

經濟部資通安全事故調查結果報告

事故說明	
事故編號	(MOEA-AIR-西元年-流水號 3 碼，流水號每年由 001 開始累計，AIR：Accident investigation report)
事故發現日期	年 月 日 時 分
作業人員	
事故描述	
通報單 ID	(國家資通安全通報應變作業發配之編號，無則免填)
通報作業日期	通報日期： 年 月 日 通報結案日期： 年 月 日
設備及證物(硬碟)資訊	
設備 IP	
設備使用者	
設備 Patch 狀態	
防毒軟體版本	
證物廠牌	(未保留證物則不需要)
證物型號	(未保留證物則不需要)
證物容量	(未保留證物則不需要)
證物外觀	(證物照片，未保留證物則不需要)
調查暨處理過程描述	
使用工具	調查時使用之軟硬體工具
檢查項目	使用者登入紀錄痕跡、系統機碼分析、文件開啟痕跡、USB 使用痕跡、上網痕跡、E-mail 痕跡、WebMail 痕跡、IM 聊天痕跡、軟體使用痕跡、記憶體分析、關鍵字搜尋等
發現狀況說明	遭植入惡意程式、有被打包資料殘留等
疑有資料遭竊	<input type="checkbox"/> 是 <input type="checkbox"/> 否
事故原因及手法分析	發生時間分布圖、惡意網路連線關係圖、運用手法及運用系統漏洞等

經濟部資通安全事故調查結果報告

處理作業說明	停用網路服務、清除惡意程式等				
惡意程式或工具分析					
檔名					
存在路徑					
建立日期					
修改日期					
存取日期					
擁有者					
檔案大小(Bytes)					
MD5					
防毒軟體掃描結果					
行為描述					
檢討及建議事項					
資料檔案檔名列表					
序號	檔名	檔案大小 (Bytes)	建立日期	修改日期	擁有者