電子郵件安全指引 - 電子郵件過濾機制篇

自從電子郵件開始大量的出現廣告信件以及釣魚信件後，防範這些信件入侵我們的信箱已成了所有郵件系統最重要的功能之一，長年以來，面對不斷進化的廣告信件以及釣魚信件，發展出許多種電子郵件過濾的機制，本期將針對較常見的電子郵件過濾技術進行介紹。

RBL 黑名單資料庫

RBL（Real-Time Black List）指的是由某些資訊安全組織或公司建立的龐大線上黑名單資料庫，包含各種可疑 IP 位址、電子郵件地址，以及未註冊的 DNS 網域名稱，並提供使用者下載更新這些黑名單資料，並利用黑名單資料來進行郵件過濾。

MailGates - *RBL 黑名單資料庫介紹*

MailGates 郵件防護系統提供三個 RBL 資料庫供使用者選用，勾選後郵件伺服器便會即時下載更新這些 RBL 資料庫來做為判斷垃圾郵件的依據。

MailGates 黑名單資料庫

SPF 防偽技術

SPF（Sender Policy Framework）是一種防止偽造郵件地址的防偽技術，透過標示本身網域中的合法發送 IP 位置，讓其它收件端收到信件時，根據送信端宣稱的寄送網域，查詢該合法寄信的 IP 位置，透過比對信中的來源 IP 來判斷該信件的真偽。

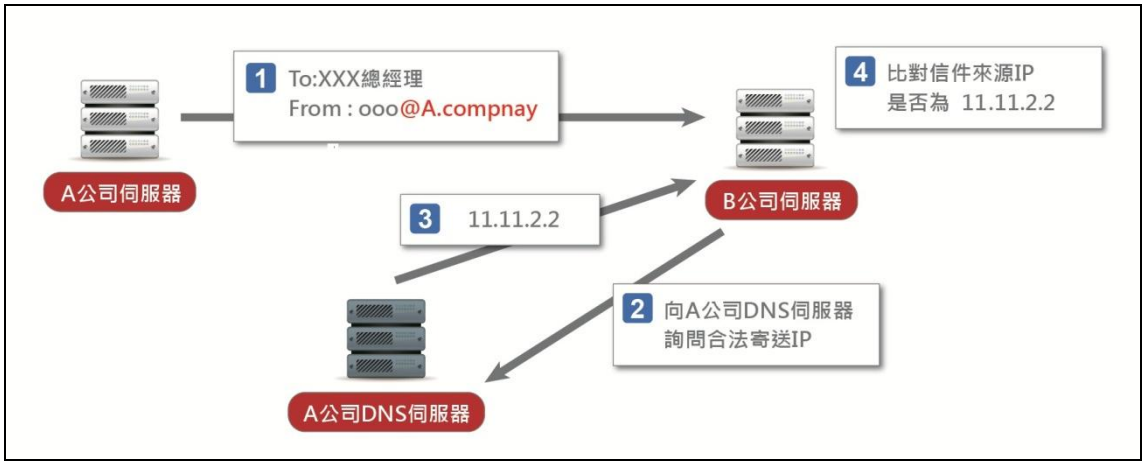
SPF 防偽運作流程說明如下：

(1) B 公司收到 A 公司的來信。

(2) B 公司根據信件中來信的網域名稱(A)，向 A 公司的 DNS 伺服器詢問合法寄信的 IP 位置。

(3) A 公司的 DNS 伺服器回覆只允許由 11.11.2.2 寄信。

(4) B 公司判斷信件中來源的 IP 的確是 11.11.2.2 便將信件收下。



SPF 示意圖

網域認證金鑰

網域認證金鑰（DomainKeys）運用加密及簽章方式來認證信件的來源。原理是送件端寄出的信件，會先用自身的私密金鑰做簽章，收件端收到信件後，根據信件所標示網域，向 DNS 伺服器取得公開金鑰，並進行驗章的動作。

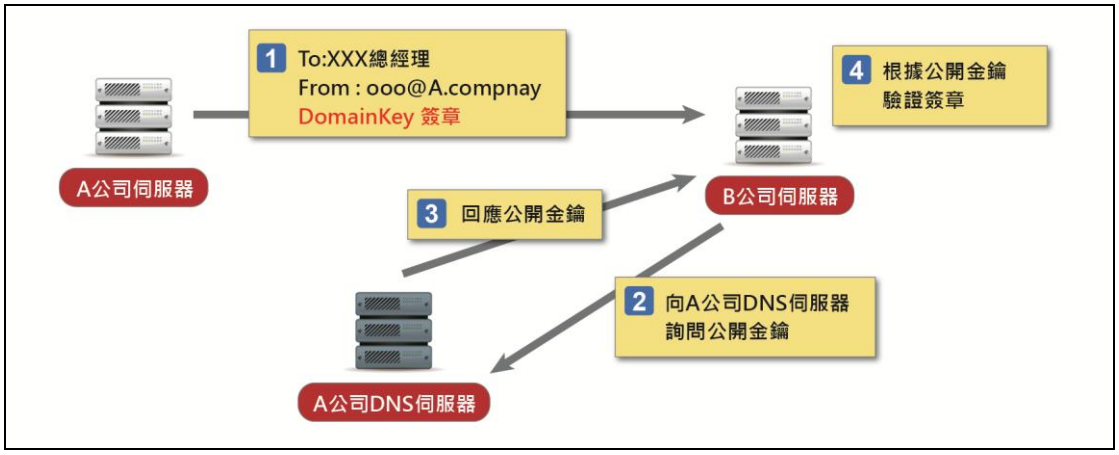
網路認證金鑰（DomainKeys）運作流程說明：

(1) 送信端發送一封經過私密金鑰簽章的信件，並在信件標題中宣告網域。

(2) 收信端根據信件標題中宣告網域，向 A 公司 DNS 伺服器取得公開金鑰。

(3) 該網域回傳公開金鑰。

(4) 利用公開金鑰對信件中的簽章進行驗證。



DomainKeys 示意圖

MailGates - *網路認證金鑰介紹*

MailGates 系統中可選擇使用***網路認證金鑰***（DomainKeys）功能，輸入基本的***網路認證金鑰***（DomainKeys）基本資料後便可快速啟用此認證機制。

MailGates DomainKeys 設定畫面(1)

MailGates DomainKeys 設定畫面(2)

MailGates DomainKeys 設定畫面(3)

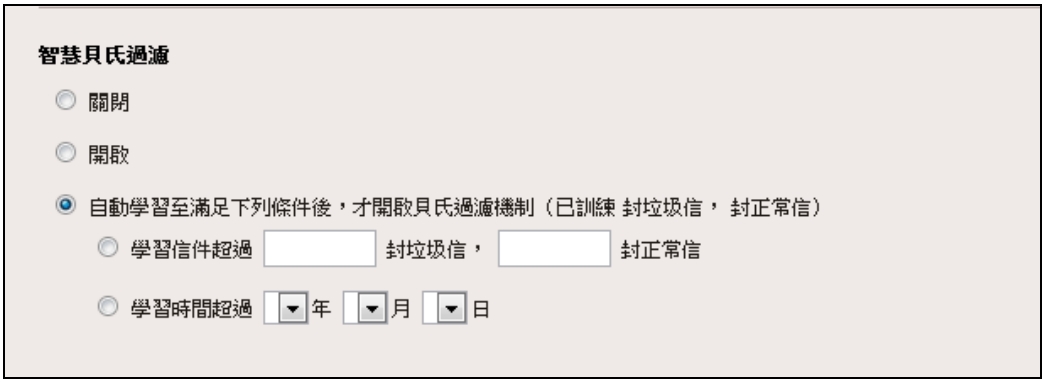
貝氏過濾法

垃圾信件過濾技術中，貝氏過濾法（Bayesian filtering）可說是最被廣泛討論且應用的技術之一，它是根據貝氏定理的事前機率與事後機率所發展出來的垃圾信過濾規則。

貝氏過濾法和人類經驗法則很相似，經驗法則告訴我們「全裸」、「學生妹」、「視訊聊天」等詞彙九成九都是垃圾信件，因此我們一看到這些詞彙的時候我們就會判斷它是垃圾信件。貝氏過濾法也是如此，只是它的判斷是根據了統計學的基礎，把垃圾信和正常信當作統計樣本，將樣本分解成一個一個單詞然後交叉判斷，算出某詞彙出現時信件為垃圾信件的機率，所以只要投入分析的信件量越大，此演算法的準確度就越高，貝氏過濾法也因擁有這不斷學習的優異能力成為目前垃圾信件阻擋的最主要工具。

MailGates - *智慧貝氏過濾介紹*

MailGates 可彈性選擇是否開啟貝氏過濾功能，還可讓使用者設定當學習信件超過特定數量後才開啟過濾機制。



MailGates 貝氏過濾功能

關鍵字過濾

關鍵字過濾是針對信件標題或內文中的特定字樣進行過濾，例如將信件內文包含「視訊聊天」設為過濾條件，當系統收到內文包含「視訊聊天」的信件，就會將此信件丟到垃圾桶或是廣告信件匣中。

Mail2000 關鍵字過濾設定畫面

看完了這一期電子報，大家是不是對於電子郵件過濾的技術有了更多的認識呢？下期電子報我們將會繼續說明，有關電子郵件系統的防護重點介紹。