郵件系統安全年，從防護、管理、備份談起

Anti-Spam 無疑是近兩年來最熱門的資訊安全議題之一。但是除了垃圾信的問題之外，病毒、詐騙、釣魚及偽造等亦是企業不可忽視的郵件安全問題。綜觀電子郵件安全管理的範疇，導入垃圾信過濾系統往往只能解決一部份問題，仍舊無法確保穩定、安全且不中斷的訊息傳遞。展望 2006 年，企業應就系統防護、郵件平台與備份管理三個主題檢視現有的郵件系統，進行整體性的 IT 規劃與佈署，打造一套完善的企業安全防護系統。

郵件防護閘道打造資訊安全

企業每天透過大量郵件往來對內外溝通，雖然加速了資訊的流通，但也帶來各種資訊安全上的威脅。垃圾郵件及病毒信件就是最常見的案例，我們可以大致歸類為內容安全層級的一環。然而，對於企業資訊安全有著重大影響，卻常常會被忽略的惡意連線、弱點掃描或阻斷攻擊等，則屬於網路與系統安全層級。此一層級的監控必須透過建置專屬的郵件防護閘道 (Email Protection Gateway) ，僅放行安全可靠的訊息進入企業內部的郵件主機，才能有效阻絕外來的安全威脅。因此在實務上，建議採取實體主機分離的佈署架構，搭配防火牆設定以提升郵件使用安全，讓內部系統可在不受干擾的環境中，提供高效能的郵件服務。

對於電子郵件系統經常遇到的惡意 SMTP 連線，例如 DoS 攻擊或是垃圾郵件業者的字典攻擊，郵件防護閘道必須能提供第一線的即時防護，避免後方重要的郵件主機受到干擾。以維護上的考量來看，即使郵件防護閘道持續進行更新升級，內部郵件系統亦可彈性整合不同的資訊環境，彼此各司其職、互不影響。

創新功能架構 Web 化郵件平台

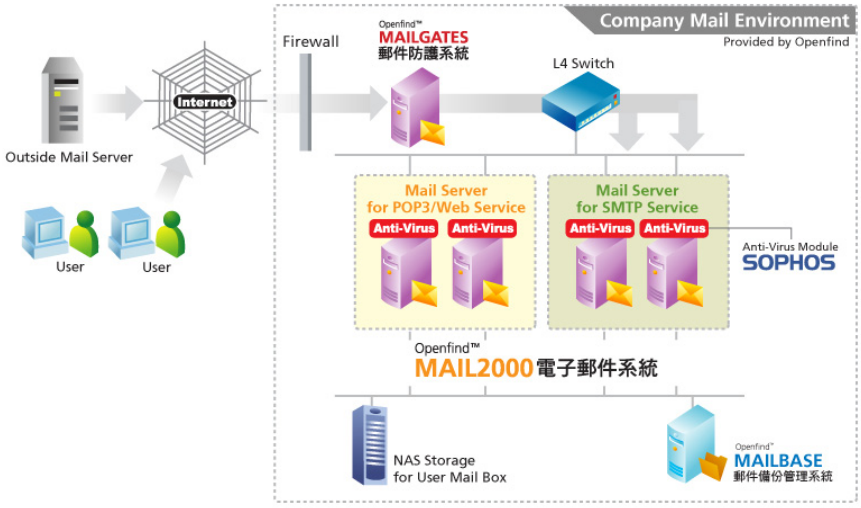
根據統計，企業郵件數量每年數以倍計地快速攀升，員工每天亦需耗費過去數倍的時間處理郵件。對於企業來說，除了在一般正常運作中能穩定收發電子郵件之外，更應著眼於應付無預警的緊急狀況與系統擴充需求。依照一般企業的實際線上數據來看，郵件系統的尖峰處理效能應為現行郵件量的三倍以上，才能確保系統效能與擴充彈性。此外，隨著近期 Microsoft 推出 Windows Live 服務，除了宣示 Web 化軟體服務的時代來臨，並揭示新一代郵件系統支援標準通訊協定之外，郵件系統亦應具備完整的 Web 使用介面與行動通訊功能，才讓員工享受 Web 化服務的便利性，並提供創新功能來提升工作效率。以最新版本的 Mail2000 為例，即規劃透過資訊整合、虛擬信匣與個人化設定等全

新設計，提供企業員工更高效率的郵件使用環境。

ILM 結合郵件備份管理

在網路 e 化的世代，有越來越多的重要資訊是透過電子郵件傳遞，其中不乏寶貴的企業知識、機密資訊以及商業交易文件。因此，隨著電子郵件在商務上的廣泛應用，美國與日本等各國已正式立法要求部份行業保存 3 到 5 年電子郵件內容，以避免公司重要機密或文件一旦外洩時，可供企業日後進行調閱與稽核。為確保現今資訊電子化的趨勢，企業應加速落實郵件備份系統的建置；同時，由於長時間持續保存所有對內、對外之電子郵件，累積資料量十分驚人，如果長期存放在成本相對高昂的硬碟空間當中，對企業將是一筆昂貴的成本支出。

此外，當企業累積了長時間大量的電子郵件備份資料，一旦需要進行調閱，該如何在數百 GB 甚至數 TB 的巨量資料中，以最方便、直覺、快速的方式找出需調閱的信件，亦為企業必須妥善評估的重點；更進一步來看，強大的郵件搜尋機制更須輔以周詳的權限管理機制，才能避免企業重要資訊外洩。因此，一套完善的郵件備份系統需可結合 ILM (Information Lifecycle Management) 儲存系統，並應同時具備完整的搜尋、調閱、權限控管與離線備份等功能。



總括而言，完整的郵件系統佈署策略應包含前端的安全防護閘道，高效能的郵件服務平台，以及後端的郵件備份管理系統。長久以來，企業多著眼於電子郵件使用問題，或是單單導入垃圾信過濾系統，但卻忽略了建置的完整電子郵件資訊安全環境，這樣的方式無法提供企業長期穩定運作的電子郵件系統。因此，企業應定期檢視並進行整體性評估，擬定符合企業環境與需求的郵件系統建置與升級計畫，才可充份發揮電子郵件效能，提升企業溝通競爭力。