

## 邮件服务器 / ML 系列报导

### 技术浅谈与应用 - 养成良好的电子信箱密码管理习惯

随着科技不断的更新、进步，公司间的通讯管道早已经是电子信箱取代为主要的交流方式之一，快速、方便的特性不但为使用者带来了极大的便利性，同时也为公司创造了更大的收益与商机。而捍卫这些信息安全的第一道防线最基本也最常见的就是利用密码做为保护，同时也是用来授予使用者权限的基本方式之一。但入侵、窃取、窜改及破解密码的案例层出不穷，也正因为如此不少使用者信箱被做为有心人士发送广告、病毒信件的跳板，甚至是存于信箱中的重要数据因此流露出去，造成个人及公司的重大损失。

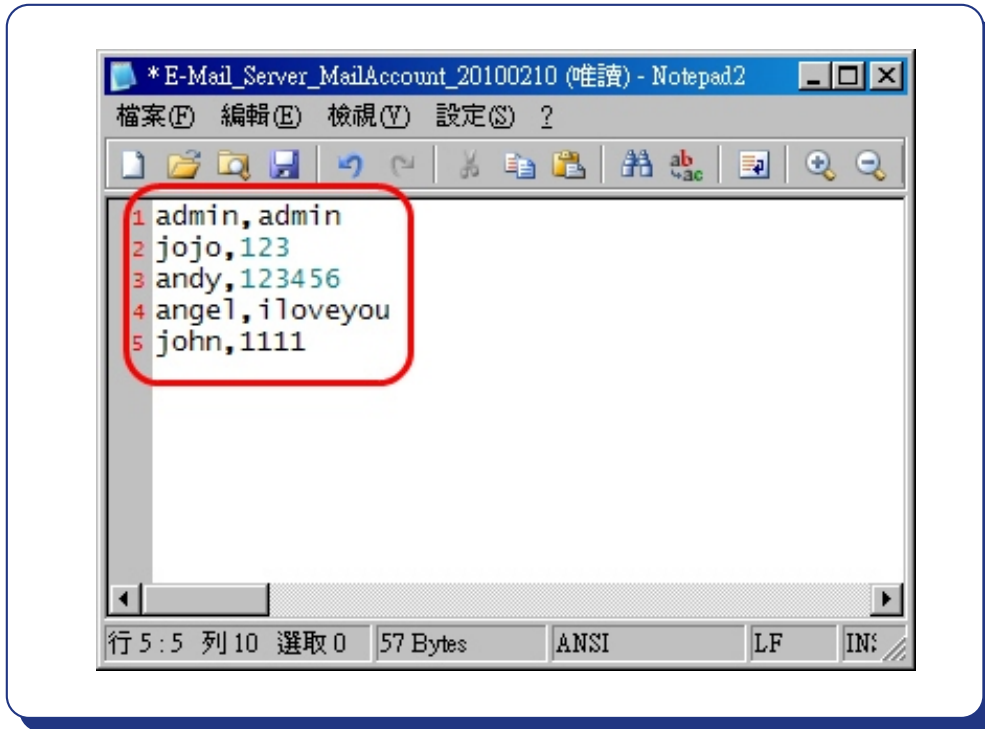
身为公司信息管理人员该如何防范才好？其实大多数的原因并不是公司内的资安设备不够力，而是不少使用者往往会因为为了在使用上方便、好记，干脆将自身信箱密码设定『123456』这类简单的懒人密码，根据统计平均每 5 人就有 1 人使用此类『懒人密码』，同时『123456』更是使用者最常使用密码的排行榜第一名。如此一来便会让使用者及公司处于高风险的环境下，相对的有心人士并不需要如何高超的技术，只要利用使用者懒惰的心态即可轻松进一步的入侵破解。

身为公司信息管理人员，辅助员工加强密码的设定以增加公司信息安全，也是首要的事情，首先必须先了解到公司内部使用者使用懒人密码的比例与密码设定的方向跟习惯，进而再来做相关的协助与教导，但管理人员又该如何利用『邮件服务器 - ML』来查阅公司内部使用者是否有密码设定不良的情况发生呢？管理人员可于『邮件服务器 - ML』的系统接口“邮件管理 > 帐号管理 > 个人”下将公司内部使用者帐号进行“汇出”动作，便可进行检查。



于 ML- 邮件管理 > 帐号管理 > 个人下汇出使用者帐号

为了有效降低公司内部信箱遭非法入侵，以防止往后不必要的损失发生，要求公司内部使用者将个人密码加强难度绝对是项必要的动作，同时相信不少管理人员在查阅过公司内部使用者所建立的账号密码后，肯定会发现内部不少使用者正是使用『懒人密码』来作为登入个人信箱的条件。所以教导使用者去了解如何正确选择、设定、更新其个人相关密码，正是管理人员的重要课题之一。



从汇出的文件查询使用者帐号密码是否过于容易破解

以下将列出几项密码管理维护所需注意之方向，以供公司或管理人员在进行对员工教育时可着重之地方，以达到有效落实加强公司内部信息安全。

### 一. 密码设定至少要达 8 个字符

密码设定过短容易遭有心人士利用辅助软件来进行排列比对破解，而效能较好的机器破解 6 个字符的密码只需两天；7 个字符的密码约 4 个月内，所以为提高密码的强度，使用者最好要达 8 个字符以上的密码较为安全。

### 二. 避免过於简单易猜测的密码

为了加强密码组合的强度，使用者尽可能的要避免掉下面几种密码设定的情况：

1. 密码和账号相同。
2. 有顺序性的数字、字母(如：123456、qwerty...)。
3. 重复性高(如：1111、aaaa、aabbcc)。
4. 使用个人生日、身份证号码。
5. 英文单字或词语(如：iloveyou、baby、honey...)。
6. 含公司、部门等公司信息。

### 三. 数字、字母、特殊符号穿插使用

字母可再配合上大小写的不同来增加破解的难度，同时加上数字与特殊符号混合使用，藉此能将使用者密码强度大大的升级。

当然，密码的设定也不需要复杂到难以记住，因为连自己都记不起来的密码组合其实也就失去其设定意义，同时还需养成良好的使用习惯，切忌将个人密码留于纸上或计算机文字文件中，以免让人容易得手。

下面则是由某知名网站百万名会员所使的懒人密码排名，由该表格可明显看出使用者于设定密码时最容易出现的问题，管理人员也可藉由此表格来针对公司内部使用密码来做相对的改善。

名次	密码	名次	密码
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

数据来源 / imperva.com

文  陈殿鸿 kim@nusoft.com.tw

## 市场营销报导 - 所有『电子邮件稽核 / 归档』需求，新软邮件服务器一次帮您搞定！！

从古至今『邮件』在商人的从商之道中一直视为重要利器，从前古人使用手写信件作为商业交易时的凭证；现代人也用电子邮件作为商业行为时的依据，所以邮件对于现代企业而言，重要性自然不可言喻。由于所有进出企业之电子邮件里所带的交易数据都算是企业商业机密，对企业而言皆属公司重要信息财产，因此『邮件稽核 / 归档』这个保护企业财产安全的概念，这几年在企业界中持续发烧。

根据统计多达九成的公司企业会透过电子邮件洽谈公司营运或是产品业务相关方面的业务，由此可见电子邮件使用的普及性和重要性，所以该如何妥善保存所有进出公司之电子邮件也成为企业不容忽视的重要问题。因此许多企业斥资添购邮件稽核 / 归档设备，主要原因不外乎是为了备份 / 稽核电子邮件，以备日后不时之需。例如：公司员工因为计算机故障导致其计算机内所有重要信件皆损毁、无法救回，这时就能利用此机制取回所有历史信件；或者配合公司政策稽查需求，定时查询稽核员工邮件是否泄密...等等需求。

新软系统产品设计理念皆以“市场需求、未来走向”为设计目标，功能多符合现代企业需求考虑，站在使用者角度所推出来的『新软系统邮件服务器 - ML 系列』，内『邮件稽核 / 归档』功能以多项强大的功能特性协助企业完成邮件稽核 / 归档之需求：

### ● 归档邮件的多向化查询方法

为了从满坑满谷的归档邮件堆里找出自己所想找的那封信，若一封一封信来找必然是费工又耗时。新软系统邮件服务器 - ML 系列里内建之邮件稽核归档机制以（寄件者 / 收件者 / 有无附加档 / 附加档档名 / 信件主旨 / 件内文关键词 / 信件收送处理方式）等多项搜寻条件来协助管理者快速找出所想要查询的信件，功能非常快速方便。

### ● 高效率的稽核机制

想要有效防范泄密事件发生，除了做事后举证以外，最好的方式当然为『事前防范』；因此新软邮件服务器推出『邮件稽核』功能，此功能着重于“事前稽核”，可由网管人员依公司政策自行设定相关邮件稽核规则（删除 / 审查 / 延迟 / 传送 / 复制）并可设定多条规则交互使用（必须符合所有规则 / 符合其一规则即可）只要有员工寄送触犯公司所设定的规则的信件，将会自动拦阻下来或者转送交由网管人员知晓，藉此能有效降低企业泄密事件发生。





- 归档邮件有效管理

倘若有员工因为计算机故障损毁导致其里头重要信件遗失的话，此问题可由管理人员搜寻出所有目标信件后，可依照任务需求做相关邮件处置（**信件取回 / 信件重送 / 信件删除**），因此可将所搜寻出来的历史信件全部取回给该名员工，便可以达成『邮件归档』之目标。另外，若像公司政策需求必须定期查询稽核员工信件的话，也可以依照搜寻规则做目标信件搜寻。


- 远程备份归档邮件

市场上许多邮件归档设备在邮件归档后会存置于其本机硬盘内，且这些数据很多都是不常读取之数据，然而企业归档信件存放期限绝不止仅短短的两三年，例如：因应沙宾法案内容要求，有些企业因为行业性质不同，在邮件归档存放期限上至少要求得存放 7 年以上，因此一般邮件归档的本机硬盘空间是无法长时间供应作为邮件存放的设备。在此，新软邮件服务器提供企业用户『远程备份』的机制，可以将归档邮件通通转存备份于远程服务器中（**NAS、File Server、SAMBA Server**）；如此一来，依靠远程服务器“长期存放”的特性，便可妥善保存重要信件数据，更不必担心信件数据是否会因为空间不够而必须删除其它信件来腾出硬盘空间的问题存在。

- 硬件软件 All In One

一般来说，邮件服务器以及邮件归档设备分属两台不同的硬设备；因此就软件功能而言，两种设备若为不同厂牌时，网管人员将得学习两套操作方式，着实麻烦；若就硬件成本来看，两台设备就得花更多经费来采购，且现在市场上的邮件归档设备大多价格昂贵，对于中小企业而言，将是一项不小的预算问题。于此，新软系统邮件服务器，除了本身的邮件服务器功能之外，也将邮件稽核 / 归档功能建置于其中，让所有功能 **All In One**，使网管人员无需分别学习两台设备不同的操作方式，也使企业节省一大笔采购预算。

对企业而言，『邮件稽核 / 归档机制的严谨度代表着企业资安防护的完整度』，因此新软系统邮件服务器 - **ML** 系列所推出之邮件稽核 / 归档机制力求稽核 / 归档所有邮件都力求能达到“滴水不漏”的目标，藉此能够给企业用户安全的信息财产保护。

文  黄政铭 [ming@nusoft.com.tw](mailto:ming@nusoft.com.tw)