抵禦垃圾郵件危害　營造乾淨使用體驗

郵件過濾管理 打造郵件安全第一步

文◎余采霏

垃圾郵件手法推陳出新
抵禦垃圾信　多層次手段大鬥法

使用無誤才能發揮作用
管理設定正確與否　攸關過濾效果

掌握大方向採購要領
預先規劃需求　盡信數據不如實測

電子郵件透過網路快速傳遞訊息使得人與人之間溝通更為順暢與方便，在現今公務聯繫上，幾乎離不開電子郵件，許多部門溝通、跨國業務執行，也都仰賴電子郵件才得以完成，對企業來說，電子郵件已經成為營運重要關鍵，不可或缺。

但另一方面，垃圾郵件也嚴重影響企業員工的工作效率，根據資安業者的研究報告顯示，2009年垃圾郵件約占所有電子郵件的九成（88%），也就是說，平均十封信件中，只有一封是正常郵件。垃圾郵件造成的危害不僅如此，許多病毒、木馬程式或是駭客也都利用垃圾郵件進行犯罪或竊取資料販賣，來牟取不法利益。

確保郵件安全的首要工作就是做好垃圾郵件過濾，讓正常郵件in，垃圾郵件out。在這一期的郵件過濾管理主題中，將探討近年來垃圾郵件手法的演進，再從技術面討論現今有何創新技術來解決這項困擾，以及IT人員如何選擇郵件過濾管理方案來協助企業因應這些垃圾郵件的挑戰。

垃圾郵件手法推陳出新

抵禦垃圾信 多層次手段大鬥法

長期以來，電子郵件的重要性一直不可或缺，由於電子郵件系統幾乎是每個企業或組織必要使用的網路應用，不管是內部營運或外部溝通都得仰賴電子郵件收發才得以完成，使得電子郵件成為企業溝通營運的重要關鍵。

然而，電子郵件也開始成為惡意入侵以及資料外洩的一大隱憂，基於利益，許多不法的應用開始規避檢驗的技術，非法性交易、詐騙持續在垃圾郵件裡發展，病毒、木馬程式或是駭客也都利用垃圾郵件來進行犯罪或竊取資料販賣，牟取不法利益。

中華數位產品暨市場營運中心產品經理高銘鍾表示，垃圾郵件已經成為常見的病毒傳染管道，不像早期以破壞形式展現，現在的病毒都與宿主共生，並且盡可能不讓宿主發現，以大量繁殖與傳染。現階段，垃圾郵件除了可以直接夾帶病毒本體之外，還是雙重攻擊的前置步驟，在使用者點進郵件內的連結而瀏覽器被感染的過程中，垃圾郵件就成了間接途徑的角色。

▲中華數位產品暨市場營運中心產品經理高銘鍾表示，垃圾郵件已經成為常見的病毒傳染管道，現在的病毒都與宿主共生，並且盡可能不讓宿主發現，以大量繁殖與傳染。

網路地下經濟惡勢力

根據今年4月賽門鐵克公佈的全球網路安全威脅研究報告，2009年垃圾郵件約占所有電子郵件的88%，平均每日來自世界各地的一千零七十億封垃圾郵件中，有85%是由殭屍網路發送，而目前至少有五百萬台電腦受到Cutwail、Rustock及Mega-D等十大殭屍網路感染、控制。這份調查同時也指出，在2009年發現受殭屍網路感染的電腦，在地下經濟體系中以每台0.03美元賤價販售。

地下經濟指的是逃避政府監管，以不法手段取得利益的一種經濟活動，而現在垃圾郵件也成為網路地下商業行為要角。專家發現，電子郵件帳號密碼在黑市的銷路水漲船高，每天公開販售的電子郵件帳號的正常交易量平均都超過30,000個帳戶，這些帳號很容易就成為詐騙的對象。黑市銷售帳戶資料幾乎可以廉價來形容，如果數據屬實的話，每10,000個Hotmail帳號密碼組合大約值90美元，而這些帳號只要有5%的回覆率，詐騙得來的利益就相當可觀。

30年戰火未熄

垃圾郵件發展至今已經超過

30年，史上首批被定義群發垃圾郵件事件是起因為DEC公司內有位職員向400名居住在美國西岸的用戶發出邀請函，希望收件者能夠參加該公司當時所推出的微型電腦展示會。

追溯早期的發展動機，形成原因其實很單純，由於網路成本相較於自印傳單或電話行銷都要來得低廉，上網申請免費信箱就能收發信件的便利性讓許多人利用郵件取代其他溝通媒體，成為另一種廣告溝通管道。由於發送電子郵件幾近零成本，而且有利可圖，慢慢地也就愈來愈猖獗。

Openfind產品經理廖享進指出，台灣電腦最常作為跳板也是因為有地下商業利益行為所致，駭客以手上擁有的殭屍電腦作為籌碼，不管是以代發一封信件為計價單位，還是以命中率收費，每秒發送的幾億封信中，到達率就算只有5%也相當可觀，這些利益成為驅動垃圾郵件愈來愈難以控制的主因。

「反垃圾郵件技術正面臨著與防毒軟體對抗病毒類似的困擾，駭客因為利益所以會不斷地規避檢驗技術，這就像一場戰爭，郵件過濾技術的生命周期很短，不到半年就換了一個議題、方向，三個月前更新的資料可能現在就不管用。如果有新的防堵垃圾郵件技術出現，很顯然地，Spammer也會馬上換一個手法或技術來規避偵測。」

垃圾郵件近期發展

垃圾郵件發送手法愈來愈高明已是不爭的事實，例如4月份受到留意的手法之一是IPv4類型的垃圾郵件劇增，駭客將惡意的IP連結網址置於垃圾郵件內文，使得網頁過濾機制無法偵測到不安全的連結，同時也規避反垃圾郵件中過濾郵件含URL技術。

VIAGRA!
V1agra!
Via<!--hi-->gra
V1agr@!
Vi<asdf>ag<asdf>ra
V' 1ag^r" a; V.i.a.gr.a; V-i-aGr.a; (add noise)
Vi ag ra

▲垃圾郵件的內容手法多變，故意寫錯字，加上符號或是插入不相關文字都是常見手法。（圖片來源：綠色運算）

5月份垃圾郵件又轉往社交網路，誘拐使用者機密資料，藉由假冒發出「重要通知」郵件誘騙使用者點選下一步，導向已被劫持的社交網路。而6月份，圖片式垃圾郵件透過殭屍網路，結合熱門時事攻擊使用者電腦，作為散播更多垃圾郵件的工具。

「這些只是較常見事件，」高銘鍾指出，垃圾郵件手法之多，光是內容演變能做的手腳就難以細數，例如為了要避開偵測，垃圾郵件會避開行銷廣告常用的字眼，改由隱諱字眼來取代，以Viagra（威而剛）為例，以前會直接把藥品名稱寫上去，現在則是用「你想要夜晚變得更勇猛嗎？」來取代，人類可以判斷隱諱意思，但是機器卻無法判斷這樣的思維。又或者是故意像小學生寫錯字，把關鍵字排成直的，中間插漂亮的花紋或是乾脆變成圖片型的垃圾郵件等等手法來規避。

殭屍網路最大發送來源

針對近期垃圾郵件，專家們也提出一些觀察，廖享進表示，目前最熱門的手法就是從殭屍網路發送垃圾郵件，根據一些調查顯示，台北市已經成為全球第二大中木馬最多的地方，成為2009年全球受殭屍網路感染最多的城市，占全球5%，足以顯示問題的嚴重性。

第二個主流是以合法掩護非法，例如駭客利用Hotmail、Gmail或Yahoo帳號提供的群組寄信功能，當使用者登入後，自動化程式碼卻在幕後悄悄透過快捷鍵反覆寫信與寄信，因為來源的IP是合法的，所以就難在第一時間辨別。

「去年2009年中到2010年初還很流行的退信攻擊，關鍵也是合法掩蓋非法，假冒受害者地址寄出大量無法傳遞的垃圾信，造成受害者被退件流量所淹沒。

A攻擊B與C，這過程中B與C都是無辜的，有時候C要追查攻擊來源還不容易，因為A很有可能就是一台殭屍電腦，退信攻擊的困擾不在於垃圾郵件，事實上垃圾郵件如果只是廣告信的利益還不夠大，關鍵是要讓殭屍網路更壯大。」

附檔垃圾郵件為大宗

新軟市場業務部產品副理程智偉認為近期的垃圾郵件的攻擊都轉向附件化，尤其是從中國大陸來的垃圾郵件更是如此。程智偉指出，像醫藥性內容就會附上.jpg檔，而一般的推銷課程則是以夾帶Word的方式來達到廣告效果。

由於檔案的附件格式很多，過濾掃描時必須先對檔案解碼才能過濾內容，這在偵測上會增加難度，「最近這種附加檔案型的垃圾郵件、木馬或攻擊就變多，之前流行的圖片型垃圾郵件、PDF垃圾郵件，也是附加檔案型的一種，為了規避偵測，Spammer一定會瞭解各種過濾的優缺點，也知道各種發送Spam型態的優缺點，附加檔案型的垃圾郵件，在防禦的難度上相對也提高了。」

反垃圾郵件防禦機制

不過，針對殭屍網路與附加檔案型垃圾郵件，目前都有防禦機制。以殭屍網路來說，IP信譽評等仍是主流的作法。

IP信譽評等

廖享進提到，現在的IP信譽評等與以前不同，早期被熟悉的是RBL（Real-time Blackhole List，即時封鎖清單），可以自己舉報、平反。新的IP信譽評等是動態的，只會設定一個期限，並不會永遠被判死刑，這個IP在Out-black期間內有逾矩行為，就會給1～2天是在黑名單內，之後就會移出來。

IP信譽評等並不只應用在郵件上，也用在Web。而且IP信譽評等的好處是如果信件出現很多釣魚網址或釣魚內容時，有IP信譽評等機制就能透過公開的查詢單位，即時地查到相關的資料。

循環樣本檢測

第二種方法是循環樣本檢測（Recurrent Pattern Detection，RPD）技術。RPD技術不同於傳統比對電子郵件內容或是黑白名單過濾法，這個技術針對全球合作夥伴所提供的垃圾郵件進行採樣，每個月偵測並分析30億封以上的垃圾郵件，收集網際網路上的郵件爆發行為，即時分析並建立郵件行為資料庫，透過循環比對的模式，判別各種語言的垃圾郵件。

廖享進表示，垃圾信的原理是同一個時間點在全球各地突然會大量地湧出，而且內容一模一樣。可能一千封或二千封。姑且不論它是不是垃圾郵件，這個行為本身就不是很合理，一般在觸動這個行為之前是要有所知會的，例如是銀行帳單、合法宣傳信件等等，如果不是在這些類別時，就有合理的理由懷疑是廣告信，而且不再用IP的觀念去阻擋，而是這個信件內容在全球各地都出現時，就直接阻擋。

▲Openfind產品經理廖享進指出，反垃圾郵件技術正面臨著與防毒軟體對抗病毒類似的困擾，駭客因為利益所以會不斷地規避檢驗技術，這就像一場戰爭，如果有新的防堵垃圾郵件技術出現，很顯然地，Spammer也會馬上換一個手法或技術來規避偵測。

內容過濾

信譽評價機制只對透過殭屍網路發送的垃圾郵件最為有效，而被破解的方法是以合法掩飾非法，因為是正常管道發出來的信件，所以不容易查覺。程智偉指出，這個時候就要仰賴內容過濾（Content Filter）技術，只從連線層來源判斷只能部分過濾。「目前內容過濾的方法有很多種，像是關鍵字過濾、貝氏過濾、指紋

過濾、針對URL的連結過濾，大部分的技術很多都針對內容過濾的變形而發展出來的偵查技術。因為垃圾郵件會混用各種手法，所以垃圾郵件過濾技術也要交叉使用，在內容過濾上，多層掃描是必要的。」

來源與特徵

附加檔案型垃圾郵件最大的問題是造成設備更大負擔，平常要掃描的垃圾郵件已經夠多了，若是每封信件的附加檔案都要先解碼，再針對文件內容過濾，無形中就會加重設備的負擔，「解決的方案是不要硬碰硬，可以先用其他過濾技術，當所有的手法都判斷不出來，但可疑性又很高時，再來針對附件分析，這樣影響設備效能的機率就比較少。」

高銘鍾舉例，像是圖片型垃圾郵件不見得一定要針對圖片掃描，OCR文字辨識引擎會消耗很多效能，只要Spammer在圖片上動手腳，光學辨識的效果又會很差，所以對付圖片型垃圾郵件會先從特徵、來源來判斷，不一定要在圖片掃描上硬碰硬，同樣的概念也可以應用在附加檔案型垃圾郵件上。

從行為出發

對付垃圾郵件，綠色運算行銷業務專案經理何婉筠認為關鍵在於行為而不是內容。她提到，目前最常見的垃圾郵件包括圖像式垃圾郵件以及殭屍電腦。圖像式垃圾郵件過去也常用OCR文字辨識引擎來處理，但是太多的影像處理軟體能變換不同的字體，往往造成OCR的錯亂。另一方面，多數的使用者經常電腦中了木馬而不自知，被駭客拿來當作發送信件的跳板，一封垃圾信可以複製成上百萬封發送，這也是常見的手法。

「從垃圾郵件發展的歷史包袱可知，Spammer對於反垃圾郵件的作法早已洞悉，不管是查來源（黑白名單、RBL、Safelist）或是從內容過濾（關鍵字過濾、內容過濾、貝式分析），現在都無法有效防止，Spammer因背後涉及龐大的商業利益，已運用商業化經營，而且結合高深的Messaging技術，運用最新的Spam Botnet+Image Spam（殭屍電腦網路與附件檔型垃圾信）攻擊手法。」

何婉筠指出，垃圾郵件為了躲避過濾軟體的偵測，多半會採用各種造假的技術。同一份垃圾信，在不同的造假版本之間，仍然會存有相當程度的相似度，利用這樣的特性就能有效阻擋，也就是說垃圾信件最大共通特徵在於造假、大量發送與相似度，而這些特徵無關於內容、語言與地域，從行為來看就能輕鬆的判斷。

多層防禦 勢在必行

殭屍電腦發送垃圾郵件爆發程度令人咋舌。看看Joey Costoya寫的「How Many Spam Can a

7大常見垃圾郵件手法

垃圾郵件層出不窮，日前賽門鐵克就發表7大垃圾郵件手法，可作為IT管理人員參考。

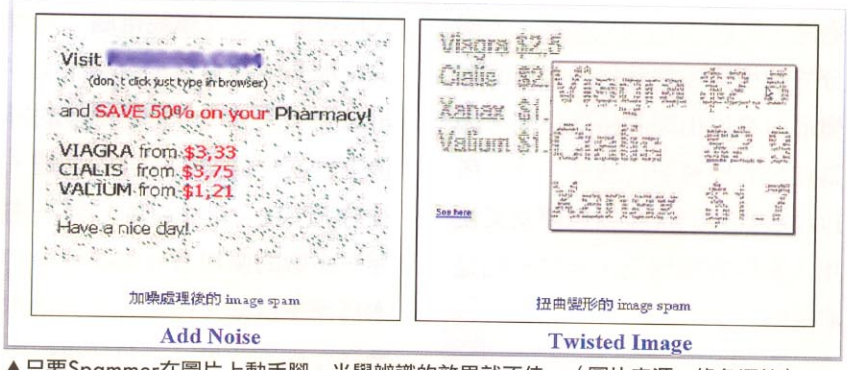
1.假邀請函（Fake Invitation）。垃圾郵件作者假藉知名社交網路，邀請使用者加入網路。利用電子郵件中的連結，重新將使用者導向另一網站。
2.帳號整合。假意對使用者宣傳帳號整合，並在使用接受此方式後，建議加入幾位好友，藉此手法盜取使用者資料，並劫持帳號散播更多垃圾郵件。
3.假冒照片標籤/意見通知（Tag/Comment）。垃圾郵件作者假冒照片標籤訊息或意見回饋通知，讓使用者毫無防備，落入陷阱，成為垃圾郵件受害者。
4.應用程式。社交網路允許開發者程式的好意，以及熱門小遊戲，也已成為垃圾郵件作者的下手目標。
5.傳送惡意程式。各式各樣的假冒通知函也是垃圾郵件作者愛用的手法之一，以散播惡意程式。尤其要注意的是，有垃圾郵件作者，透過誘使使用者下載社交網路工具列，植入木馬程式。
6.隱私權保護。社交網路的隱私權也是近日熱烈討論的話題之一，使用者要小心的是可提供使用者DIY檢測個人資料是否被社交網路盜用的產品廣告。這極可能是垃圾郵件作者的另一種手法。
7.假問卷。假藉社交網路心裡測驗等名義，讓使用者重新導入另一個網頁填寫機密資料，進而盜取。

Spam Bot Spam?」提供的數據就足以令人膽戰心驚。這篇文章以惡名昭彰的Mega-D作為測試對象，過去Mega-D算是最多產專發垃圾郵件的殭屍網路（Botnet）之一，發送量曾經高達全球垃圾訊息量的50%，現在雖然比較收斂，但仍不能小覷。

在這篇文章中，Joey Costoya在所處的惡意軟體實驗室中釋放出一支Mega-D垃圾訊息傀儡殭屍樣本，想要觀察一個殭屍網路／傀儡網路Botnet一天內能發送多少垃圾訊息。結果令人吃驚，單個傀儡殭屍在24小時之內就可產生約2,553,940個垃圾訊息，平均每分鐘產量為1,764個垃圾訊息。

顯然地，垃圾郵件製造幾乎以不受控制的速度在增長，面對這項事實，企業或者反垃圾郵件業者該如何接招？答案是多層次的防禦手法加上雲端連線的行為資料庫。

前文已經提及，垃圾郵件為了規避偵測，手法不斷更新，除了利用Word檔、PPT檔、PDF檔進行宣傳之外、信件標題、內文、圖像都是管道，為了圍堵垃圾郵件，各家反垃圾郵件設備的過濾機制也多半具備黑名單比對、關鍵字比對、來源比對、貝氏演算法，甚至還有各個RD技術團隊研發的掃描機制。以中華數位為例，一封電子郵件會經過五層掃描，包括連線模式過濾、黑白名單過濾、內容過濾、自動學習過濾來確保郵件的安全性。



▲只要Spammer在圖片上動手腳，光學辨識的效果就不佳。（圖片來源：綠色運算）

不過，即使如此，仍有1%～5%的垃圾郵件沒有辦法依靠內建的演算法判斷，為了補強這個漏洞，人工介入是最好的方式。程智偉指出，新軟有一組團隊專門就在分析這些行為，不管是從各地誘捕系統（Honey Pots）取得的樣本還是從企業回報機制得知的樣本，在經過分析後都會即時更新到企業內部的設備，以保持最佳的防禦力。

這種雲端系統下的行為資料庫作法不只新軟，多數業者都有類似的雲端系統，綠色運算、網擎、中華數位、Cellopoint、趨勢、賽門鐵克等等，幾乎所有的郵件過濾廠商都用這種方式來搜尋漏網之魚，廖享進指出，這已經是所有反垃圾郵件業者必要的作法，「我認為機器學習與文字探勘技術在實體應用上已經面臨瓶頸，雖然這些方法可以抓出特定形式的廣告信，但卻沒辦法應付人類由腦袋產生的思維，回到問題的根本是背後還是需要非常大量的樣本，需要有跨國運作的團隊，能夠針對全球的垃圾信分析，資料庫雲端支援是相當重要且基本的一環。」網管人

四大類型垃圾郵件

另外，賽門鐵克歸納出近期垃圾郵件常出現的四大事件類型：

類型一：利用天災 如海地和智利地震，利用大眾的善心上網捐款或物資，植入惡意程式。
類型二：結合時事和新聞 垃圾郵件發送者會利用諸如知名車廠召回問題車款、求職信件、世足盃、漏油事件等熱門時事，趁機冒用企業名稱散播垃圾郵件和惡意程式。
類型三：利用年節慶典 這是垃圾郵件發送者慣用的手法，不論是新年、聖誕節、母親節等，都可看見猖狂的垃圾郵件肆虐。
類型四：透過社交網路 如病毒進化一般，垃圾郵件發送者也不斷推陳出新，尋求更多管道提升其散播垃圾郵件的成功率，尤其時下正夯的社交網路，更是他們虎視眈眈的目標。

使用無誤才能發揮作用

管理設定正確與否 攸關過濾效果

垃圾郵件對企業造成的影響甚鉅。網路頻寬浪費不說，員工生產力與工作效率跟著降低；因為附件夾帶的病毒、木馬程式，使得企業資訊安全風險升高，同時也增長了管理成本。

就以員工生產力與工作效率來看，假設100人公司每天平均郵件為50封的狀況下，以現今幾近9成的垃圾郵件比例換算，平均每月的垃圾郵件就高達9萬封。假設每封信件閱讀只需一分鐘，總共要花上1500小時，約等於187.5天的工時。若以每月員工最低的工資17,280元來計算，耗損的薪資支出就高達162,000元。

這是保守數據，因為病毒、木馬程式而導致機密外洩所造成的信譽損失以及法規罰則更難估計。這也是為什麼，垃圾郵件發展多年來，每年都在上演著攻防戲碼，尤其垃圾郵件危害日增，企業需要可靠的郵件過濾設備來加以防堵，不過IT人員可能不知道，就算找來功能最齊全、防護面最完善的機種，如果規則政策或組態設定出錯，就等於為垃圾郵件開了後門，曝露在風險中。接著就以企業內部常見的錯誤設定為主軸，邀請專家暢談他們的看法。

關鍵字造成系統錯亂

綠色運算行銷業務專案經理何婉筠分析，許多企業內部部署的郵件過濾設備在使用多年後，因為加入太多關鍵字而造成設備在判定時的混淆，以前陣子最受矚目的世界足球賽來說，A使用者認為有世足字眼的信件一律都是垃圾郵件，但B使用者卻認為不是，當不同的使用者有不同的判定並且回報給系統時，就很容易導致系統錯亂。

何婉筠認為，垃圾郵件的造假行為，就像是金光黨的詐騙手法，一直在翻新，經常使用關鍵字過濾的結果常常會導致誤判，有時會影響企業內部運作。「最好的方式還是以行為來判別，而不是由內容，就像高雄醫學大學本來是利用Open Source軟體自建郵件系統，常常加一些關鍵字。因為學生的論文多半從外部信箱寄送到教授的信箱內，而且文章中又加入很多藥品字眼，常常就被誤判為垃圾信，如果發生在期中考或期末考，學生的成績就會變零分，這對電算中心來說就很有壓力。改用NOPAM之後，這個問題就有效解決了。」

黑白名單與帳號密碼

從技術上來看，個人主觀判斷是垃圾郵件過濾技術長久以來都無法突破的一道牆，使用者的抱怨對於IT管理人員的工作績效更有極大的殺傷力，但同一封信件，部分收信者認為是垃圾郵件，但另一些收信者卻認為不是，該如何解決？新軟市場業務部產品副理程智偉認為，解決誤判的最好做法就是將垃圾信件先放在隔離區裡，系統會對使用者定時發送通知信，告知有那些信件被放在隔離區內，讓使用者可

以取回垃圾信。

「企業最大的問題並不在於誤判，而是黑白名單設錯，許多人會認為公司內部互寄的郵件一定是正常信件，但是現在很多垃圾郵件都是偽造公司郵件位址，如果是這種狀況就會全數通過。」

程智偉提醒，企業防堵垃圾郵件時，很重要的一件事是「會不會成為垃圾郵件的跳板」，萬一電腦中毒，往外發送垃圾郵件造成的影響更大，沒多久就會被RBL當作黑名單，這比垃圾郵件還要頭痛，因為企業將被劃為垃圾郵件來源，這是無盡的惡夢，除了要跟各個RBL申訴，而且這段時間與客戶往來的信件也都不能順利寄達，雖然有解決的方法，但還是很麻煩。

效能錯估與細部管理

Openfind產品經理廖享進認為，企業常見錯誤觀念有兩點，一是效能的錯估，另一則是管理者對於個人使用設定的管控。

他表示，由於防垃圾郵件產品大部分已經被包裝成設備導向，通常都會以為買一台設備就可以解決所有問題，最容易發生的是錯估流量的負荷，因為反垃圾郵件設備並不像郵件伺服器單純把信件收下來就沒事，反垃圾郵件設備可能需要經過非常多的過濾技術，一般的思維會把需求設定與郵件伺服器相同的等級，然後就能應付相同的流量，但是這是錯誤的觀念。

「做為防護的設備一定會比單純傳遞資料所需的硬體資源要多一些。在導入時一定要非常清楚流量規模如何？甚至要考慮未來流量要成長到什麼地步，而且垃圾郵件攻擊是一陣一陣的，設備能撐到最大極限值為何？功能能否執行、合不合乎需求是一回事，如果這一關都過不了的話，連正常的傳遞都做不到。能負擔的流量上限至少要算到正常值的1.5倍，才是保險的界線。」

另一個容易發生的困擾是管理者對於個人使用設定的管控。有些使用者對於電腦一竅不通，而且對反垃圾郵件技術也不熟悉，偏偏又是主管、人事或副總而且不會設定，遇上這樣的狀況，管理者只能跟對方要密碼，去改他的個人設定，這就會有風險，很少產品會提供管理者中控所有使用者的設定，或是進入單一使用者，但這很重要，這能減少許多管理上負荷。

白名單誤設及密碼管理不當

中華數位產品暨市場營運中心產品經理高銘鍾表示，大部分較嚴重問題都是設定錯誤造成，尤其是白名單的設定問題。「很多的使用者怕郵件被誤攔，所以經常使用白名單，但又以最大法則來設定，例如Yahoo寄來的信不希望被攔，所以白名單就設Yahoo.com.tw，如此一來，垃圾信就一直穿透，而無法防阻。」

第二個部分是密碼管理不當被破解，因而對企業內部大量攻擊，例如帳號是Abbott1234，密碼也設為Abbott1234。「我認為這個觀點是需要被宣導的，許多使用者並沒有意識到密碼的設定不應該能夠從一些線索去猜到，但這卻非常重要，中華數位有一個工具可以協助檢查信件帳號密碼設定是否強健，再協助IT管理人員加以改善。」

另外，他也建議IT管理人員不要一直調校郵件過濾設備，企業在部署之初可以針對企業內部的現狀做最好的調整，但之後便不要常常調校，一來是IT人員會覺得很煩，二來是修改任何設定都有風險，需要小心謹慎地進行。「除非是瞬間有垃圾郵件大量攻擊時，在緊急狀況下可以請原廠支援馬上設關鍵字封鎖，等到原廠更新Pattern到設備內時，再開放設備過濾。」

工欲善其事，必先利其器。垃圾郵件不斷蜂擁而來，企業又該如何選購合適的工具來加以防堵？另一方面，個人資料保護法已經三讀通過，雖然細則尚在制定，但因應個資法，企業在郵件方面又該留意那些？下一篇文章將會針對這些議題加以討論。網管人

掌握大方向採購要領

預先規劃需求 盡信數據不如實測

企業佈建電子郵件的目的原先是為了增進溝通效率、降低營運成本並且用來提升業績，但是垃圾郵件的出現，不僅造成使用者工作上的不便，對IT管理人員來說也是一項大挑戰，病毒、蠕蟲、木馬、網路釣魚、惡意網頁，搭配駭客的精細手法以及垃圾郵件發送，讓企業的資訊安全曝露在高度風險中。

防範垃圾郵件成為企業營造乾淨使用電子郵件環境中重要的一步，經過多年與垃圾郵件交手歷程，許多反垃圾郵件設備早已不再單純只有垃圾郵件過濾機制，防毒、稽核、備份等功能穿插加入，甚至延伸到政策管理，為的就是打造完整的電子郵件防護。

由於防範垃圾郵件的形態很多，企業在郵件伺服器、郵件過濾防毒相關的閘道器、UTM以及相關的反垃圾郵件或郵件內容安全軟體都能找到解決方案，企業要選擇何種方式部署，還是要看企業原本已建置那些基礎設備或系統，才能因地制宜，找出最合適的方案，因此本文的採購法則將跳脫不同解決方案的比較，主要還是以應具備的採購思維為主。

大公司不要買小機器

企業採購預算當然是優先考量，但卻不能做為唯一的法則。前文提到企業最容易發生錯估流量的負荷的判斷，以為只要把需求設定與郵件伺服器相同的等

番外篇

因應個資法 企業該有的因應對策

新版個人資料保護法已經三讀通過，個資法對於企業有兩項影響，一旦洩漏個資，在民事損害賠償上，總額上限從2千萬元提高至2億元，而且還可透過眾人的力量來集體控訴。

落實到電子郵件上，新版個資法對於企業郵件的要求是，郵件不應該有可以看得到的個資。這意思是，個人資料不應該在沒有告知當事人的狀況下，透過網路而被截取或外洩。由於個資法處罰的對象是負責人，因此企業會開始正視個資流洩的問題，尤其是可能從郵件與網頁而造成的外洩風險。

多數專家都建議，在郵件的外寄行為上必須要要有稽核功能，不只內對外，內對內也是一樣，最好要能智慧到判斷那些內容是身份證字號、信用卡號碼、個資，遇到這些內容就要攔下來做處置，像是給主管看過後再放行的機制，或是直接阻擋告訴寄件人這是個資，違反公司的使用政策等等，先把風險攔下來再決定如何處理。

目前許多相關垃圾郵件設備供應商在稽核部分都提供相對應的解決

級，然後就能應付相同的流量，但是這是錯誤的觀念。

即使IT管理人員不能清楚知道流量，目前也有以人數作為簡單判斷的依據，但要在一個苛刻的環境下，希望能達到高效能的表現，幾乎是做不到的事，效能上也會大打折扣。

新軟市場業務部產品副理程智偉提到，大公司用小機器只適合在流量低的狀況下才行得通，若是不知道公司流量，最好是直接借設備來測試，結果立見。

不過，現今多數的反垃圾郵件解決方案，除了垃圾郵件過濾之外，為了達到有效防範，還會附加其他功能，像是病毒過濾、稽核功能等等，企業若需要將所有的功能全部啟用，那麼就一定會影響效能，最好還是避免選擇小機器。

確立郵件政策

由於每個人對於垃圾信件的認定不同，因此企業導入垃圾郵件過濾管理設備時，要思考的問題是，企業控管垃圾郵件的政策是什麼？如果政策是中控式，就是由企業來統一管理時，就要宣告公司的觀點為何，並且設立政策。

Openfind產品經理廖享進解釋，如果企業容許個人觀點的存在，就必須思考購買的設備有沒有企業有一套觀點，但個人也有一套觀點，並且可以決定優先順序的功能。假設今日企業把有「世界杯足球」字眼的郵件列為黑名單，但個人有可能把它列為白名單，如果容許這樣的政策存在，那麼郵件攔檢設備必須要個人設為白名單時就讓通過，而針對其他的使用者就阻擋起來的功能。

▲綠色運算行銷業務專案經理何婉筠提到，長期以來，廠商致力於攔截率的提升，面對全世界垃圾郵件發送比例逐年增高，反垃圾郵件業者必須優先想辦法提升攔截率。

「最根本的作法是，IT管理人員要想清楚，如果公司的政策希望大家都滿意，那麼產品的選擇最好要選可以開放個人設定的方案。」

方案，甚至有些已經內建在反垃圾郵件過濾設備中，企業不妨多加深入瞭解。當然，在導入稽核解決方案之前，IT部門、負責稽核工作的法務部門以及主管高層，連同供應商都應該坐下來討論，再進行導入工作。

免責聲明與主動告知

除了找到合適的工具外，企業最好加上兩項工作來確保法律層級的風險。

廖享進提醒IT人員，外寄郵件最好主動幫使用者加上免責聲明。聲明的內容必須指出，如果今天不幸有個資在文件內容中，要表明這個人的信件是公務上的信件，但內容不是公務上的內容時，不代表公司立場。

第二個關鍵是如果行為內有個資的話，必須在免責聲明中清楚寫明個資取得方式，例如企業在發送EDM時就必須自動聲明個資的取得方式是由合法來源取得，這要盡到主動告知的義務，而且最好是由公司中央控管，若是沒有做到這些工作，被外洩的對方可以拿這封信件去打團體訴訟，爭議在沒有允許的狀況下，使用到個資。

日本早在2005年便制定個人情報保護法，規定企業或團體組織有義務保護個人資料防止洩漏，須保存資料並確保可有效取得，因此日本反垃圾郵件業者為了防範使用者不小心外洩個資因而設計一項很有趣的功能叫誤送信防止。這項功能的原理很簡單就是強制使用者再看一次，寄信時會再跳出整封信件的內容讓使用者看清楚，同時也代表公司已經盡了義務與責任。

追蹤與舉證

稽核是為使用者誤寄信件而設的把關動作，萬一真的不小心外洩，就必須靠追蹤與舉證來擺脫法律上的

▲新軟市場業務部產品副理程智偉提到，大公司用小機器只適合在流量低的狀況下才行的通，若是不知道公司流量，最好是直接借設備來測試，結果立見。

攔截率與誤判率

攔截率與誤判率向來就是反垃圾郵件設備或功能的一項重要指標，它關係著企業會收到多少比例的垃圾信，以及使用者必須多常到信件隔離區撈回郵件。一般來說，業者的攔截率普遍都有90%以上的水準，甚至到95%～99%。不過，並不是所有的方案都能不經過調校就能達到這麼高的水準，部分方案還是需要實際上線調校才行。而有攔截就表示有誤判。如果使用者常常需要從隔離區撈回信件，肯定會招致抱怨，因此最好的狀態是誤判率能夠愈低愈好。

長期以來，廠商也都致力在攔截率的提升，綠色運算行銷業務專案經理何婉筠提到，全世界垃圾郵件發送比例逐年增高，就算攔截率高達99%，但過濾一萬封與一百萬封垃圾郵件的結果就是不同，以往使用者可能只會收到兩封，但是現在因為垃圾郵件數量增多，一天可能會收到十封，「當然這是反垃圾郵件業者必須面對的課題，廠商優先要想辦法提升攔截率。」

訂定測試指標

採購任何一種解決方案的初期，服務廠商一定都會提供規格及功能參考。反垃圾郵件方案已經算是很成熟的產品，許多設備在功能面上也都大同小異，管理介面也儘量朝向人性化設計，多數的採購人員最後還是會聚焦在成本效益上。

中華數位產品暨市場營運中心產品經理高銘鍾認為，一般人都會希望功能愈多愈好，但是企業要的究竟是多功能，還是功能多？只是要規格還是要深度？最佳的方式還是訂定一些測試指標來挑選，這會比只有比較規格要來得更為精準，「功能多並不一定好，因為往往有些產品各種功能並不能同時運作，所以比較防護性的深度是很重要的。」編管人

責任。追蹤指的是系統必須要能很快地知道這封信件的來龍去脈：從那裡進來、那一位使用者寄的、寄給了誰，什麼樣的內容，與這封信相關的信件有那些？

廖享進表示，不管是前端垃圾郵件過濾產品或是後端垃圾郵件歸檔稽核產品，都必須要有追蹤的功能，這是調閱的前提，如果沒有這個功能的話，IT人員買到的就是看起來很華麗但用起來不符合需求的產品，而且有個問題是出事了才知道好不好用，但與其出事，不如事前想清楚。

而舉證就涉及到儲存的信件與原始內容是否相符，是有被竄改的可能，因此管理者雖然是技術人員，但是卻不能賦予信件的內容或儲存的內容有任何異動的權限，這在權限管理設定上很複雜，最好功能面上能支援郵件歸檔的加密，或是只能寫一次但可以無限制讀取的機制，這些都是非常重要的事項。

廖享進認為，傳統對於資料保護都以訊息安全來稱呼，但其實應該進化到Assurance（保證），這個觀念在國外早就行之有年了，所有訊息傳遞與保存的過程中所有可能遇到的風險，都要有相對應的對策，這個對策不只是政策上也有技術上的，甚至包括資料的保存都要考量在內。

全方面的考量

企業電子郵件透露個人資料有很多種可能性，上述的論點都是假設使用者是不小心或故意寄出郵件，企業在事前與事後應該有的作為，但高銘鍾也提到，企業不該忽視另一種無意識的情況：萬一電腦被感染病毒，電腦內的資料一直被吐出去，洩露個資的可能性就大增。「企業在考量郵件可能存在的洩密風險時，更應強化對付風險入侵的部分，這樣才有可能會減低在無意識中洩露的風險。亦即在一般的功能之外，整合管理與資安防護，才能做到滴水不漏。」