ShareTech垃圾郵件過濾解決方案

電子郵件是成為現在人資訊溝通的主流，不僅具有跨國界、高效率的特性，而且所耗成本低。但是目前垃圾郵件已成為許多企業的共同議題，因為垃圾郵件平均來說已經占總郵件量一半以上，有些垃圾郵件量甚至高達 95% 以上，不僅耗費郵件主機儲存的空間，甚至再有些郵件中還會摻雜一些有害的釣魚網站，目的就是要讓使用者在不注意的時候啟動，造成個人機密資料的外洩。

目前市面的垃圾過濾產品大致上有軟體、硬體設備之分，而採用軟體的好處是可以自己組裝硬體，將效能提升至最高。但是軟體的安裝對大多數企業來說總是麻煩的，因為不僅耗時且需要專業人士維護，而且還須擔心軟體系統與硬體設備是否相容，且維護是否方便妥善。而硬體設備對企業建置來說，方便快速，而且在後續維護上更容易，眾至資訊目前在郵件過濾硬體設備方面提供郵件郵件過濾器設備。

眾至將許多垃圾郵件過濾機制導入到 MS 郵件伺服器，其中包括垃圾郵件過濾機制、快速 ST-PTC 多維圖形辨識技術，垃圾信學習過濾機制、個人黑白名單過濾機制、指紋辨識過濾、貝氏學習過濾、垃圾郵件特徵過濾、灰名單過濾等，使得垃圾郵件辨識的比率可高達，協助企業避免垃圾郵件問題日益增加。

台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

台北分公司 02-2501-1185
台北市中山區松江路129號6F-2

高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

免付費專線 0800-666-188
官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

垃圾郵件過濾機制

過濾的條件可以依照郵件分數、寄件者、寄件者 IP、收件者、檔案大小、郵件內容、主旨...來過濾信件，並可設定垃圾郵件的處理方式包含送至隔離區保留、直接刪除、不做垃圾信過濾等動作。 (圖一)

在垃圾郵件過濾部份，完全是由管理者操作設定，並非像是過濾引擎的自動分析方式，因此郵件內容過濾功能也可以用來做稽核。管理者也可以做進階管制，例如：抄送副本或通知信的功能。假設某個員工寄出的信件或收取的信件是必須傳送給她的主管，管理者可以設定該員工寄收的信件都會自動拷貝一份給她的主管。

過濾器條件的運作	設定
過濾條件組合方式	設定的條件(欄位)皆須符合(AND) ▼
*寄件者包含	本機網域 不包含
寄件者偽造本機網域	
*收件者包含	本機網域 不包含 所有收件者符合
寄件者來源 IP 位址包含	Ipv4 Ipv6 不包含
郵件表頭包含	不包含
*郵件主旨包含	不包含
*郵件內容包含	不包含
郵件容量大於	K bytes
*郵件附件檔名包含	不包含

圖一：垃圾郵件過濾機制

貝氏學習過濾

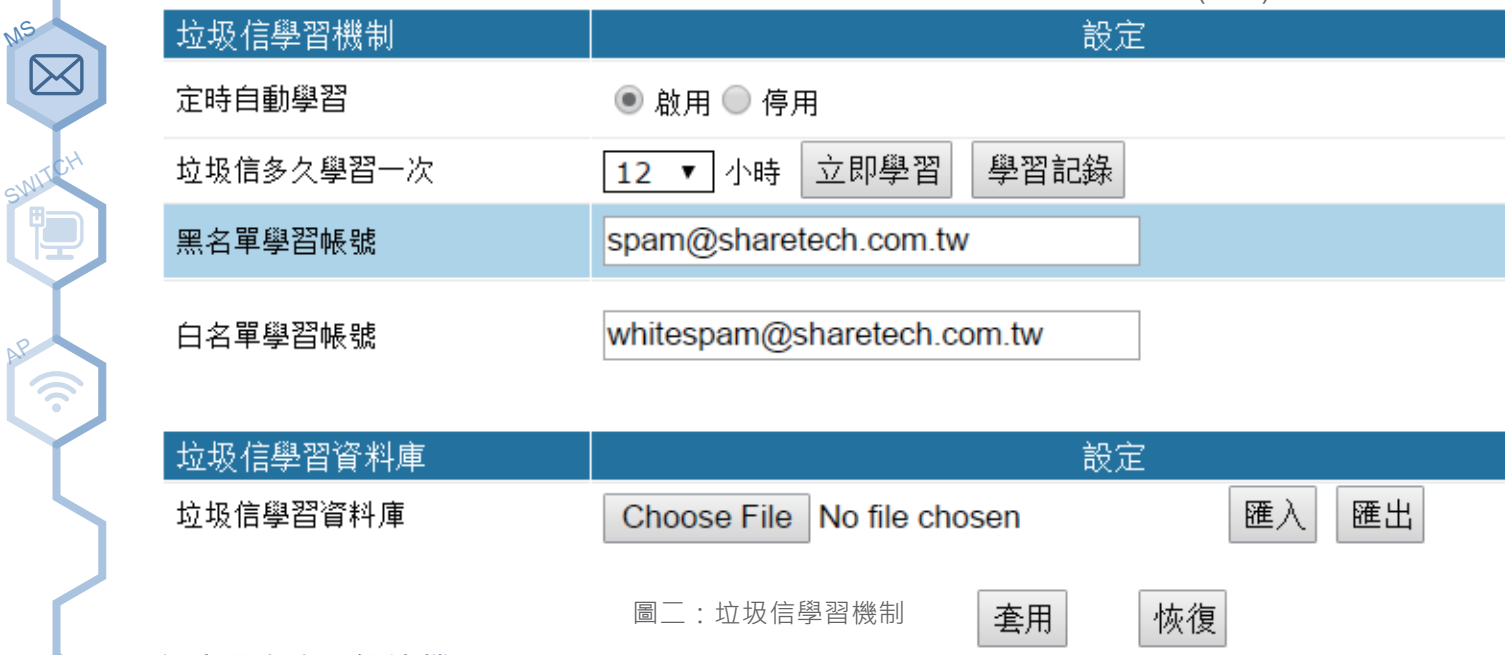
貝氏過濾法是將信件之內文以貝氏資料庫之規則來評分，分數越高者其越有可能是垃圾信件。一般來說「貝氏過濾法」會有個資料庫，當一封信件進入系統的時候會把信件分解成單詞，比對目前「貝氏過濾法資料庫」，分析以往的經驗，來判別此封信件為垃圾信件的機率，且貝氏過濾資料庫具有自動學習的功能，可以依照不同企業收信的狀態來調整最適合的過濾條件。

指紋辨識過濾

所有進入郵件閘道的信件都會以特殊的方式處理，將信件以特殊的方案轉換成為一指紋碼，在跟網路上的資料庫做比對，如果特徵相符合就歸為垃圾信件。由於資料庫是長期累積而來，當一封郵件在經過比對後被歸為垃圾信件時，資料庫就會存在該封信件的指紋碼。

垃圾信學習過濾機制

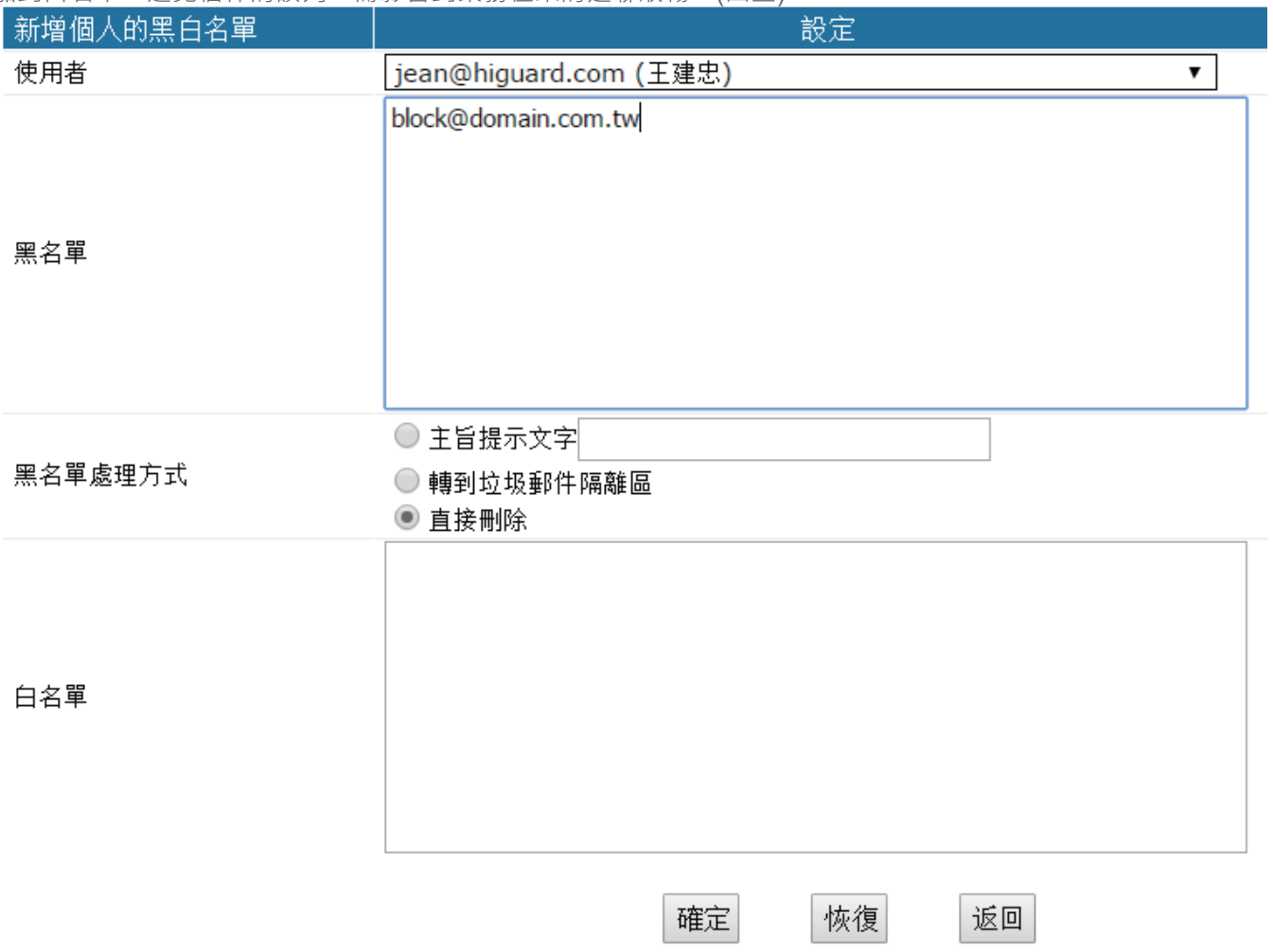
ShareTech 郵件伺服器對於增加垃圾郵件判斷率的作法是使用學習機制，垃圾郵件的掃描引擎中有一個學習資料庫，它的設定方式就是設計 2 個郵件帳號，黑名單學習帳號、白名單學習帳號，一旦使用者認為他的郵件被郵件伺服器誤判，則可以將被誤判的信件寄到黑名單學習帳號或白名單學習帳號，下一次同一位寄件者寄來的信件，就不會被誤判，但是在學習的時候必須以單封信轉寄學習，不能以群組夾檔轉寄學習。(圖二)



圖二：垃圾信學習機制

個人黑白名單過濾機制

由於每個人對於垃圾郵件的定義不同，為了避免企業員工的報怨，眾至都會定時寄發通知信，告知目前使用者隔離區內的郵件，如果有誤判還可以自行取回，另外使用者還可以設置黑白名單，可以先將平常有在連絡的客戶先加到白名單，避免信件的誤判，而影響到業務往來的通聯順暢。(圖三)



圖三：個人黑白名單過濾機制

UTM

MS

SWITCH

AP

垃圾郵件特徵過濾

由於垃圾郵件發送的特徵不斷的在做改變，眾至除了透過使用者定時回報，持續不斷累積「過濾經驗」，經由特徵採樣、資料庫更新速度和自動學習的能力提高設備過濾的及時性與效率。

灰名單過濾

灰名單過濾功能只要是過濾垃圾郵件行為，一般來說廣告業者在第一次發送廣告信件時，如果收件者拒收，就不會再發送第二次，而灰名單過濾主要就是發揮這種特性，對於第一次陌生寄送的帳號都拒收。

正常的郵件主機，在信件第一次發送失敗時，會在傳送第二次、第三次，則灰名單過濾機制在正常郵件第二次寄送時就會收下信件，往後此寄件者的來信都不會做阻擋，除非使用者有將它列入黑名單或其他判別條件中。

IP 位址反解驗證

ShareTech 郵件伺服器收到外部寄件者，去驗證該帳號的來源 IP 位址是否有做 IP 反解，如果沒有，則按照「未通過驗證處理方式」設定方式處理該封郵件是否要直接刪除或者轉到垃圾郵件隔離區，系統並會同時發送清單。

SPF 驗證

「SPF 驗證」，可驗證電子郵件的來源網域名稱，有助於防止「詐騙」和「網路釣魚」。會根據宣稱為傳送網域的擁有者來驗證寄件者的 IP 位址，以驗證電子郵件訊息的原始位置已確認該帳號的來源是否 SPF 合法。

舉例來說：常常媒體新聞報導詐騙事件，假藉是司法人員打電話或寄存證信函給你，進行金錢的勒索。在過程中利用假以亂真的資料或台詞取得你的信任。而同樣的事情在網路上也一再的發生：盜用別人的信箱進行詐騙行為，除了避免讓信件退回自己的信箱外；也避免曝光自己的行蹤；或是帳號密碼盜賊假裝成好友的來信竊取私人機密...等等不勝枚舉。

DKIM 驗證

由於 SMTP 規範的一些小漏洞(讓有機人可趁)，寄件人的 Mail Address 和實際寄信的 Mail Server 是可以不一樣的。就像您可以從台中寄信，但是寄件人的地址卻可以填寫台北的地址一樣。雖然可以憑郵戳追蹤是由哪個地區寄出的，但是多數的使用者並不會去注意這細節。

同樣的，雖然郵件系統也會在每一封寄出的信件加註郵件主機等相關資料，但是一般的使用者在收取信件時並不會特別注意這些事項。產生的問題就是您可能會收到假冒你的 Mail Address 透過你公司的 Mail Server 寄給你自己，或透過其他 Mail Server 寄給其他公司。

DKIM 的目的就是用來防止垃圾郵件製造者偽造您網域的寄件者來傳送郵件。 DKIM 使用簽章的方式，在外寄郵件的郵件標頭加上一個數位簽章，收件者只要檢查郵件中是否包含這個網域簽名，即可確認該郵件的寄件者地址確實屬於您網域中的地址，而且未在寄件途中遭到竄改。