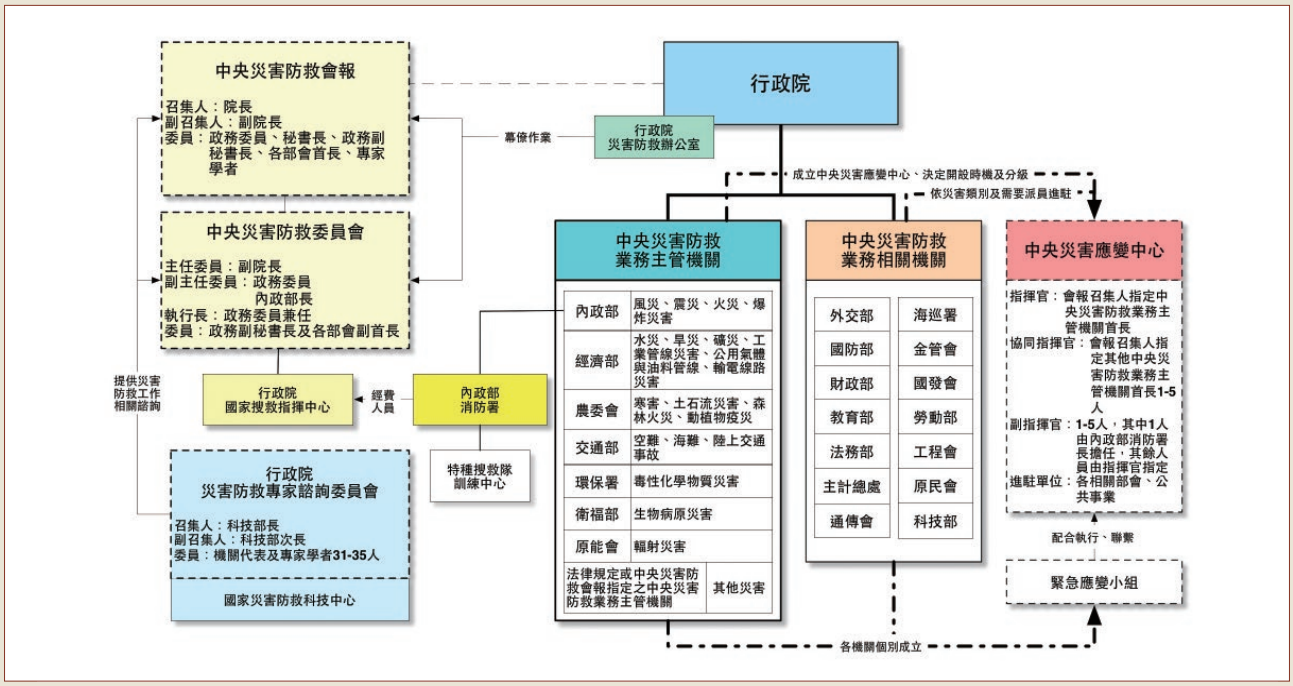

圖1 ▶ 中央災害防救體系組織架構

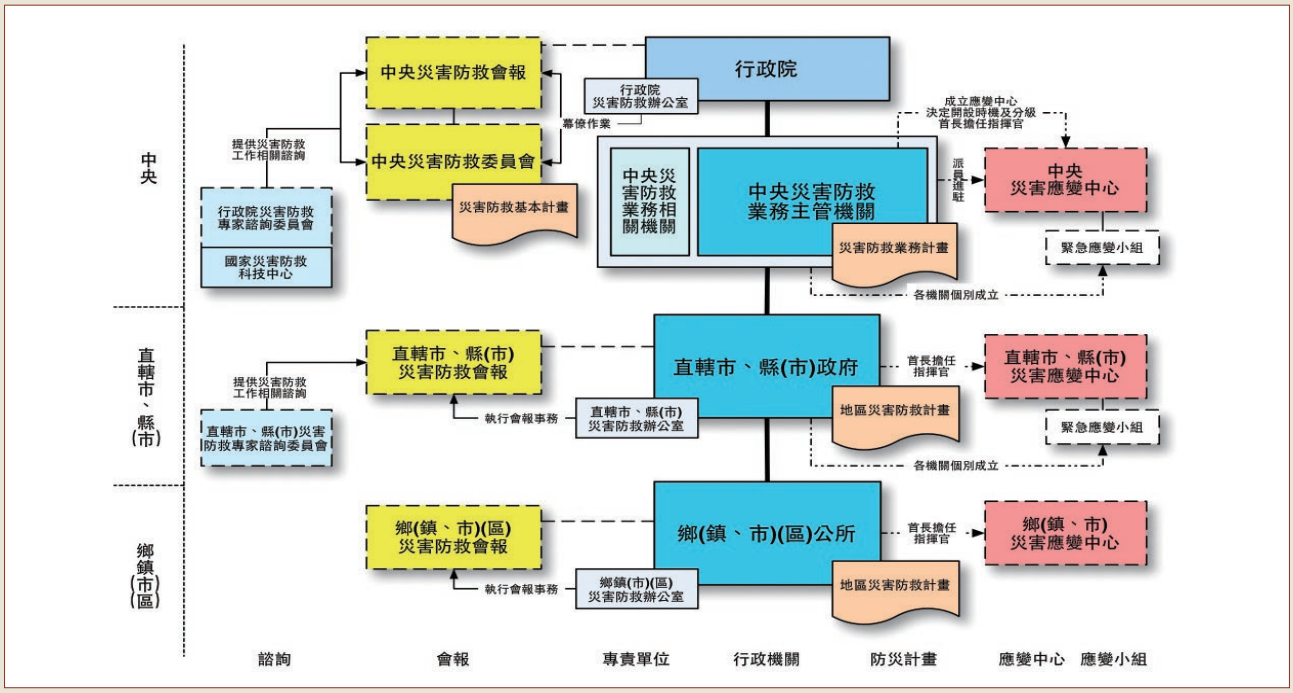

圖2 ▶ 中央至地方防救體系架構

罰款機制下的信任監理

美國行動寬頻資安相關技術發展及監理探討

■ 李福懿

一、前言

為強化國內行動寬頻網路資安管理能力，蒐集國外行動通信相關基站資安管理經驗及國際標準，研析適合我國環境之管理方針，以研議行動寬頻網路資訊安全相關規範及未來發展政策。國家通訊傳播委員會（以下簡稱本會）於105年1月參訪美國電信主管機關、檢測實驗室、研究中心，針對行動寬頻資安檢測標準發展，蒐集美國行動寬頻基站資安及相關檢測技術現況；並就法規或是在共同協防的流程、國外政府針對電信設備或是基礎設施相關資安問題的處置方式及後續規範的制定進行探討，以作為我國未來建置基站資安檢測環境的參考。

二、美國國家標準局NIST - ITL

ITL實驗室電腦安全部門重點研究領域相關探討議題摘錄如下：

（一）Insights on Security Research at NIST

網路世代的崛起，各式各樣的線上服務與應用也如雨後春筍般地出現。在龐大商機的背後，其實也隱含各種潛在的攻擊與威脅；而威脅的範圍極大，一般美國企業相信每年因私有資訊被竊所造成的損失，從十億上看到幾兆美金。為了因應這樣的威脅與損失，ITL 被賦予的主要任務包括：

- 制定標準、準則、工具與量測方法。
- 提供各院校與組織相關的電腦安全教育，以提高電腦或網路使用者的警覺性。
- 提供各種身分（識別碼）的管理系統。
- 依據所制定的各種標準，規劃全國電腦安全的發展藍圖。
- 改善電腦安全的基礎建設，以提升美國關鍵基礎建設的安全與回復。關鍵基礎建設包含電力系統、水利系統、交通系統等，當這類系統的電腦控制系統受到攻擊時，將嚴重影響人民生活與企業運作，所造成的損失難以估計。因此，為防範未然，NIST 專責制定相關標準，並協助處理相關問題。

ITL目前的研究範例，包括風險管理、系統配置相關的準則、安全管理的自動化、弱點管理、虛擬機與雲端運算、大型金鑰管理框架與管理系統、下世代的密碼學（新密碼演算法、輕量、量子化加密等），行動安全（包括行動 App 的測試準則、行動 App 的軟體品質需求、行動裝置的信任）、網路安全、軟體品管與使用性、識別碼管理系統等。制定標準或開發安全工具時，除了傳統的安全與隱私等考量因素，回復能力也相當重要。此外，還必須考慮到不同世代的文化變化與差異，才能提供較完善的法則與估測方式。

（二）Vetting the Security of Mobile Applications

TransApps，一套應用於軍事上的行動安全的Android 應用程式。TransApps 以戰爭為場域，解決士兵使用行動應用時的不安全設定（配置）等問題，例如因不當設定造成敏感性資料被未授權存取、未經授權的網路通訊等等。TransApps 於 2010 年開始啟動，一年半後，正式應用於阿富汗戰場，使用者約有 3,000 多人。透過一個彈性的框架，TransApps 希望能廣納各方提供的服務與應用，提供地理環境的分析、文化分析等服務。重點是，這些服務都必須要運行於一個安全的環境。為了提供此安全環境，NIST 也與美國國防部合作，以用戶應用場域為基礎，利用功能性回歸測試和定量性能測試，協助進行 TransApps 的安全性評估。為此，在測試行動 App 方面，NIST 也制定出標準測試流程，並開發出 AppVet 系統（開源套件，可於 github 上取得），以檢測行動 App 的漏洞與安全問題。

（三）A Multilayer Overview of IoT Security Inefficiencies

IoT（Internet of Things，物聯網）是一種新型的網路通訊架構，主要的概念是透過機器與機器間的互動，來達到生活便利、資料蒐集、功能控制的作用。IoT早在1999年就被Kevin Ashton所提出，IoT也可以透過機器間的通訊來達到自我設定的目的。相對於現有的網路架構，使用者就不會再是這種網路架構的中心，一切以資料和機器為主。這樣子的網路架構在於能夠大量地蒐集環境的情況，以及自動回應現有的環境。因為全部的通訊都是機器自動去處理，當預設的事件發生時，也能夠快速地、自動地通知管理者。然而，IoT這種網路環境，因為少了人的參與，可能會擴大被感染裝置攻擊的威脅。

IoT現有的應用範疇非常廣泛，包含智慧家電、運輸、購物、工業、家庭照護等。智慧家電像是家庭的自動化、自動節能或是家庭安全性。IoT在運輸上現有的應用可以是道路安全、交通流量管制，在工業環境中，小裝置可以幫助品質控管、錯誤發生的預測、生產力改進。家庭照護像是病人狀態的監控、遠端治療、個人化的小裝置，都可以是利用IoT來實現。由於以上的應用，現有的IoT裝置有些許的安全疑慮，例如90%的IoT裝置會蒐集個人隱私資料，如何妥善保護這些資料，會是一個重要的議題。除此之外，由於IoT裝置為了成本考量，通訊的演算法難以採用較安全的加密演算法。

著名的網路組織OWASP（The Open Web Application Security Project）也針對IoT裝置可能遭遇到的安全弱點列舉下列10點：

- 不安全的網頁介面
- 不安全的雲端介面
- 無效率的認證/授權
- 無效率的行動介面
- 不安全的網路服務
- 不安全的網路配置
- 無傳輸層自動加密
- 不安全的軟體/韌體
- 隱私資料
- 無實體安全性

IoT裝置網路的威脅，因為IoT裝置都需要連接網路，利用內部網路做傳輸，如果有惡意攻擊者用更強大的無線訊號欺騙IoT裝置連上，則該偽裝的無線存取點可以破壞此IoT環境的可用性，造成DoS（Denial of Service，阻斷服務攻擊）攻擊。或是因為IoT裝置間因為缺乏加密機制，讓攻擊者很容易地可以進行中間人攻擊，來竊取或是竄改資料，因此，近年IoT裝置的安全性還是相對薄弱。

（四）Describing Authentication

身分認證主要由3個步驟所組成：識別（Identify），認證（Authenticate），授權（Authorize）。識別的內容是在於區分來做認證不同的個體，像是區分兩個人，兩台機器，或是兩種生物。識別的技術可以由名稱、圖像、區域等資訊來劃分。認證是核對該識別出來的個體，來判斷是否為系統已知的對象。這邊需要有雙方彼此才知道的資訊，或是一個交換過的資訊。最後是授權，也是身分認證的最主要目的，將適當的權力給予該認證過後的個體，授權的內容可以是存取能力、對物體操作、對其他個體的互動等。

認證的方式有許多種，像是密碼認證、生物識別認證；而認證的過程可以是人對機器認證或是機器間的認證。機器間的認證比較簡單，都是數位化的關係，大部分都是以金鑰的方式來做認證；而人與機器認證的方式比較多樣，主要可以分做Something you know（密碼）、Something you have（裝置）、Something you are（生物資訊識別）。還有比較進階的認證方式，像是連續性的認證過程，像是行為上生物資訊，像是敲鍵行為、滑鼠使用特徵、步態認證、手寫簽章、語調分析等。更新穎的研究還有利用認知生物識別來進行認證，像是每個人生理無意識的反應，像是腦波、心電圖、神經刺激反應、血壓等等。許多資訊都可以用來區分個體，而如果特定集合的特徵足夠獨特，則可以用來做認證。

認證在生活上已經非常頻繁，而且許多認證機制已經被自動化，讓使用者察覺不到。舉例來說，一個使用者在一個有HTTPS保護的網站上購物，中間的過程包含了3種認證。第一個是網站與使用者裝置間的TLS連線，TLS需要憑證來驗證對方的身分，雖然目前HTTPS只有單方認證，並不會認證使用者身分，但是現有的瀏覽器一旦無法驗證連線網站的身分，都會警告使用者該網站的身分可疑。第二個認證是該網站對此使用者的認證，目前一般的網站都僅用密碼來當作認證的方式，使用者輸入之前在該網站設定的密碼後，讓網站比對是否相同。確定使用者身分之後，才能夠確保購物的清單屬於該連線用戶。最後是信用卡的驗證，利用信用卡上的資訊來作身分的確認，包含信用卡號碼、背後的三碼安全碼、有效日期等。

身分認證理所當然是越複雜越多樣所能提供的安全性越高。然而，在實際的使用情況中，太過繁複的身分認證方式會引起使用者反感。在實作一個系統的認證機制時，需要衡量身分認證的強度以及合適度。認證強度在於該認證機制是否能夠被有效率的破解，像是密碼長度、字元複雜性、偽造的難易度等等。認證資訊的安全度在於這個資訊夠不夠獨特？足以區別出所有的使用者。這個資訊會不會改變？像是生物識別資訊可能會因時間的關係而有所變化，再者資訊容不容易保護？會不會很容易取得或是複製？以上的考量因素會決定認證的強度。

後續需要考量的是合適度，對於一個比較沒有經濟價值的系統，採用過度複雜的認證機制，並不是一個好的選擇。考慮使用性來說，第一個是認證的有效性，探討該認證系統的準確度，對於生物識別的認證來說，往往認證的準確度無法像數位密碼般，能夠百分之一百的準確；第二個是效率問題，進行這個認證過程中會不會太過耗時或是繁雜，整體認證資訊的比對與取得會不會需要大量的儲存空間、計算能力、運算時間等；第三個是體驗的滿足感，使用者會不會直覺性的接收、採用該認證方式。

（五）U.S eID Effort The Personal Identity Verification（PIV）Standard

聯邦政府目前有500萬張智慧晶片卡用來做人員識別，主要的用途是管制實體建築的人員進出，利用識別卡來管制電腦設備的使用數位資源，或是用來做跨部會機關認證的機制。通常跨部會都會需要有Two-factor authentication強度以上的認證機制。目前PIV的技術已經發展成熟，NIST本身也撰寫了許多規範與準則來要求PIV的安全性。

除此之外，PIV技術不僅用卡片來做識別，目前美國聯邦政府也有考慮用智慧型手機當作識別的一種來源。原因在於卡片通常需要一個讀卡機，而且卡片是一個額外的攜帶品，有鑒於智慧型手機是現有人類的必需品，PIV系統結合智慧型手機是未來的趨勢。此標準定義在NIST SP 800-157中，主要是利用公開金鑰基礎設施（PKI）架構，遵循著X.509的信任關係，來建立PIV的身分認證訊息。而生成的機密資訊（Derived Credential）是一種用來證明身分的識別，或是用來確定該用戶擁有該PIV卡片。在智慧型手機上的Derived PIV Credential中，可以嵌入在行動裝置中的軟體、特殊的嵌入式硬體或是存放在一個儲存裝置中的記憶卡、USB或UICC。在考量利用智慧型手機當作PIV的認證裝置時，還需要考慮智慧型裝置上的變異性，例如製造商、作業系統版本、網路連線能力、螢幕大小、輸入裝置、支援的通訊協定等。

（六）Secure Indirection Networks for Efficient DDoS Attack Mitigation

DDoS的定義是對特定的使用者，利用大量且地區分散的機器來阻斷其網路資源或是硬體資源。DDoS仍然是現有網路上一個非常有效且嚴重的攻擊手法，可以造成銀行或交易網站實體金錢的損失，或是政府機關聲譽上的損失。

抵擋DDoS的方法主要有3種方式：過濾方式（Filtering-based approaches）、覆蓋網路架構式（Overlay-based defenses）、移動目標（Moving target defenses）。過濾方式的防護機制在於分析攻擊的流量，並且將可疑的流量丟棄，藉以避免目標被攻擊。但是這種方式需要網路設備的支援，才能有效的達到目標。第二種是利用疊覆網路（Overlay network）的特性來阻絕DDoS攻擊，Overlay network 因為路由的路徑不是固定，所以可以減緩及吸收分散式來源的攻擊流量。第三種是移動目標，此方式的做法是將被攻擊的目標移動到其他的網路環境中，讓使用者的服務不受到中斷。

DDoS的攻擊手法日新月異，而且攻擊的強度越來越強。隨著全球計算裝置的成長，智慧型手機甚至也可以加入殭屍網路進行攻擊。如果僅靠著存取控制清單（Access Control List, ACLs）已不足夠分析各式各樣的DDoS攻擊流量。

一種建立在雲端環境的DDoS抵禦機制，主要可以用來抵擋網路層的DDoS以及運算層的DDoS。利用移動目標方法，來達到抵禦DDoS的方式，把攻擊者與一般使用者的流量分開，讓他們面對不同的伺服器。這樣一來，攻擊者既以為自己已經攻擊成功，而使用者仍能夠獲得網站的服務。該方法已用模擬法來驗證其有效性。

三、美國聯邦通訊委員會FCC

Federal Communications Commission（FCC）共安排二場會議，第一場會議由本會及財團法人電信技術中心（以下簡稱TTC）、交通大學（以下簡稱NCTU）與FCC進行Security Standards and Security Issues交流。第二場則由FCC進行5G—Mobile Broadband in mmW Bands介紹。

（一）Security Standards and Security Issues

以下為問答重點摘要：

Q1：在美國，有沒有實際的LTE（Long Term Evolution）資安攻擊行為發生？

目前並沒有聽到真實世界有對LTE網路架構從外部做攻擊，只有內部人員洩露資料的新聞。

Q2：FCC對於基站安全或基站管理是否有查驗機制

FCC對於安全著重在與人體有害及通訊保障，因此主要規範為電磁波檢查及911緊急通訊服務，Security為電信業者範疇。

Q3：FCC是否要求或是建議電信商，採用IPSEC Backhaul（Internet Protocol Security Backhaul，網際網路安全協定後置迴路）

安全議題為電信商運營首要考量議題之一，為提供用戶有保障的服務，相信電信商針對其核心網路有層層防密考量，Backhaul也會採取專線電路，不會透過不安全的網路連線，讓核心網路暴露在外面，讓攻擊者可以遠端存取。FCC並不會硬性或是強制規定業者啟動。

Q4：FCC是否有認可之實驗室，進行LTE 一致性、相容性或是資安檢測。

FCC主要是依據1934年通信法案所創立，主要負責執行1934年通信法案，FCC規定及命令和通信授權的條款，並無實驗室進行LTE一致性、相容性或是資安檢測，此部份建議可參考NIST PSCR（National Institute of Standards and Technology，美國國家標準技術研究所）的LTE Demonstration Network Test Plan相關文件。

（二）5G—Mobile Broadband in mmW Bands

在ITU-R確定IMT-2020（5G）的願景、關鍵能力需求規範與發展時程後，接下來就是全球通訊業者，要開始忙著開發系統解決方案，並將其標準化。如何滿足一千倍的挑戰，大致可從3個維度來尋求解決之道；除佈建更多基地臺，改善頻譜效率（Spectrum Efficiency）外，就是增加使用的頻寬。然而在全球已經被凌亂分配的頻譜情況下找到可運行頻帶，則需往高頻頻帶尋找。

ITU-R於是開始探討利用6GHz以上頻帶做為行動通訊用之可行性，一般預期，未來在高頻應該要可以找到共通的1GHz頻帶，做為未來5G使用。如此，相較於4G LTE-A的100MHz運作頻譜寬度，就有十倍成長。

由於訊號在高頻傳遞，其傳遞衰減、雨衰、受地形地物阻擾等影響，品質會變得非常差，因此愈高頻愈不適合作長距離的行動通訊之用。不過，由於在高頻波長極短，可使用極小天線，因此可以將大量天線形成陣列天線（Array Antenna），加上技術的進展，如大規模多重輸入多重輸出（Massive MIMO）、波束成型（Beamforming）、波束追蹤（Beam Tracking）等，讓大家對高頻用於行動通訊的應用抱著樂觀態度，也因此FCC也開始關注於毫微米波（Millimeter Wave, mmWAVE）通訊系統研究。

四、結語

以行動寬頻資安而言，FCC並未有任何規管及查驗的規範，其認為Security應屬於電信商範疇，電信業者有責任建構一套安全不受使用者入侵、竊取資料之行動寬頻網路，如有資料外洩或是消費者權益受損，則有罰款機制。建議針對國內電信業者對所建置的行動寬頻網路，如因其系統網路安全事件，導致消費者權益受損，亦應課予其適當責任。

NIST對於行動應用程式安全風險評估與審驗，如基本資安檢測項目訂定、檢測項目所須檢測之各項檢查事項、預期之檢測結果及各結果之形成條件等已有成果，可供本會參考制訂相關規範時參考。

針對行動寬頻資安議題，美國目前並無任何透過基站為媒介而發生的資安事件，綜觀各文獻分析許多可能存在的風險、攻擊及威脅，在3GPP的標準規範建議、業者的防備及設備商的阻絕能力產品設計下，尚未發生。FCC並無介入管制電信業者於可信賴的骨幹網路（Trusted Backhaul）採用IPSec（網際網路安全協定）加密傳輸，僅NIST於研討會或是文獻發表上的建議。美國政府對於電信商的行動寬頻網路安全，是充分信賴電信商，其認為若有發生問題，最大的損失會是電信商，其有可能遭受消費者流失、信譽喪失或是來自聯邦的罰款。然資安問題日趨嚴峻，國際標準組織3GPP/GSMA已開始規劃行動寬頻設備之資安認證規範，建議持續投入經費與人力來研究及注意國際行動寬頻資安認證規範之發展趨勢，以與國際接軌。

（作者為基礎設施事務處技正）

5大要求 排除基站安全疑慮

從國際資安發展趨勢，論行動寬頻基站安全要求

蔡明德

一、前言

電信網路為國家資訊化的重要基礎設施，行動寬頻網路扮演電信網路中的重要構件，隨著科技的持續演進，在可預見的未來，行動寬頻網路將成為通訊主流，在智慧型手機高滲透率帶動全球行動上網需求下，行動數據訊務量預期將大幅成長，躍升為經濟資訊流通及交易的重要通道。

當網路與無線技術結合時，使用者不必被侷限在固定空間就能上網，帶來方便性更勝以往，然而，眾人沉醉於行動寬頻網路的迷人之處時，卻很容易忽略潛藏的安全危機，既有有線網路仍遭受許多安全威脅，更遑論行動寬頻網路以空氣為介質傳輸訊號，若有心人士不著痕跡蒐集空中傳遞的封包資料，將造成行動寬頻網路在安全上更多不可忽視的危機。

相較於2G與3G等傳統行動通訊系統，新一代4G通訊系統－LTE之網路架構最大的變革在於扁平化與IP化，基於行動寬頻網路設計架構，基站系統與核心網路之間若無完善安全控管與保護，未來可能成為各種不法攻擊的途徑，造成通訊上的安全疑慮，由於基站是通訊節點上，使用者所連接的第一道接取設備，也是整個行動寬頻系統中，僅次於使用者裝置，數量最多的網路元件，這種情況突顯了行動寬頻基站系統資訊安全管理的重要性。欲解決這些安全威脅，國際間已有不同資訊安全組織持續推動資安標準，因此，本文就資安發展趨勢與行動寬頻LTE/SAE安全架構演進需求，探討行動寬頻基站系統資訊安全，以提供國內相關產業及主管機關做為參考。

二、國際資安發展趨勢

多年來，國際電信聯合會（International Telecommunication Union, ITU）電信標準化部門（ITU's Telecommunication Standardization Sector, ITU-T）一直積極參與電信和資訊技術安全研究，負責制定無線通訊標準與分配無線頻譜等工作。在其建議書X.805[1]中，建立不同面向安全議題的統一詞彙表，提供一般性通訊系統安全框架模型。將該模型套用於行動寬頻網路，在安全框架體系基礎之上，建立有效的評估指標體系，通過對指標參數的評價確定系統安全等級，從而形成較完整實用的評估準則與方法。因此，本文將列舉國際三大標準：ITU X.805通訊系統安全框架、資通訊產品國際標準ISO/IEC 15408共同準則與美國聯邦資料處理標準FIPS140-2進行介紹。

（一） ITU X.805通訊系統安全框架

ITU-T X.805旨在建立電信網路體系安全框架，安全框架模型的定義基於層級和平面兩個主要概念。安全層級討論端對端網路的網路元件與系統安全要求，區分基礎設施層、服務層和應用層之安全要求；安全平面討論

網路中實施活動的安全性，定義了管理面、控制面與終端用戶面，說明三種網路中受保護的活動，分別討論與網路管理活動、網路控制、信令活動與終端用戶相關的安全需求，透過該框架劃分電信網路中各項安全觀點，提供全面、端對端網路的安全全貌，可以應用於任何網路技術（例如無線、有線、光纖網路）以及多種網路（例如服務供應商的網路、數據中心的網路、政府網路等等），確保涵蓋所有跨層交錯的威脅定義，最終具體用途可以應用於所有電信網路產品類別。如圖1所示。

基於安全層級與安全平面，該框架定義了網路安全的8個維度，用於解決所有可能的網路產品漏洞，分別為：

（1）存取控制：限制與控制存取網路單元、服務、應用的方法，例如密碼、ACL（Access Control List）、防火牆。

（2）身分認證：提供身分證明的方法，例如共享金鑰、公開金鑰基礎建設（Public Key Infra-structure, PKI）、數位簽章、數位憑證。

（3）不可否認性：防止否認網路已發生活動的機制，例如系統日誌、數位簽章。

（4）資料保密性：確保資料保密性的機制，例如加密。

（5）通信安全：確保資訊只能從來源端傳送到目的地的方法，例如VPN、多重通訊協定標籤交換傳輸（Multi-Protocol Label Switching, MPLS）、第2層通道協定（Layer 2 Tunneling Protocol, L2TP）。

（6）資料完整性：確保接收到的資料如發送或檢索儲存的方法，例如訊息摘要演算法（MD5 Message-Digest Algorithm）、數位簽章、防毒軟體。

（7）可用性：確保提供給合法用戶可用的網路元件、服務與應用之方法，例如入侵偵測系統（Intrusion-detection system, IDS）／入侵預防系統（Intrusion Prevention System, IPS）、網路備援、營運持續運作（Business Continuity, BC）、災難復原（Disaster Recovery, DR）。

（8）隱私：確保以保密的方法識別、網路的使用，例如網路位址轉譯（Network Address Translation, NAT）、加密。

這8個安全維度適用於3個安全層級與3個安全平面所構成8x3x3安全矩陣，以決定適當的控制措施，提供模組化、系統化與組織化方式對網路進行安全評估和規劃，每項安全觀點對應各自的威脅和漏洞，得出其安全目標。

（二）資訊技術安全評估共同準則（Common Criteria for Information Technology Security Evaluation, CC）

以國際標準ISO/IEC 15408共同準則（Common Criteria, CC）與ISO/IEC 18045共同準則方法論（Common Evaluation Methodology, CEM）為資通訊產品之安全認證與驗證規範，提供測試實驗室針對資通產品進行安全性與安全等級之評估與測試驗證，是以國際合作角度，建立共同的基準。解決過去區域性準則之間的差異與衝突，提供一個共同的結構和名詞定義，來表達系統與產品安全的需求，其安全產品驗證適用範圍包括資通訊相關的軟體、硬體與韌體或是三者任一組合之安全功能與強度評估。資通訊產品之認證等級依據其高低不同而有評估檢測深度與廣度區分，程度係以評估保證等級（Evaluation Assurance Level, EAL）為基準。

目前CC認證也是我國的國家標準（CNS15408）共同準則（ISO/IEC 15408）包括3個部分：

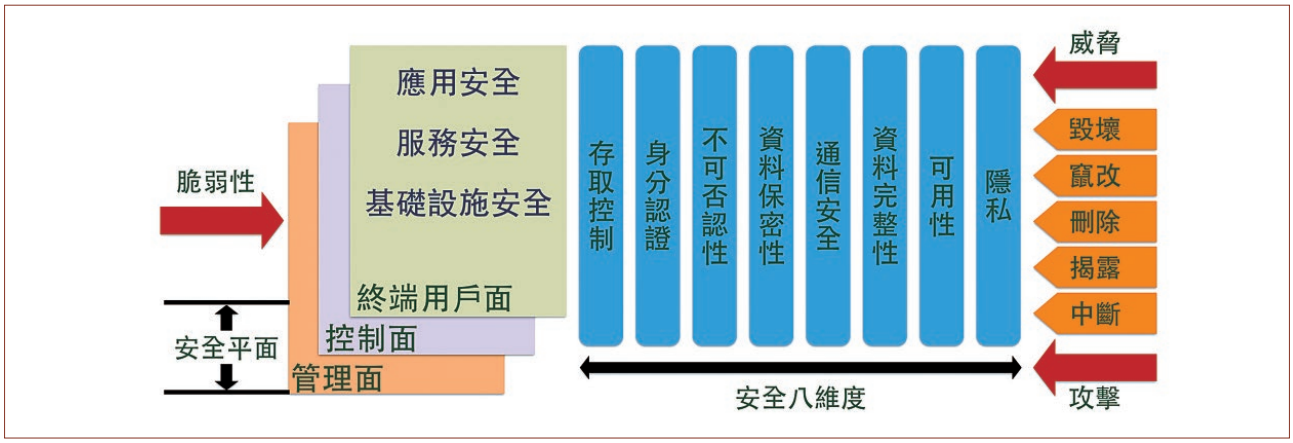

圖1 ITU-T X.805通訊系統安全框架
資料來源：ITU-T X.805及本研究整理

- 第一部分-簡介及一般模型（CC Publications Part 1：Introduction and general model）：描述產品安全要求的共通架構與語言，以及定義保護剖繪（Protection Profile, PP）與安全標的（Security Target, ST）之架構。
- 第二部分-安全功能要求（CC Publications Part 2：Security Functional Requirements）：提供保護剖繪與安全標的的概念，並將要求分類成元件（component）、家族（family）與類別（class），作為表達評估標的（Target Of Evaluation, TOE）安全功能要求的標準方式。
- 第三部分-安全保證要求（CC Publications Part 3：Security Assurance Requirements）：提供評估產品的方法與架構，詳列安全保證要求與其評估準則，定義安全保證要求的類別、屬別、組件、元件等，並將其量化為7個評估保證等級（EAL）。

共同準則是一套標準方法，用來評斷產品或服務在某種層面上的表現，當產品或服務經過此種方法評估並通過之後，就可以確定該產品或服務達成了準則中定義好的某種資訊安全功能或等級；例如，當一個IT產品經過資訊安全的評估準則評估並通過認證之後，即代表該IT產品本身已實現了評估準則中的安全功能或者安全等級，具有國際公信力，則消費者在選購時，便可依需求選用適合的資通安全等級產品，來確保資訊運作的安全。

（三）美國聯邦資料處理標準（Federal Information Processing Standards, FIPS）

FIPS是美國除了軍事機構以外的政府單位與政府承包商在採購及存取資訊與通訊安全設備時，必須使用與遵守的標準。FIPS 140為FIPS第140號標準，第一版FIPS 140-1經由美國「商務部」核准，於1996年由美國「國家標準與技術研究院」制定完成並公布，第二版FIPS 140-2於2001年公布，FIPS 140-2標準訂定密碼模組的四種安全等級，從最低要求的第一級到最高階的第四級，且高等級須滿足前一級的安全要求，每個安全等級各須滿足11個安全要件。

（1）密碼模組規格（Cryptographic Module Specification），「密碼邊界」為代表密碼模組的物理邊界範圍。「密碼模組」是指包含實體埠、邏輯介面、資料輸出輸入的邊界等硬體、軟體、韌體或任意的組合於邊界內實作包含金鑰的產生、密碼的加解密等密碼演算法。

（2）密碼模組埠口與介面（Cryptographic Module Ports and Interfaces），對於密碼模組中的資料流必須被限制僅能經由實體物理埠或邏輯介面來存取或操作。定義一個密碼模組應具備的4個邏輯介面：資料輸入介面、資料輸出介面、控制輸入介面、狀態輸出介面。

（3）角色、服務與身分鑑別（Roles, Services, and Authentication），密碼模組必須支援不同的認證角色與服務，依照角色給予對應的服務。FIPS 140-1規定密碼模組必須提供使用者角色（User Role）與管理者角色（Crypto Officer Role）；如果密碼模組有提供維護模式，以提供密碼模組實體與邏輯的維護與修正，則必須提供維護者角色（Maintenance Role），包含顯示狀態服務（Show Status）與執行自我測試及服務（Perform Self-test）兩項服務，及執行核可安全功能（Perform Approved Security Function）的需求服務，密碼模組必須執行至少一個FIPS核可的運算模式（Approved mode of operation）。

（4）有限狀態機模型（Finite State Machine），密碼模組必須使用有限狀態機模型的狀態轉移圖（state transition diagram）或狀態轉移表（state transition table）來描述其運作方式，並且明確指明其運作與錯誤的狀態；必須包含以下狀態：電源開關狀態（Power on/off states）、密碼管理者狀態（Crypto officer states）、金鑰/機敏參數登錄狀態（Key/CSP entry states）、使用者服務狀態（User service states）、自我測試狀態（Self-test states）、錯誤狀態（Error states）；此外，也可能會包含一些其餘的狀態，例如：未初始化狀態（Un-initialized states）、閒置狀態（Idle states）、旁通狀態（Bypass states）、維護狀態（Maintenance states）。

（5）實體安全（Physical Security），密碼模組必須使用實體的安全機制，來限制對於密碼模組的非授權存取，實體部分區分成單晶片模組、多晶片嵌入式模組、多晶片獨立模組3種。

（6）作業環境（Operational Environment），作業環境包含作業系統與操作密碼模組所需之相關軟體、硬體、韌體或任意之組合。主要分成一般作業環境、限定作業環境、可改作業環境3種，依照不同安全等級必須滿足不同的要求。

（7）金鑰管理（Cryptographic Key Management），

金鑰管理的安全要件涵蓋密碼金鑰的整個生命週期、金鑰的元件、與模組用到的密碼安全參數，包括針對亂數的產生做出詳細的說明，分成核可的亂數產生器用於產生金鑰，非核可的亂數產生器可以用來產生核可亂數產生器的輸入種子與核可安全函數的初始輸入。

（8）電磁干擾／電磁相容（EMI/EMC），密碼模組的電磁干擾／電磁相容應符合FCC的要求。

（9）自我測試（Self-Tests），密碼模組應該要具有開機自我測試（power-up self-tests）與條件自我測試（conditional self-test）。當測試失敗時，密碼模組必須進入錯誤狀態，並且從模組的狀態介面輸出錯誤標示，同時，所有密碼有關的操作與運算都必須停止，也要停止資料從資料輸出介面輸出。

（10）設計保證（Design Assurance），要求密碼模組供應商從模組的設計、開發、佈署與操作等過程都達成最佳的實務，來保證模組被適當的測試、設定、遞送、安裝與開發，並且同時提供適切的文件說明。

（11）避免其他攻擊（Mitigation of Other Attacks），密碼模組要盡量避免遭受其他實務上難以測試的攻擊手法，例如：電源分析（power analysis）、時間分析（time analysis）與錯誤注入（fault induction）攻擊等。電源分析攻擊是透過電源供應時，使用的電量上的些微差距，來分析得出金鑰資訊。時間分析攻擊則是透過不同的輸入，必須耗費不同的時間來得到結果的特性來分析金鑰的資訊。錯誤注入攻擊則是強制操控模組運作的外部參數，例如：電壓、微波與溫度等，使得模組在非正常的運作環境下產生錯誤的結果，甚至洩漏金鑰與相關密碼安全參數的資訊。

三、行動寬頻基站安全架構

3GPP（3rd Generation Partnership Project）成立於1998年12月，會員來自各個國家區域的組織合作夥伴，成員為各地域通訊相關技術的標準組織，包含ARIB（日本）、ATIS（美國）、CCSA（中國大陸）、ETSI（歐洲）、TSDSI（印度）、TTA（韓國）、TTC（日本），基於ITU在IMT-2000計畫的規範下，負責決定3GPP主要的方針與發展方向，從GSM到LTE架構的演進相關技術，包含2G、3G及4G等各項行動通訊標準，加入區域性的考量，使得制定的規範能夠適用在不同的國家地域。

3GPP在 2008年開始積極的規劃行動寬頻4G LTE的標準，包含了許多系統架構、無線通訊、通訊安全的設計與實作，其中TS33.401標準定義了LTE整體的安全體系架構，包括演進數據封包系統（Evolved Data Packet System, EPS）、演進數據封包核心網路（Evolved Packet Core, EPC）的安全功能與機制，以及在EPS與EPC中運行的安全程序，針對基站eNodeB定義了5項安全要求，相關的安全要求適用於所有基站類型，對於某些特定類型的基站（如微基站HeNB）則具備更嚴格要求，可參考其它3GPP標準的安全要求。以下說明基站安全要求定義。

（一）設定與組態要求

eNodeB應經過認證與授權，才能設定與進行組態配置，因此攻擊者無法透過本地或遠端修改eNodeB設定與軟體組態。

- eNodeB與EPC應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB與eNodeB應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB與O&M應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB應確保軟體與數據變更嘗試得到授權。
- eNodeB應使用經授權的資料或軟體。
- 確保軟體傳送到eNodeB的保密性保護與完整性保護。

（二）內部金鑰管理要求

EPC提供給eNodeB的用戶會話（session）金鑰，以及使用於身分認證與安全連結建立程序的長期金鑰，應保護所有存放在eNodeB中的金鑰。存放在eNodeB中的金鑰應不能離開eNodeB中的安全環境，除了有其它3GPP標準規定的情形。

（三）eNodeB用戶層資料要求

eNodeB的任務包括Uu介面與S1/X2介面的用戶層（User Plane）封包加解密，以及處理S1/X2介面的用戶層封包完整性保護。

- 在相關金鑰存放的安全環境下，處理用戶層資料加解密與完整性保護。
- 確保eNodeB處理S1-U與X2-U用戶資料傳輸具備完整性、保密性與重傳保護，不受到未經授權方攻擊。如果需要透過加密方式實現，則可使用IPsec ESP技術。

（四）eNodeB控制層資料要求

eNodeB的任務在於提供S1/X2介面的控制層（Control Plane）封包的機密性與完整性保護。

- 在相關金鑰存放的安全環境下，處理控制層資料加解密與完整性保護。
- 確保eNodeB處理S1-MME與X2-C的控制資料傳輸具備完整性、保密性與重傳保護，不會受到未經授權方攻擊。如果需要透過加密方式實現，則可使用IPsec ESP（IP Encapsulating Security Payload，網際網路安全協定的資料封裝加密功能）技術。

（五）安全環境要求

eNodeB的安全環境為一種邏輯上的定義，安全環境可以透過相關功能或敏感性操作來實現。

- 安全環境應支援敏感資料的安全化儲存，例如對機密與重要組態資料加密。
- 安全環境應支援敏感功能執行，例如用戶資料的加解密與認證協定。
- 安全環境中的敏感資料不應暴露給外部實體。
- 應確保安全環境的完整性。
- 經授權才能使用或儲存安全環境中資料，或是執行其中的安全功能。

從前述5項安全要求可以發現LTE採取扁平化架構後，eNodeB納入了更多的控制功能，在考量eNodeB安全要求時，除了eNodeB自身的安全性，eNodeB間共用線路的資料傳輸也是重點之一，也就是後置迴路（backhaul）之安全機制。3GPP以S1與X2介面探討LTE後置迴路之安全性，傳輸用戶資料與控制資訊時，都應具備相應之安全保護機制。

四、行動寬頻基站的安全威脅

由於基站部署在非受控之暴露環境，同時也是LTE網路EPC核心系統的主要入口，因此很容易成為安全上的威脅目標，可能的威脅面向包括通訊鏈路破壞（T2及T4），以及eNodeB裝置本身遭受的攻擊威脅（T3），如下圖2所示。

（一）LTE eNodeB遭受非法控制

當eNodeB被攻擊者非法佔領控制時，UE（User equipment，用戶端設備）切換eNodeB時，目標eNodeB上使用的金鑰KeNB，係從來源eNodeB上的金鑰KeNB推演得到，因此攻擊者獲取來源eNodeB上使用的金鑰KeNB後，可以推演得到目標eNodeB上使用的金鑰KeNB，進而威脅其它的eNodeB。

（二）攻擊者嘗試植入惡意程式碼到後端系統

如果eNodeB或終端裝置UE不慎被植入惡意程式碼，則此惡意程式碼很有可能會感染後端EPC核心系統，以致於無法提供正常的行動通訊服務。因此，如何確保eNodeB與UE的系統完整性與配置安全度即成為電信業者首要的檢測項目。

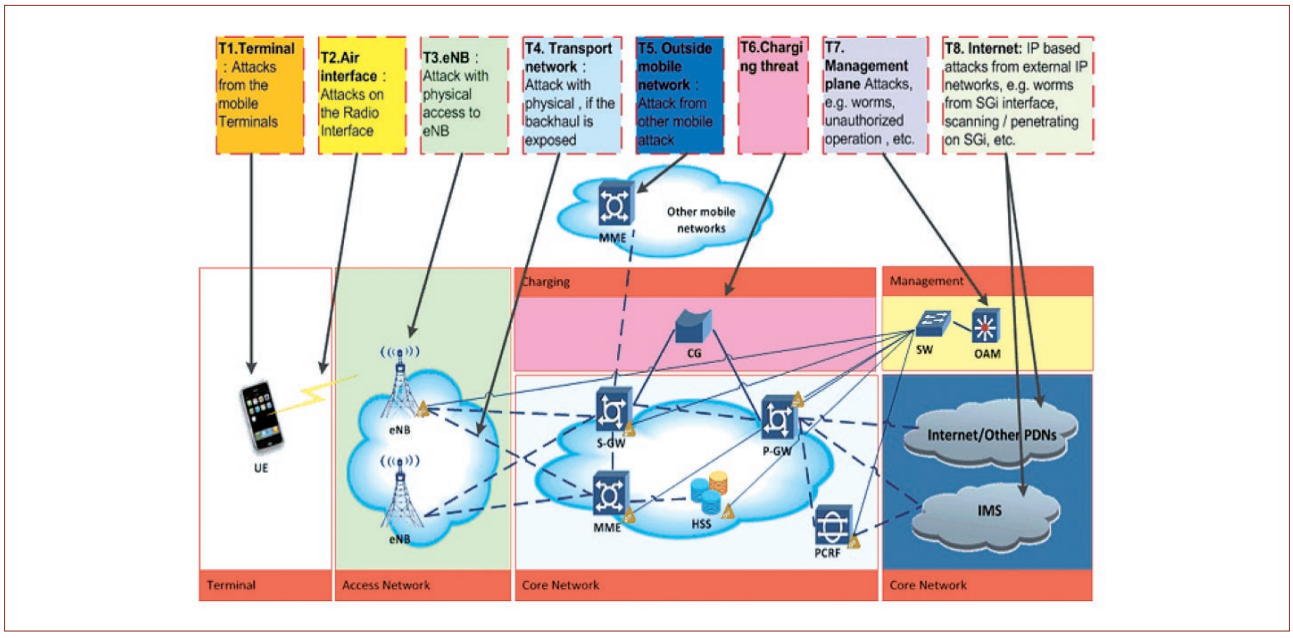

圖2 LTE安全威脅示意圖
資料來源：3GPP

（三）對HeNB之攻擊

在4G時代來臨後，數據訊務量需求持續擴增，小型基站（Small Cell）佈建需求增加，扮演強化網路覆蓋率與提供訊務量分流的重要功能，可能經由家中ADSL、Cable Modem或是FTTx與電信業者機房傳輸資料。這類裝置位於網路邊界，加上低成本及低複雜性，容易成為攻擊目標，形成資安懸崖（Security Cliff）。相關的安全威脅包括[2]：

（1）憑證破解

HeNB與網路間的通訊憑證可能會被破解，如果認證演算法或憑證過於脆弱，就可能被暴力破解、物理入侵未存放於受保護領域的HeNB認證資料或其它非法接取。此外，複製認證憑證與非法的HeNB也有可能，這種攻擊可以規避認證演算法與憑證。

（2）中間人攻擊

為一種主動竊聽的攻擊方式，攻擊者在受害者雙方中間搭建訊息連結，受害者並無法察覺交談是透過中間的攻擊者，事實上整個對話是由攻擊者所控制。此類攻擊可能會發生在HeNB啟始首次對業者網路的聯繫期間，業者端點無法可靠地識別該端點，網際網路上的攻擊者可以攔截所有來自HeNB的訊務量，隨後取得所有個人資訊，假冒HeNB。在與網路的首次聯繫點使用認證憑證可以避免此類型的攻擊，業者應確認這些憑證，USIM與廠商憑證可運用於此。

（3）重送攻擊

惡意重複或延遲數據傳輸，攻擊者擷取傳輸數據並進行重傳攻擊。發生於缺乏唯一身份驗證資料與遞增每次通訊會談ID的HeNB。透過遞增通訊會談ID可以讓接收端確認是否為重送封包，避免被攻擊。

（4）阻斷服務攻擊

攻擊者阻斷合法用戶的服務申請，持續向目的端點發送假請求或是數據，迫使通訊連結能力喪失或暫時失效。使用具備IKE協商的請求避免此類型攻擊，以及使用IKEv2的ESP加密訊務量。

（5）竊聽

在HeNB缺乏保護機制下，用戶資料不具安全性，因而遭受有心人士竊聽。

（6）偽裝基站

攻擊者購置非法HeNB，並將組態設定為類似封閉式用戶群組（Closed Subscriber Group, CSG）的基站，然後更改為沒有加密設定與完整性級別，或是取得HeNB中用戶的金鑰，藉此進入骨幹網路或入侵更多基站。將CSG設定隱藏可避免這種攻擊，同時HeNB與用戶間應具備驗證能力，HeNB也應該由網路端認證。

五、結語

目前國家通訊傳播委員會頒布實施之電信事業資訊通訊安全管理作業要點及管理手冊，規定了電信事業在整體經營風險框架下建立、實施、運行、監視、評審、維持和改進其文件化之要求，鑒於我國電信事業已參照ISO/IEC 27000系列國際標準，包括：資訊安全管理系統要求事項（ISO/IEC 27001）、資訊安全管理作業規範（ISO/IEC 27002）、資訊安全管理系統實施指引（ISO/IEC 27003）、資訊安全管理風險管理（ISO/IEC 27005）等，建立資通安全管理機制，但在4G行動通訊系統下，可能面臨之安全威脅，缺乏適用基站資安管理之控制措施及基站安全檢測。

故本文一開始，介紹以ITU X.805通訊系統安全框架為策略，展開行動寬頻網路的資安威脅，所應具備的安全視野，接著聚焦於研究主體-基站，探討3GPP組織所制定的基站安全要求，這些規範是為了開發而參考，是電信設備商所參考的依據，但各國不同市場需求或廠商技術能力，實作上仍會有些許的差異，因此透過介紹國際間的資安產品檢測的標準：共通準則（CC）和美國聯邦資料處理標準（FIPS），探討兩標準間資訊安全要求之內涵。相關產業及主管機關面對行動寬頻基站的安全威脅，一方面基站安全環境的標準可以參考3GPP的規範，另一方面基站檢測的流程可以參考共通準則（Common Criteria）和聯邦資料處理標準（FIPS-140）之概念，即早建立應有的安全思維與優先順序，展開行動方案。

（作者為財團法人電信技術中心工程師）

1 ITU, ITU-T Recommendation X.805 Security architecture for systems providing end-to-end communications”, 2003/10.

2 3GPP TR 33.820 V8.3.0, 2009/12.

委員會議重要決議

105.9.1-105.9.30

日　期	事　項
105年9月7日	照案通過依本會委員會議審議事項及授權內部單位辦理事項作業要點第5點、第7點所列案件清單計387件及第4點、第6點所列業經本會第555次分組委員會議決議案件計34件。
	審議通過「行動寬頻業務終端設備技術規範」第二點及第五點修正草案及「第三代行動通信終端設備技術規範」修正草案，並依本會法制作業程序辦理發布事宜。
105年9月14日	照案通過依本會委員會議審議事項及授權內部單位辦理事項作業要點第5點、第7點所列案件清單計381件及第4點、第6點所列業經本會第556次分組委員會議決議案件計13件。
	核准亞太電信股份有限公司變更行動寬頻業務事業計畫書。
	一、核准台灣大哥大股份有限公司變更行動電話業務事業計畫書。 二、核准台灣大哥大股份有限公司變更行動寬頻業務事業計畫書。 三、有關台灣大哥大股份有限公司所報行動電話業務系統建設計畫變更案，本會洽悉。 四、核准台灣大哥大股份有限公司變更行動寬頻業務系統建設計畫。 五、核准台灣大哥大股份有限公司繳回行動電話業務1800MHz頻段部分頻率上下行各5MHz（上行1748.7 MHz ~1753.7 MHz，下行1843.7 MHz ~1848.7 MHz），該公司並應於105年9月28日起，停止使用上揭頻率。 六、核准台灣大哥大股份有限公司行動電話業務獲核配之國內信號點碼共21個及系統使用之用戶號碼38,700個，變更為供行動寬頻業務使用。
	審議通過「衛星廣播電視購物頻道插播式字幕管理辦法」草案，並依本會法制作業程序辦理後續發布事宜。
	一、許可美商國家地理頻道有限公司台灣分公司所屬「福斯家庭電影台」、朝禾事業股份有限公司所屬「彩虹E台」及亞洲衛星電視股份有限公司所屬「寶寶世界頻道」等3頻道換發執照。 二、請通知該等公司依諮詢會議建議確實執行，相關執行情形將納為未來評鑑及換照之重點審查項目。
	一、許可宜蘭之聲廣播電台股份有限公司、財團法人天主教臺灣省基隆市益世堂益世廣播電台、快樂廣播事業股份有限公司、美聲廣播股份有限公司、財團法人民生展望廣播事業基金會、人生廣播電台股份有限公司及南方之音廣播股份有限公司換發廣播執照。 二、請通知該等事業依審查諮詢委員會建議確實執行，相關執行情形將納為未來評鑑及換照之重點審查項目。
	審議通過「有線廣播電視系統經營者營業讓與合併及投資案件准駁標準」草案，並依本會法制作業程序辦理後續發布事宜。
	審議通過「申請經營有線廣播電視服務履行保證金繳交辦法」草案，並依本會法制作業程序辦理後續發布事宜。

日　期	事　項
105年9月21日	照案通過依本會委員會議審議事項及授權內部單位辦理事項作業要點第5點、第7點所列案件清單計354件及第4點、第6點所列業經本會第557次分組委員會議決議案件計15件。
	審議通過因應行動電話業務終止用戶權益保障行動方案，並依行政程序辦理後續相關事宜。
	審議通過「廣播事業設立許可辦法」部分條文修正草案，並依本會法制作業程序辦理後續預告事宜。
	審議通過「衛星廣播電視節目起迄時間認定與廣告播送方式及數量分配辦法」草案，並依本會法制作業程序辦理後續預告事宜。
	依行政程序法第107條規定辦理新永安及大揚有線電視股份有限公司申請變更董事長、董事、監察人、經理人及公司章程修正案聽證事宜。
105年9月29日	照案通過依本會委員會議審議事項及授權內部單位辦理事項作業要點第5點、第7點所列案件清單計157件及第4點、第6點所列業經本會第558次分組委員會議決議案件計7件。
	一、審議通過「本會受理民眾廣播電視陳情事項處理說明及制度革新規劃」。 二、請參酌諮詢會議公民團體、專家學者意見，作為未來修正本會申訴系統、精進革新規劃之重要參考，另請於自動核轉機制建立前徵詢相關業者意見。
	審議通過「有線廣播電視法施行細則」修正草案，並依本會法制作業程序辦理發布事宜。
	「申請經營有線廣播電視服務審查辦法（草案）」，並依本會法制作業程序辦理發布事宜。
	一、審議通過「申請經營有線廣播電視服務籌設辦法（草案）」，並依本會法制作業程序辦理預告及公開說明會等事宜。 二、審議通過「有線廣播電視服務籌設須知（草案）」，並依本會法制作業程序辦理發布事宜。
	一、許可台北影業股份有限公司所屬LUXE TV Channel、Arirang TV及TV5MONDE等3頻道換發境外衛星廣播電視節目供應者執照。 二、許可美商特納傳播股份有限公司台灣分公司經營Boomerang頻道，並通知該公司依本(105)年9月23日承諾事項確實辦理，其執行情形將納為未來評鑑及換照之重點審查項目。
	審議通過「推動通訊傳播產業創新研究發展補助辦法(草案)」，並依本會法制作業程序辦理預告事宜。
	「衛星廣播電視事業負責人監督管理辦法（草案）」，並依本會法制作業程序辦理預告事宜。

國內
郵資已付
板橋郵局許可證
板橋第01489號
中華郵政台北雜誌
第1102號
無法投遞請退回

國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION
地址：10052臺北市仁愛路一段50號
電話：886-2-33437377
網址：http://www.ncc.gov.tw

為地球盡一份心力，本書採用環保紙印製。

ISSN：1994-9766
GPN：2009600628
定價：新臺幣100元