以系統動力學探討電腦病毒防治政策

宋佩貞*
國立中正大學資訊管理學系

古政元
國立中正大學資訊管理學系

陳加屏
國立中正大學企業管理學系

摘要

電腦病毒防治乃是資訊安全政策的核心任務之一，然而現今防範電腦病毒的研究多集中在技術面，在實證研究部份則因資料數據取得困難，故較少探討。為彌補此缺口，本研究採用系統動力學的方法，建立電腦病毒傳播的動態模式，藉以探討用戶端防毒政策的成效。多數研究認為定期更新病毒碼或成立資訊安全事件通報小組，能有效遏止電腦病毒散播，除此之外我們更進一步確認下述現象：(1)電腦接觸外來媒介的頻繁對於電腦病毒感染速率具高度敏感；(2)透過用戶端通報異常狀況存在著時間滯延，因此較不能快速減緩電腦病毒的散播；(3)自動通報機制可以有效控制高峰期的已感染電腦數量並縮短疫情持續時間，故防治效果比較佳；(4)公共衛生政策裡的隔離措施亦可有效抑制電腦病毒的傳播。

關鍵詞：電腦病毒傳播、系統動力學、傳染病散播模型、電腦病毒防治政策

* 本文通訊作者。電子郵件信箱：pcsung@mis.ccu.edu.tw
2011/02/19 投稿；2011/07/18 修訂；2011/10/11 接受

Research of the Computer Viruses Prevention Policy Using System Dynamics

Pei-Chen Sung*
Department of Information Management, National Chung Cheng University

Cheng-Yuan Ku
Department of Information Management, National Chung Cheng University

Chia-Ping Chen
Department of Business Administration, National Chung Cheng University

Abstract

Anti-virus action is the core of information security policy. Many researchers focus on the technology of anti-virus, but not on the anti-virus policies because of the difficulty for obtaining data in empirical research. The research goal of this paper is to explore and evaluate the effectiveness of anti-virus policies by using the System Dynamic Model. Most computer users think that updating the virus pattern files regularly or setting up the security incident reporting team can effectively control the spread of computer viruses. However, the research results of this study indicate: (1) computer virus infection rate is very sensitive to the frequency of contact with other media; (2) relying on the manual reporting mechanism of clients will delay the development of anti-virus vaccine; therefore, this method can slow down the spread of computer virus a little; (3) automatic reporting system can effectively control the number of infected computers and shorten the duration of infection peak; (4) isolation policies can effectively reduce the spread of computer virus.

Keywords: Computer Virus Propagation, System Dynamics, Epidemic Model, Anti-Virus Policy

* Corresponding author. Email: pcsung@mis.ccu.edu.tw
2011/02/19 received; 2011/07/18 revised; 2011/10/11 accepted

壹、緒論

網際網路自 60 年代開始發展，到了 90 年代開放商業及公眾使用後更加蓬勃繁榮，不僅帶動產業、技術與服務的創新，也逐漸改變人們的工作方式與生活習慣。雖然網際網路帶給我們快速與多樣的資訊服務，但也因容易散播電腦病毒而造成令人頭痛的困擾。美國 CSI（Computer Security Institute）曾針對企業、政府、金融機構、醫療機構及大學等單位中實際參與資訊安全工作者進行電腦犯罪與安全調查，報告中顯示長期以來電腦病毒常位居資訊安全事件的榜首（如圖 1 所示），而為了防範電腦病毒，幾乎高達 97%的機構組織會使用防毒軟體來防範，但仍無法完全避免電腦病毒的感染與擴散（CSI 1999-2008；CSI 2009），這也造成全球重大的經濟與財務上的損失。

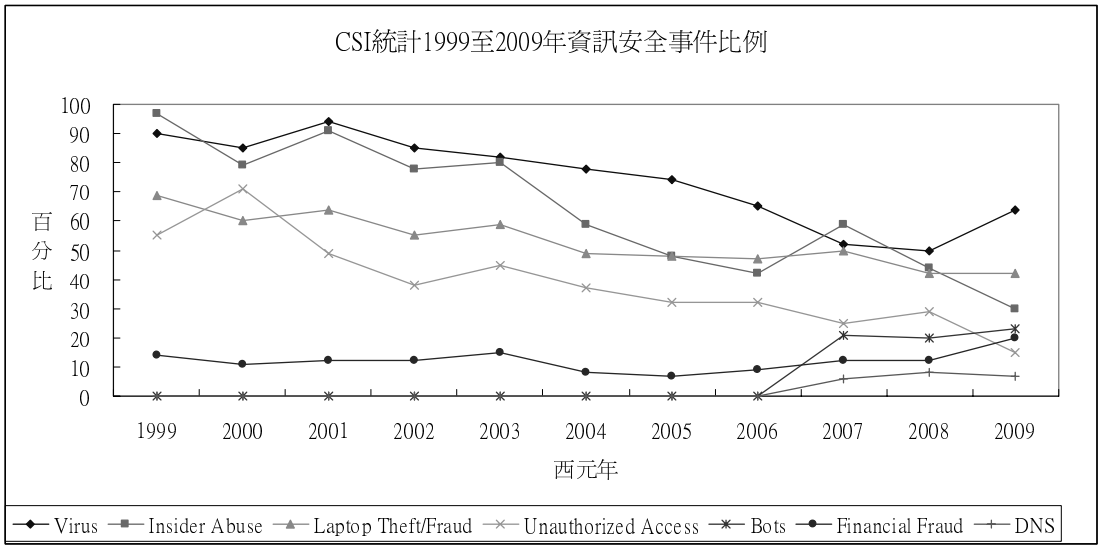


圖 1：CSI 統計 1999 至 2009 年資訊安全事件發展走勢（CSI 1999-2008；CSI 2009）

面對資訊安全問題愈來愈嚴重之際，企業在人力與成本的考量下，多採取防毒業者建議的防毒方案，但是這些方案的成效未必有太多驗證。多數資訊安全學者也都同意，人員的認知、政策、技術是保護資訊並讓資訊系統免於危險的三項核心因素，而政策尤其是資訊安全的核心（Whitman & Mattord 2008），但根據國內外調查有關資訊安全文獻得知，資訊安全政策之相關研究相當缺乏（Smith et al. 2010; 蘇建源等 2010）。有關如何防範電腦病毒的研究大多集中在技術面，如：

防火牆與入侵偵測系統封包過濾規則或結合人工智慧技術進行攻擊行為的探勘預測等，至於有關電腦病毒防範政策面的研究則較罕見。就資訊安全管理與政策研究所採用的研究方法而言，以問卷調查與個案研究居多。採用問卷調查法進行研究的學者皆指出可取得的研究樣本獲取不易而導致回收率過低（Albrechtsen & Hovden 2009; DTI 2004; Kotulic & Clark 2004; 黃士銘等 2006; 蔡思達 2007; 蘇建源等 2010），究其原因主要是資訊安全係企業較敏感性的議題，且企業與研究學者互信程度不高，故不願分享或提供相關資訊（Albrechtsen & Hovden 2009; DTI 2004; Kotulic & Clark 2004; Silva & Backhouse 2003; 郭家宏 2005; 蔡思達 2007; 蘇建源等 2010），至於個案研究法雖可深度探究，但某一成功或失敗的個案是否放諸四海皆準不無疑問，因此有其外推效度的限制。

雖然已有不少電腦病毒傳播的研究，但本研究仍著重於此議題探討防範政策的成效，其原因有以下四項：（一）目前企業多採取防毒業者提出的防毒方案，但這些防毒方案的成效並未獲得證實；（二）對企業來說，資訊安全屬較敏感性的議題，因此多不願分享與提供相關資訊，以致於探討電腦病毒的研究多集中在技術面，探討電腦病毒防範政策面的研究非常少；（三）企業遭受電腦病毒攻擊會帶來龐大損失（CSI 1999-2008；CSI2009），從資訊安全管理的角度來看，要減少電腦病毒的攻擊，必須從第一線的使用者著手，故有必要讓使用者了解各種可採用防治方案以及所產生的防治效果；（四）目前有關電腦病毒傳播的研究都將電腦病毒視為唯一參與者來進行探討（Mishra & Pandey 2010; Piqueira & Araujo 2009; Yang et al. 2008; Yuan et al. 2009），但實際上，電腦病毒傳播是一個非線性、具動態回饋與時間滯延的過程，因此，本研究以系統觀點，將電腦病毒、使用者與防毒軟體公司皆納入考量，將使用者更新病毒碼與防毒軟體公司技術能力等因素加入以符合現實情況。我們採用系統動力學（System Dynamics）為研究方法，系統動力學擅長處理多個參與者所構成的複雜問題，且在資料有限的情況下仍可進行（Sterman 2000），因此非常適合用於本議題。從學術文獻可知，目前利用系統動力學研究電腦病毒傳播特性的成果不多，就我們所知，僅張宏琳（2007）曾以生物免疫原理，使用系統動力學建立網路蠕蟲傳播模型，利用良性與惡性蠕蟲之間的對抗，保護電腦網路免受網路蠕蟲攻擊，但對於防毒政策並未加以探討。本研究將以探討防毒政策為主，首先建構電腦病毒傳播之動態模型，然後用模式模擬評估防毒政策的成效，為用戶提供採用不同防治政策的績效分析。

惡意程式是指未經允許而進入使用者電腦系統中，影響電腦正常運作，進行干擾、破壞或惡作劇等行為的程式，如：病毒、蠕蟲、特洛依木馬或間諜程式等，不過要將惡意程式明確地分門別類不太容易，因為惡意程式的某些行為特徵是有重疊的（Stallings 2006）。對於電腦病毒的定義，許多學者也提出不同的看

法，Cohen（1984）是最早具體描述電腦病毒定義的學者，他指出病毒是會感染其他軟體的程式，透過自我繁殖的特性，將自己附著在被感染程式中，再藉由感染的特性，擴散至整個電腦系統或網絡上，感染每個使用者的程式，而受感染的程式也變成傳染源，使得感染繼續擴張。這種不經使用者同意下任意進行複製的特性，讓使用者受感染而不自知，一旦使用者觸發病毒的破壞行為，就可能釀成災情。Ludwig（1996）認為，電腦病毒的認定並非以是否具有破壞性來判斷，只要是程式具有自我繁殖能力，就應視為電腦病毒。Peter（2005）也認為不論是否詢問使用者意願，只要具有自我繁殖功能，就屬於電腦病毒。隨著網際網路的普及化，電腦病毒從傳統的一對一感染方式，已經演變為多重途徑感染，只要在網路環境下所有電腦都有被感染的可能。不同種類的惡意程式具有重疊的特性，如電腦病毒、蠕蟲及特洛依木馬，都具有一經觸發即無限制擴散傳播特性，加上有愈來愈多的惡意程式都走向複合型態，如梅莉莎（Melissa）病毒即結合傳統病毒及蠕蟲兩項特性。由於電腦病毒幾乎已成為惡意或有害電腦程式之通稱，且多數人無法釐清各種惡意程式間的差異，習慣以電腦病毒這個名詞概括稱之，因此本研究並不特意區分惡意程式的種類與差異性，統一使用電腦病毒這個名詞，著重探討網路環境下惡意程式的散播以及使用者的防治政策。

本文鋪陳如下：首先歸納整理用戶端常用的防毒政策，接著說明研究方法與步驟。根據電腦病毒生命週期並輔以學者常使用的電腦病毒傳播模型為基礎，建立電腦病毒傳播之系統動力模型，然後模擬電腦病毒之動態行為並進行效度分析，最後再探討防毒政策在電腦病毒傳播過程中的影響以獲得重要結論。

貳、用戶端防毒政策探討

用戶端常用的防毒措施有三項：(1)制定管理政策；(2)使用防毒軟體；(3)進行資料備份（Post & Kagan 2000）。根據行政院主計處針對 30 人以上人力規模的電腦用戶所進行的調查顯示，民國 98 年用戶遭遇的資訊安全事件仍以電腦病毒破壞最多（43.81%），而已建置資通安全防護的用戶則高達 97.01%，其中主要的防護措施為防毒軟體（96.08%），其次則有防火牆（84.39%）與入侵偵測系統（30.55%）等（行政院主計處 2010）。相較於我國，美國 CSI 電腦犯罪與安全調查組織所收集的資料顯示，2008 年美國用戶使用防毒軟體占 97%，其次是防火牆占 94%，入侵偵測系統則占 69%（CSI 1999-2008）。這顯示除了防毒軟體之外，防火牆以及入侵偵測系統也是國內外企業組織最常使用的防護裝置。但縱然有完整的軟硬體防護裝置，仍然無法監測出所有的人為疏失，因此組織內需要一套管理制度規範內部成員的作業行為，學者 Post 與 Kagan（2000）將防毒管理政策分為兩類：限制/約束類（Restrictive）與主動類（Proactive）。限制/約束類的管理政

策包括：限制員工使用網路、共享軟體、遊戲或監看員工電腦、制定違反罰則等，主動類則包括使用防毒軟體掃瞄磁碟等。

一、限制/約束類

依行政院主計處的調查顯示，受訪企業所制定資訊安全管理作業包括：訂定 e-Mail 使用規定、訂定使用者註冊制度、定期更換通行密碼、區分資料安全等級、管制進出機房、安全稽核、納入委外契約條款、演練應變回復作業、舉辦相關訓練宣導、指定專人負責辦理等，但與電腦病毒相關的管理政策卻似乎付之闕如。ISO 27001（2005）是目前最廣為人知的一套資訊安全管理系統國際標準，此標準幫助組織降低資訊安全弱點所造成的傷害，並協助組織事前預防潛在風險對組織的危害，許多企業也以它作為加強人員對資訊安全認知的準繩。

ISO 27001（2005）包括 11 個領域、39 個控制目標以及 133 個控制措施，其中與惡意程式相關的控制措施有：(1)A10.4.1 對抗惡意碼的控制措施；(2)A12.6.1 技術脆弱性控制；(3)A13.1.2 通報安全弱點（ISO 27001 2005）。

（一）A10.4.1 對抗惡意碼的控制措施

主要採取防範惡意程式的偵測、預防及復原控制措施，包括使用者安全認知，以防止惡意程式植入軟體或資訊處理設施。使用者應認知到惡意程式的危險性，對網路上不明的軟體與網址，在下載與連線前應謹慎，必要時也要進行檢查。安裝並定期更新惡意程式碼與修復軟體，在使用檔案（包括自網路上收到的檔案）以及自電子郵件打開附加檔案之前，先進行檢查。最好將防範惡意程式軟體設定為自動更新病毒定義碼和掃瞄引擎，以確保防護版本為最新版。

（二）A12.6.1 技術脆弱性控制

作業系統或其他使用中的應用系統有可能存在技術脆弱性，而這些脆弱性都可能引來駭客的惡意攻擊。因此有需要隨時注意資訊系統技術脆弱性的及時資訊，並建立資產清冊（包括：軟體廠商、版本編號、目前部署狀態及負責人等），以確保收到資訊系統技術脆弱性及時資訊時，可以採取適當的行動。

（三）A13.1.2 通報安全弱點

此項控制措施主要指使用者若觀察或發現到系統有可疑的安全弱點時，應注意並通報組織管理階層或系統服務提供者，以防止資訊安全事故發生。在未得到確認之前，切勿試探可疑的安全弱點，以免引發對系統或服務的損害。

二、主動類

（一）防毒軟體

用戶端安裝防毒軟體以預防感染電腦病毒。使用者視需求自行掃瞄檔案，或將防毒軟體常駐於記憶體中，隨時偵測是否有病毒行為。防毒軟體依照病毒特徵（如：結構、攻擊邏輯等）來辨識病毒，並使用檢查條件（如：程式碼片段、完整性檢查等）查看是否有中毒現象。一般防毒軟體至少包括三種技術（Hruska 1990）：

1. 檢查校驗（Checksumming）：部份電腦病毒會依附在檔案上，所以被感染的檔案可能會產生大小改變或檔案日期被修改的現象。防毒軟體安裝後就自動將硬碟中的所有資料做匯總，計算 Checksum 並加以保存。日後當使用者啟動防毒軟體時，防毒軟體就會檢查目前檔案的 Checksum 與原來保存的是否一致，以判斷檔案是否被修改。這種技術可檢測出已知與未知病毒，但有其缺點：(1)不能判斷病毒的種類以及名稱；(2)容易誤判，例如軟體版本更新或文件內容更改，有可能是人為正常程序，並非感染電腦病毒所致。
2. 掃瞄（Scanning）：分析已知病毒的特徵模式，並儲存在病毒資料庫中。當啟動掃瞄程序時，即比對病毒資料庫中的病毒特徵檔，若發生一致，表示有可能已遭受病毒感染。此技術的成效有賴於病毒資料庫內已知的病毒特徵是否齊全，因此若透過掃瞄程序發現感染病毒時，可以從資料庫中判斷病毒的種類、名稱及處理方法。然而面對新種電腦病毒不斷出現，病毒資料庫必須不斷更新，否則無法準確發現電腦病毒。因此，用戶端必須加強自我防疫，養成主動下載更新病毒碼以及相關程式的習慣。
3. 監測（Monitoring）：防毒軟體啟動後，即常駐在記憶體中，監測輸入輸出裝置，並檢測是否有病毒活動。早期因缺少有效的監測技術，沒有建立判斷規則，導致誤判的機率高，但隨著人工智慧技術的進步，監測的技術也隨之提升。

（二）防火牆

防火牆是佈署在內部網路連上網際網路出入口的裝置，其目的是在不影響連線的情況下控制資料封包的進出，藉以達到保護內部網路、降低外來威脅的目標。它透過清單來控制進出權限，例如管制封包繞送或連線的狀態等，因此形成一道關卡。它本身也是一個網路管理平台，管理者可以在此記錄與稽核網路使用情形、進行網址翻譯等，也可以建置虛擬私有網路。

（三）入侵偵測系統

入侵偵測系統是防火牆後的第二道防線，它建立偵測規則，判斷是否有異常

行為，如有則通知管理者做進一步處理，不過在實務應用上，正確偵測的機率仍有待提升。

以上為用戶端常用的安全防護工具。限制/約束類屬於被動的管理政策，而資訊安全公司等專業廠商為了能在第一時間發現惡意程式動態，紛紛提出自動通報機制的概念，當系統發現網路中有用戶端的異常行為，管理主機會將疑似病毒樣本送到病毒分析主機進行行為和結構的分析、萃取病毒碼、產生疫苗，再將疫苗傳送給管理主機，讓所有電腦都會收到新的疫苗。依據國內外的統計顯示，防毒軟體是企業組織主要採取的防護措施，但除此之外，企業組織同時還多會採用防火牆或入侵偵測系統。光採用防毒軟體是不是防禦能力就比較弱？是不是一定要配合其他政策才能有效？什麼樣的組合政策才是最有效的？這些問題至今沒有研究可以證實。因此本研究將針對用戶端的防毒政策進行探討，以 ISO 27001（2005）中與惡意程式相關的控制措施為基礎，考量以下四項政策對電腦病毒傳播的影響：(1)用戶端採用防毒軟體；(2)用戶端的自我防疫力；(3)用戶端的通報率；(4)用戶端採用自動通報機制。希望透過系統動力學研究不同政策的績效，以提供管理者防毒決策之參考。

參、研究方法

本研究使用系統動力學為研究方法，其融合了資訊回饋控制理論、決策程序、實驗方法系統分析、電腦模擬等四項理論基礎，主要用於分析並解決複雜動態問題的一種方法（Forrester 1961）。使用此方法的主要原因有：(1)動態複雜性，包括時間滯延、因果回饋、非線性（Sterman 1989; 黃經洲等 2009）。電腦病毒傳播屬於非線性，且存在動態回饋與時間滯延，而感染電腦病毒背後可能的原因都是環環相扣，互為因果，因此使用系統動力學來模擬與分析，會比一般使用數理解析法更符合真實；(2)有利於防制政策的評估。系統動力學的效用以策略分析為其專長，目前探討電腦病毒傳播的研究都只強調傳播模型與檢測，對於防毒政策的評估非常缺乏，因此本研究除了改善現有傳播模型之外，還會針對不同的防毒政策進行模擬與評估；(3)在數據缺乏的情況下仍可進行研究（Sterman 2000; 蘇懋康 1988）。要取得數據進行資訊安全管理方面的實證研究相當困難，以致於目前研究不足（Kotulic & Clark 2004），系統動力學的模型以回饋與因果循環為基礎，只要估計的參數在寬容範圍內，系統行為仍舊能顯示出接近的模式。

以下研究步驟分五個階段進行：（一）透過文獻蒐集了解電腦病毒的生命週期；（二）透過文獻蒐集研討電腦病毒傳播模型；（三）建立電腦病毒感染之因果關係；（四）建立系統動力學之動態模型；（五）進行模擬與結果效度檢驗，並評估防治策略。

一、電腦病毒生命週期

生物學上的病毒透過傳染途徑感染生物，生物進而染病、被治療、痊癒、再染病（Anderson & May 1991）。電腦病毒的傳染模式就如同生物學的病毒運作模式，也會散布給其他電腦使用者。Ferbrache（1992）引用學者 Farmer 與 Belin（1991）的研究指出，電腦病毒本身也具備人工生命力，包含：(1)具有行為模式；(2)自我繁殖；(3)病毒碼如同生物的遺傳密碼；(4)新陳代謝；(5)與環境互相影響；(6)互相依賴；(7)適應環境；(8)演化的能力；(9)成長或擴張（Farmer & Belin 1991; Ferbrache 1992）。因此，許多學者認同以流行病學的傳染病模式來說明電腦病毒散佈情形（Ferbrache 1992; Murray 1990），以流行病學模式為方法的相關研究也陸續被發表（Chen et al. 2003; Cho et al. 2007; Kephart & White 1991；Kephart & White 1993; Piqueira & Araujo 2009; Wang et al. 2010; Wierman & Machette 2004; Zou et al. 2002）。

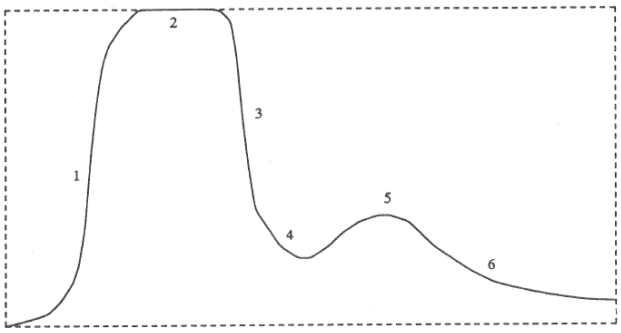


圖 2：感染電腦病毒可能的模式（Ferbrache 1992）

一般而言，電腦病毒侵入主機後，其生命週期可分為四個階段（Stallings 2006）：(1)潛伏階段：電腦病毒尚未行動，正等待某些事件被喚醒；(2)繁殖階段：電腦病毒自我複製並潛入其它程式；(3)觸發階段：受到某些系統事件的驅動，啟動電腦病毒的破壞功能；(4)執行階段：電腦病毒的破壞功能被執行。Ferbrache（1992）也對電腦病毒的成長到死亡做出論述，描繪感染電腦病毒可能的模式，分為六個階段如圖 2 所示。他認為初期電腦病毒的散播情況視使用者的使用行為不同而呈現 S 曲線或指數成長曲線，其中 S 曲線表示是一般傳統的使用情況，指數成長曲線則表示存取行為較複雜（圖 2 中之 1）。在被偵測之前，會有一段潛伏期或偽裝期（圖 2 中之 2）；潛伏期後，使用者紛紛發現中毒，因此會使用防毒軟體掃毒，此時感染情形急速下降（圖 2 中之 3）；少數電腦病毒沒被觸發到，因此還沒被破壞，使用者以為沒中毒，所以並未進行掃毒（圖 2 中之 4）；沒進行掃毒的那一批電腦發作了（圖 2 中之 5）；進行更新系統、病毒碼或隔離無法

恢復的電腦，減緩了電腦病毒的感染（圖 2 中之 6）。基於以上探討，我們可以得到以下結論：(1)電腦病毒生命週期如同生物的成長模式；(2)電腦病毒傳播模式與流行性傳染模式類似。

二、電腦病毒傳播模型

電腦病毒傳播常探討的研究模型整理如下：

（一）SI 模型（Susceptible-Infectious Model）

這個模型源自於最基本的傳染病模型（Bailey 1975）。每台電腦保持易感染的（Susceptible）和感染的（Infectious）兩種狀態。假設電腦一旦被感染，就保持被感染狀態，SI 模型的微分程式請參考 Cho 等（2007）。SI 模型是最簡單的傳播模型，因此整體來說並不周延，模型裡只考慮易感染的（Susceptible）和感染的（Infectious）兩種狀態，沒有考慮到電腦可能會復原。就電腦病毒初期散布的情況來說，SI 模型可以描述出電腦病毒的行為，但以長時間來看，當使用者發現自己的電腦中毒之後，都會想辦法解決中毒的問題，因此 SI 模型無法反應電腦中毒後的解決情形。

（二）SIR 模型（Susceptible-Infectious-Removed Model）

SIR 模型也是起源於傳染病模型（Hoppensteeadt & Waltman 1970）。此模型是 SI 模型的加強版，其狀態分為易感染（Susceptible）、已感染（Infectious）、復原（Removed）三種。其中，復原狀態不具有傳染性並且不會再被感染，包括復原（Recover）、死掉（Died）、免疫（Immune）或被隔離（Isolated），SIR 模型的微分程式可參考 Cho 等（2007）。

SIR 模型以 SI 模型為基礎，並考慮到受感染的主機可能被移除或復原的情況，因此可以用來描述不具第二次感染性的病毒攻擊，但此模型仍有缺點：(1)復原電腦一定要經過感染過程，因此無法描述當使用者主動執行掃毒程式、系統修補、更新病毒碼等對抗電腦病毒的手段時，電腦從易感染或已感染轉為復原的狀態；(2)假設感染率為常數，並不符合電腦病毒快速傳播的特性（Zou et al. 2002）。

（三）SIS 模型（Susceptible-Infectious-Susceptible Model）

SIS 模型假設每一個電腦都有相同被感染的機率，也就是復原電腦像易感染電腦一樣，仍有相同的機率變成感染電腦。其描述的狀況沒有考慮到感染電腦自行下載修補程式或更新病毒碼而對電腦病毒免疫（Qing & Wen 2005），然而在現實生活中，當使用者知道電腦中毒之後會進行解毒，在電腦病毒移除且病毒碼更新之後，該電腦即對病毒碼資料庫中的電腦病毒具免疫力，因此不適合用來描述

真實世界下電腦病毒感染的情形。

（四）TF 模型（Two-Factor Worm Model）

TF 模型是 Zou 等（2002）以 SI 模型與 SIR 模型為基礎，針對紅色警戒病毒所發展的。TF 模型改善 SI 與 SIR 模型的缺點，強調：(1)TF 模型的感染率會隨著時間做動態改變；(2)考慮人為採取的對抗措施，讓電腦從已感染電腦中恢復或從易感染電腦中直接免疫。因此，TF 模型除了有易感染、已感染的狀態之外，還有移除、免疫狀態。

TF 模型是 SI 與 SIR 模型的延伸且彌補了兩模型的不足，但 TF 模型還是有缺失：(1)移除率和免疫率是常數，這與現實情況不符，因為隨著時間，人們對電腦病毒的認識愈多，移除率和免疫率應提升；(2)沒有考慮到防毒軟體公司的技術能力對電腦病毒傳播的影響。因為當電腦病毒被防毒軟體偵測到之後，防毒軟體公司會分析其行為並研發出疫苗，所以電腦病毒傳播趨勢會減緩。

三、因果關係的建立

本研究的電腦病毒傳播之因果關係圖是透過文獻探討與專家討論而建立的，由三個增強環（R1~R3）與五個調節環（B1~B5）所組成，如圖 3 所示。

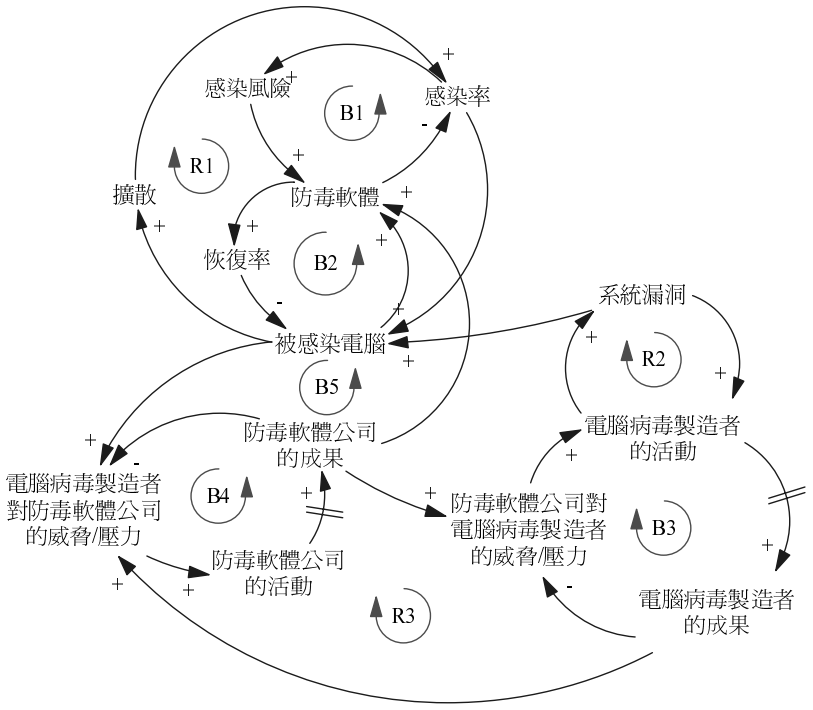


圖 3：電腦病毒傳播因果關係圖

以系統的角度看電腦病毒傳播過程有三個參與者：電腦（包括個人電腦、主機等裝置）、電腦病毒製造者（Virus Writer）、防毒軟體公司（Anti-Virus）。所有曝露在網路上的電腦，都是受感染的危險群。電腦之所以會受到電腦病毒的傳染，是因為存在感染源。感染源之所以會存在，表示電腦病毒製造者知道使用者所使用的系統或軟體有漏洞，因此設計破壞活動。若系統存在弱點，電腦病毒製造者破壞系統安全的動機就愈強，使得系統漏洞被發現得也愈多（圖 3 中的 R2）。若使用者的電腦不進行系統漏洞修補，成為被感染電腦的機會就會增加。這些被感染的電腦經過網路等媒介將電腦病毒擴散，增加感染率，所有曝露在網路上的電腦就愈容易被感染（圖 3 中的 R1）。感染率會增加電腦感染病毒的風險，故曝露在網路上的電腦若懂得使用防毒軟體，就可以減少受感染的機會，因此使用者需要防毒軟體進行掃毒或更新病毒碼，以降低被感染的可能性（圖 3 中的 B1）。若電腦受感染，使用者要用防毒軟體協助移除電腦病毒等惡意程式，恢復為正常電腦（圖 3 中的 B2）。面對電腦病毒製造者的破壞行動與被感染電腦增加的數量，會激發防毒軟體公司持續研發新的防毒功能，使得防毒軟體更強化以供使用者下載來解決電腦被感染的問題（圖 3 中的 B5）。

本研究認為電腦病毒製造者和防毒軟體公司兩方存在競爭的關係，所謂競爭是指為了保有自己的福祉，必須建立在勝過對手的基礎上（Senge 1990）。只要有一方領先，另一方就會感受到威脅，導致他更加積極，結果使得對方感到威脅，提升自己行動的積極程度。圖 3 中的增強環 R3 是競爭基模，包含兩個調節環 B3 與 B4。電腦病毒製造者通常需要高人一等的技巧和知識，因此，這一類的人為了要證明自己是非常厲害的高手，通常會以政府或著名企業機關的安全系統為標的，製造一些令人難以偵測與防範的病毒，來炫耀自己的能力與成就（林宜隆& 黃讚松 2001）。一旦他釋放出新的電腦病毒後，感染電腦病毒的裝置經過潛伏期以及觸發事件，引發電腦病毒攻擊。由於是新的電腦病毒攻擊事件，防毒軟體公司來不及分析電腦病毒行為，因此減少了對電腦病毒製造者的威脅（圖 3 中的 B3）。面對層出不窮的電腦病毒危害事件，防毒軟體公司感到威脅，因而致力於產品、技術的研發，更新防毒引擎以及病毒碼，減少使用者受到電腦病毒威脅（圖 3 中的 B4）。電腦病毒攻擊事件威脅到防毒軟體公司，因此著手進行病毒行為分析以及研發疫苗，增加防毒軟體的可用性，同時也增加對電腦病毒製造者的威脅。電腦病毒製造者可能因為成就感降低，因而繼續發展更強電腦病毒，以彰顯自己的能力與成就（圖 3 中的 R3）。從電腦病毒的生命週期中可以知道感染電腦病毒後通常會有一段潛伏期以及觸發階段才會引發電腦病毒活動，因此在製造者釋放出電腦病毒後到攻擊事件出現這段期間，存在著時間滯延。當防毒軟體公司偵測到電腦病毒攻擊事件後，需要時間分析病毒行為，因此直到完成更新防毒引擎或病毒碼的這段期間，也存在時間滯延。

四、建立電腦病毒傳播模型

本研究所建立的電腦病毒傳播模型以 SIR 模型為基礎，探討電腦感染到一個新的電腦病毒時的情況，並以易感染電腦、已感染電腦及已復原電腦為三個主要階段。本模型與以往研究的不同之處有：(1)現實生活中，人們會主動更新病毒碼或系統程式以避免電腦遭受電腦病毒的攻擊，然而許多研究未考慮到此情況，因此本研究模型加入防疫力以更貼近現實；(2)考慮防毒軟體公司技術能力進步後會提升偵測到新電腦病毒的能力，因此更符合動態性；(3)將通報率加入模型中，以觀察使用者主動通報可疑惡意程式是否會影響電腦病毒的傳播。模型中的變數以及定義列於表 1。

表 1：變數定義

變數	定義
FINAL TIME	= 24. 模擬的全部時間為 24 小時。單位：小時
INITIAL TIME	= 0. 模擬的開始時間為 0 小時。單位：小時
被偵測機率 (dp)	防毒軟體公司偵測到新電腦病毒的機率。防毒軟體公司技術能力愈高，偵測到的機率也愈高
已復原電腦 (R)	不會再被感染的電腦，包括免疫或復原的電腦，屬於積量。單位：電腦數
已感染電腦 (I)	受電腦病毒感染而且有感染能力的電腦，屬於積量。單位：電腦數
平均防禦空窗時間 (t)	顯示從電腦病毒發作到防毒軟體公司研究出對策再到處理感染電腦所需的時間。單位：小時
復原率 (RR)	由感染電腦轉變為已恢復電腦的速率。單位：電腦數/小時
感染力 (i)	電腦暴露在被感染的環境下可能中毒的機率。初始值=0.25
感染率 (IR)	易感染電腦轉變為感染電腦的速率。單位：電腦數/小時
感染量與壓力關係函式 $(f_{ip}(x))$	被感染電腦數量與防毒軟體公司壓力之關係。被感染電腦數量愈多，防毒軟體公司愈有壓力，所以會愈努力將能力增強。屬表函數
接觸率 (c)	表示電腦接觸外來媒介（如網路、USB、磁碟片等）的頻率。單位：次/小時。初始值=20
易感染電腦 (S)	未受感染但因有弱點而容易被感染的電腦，屬於積量。單位：電腦數

未被感染電腦的比例	易感染電腦(S)占易感染電腦(S)加已感染電腦(I)的比例
通報率(r)	使用者發現到系統有可疑的安全弱點時通報防毒軟體公司的比率（根據 ISO 27001 A13.1.2 通報安全弱點的定義）。初始值=0.5
防毒軟體公司壓力(ap)	指防毒軟體公司面對電腦病毒事件發生時所感受的壓力
防毒軟體公司技術累積(AT)	指防毒軟體公司對新電腦病毒的防禦技術進步累積。防毒軟體公司的能力靠知識、技術與經驗累積，屬於積量。初始值=0
防疫力 (p)	使用者主動更新病毒碼的比率。初始值=0.1
防禦技術與可被偵測機率關係函式$(f_{dp}(x))$	防毒軟體公司的防禦技術能力與其偵測機率之關係。防禦能力愈高，偵測到病毒的速率愈快。屬表函數
可被偵測機率與平均防禦空窗時間關係函式$(f_d(x))$	防毒軟體公司的產品其偵測電腦病毒之能力與平均防禦空窗時間之關係。偵測到新電腦病毒的機率與速度愈高，平均防禦空窗時間愈短。屬表函數
防禦技術進步速率(TI)	防毒軟體公司技術進步的速率
電腦總數(N)	系統中所有的電腦數量，即易感染電腦、感染電腦與恢復電腦的加總。單位：電腦數。初始值=100000
預防率 (PR)	因主動防疫而由易感染電腦轉變成已恢復電腦的速率。單位：電腦數/小時

本研究依據相關文獻與專家訪談來建構模式，整個模式分為三個次模式，分別為：（一）感染電腦擴散流；（二）易感染電腦免疫與感染電腦恢復流；（三）防毒軟體公司技術提升流。各個次模式包括的主要變數與模式說明如下：

（一）感染電腦擴散流

所有曝露在網路上的電腦（包括個人電腦、主機、行動裝置等），都屬於易感染電腦。使用者透過網路或 USB 存取資料、服務而感染到病毒，變成感染電腦，但並非所有連上網路或存取 USB 資料的電腦都會受感染，一般來說，接觸的頻率愈頻繁，感染電腦病毒的可能性愈高。使用者發現電腦受感染後，會更新防毒軟體病毒碼並掃瞄系統，將電腦病毒移除或刪除。由於更新後的防毒軟體中已包含更新的病毒碼，因此不會再受到感染，成為復原電腦。圖 4 中易感染電腦至已感染電腦之過程屬於感染電腦擴散流。假設I_0表示被感染電腦之初始值，R_0表示恢復電腦之初始值，針對電腦從未感染、受感染一直到恢復正常的狀態移轉過程，易感染電腦（S）、已感染電腦（I）、感染率（IR）之模式可用公式(1)表

示：

$$\begin{cases} N = S + I + R \\ S = INTEGRAL\left(-IR, N - I_0 - R_0\right) \\ I = INTEGRAL\left(IR - RR, I_0\right) \\ IR = \left(c \cdot i \cdot S\right) \cdot \left(I/N\right) \end{cases} \tag{1}$$

電腦以接觸率（c）相互接觸，接觸的範圍可以是網路節點或是抽取式行動設備。網路是感染病毒的主要管道，大部份使用者連上網際網路後會點選有興趣的網頁或廣告，然而這些瀏覽行為都造成了感染病毒的風險。易感染電腦單位時間內接觸量為（$S \cdot c$），接觸的對象是感染電腦的機率為（I/N），但並不是與已感染電腦接觸就一定都會被感染，因此模式中感染力（i）表示與感染電腦接觸而被感染的可能性。

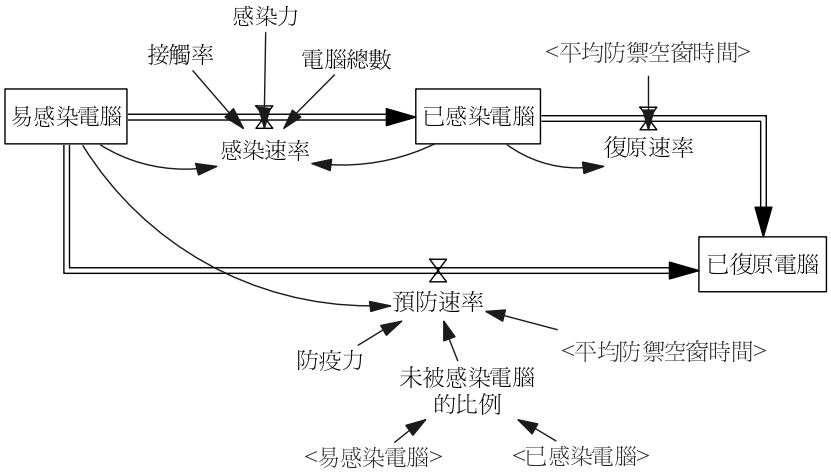


圖 4：感染電腦擴散流、易感染電腦免疫流與感染電腦恢復流

（二）易感染電腦免疫與感染電腦恢復流

並非所有電腦都必須經過感染過程，使用者擔心電腦感染病毒會帶來危害，可以主動更新病毒碼以及系統程式，讓電腦免於電腦病毒感染。若電腦不幸受感染，也可更新防毒軟體公司公布的最新病毒碼或掃瞄引擎，移除電腦病毒，轉為復原電腦。圖 4 中易感染電腦至已復原電腦的過程屬於易感染電腦免疫流，已感染電腦至已復原電腦之過程屬於感染電腦恢復流。因此，針對使用者主動預防與事後彌補，復原電腦（R）、預防率（PR）、復原率（RR）之模式可用公式(2)表

示：

$$\begin{aligned} R &= INTEGRAL(RR + PR, R_0) \\ &= INTEGRAL((I/t) + (p \cdot S \cdot (S/(S+I))/t), R_0) \end{aligned} \tag{2}$$

復原電腦（R）表示不會被再感染的電腦，包括復原與免疫的電腦。復原率（RR）表示由感染電腦轉變為恢復電腦的速率，此速率必須視防毒軟體公司自發現病毒到研發出疫苗的處理時間而定，因此除上平均防禦空窗時間（t），表示防毒軟體公司可在（t）小時解決新電腦病毒事件。預防率（PR）是指易感染電腦主動防疫而轉變成恢復電腦的速率，由易感染電腦（S）乘上 p 表示易感染電腦中，使用者主動更新病毒碼或系統程式的比率，從易感染電腦直接轉為復原電腦表示電腦並未經過感染階段，所以乘上未被電腦病毒感染的比例，$\left[S/(S+I)\right]$，最後再除以平均防禦空窗時間（t）。

（三）防毒軟體公司技術提升流

本研究模型的防毒軟體公司技術提升流主要來自感染電腦數量與使用者通報的壓力。假設防毒軟體公司技術累積（AT）來自於知識、技術與經驗的累積，技術進步來自於電腦病毒事件所造成的壓力（ap），壓力與被感染的電腦數量成正向關係。使用表函數（$f_{ip}(x)$）來表示防毒軟體公司的壓力與被感染電腦數量的關係，被感染電腦數量愈多，防毒軟體公司愈有壓力，所以更會努力提升自身能力。防毒軟體公司偵測到電腦病毒機率與其技術成正向關係。使用表函數（$f_{dp}(x)$）來表示防毒軟體公司的能力與其偵測機率之關係，防毒軟體公司技術愈強，偵測到病毒的可能性愈快愈高；反之則愈低。防毒軟體公司偵測到新電腦病毒的機率與平均防禦空窗時間成負向關係。使用表函數（$f_d(x)$）來表示兩者之關係，防毒軟體公司偵測到新電腦病毒的機率愈高，平均防禦空窗的時間將愈短。模式中的通報率（r）是指使用者發現異常狀況時，回報防毒軟體公司的比率，因此通報率愈高，防毒軟體公司壓力就愈大；反之則愈低。圖 5 為防毒軟體公司技術提升流，相關模式可用公式(3)表示：

$$\begin{cases} ap = (I/N) \cdot r \\ TI = f_{ip}(ap) \\ AT = INTEGRAL(TI, AT_0) \\ dp = f_{dp}(AT) \\ t = f_d(dp) \end{cases} \tag{3}$$

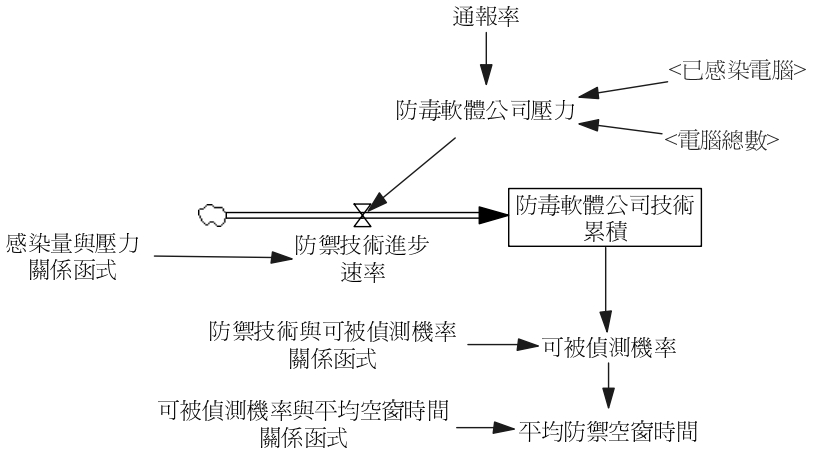


圖 5：防毒軟體公司技術提升流

肆、模擬與討論

一、模擬結果

本研究使用 Vensime PEL 工具進行模擬，依據上節的模式與初始值，模擬出的電腦病毒傳播情形如圖 6。接下來對模擬結果進行效度檢驗以及模型敏感性測試。系統動力學的模型效度檢驗包括：(1)結構效度（Structural Validity）：指模型中的方程式是否有理論、文獻或證據的支持（Sterman & Wittenberg 1999）；(2)行為效度（Behavior Validity）：指模型模擬的行為與真實行為相似的程度，亦即模擬出的行為型式是否能重現真實行為（Sterman 2000）。敏感性測試是針對模型的穩定性做測試，觀察數值變化是否讓模型產生重大的改變（Sterman 2000）。

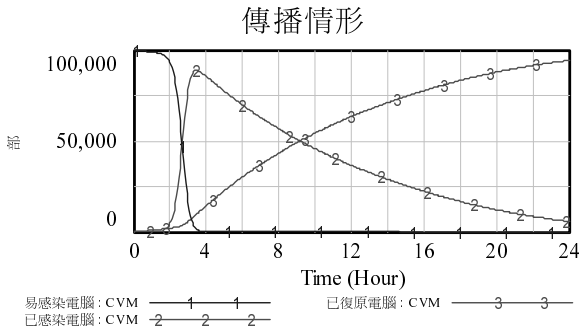


圖 6：基本設定下之易感染、已感染與已復原電腦的模擬結果

（一）結構與行為效度

本研究模型中的方程式皆根據相關理論與文獻建構，並有專家參與，因此與電腦病毒傳播之理論與文獻一致，符合系統動力學結構效度的要求。此外，模擬結果顯示，易感染電腦在第 2 小時起急速減少，已感染電腦在第 3.4375 小時最高，達到 88635 部電腦，隨後逐漸下降，已復原電腦則是隨著時間而上升。此行為模式與學者們之研究相似（Mishra & Pandey 2010; Yang et al. 2008; Yuan et al. 2009），因此判斷具有行為效度。

（二）模型敏感性分析

若電腦總數增加至 200000 部，感染力增加至 0.5，接觸率增加至 50，其餘變數固定不變，模擬結果如圖 7。電腦總數倍增，感染速率也爆增（圖 7 中的 4 爆增至 1）。這可以分兩點分析：第一，電腦數量多，表示高危險群電腦也多，因此若一部電腦中毒了，受感染的數量可用指數成長來預估；第二，電腦數量多，表示網路上的惡意電腦也可能增加，因此更增加網路使用的危險性。此外，感染力與接觸率增加不僅會提前感染高峰期，也會加快感染速率，其感染速率加快的程度比電腦總數倍增時更高（圖 7 中的 2 與 3、圖 8）。雖然數值改變，但模擬結果顯示電腦病毒傳染行為並未改變，因此判斷本模型具有穩定性。

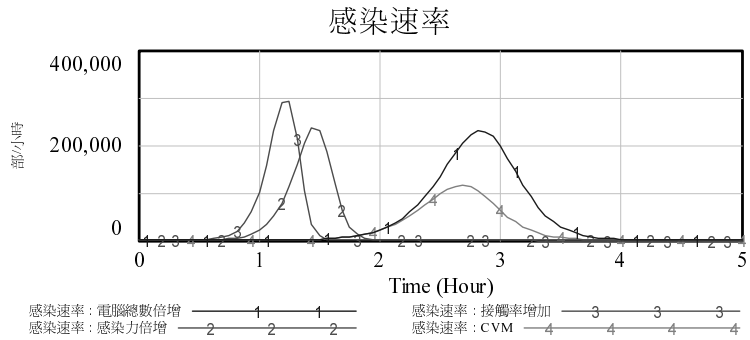


圖 7：模型敏感性分析

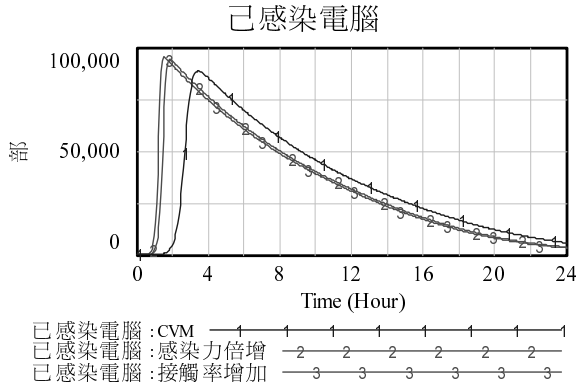


圖 8：感染力與接觸率增加影響已感染電腦

二、用戶端防毒政策測試與討論

ISO 27001 中與惡意程式相關的控制措施有：(1)A10.4.1 對抗惡意碼的控制措施；(2)A12.6.1 技術脆弱性控制；(3)A13.1.2 通報安全弱點（ISO 27001 2005）。由於 A12.6.1 技術脆弱性控制涉及系統軟體廠商，超出本研究模型範圍，因此本研究僅針對 A10.4.1 與 A13.1.2 進行政策測試。

（一）A10.4.1 對抗惡意碼的控制措施

此項控制措施主要在於偵測與防止電腦病毒，屬於防毒軟體的應用範圍，要使防毒軟體有效地應用，必須有兩個前題：(1)防毒軟體公司所研發的疫苗是有用的；(2)使用者能做到自我防疫。我們以這兩個前題進行政策測試。

1. 防毒軟體公司所研發的疫苗有用：若電腦病毒疫苗有用，表示防毒軟體公司的技術很強，此時若使用者能主動做自我防疫，確保防護版本為最新版本，則可達到防護的目的。圖 9 顯示當防毒軟體公司研發的疫苗有用時，使用者執行自我防疫的比例從 0.1 提升至 0.3 時對感染數量的影響，所以疫苗有用且使用者資訊安全認知提高，感染電腦病毒尖峰數量很明顯驟降許多。

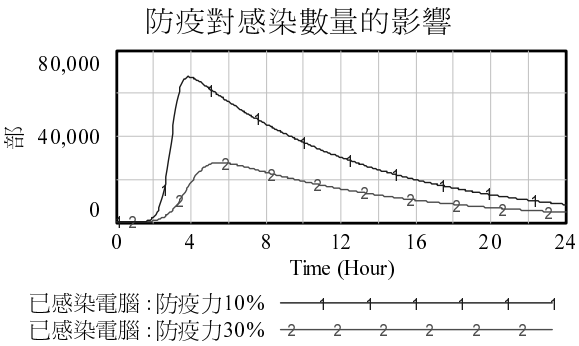


圖 9：防疫力從 0.1 提升至 0.3 後對感染數量的影響

2. 使用者能做到自我防疫：電腦病毒被偵測機率受防毒軟體公司的技術所影響，而平均防禦空窗時間則受防毒軟體公司偵測到病毒的機率所影響，圖 10 顯示防毒軟體公司技術與使用者防疫力對已感染電腦之關係。

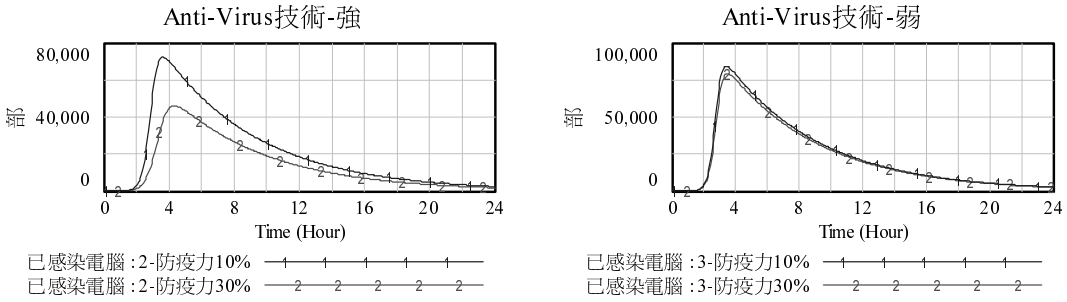


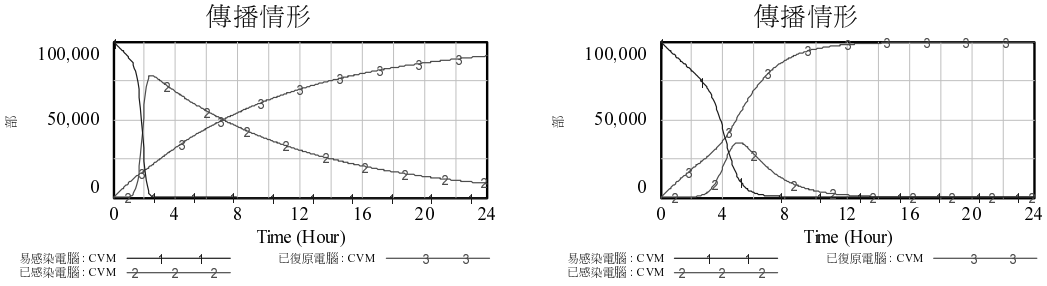
圖 10：防毒軟體公司技術與防疫力對已感染電腦之關係

使用者自我防疫的行為很重要，但還要有更新效率很及時的防毒軟體，才能有效降低已感染電腦數量。使用者有資訊安全認知，安裝防毒軟體並且同時執行自我防禦，則防範惡意程式的預防成效，視防毒軟體的技術優劣能力而定。若防毒軟體公司能及時研發有用的疫苗，則使用者自我防疫行為就成為有效降低已感染電腦數量的重要關鍵；但若防毒軟體公司不能及時研發有效疫苗，雖然使用者懂得自我防疫，感染情況並不會大幅改善，所以防毒軟體公司的能力是有效降低已感染電腦數量的重要關鍵。因此，使用者一定要做自我防疫，還要選擇一個技術能力強的防毒軟體，才能降低電腦病毒的威脅。

（二）A13.1.2 通報安全弱點

本研究模型的通報率是指用戶端使用者發覺有可疑的狀況時，通報防毒軟體公司的比率。模擬結果發現，通報率正向影響防毒軟體公司壓力，促進防禦對策盡快產生，所以對防毒軟體公司而言，通報機制顯得非常重要。如果通報率僅稍微提升，則偵測機率也增加不多，所以平均防禦空窗時間縮短地有限，除非通報速率可以非常迅速，因此有效疫苗就能盡快產出，則病毒傳染狀況不會太嚴重，因此異常事件的通報機制乃是防衛技術進步的關鍵因素。

由此可知，透過使用者通報異常狀況存在較長的時間滯延，因此會延誤防毒軟體公司研發防毒疫苗的時程。要改善上述問題，企業組織除了使用防毒軟體來預防之外，也可以與防毒軟體公司等專業廠商合作建立自動化通報機制。在還沒發生疫情之前，自動通報機制即從少數已感染電腦中監視到疑似的病毒行為，經過分析確認為病毒行為後，即著手研發防毒疫苗，因此將縮減平均防禦空窗期並降低感染力。假設啟動此機制後，感染力由 0.4 降低至 0.2、平均防禦空窗期由 10 縮減至 2，電腦病毒傳播情形如圖 11。已感染電腦由原本 2.4375 小時 78453 部電腦，減緩到 5 小時 35307 部電腦，且已復原電腦領先已感染電腦。此時若使用者的防疫力提升，則已感染電腦下降幅度更大（如圖 12）。這顯示雖然防毒軟體公司主動發現異常情形並研發出防毒疫苗，再加上使用者主動防疫，才能有效抑制電腦病毒感染情形。



(a)感染力=0.4，平均防禦空窗期=10　　(b)感染力=0.2，平均防禦空窗期=2

圖 11：防毒軟體公司啟動自動通報機制前後的電腦病毒傳播變化

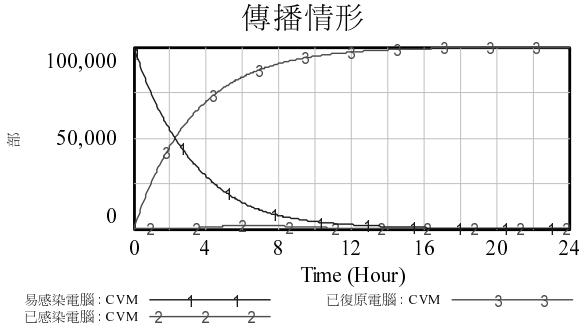
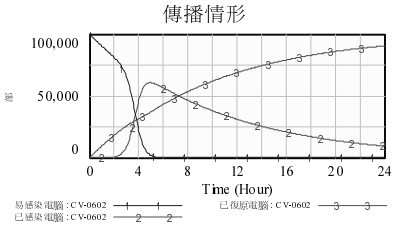
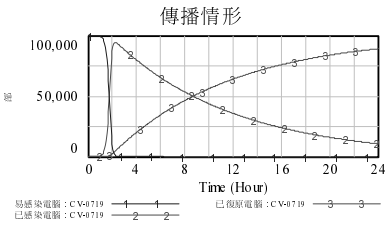
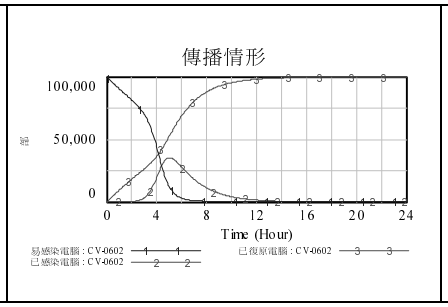


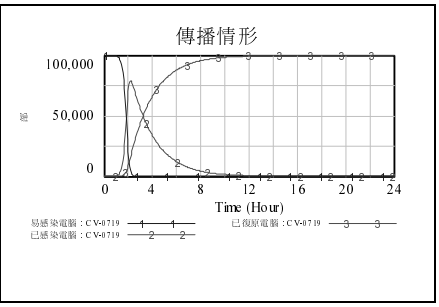
圖 12：防毒軟體公司啟動自動通報機制且使用者防疫力提升至 0.3 的傳播情形

本研究將用戶端有無採用通報機制以及是否使用防毒疫苗的情形做交叉分析，分別為方案一至方案四，整理如表 2，並以已感染電腦達高峰的時間、已感染電腦達高峰之數量及已感染電腦達高峰後下降的速度為指標，衡量各方案的績效表現，整理如表 2。

表 2：防治政策交叉分析

防治政策—疫苗 / 防治政策—自動通報機制	使用疫苗 [a]	無使用疫苗 [b]
無採用自動通報機制 [c]	方案一： 已感染電腦高峰在第 4.9375 小時，占 60.84%；已恢復電腦在第 10.75 小時達 64%以上 	方案二： 已感染電腦高峰在第 2.25 小時，占 94.39%；已恢復電腦在第 10.75 小時達 59.34%以上 
有採用自動通報機制 [d]	方案三： 已感染電腦高峰在第 5 小時，占 35.31%；已恢復電腦在第 10.75 小時達 97%	方案四： 已感染電腦高峰在第 2.1875 小時，占 79.13%；已恢復電腦在第 10.75 小時達 98.9%





a 用戶端使用防毒軟體公司所提供的最新防毒疫苗，病毒感染力降低至 0.2

b 用戶端沒有使用防毒軟體公司所提供的最新防毒疫苗，病毒感染力為 0.4，防疫力為 0

c 用戶端沒有採用自動通報機制，平均空窗期為 10 小時

d 用戶端採用自動通報機制，平均空窗期縮短為 2 小時

表 3：各方案之績效表現

衡量指標	績效表現優先順序
已感染電腦達高峰的時間	方案三、方案一、方案二、方案四
已感染電腦達高峰之數量	方案三、方案一、方案四、方案二
已感染電腦達高峰後下降的速度	方案四、方案三、方案一、方案二

方案三在已感染電腦達高峰的時間指標中，發生的時間最晚，其次依序是方案一、方案二與方案四。從結果可知，使用疫苗的方案在此衡量指標中表現較佳，其表示在無法避免感染電腦病毒的情況下，疫苗的有效性有助於延緩大量感染的時間，並提升用戶端的反應時間。在有無採用自動通報機制的情況下，比較已感染電腦達高峰之數量，發現採用自動通報機制的方案三與方案四的表現都比無採用自動通報機制的方案一與方案二還好。這表示自動通報機制可以控制已感染電腦達高峰量。從表 2 中各方案的已感染電腦曲線計算斜率，得到已感染電腦達高峰後下降的速度由快到慢依序為方案四、方案三、方案一、方案二，由此可知採用自動通報機制的方案，對電腦病毒感染疫情的控制能力較強，因此能在已感染電腦數達高峰後，以較快的速度控制已感染數量。

自動通報機制對於控制已感染電腦的高峰量以及疫情下降的速度有較強的成效；而疫苗的有效性則與已感染電腦的高峰時間發生的早晚有關。由上述模擬可證明，定期更新病毒碼雖然可以但並不能完全有效抑止病毒散播，除非病毒碼確定是有效，這時自動通報機制就顯得非常重要，因其可以確保病毒碼可以對抗最新病毒，如此將有效控制已感染電腦的高峰量以及疫情下降的速度，故自動通報機制與疫苗必須相輔相成。用戶端無法絕對避免電腦病毒的侵害，假設發生電腦病毒感染事件，當然希望儘量減少傷害，並且能快速控制疫情。因此建議用戶

端，在採購安全防護設備時若經費允許購買具有自動通報機制的設備，則應優先考慮採購，如此將可以對疫情的控制盡到一部份心力。

綜合上述分析結果，本研究發現：(1)電腦接觸外來媒介的頻率、病毒感染力、電腦數量對於電腦病毒感染速率具敏感性，尤其以電腦接觸外來媒介的頻率為最；(2)透過用戶端通報異常狀況，存在時間滯延，會延誤防毒疫苗的研發時程，因此減緩電腦病毒散播的效果稍弱；(3)自動通報機制較能有效控制高峰期的已感染電腦數量並縮短疫情持續時間，故防治效果較佳。就電腦接觸外來媒介而言，現今行動裝置等可攜式媒體眾多，企業組織為防止資訊資源被破壞，多遵循 ISO 27001 A.10.7.1 制定可移除式媒體的管理（ ISO 27001 2005），限制或禁止內部成員使用如 USB、磁碟機等可攜式媒體。但企業以營運為考量，不可因網路可能帶來電腦病毒而中斷網路的使用，因此有賴自動通報機制與防毒疫苗來防護高危險性的接觸。此外，透過自動通報機制比藉由用戶端通報更能即時反應異常狀況以縮短時間滯延，故自動通報機制在電腦病毒防治上扮演非常重要的角色。

三、隔離政策

「早期發現、立即通報、有效隔離和找出病原」是疾病感染管制的原則。隔離政策是世界各國政府與衛生醫療組織在抑制疾病傳播的一項重要公共衛生做法。雖然電腦病毒的傳染模式與生物學的病毒運作模式十分相似，但現代人極度依賴網路，以致於隔離政策在現有電腦病毒防治政策中較不被接受。本研究將隔離政策納入感染電腦擴散流中並進行模擬，修改後的感染電腦擴散流如圖 13 所示。一旦發現電腦受感染時，即切斷該電腦與外界的連繫，以避免傳染更多電腦，並進一步對被隔離的電腦進行復原。假設Q_0表示被隔離電腦之初始值，qr表示隔離率，QR表示隔離速率，qrr表示隔離後的復原率，QRR表示被隔離後的復原速率，則被隔離電腦（Q）與復原電腦（R）之模式可用公式(4)表示：

$$\begin{cases} QR = I \cdot qr \\ Q = INTEGRAL(QR - QRR, Q_0) \\ QRR = Q \cdot qrr \\ R = INTEGRAL(RR + PR + QRR, R_0) \end{cases} \tag{4}$$

當使用的電腦感染病毒時，可能只有部份的使用者願意執行隔離政策，因此被隔離的數量為已感染電腦乘上隔離率；同理，被隔離的電腦中，可能只有部份被及時救援，所以成為已復原電腦的數量是被隔離電腦乘上隔離後復原率。實施隔離政策後，復原電腦（R）除了免疫與感染後復原的電腦之外，還包含因感染而被隔離，之後再復原的電腦。

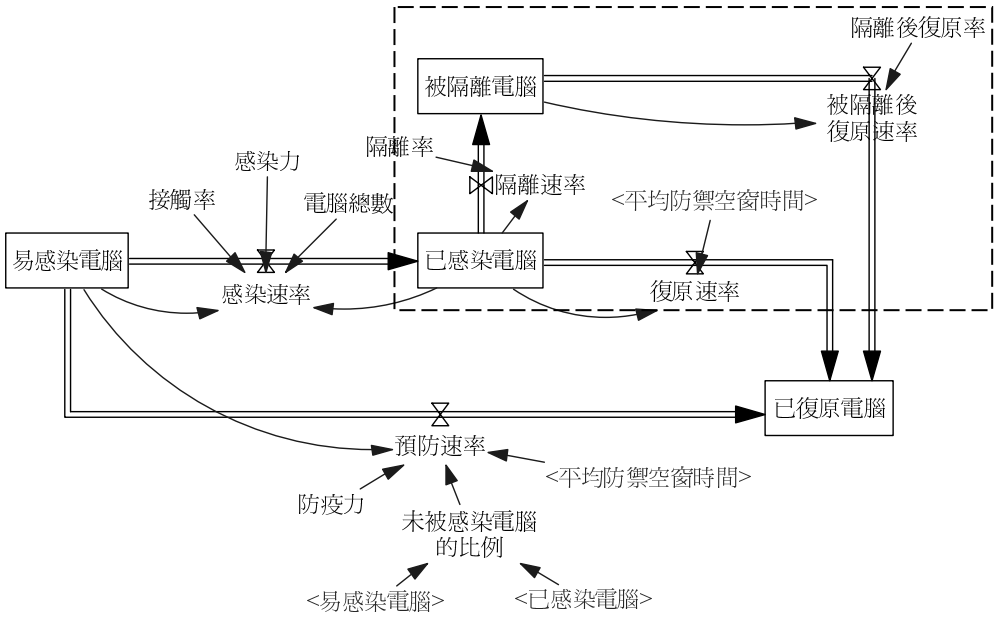
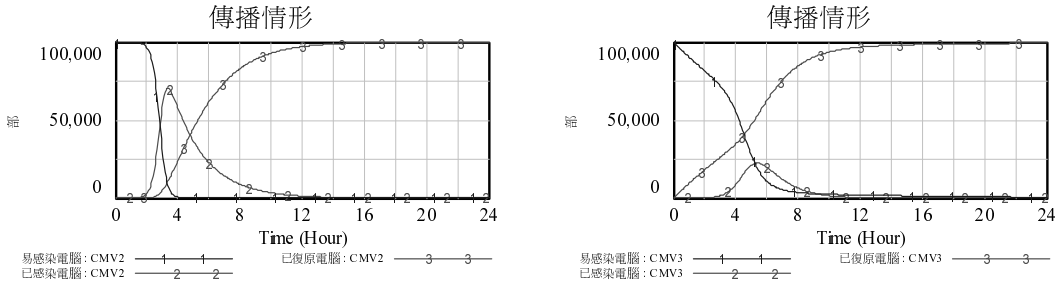


圖 13：加入隔離政策後的感染電腦恢復流（虛線框住部份）

加入隔離政策後的電腦病毒傳播情形如圖 14 所示。當隔離率 = 0.3；隔離後復原率 = 0.7，其餘變數之初始值不變，其傳播情形如圖 14(a)。與圖 6 相比，很明顯的可看出已感染電腦的傳播情形和緩許多。我們將用戶端防治政策再進行交叉分析，表現績效最好的方案三與隔離政策結合，結果顯示加入隔離政策更可能抑制已感染電腦的散播（如圖 14(b)）。



(a)隔離率 =0.3；隔離後復原率 =0.7　　(b)方案三結合隔離政策後的傳播情形

圖 14：加入隔離政策後，易感染、已感染與已復原電腦的模擬結果

就電腦病毒隔離政策而言，目前具體的作法是防毒軟體偵測到疑似被感染的檔案後，將檔案移至隔離區，但此作法無法阻止被感染電腦與外界接觸。本研究認為，依據現有的網路環境與軟硬體技術，可將隔離政策建立在分散式架構或雲端計算環境中，透過代理人執行。此代理人主要的工作如下：(1)蒐集電腦病毒最新特徵資料與使用者端遭受電腦病毒攻擊事件的記錄；(2)派送最新的電腦病毒特徵資料給使用者端；(3)當發現有最新電腦病毒攻擊手法時，自動通報伺服器端進行處理；(4)當使用者電腦被感染時，代替被感染電腦執行存取行為。因此，已被感染的電腦是透過代理人存取網路資源，使用者不會與網路完全切斷，但又可以阻斷被感染電腦散播病毒。

伍、結論與建議

一、研究結果說明

本研究以系統動力學探討電腦病毒的傳播與擴散以及防毒政策之效果評估，我們以傳染病模型為基礎，建立了電腦病毒傳播與擴散的系統動力學模型，加入用戶端主動更新病毒碼以避免電腦遭受病毒攻擊的行為，以及考量防毒政策對電腦病毒擴散的影響，因此更符合真實的現況。敏感性分析結果顯示電腦接觸外來媒介（如網路、USB、磁碟片等）的頻率對電腦病毒感染速率與擴散最具敏感性，其次才是電腦病毒感染力與電腦數量（包括個人電腦、主機、行動裝置等）的增加。現代人仰賴網際網路，加上數位產品充斥，一旦感染電腦病毒，實際的擴散速度與模擬結果相比較將會有過之而無不及，值得警惕。

依據本研究模擬的電腦病毒防治政策，其結果整理如下：

1. 當防毒疫苗有用且使用者資訊安全認知提高，主動做自我防疫時，則感染電腦病毒數量會明顯降低許多。當使用者能做到自我防疫時，防毒軟體公司的技術能力則是有效降低已感染電腦數量的重要關鍵。
2. 雖然使用者通報機制大多存在於現行的資訊安全管理政策中，但模擬結果顯示些許的通報率變動對電腦病毒傳播的影響不是太大，原因是使用者通報機制存在時間滯延，會影響研發防毒疫苗的時程。
3. 防毒疫苗的有效性有助於減少大量感染的電腦數量與延緩大量感染的時間。不論是否採用自動通報機制，使用疫苗的已感染電腦的高峰時間（方案一、三）比無使用疫苗（方案二、四）延後超過兩倍的時間，因此防毒疫苗的有效性可以提升用戶端的反應時間。
4. 自動通報機制對於控制已感染電腦的高峰量有較強的成效。在使用疫苗的情境下（方案一、三），已感染電腦高峰發生時間相差不多，但所占的數量卻相差 25%以上，在無使用疫苗的情境下（方案二、四）則相差約

15%。

5. 自動通報機制對於疫情下降的速度有較強的成效。比較是否採用自動通報機制時，使用疫苗的情境下（方案一、三），已恢復電腦在第 10.75 小時的數量相差 33%；在無使用疫苗的情境下（方案二、四）則相差約 40%，其效果更為顯著。
6. 加入隔離政策後的模擬結果顯示，隔離政策能有效抑制電腦病毒傳播。

防毒軟體已成為電腦使用者必備的防毒工具，但光靠安裝還不夠，使用者一定要做自我防疫，確保防護版本為最新版本，做到電腦病毒的偵測、預防及復原等控制措施，才能降低電腦遭受電腦病毒感染的機率。此外，防毒軟體公司的技術能力占非常重要的角色，因為使用者自我防疫的有效性有賴於疫苗的有用性與即時性。防毒軟體公司的技術能力強，疫苗發展的速度就會提高，才能有效地偵測和預防電腦病毒，因此使用者必須慎選防毒軟體，否則防毒軟體將淪為裝飾品。由於使用者對電腦病毒的認識有限，當使用者發現異常情況並通報防毒軟體公司，再由防毒軟體公司分析、確認，通常存在時間滯延，因此遏止電腦病毒擴散的效能較有限，但對防毒軟體公司而言，這只是加快防禦效率的步驟之一，模擬結果顯示疫苗的有效性與已感染電腦高峰時間的早晚有關，而自動通報機制則是加快防禦效率的主角，其能有效控制已感染電腦高峰的時間與數量以及疫情下降速度，因此自動通報機制相當重要，但要使電腦病毒感染情形降到最低，兩者是缺一不可的。然而，要抑制病毒繼續傳播，公共衛生政策上傳統的作法即是實施隔離政策，斷絕被感染者與外界的接觸，但在電腦病毒的防治上卻較不被人接受。一方面是使用者根本不知道電腦已被感染，另一方面是使用者太過依賴網路，因此多半不願意被隔離。本研究針對這個問題，提出網路代理人機制，雖然實際架構仍有待開發，但此機制能讓隔離措施有效地抑制電腦病毒傳播，又可讓使用者在被隔離的情況下仍能接收網路上的資訊，值得防毒軟體與資訊安全廠商參考。

二、研究貢獻

分為學術以及實務上的貢獻，分述如下：

（一）學術貢獻

1. 目前以管理面探討的資訊安全相關研究較少，其中以資訊安全政策為研究主題的文獻更少，因此本研究可補充這個缺口，增加資訊安全管理方面的研究。
2. 資訊安全管理與政策研究多採用問卷調查法，但此法可能會遇到可取得的研究樣本獲取不易而導致回收率過低的問題。為了克服此障礙，我們採用

系統動力學為研究方法，一方面是因為此研究方法以政策設計與分析為重點，有利於評估防毒政策的成效，另一方面則是因為此方法在數據缺少的條件下仍可進行研究。

3. 由於企業在人力與成本的考量下，多採取防毒業者建議的防毒方案。依據國內外的統計顯示，企業組織主要採取的防護政策有安裝防毒軟體、防火牆或入侵偵測系統（行政院主計處 2010; CSI 1999-2008）。而現行的資訊安全管理系統，與惡意程式相關的控制措施也強調用戶端通報機制的重要性。然而，光採用防毒軟體是不是防禦能力就比較弱？是不是一定要配合其他防毒政策才能有效？什麼樣的組合政策才是最有效的？這些問題至今沒有研究可以證實。因此，本研究以 ISO 27001（2005）中與惡意程式相關的控制措施為基礎，測試用戶端防毒政策對電腦病毒傳播的影響，並驗證了現行使用者防毒政策的有效性。

（二）實務貢獻

1. 從資訊安全管理的角度來看，要減少電腦病毒攻擊必須從站在第一線的使用者開始著手。因此有必要讓使用者了解電腦病毒防範政策與其績效表現。以企業的角度，人力與成本的考量尤其重要，因此需要了解應採用何種防治方案才能以最少的成本達到最好的效果。而本研究主要探討電腦病毒防範政策的防毒成效，模擬出的防範建議可提供給實務界參考。
2. 現今生活離不開電腦網路，電腦病毒認識與防治應為全民所必須具備的素養。在資訊科技進步的同時，人民也要提高資訊安全認知，才可以減輕網路所帶來的負面影響。若使用者對電腦病毒存有不正確的觀念，導致戒心不足，則容易反覆受到電腦病毒威脅。本研究以系統的角度描述電腦病毒傳播之因果關係，並從使用者觀點探討電腦病毒之防治政策，有助於讓使用者了解電腦病毒傳播之始末、可採取的防治政策以及最佳的防治措施。所謂「病毒防治，人人有責」，民眾對電腦病毒傳播行為有正確的認識後，對可能會受到的危害自然會有所警惕並小心防範。
3. 近年來許多資訊服務提供者投入雲端運算的服務與架構開發，主要是因為雲端運算具有即時偵測、可擴充性、持續性、低成本等特性，非常適合快速、多元的網路服務趨勢。因此，本研究的模擬結果與提出的概念性隔離作法，可提供防毒軟體與資訊安全廠商參考，藉此評估並設計如何在分散式或雲端架構下，提供更完善的網路安全防護與服務。

三、研究限制

為了解電腦病毒的生態，本研究利用系統動力學進行初步的分析與模擬，未

來將深入探討更多相關的變數與模組，此外仍有以下三點研究限制尚待克服：

1. 本研究議題的參與者應包括電腦病毒製造者，但現實環境中這個群體的成員行事低調不願曝光，因此要找到願意接受訪談的人，實屬困難，因此本研究僅依據文獻假設電腦病毒製造者與防毒軟體公司兩者之間存在競爭的關係。
2. 電腦病毒可能是電腦病毒製造者察覺系統弱點後所製造，因此防範電腦病毒的方法，除了自防毒軟體公司下載更新病毒碼和掃瞄引擎之外，使用者也必須適時下載修補程式，以修補系統的弱點。然而本研究模型只包括使用者接種疫苗，因此無法呈現系統軟體修補程式與電腦病毒傳播之關係。
3. 用戶端為電腦網路使用者，大多數皆為非資訊安全專業人員，因此對電腦病毒防範的需求較迫切，故其需要了解如何採用防治方案才能以最少的成本達到最好的效果，所以本研究僅針對用戶端防毒政策進行政策測試，未探討防毒軟體公司的策略。

四、未來研究方向與建議

未來可考量系統或軟體供應商所扮演的角色，將電腦系統或應用程式之修補行為納入研究模型，以探討其對電腦病毒傳播之影響。

參考文獻

行政院主計處（2010），『98 年電腦應用概況報告』，available at http://www.dgbas.gov.tw/ct.asp?xItem=28145&CtNode=5526&mp=1 (accessed 18 January 2011)。

林宜隆、黃讚松（2001），『網路犯罪學之探討』，*中央警察大學學報*，第三十八期，頁 325-348。

張宏琳（2007），『網路蠕蟲傳播過程的系統動力學模型研究』，未出版碩士論文，中國陝西師範大學智能信息處理與信息安全研究所，中國。

郭家宏（民 94），『從組織決策觀點探討資訊安全控管程度及其有效性之研究—以企業資訊部門為例』，未出版碩士論文，國立東華大學企業管理研究所，花蓮縣。

黃士銘、張碩毅、蘇耿弘（2005），『企業導入 BS7799 資訊安全管理系統之關鍵成功因素—以石化產業為例』，*資訊管理學報*，第十三卷，第二期，頁 171-192。

黃經洲、陳加屏、艾昌瑞（2009），『以系統動力學模擬登革熱擴散現象與評估防治策略效果－台南市為例』，*臺灣公共衛生雜誌*，第二十八卷，第六期，頁 541-551。

蔡思達（民 96），『以適應性結構化理論探討資訊安全管理系統導入之徵用過程與成效』，未出版碩士論文，國立臺灣科技大學資訊管理系，臺北市。

蘇建源、江婉媚、阮金聲（2010），『資訊安全政策實施對資訊安全文化與資訊安全有效性影響之研究』，*資訊管理學報*，第十七卷，第四期，頁 61-87。

蘇懋康（1988），*系統動力學原理及應用*，上海交通大學出版社，中國上海。

Albrechtsen, E. and Hovden, J. (2009), 'The information security digital divide between information security managers and users', *Computers & Security*, Vol. 28, No. 6, pp. 476-490.

Anderson, R.M. and May, R.M. (1991), *Infectious Diseases of Humans: Dynamics and Control*, Oxford University Press, Oxford.

Bailey, N.T.J. (1975), *The Mathematical Theory of Infectious Diseases and its Application*, Charles Griffin, London.

Chen, Z., Gao, L. and Kwiat, K. (2003), 'Modeling the spread of active worms', *Proceedings of IEEE INFOCOM2003*, San Francisco, California, USA, March 30-April 3, pp. 1890-1900.

Cho, K., Lee, J., Lim, J. and Moon, J. (2007), 'Verification method of network simulation for pervasive environments', *Proceedings of the Third International Conference on Security and Privacy in Communication Networks and the Workshops*, Nice, France, September 17-21, pp. 155-161.

Cohen, F. (1984), 'Computer viruses theory and experiments', *Proceedings of the 7th DoD/NBS Computer Security Conference*, Gaithersburg, Maryland, USA, September 24-26, pp. 240-263.

CSI, (1999-2008), *Computer Crime & Security Survey*, Computer Security Institute.

CSI, (2009), *Computer Crime & Security Survey Executive Summary*, Computer Security Institute.

DTI, (2004), *Information Security Breaches Survey*, Department of Trade & Industry.

Farmer, J.D. and Belin, A.d'A. (1991), 'Artificial life: the coming evolution', in C. Langton, C. Taylor, J.D. Farmer, and S. Rasmussen (Eds.), *Artificial Life II, Addison-Wesley*, California, pp. 815-840.

Ferbrache, D. (1992), *A Pathology of Computer Viruses*, Springer-Verlag, London.

Forrester, J.W. (1961), *Industrial Dynamics*, MIT Press, Cambridge.

Hoppensteeadt, F. and Waltman, P. (1970), 'A problem in the theory of epidemics', *Mathematical Biosciences*, Vol. 9, pp. 71-91.

Hruska, J. (1990), *Computer Viruses and Anti-virus Warfare*, Ellis Horwood, New York.

ISO (2005), 'ISO/IEC 27001 information technology - code of practice for information'.

ISO (2005), 'ISO/IEC 27001 information technology - security techniques - information security management systems-requirements'.

Kephart, J.O. and White, R.S. (1991), 'Directed-graph epidemiological models of computer virus', *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, California, USA, May 20-22, pp. 343-359.

Kephart, J.O. and White, R.S. (1993), 'Measuring and modeling computer virus prevalence', *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, California, USA, May 24-26, pp. 2-15.

Kotulic, A.G. and Clark, J.G. (2004), 'Why there aren't more information security research studies', *Information & Management*, Vol. 41, No. 5, pp. 597-607.

Ludwig, M.A. (1996), *The Little Black Book of Computer Viruses*, American Eagle Publications, Arizona, USA.

Mishra, B.K. and Pandey, S.K. (2010), 'Fuzzy epidemic model for the transmission of worms in computer network', *Nonlinear Analysis: Real World Applications*, Vol. 11, No. 5, pp. 4335-4341.

Murray, W.H. (1990), 'The application of epidemiology to computer viruses', in Harold Joseph Highland FICS (Eds.), *The Computer Virus Handbook*, Elsevier Science, Oxford, pp. 15-25.

Peter, S. (2005), *The Art of Computer Virus Research and Defense*, Addison Wesley Professional, Boston.

Piqueira, J.R.C. and Araujo, V.O. (2009), 'A modified epidemiological model for computer viruses', *Applied Mathematics and Computation*, Vol. 213, No. 2, pp. 355-360.

Post, G. and Kagan, A. (2000), 'Management tradeoffs in anti-virus strategies', *Information & Management*, Vol. 37, No. 1 , pp. 13-24.

Qing, S. and Wen, W. (2005), 'A survey and trends on Internet worms', *Computer & Security*, Vol. 24, No. 4 , pp. 334-346.

Senge, P.M. (1990), *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday, New York.

Silva, L. and Backhouse, J. (2003), 'The circuits-of-power framework for studying power in institutionalization of information systems', *Journal of the Association for Information Systems*, Vol. 4, No. 6, pp. 294-336.

Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010), 'Circuits of power: a study of mandated compliance to an information systems security De Jure standard

in a government organization', *MIS Quarterly*, Vol. 34, No. 3, pp. 463-486.

Stallings, W. (2006), *Cryptography and Network Security Principles and Practices (4nd ed.)*, Pearson Prentice Hill, New Jersey.

Sterman, J.D. (1989), 'Modeling management behavior: misperceptions of feedback in a dynamics decision making experiment', *Management Science*, Vol. 35, No. 3, pp. 321-339.

Sterman, J.D. (2000), *Business Dynamics: System Thinking and Modeling for a Complex World*, McGraw-Hill, New York.

Sterman, J.D. and Wittenberg J. (1999), 'Path dependence, competition, and succession in the dynamics of scientific revolution', *Organization Science*, Vol. 10, No. 3, pp. 322-341.

Wang, F., Zhang, Y., Wang, C., Ma, J. and Moon, S. (2010), 'Stability analysis of a SEIQV epidemic model for rapid spreading worms', *Computers & Security*, Vol. 29, No. 4, pp. 410-418.

Whitman, M.E. and Mattord, H.J. (2008), *Management of Information Security (2nd ed.)*, Thomson Course Technology, Boston.

Wierman, J.C. and Machette, D.J. (2004), 'Modeling computer virus prevalence with a Susceptible-Infected-Susceptible model with reintroduction', *Computational Statistics & Data Analysis*, Vol. 45, No. 1, pp. 3-23.

Yang, Y., Fang, Y. and Li, L.Y. (2008), 'The analysis of propagation model for Internet worm based on active vaccination', *Proceedings of Fourth International Conference on Natural Computation*, Jinan, China, October 18-20, pp. 682-688.

Yuan, H., Chen, G., Wu, J. and Xiong, H. (2009), 'Towards controlling virus propagation in information systems with point-to-group information sharing', *Decision Support Systems*, Vol. 48, No. 1, pp. 57-68.

Zou, C.C., Gong, W. and Towsley, D. (2002), 'Code red worm propagation modeling and analysis', *Proceedings of 9th ACM Symposium on Computer and Communication Security*, Washington, DC, USA, November 18-22, pp. 138-147.