**Mail Archiving Expert**

# MAE 电子邮件归档专家

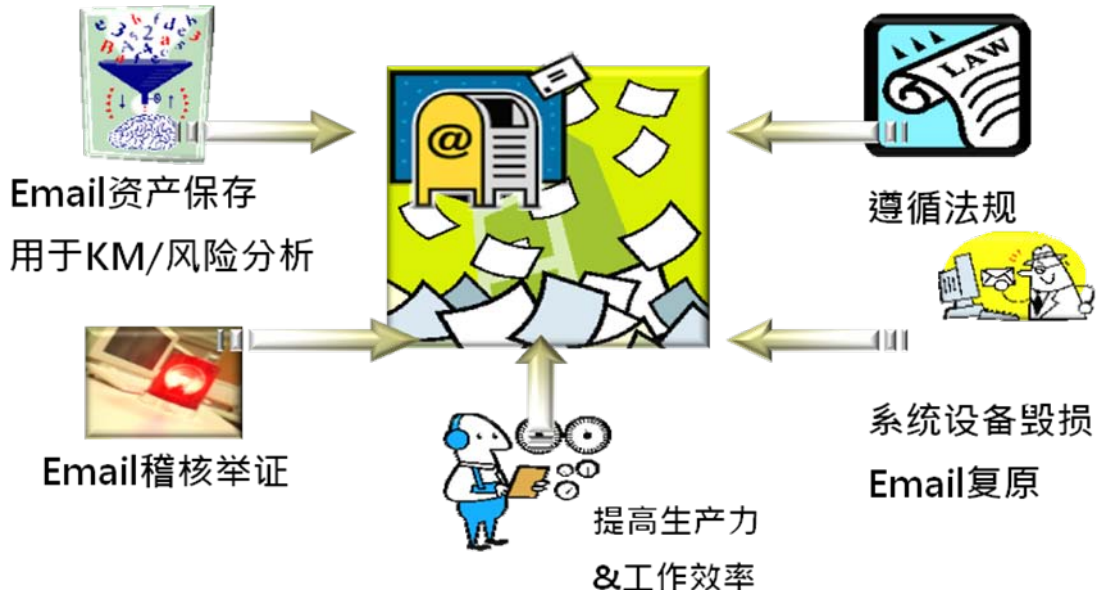
---

## 产品白皮书

# 目录

# 1、为何需要建立电子邮件归档机制？

电子邮件已成为现代人生活不可或缺的联络及沟通管道，对于企业而言，更是常常通过电子邮件对内传达讯息以及从事对外商业交涉，因此电子邮件机制俨然已经成为企业正式文件的传递管道。然而，我们对于邮件良好的备存处理，常常不经易地忽略，对于企业而言，短时间虽然感觉不到，但长期来看会有一定程度的影响，因此希望通过本白皮书，能增进用户对电子邮件归档更多一点的认识。




以下为电子邮件归档机制的必要性说明：

## 1. 建立电子邮件归档机制将有助于电子邮件稽核举证

近年来因企业内部信息安全事件以及商业犯罪事件频传，常常会听到某科技大厂内部员工将重要的智能财产通过电子邮件夹带附件的方式提供给竞争对手，亦或是内部员工将内部极机密之商业营运数据外泄等事件，可以想见稽核机制的建立是相当必要的，然而检调单位在搜寻任何的犯罪线索时，电子邮件纪录常被视为一项重要关键性证据之丨，虽然不见得直接找到犯罪证

据，但是仍然可以通过电子邮件沟通的过程中找到蛛丝马迹，如此一来，电子邮件归档机制的建立将会提升企业营运的安全性。

## 2. 建立电子邮件归档机制将有助于知识管理与风险分析

电子邮件传达的不仅仅是电子邮件本身，其也间接联系了人与人之间的关系，以及提高知识智能的共享性。对企业而言，除了知识管理之外，风险的分析也相当重要。通过健全的电子邮件归档机制，可以将电子邮件中的菁华加以分类、搜集以及整理，企业内的每个员工，可以轻松通过简易的搜寻，即可找到他所想要的、并且有帮助的信息。

另外从风险分析的角度来看，通过良好的电子邮件归档机制，可以从日常的电子邮件流量中得知邮件服务器的承载，以及早做好因应。除了一般公司内部的稽核单位外，每个单位也应有专人负责该单位人员的邮件使用状况，了解是否有人利用公司的资源发送大量信件占用带宽，或者是有人利用公司资源遂行私人之行为，再者业务的报价是否确保公司的权益，以上事件发生后是否有实时反馈机制等，这些都应该藉由良好的电子邮件归档机制，以确保公司权益。

## 3. 建立电子邮件归档机制将有助于遵循法规的要求

除了以上从企业内外部稽核管理的角度来看，企业目前最常面临到的乃为法规的稽核。在这些法规中，最常听到的莫过于美国沙宾法案。2002 年美国由于安隆案的发生，造成投资人信心大失，对企业所公布的财报也表达不信任之态度，因而对经济造成重大的影响！因此为挽回投资大众的信心，因此便颁布了美国沙宾法案，希望通过财务报表的透明及业务分权制度的建立，挽回大众的信心，其中针对电子纪录(含邮件)的要求更是明确，一般资料要保留五年，跟会计、财务相关的电子纪录必须要保留七年。然而除了要确实做好归档之外，还要配合外部稽核单位的调阅纪录需求，必须要在规定的时间之内，调阅到符合稽核单位需求的信件，否则将会处以罚则。虽然在台湾未曾听过开铡的案例，不过许多与欧美日合作的台湾企业，在合作前也常常被

要求必须符合法规的规范，此讯息国内企业将不可不知。因此为了调阅的方便性，应建立可自行设定归档政策的机制，以因应未来稽核单位调阅电子邮件纪录的需求。

## 4. 建立电子邮件归档机制将有助于达成信息生命周期

电子邮件归档的另一重要目的，乃希望能完成信息生命周期(ILM)。然而在进行周期前，必须对电子邮件的数据重要性、类型、档案大小、储存年限等等有所定义。定义之后，将可规划将电子邮件依其特性规划储存在高级储存设备(storage)、磁带机以及以 DVD-ROM 的形式储存。另外若是配合法规的要求，则可针对特定类型的电子邮件，依年限的规定储存，当年限一到，便可自动执行搬移的动作，如果需要执行调阅电子邮件纪录，也能很快达到需求。以上的机制如果能妥善运作，将会对企业在储存资源以及电子邮件纪录的活用上相当大的帮助。

# 2、从数据外泄延伸法规遵循的应用与规划

进入 21 世纪后，全世界高科技的蓬勃发展相当迅速，因特网的全方面应用更超出一般人的想象。然而，当全世界均处在一股因特网的便利所带来的热潮时，却有些许人心怀不轨，想藉由如此便利的沟通管道遂行非法之行为。除了一般常见的黑客入侵、计算机中毒之外，最常见也最难预防的即是内部数据外泄。

数据的本身是否具有机密性，得视该数据对该企业的影响程度而定，然而就企业竞争力以及营运影响而言，任何跟公司有关的资料通过非法的管道外泄至他人手上，均可能隐藏着潜在危机。

我国营业秘密法第二条规定：「本法所称营业秘密法，系指方法、技术、制程、配方、程序、设计或其他可用于生产、销售或经营之信息，而符合左列要件者：一、非一般涉及该类信息之人所知者。二、因其秘密性而具有实际或潜在之经济价值者。三、所有人已采取合理之保密措施者。」在上述的法条中清楚表示，若并非所有人都已采取合理的保密措施，则即便是公司自认为很重要的信息或是数据，亦非以营业秘密视之，此点对企业非常重要，因为它已指出，当企业资料外泄的事件发生后，若该企业在事件发生前并无针对该企业内部数据进行控管及保护，则可不用以机密数据外泄角度而定，因此企业必须立即着手规划针对内部数据控管及保护的解决方案。

一般在企业之间的联络方式，除了传统以电话及传真联系之外，使用最多的当属电子邮件(E-mail)。电子邮件的使用也已经成为犯罪的温床。以电子邮件、实时通讯来传递机密文件或是业务数据，可能会为公司带来潜藏的危机。如何安全地传递电子邮件，已成为信息部门不容忽视的课题。虽然计算机黑

客常对电子邮件造成威胁，但是最大的安全问题常常出于企业内部员工，特别是员工通过因特网上传送机密讯息时，可能因故意或过失而使机密数据外泄，造成公司的损失。据一位不愿具名的高科技高级主管表示：「之前曾耳闻有竞争厂商欲对我们公司进行激烈之手段，但并未亲眼目睹，待新闻媒体报导半导体大厂因研发专利互告的新闻不断上演后，我们也决定加强邮件安全的稽核与备份机制，遂赫然发现的确有内部员工以电子邮件的方式正和竞争对手洽谈个研发团队跳槽的事宜，因此便实时将不法员工解雇，也将企业机密资料及时救了回来。」由此可见邮件安全保护的重要。

有些企业为了防止员工将机密数据外泄，采取监视员工电子邮件的方式，但此会将会引发是否侵犯隐私权的争议。也有些公司行号要求员工在传送电子邮件之前，先将数据加密，但若加密运用不当，反而会对公司造成伤害。因为法律原则上禁止发信人与收信人以外之其他任何人窃听、存取或揭示电子邮件的内容。但有以下两种例外：一、事先征得员工的同意，二、或因执行公事所需。若有以上任一种情形时，则雇主可以监视员工的电子邮件。所谓「因执行公事所需」是指，即使雇主事先并未征得员工的同意，但因公事所需，亦可监视员工的电子邮件，且无须告知员工。但须注意的是，雇主之监视必须在一般正常的公事范围内，而且其所监视之通信内容的主题，需符合雇主的合法利益才可以。

若公司制订一清楚明确的电子邮件安全规定，言明公司将会监视员工的电子邮件或 IM 通讯内容，并将之充分告知员工，取得员工的同意书，则可使员工对于电子邮件隐私权之期待降低。如此，便可减少员工与公司的诉讼。即使一旦涉讼，公司亦会取得较有利的诉讼位置。

目前企业在执行信息安全的防护上隐藏着某些不妥之处：

企业机密数据的外流风险，来自于内部拥有数据合法访问权限者，也就是合法存取却非法使用的人员。身分认证与访问权限的设计是最初的基本工作，但仅以单纯的访问权限控管作为数据保护措施，是绝对无法防范预谋不轨的不肖员工。

受害企业在员工泄漏数据的 2 年间，信息部门竟未去调阅系统数据是否有异常存取的 log 纪录，可见在稽核管理制度上出现瑕疵。若稍有警觉，在怀疑数据外流的第一时间应立即比对系统存取 log 文件与邮件外送备份资料，应可更早发现资料外流的问题，也不至于造成偌大的损失。

国内的内部信息安全政策虽然也有某些产业提出「美国沙宾法案」、「个人资产保护法」等相关规范的法条，但实际上台湾企业不见得会马上遵循。往往都是因与其他国家的企业合作时对方所提出的要求，我们才可能会因此遵循。不过经过信息安全事件层出不穷的推波助澜以及政府的鼓吹教育之后，针对邮件安全稽核及备份管理的部分应会逐渐自我要求，并导入适宜的解决方案。

# 3、邮件归档的整体考虑

邮件良好的归档管理，常常会不经易地被忽略，但对于企业而言，短时间虽然感觉不到，但长期来看会有一定程度的影响，尤其是当企业愿意开始着手进行邮件归档的规划，未来一定会碰到储存空间规划的问题，但除了储存空间规划之外，分权管理的问题其实也经常发生。本段乃针对电子邮件归档与空间规划、分权管理作以下说明：

## 1. 企业最常碰到的邮件归档原因为何？

就经验来看，企业会决定开始进行邮件归档往往有几个原因，无非是作未来发生商业纠纷时可能的举证，亦或是当邮件服务器或是个人端的邮件信箱出现问题时，尚可将预先备存的信件作复原及取回的动作。这是一般企业最常遇到的情况。法规的强制性尚且不足，因此除非需要在美国上市，或是与欧美企业有生意往来，才有可能因此而必须遵循法规。

然而，因为近来国内政府针对企业、金控机构进行内部稽核的动作，导致许多企业及金融机构人心惶惶，也因此将邮件归档机制纳入成为必须实施的方向。

## 2. 「邮件归档」与「邮件备份」有何不同？

许多人常把「邮件归档」与「邮件备份」搞混，其实两者是不太一样的。企业其实平日均已针对邮件的部份做备份，一般备份做法往往将所有信件包含系统备成一大包，再将此备份文件备至磁带区备存。如果真的遇到要调阅历史信件的状况，会出现需要花费许多时间来寻找邮件的情况，如此可能会因为耗费时间而失去了商机或其他不利的情况。

然而，如果平日作的不只是「邮件备份」，而采用的是「邮件归档」的方式，则结果就不太一样了，原因是「邮件归档」的定义可以比喻为图书馆藏书，书籍上架之前会先依书籍性质作分类，如此未来在调阅时就可以轻松找

到想要的书。同理可证，如果将邮件性质定义后做邮件分类，如此一来无论是要找老板的信，或是稽核单位的信，甚至个人自行取信，都将因为有事先做分类，在未来调阅信件或取信时都会显得相当轻松。

### 3. 邮件归档的近线归档适合什么样的储存设备？建议在线备存多久呢？

何种储存设备较为适合？是根据企业或是机关单位本身的需求而定，在邮件归档中比较建议在归档前先针对该档案作定义，一般的定义是较重要的邮件数据摆在较高档的储存设备，较不重要的可以选择较低阶的储存设备或是刻成光盘储存。

在实际与客户的互动经验中发现烧成光盘储存的机会比较少见，一般都是采用 storage(磁盘驱动器)与 tape(磁带)作储存。不过如果要从磁带机上调数据，首先当然必须要知道数据放在哪一卷，如果数据较久远的话，通常只是大略猜测放在哪几卷，再将磁带中的数据倒回至某一个磁盘驱动器的空间中，再从该空间中找寻想要的数据，过程相当繁复。然而由于磁盘驱动器(storage)技术提升迅速，价格也因竞争越趋白热化而逐步下跌，新的邮件调阅技术中已经可以做到直接将 storage 上的空间挂载之后，直接调阅该信并将信取回，此作法比较起来比前一个方式快速且方便许多。

至于信件要备存多久，则端看公司策略而定，以及实际的每日平均信件量而定，如果每日信件量平均有 10G，每个月就大致需要 300G，如果希望在线(on line)保存半年的话，大致上就需要规划 2TB 的容量，以此类推。

### 4. 分权管理的必要性：

当储存数据的定义以及 storage 的导入完成后，一般管理员就会开始询问并说明分权管理的必要性及重要性，因为每个部门都不希望让其他部门了解该部门之邮件精华，除此之外也会出现某些主管希望能得知该部门信件的状况，甚至老板也不希望管理员能看到其信件等各式各样的状况，由此可见分权管理将会是企业导入邮件归档建购之后所必定会面对到的难题。

从以上几点说明，可以清楚了解电子邮件归档与储存空间规划的重要性，

以及分权管理的必要性，但是只有了解而没有后续的执行，也等于是功亏一篑。因此平常便必须养成定期归档的好习惯，当然也要时常观察储存设备的运作状态，避免出现当机或出现异常之状况。其实对企业而言，无论是业务所需或是应付法规稽核，只要平常准备得宜，就可以不用担心面对突发状况。对个人而言，如果遇到个人的信箱出现状况，也能将邮件重新取回，达成灾后复原的目的。重新检视内部需求，订定合适且高效率的电子邮件归档政策及规划兼具高效能及高稳定性的储存设备。

# 4、建立安全无虞的邮件归档机制及储存空间规划

许多管理员对「邮件归档」大致上都有一些概念，但是对于后续的执行却存在着许多疑问，因为他们知道「邮件归档」这四个字不仅仅只是单纯将信件备份，而是还要思考后续所有调阅的可能，因此在整体空间的规划以及历史邮件的归档，执行上的负担相当大，通常在每年的信息需求计划上虽然都会提出，但是往往又会被忽略掉，或是延后执行，由此可见其棘手程度。特别是历史邮件归档及调阅的部份，无论是使用 Exchange 或是 Lotus Notes 的企业，对于历史邮件的归档调阅，都认为相当困扰。由于大部分的企业都认为储存空间(storage)的费用目前仍是稍高，因此便利用其来执行较高级的使用，但相对于邮件归档的认知，便不是那么重视，尤其是历史邮件，最常见的处理方式不是利用磁带备份，便是利用 DVD 光驱刻录，备份的问题固然可以解决，但是一旦需要执行邮件调阅，如果没有事先做好索引，绝对需要耗费相当多的时间。

传统邮件归档方式如下图；

一般用户对于邮件归档的空间规划经验普遍是比较缺乏的，所以经常都会希望倚重专业的规划建议。一般用户必须提供实际的每日邮件的流量大小，包括内收信、外送信以及内部对内部的信件流量，之后才能再作进一步的空间规划计算，举例如下：

**所需空间建议**

一天以 30 万笔记录计算，每笔 200 Bit ( Inbound 50,000 笔 /Outbound 50,000 笔 / 内部信 200,000 笔)

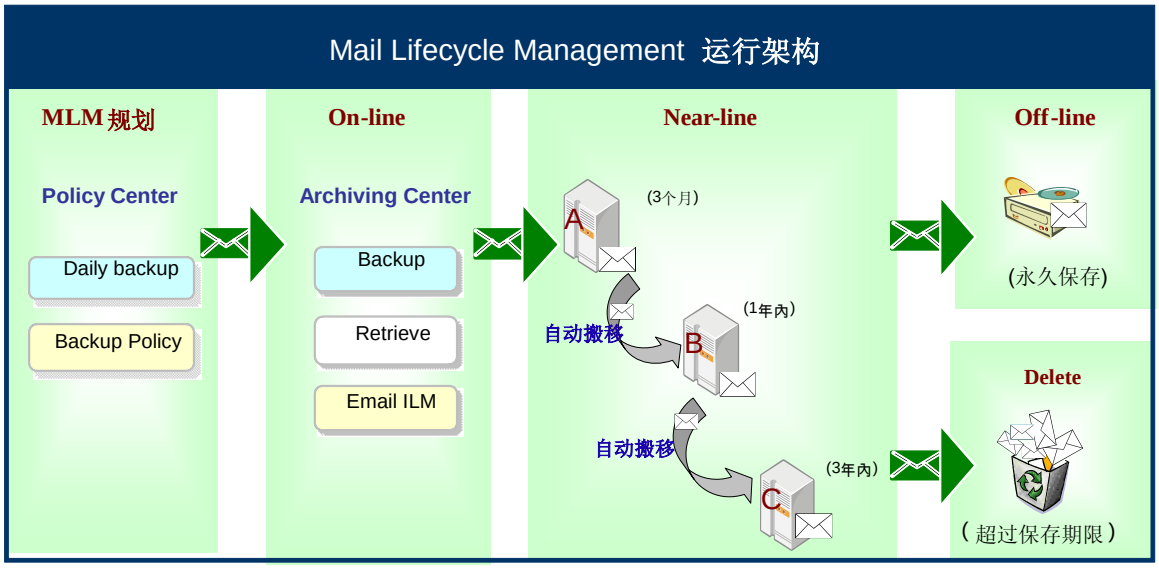
| 时间 \ 所需空间 | 邮件记录 | EML 实体(GB) | 建议空间 |
|---|---|---|---|
| 一天所需空间 | 7.15 MB | 30 GB | 30 GB |
| 一个月所需空间 | 215 MB | 900 GB | 1 TB |
| 一年所需空间 | 2.6 GB | 10,800 GB | 12 TB |
| 五年所需空间(不含成长预估) | 13 GB | 54 TB | 60 TB |

如果有以上的资料，如此就很容易可以估算出来实际需要多少的空间。然而实务上的空间规划可以从需求中找出几个面向来看：

1.遵循法规的空间规划：一般在法规的要求中，财务相关的数字文件需要保留七年，一般的数据需要保留五年，故若有跟法规遵循议题相关的客户可以依此来规划储存空间。然而因为法规的归档年限要求较长，所以一般会这样规划储存装置：SAN(一年内)→NAS(三年内)→Tape 或 DVD(三年以上)

2.一般企业内部需求的空间规划：一般企业的规划可以依邮件的调阅频率以及使用程度来做规划，就经验来看一般企业其实仅会针对三年内的邮件做备存，所以我们从预算及效能来做规划考虑，如果是大于 500 个员工账号以上的企业，建议采用 SAN storage 来做邮件备存，如果是 300~500 个员工账号的企业，建议其使用 Disk Array 的储存装置，至于 300 个员工邮件账号的企业，则会以 NAS 设备为优先考虑规划的储存装置，而空间大小则会建议规划 3TB，之后再视情况予以调整。

3.备份后的调阅速度跟储存装置有很大的关连性：企业往往会面临到预算与空间规划的挣扎，因为预算不够就没有办法购买较高速的 storage，转而藉由光盘或磁带来做备份，可是如果有紧急的调阅需求的话，这样子的备份选择其实不是理想的方式，常常会发现客户因为有专利权纠纷而需要提出证据作为左证时，调阅邮件时效拖的太久反而会有损企业在宝贵第一时间的反应，所以一般认为仍然必须要使用到 NAS 以上的储存装置做为媒介才有机会缩短调阅时间，但如果真的因为预算的关系会影响到储存空间的规划，则可以规划每个 user 定期的归档邮件期限，例如说限制公司仅备份每个 user 一年内的信件，如果超过这个期限则由系统自动删除，这样对企业而言也可以同时解决空间以及预算的问题，不过要注意的当然有可能调阅不到历史较久远的邮件本体，这是必须要去思考的。




4.而「邮件归档」除了执行上述的备份因应之外，其实尚有一个需求，乃来自于稽核部人员。稽核部人员在工作职责上，无非就是确实的掌控所有可能出现对有损公司利益的任何要件，当然，这几年来通过邮件可能造成的机密外泄事件，已成为稽核部人员在作内部稽核时的重要工作。有鉴于此，如何协助稽核部人员确实掌握进出公司或者是内部的交换邮件的详细状况，也是管理员的重要任务与职责所在。


流量报表2009-06-09
(统计数据最近更新时间：2009-06-11 00:00:10) 立即更新
时间区间
前一条
后一笔
搜寻
流量图表
输出
群组
外寄邮件
内收邮件
内部邮件
产品技术部
0 (封) 0 (KB)
0 (封) 0 (KB)
12 (封) 140 (KB)
人员
外寄邮件
内收邮件
内部邮件
cuiraciy ▸ raciy.cui@softsqr.com.cn
0 (封) 0 (KB)
0 (封) 0 (KB)
6 (封) 70 (KB)
jujessy ▸ jessy.ju@softsqr.com.cn
0 (封) 0 (KB)
0 (封) 0 (KB)
3 (封) 35 (KB)
wumichael ▸ michael.wu@softsqr.com
0 (封) 0 (KB)
0 (封) 0 (KB)
3 (封) 35 (KB)
Mail Archiving Expert - Windows Internet Explorer
http://192.168.50.20/snmsqr/mail_static/mbr_log.asp?mbrmail=raciy.cui%40softsqr.com.cn&sqlc=ZGF0ZXM9JzIwMDktMDYtMDkn&orgmail=%3Craciy.cui%40
raciy.cui@softsqr.com.cn 个人邮件明细(统计数据最近更新时间：2009-06-11 00:00:10)
第 1 页/共 1 页( 共 13 条记录 )
导出
邮件处理状态
日期
寄件人
收件人
主题
附件文件名
大小
发送 IP
备份名
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: 关于美... 3 by exchange... 143821002....
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: 智航防毒 5 by exchange... 143821001....
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: 多种收... 4 by exchange... 143820001....
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: 测试密... 5 by exchange... 143819001....
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: 测试密... 3 by exchange... 143803001....
邮件复制 2009-06-09 jessy.ju@sof... raciy.cui@so... 答复: test 3 by exchange... 143802001....
邮件复制 2009-06-09 raciy.cui@so... jessy.ju@sof... test 2 by exchange... 141959001....

# 5、电子邮件稽核的重要性

## 1. 电子邮件稽核的原因为何？

企业执行稽核的原因相当多，但还是可以归纳出几个重点因素：

(1)法规遵循：首先最常听到的还是法规要求的部份。实际上，法规的要求从2002 年的美国安隆案发生后制定的「沙宾法案」开始至今，一连串无数的法案应运而生，无非就是希望上市柜企业的财务相关资料能够诚实公开，对广大的投资大众能有所交代。另外还有金融业的「新巴塞尔资本协议」、医疗公共卫生的「HIPPA 法案」等均是针对重点文件公开及备存。另外日本也针对本国上市柜企业以及业务范围内第三方公开要求必须遵守「J-SOX，日本沙宾法案」，同样是要求企业公正公开相关财务信息。至于我国的政府机关，也逐渐开始要求所有机关必须依其所属机关资安等级规定执行相关信息安全实施及措施。最近行政院也颁布「电子邮件安全参考索引」，内容也提及各级政府机关必须针对电子邮件安全机制的部份进行加强及督导，防止非属该应有权限的人员任意使用电子邮件进行不法之行为。由此可见，无论是企业或是政府机关，也纷纷准备搭上电子邮件稽核的列车。

(2)企业机密安全所需：上述虽提及许多关于法规的规定，从稽核的角度来看，其实是比较偏「事后稽核」。然而对于国内的企业及政府机关而言，其实实际状况是不同的。先就政府机关来说，安全的要求程度较企业来的低，因此对于电子邮件实时稽核的兴致不高。至于一般企业的状况就完全不同了，因为企业商业内部机密外泄情况相当严重，因此对于电子邮件的使用相对要求较严，因此电子邮件实时稽核的需求相当多，甚至曾经遇过用户要求所有的信件在到外部前先通过电子邮件安全设备将信留在审核区，再由稽核人员作后续邮件的处理，这种情况在企业里是比较常见的。

(3)合作伙伴要求：国内企业与全世界的企业一向接触及合作相当频繁，在海

外对信息安全观念较国内成熟的情况之下，往往在合作前会被要求强化信息安全等相关机制，尤其是电子邮件的实时稽核，有很多的海外订单或报价都是通过电子邮件的夹带寄送，因为电子邮件已成为商业不可或缺的沟通管道。(4)自我提升企业形象：某些企业会通过信息安全防护网的建构，藉以彰显企业在安全上是相当重视的，尤其营业内容是跟交易服务相关的，例如银行、证券、保险等机构。

## 2. 电子邮件稽核最常用在哪些地方？

其实电子邮件稽核的导入及运作与企业所属业种性质有关，大多数乃会针对其日常业务性质而作定义。例如：

**金融业**—所有的作业都需要进行两道认证手续才得以执行，有效保障日常作业流程安全并保护个人资料外泄。

**法律事务所**—所有的电子邮件均须主动另外寄送一份给高级主管，除了确保案件状况之外，对所内律师相关案件的均时时掌握。

**证券业**—因为所有的交易凭证均是通过电子邮件夹带寄送，因此证券业常见做法则是将所有跟交易凭证相关的信件都需要主管看过之后再允许寄出。

**医疗业**—医疗机关最担心病人数据外漏，因为可能会带来医疗纠纷，因此医疗业会针对跟病人相关的交谈及互动过程，尤其是病历数据，如果有符合上述所提的相关信件，都会暂时交由稽核单位或是单位主管了解之后才允许寄出。

**制造业**—中国制造业表现在全世界经常名列前矛，也申请了无数多的专利，但是由于竞争激烈，因此想见的是商业间谍无所不在，尤其最难掌握的反而是自己企业的员工，因此国内的制造业用户常会针对特定业务性质的员工信件做管控及稽核，尤其是研发及业务部门，无论是夹带研发设计数据或是业务相关报价的信件，均会由稽核人员审核后才能顺利往外寄送。

以上几个范例，均是针对比较常见的「实时稽核」的处理方法，但事实上在国内的大多数企业或是政府机关，可能因内部政策尚未确定以及执行较困

难，往往都会选择「事后稽核」的方式在过程中比较没有那么复杂，其实在实务上，两种方式若都能并行，对企业或是政府机关的内部机密外泄的情况应该能有效遏止。

### 3. 电子邮件稽核的相关权责分工？

在组织里负责稽核业务承办的，常常是企业或政府机关常设的稽核人员，但若是针对电子邮件稽核的部份，可能在权责及定义上可能就不会只有常设的稽核人员来负责，而也有可能交由每个单位的部门主管来负责管理该部门的邮件状况。我们往往也会遇到某种情况，企业高级主管希望系统管理部门规划电子邮件稽核机制，但同时也希望系统管理员没有调阅或读取该邮件的权限，或者是说对读取该邮件的相关执行行动留下纪录，这都是在导入电子邮件稽核流程中常见的状况。

### 4. 电子邮件稽核未来必须努力的方向：

电子邮件稽核是个必须执行，也可能走不完的一趟旅程，毕竟随着企业或政府机关组织文化不断随着社会需求而变动，稽核的内容以及方式也随着科技的演变而有所不同。未来的电子邮件稽核也许也会因法规的要求，而在水平及垂直组织的权责定义上更加明确。然而无论稽核方式如何改变，不会变的还是电子邮件稽核的精神，但迎面而来的，也可能是来自于用户的反抗。

因此无论是外部环境的变迁或是内部环境调整的影响，稽核部门任务的重要性与数年前的情况已不能同日而语，因为全世界无论大小产业都必须承受着一定程度的风险及抗衡，故任何牵涉影响到企业重要权益的机会都必须加以排除，将企业的风险安全程度提升到最大值。在电子邮件的使用程度已达到企业与企业之间讯息交换的极致时，相关的重要讯息的确是必须加以保护的。

# 6、经典案例分享

**1.金融机关：**

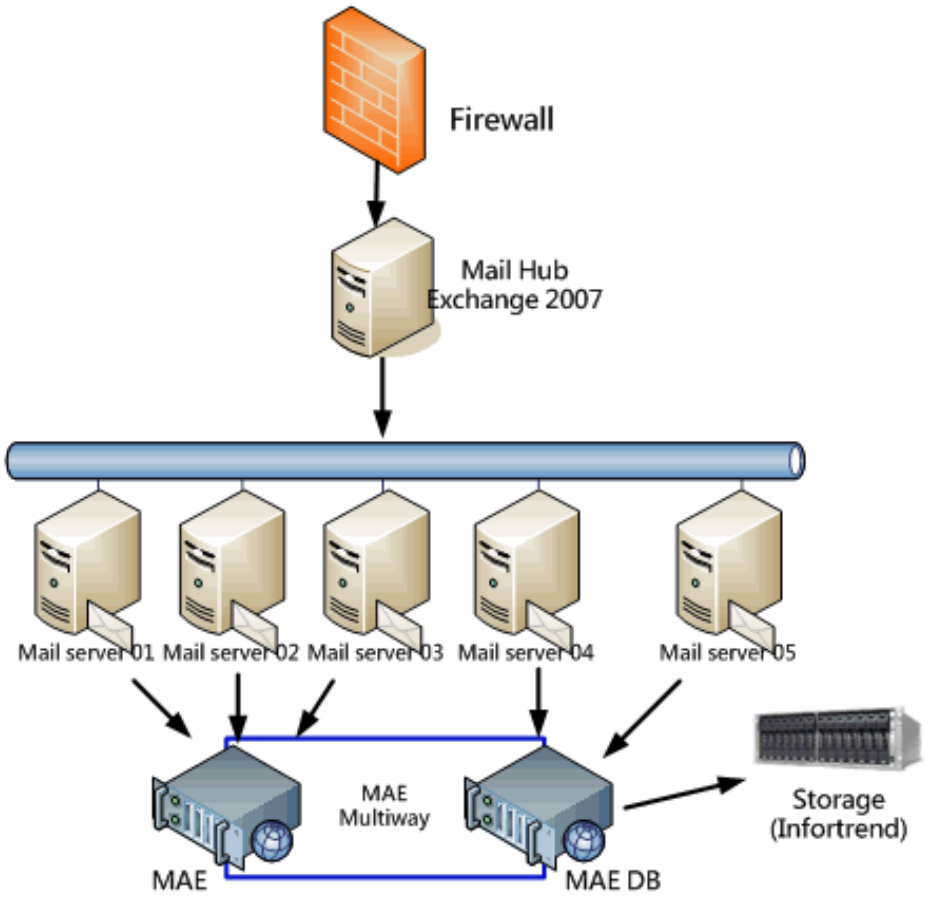
环境：Exchange2007*7

用户数：6000

导入原因：公司内部上级要求必须将全公司的邮件加以备存，以应未来调阅需求

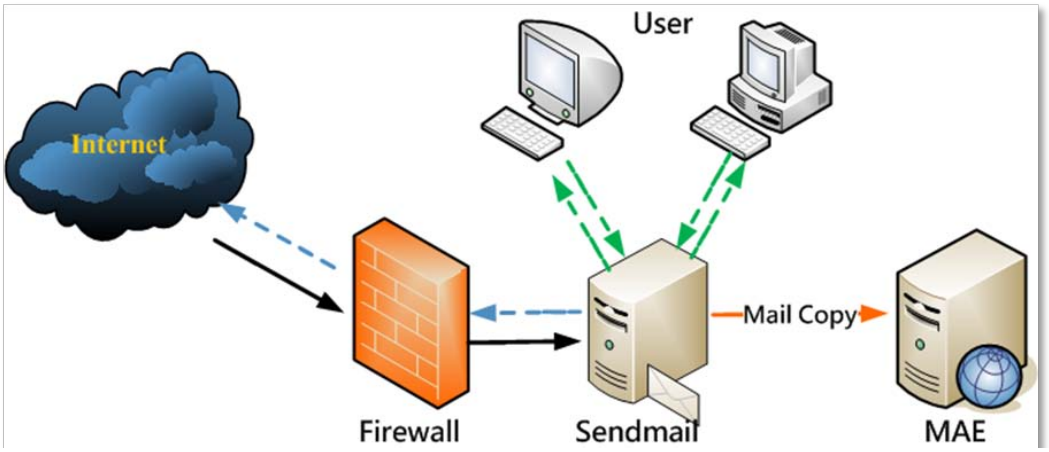
特别说明：客户端为 MAE 异地 multiway 架构，两台 MAE 分工收所有 mail server 的信后，再进行同步。在 MAE DB 上可以调阅到所有的邮件

储存规划(39TB)：预定保留三年内的邮件，视实际邮件备存量再调整空间。




统一界面可调阅邮件。

2.某法律事务所：




用户背景说明:

1. 国内知名大型国际专利法律事务所
2. 邮件服务器为 Sendmail

问题说明:

1. Sendmail 上设定邮件政策,当天的信会自动转寄到领导的信箱
2. 没有办法快速调阅到已备份至磁带上的邮件
3. Sendmail 上的设定条件有限制且操作不易,因此希望有较易使用的产品取代 Sendmail 的管理设定

导入架构说明:

1. In / Outbound /内部信到 Sendmail 时,会即时进行 Mail Copy 至 MAE
2. 在 MAE 上设定转寄邮件时自动 BCC 给指定管理者,以防止机密外泄行为发生
3. 管理者可至 MAE 的界面上查询调阅所有的邮件记录

# 7、结论

从以上几点说明，我们可以清楚了解电子邮件归档的重要性及必要性，但是只有了解而没有后续的执行，也等于是功亏一篑。因此无论是企业亦或是个人，在日常生活中便必须养成定期归档的好习惯，对企业而言，无论是业务所需或是应付法规稽核，只要平常准备得宜，就可以不用担心面对突发状况。对个人而言，如果遇到个人的信箱出现状况，也能将邮件重新取回，达成灾后复原的目的。希望各位管理员能重新检视需求，订定合适且高效率的电子邮件归档政策。而相信在未来的企业及各机关，针对邮件安全管理与备份机制应该至少会有以下几项规定：

1.定期做好邮件备份，并将备份下来的邮件依单位或机密程度依年份管理。

2.不定期做邮件稽核，针对可疑信件做注记并加以观察。

3.定期检视企业内部信息安全政策，是否在执行内容上有需要再做调整，以因应瞬息万变的信息化环境。