利用公務智慧型手機接收公務資料交換郵件研究

行政院海岸巡防署自行研究報告

印製時間：中華民國107年 1月

利用公務智慧型手機接收公務資料交換郵件研究

單位:通電資訊處

研究人員:林展瑋、蕭考量、莊士萱

行政院海岸巡防署自行研究報告

中華民國 107 年 1 月

目次

圖 次 …… （2）

提 要 …… （3）

第一章 前 言 …… （4）

第一節 研究緣起與背景…… （4）

第二節 研究目的及研究重點…… （4）

第三節 研究方法與步驟…… （5）

第四節 預期目標……（6）

第二章 架構安全性研究與探討…… （7）

第一節 本署資訊安全歷史探討……（7）

第二節 工作流程電子表單資料交換機制 ……（7）

第三節 本署公開金鑰基礎建設暨憑證系統安全強度探討……（8）

第四節 本署可攜式媒體相關規定範疇……（9）

第三章 系統實作 ……（10）

第一節 伺服器安裝與系統建置 ……（10）

第二節 郵件路由設定 ……（11）

第三節 憑證製發與安裝 ……（11）

第四節 郵件信箱設定與郵件寄送測試 ……（13）

第五節 郵件紀錄稽核 ……（18）

第六節 手機遺失防護措施 ……（19）

第四章 研究發現、結論與建議 ……（23）

第一節 研究發現 ……（23）

第二節 結論 ……（23）

第三節 建議 ……（25）

參考文獻……（26）

圖　次

圖一：系統架構圖……（10）
圖二：設定中繼郵件伺服器路由……（11）
圖三：製發本署個人憑證……（12）
圖四：安裝本署個人憑證……（12）
圖五：公務手機上設定海巡署公務郵件信箱……（14）
圖六：公務手機接收外部機關郵件架構圖……（14）
圖七：透過Gmail寄送郵件至海巡署信箱……（15）
圖八：公務手機上公務信箱收到測試郵件……（15）
圖九：海巡署內網公務信箱收到郵件……（16）
圖十：內部寄送郵件流程圖……（16）
圖十一：工作流程電子表單-公務資料交換機制……（17）
圖十二：公務手機上公務信箱收到郵件……（17）
圖十三：中繼郵件伺服器稽核畫面……（18）
圖十四：電子郵件過濾系統SPAM稽核畫面……（19）
圖十五：手機遺失時，透過中繼郵件伺服器中止與公務手機同步……（20）
圖十六：透過Gmail寄送測試信件至海巡署內網公務信箱 ……（20）
圖十七：海巡署內網公務信箱已收到測試郵件……（21）
圖十八：驗證中止同步後，公務手機即無法收到公務郵件……（21）
圖十九：從管理介面清除手機上可瀏覽之公務郵件……（22）
圖二十：驗證公務手機上已無公務郵件……（22）

提 要

鑑於我們身處於一個資訊爆炸的年代，無論是知識、技術或產品均以極快的速度在不斷的翻新，本署身為打擊犯罪、查緝走私、維護海洋生態與捍衛海疆的行政機關，自應當隨著日新月穎的科技與時俱進，強化本署執行核心任務的效率。

本署因勤務具高度敏感性與機敏性，針對資訊安全防護方面不遺餘力，特於民國 94 年成立通電資訊處資通安全科[1]，並於 95 年全面採取內、外資訊網路實體隔離政策，避免相關機敏資訊外洩，正因資訊安全的強化，相對的同仁處理公務上檔案交換或是郵件收寄產生不方便，尤其是同仁差勤在外，如遇緊急公務事件，僅能以電話方式回報，無法及時運用行動裝置(Mobile Device)[2]與內部同仁實施電子檔案與郵件資訊交流，造成安全與方便無法兼得之情形。

本次研究考量到因為資訊技術的日新月穎，通訊設備從早期的個人呼叫器(BB Call)[3]到 2007 年第一隻 IPhone[4]手機問世，行動裝置演進快速大躍進，彷彿昨日人類尚知用火，今日轉眼就登陸月球一樣，人人皆有行動裝置，並產生所謂自攜電子設備(Bring Your Own Device，縮寫：BYOD)[5]風潮，然而這種所謂自攜電子設備風潮是一種允許員工使用個人行動裝置辦公的作業方式，據信可以提升員工生產力，但 BYOD 必須面對最大的問題是易產生公務家辦，進而導致易有公務(公司)資料外洩風險。

因此，本研究旨在以資訊安全防護為第一優先情況下，藉由本署資訊人員的資訊防護專業技術與能量，研究如何利用公務智慧型手機接收外部機關寄送之電子郵件，或內部同仁結合工作流程電子表單-公務資料交換機制寄送之內網重要郵件，提升本署同仁處理公務便捷性，同時亦研究如何運用本署自建之公開金鑰基礎建設與憑證系統製發之個人專屬憑證，達成資訊安全上的鑑別性、機密性、存取管控、不可否認性及可稽核性等資訊安全要求，避免因提高同仁便利，而造成資安管控漏洞。

關鍵詞：公務智慧型手機接收信件、憑證、存取管控、可稽核性

---

[1] 綜理本署對外、對內資訊安全防護之資安設備管理、病毒碼更新與即時資安應處等相關事項。
[2] 行動裝置(英語：Mobile device)，大多數為口袋大小的計算裝置，包括手機、平板電腦、POS 機等。
[3] 呼叫器(台灣通稱呼叫器，俗稱 BB.Cal)，是一種具有接收和傳送簡易文字信息功能的無線電通訊工具。
[4] iPhone 是美國蘋果公司研發並販售的智慧型手機系列，它搭載該公司研發的 iOS 行動裝置作業系統。
[5] 是一種允許員工使用個人行動裝置進入他們工作區域並用以處理公司資訊與應用程式的作業方式。

第一章　　前言

第一節 研究緣起與背景

本署為確保資訊安全與強化資安防護能量，網路採取內、外網隔離政策，故同仁出差或休假在外，無法即時接收外機關(例如：行政院、立法院)傳送至本署內網公務信箱之電子郵件，且臨時需要提供資料供上級長官決策或答詢時，須將資料寄送至同仁私人信箱(如 Gmail 信箱)，再透過私人手機連結私人信箱收信與瀏覽，或影印紙本資料親送至需求單位，影響公務效率與易有公務資料外流之風險，本次在兼顧資訊安全與同仁便利性的考量下，研究如何透過公務手機，接收外機關傳送至本署內網公務信箱，或透過本署工作流程電子表單系統-公務資料交換機制[6]寄送之內網郵件。

第二節 研究目的及研究重點

根據 Tech Pro Research[7]研究公司 2016 年研究報告顯示，有超過 76%員工會攜帶自己的行動裝置上班，並處理與工作上相關事項，此一趨勢我們稱為 BYOD(Bring Your Own Device)，本次研究依 Tech Pro Research 公司研究報告所提趨勢，規劃運用本署現有系統，設計能讓具有行動裝置收信需求之同仁，可在行動裝置上收到公務信件，另考量現行研究僅為實驗性質，且私人行動裝置管控不易，初期先以公務智慧型手機為研究主體，探討如何在兼顧資訊安全前提下，使用公務智慧型手機接收外機關傳送至本署內網公務信箱信件，或同仁以本署工作流程電子表單系統-公務資料交換機制寄送之內網郵件，據以提供同仁差勤或休假在外，能即時接收外機關傳送之重要郵件或本署內網郵件，避免同仁將敏感性公務資料寄送至私人信箱。

另前述之新趨勢 BYOD，研究指出雖能提升工作效率，且透過移動辦公方式，滿足現今 E 世代講求行動、效率之需求，不過事實上絕大多數資訊部門皆不願意接受 BYOD 此一趨勢，深究原因無非 BYOD 帶來便利的同時，需輔以最嚴密的資安政策控管，否則在資安這一環節，人性與便利交織出的無疑是最脆弱的安全防護。

---

[6] 本署現用電子表單系統，計有請假、加班、房屋修繕、物品申請、派車、公務資料交換、資訊耗材請領等 11 大類 22 項表單電子表單，其中公務資料交換表單可經權責主管核准後，將內網資料與郵件交換至外網。

[7] 位於美國舊金山的資訊顧問公司，主要從事資訊問題解決方案與市場研究。

第三節 研究方法與步驟

一、雛型規劃與設計：

運用本署現有電子郵件系統(Exchange)、工作流程電子表單系統與電子郵件過濾系統(SPAM)路由、主機表及稽核規則的新增，並另行建置一台中繼郵件伺服器(CCMail)，再結合手機上郵件收發程式，規劃符合本署實際需求之公務智慧型手機接收公務資料交換郵件系統與機制，並透過本署自建之公開金鑰基礎建設及憑證系統製發之憑證，達成資訊安全上的鑑別性[8]、機密性[9]、完整性[10]、不可否認性[11]、可存取管控及可稽核性等資訊安全要求。

二、系統測試與展示：

區分為伺服器安裝及系統建置、郵件路由設定、憑證產出與安裝、郵件信箱設定與郵件寄送測試、郵件紀錄稽核及手機遺失防護措施等六階段系統設計、實作與測試步驟，結合本署公務智慧型手機，實際測試是否能接收外機關寄送郵件，或工作流程電子表單系統-公務資料交換機制寄送之內網郵件，以及公務手機接收郵件所需時間，並假定手機遺失情況下，研究能否透過遠端方式，中止公務信件持續傳送與清除公務手機內相關信件，降低公務資料外洩風險。

三、問題探討：

在本署網路實體隔離政策與資訊安全為最高指導原則下，如何規劃系統及網路架構，使得導入公務手機接收公務郵件這種另類的 BYOD 符合相關政策要求；除此之外，公務手機雖較私人手機易管控，但依據過往經驗法則，現今多數資安事件脫離不開人為因素，故仍需考量行動裝置管理(Mobile Device Management，縮寫：MDM)[12]與行動應用管理(Mobile Application Management，縮寫：MAM)[13]等配套措施，君不見國軍雖與時俱進開放官兵同仁使用個人行動裝置，但需安裝由中科院自行開發的國軍 MDM 軟體[14]。

---

[8] 鑑別性(Authentication)：確認網路的使用者或資料傳送者的身份。
[9] 機密性(Confidentiality)：保護資料內容不讓非法使用者得知。
[10] 完整性(Integrity)：確保網路所傳輸的資訊與原來的一致，沒有被竄改或偽造。
[11] 不可否認性(Non-repudiation)：傳送端不可否認其傳送的資料或完成的交易行為。
[12] 是一種組織或企業管理公務行動裝置(例如：智慧手機與平板電腦）的方式。
[13] 負責管控公司提供的自攜設備，使管理員能夠管理和保護應用程式與資料。
[14] 一種國軍用於管控官兵個人行動裝置功能所使用的軟體。

第四節 預期目標

一、導入 BYOD 概念，提供同仁差勤在外處理公務之便利性，有效提升公務處理效率。

二、運用自建公開金鑰基礎建設機制及電子郵件設備稽核管理，優化資訊安全防護強度，降低公務資料外洩之風險。

三、符合資訊安全規範，加速資料傳遞速度，滿足各式海巡任務需求，進而提供決策者獲得迅速及精準之資訊。

第二章　架構安全性與研究探討

第一節 本署資訊安全歷史探討

本署因業務性質具備高度機敏性，且依據趨勢科技[15]2017 年統計數據，我國為遭駭客、病毒、DDoS 攻擊[16]電腦裝置全球第九名國家，為確保本署資訊安全，前於民國 89 年 1 月由網路管理科兼管資安工作，續於民國 94 年 7 月成立專責單位「通電資訊處資通安全科」，並於民國 95 年 7 月執行「網路實體隔離政策」，強化本署資訊安全防護能量。

為持續提高資訊安全強度與自我監督機制，本署於民國 95 年導入 ISO 27001 資訊安全管理系統(Information Security Management System，縮寫：ISMS)[17]，同年 10 月成立資安推動組及風險處理分組，隔年 6 月成立稽核分組，並於民國 97 年 5 月設立專責防護的資安防護管理中心(SOC)，以便 24 小時即時處理各類資通安全狀況，而因應行政院資訊向上集中政策與有效運用人力，民國 104 年 2 月成立通資管理中心，將本署各通資電系統整合，統由專責單位「通資管理中心」集中監控維運。

第二節 工作流程電子表單系統資料交換機制

本署現用工作流程電子表單系統前於民國 100 年建置，系為推展表單無紙化與線上簽核流程，發展至今系統電子表單計有請假、加班、房屋修繕、物品申請、派車、公務資料交換、資訊耗材請領等 11 大類 22 項表單電子表單，其中公務資料交換表單現行機制為承辦人提出申請後，由主管核定是否可交換(主管請假時代理人不可核定，系統表單自動轉至上一級主管)，本次研究案透過現有嚴謹公務資料交換機制(內寄外)，結合電子郵件過濾系統、電子郵件系統與中繼郵件伺服器，達成公務手機可接收內部公務郵件目標，且郵件內容須經過單位主管審核，透過系統端留下紀錄方式，使內部公務郵件寄送具備管制與可稽核性，避免公務資料隨意外洩。

---

[15] 趨勢科技股份有限公司(Trend Micro Inc.，簡稱：趨勢科技)為臺灣軟體公司，屬電腦防毒及網路安全廠商，由臺灣出身的創辦人張明正兼任行政總裁。

[16] 阻斷服務攻擊(Denial-Of-Service Attack，縮寫：DoS)亦稱洪水攻擊，是一種網路攻擊手法，另當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊(Distributed Denial-Of-Service Attack，縮寫：DDoS)

[17] ISO/IEC 27000 系列標準（又名 ISO/IEC 27000 標準系列）是由國際標準化組織（ISO）及國際電工委員會（IEC）聯合制定有關資訊保安管理的建議。

第三節 本署公開金鑰基礎建設暨憑證系統安全強度探討

本署「海巡資訊系統」運用我國電子化政府公開金鑰基礎建設(Public Key Infrastructure，縮寫：PKI)[18]之整體架構規劃，民國 90 年開始推動本署電子化應用及導入公開金鑰與憑證系統[19]，建立安全可信賴的資訊運用環境，除提供「單一簽入機制[20]」及「身分安全認證機制」外，尚可提供電子郵件資料傳收接送時，「收送雙方之不可否認性」、「文件加密之機密性」、「資料傳遞之完整性」、「收發方身分之認證性」及「資料存取之授權性」等安全認證機制，是本署推動電子化應用及資訊安全的重要機制。

本次研究係以本署現有公開金鑰基礎建設及憑證系統為基石，建構公務手機收發公務電子郵件系統之「身分安全認證機制」，透過運用本署製發之憑證安裝於公務手機內，輔以超文字傳輸安全協定(Hypertext Transfer Protocol Secure，縮寫：HTTPS)[21]方式，連線至本署自建中繼郵件伺服器，以確保僅認證過使用者可收取公務郵件。

本署現行公開金鑰基礎建設及憑證系統，所發憑證密碼雜湊函式為安全雜湊演算法 1(Secure Hash Algorithm 1，縮寫：SHA-1)[22]是由美國國家安全局設計，SHA-1 會產生 160 位的雜湊值長度(40 個英文/數字組成的)，理論上如要使用暴力方式破解，需要 1 個中央處理器 (CPU)[23]運行 6500 年，或是 1 個圖形處理器(GPU)[24]運行 110 年，但在實務上並不可行，另外本署也將隨著技術演進，持續提升憑證安全強度，後續將以升級為安全雜湊演算法 2(Secure Hash Algorithm 2，縮寫：SHA-2)[25]為目標進行。

---

[18] 公開金鑰基礎建設(Public Key Infrastructure，縮寫：PKI)，又稱公開金鑰基礎架構、公鑰基礎建設、公鑰基礎設施或公鑰基礎架構，是一組由硬體、軟體、使用者、管理者、管理政策與流程組成的基礎架構，其目的在於創造、管理、分配、使用、儲存以及撤銷數位憑證。

[19] 憑證是有一定證明效用的物件，用以證明某項效力，通常以檔案為載體，票券、憑證是市面上最為常見的憑證。

[20] 單一登入(Single Sign-On，縮寫：SSO)，又譯為單一簽入，一種對於許多相互關連，但是又是各自獨立的軟體系統，提供存取控制的屬性；當使用者登入擁有這項屬性時，就可以取得所有系統的存取權限，不用對每個資訊系統都逐一登輸帳號密碼。

[21] 超文本傳輸協定(HyperText Transfer Protocol，縮寫：HTTP)是一種用於分佈式、協作式和超媒體資訊系統的應用層協議。

[22] 安全雜湊演算法 1 (Secure Hash Algorithm 1，簡稱：SHA-1)是一種密碼雜湊函式，由美國國家安全局設計，並由美國國家標準技術研究所(NIST)發布為聯邦資料處理標準(FIPS)。

[23] 中央處理器(Central Processing Unit，縮寫：CPU)，是電腦的主要裝置之一，功能主要是解釋電腦指令以及處理電腦軟體中的資料。

[24] 圖形處理器(Graphics Processing Unit，縮寫：GPU)，又稱顯示核心、視覺處理器、顯示晶片或繪圖晶片，是一種專門在個人電腦、工作站、遊戲機和一些行動裝置(如平板電腦、智慧型手機等)上執行繪圖運算工作的微處理器。

[25] 安全雜湊演算法 2(Secure Hash Algorithm 2，簡稱：SHA-2)，是一種密碼雜湊函式演算法標準，由美國國家安全局研發，並由美國國家標準與技術研究院(NIST)在 2001 年發布，屬於 SHA 演算法之一，是 SHA-1 的高階版，相較起來更為安全。

第四節 本署可攜式媒體相關規定範疇

本署為加強管理可攜式資訊設備(即 BYOD 設備)及儲存媒體，防止蓄意竊取、遺失或惡意程式入侵導致資安事件發生，於民國 95 年訂定現行「海岸巡防機關可攜式資訊設備及儲存媒體管理要點」[26]，區分可攜式資訊設備及儲存媒體，規範內更要求，私人可攜式資訊媒體一律嚴禁使用，但使用單位專案簽陳機關副首長以上長官核准者，不在此限，然應有攜出入單位紀錄備查。

另本署「海岸巡防機關資通安全政策」[27]亦針對網路安全管理明文規範，無線存取網路在未訂定相關規範前禁止連接本署任何網路，且電子郵件傳送機敏性資料時，應依國家機密保護法[28]規定以國家認可加密機制傳送。

因此本次研究係以本署公務智慧型手機，在維護資訊安全為前提下，實際測試是否能接收外機關寄送之郵件，或工作流程電子表單系統-公務資料交換機制寄送內網郵件，以符合本署各項資訊安全規範。

[26] 本署為加強管理可攜式資訊設備及儲存媒體，防止蓄意竊取、遺失或惡意程式入侵導致資安事件發生，特訂定之要點。

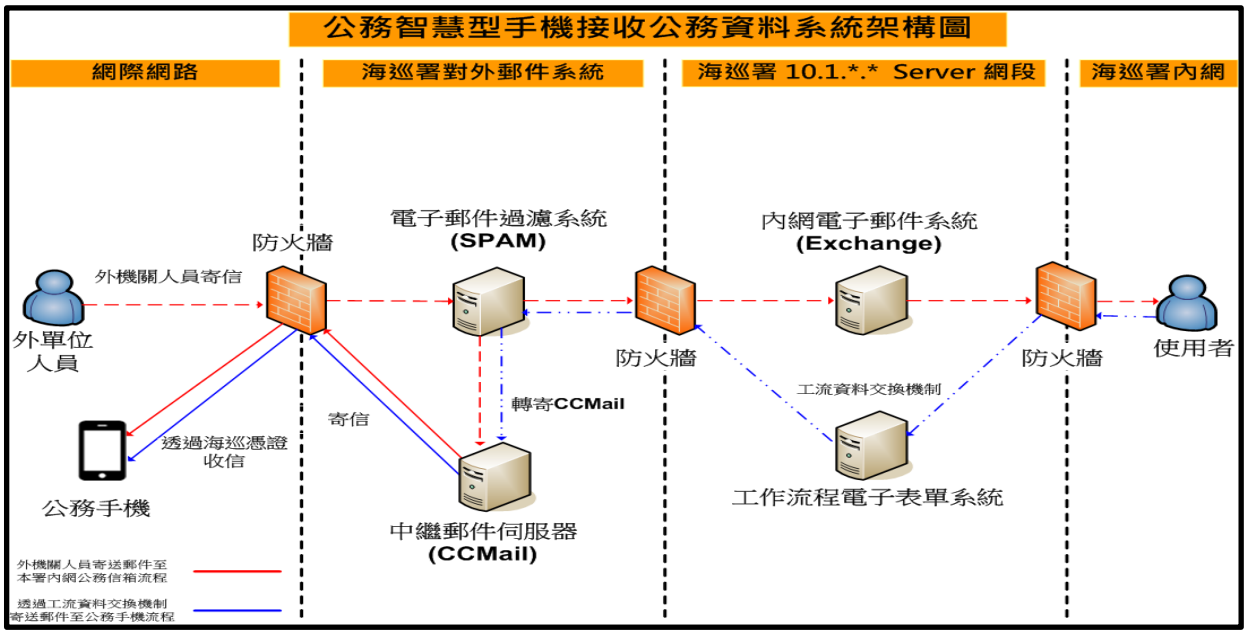
[27] 本署為使同仁及相關資訊服務之廠商明確認知本署資訊安全政策，以利本署資通安全管理，並導入資訊安全管理系統(ISMS)，特訂定之資通安全政策。

[28] 為建立國家機密保護制度，確保國家安全及利益，特制定之法規。

第三章　　系統實作

第一節 伺服器安裝與系統建置

本署因採行內、外網實體隔離政策，外部網路寄送至本署電子郵件，一律透過電子郵件過濾系統與電子郵件系統傳送至本署內網公務信箱，非經核准無法轉寄出去，鑒於2017 年我國發生遠東銀行遭駭客駭進匯款系統平台(Society for Worldwide Interbank Financial Telecommunication，簡稱：SWIFT)，外幣帳戶六千多萬美元遭轉帳至斯里蘭卡、柬埔寨及美國等地銀行的帳戶，為避免提升同仁便利造成資安風險，本次研究目標「外部網路寄送」及「本署工作流程電子表單系統-公務資料交換機制寄送」之郵件能轉寄至公務手機等 2 項功能，系規劃以額外建置於本署外網之中繼郵件伺服器執行郵件轉寄動作，以達成研究目標、確保資訊安全及完善郵件轉寄流程可稽核性。(系統架構圖如圖一)



圖一：系統架構圖

第二節 郵件路由設定

在安裝完外網中繼郵件伺服器後，為使外部郵件或內部公務資料交換機制寄送之郵件傳遞至電子郵件過濾系統時，可順利透過中繼郵件伺服器執行郵件轉寄至公務手機功能，本次研究另須於本署電子郵件過濾系統上設定轉寄路由，以確保郵件傳遞正確與郵件流程可被稽核性，避免後續遇到須查明公務資料外洩原因時，無任何跡證可供查察。(如圖二)

圖二：設定中繼郵件伺服器路由

第三節 憑證製發與安裝

在講述如何實作使用本署自建之公開金鑰基礎建設及憑證系統製發個人專屬憑證前，先來討論 2017 年 12 月左右的新聞，大多數的資訊人員應該都聽過所謂的暗網(Dark Web)[29]，也就是需要透過特殊瀏覽器方可瀏覽的網站，在暗網裡流出了高達 41 GB 的資料檔案，檔案內包含約十幾億份以明文(未加密)[30]形式儲存的郵件帳號及登入密碼，裡面內容包羅萬象，你我常用的郵件系統(例如：Gmail)也有許多帳戶遭揭露，更嚴重的是因

[29] 暗網（Darknet 或 Dark Web），通稱只能用特殊軟體、特殊授權、或對電腦做特殊設定才能連上的網路，使用一般的瀏覽器和搜尋引擎找不到暗網的內容，且暗網的伺服器位址和資料傳輸通常是匿名、匿蹤以避免被有心人士輕易找到。

[30] 在密碼學中，明文經過加密所產生的信息被稱為密文，而密文經過解密而還原得來的信息被稱為明文。

為多數人在登入帳號密碼時，並未設定多重驗證[31](例如：登入需額外輸鍵手機簡訊接收之登錄碼)，導致此次流出帳號密碼多數可輕易登入個人信箱。

有鑑於此，再強再長的密碼都有可能因為系統商的疏忽遭流出，從而失去高強度防護效果，故本次研究系為確保僅認證過公務手機可接收公務郵件，透過將本署核發之憑證安裝於公務手機內(如圖三、四)，使公務手機於連接郵件伺服器接收郵件時，須經核對憑證程序，確認憑證無訛後方可連接，避免類似前述洩漏帳密即可登入案例發生。

圖三：製發本署個人憑證

圖四：安裝本署個人憑證

[31] 多重要素驗證（英語：Multi-factor authentication，縮寫為 MFA），又譯多因子認證或多因素驗證，是一種電腦存取控制的方法，用戶要通過兩種以上的認證機制之後，才能得到授權，使用電腦資源[1][2]。例如，使用者要輸入 PIN 碼，插入銀行卡，最後再經指紋比對。

第四節 郵件信箱設定與郵件寄送測試

鑑於個人電腦用戶端及行動裝置常因人為輕忽，成為網路安全防護最脆弱的一環，易常被駭客透過各式攻擊手法攻擊，例如 2017 年席捲全球的 WannaCry[32]攻擊，該病毒被認為是一種利用美國國家安全局所發現之漏洞加以改寫，並透過網際網路對全球安裝微軟作業系統[33]的電腦進行攻擊的加密型勒索軟體[34]兼蠕蟲病毒[35]，因此世界各國對於過往所推行的個人電腦用戶端組態安全管理更加重視，且視為重要的資訊安全因應對策。

同時我國也參考美國主導推動之政府組態基準(Government Configuration Baseline，簡稱：GCB)[36]，制定符合我國國情與實況之政府組態基準，並於 102 年推動行政院各機關導入，規範電腦用戶端的一致性安全設定，降低資訊安全風險。

本署除配合政府組態基準推動外，亦於 106 年 9 月完成本署內、外網導入電子郵件加密傳輸服務(HTTPS)，因此本次實作亦運用公務手機上設定透過 HTTPS 連線方式，以憑證認證後登入海巡署個人公務信箱(如圖五)，並進行以下兩種寄送方式測試，實地驗測前述規劃與架構設計是否可行：

一、依照前述規劃設計之架構（圖六，紅色實、虛線部分)，驗證外部個人 Gmail 寄送郵件至本署內網公務信箱時，透過本署電子郵件過濾系統轉寄至中繼郵件伺服器，並由公務手機連線至中繼郵件伺服器收信，且本署內網公務信箱亦可同時收到郵件。(如圖七至圖九)

---

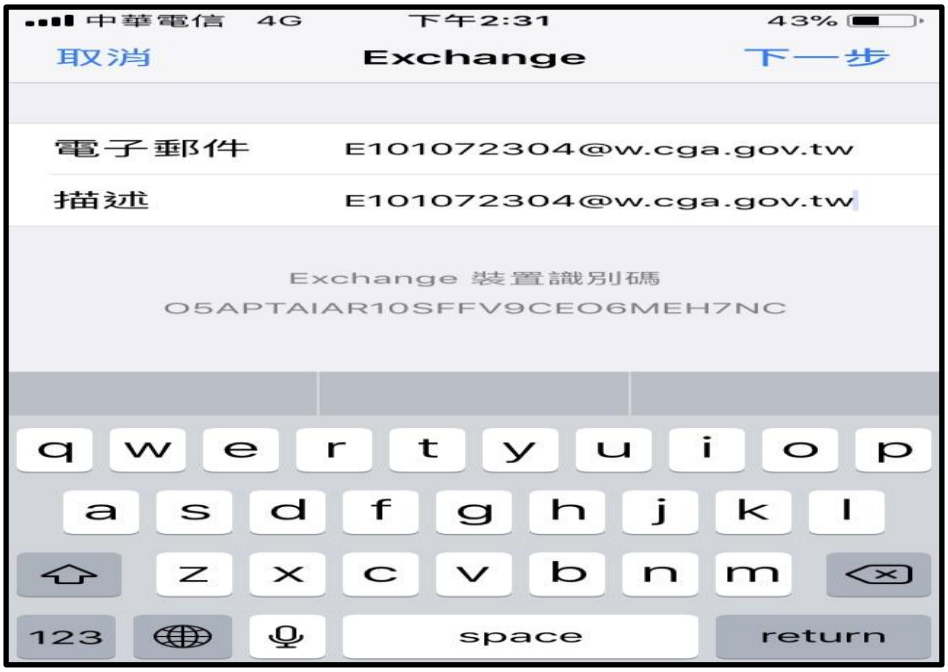
[32] 是一種利用透過網際網路針對微軟作業系統的電腦進行攻擊的加密型勒索軟體兼蠕蟲病毒。

[33] 微軟作業系統(Microsoft Windows)，是微軟公司推出的一系列作業系統。

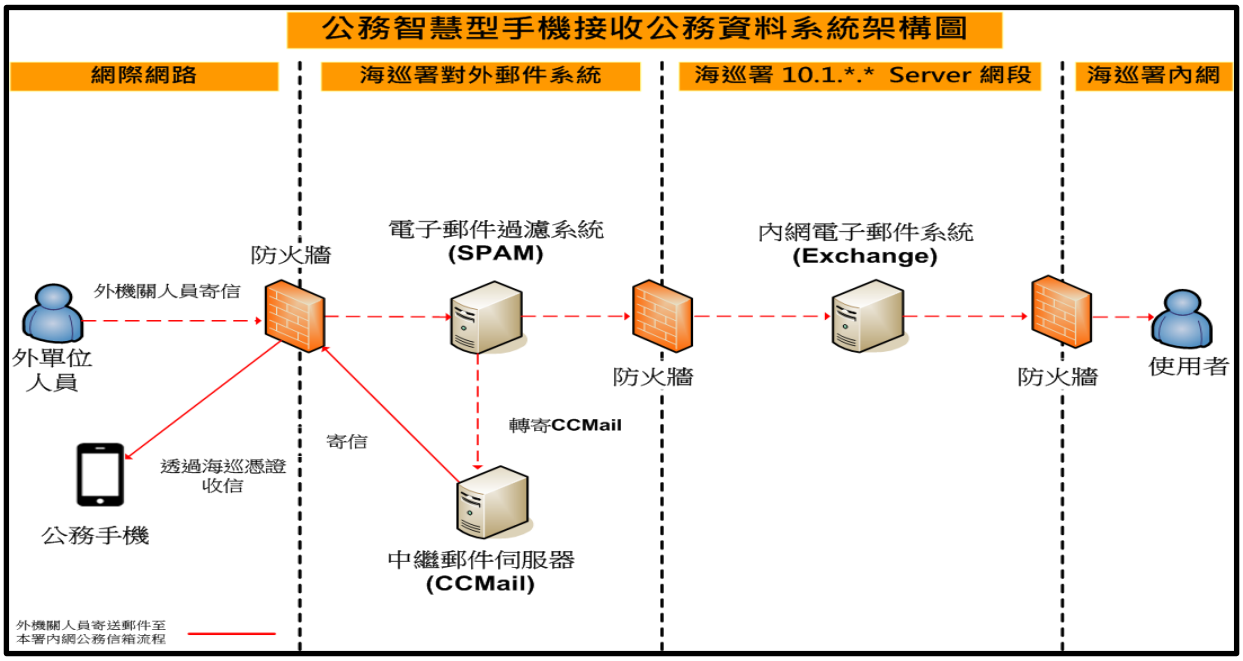
[34] 勒索軟體是一種特殊的惡意軟體，與其他病毒最大的不同在於駭客將受害者的電腦鎖起來，或是加密受害者硬碟上的檔案，並要求受害者繳納贖金以取回對電腦的控制權或解密檔案。

[35] 電腦蠕蟲與電腦病毒相似，是一種能夠自我複製的電腦程式，但濡蟲與電腦病毒最大的不同是電腦蠕蟲不需要附在別的程式內，駭客無須介入操作也能自我複製。

[36] 政府組態基準(Government Configuration Baseline，簡稱 GCB)目的在於規範資通訊終端設備的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

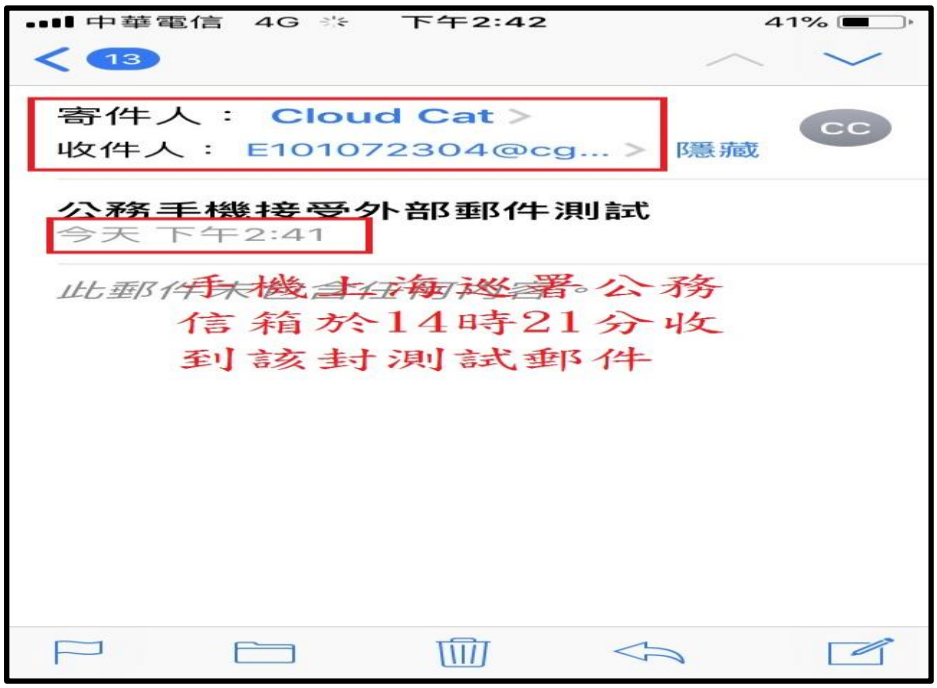


圖五：公務手機上設定海巡署公務郵件信箱



圖六：公務手機接收外部機關郵件架構圖

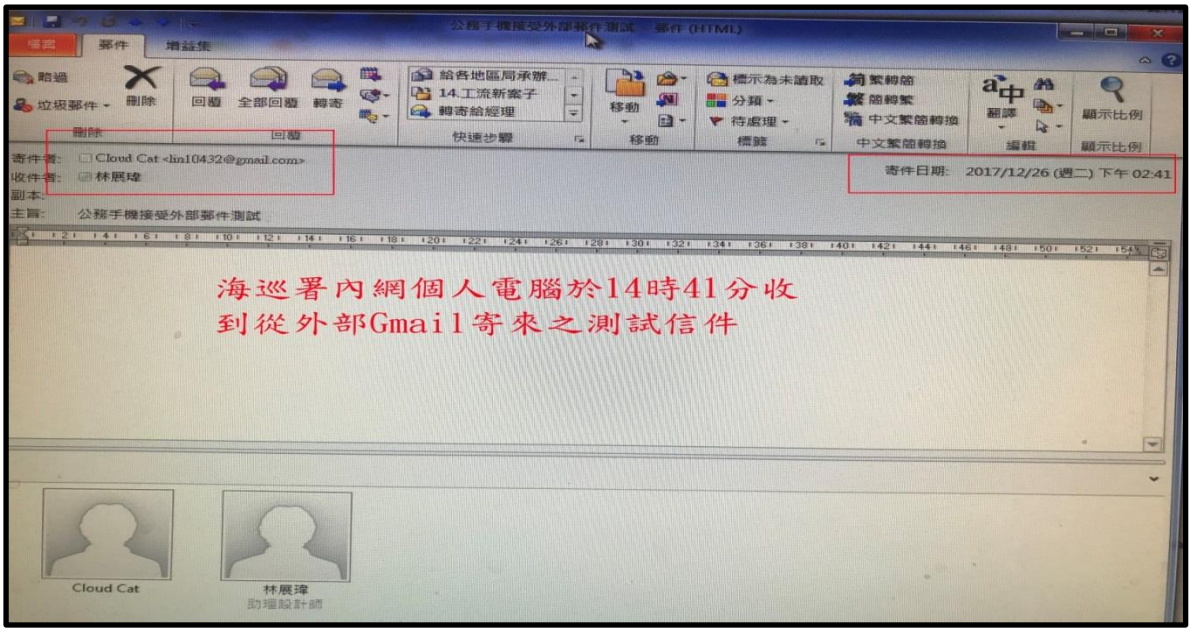
圖七：透過 Gmail 寄送郵件至海巡署信箱



圖八：公務手機上公務信箱收到測試郵件

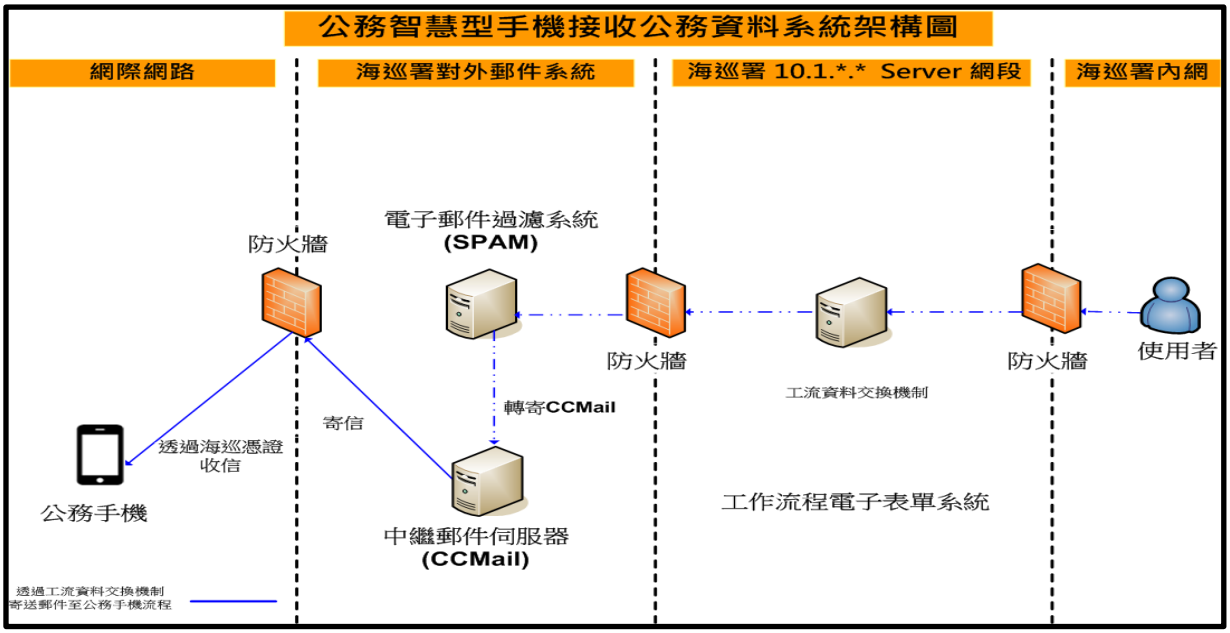
(一)經測試公務手機與本署內網公務信箱均可在外部信箱寄送測試郵件後，收到相關測試郵件，本項規劃設計之系統架構，經驗證可達成研究目標。

(二)經測試外部信系寄送測試郵件時間與公務手機接收郵件時間，僅 1 分鐘落差，符合第一章第四節，加速資料傳遞速度，滿足各式海巡任務需求，進而提供決策者獲得迅速及精準資訊之研究目標。

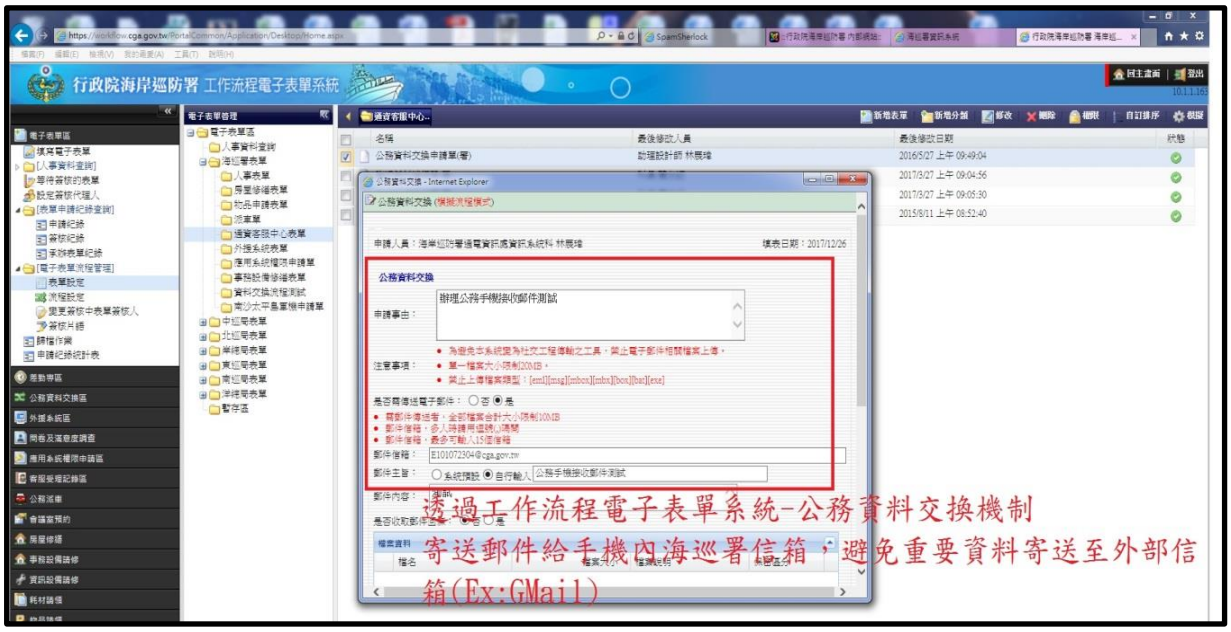


圖九：海巡署內網公務信箱收到郵件

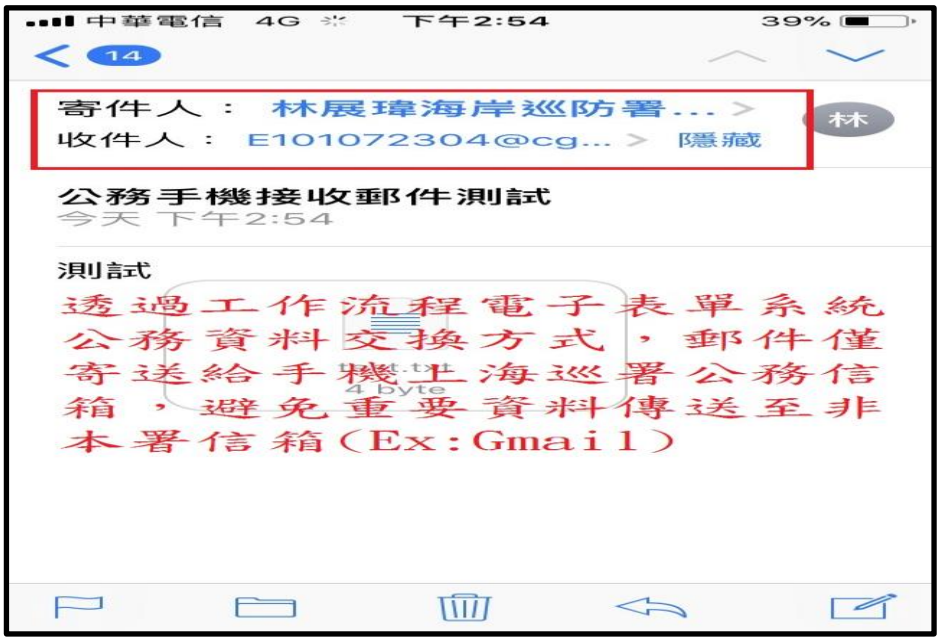
二、依照前述規劃設計之架構（圖十，藍色實、虛線部分），驗證本署工作流程電子表單系統-公務資料交換機制(內寄外)，可使公務手機收到交換寄出之郵件。(如圖十一、圖十二)



圖十：內部寄送郵件流程圖



圖十一：工作流程電子表單-公務資料交換機制，申請寄送內部郵件



圖十二：公務手機上公務信箱收到郵件

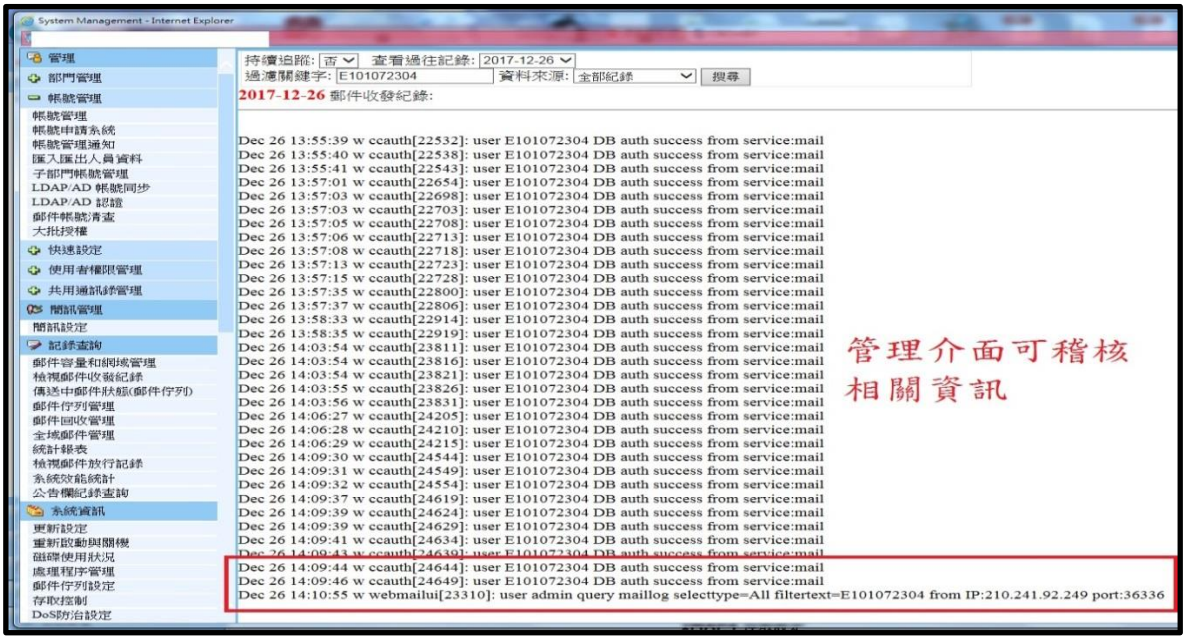
(一)經測試公務手機於本署工作流程電子表單系統-公務資料交換機制寄送郵件後可，收到相關測試郵件，本項規劃設計之系統架構，經驗證可達成研究目標。

(二)經測試工作流程電子表單系統-公務資料交換機制寄送之測試郵件時間與公務手機接收郵件時間，僅 1 分鐘落差，符合第一章第四節，加速資料傳遞速度，滿足各式海巡任務需求，進而提供決策者獲得迅速及精準資訊之研究目標。

三、經過上述兩種寄送方式測試，確認設定本署公務郵件信箱於公務手機上，可同步收到外部網際網路(例如：Gmail)寄送至本署內網個人公務信箱，以及透過本署工作流程電子表單系統-公務資料交換機制(內寄外)，轉寄之內網公務郵件，本次研究目標達成。

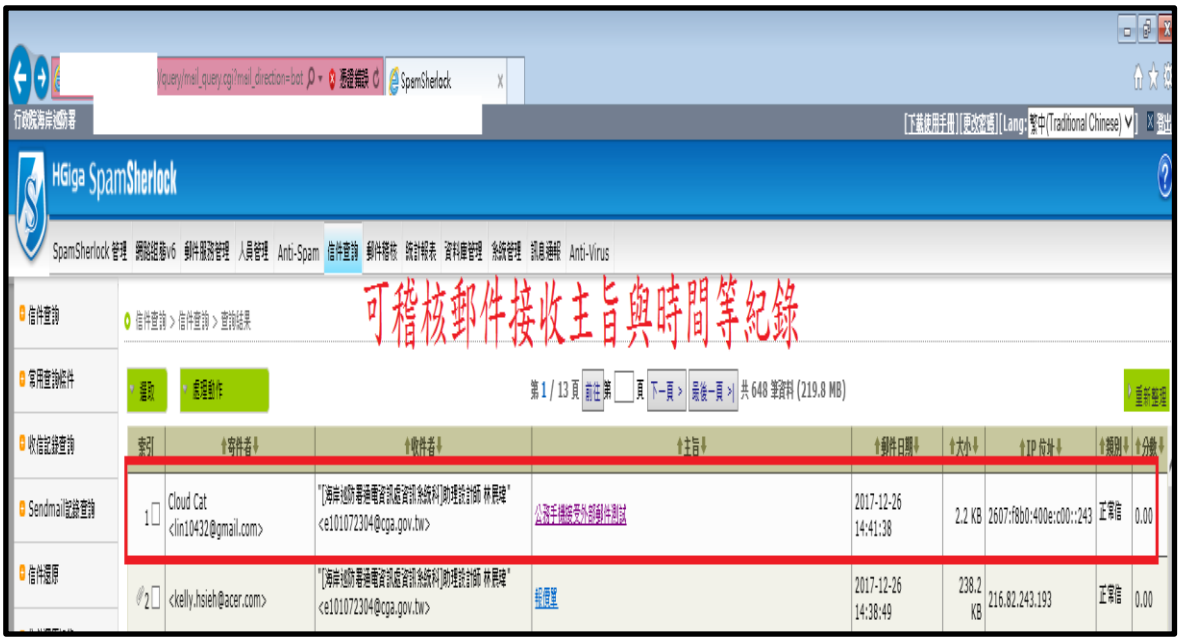
第五節 郵件紀錄稽核

經研究公務手機確實可收到電子郵件，除了實作成功外，更重要的是稽核，現在最流行的就是所謂的「數位鑑識[37]」，古云凡走過必留下痕跡，相關管理機制與規範建立，除為了避免本署機敏資料外洩，亦或者事件發生時需追查源頭，前述兩種寄件方式，「工作流程電子表單-公務資料交換機制」可由權責長官審核寄送內容，其餘可透過中繼郵件伺服器及電子郵件過濾系統來稽核郵件寄送過程、時間與來源等相關資訊，達成郵件寄送資訊具備可稽核性。(如圖十三、圖十四)



圖十三：中繼郵件伺服器稽核畫面

[37] 數位鑑識（有時又被稱作數位鑑識科學）乃是鑑識科學的其中一個分支，主要在針對數位裝置中的內容進行調查與復原，這常常是與電腦犯罪有所相關。



圖十四：電子郵件過濾系統 SPAM 稽核畫面

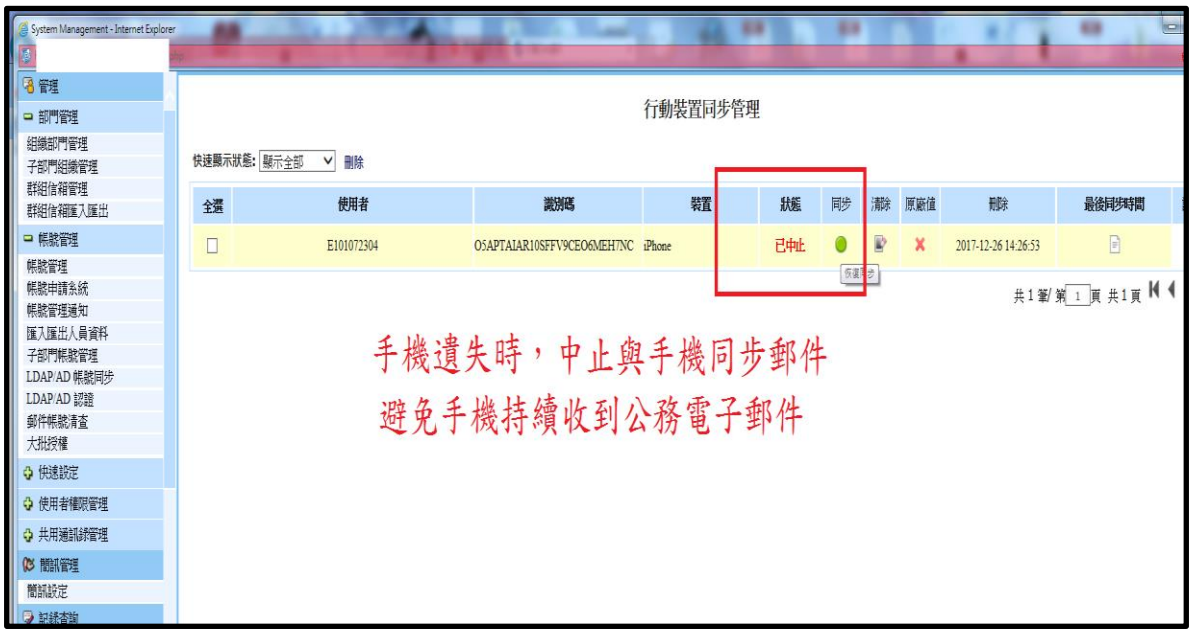
第六節　手機遺失防護措施

依據國外媒體Courier Mail[38]於 2016 年 10 月份的報導，4 名澳洲布里斯本的手機零售店員工在未經其他女員工以及顧客的同意下，私下拍攝許多他們的照片，並互相分享與對他們的長相評分，更可怕的是其中還有一些照片是從顧客送修的手機裡偷擷取出來的，讓人不禁對行動裝置的資訊安全感到相當憂心。

本次研究鑒於手機資料外洩意外層出不窮，無論是蓄意或是不小心，資料外洩即造成對單位形象之傷害，故秉持著國軍救災時「超前佈署」的未雨綢繆精神，預先設想當公務手機遺失且可能洩漏機密時，如何即時應變以避免資訊外洩，相關應變措施計有「中止同步」與「清除公務手機郵件資料」等兩項，相關說明如下：

一、中止同步：可透過管理介中止與遺失之公務手機同步，避免公務電子郵件持續同步傳送至手機上海巡署公務信箱(如圖十五至圖十八)。

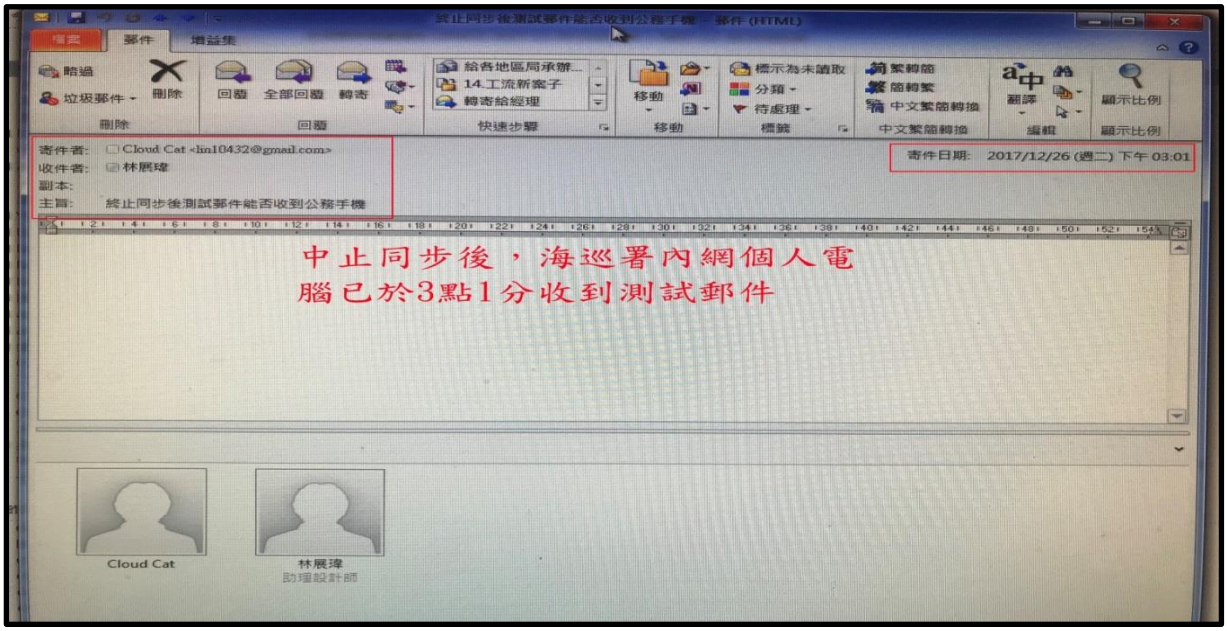
[38] 快遞郵報，一家位於澳洲，創立於 1864 年的報社。



圖十五：手機遺失時，透過中繼郵件伺服器停止與公務手機同步

(一)為驗證中止同步功能是否可行，於中繼郵件伺服器管理介面停止同步後，透過個人信箱寄送測試郵件。

圖十六：透過 Gmail 寄送測試信件至海巡署內網公務信箱

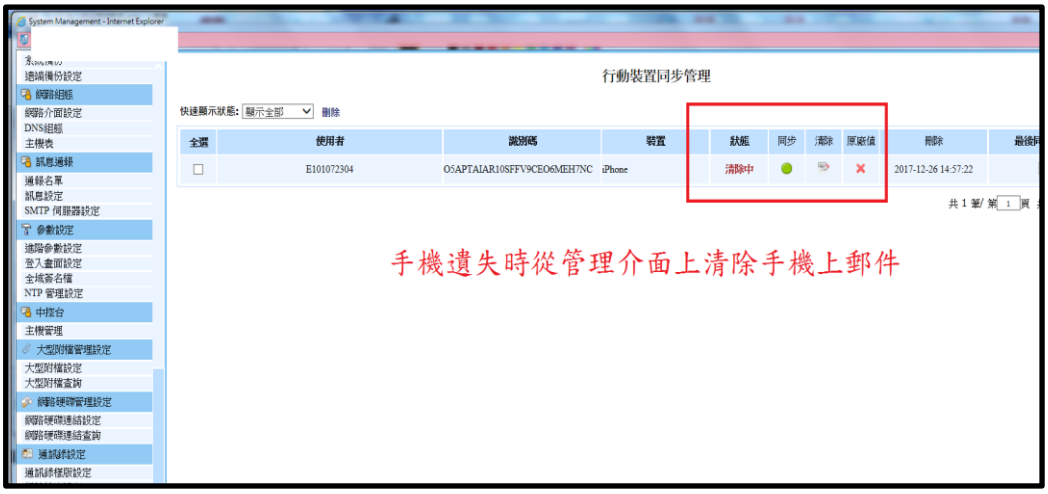


圖十七：海巡署內網公務信箱已收到測試郵件

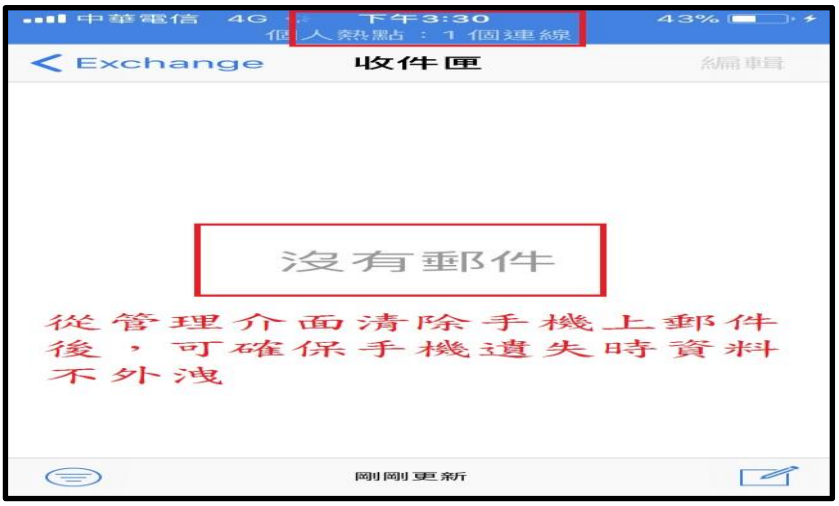
圖十八：驗證中止同步後，公務手機即無法收到公務郵件

(二)經驗證於中繼郵件伺服器管理介面停止同步後，寄送之測試郵件均無法順利傳遞至公務手機，可確保手機遺失時不在同步公務郵件，降低資料外洩風險，本項研究目標達成。

二、清除公務手機郵件資料：透過管理介面清除中繼郵件伺服器上郵件資料，可使公務手機上無法在讀取相關郵件(需公務手機可連結網際網路)，確保遺失之公務手機上無儲存任何本署郵件快取資料。(如圖十九至圖二十)



圖十九：從管理介面清除手機上可瀏覽之公務郵件



圖二十：驗證公務手機上已無公務郵件

三、經過上述兩種管理機制驗證與測試，確認設定有海巡署公務信箱之公務手機，可透過中繼郵件伺服器管理介面中止同步，及在公務手機連網情況下，透過清除中繼郵件伺服器上公務郵件，達成公務手機無法再瀏覽相關公務郵件，本次研究除達成公務手機可接收公務郵件外，亦達成相關資訊安全要求。

第四章　　研究發現、結論與建議

第一節 研究發現

資訊便利與資訊安全是個相對性的議題，本次研究主軸為「利用公務智慧型手機接收公務資料交換郵件」，亦須在兼顧資訊安全情況下設計系統架構與實作，達成提升同仁處理公務便利性，故以「憑證產出與安裝」、「郵件信箱設定與郵件寄送測試」、「郵件紀錄稽核」及「手機遺失防護措施」等四項研究、實作與測試，確保公務手機接收公務郵件符合資訊安全要求。

經過前述實作與測試，透過本署自建之公開金鑰基礎建設系統製發之憑證及中繼郵件伺服器，確保僅認證過公務手機可透過憑證驗證後接收公務郵件，的確可以使差勤在外之同仁公務手機，便利地接收公務電子郵件，反之亦可運用相同機制，及時回覆電子郵件與本署內網電子郵件信箱，期可提升差勤在外同仁處理緊急或長官臨時交辦事項之處理效率。

另結合憑證認證與公務手機同步方式，可於手機遺失時(需連結網路)，運用自建中繼郵件伺服器管理介面，中止與該遺失公務手機同步關聯，確保該公務手機停止接收公務郵件，並藉由清除中繼郵件伺服器上郵件資料，使遺失之公務手機上無法讀取本署公務郵件，避免公務資料外洩，達成資訊安全上的鑑別性、機密性、完整性、存取管控、不可否認性及可稽核性等資訊安全要求。

第二節 結論

根據 2017 年 iTHome[39]針對 CIO[40]所做的調查，臺灣有超過 4 成企業於 2016 年遭遇 1 至 9 次不等的資安攻擊事件，遭到 50 次以上攻擊的企業也有超過 2 成 5，而各產業的資安事件來源前三名，分別以駭客[41]、內部員工和離職員工為主；另政府機關與學校因為是 APT[42](Advanced Persistent Threat，簡稱：APT)攻擊鎖定的對象，其他較特殊的是約 1 成政府部門資安事件來源是該機關目前合作的資訊供應商。

依據前述資料顯示，在現今資安威脅日益高漲的環境下，本次研究主軸雖為公務手

[39] 是臺灣第一個網路原生報，提供 IT 產業即時新聞。
[40] CIO 是企業裡的高階主管職位之一，通常是負責對企業內部資訊系統和資訊資源規劃和整合的高級行政管理人員。
[41] 駭客通常是指對電腦科學、編程和設計方面具高度理解的人
[42] 進階持續性滲透攻擊 (Advanced Persistent Threat，簡稱：APT) 是一種常見的網路攻擊型態，攻擊者往往都是相當龐大且有組織的集團，且有明確性目標，而並非像一般的駭客事件可由單一駭客所為。

機接收公務郵件，但仍離不開相關資訊安全規範與執行，故本次研究目標除導入 BYOD 概念，輔以本署可攜式媒體的規範下，研究以公務手機為實驗主體，透過本署自建之公開金鑰基礎建設、憑證系統及中繼郵件伺服器，讓差勤或休假在外同仁，不用透過使用行動數據 VPN 無線網路(Mobile Data Virtual Private Network；MDVPN)[43]連結本署內部網路，也能即時接收外機關傳送之重要郵件，並避免同仁將敏感性公務資料寄送至私人信箱外，亦著重在如何透過郵件紀錄稽核及手機遺失防護等措施，來降低公務資料外洩風險，然當遺失設備在沒有網路的環境下，是無法進行清除公務手機郵件資料，再者亦無法限制公務郵件在公務手機上轉寄或截圖，故在所有防範措施皆執行情況下，資安事件最大危險因子仍然是人。

從行動裝置管理(MDM)角度來看，本署內、外網路實體隔離政策及可攜式媒體管理規範，已阻絕多數資安問題，然資訊安全防護除事後預警或稽核外，亦應建立在防患未然手段之上，我們相信每位同仁都不會蓄意洩露機密資料，只是人非機器人，在嚴謹的規範難免百密一疏，故除事先防微杜漸，主動發掘問題，解決問題外，仍須依政府機關資通安全責任等級分級作業規定，資安人員(資訊人員)至少 1 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練，而每年一般使用者與主管至少須接受 3 小時，透過不斷的教育訓練、耳提面命及人員考核作業，方可降低資訊安全的風險。

以行動應用管理(MAM)角度來看，使用本署工作流程電子表單系統-公務資料交換審查機制寄送之郵件，結合本署自建之公開金鑰基礎建設與憑證系統，再透過個人專屬憑證實施驗證，仍無法比擬桌面虛擬化(Virtual Desktop Infra- structure，簡稱：VDI)[44]的作業方式，可以讓同仁以虛擬私人網路[45](Virtual Private Network，簡稱：VPN)安全的連線方式連回機關，系統即會推送虛擬桌面到使用者的行動裝置，讓使用者在獨立的環境中存取系統的資料，VDI 雖然安全性高，但架構要先完成底層架構的虛擬化，必須投入較高額的成本，且效益並非顯著。

[43] MDVPN (Mobile Data Virtual Private Network，簡稱：MDVPN)為可以使同仁透過多種連線方式，直接連接單位網路執行公務，達到高效率與高效益之目的。

[44] 是一種桌面服務提供的模型，可讓使用者存取資料中心執行的 OS 映像檔。

[45] 虛擬私人網路是一種常用於連線中、大型企業或團體與團體間的私人網路的通訊方法。

第三節 建議

本次研究在兼顧資訊安全前提下完成系統規劃、設計、實作與測試，惟考量公務手機遺失時若無法連結網路，已接收之公務郵件將無法清除，尚具備一定安全風險，建議本署同仁若有公務手機接收公務郵件需求，應由權責長官核定後移由通資處協助設定，並應定期接受通資處資訊安全檢查，且機密文件不可透過本機制傳送，以降低公務資料外洩之風險。

參考文獻

一、註 2：維基百科-行動裝置網頁。(https://zh.wikipedia.org/wiki/行動裝置)

二、註 3：維基百科-傳呼器網頁。(https://zh.wikipedia.org/wiki/傳呼器)

三、註 4：維基百科-IPhone 網頁。(https://zh.wikipedia.org/wiki/IPhone)

四、註 5：INSIDE/趨勢網頁(民 105 年 8 月 1 日)。
(https://www.inside.com.tw/2016/08/01/bring-your-own-device)

五、註 8：知識力專家社群/密碼學原理網頁。
(https://www.ansforce.com/post/S1-p529)

六、註 9：知識力專家社群/密碼學原理網頁。
(https://www.ansforce.com/post/S1-p529)

七、註 10：知識力專家社群/密碼學原理網頁。
(https://www.ansforce.com/post/S1-p529)

八、註 11：知識力專家社群/密碼學原理網頁。
(https://www.ansforce.com/post/S1-p529)

九、註 12：維基百科-行動裝置管理網頁。
(https://zh.wikipedia.org/wiki/行動裝置管理)

十、註 13：維基百科-行動應用管理網頁。
(https://zh.wikipedia.org/wiki/行動應用管理)

十一、註 15：維基百科-趨勢科技網頁。(https://zh.wikipedia.org/wiki/趨勢科技)

十二、註 16：維基百科-阻斷服務攻擊網頁。
(https://zh.wikipedia.org/wiki/阻斷服務攻擊)

十三、註 17：維基百科-ISO2700 網頁。(https://zh.wikipedia.org/wiki/ISO2700)

十四、註 18：維基百科-公開金鑰基礎建設網頁。
(https://zh.wikipedia.org/wiki/公開金鑰匙基礎建)

十五、註 19：維基百科-憑證網頁。(https://zh.wikipedia.org/wiki/憑證)

十六、註 20：維基百科-單一登入網頁。(https://zh.wikipedia.org/wiki/單一登入)

十七、註 21：維基百科-超文本傳輸協定網頁。
(https://zh.wikipedia.org/wiki/超文本傳輸協定)

十八、註 22：維基百科-安全雜湊演算法 1 網頁。
(https://zh.wikipedia.org/wiki/安全雜湊演算法 1)

十九、註 23：維基百科-安全雜湊演算法 2 網頁。
(https://zh.wikipedia.org/wiki/安全雜湊演算法 2)

二十、註 24：維基百科-中央處理器網頁。
(https://zh.wikipedia.org/wiki/中央處理器)

二十一、註 25：維基百科-圖形處理器網頁。
(https://zh.wikipedia.org/wiki/圖形處理器)

二十二、註 26：海巡署資通安全政策網頁(民 103 年 8 月 19 日)。
(http://www.icsm.cga.gov.tw/icsm/upload/isms/newSYS/L1/CGA-L1-A5-001.pdf)

二十三、註 27：海巡署海巡法規網頁(民 106 年 6 月 14 日)。

(http://www1.cga.gov.tw/law2/law_06/通電資訊處/海岸巡防機關可攜式資訊設備及儲存媒管理作業要點)
二十四、註 28：植根法律網/法規資訊網頁。
(http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040030000007600-0920206)
二十五、註 29：維基百科-暗網網頁。(https://zh.wikipedia.org/wiki/暗網)
二十六、註 30：維基百科-明文網頁。(https://zh.wikipedia.org/wiki/明文)
二十七、註 31：維基百科-多重驗證網頁。
(https://zh.wikipedia.org/wiki/多重驗證)
二十八、註 32：維基百科-WannaCry 網頁。
(https://zh.wikipedia.org/wiki/ WannaCry)
二十九、註 34：維基百科-勒索軟體網頁。
(https://zh.wikipedia.org/wiki/勒索軟體)
三十、註 35：維基百科-蠕蟲病毒網頁。(https://zh.wikipedia.org/wiki/蠕蟲病毒)
三十一、註 36：行政院國家資通安全會報技術服務中心/政府組態基準說明網頁。
(https://www.nccst.nagov.tw/GCB)
三十二、註 37：維基百科-數位鑑識網頁。
(https://zh.wikipedia.org/wiki/數位鑑識)
三十三、註 39：iThome/關於我們網頁。(https://www.ithome.com.tw/aboutus/)
三十四、註 40：維基百科-CIO 網頁。(https://zh.wikipedia.org/wiki/CIO)
三十五、註 41：維基百科-駭客網頁。(https://zh.wikipedia.org/wiki/駭客)
三十六、註 42：Vavrin Chen,台灣微軟資安部落格/資安小常識網頁(民 102 年 7 月 13 日)。
(https://blogs.technet.microsoft.com/twsecurity/2013/07/07/apt/)
三十七、註 43：中華電信/行動數據群組企業網路/企業產品說明網頁。
(https://www.cht.com.tw/enterprise/mdvpn.html)
三十八、註 44：財金資訊季刊 第 66 期網頁(民 100 年 5 月 4 日)。
(https://www.fisc.com.tw/tc/knowledge/quarterly1.aspx?PKEY=57ab6f4f-da27-41fb-97dc-cc60ffc04d05)
三十九、註 45：維基百科-VPN 網頁。(https://zh.wikipedia.org/wiki/VPN)