# 雲端環境下的最佳訊息保全選擇 – Openfind Message Assurance 解決方案

Openfind 產品經理 廖享進

睽違了近二年的 Openfind Solution Day，在大家的殷殷期盼下，於 2010 年 6 月 10 日圓滿落幕。在這場盛會中，Openfind 除了依據自己 10 年來豐富的雲端經驗，提出進入雲端環境需要注意的訊息安全風險外，更有別於一般產品型公司只單純銷售產品而不注重解決方案的走向，提出了「Message Assurance」的概念，並且開始揭露在 Openfind 各個產品中，與此概念相關的設計。

在「買張保險，安心上雲端」的主題中，我們簡述了 Openfind 從 1999~2009 年的雲端服務發展史，並大致複述了未來個資法通過之後，在雲端環境普及下為組織企業帶來的可能風險。其中所介紹的 Message Assurance 信息安全方案，能提供完整的資料外洩防護，符合相關資安法規，並從資料的啟始、傳遞、到保存階段，均能完整考慮到相關的風險預防政策。如方案中的 Mail2000 MLP Pack 郵件外洩防護套件包，運用虛擬鍵盤、密碼強度提示與動態密碼等機制強化郵件登入身分識別與密碼安全；MailBase 3.0SP1 則強化使用者雙重認證／稽核信件功能，並提供關鍵字追蹤功能，可主動追查歸檔的歷史郵件是否有關鍵機敏資訊，保存的訊息也具數位證據效力；同時據實測數據指出，1,836 萬筆郵件紀錄數中全文搜尋僅需 5.6 秒，較友商快 50 倍以上，能在大量電子郵件的歸檔風險中，預防調閱速度緩慢，甚至調閱困難的風險。

方案中也提到 MailGates 的雲端雙核心垃圾信防護引擎，具備完善郵件稽核管理、郵件隨選加密，以及精準、快速的郵件紀錄追蹤；該產品同時也從美國、英國、香港、台灣、中國、日本各地同步累積每月 30 億封以上的信件樣本，以郵件發送行為作判斷，各國語系垃圾信件攔截率高達 99%。另外，新提供的 Mail2000 軟體叢集解決方案，能協助客戶用軟體網路叢集機制取代傳統昂貴的 L4 交換器硬體設備，搭配 Openfind 認證過的高 C/P 值 NAS 裝置，提供低於 1 秒切換的網路備援能力，並具備 AA(Active-Active) 和 AS(Active-Stand By) 的架構能力。最近剛上市的 Openfind Enterprise Search(OES) 3.0SP1，也提供「機敏資料檢測」的功能，配合「查詢結果排外設定」，能幫助搜尋網頁、文件、資料庫等相關索引資料源是否含有可能洩漏的個資或特定型式資料，並確保敏感資料不被外界搜尋到。

在這場演講中，Openfind 針對軟體產品的使用風險特別額外指出，使用 Open Source 開放源碼拼裝方式為核心，建置的郵件系統，除了管理與服務上的複雜化，其資安風險超過想像。依 osvdb.org 網站指出，像是時下部份廠商常使用的 Postfix + Sendmail + MySQL + Lucent + PHP 等系統，光 2009 年就被揭露出超

過 200 個資安漏洞。而 Openfind 提出的 Message Assurance 方案完全採自主研發，全系列產品均獲台灣精品獎及傑出資訊應用暨產品獎肯定，也是唯一國產廠商能通過日本嚴謹的個人情報保護法考驗的產品，安全並值得信賴。

除了提出「Message Assurance」的概念，Openfind 也強調 100% 自主技術、高穩定性、可擴充性架構、低成本、高效能及豐富實戰經驗的優勢，相信能提供企業最穩定的郵件溝通／防護／歸檔／稽核系統，並提供即時性的服務。同時 Openfind 也深信未來「端」的應用與部署將決定雲端環境的走向和需求，因此，在熱門的雲端運算議題上，Openfind 也特別重視「端」的部分。除了提供 Mail2000 的 iPhone 模組外，也正在研發桌面平台上的 AirMail 與 Android 等相關智慧型手機平台的解決方案，實現 PC、Mobile 裝置與 Web 訊息同步閱讀、管理的一元化機制。

語末，Openfind 也針對雲端「隨選即用」的特性，提出 MailCloud 雲端緊急備援的新服務，藉由定期將企業郵件系統資訊至雲端，萬一企業自建的信件系統損毀時，僅需更動 DNS 設備啟用雲端備援機制即可，如此一來，將能提供客戶固若金湯的資安防護與低成本的緊急備援機制，完整符合 Message Assurance 資料保存零風險的最高原則。