教育部

教育部電子郵件服務與管理調查

相關產品應對功能說明書

中華民國 106 年 01 月 24 日

目　　錄

1. 電子郵件服務與管理調查項目

1.1. 電子郵件服務與管理調查項目

	說明:	非單位人員，例如服務客戶帳號
九、	電子郵件安全防護與管理	
	●	帳號/密碼管理
	●	設定不得自動轉發信件
		郵件加密功能
	●	傳送郵件LOG保存
		郵件APT偵測
	●	弱點偵測與修復
	●	納入資訊安全管理制度(ISMS)
	●	訂定電子郵件服務管理規定

1.2. Mail2000 對應功能列表

以下列出電子郵件建議的管理項目，並整理出 Mail2000 對應管理項目中的功能列表說明

電子郵件服務與管理調查項目	Mail2000 對應功能列表
帳號/密碼管理	● 圖形驗證與虛擬鍵盤 ● 密碼政策 ● 弱密碼分析 ● 登入失敗鎖定 ● 雙重認證 ● 異常登入警示
設定不得自動轉發信件	● 關閉自動轉寄功能 ● 驗證自動轉寄設定 ● 自動轉寄監控報表
郵件加密功能	● 傳輸加密 ● PKI 簽章與憑證 ● 重要郵件自動加密
傳送郵件 Log 保存	● 所有收發信 Log 完整保存

電子郵件服務與管理調查項目	Mail2000 對應功能列表
	● 使用者自行查詢信件傳遞狀態 ● 完整郵件歸檔
郵件 APT 偵測	● 垃圾病毒信防護 ● 線上預覽模組 ● 整合 APT Solution ● 無害化電子郵件
弱點偵測與修復	● 重視開發過程的安全 ● 同時採用多套原始碼檢測及弱點掃描 ● 定期進行白帽駭客演練
納入資訊安全管理制度 (ISMS)	● 建議學校導入資訊安全管理制度 (ISMS)
訂定電子郵件服務管理規定	● Openfind MailCloud 參考使用條款

2. Mail2000 對應功能說明

2.1. 帳號/密碼管理

帳號密碼有如門鎖，若不夠嚴謹則可能如郵件門戶大開，對個人或系統都會藏著資訊安全的危機。Mail2000 提供完整的郵件帳號機制，提供本機帳號及整合 AD 或 LDAP 機制，並透過密碼政策、弱密碼分析等，幫助管理者監管使用者密碼強度，提高系統安全。

圖形驗證與虛擬鍵盤

Mail2000 提供完善的安全登入機制控管，使用者可透過虛擬鍵盤防止有心人士側錄密碼，並提供聰明圖形驗證功能，可在使用者登入密碼錯誤達到指定次數時自動判斷出現圖形驗證碼，在盡量不打擾使用者下提供安全的登入機制。

密碼政策

Mail2000 提供密碼管理政策，透過密碼政策要求使用者必須設定一定強度的密碼，以避免因密碼過於簡單而被輕易破解。其密碼政策包含強迫修改密碼、密碼設定的最小長度、強制密碼複雜度等等。

弱密碼分析

Mail2000 提供弱密碼分析報表，透過此報表提供給管理者了解目前使用者密碼設置的情況，並能進一步要求使用者進行密碼強度的調整。其弱密碼檢查範圍可包含帳密相同、符合弱密碼字典及符合企業自行定義的弱密碼字串等。

登入失敗鎖定

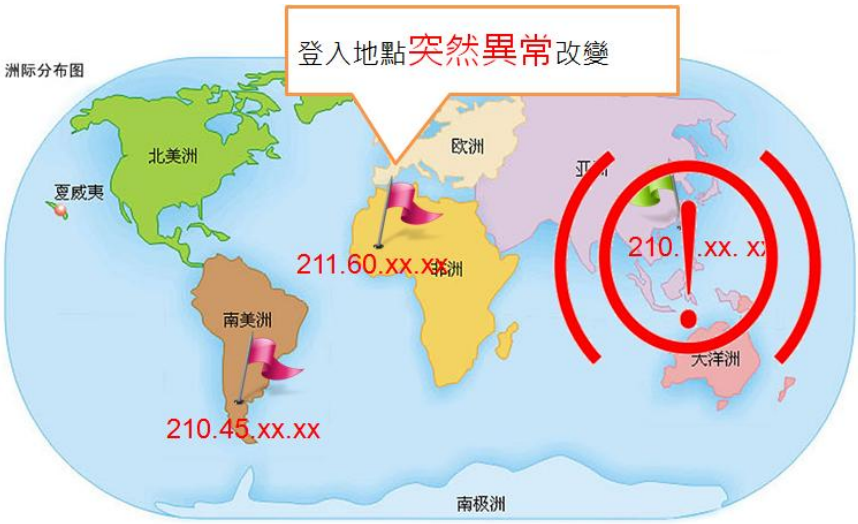
Mail2000 管理者可指定使用者登入失敗時的處置方式，例如設定登入失敗的重試次數及鎖定時間等，以防止駭客或有心人士進行帳號的暴力破解。

雙重認證

Mail2000 提供雙重認證功能，並整合個人 Mail2000 APP 接收 OTP (One time password)，使用者在登入過程中，除了必要輸入即有的 Mail2000 帳號，並且必須再透過手機接收到第 2 個 OTP 密碼，透過此雙重密碼才能正確登入自己的郵件帳號。

異常登入警示

在使用者突然後習慣登入的外地 IP 登入時，系統會主動通知管理者及使用者異常登入，若發現異常則可趕緊修改密碼，保障系統安全。



2.2. 設定不得自動轉發信件

自動轉寄功能可便使用者將信件統一轉寄至備用信箱，或在職務代理時，可將信件自動轉寄一份給代理人。但是此動作也可能因為不小心成為有心人士盜用資訊的管道之一，在資訊安全為重的時代必須針對自動轉寄功能進行管控，例如只允許特定人員開啟此功能，或針對此功能進行監控轉寄目標等，以確保郵件系統的安全。

關閉自動轉寄功能

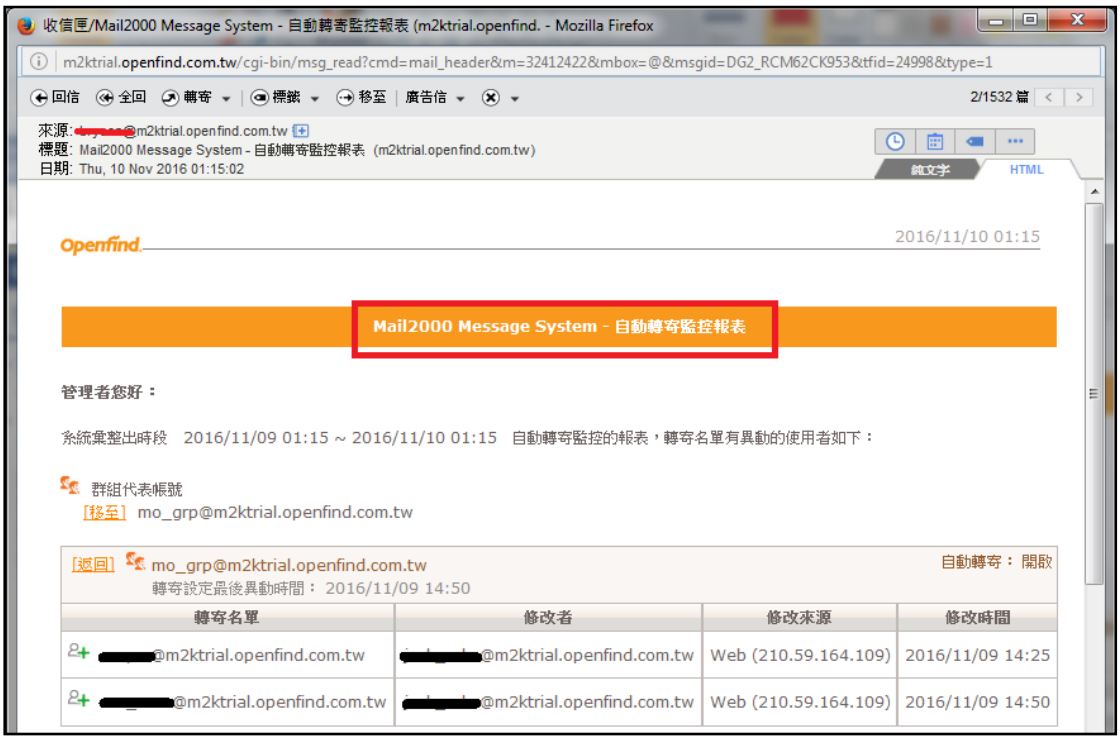
Mail2000 系統管理者可依等級方式設定自動轉寄使用權限，僅開放業務必要人員使用此自動轉寄功能，或將此功能完全關閉等。

驗證自動轉寄設定

若因業務需要必須開放自動轉寄功能給指定人員時，管理者可要求使用者在設定自動轉寄時，使用者必須再輸入一組有別於登入系統的密碼，透過雙重密碼的保護，以確保設定此轉寄帳號者確實為本人

自動轉寄監控報表

自動轉寄功能若因業務上需要非得提供時，在安全與方便的考量下，適當的監控特別重要，Mail2000 會依目前自動轉寄的設定情況每日發送自動轉寄監控報表給管理者，讓管理者清楚掌握目前信件被轉送的狀況，在發現異常時可即時防範及攔阻。



2.3. 郵件加密功能

傳輸加密

Mail2000 在郵件主機溝通時支援完整的 TLS/ STARTTLS 等加密協定，在主機與用戶端的溝通也支援完整的 Https, Smtps, POP3s, IMAPs 等加密協定，讓郵件訊息的溝通更加安全

PKI 簽章與憑證

Mail2000 可整合自然人或第三方單位的憑證，讓使用者在登入 Webmail 時可直接透過卡片或軟體憑證登入系統，並在 Webmail 上讀取對方憑證及將郵件進一步加密寄出，透過 PKI 機制，讓信件在傳送時達到防偽造及內容加密等安全防護。

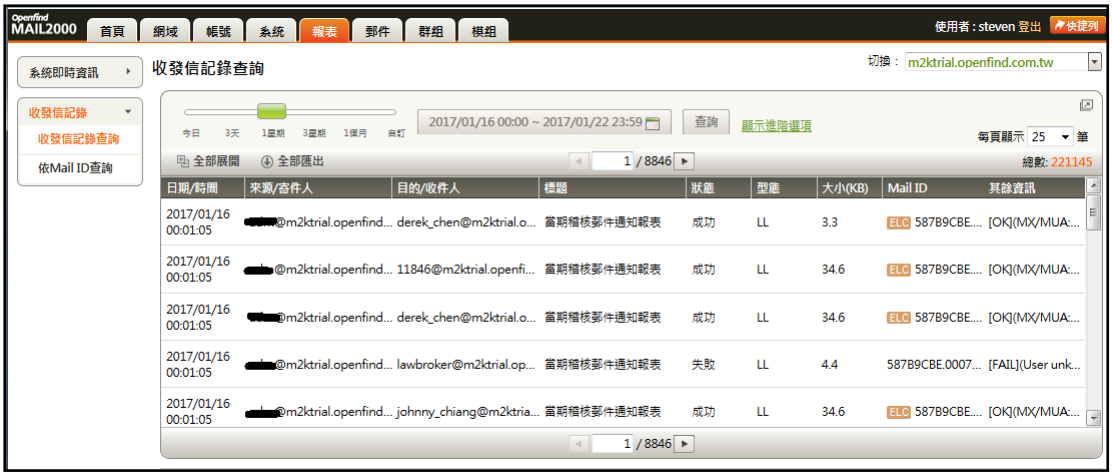
重要郵件自動加密

郵件訊息溝通過程中，經常會有許重要或機敏的訊息，例如附檔內容包含大量個人資料、機密公文、薪資資訊等等。Mail2000 只要搭配 MailAudit 郵件稽核功能，則可將這些郵件內容在傳遞的過程中將其自動加密後再寄出，並透過自動密碼通知信功能，讓收件者可透過額外的通知管道通知收件者，將其解密後閱讀信件內容，以達到重要郵件自動加密的安全功能。

2.4. 傳送郵件 Log 保存

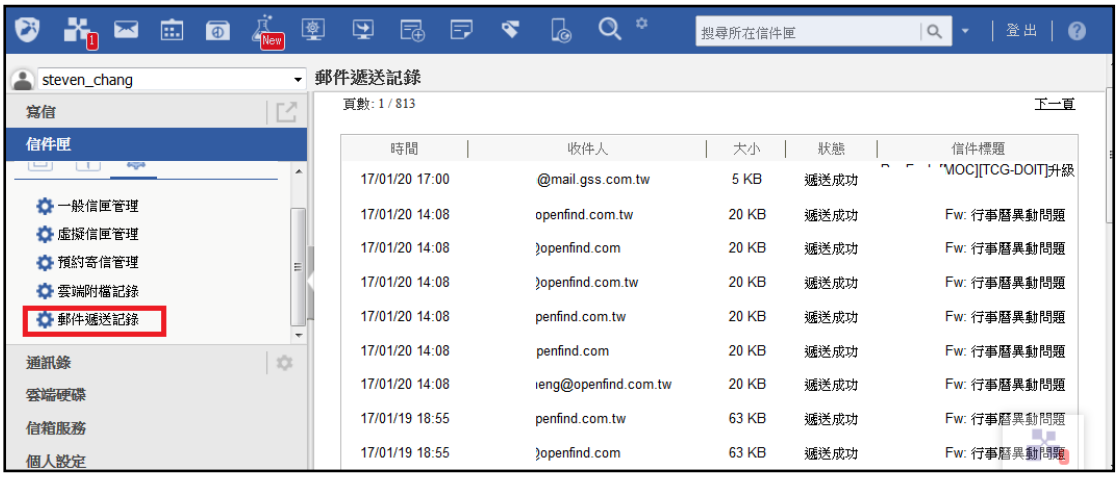
所有收發信 Log 完整保存

Mail2000 會將所有的 Log 皆完整保存，包含郵件的收發狀況、連線的 IP 資訊、信件是否成功送達等資訊。在使用者對信件寄送過程中有任何問題時，管理者可透過完整的 Log 資訊查詢正確的告知使用者信件狀態。



使用者自行查詢信件傳遞狀態

Mail2000 提供給使用者自行查詢信件遞送記錄，了解每封信件是否有成功送出。不需每一次都要與管理者確認，不僅可節省溝通時間，也可幫助管理者掌握信件溝通狀態。



完整郵件歸檔

Mail2000 不僅將所有的郵件流通 Log 完整保存，並可搭配 MailBase 郵件歸檔功能，將所有信件及其附檔內文完整歸檔。配合完善的郵件生命週期管理，將信件自動化保存在線上端(online)、近線端(nearline)及離線端(offline)，並透過友善的搜尋、調閱及還原功能，讓使用者可輕鬆查閱歷史郵件，而管理者可輕鬆管理及封存歷史郵件。

2.5. 郵件 APT 偵測

垃圾病毒信防護

Mail2000 搭配 MailGates 雙雲端郵件防護系統，能有效防止垃圾信件、釣魚信件及病毒信件等攻擊，並透過社交工程防護機制，有效避免使用者誤擊有害連結，在郵件門口進行第一層的把關。

線上預覽模組

APT 攻擊通常會在鎖定攻擊目標後進行郵件攻擊，透過寄送郵件所夾帶的附檔給指定目標，並透過社交工程誘捕目標開啟附檔而進行資料竊取。Mail2000 提供線上預覽功能，讓使用者在不需要開啟及下載附檔前，直接線預覽附檔內容的真實性，當發現異常時則可直接刪除此信件，並通報管理者，防止災害的發生。

整合 APT Solution

APT 為針對性的攻擊，在駭客鎖定對象後則會設法入侵，並開始對目標進行客製化的攻擊。因為郵件是普遍的溝通工具，且能直接接觸到指定對象，所以通常 APT 攻擊，郵件系統將會是第 1 個被鎖定的攻擊目標。針對 APT 攻擊，Mail2000 提供許多解決方案作法，包括整合歐洲第一大品牌專業郵件防護系統，透過其強大的零時差 APT 防護技術，確保郵件系統安全

無害化電子郵件

Mail2000 提供的無害化電子郵件架構，在日本短短數個月即完成 50 家以上的政府機關導入，並獲得非常好的好評。政府、學校或企業在導入無害化架構後，能夠完全阻檔 APT 有害的附檔及連結被使用者點擊，透過內外網隔離的架構，更是確保實體隔離的安全環境

2.6. 弱點偵測與修復

重視開發過程的安全

Openfind 重視產品開發過程中的安全，透過教育訓練教導工程師注重系統安全，系統開發時確認是否有確實使用原始碼檢測工具來掃描系統漏洞，並落實測試階段透過多種弱點掃描軟體進行偵測，上線後的技術支援也要求必須確實執行資安檢查的政策。

同時採用多套原始碼檢測及弱點掃描

Mail2000 在產品開發及 QA 流程都會同時採用多套指標性防護軟體進行原始碼檢測及弱點掃描，以確保產品在最新的防護架構。若在檢測過程中，有發現漏洞或弱點時，則會即時進行修補並更新到所有客戶的 Mail2000。許多 Mail2000 客戶在使用 Mail2000 後也會自行定期進行弱點偵測，若有回報發現漏洞，Mail2000 亦會立即配合其單位進行修補。

定期進行白帽駭客演練

Openfind 會定期以付費的方式邀請白帽駭客模擬進行系統的攻擊，在攻擊的過程中了解產品是否有潛在的風險，透過白帽駭客的回饋分享進一步了解產品是否有存在弱點進而進行修復，已確保產品開發更加安全。

2.7. 納入資訊安全管理制度 (ISMS)

建議學校導入資訊安全管理制度 (ISMS)

資訊安全管理制度 (ISMS) 是一套有系統地分析和管理資訊安全風險的方法，建議學校透過導入此制度來強化資訊安全。Openfind 本身提供 MailCloud 郵件代管服務，此服務為 Mail2000 電子郵件系統的雲端服務版，已提供中小企業、兩岸三地的郵件代管服務超過十年。由於本身提供系統給龐大的用戶使用，Openfind 於 2009 開始就積極導入 ISMS，藉由此制度強化資訊服務上的安全。

2.8. 訂定電子郵件服務管理規定

電子郵件服務已經是日常生活中溝通的重要工具，使用者在方便使用之餘必須有良好的管理機制，才能讓相互間的溝通更加的順暢、安全。政府機關、學校單位或企業組織針對不同的屬性都會有不同的郵件使用辦法，以下提供 Openfind MailCloud 在雲端郵件服務的管理規定，可供學校在訂定辦法時的參考：

Openfind MailCloud 參考使用條款

你必須遵守相關法令規範，並且對於經由使用者帳號和密碼所進行的任何行為、以及所儲存的所有資料負責。你承諾不從事以下的行為：

(1)傳送何任違反中華民國技術資料輸出等相關法令之郵件。

(2)傳輸、發送或儲存任何誹謗、詐欺、傷害、猥褻、色情、賭博或其他違反法令或侵害他人權益之郵件、檔案或資料。

(3)傳輸、發送或儲存任何侵害他人智慧財產權或其他權益的資料。

(4)未經同意收集他人電子郵件位址以及其他個人資料。

(5)傳輸、發送、儲存病毒、或其他任何足以破壞或干擾電腦系統或資料的程式。

(6)破壞或干擾本服務的系統運作或違反一般網路禮節之行為。

(7)任何妨礙或干擾其他使用者使用本服務。

(8)傳送幸運連鎖信、垃圾郵件、廣告信或其他漫無目的之郵件。

(9)任何透過不正當管道竊取本服務之會員帳號及密碼以及存取權限之行為。

(10)其他違反本使用條款或不符合本服務所提供的使用目的之行為。

(11)利用不正當管道竊取他人的帳號密碼，以及郵件存取權限之行為。

(12)沒有經過合法授權，即擅自進行重製、改作之行為。

(13)帳號販售或以任何形式轉讓或提供他人使用以獲取對價。

(14)偽造寄件人辨識資料傳送郵件，企圖誤導收件人判斷之行為。

(15)其它任何不符合或違反 Mail2000 使用目的之行為。

使用者違反前項約定時，本公司得不經通知，隨時暫停或中止提供本服務之全部或一部，凍結存取權限，刪除或移置相關檔案或資料，之全部或一部，使用者不得因此對於本公司為任何法律上主張。

網擎資訊軟體股份有限公司

地　　址：台北市重慶北路二段 243 號 7 樓

電　　話：02-25532000　　傳　　真：02-25530707

網　　址：http://www.openfind.com

E-mail： pre-sales@openfind.com