高雄市政府
資安事件監控分析

目 次

第一章 前言

廿一世紀資訊科技運用的普及與網際網路的蓬勃發展，使資通訊科技應用儼然已成為每個人日常生活中的一部份，並改變了人類生活模式，然令人擔憂的是資訊科技帶來的資通訊安全問題，促使資通訊安全議題成為關注的焦點。

近年來資安事件層出不窮，政府機關儼然也成為攻擊的目標之一，機密資料與個資漏失等的資安威脅，無時不刻的與日俱增，資通安全的管理就成為本府極重要的重點工作。

面對越來越多新型態攻擊手法的威脅，資訊安全管理日趨複雜與多元，除了事前的防護之外，事中監看、事後處理也同等重要，因此需要一個統一監控的管理平台，綜合各種威脅與監控資訊來研判與因應，以降低資安風險。

第二章　資安威脅趨勢

隨著時代改變與資通環境變化，電腦網路科技的發展，為人類帶來無限的便利，近年來興起的網路社群風潮、行動通訊、電子商務、雲端服務等，嚴重改變消費者使用行為，日常生活均離不開網路的使用，不明郵件、惡意程式、廣告、連結、系統程式漏洞無所不在，因而面臨嚴峻的資安威脅。

一、組織化網路犯罪猖獗

目前駭客攻擊已從個別、單純的炫耀，走向組織化、專業化分工，擁有高度技術及豐富資源，針對特定目標攻擊，以政府、金融或高科技產業為常見攻擊目標 。因不受時空、地域限制可能發動網路戰爭，影響國家安全。例如美國白宮網路遭駭客入侵、美國人事管理局遭駭客攻擊、台灣蘋果日報網站遭到駭客攻擊導致網站及內部電郵癱瘓，香港的蘋果日報網站也遇到相同情形等。

二、個人隱私資料被竊與金融詐騙事件頻傳

駭客透過電子郵件社交工程或利用網站應用程式漏洞、網頁掛馬等方式，在受害電腦植入惡意程式，以竊取個人隱私資料，並與犯罪集團合作，進行金融詐騙。例如美國摩根大通銀行遭駭客入侵、歐洲中央銀行網站遭駭、美國國稅局遭駭客入侵、丹堤咖啡遭駭，5000 筆會員個資外洩、淘寶上千萬筆帳號遭入侵、孟加拉央行帳戶遭駭等。

三、關鍵資訊基礎設施資安風險增加

涉及能源、水資源、通訊傳播、交通、高科技園區等關鍵資訊基礎設施被駭客攻擊事件有增加的趨勢。在數位經濟時代，重要資通訊設施一旦遭受破壞，勢將影響經濟、民生及整體政府運作。例如南韓水力與核電公社(KHNP)傳出遭到駭客入侵、美國運輸司令部承包商遭中國大陸駭客入侵多次等。

四、進階持續性（APT）威脅增加

APT 攻擊重點在於針對特定目標，低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。其有五種典型的特色 1.高度針對性。 2.具有潛伏並保持低調的技術能力。 3.擁有資料情報分析之能力。 4.擁有多樣工具的多重面向攻擊方式。 5.資金充裕。其目的為竊取資訊、政治因素、金錢利益。例如美國第二大連鎖零售商店 Target 端點銷售系統(POS)受駭遭到駭客侵入、索尼影業遭到駭客入侵、資安廠商 Hacking Team 遭駭客入侵等。

五、行動裝置威脅持續成長

行動裝置最大的威脅並非漏洞，而是惡意程式，智慧型手機與平板電腦等行動裝置由於攜帶方便、輕巧靈活，並可提供如：收發電子郵件、儲存文件、瀏覽簡報、遠端存取資料，甚至遠端存取其他網路設備等功能特性，有助提高行動辦公環境的生產力與效率，但同時也帶來新的資安威脅。例如行動裝置詐騙，最普遍為使用即時通訊軟體 LINE，利用引誘、偽造、欺騙以及資訊拼圖等社交工程手法進行詐騙，藉此獲取金錢財物多重面向攻擊方式。另行動支付系統將成為全球駭客的新一波攻擊目標。

六、分散式阻斷服務攻擊將持續並擴大

攻擊方式一般分為頻寬消耗型攻擊，利用殭屍程式傳送大量流量至受損的受害者網路設備、系統，目的在於堵塞其頻寬，使服務暫時中斷或停止。另資源消耗型攻擊利用大量連線消耗網路設備、伺服器、系統程式資源。例如全球最大反垃圾郵件非營利組織 Spamhaus 遭受流量 300Gbps 之 DDoS 攻擊，持續近一週，致使合法用戶無法使用 Spamhaus 系統、另程式碼代管網站 GitHub 遭遇大規模 DDoS 攻擊、英國 BBC 新聞網站遭美國反 IS 駭客團體新世界駭客攻擊、英匯豐銀行遭 DDoS 攻擊等。

七、零時差攻擊造成資安防護困難

所謂零時差攻擊就是當系統或應用程式上被發現具有風險性之弱點

後，但是在修正程式發佈之前，或是使用者更新前所進行的惡意攻擊行為。由於該弱點尚未被揭露，因此零時差攻擊發生時，往往會造成比一般性漏洞更大的危害。

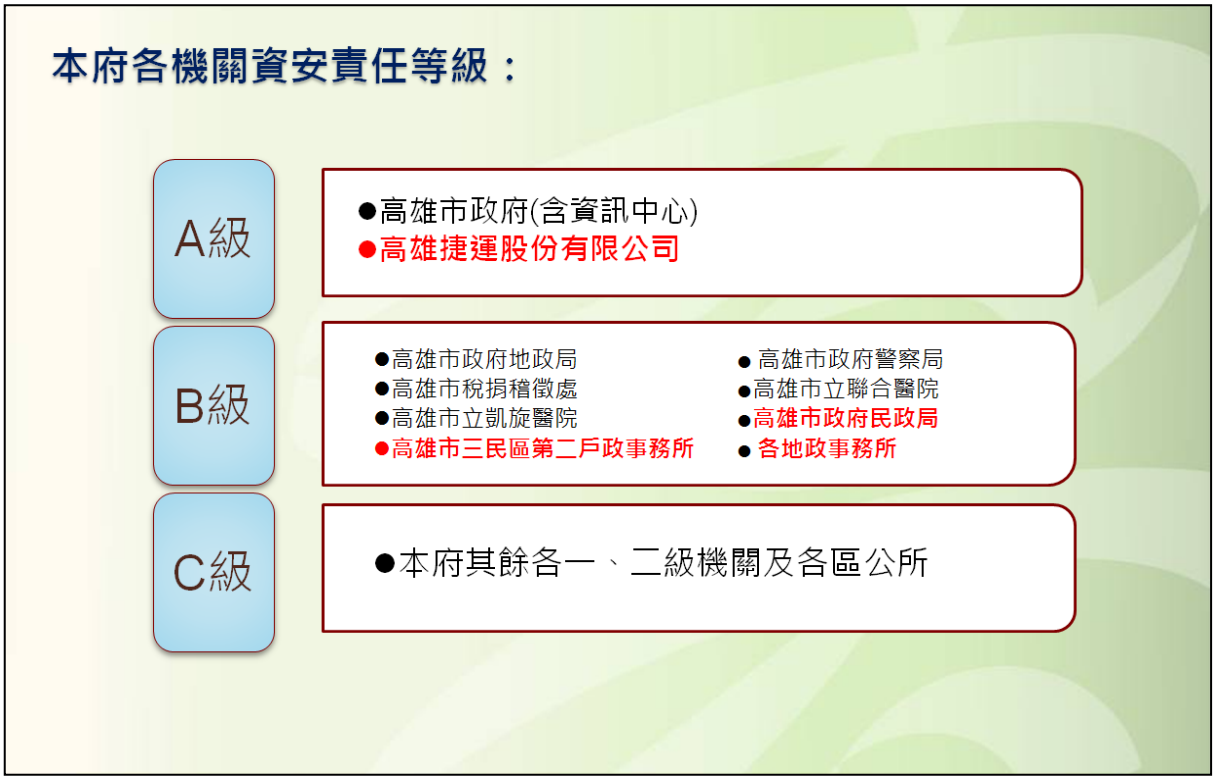
八、勒索軟體的猖獗

最近感染勒索軟體有增加趨勢，以感染途徑來看，勒索軟體是透過電子郵件中的附件或連結來散佈，或透過瀏覽器連結到惡意網站的方式感染若使用者風險意識不夠，就很可能受害，導致被加密檔案無法存取。面對加密勒索威脅時，人員資安意識、軟體系統更新，以及檔案備份，就是很重要的三大步驟，尤其是安全備份這一塊，才能降低加密勒索的風險。面對加密勒索軟體不斷更新、進化，使用者勢必要提高警覺，才不會讓工作成果付之一炬。

第三章　資安現況分析

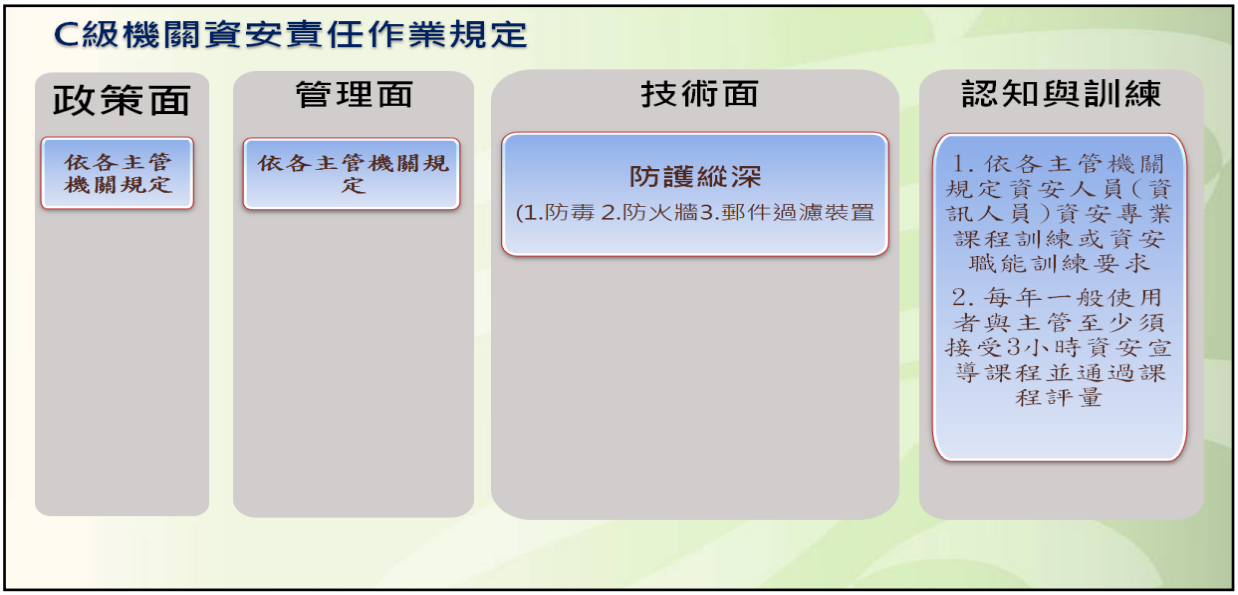
市府各機關資安防護是依據行政院國家資通安全會報訂頒之「政府機關(構)資通安全責任等級分級作業」規定辦理。

一、本府機關依資安重要程度分 A、B、C 三級，執行資訊安全管理應辦事項。




A級機關資安責任作業規定
政策面
104年完成資訊系統分級
105年完成資訊系統資安防護基準要求
管理面
全部核心資訊系統完成ISMS導入
通過第三方驗證
專責人力x2
每年2次內稽
每年辦理核心資訊系統持續運作演練
技術面
防護縱深 (防毒、防火牆、郵件過濾裝置、入侵防禦IPS、Web應用程式防火牆、APT攻擊防禦)
安全性檢測 (每年網站安全弱點檢測、系統滲透測試、資安健診)
監控管理 (SOC監控)
認知與訓練
每年資安人員須接受資安專業課程訓練或資安職能訓練
每年維持至少2張國際資安專業證照與2張資安職能訓練證書之有效性


B級機關資安責任作業規定
政策面
104年完成資訊系統分級
105年完成資訊系統資安防護基準要求
管理面
至少2項核心資訊系統完成ISMS導入
通過第三方驗證
專責人力x1
每年1次內稽
每2年辦理核心資訊系統持續運作演練
技術面
防護縱深 (防毒、防火牆、郵件過濾裝置、入侵防禦IPS、Web應用程式防火牆、APT攻擊防禦)
安全性檢測 (每年網站安全弱點檢測、2年1次系統滲透測試、2年1次資安健診)
監控管理 (SOC監控)
105年底前
認知與訓練
每年資安人員須接受資安專業課程訓練或資安職能訓練
每年維持至少1張國際資安專業證照與1張資安職能訓練證書之有效性



二、本府資安概況重點工作如下：

（一）加強同仁資安知識與常識：透過教育訓練或定期會報，提供同仁最新資安知識與常識，避免同仁疏失造成資安漏洞。

（二）培育資安專業人才：鼓勵同仁參加各項資通安全訓練，以取得最新資安技術。

（三）通報演練：舉辦資通安全通報演練，模擬各類資安事件，加強市府各機關資安聯絡人於資安事件發生時，如何因應與處理程序。

（四）電子郵件社交工程演練：為提高機關人員資安警覺性以降低電子郵件社交工程攻擊風險。

（五）網站、網頁安全管理：辦理主機弱點掃瞄、滲透測試、程式碼檢測、網頁漏洞如SQL Injection等。

（六）第三方資安驗證：以制度面的改善做最基礎防線之設計，市府資訊中心為資安等級A級之機關，已於96年10月23日通過國際認證公司SGS台灣檢驗科技股份有限公司之ISO27001資訊安全系統認證；而市府資安等級B級之機關亦皆通過ISO27001資訊安全系統認證。

（七）每日資安警訊及流量管理。

（八）透過SOC進行資安事件監控，將資安攻擊防護訊息即時回傳通報行政院技服中心，以達資安聯防功效。

三、資安設備防護與監控

引進先進之資安軟硬體設備做為資安防護的利器,加強防護縱深觀念，在每個重要網路節點佈置適當防火牆、入侵監測系統等設備、監控方面除了網路流量監控系統之外，還建置資安事件監控平台。

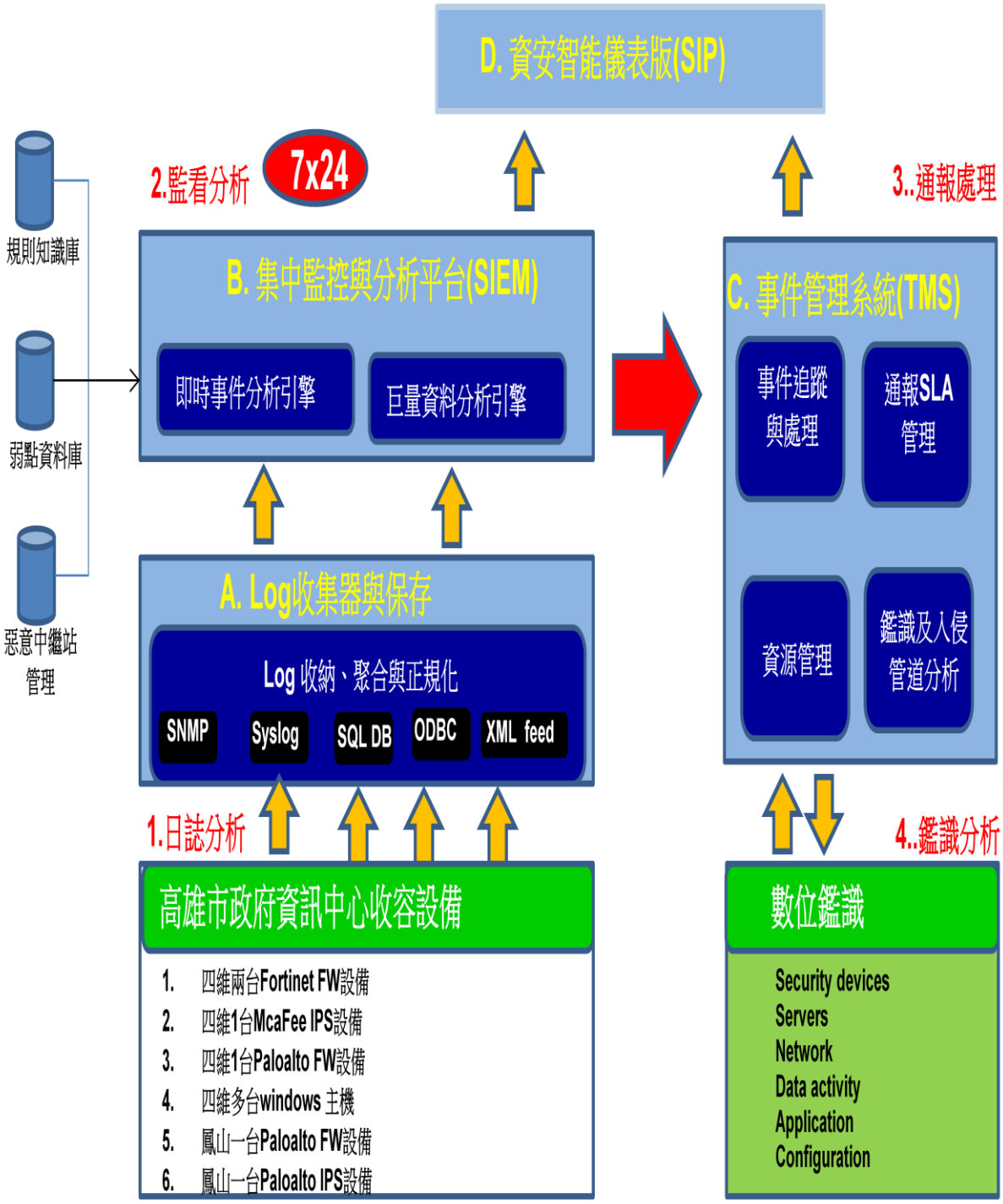
(一)於本府四維及鳳山行政中心重要網路節點上建置各項資訊安全防護措施，加強整體資通安全，減少因駭客或病毒入侵，或內部人員不當使用而造成之損失。為確保資訊之機密性、完整性及可用性，保障安全地使用與傳送資訊，辦理執行資訊安全防護監控服務事宜，以落實資通安全。提供高雄市政府四維及鳳山行政中心監控環境部署、資安事件(故)監控、資安事件(故)通報與應變處理及資安威脅預警等資安服務。

(二)偵測四維及鳳山行政中心網路環境、重要伺服器、系統環境與網際網路所產生的資安事件(故)，適時進行通報應變、事件(故)分析、追蹤處理等回應。

(三)應用國內外資安組織之資安威脅資訊,即時提供資安預警通報與建議防護措施。

(四)依照行政院資安全辦公室規範,透過資料交換協定提供資安事件(故)情資，與G-SOC形成資安聯防體系。

第四章　市府資安事件監控架構



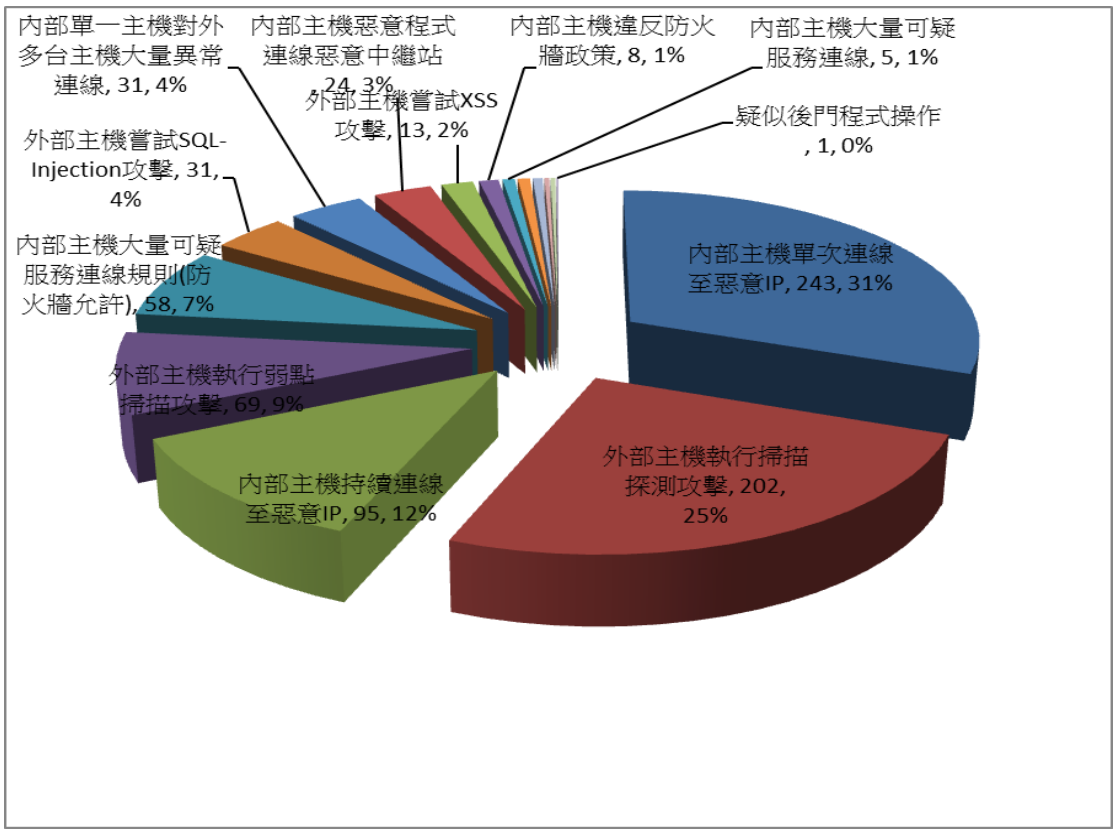
第五章　資安事件統計分析

一、監控通報事件統計分析

(表一)104 年度監控通報事件統計列表

監控規則名稱	事件數量											
	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	十一月	十二月
內部主機大量可疑服務連線_高雄市政府	1	0	3	0	1	0	0	0	0	0	0	0
內部主機持續連線至惡意 IP_高雄市政府	22	5	13	3	4	12	5	4	2	13	9	3
內部主機單次連線至惡意 IP_高雄市政府	16	9	17	12	10	10	23	18	27	36	38	27
內部主機大量可疑服務連線規則(防火牆允許)_高雄市政府	1	3	5	3	6	1	6	12	7	11	2	1
內部主機違反防火牆政策_高雄市政府	0	0	3	2	3	0	0	0	0	0	0	0
外部主機嘗試 SQL-Injection 攻擊_高雄市政府	3	3	0	0	1	8	0	0	2	2	0	12
外部主機執行弱點掃描攻擊_高雄市政府	1	3	5	13	15	5	3	5	0	3	14	2
內部主機觸發未阻擋 IPS 事件_高雄市政府	4	0	0	0	0	0	0	0	0	0	0	0
外部主機執行掃描探測攻擊_高雄市政府	14	9	13	22	13	29	14	10	11	10	15	42
外部主機觸發未阻擋 IPS 事件_高雄市政府	4	1	0	0	0	0	0	0	0	0	0	0
不合法目的 IP 連線_高雄市政府	0	1	0	0	1	0	0	0	0	0	0	0
內部單一主機對外多台主機大量異常連線_高雄市政府	9	4	0	2	0	16	0	0	0	0	0	0
外部主機嘗試 XSS 攻擊_高雄市政府	0	0	0	0	1	0	0	1	0	2	7	2
外部主機疑似進行阻斷服務攻擊_高雄市政府	0	0	0	1	1	0	0	0	0	0	0	0
內部主機惡意程式連線惡意中繼站	0	0	0	0	0	0	9	0	2	5	7	1
疑似後門程式操作	0	0	0	0	0	0	0	0	0	0	1	0
合計(件)	75	38	59	58	56	81	60	50	51	82	93	90

(表二)104 年度通報事件百分比分佈圖



(一)104 年度事件經統計,觸發事件大部分集中於外部主機執行掃瞄探測攻擊，該事件若已於 FW 阻擋，攻擊未成功，觀察即可。

(二)內部主機單次連線惡意 IP，所有的連線皆被 FW 所阻擋，若有兩次以上的連線行為，針對此台主機需進一步的處理措施。

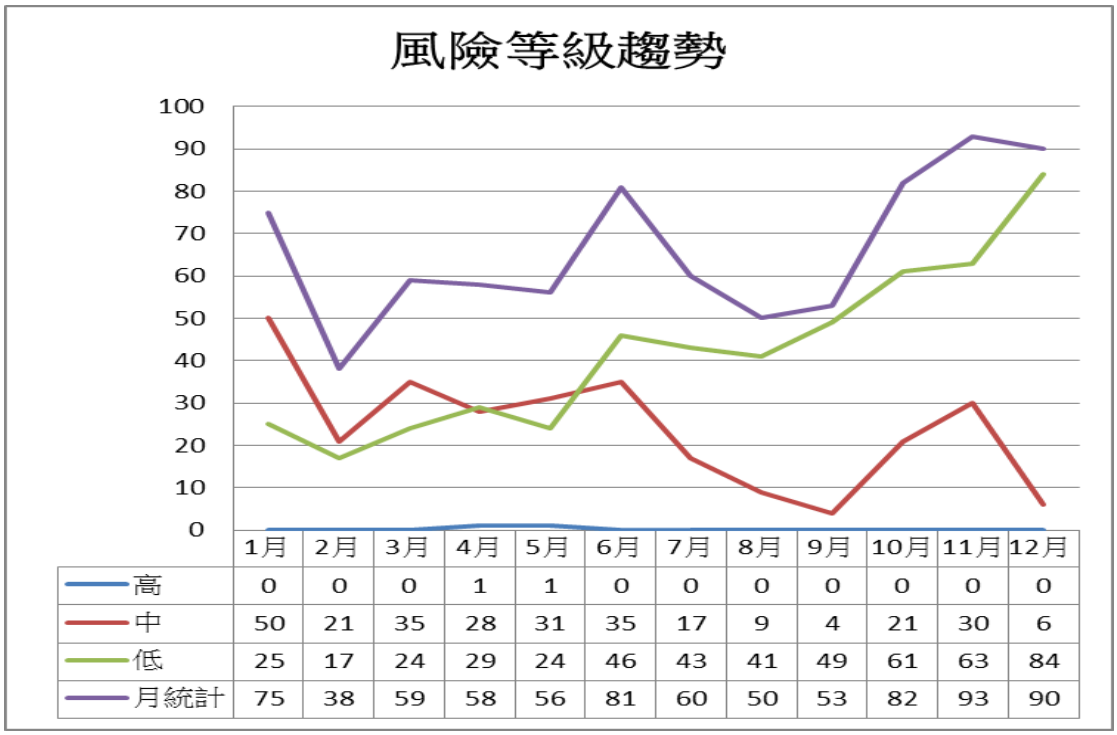
(三)104 年度事件經統計，另外觸發了些許 SQL-Injection 攻擊，因此類攻擊都被 IPS 所阻擋，攻擊未成功，觀察即可。

(四)104 年度有觸發了一些內部主機大量可疑服務連線規則(未阻擋)，經排除一些正常行為，此一觸發事件已經大幅下降。

(五)四維行政中心有多次觸發內部主機連線惡意 IP，透過 SOC 監控可有效的歸納出特定來源及目的 IP，針對多次連線的主機進行告警，有效降低資安事件觸發，該觸發事件皆已被阻擋，建議清查內部主機。(每個月平均可抓到 20 筆連線惡意 IP 之主機)

(六)外部主機探測掃瞄攻擊，透過 SOC 關連規則，可於當下確認掃瞄之特定 Port 是否有進行阻擋，避免衍生後續的風險。(每月約有 30 筆外部探測事件，可提供當作資安防禦參考)

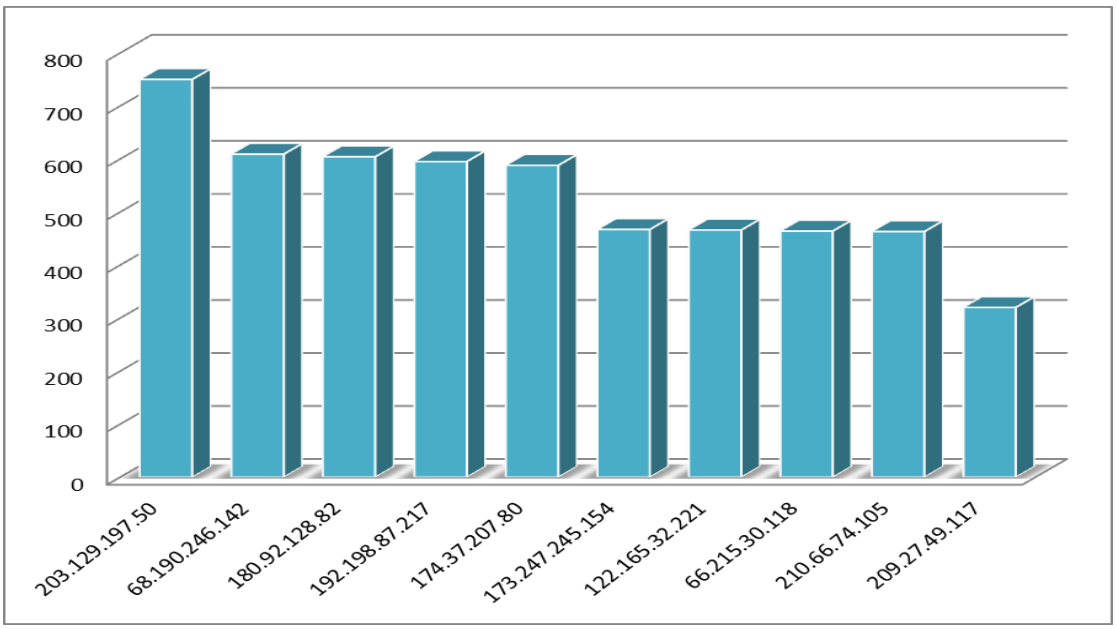
（表三）風險等級趨勢圖



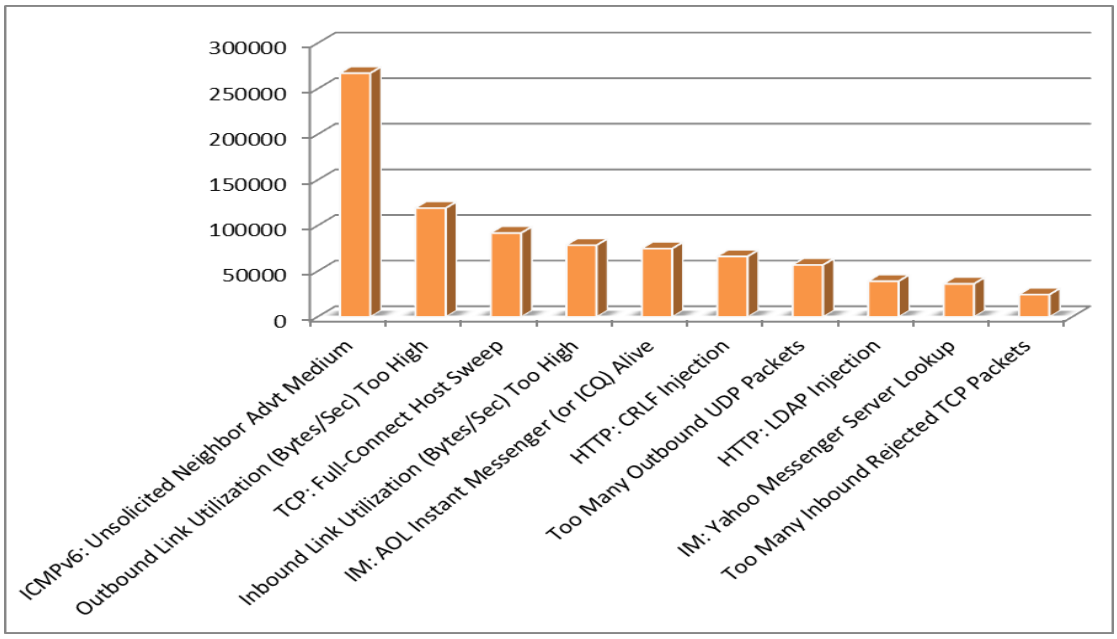
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
高	0	0	0	1	1	0	0	0	0	0	0	0
中	50	21	35	28	31	35	17	9	4	21	30	6
低	25	17	24	29	24	46	43	41	49	61	63	84
月統計	75	38	59	58	56	81	60	50	53	82	93	90

二、入侵告警事件統計報表

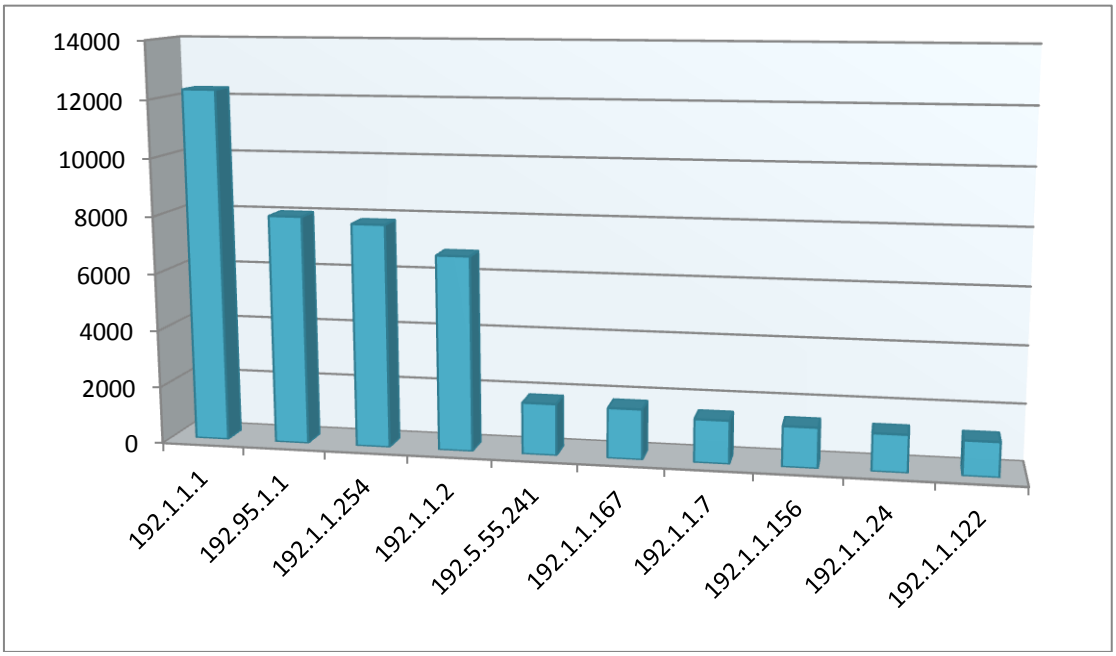
（表一）104 年度前十大連線惡意中繼站統計



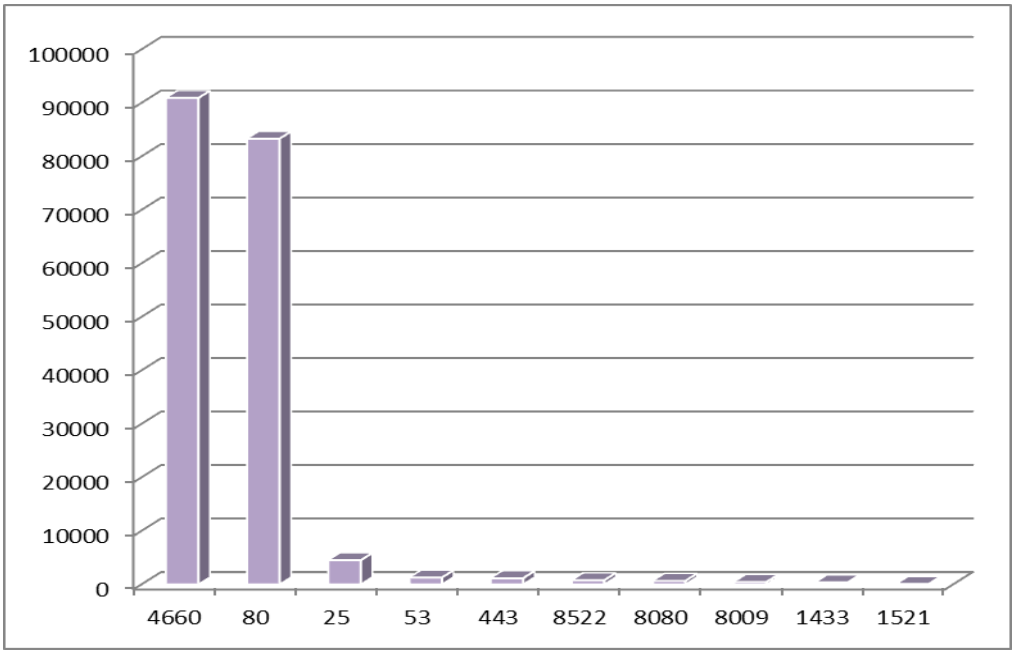
（表二）104 年度前十大可疑事件類型統計



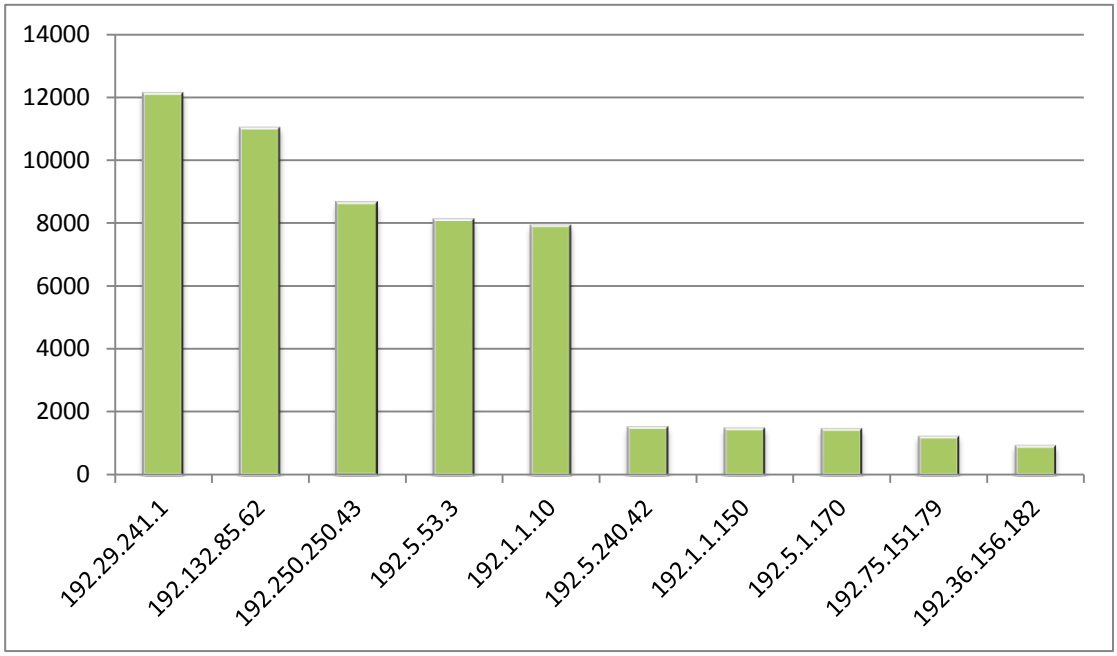
（表三）104 年度前十大目標 IP 統計



（表四）前十大目標 PORT 統計



(表五)前十大來源 IP 統計



第六章　事件性別分析

在網路使用相當蓬勃的背景下，各個不同的性別差異中，有各自喜好的網路產業使用類別，而線上遊戲、情色在男性佔有一定程度的比例，這些網站安全性較低，中惡意程式風險比率較高。女性部分則著重生活相關產業議題，不管是生活資訊搜尋、購物中心、醫療資訊或社群、部落格使用，這些網站中惡意程式風險比率較低。

依據監控通報統計資料中，從市府內部電腦 IP 連線惡意中繼站資料統計男女比率約 7 比 3，男性使用電腦被植入惡意程式、中毒機率高很多。主要原因為上網習慣、瀏覽網頁內容安全等，雖然大部份公務電腦均有裝防毒軟體，但目前防毒軟體無法百分百辨識出惡意後門，另外亂開來路不明信件也是中惡意程式主因。

電腦防護準則不外乎作業系統及軟體定期更新修補至最新版本、不要點擊來路不明網站及廣告、不要開啟來路不明的電子郵件，也不要點選可疑連結與附加檔。

第七章　結論

從 104 年度所進行的資安事件監控管理服務通報事件的分析中，可以發現所觸發的通報事件大部分都是分類為中低風險的事件，例如:觸發防火牆 FW 的通報事件「內部主機連線至惡意 IP」。雖經分析與觀察後確認大部分均為被阻擋之連線。但仍需管理者對來源主機進行掃毒，並確認是否有使用相關應用程式進行連線，若為異常程式則建議進行移除，將個人主機受駭的風險降至最低，提高整體網路資訊的安全。另外針對入侵偵測 IPS 所觸發的高風險事件，如未經阻擋可透過 SOC 監控發現，並提醒市府各局處資安聯絡人進行阻擋動作。

透過資安事件監控 SOC 7X24 小時全年無休，持續不間斷對網路與設備進行監控與通報，且由資安專家進行專業的事件關連性分析與規則調校，雖可以立即發現資安問題與漏洞，並防止資安事件擴大。不過駭客攻擊手法日新月異且資安漏洞層出不窮，因此資安事件的防範仍需 SOC 與市府資安人員持續密切的合作才能確保網路與資訊使用上的安全。

雖然104年度有觸發了一些內部主機大量可疑服務連線規則(未阻擋)，

經排除一些正常行為，此一觸發事件已經大幅下降。內部主機單次連線惡意IP，所有的連線皆被防火牆FW所阻擋，若有兩次以上的連線行為，需針對此台主機進行進一步的處理措施。另外針對檔管局公文系統主機後續會收容至SOC進行監控，依照業務機關提供文件進行相關設定，並提供系統主機IP資訊管控。

資安防護無100%安全解決方案，目前亦無單一資安設備產品，可解決所有資安問題，適宜做法是在各相對網路區段，建置佈署適當防護設備，並搭配資安監控分析，以縱深防護方式，做好全面資安防護。