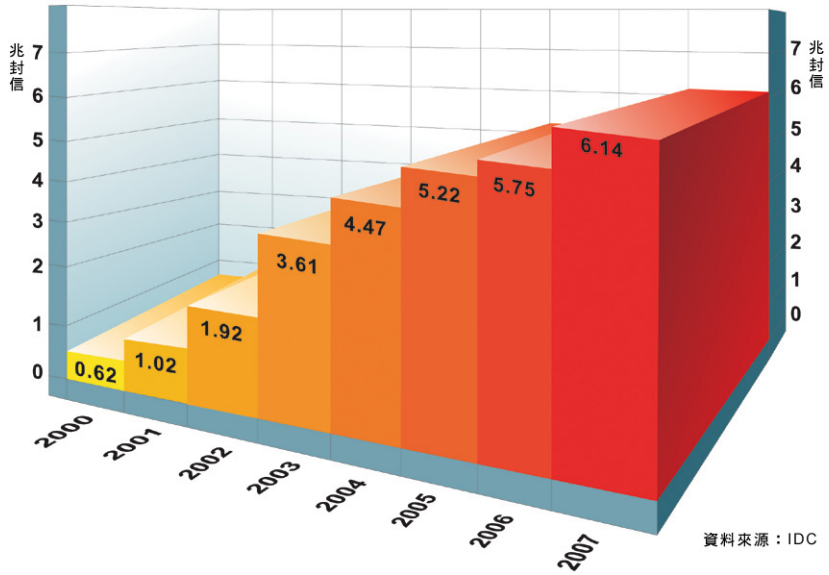
一場永無止盡的戰爭

反垃圾郵件市場的概況與技術解析

何謂「垃圾郵件」

「這些討厭的廣告信怎麼永遠都刪不完！」、「客戶剛剛跟我抱怨說沒辦法寄 email 到我的信箱，搞了半天原來是又被垃圾郵件塞爆了！」諸如此類的話語每天都發生在你我的周遭。隨著時代的演進，電子郵件已經成為許多人工作、生活中不可欠缺的一部份。但在享受電子郵件的便利的同時，垃圾郵件卻也在不知不覺當中地入侵到每一個人的電子郵件信箱裡。

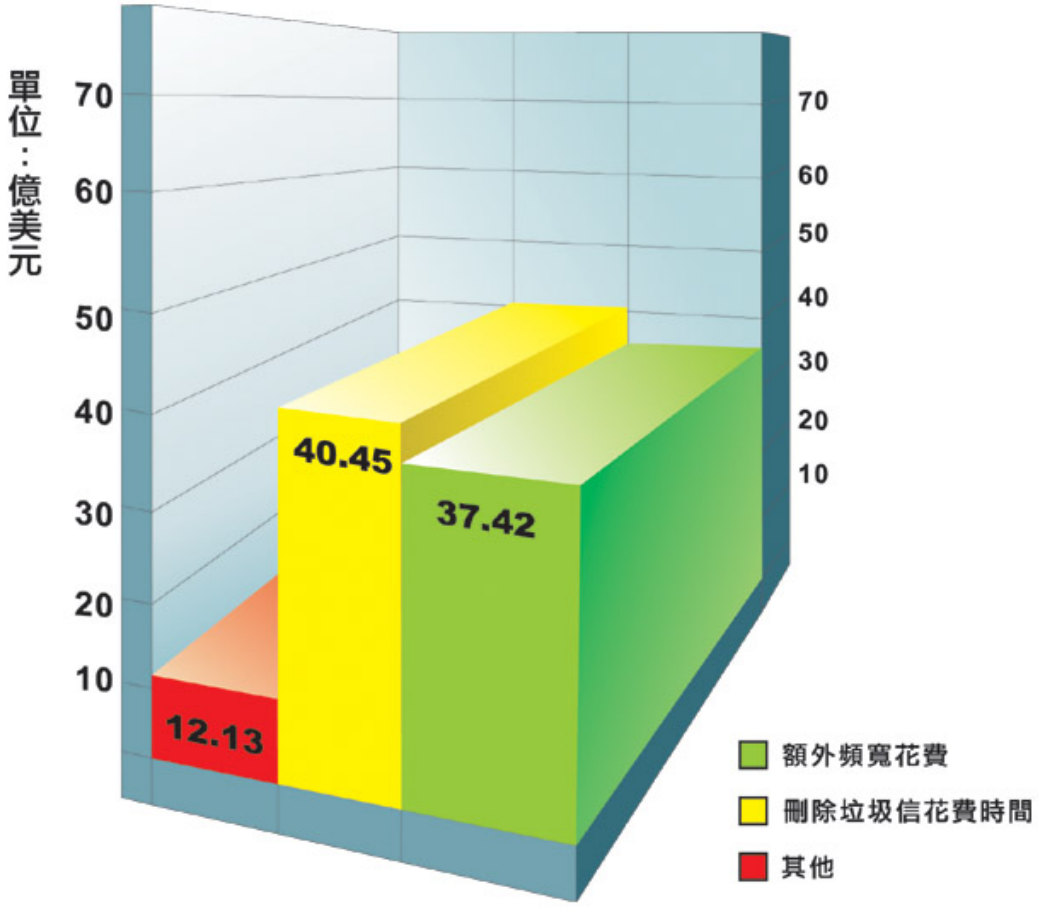
根據研調機構 IDC 公布的「2003 至 2007 年全球電子郵件使用預估：垃圾郵件與及時傳訊侵蝕電子郵件根基」報告，2003 年一整年全球送出的垃圾郵件就有 3 兆 6,100 億封，到 2007 年將會成長到 1.7 倍，達 6 兆 1,400 億封。



到底什麼是「垃圾郵件」呢？垃圾郵件指的是：「垃圾郵件是一種利用公眾網路傳送、不請自來的廣告資訊，包括電子郵件」。由於垃圾郵件通常是大量寄發，不但對收件人造成困擾，也會對 ISP 業者或公司郵件主機造成流量的負擔與經濟上的損失。

垃圾郵件為企業帶來可觀的損失

根據 Ferris Research 發布的一項研究報告估計，2002 年垃圾郵件造成美國企業損失八十九億美元，其中 40 億美元是因員工刪除垃圾郵件而造成生產力的減少，平均刪除 1 封垃圾郵件得花 4.4 秒；另外 37 億美元的花費，是為了因應超大量的資料流量，企業因而添購頻寬及性能更佳的伺服器；其餘的損失則是公司為降低員工因垃圾郵件產生的困擾，替員工提出的支援部份。



對於員工來說，每天都必須處理許多不請自來的垃圾郵件，不僅費心而且費時，並連帶造成工作效率的降低；對於企業來說，大量的垃圾郵件將會造成頻寬成本的大幅提昇，並造成生產力的損失。電子郵件安全服務商 Message Labs 分析該公司全球企業客戶傳送的 1 億 3,390 萬筆訊息後發現，2003 年 5 月份廣告郵件佔所有職員收件訊息的 51%，首度超過合法的郵件。市調公司 Gartner 預估，以一家 1 萬名員工的公司來說，內部產生的垃圾郵件便足以使公司損失相當於 1300 萬美元的生產力。若再加上來自網路的部分，損失更是可觀。

全球各國政府立法抑制垃圾郵件

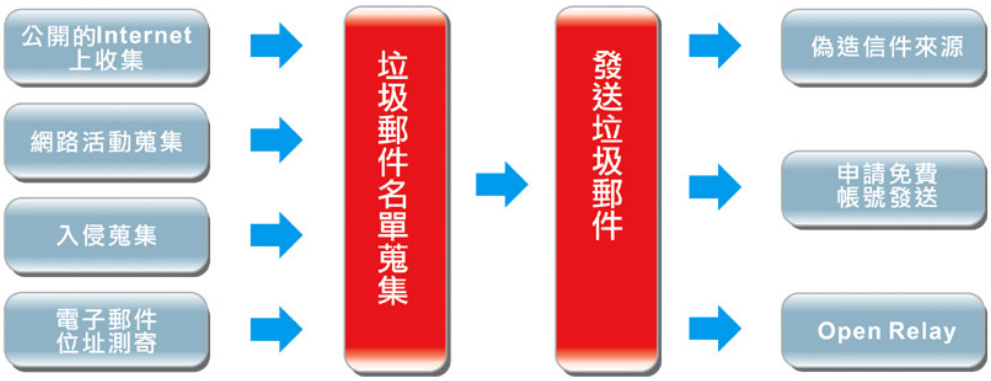
美國統計垃圾郵件已佔總郵件的 40%。美國聯邦政府、加州、佛州、英、澳洲及日、韓等國已相繼立法限制電子郵件的寄發量及標示方式。例如韓國規定廣告郵件寄件者，必須以「ADV（廣告）」字樣標示在郵件標題上，日本也要求廣告郵件提供收件者不再續訂的選擇機制等等。

相較之下，我國目前和電子郵件相關的只有刑法三百六十條，針對破壞 ISP 系統灌爆使用者信箱的行為處罰。不過該法條和駭客較相關，較無法管制垃圾郵件；另外就是刑法修正條文第三百五十二條第二項「規定凡干擾他人電磁紀錄之處理、足以損害於公眾或他人者，處三年以下有期徒刑、拘役或一萬元以下罰金」，但如何舉證垃圾郵件所帶來的損害，電子郵件散發如何確認為干擾，都很難認定。

中原大學財經法律教授周天指出，「電子郵件是跨國問題，單靠一國立法無法解決問題，跨國合作是較好辦法」但他指出，「跨國組織機構管理還牽涉到如何執行，以及管轄權的問題。」目前已有全球商業對話（Global Business Dialogue , GPD）等非營利組織開始聯合會員防範垃圾郵件。

垃圾郵件的發送

想要將垃圾郵件順利寄送到收件人的信箱，最基本的就必須完成兩個步驟： 取得有效的收件人名單→使用的免負責任的郵件伺服器寄送垃圾郵件。接下來我們就來談談垃圾郵件業者如何進行這兩個步驟。



1. 名單搜集：

A. 從公開的 Internet 上收集：

有許多人會將自己的電子信箱公布在網路上，有心人只要利用電子郵件收集軟體，就能夠收集到許多帳號。這種軟體的運作原理是不斷的瀏覽網頁，從網頁中抽取具有@符號的字串，這樣的字串通常就是電子郵件帳號。這樣的蒐集方式並不違法，也很難防制。根據美國聯邦貿易委員會 FTC 調查，蒐集他人電子郵件地址的最「熱門」的場所者為網路聊天室、新聞群組以及網頁。

B. 利用網路活動蒐集：

許多在網路上舉辦的會員註冊或是抽獎活動，使用者都必須先留下基本資料才能夠參與。有些垃圾郵件業者就利用這樣的方式蒐集有效的電子郵件帳號，販賣給有心人士或是自行寄送大量垃圾郵件。

C. 入侵蒐集：

透過網路入侵等方式，偷取其它站台的電子郵件帳號資料。

D. 直接產生電子郵件位址：

垃圾郵件業者直接選擇特定網域名稱，然後自動產生數百萬可能的地址，或是運用字典檔嘗試寄送，例如「Mary@yahoo.com.tw」、「book@yahoo.com.tw」等等。這樣的作法通常會造成大量的垃圾信流量寄進郵件伺服器，佔用企業很大的頻寬資源，甚至導致郵件伺服器故障。

2. 郵件發送

A. 偽造郵件來源：

垃圾郵件者常常會對垃圾郵件的來源進行偽造，使其更像來自正常的發送者。

B. 申請免費郵件帳號：

垃圾郵件業者會利用提供免費郵件服務的廠商，或經常「租借」不同 ISP 的網絡上的時間。它們一般掛到一個 ISP 的網絡上，發送數以百萬計的電子郵件後再撤走。

C. 使用 Open Relay 主機發送：

當一個郵件伺服器不管郵件寄件者和收件者是誰，而是對所有郵件進行轉發（relay），則該郵件伺服器就被稱為 Open Relay 的。 Open Relay 是存在一些舊版本郵件伺服器的安全缺陷，目前絕大多數郵件伺服器都已經具有關閉或限制 Open Relay 的功能。但是由於一些系統管理員的疏忽，仍

然還有很多舊郵件伺服器是 Open Relay 的，這樣就允許任何人通過該 SMTP 伺服器向任何地址發送垃圾郵件。

對抗垃圾郵件的技術

對於似乎永無止境的垃圾郵件，企業又該如何應對呢？一般來說，對抗垃圾郵件的技術可概為以下幾種：

1. 黑、白名單：

優點：簡單、攔截效率高

缺點：過濾效果不佳

這是市面上幾乎所有垃圾郵件廠商都有提供的功能。「黑名單」是指一個事先建立的郵件名單，凡是列入名單上的信件來源，將會被排除在郵件伺服器之外。目前在黑名單技術上最受重視的是 RBL（Real-time Blackhole List，即時黑名單）技術。通常該技術是通過 DNS 方式（查詢和區域傳輸）實現的。

即時黑名單實際上是一個可供查詢的 IP 地址列表，通過 DNS 的查詢方式來查找一個 IP 地址的記錄是否存在，來判斷其是否被列入了該即時黑名單中。

但是，當篩選排除名單的範圍日益擴大時，往往會將一些無辜的電子郵件一併當作垃圾郵件處理，於是又有了所謂「白名單」的出現。相較於黑名單列出的非法信件來源，白名單當中列出的則是合法的信件來源，某些功能完備的電子郵件軟體例如 Mail2000，也提供使用者自建黑、白名單的功能。

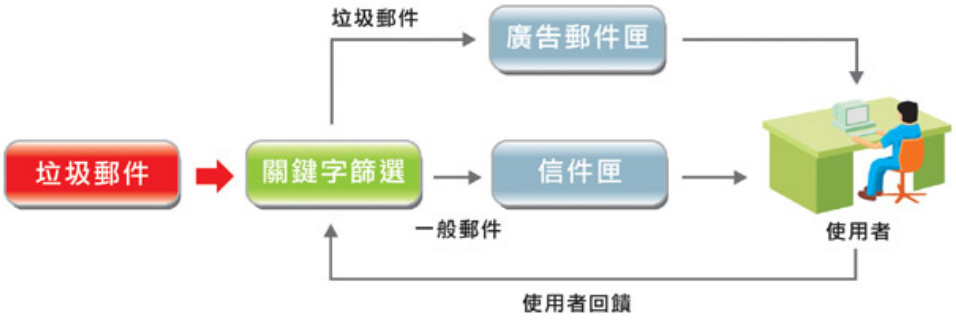
2. 關鍵字篩選：

優點：設定容易、攔截率高

缺點：後續維護不易、誤判率高

這也是目前市面上幾乎所有垃圾郵件防制廠商都有採用的一種方式。對於郵件特定內容的過濾以設定關鍵字的方式進行，只要出現這些字眼就一律進行攔阻。這是目前最常見的郵件過濾方式，例如凡是填有「色情」、「報表」等字眼，則一律攔阻，並通知管理者。這種方式在處理上比較簡單，並不會對原先的電子郵件遞送速度造成太大影響。

這種作法的缺點，就是管理者及使用者都必須在訂定規則上投入相當的時間精力，並且每隔一段時間就必須重新審視規則的適當性，才能維持垃圾信過濾的品質。另外，就是會有誤判的可能。因此一些軟體廠商，如 Mail2000 或微軟的作法就是另外設置另一信匣，例如廣告信匣，將系統判斷為垃圾郵件的信先集中放入此信件匣，待使用者確認後才刪除，以降低誤判的風險。

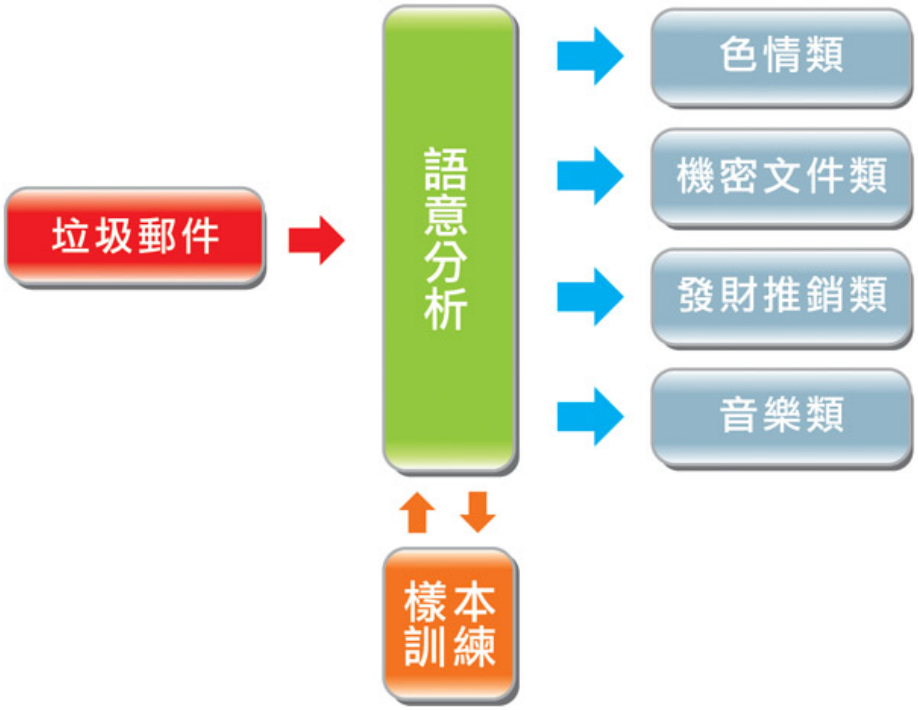


3. **自動語意分析**

優點：可針對特定種類的垃圾郵件進行攔截

缺點：精確性低，需輔助其他技術輔助，並需事先建立類型樣本。

企業可以預設幾種分析的結果類型，例如「機密文件類」、「色情類」或是「發財推銷類」等等。然後必須先提供足夠數量的各類型樣本，讓系統分析學習並建立模式，透過分析樣本的訓練，日後電子郵件過濾系統將會自動判斷。採用這類技術，企業可以設定多組不同過濾目標，並且誤判或漏失的機會較低。



像微軟的「SmartScreen Technology」機制，判斷追蹤標準是由數以萬計的 Hotmail 會員自願幫助分類合法郵件與垃圾信件，並累積至超過 50 萬筆垃圾郵件特徵可供追蹤比對。在這麼多的郵件樣本訓練之下，誤判的機率將會大為降低。

4. 各類的經驗法則

優點：簡單容易設定

缺點：攔阻率低、只能作為輔助

根據一些長期防制垃圾郵件的經驗，郵件服務商常常可以綜合出一些垃圾郵件或非垃圾郵件的共同特徵，例如：

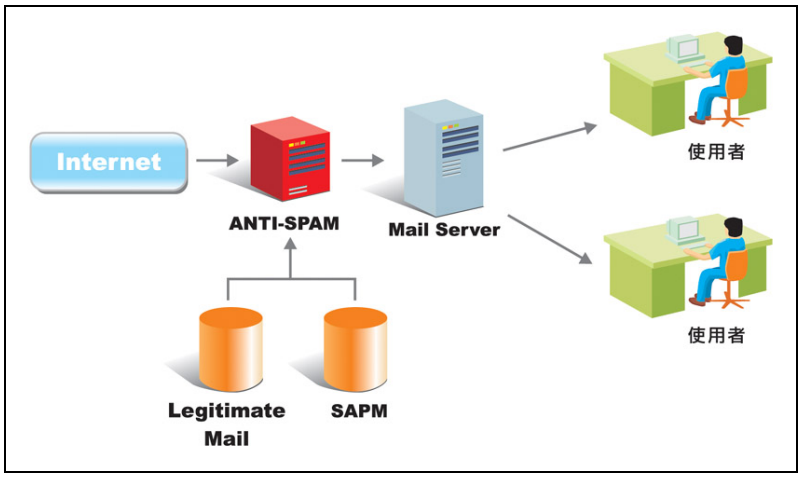
- **偽造寄件人：**
  SMTP 命令裡面的 Mail From（技術上稱為 Envelope From）和信件內裡面的 From 不一致，或寄件人的 email 不是真實存在的 email，就有很有可能是垃圾郵件。
- **信件大小：**
  垃圾信發送者因為要在最短時間發送最多郵件，所以會儘量降低每封信件的大小。所以一般來說當某封電子郵件的大小大於某個值的時候，通常是正常的信件。
- **信體內容帶有特殊的 HTML tag**
  為了嵌入更多的內容和 script，垃圾郵件往往會使用一些一般郵件不會使用的 HTML tag，如 iframe, frameset , object 等。
- **發送時間超過目前時間：**
  有些垃圾郵件為了在客戶端保持最前端的位置，會將發送時間強行修改到一個未來的時間，例如 2006 年 1 月 1 日。

5. 貝式分析過濾（Bayesian Filtering）

優點：攔截率高、誤判率低

缺點：系統必須預先接受訓練

Bayesian Filtering 是最近相當熱門的垃圾郵件防制技術，也有許多公司採用，其特徵是從信件中內含的文字作判定。一開始的時後系統會先準備兩組郵件樣本，一組是垃圾郵件另一組則是正常郵件，系統會先試著分析這兩組樣本中包含的文字，計算出各文字出現的比率。譬如「致富」在百分之八十的垃圾郵件中出現，而「請問」則只有出現在百分之五的垃圾郵件。



當收到電子郵件時，系統會找出十五到二十多個在兩組樣本郵件中出現頻率最高的文字，然後再運算評估這封信為垃圾郵件的可能性。由於 Bayesian Filtering 將非法與合法的郵件一同列入分析，因此能夠降低誤判的機率。

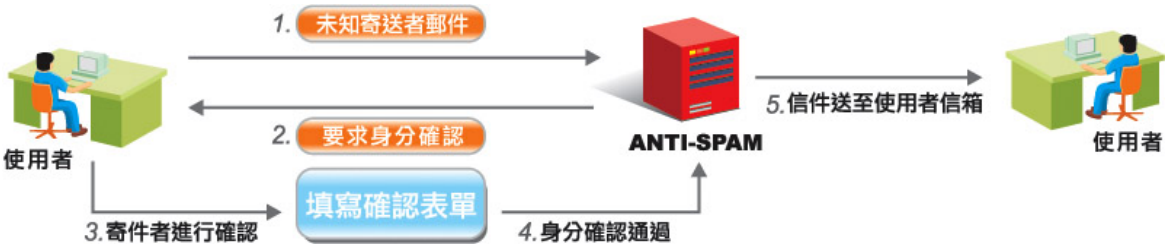
Bayesian Filtering 的效果相當優秀，不但攔截率高而且誤判率低，但在過濾夾雜正常內容的垃圾信時效果較差，而系統也必須事先加以訓練才能使用。

6. 許可清單過濾（Challenge-Response Filtering）

優點：攔截率高

缺點：對寄件者造成困擾、影響時效性

當使用者收到一封電子郵件，是來自從未接觸過的寄件人，系統會自動回覆一封電子郵件給寄件來源，請寄件人先至某一網址填寫表單，或是詢問收件人是否願意接收這封電子郵件，然後郵件才會被傳送到收件人信箱。



這種方式在台灣還未有廠商採用，但在美國卻已經有公司實際採用這項技術。實際使用的結果，確實是將收到的垃圾信大幅降低，但同時也提昇了收件人與寄件人的負擔。有時當寄件人不願進行確認的手續，使用者將無法接觸到某些潛在的重要郵件。當收到偽造寄件人的垃圾郵件時，也會帶來額外的困擾，甚至造成另一次的垃圾郵件干擾。

還有一個比較嚴重的問題就是時效性。假如寄件者寄出一封必須立刻處理的電子郵件給使用者之後就離開電腦，那麼他將無法進行後續的確認動作，而使用者也將無法及時獲得迫切的資訊。另外這種方式也經常搭配像是 HIP（Human Interactive Proof）的技術，以避免遭到自動確認的破解。

7. 定義碼比對過濾（Signature-Based Filtering）

優點：誤判率低

缺點：攔截率低

垃圾郵件防制廠商會利用一些偽造的電子郵件位址不斷收集各式各樣的垃圾郵件，然後持續綜合出一些特徵進行分析比對。當系統判斷某封電子郵件符合垃圾信的特徵，那麼這封郵件將會被排除在外

這種方式的優點是誤判率低，但相對應的卻是低攔截率。當發現到垃圾信件被攔截的時後，垃圾郵件發送者應對的手法則是將正常的文字夾雜在廣告當中。有時我們會在廣告信中看到一些無意義的字眼，就是發送者用來規避的手段，也造成這種過濾方式的效果不佳。

防制垃圾郵件的實際作法

在談了這麼多的垃圾郵件防制技術之後，接下來我們要討論的就是在實務面上的垃圾郵件防制作法，可分為三個方面來說，包括「ISP 以及網路業者端」、「企業郵件伺服器端」與「使用者端」三個部分。

1. ISP 及網路業者的防堵

- **新郵件信箱申請管制：**
  為了避免成為垃圾郵件的發送處，許多免費信箱服務廠商紛紛更新了帳號申請的流程，不讓垃圾郵件業者利用程式自動產生大量帳號。例如微軟的 HIP（Human Interactive Proof）技術要求使用者在申請帳號時，必須手動輸入隨機產生的文字，使得業者無法使用程式或其他自動機制設定帳號；雅虎奇摩也於去年開始，要求郵件帳號申請者填上身份證字號及大哥大號碼等資料，以強化掌控。

- **現有信箱控管：**
  針對可能成為垃圾郵件來源的信箱加以管制。例如 Mail2000 與 Hotmail 都限制用戶每次最多只能發出 100 封郵件等等。

- **排除垃圾信件來源：**
  除了採用黑、白名單的方式之外，並針對有異常發送郵件行為的特定 IP 來源，暫時強制關閉其送信功能。例如 So-net 當會員三十分鐘內發信超過九百封、或十分鐘內連線次數超過兩百次等就會限制該網路位置寄信一個小時；雅虎奇摩將一日發信超過 500 封信以上的 IP 視為垃圾郵件來源，並攔截此 IP 之後發出的信件；Hinet 若發現垃圾郵件濫發者，則暫時攔阻所有 IP 網段的發信功能，直到事件處理完成，並對濫發者採取停用處份。

- **設置廣告信件申訴信箱**
  為了更精確地判斷垃圾郵件，一些郵件服務廠商向使用者提供了廣告信件申訴信箱，由使用者自行判斷怎樣的信件屬於「不請自來」，再從這樣的互動模式當中建立垃圾郵件判斷模式。例如 Mail2000 的使用者在收

到垃圾信件的時候，就可以直接點選「檢舉廣告信」向系統申訴，系統會根據在一段時間內的同性質或同來源的信件數量，自動將符合的信件來源列入黑名單；而微軟的「SmartScreen Technology」機制，就是建立在判數以萬計的 Hotmail 會員自願幫助分類合法郵件與垃圾信件之上，並累積至超過 50 萬筆垃圾郵件特徵可供追蹤比對。

- **拋棄式信箱**

  這是雅虎奇摩最近採取的新作法。所謂可拋式的郵件地址，就是使用者可在一個長期有效的郵件地址上，自行訂定一個變化的帳號名稱以及郵件的使用期限，過了期限後，這個經個人變化過的郵址就不再有效，垃圾郵件就會減少。可拋式郵件可使用的場合包括，有必要填郵件地址、卻不想讓對方長期騷擾，以及只需要短期內聯絡等情況。

- **網域金鑰比對**

  這是 Yahoo 在 2004 年 1 月提出的概念，預計在 2005 年開始實施。「網域金鑰」軟體從金鑰認證著手，發信端與收信端均需安裝，它讓發信系統在發出的郵件訊頭中內建一副私密金鑰，收信系統則以發信系統在網域名稱系統（DNS）登錄的公共金鑰來解密，如果能夠解開，這封電郵就被視為經過授權，送達用戶；如果解不開，這封電郵就是來路不明，會被伺服器阻擋過濾。

2. 郵件伺服器端的垃圾信防制

- **購買郵件過濾軟體**

  現在市面上有許多廠商都有提供這樣的產品，按照產品形式來分，可分為核心或閘道整合的方式。功能從垃圾郵件過濾、郵件稽核到郵件防毒等等都有，系統管理者可以考量不同產品形式、不同技術的優缺點，再配合企業本身的資訊安全政策、現有環境與網路架構、郵件流量等問題，審慎地進行評估。

- **禁止 Mail Rely**

  若企業使用的是微軟的 Windows NT、 Windows 2000、Windows XP 或以上的作業系統時，當安裝了 IIS（Internet Information Services）服務，並啟動了 SMTP Service (外寄伺服器服務)，此時若網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔，那麼任何人都可以藉由系統的 SMTP Service 寄發信件！此時企業的 Mail Server 就有可能被有心人士當成廣告信跳板，濫寄廣告信件。

- **設置垃圾信匣**

  系統會自動辨識可能為垃圾郵件的信件，再配合使用者自訂的黑、白名單，將系統認定為垃圾郵件的信件放入特定的垃圾信匣當中，使用者再自行瀏覽或刪除，這樣可以提升使用者處理的效率，也避免系統誤將重要郵件直接刪除的情形發生。像 Mail2000 或 Exchange 2003 ＋ Outlook 2003 都有具備類似的功能。

- **禁止外部連結**

  一些垃圾郵件業者會大量發送測寄信件，在信件當中會有所謂「網路信標 (Web beacon)」影像，在收件者開啟郵件時回傳訊息至發信端，讓業者確定此電子郵件帳號為有效的。 Exchange 2003 為防止部分垃圾郵件業者透過，於是讓使用者可以在審視過郵件內容之後，再選擇開啟不明郵件的影像檔案。

3. 使用者端的垃圾郵件防制：

- **自訂過濾規則**

  例如 Mail2000 可以讓使用者可以針對特定的信件欄位，像寄件人、主旨、信件大小等等，再選擇符合條件郵件的處理方式。例如：
  如果「主旨」「包含」「廣告」，則「刪除信件」
  如果「寄件人」「等於」「網擎資訊」，則「放入重要信件匣」
  而 Outlook 或 Outlook Express 也提供使用者類似的過濾功能。

如果	標題 寄件人 收件人 副本 信件大小 來源主機 附檔名稱 附檔大小	等於 包含 不包含 開頭是 結尾是	關鍵字	則	轉寄 刪除 放入指定信件匣 簡訊通知

《Mail2000 的過濾規則設定》

- **自訂黑、白名單**

  與之前提到 ISP 訂定的黑、白名單方法類似，只是讓單一使用者自行決定信件來源是否為垃圾信件。例如 Mail2000 提供使用者自行建立「合法收、寄件人」以及排外名單的功能，再配合廣告信件匣搭配使用，就可以排除相當程度的垃圾郵件騷擾，而微軟的 Exchange 2003 ＋ Outlook 2003 也擁有類似的功能。

- **慎用自動回覆功能：**

  許多郵件服務提供商提供了很方便的「自動回復」的功能，但鑒於垃圾郵件問題的日益嚴重，在使用上應該更加謹慎小心。因為許多垃圾郵件程序都利用了這一功能，在隨機測寄過程中，會有目的地搜索收集自動回復郵件的有效地址，然後建立用戶列表，以便進一步騷擾用戶。

- **對於在網路上的個人資料更謹慎：**

  不隨便在公開的網路上留下自己的電子郵件位址，在填寫一些網站註冊的資料時要特別注意，要勾選不要洩漏 email 給別家廠商的選項，並且避免訂閱一些不熟悉的網站電子報。

- **使用多重 email 帳號：**

  在不熟悉的網站註冊時，最好使用無關緊要的電子郵件帳號。

垃圾郵件過濾—評選指標

1. 易安裝、導入，對網路配置影響低
   能夠快速導入原有的資訊系統，與運行中的郵件系統整合，讓對企業造成的影響降到最低。
2. 易管理，不需大量人為設定
   良好的反垃圾郵件系統應該擁有友善的 Web 介面，方便系統管理員操作管理，減輕管理人員的負擔。
3. 多層次過濾功能
   沒有一種垃圾郵件過濾技術可以一勞永逸的解決所有問題，因此好的反垃圾郵件系統最好能結合多種過濾技術，如此才能將垃圾郵件帶來的困擾大幅降低。
4. 攔阻率高，誤判率極低
   除了高攔阻率之外還必須附加的是低誤判率。如果只著眼在根除垃圾郵件卻誤刪了重要信件，想必是得不償失。
5. 高效能，避免造成信件延遲
   在將垃圾郵件攔阻的同時亦能讓郵件系統維持高效能運作，這才是真正優良的反垃圾郵件系統。
6. 個人化垃圾郵件管理/回饋功能
   垃圾郵件是非常主觀的，因此如何將使用者的回饋納入系統的運作是非常重要的。
7. 即時更新（filter engine/pattern）
   垃圾郵件發送者的手法層出不窮，因此能否隨時應變發展出對應的技巧，也是反垃圾郵件系統的考量重點。
8. 成本

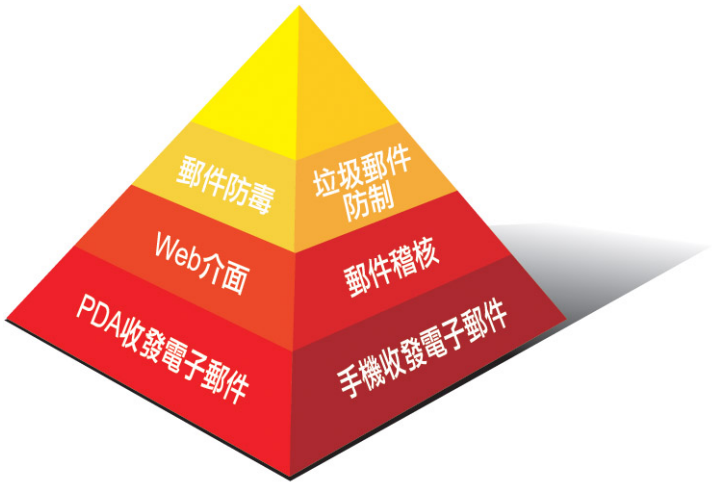
過濾技術面臨的挑戰

Osterman Research 在 2003 年底的一份研究顯示，只有 25%的使用者對他們的垃圾過濾產品的判斷能力表示滿意。垃圾郵件雖然煩人，但與無法收發電子郵件所帶來的影響相比之下，大部分的使用者還是選擇忍受。畢竟對使用者來說，垃圾信的定義都因人而異，因此很難訂定出一定的準則。在沒有找到提高準確率的有效辦法之前，與其在嚴格的過濾條件之下誤將重要信件刪除，一般企業還是寧願選擇遵循一些通用的部署準則，來減少可能被垃圾郵件過濾軟體誤判的合法電子郵件數量。

垃圾郵件防制的未來趨勢

雖然垃圾郵件防制已經是國內外資訊安全的熱門話題，但是賽門鐵克技術長 Robert Clyde 卻認為，這塊市場將在三年內崩解。Robert Clyde 指出，反垃圾郵件最終應該併到更廣泛的內容管理範圍中，而不再會是獨立的議題。

垃圾郵件對企業、個人帶來的影響已經是不容置疑。在企業倚賴電子郵件的程度日益增加，在享受到電子郵件帶來的便利的同時，當然也免不了要面對電子郵件帶來的負面影響，像是病毒郵件、垃圾郵件、機密資料外洩等等問題。在成本與效能的考量之下，企業不可能將各個問題分開獨立解決，因此垃圾郵件防制的功能必定會跟其他郵件軟體整合，成為企業電子郵件系統整體解決方案的一環。



電子郵件系統整體解決方案

結語

防制垃圾郵件絕非一蹴可及，必須要從技術到立法，如精進的技術、產業自我規範、消費者教育和有效的立法及給予非法垃圾信件業者加以處罰，以及從伺服器端到使用者端的相互配合，才能有效的抑制垃圾郵件繼續氾濫。就企業管理者的角度來說，企業必須根據公司內部的情況，慎選合適的垃圾郵件產品，並且不斷的完善過濾規則和判斷方法；就使用者而言，除了不隨便在公開網路上洩漏郵件位址之外，更必須與系統管理員配合，將垃圾信的判別回饋到伺服器端。也唯有在雙方面的攜手配合之下，才能夠將垃圾郵件造成的損失降到最低。