新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/2/9- 2009/2/22 第85期

## 網路記錄器 / IR 系列報導

# 技術淺談與應用 - 記錄儲存空間的分配問題

在目前的公司、企業中，為了保密防諜以及提升員工的工作效益，從過去網路側錄設備漸漸的被廣範使用，一直到目前為止，對公司、企業而言，網路側錄設備幾乎是項不可或缺的網路安全設備之一。網路側錄設備不只是要能夠達到完整的分析、全面化的管理，當然最為重要的不外乎是要能夠支援全方面的記錄功能及詳細的記錄內容。

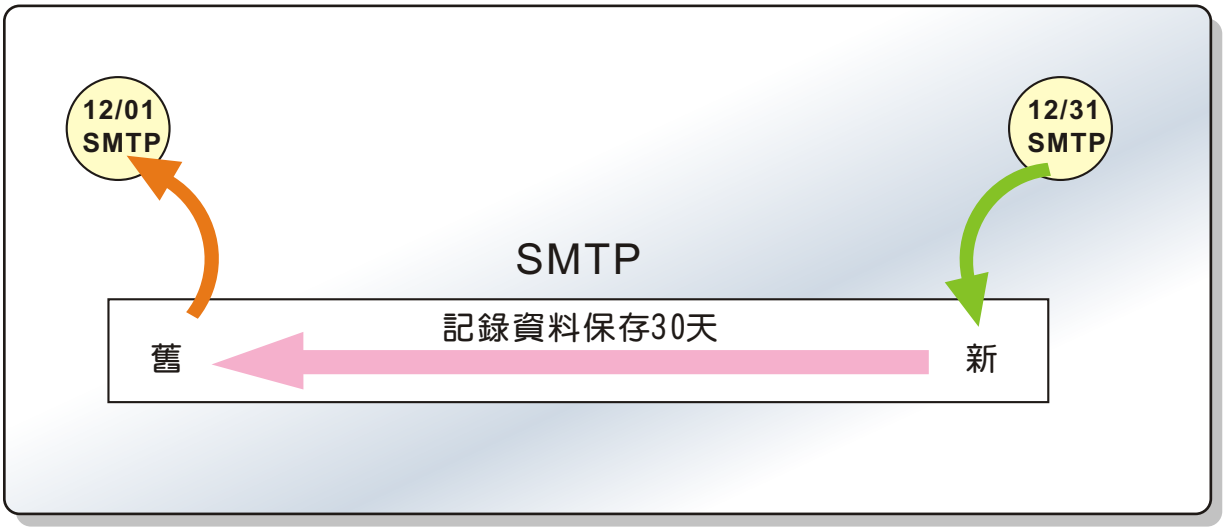
然而在詳細記錄內容下，資料一筆筆的不斷增加，相對的若是沒有足夠的儲存空間來將所記錄下來的內容做妥善保存也是徒勞無功。但是只需要大量空間來提供儲存記錄就能夠解決如此的問題嗎？其實大量的空間固然是可以解決一時資料儲存的需求，不過從長遠的眼光來看這並不是一種最適當的解決方法。所以為了能做到最完善資料儲存，同時還必需搭配有規畫性的儲存方式才是最佳的解決處理辦法。

新軟系統『網路記錄器-IR』在記錄儲存空間方面，可以依各項服務類別之記錄，依照對公司的重要性而言來自行靈活運用調配。記錄資料所保留天數對公司而言，哪項記錄服務類別重要性高，所分配的記錄就可設定較長的天數；相對的重要性較低的記錄資料，所設定的保留天數即可設定較短，例如 HTTP 這種看過即可的資訊，可設定較短的保留天數；而像是 IM/MAIL（包含 SMTP、POP3、Web SMTP、Web POP3）此類較為重要的資訊，就可設定較長的保存天數，如此一來即可大大的減省掉不必要浪費的儲存空間。

新軟網路記錄器資料保存方式可分為兩種情況，一種是內建硬碟尚未達上限，另一種則是內建硬碟已達上限。除了使用保存天數的方式來確保硬碟的空間外，同時也採用了儲存空間臨界值預防機制。當新軟網路記錄器的記錄資料，達到設定的保存期限時，即會將其立即清除；若是在資料保存期滿前，儲存空間就已達上限，新軟網路記錄器會依照儲存資料的歷史排序，從目前保留最久、最早建立的記錄開始刪除的動作，騰出一定比例的空間，以維持後續側錄動作。

## 一．內建硬碟尚未達上限

新軟網路記錄器-IR 在記錄儲存空間方面可分為 SMTP、POP3 / IMAP、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET 八大項類別，並且可依照每個公司的重視情況來自行決定記錄之保存天數，以達到靈活運用及不浪費儲存空間的最佳效果，換句話說則是將所記錄之資料內容附上保存期限，依照保存天數來交由系統決定何時可將已達保存天數時效內的資料加以刪除。例如：以 SMTP 這項類別為例，欲將此項服務類別中的記錄資料設定保存為 30 天，而當12 / 01 日所被記錄的資料會一直保存到12/30日，直到12 / 31 這一天時，系統則會自動將12 / 1 中所記錄之 SMTP 記錄全數刪除。

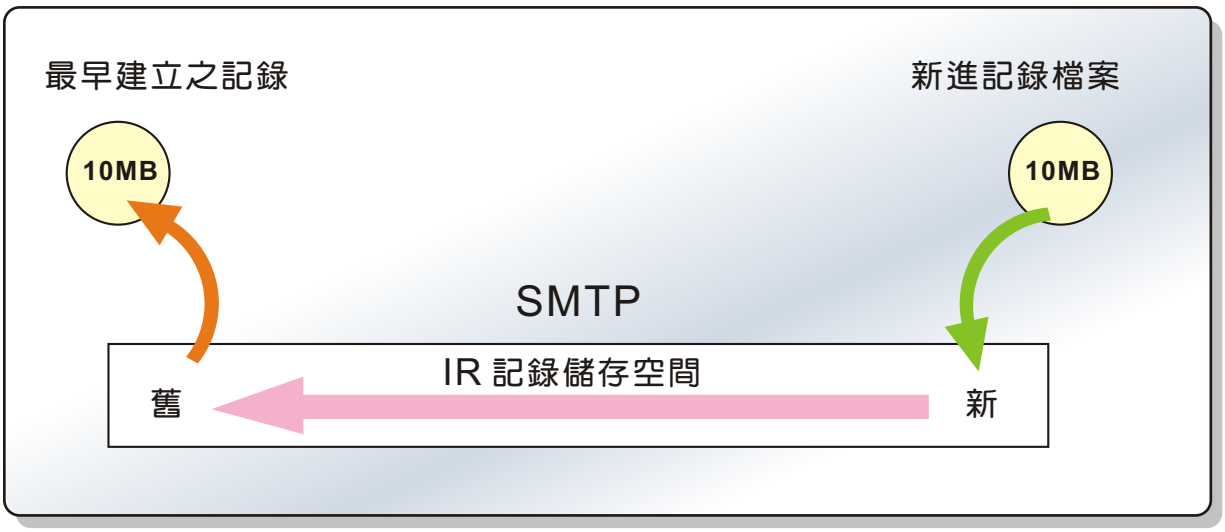



資料保存天數示意圖

## 二．內建硬碟已達上限

第二種情況則是 IR 所內建之硬碟若是在資料尚未超過保存天數時硬碟空間就已經達到上限時，IR 的記錄空間儲存分配方式。IR 在遇到內建硬碟已達上限時，記錄空間的儲存分配方式會依照先進先出的原則方式，以儲存資料的歷史排序，將最早記錄於內建硬碟中的記錄**不分服務類別項目**的加以刪除，而這方式和內建硬碟未達上限的處理方式到底不同於哪裡呢？

內建硬碟未達上限時，系統所刪除的記錄是依照該項類別（如：SMTP 的記錄在到期後只會刪除 SMTP 該項服務類別中所到期的記錄）。但遇到內建硬碟已達上限時，系統則會依照下筆新進來記錄的容量大小，將最早建立保存於 IR 中的記錄刪除相對之容量大小，騰出空間來支付新進記錄所需要容量，如：硬碟已飽和時，下筆新進入 IR 的記錄資料為 10MB(不分類別)，系統則會刪除最早存於 IR 中的記錄 10MB(不分類別)，此時所刪除的記錄並不一定會是與新進記錄所屬同類別的資料，所刪除之資料是以建立的時間早晚來做定論，換句話說，新進入的記錄資料若為 SMTP，而被刪除的記錄有可能為其他服務類別。




空間分配示意圖

為了因應企業在各法規的實行下，要達到長時間保留所有往來資料以供查閱的需求；並且同時防止用使用者郵件遺失或誤刪的情形發生，同時也可利用 IR 系統中所內建的 NAS 遠端備份機制來進行資料的備份，將欲長期保存之記錄資料儲存到 File Server、NAS、Samba Server、Windows 網路芳鄰…等備份設備中，來達到空間無上限及長期保存的效果。

文 陳殿鴻 kim@nusoft.com.tw

## 市場行銷報導 - 有規劃的即時通訊控管，也可有效預防病毒入侵

資訊科技發達的時代下，網路病毒層出不窮，幾乎只要有牽扯到網路的東西，都會有病毒的蹤影出現，而利用病毒來達到入侵、竊取及破壞的事件也是持續不斷的在發生。然而，近期發現新型態的竊取資料犯罪手法，是一種駭客控制傀儡網路的新方式。

對於現在大多數人仰賴即時通訊軟體便利的情況下，越來越多駭客開始透過植入即時通訊機器人程式（Bot，也稱為傀儡程式），此方式讓駭客可隨心所欲的利用下達相關指令來偷取使用者電腦中的資料、回傳該台電腦上的所有檔案，甚至是使用者目前正在操作中的電腦螢幕截圖；使用者電腦將完全赤裸裸的呈現給欲竊取檔案資料的有心人士。對公司而言遭受入侵所造成的影響，情況小的可能是電腦設備系統被破壞，因此使得公司無法正常的照進度營運，情況大的則可能發生公司內部相關機密被竊取，甚致因此而損失掉巨額的商機。

此種病毒的傳播路徑依舊是透過軟體的各種漏洞、植入各種後門程式，或者是透過惡意連結及利用檔案傳送的方式讓使用者下載並安裝此類惡意程式。因此，即時通訊軟體就成了最佳傳播途徑之。

在面對即時通訊軟體病毒如此泛濫的問題，身為公司管理人員又該如何去處理呢？就目前現況而言，公司內部人數眾多的環境下，最佳解決辦法就是有效的控管底下使用者對於網路即時通訊軟體的使用，藉此來預防及降低病毒入侵的機率。公司倘若不能夠有效的控管內部即時通訊軟體的使用，及在使用上規則的限制時，相對的就必須得承擔隨時突然發生病毒藉由即時通訊軟體此種管道入侵的風險。

但公司內部員工的人數眾多，對於網路通訊軟體的使用需求又不盡然的全都相同。內部人員、部門有些是完全不必要用到網路通訊軟體，但有些部門或是特定人事必需開放使用即時通訊軟體來跟外部子公司或是客戶間作聯繫，因此而無法做到全面性顧及的限制，但卻又不能因此而放任所有人員去濫用即時通訊軟體，甚至是任意藉此做檔案的傳輸動作…等，管理人員又該如何去限制及規範？

新軟系統『網路記錄器-IR』，便可以輕鬆的解決相關的問題，網路記錄器-IR 除了擁有詳細的記錄內容、簡單易懂的操控介面，更是支援了市面上多數通訊軟體的控管機制，並且還可細分是否允許登、是否允許傳檔、僅允許使用未加密之即時通訊軟體及僅允許使用通過認證的即時通訊軟體…等設計，讓管理者能應付各種不同的使用者需求，同時還支援 Web IM 的相關管制與使用。除此之外，新軟系統 IR 對於即時通訊軟體是利用軟體中的特徵碼來進行阻擋及控管，因此能達到高準確率管制效果。

對於不同部門、不同人員，不同的需求下，管理人員只需要搭配利用 IR 中所內建的群組功能、認證管理功能來加以應用，即可針對不同部門、不同人員來做到不同的限制控管規則，有效的幫助公司輕鬆的解決即時通訊控管的種種問題，同時也幫助公司創造一個良好、有規律的網路使用環境，幫助公司帶來豐厚的商機及減少員工利用即時通訊軟體摸魚的情況。讓管理人員可輕鬆掌握整個企業網路的即時通訊。

| 目前所支援的 IM 應用程式 | | |
|---|---|---|
| 可記錄內容 | 阻擋登入 | 阻擋檔案傳輸 |
| MSN | MSN | MSN |
| Yahoo Messenger | Yahoo Messenger | Yahoo Messenger |
| QQ | QQ | QQ |
| ICQ | ICQ | ICQ |
| AIM | AIM | AIM |
| Gadu-Gadu | Gadu-Gadu | Gadu-Gadu |
| Skype | Skype | Google Talk |
| 官方 Web MSN | Google Talk | |

| 目前可阻擋的 Web IM 網站 |
|---|
| 官方 Web MSN、Buddy、I Love IM、Meebo、IM haha、Kool IM、Messenger FX、Communication Tube、IMUnitive、Goowy、MSN2Go、TotMoMo、Mabber、Wablet、Mobile、webQQ. . .等 |

網路記錄器即時通訊支援表格

| | MSN | Yahoo | QQ | ICQ/AIM | Skype | Gadu-Gadu | Google Talk |
|---|---|---|---|---|---|---|---|
| 僅允許使用未加密之即時通訊軟體 | ○ | – | – | – | – | ○ | – |
| 僅允使用認證成功且未加密即時通訊軟體 | ○ | – | – | – | – | ○ | – |
| 僅允許使用通過認證的即時通訊軟體 | ○ | ○ | ○ | ○ | – | ○ | – |
| 全部允許使用即時通訊軟體 | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 全部禁止使用即時通訊軟體 | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 僅允許使用密碼正確的即時通訊軟體 | – | – | ○ | – | – | – | – |
| 僅允許使用認證成功且密碼正確之即時通訊軟體 | – | – | ○ | – | – | – | – |
| 僅允許安裝“外掛輔助程式”之電腦 | – | – | – | – | ○ | – | – |
| 僅允許使用官方版本 Web IM | ○ | – | – | – | – | – | – |
| 允許使用 Web IM | ○ | ○ | ○ | ○ | – | – | – |
| 禁止使用 Web IM | ○ | ○ | ○ | ○ | – | – | – |
| 即時通訊軟體檔案傳輸管理 | ○ | ○ | ○ | ○ | – | ○ | ○ |

即時通訊軟體支援管理功能表

『即時通訊檔案傳輸管理』（僅適用於網路記錄器採用橋接方式架設）

文 陳殿鴻 kim@nusoft.com.tw