發展電腦病毒之災害應變的決策模擬系統

戚玉樑　　陳毅瑞
中原大學資訊管理研究所　　中原大學資訊管理研究所
maxchi@cycu.edu.tw　　g9894027@cycu.edu.tw

摘要

網際網路的發展帶動了資訊科技的成長，資訊科技的成長卻也成為了電腦病毒攻擊的溫床，在這些充滿威脅性的病毒攻擊下，如何將電腦病毒所引起的災害降低，企業的即時應變方式是重要的決策問題，因此本研究將藉由使用知識本體(Ontology)的架構下結合災害復原規劃(Disater Recovery Plan；DRP)的方式，針對電腦病毒所造成的災害，藉由訪談領域專家以及部門決策者的方式，來建立災害應變決策情境並找尋出適用的應變方法，推論給決策者輔助決策的災害應變的專家系統。建制災害復原計畫，所要達到的目的在於組織營運不中斷，以及當災害發生之時，災害復原計畫要能夠確保組織當中最有價值的資產不會遭到破壞或損毀，在本研究的災害復原計畫下，首先假定電腦病毒可進行偵測，參考過去電腦病毒的災害復原計畫，建立應變模型，組織對於相同的電腦病毒卻有著不同的情境其災害所適用的應變方法也不相同，因此藉由本體來模擬情境並且結合群體決策的方法來推論出適用的應變方法，輔助決策者來進行災害復原。

關鍵詞：知識本體、專家系統、群體決策、災害應變、決策情境。

1. 緒論

1.1 研究背景與動機

隨著網際網路的普及人們對於資訊社會有著高度的依賴，電腦病毒出現所造成的災害，對於企業組織造成了龐大金額的損失，為了降低災害對於組織資產所造成的損害而建立災害復原計畫。網路對於人們的生活型態以及企業的商業運作有著巨大的轉變，而資訊安全的風險問題也隨之提高，在這些風險下，電腦病毒的攻擊促使了企業組織投入資訊安全相關的資金也隨之提高，資策會資訊市場情報中心(MIC)統計，台灣於 2008 年對於資訊安全市場所投入的資金為新台幣 142 億元，預估到 2011 年時所投入的資金將會達到 218 億元，平均每年成長約 15.5%；在 2009 年有 30%的金融業以及醫療業計畫增加資訊安全的投資，從上描述將瞭解降低資訊安全投資的企業不到 10%，根據美國消費者聯盟所做統計過去在 1999 年 Melissa 電腦病毒其造成全球數百萬部電腦的影響，估計造成全球 8,000 萬美元的損害，由上述可知企業組織對於電腦病毒的攻擊所造成旁大的損失，因此近年來企業組織對於資訊安全所投注的金額也陸續的增加。

目前科技的進步，防毒軟體廠商對於病毒的出現，已經能夠進行偵測，而對於被偵測的電腦病毒可能入侵於組織的電子設備當中，並對造成某種程度的傷害以及擴散，針對災害的發生，組織對於災害所造成的損害，藉由建立災害復原計畫，期望能夠在災害發生的同時，有效的降低災害對於組織資產上所造成的損害。災害復原計畫主要藉由定義、分級並保護組織最有價值的資產，以使災害發生的同時能夠將損失降到最低，災害是任何意外事件以及藉由各種媒介導致 IT 功能損害(Peter W., 1996)。另外，在災害復原計畫的使用當中，比較災害復原計畫與系統生命週期理論的差異，提出一個規則及案例知識來表達災害復原計畫，並發展一個結合規則式推理(RBR)及案例式推理(CBR)優點的災害復原計畫推理法則雛形系統（王仁宏，

2003)，除此之外在對於組織經營者的角度下必須有一個完整的計劃定義災害復原所需的資源、包括人事、硬體及基礎架構(Howard,1997)。

過去災害復原計畫按照固定的應變框架來保存組織的重要資產，其復原計畫內容也並無考量到現況的不同而給予不同的應變決策，在這樣不彈性框架下，並沒有考量到針對災害發生的同時，對於相同的電腦病毒所造成的災害下，部門在當時所面臨的情境有所不同，在此一情況下建構出知識本體為基礎之災害復原規劃的決策模擬系統，當災害發生時部門將針對現況的不同，而給予應變方法，如果不考慮現況的情況下，進行應變決策，則會增加風險的發生，在根據部門現況給予應變方法，並藉由推論的方式，推論給決策者，決策者則根據這些應變方法來挑選適用的來給予進行應變決策，此方法方能降低災害對於組織的傷害。

災害應變計畫是不管企業、政府機關或者學校處室當遭遇災害時所採取的應變措施，並持續維持正常營運，而意外事故的發生在所難免，因此事前的準備工作則有賴於緊急應變計畫的想定與排練，因此當災害所造成的傷害時，現場工作人員也能夠瞭解狀況並掌握狀況，接著執行應變計畫當中的各項工作，藉由災害應變計畫的建制才能夠大幅度的降低當災害造成時所產生的風險。

組織營運的過程中，會充斥著許多可預期以及不可預期的挑戰與變化，許多異常事件若沒有一個良好的制度並妥善的管理，那其異常事件將急速的擴大成為危機與災難，因此災害應變計畫的建立期望能在災害發生的同時，能夠縮短災害造成營業中斷的影響時間，當企業面對電腦災害發生的同時藉由災害應變計畫的建制，來加速復原其受損害的設備能夠盡早重新上線。

當災害發生之時 IT 從災害事件中復原，其復原的時間是最重要的關鍵，組織期望復原的時間縮短，才能夠有效的降低組織成本，反之復原的時間拉長，組織所耗損的成本就會相對的增加，因此在災害復原計畫的建制上就必須要全盤考量，考量組織當中有哪些部門(例:產品部門、銷售部門、人力部門、開發部門、會計部門)，而部門擁有哪些資源(例:軟體、硬體…等)，當組織部門遭遇到威脅，當下所要考量的情境有哪些，由於部門的不同，因此所提供的應變情境也相對的不同，在決定好情境之後部門針對電腦病毒所造成的災害，藉由本體推論其部門適用的應變方法，給予決策者來做最後的應變決策，並選擇成本最低的方式來執行復原計畫，以降低災害發生後的損害，來達到組織永續營運的目的。

1.2 研究問題

目前的災害復原計畫,都是以利益考量下建置的災害復原計畫，其復原計畫的內容都是以一個災害復原框架的流程，並按照框架的流程來進行災害的應變，這些災害復原計畫所制定的內容以及目標都是以企業整體的資源下去考量，但是，在電腦病毒災害發生之時，其所造成的災害由使用過去的災害應變方法並無法將災害所造成的損失降至最低，因此本研究對於災害復原計畫建置的問題將會歸類為以下兩點：

1.受限於災害復原計畫通常都事前訂定,企業因而對病毒的災害應變缺乏彈性:

根據組織內不同的部門，其所考量的項目也將會不同，軟體、硬體、環境都有著不同，在面對災害發生之時，當下所要考量的要素繁多，組織部門要如何從中找尋方法來解決利益衝突以及風險考量並綜合這些要素來進行決策，因此災害復原計畫應該要當災害發生之時，當下部門所面對不同的情況時，能具有彈性的進行修改，過去的災害復原計畫框架，在災害發生之時並無法快速的復原、復原的計畫不夠彈性，這樣對於企業相對所造成的風險也會增加。

2.針對組織所建置的災害復原計畫無法提供重複使用:

本研究藉由以知識本體的方式所建立的病毒災害復原計畫，是期望當組織遭遇病毒攻擊災害之時，病毒對於組織所造成的災害可藉由使用知識本體的方式模擬出組織各部門遭遇電腦病毒災害之時，各部門所要考量的威脅性、當下災害發生所選用方法的衝突性，來考量並推論出適用的應變方法，而本系統最終的訴求是希望能夠達到多個部門對於災害發生的當下，其部門對於災害所提供的情境，並提出應變方法給予組織的最後決策者來做應變方法的選取，而最後的決策者可能是組織當中的 CEO 或 CIO 來做最後的決策,使用知識本體建置的方式，只要經由修改實例資料即可符合另外一間公司所使用，過去的災害復原計畫並不夠彈性的應用於每一種企業，因此要做大幅度的更動以及修改。

1.3 研究目的

針對電腦病毒的災害,本研究希望藉由使用知識本體的方式來根據組織中不同的部門針對電腦災害的發生根據當下的情境，組織部門的部門決策者藉由此情境給予彈性的應變方法，並將方法提報給決策者，而決策者從中挑選適用的應變方法來支援決策，即可達到群體決策的目的，對於電腦病毒所造成的災害性，過去的作法是由防毒專家對於所發生的災害進行分類，如果分類為電腦病毒災害，那將針對所發生的電腦病毒災害，來給予災害應變的方法，來解決災害所帶來的傷害（例:疾風病毒-當電腦中了此病毒，則會造成系統不穩定或應用程式無法執行，及自動關機等異常情）,但是這樣的方法在電腦病毒災害發生之時,無法將災害的成本降至最低。本研究為了期望能夠降低災害所造成的傷害，因此先從組織部門的部門決策者對於電腦病毒所造成災害，藉由參考過去的災害復原計畫的應變方法，但是，組織各部門對電腦病毒所造成的災害對於其部門當下的情境中所重視的程度以及項目有著著實的不同點，對於不同的情境，其部門所採取的行動也會不同，因此各部門將會在情境的考量下來合議出適用於其部門的應變方法，有著適用的應變方法，才能夠降低組織因為災害所造成的額外成本，災害復原計畫如果不夠無法達到彈性的修改則無法確實的降低其所需的資源(例:人力資源、…等)，因此本研究希望藉由知識本體的方式，將組織各部門針對電腦病毒所造成的災害，建置應變模型，並根據各部門的情境下推論出適用方法給予決策者來輔助決策。

2. 文獻探討

2.1 電腦病毒的分類

電腦病毒是一種具有自我複製以及感染能力的電腦程式，它會使電腦產生不尋常的錯誤訊息出現，並且造成其他的檔案或程式遭到感染，創造病毒的製作者可以根據其動機來進行指令的傳輸來達到其目的。 (例:刪除或者修改檔案、網路阻斷攻擊造成網路癱瘓) (Fred Cohen, 1984)。

全世界第一隻的電腦病毒是在 1987 年所誕生的大腦病毒，它是由一對巴基斯坦兄弟所撰寫，其原先的目標在給予那些非法拷貝軟體的人一些懲罰，不過後來被一些有心的人士將其改寫並作於其他用途進而發揚光大，1988 年，第一個網際網路病毒”蠕蟲”的誕生，其特點在於自動的自我複製並且造成網路速度的癱瘓，蠕蟲的出現也代表著病毒正式進入了網路時代，電腦病毒是一段惡意程式的程式碼，會將自身附掛在檔案或者程式當中，當檔案或者程式的執行時及觸發電腦當中的惡意程式碼並造成軟體、硬體或檔案的損害。
現今電腦病毒的演進速度非常之快，並藉由網路的方式快速的散播，而這數量也一直在不斷的攀升，卡巴斯基以及趨勢科技都針對變化快速的電腦病毒進行分類探討，譬如趨勢科技公司針對 2001 年所爆發的 Code Red 電腦病毒,為其定義為駭客型病毒的分類，而賽門鐵克公司也對近年網路上的威脅新增惡意程式碼的分類。
近年來對於病毒的相關研究也相繼的熱

絡，例如使用靜態分析的技術萃取出病毒的特徵 ，再利用資料探勘的方式進行有效偵測出現有的惡意程式(蕭崑賢，2005)。使用演算法藉由字串比對的方式並且於記憶體的使用效率來辨識出已知的惡意攻擊字串，來防止惡意程式的入侵(戴鈺唐，2007)，另外也有透過負面表列清單並採取平行比對手法，搭配正面表列清單與決策樹模型判斷所形成之『混合偵測演算法』，對其進行偵測與分析來提高作業系統的防護能力 (陳英裕，2008)除此之外也有學者提出一種使用語意學習方式來檢測出惡意軟體特徵的演算法，可檢測出惡意軟體(Christodorescu & Jha, 2003)。

2.2 災害復原規劃

災害復原規劃（Disaster Recovery Plan）為企業永續經營（Business Continuity）當中的一個環節，在組織企業當中，除了做好事前的預防以及資訊安全的防護，企業永續經營也成為組織所關注的一環。災害復原規劃其被定義為當災害發生之時，建立一套標準作業程序，可以在組織商業機能在遭受中斷之時，可以獲得快速回應能力的應變計畫，藉由規劃以及建置災害復原計畫，企業組織可以在受到破壞時，以最短的時間恢復組織商業機能使其正常營運，是災害復原計畫的最大目的，使商業機能中斷原因包含了天災、人為災害、系統損害、病毒災害、系統安全問題等，災害復原計畫是以全盤的考量整個組織企業所擁有的資源、商業機能到整個組織。災害復原規劃目的在於組織發生災害時能夠將災害所造成的損失降至最低，以及保障組織當中最有價值的資產(Fallara, 2004)，災害復原計畫在撰寫的過程應按照邏輯規則來進行，並撰寫在標準的格式下(Wold, 2002)。

Bryson 於 2002 年認為災害復原計畫提應包涵四種屬性

(1)可行性:從資源的角度去切入，來評估技術非技術人力、軟硬體以及時間是否可行。

(2)完整性:復原計畫是否有考量到整個組織的資源以及功能免於因災害所造成的重大損害。

(3) 一致性: 在災害復原計畫的執行時，在資源的使用上是否有一致性也是所要考慮的重點。

(4) 可靠性:為了達到組織營運不中斷的目標，復原計畫的可靠性則為其重要。

本研究針對災害應相關的文獻按照年度，彙整出具有代表性的文獻探討關於災害應變計畫的研究。

2.3 群體決策

在企業當中，對於發生的災害，並不是單單以單一部門的單一決策者，所給予的解就是最佳解，而是企業整體針對災害所造成的影響，並藉由組織各部門的決策者一同來商討並且合議出適合的應變方式來給予合用的解答，這樣的決策模式才是考量組織整體架構以及價值。

決策者面臨的內外部環境日益複雜多變，許多問題的複雜性不斷提高。 相應地，要求綜合許多領域的專門知識才能解決問題，這些跨領域的知識往往超出了個人所能掌握的限度。

對於那些複雜的決策問題,往往涉及到目標的多重性、時間的動態性和狀態的不確定性，這是單純個人的能力遠遠不能駕馭的。群體決策因其特有的優勢得到了越來越多的決策者的認同並日益受到重視。

決策者個人的價值觀、態度、信仰、背景有一定的局限性。 然而，這些因素會對要解決的問題類型和解決問題的思路和方法產生影響。如果決策者格外關注動物保育，就會用生態平衡的觀點來考慮問題。另一方面，決策者個人不可能擅長解決所有類型的問題，進行任何類型的決策。

決策相互關聯的特性客觀上也要求不同領域的人積極參與，積極提供相關信息，從不同角度認識問題並進行決策。

產生群體決策的原因：

(1)分散決策責任-群體決策對於決策者的角度來說使得決策者能夠對於決策的責

任以及風險的分散，即使決策失敗也不會由一個人單獨承擔，

(2)群體氛圍-群體成員的關係越好，對於問題的想法越一致，則決策時就缺乏衝突的力量，越可能發生群體轉移。

(3)領導的作用-群體決策往往會因為領導的影響，而這些人的冒險性或保守性會影響到群體轉移傾向。

(4)文化價值觀的影響-群體成員將會按照其社會文化與背景的不同來反映到其群體決策的成果當中，例如:日本人做事以謹慎著稱，所以其群體決策更富於謹慎的特性。

2.4 知識本體

當災害應變計畫建立之後，所涉及的項目非常多，因此需要進行應變計畫的模擬，本研究將使用知識本體的方式，來模擬當組織部門遭遇電腦病毒災害之時，需要考量哪些因素以及部門針對應變方法要做哪些調整以及修改，來輔助決策者做決策的模擬，後面將針對知識本體以及知識表示法的介紹。

知識本體源自於哲學上探究萬物而加以歸納分析的學說，並且遵尋著對萬事萬物追本溯源的概念並加以描述，且說明事物是由哪些物件所組成，以及瞭解物件與物件之間彼此的關聯性。而本體論一詞最早出現於 1613 年，由 Rudolf Gockel 及 Jacob Lorhard 兩位學者，在各自著作中(Lexicon philosophicum & Theatrum philosophicum)所提出知識本體將特定領域知識明確的表達出來，並藉由已知的顯性關係，推導致未知的隱性關係，因此常被定義為「知識本體論是概念化的一種明確描述」(Gruber, 1993)，學者 (Guarino, 1997)也提出知識本體是邏輯理論的集合，且是一個明確規格的概念，能夠重複設計及重複使用的知識系統元件，目前知識本體被廣泛的應用於電腦科學領域當中。

知識本體發展在知識庫的過程中分為知識本體的建置與規則推論的應用(Chi, 2008)，而其中知識本體建置的過程包涵，知識擷取、知識塑模及知識表達(Noy & McGuinness,2001)但是在知識本體的建置過程則是著重於知識擷取與知識塑模。知識擷取(Knowledge Acquisition)方式通常是取自於專家的專業知識或者書籍當中的相關知識 (Chi, 2007)並將知識做抽象化，所抽象化的方式也會與所應用領域的不同而有不同的擷取方式，而知識塑模則是將收集到的知識或資料，整合起來建立起一個完整的知識網路，可幫助我們瞭解知識的階層性以及邏輯性並可迅速的瞭解其關係，因此在知識本體建置的過程中，將概念做塑模是非常重要的工作。知識表達則是將所塑模的知識模型於電腦中轉換為系統可解讀的形式。過去研究中提到利用 Ontology 所建立的系統較傳統系統複雜，本體是經專家所訂定的知識，因此對知識庫的查詢是知識擷取有別於傳統單純以關鍵字或關聯資料庫的比對查詢(戚玉樑，2005)在。

近年來以 XML 為基礎建構知識本體的方法陸續被提出，如：RDF、OWL 等。其中 OWL(Web Ontology Language)是 2003 年 W3C 所建議的知識本體描述語言，使 OWL 成為重要的知識表達規範之一。

3.研究設計

本章節根據研究問題的描述，本研究想要解決當災害發生後，來針對所造成的災害推論出解決方案，來給予決策者作決策。因此本研究將災害的議題定義為電腦病毒災害的發生，透過現有的災害類別特徵屬性，以及找尋電腦病毒專家的解決方式及組織各部門的決策者對於災害情境提出其權重，並使用知識本體的方法，建置出電腦病毒的災害應變知識庫，幫助決策者處裡電腦災害的復原計畫。

3.1 研究架構

過去針對電腦病毒所造成的區域性或全面性災害，依靠著防毒軟體以及更新系統的方式來處理病毒，防毒軟體公司大都以電腦病毒出現後才開始針對病毒給予應

變，在新病毒出現時都以先對組織系統造成災害，因此本研究使用知識本體技術，建置出以電腦病毒災害為模型建立的知識庫系統，電腦病毒災害發生的同時，藉由參考過去的災害應變計畫並結合組織部門的部門決策者根據關注項目的不同以及現況的發生有著不同的威脅性，並合議出適用於其部門的應變對策，並給予決策者從中選擇適用的方法來進行應變的決策模擬，才能夠對組織的傷害降至最低。圖 1 為本研究的系統架構其功能描 `如下:

1. 災害應變資料萃取：當電腦病毒災害產生之時，必須先將災害的類型與因素萃取出來，並分析出此災害所影響的範圍(例:影響到組織哪些部門、影響到的內容及應變方法)，本研究針對電腦病毒所造成的災害，由過去所建立的災害復原計畫，讓組織部門的部門決策者根據各部門所關注的項目不同，因此合議出適用的應變方法。
2. 災害應變知識模型：經由資料萃取階段所建置的災害處裡資料庫中，知識收集的結果為建置知識模型的素材收集的前處理，知識塑模目的是將真實世界的情況，利用抽象化方式表達成解決其特定目標問題領域中的一般化模型，最後將模型建置於所使用的資訊系統當中，成為知識庫的知識架構，給予資料邏輯及關係的定義。因此，知識庫中所存放的是具備邏輯意義的資料，往後於知識的應用系統當中使用者只需進行查詢的動作即可完成。完成知識收集可得到重要的概念與屬性，然而，真實世界的問題是由實例之間交互產生某些關係導致，由於實例是承襲所屬概念的定義，因此只需明確定義概念之間的關係，實例自然就會繼承概念所賦予的定義，而實例之間的差異則可以藉由屬性值加以區別。
3. 規則推論：知識模型階段中建立出知識本體模型後換產出 OWL 檔;規則推論階段撰寫災後復原的規則，並經由規則語言 SWRL 的寫入，推論引擎將推論出災後復原計畫，則此結果將可以推薦決策者當遇到某類型的病毒災害可採取的適用方法。

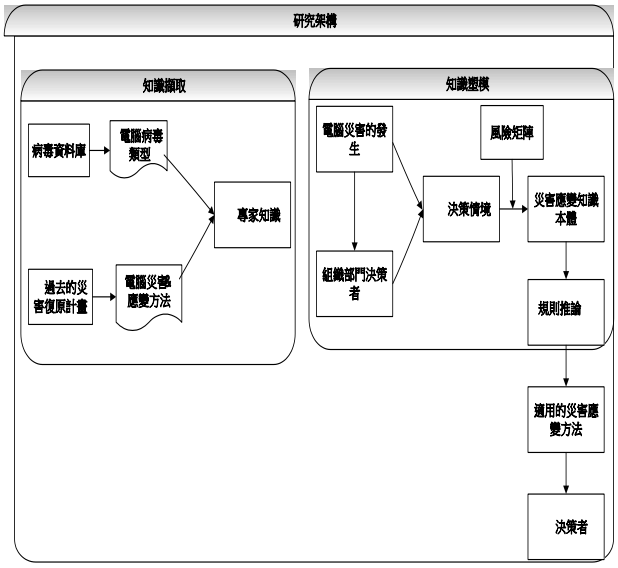

圖 1 研究架構

3.2 知識擷取

在問題領域界定後，我們需對「領域」展開知識收集的作業，以期獲得後續知識建模的素材。

- 萃取：根據文獻探討當中所發掘出災害復原規劃的特徵項目。此外，亦須取得電腦病毒廠商所提供的電腦病毒特徵，最後將這些項目歸納整理為基本的素材。
- 分析：利用心智圖法，大略分析這些素材的從屬關係，再根據問題領域逐一篩選出重要的素材。
- 轉換建置：在知識本體中，每個概念至少擁有一個屬性加以定義，因此必須將前面得到的重要素材，轉換為概念及其依附的屬性，其呈現方式為{概念：屬性 }。譬如：{公司：生產產品類型、產業別……}。

對收集過去所使用的災害應變計畫，並在這些應變計畫當中，所有屬性值符合的案例才可以被擷取，以及部份屬性案例符合也同樣可被擷取。例如資料庫損壞的案例，組織內可提供過去發生資料庫損壞的應變方法，讓使用者可重複使用類似的應變計畫，針對問題領域的界定下所蒐集的災害應變計畫，此步驟所需蒐集的工作有下列三點。

1. 電腦病毒：從過去對於電腦病毒的相關性問題作探討，從目前現存的防毒軟體公司所提供的病毒資料庫當中擷取，其電腦病毒的類型對於系統所造成的影響有哪些，並瞭解到這類型的電腦病毒所造成的電腦災害，並將這些電腦災害的內容將可萃取出知識並建置於知識本體當中。
2. 災害應變計畫：對於災害發生之時，提供災害應變計畫對於所發生的電腦災害進行應變並減輕災害所造成的影響，而災害應變計畫是企業永續計畫當中的一環，因此本研究在蒐集災害應變計畫當中，所要針對的應變計畫為電腦災害所建置的災害應變計畫，為所要擷取之目的，本研究根據台灣電腦網路危機處理中心通訊所提供電腦災害應變計畫，為研究基礎，當中所提供的應變計畫可作為本研究的屬性資料，並建置在知識本體當中。
3. 應變方法：組織部門按照所關注的項目不同，因此所產生的應變方法也相對的不同，這些應變方法根據電腦災害中的因素進行分析，來探討其對組織內部的威脅，最後比對後可能選出多種應變方法，本研究根據防毒軟體公司所提供的病毒資料庫中的病毒實例，經由防毒軟體公司的分析從中擷取出病毒災害所影響的因素與影響的範圍，並結合電腦災害應變計畫所提供應變方式，並擷取出來成為本研究的知識。

3.3 災害應變知識本體模型

研究中的知識本體建置階段，知識本體的塑模過程，包括決定知識本體的領域範圍、考量可延伸引用的知識本體模型、列舉知識本體中的重要詞彙、定義類別與類別階層、定義類別屬性、定義屬性的限制及建立實例。以下為本研究塑模本災害應變知識模型。

首先在於領域定義有許多面向，知識庫系統通常適用於解決特定的問題，問題分析即為領域再予細分問題的特徵，將其概念收集，確認要獲得的結果；知識庫系統針對特定問題提出解決辦法，因此適合於解決目標導向問題，界定明確的問題領域是知識工程發展的關鍵，知識有許多不同的面向，特別是知識庫系統較適合目標導向(Goal-oriented)的問題，因此清楚界定問題領域將是進行後續知識庫系統建置的關鍵(Chi,2009)。本研究將定義解決災害發生後所做的後續復原規畫的處裡措施，所以在決定領域的知識本體方面，以災害問題為出發點，其電腦中毒所造成的災害與應變的方式將是本研究所討論的範圍。
在本研究的災害知識本體當中，災害的種類有非常多種且災害發生的同時，會產生不同的損害，如天災造成一般性的損失、電腦病毒造成資訊系統的毀損。根據我國所訂出的災害防救體系中，災害預防的計畫不外乎有災害預防的事項、緊急應變的對策、重建的事項、其他單位的會報、災害防救的規定等(鄭美華，2003)。

在本研究的災害知識模型中，災害的內容為災害模型的主要關鍵因素，例如自然災害與軟體的災害影響的範圍內容都不盡相同，因此如何判斷發生何種災害，當此災害發生時如何對應到應變的作為。舉例來說，當電腦發生中毒災害，首先必須先確立影響的內容，在考量的內容下有硬體、軟體、系統等，因此災害的目的即是啟動災害應變計畫，在針對災害的發生所使用的應變方法。

3.4 規則推論

OWL 是用來設計知識本體的語言，為目前 W3C 所推薦的知識本體論描述語言。其主要由敘述邏輯的概念演變而來，目的為明確地表達類別的意思。本研究將採用使用 Protégé 作為編輯知識本體的工具，Protégé 為史丹佛大學醫學資訊中心開發出的工具，可以支援 OWL-based 的知識本體編輯，並作為執行知識系統的平台，成為目前較成熟的 OWL 開發工具之一(Noy et al., 2001)。並且搭配 JESS 推論引擎(Java Expert System Shell)進行知識庫內知識推理，當電腦病毒造成哪些電腦病毒災害的同時，組織部門的部門決策者，參考

過去災害應變計畫所提供的適用方法作為電腦病毒災害的解決方法，本研究將建立風險矩陣結合語意規則 SWRL 的方式，當電腦病毒災害發生的同時，電腦病毒影響的內容，藉由規則推論的方式來判定，電腦病毒所造成的災害，在風險評估下有哪些適用於組織部門的方法給決策者做輔助決策，因此本研究將嘗試建立一可結合各部門相關的威脅矩陣，判斷電腦災害於各部門的所造成威脅的程度及對於決策者所認知的威脅程度組合，進而判定該電腦災害對於部門的威脅程度，並透過 SWRL 將電腦災害所造成的威脅給予組織最高決策者進行決策的參考依據，Chi (2008)開發推論規則的二個階段步驟：

(1)藉由專家的知識經驗分析開發合理的規則步驟:

{推論屬性名稱：步驟描述 1；步驟描述 2；.. 步驟描述 n}

{推論威脅程度 Rule：從每一個被「關注項目(?x)」均擁有其 「has_部門(?x, ?y)」，針對這些項目整個組織對不同的部門會有不同的 「has_嚴重程度(?y, ?a)」，以及部門對這些項目也有屬於各部門自己認為的 「 has_嚴重程度(?X, ?b)」，透過 SWRLB 將雙方認知的權重進行加權產生對組織的威脅程度，SWRL 規則的設定}

(2) 知識工程師將規則步驟撰寫為 SWRL 規則：知識工程師須將步驟(1)的口語表達式對應至正確的概念或屬性名稱，並表達成 SWRL 規則：

(Atom1 .. Atomn → Inferred Property)。

譬如：決策情境(?x) ∧ has_部門(?x, ?y) ∧ has_嚴重程度(?y, ?a) ∧ has_嚴重程度 (?X, ?b) ∧ 權重值(?a, ?z) ∧ 權重值(?b, ?c) ∧ swrlb:add(?n, ?z, ?c) → 威脅程度 (?x, ?n)

譬如：決策情境 (?x) ∧ has_部門(?x, ?y) ∧ has_嚴重程度(?y, ?a) ∧ has_嚴重程度 (?X, ?b) ∧ 權重值(?a, ?z) ∧ 權重值(?b, ?c) ∧ swrlb:add(?n, ?z, ?c) → 威脅程度 (?x, ?n)

上述範例括號內的變數(例如：?a) 在推論運算時均會以實例代入。

決策者對於災害所關注的內容，部門都有一個認定的威脅程度(縱軸)，以及部門也有對於電腦災害的重要程度(橫軸)。該矩陣如表1所示。

表 1 決策矩陣

部門 / 決策者	可忽略	不太重要	重要	很重要	非常重要
可忽略	1	2	3	4	5
不太重要	2	4	5	6	7
重要	3	5	6	7	8
很重要	4	6	7	8	9
非常重要	5	7	8	9	10

上表是一個例子，部門所認定的威脅程度(縱軸)是被視為實例(instance)，可由使用者自訂；決策者認為其電腦災害的重要程度(橫軸)亦為可被使用者自訂的實例(instance)。在這個例子中採用五等第來區分的相關性從高度重要到可忽略，矩陣所產生的結果代表了決策者與部門對於電腦災害所產生的威脅程度。

4. 系統實作

4.1 知識收集與建置本體

本研究將建置知識本體災害復原應變計畫，對於企業發生電腦病毒災害發生之時，由於組織部門的不同，所考量的項目、風險也有著實性的不同，因此企業組織部門能夠對於災害所造成的傷害來給予不同的應變方法，以達到調適性的應變計畫，因此將透過知識庫系統適合目標導向(Goal-oriented)的問題且清楚界定問題領域的特性，建置一知識本體並以問題領域界定、知識收集、知識塑模、知識表達與推論應用等五項程序實施，其中推論應用的描述主要在雛型系統的遞送智慧在一併說明。

知識本體的設計將針對下列問題：1. 當電腦病毒災害發生之時，不同的災害其所使用的應變方法也不同；2. 電腦病毒災害對各部門的關注項目的不同，其所使用的應變方法也不盡相同，因此也造就了不同的風險程度。本研究將透過知識本體處理這些問題，建置災害復原應變計畫。

1. 建置知識本體-問題領域界定

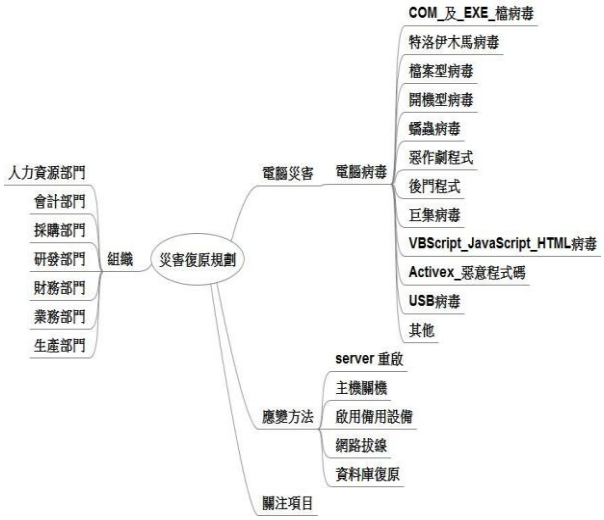

圖 2 問題領域心智圖

(1) 取材領域

首先對於防毒軟體公司所取得的電腦病毒的分類以及電腦病毒所造成災害的型態，對於所造成的災害下，將可參考 CERT 所建置的災害復原計畫，並從其中所蒐集的應變方法，來提供給組織各部門來使用，而組織各部門又按照其所關注項目的不同，對於電腦病毒災害的風險作為領域問題的素材。

對於災害復原規劃的知識擷取方式，本研究將災害復原規劃的所需素材藉由心製圖的方式來完整表現出來。

圖 3 所需素材心智圖

藉由所收集到的素材藉由表格的方式將其概念與屬性的關係描述出來，藉此瞭解其內涵 。

表 2 概念屬性表

概念	宣告屬性	推論屬性
應變方法	所解決的電腦災害	
電腦災害	Has_電腦災害相關 生產力低下 名譽受損 財產受損	
決策者	Has_關注項目 決策者掌控的部門 所出現的電腦災害	決策者採取的應變方法
部門	Has_嚴重程度 所發生的電腦災害 立即回應 系統功能性有關 組織機能有關 資料同步有關 運作環境有關 部門對於決策者 部門的關注項目	
關注項目	Has_嚴重程度 災害的關注項目 Has_部門 所關注的決策者	災害的關注項目 威脅程度
嚴重程度	權重值	

(2) 使用社群

本系統主要提供給企業組織的決策者使用，按照各部門所考量的項目不同以及風險程度的不同，按照所發生的災害提供適用的應變方法，並提供決策者來做決策模擬。此建立的災害復原計畫，可針對各企業來進行使用，只需事先透過知識的收集將產業知識建置知識本體中的實例，而組織部門也可藉由其風險的不同來提出應變方法。

(3) 應用項目

應用於組織部門對於電腦災害發生之時，可透過語意規則將適用的應變方法推論給決策者給予參考與使用。

2. 建置知識本體-知識收集

透過語領域專家討論後，萃取專家的知識並進行知識的分析，將結論轉換為概念及其依附的屬性，將主題對應至知識本體的概念，以及將特徵項目對應至概念的屬性，並以{概念：屬性列..}通式作為表達的形式，下列為本階段部份的結果。

{應變方法：立即回應;運作環境有關;系統功能性有關;資料同步有關;組織機能有關 }

{電腦災害：生產力低下;名譽受損;財產受損}

{部門:對於部門所關注的項目;部門的上司;決策情境 }

{決策者:決策者關注的項目;決策者的下屬;所出現的電腦災害;採取的應變方法}

{關注項目：部門 }

{威脅程度：權重值}

建置知識本體-知識塑模

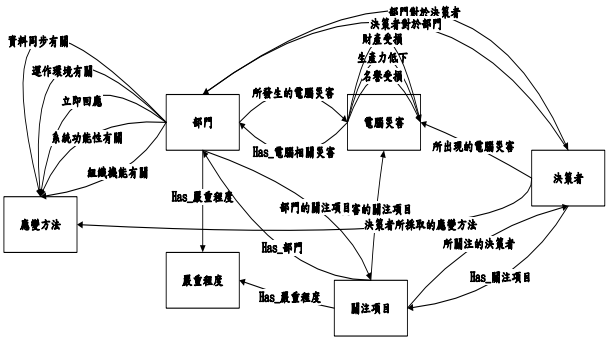

圖 4 建置知識本體模型

在此階段主要給予知識庫具備資料的邏輯性以及關係的定義。因完成知識收集可得到重要的概念與屬性，要使知識庫可以處理真實世界的問題需要藉由實例之間交互產生的關係，關係主要概分為繼承關係及擁有關係。

(1) 繼承關係：類似程式中物件技術的主從關係。例如企業與部門即具有繼承關係，亦即公司概念所擁有之邏輯定義與限制式，亦將同時存在於部門概念中。

(2) 擁有關係：概念所擁有屬性的關係即為擁有關係。例如某應變方法類別概念的實例擁有某些概念的實例。

本研究的災害復原計畫知識模型即是以探討電腦病毒的災害與組織部門所考量的項目為主，以及所考量的項目與應變方法的關係，分別解釋重要的概念關係：

（1） 電腦災害與部門之間的關係

在電腦災害發生之時，部門必須瞭解到所發生的是哪類型的災害，以及某類型的災害對於部門，所要關注的項目作為決策情境的依據考量，因此部門對於災害會有先行的假設。

（2） 部門與應變方法

當電腦災害發生之時，部門會對於所發生的災害，並且考量其關注項目，而其關注項目當中，也有著不同的嚴重程度存在，來考量採取應變的順序，並且對於其嚴重程度高的電腦災害，來優先決定其應變方法。

（3） 決策者與應變方法

當電腦災害發生之時決策者將會按照組織各部門所給予的關注項目，以及嚴重程度來判斷在此一情況下，要給予其合用的應變方法。

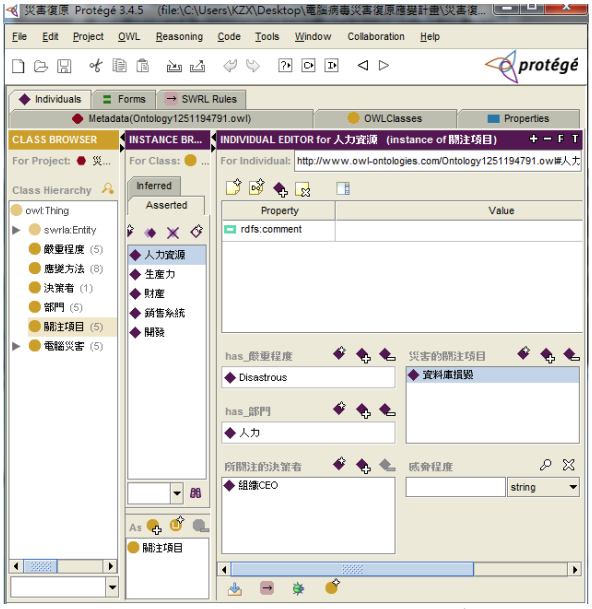

圖 5 知識本體工具 protégé 使用畫面

,

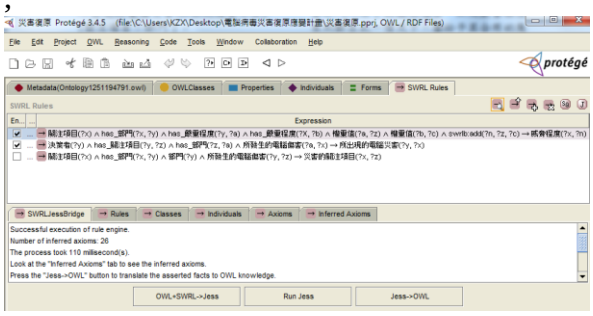

圖 6 知識本體規則推論

4.2 建置知識本體-知識表達

當完成知識塑模之後，需要將知識運用在資訊系統中，本研究所使用的 OWL 編輯軟體為史丹佛大學醫學資訊中心所研發的 Protégé，利用 Protégé 使知識可以在資訊系統中以 OWL 的方式呈現，Protégé 的編輯區域主要分為三大區域，最左的區域為概念編輯區，中間區域為實例編輯區，右邊的區域為屬性編輯區，Protégé 是一介面化的軟體，因此不用直接撰寫 OWL 的語言，只需建立概念、屬性及實例便會產生出 OWL 檔。

規則推論：

規則一：透過"決策者(?y)"擁有其" has_關注項目(?y, ?z) "找到" has_部門(?z, ?a)"，對於其"所造成的傷害(?a, ?x)"將可以瞭解所出現的電腦災害為”(?y, ?x)”，藉 此可以運用 SWRL 語意規與 JESS 推論器將，SWRL 規則的設定如下：

決策者(?y) ∧ has_關注項目(?y, ?z) ∧ has_部門(?z, ?a) ∧ 所造成的傷害(?a, ?x) → 所出現的電腦災害(?y, ?x)

規則二：每一個被關注項目(?x)均擁有其 has_部門(?x, ?y)，針對這些項目整個組織對不同的部門會有不同的 has_嚴重程度(?y, ?a)，以及部門對這些項目也有屬於各部門自己認為的 has_嚴重程度(?X, ?b)，透過 SWRLB 將雙方認知的權重進行加權產生對組織的威脅程度，SWRL 規則的設定如下：

關注項目 (?x) ∧ has_部門(?x, ?y) ∧ has_嚴重程度(?y, ?a) ∧ has_嚴重程度(?X, ?b) ∧ 權重值(?a, ?z) ∧ 權重值(?b, ?c) ∧ swrlb:add(?n, ?z, ?c) → 威脅程度(?x, ?n)

4.3 結論與討論

對於不同的部門其所擁有的關注項目不同之下，對於電腦病毒所造成的電腦災害按照不同的部門於當下的情境中，所要考量的項目不同，按照其嚴重程度即可瞭解對於其部門對於此災害所採行的應變方法，給予組織的最終決策者來斷定其應變方法的適用性。

5. 結論

本研究藉由知識本體及語意規則並行的方式，以電腦災害復原計畫為應用領域仿效人類決策者對於採取方法的判斷準則建置成為知識庫，藉以推論經驗法則的判定。實作過程中解決本研究所提之問題，最後，餵證實知識本體及語意規則的公用，本研究以組織部門根據電腦災害的發生對於其部門的關注項目下有著不同的權重值來判定所採取的應變方法作為其決策支援的目的並達到知識共享的效果。

參考文獻

[1]戴鈺唐，最佳化字串比對演算法設計針對記憶體架構病毒偵測系統，國立清華大學資訊工程學系，2007。

[2]戚玉樑，以本體技術為基礎的知識庫建置程序及其應用，資訊科技與社會，2005。

[3]蕭崑賢，基於靜態分析與資料探勘技術之惡意程式偵測系統，國立台灣科技大學資訊工程研究所碩士論文，2006。

[4]鄭美華，危機管理機制建立之研究，通識研究集刊， 2003。

[5]陳英裕，一個針對電腦蠕蟲防治的混合偵測演算法，國立交通大學，2009。

[6]王仁宏，災害復原規劃之知識表達及推理法則研究，國立中央大學資訊管理研究所碩士論文，2003。

[7]Christodorescu, M., & Jha, S,. Static analysis of executables to detect malicious patterns. In Proceedings of the 12th conference on USENIX Security Symposium -. Washington, DC: USENIX Association, 2003, Vol.12 , pp. 12-12.

[8]Chi, Y.-L. "Elicitation synergy of extracting conceptual tags and hierarchies in textual document," Expert Systems with Applications, 32(2), 2007, pp.

349-357

[9]Chi, Y.-L. and Lee, H.-M. "A Formal Modeling Platform for Composing Web Services," Expert Systems with Applications, 34(2), 2008. pp.1500-1507

[10] Cohen, F., 1987. "Computer Viruses Theory and Experiments," Computers and Security, 1987, vol. 6, pp. 22-35.

[11] Fallara, P,. Disaster recovery planning. Potentials, IEEE, 2004,vol. 5, no 225,pp. 42-44,

[12] Gruber T.R, “Translation approach to portable ontology specification,” Knowledge Acquisition, 1993, vol. 5, no. 2, pp. 199-220.

[13] Guarino N., “Understanding, building and using ontologies: a commentary to using explicit ontologies in KBS development,” International Journal of Human and Computer Studies, 1997 vol. 46, pp. 293-310,.

[14] Howard, L., Time is of the essence', disaster pro says. National Underwriter , 1997,pp. 13–14.

[15] Noy N.F. and McGuinness. D.L., “Ontology development 101: a guide to creating yourfirst ontology,” Stanford KS Lab, California, Tech Rep. KSL-01-05,2001.

[16] Peter, W.,”Network Disaster Contingency Planning,”Computers & Security, 15(5), 1996 , pp. 411.

[17] Wold, G. H,. Disaster recovery planning process, 2002.