教育部補助技專校院發展學校重點特色計畫

97 年度計畫成果報告

(資安防護監控技術之教學研究與服務)

(Teaching, Research and Services for Technology of Security Operation Center)

台技(一)字第 0970059628-y 號

全 程 計畫：自民國 97 年 5 月 至民國 99 年 12 月 止
本年度計畫：自民國 97 年 5 月 至民國 97 年 12 月 止

執行學校名稱：中國科技大學
計畫撰寫日期：97 年 11 月 2 日

目錄

圖目錄

壹、計畫基本資料表

計畫型態	■校內整合型　□校際合作型		計畫歸屬	■新申請案　□延續案	
計畫領域	■政策型：（資訊服務　　）□特色型：（　　）				
總計畫名稱	資安防護監控技術之教學研究與服務				
執行單位	■校內：資訊學院 □校際： 主辦學校： 夥伴學校：				
計畫總主持人	姓　名	王伯群	計畫聯絡人	姓　名	陳信宏
	電　話	03-6991358		電　話	02-29313416 ext. 2351
	傳　真			傳　真	02-29336290
	E-mail	borchyun@cute.edu.tw		E-mail	shchen@cute.edu.tw

	執行年度	經常門	資本門	小計（補助經費）	學校配合款	合計(補助經費+配合款)
計畫核定經費	97	0	7,130,000	7,130,000	1,971,000	9,101,000
	合計	0	7,130,000	7,130,000	1,971,000	9,101,000

計畫序號	計畫名稱	主持人	職稱	服務單位
總計畫0	資安防護監控技術之教學與服務	王伯群	院長	資訊學院
分項計畫1	資安防護監控中心系統建置與維運	孫丕華	主任	電算中心
分項計畫2	入侵模式教學環境建置與課程規劃	陳信宏	系主任	資管系
分項計畫3	資安知識庫研究發展與產學合作	蔡輝榮	系主任	資工系

貳、整體計畫中文摘要

近年來企業為反應國際快速變化之環境需求，紛紛導入企業電子化機制，並投入大量電腦及網路資源，然而近年來企業常遭遇「電腦病毒」、「網路攻擊」或「資訊洩露」等危機，依據台經院 2007 年資安調查報告指出，我國網路犯罪與環境風險仍高居不下，國內大型企業投入資安資源經費很高，但中小企業則相對少很多，而資安人力投入部分亦差異甚大，中小企業對資安演練仍不重視，學校資安防護力弱且事件發生率高成為資料外洩死角。

本計畫整合院內各系與校內電算中心相關網路資源與設備，分三年發展本校成為區域資安防護中心為目標，以下分別簡述各年度執行重點：

一、97 年度：

(一)系統整備：以建構『資安防護監控中心(Security Operation Center，以下簡稱 SOC)』[1]為基礎，透過監控校園網路使用環境，電算中心網管人員累積各類資安事件處理能力，為日後學校對外提供社區資安服務奠定基礎。

(二)種子師資培訓：資訊學院彙集各系具備資安專長教師，實施 SOC 操作訓練與國際資安專業證照外，並配合電算中心參與 SOC 實際運作，為次年實務教學活動熱身，亦為區域教學中心注入新能量。

(三)課程規劃：針對 SOC 操作環境能力需求及資安相關知識技能，發展資訊安全學程所需相關課程及教學大綱。

二、98 年度：

(一)教學環境建置：建置為教學使用之 SOC，可將校園實際遭遇之資安事件或攻擊手法導入此一仿真環境，使學生置身於仿真環境學習，增進教學效果，同時可作為教師進行入侵模式研究分析之環境。

(二)學生培訓：依據資安學程課程安排，陸續開放學生選修，並結合國際資安證照輔導，除傳授資安相關專業知識外，配合資安監控實務環境之實習操作，習修者能真實感受網路環境之各項危機，為產業界儲備優異資安人才。

(三)入侵模式研究：SOC 主要功能之一，即是對入侵攻擊事件的即時監控能力，及對長期網路威脅分析與防範建議。利用為教學使用之 SOC 環境，將校園實際遭遇之資安事件或攻擊手法導入，可進一步研析各事件關聯規則。

三、99 年度：

(一)社區資安服務：累積兩年之資安防護監控經驗，電算中心網管人員除可構建校園資安防護網外，並可對外向校區鄰近企業提供資安防護服務。

(二)產學合作：本案相關系種子教師之工作項目及角色是從事 SOC 實務教學及入侵模

式之研究；而產業界負責 工作與角色則是除提供 SOC 之導入協助外，更能提供本校學生實習機會，學生可實際接觸與體驗職場環境，使其更具就業競爭力。

(三)持續進行學生培訓：依據資安學程課程安排，持續開放學生選修，並結合國際資安證照輔導。

總結而言，本計畫包含系統建置規劃、資安專業國際認證課程實施及資源整合、種子教師培訓、學生實習、認證考試、產學合作、社區資安服務與區域教學中心等；預期整體成效，對學校教師而言應可提升實務技能，增進教學效果與擴展實務研究範疇；對學生而言，可得到完整資安防護訓練，以利就業；對資安廠商而言，透過產學合作，增強產學交流有利合作研發；對社區企業而言，有利於提供網路使用之防護；專業認證的引進，將有利於企業選才。

各年度執行重點

年度	計畫項目	
97	系統整備(建構『資安防護監控中心，SOC)	基礎建設建立
	種子師資培訓	
	課程規劃	
98	教學環境建置之 SOC	教學環境建立
	學生培訓	
	入侵模式研究	
99	社區資安服務	社區服務
	產學合作	
	持續進行學生培訓	

參、整體計畫英文摘要

As the global environment marching rapidly, corporations are heading e-business system and investing plenty on computer equipments and network database one by one for survival in latest years. However, the challenges of these corporations are working with on threats of computer virus, network attacks and information leakage crises. According to a survey of information security from Taiwan Institute of Economic Research, there was no tendency to decline in cybercrime and network risk in our country. Nevertheless, small and medium enterprises are poor investment in security compared to the well organized company including human resource. On the other hand, small and medium enterprises do not pay much attention to the security drill. Furthermore, school is another security dark corner and the ratio of incidents is quite high.

In this project, we are going to integrate network resource and equipments from all departments of college of computer science and computer center in our school. The objective is to develop us to be the regional security operation center in three years. Here are our executive key points by each year below:

I. The semester of 97:

A. System preparing: Computer center would accumulate the ability and experience of their administrators by monitoring school network environment under the system of SOC (Security Operation Center) as a practice of community security service.

B. Seed teacher training: Our college of computer science would integrate teachers have expertise in information security to train the operation of SOC and international security certification program. We would be ready for education activities of next year by cooperating with computer center to join the operation of SOC. On the other hand, these training are expected to inspire new ideas of local education center.

C. Curriculum planning: We will plan our relative security curriculum and guideline according to the requirement of operating SOC ability and relative knowledge and skill.

II. The semester of 98:

A. Teaching and learning environment to build: We are going to create a set of SOC for educational purpose, which simulates the real incidents and attacks from school environment. It can be used in course to improve educational effect and analyzed into

attack model by teachers.

B. Student training: We will encourage students to elective by our security curriculum and to counsel with the requirement of international security certification. In our course, we not only impart relative knowledge but also operate and monitor security in reality. Our student can experience all kind of network crisis to become the best employee in the further.

C. Attack model research: One of the major function of SOC is to monitor attack incidents in time and provide analysis and advice of network threats in long term. We will use the experience of security incidents and network attacks happened in school to research the relationship of each incident furthermore.

III. The semester of 99:

A. Community security service: After two years experience of security operating, our computer center administrators can not only construct school security firewall but also provide neighbor corporations managed security service.

B. Business-education cooperative project: In this project, the achievement and main duty of our project teachers are imparting SOC in reality to students and researching attack model. On the other hand, our cooperative business is to assist the implement of SOC and provide job opportunities for our students to experience real career and work. Besides, after these experiences in reality, our students would be much competitive in career.

C. Continued student training: We will keep encourage students to elective security course and counsel with the requirement of international security certification.

To conclude, this project is combined with system construction planning, implementing international security certification program and resource integrating, seed teacher training, student practicing in reality, certification exam, business-education corporate project, community security service and local education center. The expected achievement of teacher would be experiential skill, improving impartation effect and extending the range of research in reality; student would be competitive in career from fully security training. And the benefit of cooperative business would be increasing cooperative research and development through business-education cooperation; regional corporation would be provided network security. Moreover, the recognized of license by corporation will be a benefit of recruitment.

肆、年度計畫執行成果中文摘要

依據核定計畫內容，本年度(97)計畫執行內容主要包括：(1)資安防護監控中心(SOC)之建置；(2) SOC 第二線監控處理分析人員之系統教育訓練；(3)校園重要伺服主機、防火牆、入侵偵測系統、及相關網路設備等之資安防護監控作業；(4)完成資安學程規劃及相關課程教學大綱之研擬;(5)本校電算中心 ISO 27001 [2]資訊安全管理系統制度導入等,計畫執行成果摘述如下：

一、資安防護監控中心(SOC)之建置。

(一) 電腦硬體環境及設備建置部分，於 9/18 完成設備採購與驗收測試。

(二) 資安防護監控軟體平台建置部分，於 8/25~10/24 完成 SOC 系統相關軟體安裝測試。

(三) 資安防護監控室建置，於 9/18 完成內部規劃設計，並施工完畢，自 10/6 起開始監控校園網路。

二、SOC 第二線監控處理分析人員之系統教育訓練。

(一) EC-Council 國際認證技術教育訓練部分，網路安全管理(Network Security Administrator，NSA)[3]課程訓練已於 8/23、24、25、30、31 完成。

(二) EC-Council 國際認證技術教育訓練部分，駭客殺手認證(Certified Ethical Hacker，CEH)[4]課程訓練已於 9/1~5 完成。

(三) 資安防護監控系統之操作教育訓練，配合台灣 Novell[5]原廠教育訓練期程，已於 9/11 完成。

(四) 資安防護監控處理及分析之技術教育訓練，配合台灣 Novell 原廠教育訓練期程，已於 9/12 完成。

(五) EC-Council 國際認證技術教育訓練部分，電腦鑑識認證(Computer Hacking Forensic Investigator，CHFI)[6]課程訓練已於 10/5、6、13、19、20 完成。

(六) EC-Council 國際認證技術教育訓練部分，資訊安全分析及滲透測試認證(EC-Council Security Analyst / License Penetration Tester，ECSA/LPT)[7]課程訓練已於 11/2、9、16、23、30 完成。

(七) Novell Sentinel 平台實務面操作教育訓練，已於 12/1~4 完成。

(八) 截至目前為止，參與本案之種子教師：資訊管理系陳信宏主任已考到 NSA、CEH、CHFI、ECSS [9]四張證照；資訊管理系林華乙老師、李琦峰老師及資訊工程系尹德龍老師亦皆已考到 NSA、ECSS 兩張證照；電算中心系統網路組陳世賢組長已考到 CEH、Security+[8]兩張證照。

三、校園重要伺服主機、防火牆、入侵偵測系統、及相關網路設備等之資安防護監控作業，

已於 10/6 開始啟動。

四、完成資安學程規劃及相關課程教學大綱之研擬

(一)教育部通資安全學程報部，已於 9/18 獲教育部補助通資安全學程申請案，預計 2 年內有 20 位學生可獲得學程證明書。

(二) 資安課程教學大綱，完成「資訊安全」、「資訊安全 ECSS 認證」、「ISO27001 資訊安全管理系統」等三科目設計，且資訊安全、資訊安全 ECSS 認證、資訊安全管理系統(ISO27001)三門科目已開課。

五、本校電算中心 ISO 27001 資訊安全管理系統(ISMS)制度導入，8/28、9/9 已完成檢視現行作業及落差分析報告、8/21 完成 ISO 27001 架構及條文解析、9/3 已完成資訊安全管理系統簡介、9/25 已完成資訊安全風險管理 3 門 ISMS 教育訓練課程、9/12~10/9 完成 5 項 ISMS 四階文件輔導討論、10/20-10/31 進行伺服器群滲透測試、11/15-11/30 進行組織資產風險評鑑、12/15-12/30 進行 ISMS 適用性聲明報告 SOA。

六、已建立整體計畫執行過程管考機制，以求計畫執行更具成效，管考會議每週例行開會，以確保各單位配合無礙。

七、11/28 辦理「校園資安防護監控機制成果發表會」，共 145 人次參加，圓滿完成。

伍、年度計畫執行成果英文摘要

According to our verified project guideline, the main accomplishment of this year (the semester of 97) as follows:

1. Set up Security Operation Center(SOC)
2. Train and educate second line monitoring and data analyst of SOC
3. The security master server, firewall, intrusion detection system and relative network equipments.
4. Complete security curriculum and relative course guideline.
5. Introduce ISO27001[2] information security management system to our computer center.

Our project results summary as follows:

I. Set up Security Operation Center(SOC)

A. Hardware and facilities have been purchased and tested well function on September 18.

B. Stage of SOC and relative software have been set up and tested during August 25 to October 24.

C. Control room of SOC have been designed and implemented on September 18, then operated and monitored our school network since October 6.

II. Training and educating second line monitoring and data analyst of SOC

A. The course of Network Security Administrator, NSA [3] of EC-Council Certification Training was accomplished on August 23, 24, 25, 30 and 31.

B. The course of Certified Ethical Hacker, CEH [4] of EC-Council Certification Training was accomplished on September 1st to 5th.

C. Taiwan Novell [5] training schedule of SOC system operation training was accomplished on September 11.

D. Taiwan Novell training schedule of SOC operation and analysis training was accomplished on September 12.

E. The course of Computer Hacking Forensic Investigator, CHFI [6] of EC-Council Certification Training was accomplished on October 5, 6, 13, 19 and 20.

F. The course of EC-Council Security Analyst/ License Penetration Tester, ECSA/LPT [7] of EC-Council Certification Training was accomplished on November 2, 9, 16, 23 and 30.

G. The training of operating the stage of Novell Sentinel in reality was accomplished during December 1 to 4.

H. So far, seed teachers have these achievements: Department of information management chairman, Shing Hong Chen, has four certificates - NSA, CEH, CHFI and

ECSS; faculty of department of information management, Hua-Yi Lin and Chi-Feng Lee, and Te-Lung Yi, teacher of department of computer science and information engineering, have two certificates - NSA and ECSS; team leader of computer center system and network team, Shin-Shung Chen, has two certificates – CEH and Security+[8].

III. The security master server, firewall, intrusion detection system and relative network equipments was activated on October 6.

IV. Accomplish security curriculum and relative course guideline

A. Our information and communication security program has been submitted and been supported by Ministry of Education on September 18, and expects that there will be 20 students get this program certification within two years.

B. “Information security”,”The guidance of ECSS certification[9]” and “ISO27001 information security management system” had been accomplished course guidelines planning and are running well now.

V. Introduce ISO27001 information security management system (ISMS)[10] to our computer center had been reviewed operation process and reported execution analysis on August 28 and September 9. The framework and clauses explanation of ISO27001 had done on August 21, and the introduction of information security system had done on September 3. Three ISMS training courses of information security risk management had finished on September 25. Five of ISMS four stages guidance discussion had done during September 12 to October 9, and sever group penetration test had run during October 20 to 31. Organization property risk was evaluated during November 15 to 30, and the statement of applicability (SOA) of ISMS was processed during December 15 to 30.

VI. To ensure the project executive accomplishment, we created a control and evaluate system to hold a meeting once a week to communicate with every department.

VII. “Exhibition of Information Security Operation Applied in School” was held successfully on November 28, and there were 145 members anticipated.

陸、年度計畫執行內容及成果說明

一、計畫目標

本計畫構想以建構校園資安防護體系為核心，並朝教學、研究及服務等三方向漸進發展，本計畫預計於 97-99 年度逐年達成下列目標：

(一)建構資安防護實務教學環境：

- 提升師生實務技能
- 培養資安防護人才
- 符合民間企業需求
- 共同建立國家資通安全環境

(二)推動與資安業者產學合作

- 以達實務教學及業界實習之目的
- 以達成產學合作研究之目的

(三)建構資安防護體系

- 協助社區中小企業進行主機監控防護之服務工作
- 建立緊急通報應變處理服務機制。

(四)結合國際資通安全趨勢

- 導入國際資通安全認證教學
- 強化整體資通安全基本認知

二、總計畫與分項計畫，各分項計畫間的整合架構與互動關係

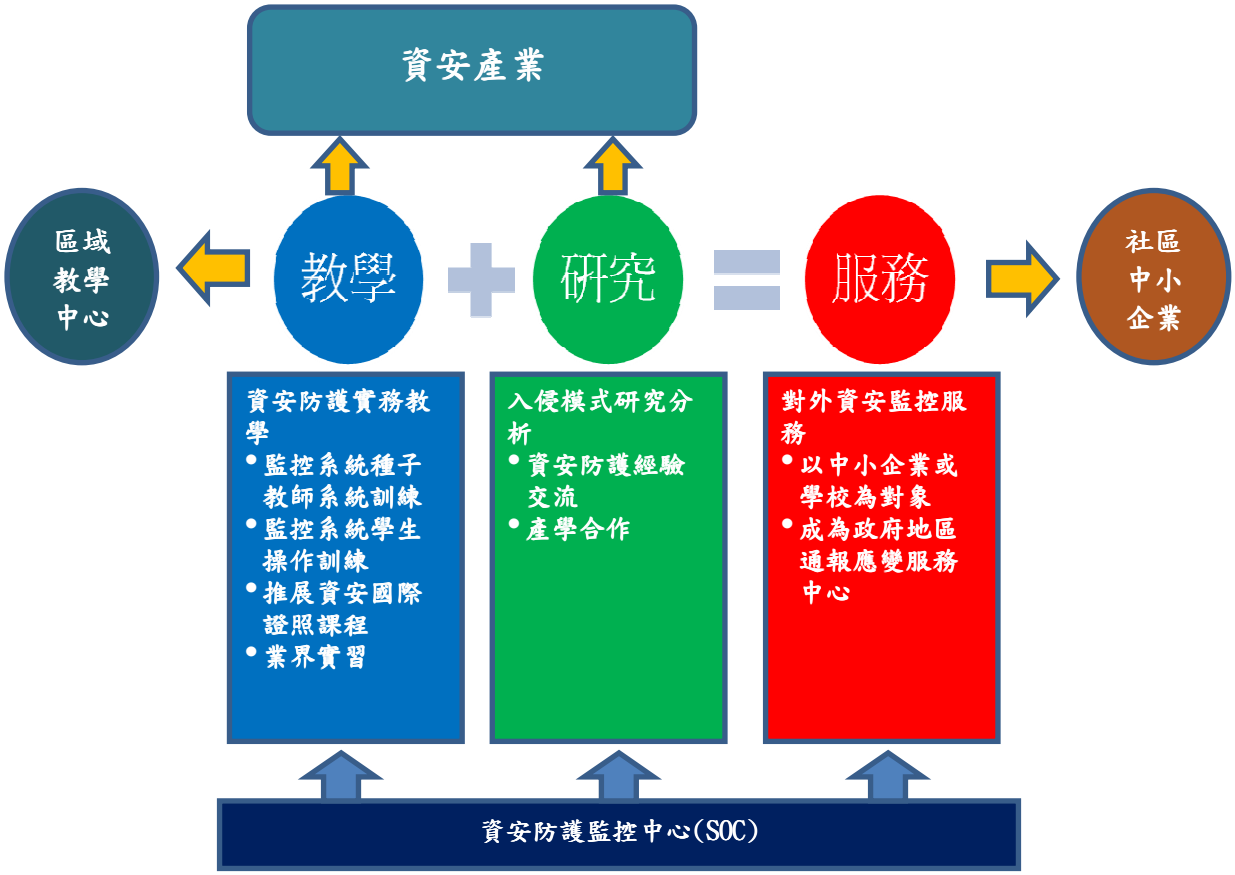


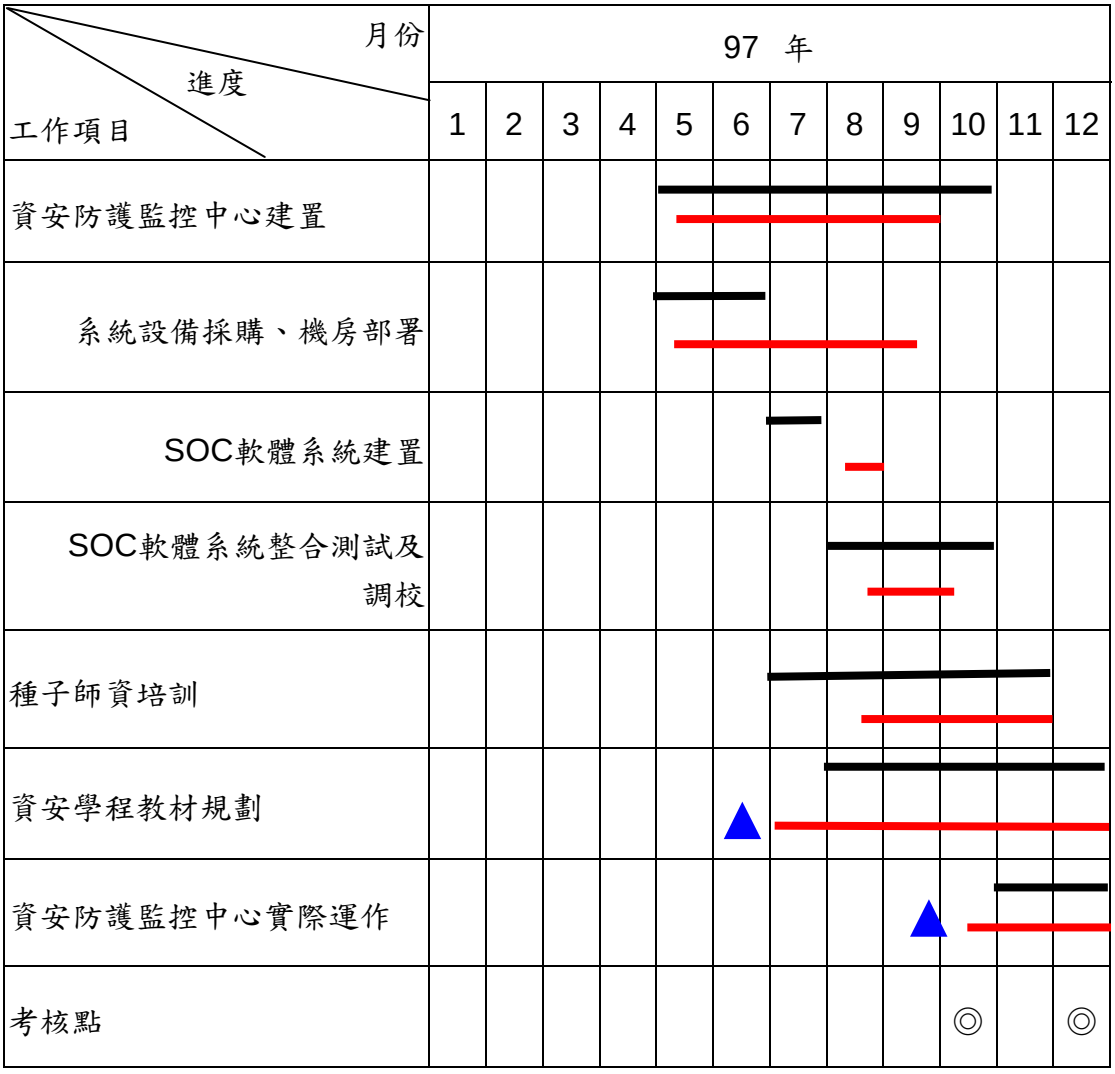
圖 1：計畫構想圖

教學發展部分係以建構一套具備實際資安防護功能之 SOC 教學環境，此環境可訓練資安防護之相關系統操作，並配合本校資安國際認證課程之推動，定期訓練三、四年級資訊學院學生，學生畢業時已具備兩年實務工作經驗，可立即投入資安產業行列服務；而種子教師所累積之資安實務教學經驗，亦可分享區域教學中心各聯盟學校。

研究發展部分，藉由參與電算中心實際 SOC 之運作所累積之實務經驗，並與關貿網路、數聯資安等國內知名資安專業公司實務經驗交流，並請其提供實務上所面對之問題，作為產學合作計畫之議題。透過研究及教學相互運作，充實整體實驗及教學環境，並與國際資安趨勢接軌。

服務發展部分，則以本校電算中心為對象建置資安防護監控中心，本校校園網路為實驗環境，由電算中心人員實際執行資安防護監控任務，而資訊學院相關系科(資工、資管)種子教師協力進行各類資安事件分析作業。透過兩年實際運作，資院師生將累積資安防護之處理及分析能力與實務經驗，此時便可擴展其防護能量，監控代管本校台北及新竹兩校區鄰近企業之主機設備為主，提供鄰近企業資安緊急應變處理之服務。

三、計畫管理



計畫進度：　　實際進度：　　提前之進度：

圖 2：計畫進度甘特圖

(1)資安防護監控中心建置(6 個月)

(A)系統設備採購、機房部署(2 個月)

- ◆ 採購資安防護監控中心所需設備。
- ◆ 機房隔間及所有設備部署。

(B)SOC 軟體系統建置(1 個月)

- ◆ 建置資訊安全訊息管理平台之所有軟體系統。
- ◆ 建置管理作業中心系統。

(C)SOC 軟體系統整合測試及調校(3 個月)

- ◆ 資訊安全訊息管理平台與連接之設備或系統之測試。
- ◆ 資訊安全訊息管理平台之蒐集器運作測試。
- ◆ 資訊安全訊息管理平台之蒐集管理系統運作測試。
- ◆ 資訊安全訊息管理平台之事件關連分析運作測試。
- ◆ 資訊安全訊息管理平台之事件追蹤運作測試。
- ◆ 資訊安全訊息管理平台之報表產生運作測試。
- ◆ 管理作業中心系統之運作測試。

◆ 管理作業中心系統與資訊安全訊息管理平台所有系統之整合測試。

雖因學校作業程序的關係造成資安防護監控中心建置時間稍有延誤，但之後靠著資安團隊反覆檢討改進及合作廠商經驗的教授，終能在原定進度內完成。

(2)種子師資培訓(5 個月)

(A)以本校資訊學院之師資為主，進行相關系統操作及資安教育訓練，若屬國際證照課程，則配合取得考試認證。

(B)參與資訊安全訊息管理平台所有軟體系統之測試作業。

因教材交付的時間遲延，故種子師資課程訓練的部份比原定進度晚一個多月的時間才進行，但最後還是在原定時間內完成訓練課程。

(3)資安學程教材規劃(5 個月)

(A)透過教育訓練及實際參與軟體系統測試後，由種子師資思考資安防護監控中心第一線監控操作人員應該具備之技能、知識，參考教育部顧問室之資通安全課程及國際資安課程，規劃本校之資訊安全學程課程大綱

(B)規劃及設計資訊安全學程教材內容、實作腳本及時數

7/17 即完成教育部通資安全學程計畫申請，9/18 獲教育部同意補助此申請案，目前已完成「資訊安全」、「資訊安全 ECSS 認證」、「ISO27001 資訊安全管理系統」等三科目資安課程教學大綱的設計，且資訊安全、資訊安全 ECSS 認證、資訊安全管理系統(ISO27001)三門科目已開課，進度超前。

(4)資安防護監控中心實際運作(2 個月)

(A)由本校電算中心主導運作

(B)實際監控資訊中心資安設備及主機系統等

(C)事件資料蒐集及智識庫資料建立

原定於 11 月進行，因資安防護監控中心建置比原定時間提早完成，故提前至 10/6 進行。

(5)考核點

(A)9 月考核項目

◆ 資安防護監控中心建置狀況檢核

◆ 種子師資教育訓練及國際證照取得狀況檢核

(B)12 月考核項目

◆ 資安學程課程規劃設計狀況檢核

◆ 資安防護監控中心運作狀況檢核

四、計畫實施方式

(一)建立整體計畫執行過程管考機制,以求計畫執行更具成效,管考會議每週例行開會,以確保各單位配合無礙。且有明確的聯絡窗口,若計畫執行期間產生任何疑問,皆能以最短時間聯繫並解決,確實掌控計畫進度。

(二)計畫專屬網頁之建置 http://ccnt1.cute.edu.tw/mis/97project/index.htm

(三)8/22 EC-Council 國際認證教材到貨,廠商隨即安排種子教師之訓練課程,透過此教育訓練,有 3 位教師已取得 ECSS 與 NSA 證照。

(四)9/18 獲教育部同意補助通資安全學程計畫申請案,目前已完成「資訊安全」、「資訊安全 ECSS 認證」、「ISO27001 資訊安全管理系統」等三科目資安課程教學大綱的設計,且資訊安全、資訊安全 ECSS 認證、資訊安全管理系統(ISO27001)三門科目已開課,

(五)待設備皆就位,隨即安排廠商進行驗收測試,測試完成後即安排 SOC 第一線監控人員及管理者的教育訓練,建立校園資安事件處理的通報回應機制(如圖 2),編製工作手冊,10/6 資安防護監控中心開始實際運作,產生 SOC 運作狀況記錄表、每日事件圖表、每日工作報告表、第一線人員工作記錄表、簽到表等文件。

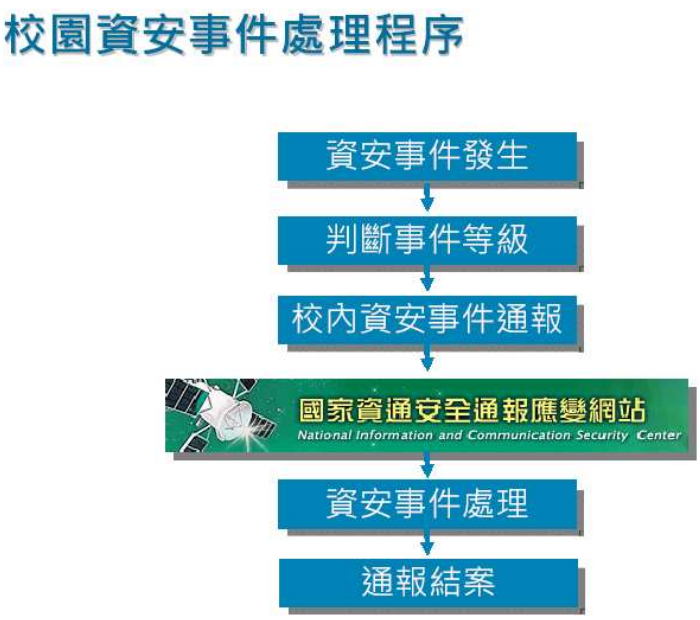


圖 3： 校園資安事件處理程序圖

五、人力運用情形說明

本計畫人力運用之情形，如下表所示：

單位	計畫成員職稱		姓名	工作性質
資訊學院	計畫總主持人		王伯群院長	計畫總主持人
資訊管理系	計畫聯絡人與分項計畫主持人		陳信宏主任	計畫管控
台北校區電算中心	分項計畫主持人		孫丕華主任	校園 SOC 機制建立
資訊工程系	分項計畫主持人		蔡輝榮主任	資安產學合作推動
翊利得資訊公司	系統整合商		邱華明先生	負責專案時程的控管、問題協調、風險管理及資安教育訓練教材的交付。
			張至伶小姐	
			蕭鈺茹小姐	
關貿網路公司	資安防護監控中心系統小組	組長	王瑞祥先生	負責伺服器作業系統安裝、資安防護監控系統功能測試、資安防護監控系統與前端蒐集器運作測試及資安防護監控系統整合測試。
		小組長	黃明哲先生	
		組員	高振元先生	
		組員	蔡惠妙小姐	
Novell 網威		教育訓練	周金龍先生	負責資安防護監控系統教育訓練安排事宜。
捷合科技公司	資安防護監控室建置小組	組長	許清泰先生	負責監控室工程施工、控制台電腦與液晶電視連接顯示施工、投影機架設及線路施工。
		組員	蔡建平先生	

表 2：本計畫人力運用情形

行政支援情況:

單位	組別	人員	工作性質
教務處	教學品質組	余惠平小姐	負責收、發教育部之來文並通知各相關單位。
總務處	事務組	王紫綾小姐	負責設備採購之一切事宜。
	保管組	洪慈蓮組長 朱欣怡小姐	負責設備驗收及財產列帳。
	出納組	周雪娥組長	負責預算管控、經費核銷、傳票製作、撥款等工作。
會計室	會計	廖麗敏主任 林育宣小姐	負責預算管控、經費核銷、傳票製作、撥款等工作。
電算中心	網路組	蘇世昌先生	協助重點特色案網頁之建置。
		羅嘉琪小姐	負責設備驗收及管理。
	新竹網路組	陳朝發先生	負責監督資安監控中心工程之進度與問題回報。
資訊管理系	行政支援	李琦峰老師	負責建置及維護重點特色案專屬網頁。
		朱涵纓小姐	負責設備驗收及管理。
		鄭以君	負責計畫各人員之聯絡、溝通協調事宜。

表 3：行政支援情形

六、經費運用情形說明

本年度教育部補助資本門經費共 713 萬元，學校配合款補助資本門共 7 萬 2000 元、經常門共 189 萬 9000 元。其經費之運用情形如下表所示：

類別	用途	設備	細目	數量	單價	總額	經費來源		實支經費
							教育部補助	校方配合款	
資本門	資安防護監控室建置	監控作業42"液晶顯示器		2	50,000	100,000	100,000		100,000
		管理作業系統主機	電腦主機	2	18,000	36,000	60,000		52,000
			19吋液晶顯示器	2	8,000	16,000			
		單槍投影機		1	29,000	29,000	100,000		41,800
		投影幕		1	12,800	12,800			
		會議桌		1	57,400	57,400	520,000		420,000
		辦公椅		12	2,500	30,000			
		屏風辦公桌		2	7,780	15,560			
		隔間工程		1	317,040	317,040			
資本門	資安防護監控中心硬體環境及設備建置	資料庫伺服器		1	130,000	130,000	280,000		130,000
		CISCO Network Access Controller		2台/1套	297,500	595,000	600,000		595,000
		Sentinel伺服器		1	112,800	112,800	195		112,800
		事件收集伺服器(含WIN 2003 Server R2英文標準版授權 (By Server,含5個Client))		1	105,200	105,200	165,000		105,200
資本	資安防護監控中心	Novell Sentinel 6	作業系統OS：Novell SuSE Linux	3	3,000	9,000	2,690,000	72,000	2,760,000

類別	用途	設備	細目	數量	單價	總額	經費來源		實支經費
							教育部補助	校方配合款	
門	系統軟體(含操作訓練)	資安事件監控與管理平台	資料庫系統DB：Oracle log(含同等品以上版本)	1	100,000	100,000			
			Novell Sentinel 6資安事件監控	1	2,651,000	2,651,000			
		Novell Sentinel 6資安事件監控Advisor知識庫更新	Novell Sentinel 6資安事件監控Advisor知識庫	1	320,000	320,000	320,000		320,000
資本門	種子師資培訓教材	網路安全管理課程教材(國際證照)		6	50,000	300,000	300,000		300,000
		駭客殺手認證課程教材(國際證照)		6	60,000	360,00	360,000		360,000
		電腦鑑識課程教材(國際證照)		6	80,000	480,000	480,000		480,000
		滲透測試課程教材(國際證照)		6	160,000	960,000	960,000		960,000
資本門	資訊安全認證課程工具軟體	Encase軟體		1	112,000	112,000	標餘款463,200	標餘款2,000	465,200
		現場鑑識工具箱		1	58,000	58,000			
	擴充資安事件收集儲存空間	硬碟機		10	27,320	273,200			
		網路交換器		2	11,000	22,000			
經常門	專案技術助理聘用	資管系專案助理,協助處理專案		1	299,000	299,000		299,000	298,396

類別	用途	設備	細目	數量	單價	總額	經費來源		實支經費
							教育部補助	校方配合款	
經常門	成果發表會	校園資安防護監控機制成果發表會		1	100,000	100,000		100,000	120,604
經常門	ISO27001驗證輔導	ISO 27001資訊安全管理系統制度ISMS導入		1	1,500,000	1,500,000		1,500,000	1,480,000
合計						9,101,000	7,130,000	1,971,000	9,101,000

資本門經費之標餘款經鈞部同意，購置現場鑑識工具箱、Encase 軟體、硬碟機、網路交換器 四項設備，共花費 46 萬 5200 元整；另外，經常門人事經費共餘 604 元，ISO27001 驗證輔導標餘款共餘 2 萬元，流至成果發表會運用，共 12 萬 604 元整。

七、 年度計畫執行成效

(一)資安防護監控中心(SOC)之建置：

(A)系統設備採購、機房佈屬

- 本計畫電腦主機設備、投影機相關設備、資安防護監控室建置(含隔間工程)、監控中心系統軟體及網路相關設備等各項資本門設備，已於 8/8 前完成採購程序。
- 網路設備(CISCO network access controller)於 8/5 送達並開立驗收證明。
- 電腦主機設備(含監控室主機、資料庫伺服器、Sentinel 伺服器、事件收集伺服器等)於 8/18 送達並開立驗收證明。
- 投影機相關設備於 8/19 送達並開立驗收證明。
- 種子師資培訓教材：EC-Council NSA、CEH、CHFI、ECSA/LPT 四項教材各六套，已於 8/22 完成交付，置於台北校區資管系辦公室。
- 資安防護監控室建置於 9/18 日驗收完畢，並開立完工證明。(投影機相關設備、資安防護監控室建置(含隔間工程)設置在新竹校區電算中心;資訊相關設備及網路相關設備設置在台北校區電算中心)。

(B) SOC 軟體系統建置

- SOC 軟體系統(Novell Sentinel 6)建置作業由關貿網路公司負責執行，自 8/18~8/22，5 個工作天。
- SOC 軟體系統(Sentinel)，系統操作部分訓練由台灣 Novell 原廠辦理，並於 9/11、9/12 日進行，參訓人員包括本校電算中心網路組成員及種子教師，共計八位參訓。
- 12/1~12/4 進行 Novell Sentinel 平台實務面操作教育訓練服務。

(C) SOC 軟體系統整合測試及調校，由關貿網路公司負責執行，自 8/25~10/24 止。

(二)種子師資培訓

為提升教師資安知能之教育訓練，計畫內安排四種 EC-council 國際資安認證課程(NSA、CEH、 CHFI、ECSA/LPT)，參訓教師包括資工系 2 位教師，資管系 4 位教師；

- 8/23、24、25、30、31 共五日，進行 EC-Council NSA 的訓練課程。
- 9/1~9/5 共五日，進行 EC-Council CEH 的訓練課程。
- 10/5、10/6、10/13、10/19、10/20，共五日，進行 EC-Council CHFI 的訓練課程。
- 11/2、11/9、11/16、11/23、11/30，共五日，進行 EC-Council ECSA/LPT 的訓練課程。

(3)資安學程教材規劃

- 資安學程部分，於 7/17 向教育部提出通資安全學程申請。
- 資安課程教學大綱之研擬：配合 97 學年度開課需求，已完成「資訊安全」、「資訊安全證照輔導(ECSS)」及「資訊安全管理系統(ISO027001)」等 3 課程大綱與教學規範之編撰。

(4)資安防護監控中心實際運作

SOC 實際運作測試，自 10/6 起開始進行，比原訂計畫自 11 月起開始實施，進度超前約一個月。

(5)ISO27001 資訊安全管理系統導入

ISO27001 資訊安全管理系統服務 7 月 15 日公開招標，由工業技術研究院得標，於 8/21、9/3、9/25 進行資訊安全教育訓練，9/9 進行落差分析報告討論，弱點偵測結案報告於 11/14 完成。

(6)資安防護監控機制成果發表會

本計畫於 11/28 辦理為期一天的「校園資安防護監控機制--SOC 成果發表會」，邀請 Novell 台灣網威股份有限公司黃成弘經理、關貿網路股份有限公司網安服務課孫志邦課長及翊利得資訊科技有限公司邱華明副總經理發表演說，並安排 SOC 監控中心實地參觀及解說。當天受邀出席者有清華大學、元智大學、國防大學、臺灣海洋大學、清雲科技大學等知名大學院校之電算中心人員、資訊學群之教職員，本校學生亦熱情參與，共 145 人次參加本次成果發表會。

活動剪影如下：


Novell


會場內禁止飲食


會
會場內禁止飲食









控


音場内禁止飲食



















八、 參考文獻--網路資料

[1]資訊安全服務(SOC) http://www.tradevan.com.tw/web/guest/soc

[2] ISO27001 資訊安全管理驗證服務
http://www.tw.sgs.com/zh_tw/iso_27001_2005_information_security_management_system_certification?serviceId=10015755&lobId=27209

[3] 網路安全管理(Network Security Administrator，NSA)
http://www.mos.org.tw./1gc/ec0808051.asp

[4] 駭客殺手認證(Certified Ethical Hacker，CEH)
http://www.mos.org.tw./1gc/ec0808052.asp

[5] Novell 台灣網威股份有限公司 http://www.novell.net.tw/

[6] 電腦鑑識認證(Computer Hacking Forensic Investigator，CHFI)
http://www.mos.org.tw./1gc/ec0808054.asp

[7] 資訊安全分析及滲透測試認證(EC-Council Security Analyst / License Penetration Tester，ECSA/LPT) http://www.mos.org.tw

[8] Security+ 認證 http://www.iiiedu.org.tw/ites/CS.htm

[9] 資訊安全 ECSS 認證 http://www.mos.org.tw./1gc/ec0808055.asp

柒、經費運用情形一覽表

計畫序號及名稱	年度	本年度核定經費（單位：元，含配合款）					實際執行數（單位：元，含配合款）					執行率（%）			備註
		經常門			資本門(軟硬體設施費)	合計	經常門			資本門(軟硬體設施費)	合計	經常門	資本門	合計	
		人事費	業務費	其他（請說明）			人事費	業務費	其他（請說明）						
分項計畫1：資安防護監控中心系統建置與維運	97	299,000	1,600,000	0	7,202,000	9,101,000	298,396	1,600,604	0	7,202,000	9,101,000	100%	100%	100%	
合計		299,000	1,600,000	0	7,202,000	9,101,000	298,396	1,600,604	0	7,202,000	9,101,000	100%	100%	100%	

註：一、本表所填各項數據應與『經費收支結算表』一致。

二、「經常門」執行率未達80%以上或「資本門」執行率未達90%以上，應於「備註」說明具體理由，並附相關證明文件，否則將依規定刪減、停撥下一年度之經費補助或終止補助。

補充說明：

1.資本門標餘款尚餘 46 萬 5200 元，經鈞部同意增購設備(詳見「經費收支結算表」)。

2.經常門部分，專案助理人事費尚餘 604 元；ISO 27001 資訊安全輔導服務案標餘款尚餘 2 萬元，流為成果發表會推動之經費，共 12 萬 604 元。

捌、年度計畫查核點執行情形

計畫序號及名稱	年度查核點	執行進度			落後原因說明
		超前	符合	落後	
總計畫	1. 資安防護監控中心系統建置與維運		✓		
分項計畫 1：資安防護監控中心系統建置與維運	1. 資安防護監控中心建置狀況	✓			
	2.種子師資教育訓練及國際證照取得狀況		✓		
	3.資安學程課程規劃設計狀況	✓			
	4.資安防護監控中心運作狀況	✓			

※ 「年度查核點」之填寫應與核定後之詳細計畫申請書所列內容一致。

玖、所面臨問題與因應措施

遭遇困難與解決方法	遭遇困難	解決方法
	1.SOC 系統複雜度高，操作人員或教師學習較為耗時，後續維運費用甚高。	與系統廠商互動交流是必要的，定期舉辦 workshop，可以增進技術認知，並可建立業界實習管道，亦期望獲鈞部大力支持，成為技職體系資安教學研究的示範點。
	2.	
	3.	
	4.	
	N.	
特色	1. 為 大 SOC 系統 ， 時進 ISO27001 資安 管 系統 。 以 資安 作 。 2. 資安教 ，資 學 資 安 ， 9 。 3.為 資安人力， 資安 學 ， 學 習， 學 亦 教 部 動 。 4. 實施，與 作 ， 可 SOC 運作 交流 ， 為學 業界實習 定 。 5. 教師 與 ， 6 以 資安 ， 教師 職學 。	