

100年度 雲嘉區域網路中心成果報告

報告單位：中正大學

報告人員：李新林

王鐵雄

郭錦賢



報告內容(1/2)

- 壹、區網基本資料及人力狀況
- 貳、資通安全環境整備
- 參、區網中心運作情形
- 肆、推動網路資訊應用環境之導入情形
- 伍、網路應用創新服務情形



報告內容(2/2)

陸、辦理教育訓練及推廣活動情形
柒、區網維運配合款及經費運用
捌、綜合建議



壹、區網基本資料及人力 狀況



中心基本資料 (1/2)

- 中心主任：李新林教授
- 業務分四組：資源管理組、管理資訊組、系統支援組及研究發展組
- 行政單位：行政支援
- 中正大學網址 <http://www.ccu.edu.tw>
- 雲嘉區網網址 <http://ycrc.tanet.edu.tw>



中心基本資料 (2/2)

- 網管業務負責人員：王鐵雄、黃柏森、郭錦賢
- 資安業務負責人員：蕭文科
- 連絡電話：05-2720480
- 單位傳真：05-2720485
- 人員E-mail：

王鐵雄：tswang@ccu.edu.tw

黃柏森：jason@ccu.edu.tw

郭錦賢：jsguo@ccu.edu.tw

蕭文科：vchsiao@ccu.edu.tw



中心人力狀況

- 電算中心人員共計39人。
(包含負責大學甄選入學業務及其他計畫案)
- 雲嘉區網中心專任人員2人，兼任人員1人。
(專任人員為教育部補助之網管人員及資安人員各1人，2人均擁有ISMS主導稽核員證照)
- 本中心共有7人擁有ISMS主導稽核員證照。



貳、資通安全環境整備



網路安全防範機制

- 雲嘉區網透過2部「TippingPoint 2400E網路威脅管理與防禦系統」防範各種網路攻擊。
- 本校定期於每年第4季辦理全校「資安演練」(現場展示資料佐證)。
- 本校定期分2次辦理全校「電子郵件社交工程演練」(現場展示資料佐證)。
- 自行開發「[校內主機病毒監視系統](#)」，每天監督使用者病毒狀況，以遏阻病毒漫延。
- 每月辦理網站應用程式弱點掃描，協助各單位排除網站弱點問題。



網路安全通報機制

- 透過教育機構資安通報平台進行網路安全通報服務。
- 一經通報後，本中心資安人員隨即打電話通知該單位業務負責人員進行處理。
- 追蹤各單位回報情況，直到通報完成為止。



智財權檢舉案件追蹤

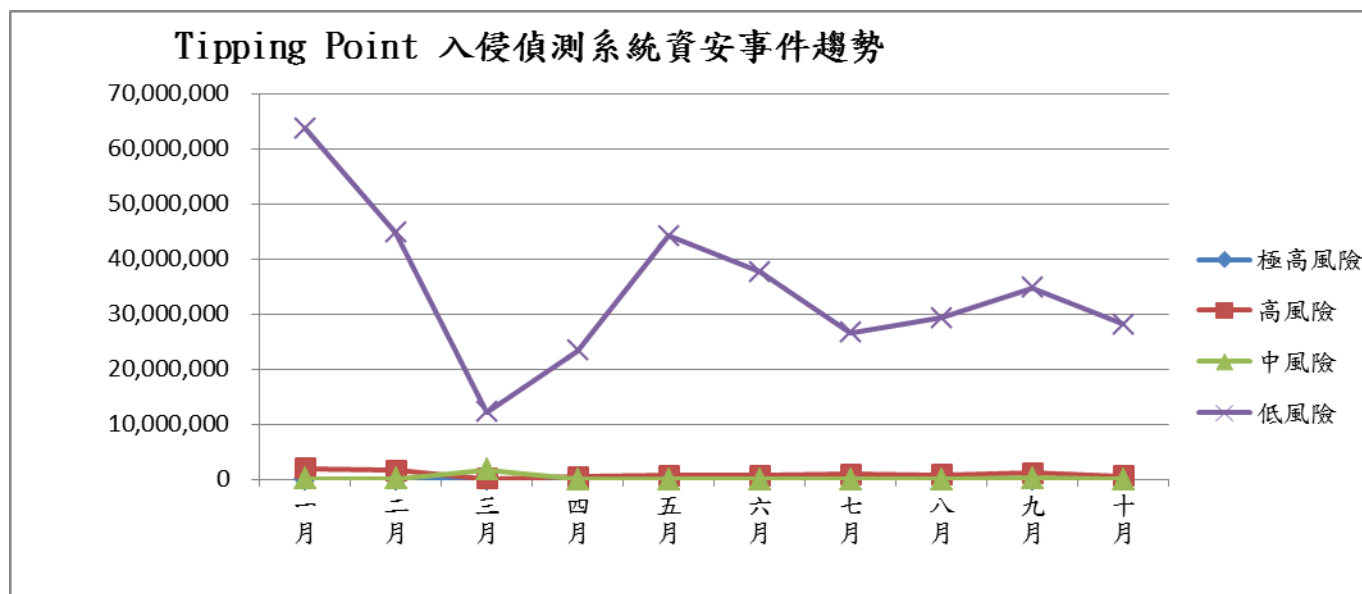
- 本校辦理智財權檢舉案件追蹤均依部訂SOP辦理。
- 違反規定者停止網路使用權，並函請單位系所告誡，並依「學生獎懲要點」、「國立中正大學校園網路使用規範」、「國立中正大學校園伺服器管理辦法學生」及「國立中正大學宿舍網路管理辦法」等相關規定辦理。
- 案例：現場展示佐證資料。



中正大學資安事件統計-Tipping Poing

事件來源：Tipping Point入侵偵測系統（事件統計）

100年	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	總計
極高風險	0	0	11	0	0	0	0		0	0	11
高風險	1,982,656	1,579,348	83,238	438,166	650,205	621,708	867,695	799,911	1,107,836	519,620	8,650,383
中風險	80,609	50,074	1,752,670	8,558	37,428	23,053	28,955	30,372	246,873	6,860	2,265,452
低風險	63,678,502	44,811,748	12,238,655	23,369,003	44,212,445	37,721,149	26,607,266	29,277,733	34,776,644	28,172,695	344,865,840

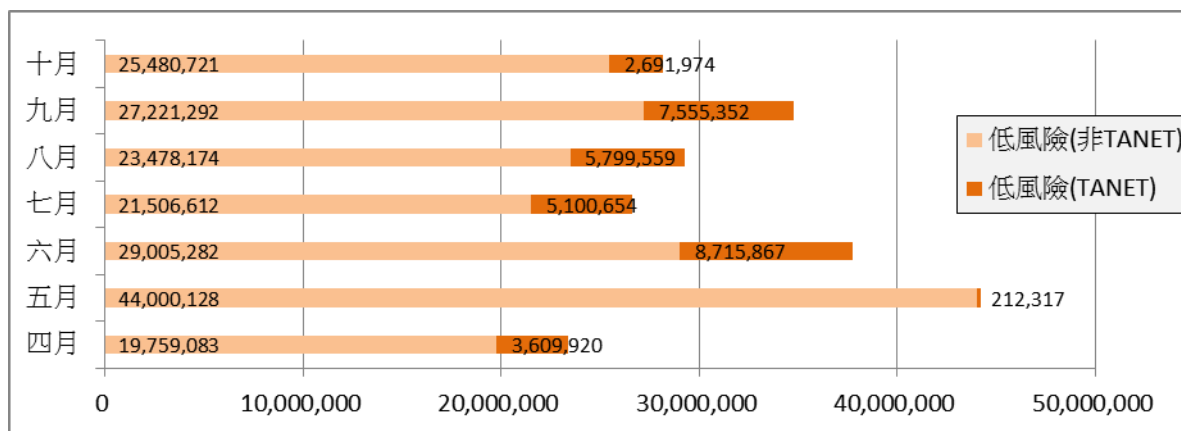
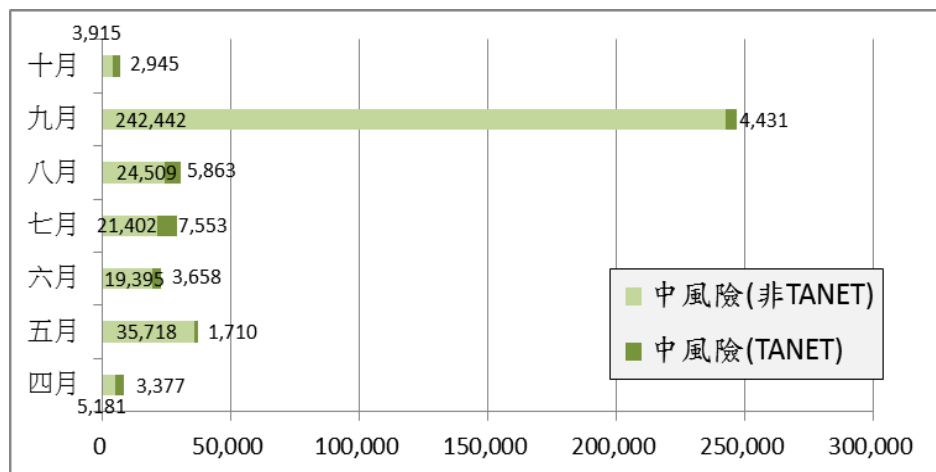
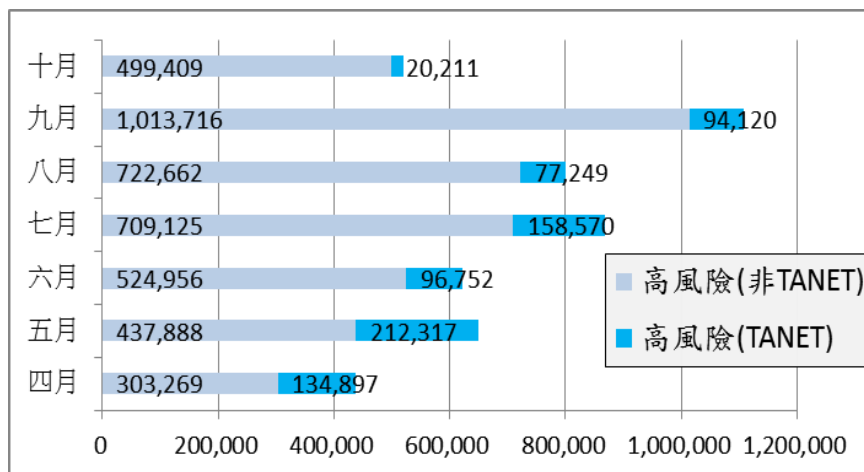


- 監測回報處理校內資訊安全事件，使高風險攻擊行為持續降低



中正大學資安事件統計-Tipping Poing

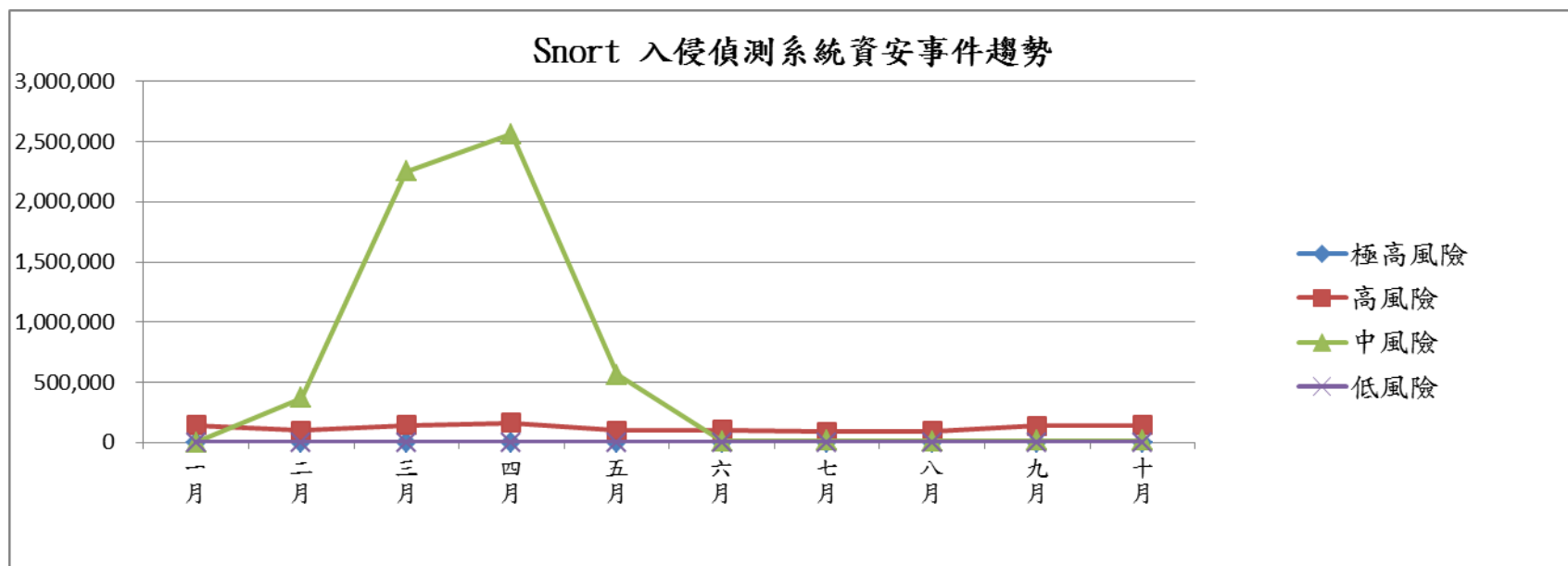
- 攻擊事件中來自TANET IP的比例逐漸遞減



中正大學資安事件統計-Snort

事件來源：Snort入侵偵測系統（事件統計）

100年	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	總計
極高風險	470	294	656	578	334	260	159	331	313	267	3,662
高風險	141,793	101,271	145,558	162,917	100,877	102,370	89,089	95,861	141,583	143,411	1,224,730
中風險	1,179	371,162	2,253,583	2,564,584	561,968	8,776	15,004	12,890	15,551	15,660	5,820,357
低風險	0	0	0	0	0	0	29	33	35	25	122

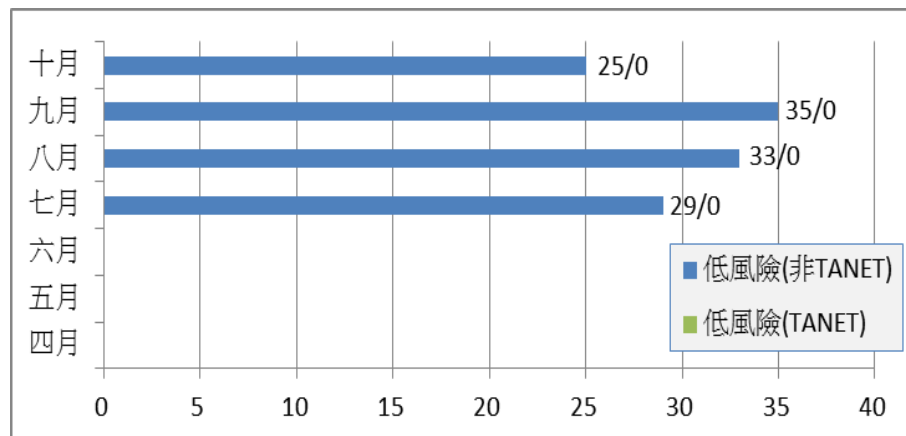
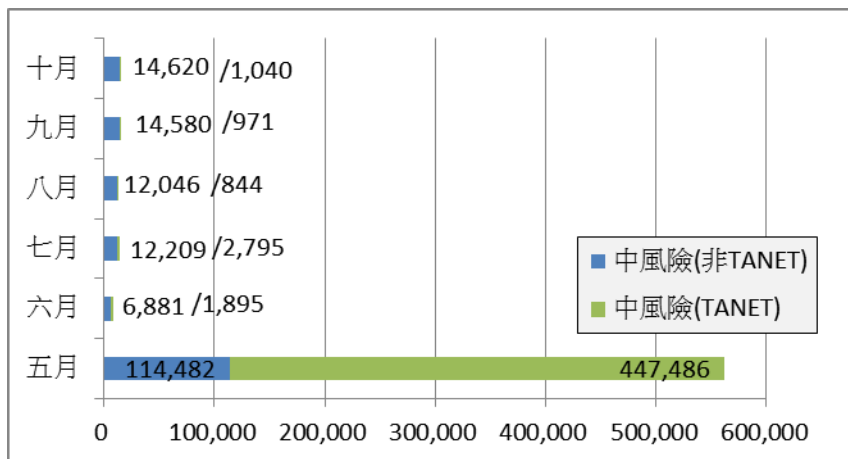
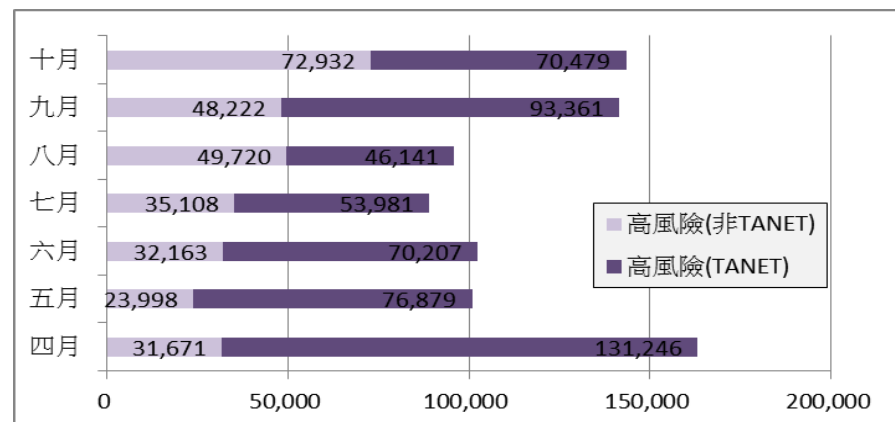
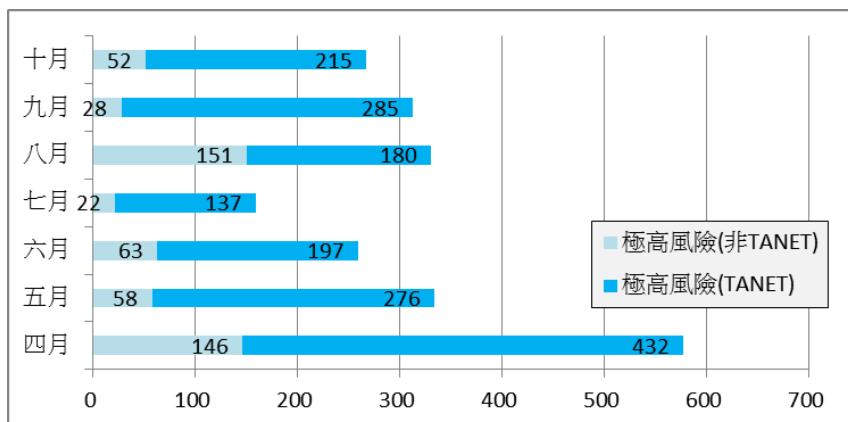


- 定期回報處理發現之校內Bot主機，使資安事件持續降低



中正大學資安事件統計-Snort

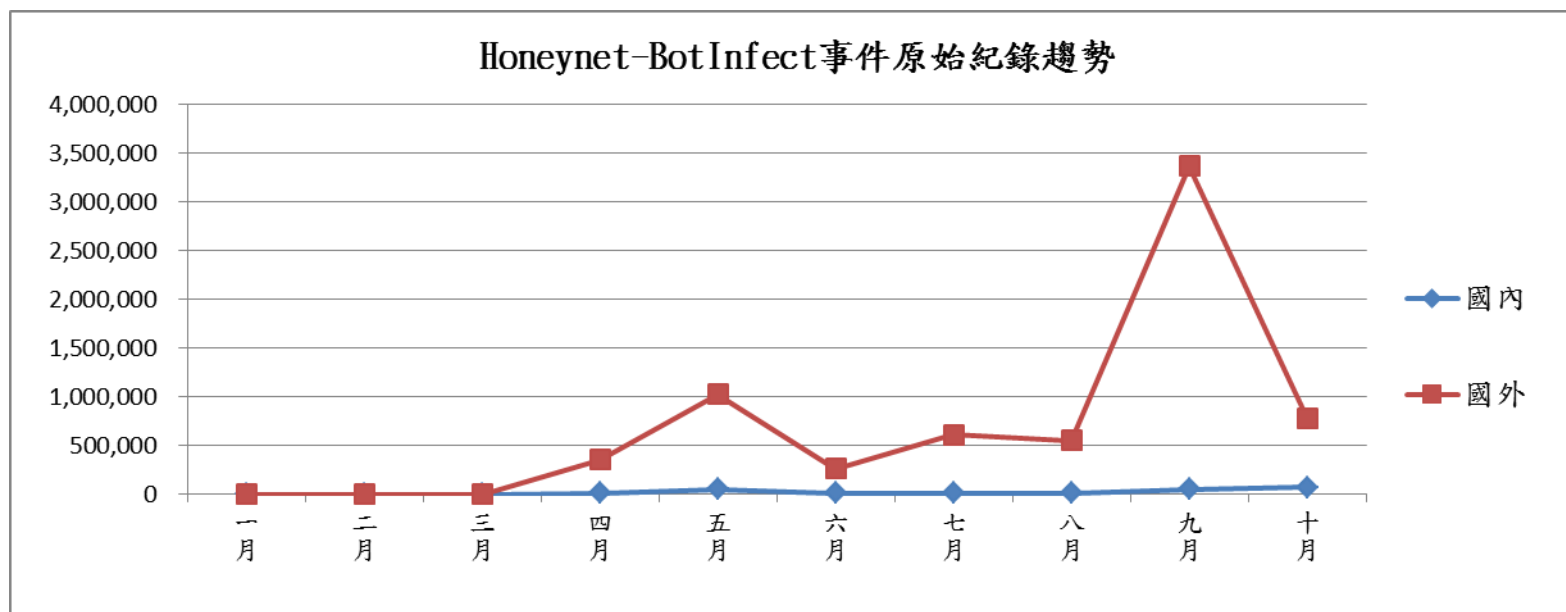
- 攻擊事件中來自TANET IP的數量逐漸遞減



中正大學資安事件統計

事件來源：Honeynet 誘捕系統

100年	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	總計
國內	812	0	6	16,946	55,995	16,838	17,838	17,523	53,281	72,108	251,347
國外	276	659	516	354,027	1,029,299	261,674	611,451	554,817	3,367,340	784,139	6,964,198

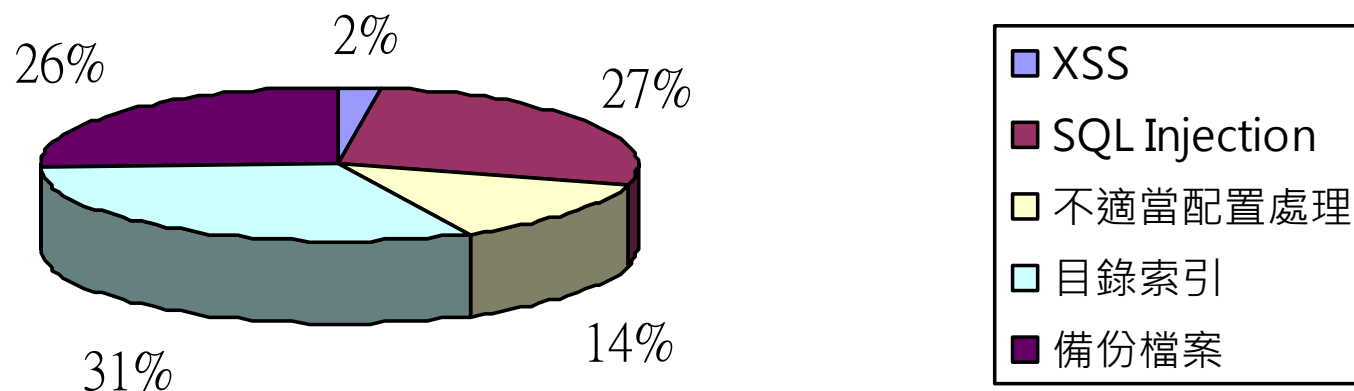


- 誘捕系統分佈於校內不同網段，並持續變更佈署策略，使收集到的惡意程式及補獲的惡意行為成效漸增。



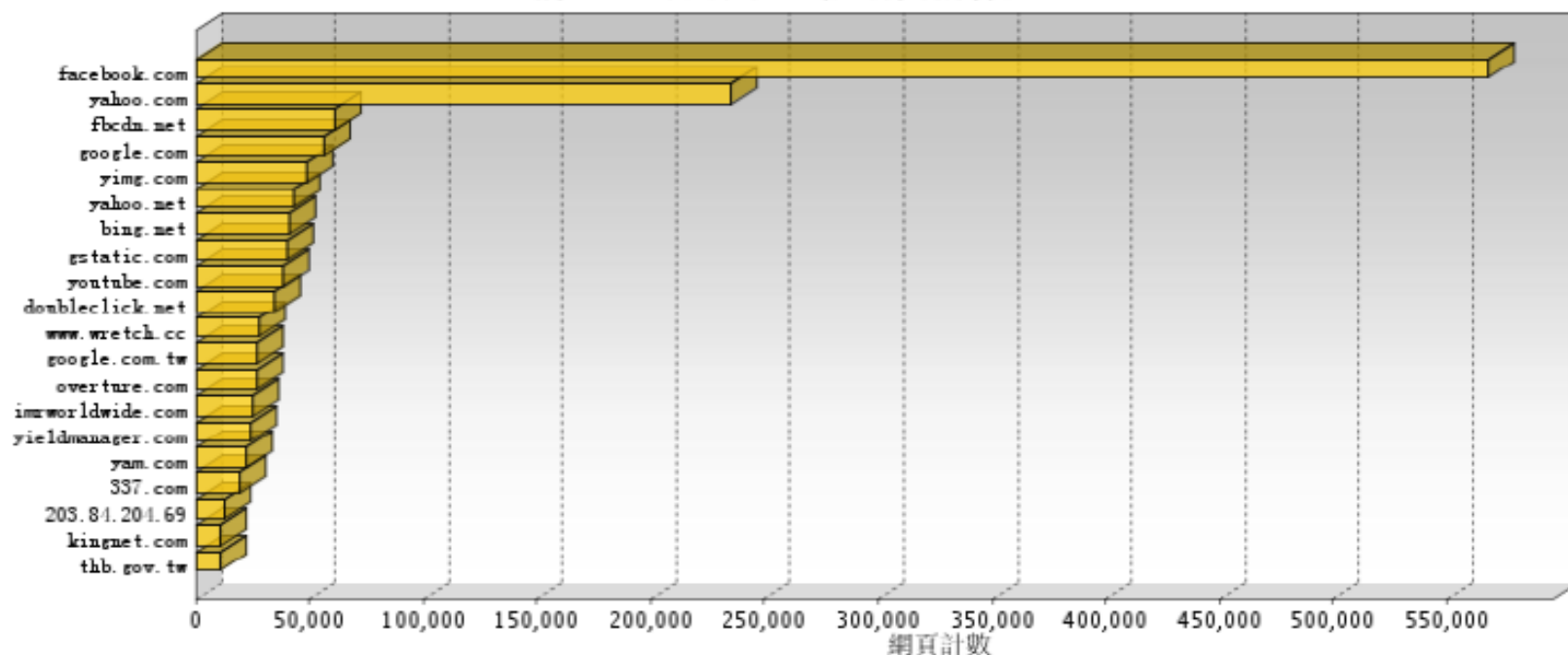
教育部網站應用程式弱點監測平台

檢測弱點類型統計表

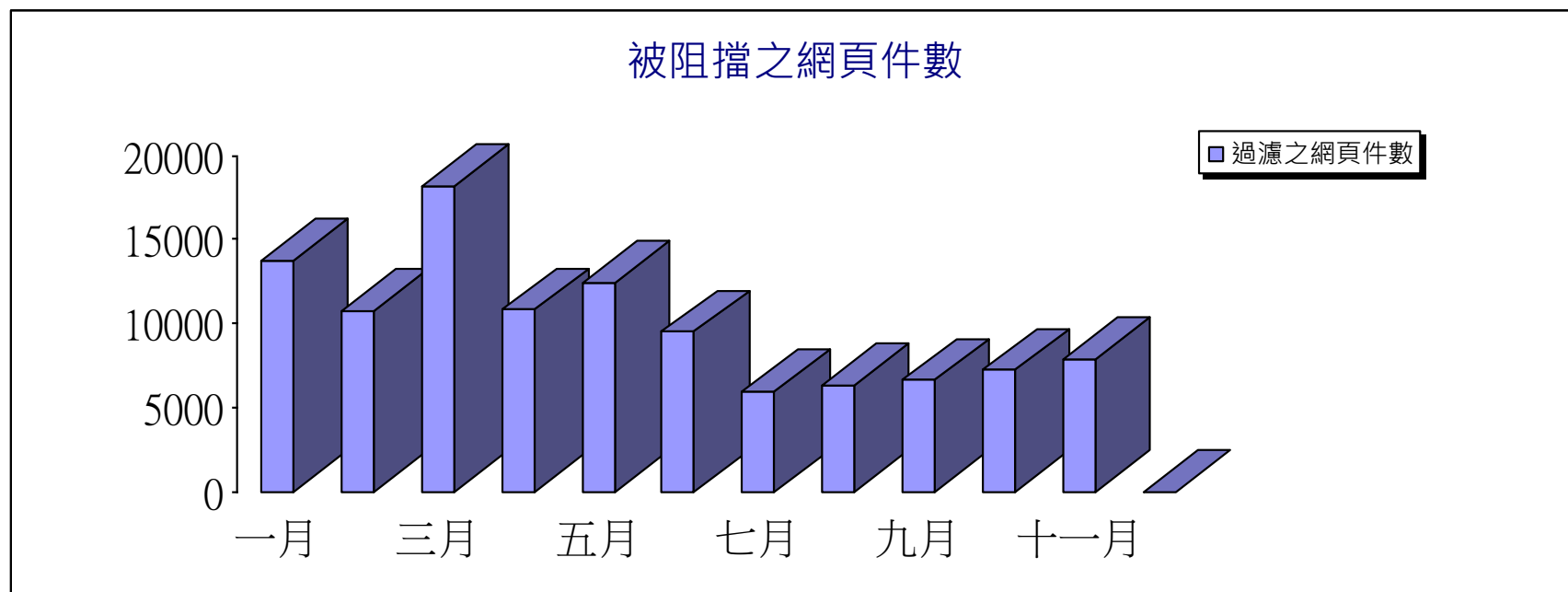


不當資訊過濾防制系統 (1/2)

前 20 名網站 (依網頁計數)



不當資訊過濾防制系統 (2/2)



網路中心及連線學校資安事件緊急通報 處理之效率與通報率

- 1. 區網中心1、2級資安事件量
 - (1). 自行通報數 : 187 件
 - (2). 非自行通報數 : 172 件
 - (3). 平均通報時數 : 2.16 小時
 - 資安事件平均處理時數 : 6.10 小時
 - 資安事件通報平均審核時數 : 16.22 小時
- 2. 區網中心3、4級資安事件量
 - (1). 自行通報數 : 0 件
 - (2). 非自行通報數 : 0 件
 - (3). 平均通報時數 : 0 小時
 - 資安事件平均處理時數 : 0 小時
 - 資安事件通報平均審核時數 : 0 小時
- 3. 資安事件審核數量 : 359 件



網路中心配合本部資安政策

1. 資通安全通報應變平台之所屬學校及單位的聯絡相關資訊完整度：100%

- 由教育部參照資安通報演練作業現況所提供資料，所屬學校資通安全通報應變平台第一、二聯絡人資料完整性100%。

2. 區網網路中心依資通安全應執行事項：

(1) 是否符合防護縱深要求？：是

- 區網中心運用IPS、WAF及相關資安設備進行偵查（Detection）與防堵（Prevention）工作同時也以應用程式弱點掃描系統做資安檢測，如此層層不同的防禦機制確保網路安全。

(2) 是否符合稽核要求？：是

- 區網中心區網中心於98年7月20日通過教育機構資安驗證中心認證。
證照有效日期至101年7月20日止。
100年6月15日再次通過第三年度教育體系資通安全管理規範驗證（ISMS）。

(3) 符合資安專業證照人數：7員

- 七位同仁皆通過「資訊安全管理系統主導稽核員訓練課程」（ISO27001 Lead Auditor Training Course Certificate）並取得證書。

(4) 維護之主要網站進行安全弱點檢測比率：100%

- 區網網站定期進行系統修補與備份，同時也運用弱點掃描系統進行檢測



配合教育部或自辦所屬、連線學校資訊安全 教育訓練及推廣活動

資訊安全推廣活動

日 期	協 辦 單 位	議 題
100/3/30	雲林縣教育網路中心	社交工程與個資安全
100/5/25	環球科技大學	生活中的雲端科技應用
100/6/9	雲林縣教育網路中心	個資法的因應與介紹
100/10/5	國立中正大學	網路著作權
100/11/23	嘉義市教育網路中心	個人資料保護法的介紹與因應
100/11/30	嘉義縣教育網路中心	資安管理與技術

年度營運持續計畫演練

- 雲嘉區網中心100年度營運持續計畫演練
 - (1). 演練計畫書
 - (2). 情境一成果報告及情境二成果報告



網路中心配合教育部資安政策

- 區網中心於98年7月20日通過教育機構資安驗證中心認證。
- 證照有效日期至101年7月20日止。

教育機構資安驗證中心
教育體系資通安全管理規範驗證證書

教育機構
資安驗證中心

證書編號：98072004

茲證明

國立中正大學電子計算機中心(雲嘉區域網路中心)
地址：嘉義縣民雄鄉大學路168號

經評鑑結果為符合教育體系資通安全管理規範(中華民國96年5月30日版)
，予以認可登錄範圍如下：

機房處理 TANet 業務活動之維運作業及學籍系統
之維護作業。

並與適用性聲明書（編號：RNC-CCU-D-012，版次：1.1）相符合。
097-002

原始登錄日期：中華民國 98年 7月20日
發證日期：中華民國 98年 7月20日
有效日期：中華民國101年 7月19日

教育機構資安驗證中心



參、網路中心運作情形



區網中心與連線單位互動

- 本年度召開區網管理委員會議：3次。
- 為了營造良好的互動環境，雲嘉區網親自赴連線單位舉辦5場次智財權及資安議題宣導活動。
- 單位分別為雲林縣網2場次、嘉義縣網1場次、嘉義市網1場次及環球科技大學1場次。



定期召開會議

- 本年度雲嘉區網分別於3/8、8/10及12/1，召開3次管理委員會會議及技術研討會。
- 3/8假獨角仙休閒農場舉辦會議，邀請中華電信及國網中心一起技術研討3個主題。
- 8/10邀請NII吳昭儀 經理做 ISMS 『資訊系統分類、分級』 分享。
- 12/1邀請麟瑞科技張晃峻 副處長做 『互動社群在教學上的應用』 分享。
- 相關會議紀錄網址：<http://ycrc.tanet.edu.tw/asso/>



營運計畫達成狀況與參加率

- 網路中心年度營運計畫達成率：92.9 %。
- 出席TANet會議及活動參與率達75% 以上。
- 區網連線單位會議平均出席率 75 % 。



連線單位通訊資訊有效性

- 隨時針對連線單位網管人員緊急聯絡進行檢視及更新。
- 前項檢核清冊日期為：100.12.2
- 書面資料(現場展示)。



網路使用狀況

- 透過「[雲嘉區網流量統計系統](#)」監督網路狀況。
- 提供雲嘉區網IPv6「[流入](#)」及「[流出](#)」流量統計。



流量統計分析

- 透過「Nagios Core」[監測系統](#)，了解各單位使用率。
- 本系統提供各單位[Hosts](#)及[Services](#)服務狀況。
- 本系統依需求可提供區網各連線單位1年內連線狀況之有效使用率([IPv4](#)、[IPv6](#))。



路由器網路流量分析服務

- 本校透過[Cisco Service Control Engine \(SCE\)](#)系統做路由器網路流量分析。
- 本系統可以提供不同[services](#)流量狀況，包括P2P、Bittorrent、Skype、FTP、SIP、E-mail等之控管。



機房監控與管理

- 雲嘉區網機房透過「**隼眼機房安全監控系統**」監測機房溫度、濕度、UPS輸出/入電壓等。
- 系統會自動傳送**簡訊**及**E-mail**訊息通知管理人員處理。
- 監控網頁網址：<http://140.123.26.8/>



肆、推動網路資訊應用 環境之導入情形



推動相關基礎建置及營運效能

- 對連線學校完成相關的基礎環境的建置並達下列目標
 - 校園網路可使用IPv6環境並自動配送IP，達 18/256=7 %（256網段有18網段使用）。
 - 網路電話互連互通，與教育部完成互通且建置連線學校數：9校，百分比為37.5%。
 - 校園網路之：
 - (A)首頁網站使用IPv6達：10校
 - (B)DNS使用IPv6達：10校
 - (C)提供校園網路語音介接交換功能並支援IPv6達10校
 - 提供校園無線網路漫遊服務(含帳號管理)：是



推廣網路相關應用服務及分享

- 本校免費提供NOPAM系統給學術單位使用，目前約有84單位在使用。
- 開發「數位學習平台」提供其他單位分享。
- 本校吳昇教授開發之NuWeb系統，提供給嘉義縣網分享。



網路電話 VOIP 佈建情形

- 有關區網中心建置SIP Server部分
 - 1.區網於98/3/20完成建置SIP Server系統。
 - 2.目前提供連線單位網路語音交換服務計有9個單位，包括雲林科技大學、虎尾科技大學、吳鳳科技大學、環球科技大學、南華大學、東石高中、協同中學、華南商職及本校等，尚未連線15單位我們努力推廣中。



其他網路應用

- 全國各級學校運動人才資料庫
- 資訊安全監控中心(A-SOC)暨殭屍電腦防禦機制建置計劃
- 資訊能力線上測驗系統



伍、網路應用創新服務情形



RFID在校園安全之應用

- 本中心李新林主任及熊博安組長共同領導之RFID工作團隊，開發「校園安全應用RFID協助學生安全建置」。
- 嘉義啟聰學校及嘉義大學附小協助情境模擬開發。
- [相關資料](#)。



開發中華函授學校課程

- 中華函授學校主要提供華語文及職業技術函授與網路課程。
- 提供海外僑胞終身學習機會。
- 提供海外僑胞函授及網路選讀之雙軌學習服務。
- 建構全球知識學習分享網絡。
- 中華函授學校網址：<http://chcs-opencourse.org/portal/>



陸、辦理教育訓練及推廣活動情形



辦理教育訓練活動及研討會活動

活動類型	日期	活動名稱
網路管理及應用	100/03/08	以OpenSource資源打造高速雲端運算環境
	100/03/08	以OpenID建立Single Sign On服務
資訊安全	100/05/25	生活中的雲端科技應用（環球科技大學）
	100/09/27	惡意軟體的分析與鑑識
	100/11/30	資安管理與技術（嘉義縣網）
智慧財產權	100/03/18	保護智慧財產權及個人資料保護
	100/10/05	網路著作權
個資保護	100/06/09	個資法的因應與介紹（雲林縣網）
	100/11/23	個人資料保護法的介紹與因應（嘉義市網）



維運人力專業能力教育訓練

- 專屬維運及資安人員專業能力教育訓練

(1). 100年06月10日參加由SGS-何星翰產品經理主講之『個資法的衝擊及因應』專題演講。

(2). 100年9月27日參加由警政署-叢培侃巡官主講之『惡意軟體的分析與鑑識』專題演講。

(3). 100年9月27日參加由警政署-李相臣主任主講之『SPAM與網路犯罪現況分析』專題演講。



辦理教育訓練活動情形

- 辦理教育訓練活動全年超過100場次以上
- 內容包括資訊安全與防毒介紹、多媒體：聲音剪輯、統計軟體處理與應用、資料備援與安全保護等。
- 本中心資訊推廣教育網址：
http://osa.ccu.edu.tw/info_class/show_news.php



柒、區網維運配合款及經費運用



經費運用

- 教育部核定計畫金額：\$1,372,500元
- 教育部核定補助金額：\$ 1,372,500元
- 學校編列之自籌金額：\$1,226,995元
- 學校編列之維運配合款：\$ 1,226,995元
- 實際累計執行數(至11/20)：\$2,414,667元



學校對區網配合款

- 本校今年度更新校際無線網路漫遊核心控制模組，費用910,000元。
- 增購乙批Cisco AP共54,995元。
- 添購『機房監控與管理系統』費用200,000元。
- 機房UPS設備維護費用 98,000元。
- 學校對區網配合款\$ 1,226,995元。



捌、綜合建議



綜合建議

- 由於南部往北部電路頻寬經常擁塞，建議教育部能擴充頻寬嘉惠南部學校。
- 雲嘉地區有高中職反應中華電信電路費太貴，建議部裡能要求其降價。
- 感謝教育部長官撥款補助「TANet區網中心基礎維運與資安防護計畫」有關網管及資安人員之聘用，此2位同仁對區網業務推動幫助很大，建議每年持續聘用。



謝謝大家

- 感謝各位評審委員及各位伙伴們
耐心的聆聽。
- 敬請大家指教。

