

## 網路記錄器 / IR 系列報導

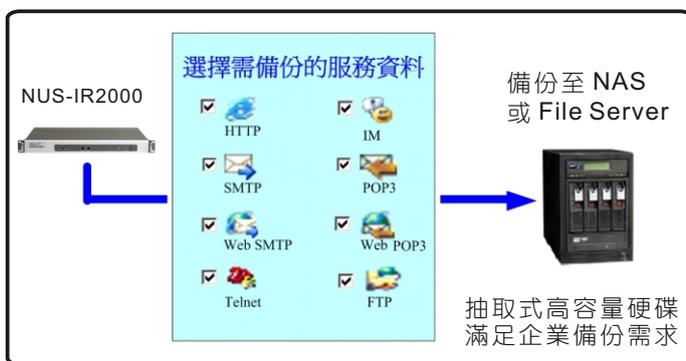
### 技術淺談與應用 - 記錄資料備份

網路記錄器每天不停的記錄資料，會不會發生硬碟空間不足而無法再記錄的問題呢？以 NUS-IR2000 來說，它的硬碟雖然多達 250G，但也會有用完的時候。因此 NUS-IR2000 可讓管理員自行分配各種記錄的儲存期限。舊記錄一旦過了儲存期限，就會自動將它移除，騰出硬碟空間，以便能再記錄新的資料。倘若這些記錄十分重要，需要保存個三五年才能銷毀時，那該怎麼辦？（歐美各國已立法要求部份行業必須保存往來電子郵件 三 至 五 年，以供日後調閱。）這時，就需要依靠 NUS-IR2000 獨特的遠端備份功能來保存這些記錄。

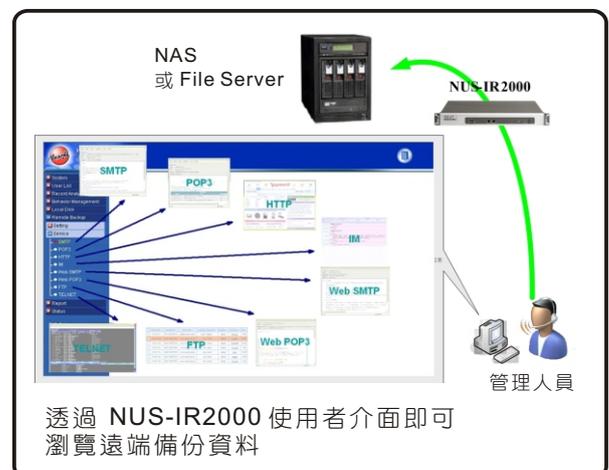
利用 NUS-IR2000 的遠端備份機制，管理人員可視需求，將記錄內容備份至遠端的 NAS 或是 File Server 中。不僅可選擇所需備份之服務（如：E-Mail、I M... 服務），更可以訂定自動備份之時間，使企業可自由選擇網路離峰時間進行備份，避免在備份時無法記錄資料的窘境。而將記錄資料備份至遠端 NAS 或 File Server 中的抽取式大容量硬碟，不但能使 NUS-IR2000 的硬碟空間，可得到充分靈活的運用，更能提高資料保存的安全性。

總括來說，NUS-IR2000 的遠端備份機制，擁有下列特點：

1. 延伸硬碟空間，使儲存容量不受限於本機硬碟的限制。（如圖一）
2. 避免紀錄遺失，例如誤刪、記錄超過儲存期限後被自動刪除、系統發生問題。
3. 網路記錄器仍可瀏覽遠端 NAS / File Server 所備份的記錄。瀏覽簡單、方便。（如圖二）



(圖一)



(圖二)

就「備份機制」來說，新軟 IR 系列產品和市售產品的比較（如下表）：

	新軟公司 NUS-IR2000	市售其他側錄設備(採用光碟燒錄備份)
備份所需時間	6 分鐘可備份 2G 的資料容量。	一張光碟需 6 分鐘或更長的燒錄時間。
備份空間大小	視 NAS 或 File Server 硬碟決定，多數為 250G 以上。可備份大型企業約 85 天的記錄資料。	一張光碟僅能備份 600M，約大型企業 4 小時的紀錄容量。
專人操作	可選擇自動備份，無須專人操作。	由於需人工更換光碟片所以僅能專人操作。
備份時機	可選擇半夜或網路離峰時間自動備份，不會影響正常記錄。	由於需專人操作，所以僅能於上班時間作業。而備份時將佔用大量系統效能干擾資料之正常側錄。
存放空間	無須另闢空間存放。	需有足夠的空間保存光碟。
資料保護機制	NAS 或 File Server 可使用磁碟陣列，避免硬碟損毀、造成資料遺失。	增購光碟保存設備，但無法 100% 保證光碟耐用，一旦光碟損毀資料將無法還原。
硬碟空間佔用	直接備份至遠端 NAS 或 File Server，無資料重複與佔用設備硬碟空間之虞。	光碟燒錄時需先將記錄資料轉換為 ISO 格式，儲存於設備中造成資料重複與佔用設備硬碟空間。

就「資料瀏覽」來說，新軟 IR 系列產品和市售產品的比較（如下表）：

	新軟公司 NUS-IR2000	市售其他側錄設備(採用光碟燒錄備份)
瀏覽方式	直接於管理介面瀏覽。	需使用檔案辨識軟體解讀取光碟資料後方能瀏覽。
瀏覽地點、時間	在任何地點、時間，只需連線至網路記錄器之控制介面即可瀏覽。	需在特定安裝辨識軟體的電腦中，讀取光碟資料，無法隨時隨地瀏覽。
資料找尋	可透過管理介面中搜尋機制，在第一時間找出所需資料。	需於眾多光碟中找尋出所需資料光碟。如無法確定資料位於那片光碟，則必須每片光碟一一尋找。
多人同時使用	可提供多人同時查閱	同一時間內僅能提供一人查閱
軟體安裝	無須另外安裝軟體，僅需網頁瀏覽器皆可完成相關查詢動作	需安裝特定的檔案辨識軟體

文  程智偉 rayearth@nusoft.com.tw

## 市場行銷報導 - 網路記錄器需包含的基本功能

在目前網路資訊傳遞蓬勃發展的環境中，運用得當可做為商場競爭的一大利器。反之，則成為企業向前邁進的絆腳石。而目前對企業最大的衝擊，無疑是內部員工想盡辦法利用公司網路，從事私人或非法的活動（例如：利用即時通訊軟體聊天怠工、持續佔用寬傳送大型檔案、洩漏公司機密資料…）。

在以往企業只能耗費大量的人力，做收效有限的查緝和嚇阻動作。為了因應上述的需求，網路側錄設備如雨後春筍般充斥在市場上。這些商品無不標榜能完整記錄或控管員工的網路行為，但往往呈現出來的是，不夠清楚或難以閱讀的資料，且模糊了原有的產品定位。

有鑑於此，新軟公司在開發網路記錄器時，則特別著重於資料的搜集、探勘和分析：

1. 詳實紀錄 8 種常用的服務：  
HTTP、SMTP、POP3、WEB Mail(Web SMTP & Web POP3)、IM、FTP和TELNET。
2. 將記錄依使用者和服務名稱分類呈現：

資料分類方法 \ 產品	新軟網路記錄器	一般市售網路側錄設備
使用者	可依據使用者名單找到特定使用者，了解其所有上網行為，並提供今日記錄功能，使管理人員能在第一時間內查詢特定使用者今日所有記錄資料。	僅能透過服務名稱搜尋相關使用者，使管理人員欲查尋單一使用者網路行為時，往往浪費許多的時間在搜尋特定使用者上，降低了工作效率。
服務名稱	可以依照服務名稱搜尋各項服務記錄，了解哪些使用者使用該項服務，大大減少搜尋的時間。	

3. 提供全方位的檢索介面：

查閱能力技術 \ 產品	新軟網路記錄器	一般市售網路側錄設備
搜尋功能	透過強大的搜尋系統，能以網站、使用者、網頁內容、時間區間等資訊，在龐大的資料中重點搜尋。當管理人員對其所需條件輸入關鍵字時，皆可迅速、輕易的找到所要的記錄。	無法針對標題搜尋，必須經由管理人員一一確認。
內容檢索	利用此獨創技術，在龐大的資料庫中快速且正確找到所需的資料，有效提高管理效能。	

#### 4. 即時和歷史性的網路流量排序：

流量排行方式 \ 產品	新軟網路記錄器	一般市售網路側錄設備
今日排行榜	利用時間捲軸拖曳至所需的時段，即可分析時段內的各項流量，藉此揪出危害網路頻寬的使用者。	僅能針對單一時間點內的記錄做分析，且無法分析預設服務以外的各類型資訊，不僅無法符合企業多元化的網路服務需求，更不能藉此協助企業排除危害網路使用者。
歷史排行榜	記錄企業網路所有流量分析資訊，全方位的分類查詢有助於企業即時掌握所有網路流量資訊。	

#### 5. 透過網路備份完整資料：

	新軟網路記錄器	一般市售網路側錄設備
備份機制	可視管理需求，將要備份的服務記錄內容，以定期或立即的方式，傳送至遠端的 NAS 或是 File Server 儲存，可選擇離峰時間備份，有效避免了備份時無法記錄的危機。	多半採用光碟燒錄輸出方式進行備份，必須於上班時間內由專人進行備份工作。在備份時往往需停止記錄動作，於備份完成時在進行記錄工作。

根據上述五大項特性，再輔以異常流量偵測和群組管理機制，將管理的權責分擔給各部門負責人，減輕管理員的負擔，並隨時監視網路使用情形，避免異常流量損及使用者的權益。使網路記錄器無形中成為資安系統中，不可或缺的管理利器。

文  陳昱昇 [josh@nusoft.com.tw](mailto:josh@nusoft.com.tw)