

## 网络记录器 / IR 系列报导

### 技术浅谈与应用 - HTTP 网页浏览、文件上传下载及网络布告栏 PO 文『全都录』

网络虽然带给企业相当便捷的联络管道，但同时也提供了企业旗下员工网络摸鱼的最佳途径。为杜绝此网络摸鱼歪风盛行，除了透过公司的网络使用政策来倡导警告外，最根本的办法就是透过安装网络侧录设备来监督员工的网络使用情况。一般来说，企业员工的网络摸鱼行为除了实时通讯聊天与收发私人电子邮件之外，最多最严重的莫过于透过「HTTP」服务来消磨时间。

为什么上段叙述的是「HTTP」，而不是「浏览网页」呢？其实，企业员工透过「HTTP」服务来打混摸鱼的花招可多着呢！除了大家常见的「网页浏览」外，还经常用来下载 MP3、MPEG、AVI 等影音文件，以及聊天室聊天、部落格留言、网络拍卖交易...。这么多样化的网络摸鱼行为，坊间一般网络侧录设备却只能单纯记录员工所浏览的网页 URL 路径，最多也只多条浏览时间的记录，如此的简陋记录功能对于企业来说根本就不敷使用，MIS 人员欲追查也会无所适从。

新软系统针对一般使用者使用「HTTP」这项服务的习惯，于网络记录器（IR 系列产品）上特别详细记录－「网页浏览」、「HTTP 下载、上传文件」、「网页布告栏发表文章」

#### 『网页浏览』－

新软 IR 产品不仅可记录员工浏览网站的时间外，也能把网站的「完整 URL 路径」与「网页名称（Title）」清楚地记录下来。特别的是，连网页上所有的内容（包含图片、文字、连结等信息）也能如同拍照般巨细靡遗的记录下来，未来网管人员只要點選 IR 上的 HTTP 浏览记录，即可清楚地看见网页的所有信息。



【图一】IR 所记录的 HTTP 完整网页信息

## 『HTTP下载、上传文件』 —

一般使用者的下载、上传文件动作除了透过 FTP、P2P 等传输软件外，最常见的莫过于 HTTP 了。透过 IR 的 HTTP 记录功能，只要员工从网页下载文件（安装程序、压缩文件、图片、MP3...）或是将文件上传至网页（网页电子贺卡、部落格制作...），IR 都能将所上传下载的文件名称、来源路径完整记录下来，并在 IR 的管理接口上标明传送方向。如此一来，网管人员不仅可得知员工从哪里下载文件或是将文件上传到何处，如欲查看文件内容也可透过点取文件记录的方式来查阅，相当方便及人性化。

<input type="checkbox"/>		Date/Time	User Name	Web Site
<input type="checkbox"/>		12/27 19:00	172.19.20.9	iframe.txt
<input type="checkbox"/>		12/27 19:00	MailServer	_Snap1.jpg
<input type="checkbox"/>		12/27 19:00	172.19.20.9	u0607q.xml.dif
<input type="checkbox"/>		12/27 18:14	MailServer	u0607q.xml.dif
<input type="checkbox"/>		12/27 11:25	172.19.20.9	u0607q.xml.klz

【图二】IR 所记录的上下传文件名称与传送方向

## 『网页布告栏发表文章』 —

聊天室、部落格、公司讨论区... 是许多使用者发表文章、抒发心情的好去处。不过，当使用者蓄意利用这些管道来发表文章做人身攻击、毁谤的动作，或是不断的重复张贴扰人的广告文，而发表者又是以昵称的形式表达，此时网管人员该如何是好？该如何抓到真正的凶手？

透过 IR 的 HTTP 记录功能，可将发文的「完整文章内容」、「来源计算机信息（计算机名称 or IP）」及「日期时间」无一遗漏的详细记录下来，即使以昵称的方式来发文也逃不过新软网络记录器的法眼，全都将以最真实的一面呈现在 IR 的 HTTP 记录表上。从此之后，网管人员再也不必担心到底是谁在网页布告栏上做坏事，因为透过 IR 的 HTTP 记录功能，这些藏镜人将无所遁形！

网络服务	新软网络记录器	一般网络侧录设备
	可记录的数据来源	
网页浏览记录	网页名称 (Title)、URL (完整路径)、浏览时间、网页所有内容 (图片、文字...)	仅网页 URL (不一定完整)、浏览时间
文件上传、下载记录	文件名称、来源路径	—
于网页布告栏发表文章	发文者来源 (计算机名称、IP 地址)、发文时间、发表的【完整文章内容】	—

【表一】新软网络记录器与一般网络侧录设备於 HTTP 服务方面的记录能力差异

文 黄赞中 isaac@nusoft.com.tw

## 市场营销报导 - 网络记录器是否侵犯到员工的隐私权

为求防止机密外泄及网络资源滥用，用网络记录器对员工的 E-mail 收发与实时通讯交谈的内容等网络行为进行拦截及监控，早已是全球业界普遍施行的管理措施。

然而企业设置网络记录器监控员工的上网行为是否侵犯隐私权，想必你我对这个问题都有疑惑。网络记录器替雇主记录所有通过的封包，加以分析归纳出使用者名称、账号、IM 交谈的内容、电子邮件的内容、及浏览过的 web 画面等网络行为，而这些记录很可能透露出员工的姓名、特征、婚姻、家庭、健康、社会活动等其它足以辨别该个人的资料，将这些个人资料搜集起来是否真不触法呢？但若不架设网络记录器又无法确保企业机密安全及吓阻员工上班滥用网络资源，这也许是企业在选择是否架设网络记录器最挣扎的问题吧。

根据中华民国行政院主计处在八十四年八月十一日公布的「计算机处理个人资料保护法」第三章第十八条、第二十三条规定，说明了非公务机关对个人数据的搜集或计算机处理，可经由员工书面同意合法记录做为特定目的之用途（如：为企业机密资料安全审察用）。换句话说如果企业将搜集到的个人资料用在非当事人同意的特定用途上就属违法（如：散播 IM 记录内容，侵害当事人权益）。

新软系统建议企业雇主在设置网络记录器前务必对该安全机制订定施行规章并告知全体同仁，甚至以书面与员工签属同意书，来保障该安全机制的合法性，并将网络记录器设定管理权限，仅供特定管理人员进入系统察看，且对管理人员实行法律教育规范，如此一来便可兼备企业机密资料及员工隐私权的保障。

\* 附注：「计算机处理个人资料保护法」之第十八条、第二十三条条文内容

### 第十八条：

非公务机关对个人数据之搜集或计算机处理，非有特定目的，并符合左列情形之一者，不得为之：

- 一、经当事人书面同意者。
- 二、与当事人有契约或类似契约之关系而对当事人权益无侵害之虞者。
- 三、已公开之资料且无害于当事人之重大利益者。
- 四、为学术研究而有必要且无害于当事人之重大利益者。
- 五、依本法第三条第七款第二目有关之法规及其它法律有特别规定者

### 第二十三条：

非公务机关对个人资料之利用，应于搜集之特定目的必要范围内为之。但有左列情形之一者，得为特定目的外之利用：

- 一、为增进公共利益者。
- 二、为免除当事人之生命、身体、自由或财产上之急迫危险者。
- 三、为防止他人权益之重大危害而有必要者。
- 四、当事人书面同意者。

文  黄智杰 alex@nusoft.com.tw