

## 郵件伺服器 / ML 系列報導

### 技術淺談與應用 - 養成良好的電子信箱密碼管理習慣

隨著科技不斷的更新、進步，公司間的通訊管道早已經是由電子信箱取代為主要的交流方式之一，快速、方便的特性不但為使用者帶來了極大的便利性，同時也為公司創造了更大的收益與商機。而捍衛這些資訊安全的第一道防線最基本也最常見的就是利用密碼做為保護，同時也是用來授于使用者權限的基本方式之一。但入侵、竊取、竄改及破解密碼的案例層出不窮，也正因為如此不少使用者信箱被做為有心人士發送廣告、病毒信件的跳板，甚至是存於信箱中的重要資料因此流露出去，造成個人及公司的重大損失。

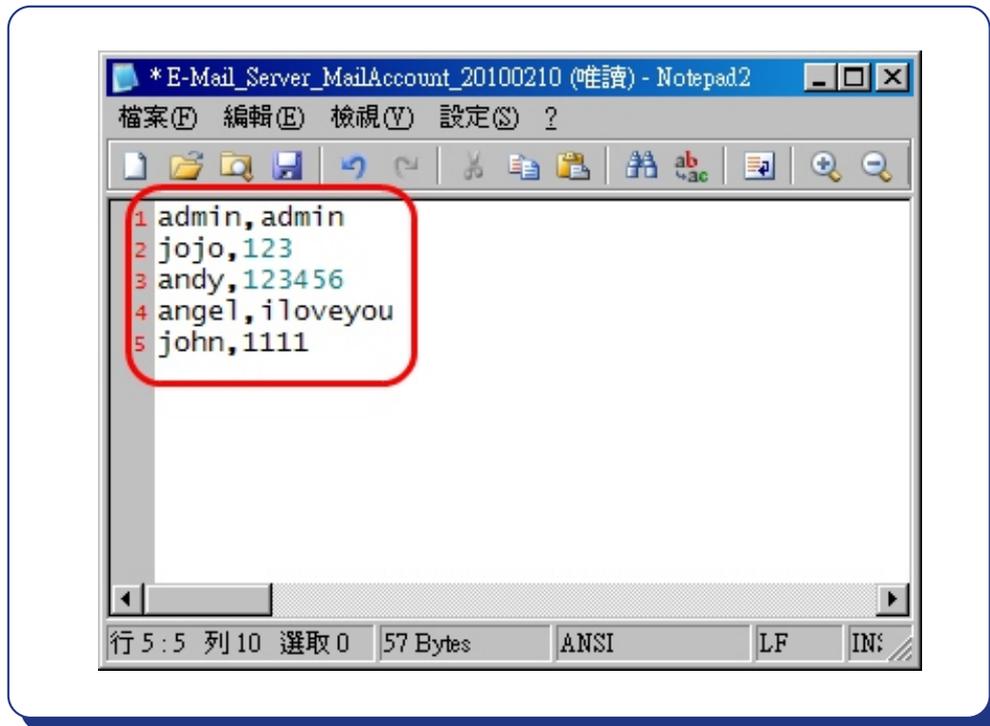
身為公司資訊管理人員該如何防範才好？其實大多數的原因並不是公司內的資安設備不夠力，而是不少使用者往往會因為為了在使用上方便、好記，乾脆將自身信箱密碼設定『123456』這類簡單的懶人密碼，根據統計平均每5人就有1人使用此類「懶人密碼」，同時『123456』更是使用者最常使用密碼的排行榜第一名。如此一來便會讓使用者及公司處於高風險的環境下，相對的有心人士並不需要如何高超的技術，只要利用使用者懶惰的心態即可輕鬆進一步的入侵破解。

身為公司資訊管理人員，輔助員工加強密碼的設定以增加公司資訊安全，也是首要的事情，首先必須先瞭解到公司內部使用者使用懶人密碼的比例與密碼設定的方向跟習慣，進而再來做相關的協助與教導，但管理人員又該如何利用『郵件伺服器 - ML』來查閱公司內部使用者是否有密碼設定不良的情況發生呢？管理人員可於『郵件伺服器 - ML』的系統介面“郵件管理 > 帳號管理 > 個人”下將公司內部使用者帳號進行“匯出”動作，便可進行檢查。



於ML-郵件管理 > 帳號管理 > 個人下匯出使用者帳號

為了有效降低公司內信箱遭非法入侵，以防止往後不必要的損失發生，要求公司內部使用者將個人密碼加強難度絕對是項必要的動作，同時相信不少管理人員在查閱過公司內部使用者所建立的帳號密碼後，肯定會發現內部不少使用者正是使用『懶人密碼』來作為登入個人信箱的條件。所以教導使用者去瞭解如何正確選擇、設定、更新其個人相關密碼，正是管理人員的重要課題之一。



從匯出的檔案查詢使用者帳號密碼是否過於容易破解

以下將列出幾項密碼管理維護所需注意之方向，以供公司或管理人員在進行對員工教育時可著重的地方，以達到有效落實加強公司內部資訊安全。

### 一. 密碼設定至少要達 8 個字元

密碼設定過短容易遭有心人士利用輔助軟體來進行排列比對破解，而效能較好的機器破解 6 個字元的密碼只需兩天；7 個字元的密碼約 4 個月內，所以為提高密碼的強度，使用者最好要達 8 個字元以上的密碼較為安全。

### 二. 避免過於簡單易猜測的密碼

為了加強密碼組合的強度，使用者盡可能的要避免掉下面幾種密碼設定的情況：

1. 密碼和帳號相同
2. 有順序性的數字、字母(如：123456、qwerty...)
3. 重覆性高(如：1111、aaaa、aabbcc)。
4. 使用個人生日、身份証號碼。
5. 英文單字或詞語(如：iloveyou、baby、honey...)
6. 含公司、部門等公司資訊。

### 三. 數字、字母、特殊符號穿插使用

字母可再配合上大小寫的不同來增加破解的難度，同時加上數字與特殊符號混合使用，藉此能將使用者密碼強度大大的升級。

當然，密碼的設定也不需要複雜到難以記住，因為連自己都記不起來的密碼組合其實也就失去其設定意義，同時還需養成良好的使用習慣，切忌將個人密碼留於紙上或電腦文字檔中，以免讓人容易得手。

下面則是由某知名網站百萬名會員所使的懶人密碼排名，由該表格可明顯看出使用者於設定密碼時最容易出現的問題，管理人員也可藉由此表格來針對公司內部使用密碼來做相對的改善。

名次	密碼	名次	密碼
1	123456	17	michael
2	12345	18	ashley
3	123456789	19	654321
4	password	20	qwerty
5	iloveyou	21	iloveu
6	princess	22	michelle
7	rockyou	23	111111
8	1234567	24	0
9	12345678	25	tigger
10	abc123	26	password1
11	nicole	27	sunshine
12	daniel	28	chocolate
13	babygirl	29	anthony
14	monkey	30	angel
15	jessica	31	FRIENDS
16	lovely	32	soccer

資料來源 / imperva.com

文  陳殿鴻 kim@nusoft.com.tw

## 市場行銷報導 - 所有「電子郵件稽核 / 歸檔」需求，新軟郵件伺服器一次幫您搞定！！

從古至今「郵件」在商人的從商之道中一直視為重要利器，從前古人使用手寫信件作為商業交易時的憑證；現代人也用電子郵件作為商業行為時的依據，所以郵件對於現代企業而言，重要性自然不可言喻。由於所有進出企業之電子郵件裡所帶的交易資料都算是企業商業機密，對企業而言皆屬公司重要資訊財產，因此「郵件稽核 / 歸檔」這個保護企業財產安全的概念，這幾年在企業界中持續發燒。

根據統計多達九成的公司企業會透過電子郵件洽談公司營運或是產品業務相關方面的業務，由此可見電子郵件使用的普及性和重要性，所以該如何妥善保存所有進出公司之電子郵件也成為企業不容忽視的重要問題。因此許多企業斥資添購郵件稽核 / 歸檔設備，主要原因不外乎是為了備份 / 稽核電子郵件，以備日後不時之需。例如：公司員工因為電腦故障導致其電腦內所有重要信件皆損毀、無法救回，這時就能利用此機制取回所有歷史信件；或者配合公司政策稽查需求，定時查詢稽核員工郵件是否洩密…等等需求。

新軟系統產品設計理念皆以“市場需求、未來走向”為設計目標，功能多符合現代企業需求考量，站在使用者角度所推出來的「新軟系統郵件伺服器 - ML 系列」，內建「郵件稽核 / 歸檔」功能以多項強大的功能特性協助企業完成郵件稽核 / 歸檔之需求：

- **歸檔郵件的多向化查詢方法**

為了從滿坑滿谷的歸檔郵件堆裡找出自己所想找的那封信，若一封一封信來找必然是費工又耗時。新軟系統郵件伺服器 - ML 系列裡內建之郵件稽核歸檔機制以（寄件者 / 收件者 / 有無附加檔 / 附加檔檔名 / 信件主旨 / 信件內文關鍵字 / 信件收送處理方式）等多項搜尋條件來協助管理者快速找出所想要查詢的信件，功能非常快速方便。

- **高效率的稽核機制**

想要有效防範洩密事件發生，除了做事後舉證以外，最好的方式當然為「事前防範」；因此新軟郵件伺服器推出「郵件稽核」功能，此功能著重於“事前稽核”，可由網管人員依公司政策自行設定相關郵件稽核規則（刪除 / 審查 / 延遲 / 傳送 / 複製），並可設定多條規則交互使用（必須符合所有規則 / 符合其一規則即可），只要有員工寄送觸犯公司所設定的規則的信件，將會自動攔阻下來或者轉送交由網管人員知曉，藉此能有效降低企業洩密事件發生。

- **歸檔郵件有效管理**

倘若有員工因為電腦故障損毀導致其裡頭重要信件遺失的話，此問題可由管理人員搜尋出所有目標信件後，可依照任務需求做相關郵件處置（信件取回 / 信件重送 / 信件刪除），因此可將所搜尋出來的歷史信件全部取回給該名員工，便可以達到「郵件歸檔」之目標。另外，若像公司政策需求必須定期查詢稽核員工信件的話，也可以依照搜尋規則做目標信件搜尋。

- **遠端備份歸檔郵件**

市場上許多郵件歸檔設備在郵件歸檔後會存置於其本機硬碟內，且這些資料很多都是不常讀取之資料，然而企業歸檔信件存放期限絕不止僅短短的兩三年，例如：因應沙賓法案內容要求，有些企業因為行業性質不同，在郵件歸檔存放期限上至少要求得存放 7 年以上，因此一般郵件歸檔的本機硬碟空間是無法長時間供應作為郵件存放的設備。在此，新軟郵件伺服器提供企業用戶「遠端備份」的機制，可以將歸檔郵件通通轉存備份於遠端伺服器中（NAS、File Server、SAMBA Server）；如此一來，依靠遠端伺服器“長期存放”的特性，便可妥善保存重要信件資料，更不必擔心信件資料是否會因為空間不夠而必須刪除其他信件來騰出硬碟空間的問題存在。

- **硬體軟體 All In One**

一般來說，郵件伺服器以及郵件歸檔設備分屬兩台不同的硬體設備；因此就軟體功能而言，兩種設備若為不同廠牌時，網管人員將得學習兩套操作方式，著實麻煩；若就硬體成本來看，兩台設備就得花更多經費來採購，且現在市場上的郵件歸檔設備大多價格昂貴，對於中小企業而言，將是一項不小的預算問題。於此，新軟系統郵件伺服器，除了本身的郵件伺服器功能之外，也將郵件稽核 / 歸檔功能建置於其中，讓所有功能 All In One，使網管人員無需分別學習兩台設備不同的操作方式，也使企業節省一大筆採購預算。

對企業而言，「郵件稽核 / 歸檔機制的嚴謹度代表著企業資安防護的完整度」，因此新軟系統郵件伺服器 - ML 系列所推出之郵件稽核 / 歸檔機制力求稽核 / 歸檔所有郵件都力求能達到“滴水不漏”的目標，藉此能夠給企業用戶安全的資訊財產保護。

文  黃政銘 [ming@nusoft.com.tw](mailto:ming@nusoft.com.tw)