垃圾郵件之防治策略與成效

游適彰、費雯綺

前　　言

近年來隨著網際網路的盛行，垃圾郵件橫行肆虐的現象已經造成了網路世界最嚴重的問題。本所歷年來跟隨著時代潮流，防治垃圾郵件不遺餘力，茲於本文中淺談垃圾郵件之認知與概念，並以本所電子郵件安全防護體系之內容架構與運作模式，展現垃圾郵件之防治策略與實質成效。

垃圾郵件之認知

一般使用者對於垃圾郵件的認知大多一知半解，其實我們可以將它與真實郵件做個比較。相信家家戶戶的郵筒內總是會塞滿一堆不請自來的廣告信或宣傳單等，有些載明地址多由郵差送來，然而更多的是工讀生挨家挨戶塞進來的。它們不一定會載明寄件者或收件者，也可以不署名或是隨意編造，一樣可以將信件塞進郵筒中。電子郵件也是一樣，e-mail 信箱就是郵筒，任何人都可以寄信進來，所以一般使用者會質疑垃圾郵件上載明之寄件者、收件者與現實不符，其道理是相通的。垃圾郵件來源者可以在網路上收集我們公開的 e-mail 地址，類似病毒的作法，隨機抓取通訊錄兩筆紀錄充當寄件者與收件者，真正收件者置放於『密件副本』中，所以傳送郵件之便利性與隱密性更勝過真實郵件。

至今仍有許多使用者對於垃圾郵件的判定未盡明瞭。首先，垃圾郵件通常無特定寄件者，所以持續收到同一位寄件者來信，大多不是垃圾來源，可能是某位廠商或朋友在未取得同意下，任意將其加入電子報或發送名單中，只要回信告知即可解除騷擾。但是碰到千真萬確的垃圾郵件，千萬不能再回信告知，一來垃圾來源端可能造假，只有徒增伺服主機負荷，二來可能掉入陷阱，落入對方郵件名單之身份確認者 VIP 名單中，那就因小失大了。其次，如同前述說明，垃圾郵件寄件者大多偽造，所以收到熟識的寄件者甚或是自己發送之垃圾郵件，千萬不要太過衝動回頭找當事者或系統管理員理論，因為都是垃圾郵件惹的禍。一般郵件表頭隱藏的資訊，必須打開郵件詳細內容才能觀其全貌，許多垃圾郵件在攤開表頭內容後便無所遁形，所以是一項重要的追蹤依據。

行政院農業委員會農業藥物毒物試驗所技術專刊第 155 號。

一般使用者總是喜歡奇聞共欣賞，所以收到一封自覺必要轉告週知之郵件後，馬上好心地傳送給通訊錄裡面的親朋好友甚或是單位內部所有員工，然而所有收件者名單通常是洋洋灑灑公開陳列在郵件表頭中，藉由轉寄過程顯示在郵件內文一覽無遺，不小心落入郵件名單收集者手上，立刻被一網打盡，全數落袋。所以建議使用者在轉寄郵件時，將收件者名單全部放入『密件副本』中，如此一來收件者名單就不會曝光了。

垃圾郵件之防治策略

近年來隨著網路普及化之後，垃圾郵件已經成為最嚴重的網路問題，真實世界之廣告信函無法避免，還好網路世界有資訊廠商研發了許多對抗垃圾郵件之技術設備，可以協助我們防禦垃圾郵件之橫行。

本所約於七年前開始進行垃圾郵件之過濾功能，當初採用的是簡易型郵件防毒與內容過濾軟體，所有過濾條件完全自行定義，猶如螳臂擋車一般，規則條件定義之速度根本趕不上垃圾郵件千軍萬馬式的襲擊，所以成效十分有限。系統管理員在處理隔離郵件過濾放行之沈重負荷下，縱使有心對抗，亦只能徒呼負負，盡力而為。隨著垃圾郵件問題日益嚴重，市場需求面大增，相關資訊廠商亦投入大量研發技術產出設備。於是本所開始尋求反垃圾郵件產品設備之功能檢測，進行功能評比與適用度評估，兩年前本所順利建置妥當完整之電子郵件安全防護體系，不僅大幅淨化了所內同仁電子信箱，更減輕了系統管理員的負荷，讓垃圾郵件不再是心頭大患。

垃圾郵件的危害除了造成信箱爆滿影響正常運作外，其背後包藏禍心的陷阱更是危機重重。諸如電腦病毒、網路釣魚、後門程式等，意圖破壞電腦運作、騙取使用者名稱密碼、入侵竊取資料文件等，成為資訊安全防護體系重要的一環。本所在電子郵件流程管理中部署了多層次關卡設備(圖 1.)來對抗垃圾郵件；首先第一層是路由器入口端，經由入侵偵測系統過濾病毒夾帶與郵件攻擊行為，進入網路防火牆系統再經一道病毒過濾，確保無毒郵件方可進入。接著進入第二層電子郵件安全閘道器中，依據郵件表頭與內容掃瞄，透過寄件人評等機制(Reputation Filters)進行全球性垃圾來源資料庫(SenderBase)之追蹤比對，提供有效的過濾預防郵件之攻擊。系統包含閘道過濾器與郵件隔離主機，閘道器負責電子郵件入口端第一道防線，經判斷疑似垃圾郵件即送至隔離主機供使用者自行判定是否收取該郵件。經約一年檢測結果，由建置前半年平均隔離阻絕之垃圾郵件約佔所有郵件之 5～6 成(圖 2.)，至建置滿一年統計結果卻已逼近 7～8 成(圖 3.)，可見垃圾郵件成長之驚人速率。平均正確攔截

率約可達 95%，已經可以阻檔絕大多數的垃圾郵件，另外針對 5%漏網之魚隔離補強作法，一是等待系統自動更新黑名單資料庫，二是在第三層郵件內容過濾軟體系統中，手動新增隔離黑名單之關鍵字比對規則(來源 IP、內文網址、特定字眼…)。最後到達使用者端仍然逃脫時，可以將垃圾信檢舉回報至本所管理員信箱，提供最後一層機制讓使用者進行判定或防堵措施。在垃圾郵件隔離區(圖 4.)中，系統整合本所『目錄服務系統(LDAP)』帳號密碼進行驗證，使用者可以登入檢閱個人化系統隔離之垃圾郵件，遇到被系統誤判之郵件可立即點選回送使用者信箱。經檢測結果僅有少部分電子報被系統誤判隔離，將其加入系統白名單即可。個別使用者幾乎可以不需理會其他被隔離的郵件，因為隔離正確率將近 99%。

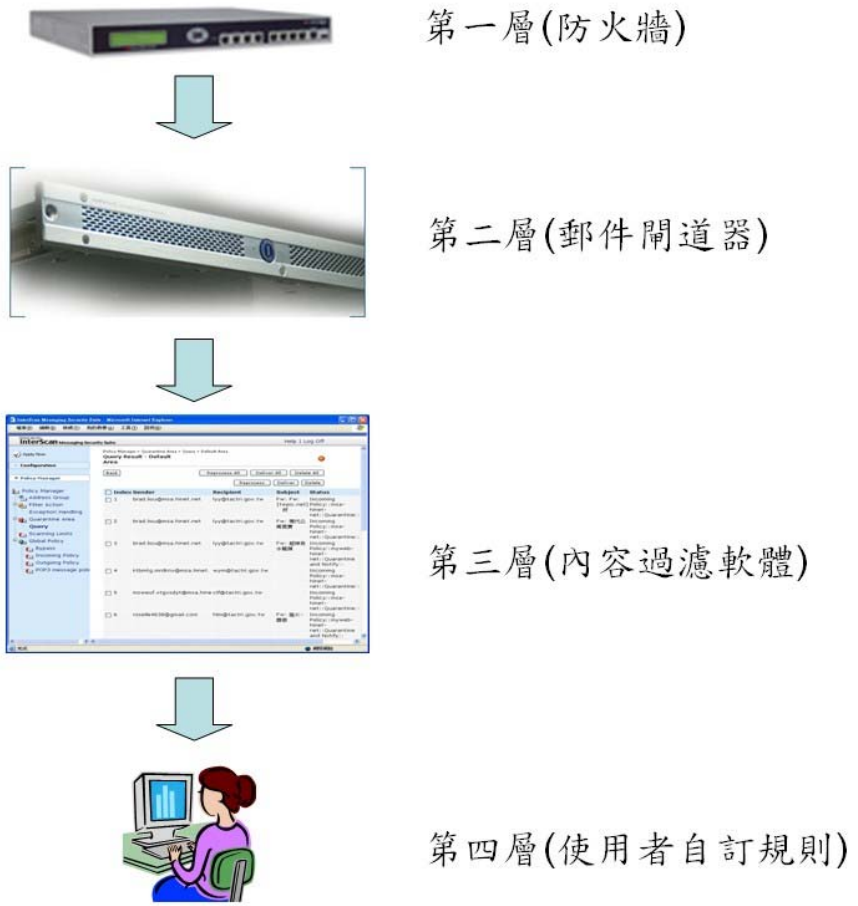

圖 1. 電子郵件安全防護關卡流程。

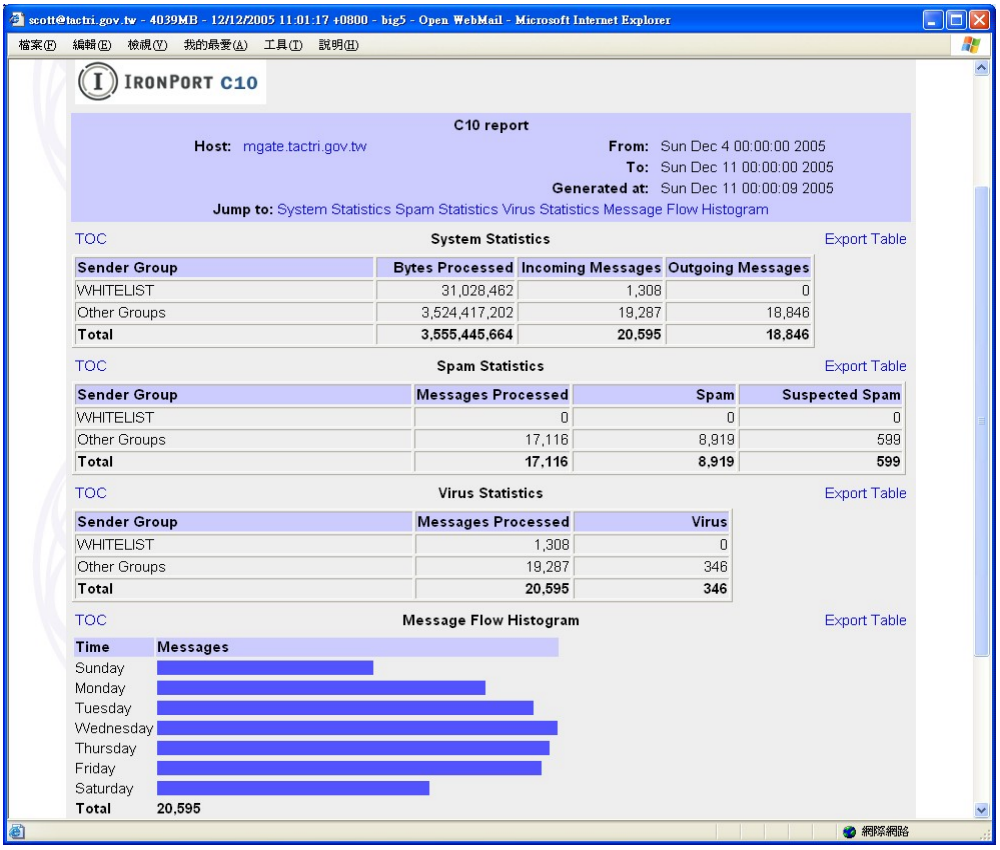

圖 2. 電子郵件閘道器建置半年統計報表。

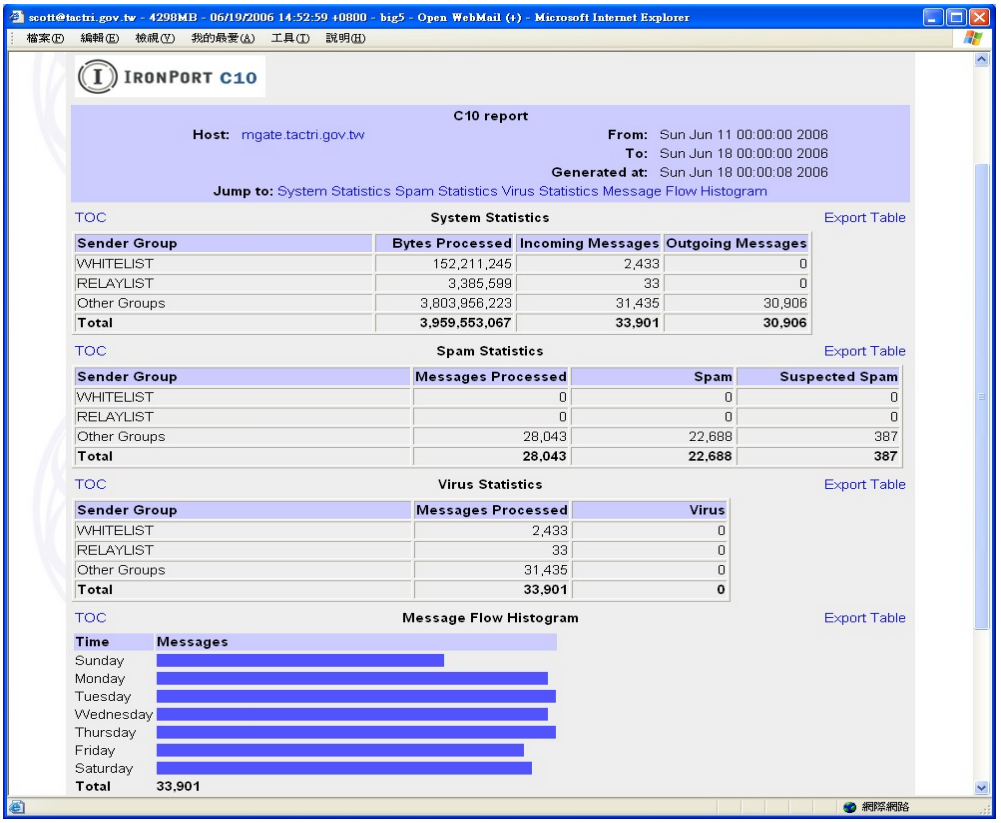

圖 3. 電子郵件閘道器建置一年統計報表。

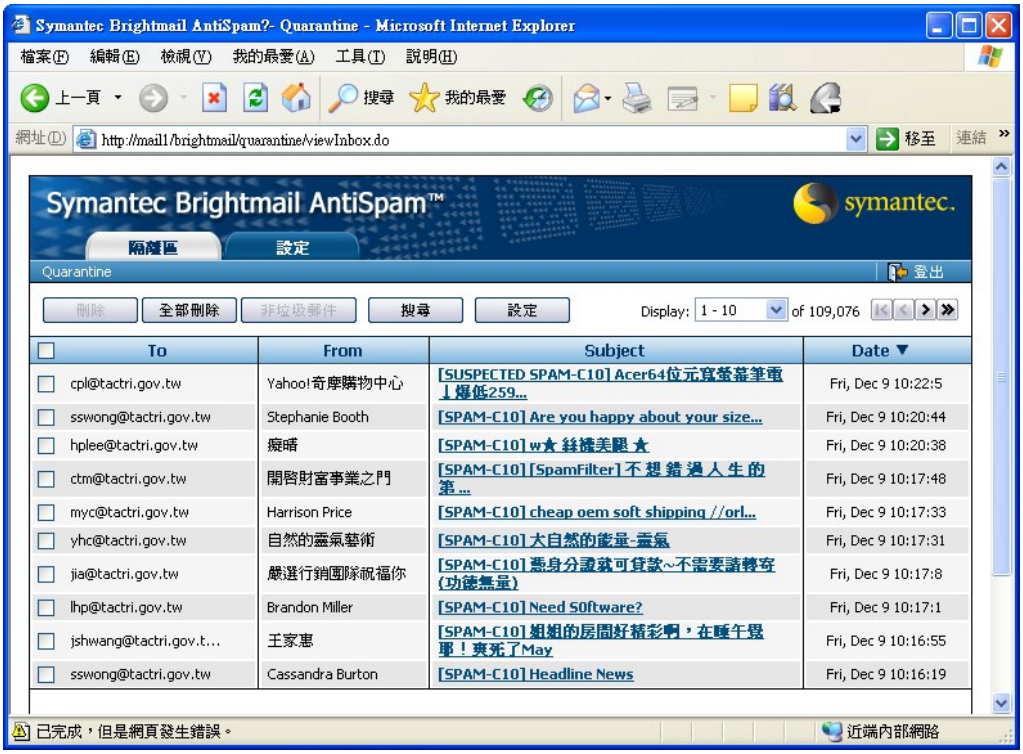

圖 4. 垃圾郵件隔離區。

電子郵件管理成效

一套優良的反垃圾郵件產品必須具備四大要點：效能佳、精確率高、管理簡化、後端資料庫永續支援。本所在建置電子郵件安全防護體系過程中，審慎評估挑選廠商設備，進行借用測試實機上線運作，瞭解每一家設備是否符合上述四大要點。尤其重視的是管理層面是否人性化，部分產品強調之個人化隔離功能，卻是在正常郵件中夾雜隔離郵件通知，形同是另一種精神轟炸，畢竟眼不見為淨才是真正隔離。另有產品強調不做內文掃瞄效能奇佳，其實正好落入垃圾郵件暗藏玄機的陷阱中。有些產品更是完整記錄所有郵件的收發內容，雖然有助於管理者進行垃圾郵件之分類定義，但是對於郵件隱私權之尊重，似乎未盡妥當。然而最終選擇的產品依然無法提供百分百的信賴度，所以我們才必須在第三層增加人工化郵件內容過濾軟體系統，攔截系統無法正確判定之垃圾郵件，提供管理員更彈性的自主空間，雖然增加一些管理負擔，但是確保使用者擁有幾近淨化的郵箱空間，才是終極管理之目的。

在使用過程中曾經發生因緣際會之狀況，顯示出完整防護體系之重要性，因而達到了系統備援之功效。其導因於第二層之郵件閘道器設備因有原廠提供之一年有效使用授權，到期後未及時續購，導致系統自動

終止郵件過濾之動作，結果宛如河川潰堤般，造成垃圾郵件如入無人之境直攻第三層，怨聲載道因而四起。所以趕緊進行夾攻防堵策略，在第一層與第三層分別加入郵件過濾規則，依重點關鍵字清除垃圾來源，在短時間內即刻恢復基本防護功能。但是畢竟無法達到原始設備精確防治之功效，同時也造成系統管理員必須承受更大的負擔，以因應備援期間可能的風險。使用者在習以為常之體系保護下，頓時遭受垃圾郵件之攻擊，更凸顯出垃圾郵件之防治對於使用者之切身影響不可言喻。

架構完成電子郵件安全防護體系以來，目前遭遇最大的問題還是垃圾郵件製造者刁鑽的本性難防，一年多前大量的垃圾郵件寄件者均為 msa.hinet.net，不僅帳號採用隨機亂數產生，發信來源更是採用動態 IP 位址。有了中華電信合理提供之護身符與機動式 IP 的攻擊行為掩護下，完全逃脫反垃圾郵件的搜捕陷阱，所以辛苦的系統管理員為了應付此類新興模式行為，只好回到早期過濾放行的痛苦日子，針對 msa.hinet.net 的大量郵件逐一清查，似乎又在走回頭路了。依大致統計結果，每日處理 msa.hinet.net 來源信件中，屬於正常郵件必須放行者，少則一成多則五成，為了多達半數以上的垃圾郵件持續奮力抵抗中。近來駭客集團盜取帳號密碼的行徑風行草偃，垃圾郵件亦跟上了時代潮流，開始大量利用盜取帳號進行正大光明的傳送手段，或是在各大入口網站申請免費帳號橫行肆虐，可惡的是光憑郵件表頭根本不會被攔截，管理員僅能針對郵件內文進行人工過濾。因為垃圾郵件千變萬化最終的目的還是希望使用者點選連結至特定行銷之網站，所以針對內文網址連結進行阻絕，尚可收到一些防範後續大量來襲之功效，但所謂的道高一尺、魔高一丈，最終結果仍是防不勝防，僅能達到被動式防禦的功效。

結　　論

目前反垃圾郵件的問題比起電腦病毒肆虐的現象，實在是有過之而無不及。電腦病毒有其特徵碼可供辨識，垃圾郵件卻是無孔不入，更擅長於偽裝、欺騙、易地、整容，甚至已經成為電腦病毒與後門入侵惡意程式散播之最佳途徑。所以反垃圾郵件的技術必須再更加精進，否則未來只好走向安全郵件的收發模式，對於電子郵件的限制越多，其便利性亦將相對受到考驗。雖然各國極力推動垃圾郵件立法禁止之罰則，國內亦有『濫發商業電子郵件管理條例草案』與『電子廣告信件管理法草案』待審中，但是平心而論所有的法律畢竟只是規範，在網路無國界的環境下，擅長鑽研取巧的垃圾郵件應該還是會想盡辦法鑽法律漏洞，誰是輸家實難以斷定。

對抗垃圾郵件必須要從上游做起，如同在單位內部若未建置閘道端郵件過濾機制，每位使用者皆須設定郵件規則以防堵垃圾郵件，不僅成效不彰，反而更增加使用者的困擾。國內之郵件服務提供者不論是付費或是免費，都必須有自律精神合力對抗垃圾郵件，而不是以商業利益為考量，任由網路資源遭受濫用，反倒替垃圾郵件製造者孕育了溫床。使用者本身亦必須建立拒絕垃圾郵件誘惑的正確觀念，不隨意點選垃圾郵件內文以避免落入陷阱中，濫發郵件之始作俑者在沒有生意上門之狀況下，自然就不會再大量採用電子郵件的行銷手法了。