E-News

發行人：捷宇網安行銷部　發行日期：2011.12.5

## ●個資法細則出爐，企業須落實安全維護

2011 年 11 月新版個資法有規定，企業應有適當的安全維護措施，以防止個人資料遭竊取、竄改、毀損、滅失或洩露。法務部法律事務司科長黃荷婷指出，企業可按 P、D、C、A 方式，來落實安全維護措施。

| | |
|---|---|
| <P>為企業規劃之責任： | 「成立管理組織、配置相當資源」、<br>「界定個人資料之範圍」、<br>「個人資料之風險評估及管理機制」、<br>「事故之預防、通報及應變機制」。 |
| <D>為企業必要負擔之執行： | 「個人資料蒐集、處理及利用之內部管理程序」、<br>「資料安全管理及人員管理」、<br>「認知宣導及教育訓練」、<br>「設備安全管理」。 |
| <C>為企業應負之稽核： | 「資料安全稽核機制」、<br>「必要之使用紀錄、軌跡資料及證據之保存」。 |
| <A>為企業應承擔之矯正責任： | 「個人資料安全維護之整體持續改善」。 |

NetAxle 捷宇網安為專業的網路安全防禦系統研發商，其開發的產品 NetIRS 資安網管防護設備囊括的範圍有：

- 網路流量分析報表管理
- 入侵偵測防禦隔離
- 使用者身份識別與認證管理
- 歷史資料儲存紀錄

可以幫助企業落實個人資料安全維護防禦措施。

E-News 前幾期已針對「使用者身份識別與認證管理」之範圍、方法、與應用做概略介紹，接下來將著重其它方向的資安管理來說明。

(以上有關個資法文章，摘錄整理自 iThome 電腦報第 528 期 2011/11/05)

## ● 入侵偵測防禦隔離—IRS

IRS(Intrusion Response System)為 NetAxle 研發之技術，用於遇到異常事件時的回應。它回應的重點在於可以迅速而且精確的辨識異常 IP 在網路上的位置，透過 SNMP 方式，

使 NetIRS 下指令將其趕出網路，這樣的回應動作，可以在非常短的時間、甚至於趕在病毒要擴散之前即立刻阻止，所以 IRS 在建構網路嚴密的安全保壘上扮演相當重要的角色！

當偵測器偵測到異常事件時，必須要有執行隔離的能力，若無法解決此異常事件，就算偵測到也是徒然無功的。所以選擇產品的關鍵就在於其執行隔離的能力與效果了。

**NetIRS 針對異常行為共提供了四種隔離方式：**

1、**Switch Port Shutdown**：直接關閉駭客連接埠，而不影響其他埠的連線狀況，為最安全的方式，Switch 需支援 SNMP。

2、**Create ACL** (IP ACL 與 MAC ACL)：若為網外使用者，則直接在路由器或交換器上寫入。IP ACL 權限設定支援多種廠牌，如：Alcatel、Cisco、Extreme、Foundry、Juniper 等。

3、**Move to Quarantine VLAN** (隔離至虛擬網路隔離區)

4、**Create ARP** (產生 ARP 過濾表)