

郵件歸檔方案大直擊（上） 個資法總動員 從郵件歸檔做起

作/曹乙帆



“當前不論來自於外部或內部的安全威脅與攻擊，其發起的動機及瞄準的目標，不再是過去單純的報復、破壞或獲取名聲，而早已轉變成金錢利益。而能讓攻擊者獲取金錢利益的，莫過於機密資料的竊取，也因為如此，個資外洩事件遂不斷發生，並成為近年來最讓人頭痛不已的嚴重問題”

再加上當前資料外洩的管道實在多不勝數，從傳統的電子郵件、即時通訊、P2P到Youtube、Flash、社交網站等各種Web 2.0應用，使得資料外洩的防護戰線實在太廣太長，企業必須耗費更多的人力、時間及成本來降低可能的風險。隨著新版個資法即將通過，企業勢必儘早做好相關的安全防護措施。由於防護的面向實在太多，企業不太可能有充裕的能力、時間及預算做到面面俱到的程度，所以唯有透過漸近式做法才能逐步讓整個資料外洩的基礎建設及防護層面更加完善。

儘管Web2.0當道，但電子郵件對企業乃至駭客而言都是最重要的溝通與攻擊管道之一。尤其企業在商務溝通上，電子郵件遠比即時通訊、視訊會議或Facebook等社交網路都來得重要，所以對該應用的

依賴程度自然不在話下。也因為如此，長久下來電子郵件（可能包含各種影音夾檔）所累積衍生的資料量之大，也一直居企業內部各種資料之冠。在巨量的電子郵件中可能不乏垃圾郵件，也可能充斥著許多機密與個資，所以企業絕對必須具備良好的安全過濾、保護及保存機制來處理不斷激增的電子郵件。

也因為如此，在個資外洩與個資法防護的因應上，電子郵件絕對會是第一優先的導入重點。換言之，企業不妨先從電子郵件相關安全機制的導入，伴隨觀念宣導、人員教育、安全流程建置與安全政策的擬定開始，然後再逐步強化其它可能外洩管道與面向的防護工作。事實上，大部分的企業莫不早已投入許多垃圾郵件過濾與郵件防毒等安全機制的建置工作。唯獨缺乏的，是完善郵件備份及歸檔機制的落實，

相信這會是接下來企業因應個資法防護，尤其是訴訟舉證上非做不可的重點工作。

郵件歸檔因應個資法之最佳化細節及要點

在安全防護上，通常會有所謂的前稽與後稽機制，其中資料外洩防護(DLP)方案即屬於前稽核，郵件歸檔則被視為後稽核方案。網擎資訊軟體研發協理葉慶章表示，在因應個資法之法規遵循需求上，郵件歸檔可以發揮郵件機敏內容的探勘，在對郵件備份中充份掌握到可能機密與個資的分佈狀況後，便可對管理者發出安全預警。企業一方面可以對這些資料善盡保護之責，同時也可在日後提升法規舉證的能力與速度。

葉慶章認為，郵件歸檔針對個資法的最佳化重點不外個資盤點的落

實，如此一來便如同證明自己有善盡個資保護之責，同時也能讓管理者能在法規所規定的時效內快速回應使用者請求瀏覽的需求。中華數位產品暨市場營運中心產品經理王智衛提醒表示，企業透過郵件歸檔因應個資法會有幾個要特別注意的重點：亦即舉證能力、舉證資料完備度、舉證速度、專責人員及免責聲明等。

首先，在舉證能力及善盡保護之責上，由於個資法第29條規定：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」換言之，企業必須盡可能收集資料以證明自己並無任何故意或過失。面對經年累月的巨量電子郵件，企業必須要有良好的郵件備份策略及緊急調閱機制，如此才能在未來所可能面臨的法規訴訟時，能立即準備好證明自己無

故意或過失，以及確實有善盡保護之責的證明。如今的郵件歸檔方案，便可協助企業建立郵件資料方面的完善舉證能力。

再者，由於個資法第30條規定：「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」換言之，個資受害者可以向企業追溯2至5年前的個資外洩責任，所以企業必須具備快速提供5年內郵件資料的能力以為因應，所以企業重要郵件至少都必須保存5年才行。對此，王智衛剖析道，企業可以透過郵件生命週期管理(ELM)機制的導入，即可確保郵件保存期限以化解個資賠償請求追溯權的可能風險。

再就舉證速度來說，個資法第13條規定：「公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得

逾十五日，並應將其原因以書面通知請求人。」換言之，因應個資訴訟，企業最多只有30天的舉證資料準備時間。企業如果沒有良好的ELM與郵件檢索調閱機制，很有可能錯失了自我舉證的時機。如果企業能夠儘快導入具備良好檢索與搜尋調閱機制的郵件歸檔方案，便可以即時做好充份舉證資料的準備作業，並快速回應使用者的請求瀏覽需求。

網擎資訊軟體產品經理廖享進表示，該公司郵件歸檔特別針對地址、電話或身分證字號等個資相關的關鍵字提供預設的版型。任何郵件進入主機之際，會以該版型比對郵件內容，一旦符合會加上特別的標記。如此一來，管理人員可以透過清楚的標記進行個資盤點、監控或警示等安全作業。此一做法有別於一般關鍵字查詢及檢索等做法，係為該公司專門針對個資法的最佳化探勘機制。

遠端儲存資源管理							
選取 ▾ 編輯 ▾ 動作 ▾							
<input type="checkbox"/>	說明	主機位址	主機名稱	網域	使用者帳號	備份位置	狀態
<input type="checkbox"/>	遠端備份主機	192.168.100.168	Pail-PC		test	Share/history...	
<input checked="" type="checkbox"/>	遠端郵件位置	192.168.4.111	ad		administrator	MailBackup	郵件索引檔,2008-11-19 郵件壓縮檔,2008-12-01 ~ 2...
							郵件索引檔,2008-11-19 郵件壓縮檔,2008-12-01 ~ 2008-12-02

►Soffnext 郵件壓縮檔近線調閱畫面。

除此之外，個資法第18條並規定：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」第27條則要求：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」歸納兩條法規的重點，不外要求企業必須要有專責人員，以確保善盡保護之責。對此，企業應該要建立一套嚴密安全的郵件調閱流程，同時因應不同層面及需求皆有專人加以嚴格把關，以確保機密文件在保存、流向及需求回應上的所有可能風險都能受到控制。

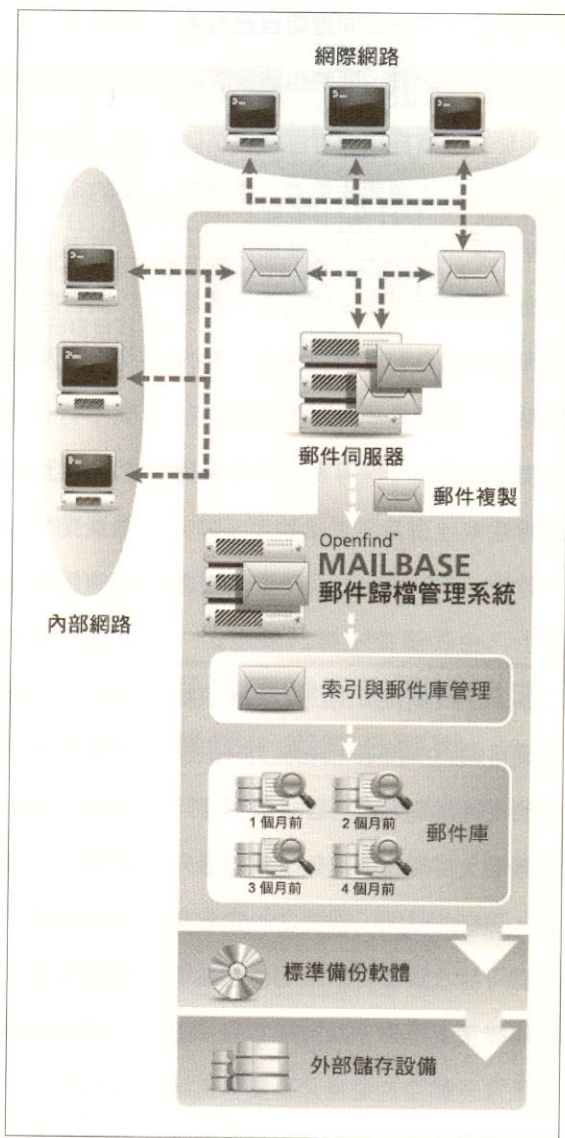
對此，中華數位提供雙帳號認證機制，該機制允許各部門主管皆有權責所及的郵件檢索搜尋的權限。當找到想調閱的郵件時，必須會同專責人員，才能將確實內容調閱出來。由於專責人員可做為最後一道安全關卡，因而能確保個資或機密的外洩。而在初期將郵件搜尋權限分工下放給各級主管，也可以加快郵件搜尋的速度，在因應前述30天的舉證資料準備時間會有很大的幫助。有了上述嚴密的安全流程與專

責人員把關機制，企業一方面可以確保機密郵件內容的安全無虞，同時也可作為日後法律訴訟時表明自己已善盡保護之責的舉證。

最後，則是與個資法第8條規定有關的善盡事前告知以免責的要求，該條指出：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項……。」換言之，今後企業想要使用個資時，必須事先行文告知對方：自家公司機關名稱、蒐集目的、個資類別、個資利用期間、地區、對象及方式等資訊。

但在企業內部，由於使用者的有意無意、不良習慣或觀念，使得電子郵件往往成為資料外洩最嚴重的管道之一，這當然也與郵件方便夾

檔轉寄的特點有很大的關係。企業除了須對內部人員進行正確觀念的宣導及教育外，更重要的，莫過於必須事先在電子郵件中添加免責權聲明，如此一來，即使有員工有意無意發生經由郵件寄送的個資外洩事件，也屬與公司無關的員工個人



► Openfind Mailbase架構圖。

行為。換言之，企業必須慎選支援郵件寄送過程中會自動在每封信上加註免責權聲明的郵件歸檔方案，如此才能避免不必要的訴訟風險。

此外，各家郵件歸檔方案莫不強調支援郵件檔案格式多寡及探勘深度（亦指檔案副檔名遭竄改也能加以辨識）的重要，畢竟當前企業內部可能充斥不同格式的郵件檔案，為了因應個資法舉證之需，當前郵件歸檔在檔案格式的支援上當然是多多益善最好。

郵件歸檔與郵件備份的差異

為了因應未來可能發生的訴訟舉證需求，企業勢必需要長期妥善保存好電子郵件，以做為舉證上的有力後盾。雖然對電子郵件做好定期的備份作業會是最簡便的做法，但是長久下來，面對容量驚人且毫無分類的電子郵件備份，企業實在很難因應個資法的要求，提供即時有

效的郵件舉證資料。唯有郵件歸檔機制才能滿足這方面的需求，並有效降低可能的安全及訴訟風險。

但許多人並不清楚郵件備份(E-mail Backup)與郵件歸檔(E-mail Archiving)之間的差異，甚至混合為一談。對此，王智衛剖析指出，郵件備份與郵件歸檔間大致會有作用目的、儲存空間利用、儲存週期管理，以及搜尋速度等4個面向的顯著差異。

首先就作用目的而言，郵件備份會另外將一模一樣的複製存放在別處，以做為災難備援之用。換言之，一旦主系統掛點或郵件資料遺失，可以立即從事先做好的備份進行還原。至於郵件歸檔其目的在於方便日後的搜尋，它可在郵件歸檔儲存之際，同時做好索引化及分門別類的作業。至於儲存空間的利用上，郵件備份是有多少就備多少，所以儲存空間很難能有節省的餘地。至於郵件歸檔則會進行重複資

料刪除的動作，亦即重複內容的信件只會備存一份。

再就儲存週期管理來說，郵件備份只能按照日、週、月、年等固定週期來備存，但如此一來難免會有重複備份的狀況。為了避免重複與備份量過大，會在日常進行不必要信件的刪除動作，但如此也可能造成之後備份內容的遺漏或不完整。反觀郵件歸檔，一經郵件主機的信件會立即另外複製一份進行歸檔，所以即便使用者誤刪了某郵件也沒關係，因為已事先做好完整的歸檔。再來，在歷史郵件的搜尋上，郵件備份必須麻煩地先將資料倒回，然後再透過具備搜尋功能的使用者介面進行搜尋。該搜尋功能最多只能做到郵件標頭、寄件或收信人等關鍵字搜尋的程度而已。郵件歸檔在郵件一收進來之際便完成檢索化的作業，再加上獨立搜尋引擎的提供，因而可以做到精準且即時的全面性搜尋能力。■

郵件備份 vs 郵件歸檔差異比較表

	目的	空間佔用	重複刪除	備份週期	備份完整度	搜尋機制	搜尋速度	搜尋結果
郵件備份	異地備援	大	無	按時程	不完整	關鍵字	慢	不精準
郵件歸檔	郵件搜尋	小	有	即時	完整	檢索化	即時	精準