國立台東大學教育學系(所)

教學科技碩士班

碩士論文

指導教授：鄭承昌 先生

電腦病毒迷思概念與概念改變教學成效之研究

研究生：梁雅琇 撰

中華民國九十六年七月

國立台東大學教育學系(所)

教學科技碩士班

碩士論文

電腦病毒迷思概念與概念改變教學成效之研究

研 究 生：梁雅琇　　撰

指導教授：鄭承昌 先生

中華民國九十六年七月

國立台東大學
學位論文考試委員審定書

系所別：教育學系(所)教學科技碩士班

本班 梁雅琇 君

所提之論文 電腦病毒迷思概念與概念改變教學成效之研究

業經本委員會通過合於 ☑ 碩士學位論文 ☐ 博士學位論文 條件

論文學位考試委員會：

王明習
（學位考試委員會主席）

（指導教授）

論文學位考試日期：96年6月29日

國立台東大學

附註：1. 一式二份經學位考試委員會簽後，送交系所辦公室及註冊組或進修部存查。

2. 本表為日夜學制通用，請依個人學制分送教務處或進修部辦理。

博碩士論文授權書

本授權書所授權之論文為本人在 國立台東大學 教育學 系(所)
教學科技碩士班 95 學年度第 2 學期取得 碩 士學位之論文。
論文名稱：電腦病毒迷思概念與概念改變教學成效之研究

本人具有著作財產權之論文全文資料，授予下列單位：

同意	不同意	單　位
☑	☐	國家圖書館
☑	☐	本人畢業學校圖書館

得不限地域、時間與次數以微縮、光碟或其他各種數位化方式重製後散布發行或上載網站，藉由網路傳輸，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為：＿＿＿＿＿＿＿＿，請將全文資料延後半年再公開。

公開時程

立即公開	一年後公開	二年後公開	三年後公開
✓			

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

指導教授姓名：鄭永昌　(親筆簽名)
研究生簽名：梁雅琇　(親筆正楷)
學　　號：g9401007　(務必填寫)
日　　期：中華民國 96 年 7 月 19 日

1.本授權書 (得自 http: //www.lib.nttu.edu.tw/theses/ 下載) 請以黑筆撰寫並影印裝訂於書名頁之次頁。
2.依據 91 學年度第一學期一次教務會議決議:研究生畢業論文「至少需授權學校圖書館數位化，並至遲於三年後上載網路供各界使用及校內瀏覽。」

授權書版本:2005/06/09

謝　辭

沒有想過會來到台東這塊土地上唸書，印象中的台東是放鬆心情的淨地，而我在台東的日子卻是與論文和報告打拼，從研究室看出去的風景是一片藍色的大洋，卻無法盡情享受美麗的景緻；終於，在論文完成後，我可以坐在海邊開懷的吹著海風！

在這段日子以來，感謝指導教授鄭承昌老師，給我們不斷的鼓勵為我們量身訂定階段目標，因為老師的鞭策讓我們能如期完成論文，感謝師母的關懷與照顧，協助我們舒緩緊張的情緒；感謝王明習老師、蔡東鐘老師與連廷嘉老師對我的啓發與建議，讓我對自己的研究有更多的省思；謝謝新生國小的老師提供給我教學的機會，並如此全力支持我。在兩年的學習過程中要感謝的人太多，不只是做研究方法而已，而是學習到更多做事的態度，勇敢的去面對過程中的問題，不要後悔，生活裡就會充滿溫暖。

在求學的過程中，最感謝我的阿爸阿母，給我精神上永遠的支持以及做我的經濟後盾，讓我專心的完成這件事；同時也感謝阿姐們和姊夫時時捎來關心的電話，家庭的支持是繼續前進的動力。

最後，感謝我的男朋友張義斌，陪我走過寫論文的苦與樂；感謝研究室裡的同伴小兔、小貞貞、智元等人的陪伴，在此將論文完成後的歡喜與大家分享，最後要說的話仍是：謝謝大家！

雅琇 謹誌

2007.07

電腦病毒迷思概念與概念改變教學成效之研究

作者：梁雅琇
國立台東大學教育學系(所)教學科技碩士班

摘要

本研究以自編之電腦病毒概念圖作爲發展紙筆測驗及課程內容的架構，並以系統化教學設計中的 ADDIE 模式做爲發展電腦病毒概念改變課程的流程依據，採準實驗研究法，研究對象以方便取樣方式擇取台東市某國小六年級共三個班的學童，設定爲實驗組 1、實驗組 2 以及控制組，人數分別爲 31 人、27 人與 30 人；實驗組 1 的學童施以研究者自編之電腦病毒概念改變課程，實驗組 2 的學童施以電腦病毒推廣教材，而控制組則不施以任何教學。經實驗教學後，以量化統計分析探討三組學生在電腦病毒概念的學習成效，研究結果爲：(一)男學童以及有電腦病毒經驗的學童在電腦病毒概念的前測成就表現較佳；(二)學童每天平均上網時數與學校教師是否曾教授電腦病毒課程此二個背景變項，在電腦病毒概念的前測成就上沒有差異；(三)學童在電腦病毒概念的「基本原則」、「行爲特性」、「廣義病毒」以及「防毒策略」皆存有迷思概念；(四)在教學實驗後，實驗組 1 的電腦病毒概念學習成效測驗顯著優於其他兩組；(五)教學實驗後，仍有些迷思概念無法獲得澄清，分別爲學童認爲電腦病毒是寄生在網路線上進行傳播的、防治電腦病毒觸發最好的方法是調整系統時間、電子郵件病毒可於系統背景下自動發信、立即造成無法正常開機的電腦病毒傳播範圍廣、重要資料備份只要在每年年底執行即可、以及認爲防毒軟體的隔離區即爲系統的資源回收筒上。最後，依據研究結果對於本研究的課程設計與教學提出建議，提供給未來研究者作爲參考。

關鍵字：電腦病毒、迷思概念、實驗研究、系統化教學設計

Computer Virus Misconception and Teaching Effect of Conceptual Change

Ya-Hsiou Liang

ABSTRACT

The purpose of this study is to find misconceptions of computer virus and access the effectiveness of conceptual change after teaching. At first, a conceptual graph was illustrated to present necessary constructs to understand characteristics of computer virus. In order to access the misconceptions of computer virus, a paper-and-pencil test based on the conceptual map then was designed to test the constructs. To reconcile the teaching with strategy and materials and control the other variables that could affect learning, an instructional design based on ADDIE model was performed to develop program for conceptual change of computer virus. A quasi-experimental design was conducted with 3 classes of 6th graders in Taitung City: One class was assigned as an experimental group (E1) with 31 students participated in conceptual change program of computer virus; the second class was assigned as anther experimental group (E2) with 27 students received a program suggested by the Ministry of Education; then the last one was assigned as a controlled group received no treatment. With the test developed in this study, data collections and comparisons were made before and after the programs and among the three classes. The major findings of this study are as follows: 1) Male students and students who have experiences of computer virus infection perform better than the others in pretest; 2) There are no significant differences on pretest in terms of the average of everyday online hours and whether students have been taught computer virus concepts by school teachers; 3) Students have misconceptions on 4 constructs including the fundamental principles of computer virus, characteristics of virus behaviors, general definition of computer virus, and anti-virus strategy; 4) After the treatments, the overall program learning effects of E1 are better than the other groups. However, not all misconceptions are clarified after the designed program.

Keywords：Computer virus, misconception, quasi-experiment, systematic instructional design, ADDIE

目錄

表次

圖次

第一章　緒論

從個人電腦發展史來看，在 1976 年 Apple 首度推出個人電腦前，「電腦病毒」就已略有雛形，但並未定義；Fred Cohen 在 1984 年發表的論文中始對電腦病毒做了明確的定義；1986 年首隻於 MS-DOS 個人電腦運作的病毒「Brain」出現，宣示了電腦安全攻防戰的到來(黃賢麟，2002)。

如今，電腦與生活緊密結合，因此認識電腦病毒與防治應成爲全民須具備的電腦能力之一，若從教育著手，期望可使宣導普及，來提高成效；但研究者發現目前九年一貫資訊教育中雖明訂有關資訊安全相關的能力指標，但因資訊教育僅列於重大議題中，並沒有標準的資訊參考用書，多由資訊教師自行規劃課程，課程中則以訓練學童電腦技能爲主，屬於資訊道德中的電腦病毒議題因此容易受到忽視。

本研究欲探究目前國小學童的電腦病毒概念能力，並以系統化教學設計模式發展一套電腦病毒概念課程，對台東市國小六年級學童進行實驗教學，審視該課程對於學童的電腦病毒概念改變是否具有顯著成效。

本章共分五節，分別爲研究動機、研究目的、研究問題與研究假設、研究範圍以及名詞解釋，分述如後。

第一節　研究動機

Intel 總裁 Craig Barrett 提出 1999 年進入「後個人電腦時代」(Post-Pc Era)(鄭媛媛，2003)，資訊產業的整合、個體間的連結以及獲取資訊都透過網際網路來運作與傳輸;而電腦病毒的發展趨勢與電腦發展史有極高的相關性，1996、1997、1998 年間，每千台電腦中分別有 10、21、31 台電腦感染電腦病毒；但自 1999 年起，首隻藉由電子郵件散佈的病毒 Melissa 現身後，感染率比前年躍升兩倍之多，約爲 80 台，直至 2004 年，每千台電腦仍有 116 台受到感染，感染速率雖趨緩和，但數量卻是逐年增加，其中 92%的病毒以電子郵件爲其傳播途徑 (ICSA, 2004)。人民對於 Email 病毒仍無法確實防禦，

就如 1989 年已知的「buffer overflow」漏洞，仍於 2000 年再次受到病毒攻擊(Spafford, 2000)，相同的錯誤仍持續發生。

綜合上述所見，資訊技術更發達，人民的資訊安全素養未見提高，方便迅速的網路通路反而成爲病毒傳播的重要途徑。

研究者認爲，民眾對於電腦病毒的概念與戒心明顯不足，可能在過去學習的經驗中，未被授與相關知識，或透過不同媒體如電視、同儕、父母獲得錯誤的處理態度與概念，再者因爲方便的網路通道與民眾對電腦的依賴，降低了對電腦病毒的防禦心，而這些錯誤概念亦或稱迷思概念，在未獲得改變前將持續伴隨個體成長。

在從電腦病毒犯罪的年齡層降低來探討，一名高中生入侵「資安人」網站竊取資料，藉以炫耀，在更早之前更曾駭入八個網站，而學校則對他的行爲不甚清楚。最有名的電腦病毒事件爲 1998 撰寫 CIH 病毒的作者，當時仍就讀大同工學院，造成國內許多大企業及民眾個人電腦遭受病毒侵害。不只國內的入侵罪犯年齡層降低，國外亦同，2000 年的「I Love You」情書病毒，是菲律賓馬尼拉的 23 歲年輕人，透過 e-mail 的方法傳送到全球；而美國 18 歲青少年 Jeffrey Lee Parson，則是改寫原版的疾風病毒(Sophos, 2005)。

這些訊息告訴我們目前青少年的學習能力強，且透過網路資訊取得容易，促使犯罪年齡層降低，網路的私密性給予個人盡情發揮的場域，卻成爲資訊安全的死角，這些消息都顯露出資訊安全素養在道德面的淪喪。

要如何指正這些電腦病毒迷思概念，多數專家認爲需透過教育來提升國人對資訊安全的素養與認知，郭耀煌(2006)指出，各級人員對資訊安全議題的不熟識與漠視是造成資安威脅的因素之一；不論個體處於家庭、學校或公司時，都須具備能讓電腦安全作業的策略，因此學校必須訓練學生相關技能，避免在其未具備任何資訊安全訓練前就進入危機環境(Cathie & Evelyn, 2004)；另，Yang (2001)也提到除了技能的訓練，資訊安全的道德教化也是教育課程中重要的課題。由此可知要促使個體概念改變的方法，首重由教育著手，若從我國的教育體系來看，國中小學教育是全民性的，極適合用來宣導與推廣概念性的基本認知能力與態度。

只要有電腦，電腦病毒就有存在的可能，從目前國中小的資訊建設來看，自 1998 年起，行政院實施「擴大內需」方案，工作重點爲使全省國中小都有電腦教室，以上課時一人一機爲目標，並推動台灣學術網路(TANet)至國中小學，於 1999 年 6 月完成全國國小都有電腦教室及網路連線的政策，國中小的電腦軟硬體設備在這段時期已俱全，爲落實以資訊教育來提升資訊技能與素養，教育部於 2001 年宣布「中小學資訊教育總藍圖」，此藍圖的策略著重在透過網際網路使學習無時間與地理的障礙，藉由檔案共享使教材資源更豐富，使校園行政運作有效率，「師師用電腦，班班上網路」網際網路從此深入校園(教育部，2001)，自此，國小即爲目前讓學生最早接觸電腦正規劃教育的學校場域。

根據教育部九年一貫資訊課程綱要中載明，資訊教育的課程目標之一爲導引學生了解資訊倫理、電腦使用安全及資訊相關法律等相關議題(教育部，2003)，但課程綱要中對於資訊倫理與電腦使用安全尚未有明確的範疇與定義，根據 Hong Kong Productivity Council(2004)、ERNST(2004)和中華民國資訊統計網(2005)資訊安全調查資料顯示，電腦病毒(Virus)、蠕蟲(Worm)以及特洛伊木馬(Trojan)是多數公司企業與用戶面臨最大的資安事件，因此於資訊教育課程中教授電腦病毒知識是迫切且必要的，即早接觸電腦病毒議題可提升學童對資訊安全的關切與警覺心。

綜上所述，本研究欲調查國小高年級學童具有哪些電腦病毒迷思概念的主要原因即爲：(1)電腦病毒已成爲全球在資訊發展上的共同威脅，需將此議題加入課程中，藉由教育來喚起全民的注意；(2)電腦犯罪的年齡層降低，因此資訊安全教育必須即早實行；(3)國小爲學校教育中最早讓學生接觸電腦與網際網路的場所，也就是在國小階段，學生就可能面臨電腦病毒的危害；(4)在九年一貫資訊教育的課程能力指標中，高年級學童已有基礎的資訊安全概念，也已習得作業系統的基本操作模式，對於檔案的管理、軟體使用與網際網路的功能與操作都有概念。因此研究者認爲高年級學生已具備了電腦病毒的先備知識，有必要在此時進行電腦病毒迷思概念的檢測，並對學童進行電腦病毒迷思概念改變教學，期望在進入國中後有正確的電腦安全概念，並能遵守網路規範。

基於上述原因，研究者選擇以國小六年級學童進行電腦病毒迷思概念的研究，調查國小階段的學童的電腦病毒迷思概念，並以系統化教學設計模式發展一套電腦病毒概念課程並進行實驗教學，期望此課程能有效澄清學童的電腦病毒迷思概念。

第二節　研究目的

本研究旨在探討國小高年級學童的電腦病毒迷思概念，經由研究者依據相關理論與文獻歸納病毒的概念圖後，自編一份關於電腦病毒概念的紙筆測驗，來分析學童的電腦病毒迷思概念與推論可能形成迷思概念的原因，並作爲發展電腦病毒概念課程時，在需求分析與學童起點行爲階段的參考依據，期望課程能有效提升學童正確的電腦病毒概念。

本研究的研究目的如下：

一、 利用研究者自編電腦病毒概念測驗試卷來分析國小高年級學童的電腦病毒迷思概念。

二、 探討性別、是否有電腦病毒經驗、每天平均上網時數以及學校教師是否曾教授電腦病毒知識，對於學童在電腦病毒概念上是否有差異。

三、 採系統化教學設計模式，設計一套合適的電腦病毒迷思概念改變課程。

四、 探究實驗處理後，評析電腦病毒概念改變課程是否能有效澄清學童的電腦病毒迷思概念。

第三節　研究問題與研究假設

本節分別敘述本研究所欲探究之問題與研究假設：

一、 研究問題：

研究者依據研究目的設定並依循該次序，條列下列研究問題：

1. 探討國小六年級學童具有哪些電腦病毒迷思概念？

2. 探討國小六年級學童的性別、是否有電腦病毒經驗、每天平均上網時數、學校教師是否曾教授電腦病毒知識等因素，在電腦病毒概念前測中的「基本原則」、「行爲特性」、「廣義病毒」、「防毒策略」四個面向的概念上，是否存有顯著差異？

3. 探討國小六年級學童在接受以系統化教學設計發展的電腦病毒概念改變課程後，其電腦病毒概念成就表現是否與接受其他電腦病毒課程的學童有顯著差異？

4. 探討學童在接受教學後是否能有效澄清電腦病毒迷思概念？

二、 研究假設

1. 國小六年級學童在電腦病毒「基本原則」、「行爲特性」、「廣義病毒」、「防毒策略」的概念上具有迷思概念。

2. 性別、是否有電腦病毒經驗、每天平均上網時數、學校教師是否曾教授電腦病毒知識等因素，在電腦病毒概念前測中的「基本原則」、「行爲特性」、「廣義病毒」、「防毒策略」四個面向的概念上有顯著差異。

3. 國小六年級學童在接受以系統化教學設計發展的電腦病毒概念改變課程後，其電腦病毒概念成就表現與接受其他電腦病毒課程的學童有顯著差異。

4. 學童在接受教學後能有效澄清電腦病毒迷思概念。

第四節　名詞解釋

爲提供本研究的閱讀者能快速了解本文中所闡述的觀念，茲將本研究的重要名詞先行說明與定義，使讀者達到有意義的閱讀。

一、電腦病毒：

電腦病毒是一種電腦程式，可以複製自己至電腦中，並將自己附著到電腦檔案裡，當執行檔案時就會執行到病毒程式，進行一些使用者不願意做的事，如刪除檔案、修改資料等破壞正常檔案的行爲，除了這些，電腦病毒並可透過網路或磁片進行散佈，輕者讓個人電腦無預警的當機或佔據部分記憶體資源；嚴重者，會格式化硬碟、刪除檔案或造成電腦無法運作。(Sophos, 2001 ; Symantec, 2004)。

二、迷思概念：

任何概念的形成，與該領域專家的定義不一致，則所形成的概念即被稱爲是迷思概念。

三、電腦病毒概念：

本研究所指的電腦病毒概念，包括能理解構成電腦病毒的基本原則與行爲特性，並能正確區分各式廣義病毒間的差異，在防毒策略面向中則能了解電腦病毒的處理流程與具備防治電腦病毒技巧的概念；綜合言之，本研究所定義的電腦病毒概念範圍限於研究者所發展的電腦病毒概念圖中的各個面向，各面向之詳細定義請參考第三章研究工具中表 3-3-2 電腦病毒概念試卷雙向細目表。

四、電腦病毒迷思概念：

本研究所定義之電腦病毒迷思概念，是指國小六年級學童的電腦病毒概念認知與本研究所定義正確的電腦病毒概念不一致，透過紙筆測驗來估量學童電腦病毒的認知能力，若無法正確作答，即代表學童有迷思概念。

五、系統化教學設計：

教師在發展課程前採階段性、有步驟、有系統的規畫與掌握教學過程中每一個因素，如學習者特質、教學目標、教學方法與評鑑來協助學習者學習，以期達到學習目標，此程序即稱爲系統化教學設計。常見教學設計模式有ASSURE、KEMP、Dick & Carey 以及 ADDIE 等，本研究採 ADDIE 教學設計模式規劃教學課程，該模式以分析(Analysis)、設計(Design)、發展(Development)、實施(Implement)、評鑑(Evaluation)五項階段目標來策畫教學計畫(徐新逸，2003)。


NTTU Library

第二章　文獻探討

電腦病毒起緣已久，自電腦創造以來，電腦病毒即隨之發展並階段性的改變型態，經過數十年來的演變，病毒已成爲電腦用戶在資料維護面最大的威脅；其實，最早有形體的電腦病毒是由三位貝爾實驗室的工程師發展的電腦遊戲，後因電腦病毒程式撰寫方法的公佈與正式的定義，並供給有志趣撰寫者協助與開發；爾後，更因個人電腦使用的普及及網際網路的興起，造成電腦病毒傳播無遠弗屆，防堵電腦病毒則因此成爲全球性的重要工作。

本章將分成七節依序進行探討，從電腦病毒的歷史、電腦病毒概念、迷思概念的定義與研究、電腦病毒迷思概念、資訊教育中與電腦病毒相關之研究、電腦病毒概念圖以及系統化教學設計分述之。

第一節　電腦病毒的歷史

電腦病毒並非近期內的產物，早在 1949 年就由發明電腦的先驅者約翰・范曼紐(John Von Neumann)提出概念，在其所發表的論文「複雜自動裝置的理論及組織的進行」(Theory and Organization of Complicated Automata)裡，即說明了自我複製的程式的概念(李進寶，1990；高大宇、王旭正，2003)。

在十年後，也就是 1959 年，由美國電話電報公司(AT&T)貝爾實驗室的三位工程師 H,Douglas McIlroy、Victor Vysottsky、Robert T.Morris 開發出電腦遊戲「核心大戰(Core War)」亦稱「磁蕊大戰」，由雙方各寫一程式，採 Redstone Code 或爲 Redcode 電腦指令集建立模擬對戰的程式，於記憶體中相互追殺，可覆寫或破壞對方程式留在記憶體中的資料，在受困時會採複製自己一次的方法避免被消滅，遊戲直至將對方趕出記憶體而結束，此電腦遊戲證實了范紐曼所提出的自我複製程式的概念，但該遊戲僅存在於研究室中，並未公開(高大宇、王旭正，2003；黃大任、黃賢麟，2002)。

當時科幻小說也都嘗試以電腦程式作爲正邪二方攻擊道具，1975 年 John Brunner 在其撰寫之科幻小說《The Shockwave Rider》中首度提出「Worm」一詞，故事中描述集權政府利用電腦網路控制人民，後由自由戰士利用「錄

音蟲」(Tapeworm)電腦程式癱瘓集權政府的網路，最終瓦解集權政府(Sophos,2006；黃大任、黃賢麟，2002)；這裡所提出的 Tapeworm 攻擊模式似乎與之後的蠕蟲「Worm」有雷同之處。1977 年另一科幻小說《The Adolescence of P-l》由 Thomas J. Ryan 所著，也假想了可相互感染電腦的病毒，最終感染七千台電腦，引起一場浩劫(徐廣寅，2004)。

傑出電腦獎得獎人也是 Unix 系統的創作者柯恩‧湯普遜(Ken Thompson)於 1983 年的頒獎典禮上公開發表電腦病毒正式存在，並告知如何撰寫電腦病毒程式；同樣是公開病毒撰寫的事例爲 1984 年 A.K.Dewdney 於《Scientific American》月刊的「Computer Recreation」專欄中發表一系列「核心大戰」的文章並協助讀者開發遊戲(李進寶，1990；高大宇、王旭正，2003)。

電腦病毒一詞正式公開定義是在 1984 年，由 Fred Cohen 於美國國防部電腦安全會議中提出，該定義爲「一個能夠修改對方程式，使該程式包含一份病毒本身的複製，來感染對方的程式。」(黃賢麟，2002)。

上述的資料顯示電腦病毒的前身與雛型，第一隻真正被認定爲電腦病毒且具傳播力的程式 Brain(大腦病毒)，爲巴基斯坦的拉荷爾兄弟發展，後於 1986 年由 19 歲青年巴歇特‧亞爾維(Brsit Alvi)撰寫程式，目的是爲了處罰購買盜版軟體的使用者，是一隻具有隱形特性的病毒，可感染啓動磁區，同時也是第一隻可影響 MS-DOS 的病毒(黃賢麟，2002；劉景熙、劉建虹，1994)。

研究者參考多份有關電腦病毒歷史資料，整理如上，接下來將依照電腦發展的歷程來看電腦病毒的發展史。

一、 電腦病毒與電腦發展的相關性

本節將把電腦的發展史與病毒的發展史連結，來對應兩者間的關係，病毒隨著電腦的發展不斷的修正與改變型態，將可透過這樣的比對清楚的看出。

第一代電腦的發展時間爲 1945~1953，又稱真空管時期，在 1946 年發展出第一部自動化數位計算機 ENIAC(杜德煒、杜經文，1985)；在 1949 年時，約翰‧范曼紐(John Von Neumann)提出內儲程式(Stored Program)的觀念，同年就由約翰‧范曼紐提出程式自動複製的概念，由此可知電腦發展前期，電腦病毒就已經具有雛形了。

1970 年代初爲個人電腦時代，在這段時期病毒的消息很少，這是因爲研究室的人員有不成文的規定不公佈這些程式的撰寫法(李進寶，1990)，但從這裡對應到第一節中所提到的作家也都開始撰寫以電腦攻擊爲主軸的科幻小說，可見電腦已是多數民眾認同的產物；在此時除了科幻小說的預測外，確實也有病毒流落在外，1974 年比爾・甘迺迪報導了一隻 Rabbit 病毒，會影響大型電腦，此病毒可能是已知的最早病毒之一(劉景熙、劉建虹，1994)。

1976 年 Steven Job 及 Steve Wozniak 製成了蘋果電腦公司的第一部個人電腦「蘋果一號」，可定位爲第一部真正的個人電腦；在 1977 年推出蘋果二號爲十分成功的個人電腦，個人電腦進入風起雲湧階段(杜德煒、杜經文，1985)。此時期的電腦病毒多以 Apple 爲目標，在 1981 年已有專門攻擊蘋果二號的病毒出現，而於 1983 年初現身的 ELK CLONER VIRUS，感染後會在螢幕上顯示一首詩，並會造成螢幕顯示顛倒或喇叭嗶嗶叫，不過此些病毒在當時並未傳出損害報告(黃賢麟，2002；劉景熙、劉建虹，1994)。

第四代個人電腦於 1981 年由 IBM 所製造，爲 16 位元個人電腦並搭配微軟的 MS DOS 作業系統，稱 IBM PC，在短短三年內佔據了 33%的市場。促使個人電腦更爲茁壯的另一原因，是 1980 年代的教育改革，在 1982 年美國史帝文森理工學院規定大一新生必須備有一部個人電腦，引領電腦進入教育場域，如今電腦已成爲人人必備的工具(杜德煒、杜經文，1985)。

在個人電腦風行的同時，電腦病毒撰寫法於 1983 年被公開，以致於病毒也開始流傳，1986 年首隻可感染 MS DOS 的「Brain」大腦病毒產生，開始了一系列 MS DOS 病毒，此時期的病毒多爲檔案型病毒(感染*.com、*.exe、*.sys)以及開機型病毒(感染開機磁區)，透過磁片進行單機的感染。

1990 年微軟推出 Windows 3.0 版進入 16 位元的作業系統，病毒演變爲可感染 16 位元的 NE 可執行檔案，1992 第一隻 NE 病毒 WINVIR 產生(McAfee, 2006)；微軟於 1995 再推出 32 位元的作業系統 Windows 95，該作業系統的可執行檔案格式爲 PE，1996 年第一隻感染 PE 型病毒 BOZA 現身(Symantec, 2006a；金帥，2006)，原本被設計爲可自動檢查病毒與修復軟碟的 Windows 95 神話就此被打破(微軟，2006；林順喜，1993)。

搭配 Windows 95 所出產的 Microsoft Office 95 含 Word、Excel 、PowerPoint ，這些應用軟體也躲不過病毒的侵襲，1995 年 8 月出現世界第一隻 Word 巨集病毒「WM/Concept」，此病毒更因某些公司出版的光碟片中含有被此病毒感染的檔案，因而擴散開來；而 1996 中旬出現的 XM/Larxou 則爲 Excel 病毒(金帥，2006)。

二、 電腦病毒與網路發展的相關性

1959 年在「磁蕊大戰」病毒被撰寫時，適逢網路發展前期，研究室的研究者們爲避免病毒在個人電腦與網路蓬勃發展的時期造成流行，因此抱持著不公開病毒程式撰寫方法的信念;真正的網路始於 1969 年的 ARPANET 在加州洛杉磯大學、史丹福研究院、加州聖塔芭芭拉大學、猶他大學部署四個節點，同年，密西根大學及 Wayne 州立大學建置了第一個校園網路(陳豐偉，2001)，1970 年在網路初期的年代即有「啄木鳥(Creeper)病毒」(劉景熙、劉建虹，1994)，可在 ARPANET 網路中通行，電腦病毒不單只與電腦發展同步被創造,也與網路共生。網路技術不斷精進,1982 年時 TCP/IP 成爲 ARPANET 的標準通訊協定，Internet 自此始有確切的定義，而 ARPANET 在 1990 年即不復存在(陳豐偉，2001；黃正傑，2000)，一系列的網際網路應用活絡不已，電子郵件、全球資訊網(WWW)、與區域網路、FTP、Telnet 都在此階段醞育而生；正猶如當時研究者的擔憂，1988 年首隻 Internet 病毒誕生，爲康乃爾大學的研究生所做，利用電子郵件的漏洞進行攻擊，透過網路流傳造成六千台主機無法作業，許多郵件就此破壞(李進寶，1990；黃賢麟，2002；劉景熙、劉建虹，1994)。

談到網路的應用，不得不提及帶給我們便利服務的電子郵件 email，但越方便越被人倚賴的工具，越是無法避免被病毒利用，1999 年在中國農曆年過後，首隻利用 email 傳播的病毒「Happy 99」將自己附帶於信件中傳送出去；同年，一隻會感染 Word 檔，並且在感染後會自動發送 50 封附夾病毒檔 LIST.dot 的郵件給信箱連絡簿中的名單，「Melissa」在當時被譽爲是散播能力最強的病毒(金帥，2006)。

網路日益發達，病毒散布的手法也日新月異，WWW 發展成可整合圖形影像、聲音、文字的平台，滿足了大家的需求，專屬網站不單成爲企業組織

的必需品，近年來的部落格則可爲個人打造專屬風格的網頁，瀏覽器已是作業系統必備的要件，但相同的瀏覽器與網頁也被不法人士鎖定目標，2001 年起開始有病毒會感染網頁檔案，如「HappyTime」，同時也有針對瀏覽器漏洞進行攻擊的病毒，如「CodeRed」；網路上的傳播能力遠比早期單機傳染大的多，2003 年的「疾風病毒(Blast)」 透過網路直搗 Windows 作業系統的漏洞，則更讓全球電腦陷入一片淒迷，這些新型態的攻擊手法再加上網路的無遠弗屆，都在在的顯示病毒將依附著電腦持續生存(金帥，2006)。

三、 全球電腦病毒事件概況

根據中華民國資訊統計網(2005)、全球資訊安全報告以及 Hong Kong Productivity Council(2004)調查資料都顯示，電腦病毒(Virus)、蠕蟲(Worm)以及特洛伊木馬(Trojan)是多數公司企業與用戶面臨最大的資安事件。依據陳清芳(2002)的數據顯示，從 Internet 尚未熱絡前，病毒可能要花 3 年才能擴散至全球，而今就算是無心的開啓病毒檔，因傳播的速率變快以及無時空限制的狀況下，約在 4 小時內病毒即可能危害全球的電腦運作(陳清芳、趨勢科技紅色警戒小組，2002)，如表 2-1-1。

表 2-1-1　病毒傳佈全球所需時間

年代	病毒名稱	病毒傳佈全球所需時間
1990 年	Form	3 年
1995 年	WM/Concept	4 個月
1999 年	Mellisa	4 天
2000 年	LoveLetter	4 小時

資料來源：引自陳清芳(2002：180)

ICSA(2004)「病毒來源」調查報告中顯示，目前病毒傳染的最大途徑由早期的磁片演變成網路平台，根據資料可見病毒傳染途徑的前二名分別爲 Email 郵件共佔了 92%、網路瀏覽則佔了 8%。病毒傳播的方式已從傳統的磁片感染轉爲 Email 電子郵件的傳播方式，可知網路爲目前電腦病毒擴散的主要媒介。

除了病毒的傳播速度加快外，病毒所造成的經濟損失更是呈現直線成長狀態，ICSA(2004)提出 2004 年修復被病毒破壞的機器上所花的時間比 2003

年多了 7 個工作天，花費的資金也多了 30100 美元，Computer Economics 整理了 1995~2005 年全球財務受病毒影響的數據，如表 2-1-2：

表 2-1-2　全球財務受病毒影響數據表

年	病毒影響全球財務的金額 (US $)
2005	14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

資料來源：ICSA(2004)

由表中可看出，自 1999 年開始電子郵件病毒出現起，損失的金額即成倍數翻漲，並且沒有消退的跡象，網路平台帶給病毒最好的流通管道，而人們對於電腦的依賴，則是病毒攻擊的最大依據。另，TredLabs 在 2001 年的報告指出，2001 年單由 CodeRed 以及 Sircam 病毒所造成的損失就達 36.7 億，這是因爲 CodeRed 以不同於電子郵件病毒的攻擊手法出現，由此可知每當新型態的病毒出現時總會造成全球大量的損失。

四、 小結

由以上歷史的探究推論，電腦病毒隨著電腦發展的變革不斷衍生新型態的病毒，其對資訊社會的威脅性更因網路的普及而呈現驚人的成長，病毒攻擊事件已是企業組織資訊安全領域中影響最大，並蟬聯多年資訊安全調查報告中最多回報數目的項目；研究者認爲，從電腦病毒的發展歷程中了解病毒的成因與特性，訂定確切的防禦規則，並對資訊教育發展給予關切，提早預測病毒變革走向，以期能有效防範病毒侵略。

第二節　電腦病毒概念

電腦病毒最早且明確的定義爲「一個能夠修改對方程式，使該程式包含一份病毒本身的複製，來感染對方的程式」(Cohen,1984)。同時也作了另一則說明:「有了這樣的感染機制，病毒可以透過電腦或透過網路取得使用者的權限，進而感染程式」，在此定義發表 20 多年後，就如 Cohen 的說法，電腦病毒已成爲全球電腦最大的威脅。

本節將分別以電腦病毒基本定義、電腦病毒行爲特性、電腦病毒種類、電腦病毒的防治方法四項進行電腦病毒概念探究。

一、　電腦病毒基本原則

人們習慣把各種類型的惡意程式，如蠕蟲(Worm)、特洛依木馬(Trojan Horse)都歸類爲電腦病毒，Symantec(2004)、Sophos(2001)以及 Trend(2003)三家防毒軟體廠商指出，電腦病毒(Computer Virus)是一種電腦程式，在未取得電腦使用者的同意下將自己複製至電腦中，並將病毒程式附著到電腦檔案裡，每當執行檔案時就會執行到病毒程式，進行一些使用者不願意做的事，如刪除檔案、修改資料等破壞正常檔案的行爲，除了這些，電腦病毒並可以透過網路或磁片進行散佈，輕者僅讓個人電腦無預警的當機，或佔據些許記憶體資源；嚴重者，會格式化硬碟、刪除檔案或造成電腦無法運作。Ludwig (1996)認爲並非所有具破壞性的程式都是電腦病毒，僅當該程式具有自我複製能力時才可認定爲病毒。對於電腦病毒的定義也有研究者提出不同的看法，其認爲判定是否爲電腦病毒應確認是否該程式會自我複製到其他目標中爲準則，對於那些會詢問使用者意願”你是否想要感染其他檔案”的電腦病毒，若也具有自我自製功能者，也應判定爲電腦病毒(Peter, 2005)。這樣的說法與”未經使用者同意而自我複製”的定義有出入，在本研究中，我們則採用較嚴謹的定義，即具有自我複製能力的惡意程式才稱爲電腦病毒。

而所謂的惡意程式是指一切不懷好意的程式，病毒、蠕蟲、間諜程式等都包含於其中，但因多數人對於各種惡意程式間的差別無法釐清，因此媒體報章雜誌常以「病毒」概稱，負責對抗惡意程式的專業人員則必須要清楚了解期概念間的差異(賴榮樞，2005b)；但也有文獻持相反態度，認爲未經同意

即進入他人電腦中，從事干擾電腦正常運作、損壞檔案或軟硬體的有害程式如蠕蟲、木馬、變形引擎、遠端遙控程式等，這些惡意程式都應納入的電腦病毒的範疇中(林修遠，2002；程秉輝，2004)。

Symantec(2006b)表示電腦病毒、蠕蟲以及特洛依的最大不同點在電腦病毒是將惡意的病毒碼附加在電腦中乾淨的檔案上，蠕蟲以及特洛依木馬則不依附在其他檔案上，而是整個檔案都是惡意程式，如圖 2-2-1；但有些病毒會把病毒碼會完全覆蓋掉乾淨的檔案，造成乾淨的檔案會完全被破壞而無法挽救(黃文杰，2000)，如圖 2-2-2。

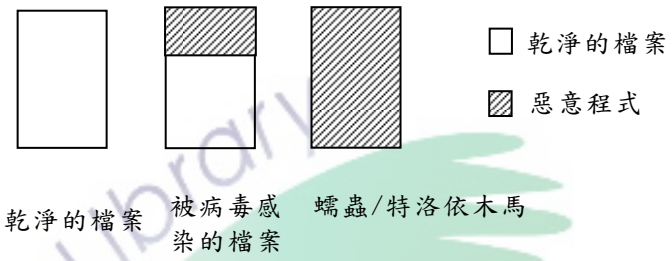


圖 2-2-1　電腦病毒、蠕蟲、木馬感染示意圖
資料來源：Symantec(2004)

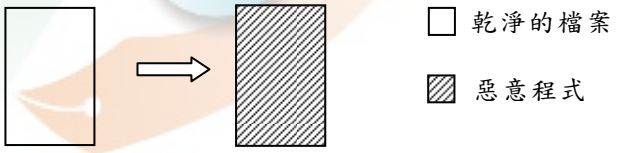


圖 2-2-2　遭病毒完全覆蓋的檔案
資料來源：黃文杰(2000)

正因感染的方式不同，解毒過程也會採不同的對待方式，當偵測到電腦蠕蟲與特洛伊木馬時，防毒軟體採取的方式爲直接刪除該惡意程式；若檔案感染病毒，則需將病毒程式從該檔案中清除，還原成乾淨的檔案。

惡意程式間有相當明確的差異，因此研究者認爲在探討電腦病毒迷思概念的同時應該將惡意程式區分清楚，不該混爲一談，歸納電腦病毒、木馬以及蠕蟲的定義分述如表 2-2-1、表 2-2-2 及表 2-2-3：

表 2-2-1　電腦病毒定義

編號	項目	說明
電腦病毒	未經授權	在使用者不知情或未經使用者同意的狀態下，進入電腦。
	自行複製	將病毒程式碼植入其他執行程式的檔案中，也可能將其執行檔完全取代受感染的檔案。
	自行執行	進行自行複製的原因，是病毒可藉由受感染的檔案執行時也隨之被啓發。

表 2-2-2 電腦蠕蟲定義

編號	項目	說明
蠕蟲	未經授權	電腦病毒在使用者不知情或未經使用者同意的狀態下，進入電腦。
	主動繁殖	不會將病毒程式碼植入其他執行程式的檔案中，只會透過網路不斷的，主動的將病毒本身複製到其他電腦中。

表 2-2-3　特洛依木馬定義

編號	項目	說明
特洛依木馬	未經授權	在使用者不知情或未經使用者同意的狀態下進入。
	被動繁殖	假藉爲正常、有趣或有用的程式吸引使用者下載執行才得以入侵電腦，偷切電腦用的檔案或機密資料，Hawke (2004)指出若木馬像蠕蟲會主動繁殖到網路上的其他電腦中，則木馬作者每天會收到過多的回傳資料，使的檔案過於龐大而無法處理，這是蠕蟲與木馬間差異的主要原因。

由上述定義可以清楚看見，電腦病毒、蠕蟲、木馬程式都具有未經授權的相同定義，但在其傳播的方式上三者都不相同。近年來電腦病毒的發展衍生爲與惡意程式如蠕蟲或木馬程式結合，以達到廣泛傳播的目的，如 2001 年「Nimda 病毒」，除感染 HTML、HTM、ASP 檔外，並利用 IE Unicode 漏洞攻擊 IIS Server；2002 年的「熊蟲蟲(Bugbear)」則結合蠕蟲與木馬程式特性，一方面大量發送信件，並利用 IE 的 IFrame 漏洞進行感染，使用者不需開啓附加檔案僅是瀏覽到此信件即會受到侵入，並植入後門程式，進行遠端遙控並聯合鍵盤側錄來竊取 ID 與密碼等資訊。病毒手法在近幾年呈現多元複雜的狀況，在本研究要探討的是電腦病毒的概念性問題，因此更應將病毒、蠕蟲、木馬等惡意程式的差異給予清楚的定義與界線，此將有助於規範電腦病毒的防治與解毒流程。

二、 電腦病毒行為特性

除了解電腦病毒的基本原則外，也需知悉電腦病毒的行爲特性，才能提早發現中毒徵兆，有效防範電腦病毒。

黃大任、黃賢麟 (2005)指出，電腦病毒藉由修改對方程式，將自己隱藏在受感染的檔案中，在該程式被執行時電腦病毒也隨之被執行，並將病毒製成的結構分成三機制，如表 2-2-4 所示。

表 2-2-4　電腦病毒製成結構三機制

編號	項目	說明
1	感染機制	此爲病毒最重要的行爲之一，即是病毒的自我複製，也就是將病毒程式碼附加於乾淨的檔案中，此行爲也影響了我們對病毒的分類準則，例如開機型病毒即是感染磁碟的開機磁區；檔案型病毒即是感染電腦中的自動執行檔，如 *.exe、*.com 等等，又如有些許病毒採多形技術，改變病毒的程式碼，來逃避防毒軟體偵測；或在檔案感染後，使檔案大小與檔案日期維持不變來躲避使用者直觀的檢查。

表 2-2-4　電腦病毒製成結構三機制(續)

編號	項目	說明
2	行爲機制	電腦受到感染後，因惡意程式的感擾與破壞會造成電腦呈現一些問題，如電腦螢幕顯示訊息或圖示、檔案變大或檔案被刪除、系統操作緩慢、或網路連線速度變慢、大量發送病毒信件等，下手較重的病毒則會將病毒程式覆蓋掉整個乾淨的檔案，使原本的檔案完全被破壞掉或是格式化硬碟；電腦病毒的破壞行爲端看病毒作者的動機與心態，但有時錯誤的程式撰寫或系統的差異都可能產生一些非病毒作者預期會出現的行爲。 基本上，行爲機制愈顯著愈容易被發現，如 Hybris 病毒感染後，會在螢幕上顯示黑白漩渦狀的圖示，使用者無法操作系統畫面；又如 Navidad 與 Emmanuel 感染後會在工具列上產生小圖示；近幾年來最令人束手無策的即是疾風病毒(Blaster)，感染會造成不斷重開機，使用者無法操作電腦而恐慌。
3	觸發機制	病毒侵入電腦後，會設定啓動病毒的時間，使病毒可自動執行繼續進行破壞與傳遞，通常病毒會依據時間日期、或根據計數器來觸發行爲機制，如有名的十三號星期五病毒就會在十三號星期五當天刪除電腦中的執行檔；而台灣 NO.1 巨集病毒，若感染者在在每月十三號時開啓文件，就會在螢幕上出現心算遊戲的方塊視窗來跟你挑戰，若答錯會開啓 20 個文件檔；在病毒觸發前稱爲潛伏期，此時期病毒會盡其所能的感染最多的檔案，但有些病毒會以慢速進行檔案感染，爲避免被偵測到，多數病毒會檢查檔案是否已被感染，避免重複感染。

Cohen 對於電腦病毒特徵描繪，整理如表 2-2-5 所示(引自黃賢麟，2002)：

表 2-2-5　Fred Cohen 電腦病毒三特徵

編號	項目	說明
1	普遍性	病毒作者會以多數人使用的作業系統爲攻擊目標的首要考量，因此目前 Windows 病毒數量多於 Mac 病毒。但 Microsoft Office 可適用於兩種作業系統中，因此巨集病毒可跨平台感染
2	範圍大	多數的病毒一旦開始進行自我複製，就希望能散播的更遠，而讓系統崩潰的病毒，是無法散佈太遠的，因此多數病毒會讓寄主電腦能正常運作，才不至於被滅絕。
3	持久性	病毒能捲土重來。

林修遠(2003)整理出電腦病毒應具有 12 種特性，分述如表 2-2-6：

表 2-2-6　電腦病毒 12 項特性

編號	項目	說明
1	程式性（可執行性）	爲一段可執行的程式，電腦病毒感染可執行檔後，會在該檔案執行時也隨之被執行，病毒程式被執行後若符合觸發機制的設定則開始進行破壞，但只要病毒程式被執行到就會佔去記憶體，可能造成系統功能的喪失。
2	傳染性	電腦病毒感染的途徑最早透過磁碟散佈，僅能感染單機，發展至今能透過多元方法如電子郵件、共享目錄，下載檔案、甚至僅僅瀏覽網頁也會中毒，到近期病毒多利用微軟的系統漏洞進行大規模的攻擊與破壞。
3	潛伏性	電腦病毒具兩種潛伏性，一是傳染的潛伏性，當病毒在進行感染(自我複製到正常的檔案中)時，他的速度是快速的，不會產生外部行爲，因此使用者難以發現。二是病毒程式存在的潛伏性，依附在正常檔案中不易被發現，一但觸發了病毒，就會使對電腦系統產生破壞行爲。

表 2-2-6　電腦病毒 12 項特性(續)

編號	項目	說明
4	可觸發性	促使病毒發作始進行破壞感染或攻擊的技術即爲病毒的觸發性。這些觸發機制是用來控制感染和破壞行爲頻率的程式，當符合觸發條件時(觸發條件有可能是時間、文件型態或某些特定資料)，即會啓動病毒行爲。
5	破壞性	電腦病毒是一段可執行的程式，所以一但電腦病毒執行了，都會佔據系統資源，降低系統的工作效率。病毒的破壞行爲取決電腦病毒設計者的目的，能徹底毀壞電腦系統，使之無法正常作業；或是破壞刪除系統檔案或文件，使資料無法回復，若是幾隻沒有危險性的病毒交叉感染，也有可能造成系統崩潰。
6	攻擊的主動性	病毒是主動攻擊的，因具有不可預測性及衍生性的特性，以至於無法有效遏止與立即偵測。
7	非授權性	非授權性指的是未經過使用者同意即自行載入或執行，侵入後藏匿在正常程式中，隨著該檔案被執行而伴隨著啓動，開始進行病毒行爲，使用者多在不知不覺中受到感染。
8	衍生性	新一款電腦病毒產生後，其病毒結構受有心人複製修改並流通，則會衍生出新的病毒，即稱作「變種」，而這種變種病毒經過翻修可能使其破壞力增強，後果可能更嚴重。如目前變種數最多的爲 NetSky。
9	寄生性（依附性）	一但電腦病毒本身執行了，進入到電腦中，即尋可感染的宿主程式(如執行檔規格的檔案)進行嵌入動作，並可能覆蓋該寄主程式，一旦寄主程式被執行了，病毒也會隨之啓動。
10	不可預見性	從電腦病毒的類型中我們可以發現，病毒設計程式與感染方法會隨著電腦的演進不斷進行更新，雖保有基本特徵，如常駐記憶體、更改中斷向量，但病毒不斷的演化爲躲藏偵測，這些特徵都可以被隱藏，而無法發現。

表 2-2-6　電腦病毒 12 項特性(續)

編號	項目	說明
11	謠言現象	病毒謠言是利用電腦用戶對病毒的防衛心理，敘述有一隻破壞力強大或是目前尚無解毒碼的病毒產生，但這些謠言多數不具有破壞性，只是透過民眾相互告知的心態而大量將訊息傳遞出去，造成網路壅塞。
12	持久性	電腦感染病毒後，即要進行系統及檔案解毒的還原動作，此動作除了感染寄主系統外，還可能會透過網路進行交叉反覆的傳染，要到達完全解毒的過程變的十分複雜與困難，處理的工時因而會增加。

高大宇(2003)指出電腦病毒具下列 8 特性，如表 2-2-7：

表 2-2-7　電腦病毒 8 特性

編號	項目	說明
1	未知性	當防毒軟體顯示無病毒存在，是否真的就代表沒有病毒，防毒軟體依據其所有的病毒碼去偵測病毒，當未有新病毒的檢查碼時，使用者則無法確保電腦是乾淨的。
2	傳播速度快	病毒碼的開放與網路的普及，且病毒多半沒有特定的攻擊目標，因此會造成大量的流傳。
3	多樣性	電腦病毒不單單只影響電腦主機，透過網路也影響了個人電腦用戶，並結合病毒、蠕蟲、木馬等惡意程式進行攻擊。
4	破壞性	病毒發作可以產生訊息、動畫或毀損系統，有些病毒並無顯著破壞行爲，但仍會佔取一些系統資源，破壞行爲越明顯，則更容易被發現，這裡指出最可怕的病毒是靜靜的潛伏在電腦中進行感染，在一次觸發後大舉毀壞資料，因此電腦病毒的破壞程度去取決於病毒作者的動機與心態。

表 2-2-7　電腦病毒 8 特性(續)

編號	項目	說明
5	感染性	病毒初進入電腦時，採緩慢的形式進行檔案的感染，會主動的尋找可感染的檔案，可能將程式碼編碼、改變特徵字串，採隱藏方式降低被發現機率；或將程式碼切割成小塊，置於不同檔案磁區，必要時在相互呼叫爲了逃避追蹤，並不立即破壞系統，竭盡所能的讓病毒程式成長與備份。
6	傳染性	可透過磁片、檔案交換、網路傳輸來傳染。
7	觸發性	靠時間日期或特定數字與文字或計數器來啓發病毒破壞行爲，一但符合條件就行破壞動作，
8	難以滅絕性	沒有人敢宣稱一隻病毒完全絕跡，因病毒碼的公開加深根除病毒的困難性。

依據上述所整理之資料發現，電腦病毒行爲特性的命名，因每位作者不同定義而有差異，研究者依循各個特性之定義，將具有相同概念的行爲特性進行整合，未來將融入於研究者自編之電腦病毒概念測驗試卷與電腦病毒概念課程中。針對 Fred Cohen 提出的「範圍大」的特性，因涉及病毒的破壞力，因此將此特性歸納爲「破壞性」，而「普及性」因與寄主電腦相關，因此納入「自我複製」的基本定義中。在林修遠所提出的 12 項特性中，其中「程式性」、以及「寄生性」都屬於電腦病毒的基本原則，而「謠言現象」此特性研究者則認爲屬於惡意程式中的「謠言信」。最後，高大宇提出「傳播速度快」此性質則與林修遠所提的「攻擊主動性」相關，「難以滅絕性」即是多數研究者認爲的「持久性」，再者「多樣性」、「未知性」與「衍生性」的定義則與林修遠所提的「不可預測性」相仿。

研究者在進行病毒特色整理時也發現到，自電子郵件病毒流傳後，會利用信件主旨、內文或附加檔案的僞裝計巧，來引誘使用者開啓含帶電腦病毒的附加檔案，增加病毒傳播機會，且在節慶前期更是病毒郵件散佈的好時機，如情人節、新年假借賀卡方式、假裝爲微軟的更新程式或冒用防毒軟體的名聲，如在信件中有 Happy Valentines day 的字眼，或說明某防毒軟體廠商證實該附件無毒等訊息，來提高用戶對信件的信任度，因此研究者將病毒的「僞裝技巧」附屬於「不可預見性」中。

綜合上述所言，研究者將電腦病毒的行爲特性分爲八項，分別爲「非授權性」、「傳染性」、「主動攻擊性」、「持久性」、「不可預見性」、「破壞性」、「觸發性」、「潛伏性」。

三、 電腦病毒種類

研究者發現，過去對電腦病毒種類做分類的依據多以年代區隔，陳清芳、趨勢科技紅色警戒小組(2002)將電腦病毒類別分爲四個發展階段，如表 2-2-8：

表 2-2-8 電腦病毒發展趨勢(一)

電腦病毒發展趨勢				
年代	1987-1993	1993-1995	1995-1998	1998-目前
病毒種類	*DOS 檔案型 *DOS 常駐型 *開機型 *毀滅型木馬	*Win16 檔案型	*MSOffice 系列巨集病毒 *後門程式	*Win32 檔案型 *Win32 常駐型 *跨應用程式感染型 *DDOS 阻斷型木馬 *遠端遙控型 木馬 *e-mail 蠕蟲 *區網型蠕蟲 *系統漏洞型 蠕蟲

另外，高大宇、王旭正(2003)則將病毒區分爲二大期，如表 2-2-9：

表 2-2-9 電腦病毒發展趨勢(二)

電腦病毒時代典型	
傳統型電腦病毒 早期	綜合型病毒 1990~目前
*檔案型病毒 *開機型病毒 *巨集型病毒	內建電腦病毒、蠕蟲、木馬以及攻擊工具，稱綜合型病毒

林修遠(2003)將電腦病毒分爲三波，如表 2-2-10：

表 2-2-10　電腦病毒發展趨勢(三)

波期	第一波：早期的病毒	第二波：網路時代 90 年代中期	第三波：蟲的回合 90 年代末期
病毒種類	*開機型病毒 *檔案型病毒 *第一代的蟲 *謠言信 *連鎖信 *特洛伊木馬	*巨集病毒 *第二代的蟲	*描述語言病毒 *駭客型病毒

爲統合這些不一致的時期階段，研究者依照第一節電腦病毒的發展史，重新歸納病毒種類的發展趨勢，並對病毒種類進行說明，如表 2-2-11：

表 2-2-11　電腦病毒發展趨勢(四)

年代	1986-1992 MS DOS 病毒	1992-1999 Windows 病毒	1999-至今 綜合型態的網路時代
病毒種類	*開機型病毒 *檔案型病毒 *混合型病毒 *第一代蠕蟲	*NE、PE 格式檔案型病毒 *巨集病毒	*e-mail 病毒 *描述語言病毒 *駭客型病毒

(一) 1986-1992 MS DOS 病毒

1、 開機型病毒：

以 1986 被認定爲第一隻病毒的程式「Brain」爲開機型病毒的先例。開機型病毒藏在磁碟片啓動磁區和硬碟的啓動磁區或系統分割表，因爲 DOS 的設計，病毒會在開機後與作業系統啓動前被載入記憶體中，因此可對 DOS 系統做完全的控制並能繼續感染其他插入的磁片或硬碟，又稱爲系統型病毒。感染的過程爲在乾淨的磁片中，先複製啓動磁區 0，並將病毒

碼覆寫到啓動磁區 0，因此如利用受感染的磁片開機，就因此會先執行到病毒,然後病毒再重新指向到原始的開機磁區 0,使系統仍能正常的運作(高大宇、王旭正，2003；陳清芳、趨勢科技紅色警戒小組，2002；黃明仁，1993；劉景熙、劉建虹，1994)。

而有名的開機型病毒如「米開朗基羅」,每年 3 月 6 日發作,行 Format 硬碟之破壞行爲。

2、 檔案型病毒

1987 年所發現的「Lehigh 病毒」爲首隻檔案型病毒,感染 MS DOS 下的 command.com 檔案(劉景熙、劉建虹，1994)。檔案型病毒是將病毒程式碼附著在可執行檔案中，在 MS DOS 時期的執行檔爲*.COM、*.EXE、*.SYS、*.BAT、*.OVL，藉由受感染的執行檔被開啓，病毒程式也因此被執行，繼續感染其他檔案，又可分爲常駐型與非常駐型：

(1) 常駐型：感染的執行檔開啓後，病毒即常駐於記憶體，可持續感染其他檔案。
(2) 非常駐型：執行受感染的檔案後，會開始搜尋可感染的對象並加以感染。

有名的檔案型病毒如「十三號星期五」，爲非常駐型病毒，感染 command.com 以外的*.com 檔，遇到 13 號星期五時，會刪除使用者執行的中毒程式(陳清芳、趨勢科技紅色警戒小組，2002；黃明仁，1993)。

3、 混合型病毒

兼具有開機型及檔案型病毒特性的病毒，可以感染執行檔以及開機磁區，因此傳染力比上述兩者更厲害。

4、 第一代蠕蟲

蠕蟲與病毒的最大差異在病毒需依附在其他程式上執行，而蠕蟲不需有寄主程式，由本身的自我複製以及透過網路連結來造成電腦間的感染，早期的蠕蟲如 1987 年「Chrismas Tree 蟲」在 IBM 公司的內部網路中流竄，

利用連鎖信型態引誘收件者去執行該程式，執行後會在螢幕上呈現一棵聖誕樹，同時也將蠕蟲自己再寄給通訊錄中的電子郵件帳號。

1988 年的「Inernet Worm」則是利用郵件軟體的漏洞進行傳播，於當時造成大量郵件主機運作停擺及郵件的遺失。

(二) 1992-1999 Windows 病毒

1、 NE、PE 格式視窗型病毒

NE 與 PE 分別爲 Win3.x 以及 Win9.x 的執行檔規格，這裡所指的 NE、PE 格式視窗型病毒其感染程序與 DOS 檔案型病毒雷同，透過用戶執行被感染的程式，來感染電腦檔案。在此時期，最著名的 PE 格式視窗型病毒爲 1998 年的「CIH 病毒」，電腦中毒後，使用檔案總管瀏覽到副檔名爲 EXE 者均會被此病毒感染；發作時，會將記憶體的內容貼到硬碟的 Partition、Boot、FAT、ROOT 以及資料區，BIOS 也會被填入垃圾碼，導致硬碟無法開機，必須更換 BIOS 晶片或直接更換主機板(金帥，2006)，圖 2-2-4 爲 CIH 感染檔案的方式。

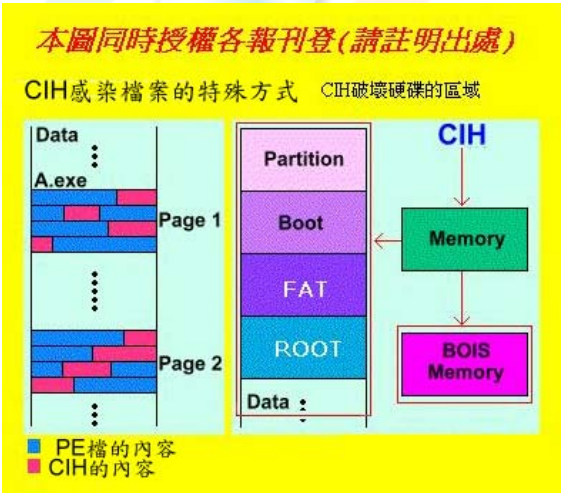


圖 2-2-4 CIH 病毒感染流程圖

資料來源：引自金帥(2006)

因 CIH 病毒出現後，對於電腦病毒無法破壞硬體的說法已受到考驗，且 CIH 並非第一隻讓使用者丟棄硬體的電腦病毒，但目前仍沒有確實的數字統計有多少因電腦病毒而被丟棄的硬體(黃賢麟，2002)。

目前常被電腦病毒利用的執行檔規格爲*.exe、*.com*、*.scr 、*.pif 、*.ocx、*.lnk、*.bat。

2、 巨集病毒

巨集是使用者將一連串重複動作重新定義成一個自動化程序指令的工具，可省去許多繁雜的例行性工作。一但巨集指令被電腦病毒利用後，可以做到執行、建立病毒碼、或將病毒碼複製到其文件等動作，凡軟體具有巨集功能者，都可能受到感染。目前則以廣爲使用也可跨 Windows 及 Mac 平台運作的 MS Office 最常成爲巨集病毒下手的目標，以感染 Word 爲例，病毒將惡意的巨集程式寫入 Word 的共用範本檔 NORMAL.DOT 中，利用各種常見的巨集語法如 AutoExec、AutoNew、AutiOpen、AutoClose、AutoExit、FileSave 等巨集指令(黃文杰，2000；黃大任、黃賢麟，2002)，使用者在開啓 Word 程式、開啓新舊檔、關閉文件程式或儲存檔案等相關動作時，都會觸發病毒來感染其他文件檔，目前已經有發現感染 Word、Excel 以及 PowerPoint 文件的病毒，有名病毒如「台灣 No 1」，病毒發作時會與用戶玩猜數字遊戲，如圖 2-2-5，若猜錯則會開啓 20 份 Word 視窗，一直循環下去，直到答對。

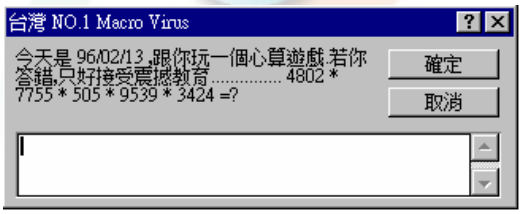


圖 2-2-5　台灣 NO.1 病毒發作圖

資料來源：金帥(2006)

巨集病毒的程式語言與 script 語言類似，因此若巨集惡意程式附著在 Word、Excel 等文件中時就是巨集病毒，若是附著網頁格式的 Script 程式中，就是描述語言病毒，如副檔名爲*.vbs、*.vba、*.vbe 等的檔案，只是兩者寄主程式不同的差異而已。

(三) 1999-至今 綜合型態的網路時代

1、 E-Mail 病毒

自 1999 年來，病毒開始以 e-mail 的傳播方式大規模掃蕩電腦用戶，將各式型態的病毒如巨集病毒、檔案型病毒、VBS 病毒、蠕蟲、木馬等皆可以郵件附加檔案傳送(Shin, 2004；劉順德，2000)。此類病毒具自動發信機制可自行將病毒檔案傳遞給感染電腦 Outlook 聯絡簿中的所有帳號，除造成大規模感染外，也造成網路擁塞，使組織運作停擺。

這時期的郵件病毒，爲了讓使用者開啓附加檔案多採取誘騙手法，採取的方法爲利用吸引人的主旨與內文、假借爲好友的寄件者姓名等方式，如 1999 年的「Happy99」主旨是假借新年賀卡的標題"Happy New Year 1999 !!"，而「Mellisa」信件主旨爲"Important Message"，採用社會工程的心理操控手法來哄騙電腦用戶中毒，來達到病毒作者的目的(黃賢麟，2002)。

根據 Dong & Hsiu(2004)統計的資料中顯示各種類型的病毒利用 e-mail 做爲傳播工具的比例中可知最常使用 e-mail 爲傳播媒介的是蠕蟲，也可看出大多數的病毒都會採此方法來散播，如圖 2-2-6：

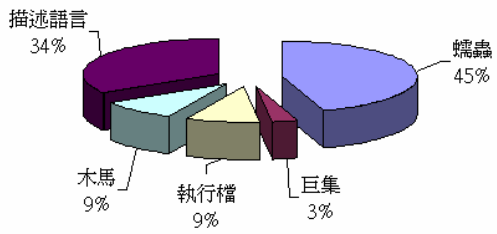


圖 2-2-6 e-mail 夾帶病毒類型比例圖

資料來源：Dong & Hsiu, 2004

在該文獻中也統計出最常被用來當作附加檔案的副檔名格式比例，這些資料值得提出來讓用戶在收電子郵件時多加注意，資料如表 2-2-12：

表 2-2-12 電子郵件附加檔案的副檔名比例

附件格式	EXE	VBS	SCR	PIF	BAT	CHM	COM	DOC	Others
比例	50%	18.6%	11.4%	11.4%	11.4%	5.7%	4.3%	4.3%	14.3%

資料來源：Dong & Hsiu, 2004

2、 描述語言病毒

1998 年推出 Windows98 始預設有 WSH(Windows Script Host)，這是 Windows 系統的 Script 執行環境，用來簡化一些系統中重複性或例行性高的流程，可直譯 VBScript 以及 JavaScript，日後的 ASP 則以此爲基本架構再行擴展；若將 WSH 架構嵌入軟體中就成爲應用軟體的巨集語言(賴榮樞，2005a)，由此推知也可產生巨集病毒了。

多數的描述語言病毒以 VBScript、JavaScript、ActiveX 程式撰寫爲主，原本是是爲了擴充 Html 的網頁功能，卻成爲電腦病毒毒害他人的手法，VBS 病毒剛開始不久，世界第一個 VBS 病毒產生器「Senna Spy Internet Worm Generator 2000」現身，只要輸入病毒名字、信件主題、信件內容，就可以製造出一堆 VBS 病毒。

圖 2-2-7 VBS 病毒產生器介面

資料來源：金帥(2006)

常用的傳播方法如將含有惡意程式的*.vbs 當信件附加檔案傳送出去，這時期的描述語言除了在主旨或內文上採社會工程的誘騙手法外，也利用雙副檔名的格式誘騙使用者上當，如 2000 年的「LoveLetter 情書病毒」

其附加檔案爲 LOVE-LETTER-FOR-YOU.TXT.vbs；2001 年的安納庫妮可娃「AnnaKournikova 病毒」，附加檔案爲 AnnaKournikova.jpg.vbs，因爲*.txt 以及*.jpg 都不是可執行檔規格，會讓使用者信不覺有毒而開啓；2002 年的「Winl0g0n」蠕蟲附加檔案則爲”Readme.txt .pif” (副檔名中間空了很多空白)，過長的附加檔案名稱，會讓使用者看不到真實的檔案格式，如圖 2-2-8，雙副檔案以及檔名過長的手法爲當時 e-mail 病毒喜愛使用的方法。

圖 2-2-8　Winl0g0n 蠕蟲信件

資料來源：研究者製圖

除了以郵件附加檔案傳播之外，另一種方法爲於信件內文中嵌入惡意 Script 語法，具有與巨集病毒有異曲同工之妙之處，使用者僅是閱讀該網頁格式的內文，不用執行附加檔案，也能自動啓發病毒，如 2000 年的「BubbleBoy」是第一隻閱讀信件內文就會啓動病毒，見圖 2-2-9，這其實是微軟 IE 瀏覽器的漏洞所致，但微軟也早於 1999 年 10 月 2 日就釋放更新包給使用者更新，由此可知使用者對於系統更新的疏忽與漠視。演化後的 VBS 病毒也可感染在區域網路中搜尋到描述性語法檔案如*.vbs、*.vbe、*.js、*.jse、*.css、*.wsh、*.sct、*.hta 等檔案格式。

圖 2-2-9　BubbleBoy 病毒信件

資料來源：金帥(2006)

3、 駭客型病毒

駭客的目的是是入侵他人或組織企業電腦，藉以竊取資料，多以微軟系統漏洞來攻堅防衛較縝密的機關，若無法直接入侵目標電腦，則改採電子郵件夾帶病毒、木馬程式以期達到其目標(Hawke, 2004)，當駭客與病毒結合後，將使破壞行爲更強勁。

2001 年 7 月「CodeRed」結合駭客與蠕蟲攻擊微軟 Windows NT/2000 IIS 系統漏洞來植入後門程式,造成電腦重複開機及連續不斷的攻擊網路上的電腦，引起網路延宕；金帥(2006)指出，就算用戶更新病毒定義檔也無法有效防制「CoreRed」變種駭蟲，唯一有效的方式爲下載微軟所釋放的系統修正檔進行安裝,單就 CoreRed 的影響,全球約 100 萬台電腦受攻擊，損失約 26.2 億美元(陳清芳、趨勢科技紅色警戒小組，2002)。同年 9 月，「Nimda」掀起另一波高峰，結合駭客、蠕蟲及描述語言病毒展開襲擊與破壞，利用 Unicode 漏洞攻擊 IIS Server，並感染該機中的 HTML、HTM、ASP 檔，並持續對其他網站發出攻擊行爲，而用戶端一旦瀏覽受感染的網頁就會中毒，並刪除區域網路中的*.exe 檔以及自動發送附加檔案爲 readme.eml 的信件，攻擊猛烈並以多重管道同時進行。

目前常見的系統漏洞有 IIS、Apache、FTP Server、MIME、IFrame 或 SQL Server 以及 MySQL 都已有相關的病毒產生。

除了上述的電腦病毒、蠕蟲和特洛伊木馬，在黃大任與黃賢麟(2005)及陳清芳(2002)都爲惡作劇病毒或謠言提出解釋，研究者統稱這些爲「病毒謠言」。病毒謠言的基本概念是信件中宣稱有一隻破壞力及傳染性的病毒，但大多數這些病毒是不存在，該信件的目的僅是爲了讓收件者恐慌，進而轉寄信件，這些大量寄出的郵件可能造成網路擁塞，在轉信的過程中，工作時間也被浪費掉，且使用者也可能聽由信件建議刪除了某些檔案，造成系統無法正常運作。

不同的電腦病毒配合當時電腦的發展階段而有不同的傳播方式，根據上述文獻整理歸結出約有 4 種傳播方法，分別爲：

1. 儲存設備：具開機功能者如磁碟片、硬碟皆屬之；隨身碟、光碟、隨身硬碟則可爲電腦病毒裝載設備。

2. 網路下載：惡意程式假借爲有用軟體吸引用戶下載而失誤執行，下載點可能分布在 BBS、FTP 站台或 HTTP 連結。
3. E-Mail：透過 E-Mail 傳播爲目前常見的手法，可以附件夾帶多種惡意程式，或將惡意程式語法嵌於信件內文中，不用開啓附件只要瀏覽該封信即會造成感染。
4. 系統漏洞：微軟作業系統爲目前使用率最高的平台，因此易招來駭客覬覦，一但受到攻擊則易成爲全球性的破壞。

四、 電腦病毒的防治方法

電腦病毒不只有經濟面的危害或電腦無法使用，ICSA (2004)對 300 位回報者作出統計，多數的組織指出生產力的損失是最大的問題，而這個損失都牽涉電腦檔案或系統遭受破壞後所引發的操作後遺症，以及電腦中毒與維護時停止運作的工時和員工信心的重建等，其可能發生的影響如圖 2-2-10 所示：

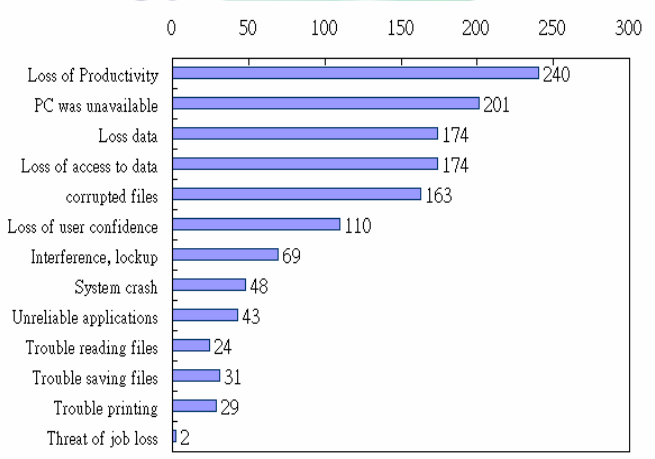


圖 2-2-10 電腦病毒所造成影響報告

資料來源：ICSA(2004)

因爲電腦病毒日益猖獗，因此在多次事件後，許多組織都發起了一套標準防制流程，而制定一套有系統的、定時更新的規範，於 2005 年開始成爲企業中首重的作業。徐廣寅(2004)提出一套全面性的安全策略須具備有多種特質：

1. 必須強制執行，能貫穿組織階層的連續性。
2. 此安全策略能在被攻擊時能首先提出應變方法。

3. 安全策略須隨著需求與技術改進而更新。
4. 當安全策略進行改變時，必須讓全體員工都知悉此改變的重要性，使其能確實遵行。

究竟要如何防治病毒侵入，研究者針對防治個人電腦中毒方法與中毒後的處理流程，整理如表 2-2-13 及表 2-2-14：

表 2-2-13　防治個人電腦中毒方法

研究者	防治個人電腦中毒方法
Hawke(2004)	1. 盡量關閉電腦磁碟的共享目錄以及設定複雜(英文與數字混合)的登入密碼，必要時關閉 139Port。 2. 定期更新作業系統的漏洞修補程式。 3. 安裝防火牆與防毒軟體並要常駐該軟體的監控程式，執行下載檔案與開啓信件時都先經由防毒軟體過濾。 4. 定時檢測登入系統時的自動啓動區，如 win.ini、system.ini、登錄檔的 Run 區或 start up 啓動資料夾以及系統服務，共五處，並要熟識電腦中預設與必要啓動的程式。 5. 留意 email 的附加檔案與關閉 scrip 語法的自動執行設定及留意郵件程式及瀏覽器漏洞的修補，可避免字洞執行附加檔案或受到視窗炸彈的破壞；不聽信電子郵件的搧動；並定時清除電子郵件伺服器上的信件，避免受到郵件炸彈的攻擊。

表 2-2-13　防治個人電腦中毒方法(續)

研究者	防治個人電腦中毒方法
陳清芳、趨勢科技紅色警戒小組 (2002)	1. 隨時注意系統修復更新的訊息通知並定期更新。 2. 當不需要使用網路時，則中止網路連線。 3. 利用其他非主流的電子郵件軟體。 4. 可安裝防火牆以及防毒軟體。 5. 定期更新防毒軟體的病毒定義檔。 6. 對於來路不明、內容奇怪非預期內的郵件則勿開啓，特別是在節日或特別紀念日的時期;也不隨意相信內容的指示，如刪除電腦中的某檔案。或在開啓檔案前必定要通過防毒軟體檢查，使中毒可能性減少。 7. 不隨意下載免費或盜版軟體使用，或執行一定要經由防毒軟體掃描無誤後才得以開啓。 8. 養成每日備份習慣。 9. 定期閱讀電腦病毒的相關消息。 10. 關閉可能造成病毒入侵的系統漏洞，如停止 script 語法的直接執行 11. 瀏覽系統檔案應顯示所有檔案的副檔名稱。 12. 勿關閉巨集文件的巨集執行警示
黃銘祥、張季珠、廖立茹(2001)	1. 不使用來源不明的軟體、光碟或磁片。 2. 不開啓標題聳動或引人好奇的電子郵件，除非其副檔名是*.jpg 或*.mpg。 3. 安裝防毒軟體，並定期更新病毒碼及掃毒引擎。 4. 要隨時掌握電腦病毒的訊息。 5. 適時關閉會自動執行 scrip 語言的網路設定。 6. 注意電腦的異常情形。 7. 定時備份於不同儲存媒體上，不要只備份在一處。 8. 對防毒軟體有正確的認知，防毒軟體是一種防治的方法，是事後補救的措施，並非絕對的保障。

表 2-2-14　電腦中毒處理方法

電腦中毒後的處理方法	
劉景熙、劉建虹(1994)	1. 一旦懷疑遭受病毒襲擊，則須立即識別並隔離可能被病毒感染的電腦或儲存設備。 2. 尋求專家協助處理消除病毒的連串流程。 3. 需確認病毒如何被引進電腦，若是經由磁片、光碟等可攜帶的儲存媒體則需通知所有人員與顧客。
陳清芳、趨勢科技紅色警戒小組(2002)	1. 立即關閉電腦電源，以及拔除網路線來停止網路連線，讓病毒能停止破壞行為，減低傷害。 2. 使用防毒軟體進行掃描，並進行重要檔案備份，了解防毒軟體的刪除檔案、清除病毒、隔離檔案等訊息。 3. 若是透過系統漏洞傳散者，立即進行系統檔案修補。 4. 與專家聯繫進行病毒的分析，如利用磁片或網路傳送可疑的、尚未解毒的中毒檔給專家進行判讀，並提供詳細的病毒發作情形，與用戶電腦的基本設備，以利儘早提出解決策略。

資料來源：研究者製表

由上述資料中顯示，個人在電腦病毒的防治概念的重要性優於事後解毒的能力，防毒不該只是專業人員的責任，而是全民必備的知識，除了知識面的防毒概念，例如不開啓來路不明的檔案、重要資料要備分等敘述性知識外，更應具有基礎的技術性能力，如設定安全裝置、了解系統的基本架構如啓動區或副檔名的觀念等，而組織中該領域的管理人員更應隨時留意病毒的趨勢，調整安全策略，以及全面性的推廣與強制，才能使電腦病毒的防治策略得以有效實踐。

五、　小結

從 2001 年 CodeRed 掀起驚濤駭浪後，緊接著 2002 年「Klez 病毒」、2003 年的「疾風駭蟲」、2004 年「Sasser 駭蟲」都以微軟系統漏洞爲攻擊目標，造成全球極大的損失，值得注意的是微軟早在病毒尚未出現前就已經公佈這

些系統漏洞的修補程式，但用戶的忽視與對系統安全的關注不足才使新型態病毒得以大肆其道，用戶當對自己的疏失負起最大責任。

有意思的是，2005 年起，電腦病毒的整體生態又有了新的轉變，分別由「Sobig」、「Netsky」、「Beagle」的一系列變種駭蟲佔領了病毒的天下，且在全球資訊安全調查中第一次由「遵從規範(compliance with regulation)」領先了病毒與蠕蟲對企業的影響，表示組織已經針對資訊安全訂定了一套標準化的規範，將可有效遏制與縮減電腦病毒帶來的災害(Ernst & Young, 2005b)。

研究者在本節所整理的文獻將構成電腦病毒的基本概念，可作爲研究者發展課程與評量工具的參考依據，也是評鑑學童是否持有電腦病毒概念迷思概念的基準，在下一節我們將探討迷思概念的定義與形成因素及特性，未來研究者可依此推論導致學童產生電腦病毒迷思概念的可能因素，藉此在發展概念改變課程時，可對症下藥加強教育，方可有效澄清學童的迷思概念。

第三節　迷思概念的定義與研究

本節將探討迷思概念的相關理論基礎，說明個體在學習過程中概念形成可能產生的問題。本節將討論概念的意義、概念的分類、概念的定義、概念的成因與特性，並探究概念改變的相關研究，作爲研究者設計評量工具、發展電腦病毒概念課程時的參考依據。

一、 概念的意義

將具有共同重要屬性或特徵的事物歸爲一類，即形成一概念(鄭麗玉，1994)。或是以一個符號來代表同類事物的總名稱，包含同一類的物品(如椅子、球)、事件(如跑步、談話)、有生命的有機體(如人、馬)甚或至抽象的事物(如愛情、真理)或見解(如 A 比 B 聰明)(林清山譯，1992)。另有學者指出個體在生長過程中所接觸的事物或現象，依據概念的共同性來劃定分類的規則與範圍，並透過符號爲其命名，使個體間得以進行雙向溝通，因此概念是學習的基本單位能協助人們理解與思考(黃台珠，1984)，在該文中則採潘恩思的圓錐結構來說明概念精練的過程：

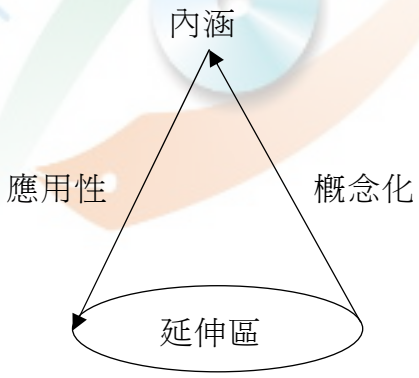


圖 2-3-1 潘恩斯圓錐結構

資料來源：引自黃台珠(1984)

下方延伸區爲包含具有同屬性的事物，例如探討「狗」的概念，在延伸區定義「狗」的特性有四條腿；慢慢的將狗的屬性歸納並收斂，如身體爲毛髮覆蓋、有牙齒、哺乳類，從延伸區向內涵演進的過程稱「概念化」，而狗最後的內涵除了具延伸區與概念化過程的屬性外，加上必要屬性爲具有「汪汪」的叫聲，即爲狗之概念。

反推，從內涵到延伸區稱之爲「應用性」，也就是個體對於事物的分類規則與定義具有區別與推演能力，例如「貓」雖具有與狗雷同的表徵，卻與狗的叫聲大不相同；而黑狗、白狗雖毛色不同，但卻符合所有屬性，當個體能做出正確判斷即具有該事物的概念。

綜合上述所言，將具有相同屬性或特徵的事物給予命名後即爲概念。概念命名有助於概念的形成，因命名後的概念使環境簡化與標準化，個體不須親身經歷即可以透過知識的傳承習得概念，以及讓個體在新事物學習上可以名稱作爲分類的憑據，並能有效結合舊經驗(邵瑞珍、皮連生，1993；鍾聖校，1997)。

二、 概念的分類

多數的研究者將個體所持有的概念區分爲兩類。鍾聖校(1997)將概念分爲「自然概念」與「邏輯概念」，前者是指爲了應付日常生活中的需要所產生的概念，沒有具體或特殊的屬性，是模糊與定義不清的；後者則是在許多領域中以概念間的關係爲本質進行分類與推理的基礎。鄭昭明(1997)也有一致的看法，其將概念分爲「人工概念」和「自然的概念」。前者具有極明顯的屬性，如大小、形狀、顏色等。後者爲生活中所見的自然事物，極難以屬性的全有或全無去界定清楚的。

國外學者維高斯基也將概念區分爲二，一爲「自發性(spontaneous)概念」，即個體從日常生活經驗中自然反應出來的概念，屬於發展的層面，爲由下往上發展到抽象概念；二爲「科學性(scientific)概念」，即在科學理論裡有明確的定義，可以經由一套技術的教育方式來教導小朋友學習，屬於學習的層面，是從抽象的概念開始，由上往下推演到個人的生活經驗(熊召弟、王美芬、段曉林和熊同鑫譯，1996)。

上述文獻都呈現了相同的概念分類原則，一爲自然概念，是個體在生活經驗中爲生存需求對事物所產生的主觀性想法；二爲人爲概念，是經過各領域的專家發展出具有邏輯性、有組織的概念，需要後天的學習才能取得，而這兩者概念交互作用後所產生的不一致看法，即形成所謂的迷思概念。

三、 迷思概念的定義

在國內外許多學者對於迷思概念採不同的解釋方法，並沒有概括性的單一名稱，國內外多數學者常用「迷思概念」或「另有架構」來做概念的探討，但兩詞在意義上不同，另有架構主要是個體在概念學習的過程中，其推論或預測的規則或想法，也就是個體的認知架構與該領域專家的架構雖不相同，但脈絡可能是正確的；而迷思概念則是指個體的概念結果是模糊的、錯誤的、對概念仍有不足之處(鄭麗玉，1998；謝青龍，1995)。在本研究中，研究者主要探討學生電腦病毒有哪些錯誤的概念，並進行改正，因此本研究將統一稱爲迷思概念。

四、 迷思概念的成因

從概念的分類中可知，自然概念爲個體在尚未受到教育前就已具備，因此學生並非毫無概念進入學校場域，而是帶著其在日常生活應對上的先備知識來學校學習，在學習的過程中，認知結構因接觸新知識而不斷的進行修正與改變，這些學習所得的經驗都可能導致迷思概念的形成，表 2-3-1 條列了多位研究者對迷思概念形成可能原因的看法：

表 2-3-1　迷思概念形成原因

研究者	迷思概念形成原因
Fisher (1985)	迷思概念的形成原因有三： 1.會在概念演化歷程中發生不正確的連結和錯誤。 2.在學校教學過程或其他環境所造成。 3.透過其他個體的一般經驗分享所致，如大眾傳播媒體或父母。
Head(1986)	提出五種迷思概念的形成原因，分別爲： 1.來自日常生活中的經驗與觀察。 2.從類推產生的混淆而來。 3.使用錯誤的隱喻。 4.來自同儕團體。 5.來自個體直覺的觀點。

表 2-3-1 迷思概念形成原因(續)

研究者	迷思概念形成原因
王美芬(1991)	教師對該領域貧乏的了解以至於產生不適當的教導、教科書編排的錯誤例如在描繪物件時採用不合適的尺寸或模型都可能產生迷思概念；而另一個原因則歸於學童不適當的認知階段，以至於學童採自我中心語言來解釋。
熊召弟(1996)	說明學童概念架構的來源主要是經由以下五點來獲取： 1.感官的印象。 2.日常用語。 3.大腦內部構造。 4.學生在社會環境中的學習。 5.教學的過程。

綜合上述觀點，迷思概念來自多方管道，個體在學習前利用觀察或類推日常生活中所得的觀點，學習過程中也可能受到同儕、教師或教科書錯誤的導引，而這些錯誤概念將隨著個體持續學習而進行融合與改正。

五、 迷思概念的特性

由迷思概念的來源來看，我們可以知道這些錯誤的概念是個體在成長的過程中與學習環境互動中所產生的，綜合 Fisher (1985)、熊召弟等人(1996)與鍾聖校(1994)研究後提出，迷思概念具有下列特性：

(一) 過程性：在概念形成的歷程中產生錯誤連結：如片斷擷取概念，或是透過非專業媒體、父母或同儕的傳授未經證實的概念；甚或爲前領域專家所遺留下來的錯誤概念。

(二) 不完備性：在學校教學過程與環境影響所致，教師因應學童受教階段給予深淺不同的知識，若爾後沒有繼續接觸相關知識，遇到問題僅能使用現有概念進行推論，甚或學童完全沒有該領域的概念，而從其他現象類推所致。而不完備的知識也可能形成個體對該概念的不穩定性與矛盾性，因爲不了解所以容易忘記，或做出前後不一致的推論。

(三) 普遍性：不分國籍、不具有區域性，大多數的個體都具有相同的迷思概念。

(四) 頑固性：一旦學生常用錯誤的方法解決或描述事件，且當下能有效處理，則會導致教師在教授正確概念時，無法修正學生的觀點，除非學生在日後持該方法卻無法解決問題時，才得以導正。

(五) 非正統性：與學科領域的專家概念不一致，被認定爲是錯誤的或待修正的。

(六) 個別性：有許多錯誤概念及其想法是相當特別的，屬於個體專有。

六、 概念改變

錯誤概念研究的目標是在了解錯誤概念的內容與成因、修正錯誤概念以及追求教學績效(鍾聖校，1994)，研究者認爲在該研究中所指的修正錯誤概念即屬於概念改變的其中一環；Posner 等(1982)認爲要促進學生概念改變，最好的方式是個體在學習新知識的過程中對於證據進行判斷並能能提出詢問，其指出學生必須依賴其既有概念才能在面對新知識時有能力提出問題或區別現象中的相關屬性，而學生會在下述條件滿足後才進行概念改變行爲：

(一) 個體不滿足既有的概念。

(二) 新概念必須是清晰可理解的。

(三) 新概念具有能合理解決問題的能力以及當個體發現新概念與他的想法、舊經驗或與其他理論一致時。

(四) 新概念可以解釋更多的研究流程，並具有新領域的延伸性。

這些概念改變的基礎理論可從認知心理學的角度來推論，認知心理學的主要代表爲 Piaget 的認知發展論，以平衡與失衡來描述個體在環境中的學習與適應過程，當個體能運用既有基模處理新事物，即是將新事物納入既有基模中，此爲知識的類推運用，稱爲同化，一旦同化了心理上會感到平衡；若既有基模無法直接同化新知識時，會感到失衡並形成一種自我調節的內在趨力，驅使個體改變既有基模使其能容納新知識，此稱爲調適，而個體則在平衡與失衡交替的過程得以使基模精緻化，促成個體知識發展(王美芬，1991；張春興，1996)，由認知心理學演化而成的概念改變流程可參考圖 2-3-2。

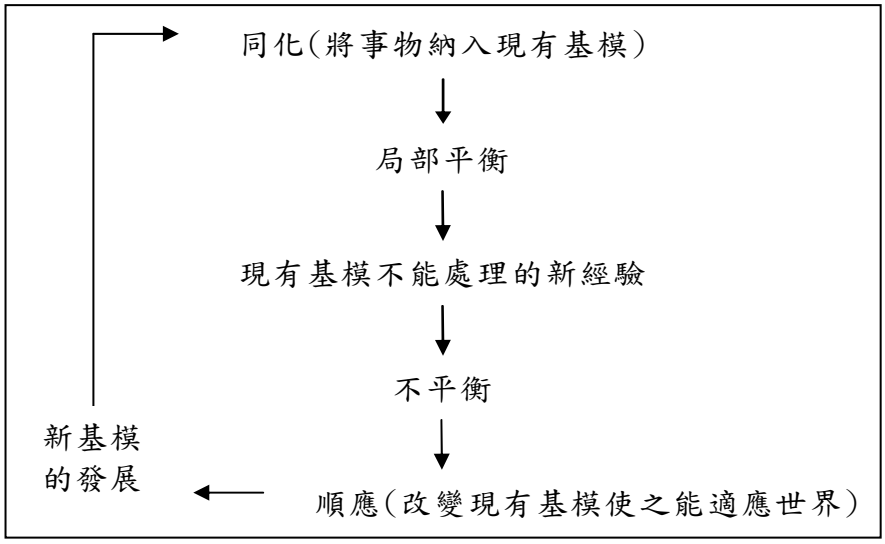


圖 2-3-2 認知改變模式圖

資料來源：引自鍾聖校(1997)

與概念改變相關的另一理論爲奧蘇貝爾的學習理論，涉及了學習、教學與課程三部份，在學習部分奧蘇貝爾提出有意義的學習論，教學者必須在學生已有充分的先備知識基礎下，配合其認知結構，授予他學習新知識。奧蘇貝爾將概念視爲層次性的結構，結構上層者爲要領概念，爲個體對事物的整體認識；居下層者，爲附屬概念，代表個人對事物特徵的細部記憶，例如成人普遍具加法的演算能力，但已不記得國小所做過的加法練習，而加法是學習乘除法前的必備能力，這些持久不忘的要領概念即爲先備知識；在教學的部份，教師在教學前將新知識中的要領概念提出來與學生的先備知識相關聯，將有助於學習，將這樣的教學步驟稱爲前導組織；而在課程的部份，提倡講解式教學，但須遵循漸進分化及統整調和步驟，由這些方法來使學生產生有意義的學習(張春興，1996)。

再來爲 Gagné所提出的學習條件，其表示個體的學習成果與能力都須具備內在條件及外在條件，內在條件與奧蘇貝爾的先備知識相呼應，指的是學習者長期記憶中的先備知識和技能；而外在條件則是學習情境，主要是教師的教學活動設計，Gagné強調不同的學習結果需要不同的先備知識以及不同的教學活動設計(張新仁，2003)。

自皮亞傑首先提出認知發展理論以來，已有許多學者以認知理論作爲概念改變的理論依據。王美芬(1991)與鄭麗玉(1998)認爲概念改變必須在個體處理新事物時，引發其內在的不平衡或認知衝突，來促使個體進行調適，產生新的認知架構或調整既有架構，使個體重新回歸平衡，並指出一套有效的教學策略在概念改變的過程中扮演了一個重要的角色。

綜合上述所言，概念改變流程的起點爲個體在正式教育前的自我學習與生活經驗，經由教育得以獲得修正概念的機會，朝向正統的領域專家的定義邁進，圖 2-3-3 清楚的描繪了迷思概念的形成背景以及概念改變過程的整體架構，詳細解釋了概念改變的運作流程。

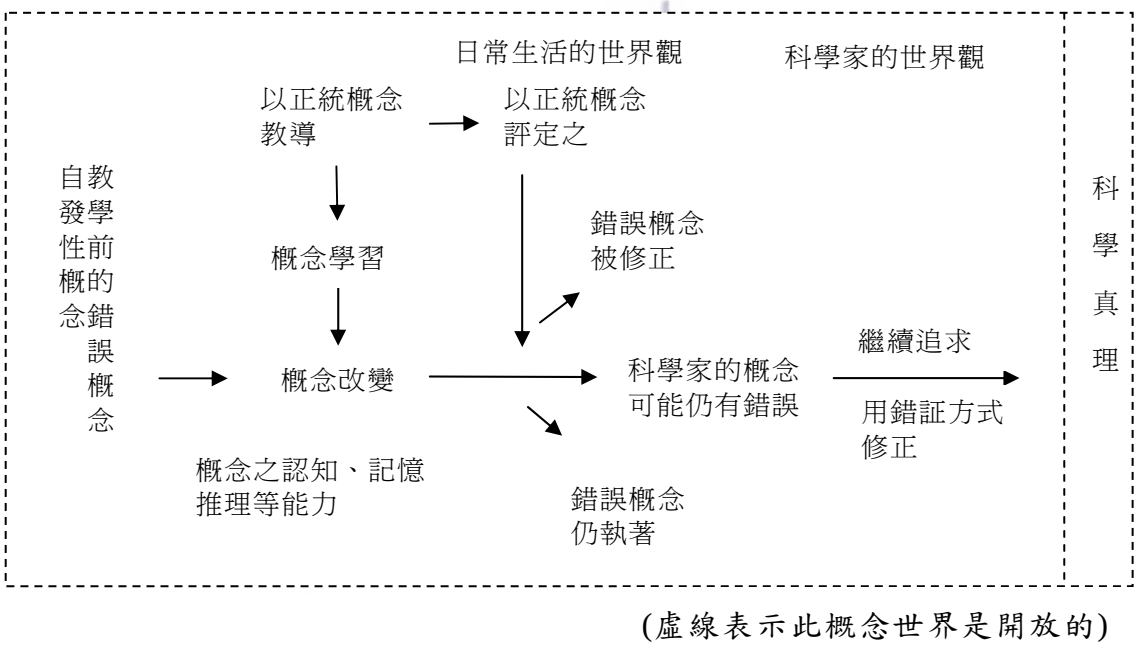


圖 2-3-3 概念改變的流程圖

資料來源：引自鍾聖校(1994)

研究者發現近年來國內在概念改變上的研究，多以施行補救教學論文爲多，表 2-3-2 爲研究者在全國博碩士論文網依據學童迷思概念進行補救教育爲題幹之研究所做的統整資料：

表 2-3-2　迷思概念補救教育成效研究

研究者	研究題目	研究結果
洪素敏(2003)	國小五年級學童分數迷思概念補救教學之研究	先以紙筆測驗取得學生的迷思概念，再進行教學後，發現學生在「以整數的運算類推分數的加法」、「等值分數的求法和分數的乘法混淆」及「無法將分數視爲數線上的一個數值」的迷思概念上仍有將近一半的學生無法克服。
侯雪卿(2004)	國小高年級學童圓概念教學模組補救教學之個案研究	採個案研究法探查國小高年級的四位學童「圓」相關迷思概念，在補救教學後對於「圓面積的公式應用」和「圓面積與直徑、半徑、周長三者間倍增關係」等概念仍有存有迷思。
林月芳(2004)	資訊融入教學以提昇國小學童天文學習效能之研究-以「月亮」單元爲例	採用準實驗研究法爲高雄縣翁園國小四年級學童進行實驗教學，但在月面的觀測、月亮每天晚 50 分鐘出來的應用、月相的傾斜角度隨時間的改變單元成效仍不盡理想。
蔡名杉(2004)	國小月相另有概念改變教學之行動研究	透過行動研究的方式，探究學童月相學習與另有概念改變的情形，在教學後經過後尚未能改變之另有概念有兩個： 1. 學童以自己的觀點判斷月相，例如滿月是全亮而朔月就是照不到太陽、下弦月是因爲太陽光照亮月亮右半邊。 2. 認爲同一天或每天月相的改變是因爲月亮被雲或地球的影子遮住。

研究結果如 Hashweh(1988)所提出的看法，學生有些先備知識以及迷思概念在教學後仍會存在，並且阻礙新概念的學習，要達到完全的概念改變是一項困難的作業，教師應重視兒童的先前概念或錯誤概念，再針對錯誤概念進行補救教學；此外教師也需進修，同時並重視教學法，針對兒童的認知階段施以教學，才能達到教學目標(王美芬，1992)。

第四節 電腦病毒迷思概念

目前國內外在迷思概念的研究上以自然及數學科目爲多，反觀在電腦病毒迷思概念的文獻並不充裕，多爲個人論述之文章，缺少實徵性研究，但這些資料仍值得參考，做爲未來進行實際調查驗證的依據。

研究者整理近幾年來國內在電腦病毒迷思概念相關的實徵性研究，僅有兩篇。林珊如、劉旨峰、袁賢銘(2001)採問卷調查及晤談法調查技術學院資訊相關科系學生的電腦病毒迷思概念，研究顯示學生具下列五大項迷思：

一、 對電腦病毒概念模糊的迷思：當電腦運作不正常時就是病毒所造成的，將電腦問題怪罪於電腦病毒。
二、 對電腦病毒潛伏及感染標的物的迷思:電腦病毒除了感染程式之外也會感染電腦的 CPU 等硬體。
三、 把電腦病毒類比爲生物性病毒的迷思:認爲已經感染過電腦病毒的電腦會變的更虛弱，而更容易再次被感染。
四、 電腦病毒發作與週期的迷思：電腦病毒發作後，會造成滑鼠不順，程式打不開等問題。
五、 對電腦病毒傳染擴散途徑的迷思:認爲電腦病毒會附著在電線上而傳給家電用品。

在該文獻中以晤談與試卷的方法來測量學生的電腦病毒概念，晤談大綱與試卷題目相同，題型採論說題的方式由學生自由回答；另外，從該試卷的概念分布來看，七道題目中分別隱含病毒定義、病毒的潛伏與感染標的物、生物性病毒類推、發作症狀與週期五大項概念，因此試卷有重複概念的題型，在本文中未見研究者歸納電腦病毒整體概念，即進行問卷的設計，是否會造成電腦病毒概念的構成項目上有所遺漏，而文中也未交代試卷的內容信度與專家效度；至於當論說題採晤談方法進行時，受訪者尚可經由訪問者的引導說出較深入的想法，相對於那些問卷受試者在缺乏指引的狀況下，可能隨性作答而造成描述過於簡單或無法全面性的指出病毒概念，以至於容易低估受試者真正的能力，余民寧(1995)也指出論文題容易產生的問題是試題取樣不廣且不均，無法涵蓋教材內容的全部以及由學生自由發展表達觀點，很難與

所要學習的結果產生關聯，還有在評分上也易受到個體主觀的影響。然而該研究中提出學生具有將電腦病毒類比爲生物性病毒的迷思概念，研究者也將此列入電腦病毒的行爲特性中，名爲「類比爲生物性病毒」。

另一篇電腦病毒的實徵研究顯示，大學與研究生對於電腦病毒仍有普遍性的迷思概念(梁雅琇、張義斌、鄭承昌，2006)：

一、 副檔名的迷思：多數學生對於可執行檔的副檔名不熟悉，除了常見的*.exe 及*.com 外，對於*.pif 或*.scr 等執行檔缺乏概念。使用者對於雙副檔名的概念亦不清楚，認爲雙副檔名是執行第一個副檔名，因此認爲「.jpg.pif」的檔案不是可執行檔。

二、 對電腦病毒「自動攻擊」概念的迷思：認爲感染 e-mail 電腦病毒後，仍可以繼續上網，電腦病毒不會自動發信給連絡簿中的人。

三、 對電腦病毒「僞裝技巧」概念的迷思：當收到微軟系統更新信件通知時，可以開啓附加檔案，進行漏洞更新，殊不知這是病毒使用的社會工程手法。

四、 對電腦病毒「潛伏性」概念的迷思：認爲病毒寫入檔案中的惡意程式越多就越容易被執行。

五、 對於病毒、蠕蟲與木馬概念區分的迷思：無法將此三種惡意程式的定義區分清楚，在謝淵任(2004)調查中學生的資訊安全概念也顯示相同的問題，多數學生認爲電腦病毒與電腦蠕蟲其實是指同一種惡意的電腦程式，因爲判定不清因此都統稱爲「病毒」。

六、 易受病毒謠言影響的迷思：容易被聳動的信件內文影響，而執行信件內文所要求進行的事項。

此篇研究先描繪出電腦病毒的整體概念後，依據概念的分類設計試卷，如此該試卷才得以廣納電腦病毒的概念；另，試卷採選擇題形式，爲今成就測驗常用的命題類型，具有可廣泛測量到各層次的成就水準，較是非題更可以避免學生的猜測，計分上也較客觀，且若有精心設計的誘答選項則可以提供有價值的診斷訊息(余民寧，1995)。但缺憾是該篇文獻中未呈現試卷的難度與題項的選定準則，因此建議未來研究中除加入試卷的難度、鑑別度與誘答力分析，以利進行題型的修正或增刪，盼能讓試卷具有信效度。

在上述兩篇研究中可見多數學生仍具有電腦病毒迷思概念，資料中也呈現了男生的電腦病毒概念優於女生，且年級較高概念較好，曾有電腦病毒經驗的概念優於沒有電腦病毒經驗者。

另外在個人論述的文章部分，研究者整理 Alabama(2001)、Dong(2004)、Garry(2002)、Rosenberger(1988)、Symantec(2004)、Zach(2001)文章中所描述的電腦病毒迷思概念，發現這些資料雖未經過實徵性研究，缺乏確切的數據來佐證作者的論點，但這些論點都隱含電腦病毒的行爲特性，因此研究者自行將這些迷思概念依據特性給予分類，可做爲電腦病毒測驗試卷的參考文獻，資料如表 2-4-1 所示：

表 2-4-1　電腦病毒迷思概念文獻

特性	迷思概念
未授權性	1. 有好的和壞的病毒。
自動執行	1. 如果我備份了一隻病毒，那我的備份磁碟就會被損壞。
破壞性	1. 大部分的病毒都會進行檔案的破壞，或格式化磁碟。 2. 使用微軟 Office 時，所出現的巨集警告，是巨集病毒。 3. 電腦硬體出現問題，如發出嗶嗶聲及螢幕沒有顯示就認爲是中毒。
傳染性	1. 不法的軟體(開放的或免費的軟體)是主要造成病毒流傳的原因。 2. 防盜拷的軟體是安全的。 3. 不打開郵件的附加檔案就不會中毒。 4. 我使用無線網路因此我的 e-mail 是安全的。 5. 大部分的 BBS 都感染了病毒。 6. 我登入了被感染的 BBS，所以我也會被感染。
僞裝性	1. 我認得寄 Email 給我的寄件者，因此可以放心開啓附加檔案。
持久性	1. 病毒和木馬都是近期的現象。 2. 病毒問題時間增長而消退。
廣泛性	1. 每一隻病毒都會造成大傳播。

表 2-4-1　電腦病毒迷思概念文獻(續)

特性	迷思概念
主動攻擊性	1. 我不瀏覽網頁我就不會中毒。 2. 我只是閱讀信件以及做文書處理，因此不需要做系統更新。
防毒祕招	1. 設定電腦存取密碼以及加減密能有效對抗電腦病毒。 2. 調整系統時間就可以避免觸發到病毒。 3. 將檔案特性設定爲”唯讀”的狀態就可以保護檔案免於受到感染。
防毒軟體	1. 購賣電腦時，硬體及系統提供廠商應該要保護我們的電腦不受攻擊。 2. 防毒軟體是最能夠保護電腦遠離電腦病毒的工具，必須保證我的病毒定義檔有更新。 3. 我的防毒軟體沒有偵測到任何病毒，我就沒有受到感染。 4. 安裝兩套防毒軟體。 5. 安裝防毒軟體就能確保我的 e-mail 是安全的。 6. 我有使用防火強所以我的 e-mail 是安全的。
廣義病毒	1. 所有惡意程式都是病毒。

資料來源：研究者製表

第五節 資訊教育中與電腦病毒相關之研究

本節從資訊倫理、資訊安全以及電腦病毒態度文獻來探討學生對於電腦病毒概念的情況，可作爲電腦病毒迷思概念的補充資料；其後進行國小九年一貫資訊教育教科書中電腦病毒單元的內容分析，來了解學童在電腦病毒可能具備的先備知識，以作爲試卷命題及教案設計的參考依據。

一、 資訊倫理研究

教育部九年一貫課程資訊教育的其中一項目標爲導引學生瞭解資訊與倫理及文化相關之議題，電腦病毒是屬於資訊倫理領域可探討之範疇(林淑芬、陳泌鍇，1997)，因此研究者認爲在探討學童電腦病毒迷思概念的同時，也可從資訊倫理的文獻中獲取些許電腦病毒的迷思概念。

尹玫君(2004)指出，國小學童在資訊倫理多具有正向態度，但仍有不正確的觀念，如學生對於轉寄未經查證的 e-mail 項目上仍有待澄清的觀念；從背景變項來看，女生的倫理態度與行爲都優於男生，該文更指出每天上網半小時至一小時的學生，其資訊安全行爲高於每天上網兩小時的學生，由此可知學生可能會受到病毒謠言的影響，而產生錯誤的行爲，如遵循信件的指示而刪除某些檔案，或一再轉寄郵件造成網路與郵件伺服器的擁塞。

對於轉寄信件態度這項待澄清的觀念，在吳怡貞(2006)的研究中也有相同的結果，國小學生認爲電子郵件是個方便的東西，可以快速將資料轉寄給朋友，一同分享；文中提到當網路上流傳可口可樂被下毒，也會盡快告知朋友，以免受害。這些文獻都明顯的指出，學生對於電子郵件轉寄的態度上是輕率的，只要有風吹草動，就容易受到影響，因此易受到謠言病毒信件的影響。

二、 資訊安全研究

除了從資訊倫理的研究可得到電腦病毒迷思概念的相關訊息外，也可從資訊安全向度上探究。研究顯示，國小學童在資訊安全的行爲與態度上的表現不凡，在於國小學童較其他年齡層的電腦用戶較常變換電腦密碼，對於來路

不明的信件會傾向找專家協助而不會置之不理，該研究者推測是因爲國小學童對資訊安全問題解決與判斷的能力較弱所致，至於國小生對於資料的備份不積極，則是歸咎於國小學生不知道要定時備份所致(廖斌毅、潘正祥、楊正宏、林子傑、劉文勝，2003)。由此可知國小生對於電腦病毒的防治方法缺乏概念，雖然國小學童知道要經常改變密碼，但是否知道設定密碼的要訣，則有待深入追查，資料備份是防範電腦病毒極重要的知識，因此強調備份重要性的解說更應融入在課程中。

另有研究者針對國小六年級學童以系統化教學模式設計一套網路互動安全課程，在教學過程中發現多數的學生沒有親自安裝過防毒軟體的經驗，而教學後仍有學生認爲只要裝了防毒軟體就可以安心收發電子郵件，該研究並指出學生對於電腦病毒的特性及防治方法的觀念仍需教導；而在電腦病毒的態度上大多知道隨意開啓來路不明的郵件是危險的，學生也認爲學習網路安全課程後對於網路的使用上有助益(林佳旺，2003)。

在針對國中生資訊安全概念程度的調查中顯示，家中有無電腦以及是否曾受過病毒駭客攻擊的學生，在資訊安全的概念認知與態度上呈現顯著差異，研究結果顯示，資訊安全概念越清楚則在資訊安全的態度就越正向，因此授予電腦病毒概念課程是值得肯定的(謝淵任，2004)。

在上述文獻中，雖皆論及電腦病毒的相關概念，但文中卻未見研究者將電腦病毒所涵蓋的層面作通盤的描繪，僅選擇小部分的內涵進行教學，這些文獻仍無法對電腦病毒概念的認知程度做整體的推論。

三、 電腦病毒態度研究

國內在電腦病毒迷思概念的文獻雖少，但仍有些許與電腦病毒防治或態度於教學上的相關研究，陳明舜(1996)調查影響電腦病毒在高中職資訊教育防治成效的因素研究，指出電腦教室使用率較高的學校其感染電腦病毒的次數會增加，以及電腦教師資訊道德觀念的強弱對於防治電腦病毒有顯著的影響，該研究最後歸結影響電腦病毒防治成效的最大因素在人，因此加強全民資訊道德應視爲一個重要的課題。

而關於電腦病毒態度的實徵研究有二，但研究對象以大專生爲主，研究指出大專生對於電腦病毒的傳播、破壞力感到畏懼、痛恨散發電腦病毒的病毒作者，期望這些病毒作者能受到處罰，但學生也對電腦病毒具有好奇的矛盾心理，對於如何消滅病毒有興趣，希望能多認識電腦病毒來對抗侵擾，因此會自行尋找相關議題閱讀(劉旨峰，2004；劉旨峰、林珊如、袁賢銘，2002)。

這些資訊顯示多數學生對於電腦病毒的概念仍未健全，對於電腦病毒抱持著喜歡但又怕受傷害的心理，可看出學校的資訊教育缺乏電腦病毒教育，可能會帶給學生錯誤的概念或偏頗的資訊倫理態度與認知。

四、 參考書內容分析

目前資訊教育的現況大多著重在軟體的操作應用上，但國小資訊教育應著重在培養學生使用電腦的興趣，不應過度的給予技能訓練，且國小適用的資訊教材與教法中應含電腦病毒主題，教授電腦病毒的來源、傳染方式以及預防之道，避免日後將電腦問題都歸於電腦病毒(汪富明，1998)。

(一) 現行參考書的電腦病毒概念

研究者將九年一貫資訊教育的分段能力指標裡與資訊道德相關的內容依照主題軸整理如表 2-5-1：

表 2-5-1　九年一貫資訊教育與資訊倫理相關之指標內容

主題軸	指標編號	指標內容
1. 資訊科技概念的認知	1-2-3	教導學生注意軟硬體的保養、備份資料等資訊安全概念。
5.資訊科技與人文素養的統整	5-2-1	認識網路規範，了解網路虛擬特性，並懂得保護自己。
	5-3-1	了解與實踐資訊倫理，遵守網路上應有的道德與禮儀。

資料來源：教育部(2003)

依據上表資料，從國小三年級起就有資訊安全課程的規劃，多數的指標內容是規範網路上的道德行爲爲主，但並未明確規範電腦病毒概念的教授；除了參考九年一貫課程綱要外，研究者並針對市售的資訊教科書的電腦病毒單元進行內容分析，發現爲多數教科書並不重視電腦病毒概念單元，僅佔該書中的一小部分，內容缺連貫性與完整性，且未依據電腦病毒迷思概念來設計課程。研究者發現電腦病毒單元多收錄於網際網路的書籍中，若教師未採用網路議題的教科書，則有可能從未教授學童電腦病毒概念相關知識。

國小資訊教育中專門談論電腦病毒概念的參考書幾乎沒有，研究者認爲了解目前參考書的內容，並檢討其缺失將可作爲未來課程規劃參考之用，因此採集幾本參考書做爲內容分析之文本，但考慮參考書中單元名稱的差異性大，研究者在閱讀後自行依據該書中所論及的電腦病毒概念歸納，並重新定義參考書的單元名稱，分別就認識病毒特性、病毒傳播方式、判斷中毒行爲、防毒軟體使用、防治病毒技巧來分析這些單元在參考書中的配重比例，也可藉此推論國小學童可能具有的電腦病毒先備知識，如表2-5-2：

表 2-5-2 參考書之電腦病毒單元

書名 / 單元	Internet 遊樂園 (小無限編輯部，2005b)	Internet 網路探險隊 (小無限編輯部，2005a)	Internet 網路漫遊我最拿手 (黃文鈺，2005)	Windows 電腦探險隊 (小無限編輯部，2006c)	Internet 網路 123 (徐盟霖，2004)	電腦基礎與 Windows98 (王炳麒，2004)	採用比例
認識病毒特性			✓	✓			33%
病毒傳播方式			✓	✓			33%
判斷中毒行爲				✓			17%
中毒處理方法			✓	✓			33%
防毒軟體使用	✓	✓	✓		✓	✓	83%
防治病毒技巧			✓	✓		✓	50%

由上述資料可得，沒有任何參考書是完整描述電腦病毒總體概念的，多數內容只是輕描淡寫帶過，正如本章第三節提到教科書內容也可能是造成學生迷思概念的原因，因此更加深研究者規劃一套電腦病毒概念課程的信念。

(二) 參考書的電腦技能概念

除了探究參考書中電腦病毒單元外，學童於資訊課程所習得的技能也是必須整理的要點，因電腦病毒是由電腦程式所組成，而電腦病毒的基本原則與行爲特性中的附屬概念即爲電腦概念所組成，如電腦病毒感染目標爲電腦中各型態的檔案格式，又如電腦病毒的傳染途徑則與電腦設備與系統相關，因此研究者認爲，要探討電腦病毒概念也需了解學童所習得的電腦技能項目，如此，在編制電腦病毒測驗試卷時，才得以界定學童能力，使試題中的電腦相關名詞不致於超過學童的經驗。

研究者列出九年一貫資訊教育中學童至國小六年級學童所應學得的技能，如表 2-5-3，可見資訊安全教育已逐漸在小學教育中萌芽；另，研究者依上述具有電腦病毒概念之參考書內容，歸納該書所含之電腦技能爲電腦設備、系統檔案、網路設備與網路操作四大項目，條列單元所屬內容，分述如表 2-5-4：

表 2-5-3　九年一貫資訊教育能力指標

主題軸	指標編號	指標內容
1.資訊科技概念的認知	1-2-1	了解資訊科技在人類生活之應用。
	1-2-2	正確規劃使用電腦時間及與電腦螢幕安全距離等，以維護身體健康。
	1-2-3	教導學生注意軟硬體的保養、備份資料等資訊安全概念。
2.資訊科技的使用	2-2-1	了解電腦教室(或教室電腦)的使用規範。
	2-2-2	熟悉視窗環境軟體的操作、磁碟的使用、電腦檔案的管理以及電腦輔助教學應用軟體的操作等。
	2-2-3	認識鍵盤、特殊鍵的使用，會英文輸入與一種中文輸入。

表 2-5-3　九年一貫資訊教育能力指標(續)

主題軸	指標編號	指標內容
3.資料的處理與分析	3-2-1	能進行編輯、列印的設定，並能結合文字、圖畫等完成文稿的編輯盡量使用自由軟體。
	3-3-2	能利用繪圖軟體創作並列印出作品盡量使用自由軟體。
4.網際網路的認識與應用	4-2-1	能進行網路基本功能的操作。
	4-3-1	了解電腦網路概念及其功能。
	4-3-2	能找到合適的網站資源、圖書館資源及檔案的傳輸等。
	4-3-3	能利用資訊科技媒體等搜尋需要的資料。
	4-3-4	能針對問題提出可行的解決方法。
5.資訊科技與人文素養的統整	5-2-1	認識網路規範，了解網路虛擬特性，並懂得保護自己。
	5-3-1	了解與實踐資訊倫理，遵守網路上應有的道德與禮儀。
	5-3-2	認識網路智慧財產權相關法律，不侵犯智財權。
	5-3-3	認識網路隱私權相關法律，保護個人及他人隱私。
	5-3-4	擅用網路分享學習資源與心得，了解過度使用電腦遊戲、bbs、網路交友對身心的影響；辨識網路世界的虛擬與真實，避免網路沉迷。

表 2-5-4　參考書內容分析

項目	單元	內容
電腦設備	認識軟硬體設備	硬碟、記憶體、CPU、光碟機、磁碟機、螢幕、鍵盤、滑鼠、喇叭、掃瞄器、印表機、磁碟片、光碟片、隨身碟
系統檔案	認識檔案格式	.exe 執行檔，.zip 與.rar 以及.grp 爲壓縮檔，.mpeg 與.rm 影片檔，.mp3 與.wav 音效檔，.txt 純文字檔，.pdf 可攜式文件檔，.doc(文書檔)、.xls(試算表檔)以及.pps 是巨集檔，.scr 螢幕保護程式，.html 與.htm 是網頁檔，.jpg、.gif、.bmp、.png 是圖片檔，.swf 動畫，未知檔
	作業系統操作	登入帳號與輸入密碼、介紹系統視窗圖型與工具列、操作檔案總管以及檔案或資料夾的更名、搬移、複製與刪除。
網路設備	硬體設備	網路卡、電話線、數據機、網路線、無線網路。
網路使用	認識網路服務	認識網際網路與區域網路。
		BBS 電子佈告欄、搜尋引擎、FTP 檔案傳輸協定、IRC 線上連天室、WWW 全球資訊網、E-mail 電子郵件、電子賀卡、即時通訊、網路遊戲、電子報、網路下載與共享。
	使用 IE 瀏覽器	認識網頁架構與超連結名詞、使用網頁搜尋、儲存/轉寄網頁、下載圖片與檔案。
	收發電子郵件	使用 web mail 與 outlook express 閱讀與傳遞文字、圖片與附加檔案以及使用回覆與轉寄信件功能、能管理通訊錄。
	即時通訊	MSN、Yahoo 即時通檔案傳輸與分享功能操作。

綜合上述分析可知，市面上的資訊教育參考書籍大致符合九年一貫資訊教育所設計的能力指標，研究者認爲高年級學童已學得相當多的電腦概念，只是多數參考書在電腦病毒單元未針對學童已有的概念進行統整與延伸應用，研究者將利用電腦病毒的概念圖與學童的先備知識連結，採系統化教學設計模式設計一套電腦病毒概念課程，期望能使電腦病毒概念學習產生顯著成效。

第六節 電腦病毒概念圖

研究者依據電腦病毒種類的特性、電腦病毒防治方法，並參考電腦病毒迷思概念的實徵性與論述性文獻以及電腦病毒相關研究，繪製文獻參考圖，如圖 2-6-1。在收集相關文獻後，將電腦病毒概念區分爲四個面向，分別爲「基本原則」、「行爲特型」、「廣義病毒」、「防毒策略」作爲上層概念，而此四個上層概念各自延伸其相關的子概念，編製成電腦病毒概念圖，如圖 2-6-2。

在教學上採用概念圖的優點在於可使學生與教師清楚了解學習材料的重點，並能提供視覺上的路徑，有效協助學生將圖像轉換成命題(Novak & Gowin，引自張漢宜、陳玉祥，2002)，研究者發展此概念圖也將作爲爾後編制電腦病毒測驗試卷，以及規劃電腦病毒教學設計之參考架構。

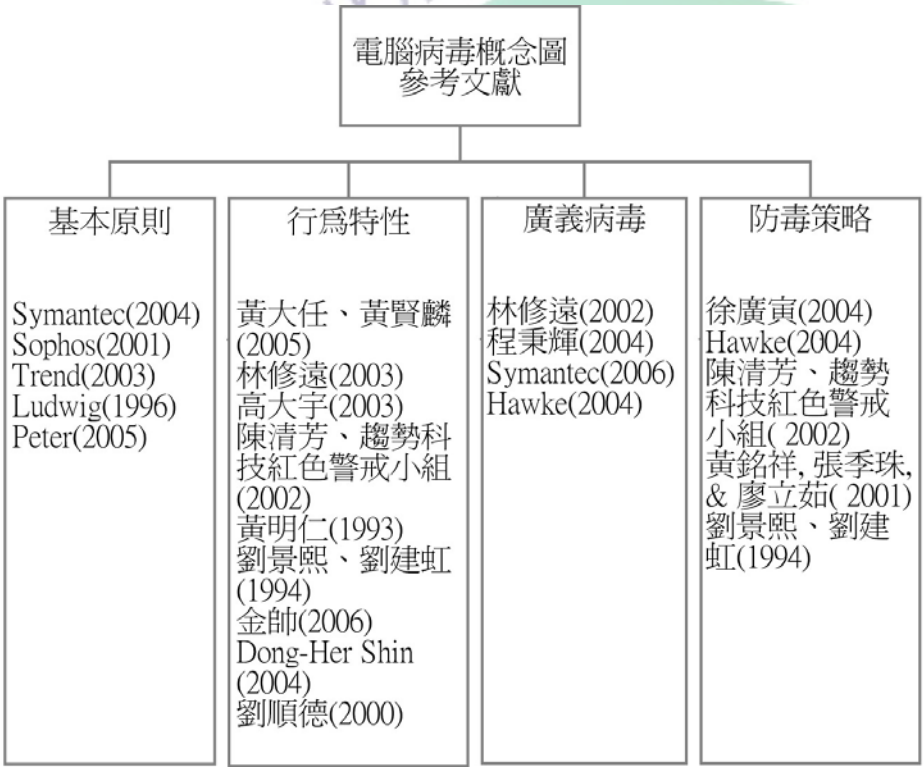


圖 2-6-1 電腦病毒概念文獻參考圖

圖 2-6-2 電腦病毒概念圖

第七節 系統化教學設計

本研究旨在發展一套電腦病毒概念課程能有效澄清學童的迷思概念，在本節中將選取一套合適的教學設計模式，並立基於電腦病毒概念圖之架構，來發展電腦病毒概念課程。本節分別以系統化教學設計意義、系統化教學模式分析各式教學模式的內涵與優缺點，小結則由研究者選定一套適合本研究的教學模式，做爲發展課程的參考依據。

一、 系統化教學設計意義

系統化教學設計注重教學過程中的每一個因素，如教師、學習者特質、學習目標、教學方法、教材選擇、學習環境與評鑑工具，各個因素間彼此相互依存與影響，因此在教學設計中每一個步驟都有其階段性目標並層層相關聯，依照先後次序來實施，以期達到教學目標(中國視聽教育學會，1988；李宗薇，1991)。

二、 系統化教學設計模式

至今有約百種系統化教學模式，研究者選擇 ASSURE 模式、KEMP 環形教學設計模式、Dick & Carey 模式以及 ADDIE 模式分別進行探討。

(一) ASSURE 模式：

爲美國印第安那大學教授 R. Heinich 與 M. Molenda 以及普渡大學教授 J.D.Russell 於 1982 年提出，專門針對教師在教學上的應用所設計，該模式透過六階段發展教學設計，分別爲「分析學習者特質」、「陳述學習目標」、「選擇媒體或教材」、「使用媒體或教材」、「要求學習與反應」以及「評量與修正」(李宗薇，1991)，其模式流程參考圖 7-2-1：

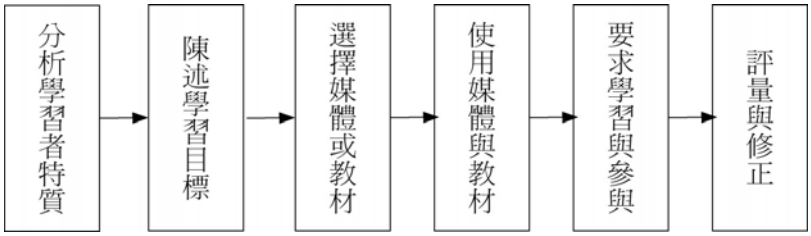


圖 2-7-1　ASSURE 教學設計模式

資料來源：引自李宗薇(1999)

ASSURE 模式缺乏需求分析、內容分析、系統實施等項目而無法適用於大規模之教學設計中，僅適合於教學現場使用，其模式則著重在教師使用媒體與教材上的系統規劃(李宗薇，1991，1999)。

(二) KEMP 模式：

於 1985 年由堪普(J. Kemp)所提出，以環狀模式顛覆線性模式所強調的順序性，如圖 7-2-2，該模式認爲一個完整的教學設計應包含下列十個要素(中國視聽教育學會，1988)，分別描述如下：

1. 確立教學目的，評估學習者需求，並決定教學設計的發展順序，此爲該模式的核心因素。
2. 選擇教學主題與單元，並設立工作項目來達到一般性目標。
3. 分析學習者或受訓人員特性。
4. 確定主題內容與工作項目。
5. 按照主題內容與工作項目訂定學習目標。
6. 設計教學方法與學習活動。
7. 選擇配合教學方法與活動的各種資源。
8. 安排教學與製作教材時所需的行政支援事項。
9. 準備學習成果的評鑑計劃。
10. 採預試的方法爲學習者作學習前的準備或調整。

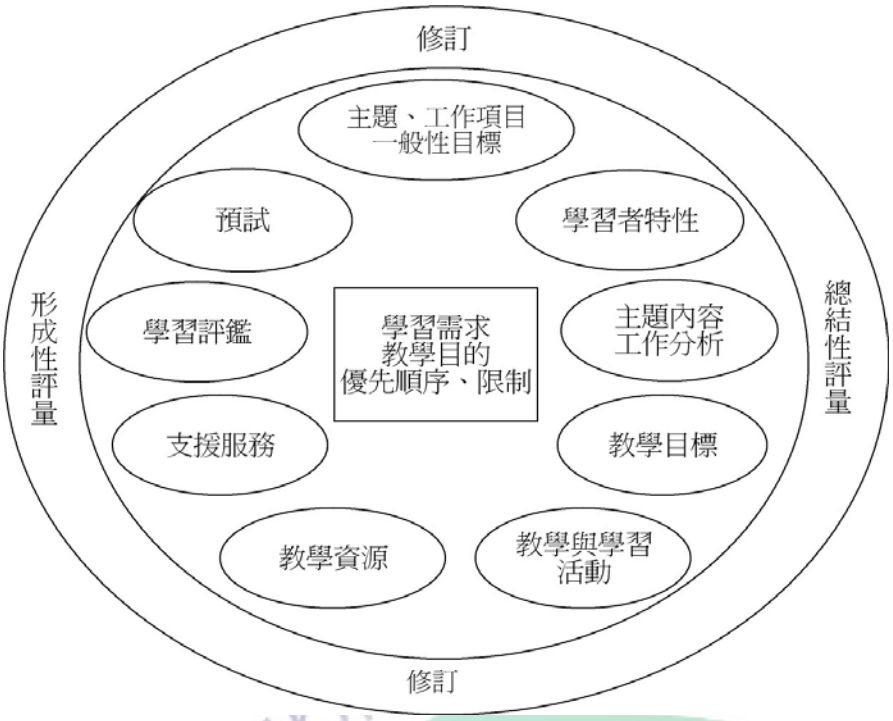


圖 2-7-2　KEMP 教學設計模式

資料來源：引自中國視聽教育學會(1988)

KEMP 的環型模式沒有特定的起點與終點，沒有箭頭也就代表沒有固定的優先順序，且各要素間是互動循環的，設計者也可自九個要素中自行選擇需要的，提高了使用彈性，若設計者也可自第一要素依照順序執行，使其能適應突發狀況或環境改變；該模式適用於大規模的教學設計，也著重由評量方式進行環形內部要素的修正(中國視聽教育學會，1988；李宗薇，1999)。

(三) Dick & Carey 模式：

Dick & Carey 教學設計模式於 1978 年提出，包含了九個階段步驟，分別爲「確定教學目標」、「進行教學分析」、「確定起點行爲特質」、「撰寫行爲目標」、「發展標準參照測驗題」、「發展教學策略」、「發展及選擇教材」、「設計並進行形成性評鑑」、「設計並進行總結性評鑑」(李宗薇，1999，陳正昌譯，1996)，步驟流程如圖：

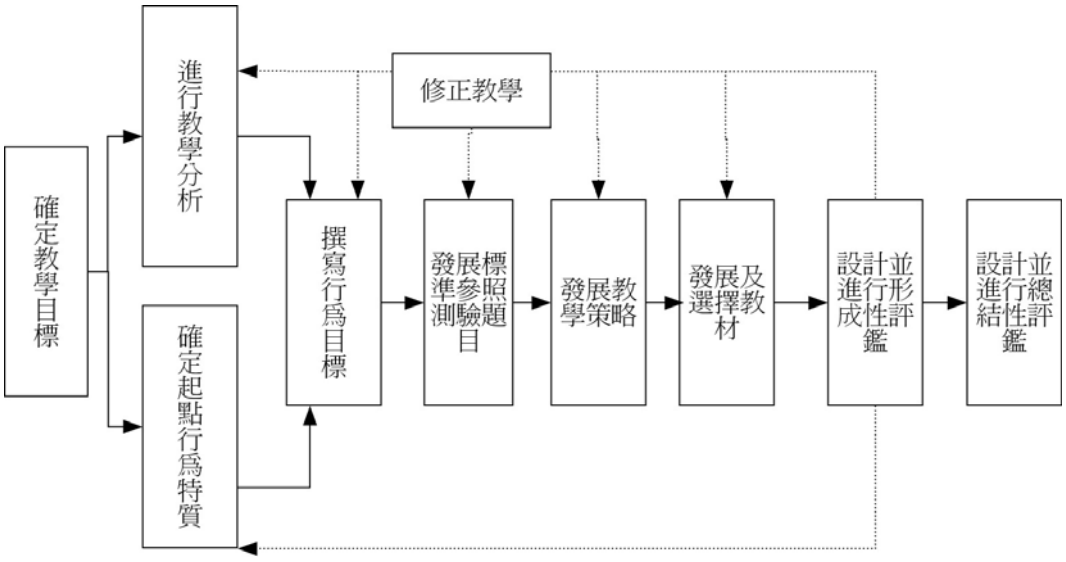


圖 2-7-3　Dick & Carey 教學設計模式

資料來源：引自陳正昌譯(1996)

Dick & Carey 此模式採系統回饋來校正系統，利用形成評量持續對每一個教學步驟進行修正，反覆修正是爲了使該教學能適用於最多的學生，該模式有四特色(李宗薇，2000)：

1. 教學前進行教學分析及學習者分析，可反映現實的需求。
2. 在分析與教學歷程間不斷進行修正，以期達到最好的成果。
3. 重視評量，透過評量來發現學習者是否達成前一步驟的目標，可隨時修正。
4. 教學目標的設定是透過客觀需求分析後考量現實所設立，並非由主組織機構之主管自行研擬。

Dick & Carey 模式可視爲一個明確的教學設計流程，設計者在大規模設計或教室內的課程規劃都可加以利用。

(四) ADDIE 模式：

ADDIE 模式於 1980 至 1990 間形成，由 Grafinger 正式提出此縮寫名詞，以分析(Analysis)、設計(Design)、發展(Development)、實施(Implement)、評鑑(Evaluation)五階段爲模式的設計流程(徐新逸，2003)，如圖所示：

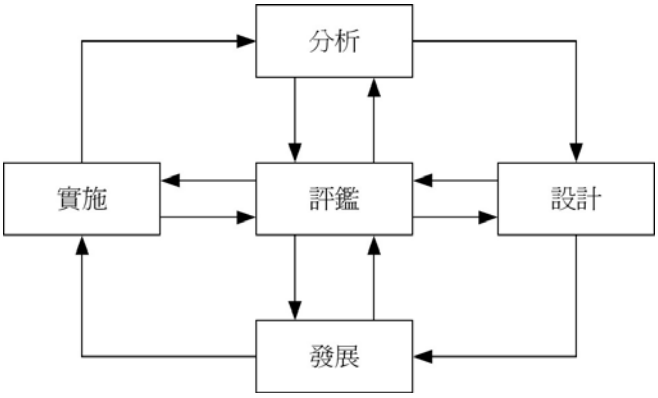


圖 2-7-4　ADDIE 教學設計模式

資料來源：引自徐新逸(2003)

ADDIE 模式並非一個靜止的線狀結構，透過評鑑持續進行各階段的修正，而呈現一個動態結構。ADDIE 過去多應用在訓練的領域，目前已成爲數位學習內容發展時常用的模式。

三、　系統化教學設計的相關研究

研究者分析國內以系統化教學模式設計教學內容，並實際於教學現場評鑑該課程的研究，發現課程實驗結束後，學生在學習成就上都能有正向的提升，整理如表 2-7-1：

表 2-7-1 國內採系統化教學設計模式設計課程研究表

研究者	研究方法	研究對象	研究結果	論文名稱
林 世 宗 (2004)	實驗法	國中二年級學生	從學生前、後測聲概念紙筆測驗中之觀察，在三個聲概念學習上，學生經由本教材之試教及試用後，答題正確比例也有小幅度的提升	以迷思概念爲基礎之電腦輔助教材開發—以國中聲音課程爲例

表 2-7-1 國內採系統化教學設計模式設計課程研究表(續)

研究者	研究方法	研究對象	研究結果	論文名稱
林佳旺 (2003)	行動研究	國小六年級 29 位學童	大多數的學生對於網路隱私安全、電子郵件和網路聊天交友安全有了基本的認識，但也有少部分學生未能有正確的觀念。	國小網路素養課程系統化教學設計之行動研究—以「六年級網路互動安全課程」爲例。
吳怡貞 (2006)	準實驗研究法	國小五年級34位學童	在國小學生網路素養能力測驗前後測結果分析發現學生在經過國小網路素養課程實驗處理後，後測成績較前測成績有大幅度的提升。	國小學童網路素養課程之系統化教學設計研究。

四、 小結

ASSURE、KEMP、Dick & Carey 與 ADDIE 系統化教學設計模式都具有獨特的設計原則與架構，但深就此四種模式可發現皆具有共同的要素，首先爲分析學習者需求及其先備知識，設定教學目標、設計教學方法與活動、透過評鑑反覆修正任一教學要素，綜觀這些要素均不脫離「分析」、「設計」、「發展」、「實施」與「評鑑」五個項目，也就是 ADDIE 模式所設立的五階段(張淑萍，2006)。

研究者依據四種模式的階段內涵評估欲發展的電腦病毒概念課程，本課程爲小型課程設計，重在概念的傳達而非媒體工具的使用，因此不選擇較複雜的 KEMP 環型模式，或著重媒體使用設計的 ASSURE 模式，依據研究需求與考量僅有一位課程設計者，亦不採行較複雜 Dick & Carey 模式，研究者

認爲 ADDIE 模式符合系統化教學的基本內涵，精簡各家模式設計而成，且可依照使用者需求調整 ADDIE 個階段的工作項目，因此本研究將以 ADDIE 模式發展電腦病毒概念課程。

本研究考量人力與時間，因此自行將 ADDIE 五階段之工作項目與以簡化，如圖 7-2-5 所示，以下將針對每一工作項目進行說明。

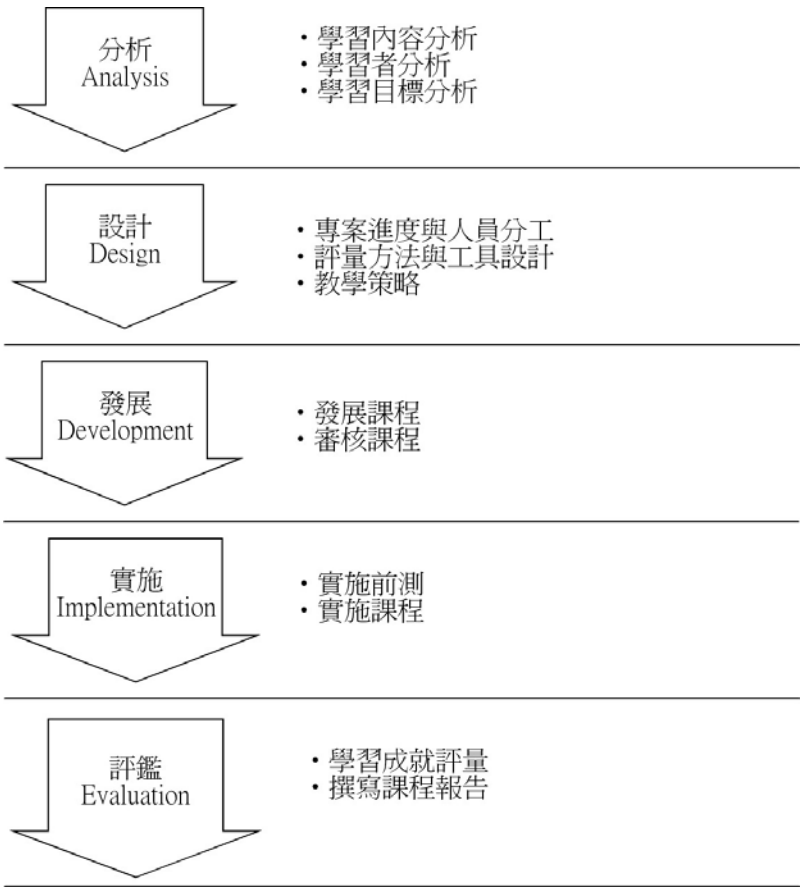


圖 2-7-5　本研究之 ADDIE 教學設計流程圖

(一) 分析階段

對所收集的課程相關資料進行分析，可作爲設計階段的參考依據，本研究設計階段包含：學習內容分析、學習者分析、學習目標分析。

1. 學習內容分析：

分析課程所包含的內容架構、整體目標課程與內容呈現順序，以及單元內容的架構與各單元間的順序。

2. 學習者分析：

了解學習的者特性，如性別、使用電腦的經驗與教育程度等，最重要的是要理解學習對於所要學習的主題所具備的先備知識，才能設計適合的教材。

3. 學習目標分析：

設定學習目標是任一教學模式的必備要素，作爲設計評量題目與教學策略的重要依據，此工作項目要界定學習範圍與學習者的行爲目標。

(二) 設計階段

設計階段主要依據學習目標規劃課程藍圖，做爲後續發展階段的施工基礎，設計階段有四：

1. 課程進度規劃與人員分工：

課程發展多有時間限制，因此必須妥善歸劃每個工作項目預定完成的時間，才能掌握進度以期在時間內達成目標。

2. 評量方法與工具設計

評量方法有兩種分別爲實作評量與紙筆測驗，需依據學習目標與學習內容來設計與選擇適宜的評量方法。

3. 教學策略設計：

規畫完善的教學環境與教學活動來引發學習者學習，常用策略如示範、討論、同儕教導、練習等方法。

(三) 發展階段

將設計階段的規劃具體實行，在此階段必須完整呈現課程單元內容。

1. 發展課程：

根據課程單元發展完整課程內容。

2. 審核課程：

交由專家審核完整課程內容，並持續進行修改。

(四) 實施階段

正式將課程呈現給學習者，在此階段仍必須依照學習者需求與反應不斷調整教學內容。

1. 實施前測：

對實驗組與對照組同學施以相同前測，前測工具爲研究者自編之「電腦病毒概念測驗試卷」。

2. 實施課程：

正式對學習者施行教學，教學活動也將依據學習者的反應進行修正。

(五) 評鑑階段

此階段是用來評估課程的實行成效，利用評量工具進行學習成效之評鑑。

1. 學習成就評量

課程的評量工具在設計階段就需設計完成，在本階段即利用該評量工具來考核學習者的學習成效，藉以看出課程設計的品質。

2. 撰寫課程報告

將學習成就評量之成績統整後，撰寫課程實施成效之報告，並提出改進與修正之建議。


NTTU Library

第三章　研究方法

本研究旨在探討國小高年級學童的電腦病毒迷思概念，並設計一套電腦病毒教學課程施以實驗處理，探究該課程是否能有效改變學童的電腦病毒迷思概念，採取量化研究來分析紙筆測驗的結果。

本章以研究架構、研究樣本、研究工具、研究流程、資料處理共五節分述之。

第一節　研究架構

一、　實驗設計

研究者以自編紙筆測驗「電腦病毒概念測驗試卷」對學童施以前測，探討學童對於電腦病毒有哪些迷思概念，再對學童實施「電腦病毒概念改變課程」實驗教學，探究教學後學童的電腦病毒概念上是否有提升。

本研究採用準實驗研究法中的不相等控制組設計方式，實驗流程爲非隨機選取三組同學，分派爲實驗組 1、實驗組 2 與控制組；並對三組同學施以相同前測；前測結束後，採研究者自行研擬之「電腦病毒概念改變課程」對實驗組 1 進行教學;採教育部於 2006 年所舉辦的提升全國高中職資訊素養與倫理之教學推廣講習時的「網路社會自我保護(一)-不當資訊」教案(以下簡稱爲電腦病毒推廣教材)，對實驗組 2 施以教學，而選擇此教材的原因爲其教學內容以介紹電腦病毒的概念爲主，與研究者所欲探討之問題相關；控制組則未給予任何實驗處理；待實驗處理完成後，再以相同的前測試卷「電腦病毒概念測驗試卷」對三組同學施以後測，實驗設計如表 3-1-1 所示：

表 3-1-1　實驗研究法不相等控制組設計表

組別	前測	實驗處理	後測
實驗組 1	O1	X1	O2
實驗組 2	O3	X2	O4
控制組	O5		O6

X1：實驗組 1 施以系統化教學設計之「電腦病毒概念概念課程」教學
X2：實驗組 2 施以教育部研習之「電腦病毒推廣課程」教學
O1 和 O3 和 O5：表示三組學童皆接受前測「電腦病毒概念測驗試卷」
O2 和 O4 和 O6：表示三組學童皆接受後測「電腦病毒概念測驗試卷」

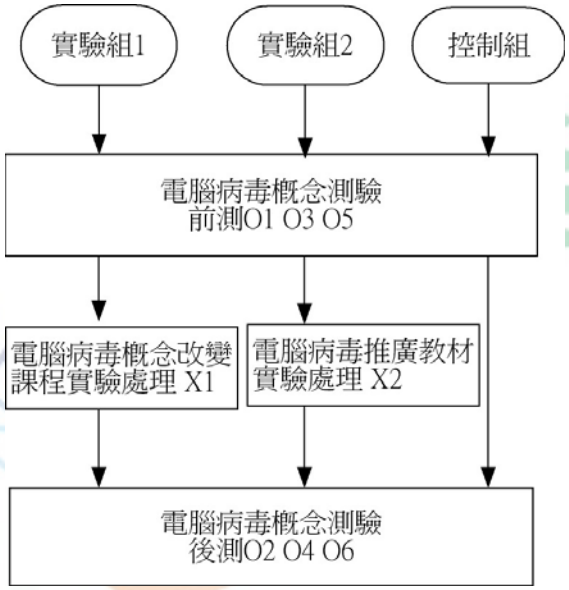


圖 3-1-1 實驗架構圖

二、 實驗變項

(一) 自變項：

1. 教學實驗：本研究自變項爲學童接受不同的教學實驗，共三種：

(1) 實驗組 1：接受研究者以系統化教學設計編製之「電腦病毒概念改變課程」教學，教材內容請參閱附錄四。

(2) 實驗組 2：接受教育部於 2006 年舉辦提升全國高中職資訊素養與倫理之教學推廣講習時所提供的「網路社會自我保護(一)-不當資訊」課程進行教學；本課程雖爲高中教材，但其內容則以講述電腦

病毒概念爲主軸，因此研究者仍採用此教案，以下文章皆將此教材簡稱爲「電腦病毒推廣教材」，教材內容請參閱附錄六。

(3) 控制組：未接受任何電腦病毒概念教學。

2. 教材內容：這部份進行實驗組 1 與實驗組 2 的教材分析，依據教學設計與教材內容分析兩者的差異，於表 3-1-2 成呈現兩者教學設計的差異，於表 3-1-3 呈現兩個教材內容的比較表。

表 3-1-2 實驗組 1 與實驗組 2 教學設計比較表

項目	實驗組 1	實驗組 2
課程名稱	電腦病毒概念改變課程	電腦病毒推廣教材
教材內容	電腦病毒概念	電腦病毒概念
教材設計模式	系統化教學設計；先描繪出電腦病毒的概念圖，再設計教材。	一般教學設計；未見完整電腦病毒概念。
教學策略	講述爲主；輔以詢問、啓發、實際連結電腦病毒相關網站；分析學童電腦病毒概念前測，對於嚴重迷思之概念，處以模擬病毒使學童獲取實際經驗。	講述爲主，輔以詢問、啓發法，並實際連結電腦病毒相關網站。

表 3-1-3 實驗組 1 與實驗組 2 教材內容比較表

電腦病毒架構		實驗組 2 教材		實驗組 1 教材	
		含	教學活動	含	教學活動
基本原則	自行複製	✓	1. 講解電腦病毒實例時，同時說明電腦病毒的種類(開機型、檔案型、巨集病毒) 2. 缺描述語言病毒	✓	1. 讓學童執行三個種類的假病毒，來認識病毒種類與副檔名的關係(檔案型、巨集、描述語言病毒) 2. 由教師口頭補充開機型病毒 3. 呈現各類病毒的實例
	自行執行			✓	1. 利用人類生物性病毒打噴嚏時病毒自動散出來說明
行爲特性	未授權性			✓	1. 利用圖片顯示”是否要執行病毒檔案””是否要刪除系統檔案”訊息，反問學童病毒是否會有此行爲

表 3-1-3　實驗組 1 與實驗組 2 教材內容比較表(續)

電腦病毒架構			實驗組 2 教材		實驗組 1 教材	
			含	教學活動	含	教學活動
行為特性	傳染性		✓	1. 提列各式傳播途徑 2. 缺隨身碟媒介	✓	1. 提列各式傳播途徑 2. 因趨勢加入隨身碟媒介
	觸發性				✓	1. 讓學童執行觸發性的模擬程式，說明調整系統日期並非防範病毒的好方法
	持久性				✓	1. 說明病毒的難以消滅性以及區域網路中毒後解毒時間的冗長
	主動攻擊性				✓	1. 說明網路是目前病毒最大的傳播媒介 2. 說明電子郵件病毒能在背景發信以及假借寄件者的特性
	不可預見性	衍生性			✓	1. 至防毒公司網站觀看變種病毒實例並說明其特性
		偽裝行為	✓	1. 提列各式偽裝行為(含系統漏洞) 2. 缺電子郵件常利用的雙副檔名偽裝術以及假借為網址格式的偽裝技巧	✓	1. 提列各式偽裝行為(含系統漏洞) 2. 教授近期常用的電子郵件偽裝技巧如雙副檔名格式以及假借為網址格式的附加檔案 3. 讓學童執行多種雙副檔名的偽裝程式。
行為特性	潛伏性				✓	1. 由人類生物性病毒的潛伏性類推潛伏性的定
	破壞性		✓	1. 提列各式病毒的破壞行為(含重新開機)	✓	1. 提列各式病毒的破壞行為(含重新開機) 2. 說明某些硬體的問題並非電腦病毒所致 3. 說明立即產生強大破壞行為病毒的特性(如無法開機)
	類比為生物性病毒				✓	1. 利用人類病毒與生物性病毒的比較表說明異同點

表 3-1-3　實驗組 1 與實驗組 2 教材內容比較表(續)

電腦病毒架構		實驗組 2 教材		實驗組 1 教材	
		含	教學活動	含	教學活動
廣義病毒	「電腦病毒」「電腦蠕蟲」「特洛伊木馬」的共通性			✓	1. 利用表格說明三者間的共同性爲都可不經使用者同意即植入與產生破壞行爲
	電腦蠕蟲	✓	1. 說明與電腦病毒的差異爲蠕蟲不會感染檔案 2. 說明電腦蠕蟲的傳染途徑主要是透過網路傳播	✓	1. 說明與電腦病毒的差異爲電腦蠕蟲不會感染檔案 2. 說明電腦蠕蟲的傳染途徑主要是透過網路傳播
	特洛伊木馬	✓	1. 說明與電腦病毒的差異爲特洛伊木馬不會感染檔案 2. 說明特洛伊木馬假借爲特殊軟體工具來吸引使用者下載	✓	1. 說明與電腦病毒的差異爲特洛伊木馬不會感染檔案 2. 說明特洛伊木馬假借爲特殊軟體工具來吸引使用者下載
	病毒謠言	✓	1. 說明謠言病毒的五個種類與判別方法 2. 說明謠言信的處理方法	✓	1. 說明謠言信的判別方法 2. 說明謠言信的處理方法 3. 缺謠言信的五個種類
防毒策略	個人防治	✓	1. 提列各式防治的方法(含備份的重要性) 2. 有提及主機要設密碼，但未提及設定一組安全密碼的原則 3. 說明中毒的處理流程	✓	1. 提列各式防治的方法(含備份的重要性) 2. 教授設立一組安全密碼的原則 3. 說明中毒的處理流程
	防毒軟體使用			✓	1. 說明防毒軟體使用的注意事項以及掃解毒的三種模式

註：✓符號，爲教材中有包含的內容

(二) 依變項：

爲三組學童在教學實驗結束後，共同接受「電腦病毒概念測驗試卷」測驗之後測成績。

(三) 共變項：

爲三組組學童在教學實驗前接受「電腦病毒概念測驗試卷」測驗之前測成績。

(四) 控制變項：

爲排除實驗干擾，本研究的實驗控制變項爲：

(1) 三組學童前後測時間相近(第二節研究對象有詳細說明)。

(2) 學生背景爲相同學校之六年級生。

(3) 研究者爲實驗組 1 與實驗組 2 的教學者。

(4) 授課時間數：實驗組 1 與實驗組 2 皆接受 5 節課的教學。

(五) 背景變項：

在本研究將探討性別、有無電腦病毒經驗、每週上網時數以及學校教師是否曾教授電腦病毒次四個變項是否會影響學童在電腦病毒概念上的程度差異。

三、 研究架構

本研究考驗三組學童在前測總成績以及四個面向「病毒定義」、「行爲特性」「廣義病毒」、「防毒策略」的前測成績來分析學童具有哪些電腦病毒迷思狀況及及成績是否會因不同背景變項而有所差異；另考驗三組學童在前後測總成績以及四個面向「病毒定義」、「行爲特性」「廣義病毒」、「防毒策略」的前後測答題狀況來分析學童電腦病毒迷思概念的轉變情形與分析三組學童在教學後個別的學習成效；並檢測三組學童在教學實驗後在電腦病毒概念的提升狀況，來探討教學實驗的效用，參考圖 3-1-2：

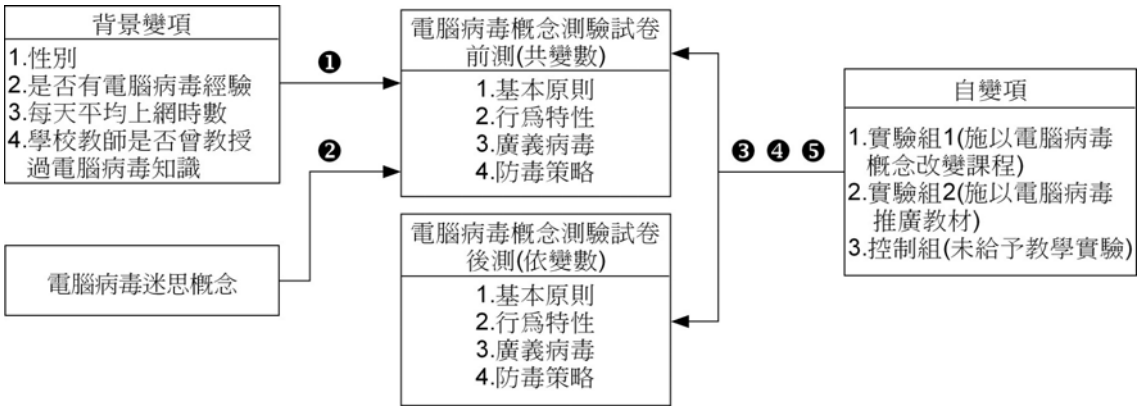


圖 3-1-2 研究架構圖

路徑❶：探討不同背景變項的實驗組同學在電腦病毒概念測驗試卷前測的差異狀況
路徑❷：利用前測分析學童的電腦病毒迷思概念
路徑❸：利用前測與後測的成績分析三組學童在電腦病毒概念的改變情形
路徑❹：探討三組學童個別在前後測成績表現的差異
路徑❺：以前測爲共變數，後測爲依變數，探討三組學童的教學成效差異

第二節　研究對象

本研究以國小六年級學童爲研究對象，並於六年級下學期末進行電腦病毒的迷思概念調查與實驗教學，期望能找出常見的迷思概念並能提升其電腦病毒正確的概念。

本節將分別以預試樣本、正式實驗樣本說明研究過程中採用的對象。

一、　預試樣本

爲求研究者自編「電腦病毒概念測驗試卷」之信度，於紙筆測驗編製完成後進行兩次預試，預試樣本皆以台東市某國小六年級學童爲主，測驗回收後進行試卷題目的分析與修正，兩次預試樣本與施測時間說明如下表 3-2-1。

表 3-2-1　兩次預試的人數表

預試	人數	時間
第一次預試	157(共 5 班)	2007.01.22 ~ 2007.01.26
第二次預試	145(共 5 班)	2007.04.24 ~ 2007.04.27

二、 正式樣本

在第一節研究架構中可見本研究共有三組正式研究對象，分別爲實驗組 1、實驗組 2 與控制組。三組學童爲台東市某所國小的六年級學童。因研究者本身並非班級或學校教師，因此無法隨機分配學童至各組別中，故以班級爲單位進行教學實驗。在教學實驗前對三組學童進行電腦病毒概念前測，爲了解學童的先備知識；在教學實驗後對三組同學在施以電腦病毒概念後測，爲了解在教學後是否能提升學童的電腦病毒正確的概念；正式樣本相關資料如表 3-2-2 所示。

表 3-2-2　正式樣本與前後測資料說明表

項目 / 組別	人數	前測時間	教學實驗時間	節數	後測時間
實驗組 1	31	5/8 8:00~8:30	2007.05.14~05.28	5	5/31 8:00~8:30
實驗組 2	27	5/9 8:00~8:30	2007.05.15~05.29	5	5/31 12:40~13:10
控制組	30	5/10 8:00~8:30	無	無	5/31 8:00~8:30

第三節 研究工具

研究工具爲達到研究目的而發展，本研究設定四項研究目的，運用三種工具爲求達到目的，工具描述如下：

一、 電腦病毒專家概念圖

研究者依據文獻探討中所提及之電腦病毒概念，以及電腦病毒迷思概念之相關研究，由研究者自行歸納電腦病毒的四項主概念，分別爲「基本定義」、「行爲特性」、「廣義病毒」以及「防毒策略」四大主軸，並階層性的衍生其相對之附屬概念。

二、 電腦病毒概念測驗試卷

爲檢測國小六年級學童是否具有電腦病毒迷思概念，研究者採紙筆測驗爲評量工具，以此來取得學童迷思概念的先備知識，本試卷請參閱附錄一。

(一) 試卷編製依據與過程

本試卷「電腦病毒概念測驗試卷」以研究者自編之電腦病毒概念圖爲發展架構，試卷含括兩個部份，分別爲學童基本資料以及電腦病毒概念試題。

研究者以電腦病毒概念圖爲基準所發展的雙向細目表，作爲本試卷題項編製的參考依據，試卷初稿先請指導教授以及一位國小資訊教師針對內容與措辭提供修改意見，加以修改後，即進行第一次預試，試卷如附錄二。

取得第一次預視資料後，進行試卷的信度考驗，協同指導教授、一位資管系老師、一位國小資訊教師以及一位大學網管人員進行試卷的修改，再次進行第二次預試，試卷如附錄三，取得預試資料後再度考驗試題信度，與指導教授商討後，完成試卷定稿。

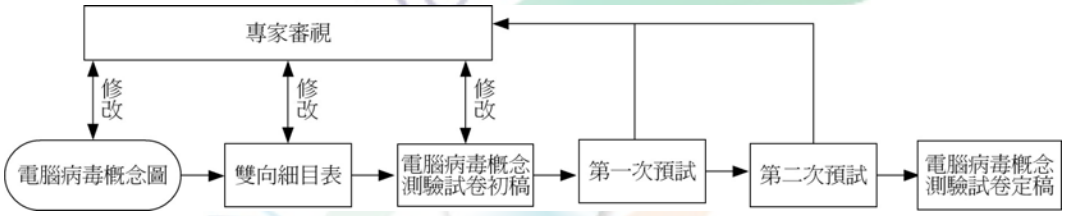


圖 3-3-1 電腦病毒試卷編製流程圖

表 3-3-1　電腦病毒概念試卷雙向細目表

概念				題號
基本原則	自行複製	對各類病毒感染目標的辨別能力		1-① ~ 1-④
	自行執行	病毒必須能自行執行來達到感染目的		4
行爲特性	非授權性	病毒在使用者不知情的狀況下植入電腦		2
		病毒未取得使用者允許就可執行破壞行爲		3
	傳染性	病毒經常使用的傳染途徑		5,6,7,8
	觸發性	病毒在觸發前的防治方法		9
		病毒觸發機制的運作		10
	持久性	病毒是難以完全消滅的		11
		區域網路內的解毒時間是冗長的		12
	主動攻擊性	電子郵件病毒的自動發信功能，寄件者可假借爲通訊錄中的名單		13
		只要在網路上就有被攻擊的可能		14
	不可預見性	衍生性	了解變種病毒的特性	15
		僞裝技巧	病毒經常使用的僞裝方法	16,17
	潛伏性	了解潛伏期的定義		18
		病毒在潛伏期間的運作		19
	破壞性	了解病毒常有的破壞行爲		20,21,22,23
	類比爲生物性病毒	從生物性病毒的觀點類推於電腦病毒概念		24,25
廣義病毒	「電腦病毒」「電腦蠕蟲」「特洛伊木馬」的共通性			26
	電腦蠕蟲	電腦蠕蟲的特性		27
	特洛伊木馬	特洛伊木馬的特性		28
	病毒謠言	病毒謠言信的判別與防範		29,30
防毒策略	個人防治	個人防範病毒的方法與技巧		31,32,33
	防毒軟體使用	防毒軟體對於防治病毒的意義		34,35
		辨別解毒的三種設定「修復」「隔離」「刪除」選項的意義		36-① ~ 36-③

(二) 試題形式及計分方法

本試卷題型以選擇題爲主，每題具四個選項；其中第 1 題與第 36 題爲配合題，其可視爲改良式的選擇題，可於短時間內測得一系列問題(余民寧，1995)。

選擇題與配合計記分方式皆則採二分法，配合題中每一題幹視爲 1 題，答對一題即得 1 分，答錯與空白者不給分，分數愈高代表電腦病毒概念能力愈好；本試卷共 41 題，總計 41 分，以電腦病毒的四個層面來看，「基本原則」面向中有 5 題，「行爲特性」共 22 題，「廣義病毒」共 5 題，「防毒策略」共 8 題。

(三) 試題分析與篩選

第一次預試與第二次預試皆採成就測驗中的難度、鑑別度、誘答力作爲篩選試題的指標數值，難度的界定範圍以 0.3~0.8 爲宜，鑑別度則爲 0.2 以上爲宜，每個選項必需符合誘答力原則，分別爲(1)每個選項至少有一位低分組學童選擇 (2)高分組錯誤選項作答人數不可高於低分組，若不符合此三標準則修改題項與選項敘述，或刪除該題項。

第一次預試後，因問題設計不恰當，因此刪除第五題，並將屬於傳染性的第 7 題移至不可預測性的僞裝行爲中，重新設定題號爲第 16 題，其餘題號皆保留，並根據每一題的誘答力分析來修正題項及選項的描述；在第二次預試試卷中的 1-1~1-4、9、13、16、23、27、28、36-1 題號，其難度或鑑別度低於判別標準，與指導教授商討後，爲維持電腦病毒概念的完整性仍予以保留，兩次預試試卷之詳細項目分析請參閱附錄八，預試題目之修改狀況請參閱兩次的預試試卷如附錄二與附錄三。

(四) 信度與效度分析

1. 信度：

因本試題以以非對即錯二分法計分，因此採 KR20 做爲信度考驗方法，其公式表示爲：$KR20=\frac{n}{n-1}\times\left[1-\frac{\sum pq}{S^2_x}\right]$，n 爲測驗的題數，p 爲答對

某一試題的百分比，q 爲答錯某一題的百分比，q=1-p，pq 則爲試題變異數之和，S^2_x 爲測驗總分之變異數，依據余民寧(2001)中指出，當 $S^2_x > \Sigma pq$ 時表示試題間具有共變數存在，而共變數是因試題間具有相互關聯時才會產生，共變數愈大，pq 值愈小，試題可測量到共同的特質，因此測驗信度的估計值會愈大。

本測驗的第一次預試人數共 157 人，以 KR20 進行試題的信度考驗，所得值爲 0.66；而第二次預試人數爲 145 人，也以 KR20 進行考驗，所得值亦爲 0.66，代表本試卷有中高信度，並具有穩定性。

2. 效度：

本試卷以電腦病毒概念圖及雙向細目表編製而成，並請教授、國小教師以及網管人員進行試卷題型與措詞的修改，使具有內容效度。

第四節 研究流程

以下分述研究流程各階段的準備工作項目，研究流程圖請參考圖 3-4-1：

一、 準備階段：

研究開始爲確認研究主題，始進行文獻收集與分析，確定研究方法，依據所收集的文獻繪製電腦病毒概念圖，藉以發展紙筆測驗「電腦病毒概念測驗試卷」作爲研究工具，爲檢驗該試卷的信度，先選取預視樣本進行預視，以進行研究工具的修正，其後選定正式研究樣本，並設計電腦病毒課程教學。

二、 執行階段

本研究以準實驗研究法之不等組前後測方法實施教學，對正式研究樣本施以相同前測，分析研究結果，用來增修電腦病毒課程教學單元，採用修正後的電腦病毒概念改變課程對實驗組 1 施以實驗處理，採電腦病毒推廣教材對實驗組 2 施以教學，實驗結束後，對三組同學進行後測。

三、 分析階段

對前測與後測進行資料分析。

四、 論文撰寫

撰寫研究結果與討論以及結論與建議，完成論文。

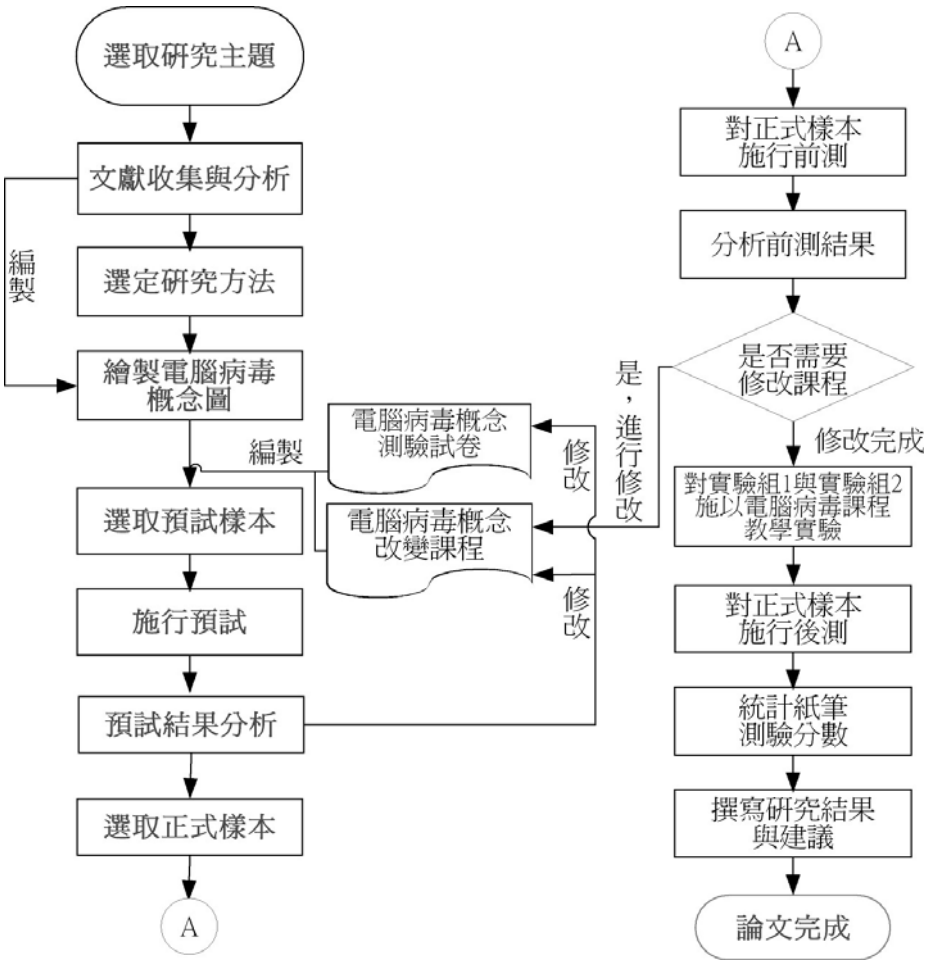


圖 3-4-1 研究流程圖

第五節　資料處理

本研究採量化分析爲主，利用社會科學套裝軟體統計程式 SPSS 爲統計工具，利用學童在電腦病毒測驗試卷前後測所得成績來進行統計結果，本研究所使用的統計方法如下：

一、描述性統計

利用描述性統計來分析電腦病毒測驗試卷試題中試題的答對率狀況，可看出學童是否具有該項目的迷思概念，並可藉由學童選擇的項目分配表來了解其所具有的電腦病毒迷思概念爲何。

二、單因子共變數分析

施行教學實驗後，爲求三組學童在電腦病毒概念成就上是否存有顯著差異，以三組學童的前測成績作爲本研究實驗的共變數，後測成績爲依數數，並以迴歸同質性檢定前測成績與組別是否會對後測成績產生交互影響，若符合迴歸同質性考驗，即採統計技術之單因子共變數分析來排除實驗中前測對後測成績的影響，以提高統計考驗的檢定力與精確度。

三、成對樣本 t 檢定

以成對樣本 t 檢定分別探究三組學童在經過教學實驗後，各組的前後測成績是否有提升。

四、獨立樣本 t 檢定

以獨立樣本 t 檢定檢測性別、是否有電腦病毒經驗、學校教師是否教授過電腦病毒，此三項背景變項在學童的電腦病毒概念成就上是否有差異。

五、單因子變異數分析

以單因子變異數分析分別探究每週上網時數此背景變項在學童的電腦病毒概念成就上是否有所影響。

第四章 電腦病毒概念課程系統化教學設計

本章依據研究者在第二章文獻探究時所選擇的 ADDIE 系統化教學設計模式來發展電腦病毒概念課程，分就「分析」、「設計」、「發展」、「實施」、「評鑑」五階段進行說明。

第一節 分析階段

本研究在分析階段主要任務爲設立電腦病毒概念課程的教學內容與目標，並分析學習者的背景與先備知識，才能規劃出適宜的課程，分就學習內容分析、學習者分析以及學習目標分析進行說明。

一、 學習內容分析

本研究之學習內容依循研究者自行描繪之「電腦病毒概念圖」來設計課程架構與內容編排順序，內容共分四個主要單元，分別爲電腦病毒的「基本原則」、「行爲特性」、「廣義病毒」、「防毒策略」，說明如下：

1. 「基本原則」單元：介紹電腦病毒所必須具備的兩個條件，分別爲自我複製以及自行執行，缺一不可。
2. 「行爲特性」單元：介紹電腦病毒的行爲與運作的特性，在此單元中共涵括九種行爲特性。
3. 「廣義病毒」單元：介紹電腦蠕蟲、特洛伊木馬的特質，並說明此兩者與電腦病毒的異同點，以及說明謠言信的判別與處置。
4. 「防毒策略」單元：說明個人防治方法以及防毒軟體使用的注意事項。

二、 學習者分析

本研究之教學對象爲台東市區某國小的六年級學童，根據教育部明定的九年一貫課程指標可知，國小六年級學童已具有「資訊科技概念的認知」、「資訊科技的使用」、「資料的處理與分析」、「網際網路的認識與應用」、「資訊科技與人文素養的統整」此五面向的能力，代表六年級學童已具有基本電腦的操作能力。

爲了解研究對象的電腦病毒先備知識，採研究者自編之電腦病毒概念測驗試卷對研究對象施以前測，並檢測學童的先備知識是否會因學童的基本資料(性別、每天上網時數、是否有電腦病毒經驗、學校教師是否教授電腦病毒知識)而有所差異，詳細數據於第五章第一節可見。

由測驗的結果中可知，在四個電腦病毒的面向中，學童皆存有普遍的迷思概念，因此有接受教學的必要性。

而在學童的個人基本資料顯示，若學童是否有電腦病毒經驗，則在電腦病毒概念的成就測驗表現較好，其它的背景變項則不會影響電腦病毒概念測驗成就，由此推論，在課程中若可讓學童實際接觸電腦病毒，將有助提升其正確概念。

三、 學習目標分析

根據教學內容分析中的四大單元，以及學習者的先備知識來規劃學習者在每一單元目標中，設定預期要達成的行爲目標，如表 4-1-1。

表 4-1-1 學習目標分析表

單元名稱	單元目標	行爲目標
電腦病毒基本原則	1. 了解電腦病毒基本原則「自我複製」、「自動執行」的意涵。 2. 認識電腦病毒種類。	1.1 能在教師提問時說出電腦病毒的兩個基本原則。 1.2 能在學習單上寫出電腦病毒兩個基本原則分別代表的意義。 2.1 能在學習單上寫出四種電腦病毒的種類。 2.2 能在教師講述後了解各種副檔名格式與電腦病毒種類的關係。 2.3 能在教師提問時正確判別出某副檔名爲何種電腦病毒的感染目標。

表 4-1-1 學習目標分析表(續)

單元名稱	單元目標	行爲目標
電腦病毒行爲特性(第一階段)	1. 瞭解電腦病毒的「未授權性」代表的意義。 2. 瞭解電腦病毒的「傳染性」代表的意義。 3. 瞭解電腦病毒的「破壞性」代表的意義。 4. 瞭解電腦病毒的「潛伏性」代表的意義。 5. 瞭解電腦病毒的「類比爲生物性病毒」代表的意義。	3.1 能在教師講述後了解未授權性的意義。 4.1 能在教師提問時，正確判斷出病毒會採用的傳染途徑。 4.2 能在學習單中寫出至少三種傳染途徑。 4.3 能在教師提問時正確判斷出軟體使用與電腦病毒的關係。 4.4 能在教師講述後瞭解系統漏洞也是電腦病毒的傳染途徑。 5.1 能在大家來找碴的活動中正確圈選出病毒視覺性的破壞行爲。 5.2 能在教師講述後了解電腦病毒非視覺性的破壞行爲，以及哪些不是病毒的破壞行爲。 5.3 能在教師講述後了解立即造成電腦無法開機的病毒是不容易造成大範圍傳染。 5.4 能在學習單上寫出至少三種破壞行爲。 6.1 能在教師講述後了解潛伏期的定義與特性。 6.2 能在學習單上正確寫出潛伏期的定義。 7.1 能在教師講述後了解人類病毒與電腦病毒的異同。 7.2 能在學習單上寫出兩種人類病毒與電腦病毒的相同處。
電腦病毒行爲特性(第二階段)	1. 瞭解電腦病毒「觸發性」代表的意義。 2. 瞭解電腦病毒「不可預見性」代表的意義。 3. 瞭解電腦病毒「自動攻擊性」代表的意義。 4. 瞭解電腦病毒「持久性」代表的意義。	8.1 能在教師講述後了解觸發性的意義。 8.2 能在執行觸發性程式時了解病毒一旦在某一天被觸發，之後病毒每天都可能被執行，並非調整系統日期後就可以避免的。 9.1 能在教師呈現變種病毒的消息後，了解變種病毒的意義與特性。 9.2 能在教師講述後了解病毒常用的僞裝技巧。 9.3 能在執行各種雙副檔名的檔案後，了解雙副檔名的僞裝技術。 9.4 能在教師提問時，正確回答常被電腦病毒利用的雙副檔名僞裝技術以及說出爲何種電腦病毒種類。 9.5 能在學習單上正確勾選出常被病毒利用的雙副檔名僞裝技術。

表 4-1-1 學習目標分析表(續)

單元名稱	單元目標	行爲目標
電腦病毒行爲特性(第二階段)	1. 瞭解電腦病毒「觸發性」代表的意義。 2. 瞭解電腦病毒「不可預見性」代表的意義。 3. 瞭解電腦病毒「自動攻擊性」代表的意義。 4. 瞭解電腦病毒「持久性」代表的意義。	10.1 能在教師講述後了解感染了以 e-mail 傳遞或系統漏洞的病毒，連上網路就會在系統背景主動攻擊其他電腦。 11.1 能在教師講述後了解電腦病毒不容易被消滅，而且有可能再次引發大流行。 11.2 能在教師講述後了解必須花費大量時間處理區域網路中的病毒。 11.3 能在學習單上正確寫出區域網路病毒解毒三步驟。
廣義病毒	1. 瞭解電腦蠕蟲的特性。 2. 了解特洛伊木馬的特性。 3. 了解謠言信的特性。	12.1 能在教師講述後了解電腦蠕蟲的特性以及與電腦病毒的異同點。 12.2 能在學習單中寫出電腦蠕蟲的破壞行爲。 13.1 能在教師講述後了解特洛伊木馬的特性以及與電腦病毒的異同點。 13.2 能在學習單中寫出特洛依病毒的傳播方法。 13.3 能在教師提問時正確回答出電腦病毒、電腦蠕蟲以及特洛伊木馬三者間的異同處。 14.1 能在教師講述後了解謠言信的特點以及預防方法。 14.2 能在學習單中寫出謠言信的正確處理方法。
防毒策略	1. 了解個人防毒的方法 2. 認識防毒軟體的操作流程與處理模式 3. 中毒的處理流程	15.1 能在教師講述後了解設定安全密碼的原則。 15.2 能在學習單上寫出一組安全的密碼。 15.3 能在教師講述後了解其他個人防毒的方法，如隨時備份。 16.1 能在教師講述後了解防毒軟體的正確觀念。 16.2 能在教師演示後了解防毒軟體的三種解毒模式。 16.3 能在學習單上寫出防毒軟體「刪除」的正確意義。 17.1 能在教師講述後了解疑似中毒時的處裡流程。 17.2 能在學習單上寫出中毒時的處理流程。

第二節 設計階段

本階段主要工作項目爲規劃課進度與人員分工、制定評量方法與工具以及研擬教學策略與教學活動，分述如下：

一、 課程進度與人員分工

爲掌控課程進度，繪製本課程之工作項目時程如圖 4-1-1，而在人員分工上，則由研究者獨立完成課程規劃與評鑑工具，交由審核委員進行校正。

圖 4-1-1 電腦病毒概念改變課程工作時程圖

二、 評量方法與工具設計

在本研究中評量方法有兩種，分別爲：

(一) 各單元的學習單：學習單爲依據單元的學習目標及學習內容設計而成，於每單元課程結束後讓學童填寫，交由研究者批閱並於下次上課時發回並檢討。

(二) 總結性評量的紙筆測驗：本研究的總結性評量與研究者分析學童先備知識時所施以的電腦病毒概念前測相同，目的爲檢測學童在接受教學後是否具有學習成效。

此紙筆測驗爲研究者依據「電腦病毒概念圖」編制而成，測驗主要爲選擇題及配合題形式，以非對即錯方式給分，因此並無分數判定上之疑慮。

三、 教學策略與教學活動

本課程採教師講述、演示、學生操作與個人競賽等教學策略，透過概念的傳遞與學生操作經驗增強概念間的連結。

在本研究的教學活動的設計流程中包含了引起注意、告訴學習者目標、刺激先前的學習經驗、呈現教材、評估學習輔導、誘發行為、提供回饋以及評定行為，這些活動因應不同的教學內容呈現，而非所有單元中都涵括了這些項目，但本研究中有固定安排的教學活動流程為：

(一) 提示學習目標：課程初始，利用電腦病毒概念圖呈現本單元的教授內容。
(二) 呈現教材：依照單元目標呈現教材內容。
(三) 評定行為：利用學習單來檢測學童能否能在單元結束後，正確回答出單元的重點問題。

四、 教學媒體的選擇

本研究的教學策略以講述佔多數，因此每單元皆以簡報呈現單元目標與課程內容，但仍有些不同的教學活動需要使用額外的教學媒體，如在基本原則中提供三個種類的模擬病毒供學童親身體驗病毒種類與副檔名格式的關係；在行為特性(II)單元中，提供病毒常用的雙副檔名偽裝程式供學童執行並模擬病毒的觸發程式，讓學童感受病毒的觸發時機；在防毒策略中則模擬隨身碟病毒行為，引導學童有自行檢查的能力。詳細媒體資料如下表 4-2-1：

表 4-2-1 教學媒體項目表

媒體特性	媒體名稱		格式	來源	單元
投影視覺媒體	電腦病毒基本原則簡報		.ppt	研究者自製	第一節
非投影視覺媒體	電腦病毒基本原則講義		紙本	研究者自製	第一節
非投影視覺媒體(實物與模型)	副檔名格式	執行檔	.exe .scr .com .pif	研究者自製	第一節
		巨集	.doc .xls	研究者自製	第一節
		描述語言	.html .vbs .htm .js	研究者自製	第一節
投影視覺媒體	電腦病毒行爲特性(I)簡報		PPT	研究者自製	第二節
非投影視覺媒體	電腦病毒行爲特性(I)講義		紙本	研究者自製	第二節
非投影視覺媒體(圖片)	電腦病毒視覺性的破壞行爲(大家來找碴)		圖片紙本	研究者自製	第二節
投影視覺媒體	電腦病毒行爲特性(II)簡報		PPT	研究者自製	第三節
非投影視覺媒體	電腦病毒行爲特性(II)講義		紙本	研究者自製	第三節
非投影視覺媒體(實物與模型)	雙副檔名格式	蜘蛛人.exe	.exe	研究者自製	第三節
		蜘蛛人.exe.txt	.txt	研究者自製	第三節
		蜘蛛人.txt	.txt	研究者自製	第三節
		蜘蛛人.txt.exe	.exe	研究者自製	第三節
		寶寶洗澡.exe .txt	.txt	研究者自製	第三節
		寶寶洗澡.txt .exe	.exe	研究者自製	第三節
	8 月 8 號觸發程式.exe		.exe	研究者自製	第三節
投影視覺媒體	廣義電腦病毒簡報		ppt	研究者自製	第四節
非投影視覺媒體	廣義電腦病毒講義		紙本	研究者自製	第四節
投影視覺媒體	防毒策略簡報		ppt	研究者自製	第五節
非投影視覺媒體	防毒策略講義		紙本	研究者自製	第五節
非投影視覺媒體(實物與模型)	隨身碟病毒.exe		.exe	研究者自製	第五節

第三節　發展階段

依據電腦病毒概念圖中四個面向設計課程，分別爲電腦病毒的「基本原則」、「行爲特性」、「廣義病毒」、「防毒策略」，其中電腦病毒行爲特性單元概念較多，因此畫分成兩節，課程安排共 5 節課，總計 200 分鐘。

一、發展課程

綜合上述學習內容與學習目標的分析、教學策略的設計、評量工具的製定以及教學媒體的選擇，進行電腦病毒概念課程內容的編寫，課程內容請參閱附錄四。

二、審核課程

課程發展完成後交由指導教授以及一位國小資訊教師審查並修改。

第四節　實施階段

本階段正式對實驗組進行實驗教學，教學內容爲研究者自行設計之「電腦病毒概念課程」，研究者本人爲施教者，以此來探討本自編課程是否具教學成效。

待前述工作項目皆完成後，即正式對實驗組同學進行教學，依照發展的教材內容依序進行，因研究者本身並非教師，因此與班級教師商量後於早自習以及利用資訊課的時間進行教學，課程長度共 5 節。爲達到本課程所設定之教學目標，在教學過程也將視課堂反應，適時調整授課內容。

第五節　評鑑階段

一、學習成就評量

爲評鑑本課程是否有效澄清學童之電腦病毒迷思概念，在本實驗課程結束後，也將針對學童再次施以紙筆測驗，以研究者自編之「電腦病毒概念測驗試卷」爲評量工具，施測時間約 30 分鐘。

二、撰寫課程報告

研究者將在實驗教學後針對實學童的前後測成績進行統計分析，分析課程的學習成效，該資料將呈現於本論文第五章研究結果中呈現。


NTTU Library

第五章 結果與討論

本章共分爲三節，分別就背景變項與電腦病毒概念測驗的分析、電腦病毒迷思概念分析以及電腦病毒概念教學成效分析來說明本研究的發現。

第一節 背景變項與電腦病毒概念測驗的分析

本研究探討性別、是否有電腦病毒經驗、每天平均上網時數以及學校教師是否曾教授過電腦病毒知識，此四各背景變項是否會影響學童的電腦病毒概念認知能力。

一、 性別與電腦病毒概念測驗的分析

研究者探討學童的電腦病毒概念成就是否會因性別而有差異，分別從前測的測驗總分、基本原則總分、行爲特性總分、廣義病毒總分與防毒策略總分，共五個面向進行獨立樣本t檢定，如表5-1-1。

表 5-1-1 性別變項獨立樣本 t 檢定

分數項目	性別	個數	平均數	標準差	t 值	自由度	顯著性(雙尾)
總分	男	57	20.316	5.754	1.345	91	.182
	女	36	18.75	4.976			
基本原則	男	57	1.667	1.041	0.976	62.824	.333
	女	36	1.418	1.296			
行爲特性	男	57	12.439	3.775	0.434	91	.665
	女	36	12.111	3.142			
廣義病毒	男	57	2.158	1.36	2.215*	91	.029
	女	36	1.557	1.133			
防毒策略	男	57	4.053	1.414	1.279	91	.204
	女	36	3.667	1.422			

*p < .05 **p < .01 ***p < .001

由表中可知，性別在五個面向所得的分數，多數未達顯著差異，代表男女在電腦病毒概念的認知上有一致性，再從平均分數來看，兩者分數皆偏低，說明男女對電腦病毒的概念是普遍不足的；僅有在廣義病毒面向中男女成就有顯著差異，從平均數可了解男生成就優於女生，在梁雅琇、張義斌、鄭承昌(2006)的研究中也發現男生的電腦病毒概念優於女生。

二、 是否有電腦病毒經驗與電腦病毒概念測驗的分析

研究者探討學童的電腦病毒概念是否會因有無電腦病毒經驗而有差異，分別以前測的測驗總分、基本原則總分、行爲特性總分、廣義病毒總分與防毒策略總分，共五個面向進行獨立樣本t檢定，如表5-1-2。

表 5-1-2　是否有電腦病毒經驗變項獨立樣本 t 檢定

分數項目	曾經感染	個數	平均數	標準差	t 值	自由度	顯著性(雙尾)
總分	是	71	20.704	5.510	3.302**	91	.001
	否	22	16.500	4.103			
基本原則	是	71	1.620	5.492	0.752	91	.454
	否	22	1.409	1.163			
行爲特性	是	71	12.958	1.098	3.341**	91	.001
	否	22	10.227	1.146			
病毒廣義	是	71	2.056	3.458	2.122*	49.777	.039
	否	22	1.500	2.959			
防毒策略	是	71	4.070	3.529	2.073*	91	.041
	否	22	3.364	1.372			

*p < .05　**p < .01　***p < .001

由表中可知，有無電腦病毒經驗的學童在測驗總分、行爲特性總分以及防毒策略總分中所得的分數有顯著差異，依據兩者的平均數來看，有電腦病毒經驗的學童其平均分數(4.07)高於沒有電腦病毒經驗的學童(3.364)，代表有無電腦病毒經驗的學童對於電腦病毒所產生的行爲以及在防範病毒的策略上有較深的了解。

電腦病毒的行爲特性多爲外顯行爲，因此學童會知道電腦已受到電腦病毒感染，多半是電腦出現不尋常的現象，並在解毒的過程中習得防範電腦病毒的技巧與處理的能力，研究者推論此爲成績產生差異的可能原因。

三、 每天平均上網時數與電腦病毒概念測驗的分析

研究者探討學童的電腦病毒概念是否會因每天平均上網時數的多寡而有差異，分別以前測的測驗總分、基本原則總分、行爲特性總分、廣義病毒總分與防毒策略總分，共五個面向進行單因子變異數分析，如表5-1-3。

表 5-1-3　每天平均上網時數變項單因子變異數分析

分數項目		平方和	自由度	平均平方和	F 檢定	顯著性
前測總分	組間	69.155	3	23.052	0.758	0.521
	組內	2706.006	89	30.405		
	總和	2775.161	92			
前測原則	組間	1.928	3	0.643	0.481	0.696
	組內	118.867	89	1.336		
	總和	120.796	92			
前測行爲	組間	45.254	3	15.085	1.22	0.307
	組內	1100.703	89	12.367		
	總和	1145.957	92			
前測廣義	組間	2.067	3	0.689	0.397	0.755
	組內	154.406	89	1.735		
	總和	156.473	92			
前測策略	組間	3.529	3	1.176	0.573	0.634
	組內	182.6	89	2.052		
	總和	186.129	92			

由表中可知，每天平均上網時數在五個面向所得的分數，皆未達顯著差異，代表學童每天上網時數的多寡並不影響電腦病毒概念的認知能力，研究者推論，學童上網時可能未留意電腦病毒的相關資訊，也沒有意識到網路爲目前電腦病毒流傳的主要媒介，僅專注於本身上網的目標與需求，可能是造成測驗成績沒有差異的原因。

四、 老師是否曾教授過電腦病毒知識與電腦病毒概念測驗的分析

研究者探討學童的電腦病毒概念是否會因學校教師曾教授過電腦病毒知識而有差異，分別以前測的測驗總分、基本原則總分、行爲特性總分、廣義病毒總分與防毒策略總分，共五個面向進行獨立樣本t檢定，如表5-1-4。

表 5-1-4　老師曾教授過電腦病毒知識變項獨立樣本 t 檢定

分數項目	教授病毒	個數	平均數	標準差	t 值	自由度	顯著性(雙尾)
總分	是	21	18.333	5.151	-1.292	90	.200
	否	71	20.099	5.596			
基本原則	是	21	1.571	1.287	0.028	90	.978
	否	71	1.563	1.118			
行爲特性	是	21	11.143	3.321	-1.711	90	.090
	否	71	12.634	3.559			
病毒廣義	是	21	1.714	0.956	-1.019	47.859	.313
	否	71	1.986	1.399			
防毒策略	是	21	3.905	1.640	-0.030	90	.976
	否	71	3.916	1.371			

由表中可知，教師是否曾教授電腦病毒知識在五個面向所得的分數，並未達顯著差異，研究者推論，電腦病毒概念測驗試卷中的題項在經由分析後，共有四個主要面向，並各自延伸多個子概念，若教師所採用的教材缺乏了其中某些面向或子概念，即可能是學童在成就測驗沒有差異的原因，因此可施以其他電腦病毒課程，來檢測教學內容是否爲影響學生電腦病毒概念成就差異的原因。

第二節 電腦病毒迷思概念分析

本研究利用「電腦病毒概念測驗試卷」針對國小六年級學童進行紙筆測驗，共93位學童接受電腦病毒概念前測，分析其紙筆測驗資料，統計各題項的答對比率，藉由此說明學童具有哪些電腦病毒迷思概念。

一、 電腦病毒「基本原則」的迷思概念

電腦病毒的基本原則爲自我複製及自行執行兩個概念，各有一題項，其中自我複製又分爲四小題，表示方法爲1(1)、1(2)、1(3)、1(4)。

(一) 自我複製：

自我複製的概念爲電腦病毒將病毒程式碼附著在不同類型的檔案格式上，即產生不同的電腦病毒類型，在本研究中分爲四類：開機型病毒、檔案型病毒、巨集病毒、描述語言病毒，要診斷學童是否了解電腦病毒的類型與檔案格式的意義。

表 5-2-1 自我複製題目表

題號	描　述		
1	電腦病毒可分爲四種，分別爲「開機型病毒」、「檔案型病毒」、「巨集病毒」、「描述語言病毒」，請你將這些病毒分別會感染的檔案**連接**起來。 **病毒種類**　　**選項** 1(1)開機型病毒 ●　　● .DOC 與 .XLS (Office 文書檔) 1(2)檔案型病毒 ●　　● .HTML 與 .VBS (網頁程式檔) 1(3)巨集病毒 ●　　● .EXE 與 .SCR (可執行檔) 1(4)描述語言病毒 ●　　● 磁碟片 與 硬碟		

第一大題自我複製概念的答題狀況如下表5-2-2：

表 5-2-2 自我複製答題狀況

題號	1(1)	1(2)	1(3)	1(4)
全體答對比例	38.71%	30.11%	9.68%	13.98%
選 1 人數	5.38%	23.66%	9.68%*	61.29%
選 2 人數	15.05%	21.51%	50.54%	13.98%*
選 3 人數	40.86%	30.11%*	12.90%	15.05%
選 4 人數	38.71%*	24.73%	26.88%	9.68%
4 題皆對比例	2.15%			

*爲該題的正確選項

從上述資料來看，每小題答對率明顯偏低，代表學童對學電腦病毒的種類以及被感染的檔案格式不了解所致。尤其是在巨集病毒與描述語言病毒的部份，學童答錯比率更高，分析結果多數的學童認爲巨集病毒感染HTML及VBS檔案，而描述語言病毒感染Office檔，此爲學童對檔案格式不明瞭所致。

而在自我複製項目中，僅有2人完全答對4小題，佔全體的2.15%，由此可知，學生對於電腦病毒種類及感染目標缺乏完整的概念。

(二) 自我執行：

自我執行的概念爲電腦病毒一旦附著於電腦檔案上，每一次當寄主程式被執行時，附著於寄主程式上的病毒程式亦會隨之被啓動。

表 5-2-3 自我執行題目表

題號	描述
4	電腦裡的檔案被電腦病毒感染後，開啓被感染的檔案，請問存在檔案裡的病毒： (1) 會隨著檔案開啓而被執行。 (2) 不會被執行。 (3) 隔幾天才會執行一次 。 (4) 病毒執行前會出現訊息，詢問你是否要執行，點選「是」病毒才會執行。

第四題自行執行概念的答題狀況如下表5-2-4：

表 5-2-4 自行執行答題狀況

題號	4
全體答對比例	64.52%
選 1	64.52%*
選 2	4.30%
選 3	2.15%
選 4	29.03%

*爲該題的正確選項

由上述的資料可發現，本題有64.52%以上的學生答對，但有29.03%比例的學生選擇選項(4)，從選項中可發現他們認爲病毒被執行前會詢問使用者是否要執行病毒程式，病毒能否執行的操控權在使用者手上，此想法與病毒的自我執行以及未授權性的概念相牴觸，若使用者保有此概念，研究者推論未來使用者可能對於不明來源的檔案都會直接開啓，而不考慮其危險性。

二、 電腦病毒「行為特性」的迷思概念

電腦病毒共細分爲9個特性，分別爲未授權性、傳染性、觸發性、持久性、主動攻擊性、不可預知性、潛伏性、破壞性、類比爲生物性病毒。以下將個別分析特性中的答對人數，並解析每一題的答題狀況，如表5-2-5。

表 5-2-5 行爲特性答題狀況

特性 (題數)	未授權性 (2)	傳染性 (4)	觸發性 (2)	持久性 (2)	主動攻擊性 (2)
全對人數	21	15	65	41	16
全對比例	22.58%	16.13%	69.89%	44.09%	17.20%

表5-2-5 行爲特性答題狀況(續)

特性 (題數)	僞裝技巧(3)	潛伏性(2)	破壞性(4)	類比爲生物 性病毒(2)
全對人數	3	25	1	29
全對比例	3.23%	26.88%	1.08%	31.18%

由上述資料顯示，在每一個特性中，能答對該特性所有題目的學生比例都偏低，9個特性中僅有觸發性全對人數超過一半，代表多數的學生在每一特性中，都存有迷思概念，因此接下來，我們將探討這些特性中所存在的問題，分別對每一個行爲特性深入探討學生在該特性中的迷思概念。

(一) 未授權性

表 5-2-6 未授權性題目表

題號	描　述
2	電腦病毒進入電腦時，會出現哪種情形？ (1) 螢幕上會出現「是否要執行病毒程式」的訊息。 (2) 電腦通常不會有明顯異狀。 (3) 螢幕會顯示「檔案已複製完成」的訊息。 (4) 電腦主機會發出像「救護車」聲音來警戒。
3	下列有關電腦病毒的描述，何者正確？ (1) 電腦病毒在取得使用者同意後，才能進入電腦。 (2) 電腦病毒會不斷發出訊息，讓使用者知道它的存在。 (3) 電腦病毒不需要使用者允許，就能進入電腦。 (4) 電腦病毒在刪除系統檔案時，會產生警告訊息。

上述兩題未授權性答題狀況分析如下表5-2-7：

表 5-2-7 未授權性答題狀況

題號	2	3
全體答對比例	30.11%	55.91%
選 1 人數	59.14%	10.75%
選 2 人數	30.11% *	25.81%
選 3 人數	4.30%	55.91%*
選 4 人數	6.45%	7.53%
2 題全對比例	22.58%	

*爲該題的正確選項

從上表中我們發現第2題，約60%的學生選擇錯誤選項(1)，由選項內容中可發現，學生認爲電腦病毒必須在使用者許可後，才能進入電腦，此迷思概念在第3題的選項1也測驗相同的概念，但在第3題中僅有10.75%的學生選擇(1)，因此可推斷學生的想法有矛盾的現象。在第3題中也有7.53%的學

生認爲電腦病毒在刪除檔案時，會警告使用者，這都是因爲學生不知道病毒取得權限進入電腦後，可以恣意進行破壞行爲。另外有超過25%的學生選擇錯誤選項(2)，認爲電腦病毒在進入電腦後，會不斷產生訊息，讓使用者發現自己的存在，而事實上電腦病毒在取得權限進入電腦後，會盡量隱藏自己的行爲，才能大量傳播。

(二) 傳染性

表 5-2-8 傳染性題目表

題號	描　述
5	電腦病毒<u>不會</u>透過下列哪種方法傳染出去？ (1) Yahoo 即時通。 (2) MP3 隨身碟。 (3) 電子郵件。 (4) 電腦的電源供應線。
6	從網路上下載非法軟體會中毒，這是因爲病毒寄生在哪種物體上進行散佈？ (1) 網路線 (2) 檔案 (3)網路卡 (4)數據機
7	有關軟體的使用，下列何者敘述正確？ (1) 新買的電腦裡面的軟體不會有電腦病毒。 (2) 使用盜版或免費的軟體，一定會中毒。 (3) 購買正版軟體就能確保不被病毒感染。 (4) 防毒軟體的更新檔案也會被電腦病毒感染。
8	哪種狀況下，比較容易讓電腦病毒侵入電腦？ (1) 使用防寫的磁片。 (2) 潮濕且發霉的磁片。 (3) 老舊的網路卡和網路線。 (4) 很久沒做漏洞更新的 Windows XP 作業系統

上述四題傳染性答題狀況分析如下表5-2-9：

表 5-2-9 傳染性答題狀況

題號	5	6	7	8
全體答對比例	55.91%	69.89%	32.26%	70.97%
選 1 人數	7.53%	25.81%	16.13%	5.38%
選 2 人數	35.48%	69.89%*	16.13%	6.45%
選 3 人數	1.08%	4.30%	35.48%	16.13%
選 4 人數	55.91%*	0.00%	32.26%*	70.97%*
四題皆對比例	16.13%			

*爲該題的正確選項

傳染性中四題全對的比例只有16.13%，接下來我們依序觀察哪些電腦病毒的傳染媒介是多數學生不知道的。從題號5中我們發現有35.48%的學生認爲MP3隨身碟不會傳染病毒，隨身碟病毒在今年(2007)被發現，並在學校區域網路內大量流傳，這代表學生尚未接觸新型態的傳播媒介，或是未發現自己已感染隨身碟病毒，且研究者發現，在坊間的電腦教科書裡介紹的病毒傳播媒介尚未提及隨身碟，因此研究者也建議未來相關的資料中也應提列此媒介。

在第6題中，有25.81%的學童認爲病毒是寄生在網路線上傳播的，這除了是對傳播媒介的誤解外，可了解學童對於電腦病毒感染檔案的模式不了解所致。

在第7題中，有35.48%的學童認爲購買正版軟體就不會感染病毒，各有16.13%的學童認爲新買的電腦裡面的軟體不會有病毒以及使用盜版或免費的軟體一定會中毒。學童不知道廠商在燒製軟體的過程，若不小心感染病毒，將會導致出產的光碟片也含有病毒，此原理也可以解釋選項(1)；而在選項(2)中，並非所有的盜版和免費軟體都有病毒，只是建議在使用軟體前仍須接受掃毒，因此在此傳染性的概念中，多數學童仍欠缺正確的軟體使用概念。

在第8題中，仍有16.13%的學童認爲老舊的網路卡和網路線容易造成病毒侵入，可看出學童認爲硬體才是傳播媒介，並缺乏系統漏洞爲近幾年來的主要傳播媒介的概念，但此系統漏洞的更新概念是必須要被提倡的。

綜合上述所言，學童仍存有的傳染性思概念爲認爲MP3隨身碟與系統漏洞不是病毒的傳染媒介，以及缺乏軟體的正確使用概念。

(三) 觸發性

表 5-2-10 觸發性題目表

題號	描　述
9	防毒軟體公司發佈一隻電腦病毒，會在 7 月 7 日當天開始發作破壞檔案，應該如何防範比較好？ (1) 把電腦時間調整成 7 月 8 日，就不會發作。 (2) 7 月 7 日那天都不要開機，隔天再開就不會發作。 (3) 7 月 7 日前先下載病毒更新檔進行掃毒。 (4) 7 月 7 日前把電腦檔案設爲隱藏，電腦病毒就找不到檔案了。
10	有一隻病毒只會在 13 號星期五當天開始刪除檔案，這代表何種意思？ (1) 病毒只會在 13 號星期五侵入電腦，其他時間電腦裡不會有病毒程式。 (2) 電腦隨時會被感染，病毒會存在電腦中，等待 13 號星期五開始破壞。 (3) 病毒只會在今年的十三號星期五內發作，明年就不會發作。 (4) 發作過一次後，下個十三號星期五就不會發作了。

在觸發性共有兩題，考驗學童對電腦病毒觸發前的防治方法與觸發機制運作的概念，兩題全對比例爲69.89%，有相當高的答對率，但仍有30%的學童對於觸發性仍有疑慮，從下表5-2-11作詳細的延伸探討：

表 5-2-11 觸發性答題狀況

題號	9	10
全體答對比例	79.57%	79.57%
選 1 人數	2.15%	13.98%
選 2 人數	11.83%	79.57%*
選 3 人數	79.57%*	1.08%
選 4 人數	5.38%	4.30%
2 題皆對比例	69.89%	

*爲該題的正確選項

在第9題中，答對比例接近8成，錯誤選項(1)與(2)測驗學童對於電腦病毒觸發時機的處理方法，共有13.98%的學童認爲預防將在7月7日觸發的病毒，最好的方法是將系統日期調整爲7月8日或隔天在開機就可以避免電腦受到破壞，這是學童不明白觸發時機一旦啓動，電腦病毒可能在觸發後的每一天都會執行，雖然觸發時機是由病毒作者自行設計，但此二選項並非正確的處理方法。

在第10題中，答對比例也將近8成，13.98%的學童選擇錯誤選項(1)，認爲在觸發條件滿足前，電腦裡不會存在電腦病毒，由此可看出學童亦缺乏潛伏期的概念。

(四) 持久性

表 5-2-12 持久性題目表

題號	描　述
11	電腦病毒在流行期過後會有下列哪一種狀況發生？ (1) 病毒會慢慢的消失不見，不再復發。 (2) 很久以前流行過的病毒，不會在新的作業系統上流傳。 (3) 曾經流行過的病毒，不會再次造成大流行。 (4) 過一陣子病毒可能會再次造成大流行。
12	有一隻病毒在學校電腦教室的網路中流傳，下面何者是正確的呢？ (1) 把老師使用的電腦清除乾淨，其他電腦中的病毒就會一起被清除掉。 (2) 其中一台電腦解完毒後，就不會再中毒了，可以繼續上網。 (3) 清除完病毒後，電腦連上網路，病毒也會再進入。 (4) 病毒只會攻擊電腦教室裡的電腦，所以校長室裡的電腦不會受到侵入。

持久性有兩題，概念爲電腦病毒難以完全消滅以及區域網路內的解毒時間是冗長的，兩題全對者僅有44.09%，代表學童在持久性上有值得探討的議題，深入分析如下表5-2-13：

表 5-2-13 持久性答題狀況

題號	11	12
全體答對比例	66.67%	59.14%
選 1 人數	12.90%	25.81%
選 2 人數	10.75%	8.60%
選 3 人數	8.60%	59.14%*
選 4 人數	66.67%*	4.30%
2 題皆對比例	44.09%	

*爲該題的正確選項

在第11題中，仍有32%左右的學童答錯，這些錯誤選項的意義爲病毒會消失，流行過的病毒不會再次造成大流行，若學童具有此概念，可能對於電腦中舊的檔案或電子郵件的敏銳度會降低，而容易再次受到感染。

在第12題中，有25.81%的學童認爲區域網路中的解毒方法爲只要清除教師電腦裡的病毒，其他電腦裡的病毒也會依同被清除；也就是認爲學生使用的電腦是不需要單機掃毒的，全仰賴教師電腦的解毒能力；同時可看出可看出學生缺乏區域網路解毒的概念，殊不知一旦感染透過區域網路傳播的病毒，解毒時間漫長且重複感染機會高。

(五) 主動攻擊性

表 5-2-14 主動攻擊性題目表

題號	描　述
13	我感染了一隻病毒，會透過電子郵件轉寄病毒程式給 Outlook 通訊錄中的聯絡人，首先應該要如何處理？ (1) 仍可繼續瀏覽網站，但不要使用 Outlook 寄信給朋友。 (2) 盡速拔除網路線來停止網路功能，使病毒無法寄信出去。 (3) 馬上改用線上信箱寄信(如 Yahaoo 免費信箱)，但仍可開啓 Outlook 來收信。 (4) 發信警告好友，不要開啓由我寄出的電子郵件。
14	哪一種情況下，電腦被病毒入侵的機會比較小？ (1) 使用隨身碟讀取檔案。 (2) 閱讀電子郵件。 (3) 我的電腦沒有上網，所以感染病毒的機會比較小。 (4) 雖然有的電腦開機會自動連上網路，但是只要不瀏覽網頁或不收信就不會感染。

主動攻擊性在本論文的定義爲電子郵件病毒可在系統背景自動發信功能，且寄件者可假借爲通訊錄中的名單以及只要連接網路就有被攻擊的可能，兩題全對者比例爲17.20%，代表大多數的學童至少都存有某一種迷思概念，如表5-2-15：

表 5-2-15 主動攻擊性答題狀況

題號	13	14
全體答對比例	25.81%	56.99%
選 1 人數	12.90%	18.28%
選 2 人數	25.81%*	4.30%
選 3 人數	7.53%	56.99%*
選 4 人數	52.69%	20.43%
2 題皆對比例	17.20%	

*爲該題的正確選項

從第13題有一半左右的學童認爲，一旦感染了電子郵件爲傳播媒介的病毒，要通知好友不要開啓由學童寄出的電子郵件，雖然這樣的行爲是出於好意，但因近期的病毒多假借好友名字作爲寄件者，因此可能不是以使用者的名字爲寄件者；另病毒可能在寄信的同時，再度流傳或附著在信件中傳出去，所以首要的處理步驟應該要先拔除網路線，避免再度擴散，並進行掃毒。另有20%的學童認爲，只要不開啓outlook寄信，仍可繼續上網，這就是缺乏只要一上網，病毒會自動發信的概念。

而在第14題中，有18.28%的學童認爲使用隨身碟讀取檔案比較不會被病毒入侵，目前的隨身碟病毒會利用自動播放的功能隨之啓動，並植入電腦主機中，等待下一位使用者插入隨身碟，再將病毒移植到隨身碟中，從學生的答案中可看出他們並不了解隨身碟病毒的運作模式；另有20.43%的學童認爲就算電腦連上網路，只要不瀏覽網頁或不收信，就不會感染病毒，這是學童缺乏網路中各種攻擊模式的概念。

(六) 不可預知性

表 5-2-16 不可預知性題目表

題號	描　述
15	電腦病毒不斷的改變原始病毒程式，來躲避防毒軟體的偵測，稱爲「變種病毒」，下列敘述何者正確？ (1) 只要防毒軟體有原始病毒的病毒碼，就可以攔截到變種病毒。 (2) 感染過原始病毒的電腦，就不會被他的變種病毒感染。 (3) 變種病毒可能會造成更大的流傳與破壞。 (4) 變種病毒的破壞能力比原始病毒小。
16	Jolin 收到四封含有附加檔案的 E-mail，請問開啓哪一個附加檔案<u>不會</u>中毒？(1)「好玩遊戲.exe」 (2)「好玩遊戲.txt.exe」 (3)「好玩遊戲.exe.txt」 (4)「好玩遊戲.txt　(中間有很多空白)　　.exe」
17	請問下列哪一封電子郵件是<u>比較</u>安全，而可以開啓的？ (1) 早上老師說要寄給我們期中考成績單，到了晚上我就收到標題爲「期中考成績單」的郵件。 (2) 收到微軟公司寄送的「作業系統更新程式」檔案，要立即執行安裝，來修補系統漏洞。 (3) 聖誕節前夕收到「聖誕老公公進城」的電腦螢幕保護程式，可以安裝來增加過節的氣氛。 (4) 收到網友寄的電子郵件附加檔案爲 www.myparty.com，可以安心點選。

本研究在不可預知性中的概念爲病毒的衍生性也就是了解變種病毒的特性，以及病毒的僞裝技巧，在本概念中全對比例爲3.23%，數據非常低，如表5-2-17，代表多數學童具有迷思概念，以下將詳細探討原因：

表 5-2-17 不可預知性答題狀況

題號	15	16	17
全體答對比例	64.52%	12.90%	51.61%
選 1 人數	19.35%	48.39%	51.61%*
選 2 人數	11.83%	20.43%	30.11%
選 3 人數	64.52%*	12.90%*	4.30%
選 4 人數	4.30%	17.20%	13.98%
3 題皆對比例		3.23%	

*爲該題的正確選項

在第15題中，有19.35%的學童認爲只要有原始病毒的病毒碼，防毒軟體就可以偵測到變種病毒，另有11.83%的學童認爲只要曾經感染過原始病毒，就不會感染變種病毒；這個想法若持續存在將影響學童缺乏變種病毒的警戒心。

在第16題中，僅有12.90%的學生答對，由此可知學生不了解雙副檔名的意義，也不知道病毒常利用執行檔格式作爲傳播的檔案，並對於無法被病毒感染的檔案格式*.txt無所知。

在第17題中，有30%的學童認爲微軟公司會寄發修補漏動程式給使用者，但實際上目前電腦都設計成會自動進行系統更新，並不需要微軟寄信通知。相同的防毒軟體也設定爲自動更新病毒定義檔，因此大多數以更新程式爲主旨寄發的電子郵件多是病毒採用的僞裝技巧；另有13.98%的學童選擇(4)，病毒將附加檔案僞裝成網址的模式，但其實也是雙副檔名的概念，最後的副檔名.com即是執行檔格式之一，而非網址。綜合上述所言，學童對於電腦病毒僞裝技巧的概念須再加強，才能有效預防病毒。

(七) 潛伏性

表 5-2-18 潛伏性題目表

題號	描　述
18	電腦病毒就像人類生病也有潛伏期，那電腦病毒的潛伏期是什麼意思呢？ (1) 從病毒被病毒作者產生，到病毒在世界上完全消失的時間。 (2) 從病毒感染檔案到病毒開始產生破壞行爲的時間。 (3) 從病毒被病毒作者產生，到病毒有解毒碼的時間。 (4) 從病毒被防毒軟體偵測到，到防毒軟體完全解毒的時間。
19	電腦病毒在潛伏期時會不斷地感染檔案，此時病毒是如何運作的呢？ (1) 病毒會不斷的重複感染相同的檔案，讓病毒程式在整個檔案中佔的比例越來越大。 (2) 病毒的潛伏期越長，代表感染檔案的能力比較弱，要花較多的時間把病毒程式寫入檔案中。 (3) 大部分病毒的潛伏期約爲一週。 (4) 病毒在潛伏期間會盡其所能的感染檔案。

本研究對潛伏性的概念爲了解潛伏期的定義以及病毒在潛伏期間的運作行爲，兩題全對者僅有26.88%，以下將進行深入探討，如表5-2-19。

表 5-2-19 潛伏性答題狀況

題號	18	19
全體答對比例	51.61%	47.31%
選 1 人數	7.53%	31.18%
選 2 人數	51.61%*	10.75%
選 3 人數	20.43%	10.75%
選 4 人數	19.35%	47.31%*
2 題皆對比例	26.88%	

*爲該題的正確選項

從第18題可得，有50%的學童缺乏潛伏期的定義，無法自行利用人類生物性病毒的經驗推論。而在第19題可知，約有31.18%的學童認爲病毒會重複感染檔案，讓病毒碼所佔的比例越來愈大，這是學童不知道病毒爲了隱藏自己，會縮小程式碼，讓檔案大小盡量不改變，因此多數病毒在感染檔案前，會檢查該檔案是否已植入病毒程式來避免重複感染。

(八) 破壞性

表 5-2-20 破壞性題目表

題號	描　述
20	電腦病毒<u>不會</u>有哪種破壞行爲？ (1) 刪除檔案或格式化磁碟。 (2) 損毀鍵盤按鍵。 (3) 感染其他乾淨的檔案。 (4) 妨礙螢幕顯示。
21	下列哪一種狀況<u>不是</u>電腦中毒後會產生的狀況？ (1) 光碟無法讀取。 (2) 電腦無預警的重新開機。 (3) 系統運作緩慢。 (4) 上網速度變慢。
22	電腦病毒感染系統後，若不進行解毒可能會有什麼狀況產生？ (1) 電腦會燒毀。 (2) 電腦散熱風扇不會轉動。 (3) 過一段時間系統會自動解毒痊癒。 (4) 程式會無法開啓。
23	會立即造成電腦無法開機的病毒，有哪種特性？ (1) 會在短時間內造成大範圍的流傳。 (2) 解毒容易。 (3) 不容易傳散。 (4) 幾分鐘後再重新開機，就會恢復正常。

本研究提出的破壞性行爲測驗中，四題全對者爲1.08%，僅有一人，因此必須深入探討何者爲多數學童缺乏的概念，分析如下表5-2-21：

表 5-2-21 破壞性答題狀況

題號	20	21	22	23
全體答對比例	78.49%	29.03%	83.87%	18.28%
選 1 人數	6.45%	29.03%*	5.38%	67.74%
選 2 人數	78.49%*	47.31%	6.45%	6.45%
選 3 人數	7.53%	8.60%	4.30%	18.28%*
選 4 人數	7.53%	13.98%	83.87%*	6.45%
四題皆對比例	1.08%			

*爲該題的正確選項

從第20題與第22題得答對人數來看，少數學童具有病毒會破壞鍵盤或造成光碟無法讀取資料的迷思概念；但從第21題與第23題來看，則顯示多數學童有迷思概念。

在第21題中顯示，47.31%的學生認爲電腦無預警的重新開機不是病毒的破壞行爲，而是認爲此現象爲硬體本身的問題，但事實爲目前許多系統漏洞的病毒就會造成電腦不斷重新開機，因此若學童不知道此爲電腦病毒問題，則無法找出解決問題。

在第23題則顯示，有67.74%的學生認爲立即造成電腦無法開機的病毒會在短時間內造成大範圍的流傳，但事實上此概念與潛伏性及傳染性有關聯，若潛伏期長，則病毒的流傳廣，一旦破壞性強大，則容易造成嚴重的損失。但若病毒一侵入電腦即刻造成無法開機，則容易導致病毒沒有時間大量傳播。

(九) 類比為生物性病毒

表 5-2-22 類比爲生物性病毒題目表

題號	描　述
24	下列關於電腦病毒的說明何者是正確的？ (1) 電腦一旦中毒，就像人類感冒一樣會變的很虛弱，因此更容易感染別的電腦病毒。 (2) 長時間使用電腦，會讓電腦疲累，此時病毒較容易侵入。 (3) 感染電腦病毒後會產生抗體，不會重複感染相同的電腦病毒。 (4) 沒有安裝防毒軟體或沒有進行系統更新，就像人類沒有抗體，容易感染病毒。
25	對於電腦病毒傳染的描述，下列何者正確？ (1) 污損的光碟片沾黏病毒，造成電腦讀取光碟時容易把病毒寫入電腦中。 (2) 醫院裡病人所散發出來的病菌容易附著在網路線或無線網路上傳送到電腦中。 (3) 電腦教室中有電腦中毒，避免讓未中毒的電腦近距離接觸感染源，所以要將未中毒的電腦搬到另一個房間。 (4) 電腦病毒就好像 SARS 病毒一樣，到任何一個國家，電腦都可能會感染相同的電腦病毒。

在本研究中對於類比爲生物性病毒的定義爲可以從人類生物性病毒的特性推論電腦病毒的特性，例如將防毒軟體比喻爲人類的抗體、電腦病毒可流傳至全世界，但仍有些人類生物性病毒的觀點是無法推論至電腦病毒的，例如電腦無法自行產生抗體。

在此概念中，兩題全對者的比例爲31.18%，代表多數學童仍具有某一迷思概念，於下表中進行深入探討，如表5-2-23：

表 5-2-23 類比爲生物性病毒答題狀況

題號	24	25
全體答對比例	47.31%	63.44%
選 1 人數	36.56%	15.05%
選 2 人數	9.68%	7.53%
選 3 人數	6.45%	12.90%
選 4 人數	47.31%*	63.44%*
二題皆對比例	31.18%	

*爲該題的正確選項

在第24題中可以看出有36.56%的學生認爲一旦電腦感染病毒，會變的很虛弱，容易感染其他電腦病毒，但事實上是電腦本身的系統出現問題時，如系統漏洞、開啓了病毒常用的port後，才容易感染其他的病毒。

在第25題中，15.05%的學童認爲污損的光碟片也會感染病毒，研究者認爲這是學童認爲不乾淨的食物會造成人類生病推論所致；12.90%的學童則認爲在同一區域網路中的電腦，只要遠離受到電腦病毒感染的電腦，就可避免受到感染，研究者推論這是學童認爲不要近距離接觸感冒的人就可以減少被感染的機會推論所致，殊不知在區域網路內的電腦就容易會感染病毒。事實上，人類生物性病毒與電腦病毒仍有不一致之處，必須釐清學童的兩者間的差異。

三、 廣義電腦病毒的迷思概念

表 5-2-24 廣義病毒題目表

題號	描　述
26	「電腦病毒」、「電腦蠕蟲」、「木馬」都是不懷好意的電腦程式，請你選出他們有什麼相同的地方？ (1)　不需經過使用者同意，就可以自行植入電腦。 (2)　都會感染乾淨的檔案。 (3)　大多會刪除系統檔案，使系統無法正常運作。 (4)　這些惡意程式都是使用者自己在網路下載才會感染的。
27	何者是「電腦蠕蟲」的特性？ (1)　取得使用者同意後才會進入電腦中。 (2)　透過網路傳送電腦蠕蟲到其他電腦中，造成網路變慢。 (3)　會感染系統中乾淨的檔案。 (4)　假借爲有用的工具軟體，吸引使用者下載。
28	下列何者**不是**「特洛依木馬」的特性？ (1)　常假借爲有用的工具軟體，吸引使用者下載。 (2)　目的多爲竊取使用者電腦中的資料。 (3)　會主動將病毒植入其它電腦裡。 (4)　使用者在不知情的狀況下被植入木馬。
29	好友寄來一封警告病毒的信件，內容是『趕快搜尋系統中是否有 jdbgmgr.exe，有的話代表你已經中毒，盡快刪除此檔，避免病毒再度流散。我也已經刪除檔案了，電腦目前很正常。』經過搜尋，電腦中真的有這個 jdbgmgr.exe 檔案，你該如何處理？ (1)　重新安裝作業系統。 (2)　依照指示把 jdbgmgr.exe 檔案刪除掉。 (3)　把這個消息再傳給我的好朋友們。 (4)　把這封警告信件傳給防毒公司進行檢測。
30	收到一封信是『最新強大病毒通知!要小心一封名爲「來抽支籤!」的郵件，收到後請勿開啓，並請立即刪除，它會讓電腦無法關機還會自行寄給你連絡簿裡的朋友。請將這個消息轉寄給在你通訊錄裡的所有人 !希望能來得及!』當你收到這封信後，應該要如何處理？ (1)　趕緊轉寄給朋友，提醒他們小心。 (2)　把信件貼到網路討論區，警告大家。 (3)　到防毒公司網站查詢相關資訊。 (4)　趕緊搜尋信箱，若有『來抽支籤!』的郵件，就將此信件刪除，並且寄信告訴大家。

廣義病毒包含了電腦蠕蟲、特洛伊木馬及謠言信三個概念，在此項目中5題全對比例僅有3.23%，代表學童至少對某一類惡意程式有迷思概念，以下將深入探討，如表5-2-25：

表 5-2-25 廣義病毒答題狀況

題號	26	27	28	29	30
全體答對比例	41.94%	38.71%	24.73%	45.16%	41.94%
選 1 人數	41.94%*	12.90%	25.81%	16.13%	10.75%
選 2 人數	19.35%	38.71%*	25.81%	25.81%	12.90%
選 3 人數	11.83%	17.20%	24.73%*	10.75%	41.94%*
選 4 人數	25.81%	29.03%	22.58%	45.16%*	34.41%
5 題皆對比例			3.23%		

*爲該題的正確選項

本試卷的第26題、第27題與第28題是在檢測學童是否能判別電腦病毒、電腦蠕蟲以及特洛伊木馬的差異性與了解其主要概念，但從答題的比例來看，每一個錯誤選項都有高比例的學童選擇，推論得知多數學童不具有病毒、蠕蟲與木馬的概念。

在第29題、30題則是檢測學童面對謠言信件時的處理方法，從選項的比例來看，多數的學童會聽信謠言信的內容刪除檔案，並將信件轉發給好友，這表示學童容易受到謠言影響，進而傷害電腦或再度造成他人的困擾。

綜合上述所言，若學童能正確分辨各種惡意程式的特性與傳播方法，將可遏止惡意程式的流傳，感染病毒後也能採行有效的處理方法。

四、 電腦病毒防毒策略的迷思概念

表 5-2-26 防毒策略題目表

題號	描　述
31	防治電腦病毒最好的方法是下列哪一選項？ (1) 登入密碼不可以是空白的，所以要設定密碼爲 abc 即可以保護電腦不被入侵。 (2) 每年年底都要進行檔案備份。 (3) 執行檔案前先掃毒。 (4) 將檔案都設成”隱藏”，病毒看不見就不會感染。
32	當你感覺電腦可能中毒了，必須要做何種處理方法？ (1) 重新安裝作業系統。 (2) 立即切斷網路，進行掃毒。 (3) 趕快備份檔案，將檔案拿到其他電腦上繼續工作。 (4) 刪除那些可能是電腦病毒的檔案。
33	請問下列哪一組電腦登入密碼最能防治病毒侵入呢? (1) 不設密碼。 (2) 簡短好記的密碼，如 123。 (3) 用英文、數字以及符號組成的密碼，如 xin09$%28。 (4) 用英文單字做爲密碼，如 APPLE。
34	下列敘述何者正確？ (1) 電腦沒有上網，因此不需要安裝防毒軟體。 (2) 有安裝防毒軟體就代表電腦已受到完整的保護。 (3) 購買防毒軟體後，防毒軟體公司能提供解毒支援服務。 (4) 防毒軟體能防護所有已知及未知的病毒。
35	防毒軟體的解毒功能，何者敘述是正確的？ (1) 只要是防毒軟體能偵測到的病毒，都能解毒成功。 (2) 防毒軟體無法解毒的檔案，必須要立即刪除檔案。 (3) 防毒軟體沒有偵測到任何病毒，代表目前未受到感染。 (4) 經由防毒軟體解毒後的檔案，不能保證可以正常執行。
36	目前市面上的防毒軟體通常有三種解毒狀況，分別爲「修復」、「刪除」、「隔離」，請將代表的意思**連接**起來？(注意：本題只有**三條**連接線) 修復 ●　● 病毒檔案被移至電腦的另一個資　料夾裡，暫時不會被偵測到。 隔離 ●　● 附著在檔案上的電腦病毒程式，已經被移除了，檔案通常可以繼續運作。 刪除 ●　● 將偵測到的病毒檔案移至資源回收筒。 ● 電腦病毒檔案在電腦裡已經找不到了。

在本研究中將防毒策略區分爲兩個面向，分別爲個人防治以及防毒軟體使用，個人防制的測驗題號爲 31、32、33，在此面向中全數答對的比例爲 24.73%；而防毒軟體使用的測驗題號爲 34、35、36，在此面向中全數答對的比例爲 2.15%。由數據可知仍有多數的學童對於防治病毒的方法尚有不足之處，將詳細探討學童有哪些想法仍待澄清，如表 5-2-37。

(一) 個人防治

表 5-2-27 個人防治答題狀況

題號	31	32	33
全體答對比例	68.82%	45.16%	59.14%
選 1 人數	11.83%	17.20%	17.20%
選 2 人數	13.98%	45.16%*	9.68%
選 3 人數	68.82%*	11.83%	59.14%*
選 4 人數	5.38%	25.81%	13.98%
5 題皆對比例		24.73%	

*爲該題的正確選項

從個人防制的面向來看，在第 31 題中，多數的學童都知道執行檔案前最好能先掃毒，但有 11.83%的學童知道密碼不可以空白，卻不知道 abc 是一組不安全的密碼；另有 13.98%的學童了解備份的重要性，但對於重要資料必須隨時備份的概念不清楚。

在第 32 題中，有約 40%的學童認爲若感覺電腦感染病毒，必須要重新安裝作業系統或是立即把那些可能是病毒檔案刪除掉。較正確的作法爲先了解感染的病毒類型，若爲系統漏洞的病毒，重新安裝作業系統並非最好的選擇，下載系統更新程式才是正確的作法；若不了解病毒的行爲特性而立即刪除疑似病毒檔案，則有可能會造成系統問題。

在第 33 題中，仍有 17.20%的學童認爲不需設置登入密碼，而有 13.98%的學童認爲以英文單字作爲密碼即可保護電腦，可看出學童缺乏設立一組安全密碼原則的概念。

(二) 防毒軟體使用

表 5-2-28 防毒軟體答題狀況

題號	34	35	36(1)	36(2)	36(3)
全體答對比例	53.76%	25.81%	49.46%	70.97%	17.20%
選 1 人數	10.75%	22.58%	15.05%	70.97%*	1.08%
選 2 人數	15.05%	32.26%	49.46%*	13.98%	27.96%
選 3 人數	53.76%*	19.35%	13.98%	8.60%	48.39%
選 4 人數	20.43%	25.81%*	21.51%	5.38%	17.20%*
5 題皆對比例			2.15%		

*爲該題的正確選項

從防毒軟體使用的面向來看，在第 34 題中，有 20.43%的學童認爲裝了防毒軟體就能防護所有已知或未知的病毒，而另有 15.05%的學童認爲安裝防毒軟體就代表電腦已受到完整保護，但事實上，多數的防毒軟體仍無法百分之百偵測到病毒，因此防毒軟體並不能保證能完全防護電腦安全。

在第 35 題中，每一個錯誤選項都有相當多的學童選擇，從這些選項中可知學童視防毒軟體爲能完全防禦病毒的工具，認爲防毒軟體一定可以清除偵測到的病毒，對於那些無法解毒的檔案就必須直接刪除，而第四個錯誤的選項則可看出學童相信防毒軟體的掃毒功能；以上這些問題都可能造成學童過分依賴防毒軟體，缺乏自行判斷檔案安全性的能力。

第 36 題又分爲 3 小題，分別請學童指出「修復」、「隔離」、「刪除」三個掃解毒模式來檢測學童使用防毒軟體的能力，在此三個項目中以「刪除」選項的答錯率最高，學童認爲防毒軟體會將刪除的病毒程式移至資源回收筒，但實際上，爲避免病毒再度被執行，因此電腦中不會存有這些被刪除的病毒檔案。

綜合上述所言，若學童認爲防毒軟體可以完整保護電腦與百分之百偵測已知與未知病毒的，一旦流傳新型態病毒，則缺乏自行判斷能力。

第三節　電腦病毒概念教學成效分析

本節爲實驗處理後，對學童施以電腦病毒概念後測所得的結果與前測成績進行比較分析，來說明學童在實驗處理後的學習成效。

一、　電腦病毒概念前後測總成績分析

分別以成對樣本t檢定來檢測三組個別在總成績的提升情況、以單因子共變數分析來檢測組別間的差異，分析如下：

(一) 電腦病毒概念前後測總成績成對樣本t考驗

研究者探究三組學童分別在總分的前後測成績表現是否有提升，採用成對樣本t檢定分別對三組學生進行分析，如表5-3-1。

表 5-3-1　三組測驗總分的成對樣本 t 檢定

組別		平均數	個數	標準差	t	自由度	顯著性(雙尾)
實驗組 1	前測總分	22.194	31	5.706	-6.834***	30	.000
	後測總分	30.387	31	6.776			
實驗組 2	前測總分	19.963	27	5.103	-3.052**	26	.005
	後測總分	22.630	27	5.386			
控制組	前測總分	17.233	30	4.681	-2.849**	29	.008
	後測總分	19.100	30	5.448			

*p < .05　**p < .01　***p < .001

在表5-3-1可得，三組學童在測驗總分面向的前後測成績表現上皆達顯著差異，實驗組1與實驗組2在接受教學後都能提升電腦病毒概念；然而未接受實驗教學的控制組在經過三個禮拜的時間後也能有所成長，研究者推論控制組在前測結束後，可能會引發學童進行團體討論或測驗引發學童對電腦病毒產生關注，甚或在其間學童親身經歷電腦病毒威脅都有可能造成控制組在測驗總成績上有顯著提升；而造成控制組成長的另一可能原因爲「強亨利效應」，同校的學生可能互相認識，而控制組學生若得知實驗組學童正在接受電腦病毒概念改變課程教學，或許會產生與實驗組學生相互競爭之意識，而使其表現提升(王文科、王志宏，2006)。

(二) 電腦病毒概念前後測總成績共變數分析

爲確認分組與前測的交互作用可能影響後測結果，以前測爲共變數，後測成績爲依變數，進行迴歸係數同質性考驗，如表5-3-2。

表 5-3-2 三組學生在「電腦病毒概念」後測成績迴歸同質性考驗摘要表

變異來源	SS	df	MS	F	P
組別*前測 (回歸係數同質性)	50.643	2	25.321	1.073	.347
Error(誤差)	1935.609	82	23.605		

由上表可知，F=1.073，P=0.347>.05，滿足迴歸係數同質性檢定的基本假設，各組組內迴歸線平行，因此可繼續進行共變數分析，如表5-3-3。

表 5-3-3 三組學生在「電腦病毒概念後測」成績共變數分析摘要表

變異來源	SS	df	MS	F	P
前測	1006.100	1	1006.100	42.549***	.000
組別	945.176	2	472.588	19.986***	.000
誤差	1986.252	84	23.646		
校正後的總數	5025.773	87			

*p < .05　**p < .01　***p < .001

由表5-3-3可發現前測的確會影響後測的分數(F=42.549，p=.000<.05)，而在去除前測的影響後，三組學生在後測上有顯著差異F=19.986，p=.000 < .05，因此以Bonferroni法進行事後比較，才能得知哪幾組樣本在後測上有顯著差異。

表 5-3-4 三組學生在「電腦病毒概念後測」成績事後比較表

組別		平均數差異	標準誤	顯著性
實驗組1	實驗組2	6.279	1.300	.000***
	控制組	7.999	1.344	.000***
實驗組2	實驗組1	-6.279	1.300	.000***
	控制組	1.720	1.319	.588
控制組	實驗組1	-7.999	1.344	.000***
	實驗組2	-1.720	1.319	.588

*p < .05　**p < .01　***p < .001

表 5-3-5 三組後測的原始平均數與調整後平均數

組別	平均數	標準差	調整後平均數	標準誤
實驗組1	30.387	6.778	28.812	.906
實驗組2	22.630	5.38	22.543	.936
控制組	19.100	5.4486	20.814	.926

在事後比較的表5-3-4中呈現，實驗組1對其他兩組在後測的成績上有顯著差異，也可由由表5-3-5可知，實驗組1後測調整後的平均數爲28.812，明顯優於其他兩組的後測調整後平均數(分別爲22.543與20.814)，這表示實驗組1所採用的教材能提升電腦病毒的概念；但實驗組2在接受電腦病毒推廣教材的實驗處理後，其後測成績與未接受實驗處理的控制組之後測成績，兩者間並無顯著差異，這表示實驗組2的教材無法有效提升學童的電腦病毒概念。

研究者分析實驗組2的教材並未涵蓋電腦病毒的所有概念，並缺乏讓學習者實際接觸病毒的經驗，因此在整體成就上無法有效提升電腦病毒的整體概念，研究者將針對試題的四個面向「基本原則」、「行爲特性」、「廣義病毒」以及「防毒策略」分別進行探究。

二、 電腦病毒概念前後測在「基本原則」成績分析

分別以成對樣本t檢定來檢測三組個別在「基本原則」成績的提升情況、以單因子共變數分析來檢測組別間的差異，以描述性統計分析各題項的測驗結果，分析如下：

(一) 電腦病毒概念「基本原則」前後測成績成對樣本t考驗

在基本原則面向的測驗中，共計5題，總分爲5分，採用成對樣本t檢定分別對三組學生進行檢測，分別分析三組學童的前後測成績在此面向中是否有所提升。

表 5-3-6 基本原則成對樣本 t 檢定

組別		平均數	個數	標準差	t	自由度	顯著性(雙尾)
實驗組 1	前測總分	1.903	31	1.193	-5.964***	30	.000
	後測總分	3.807	31	1.223			
實驗組 2	前測總分	1.7037	27	0.9929	-0.422	26	.676
	後測總分	1.8148	27	1.1448			
控制組	前測總分	1.1333	30	1.0743	-0.972	29	.339
	後測總分	1.3333	30	0.8023			

*p < .05 **p < .01 ***p < .001

由表5-3-6可知，僅有實驗組1學童在基本原則面向的前後測成績達到顯著t=-5.964 (P=.000<.05)，也就是實驗組1在經過實驗教學後能提升在電腦病毒基本原則面向上的概念。而其他兩組則未達到顯著，顯示電腦病毒推廣教材無法有效提升學生在基本原則上的概念，而未接受教學處理的控制組在此面向上也無法獲得澄清。

(二) 電腦病毒概念「基本原則」前後測成績共變數分析

此部份是針對電腦病毒概念測驗試卷中的「基本原則」面向做分析，此面向有5題，總計爲5分。

首先爲確認組別與「基本原則」前測成績的交互作用可能影響後測結果，因此以「基本原則」前測成績爲共變數，「基本原則」後測成績爲依變數，進行迴歸同質性考驗，如表5-3-7 。

表 5-3-7 三組學生在「基本原則」後測成績迴歸同質性考驗摘要表

變異來源	SS	df	MS	F	P
組別*前測 (回歸係數同質性)	2.339	2	1.169	1.016	.366
Error(誤差)	94.335	82	1.15		

由上表可知，F=1.016，p =.366<.05，滿足迴歸係數同質性檢定的基本假設，各組組內的迴歸線平行，因此可繼續進行共變數分析，如表5-3-8。

表 5-3-8 三組學生在「基本原則」成績共變數分析摘要表

變異來源	SS	df	MS	F	P
前測	0.906	1	0.906	0.787	.377
組別	93.755	2	46.877	40.732***	.000
誤差	96.673	84	1.151		
校正後的總數	202.080	87			

*p < .05　**p < .01　***p < .001

由表5-3-8可發現在去除前測的影響後，三組學生在後測上有顯著差異F=40.732，p=.000 < .05，因此以Bonferroni法進行事後比較，才能得知哪幾組樣本在後測上有顯著差異。

表 5-3-9 三組學生在「基本原則」成績事後比較表

組別		平均數差異	標準誤	顯著性
實驗組1	實驗組2	1.973	0.283	.000***
	控制組	2.400	0.287	.000***
實驗組2	實驗組	-1.973	0.283	.000***
	控制組	0.428	0.291	.436
控制組	實驗組	-2.400	0.287	.000***
	實驗組2	-0.428	0.291	.436

p < .05　**p < .01　***p < .001

表 5-3-10 三組「基本原則」後測的原始平均數與調整後平均數

組別	平均數	標準差	調整後平均數	標準誤
實驗組1	3.807	1.223	3.776	0.196
實驗組2	1.815	1.145	1.803	0.207
控制組	1.333	0.802	1.375	0.202

在事後比較的表5-3-9中呈現，實驗組1對其他兩組在「基本原則」後測的成績上有顯著差異，也可由由表5-3-10可知，實驗組1調整後的後測平均

數爲3.776，明顯優於其他兩組調整後的後測平均數(分別爲1.803與1.375)，這表示實驗組1所採用的教材能提升電腦病毒「基本原則」面向的概念；但在後測成績上，接受電腦病毒推廣教材教學的實驗組2後與未受實驗處理的控制組，兩者並無顯著差異，這表示實驗組2的教材無法有效提升學童在電腦病毒「基本原則」的概念。

(三) 電腦病毒「基本原則」概念轉變情形

表 5-3-11 三組學童在「基本原則」概念改變情形

基本原則		實驗組1		實驗組2		控制組	
概念	題號	前測 答對率	後測 答對率	前測 答對率	後測 答對率	前測 答對率	後測 答對率
自我複製	1-1	50.00%	81.25%*	38.71%	37.93%	26.67%	37.50%
	1-2	40.63%	65.63%*	19.35%	34.48%	30.00%	15.63%
	1-3	12.50%	75.00%*	12.90%	10.34%	3.33%	15.63%
	1-4	25.00%	71.88%*	16.13%	20.69%	0.00%	6.25%
自行執行	4	65.63%	78.13%	74.19%	79.31%	53.33%	65.63%

*爲該題目後測成績高於前測20%以上

在電腦病毒「基本原則」面向中的「自我複製」概念上，實驗組1在1-1~1-4題項中皆提昇了至少25%，這是實驗組1採研究者自行研擬之電腦病毒概念改變課程進行實驗處理，運用四種模擬的病毒類型程式，讓學童實際接觸電腦病毒，並帶入副檔名的概念(詳見附錄四)，但從數據可知教學後仍無法讓全體學童完全釐清不同類型的電腦病毒所感染的檔案格式，推論原因可能爲檔案格式類型過多，若一次給予學童所有概念，也可能造成學童混淆；而實驗組2與控制組在「自我複製」概念中皆未有明顯的成長，探究原因爲實驗組2採用傳統講述法說明病毒演變的歷程，並以電腦病毒案例介紹病毒種類，而無法加強學童印象；因此可說明實驗組1的教材在此概念中是有效的。

在「自行執行」的概念上，實驗組1與控制組均成長了12%以上；而實驗組2在前測的答對率(74.19%)高於其他兩組(65.63%與65.63%)，但在後測中僅成長5.12%，在實驗組2的教學中並未提及自行執行的概念，可能爲答對率未能大量提升的原因。

研究者認爲，學生實際操作副檔名與病毒種類的關係，運用學習單來反覆練習，並帶入自我執行的概念，將能提升電腦病毒基本原則面向的概念。

三、 電腦病毒概念前後測在「行為特性」成績分析

分別以成對樣本t檢定來檢測三組個別在「行爲特性」成績的提升情況、以單因子共變數分析來檢測組別間的差異，以描述性統計分析各題項的測驗結果，分析如下：

(一) 電腦病毒概念「行為特性」前後測成績成對樣本t考驗

在行爲特性面向的測驗中，共計22題，總分爲22分，採用成對樣本t檢定分別對三組學生進行檢測，分別分析三組學童的前後測成績在此面向中是否有所提升。

表 5-3-12 行爲特性成對樣本 t 檢定

組別		平均數	個數	標準差	t	自由度	顯著性(雙尾)
實驗組 1	前測總分	13.645	31	3.261	-5.162***	30	.000
	後測總分	17.226	31	3.836			
實驗組 2	前測總分	12.407	27	3.511	-1.933	26	.064
	後測總分	13.704	27	3.506			
控制組	前測總分	11.033	30	3.518	-1.343	29	.190
	後測總分	11.833	30	4.145			

*p < .05 **p < .01 ***p < .001

由表5-3-12可知，僅有實驗組1學童在行爲特性面向的前後測成績達到顯著t=-5.162 (P=.000<.05)，也就是實驗組1在經過實驗教學後能提升在電腦病毒行爲特性面向上的概念。而其他兩組則未達到顯著，顯示電腦病毒推廣教材無法有效提升學生在行爲特性上的概念，而未接受教學處理的控制組在此面向上也無法獲得澄清。

(二) 電腦病毒概念「行為特性」前後測成績共變數分析

此部份是針對電腦病毒概念測驗試卷中的「行爲特性」面向做分析，此面向有23題，總計爲23分。

首先爲確認組別與「行爲特性」前測成績的交互作用可能影響後測結果，因此以「行爲特性」前測成績爲共變數，「行爲特性」後測成績爲依變數，進行迴歸同質性考驗，如表5-3-13。

表 5-3-13 三組學生在「行爲特性」後測成績迴歸同質性考驗摘要表

變異來源	SS	df	MS	F	P
組別*前測 (回歸係數同質性)	16.239	2	8.12	0.747	.477
Error(誤差)	890.935	82	10.865		

由上表可知，F=0.747，p =.000>.05，滿足迴歸係數同質性檢定的基本假設，各組組內的迴歸線平行，因此可繼續進行共變數分析，如表5-3-14。

表 5-3-14 三組學生在「行爲特性」後測成績共變數考驗摘要表

變異來源	SS	df	MS	F	P
前測	352.041	1	352.041	32.597***	.000
組別	219.089	2	109.545	10.143***	.000
誤差	907.174	84	10.8		
校正後的總數	1716.716	87			

*p < .05 **p < .01 ***p < .001

由表5-3-14中發現前測的確會影響後測的分數(F=32.597，p=.000<.05)，在去除前測的影響後，三組學生在後測上有顯著差異F=10.143，p=.000 < .05，因此以Bonferroni法進行事後比較，才能得知哪幾組樣本在「行爲特性」的後測上有顯著差異，如表5-3-15。

表 5-3-15 三組學生在「行爲特性」後測成績事後比較

組別		平均數差異	標準誤	顯著性
實驗組1	實驗組2	2.787	0.875	.006**
	控制組	3.842	0.884	.000***
實驗組2	實驗組1	-2.787	0.875	.006**
	控制組2	1.055	0.883	.708
控制組	實驗組1	-3.842	0.884	.000***
	實驗組2	-1.055	0.883	.708

*p < .05 **p < .01 ***p < .001

表 5-3-16 三組「行爲特性」後測的原始平均數與調整後平均數

組別	平均數	標準差	調整後平均數	標準誤
實驗組 1	17.226	3.836	16.472	0.605
實驗組 2	13.704	3.506	13.684	0.632
控制組	11.833	4.145	12.63	0.616

在事後比較表5-3-15中呈現，實驗組1對其他兩組在「行爲特性」後測的成績上有顯著差異，也可由表5-3-16可知，實驗組1調整後的後測平均數爲16.472，明顯優於其他兩組的後測調整後平均數(分別爲13.684與12.63)，這表示實驗組1所採用的教材能提升電腦病毒「行爲特性」面向的概念；但在後測成績上，接受電腦病毒推廣教材教學的實驗組2與未受實驗處理的控制組，兩者並無顯著差異，這表示實驗組2的教材無法有效提升學童在電腦病毒「行爲特性」的概念。

(三) 電腦病毒「行為特性」概念改變情形

表 5-3-17 三組學童在「行爲特性」概念改變情形

行爲特性		實驗組1		實驗組2		控制組	
概念	題號	前測 答對率	後測 答對率	前測 答對率	後測 答對率	前測 答對率	後測 答對率
未授權性	2	40.63%	62.50%*	29.03%	72.41%*	20.00%	21.88%
	3	59.38%	93.75%*	61.29%	82.76%*	43.33%	43.75%
傳染性	5	68.75%	96.88%*	45.16%	75.86%*	53.33%	53.13%
	6	84.38%	71.88%	61.29%	58.62%	63.33%	53.13%
	7	31.25%	68.75%*	25.81%	31.03%	40.00%	40.63%
	8	78.13%	90.63%	54.84%	89.66%*	76.67%	65.63%
觸發性	9	78.13%	78.13%	74.19%	79.31%	83.33%	93.75%
	10	84.38%	81.25%	74.19%	79.31%	76.67%	78.13%
持久性	11	65.63%	81.25%	74.19%	82.76%	56.67%	71.88%
	12	62.50%	71.88%	64.52%	58.62%	50.00%	46.88%

表 5-3-17 三組學童在「行爲特性」概念改變情形(續)

行爲特性		實驗組1		實驗組2		控制組	
概念	題號	前測 答對率	後測 答對率	前測 答對率	後測 答對率	前測 答對率	後測 答對率
主動攻擊性	13	25.00%	56.25%*	25.81%	27.59%	23.33%	21.88%
	14	56.25%	65.63%	58.06%	72.41%	53.33%	56.25%
不可預知性	15	68.75%	75.00%	70.97%	65.52%	53.33%	81.25%*
	16	15.63%	62.50%*	9.68%	13.79%	13.33%	18.75%
	17	53.13%	81.25%*	58.06%	72.41%	40.00%	43.75%
潛伏性	18	75.00%	84.38%	45.16%	48.28%	33.33%	56.25%
	19	46.88%	62.50%*	54.84%	41.38%	36.67%	40.63%
破壞性	20	90.63%	90.63%	80.65%	72.41%	63.33%	75.00%
	21	37.50%	68.75%*	22.58%	44.83%*	26.67%	31.25%
	22	90.63%	90.63%	70.97%	72.41%	86.67%	75.00%
	23	9.38%	9.38%	25.81%	17.24%	20.00%	21.88%
類比爲生物性病毒	24	68.75%	75.00%	32.26%	37.93%	36.67%	31.25%
	25	75.00%	84.38%	61.29%	51.72%	53.33%	53.13%

*爲該題目後測成績高於前測20%以上

在「未授權性」概念中的第2及第3題，實驗組1與實驗組2皆成長了20%以上，代表在經過教學後，兩組學童都能提昇電腦病毒的概念，而控制組同學在這項目中仍然沒有成長，這代表只要有教學，學童便能澄清概念。

在「傳染性」概念中的第5題，經過教學處理，實驗組1與實驗組2學童已具有MP3隨身碟也是傳染媒介的概念，而未接受教學的控制組，仍有47%的學生不知道MP3隨身碟可以傳播病毒；研究者在此重述，在實驗組2的傳染媒介教材中，原本並無MP3隨身碟項目，此爲學生於課堂中舉手發問，教師才針對隨身碟進行補充說明，由此結果可知，只要有教學，學生便能有效釐清此迷思。

在「傳染性」概念中的第8題，經過教學處理，實驗組1與實驗組2都能了解系統漏洞也是傳染媒介的概念，而未接受教學的控制組，前測答對率爲76.67%，後測成績則下降爲65.63%，代表學生若未接受概念澄清，對於原本的認知會產生迷思概念中的不完備性，做出前後不一致的推論。

在「傳染性」概念的第7題，實驗組1在教學後提高了約37%，代表學童能了解正版軟體、免費軟體以及防毒軟體程式都可能受到病毒感染；而

實驗組2與控制組多數學童仍認爲防毒軟體不會受到病毒感染，實驗組2因教材中並未呈現軟體使用的安全面因此學童仍舊無法澄清其迷思概念。

在「傳染性」概念的第6題，三組學童的答對率皆下降，研究者發現下降的原因爲學童認爲病毒是寄生在網路線上傳遞的，就其原因爲研究者進行教學時，都有提到網路爲目前病毒傳播最大的媒介，因此有些學童則在教學過程中產生迷思概念，也就是在概念形成的歷程中產生錯誤的連結，而做出前後不一致的推論。

在「觸發性」概念中，多數學童仍維持舊有的概念，實驗組1與實驗組2在教學後並沒有提升此部分的概念；究其原因爲實驗組1教材中雖有教導觸發性的時機，但卻未教導防範病毒觸發的策略，而實驗組2則未提及觸發性的概念，因此皆無法有效澄清學童概念的狀況。

在「持久性」的部份，三組學童在第11題的答對率都有進步，代表學童在經過教學後以及在自然環境中都能成長。但在第12題中，僅有實驗組1同學的答對率提升，其他兩組答對率則有下降的趨勢，研究者分析，電腦病毒推廣教材中並未提出區域網路與持久性的關係，因此無法澄清學童的迷思。

在「主動攻擊性」的第13題中，僅有實驗組1學生對於e-mail病毒的攻擊行爲概念有提升的現象，其餘兩組則與前測維持一致的想法。研究者分析，仍有部份實驗組1的學生無法在此題中正確作答，可能爲研究者在教學時，僅說明e-mail病毒的攻擊行爲與方法，但卻未提出防範的措施，因此無法澄清更多學童的概念。而在電腦病毒教學推廣教材中，則無分析e-mail的攻擊行爲，因此學童的反應仍與前測維持一致性的表現。

在「主動攻擊性」的第14題中，實驗組1與實驗組2都有近10%的成長率，推究原因可能爲教材中都有呈現電腦病毒常用的傳播媒介，因此也能澄清主動攻擊性中的某些傳播媒介攻擊的概念，而未接受教學的控制組在此概念中則與前測維持一致的看法。

在「不可預知性」的第15題中，未受教學的控制組有20%以上的成長率，代表學童在測驗後能由教學以外的經驗習得正確的概念；實驗組1在教學後也可以得到小幅的成長；反觀實驗組2並未接收到變種病毒的概念教學，呈現小幅的退步。

在「不可預知性」的第16題中，僅有實驗組1達到近40%的成長率，本題目的爲考驗學童雙副檔名的僞裝術，與第一大題電腦病毒感染的檔案格式有關，實驗組1透過實際直際執行雙副檔名的檔案，來認識病毒的僞裝術，由成長率可見此教案的可行性；在實驗組2的教材中雖有呈現病毒的僞裝行爲，但並未提出雙副檔名爲e-mail病毒常使用的傳播手法，因此實驗組2的學童無法獲得澄清。

在「不可預知性」的第17題中，也是測驗病毒的僞裝技術，實驗組1有30%的成長，而實驗組2有15%左右的成長，兩組教材都呈現了電腦病毒的僞裝技術，尤其都指出「更新程式」爲病毒常用的技巧，因此能有效澄清學童迷思；反觀未接受教學的控制組則在病毒僞裝技巧上無法有所提升。

在「潛伏性」中，實驗組1與控制組學生都有小幅成長，而實驗組2在第19題的答對率呈現小幅下降，因該組的教材中未提出病毒於潛伏期中的行爲。

在「破壞性」中的第21題，實驗組1與實驗組2學生各有20%以上的學童在接受教學後多數能重新理解電腦重新開機也是病毒的破壞行爲，而控制組學生仍不認爲重開機爲病毒行爲。

在「破壞性」中的第23題，三組學生皆未有成長，並維持相當低的答對率，絕大多數的學童認爲會立即造成電腦無法開機的病毒能夠在短時間內造成大範圍的流傳，這是因爲學童無法整合破壞性與傳染媒介以及潛伏性的概念連結在一起，因此認爲破壞性強的病毒就能造成廣泛的流傳，雖實驗組1的教材中有針對此概念作介紹，但仍無法澄清學童迷思，可見學童在此題具有迷思概念中的頑固性，也可能此概念的傳授不適合此階段學童。

在「類比爲生物性病毒」中，僅有實驗組1在兩題中皆達到成長，而實驗組2與控制組都僅有一題成長，另一題則呈現負成長，可說明實驗組1教材能提升學童在此概念的認知能力，反觀實驗組2的教材並未包涵此概念，因此無法完全澄清學童的迷思。

研究者共歸納出電腦病毒的9個行爲特性，並依此發展實驗教材，但在電腦病毒推廣教材中，並未涵蓋此9個行爲特性，而僅著重於傳染性、破壞性及不可預知性中的僞裝技巧，可能是造成實驗組2與控制組沒有差異的原因。

由上述分析中可得，在行爲特性中的未授權性、傳染性、持久性、主動攻擊性、僞裝技巧、潛伏性、重新開機破壞行爲、類比爲生物性病毒皆可透過教學來澄清學童的迷思；而在持久性、不可預知性、潛伏性三種概念中，未接受教學的學童也能在測驗後有所成長；多數學童普遍不足並具有頑固性的迷思概念爲第23題，因爲學童仍無法將概念互相結合，以至於教學後仍無法獲得澄清，因此教師在此部份可能需要加入更清楚的說明。

四、 電腦病毒概念前後測在「廣義病毒」成績分析

分別以成對樣本t檢定來檢測三組個別在「廣義病毒」成績的提升情況、以單因子共變數分析來檢測組別間的差異，以描述性統計分析各題項的測驗結果，分析如下：

(一) 電腦病毒概念「廣義病毒」前後測成績成對樣本t考驗

在廣義病毒面向的測驗中，共計5題，總分爲5分，採用成對樣本t檢定分別對三組學生進行檢測，分別分析三組學童的前後測成績在此面向中是否有所提升，如表5-2-18。

表 5-3-18 廣義病毒成對樣本 t 檢定

組別		平均數	個數	標準差	t	自由度	顯著性(雙尾)
實驗組 1	前測總分	2.129	31	1.586	-5.338***	30	.000
	後測總分	3.710	31	1.131			
實驗組 2	前測總分	2.037	27	1.192	-1.324	26	.197
	後測總分	2.444	27	1.553			
控制組	前測總分	1.700	30	1.055	-0.656	29	.517
	後測總分	1.867	30	1.074			

*p < .05 **p < .01 ***p < .001

由表5-3-18可知，僅有實驗組1在行爲特性面向的前後測成績達到顯著t=-5.338 (P=.000<.05)，也就是實驗組1在經過實驗教學後能提升在電腦病毒廣義病毒面向上的概念。而其他兩組則未達到顯著，顯示電腦病毒推廣教材無法有效提升學生在廣義病毒面向上的概念，而未接受教學處理的控制組也無法獲得澄清。

(二) 電腦病毒概念「廣義病毒」前後測成績共變數分析

此部份是針對電腦病毒概念測驗試卷中的「廣義病毒」面向做分析，此面向有5題，總計爲5分。

首先爲確認組別與「廣義病毒」前測成績的交互作用可能影響後測結果，因此以「廣義病毒」前測成績爲共變數，「廣義病毒」後測成績爲依變數，進行迴歸同質性考驗，如表5-3-19。

表 5-3-19 三組學生在「廣義病毒」後測成績迴歸同質性考驗摘要表

變異來源	SS	df	MS	F	P
組別*前測(回歸係數同質性)	1.865	2	0.932	0.622	.539
Error(誤差)	122.932	82	1.499		

*p < .05 **p < .01 ***p < .001

由上表可知，F=0.622，p =.539 > .05，滿足迴歸係數同質性檢定的基本假設，各組組內的迴歸線平行，因此可繼續進行共變數分析，如表5-3-20。

表 5-3-20 三組學生在「廣義病毒」後測成績共變數考驗摘要表

變異來源	SS	df	MS	F	P
前測	9.724	1	9.724	6.545**	.012
組別	47.827	2	23.913	16.096***	.000
誤差	124.796	84	1.486		
校正後的總數	188.716	87			

*p < .05 **p < .01 ***p < .001

由表5-3-20中發現前測的確會影響後測的分數(F=6.545，p=.012<.05)，在去除前測的影響後，三組學生在後測上有顯著差異F=16.096，p=.000 < .05，因此以Bonferroni法進行事後比較，才能得知哪幾組樣本在「廣義病毒」的後測上有顯著差異。

表 5-3-21 三組學生在「廣義病毒」後測成績事後比較表

組別		平均數差異	標準誤	顯著性
實驗組1	實驗組2	1.241	0.321	.001**
	控制組	1.732	0.315	.000***
實驗組2	實驗組1	-1.241	0.321	.001**
	控制組	0.49	0.325	.406
控制組	實驗組1	-1.732	0.315	.000***
	實驗組2	-0.49	0.325	.406

*p < .05 **p < .01 ***p < .001

表 5-3-22 三組「廣義病毒」後測的原始平均數與調整後平均數

組別	平均數	標準差	調整後平均數	標準誤
實驗組1	3.710	1.131	3.664	0.220
實驗組2	2.444	1.553	2.423	0.235
控制組	1.867	1.074	1.933	0.224

在事後比較的表5-3-21中呈現，實驗組1對其他兩組在「廣義病毒」後測的成績上有顯著差異，也可由表5-3-22可知，實驗組1調整後的後測平均數爲3.664，明顯優於其他兩組調整後的後測平均數(分別爲2.423與1.933)，這表示實驗組1所採用的教材能提升電腦病毒「廣義病毒」面向的概念；但在後測成績上，接受電腦病毒推廣教材教學後的實驗組2與未受實驗處理的控制組，兩者並無顯著差異，這表示實驗組2的教材無法有效提升學童在電腦病毒「廣義病毒」的概念。

(三) 電腦病毒「廣義病毒」概念改變情形

表 5-3-23 實驗組與控制組「廣義病毒」概念改變情形

廣義病毒		實驗組		控制組1		控制組2	
概念	題號	前測答對率	後測答對率	前測答對率	後測答對率	前測答對率	後測答對率
綜合	26	40.63%	68.75%*	45.16%	37.93%	40.00%	15.63%
蠕蟲	27	31.25%	59.38%*	45.16%	41.38%	40.00%	59.38%
木馬	28	40.63%	56.25%	12.90%	41.38%*	16.67%	31.25%
謠言信	29	50.00%	90.63%*	45.16%	62.07%	36.67%	43.75%
	30	50.00%	93.75%*	35.48%	55.17%*	36.67%	37.50%

*爲該題目後測成績高於前測20%以上

在「綜合」中所指的是對電腦病毒、電腦蠕蟲以及特洛伊木馬間的異同，這裡可看出實驗組1的學童能區分三者間的異同，而實驗組2與控制組學童的後測成績皆低於前測成績，研究者所定義的廣義病毒爲蠕蟲、木馬以及謠言信，而在電腦病毒推廣教材中也有相同的教材，都充分呈現了蠕蟲、木馬的傳播行爲以及與病毒主要的差異（即僅有病毒會感染檔案），兩者教學內容的差異在於電腦病毒推廣教材中未呈現三者間的相同處，因此無法在此題項正確作答，而未接受教學的學童也無法在自然環境中獲得此概念的澄清。

在「電腦蠕蟲」中，實驗組1與控制組學童能提升20%的答對率，又以實驗組1成長率最高，代表接受教學更能澄清迷思；但實驗組2學童的答對率卻有下降的趨勢，研究者分析電腦病毒推廣課程，其蠕蟲項目的概念亦呈現的相當完整，推論可能爲教學過程中所導致的迷失概念。

在「特洛伊木馬」中，三組學童的答對率皆有成長，代表學童能經由教學以及在自然環境中獲得概念的澄清，但經由實驗組2的教學後成長率爲三者最高，因此代表透過教學能讓更多學童澄清其迷思。

在「謠言信」中，三組學童的答對率皆有成長，但實驗組1與實驗組2成長率皆高於控制組學童，實驗組1成長率又高於實驗組2，因此可推論接受謠言信概念改變之教學更可以釐清學童的迷思。

綜合上述所言，電腦病毒推廣教材未歸納出廣義病毒的相似處以及缺乏互動的教材，是造成實驗組2與控制組沒有差異的可能原因。

五、 電腦病毒概念前後測在「防毒策略」成績比較

分別以成對樣本t檢定來檢測三組個別在「防毒策略」成績的提升情況、以單因子共變數分析來檢測組別間的差異，以描述性統計分析各題項的測驗結果，分析如下：

(一) 電腦病毒概念「防毒策略」前後測成績成對樣本t考驗

在廣義病毒面向的測驗中，共計8題，總分爲8分，採用成對樣本t檢定分別對三組學生進行檢測，分別分析三組學童的前後測成績在此面向中是否有所提升。

表 5-3-24 防毒策略成對樣本 t 檢定

組別		平均數	個數	標準差	t	自由度	顯著性(雙尾)
實驗組 1	前測總分	4.5161	31	1.2348	-3.524**	30	.001
	後測總分	5.6452	31	1.907			
實驗組 2	前測總分	3.8148	27	1.6417	-2.311*	26	.029
	後測總分	4.6667	27	1.7321			
控制組	前測總分	3.3667	30	1.2726	-2.276*	29	.030
	後測總分	4.0667	30	1.5298			

*p < .05 **p < .01 ***p < .001

在表5-3-24可得，三組學童在防毒策略面向的前後測成績表現上皆達顯著差異，實驗組1與實驗組2在接受教學後都能提升電腦病毒概念；然而未接受實驗教學的控制組在經過三個禮拜的時間後也能有所成長，正如研究

者在測驗總分中所設的推論，學童可能因透過團體討論、親身經驗以及在測驗後提高對病毒的關注，能有效釐清一些概念，或是出現「強亨利效應」，因此其成長能表現在防毒策略的成績上。

(二) 電腦病毒概念「防毒策略」前後測成績共變數分析

此部份是針對電腦病毒概念測驗試卷中的「防毒策略」面向做分析，此面向有8題，總計爲8分。

首先爲確認組別與「防毒策略」前測成績的交互作用可能影響後測結果，因此以「防毒策略」前測成績爲共變數，「防毒策略」後測成績爲依變數，進行迴歸同質性考驗，如表5-3-25。

表 5-3-25 三組學生在「防毒策略」後測成績迴歸同質性考驗摘要表

變異來源	SS	df	MS	F	P
組別*前測 (回歸係數同質性)	2.692	2	1.346	0.501	0.608
Error(誤差)	220.179	82	2.685		

由上表可知，F=0.501，p =.608 > .05，滿足迴歸係數同質性檢定的基本假設，各組組內的迴歸線平行，因此可繼續進行共變數分析，如表5-3-26。

表 5-3-26 三組學生在「防毒策略」後測成績共變數考驗摘要表

變異來源	SS	df	MS	F	P
前測	32.092	1	32.092	12.095**	.001
組別	15.784	2	7.892	2.974	.056
誤差	222.871	84	2.653		
校正後的總數	293.716	87			

*p < .05　**p < .01　***p < .001

由表5-3-26發現前測的確會影響後測的分數(F=12.095，p=.001<.05)，在去除前測的影響後，三組學生在後測上未達顯著差異F=2.974，p=.056 > .05，代表三組學童在「防毒策略」的成就上沒有差異，從表5-3-24中可得三組間沒有差異的原因是三組在此概念中皆有顯著成長。

(三) 電腦病毒「防毒策略」概念改變情形

表 5-3-27 防毒策略概念改變情形

防毒策略		實驗組1		實驗組2		控制組	
概念	題號	前測答對率	後測答對率	前測答對率	後測答對率	前測答對率	後測答對率
個人防治	31	81.25%	68.75%	61.29%	58.62%	60.00%	71.88%
	32	56.25%	75.00%	38.71%	48.28%	40.00%	53.13%
	33	75.00%	90.63%	45.16%	68.97%	56.67%	56.25%
防毒軟體使用	34	65.63%	75.00%	58.06%	72.41%	36.67%	53.13%
	35	21.88%	59.38%*	29.03%	44.83%	26.67%	28.13%
	36-1	56.25%	62.50%	51.61%	58.62%	36.67%	53.13%
	36-2	75.00%	65.63%	61.29%	72.41%	73.33%	75.00%
	36-3	21.88%	59.38%*	22.58%	34.48%	6.67%	15.63%

*爲該題目後測成績高於前測20%以上

在個人防治第31題，實驗組1與實驗組2的答對率皆下降，研究者分析在此兩者的教學內容中皆提到備份的重要性，但教材中教導的備份時機爲隨時執行，推論學生則在教與學的過程中引發迷思概念，反觀控制組則能在自然環境中澄清迷思概念。

在個人防治第32題，三組學童答對率皆有提升，而以實驗組1的教學提升比率最高；因此可推論雖然學生能自然成長，但透過教學則可讓更多學童產生正確的概念。

在個人防治第33題，實驗1組與控制組皆能提升，以實驗組1教學提升比率最高；因此可推論雖然學生能自然成長，但透過教學則可讓更多學童產生正確的概念。

在防毒軟體使用方法中的五個題項中，三組學童皆有成長，代表學童接受教學與自然成長都可讓學童產生正向的觀念，而接受實驗教學的學童其成長比率比自然成長的學童高，因此代表接受教學更能獲得迷思概念的澄清。但實驗組1在第36-2的題號中，答對率有降低的現象，研究者分析可能爲研究者演示防毒軟體的病毒隔離功能後，接續演示回復隔離區中的病毒檔案，而使學童誤以爲隔離區即爲資源回收筒所致；以及在實驗組1教材中雖然都涵蓋了個人防毒與防毒軟體使用的部份，但學習單中卻沒有規劃

防毒軟體使用的注意事項，爲教材上的缺失。

而在電腦病毒推廣教材中並未歸納出防毒軟體使用的概念，因此也無法更提升防毒策略的概念。

綜合上述所言，在防毒策略面向中三組學童皆有成長，但仍以接受教學的學童成長幅度較高，因此教學或許能釐清較多學童的迷思概念。

第六章 結論與建議

本研究對國小六年級學童的電腦病毒迷思概念進行分析，並以系統化教學設計模式研擬出一套電腦病毒概念改變課程，進而能澄清學童的迷思概念。本研究的研究結論將依循第一章的研究假設項目來說明資料分析的結果，並根據研究過程曾面臨的問題提出研究的限制與建議。

第一節 研究結論

本研究結論將說明國小六年級具有哪些電腦病毒迷思概念，並探討不同變項(性別、是否有電腦病毒經驗、每天平均上網時數以及學校教師是否曾教授過電腦病毒知識)是否會造成學童電腦病毒概念成就的差異，也分析在教學實驗後，學童的電腦病毒迷思概念提升情形。

一、 國小六年級學童多數有電腦病毒迷思概念

研究者依據電腦病毒的四個面向，分別爲基本原則、行爲特性、廣義病毒以及防毒策略進行說明。

(一) 基本原則：

學童對於電腦病毒種類以及檔案格式之間的關係缺乏概念，在 94 名學童中，僅有 2.15%的學童能完全釐清四種病毒種類感染目標的差異。而 29.03%的學童則認爲電腦病毒在執行前時，必需取得使用者的允許才能開啓。

(二) 行爲特性：

本面向共有九個子概念，以下將分別說明：

1. 未授權性：僅有 22.58%的學童能正確回答出電腦病毒在入侵時通常不會有顯著行爲以及電腦病毒不須取得使用者同意就可進入電腦，這代表多數的學童仍具有電腦病毒必須取得使用者同意才能植入電腦的迷思概念。

2. 傳染性：僅有 16.13%的學童能完全了解電腦病毒的傳染途徑，多數學童缺乏的概念是不知道隨身碟以及系統漏洞也是傳染媒介之一。且學童認爲正版軟體與防毒軟體不會被感染電腦病毒，而盜版及免費的軟體一定含有病毒。

3. 觸發性：此概念有 69.89%的學童能完全了解觸發性的特性，錯誤作答的學童多數具有只要調整系統日期就可避免病毒觸發的迷思概念。

4. 持久性：此概念有 44.09%的學童能理解持久性的意義，多數學童仍認爲電腦病毒在流行期過後就會消失以及區域網路中毒後，只要清除教師電腦裡的病毒，其餘電腦就可以一同被清除掉。

5. 主動攻擊性：僅有 17.20%的學童有完整的主動攻擊概念，多數學童具有的迷思概念爲不曉得以電子郵件爲傳播媒介的病毒會在背景大量發信的，以及也有學童認爲就算連上網路，只要不使用網路功能如開啓網頁或收發電子郵件就不會被感染。

6. 不可預測性：此面向考驗學童是否了解電腦病毒的僞裝技巧，僅有 3.23%的學童能做出正確判斷，多數學童認爲防毒軟體只要有原始病毒的病毒定義檔就可以偵測到變種病毒，並認爲曾經感染過原始病毒就不會感染變種病毒，這是衍生性的迷思概念。另，學童認爲微軟或防毒軟體寄發的更新檔程式必須盡快執行，卻不明白這是常見的僞裝技巧；在此概念中也測出學童對於雙副檔名具有普遍性的迷思概念，僅有 12.90%的學童能辨認病毒常用的雙副檔名僞裝技巧。

7. 潛伏性：在此概念中，多數學童認爲病毒會在潛伏期不斷的重覆感染檔案，使病毒程式比例變大，病毒更能夠執行。

8. 破壞性：在此概念中，全對人數僅有 1.08%，多數學童認爲重新開機的問題並非病毒產生行爲，而是硬體本身的問題。另外有更多學童具有一個普遍的迷思概念，認爲會立即造成電腦無法開機的病毒能夠造成大範圍的傳染，這是學童無法利用破壞性與潛伏性及傳染性相互結合作出正確的推論。

9. 類比爲生物性病毒：多數學童認爲電腦像人體一樣，一旦染了病毒，就會變的更虛弱，而招致更多病毒；另有學童認爲髒污的光碟片在讀取時會感染病毒；而也有另一批學童認爲在區域網路中，只要將電腦遠離感染電腦病毒的電腦就可以避免傳染，這些都是學童以人類生物性病毒的經驗對電腦病毒所做出的錯誤推論。

(三) 廣義病毒：

在此面向中僅有 3.23%的學童具有完整的電腦病毒、電腦蠕蟲、特洛依木馬與謠言信正確概念，其它同學則無法判別病毒、蠕蟲與木馬間的異同處；而多數學童在謠言信的處理上則會遵從信件的指示進而刪除檔案或轉寄更多人，落入謠言信的圈套中。

(四) 防毒策略：

在此面向中多數學童缺乏設計安全密碼的原則概念，並認爲電腦中毒就必須重新安裝作業系統，以及認爲安裝防毒軟體就可以對電腦達到完全的防衛；而在防毒軟體的使用上，學童也缺乏掃解毒模式的概念。

二、 男學童與有電腦病毒經驗的學童其電腦病毒概念成就測驗較高

本研究發現性別變項在廣義病毒的測驗結果爲男生優於女生，推論原因可能爲男生對電腦的了解、操作能力及興趣高於女生(王照馥，2003)；而曾經感染過病毒的學童，則在行爲特性與防毒策略的分數上優於未感染過病毒的學童，代表實際接觸過病毒的學童有較好的電腦病毒概念，與梁雅琇、張義斌、鄭承昌(2006)的研究相同，此發現有利於教師在製作教材時加入讓學童體驗病毒的活動，並多注意女生的學習情況，輔助其在電腦上的操作。

另外，每天平均上網時數以及學校教師是否曾教授電腦病毒的變項並不會影響學童在電腦病毒概念成就上的差異，由此可說明學童普遍缺乏電腦病毒的概念。

三、 學童在教學後多能提升電腦病毒的概念

此部份在學童接受教學實驗後，依據其後測的答題狀況來分析教材的成效，評析何種教材較能提升學童的電腦病毒概念，分別從總成績、基本原則分數、行爲特性分數、廣義病毒分數以及防毒策略分數來說明。

(一) 總成績：從總成績來看，施以電腦病毒概念改變課程的實驗組 1 在電腦病毒概念的成就上優於其他兩組，雖然其他兩組在教學後也都能獲得概念的提升，但進步幅度較小。

(二) 基本原則分數：在此面向中，實驗組 1 在電腦病毒概念的成就上仍優於其他兩組，實驗組 1 學童對於電腦病毒種類與檔案格式間的關係都能達到 25%的成長率。而自行執行的概念也能有 12%的成長率。

(三) 行爲特性分數：在此面向中，實驗組 1 在電腦病毒概念的成就上仍優於其他兩組，學童對於九個子概念都能獲得澄清；但經過教學後，反而造成更多學童認爲病毒是寄生在網路線上傳遞的迷思概念，可了解迷思概念可能會在教學的過程中形成。且學童對於立即造成電腦無法開機之病毒，仍認爲會造成廣泛性的流傳，這爲迷思概念特性中的頑固性。

(四) 廣義病毒分數：在此面向中，實驗組 1 在電腦病毒概念的成就上仍優於其他兩組，學童在經過教學後對於電腦病毒、電腦蠕蟲、特洛依木馬與謠言信都能做出正確的判別與處理，成長率達到 20%以上。

(五) 防毒策略分數：在此面向中三組學童未達顯著差異，這是因爲三組學童在此面向的成就皆有顯著成長；但有教學實驗的組別其成長率高於未接受教學的組別。但實驗組 1 與實驗組 2 在經由教學後，學童對於備份的概念與防毒軟體隔離處理的概念則呈現負成長，此爲教與學的過程中迷思概念的形成。

綜合上述結果，接受「電腦病毒概念改變課程」的實驗組 1 進步情形在總成績以及四個電腦病毒的面向上顯著優於其他兩組；而實驗組 2 在教學後，也能澄清部份迷思概念；雖然控制組也有所成長，但成效低於接受教學的兩組實驗組；因此可推論有教學就能提升學童的認知能力，而本研究使用

系統化教學設計所分析與設計的教材，在教學後則更能有效澄清學童的迷思概念。

第二節　研究建議

研究者針對研究結果提出下列研究建議，提供給未來相關領域的研究者做爲參考資料：

一、 修正易引發學童迷思概念的教學內容

研究者在教學實驗結束後，發現由研究者自編之電腦病毒概念課程的一些教學內容無法澄清學童的迷思概念，或在教學過程中容易使學童產生迷思概念，檢討課程後，研究者針對問題提出建議與修正方案，如下：

(一)　在「傳染性」面向上：

學童在教學後誤認爲病毒是寄生在網路線上傳遞的，究其原因可能爲教學過程中，研究者多提及網路爲目前電腦病毒傳遞的主要媒介所致。

研究者建議，在教授此概念時，複習電腦病毒的「自我複製」原則，讓同學重新喚起電腦病毒是寄生在不同檔案格式上的惡意程式；並補充說明網路只是傳輸檔案的媒介，病毒不會感染網路線的概念。

(二)　在「觸發性」面向上：

有些學童仍認爲避免病毒觸發的方法是調整系統時間；研究者分析教材中有說明觸發性的時機，也讓學生執行觸發性的程式，但卻未教導防範病毒觸發的策略，因此學生無法做出正確的判斷。

研究者建議，在此觸發性概念的教學活動結束後，要加以說明一旦知悉病毒的觸發時機，要避免病毒觸發，最好的方法爲在觸發時間前更新防毒軟體的電腦病毒定義檔進行掃毒。

(三)　在「主動攻擊性」面向上：

在教學後，仍有多數學童認爲電腦感染了以 e-mail 爲傳播媒介的病毒，其處理方法爲發信警告好友勿開啓以學童爲寄件者的電子郵件。這是學童缺乏電腦病毒會僞裝寄件者名稱以及會在系統背景自動發信的能力，因此若學童仍上網發信，則會讓病毒在度流傳。

研究者分析教材中僅說明 e-mail 病毒的攻擊行爲與方式，卻未提出防範的措施。因此研究者建議，在教授「主動攻擊性」的概念後，要說明一旦發現感染了病毒，首先進行的處理行爲是拔除網路線，或停止網路功能，而這個防治的概念，也可以在防毒策略中再次加以提醒。

(四)　在「破壞性」面向上：

絕大多數的學童仍具有立即造成電腦無法開機的病毒能夠在短時間內造成大範圍流傳的迷思。研究者分析，雖在教材中有教授此概念，但仍無法釐清學童的概念，因此宜改變此概念的教學策略；也有可能這樣的概念對此階段的學童較難，不適合在此階段教授。

若要在此階段進行概念教授，研究者建議，不宜以教師講述爲主，而是利用「潛伏性」與「傳染性」的特性引導學童獲得正確的觀念，步驟爲：

1. 提問：請小朋友想一想，潛伏性愈長的病毒，感染的檔案會愈多還是愈少啊？(答案是愈多)
2. 提問：請小朋友想一想，傳染能力愈強(例如電子郵件、系統漏洞)，代表病毒能傳播到的範圍大還是小啊？(答案是大)
3. 整合：所以說，潛伏期很長而且傳染能力很強的病毒，一旦觸發時間到了，就會造成很多電腦被破壞。
4. 提問：最後小朋友再想一想，如果潛伏期很短(也就是電腦被感染後很快就被發現或是馬上不能開機)，那會不會有很多電腦被感染？(答案是不會)

研究者認爲，透過提問的方法，讓學童自行推論出答案的方式，或許可澄清學童的迷思概念。

(五)　在「個人防治」面向上：

學生在接受教學後，雖然了解備份的重要性，卻誤解備份的時機。研究者分析教材，認爲教材中的說明已很詳細，因此不需改變教學內容，但建議利用學習單讓學生透過練習，來了解備份是隨時隨地必須進行的。

(六)　在「防毒軟體使用」面向上：

在教師演示防毒軟體的隔離處理模式後，學生誤以爲隔離區即爲資源回收筒。研究者建議，在執行隔離模式後，開啓資源回收筒讓學生了解病毒不會被置於此；接下來才演示從隔離區回覆病毒檔案的模式。

二、 將電腦病毒融合於其他科目或相關的電腦課程中

研究者認爲若將電腦病毒獨立爲某學期中的課程，可能會因概念過多，且學童無法一次吸收所有訊息，而無法有較好的成效，建議可將電腦病毒的概念融合在各種電腦課程中甚或其他非資訊的課程裡，例如在教授電腦基本概念時可融入檔案格式的概念；在文書處理課程時可說明巨集病毒的相關資訊，在網頁課程時可說明描述語言病毒的相關資訊，在教授電子郵件的使用時可融入病毒的主動攻擊性與病毒常用的僞裝技巧，如雙副檔名的概念可融入檔案格式的教學中，也可電腦病毒融入一般性的課程中，而非獨立的一環。

三、 在課程中加入遊戲並提供學童實際的電腦病毒經驗

若教師有充分的時間，可在電腦病毒課程中加入活動，而非以講述爲主，可帶入提問或建構式的教學法，或以遊戲整合電腦病毒概念，在本次的教學因受限於時間，研究者取消了廣義病毒中的「病毒蹲」遊戲，利用角色扮演讓學童分別扮演病毒、蠕蟲、木馬，由教師說出某一惡意程式的特性，符合此特性的角色即蹲下，因爲研究者取消活動，所以也未能得知活動是否適宜。

另，在防毒策略中，原本要教授更多檢查病毒的方法，但也因時間限制被迫停止，實爲可惜之處，因爲在研究中即顯示了，曾經感染過病毒的學童其概念成就較好的訊息，若能讓學童多接觸病毒，推論可提升成效。

四、 缺乏教學經驗的研究者可利用教學錄影作為省思的紀錄

建議較缺乏經驗的教師可以在上課時錄影，教學後可以觀看以利檢討與改進，提高教學成效；在本研究中，因僅有研究者一人掌控教學，因此無法處理錄影事宜，因此僅能利用省思筆記紀錄教學過程中的問題，無法審視實際的教學過程。

第三節　研究限制

在研究的過程中，可能因時間、地域與教學者本身的經驗而影響了研究結果，本研究之研究限制說明如下：

一、 本研究僅施測於台東市某國小之六年級學童，研究中所歸納出的電腦病毒迷思概念項目是否可推測於其他地區之國小或其餘年級學童則待商榷。

二、 研究發現有些電腦病毒概念在教學後仍無法獲得澄清，這些迷思概念分別爲學童認爲電腦病毒是寄生在網路線上進行傳播的、防治電腦病毒觸發最好的方法是調整系統時間、電子郵件病毒可於系統背景下自動發信、立即造成無法正常開機的電腦病毒傳播範圍廣、重要資料備份只要在每年年底執行即可、以及認爲防毒軟體的隔離區即爲系統的資源回收筒上，是否爲教材過於困難，仍待驗證，也期望未來對此主題有興趣的研究者繼續探討，若呈現共同現象則更可描繪出國小階段所應學習的電腦病毒概念範圍，有助於未來資訊安全教育的推展。

三、 研究者並非班級或學校教師，在教學上的經驗仍顯不足，可能無法將教材內的完整概念傳達給學童。

四、 爲避免打擾班級老師的正常上課時間，多利用早自習時間施行教學實驗，因此在教學時間上會因學童到校時間而有延誤等問題，且學習單的撰寫必須利用下課時間完成，時間短促造成學習者無法充分思考後填答，學習單內容也未涵蓋該單元的所有概念，可能造成學習成效的問題。

五、 研究者自編之電腦病毒概念課程所含括的概念相當多，但爲了讓實驗組與傳統組在教學時數上相同，會使課程上起來較爲急促，有時必須拿掉一些教學活動而改爲講述，也都是影響學習成效的可能因素。


NTTU Library

參考文獻

一、中文部份

小無限編輯部 (2005a)。**Internet 網路探險隊**。台北：無限可能創意。

小無限編輯部 (2005b)。**Internet 遊樂園**。台北：無限可能創意。

小無限編輯部 (2006c)。**Wondows 電腦探險隊**。台北：無限可能創意。

中華民國資訊統計網 (2005)。**資訊安全整體概況**。檢索日期：2006.11.18。取自 http://www1.stat.gov.tw/public/Attachment/69718185871.doc。

中國視聽教育學會 (1988)。**系統化教學設計**。台北：師大書苑。

尹玫君 (2004)。國小學生資訊倫理態度和行爲的探討。**南大學報，38**(2)，1-21。

王文科、王志宏 (2006)。**教育研究法**。台北：五南。

王美芬 (1991)。自然科錯誤概念之研究。**台北市立師範學院學報，22**，367-400。

王美芬 (1992)。我國五、六年級學生有關月亮錯誤概念的診斷及補救教學策略的應用。**台北市立師範學院學報，23**，357-380。

王炳麒 (2004)。**電腦基礎與 Windows98**。台北：立威。

王照馥 (2004)。**大學生科技態度與網路書店購物行爲之相關性研究**。南華大學出版事業研究所碩士論文。

余民寧 (1995)。**成就測驗的編制原理**。台北：心理。

李宗薇 (1991)。**教學媒體與教育工學**。台北：師大書苑。

李宗薇 (1999)。**教學設計理論與模式的評析及應用：以師院社會科教材教法爲例。**國立臺灣師範大學教育學系博士論文。

李進寶 (1990)。電腦病毒發展史。**資訊與教育，10**，1-3。

杜德煒、杜經文 (1985)。**IBM 個人電腦入門**。臺北市：三民書局。

汪富明 (1998)。國小資訊教育的教材教法。**資訊與教育，64，**45-52。

林月芳 (2004)。**資訊融入教學以提昇國小學童天文學習效能之研究-以「月亮」單元爲例**。屏東師範學院數理教育研究所碩士論文。

林世宗 (2004)。**以迷思概念爲基礎之電腦輔助教材開發—以國中聲音課程爲例**。國立台北師範學院教育傳播與科技研究所碩士論文。

林佳旺 (2003)。**國小網路素養課程系統化教學之行動研究—「以六年級網路互動安全課程」爲例**。國立嘉義大學教育科技研究所碩士論文。

吳怡貞 (2006)。**國小學童網路素養課程之系統化教學設計研究**。國立臺北教育大學國民教育學系碩士班碩士論文。

林珊如、劉旨峰、袁賢銘 (2001)。技術學院資訊相關科系學生的電腦病毒之迷思概念研究。**資訊與教育，86**，51-61。

林修遠 (2003)。**電腦病毒於 3D 電腦動畫視覺化之研究**。私立中原大學商業設計研究所碩士論文。

林清山譯 (1992)。Richard E. Mayer 原著。**教育心理學一認知取向**。台北：遠流。

林淑芬，陳泌鍇 (1997)。由電腦犯罪談電腦倫理。**資訊與教育，59**，48-53。

林順喜 (1993)。新一代的個人電腦作業系統-WINDOWS。**資訊與教育，33**，19-21。

邵瑞珍、皮連生 (1993)。**教育心理學**。台北：五南。

金帥 (2006)。病毒資訊。檢索日期：2006.11.04。取自 http://www.ggreat.com.tw。

侯雪卿 (2004)。**國小高年級學童圓概念教學模組補救教學之個案研究**。國立嘉義大學國民教育研究所碩士論文。

洪素敏 (2003)。**國小五年級學童分數迷思概念補救教學之研究**。國立嘉義大學數學教育研究所碩士論文。

徐新逸 (2003)。數位學習課程發展模式初探。**教育研究月刊，116**，15-30。

徐盟霖 (2004)。**Internet 網路 123**。台北：巨岩。

徐廣寅 (2004)。**資訊安全管理導論**。台北：金禾。

高大宇、王旭正 (2003)。**資訊安全**。台北：博碩。

許玉霞(2006)。**國小學童網路使用現況及網路素養之研究-以臺北縣偏遠地區高年級學童爲例**。臺北市立教育大學教育行政與評鑑研究所碩士論文。

教育部 (2001)。**中小學資訊教育總藍圖**。檢索日期 2006.10.22。取自 http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU7892001/information/itpo/itprojects/itmasterplan.htm。

教育部 (2003)。**國民小學九年一貫課程綱要重大議題**。台北：教育部。

張春興 (1996)。**教育心理學—三化取向的理論與實踐**。台北：台灣東華。

張新仁 (2003)。**學習與教學新趨勢**。台北：心理。

張淑萍 (2006)。**當教學設計遇上 e-Learning**。檢索日期：2007.01.07。取自 http://www.elearn.org.tw/NR/exeres/02A76568-7FD1-4BEB-8F8A-FDEC84DF337C.htm。

梁雅琇、張義斌、鄭承昌 (2006)。電腦病毒迷思概念。發表於**台灣教育傳播暨科技學會 2006 研討會。**台灣教育傳播紀科技學會主辦。2006.12.16。台北市：台灣師範大學。

郭耀煌 (2006)。**國內教育環境的資安挑戰與對策**[投影片]。2006 iSecuTech 台北國際資訊安全論壇。

陳正昌譯 (1996)。Garné, R.M. Briggs, L. J. Wager, W. W.原著。**教學原理設計 (Principles of Instructional Design)**(初版)。台北：五南。

陳明舜 (1996)。**電腦病毒對高中職資訊教學影響之研究**。國立高雄師範大學工業科技教育研究所碩士論文。

陳清芳、趨勢科技紅色警戒小組 (2002)。**電腦病毒紅皮書**。台北：趨勢網路軟體教育基金會。

陳豐偉 (2001)。**網路不斷革命論**。台北：商業周刊。

程秉輝 (2004)。**防毒妨駭全攻略**。台北：旗標。

黃文杰 (2000)。**DIY 2001 電腦中毒急救箱**。台北：文魁。

黃文鈺 (2005)。**Internet 網路漫遊我最拿手**。台北：文魁。

黃正傑 (2000)。**電腦網路原理與應用**。台北：全華科技。

黃明仁 (1993)。**揭開電腦病毒的面紗**。高雄縣：正點資訊。

黃銘祥、張季珠、廖立茹 (2001)。**電腦病毒事典書**。台北：商翼資訊。

陳大任、黃賢麟譯 (2002)。Robert Slade, David Harley, Urs E.Gattiker 著。**病毒聖經**。台北：美商麥格羅・希爾。

微軟 (2006)。**微軟 1995 年新聞**。檢索日期：2006.07.21。取自 http://www.microsoft.com/china/press/1995/08/0831.mspx

廖斌毅、潘正祥、楊正宏、林子傑、劉文勝 (2003)。**探討網路個人行爲在資訊安全下之影響因素**。發表於 TANET2003 台灣網際網路研討會。國立政治大學主辦。2003.10.29。台北市：政治大學。

熊召弟、王美芬、段曉林、熊同鑫譯 (1996)。Shawn M. Glynn & Russell H. Yeany & Bruce K. Britton 著。**科學學習心理學**。台北：心理。

劉旨峰 (2004)。**資訊素養教育相關研究：大專生對於電腦病毒的認知與態度研究** (行政院國家科學委員會專題研究計畫成果報告，NSC 92-2520-S-008-009)。桃園縣：國立中央大學學習與教學研究所。

劉旨峰、林珊如、袁賢銘 (2002)。**大專生電腦病毒態度問卷之初探性發展：以抽樣北部兩所大專院校資訊相關科系爲例**。2002 數位生活與網際網路科技研討會。國立成功大學主辦。台南：成功大學。

劉景熙、劉建虹 (1994)。**電腦病毒手冊大全**。台北：國立編譯館。

劉順德 (2000)。**以樹狀關聯式架構偵測電子郵件病毒之探討**。國立中央大學資訊管理研究所碩士論文。

鄭昭明 (1997)。**認知心理學**。台北：桂冠

鄭麗玉 (1994)。**認知心理學—理論與應用**。台北：五南。

鄭麗玉 (1998)。如何改變學生的迷思概念。**教育研究，39**(5)，28-36。

賴榮樞 (2005a)。**Windows Server System 系統管理之 Windows Script Host**。檢索日期：2006 年 7 月 21 日，取自 http://www.microsoft.com/taiwan/technet/columns/profwin/tnawsh.mspx

賴榮樞 (2005b)。**剪不斷、理還亂的惡意軟體與間諜軟體**。檢索日期：2006.07.21。取自 http://203.204.73.37/taiwan/technet/columns/profwin/tnamalware.mspx。

蔡名杉 (2004)。**國小月相另有概念改變教學之行動研究。**國立臺南大學教師在職進修自然碩士學位班碩士論文。

謝青龍 (1995)。從「迷思概念」到「另有架構」的概念改變。**科學教育，180**，23-29。

謝淵任 (2004)。**中學生資訊安全課程設計與發展**。國立交通大學教育研究所碩士論文。

鍾聖校 (1994)。對科學教育錯誤概念研究之省思。**教育研究資訊，2**(3)，89-110。

鍾聖校 (1997)。**認知心理學**。台北：心理。

二、西文部份

Alabama, U. O. S. (2001). *Common Misconceptions about Computer Viruses*. Retrieved April 11, 2006, from South Alabama University Web Site: http://www.southalabama.edu/csc/misconceptions.htm

Cathie, L., & Evelyn, S. (2004). *Teaching computer security at a small college*. Retrieved October 29, 2006 , from The ACM Digital Library.

Dick, W., Carey, L., & Carey, J.O. (2005). *The systematic design of instruction*. (6th ed.), Boston: Pearson/Allyn & Bacon.

Dong-Her, S., & Hsiu-Sen, C. (2004). E-mail viruses: how organizations can protect their e-mails. *Online information Review, 28*(5), 356-366.

Ernst & Young (2004a). *Global information security*. Retrieved Oct 22, 2007, from http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf

Ernst & Young (2005b). *Global information security*. Retrieved Oct 29, 2006, from http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf

Fisher, K. M. (1985). A misconception in biology: Amino acids andtranslation. *Journal of Research in Science Teaching, 22*(1), 53-62.

Fred, C. (1984). *Computer Viruses Theory and Experiments*. Retrieved July 12, 2006, from http://www.all.net

Garry, S. (2002). *University of edinburgh computer virus frequently asked questions*. Retrieved April 11, 2006, from http://www.ucs.ed.ac.uk/isd/archpub/edunivfaq.pdf

Hashweh, M. (1988). Descriptive studies of students' conceptions in science. *Journal of Research in Science Teaching, 25*(2), 121-134.

Head, J. (1986). Research into Alternative Frameworks: promise and problems. *Research in Science & Technological Education, 4*(2), 203-211.

Hong Kong Productivity Council (2004). *Information Security Survey 2004*. Retrieved October 22, 2006, from http://citeseer.ist.psu.edu/689966.html.

ICSA. (2004). *Computer virus prevalence survey*. Retrieved April 11, 2006, from http://www.icsalabs.com/icsa/icsahome.php

Ludwig, M. A. (1996). *The little black book of computer viruses*. American Eagle Publications,Inc.

McAfee. (2006). *W16/WinVir.dr*. Retrieved July 10, 2006, from http://vil.nai.com/vil/content/v_111176.htm

Peter, S. (2005). *The art of computer virus research and defense*. Boston: Addison Wesley Professional.

Posner, G. J., Strike, K. A., Hewson, P. W., & Gertzog, W. A. (1982). Accommodation of as scientific conception: toward a theory of conceptual. *Science Education, 66*(2), 211-277.

Rosenberger, R. (1988). *Computer viruses myths. ACM SIGSAC Review, 7*(4), 21-24, from The ACM Digital Library.

Sophos. (2005). *Blaster-B worm author sentenced to 18 months in jail*. Retrieved Jan 11, 2007, from http://www.sophos.com/pressoffice/news/articles/2005/01/va_parsonsentence.html

Sophos. (2006). *A brief history of viruses*. Retrieved July 11, 2006, from http://eebweb.arizona.edu/help/viru_ben.pdf

Spafford, Eugene H. (1997). *One View of A Critical National Need: Support for Information Security Education and Research.* Testimony Before the US House of Representatives Committee on Science. Washington, DC, February 11.

Symantec. (2006a). *Boza*. Retrieved July 10, 2006, from http://www.symantec.com/security_response/writeup.jsp?docid=2000-121913-0709-99&tabid=1

Symantec. (2006b). *What is the difference between viruses, worm, and Trojans*. Retrieved July 10, 2006, from http://www.symantec.com

Yang, A. T. (2001). Computer security and impact on computer science education: Consortium for Computing Sciences in Colleges. *JCSC,16*(4), 233-246.

Zach, S. H. (2001). *Virus Checker*. Retrieved April 11, 2006, from http://library.georgiasouthern.edu/maa_broch/virus.pdf


NTTU Library

附錄一 電腦病毒概念測驗試卷(正式)

_____國小 六年___班 姓名：_____

電腦病毒概念測驗試卷

小朋友你好：

這份試卷是想瞭解目前你對於電腦病毒概念的理解程度。藉由你的回答，我們將可分析目前電腦病毒防治教育仍需要加強哪些部分。請根據你的了解來填答這份試卷，謝謝。

國立台東大學教學科技碩士班
指導教授：鄭承昌 博士
研究生：梁雅琇 敬啓

第一部分 基本資料

填答方法：請在空格內打勾

1. 性別： □男 □女
2. 是否有電腦病毒經驗： □有 □沒有
3. 平均每天上網時數： □1 小時以下 □1-2 小時 □2-3 小時 □3 小時以上
4. 學校老師曾教過電腦病毒知識：□有 □沒有

第二部份 電腦病毒概念測驗

填答說明：

一、本試卷共有 36 題，每一題都有 4 個選項，其中只有一個選項是正確的，請將您的答案填入( )括號中。

( )1. 電腦病毒可分爲四種，分別爲「開機型病毒」、「檔案型病毒」、「巨集病毒」、「描述語言病毒」，請你將這些病毒分別會感染的檔案**連接**起來。

病毒種類		**選項**
開機型病毒	●	● .DOC 與 .XLS (Office 文書檔)
檔案型病毒	●	● .HTML 與 .VBS (網頁程式檔)
巨集病毒哩	●	● .EXE 與 .SCR (可執行檔)
描述語言病毒	●	● 磁碟片 與 硬碟

(　　)2. 電腦病毒進入電腦時，會出現哪種情形？
(1) 螢幕上會出現「是否要執行病毒程式」的訊息。
(2) 電腦通常不會有明顯異狀。
(3) 螢幕會顯示「檔案已複製完成」的訊息。
(4) 電腦主機會發出像「救護車」聲音來警戒。

(　　)3. 下列有關電腦病毒的描述，何者正確？
(1) 電腦病毒在取得使用者同意後，才能進入電腦。
(2) 電腦病毒會不斷發出訊息，讓使用者知道它的存在。
(3) 電腦病毒不需要使用者允許，就能進入電腦。
(4) 電腦病毒在刪除系統檔案時，會產生警告訊息。

(　　)4. 電腦裡的檔案被電腦病毒感染後，開啓被感染的檔案，請問存在檔案裡的病毒：
(1) 會隨著檔案開啓而被執行。
(2) 不會被執行。
(3) 隔幾天才會執行一次 。
(4) 病毒執行前會出現訊息，詢問你是否要執行，點選「是」病毒才會執行。

(　　)5. 電腦病毒<u>不會</u>透過下列哪種方法傳染出去？
(1) Yahoo 即時通。
(2) MP3 隨身碟。
(3) 電子郵件。
(4) 電腦的電源供應線。

(　　)6. 從網路上下載非法軟體會中毒，這是因爲病毒寄生在哪種物體上進行散佈？
(1) 網路線。
(2) 檔案。
(3) 網路卡。
(4) 數據機。

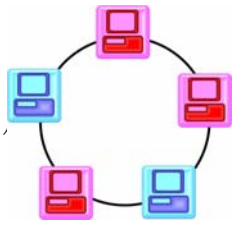
(　　)7. 有關軟體的使用，下列何者敘述正確？
(1) 新買的電腦裡面的軟體不會有電腦病毒。
(2) 使用盜版或免費的軟體，一定會中毒。
(3) 購買正版軟體就能確保不被病毒感染。
(4) 防毒軟體的更新檔案也會被電腦病毒感染。

(　　)8. 哪種狀況下，比較容易讓電腦病毒侵入電腦？
(1) 使用防寫的磁片。
(2) 潮濕且發霉的磁片。
(3) 老舊的網路卡和網路線。

(4) 很久沒做漏洞更新的 Windows XP 作業系統。

( )9. 防毒軟體公司發佈一隻電腦病毒，會在 7 月 7 日當天開始發作破壞檔案，應該如何防範比較好？
(1) 把電腦時間調整成 7 月 8 日，就不會發作。
(2) 7 月 7 日那天都不要開機，隔天再開就不會發作。
(3) 7 月 7 日前先下載病毒更新檔進行掃毒。
(4) 7 月 7 日前把電腦檔案設爲隱藏，電腦病毒就找不到檔案了。

( )10. 有一隻病毒只會在 13 號星期五當天開始刪除檔案，這代表何種意思？
(1) 病毒只會在 13 號星期五侵入電腦，其他時間電腦裡不會有病毒程式。
(2) 電腦隨時會被感染，病毒會存在電腦中，等待 13 號星期五開始破壞。
(3) 病毒只會在今年的十三號星期五內發作，明年就不會發作。
(4) 發作過一次後，下個十三號星期五就不會發作了。



( )11. 電腦病毒在流行期過後會有下列哪一種狀況發生？
(1) 病毒會慢慢的消失不見，不再復發。
(2) 很久以前流行過的病毒，不會在新的作業系統上流
(3) 曾經流行過的病毒，不會再次造成大流行。
(4) 過一陣子病毒可能會再次造成大流行。

( )12. 有一隻病毒在學校電腦教室的網路中流傳，下面何者是正確的呢？
(1) 把老師使用的電腦清除乾淨，其他電腦中的病毒就會一起被清除掉。
(2) 其中一台電腦解完毒後，就不會再中毒了，可以繼續上網。
(3) 清除完病毒後，電腦連上網路，病毒也會再進入。
(4) 病毒只會攻擊電腦教室裡的電腦，所以校長室裡的電腦不會受到侵入。

( )13. 我感染了一隻病毒，會透過電子郵件轉寄病毒程式給 Outlook 通訊錄中的聯絡人，首先應該要如何處理？
(1) 仍可繼續瀏覽網站，但不要使用 Outlook 寄信給朋友。
(2) 盡速拔除網路線來停止網路功能，使病毒無法寄信出去。
(3) 馬上改用線上信箱寄信(如 Yahaoo 免費信箱)，但仍可開啓 Outlook 來收信。
(4) 發信警告好友，不要開啓由我寄出的電子郵件。

( )14. 哪一種情況下，電腦被病毒入侵的機會比較小？
(1) 使用隨身碟讀取檔案。
(2) 閱讀電子郵件。

(3) 我的電腦沒有上網，所以感染病毒的機會比較小。
(4) 雖然有的電腦開機會自動連上網路，但是只要不瀏覽網頁或不收信就不會感染。

(　　)15. 電腦病毒不斷的改變原始病毒程式，來躲避防毒軟體的偵測，稱爲「變種病毒」，下列敘述何者正確？
(1) 只要防毒軟體有原始病毒的病毒碼，就可以攔截到變種病毒。
(2) 感染過原始病毒的電腦，就不會被他的變種病毒感染。
(3) 變種病毒可能會造成更大的流傳與破壞。
(4) 變種病毒的破壞能力比原始病毒小。

(　　)16. Jolin 收到四封含有附加檔案的 E-mail，請問開啓哪一個附加檔案<u>不會</u>中毒？
(1)「好玩遊戲.exe」
(2)「好玩遊戲.txt.exe」
(3)「好玩遊戲.exe.txt」
(4)「好玩遊戲.txt　(中間有很多空白)　　.exe」

(　　)17. 請問下列哪一封電子郵件是<u>比較</u>安全，而可以開啓的？
(1) 早上老師說要寄給我們期中考成績單，到了晚上我就收到標題爲「期中考成績單」的郵件。
(2) 收到微軟公司寄送的「作業系統更新程式」檔案，要立即執行安裝，來修補系統漏洞。
(3) 聖誕節前夕收到「聖誕老公公進城」的電腦螢幕保護程式，可以安裝來增加過節的氣氛。
(4) 收到網友寄的電子郵件附加檔案爲 www.myparty.com，可以安心點選。

(　　)18. 電腦病毒就像人類生病也有潛伏期，那電腦病毒的潛伏期是什麼意思呢？
(1) 從病毒被病毒作者產生，到病毒在世界上完全消失的時間。
(2) 從病毒感染檔案到病毒開始產生破壞行爲的時間。
(3) 從病毒被病毒作者產生，到病毒有解毒碼的時間。
(4) 從病毒被防毒軟體偵測到，到防毒軟體完全解毒的時間。

(　　)19. 電腦病毒在潛伏期時會不斷地感染檔案，此時病毒是如何運作的呢？
(1) 病毒會不斷的重複感染相同的檔案，讓病毒程式在整個檔案中佔的比例越來越大。
(2) 病毒的潛伏期越長，代表感染檔案的能力比較弱，要花較多的時間把病毒程式寫入檔案中。
(3) 大部分病毒的潛伏期約爲一週。
(4) 病毒在潛伏期間會盡其所能的感染檔案。

(　　)20.電腦病毒<u>不會</u>有哪種破壞行爲？
(1) 刪除檔案或格式化磁碟。
(2) 損毀鍵盤按鍵。
(3) 感染其他乾淨的檔案。
(4) 妨礙螢幕顯示。

(　　)21.下列哪一種狀況<u>不是</u>電腦中毒後會產生的狀況？
(1) 光碟無法讀取。
(2) 電腦無預警的重新開機。
(3) 系統運作緩慢。
(4) 上網速度變慢。

(　　)22.電腦病毒感染系統後，若不進行解毒可能會有什麼狀況產生？
(1) 電腦會燒毀。
(2) 電腦散熱風扇不會轉動。
(3) 過一段時間系統會自動解毒痊癒。
(4) 程式會無法開啓。

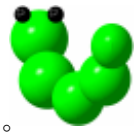
(　　)23.會立即造成電腦無法開機的病毒，有哪種特性？
(1) 會在短時間內造成大範圍的流傳。
(2) 解毒容易。
(3) 不容易傳散。
(4) 幾分鐘後再重新開機，就會恢復正常。

(　　)24.下列關於電腦病毒的說明何者是正確的？
(1) 電腦一旦中毒，就像人類感冒一樣會變的很虛弱，因此更容 易感染別的電腦病毒。
(2) 長時間使用電腦，會讓電腦疲累，此時病毒較容易侵入。
(3) 感染電腦病毒後會產生抗體，不會重複感染相同的電腦病毒。
(4) 沒有安裝防毒軟體或沒有進行系統更新，就像人類沒有抗體，容易感染病毒。

(　　)25.對於電腦病毒傳染的描述，下列何者正確？
(1) 污損的光碟片沾黏病毒，造成電腦讀取光碟時容易把病毒寫入電腦中。
(2) 醫院裡病人所散發出來的病菌容易附著在網路線或無線網路上傳送到電腦中。
(3) 電腦教室中有電腦中毒，避免讓未中毒的電腦近距離接觸感染源，所以要將未中毒的電腦搬到另一個房間。
(4) 電腦病毒就好像 SARS 病毒一樣，到任何一個國家，電腦都可能會感染相同的電腦病毒。

(　　)26.「電腦病毒」、「電腦蠕蟲」、「木馬」都是不懷好意的電腦程式，請你選出他們有什麼相同的地方？
(1) 不需經過使用者同意，就可以自行植入電腦。
(2) 都會感染乾淨的檔案。
(3) 大多會刪除系統檔案，使系統無法正常運作。
(4) 這些惡意程式都是使用者自己在網路下載才會感染的。

(　　)27.何者是「電腦蠕蟲」的特性？



(1) 取得使用者同意後才會進入電腦中。
(2) 透過網路傳送電腦蠕蟲到其他電腦中，造成網路變慢。
(3) 會感染系統中乾淨的檔案。
(4) 假借爲有用的工具軟體，吸引使用者下載。

(　　)28.下列何者<u>不是</u>「特洛依木馬」的特性？
(1) 常假借爲有用的工具軟體，吸引使用者下載。
(2) 目的多爲竊取使用者電腦中的資料。
(3) 會主動將病毒植入其它電腦裡。
(4) 使用者在不知情的狀況下被植入木馬。

(　　)29.好友寄來一封警告病毒的信件，內容是『趕快搜尋系統中是否有 jdbgmgr.exe，有的話代表你已經中毒，盡快刪除此檔，避免病毒再度流散。我也已經刪除檔案了，電腦目前很正常。』經過搜尋，電腦中真的有這個 jdbgmgr.exe 檔案，你該如何處理？
(1) 重新安裝作業系統。
(2) 依照指示把 jdbgmgr.exe 檔案刪除掉。
(3) 把這個消息再傳給我的好朋友們。
(4) 把這封警告信件傳給防毒公司進行檢測。

(　　)30.收到一封信是『最新強大病毒通知!要小心一封名爲「來抽支籤!」的郵件，收到後請勿開啓，並請立即刪除，它會讓電腦無法關機還會自行寄給你連絡簿裡的朋友。請將這個消息轉寄給在你通訊錄裡的所有人 !希望能來得及!』當你收到這封信後，應該要如何處理？
(1) 趕緊轉寄給朋友，提醒他們小心。
(2) 把信件貼到網路討論區，警告大家。
(3) 到防毒公司網站查詢相關資訊。
(4) 趕緊搜尋信箱，若有『來抽支籤!』的郵件，就將此信件刪除，並且寄信告訴大家。

(　　)31.防治電腦病毒最好的方法是下列哪一選項？
(1) 登入密碼不可以是空白的，所以要設定密碼爲 abc 即可以保護電腦不被入侵。
(2) 每年年底都要進行檔案備份。
(3) 執行檔案前先掃毒。

(4) 將檔案都設成”隱藏”，病毒看不見就不會感染。

(　　)32.當你感覺電腦可能中毒了，必須要做何種處理方法？
(1) 重新安裝作業系統。
(2) 立即切斷網路，進行掃毒。
(3) 趕快備份檔案，將檔案拿到其他電腦上繼續工作。
(4) 刪除那些可能是電腦病毒的檔案。

(　　)33.請問下列哪一組電腦登入密碼最能防治病毒侵入呢?
(5) 不設密碼。
(6) 簡短好記的密碼，如 123。
(7) 用英文、數字以及符號組成的密碼，如 xin09$%28。
(8) 用英文單字做爲密碼，如 APPLE。

(　　)34.下列敘述何者正確？
(1) 電腦沒有上網，因此不需要安裝防毒軟體。
(2) 有安裝防毒軟體就代表電腦已受到完整的保護。
(3) 購買防毒軟體後，防毒軟體公司能提供解毒支援服務。
(4) 防毒軟體能防護所有已知及未知的病毒。

(　　)35.防毒軟體的解毒功能，何者敘述是正確的？
(1) 只要是防毒軟體能偵測到的病毒，都能解毒成功。
(2) 防毒軟體無法解毒的檔案，必須要立即刪除檔案。
(3) 防毒軟體沒有偵測到任何病毒，代表目前未受到感染。
(4) 經由防毒軟體解毒後的檔案，不能保證可以正常執行。

(　　)36. 目前市面上的防毒軟體通常有三種解毒狀況，分別爲「修復」、「刪除」、「隔離」，請將代表的意思**連接**起來？(注意：本題只有**三條**連接線)

修復 ●	● 病毒檔案被移至電腦的另一個資　料夾裡，暫時不會被偵測到。
隔離 ●	● 附著在檔案上的電腦病毒程式，已經被移除了，檔案通常可以繼續運作。
刪除 ●	● 將偵測到的病毒檔案移至資源回收筒。
	● 電腦病毒檔案在電腦裡已經找不到了。

~~謝謝你的填答~~

附錄二 電腦病毒概念測驗試卷(預試 1)

_____國小 六年___班 姓名：_____

電腦病毒概念測驗試卷(預試試卷)

您好：

這份試卷是想瞭解目前受試者對於電腦病毒的概念理解程度。藉由您的回答，我們將可分析目前電腦病毒防治教育仍需要加強哪些部分。請根據您的了解來填答這份試卷，謝謝您的回答。

國立台東大學教學科技碩士班

指導教授：鄭承昌 博士

研究生：梁雅琇 敬啟

第一部分 基本資料

填答方法：請在空格內打勾

1. 性別：□男 □女
2. 是否曾感染過電腦病毒：□有 □沒有
3. 平均每天上網時數：□1 小時以下 □1-2 小時 □2-3 小時 □3 小時以上
4. 學校老師曾教過電腦病毒知識：□有 □沒有

第二部份 電腦病毒概念測驗

填答說明：

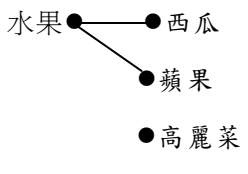
二、 本試卷共有 37 題，每一題都有 4 個選項，其中只有一個選項是正確的，請將您的答案填入( )括號中。

( )1. 電腦病毒依據感染的檔案不同，而分成開機型、檔案型病毒、巨集病毒、網頁病毒四種型態喔!!

請你把這四種病毒感染哪些檔案連起來，每一種病毒有兩個選項喔。

病毒類型	選項
開機型病毒●	● 磁碟片
檔案型病毒●	● .exe 應用程式
巨集病毒 ●	● .doc 文書 Word 檔
網頁病毒 ●	● .html 檔
	● .mp3 音效檔
	● .jpg 圖片檔
	● CPU
	● 硬碟
	● .scr 螢幕保護程式
	● .xls 試算表 Excel 檔
	● .vbs 檔

範例：何者是水果



(　)2. Jolin 每天都會上網留言給歌迷，今天晚上她上網時有一隻電腦病毒正要進入她的電腦中，請問電腦病毒進入電腦時會出現什麼狀況？：
(1) 螢幕上會出現「是否要下載檔案」的訊息視窗。
(2) 不會有明顯動作，所以察覺不到。
(3) 螢幕上會顯示「檔案已成功複製到 C:\windows 目錄」的訊息視窗。
(4) 電腦主機會發出嗶嗶嗶的聲音，警告有不明檔案進入。

(　)3. 承上題，Jolin 當時正在回覆留言板的問題，她會怎麼做？

(1) 點選訊息視窗上「否」的按鈕，病毒就不會進來。
(2) Jolin 並沒有察覺到病毒已經進入電腦了，繼續留言。
(3) 因為 Jolin 電腦有設密碼，所以病毒無法複製成功。
(4) 因為有嗶嗶聲，所以 jolin 馬上就發現病毒了。

(　)4. 電腦裡的檔案被電腦病毒感染後，開啟被感染的檔案，請問存在檔案裡的病毒會： (1)會隨著檔案開啟而被執行到 (2)不會被執行到 (3)隔幾天才會執行一次 (4)病毒執行前會出現訊息詢問你是否要執行，點選「是」病毒才會執行。

(　)5. 病毒附著在下列哪一個檔案後，開啟該檔，病毒程式最有可能被啟動？
(1)楊承零的曖昧.txt 的歌詞純文字檔案　(2)淡水阿給遊戲的.exe 執行檔
(3)小 S 照片的.png 圖像檔　(4)周捷倫 MTV 的.mpg 影音檔。

(　)6. 電腦病毒不會透過下列哪種方法傳染出去？ (1)Yahoo 即時通 (2)數位相機的記憶卡 (3)電子郵件 (4)電腦的電源供應線。

(　)7. Jolin 收到四封含有附加檔案的 E-mail，請問開啟哪一個附加檔案不會中毒？ (1)「.exe」(2)「.jpg.exe」 (3)「.exe.txt」(4)「.zip　(中間有很多空白)　.exe」

(　)8. 從網路上下載非法軟體會中毒，這是因為病毒寄生在哪種物體上進行散佈？ (1)網路線　(2)檔案　(3)網路卡　(4)數據機。

(　)9. 軟體的使用，何者正確？
(1)剛出廠的筆記型電腦，內建的軟體不會感染病毒。
(2)使用不合法的、開放的或免費的軟體裡面都會有病毒程式。
(3)合法軟體也會被病毒感染。
(4)防毒軟體公司的病毒碼更新檔，不會含有病毒。

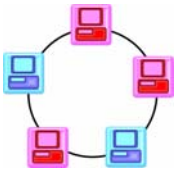
(　)10. 哪種狀況下，比較容易讓電腦病毒侵入電腦？ (1)使用防寫的磁片 (2)潮濕且發霉的磁片 (3)老舊的網路卡和網路線 (4)很久沒更新的 Windows XP 作業系統。

(　　)11.今天是 7 月 6 日，防毒軟體公司發佈一隻電腦病毒會在 7 月 7 日當天開始發作破壞檔案，應該如何防範比較好？

(1)趕把系統時間先調成 7 月 8 日就不會發作了。
(2)在 7 月 7 日那天都不要開機，隔天再開就好了。
(3)在 7 月 7 日前先下載病毒更新檔掃毒，並常駐防毒軟體。
(4)7 月 6 日前把系統檔設為隱藏，這樣就不會感染系統檔，可以保護系統。

(　　)12. 有一隻病毒只會在 13 號星期五當天開始刪除檔案，這代表何種意思？
(1)病毒只會在 13 號星期五侵入電腦，其他時間電腦中不會有病毒程式。
(2)電腦隨時會被感染，病毒會存在電腦中，等待 13 號星期五開始破壞。
(3)病毒只會在今年的十三號星期五內發作，明年就不會發作了。
(4)發作過一次後，下個十三號星期五就不會發作了。

(　　)13.電腦病毒在大流行過後，會有什麼狀況產生？ (1)如果病毒又進來，會被防毒軟體偵測到 (2)電腦會產生抗體，不會再次感染 (3) 隔一陣子可能會捲土重來，再次造成大流行(4)流行期過了病毒就會消失，不再出現。



(　　)14. 有一隻病毒在電腦教室的區域網路中流傳，下面哪一種描述是正確的呢？
(1)把老師使用的電腦清除乾淨，其他電腦中的病毒就會一起被清除掉。
(2)其中一台電腦解完毒後，就不會再中毒了，可以繼續上網。
(3)清除完病毒後，電腦連上網路，病毒也會再進入。
(3)病毒只會攻擊電腦教室裡的電腦，所以校長室裡的電腦不會受到侵入。

(　　)15.電腦感染了會透過電子郵件 e-mail 散佈的病毒，為了不把病毒傳染給信箱中的聯絡人，下列何者哪一項敘述是正確的？
(1)只要我不寄信給好友，病毒就不會附在郵件上進行散佈了。
(2)把信箱中的聯絡簿名單刪除掉，病毒也就沒辦法寄給好友了。
(3)趕快把網路線拔掉，這樣就不會傳出去了。
(4)不要打開 Outlook Express 病毒就不會寄出去了。

(　　)16. 哪一種情況下，電腦被病毒入侵的機會比較小？ (1)上網下載軟體 (2)閱讀電子郵件(3)我的電腦沒有上網，所以感染病毒的機會比較小 (4)雖然有的電腦開機會自動連上網路，但是只要不瀏覽網頁或不收信就不會感染。

(　　)17. 電腦病毒不斷的改變原始病毒程式，來躲避防毒軟體的偵測，稱為「變種病毒」，下列敘述何者正確？
(1)只要防毒軟體有原始病毒的病毒碼，就可以攔截到變種病毒。
(2)感染過原始病毒的電腦，就不會被他的變種病毒感染。

(3)變種病毒可能會造成更大的流傳與破壞。
(4)變種病毒的破壞能力小於原始病毒的破壞能力。

(　)18. 請選擇哪一封信件是比較安全的？
(1) 姐姐告訴我，她要用 E-mail 寄一份蕭啞軒的純文字檔歌詞給我，過不久後我就收到了。
(2) 收到由微軟 Microsoft 公司寄送的電子郵件，信件標題為「系統更新通知」，必須立即執行附加在信件中的更新檔案，以免病毒從系統漏洞進入。
(3) 網友寄了一個好玩遊戲的網址給我，並沒有附加檔案，所以可以安心連結，只要沒有執行任何檔案，就不會中毒。
(4) 我在新年前夕收到朋友寄來祝賀「新年快樂」的動畫檔案，可以安心開啟觀看。

(　)19. 電腦病毒就像人類生病也有潛伏期，那電腦病毒的潛伏期是什麼意思呢？ (1)從病毒被病毒作者產生，到病毒在世界上完全消失的時間 (2)從病毒感染檔案到病毒開始產生破壞行為的時間 (3)從病毒被病毒作者產生，到病毒有解毒碼的時間 (4)從病毒被防毒軟體偵測到，到防毒軟體完全解毒的時間。

(　)20. 電腦病毒在潛伏期時會不斷地感染檔案，此時病毒是如何運作的呢？
(1)病毒為了能在執行受感染的檔案時被啟動到，因此在潛伏期會不斷的重複感染相同的檔案，讓病毒程式在整個檔案中佔的比例越來越大。
(2)病毒的潛伏期越長，代表感染檔案的能力比較弱，要花較多的時間把病毒程式寫入檔案中。
(3)大部分病毒的潛伏期約為一週。
(4)病毒在潛伏期間會盡其所能的感染檔案。

(　)21. 電腦病毒<u>不會</u>有哪種破壞行為？ (1)刪除檔案或格式化磁碟 (2)損毀鍵盤按鍵 (3)感染其他乾淨的檔案 (4)妨礙螢幕顯示。

(　)22. 下列哪一種狀況<u>不是</u>電腦中毒後會產生的狀況？ (1)光碟無法讀取 (2)開機後每幾秒會重新開機 (3)系統運作緩慢 (4)無法上網。

(　)23. 電腦病毒感染系統後，若不進行解毒可能會有什麼狀況產生？ (1)電腦會燒毀 (2)電腦散熱風扇不會轉動 (3)過一段時間系統會自動解毒痊癒 (4)程式會無法開啟。

(　)24. 會刪除系統檔案或會格式化硬碟造成不能正常開機的病毒，何者敘述正確：(1)這種病毒容易引起全球性流傳 (2)較容易被發現所以解毒容易(3)病毒檔無法廣泛傳散(4)大部分的病毒都具有這些強大的破壞行為。

(　)25. 下列關於電腦病毒的說明何者是正確的？
(1)電腦一旦中毒，就像人類感冒一樣會變的很虛弱，因此更

容易感染別的電腦病毒。
(2)長時間使用電腦，會讓電腦疲累，此時病毒較容易侵入。
(3)感染電腦病毒後會產生抗體，不會重複感染相同的電腦病毒。
(4)沒有安裝防毒軟體或沒有進行系統更新，就像人類沒有抗體，容易感染病毒。

(　　)26. 對於電腦病毒傳染的描述，下列何者正確？
(1)污損的光碟片沾黏病毒，造成電腦讀取光碟時容易把病毒寫入電腦中。
(2)醫院裡病人所散發出來的病菌容易附著在網路線或無線網路上傳送到電腦中。
(3)電腦教室的區域網路內有人中毒，避免讓電腦近距離接觸感染源，所以要將電腦搬到另一個房間。
(4)電腦病毒就好像 SARS 病毒一樣，到任何一個國家，電腦都可能會感染相同的電腦病毒。

(　　)27.「電腦病毒」、「電腦蠕蟲」、「木馬」都是惡意的電腦程式，請你選出他們有什麼相同的地方？ (1)都沒有未經使用者同意就進入其電腦 (2)都會感染乾淨的檔案 (3)大多會刪除系統檔案，使系統無法正常運作 (4)都是被動攻擊，要使用者自己下載惡意程式且自己執行才會植入電腦中。

(　　)28. 何者<u>不是</u>「電腦蠕蟲」的特性？ (1)未經同意即進入他人電腦 (2)會感染電腦中乾淨的檔案 (3)多數目的為造成網路擁塞 (4)會主動將病毒透過網路植入其他電腦。

(　　)29. 下列何者<u>不是</u>「特洛依木馬」的特性？ (1)常假借為有用的工具軟體 (2)目的多為竊取使用者電腦中的資料(3)主動攻擊，會自動將病毒植入其他電腦 (4)被動攻擊，要自行下載惡意程式且經執行才會植入電腦中。

(　　)30. 好友寄來一封警告病毒的信件，內容是「趕快搜尋系統中是否有 jdbgmgr.exe，有的話代表你已經中毒，盡快刪除此檔，避免病毒再度流散。我也已經刪除檔案了，電腦目前很正常。」經過搜尋，電腦中真的有這個檔案，你該如何處理？
(1)重灌電腦系統 (2)依照指示把檔案刪除 (3)把這個消息再傳給我的好朋友們 (4)把信件傳給防毒公司。

(　　)31. 收到一封信是「最新強大病毒通知!要小心一封名為『來抽支籤!』的郵件，收到後請勿開啟，並請立即刪除，它會讓電腦無法關機還會自行寄給你連絡簿裡的朋友。請將這個消息轉寄給在你通訊錄裡的所有人！希望能來得及!」當你收到這封信後，應該要如何處理？
(1)趕緊轉寄給朋友，提醒他們小心 (2)把信件貼到網路公佈欄，警告大家 (3)把信件轉寄給防毒公司 (4) 趕緊搜尋信箱裡是否有這封郵

件，若有就將此封信件刪除。

(　　)32. 防治電腦病毒最好的方法是下列哪一選項？ (1)登入密碼不可以是空白的，所以要設定密碼為 abc 即可以保護電腦不被入侵　(2)每年年底都要進行檔案備份　(3)執行檔案前進先掃毒　(4)將檔案都設成”隱藏”，病毒看不見就不會感染。

(　　)33. 當你感覺電腦可能中毒了，必須要做何種處理方法？ (1)重灌電腦系統　(2)立即切斷網路，進行掃毒　(3)趕快把手邊的檔案儲存到磁片裡，拿到另一台電腦繼續作業　(4)自行把可能是病毒的檔案在第一時間內刪除，才不會擴大疫情。

(　)34.　請問下列那一組系統登入密碼最能防治病毒侵入呢?
(1)9876543210 超過 10 碼數字最安全(2)123 好記最重要(3)administrator 用很長的英文最安全(4)yahsiou624 英文加數字才好。

(　　)35. 下列敘述何者正確？
(1)電腦安裝兩套防毒軟體更能保護系統安全，彌補對方功能的不足。
(2)有安裝防毒軟體就代表電腦已受到完整的保護。
(3)購買防毒軟體後，防毒軟體公司能提供解毒支援服務。
(4)防毒軟體能防護所有已知及未知的病毒。

(　　)36. 防毒軟體的解毒功能，何者敘述是正確的？
(1)防毒軟體解不掉的毒，代表系統感染太嚴重了，需要直接重灌系統。
(2)防毒軟體無法解毒的檔案，必須要立即刪除掉，避免病毒再度執行。
(3)已下載了最新的病毒定義檔，當防毒軟體沒有偵測到任何病毒，代表目前未受到感染。
(4)防毒軟體無法保證所有被病毒感染的檔案在解毒後都能回到正常狀態。

(　　)37. 目前市面上的防毒軟體通常有三種解毒狀況，分別為「清除」「隔離」「刪除」，請問這三名詞分別代表什麼意思？

解毒狀況	選項
清除 ●	● 代表遭病毒感染的檔案被移至電腦的另一個空間，是暫時不會被啟動。
隔離 ●	● 病毒已經從被感染的檔案中移除掉了。
刪除 ●	● 病毒還在系統中，下次病毒啟動時防毒軟體會自動攔劫過濾，讓病毒程式執行後馬上被停止。

附錄三 電腦病毒概念測驗試卷(預試 2)

_____國小 六年___班 姓名：_____

電腦病毒概念測驗試卷

小朋友你好：

這份試卷是想瞭解目前你對於電腦病毒概念的理解程度。藉由你的回答，我們將可分析目前電腦病毒防治教育仍需要加強哪些部分。請根據你的了解來填答這份試卷，謝謝。

國立台東大學教學科技碩士班

指導教授：鄭承昌 博士

研究生：梁雅琇 敬啟

第一部分 基本資料

填答方法：請在空格內打勾

5. 性別： □男 □女

6. 是否曾感染過電腦病毒： □有 □沒有

7. 平均每天上網時數： □1 小時以下 □1-2 小時 □2-3 小時 □3 小時以上

8. 學校老師曾教過電腦病毒知識：□有 □沒有

第二部份 電腦病毒概念測驗

填答說明：

三、 本試卷共有 36 題，每一題都有 4 個選項，其中只有一個選項是正確的，請將您的答案填入( )括號中。

( )1. 電腦病毒可分爲四種，分別爲「開機型病毒」、「檔案型病毒」、「巨集病毒」、「描述語言病毒」，請你將這些病毒分別會感染的檔案**連接**起來。

病毒種類		選項
開機型病毒	●	
		● .DOC 與 .XLS (Office 文書檔)
檔案型病毒	●	
巨集病毒	●	
		● .HTML 與 .VBS (網頁程式檔)
描述語言病毒	●	
		● .EXE 與 .SCR (可執行檔)

(　　)2. 電腦病毒進入電腦時，會出現哪種情形？

(1) 螢幕上會出現「是否要執行病毒程式」的訊息。

(2) 電腦通常不會有明顯異狀。

(3) 螢幕會顯示「檔案已成功複製到 C 槽」的訊息。

(4) 電腦主機會發出像「救護車」聲音來警戒。

(　　)3. 下列有關電腦病毒的描述，何者正確？

(1) 電腦病毒在取得使用者同意後，才能進入電腦。

(2) 電腦病毒會不斷發出訊息，讓使用者知道它的存在。

(3) 電腦病毒不需要使用者允許，就能進入電腦。

(4) 電腦病毒在刪除系統檔案時，會產生警告訊息。

(　　)4. 電腦裡的檔案被電腦病毒感染後，開啓被感染的檔案，請問存在檔案裡的病毒：

(1) 會隨著檔案開啓而被執行。

(2) 不會被執行。

(3) 隔幾天才會執行一次 。

(4) 病毒執行前會出現訊息，詢問你是否要執行，點選「是」病毒才會執行。

(　　)5. 電腦病毒<u>**不會**</u>透過下列哪種方法傳染出去？

(1) Yahoo 即時通。

(2) MP3 隨身碟。

(3) 電子郵件。

(4) 電腦的電源供應線。

(　　)6. 從網路上下載非法軟體會中毒，這是因爲病毒寄生在哪種物體上進行散佈？

(1) 網路線。

(2) 檔案。

(3) 網路卡。

(4) 數據機。

(　　)7. 有關軟體的使用，下列何者敘述正確？

(1) 新買的電腦裡面的軟體不會有電腦病毒。

(2) 使用盜版或免費的軟體，一定會中毒。

(3) 購買正版軟體就能確保不被病毒感染。

(4) 防毒軟體的更新檔案也會被電腦病毒感染。

(　　)8. 哪種狀況下，比較容易讓電腦病毒侵入電腦？

(1) 使用防寫的磁片。

(2) 潮濕且發霉的磁片。

(3) 老舊的網路卡和網路線。

(4) 很久沒做漏洞更新的 Windows XP 作業系統。

(　　)9. 防毒軟體公司發佈一隻電腦病毒，會在 7 月 7 日當天開始發作破壞檔案，應該如何防範比較好？

(1) 提前把電腦時間調整成 7 月 8 日，就不會發作。

(2) 7 月 7 日那天都不要開機，隔天再開就不會發作。

(3) 7 月 7 日前先下載病毒更新檔進行掃毒。

(4) 7 月 7 日前把電腦檔案設爲隱藏，電腦病毒就找不到檔案了。

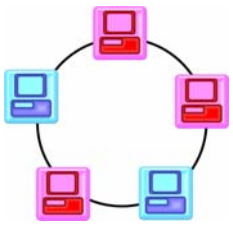
(　　)10. 有一隻病毒只會在 13 號星期五當天開始刪除檔案，這代表何種意思？

(1) 病毒只會在 13 號星期五侵入電腦，其他時間電腦裡不會有病毒程式。

(2) 電腦隨時會被感染，病毒會存在電腦中，等待 13 號星期五開始破壞。

(3) 病毒只會在今年的十三號星期五內發作，明年就不會發作。

(4) 發作過一次後，下個十三號星期五就不會發作了。



(　　)11. 電腦病毒在流行期過後會有下列哪一種狀況發生？

(1) 病毒會慢慢的消失不見，不再復發。

(2) 很久以前流行過的病毒，不會在新的作業系統上流傳。

(3) 曾經流行過的病毒，不會再次造成大流行。

(4) 過一陣子病毒可能會再次造成大流行。

(　　)12.有一隻病毒在學校電腦教室的網路中流傳，下面何者是正確的呢？

(1) 把老師使用的電腦清除乾淨，其他電腦中的病毒就會一起被清除掉。

(2) 其中一台電腦解完毒後，就不會再中毒了，可以繼續上網。

(3) 清除完病毒後，電腦連上網路，病毒也會再進入。

(4) 病毒只會攻擊電腦教室裡的電腦，所以校長室裡的電腦不會受到侵入。

(　　)13.我感染了一隻病毒，會透過電子郵件轉寄病毒程式給 Outlook 通訊錄中的聯絡人，首先應該要如何處理？

(1) 仍可繼續瀏覽網站，但不要使用 Outlook 寄信給朋友。

(2) 盡速拔除網路線來停止網路功能，使病毒無法寄信出去。

(3) 馬上改用線上信箱寄信(如 Yahaoo 免費信箱)，但仍可開啓 Outlook 來收信。

(4) 發信警告好友，不要開啓由我寄出的電子郵件。

(　　)14.哪一種情況下，電腦被病毒入侵的機會比較小？

(1) 上網下載軟體。

(2) 閱讀電子郵件。

(3) 我的電腦沒有上網，所以感染病毒的機會比較小。

(4) 雖然有的電腦開機會自動連上網路，但是只要不瀏覽網頁或不收信就不會感染。

(　　)15.電腦病毒不斷的改變原始病毒程式，來躲避防毒軟體的偵測，稱爲「變種病毒」，下列敘述何者正確？

(1) 只要防毒軟體有原始病毒的病毒碼，就可以攔截到變種病毒。

(2) 感染過原始病毒的電腦，就不會被他的變種病毒感染。

(3) 變種病毒可能會造成更大的流傳與破壞。

(4) 變種病毒的破壞能力比原始病毒小。

(　　)16. Jolin 收到四封含有附加檔案的 E-mail，請問開啓哪一個附加檔案<u>不會</u>中毒？

(1)「好玩遊戲.exe」

(2)「好玩遊戲.txt.exe」

(3)「好玩遊戲.exe.txt」

(4)「好玩遊戲.txt　(中間有很多空白)　　.exe」

(　　)17. 請問下列哪一封電子郵件是<u>比較</u>安全，而可以開啓的？

(1) 早上老師說要寄給我們期中考成績單，到了晚上我就收到標題爲「期中考成績單」的郵件。

(2) 收到微軟公司寄送的「作業系統更新程式」檔案，要立即執行安裝，來修補系統漏洞。

(3) 聖誕節前夕收到「聖誕老公公進城」的電腦螢幕保護程式，可以安裝來增加過節的氣氛。

(4) 收到網友寄的電子郵件附加檔案爲 www.myparty.com，可以安心點選。

(　　)18. 電腦病毒就像人類生病也有潛伏期，那電腦病毒的潛伏期是什麼意思呢？

(1) 從病毒被病毒作者產生，到病毒在世界上完全消失的時間。

(2) 從病毒感染檔案到病毒開始產生破壞行爲的時間。

(3) 從病毒被病毒作者產生，到病毒有解毒碼的時間。

(4) 從病毒被防毒軟體偵測到，到防毒軟體完全解毒的時間。

(　　)19. 電腦病毒在潛伏期時會不斷地感染檔案，此時病毒是如何運作的呢？

(1) 病毒會不斷的重複感染相同的檔案，讓病毒程式在整個檔案中佔的比例越來越大。

(2) 病毒的潛伏期越長，代表感染檔案的能力比較弱，要花較多的時間把病毒程式寫入檔案中。

(3) 大部分病毒的潛伏期約爲一週。

(4) 病毒在潛伏期間會盡其所能的感染檔案。

(　　)20.電腦病毒<u>不會</u>有哪種破壞行爲？

(1) 刪除檔案或格式化磁碟。

(2) 損毀鍵盤按鍵。

(3) 感染其他乾淨的檔案。

(4) 妨礙螢幕顯示。

(　　)21.下列哪一種狀況<u>不是</u>電腦中毒後會產生的狀況？

(1) 光碟無法讀取。

(2) 電腦無預警的重新開機。

(3) 系統運作緩慢。

(4) 上網速度變慢。

(　　)22.電腦病毒感染系統後，若不進行解毒可能會有什麼狀況產生？

(1) 電腦會燒毀。

(2) 電腦散熱風扇不會轉動。

(3) 過一段時間系統會自動解毒痊癒。

(4) 程式會無法開啓。

(　　)23.會刪除系統檔案或會格式化硬碟造成不能正常開機的病毒，何者敘述正確？

(1) 會在短時間內造成大範圍的流傳。

(2) 解毒容易。

(3) 會造成電腦病毒檔案也被消毀，因此不容易傳散。

(4) 絕大多數的病毒都有格式化硬碟的破壞行爲。

(　　)24.下列關於電腦病毒的說明何者是正確的？

(1) 電腦一旦中毒，就像人類感冒一樣會變的很虛弱，因此更容 易感染別的電腦病毒。

(2) 長時間使用電腦，會讓電腦疲累，此時病毒較容易侵入。

(3) 感染電腦病毒後會產生抗體，不會重複感染相同的電腦病毒。

(4) 沒有安裝防毒軟體或沒有進行系統更新，就像人類沒有抗體，容易感染病毒。

(　　)25.對於電腦病毒傳染的描述，下列何者正確？

(1) 污損的光碟片沾黏病毒，造成電腦讀取光碟時容易把病毒寫入電腦中。

(2) 醫院裡病人所散發出來的病菌容易附著在網路線或無線網路上傳送到電腦中。

(3) 電腦教室中有電腦中毒，避免讓未中毒的電腦近距離接觸感染源，所以要將未中毒的電腦搬到另一個房間。

(4) 電腦病毒就好像 SARS 病毒一樣，到任何一個國家，電腦都可能會感染相同的電腦病毒。

(　　)26.「電腦病毒」、「電腦蠕蟲」、「木馬」都是不懷好意的電腦程式，請你選出他們有什麼相同的地方？

(1) 不需經過使用者同意，就可以自行植入電腦。

(2) 都會感染乾淨的檔案。

(3) 大多會刪除系統檔案，使系統無法正常運作。

(4) 這些惡意程式都是使用者自己在網路下載才會感染的。

(　　)27.何者是「電腦蠕蟲」的特性？

(1) 取得使用者同意後才會進入電腦中。

(2) 透過網路傳送電腦蠕蟲到其他電腦中，造成網路變慢。

(3) 會感染系統中乾淨的檔案。

(4) 假借爲有用的工具軟體，吸引使用者下載。

(　　)28.下列何者<u>不是</u>「特洛依木馬」的特性？

(1) 常假借爲有用的工具軟體，吸引使用者下載。

(2) 目的多爲竊取使用者電腦中的資料。

(3) 會主動將病毒植入其它電腦裡。

(4) 使用者在不知情的狀況下被植入木馬。

(　　)29.好友寄來一封警告病毒的信件，內容是『趕快搜尋系統中是否有 jdbgmgr.exe，有的話代表你已經中毒，盡快刪除此檔，避免病毒再度流散。我也已經刪除檔案了，電腦目前很正常。』經過搜尋，電腦中真的有這個 jdbgmgr.exe 檔案，你該如何處理？

(1) 重新安裝作業系統。

(2) 依照指示把 jdbgmgr.exe 檔案刪除掉。

(3) 把這個消息再傳給我的好朋友們。

(4) 把這封警告信件傳給防毒公司進行檢測。

(　　)30.收到一封信是『最新強大病毒通知!要小心一封名爲「來抽支籤!」的郵件，收到後請勿開啓，並請立即刪除，它會讓電腦無法關機還會自行寄給你連絡簿裡的朋友。請將這個消息轉寄給在你通訊錄裡的所有人 !希望能來得及!』當你收到這封信後，應該要如何處理？

(1) 趕緊轉寄給朋友，提醒他們小心。

(2) 把信件貼到網路討論區，警告大家。

(3) 到防毒公司網站查詢相關資訊。

(4)趕緊搜尋信箱，若有『來抽支籤!』的郵件，就將此信件刪除，並且寄信告訴大家。

(　　)31.防治電腦病毒最好的方法是下列哪一選項？

(1) 登入密碼不可以是空白的，所以要設定密碼爲 abc 即可以保護電腦不被入侵。

(2) 每年年底都要進行檔案備份。

(3) 執行檔案前先掃毒。

(4) 將檔案都設成”隱藏”，病毒看不見就不會感染。

(　　)32.當你感覺電腦可能中毒了，必須要做何種處理方法？

(1) 重新安裝作業系統。

(2) 立即切斷網路，進行掃毒。

(3) 趕快備份檔案，將檔案拿到其他電腦上繼續工作。

(4) 刪除那些可能是電腦病毒的檔案。

(　　)33.請問下列哪一組電腦登入密碼最能防治病毒侵入呢?

(1) 不設密碼。

(2) 簡短好記的密碼，如 123。

(3) 用英文、數字以及符號組成的密碼，如 xin09$%28。

(4) 用英文單字做爲密碼，如 APPLE。

(　　)34.下列敘述何者正確？

(1) 電腦安裝兩套防毒軟體更能保護系統安全，彌補對方功能的不足。

(2) 有安裝防毒軟體就代表電腦已受到完整的保護。

(3) 購買防毒軟體後，防毒軟體公司能提供解毒支援服務。

(4) 防毒軟體能防護所有已知及未知的病毒。

(　　)35.防毒軟體的解毒功能，何者敘述是正確的？

(1) 只要是防毒軟體能偵測到的病毒，都能解毒成功。

(2) 防毒軟體無法解毒的檔案，必須要立即刪除檔案。

(3) 防毒軟體沒有偵測到任何病毒，代表目前未受到感染。

(4) 經由防毒軟體解毒後的檔案，不能保證可以正常執行。

(　　)36.目前市面上的防毒軟體通常有三種解毒狀況，分別爲「修復」、「刪除」、「隔離」，請將代表的意思**連接**起來？

修復 ●	● 病毒檔案被移至電腦的另一個資　料夾裡，暫時不會被偵測到。
隔離 ●	● 附著在檔案上的電腦病毒程式，已經被移除了，檔案通常可以繼續運作。
刪除 ●	● 將偵測到的病毒檔案移至資源回收筒。
	● 電腦病毒檔案在電腦裡已經找不到了。

~~謝謝你的填答~~

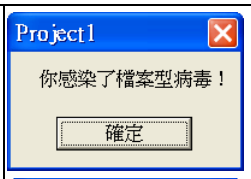
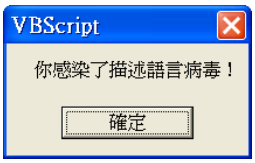
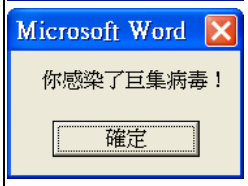

NTTU Library

附錄四 電腦病毒概念改變課程(實驗組 1)

一、電腦病毒基本原則課程設計

<table>
<tr><td colspan="6">課 程 設 計</td></tr>
<tr><td>主題</td><td>電腦病毒概念課程</td><td>單元</td><td colspan="3">電腦病毒基本原則</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>1</td><td>時間</td><td>40 分鐘</td></tr>
<tr><td>教學
目標</td><td colspan="5">4. 了解電腦病毒基本三原則「未授權性」、「自我複製」、「自動執行」。
5. 認識電腦病毒種類。</td></tr>
<tr><td>活動目標</td><td colspan="3">教學活動</td><td>時間</td><td>教學資源</td></tr>
<tr><td>引起動機(電腦病毒初體驗)</td><td colspan="3">【活動 1】認識電腦檔案格式
電腦病毒真的和人很像，所以才會被命名爲「病毒」，所以電腦病毒是附著在電腦裡各式各樣的檔案中，檔案就像人的器官一樣，也有不同的名稱和功能喔。
活動說明：由教師介紹電腦檔案格式。
(1) 學會如何設定檔案總管能顯示所有隱藏檔及副檔名(教學資源 1)。
(2)開啓 A:\檔案格式目錄，即可看到各種檔案格式(教學資源 2)。
(3)請學生唸出目錄中有哪些檔案，用來確認每位學生都設定完成。

【活動 2】實際執行各種檔案格式
活動說明： 由學生執行各種檔案
(1)讓他們分別執行副檔案格式目錄(教學資源 2)中的各個檔案。
(2)當開啓「執行檔」、「描述語言」、「巨集」時會顯示”哈哈！你已經感染某某病毒了！”</td><td>15’</td><td>1. 設定資料夾模式的教學投影片
2. 製做一個「副檔案格式」目錄，內有各式檔案格式的檔案，分別爲：
執行檔.pif
執行檔.com
執行檔.exe
執行檔.scr
Excel 巨集.xls
Word 巨集.doc
描述語言.htm</td></tr>
</table>

	   (3)請學生紀錄執行的檔案以及病毒名稱。		描述語言.html 描述語言.js 描述語言.vbs 學習單
目標 1-1：透過生活中經驗類比到病毒的「自我複製」定義	【活動 1】呈現電腦病毒基本原則的概念圖。 活動說明： 1. 教師說明何謂基本原則，利用學生已學習過的長方形定理”： ①四個角都是直角的四邊形稱爲長方形。 ②長方形的兩雙對邊互相平行且相等。 ③長方形的對角線互相平分且等長。 用此來說明要稱爲電腦病毒必須要具備的條件爲「自我複製」、「自我執行」。 【活動 2】由教師舉例，透過學生個人經驗類比來說明電腦病毒的「自我複製性」，病毒如何在電腦中生存的? 活動說明： (1) 利用投影機播放「教學資源 2」，讓學生麵包爲什麼會發霉？因爲霉菌附著在麵包裡面滋生，先讓學生對於”自我複製”有具體的影像。 【活動 3】教師講述	5’	3. 基本原則概念圖投影片 4. 黴菌在麵包上滋生的歷程投影片 5. 電腦病毒

	電腦病毒也一樣，進入電腦後就把惡意程式附著在檔案裡，然後再傳染給其他的檔案。 活動說明： (1) 利用投影機播放「教學資源 5」，讓學生對病毒感染檔案的歷程有具體的心象。		感染檔案的歷程投影片
目標 1-2：透過生活中經驗類比到病毒的「自我執行」定義	【活動 1】由教師舉例說明，透過學生個人經驗類比來說明「自動執行」的運作。 活動說明： (1) 利用投影機播放「教學資源 4」，說明生病的人在打噴嚏或咳嗽時，感冒病毒會自動摻雜在噴嚏或飛沫中，然後進入其他人的身體。開始在另一個人的身體裡複製感冒病毒，才能使人開始發燒流鼻涕。 。讓學生對病毒自動執行的運作有具體的心象。 (2)由教師說明電腦病毒也一樣，每一次被感染的檔案執行時，電腦病毒也會跟著被啓動喔，目的是要讓病毒感染更多的檔案。 【活動 3】電腦病毒統整概念 各組推派二名成員描述電腦病毒一定要具有哪種特質。	5’	6. 人類咳嗽與自動執行相關聯的投影片 集點卡
目標 1-3：認識電腦病毒的種類	【活動 1】由教師舉例說明，透過學生個人經驗，來說明「病毒種類」，使學生推論電腦病毒不只有一種。 活動說明：	20’	5.人類各器官可能感染的病毒

	(1) 利用投影機播放「教學資源 5」，說明電腦病毒就像人會生很多不同的病一樣，像肝病就是病毒在肝裡面，胃病就是病毒在胃裡面，牙齒痛就是細菌在牙齒裡面。讓學生對人類病毒的種類有概念。 (2) 播放「教學資源 6」的投影片，讓學生對於電腦病毒種類有基本的認識。 (3) 講解病毒的演變過程，並舉出四類病毒實例說明「教學資源 7」。 (4) 認識更多類似的寄主程式，例用投影片「教學資源 8」，讓學生認識更多可能被病毒感染的副檔名格式。		投影片。 6.四類電腦病毒「開機型」「檔案型」、「巨集」、「描述語言」病毒，分別會感染的檔案格式。 7.四類電腦病毒的實例。 8.分別列舉 2-4 個分屬於四種電腦病毒的寄主程式。
評量	(1) 請寫出構成電腦病毒的必要條件是什麼，並簡單說明？ (2)由教師呈現各種副檔名格式，讓學生搶答這是何種病毒。	5’	學習單 集點卡

二、電腦病毒行爲特性 I 課程設計

<table>
<tr><th colspan="4">課　程　設　計</th></tr>
<tr><td>主題</td><td>電腦病毒概念課程</td><td>單元</td><td>電腦病毒行爲特性 I</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>2</td></tr>
<tr><td>目標</td><td colspan="3">1. 瞭解電腦病毒的行爲特性有「未授權性」、「傳染性」、「破壞性」、「潛伏性」、「類比爲生物性病毒」</td></tr>
<tr><td>階段</td><td>教學活動</td><td>時間</td><td>教學資源</td></tr>
<tr><td>引起動機</td><td>【活動 1】請同學發表哪些狀況你會覺得已經感染電腦病毒？電腦病毒又是透過什麼媒介進入電腦？</td><td>3’</td><td>集點卡</td></tr>
<tr><td>呈現學習目標</td><td>【活動 2】利用電腦病毒的概念圖說明本節課的主要概念。</td><td></td><td>1.行爲特性概念圖投影片</td></tr>
<tr><td>目標 2-1：透過聯想、講述與病毒案例，了解「未授權性」定義</td><td>【活動 1】「未授權性」定義聯想
請學生想像「電腦病毒要進入電腦時會不會告訴你們「是否要執行病毒程式？」以及「是否要刪除系統檔？」
活動說明：
(1) 利用投影機播放「教學資源 2」，讓學生聯想。
(2) 請學生舉手表態，並詢問爲什麼。

【活動 2】教師講述
這是電腦病毒的「未授權性」，是指電腦病毒未經他人允許就自行進入電腦。如果電腦病毒很容易被發現，就會馬上被電腦使用者刪除掉了，因此沒有辦法繼續散播，也就是自斷後路的行爲就像小偷一樣，犯案前不會敲鑼打鼓，引人注目。且病毒在取得電腦的使用權限後，不須經由使用者同意就可以操控電腦檔案，如刪除、修改等。</td><td>7’</td><td>2.二張「是否要執行病毒程式？」以及「請問是否要刪除系統檔？」的訊息視窗圖片。
集點卡</td></tr>
</table>

目標 2-2：利用生活中經驗與遊戲了解病毒的「傳染性」	【活動 1】教師利用人類感冒病毒的傳染媒介來說明電腦病毒也需要透過媒介傳播。 活動說明： (1)利用「教學資源 3」投影片說明人體感冒多是經由手觸摸、口沫、空氣等方式所傳染。 【活動 2】利用對錯遊戲讓學生認識哪些是電腦病毒的傳染途徑？ 活動說明： (1)由教師利用「教學資源 4」呈現各式傳染的途徑。 (2)讓學生利用手比 O 和 X 來回答該方式是否正確。 (3)答對一題在「集點卡」上打勾。 (4)教師利用「教學資源 5」將傳染媒介統整爲四大類：儲存設備、網路存取、電子郵件、系統漏洞。 (5)請同學思考下面問題，並回應： 想一想：盜版的光碟一定會中毒嗎？正版的就不會中毒嗎？ 想一想：防毒軟體的更新程式與病毒更新碼不會有病毒？ 想一想：新買的電腦裡面的軟體不會有電腦病毒？ 想一想：哪些傳播媒介最能造成廣大的流傳？ (5) 教師利用「教學資源 6」說明系統漏洞是指微軟的作業系統與應用程式是由複雜的程式所組合而成，程式由不同的人員撰寫，因此都會有疏漏的地方，且	8’	3.人類感冒病毒的傳染媒介投影片 4.電腦病毒傳染途徑的投影片 集點卡 5.四大類傳染媒介的投影片 集點卡。 6.「何謂系統漏洞」的投影片

	病毒技術也不斷翻新，因此病毒利用這些錯誤而可以進入電腦中。		
目標 2-3：破壞性	【活動 1】讓學生了解病毒有哪些破壞行爲。 活動說明：大家來找碴 (1)分給學生兩份資料「教學資源 7」，一份爲正常螢幕顯示畫面，一份爲可能被病毒感染過後的螢幕畫面(呈現訊息、圖形等)，找出兩張圖有差異的地方，並請學生說明可以看見的破壞行爲有哪些。 (2)教師利用投影機顯示 Hybris 病毒的發作動畫(教學資源 8)，說明在桌面上產生黑色漩渦，使用者無法操作桌面圖示。 (3)教師利用「教學資源 9」補充說明還有哪些非視覺性的破壞行爲，如開機後每幾秒會重新開機、系統運作緩慢 、上網速度緩慢、程式無法開啓。 (4)教師利用「教學資源 10」說明破壞力強大的電腦病毒之特性。	8’	7.兩張感染前與感染後的系統桌面圖片。 8. Hybris(2001 年)病毒發作動畫。 9.破壞行爲投影片。 10.破壞力強大的病毒特性投影片
目標 2-4：潛伏性	【活動 1】讓學生明瞭潛伏期的定義。 活動說明： (1) 教師利用「教學資源 11」以人類病毒的潛伏期來說明電腦病毒的潛伏期。 (2) 學生覆誦一次。 【活動 2】由教師說明電腦病毒潛伏期會有的行爲。 活動說明： (1) 利用投影機顯示「教學資源 12」說明潛伏期間病毒的行爲是避免被偵	5’	11.從人類病毒潛伏期類推到電腦病毒潛伏期的投影片 12.製作潛伏期特性投影片。

	測、近期所能的感染檔案以及時間越長造成的影響愈大。		
目標 2-5：類比爲生物性病毒	【活動 1】說明電腦病毒與人類生物性病毒的異同。 活動說明： (1)由教師統整人類生物性病毒與電腦病毒的差異表「教學資源 13」，依序呈現 。	5’	13.製作人類生物性病毒與電腦病毒的差異表
評量	1. 請寫出至少三項電腦病毒的傳播途徑。 2. 請寫出至少三項電腦病毒的破壞行。 3. 請描述電腦病毒的潛伏期定義。 4. 請寫出至少二項人類病毒與電腦病毒相同的地方。	7’	學習單

三、電腦病毒行爲特性 II 課程設計

課　程　設　計				
主題	電腦病毒概念課程	單元	電腦病毒行爲特性 **II**	
教師	梁雅琇	節次	3	
目標	1. 瞭解電腦病毒的行爲特性有「觸發性」、「持久性」、「自動攻擊性」、「不可預見性」			
階段	教學步驟		時間	教學資源
呈現單元目標	【活動 2】利用電腦病毒的概念圖說明本節課的主要概念。		3’	1.利用投影片呈現電腦病毒概念圖，並標示本節所要講述的行爲特性概念。
目標 2-6：觸發性	【活動 1】由教師利用「教學資源 2」上一節提到的潛伏性來說明觸發性的意義，讓學生親身體驗病毒的觸發性機制。 活動說明： (1)請學生執行程式「教學資源 3」。 (2)條整系統時間到 2008/08/08，設定程式在 2007/08/08 當天以及之後被執行，都會出現”病毒從 2007/08/08 被觸發了！”的訊息，並出現圖示。 (3)請學生調整系統時間至 2007/8/09 並執行，出現”病毒已經在 2008/08/08 被觸發，以後並毒會每天被執行”訊息，由此說明觸發性並不是只有發作的當天會有破壞行爲。 (4)由教師利用「教學資源 4」說明觸發性的條件端視病毒作者的設計而定。		8’	2.以上一節的潛伏性來說明觸發機制的投影片 3.撰寫 8 月 8 號觸發程式.exe。 4.觸發性條件的投影片
目標 2-7：不可預見	【活動 1】由教師利用「教學資源 5」告訴同學電腦病毒是無法預見的。因爲病		15’	5.電腦病毒不可預見性的說明

性	毒會不斷改變攻擊方式或是一直進行變種，並利用僞裝方法想盡辦法讓你執行到病毒喔。讓學生了解變種的不可預見性。 活動說明： (1)學生連上金帥防毒網，看 2006 的病毒消息，例如 Beagle.14 就表示已經有 14 隻變種病毒了，現在最高紀錄是 Beagle 大概有 50 幾隻變種了，讓同學發表哪一隻病毒是現在變種最多的。(網址參考輔助教具 6) (2)讓學生到 2001 年病毒消息看到 Codered 變種之後可以攻擊中文系統的資訊。 (3)用上述兩個概念並輔以「教學資源 7」來說明變種病毒的特性，分別爲可能比原始病毒的破壞力還要強、電腦不會產生抗體、有原始病毒的病毒碼不一定可以偵測到變種病毒。 【活動 2】說明電腦病毒的僞裝術： 活動說明： (1)教師利用「教學資源 8」說明電腦病毒使用的僞裝技巧。 (2)請學生上網收信，依據所收到的信件發表這些病毒所使用的僞裝手法，如假借爲系統更新檔、螢幕保護程式、防毒軟體公司確認無毒信、信用卡核對程式、郵件次服器管理者、附加檔案僞裝成網址模式或在節慶前後寄信以及利用雙副檔名格式爲附加檔案，這些都是病		投影片 6.金帥防毒網 http://www.ggreat.com.tw 集點卡 7.變種病毒特性的投影片 8.電腦病毒的僞裝技巧投影片 9.製做「雙副檔

	毒常用的僞裝手法。 【活動 3】教授雙副檔案格式。 活動說明： (1)請學生設定目錄爲顯示副檔名以及所有檔案，開啓雙副檔名目錄「教學資源 10」，依序唸出所看到的檔名及副檔名。 (2)依序執行「教學資源 9」的所有檔案。 (3)在學習單上紀錄開啓檔案後的訊息。 (4)由教師統整說明，雙副檔名是看最後一個副檔名的格式來開啓的。 (5)由教師說明.txt 檔案格式不會啓動病毒 (6)搭配第一節教授的病毒感染檔案，隨機做雙副檔名的組合「教學資源 10」，讓學生搶答那一個檔案會被病毒利用。 (7)答對者，集點。 【活動 4】顯示雙副檔名在郵件附加檔案上的利用。 活動說明： (1)利用投影片顯示「輔助教具 11」，呈現雙副檔名間有許多空白的附加檔案在電子郵件中的僞裝狀態，過多的空白會讓人只看到第一個無毒的副檔名，忽略了第二個副檔名。 (2)由教師提醒收信時的注意事項。		名」目錄，內有各式檔案格式 蜘蛛人.exe 蜘蛛人.exe.txt 蜘蛛人.txt 蜘蛛人.txt.exe 寶寶洗澡.exe .txt 寶寶洗澡.txt .exe 學習單 10.利用各種容易被病毒利用的副檔名隨機組合檔案以投影片呈現 集點卡 11.製作一封雙副檔名附加檔案的電子郵件(兩各副檔名間有許多空格)
目標 2-8：透過講述	【活動 1】說明主動攻擊性的意思，只要連上網路，就有機會被入侵。	5’	

讓學生了解主動攻擊性	活動說明： (1) 教師利用「教學資源 12」說明當電腦病毒利用電子郵件會在背景中偷偷發信給聯絡簿中的所有聯絡人，因此感染電子郵件病毒後要立即中斷網路；並指出電腦病毒也會自動去偵測網路上的電腦是否有共享目錄或是系統漏洞，若有就會進行感染與入侵。 (2) 說明電子郵件病毒會隨機選取中毒電腦裡的聯絡簿名單，假借爲寄件者，因此沒中毒的使用者常成爲大家謾罵的對象，而真正的中毒者卻渾然不知。 舉例說明：Klez 病毒		12.電腦主動攻擊性的說明投影片
目標 2-9：持久性	【活動 1】由教師利用「教學資源 13」先說明區域網路內的電腦中毒，解毒時間冗長，需將區域網內的所有電腦都停止網路功能，完成所有電腦的解毒後，才可以再連上網路。 活動說明： (1)利用投影片顯示「教學資源 14」，模擬區域網路攻擊行爲，一台電腦中毒會造成連鎖反應，感染給其他電腦。 (2)說明區域網路中流傳快，要全部解毒的速度卻很漫長。 (3)利用投影片顯示「教學資源 15」，教導區域網路解毒的過程，必須將所有的電腦網路聯先去除掉，一台一台解毒，確認無毒後才可以在連上網路。	5’	13.說明區域網路解毒時間冗長的投影片 14.繪製區域網路中電腦病毒的攻擊路線投影片。 15.區域網路解毒流程投影片。

	【活動 2】教師利用「教學資源 16」說明電腦病毒大流行過後，日後仍有機會再引發流行。由教師舉病毒死灰復燃的案例活動說明： 例子： 前幾年有 SARS 病毒，每天上學前都要量體溫戴口罩，結果原本已經被控制住的 SARS 病毒，卻又因爲病毒研究室的人員研究時感染又再次流傳。 活動說明： (1)請同學推論電腦病毒可能再次流行的原因。		16.電腦病毒在流行過後仍有復發機會的投影片 集點卡
評量	1. 設計幾個雙副檔名，讓同學勾選是否爲病毒常利用的僞裝手法。 2. 請同學描述區域網路中毒後的解毒流程。	4’	學習單

四、廣義電腦病毒課程設計

<table>
<tr><th colspan="4">課　程　設　計</th></tr>
<tr><td>主題</td><td>電腦病毒概念課程</td><td>單元</td><td>廣義電腦病毒</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>4</td></tr>
<tr><td>目標</td><td colspan="3">1. 認識電腦蠕蟲
2. 認識特洛伊木馬
3. 認識謠言病毒</td></tr>
<tr><td>階段</td><td>教學步驟</td><td>時間</td><td>教學資源</td></tr>
<tr><td>呈現學習目標</td><td>【活動 1】利用電腦病毒的概念圖說明本節課的主要概念。

【活動 2】由老師利用「教學資源 2」說明惡意程式是指對電腦不好的程式，電腦病毒也是惡意程式的一種，但是除了電腦病毒之外還有其他惡意程式。就好比感冒病毒有很多種，分爲 A 型感冒、B 型感冒等等，雖然都是感冒，但是如果診斷錯誤，可能會讓身體受到傷害。</td><td>3’</td><td>1.利用投影片呈現電腦病毒概念圖，並標示本節所要講述的行爲特性概念。

2.說明電腦病毒與電腦蠕蟲、特洛依木馬是不一樣的惡意程式的投影片</td></tr>
<tr><td>目標 1：認識電腦蠕蟲</td><td>【活動 1】由教師說明什麼是電腦蠕蟲，利用蟲的特性「爬」，讓學生了解蠕蟲的具體概念。
活動說明：
(1) 教師利用投影機播放「教學資源 3」說明蠕蟲可以自己在網路裡遊走，不需要附著在檔案裡，蠕蟲最大的破壞力是讓網路運作緩慢。</td><td>8’</td><td>3.說明電腦蠕蟲傳播方法與破壞行爲的投影片。</td></tr>
</table>

	【活動 2】顯示電腦病毒與蠕蟲的差異表。 活動說明：利用投影機顯示「教學資源 4」來說明兩者的差異是蠕蟲不會感染檔案，而兩者相同之處是都不需經過使用者同意就可以侵入電腦與破壞檔案。 【活動 4】請同學想一想兩者解毒方法的差異，並由教師利用「教學資源 5」說明偵測到蠕蟲可以直接刪除掉；而偵測到電腦病毒則需要解毒，把病毒程式從檔案上移除，留下原本的檔案。		4 利用投影片顯示電腦病毒與蠕蟲的差異表 5.電腦蠕蟲與電腦病毒解毒方法的投影片
目標 2：認識特洛伊木馬	【活動 1】教師利用「教學資源 6」介紹特洛伊木馬的命名由來，由教師簡易說一下木馬屠城的故事。 【活動 2】教師利用「教學資源 7」說明特洛依木馬是包藏禍心的惡意程式，經常僞裝成有用的工具程式，誘騙使用者下載安裝，進而竊取使用者的私人資料如帳號、信用卡號回傳給木馬作者。 【活動 3】請同學想一想，爲什麼特洛依木馬不採用主動攻擊？這是因爲若大量傳輸資料到木馬作者的電腦中會造成困擾。 【活動 3】顯示病毒與特洛伊木馬的差異。 活動說明： 教師利用投影機顯示「教學資源 8」來說明兩者的差異爲特洛依木馬程式不會感染檔案，是採取被動攻擊手法。而兩者相	8’	6.特洛依木馬命名由來的投影片 7.特洛依木馬傳播方法與破壞行爲的投影片 集點卡 8.病毒與木馬的差異表的投影

	同之處爲都可以不需經過使用者同意就植入電腦或破壞系統。 【活動 4】請同學想一想兩者解毒方法的差異，並由教師利用「教學資源 9」說明偵測到木馬可以直接刪除掉；而偵測到電腦病毒則需要解毒，把病毒程式從檔案上移除，留下原本的檔案。 【活動 5】教師利用「教學資源 10」說明三者的相同點爲都不需經過使用者同意就可以植入電腦與執行破壞行爲；而三者最大的差異爲木馬和蠕蟲不會感染檔案，電腦病毒會感染檔案。		片 9.木馬與電腦病毒解毒方法的投影片 10.電腦病毒、蠕蟲、木馬三者的異同投影片
個人競賽	【活動 1】利用搶答使學生能區分電腦病毒、蠕蟲、木馬三者間的不同。 活動說明： (1) 依序呈現投影片中條列的特性(教學資源 11)，讓學童舉手回答判斷是病毒、蠕蟲或是木馬的特性。	10’	11.三種惡意程式特性的投影片 集點卡
目標 3：認識謠言病毒	【活動 1】認識謠言病毒的特色與處理 活動說明： (1) 教師利用「教學資源 12」說明謠言病毒利用人類懷疑、恐懼、好奇的心理，發送內容不實的郵件，造成收件者的恐慌，可能造成大量傳播或聽任謠言作者的指示去刪除檔案，或做了破壞電腦的行爲。並說明謠言信內容的常見字爲通知所有人、權威公司說、非	8’	12.謠言信的傳播手法與破壞行爲，以及信件特色的投影片

	常危險！、別開啓、硬碟會被完全摧毀等。 (2) 由教師呈現幾封謠言信「教學資源 13」，與謠言病毒的手法與特性相互對應。 (3) 教師利用「教學資源 14」說明謠言信的處理方法爲不可聽信信件內容而隨意刪除檔案或轉寄他人，需利用謠言信查詢網站或轉寄給防毒公司檢測真實性。 (4) 介紹可以查詢謠言信的網址「教學資源 16」，並由教師演示查詢幾封謠言信件。		13.謠言病毒信件數封 14.謠言信處理方法的投影片 16.查詢謠言信網址的投影片 www.ettoday.com.tw
評量	(1) 請寫出電腦病毒、電腦蠕蟲、特洛依木馬的相同點。 (2) 請寫出「電腦病毒」與「電腦蠕蟲、特洛依木馬」的差異。 (3) 請寫出一項電腦蠕蟲的破壞行爲。 (4) 請寫出特洛依木馬是如何傳播的 (5) 收到謠言信該如何處理。	3	學習單

五、防毒策略課程設計

課　程　設　計			
主題	電腦病毒概念課程	單元	防毒策略
教師	梁雅琇	節次	5
目標	1.了解個人防毒的方法 2.能操作防毒軟體程式 3.中毒後的處理方法		
階段	教學步驟	時間	教學資源
呈現單元目標	【活動 1】利用電腦病毒的概念圖說明本節課的主要概念。 【活動 2】請曾經中過毒的同學分享中毒的處理方法，以及請同學分享平時如何保護電腦。	5’	1.利用投影片呈現電腦病毒概念圖，並標示本節所要講述的行爲特性概念。 集點卡
目標 1：了解個人防毒的方法	【活動 1】由老師教授電腦設定密碼之方法。 活動說明： (1) 由教師利用「教學資源 2」說明密碼設定的技巧爲混合數字、小寫字母、大寫字母及符號，並建議密碼長度爲爲 8 個字元，例如例如：~acDC$27。 (2) 由教師說明盡量避免以個人身分證號碼、生日、電話爲密碼，並且定期更換密碼。 【活動 2】呈現其它個人防毒的方法。 活動說明： (1) 利用投影機顯示「教學資源 3」來說明其他防毒策略，如隨時備份、執行檔案前先掃毒、共享目錄設密碼、不開啓不明的電子郵件、定期更新系統漏洞與病毒	7’	2.　密碼設定技巧的投影片 3.其他防毒策略的投影片

	碼、不隨意下載非法軟體安裝。		
目標 2：能操作防毒軟體程式	【活動 1】防毒軟體使用事項 活動說明： (1)教師利用投影機顯示「教學資源 4」，分條說明使用防毒軟體的注意事項，如不論有無上網都需安裝防毒軟體，購買防毒軟體後有解讀上的困難要諮詢該公司、並且定期的更新才能讓防毒軟體效用增加。教師並指出，安裝防毒軟體不能保證完全受到保護，因爲病毒更新速度快，所以做好個人防護是最重要的。 【活動 2】說明防毒軟體的掃解毒模式 活動說明： (1)教師利用「教學資源 5」說明防毒軟體修復、刪除、隔離的掃解毒模式意義。 【活動 3】教導學生看病毒碼的更新日期。 【活動 4】由教師演示防毒軟體掃解毒實際操作 活動說明： (1)開啓防毒軟體，掃描病毒檔目錄「教學資源 6」，讓學生實際體驗偵測到病毒的狀況，並呈現隔離與刪除的解毒模式。	10’	4.製做防毒軟體注意事項投影片 5.防毒軟體掃解毒模式的投影片 6.病毒檔目錄。
目標 3：中毒後的處理方法	【活動 1】了解中毒處理流程 活動說明： (1) 教師利用「教學資源 7」說明中毒後要因應不同的狀況來處理，流程可以因狀況而互換程序，呈現感染破壞力強	15’	7.中毒處理流程

	大的病毒時必須盡快關機→將硬碟交由專家處理；而懷疑有病毒時則必須確認病毒碼為最新才能進行掃毒，並查詢病毒資訊，若為系統漏洞型病毒，則需修補漏洞，才得以解毒成功。 (2) 由教師說明，掃毒時建議在安全模式進行，說明開機後按壓 F8 即可僅入安全模式。 【活動 2】補充說明中毒後不應該有的行為。 活動說明： (1) 教師利用「教學資源 8」，呈現中毒後錯誤的行為，如到別台執行中毒電腦裡的檔案、中毒只要重新安裝系統就可以了、馬上刪除自己以為是病毒的檔案，並分別加以說明。 【活動 3】如何檢查電腦中是否有電腦病毒檔案。 活動說明： 1. 呈現隨身碟蠕蟲的資訊。 2. 執行程式(教學資源 9,10)模擬隨身碟蠕蟲的行為。 (1) 複製蠕蟲檔案 inetsrv.exe 至系統 windows 目錄。 (2) 修改系統登錄檔使每次開機即啓動檔案。 (3) 當讀取隨身碟時，即將病毒植入隨身碟中的 recycled 目錄。 3. 教師演示檢查流程。		投影片 8.錯誤的中毒處理行為投影片 9.撰寫程式 copy.exe 將模擬的病毒檔 inetsrv.exe 複製到’windows 目錄。 10.設計登錄檔 copy.reg，使執行後將病毒行為寫入登入檔

	4. 學生實際操作尋找病毒的流程。		中。
評量	1. 請你寫出一組安全性高的密碼(長度 8-10 個字元)。 2. 利用防毒軟體將磁片中「病毒檔」目錄下的病毒刪除，並說明「刪除」的意思。 3. 請你寫出電腦疑似中毒時該如何處理？	3’	學習單


NTTU Library

附錄五 學習單(實驗組 1)

一、電腦病毒基本原則學習單

單元 1 學習單

座號：_____ 姓名：_____

1. 請寫出構成電腦病毒的必要原則是什麼，並簡單說明？

_____

_____

2. 請寫出電腦病毒的四種類型。

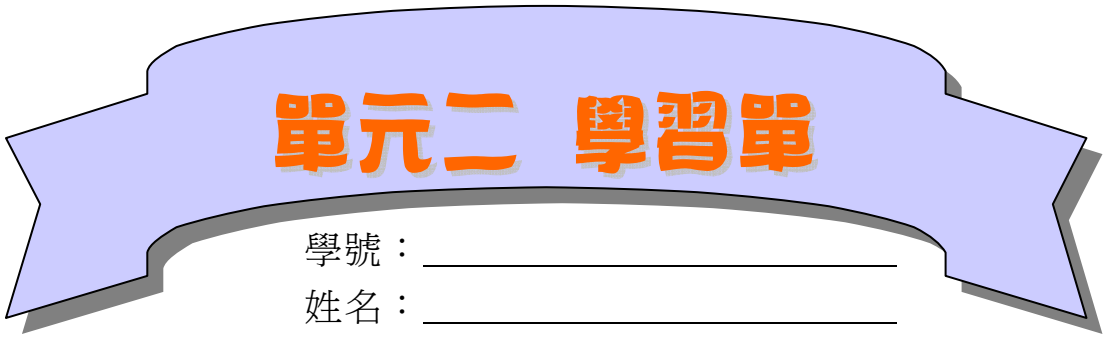
_____ _____

_____ _____

3. 請你開啓教學磁片內的「檔案格式」目錄，執行每一個檔案，並紀錄執行的檔案名稱(必須含副檔名，例如病毒.exe)以及紀錄執行後出現的訊息。

	檔案名稱(含副檔名)	訊息顯示
❶	_____	_____
❷	_____	_____
❸	_____	_____
❹	_____	_____
❺	_____	_____
❻	_____	_____

二、電腦病毒行爲特性 I 學習單



1. 請寫出至少三項電腦病毒的傳播途徑

2. 請寫出至少三項電腦病毒的破壞行爲

3. 請描述電腦病毒的潛伏期定義

4. 請寫出至少二項人類病毒與電腦病毒相同的地方

三、電腦病毒行爲特性 II 學習單

單元3 學習單

學號：_____

姓名：_____

1. 請記錄雙副檔名目錄中所有檔案的完整名稱，以及執行後的訊息。

檔案名稱	訊息

2. 請選擇病毒經常使用電子郵件附加檔格格式，在☐中打勾。

☐ 火影人者卡通.scr
☐ 火影人者卡通.txt .exe
☐ 跑跑卡丁車.txt.exe
☐ 跑跑卡丁車.vbs
☐ 真珠美人魚桌布.jpg .vbs
☐ 真珠美人魚桌布.vbs.txt
☐ 水族箱螢幕保護程式.scr .txt

四、廣義電腦病毒學習單

...單元1 學習單...

1. 請寫出電腦病毒、電腦蠕蟲、特洛依木馬的相同點。

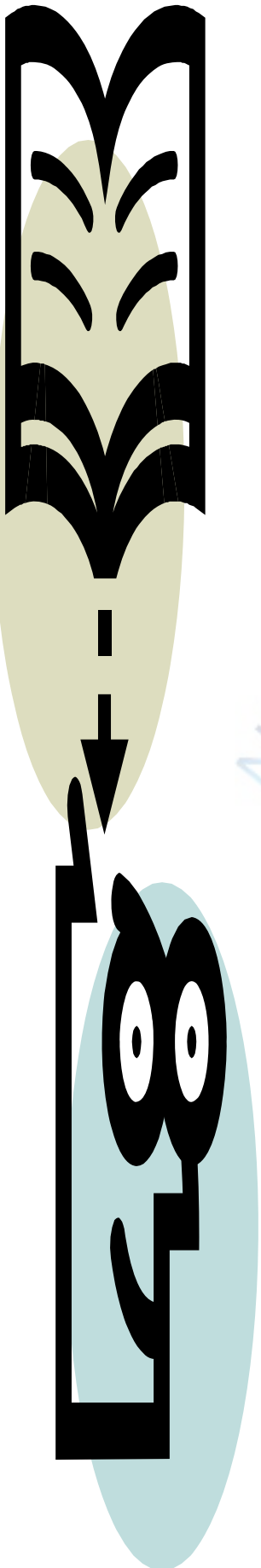
2. 請寫出「電腦病毒」與「電腦蠕蟲、特洛依木馬」的差異。

3. 請寫出一項電腦蠕蟲的破壞行爲。

4. 請寫出特洛依木馬是如何傳播的。

5. 收到謠言信該如何處理。

五、防毒策略學習單



單元5 學習單

學號：_____

姓名：_____

1. 請你寫出一組安全性高的密碼(長度 8-10 個字元)。

_____

2. 利用防毒軟體將磁片中「病毒檔」目錄下的病毒刪除，並說明「刪除」的意思。

_____

3. 請你寫出電腦疑似中毒時該如何處理？

_____

_____

_____

_____

_____


NTTU Library

附錄六 電腦病毒推廣教材(實驗組 2)

一、電腦病毒初體驗

<table>
<tr><td colspan="6">課 程 設 計</td></tr>
<tr><td>主題</td><td>電腦病毒課程</td><td>單元</td><td colspan="3">電腦病毒初體驗</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>1</td><td>時間</td><td>40 分鐘</td></tr>
<tr><td>教學
目標</td><td colspan="5">6. 了解電腦病毒的危害物。
7. 電腦病毒與垃圾郵件的防範方法。
8. 了解有害資訊出現的原因。
9. 瞭解傳統電腦病毒的定義</td></tr>
<tr><td>活動目標</td><td colspan="3">教學活動</td><td>時間</td><td>教學資源</td></tr>
<tr><td>引起動機</td><td colspan="3">【活動 1】一開始不說明課程內容，先播放一段影片讓學生欣賞。讓學生發表他觀賞後的想法。
活動說明：影片內容如下：
1.「系統中毒了！無法清除、無法隔離」
2.「系統怎麼慢的可以.....」
3.「系統 60 秒到數計時關機中....」
4.「真的有駭客入侵我的電腦嗎？」
5.「最近有人傳說上網會被盜取系統資料，真的嗎？」
6.「一堆垃圾郵件煩死了！」
7.「資訊安全不是系統管理人員的事嗎？與我有關嗎？」</td><td>2’</td><td>1.投影片(製成影片檔)內容配上凝重音效。</td></tr>
<tr><td>目標 1-1：了解網路的危害物</td><td colspan="3">【活動 1】由教師詢問學生這部影片描述了哪些事件，請同學發表。
活動說明：
(1) 請同學針對影片說明網路上有哪些會危害電腦的事物，並說明他們對電腦病毒的定義。
(2) 除了影片上的危害物外，你還有</td><td>8’</td><td>2.將同學所述及的資訊記錄在黑板上。
集點卡</td></tr>
</table>

	聽過哪些？ (3) 請同學針對影片說明這些危險的事物對於電腦的破壞行爲什麼。 (4) 請同學分享當自己的電腦安全受到威脅時的處理程序。 (5) 由教師提供自己的中毒解驗。		
目標 1-2：學習電腦病毒與垃圾郵件的防範方法	【活動 1】由教師說明要防範電腦病毒與垃圾郵件的基本能力。 活動說明： (1) 利用投影機播放「教學資源 3」，說明防範電腦病毒應具備的能力。 (2) 介紹市售與免費的防毒軟體。 (3) 利用投影機播放「教學資源 4」，說明防範垃圾郵件應具備的能力。 (4) 介紹垃圾郵件的軟體與免費過濾垃圾信的網站，呈現過濾垃圾信件的畫面。	8’	3.防範電腦病毒的投影片 4. 防範垃圾郵件的投影片
目標 1-3：說明有害資訊出現的原因	【活動 1】教師說明有線網路與無線網路，這些通訊發達的建設，讓人們溝通與取得資訊容易與迅速，是造成不當資訊流傳的主因。 活動說明： (1) 利用投影機播放「教學資源 5」，說明不當資訊流傳的原因。 (2)請同學想一想，除了發達的網路機制外，還有哪些可能的原因。 (3)利用投影機播放「教學資源 6」，呈現更多的可能原因。	5’	5.不當資訊快速流傳的主因投影片。 6.更多可能的原因投影片，如「作業系統的普及」、「資訊安全(防毒、妨害)的能力與推廣不足」 、「使用 E-mail

			隨意的轉寄信件」 集點卡
目標 1-3：傳統電腦病毒的定義	【活動 1】由教師講述傳統電腦病毒的定義。 活動說明： (1) 呈現傳統電腦病毒定義的投影片「教學資源 7」，說明電腦病毒是指會將本身程式碼複製到其他檔案或開機區的程式會干擾電腦運作。會在某特定時期發作，輕者影響電腦運作，重者破壞電腦裡的資料。 (2) 呈現 Hybris 病毒發作時佔據桌面的黑色漩渦狀圖形。 【活動 2】利用電腦病毒的案例加強電腦病毒定義概念並說明電腦病毒的類型。 (1) 教師利用「教學資源 8」舉例說明，如首隻電腦病毒 Brain 感染 ms-dos 開機區爲開機型病毒、Taiwan No.1 專攻 word 檔爲巨集病毒、CIH 電腦病毒每月 26 日格式化硬碟病感染執行檔爲檔案型病毒。	10’	7.傳統電腦病毒定義投影片。 Hybris 黑色漩渦狀動畫檔 8.以投影片呈現 Brain，TaiwanNo 1、CIH 病毒介紹
評量	1. 至少寫出三項網路上有哪些惡意程	5’	

	式。 2. 哪些因素讓惡性程式(電腦病毒、木馬程式或是電腦蠕蟲)，能快速散播？ 3. 寫出影片中惡意程式有哪些破壞行爲。 4.寫描述電腦病毒是什麼？		學習單

二、 惡意程式的定義

課　程　設　計					
主題	電腦病毒課程	單元	惡意程式的定義		
教師	梁雅琇	節次	2	時間	40 分鐘
教學目標	1. 瞭解新型態電腦病毒的定義 2. 瞭解垃圾郵件的定義 3. 瞭解網路謠言的定義				
活動目標	教學活動		時間	教學資源	
引起動機	【活動 1】請同學說說電腦病毒是什麼。		3’	集點卡	
目標 2-2：特洛依木馬	【活動 1】由教師講述特洛依病毒的定義 活動說明： (1) 教師利用投影片「教學資源 4」講解特洛伊木馬不像病毒一樣會感染其他檔案，木馬程式會將自己僞裝成一些特殊的工具來吸引使用者下載並執行。或是電腦駭客直接入侵電腦主機將惡性程式植入對方系統以破壞或竊取重要資料(如格式化磁碟、刪除檔案、竊取密碼)。 (2) 舉例說明，例如 Keylogger 木馬程式，會記錄使用者按哪些鍵(鍵盤側錄)，駭客便有機會竊取機密資料。		7’	4.特洛伊木馬定義的投影片。	

目標 2-3：電腦蠕蟲	【活動 1】由教師介紹電腦蠕蟲的定義 (1) 教師利用投影片「教學資源 5」講解電腦蠕蟲的定義，電腦蠕蟲不會感染其他檔案，但會複製很多”分身”，像蟲一般在網路中游走，最常使用的方法是透過區域網路的資料夾分享或是網際網路 E-mail 來散佈自己。 (2) 舉例說明，如 VBS_Loveletter(情書)就是利用 E-mail 大量發信。	7’	5.電腦蠕蟲定義的投影片。 7.以投影片呈現 Loveletter 蠕蟲的行爲
目標 2-4：惡意程式	【活動 1】由教師講述惡意程式是指電腦蠕蟲、特洛伊木馬，近期則是三者間的相互融合。 活動說明： (1) 教師利用「教學資源 8」說明三個惡意程式混合會帶來更大的影響。 (2) 利用例子說明混合病毒的攻擊行爲。	5’	8.混合的惡意程式投影片
目標 1-3：說明垃圾郵件的定義	【活動 1】教師講解垃圾郵件的定義 活動說明： (1) 教師利用投影片「教學資源 8」講解垃圾郵件是指將一份內容相同的電子郵件，大量寄給不同的人，且未經收信人許可，郵件內容多數是與收信人不相干的商業廣告。常會造成網路擁塞，郵件伺服次主機負擔過重，收信人必須花費金錢和時間去處理這些信件 (2) 教師蒐集一些垃圾郵件的例子於課程中呈現，與定義相互對應。	5’	8.垃圾郵件定義投影片 9.垃圾郵件的實際例子*3

目標 1-4：說明網路謠言的定義、特性與種類	【活動 1】教師講解網路謠言的定義 活動說明： (1) 教師利用投影片「教學資源 10」講解網路謠言定義爲透過電子佈告欄、新聞討論群、留言版或電子郵件散布未經證實或惡意中傷的言論，製造恐懼、傳播自殘思想或是道德教訓等等，也有的單純只爲惡作劇。因散播快且廣，對於網路族群中人際關係差或心智未成熟者常造成不安與焦慮。 【活動 2】教師講解網路謠言的特性 活動說明： (1) 教師利用投影片「教學資源 11」講解網路謠言特性，並舉例讓學生找出該信件中符合謠言的地方。 【活動 3】教師講解網路謠言的種類 活動說明： (1) 教師利用投影片「教學資源 12」講解網路謠言的 5 種類型，分別爲恐怖型、圖謀不軌型、病毒警告型、憐憫型 、好運多多型。 (2) 教師呈現真實的謠言信件(教學資源 13)。 (3) 例用投影片子，讓學生舉手配對。	10’	10.網路謠言定義的投影片 11.網路謠言特性與實際案例。 集點卡 12.網路謠言種類的投影片 13.蒐集五種不同類型的謠言信件 集點卡
評量	1.電腦病毒和「木馬、電腦蠕蟲」有什麼不同？ 2.請寫出特洛依木馬是如何傳播的。 3.電腦蠕蟲常用的傳播手法。	3’	學習單

三、電腦病毒傳播途徑

<table>
<tr><td colspan="6">課　程　設　計</td></tr>
<tr><td>主題</td><td>電腦病毒課程</td><td>單元</td><td colspan="3">電腦病毒傳播途徑</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>3</td><td>時間</td><td>40 分鐘</td></tr>
<tr><td>教學
目標</td><td colspan="5">1. 了解電腦病毒的傳播途徑
2. 了解電腦病毒常用的偽裝術
3. 能判斷可信任的電子郵件</td></tr>
<tr><td>活動目標</td><td colspan="3">教學活動</td><td>時間</td><td>教學資源</td></tr>
<tr><td>引起動機</td><td colspan="3">【活動 1】請同學發表他們所知道的病毒傳染途徑。
活動說明：
(1) 隨機抽取班上 3 位學生發表。</td><td>3’</td><td></td></tr>
<tr><td>目標 4-1：了解電腦病毒的傳播途徑</td><td colspan="3">【活動 1】由教師講述電腦病毒的傳播途徑。
活動說明：
(1) 教師利用投影片「教學資源 1」解說電腦病毒常用的傳染管道，並列舉病毒實例加以佐證，如：
① 傳統的磁片
② 網路上檔案的流通
③ 以合法管道進行非法存取
④ 作業系統漏洞
⑤ 閱讀或預覽電子郵件
⑥ 藉由電子郵件主動散播
⑦ 瀏覽器檢視 HTML 網頁中毒</td><td>10’</td><td>1.電腦病毒傳染途徑與病毒實例投影片</td></tr>
</table>

目標 4-2：了解電腦病毒常用的偽裝術	【活動 1】由教師說明電腦病毒常使用的偽裝技巧。 活動說明： (1) 教師利用投影片「教學資源 2」呈現各種偽裝技巧，如 ① 惡性程式偽裝成重要通知或有趣遊戲美麗圖片等引誘下載。 ② E-Mail 修正程式，請執行〝更新程式.EXE〞 ③ 有趣、好看或色情網頁文件圖片 ④ 防毒公司寄發的「解毒程式.exe」 ⑤ 銀行或卡務中心寄發的「信用卡確認程式.exe」 (2) 爲增加學生的印象，教師收集上述偽裝技巧的病毒資訊「教學資源 3」	10’	2. 電腦病毒偽裝技巧的投影片 3.呈現各式偽裝技巧的病毒資訊
目標 4-3：能判斷可信任的電子郵件	【活動 1】由教師說明判斷電子郵件是否安全方法： 活動說明： (1) 發給同學每人一份判斷電子郵件是否可信任的檢查表。 (2) 教師利用投影片「教學資源 4」逐項說明檢查表中所代表的意義。 (3) 教師說明如果你不確定收到的電子郵件是否足以信任，請勿開啓它，更不要回覆它。開啓郵件之前先讓防毒程式掃描附件。	10’	4.電子郵件可信賴度檢查表的投影片。
評量	1.寫出至少三項電腦病毒傳播途徑。 2.寫出至少三種病毒常用的偽裝技巧。 3.寫出至少二項不值得信任的電子郵件具備的條件。	7’	學習單

四、 電腦病毒的預防與處理

<table>
<tr><td colspan="6">課 程 設 計</td></tr>
<tr><td>主題</td><td>電腦病毒課程</td><td>單元</td><td colspan="3">電腦病毒的預防與處理</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>4</td><td>時間</td><td>40 分鐘</td></tr>
<tr><td>教學
目標</td><td colspan="5">1. 了解電腦病毒的預防之道。
2. 了解感染病毒後的處理流程。
3. 了解網路謠言的處理方法。
4. 了解郵件管理的方法。</td></tr>
<tr><td>活動目標</td><td colspan="3">教學活動</td><td>時間</td><td>教學資源</td></tr>
<tr><td>引起動機</td><td colspan="3">(1) 利用網路上所教授的方法「
告訴大家一個訊息，就是在"通訊錄"新增一個名字"!0000"(驚嘆號和四個零)，然後不要設 mail address 那些有的沒有的，要打在名字欄打上"!0000"這個名字，這樣當自己不小心中毒的話，就不會害到自己的"親朋好友"了!!
因爲"!0000"他會在連絡人的最上方 show 出來，當病毒在尋找你的好友名單時，第一筆會找到這個名字，因爲找不到 mail address 寄不出去，這樣就會停止散播病毒了!!請各位告訴各位親朋好友囉!!」
(2)讓學生想一想，這樣的防治方法究竟有沒有效呢？</td><td>5’</td><td>1.印給大家這個預防方法的文件</td></tr>
<tr><td>目標 3-1：
了解電腦病毒的預防之道</td><td colspan="3">【活動 1】由教師說明要預防病毒的法則。
活動說明：
(1)由教師利用投影片「教學資源 1」呈現預防病毒的方法，如加快病毒碼自動更新的頻率，並即時下載更新掃毒引擎程式才是上策、關閉電子郵件預覽視窗，不要開啓來路不明的電子郵件，或者安裝郵件病毒掃描程式、設</td><td>10’</td><td>1.預防電腦病毒方法的投影片</td></tr>
</table>

	定作業系統自動更新修補通知，接獲通知後立即下載作業系統修補程式，防止病毒利用系統漏洞入侵等。 (2)由教師演示關閉電子郵件預覽視窗以及系統更新的方法。		
目標 3-2：了解感染病毒後的處理流程	【活動 1】同學分享中毒處理方法，後由教師說明感染病毒後的處理流程。 活動說明： (1)由曾經感染病毒的同學發表中毒後的處理方法爲何。 (2)教師利用投影片「教學資源 2」說明中毒後的處理流程，流程如下： ① 要立即到資訊安全公司的網站下載最新病毒碼或掃毒引擎程式。 ② 清除電腦上的病毒。 ③ 更新作業系統安全漏洞。 ④ 若仍無法清除病毒，儘可能在不連接網路情形重灌系統。 (3)由教師說明這些流程必須依照不同的病毒有所改變。	8’	集點卡 2.中毒處理流程的投影片
目標 3-3：了解網路謠言的處理方法。	【活動 1】由教師介紹一些查詢網路謠言的網站。 活動說明： (1) 由教師先說明當你收到或看到某些議題，需要多方探討、多問問對相關言論有研究的人；若無法查證議題的真僞，不應再散佈出去。 (2) 利用投影片「教學資源 3」顯示可以查詢網路謠言的網站。 網路追追追：	10’	3.網路謠言查詢網站的投影片。

	http://www.ettoday.com/etrumor/index.htm 中華民國網路消費協會： http://www.net080.com.tw/chhtml/index.asp (3)點選幾封同學有興趣的謠言來說明。		
目標 3-4：了解郵件管理的方法	【活動 1】垃圾郵件有多少？ 活動說明： (1) 讓同學以一排爲單位，猜測 2004 年全球流通的電子郵件中有多少比例是垃圾郵件。答案是 74%。 【活動 2】由教師說明如何管理郵件。 活動說明： (1) 教師利用投影片呈現「教學資源 3」說明郵件管理的方法。 ① 拒收無主郵件 ② 過濾特定郵件 ③ 使用郵件遠端管理：利用金帥公司提供的郵件航站進行演示說明。	10’	集點卡 3.郵件管理方法的投影片 金帥郵件航站： http://www.mailobby.com.tw/
評量	1. 請寫出至少三項預防病毒的方法。 2. 簡易描述中毒的處理流程。 3. 寫出收到謠言信件的處理方法。	4’	學習單

五、電腦病毒相關查詢網站

<table>
<tr><td colspan="6">課　程　設　計</td></tr>
<tr><td>主題</td><td>電腦病毒課程</td><td>單元</td><td colspan="3">電腦病毒相關查詢網站</td></tr>
<tr><td>教師</td><td>梁雅琇</td><td>節次</td><td>5</td><td>時間</td><td>40 分鐘</td></tr>
<tr><td>教學
目標</td><td colspan="5">1. 利用網路查詢電腦感染病毒後的跡象
2. 能至電腦病毒網站查詢病毒相關知識
3. 能至網路謠言查詢網站尋得問題</td></tr>
<tr><td>活動目標</td><td colspan="2">教學活動</td><td>時間</td><td colspan="2">教學資源</td></tr>
<tr><td>引起動機</td><td colspan="2">【活動 1】利用防毒軟體網站或資訊安全相關網站查詢病毒的方法。
活動說明：
(1) 教師說明查詢病毒時的關鍵字。
例如：狀況 + 病毒
“自動關機 病毒”。
可疑檔案名稱 + 病毒
“kks.exe 病毒”</td><td>5’</td><td colspan="2"></td></tr>
<tr><td>目標 5-1：
了解電腦感染病毒後的跡象</td><td colspan="2">【活動 1】由教師提供一些電腦病毒教學的網址，讓學生自行探究。
活動說明：
(1) 教師利用投影片「教學資源 3」呈現電腦病毒教學網站，如。全民 e 起來 電腦病毒概念網：http://www.totematncu.net/virus/virus/virus_index.htm。認識電腦病毒：http://content.edu.tw/junior/computer/tp_ct/content7-b10.htm
(2) 由學生自行閱讀，紀錄電腦感染病毒後可能會產生的跡象於學習單上。
(3) 學生分享病毒的破壞行爲。</td><td>10’</td><td colspan="2">3.電腦病毒教學網站的投影片
學習單
集點卡</td></tr>
<tr><td>目標 5-2：</td><td colspan="2">【活動 1】由教師提供防毒軟體網址，</td><td>10’</td><td colspan="2"></td></tr>
</table>

能至電腦病毒網站查詢病毒相關知識	學生進行探索。 活動說明： (1) 教師利用投影片「教學資源 1」呈現防毒軟體網站的網址，趨勢防毒：www.trend.com.tw。諾頓防毒：www.symantec.com。金帥防毒：www.ggreat.com.tw。查不到時利用 Google 查詢：www.google.com (2) 教師指派學生查詢「疾風 Blaster」病毒資料，寫在學習單上		1.防毒軟體網站的投影片。 學習單 集點卡
目標 5-3：能至網路謠言查詢網站尋得問題	【活動 1】由教師提供網路謠言查詢的網址，讓學生進行探索。 活動說明： (1) 教師利用投影片「教學資源 2」呈現網路謠言查詢網址，如網路追追追：http://www.ettoday.com/etrumor/index.htm。中華民國網路消費協會：http://www.net080.com.tw/chhtml/index.asp (2) 由學生任選一篇謠言信，紀錄於學習單，說明此封信為謠言病毒的哪一個種類。	10’	2. 謠言信查詢網站的投影片 學習單
評量	1.請勾選電腦病毒會產生的破壞行為。	5’	學習單


NTTU Library

附錄七 學習單(實驗組 2)

單元 1 學習單

座號：_____ 姓名：_____

1. 至少寫出三項網路上有哪些惡意程式

_____

_____

2. 哪些因素讓惡性程式能快速散播？

_____

_____

_____

3. 寫出影片中惡意程式有哪些破壞行爲？

_____

_____

_____

_____

4. 寫描述電腦病毒是什麼？

_____

_____

單元二 學習單

學號：_____

姓名：_____

1. 電腦病毒和「木馬、電腦蠕蟲」有什麼不同？

_____

_____

_____

2. 請寫出特洛依木馬的傳播手法。

_____

_____

_____

3. 請寫出電腦蠕蟲常用的傳播手法

_____

_____

_____

單元3 學習單

學號：_____

姓名：_____

1. 寫出至少三項電腦病毒傳播途徑。

_____

_____

_____

2. 寫出至少三種病毒常用的偽裝技巧。

_____

_____

_____

3. 寫出至少二項不值得信任的電子郵件具備的條件

_____

_____

_____

...單元4 學習單...

1. 請寫出至少三項預防病毒的方法。

2. 簡易描述中毒的處理流程。

3. 寫出收到謠言信件的處理方法。

單元5 學習單

1. 紀錄電腦感染病毒後會產生的破壞行為。

_____

_____

_____

2. ☐ 疾風 Blaster 或(Msblast)病毒資料

☐ Iloveyou 或(Yaha)病毒資料

類型： ☐病毒(virus) ☐蠕蟲(worm) ☐木馬(Trojan)

傳播方法：

☐ 電子郵件

主旨：_____

附加檔案：_____

☐ 系統漏洞

解毒方法：

_____

_____

3. 請你簡單介紹一封謠言信，描述是什麼類型的謠言性質。

介紹：_____

_____

_____

謠言類型：_____

_____

處理方法：_____


NTTU Library

附錄八 預試試卷項目分析表

預試 1						預試 2					
題號	難度指數	鑑別度	誘答力			題號	難度指數	鑑別度	誘答力		
			選項	高分組	低分組				選項	高分組	低分組
				答對人數	答對人數					答對人數	答對人數
Q1-1	13.21%	11.32%	1			Q1-1	39.75%	12.9%	1	1	2
			2						2	6	7
			3						3	14	17
			4						4	18	13
Q1-2	0.00%	0.00%	1			Q1-2	38.45%	5.1%	1	9	13
			2						2	3	3
			3						3	16	14
			4						4	11	9
Q1-3	4.72%	1.89%	1			Q1-3	10.25%	-5.1%	1	3	5
			2						2	22	22
			3						3	5	1
			4						4	9	11
Q1-4	6.60%	5.66%	1			Q1-4	17.95%	5.1%	1	26	19
			2						2	8	6
			3						3	4	7
			4						4	1	6
Q2	15.09%	18.87%	1	12	12	Q2	26.95%	38.5%	1	13	30
			2	13	3				2	18	3
			3	2	9				3	1	0
			4	25	28				4	7	6
Q3	20.75%	3.77%	1	14	12	Q3	58.45%	55.3%	1	2	4
			2	12	10				2	2	13
			3	1	3				3	32	12
			4	25	27				4	3	10
Q4	62.26%	52.83%	1	47	19	Q4	57.7%	38.4%	1	30	15
			2	0	6				2	0	3
			3	0	3				3	0	3
			4	6	25				4	9	18
Q5	70.75%	20.75%	1	0	1				1		
			2	43	32				2		
			3	2	10				3		
			4	8	10				4		
Q6	32.08%	37.74%	1	2	12	Q5	57.7%	33.4%	1	2	1
			2	23	27				2	8	18
			3	1	7				3	0	4
			4	27	7				4	29	16
Q7	31.13%	5.66%	1	4	7	Q16	19.25%	-7.7%	1	21	16
			2	19	16				2	6	5
			3	18	15				3	6	9
			4	10	15				4	6	8
Q8	66.98%	35.85%	1	4	16	Q6	76.9%	38.5%	1	6	15
			2	45	26				2	30	15
			3	2	2				3	1	5

			4	2	8				4	2	4
Q9	48.11%	20.75%	1	6	7	Q7	46.2%	28.2%	1	3	3
			2	5	17				2	3	9
			3	31	20				3	15	16
			4	11	8				4	18	11
Q10	53.77%	39.62%	1	7	8	Q8	75.65%	33.3%	1	1	4
			2	2	3				2	0	4
			3	4	24				3	2	7
			4	39	18				4	36	23
Q11	77.36%	30.19%	1	1	4	Q9	86.4%	15.4%	1	1	3
			2	1	8				2	2	1
			3	49	33				3	36	30
			4	2	8				4	0	5
Q12	72.64%	39.62%	1	3	10	Q10	73.05%	38.5%	1	2	14
			2	49	28				2	36	21
			3	0	7				3	1	1
			4	1	8				4	0	3
Q13	33.96%	0.00%	1	33	25	Q11	66.7%	41%	1	1	5
			2	1	7				2	2	6
			3	18	18				3	2	9
			4	1	2				4	34	18
Q14	60.38%	37.74%	1	9	20	Q12	58.95%	51.3%	1	4	16
			2	1	4				2	1	8
			3	42	22				3	33	13
			4	1	7				4	1	2
Q15	13.21%	-18.87 %	1	18	16	Q13	15.35%	5.1%	1	4	7
			2	10	8				2	7	5
			3	2	12				3	0	6
			4	23	17				4	28	21
Q16	57.55%	43.40%	1	1	7	Q14	73.8%	24.6%	1	0	0
			2	1	11				2	0	2
			3	42	19				3	32	24
			4	9	14				4	7	13
Q17	64.15%	41.51%	1	6	10	Q15	65.4%	53.8%	1	3	15
			2	1	13				2	0	6
			3	45	23				3	36	15
			4	1	6				4	0	3
Q18	21.70%	-13.21 %	1	8	15	Q17	51.25%	51.3%	1	30	10
			2	32	20				2	8	13
			3	6	6				3	0	6
			4	7	11				4	1	10
Q19	50.94%	79.25%	1	0	11	Q18	61.55%	20.5%	1	1	6
			2	48	6				2	28	20
			3	1	19				3	1	4
			4	4	16				4	9	8
Q20	47.17%	45.28%	1	13	17	Q19	48.75%	35.9%	1	9	11
			2	1	10				2	2	9
			3	2	12				3	2	6
			4	37	13				4	26	12
Q21	78.30%	43.40%	1	0	9	Q20	74.35%	35.7%	1	0	4
			2	53	30				2	35	23
			3	0	5				3	2	7
			4	0	9				4	2	5
Q22	21.70%	13.21%	1	15	8	Q21	34.6%	28.2%	1	19	8

			2	17	19				2	14	22
			3	5	8				3	3	3
			4	16	18				4	3	6
Q23	75.47%	41.51%	1	1	7	Q22	80.75%	33.3%	1	1	6
			2	0	8				2	0	3
			3	1	9				3	0	5
			4	51	29				4	38	25
Q24	21.70%	1.89%	1	9	13	Q23	17.95%	-5.1%	1	15	12
			2	11	9				2	0	8
			3	12	11				3	6	8
			4	20	20				4	18	11
Q25	52.83%	49.06%	1	12	22	Q24	41.05%	51.3%	1	12	14
			2	2	8				2	1	11
			3	1	7				3	0	8
			4	41	15				4	26	6
Q26	54.72%	49.06%	1	8	16	Q25	59%	41%	1	8	7
			2	2	14				2	0	7
			3	1	7				3	0	10
			4	42	16				4	31	15
Q27	29.25%	9.43%	1	18	13	Q26	34.6%	33.4%	1	20	7
			2	6	11				2	6	10
			3	11	17				3	7	13
			4	18	12				4	6	9
Q28	19.81%	-9.43%	1	16	15	Q27	33.3%	15.4%	1	0	6
			2	8	13				2	16	10
			3	11	16				3	11	13
			4	16	9				4	12	10
Q29	30.19%	11.32%	1	7	15	Q28	15.4%	15.4%	1	15	14
			2	9	12				2	4	13
			3	19	13				3	9	3
			4	17	12				4	11	9
Q30	38.68%	24.53%	1	7	13	Q29	46.15%	41.1%	1	3	6
			2	17	15				2	9	17
			3	2	12				3	1	6
			4	27	14				4	26	10
Q31	28.30%	11.32%	1	4	13	Q30	37.2%	43.6%	1	1	13
			2	3	8				2	1	5
			3	18	12				3	23	6
			4	28	20				4	14	15
Q32	65.09%	39.62%	1	0	10	Q31	69.25%	35.9	1	0	6
			2	6	10				2	4	6
			3	45	24				3	34	20
			4	1	9				4	1	7
Q33	48.11%	24.53%	1	6	13	Q32	60.25%	33.3%	1	3	6
			2	32	19				2	30	17
			3	2	7				3	1	6
			4	13	14				4	5	10
Q34	56.60%	49.06%	1	5	9	Q33	58.3%	44.8%	1	1	7
			2	2	9				2	0	6
			3	3	18				3	35	14
			4	43	17				4	3	12
Q35	48.11%	43.40%	1	8	13	Q34	37.15%	23.1%	1	6	14
			2	2	13				2	3	10
			3	37	14				3	19	10
			4	5	13				4	10	5

Q36	27.36%	16.98%	1	12	13	Q35	46.15%	46.1%	1	2	7
			2	11	13				2	5	12
			3	11	17				3	5	11
			4	19	10				4	27	9
Q37 -1	40.57%	28.30%	1	2	6	Q36 -1	57.7%	12.8%	1	0	9
			2	29	14				2	25	20
			3	2	15				3	4	0
			4	19	13				4	10	9
Q37 -2	46.23%	5.66%	1	26	23	Q36 -2	64.15%	35.9%	1	32	18
			2	1	3				2	2	4
			3	12	10				3	3	4
			4	1	4				4	0	7
Q37 -3	48.1%	24.53%	1	1	8	Q36 -3	28.2%	41%	1	0	1
			2	19	18				2	7	8
			3	1	2				3	9	22
			4	32	19				4	19	3