

行政院國家科學委員會專題研究計畫 成果報告

以本體論為基之支援虛擬企業知識分享的存取控制技術發展(II)

研究成果報告(精簡版)

計畫類別：個別型
計畫編號：NSC 96-2221-E-343-002-
執行期間：96年08月01日至97年07月31日
執行單位：南華大學電子商務管理學系

計畫主持人：陳宗義
共同主持人：陳裕民
計畫參與人員：碩士班研究生-兼任助理人員：陳品元
大專生-兼任助理人員：張詩捷
博士班研究生-兼任助理人員：林家柔

報告附件：出席國際會議研究心得報告及發表論文

處理方式：本計畫涉及專利或其他智慧財產權，2年後可公開查詢

中華民國 97 年 08 月 07 日

行政院國家科學委員會補助專題研究計畫 成果報告
 期中進度報告

以本體論為基之支援虛擬企業知識分享的存取控制技術發展(II)

計畫類別： 個別型計畫 整合型計畫

計畫編號：NSC 96-2221-E-343-002-

執行期間：2007年08月01日至2008年07月31日

計畫主持人：陳宗義 南華大學電子商務管理系

共同主持人：王昌斌 南華大學電子商務管理系

陳裕民 國立成功大學製造工程研究所

聶澎齡 南台科技大學應用英文系

計畫參與人員：楊惠媚 大同技術學院

林家柔 國立成功大學製造工程研究所

陳品元 國立成功大學製造工程研究所

張詩捷 南華大學電子商務管理系

成果報告類型(依經費核定清單規定繳交)： 精簡報告 完整報告

本成果報告包括以下應繳交之附件：

赴國外出差或研習心得報告一份

赴大陸地區出差或研習心得報告一份

出席國際學術會議心得報告及發表之論文各一份

國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、
列管計畫及下列情形者外，得立即公開查詢

涉及專利或其他智慧財產權， 一年 二年後可公開查詢

執行單位：南華大學電子商務管理系

中華民國九十七年八月六日

一、摘要

中文摘要

虛擬企業(Virtual Enterprise)是全球化商業競爭的趨勢，為有效提昇企業競爭力的方法之一，其工作者以協同合作的工作模式貢獻自己的核心能力，分享彼此的資源及知識，以完成產品的設計、生產、組裝、行銷及提供服務。善用知識資產並創造新的知識，是企業成功的關鍵。而虛擬企業的成功主要仰賴成員間安全及適度的知識分享與任務協同。本研究針對虛擬企業於分散與跨企業的知識分享及存取控制(Access Control)上的需求，改善角色為基之存取控制(Role-based Access Control, RBAC)模型，發展以本體論(Ontology)為基的虛擬企業知識存取控制模型(Model)、方法(Approaches)、策略規範(Policy Specification)、演算法(Algorithms)、信任評估(Trust Evaluation)模式、方法論(Methodology)及系統，本研究所提出之技術能根據工作者在虛擬企業中的所扮演的角色及執行的任務，以及企業知識管理及分享的策略，來決定知識存取的權限(Authorization)。本研究提出一個三維的本體論包含組織本體論(Organizational Ontology)、工作流程本體論(Process Ontology)及產品本體論(Product Ontology)，以不同的觀點來描述實體知識，考慮知識的相關性來分享知識，以決定工作者知識存取權限的擴散(Propagation)。透過存取控制策略(Policy)的制定，可即時的調整虛擬企業知識分享的規則，以配合商業環境的需求，達到安全的跨企業的知識分享。本研究之主要研究項目有：(1)虛擬企業知識存取控制模型與系統之需求分析；(2)虛擬企業知識存取控制模型及系統發展；(3)工作者間信任評估模式開發；以及(4)虛擬企業案例的導入與方法論的發展。

關鍵詞：虛擬企業、知識表達、知識分享、角色為基的存取控制、本體論。

Abstract

Virtual enterprise (VE), an effective means of creating competitive advantage, is a global business trend under knowledge-based competition. In a VE, workers work as a team, contributing their core competences to design, produce, assemble and market a product and providing services. Using existing knowledge to create new knowledge is a key to enterprise success; above all, VE success depends mainly on securely appropriate knowledge sharing and collaboration among members. Focusing on a distributed dynamic VE environment, this study investigates the requirements for access control and knowledge sharing across enterprises. In considering these requirements, and a using role-based access control (RBAC) model, this study develops an ontology-based VE access control model, and approaches, policy specifications, algorithms, trust evaluation method, and methodology and system, which determines worker authorization for accessing knowledge based on their roles in, and responsibilities assigned by, the VE. This study proposes a three-dimension ontology comprised organizational ontology, process ontology and product ontology, which characterize knowledge using various perspectives and consider the interrelations among various conceptual-level knowledge to determine whether user authorization can be propagated. The principal tasks in this study are as follows: (1) analyzing requirements for knowledge access control model and system in a VE ; (2) developing a knowledge access control model and system for VEs; (3) designing a co-worker trust evaluation method for secure knowledge sharing; and, (4) developing a methodology for implementing the proposed model and system in a practical case.

Keywords: Virtual Enterprise, Knowledge Representation, Knowledge Sharing, RBAC, Ontology.

二、報告內容

2.1 前言

現今市場競爭日益激烈、生產製程技術不斷地革新，縮短了產品的生命週期，因此如何有效地降低生產成本、提高產品及服務品質、縮短產品上市時間及快速反應客戶需求，已成為企業當前最迫切的目標。又網路與資訊技術迅速的發展及新知識經濟時代的來臨，加速了市場與競爭的全球化，企業競爭的優勢決定於能否以迅速地創新的技術與觀點來為顧客創造更高的價值。為因應如此巨變的環境，企業不斷的追求新的管理方法與技術，變更生產製程及服務流程，為求降低生產成本、提高產品及服務品質、縮短產品上市時間及快速反應客戶個人化的需求，以期提升企業競爭力。虛擬企業(Virtual Enterprise, VE)為結合各企業的核心能力，透過企業的策略聯盟，整合價值活動、資訊、資源、核心技術與知識，以協同合作的方式完成一項產品或服務。由於虛擬企業任務導向的特性，可隨時組合及解散，已成為未來企業追求的目標；其成敗繫於虛擬企業各階段活動的資訊與知識能否有效被相關人員適時適地的根據職掌而獲取、整合、管理與分享(Xiaochuan *et al.*, 2003; Frenkel *et al.*, 2000; Zhu *et al.*, 2003)。

近年來，許多研究聚焦於探討策略聯盟組織間的知識分享與競爭優勢的關係(Rodriguez & Wilson, 2002; Skinner *et al.*, 1992; Mudambi & Helper, 1998)。然而，策略聯盟組織間的知識分享，卻存在既合作且競爭的矛盾現象，企業若能與其他組織建立良好的信任合作關係，積極從事知識分享活動，將有助於發展持續性的競爭優勢。因此當虛擬企業的成員以協同合作的方式進行產品開發時，知識必須能夠有效的即時的在所有企業成員間流通及分享。

知識的分享，信任(Trust)及安全(Security)為最重要的元素，特別是由不同的企業所組成的分散式虛擬企業環境，必須透過網路進行跨企業的資訊及知識的交換(Furst *et al.*, 2002)。綜觀目前知識管理研究領域，大多以企業內部知識之獲取、管理與分享為企業知識管理的主要研究項目，目前知識存取控制之研究明顯不足，又知識為企業最重要的資產，所以建立完善之控管機制，以保護知識資產，已是知識管理研究領域最重要的議題之一(Rao & Upadhyaya, 2006; Bertino *et al.*, 2006; Singh & Salam, 2006)。

因此，實現虛擬企業知識的分享必須提供一個安全的知識分享的環境，才能藉由企業知識的分享創造新的知識，進而提昇企業競爭力。在虛擬企業知識管理及分享的環境之下，知識可能以不同的形式，分散的儲存在不同的企業成員的知識儲存庫中，因此虛擬企業知識的管理及分享不同於以往的存取控制機制，需要一個完善的存取控制模型或方法，才能適應知識複雜的儲存模式及支援虛擬企業的分散性及暫時性，以保護虛擬企業知識資產，使虛擬企業的知識能根據合法的使用權限，即時的支援所有的虛擬企業工作者工作的進行。因此本研究之主要動機有：(1)現有之存取控制模式無一針對知識於企業分享之存取控制需求所設計；(2)現有之存取控制模式無法滿足虛擬企業之暫時性分散式組織的需求；(3)傳統存取控制模式並未考慮跨組織的協同作業知識存取權限的管理及知識實體間具有的關聯性；(4)知識以各種不同的儲存模式及媒介存在企業的角落中，知識的權限及存取控制無法以現有之存取控制模型或策略來有效管理；和(5)信任是虛擬企業知識分享的要素，目前尚無針對此問題之解決方案。

為能支援虛擬企業工作者於執行任務時知識使用權限的管理，虛擬企業知識存取控制模型必須具備下列能力：彈性、跨組織及安全的服務、集中式管理的能力及考慮知識具有流動的特質。

2.2 研究目的

在虛擬企業的環境下，企業不斷的加入或退出，根據對象的不同，合作方式亦隨之改變。知識管理的策略又必須能與企業的經營策略相配合，才能發揮知識管理系統應有的優勢，如何透過知識管理系統的支援落實企業知識管理的策略，並能隨經營策略的變動，立即反應在所有工作人員的知識存取的權限上，使企業知識能在協同的策略聯盟中適度的被

分享與使用。知識分享是知識管理的核心，尤其是隱性的知識往往是企業知識中最有價值的部份，也是知識分享最難實現的部份。知識分享有許多的方法及技術，例如面對面的溝通、知識網路(Knowledge Network)及組織學習(Organizational Learning)等。創造一個有利於知識分享的環境，才是讓知識發揮最大價值的關鍵。因此本研究將著重在跨企業的知識分享及權限的管理，主要的研究任務為發展一套能適應動態虛擬企業環境的知識管理之知識存取控制系統，使在協同運作階段的虛擬企業能形成一個知識社群，促進知識分享與取得，滿足虛擬企業的工作者能根據工作中對知識的需求及知識存取的權限，使用分散在所有企業成員中的知識，以促使知識能夠快速及安全的被分享至正確的人、時間及位置上，以提昇虛擬企業整體競爭力。

本研究的進行，除了考慮虛擬企業能以中央控制的策略來促進跨企業的知識分享，亦考慮企業能以分權自治的策略來保護企業內被分享的知識。進而從 Who、What、When 及 Where 四個維度來管理及分享知識，提出一符合虛擬企業協同工作模式的「本體論為基之知識存取控制方法」。希望藉由本研究能使(1)知識分享在安全的設計考量下，能有明確的進步；(2)企業可以根據公司的組織型態及人事策略，配置及分享知識；(3)虛擬企業可以進行跨企業的知識分享，達到知識的協同，並即時的在員工間移轉及傳達；(4)利用一統合企業內知識之本體論，提供知識庫分類與相關性地圖，使工作者可以取得適當的實體知識，並獲知知識的相關性及解決知識不易被描述的問題。

本研究共分三年進行，在本計畫第一年，本研究主要利用本體論具概念描述及概念與概念間關係表達的能力，來描述虛擬企業的概念層的知識內容，進而從(1)Who：使用者(user)的身分及角色，(2)What：user 正執行的任務，(3)When：虛擬企業所處的階段及時間點，及(4)Where：使用者所處的企業在虛擬企業中的角色。從四個不同的維度來決定使用者知識的使用權限，提出企業內知識分享模式與方法，及虛擬企業知識表達及儲存模式。第二年的研究，以第一年的成果為基，主要研究工作有：(1)虛擬企業知識分享之存取控制技術的發展，其中包含虛擬企業存取控制模型、方法、演算法、策略規範及信任評估的方法、(2)企業內知識管理及分享的促動因素分析與流程設計、(3)虛擬企業跨企業的知識管理及分享的流程設計、(4)企業知識存取控制系統的架構設計、(5)虛擬企業知識存取控制系統的架構設計、及(6)企業與虛擬企業存取控制系統整合機制的設計。

2.3 文獻探討與特性分析

為了使本研究所提出的方法能符合虛擬企業知識存取控制的需求，這一節探討虛擬企業之特性、生命週期及知識的類型。接著針對角色為基之存取控制(Role-based Access Control, RBAC)模型及一般知識表達法進行探討。

2.3.1 虛擬企業知識特性分析

虛擬企業利用企業間資源的整合為方法，以協同發展客戶所需的產品為目的。虛擬企業具有以下特性：顧客導向、動態結合、專業分工、分散合作及溝通、資訊分享與全球資源整合。虛擬企業的生命週期經常被分成四個階段：機會確認階段、形成階段、運作階段及解散階段(Strader et al., 1998)。在機會確認階段，虛擬企業的主導者藉由機會的搜尋及市場的評估，確定欲發展的產品或服務；在形成階段，進行合作夥伴的選擇，制定工作計畫並進行分工，同時進行工作者資源使用權限的設定；在運作階段，根據前面的規劃，所有的工作者執行被分派的任務，根據權限的設定，存取資源；最後進入解散階段，必須修改使用者對資源的存取權限及策略，部分的資源依然可以在新的分享策略下被使用。透過虛擬企業生命週期活動的分析，可以知道工作者於各階段所進行的虛擬企業活動及所需的知識型態。例如在運作階段，所需的是專門技術及經驗，這些儲存在員工心智或隱含在組織流程中；又如製造流程相關知識為產品製造一系列的知識，包含：(1)製程中所需要的原料及相關工具的知識，(2)產品組裝的知識，(3)生產設備使用及維護的知識。除了上述流程知識外，還包含產品相關知識：產品的生命週期中從產品的研發到使用後的回收，這些產品

相關的活動必須有特定知識的支援才能完成，例如產品的資源回收必須有資源回收的知識來支援。因此可將產品知識歸納為四大項：(1)產品的概括描述與特性描述，(2)產品開發與實現的知識，(3)產品使用的知識，(4)產品維護的知識(Uschold & Gruninger, 1996)。

知識是結構化的經驗、價值、以及經過文字化的資訊，也包含專家獨特的見解(Davenport & Prusak, 1998)。Nonaka & Takeuchi (1995)將企業內的知識分類為：(1)外顯知識與內隱知識；(2)個人知識與組織知識；(3)描述性的(Declarative)、程序性的(Procedural)及因果性的(Causal)知識。其中描述性的知識是指「know-what」的知識，即瞭解事件的概念、組成與結構的知識；程序性的知識是指「know-how」的知識，即瞭解事件的執行程序、步驟、方法的知識；因果性的知識是指「know-why」的知識，即瞭解事件發生之原因(Quinn et al., 1996)。本研究將採這三種類型的知識分類，來進行知識存取控制的發展。

2.3.2 角色為基的存取控制模型(Role-Based Access Control, RBAC)

RBAC 模型(Sandhu & Munawar, 1998; Ferraiolo et al., 2001; Bacon et al., 2002)，是以角色(Role)來當作授權的中介對象，使用者可以執行不同的角色，以控制其物件的存取權限。由於角色代表著企業一些職務的集合，本身變動的機會不大，透過如此「使用者-角色-物件」三層式架構，異動頻繁的使用者，例如離職、職務變動及職務代理等狀況，只需要更改使用者與角色的對映關係，可以簡化使用者授權的管理程序。

由於 RBAC 具備下列特性，因此企業普遍使用 RBAC 執行組織的授權管制：

- (1) **角色與使用者間的指派(User-Role Assignment, UA)**：使用者透過分派取得角色，而且不只擁有一個角色；而同一個角色可分配給許多使用者。當使用者執行特定角色時，藉由 sessions 來進行，session 為一存取控制活動的單位，在一個 session 中，使用者只能扮演一個角色。
- (2) **角色與權限之間分派 (Role-Permission Assignment, PA)**：是將職務的權限授予角色，在特定的角色中，為了能讓任務順利進行，相關單位會授予角色擁有許多責任與資格，在訂定的範圍內來運用相關的權限。而權責則可依角色的需求，被分派到不同的角色。如此，在維護使用者與角色、角色與權責之間的關係時，使用者可以輕易移轉、新增或刪除角色，而權責亦可在角色間易於移轉、新增或刪除，如此可以簡化管理的複雜度及降低管理成本。
- (3) **最低基本權限(Least Privilege)**：一個角色擁有許多不同的權限，一個使用者也可能具備多重角色，只有特定職務需要時，特定角色的權限才會授予給該職務，以避免權限遭到濫用。
- (4) **角色職務的階層與繼承(Role Hierarchy)**：角色之間的階層關係，可以有權限繼承的關係，如此可以簡化授權管理。
- (5) **角色職務的分工(Separation of Duty)**：職務分工是對多人控制安全政策，其主要目的是互斥的工作，由不同人來執行，以防止舞弊情況發生，如此才能符合企業資源管理的原則。

2.4 研究方法

為達本計畫之目標，本計畫所採之研究方法為：

- (1) **研究與實務並重之研發**：除了注重有學術價值之創新性研究，如存取控制模型及方法的建立及知識分享安全性的改善等，並期能與企業合作，實際參予企業知識管理系統的建置與上線之工作，確實了解企業對知識管理與分享實務上之需求，協助企業導入協同分工的虛擬企業概念，針對企業及虛擬企業之協同工作者對知識分享及權限管理欠缺之處，分析工作者對知識存取之需求，設計一個能符合業界實務需求，並能適時提供工作者適當知識之存取控制環境，藉以提升企業效益及解決現有企業與虛擬企業知識分享及權限管理的障礙。
- (2) **分散式虛擬團隊之同步式研發**：運用同步工程(Concurrent Engineering)及虛擬團隊(Virtual Team)之協同與整合並進的方法與技術，並輔以專案管理，實施本計畫之規劃、分工、進行、整合及研究成果的管理，使能發揮多功能團隊效率並達預期研究的效果

與目標。

- (3) **以知識管理技術進行本計畫之執行**：本計畫進行期間必須以知識管理之原則、方法與技術，進行本計畫之相關知識的獲取、整合、儲存、管理、分享與運用，以加速本計畫各階段各項任務的執行速度。
- (4) **技術引進與研發並重**：本計畫在應用技術方面將選擇適當之現有工具及技術進行應用性的整合研發，例如在存取控制模型的部份可以考慮改善現有以廣泛被使用於資料庫管理系統之 RBAC 模型，使之符合虛擬企業知識分享之需求。就存取控制策略語言的部份，可以考慮以現有之具國際安全組織認定之 XACML 標準化存取控制語言為基礎進行開發。系統建構方面亦將運用物件導向之開發工具及系統，以提高研究效率與研究成果之可用性、移轉性與擴充性。

2.5 結果與討論

本計畫第一年主要的研究工作，最初進行相關領域的研究工作、虛擬企業知識的界定及知識存取控制的需求分析，針對虛擬企業分散及協同運作的特性，考慮所有來自不同企業的工作者對知識使用權限的管理及分享的需求，及本體論對知識的表達及整合的能力，提出一個本體論為基的知識分享模型，進一步設計一個多層式的本體論為基的知識表達架構模型。在本計畫第一年所提出的知識架構模型之下，第二年的主要產出項目包含(1)一個本體論為基的存取控制模型、(2)為知識分享而設計的知識授權擴展模式、及(3)知識存取控制策略的架構及(4)知識存取策略語言模型。

在本計畫第二年的執行過程中，本研究團隊並進一步發現虛擬企業知識分享決策輔助機制在虛擬企業知識分享的重要性，對於本計畫有其影響成功之決定性關鍵。因此，已將此機制增列為未來第三年的研究主要工作之一，主要研究工作有：

- (1) **影響知識分享決策之因素探討**：組織的文化、制度與知識管理的流程會影響到員工知識分享的行為。因此本階段首先分析「組織文化與制度面」對知識分享意願的影響，幫助我們建立一個適合知識分享的知識管理的流程，以規範與提升員工知識分享的意願。接著探討「組織文化」與「知識分享」的關係，界定及分析「虛擬企業內的知識與知識分享的關係」，進一步分析「影響虛擬企業內協同工作者知識分享行為之因素」，提出「知識分享決策之模式」。許多主客觀因素，例如組織、人際互動及知識本身的特性等，皆可能影響知識分享決策的評估。將來，在本階段的研究中，可能面臨評估因素不易量化的問題。
- (2) **模糊理論為基之知識分享決策模型設計**：知識分享行為常是一個主觀判斷所產生的模糊性問題，因此需要一個適當的方法來處理人類主觀價值判斷的模糊性問題，表達不易量化或主觀的評估值。本階段將進行「信任度的評估研究」、「分享意願的評估研究」及「相關決策方法的研究」（例如，模糊理論、灰色理論及層級分析法）。本研究預期模糊理論將可應用於解決此類問題，本步驟最後提出一個「模糊理論為基之知識分享決策模型」。
- (3) **模糊理論為基之知識分享決策模型測試與評估**：建構「模糊規則庫」，並進行上一步驟提出之模糊理論為基之知識分享決策模型的測試與評估的工作。
- (4) **知識分享決策機制實作**：根據第二年所提出之「虛擬企業環境知識分享之存取控制系統的主架構」，設計「知識分享決策輔助機制的架構」，並進行此機制的實際開發。當本機制建構完成，每一位虛擬企業工作者能夠建構自己的模糊規則庫，本機制能夠根據工作者的模糊規則庫的規則來進行知識分享的決策。

三、參考文獻

1. Bacon, J., Moody, K., and Yao, W. "A Model of OASIS Role-based Access Control and Its Support for Active Security," *ACM Transactions on Information and System Security* (5:4) 2002, pp: 492-540.
2. Bertino, E., Khan, L.R., Sandhu, R., and Thuraisingham, B. "Secure Knowledge Management: Confidentiality, Trust, and Privacy," *IEEE Transactions on Systems, Man, and*

Cybernetics—Part A: Systems and Humans (36:3) 2006, pp: 429-438.

3. Chen, T.-Y., Chen, Y.-M., Wang C.-B., and Chu, H.-C. (2006) “Development of an Access Control Model, System Architecture and Approaches for Information Sharing in Virtual Enterprise,” *Computers in Industry* (58: 1) 2007, pp: 57-73.
4. Davenport, T. H. and Prusak, L. *Working Knowledge: How Organization Manage What They Know*, Harvard Business School, 1998.
5. Ferraiolo, D.F., Sandhu R., Gavrila, S., Kuhn, D.R., and Chandramouli R. “Proposed NIST Standard for Role-based Access Control,” *ACM Transactions on Information and System Security* (5:3) 2001, pp: 224-274.
6. Furst, K., Schmidt, T., and Wippel, G., “Managing Access in Extended Enterprise Networks,” *IEEE Internet Computing* (1:6) 2002, pp: 67-74.
7. Nonaka, I. and Takeuchi, H., *The Knowledge Creating Company: How Japanese Companies Create the Dynamic of Innovation*, New York: Oxford University, 1995.
8. Quinn, J.B., Anderson, P., and Finkelstein, S. “Managing Professional Intellect: Making the Most of the Best,” *Harvard Business Review*, March-April, 1996, pp: 71-80.
9. Rao, H. R., and Upadhyaya S. J. “Special Issue on Secure Knowledge Management,” *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans* (36:3) 2006, pp: 418-420.
10. Sandhu, R., and Munawer, Q. “The RRA97 Model for Role-based Administration of Role Hierarchies,” *Proceedings of the 14th Annual Conference on Computer Security Applications* 1998, pp: 39-49.
11. Singh, R., and Salam, A. F. “Semantic Information Assurance for Secure Distributed Knowledge Management: a Business Process Perspective,” *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans* (36:3) 2006, pp: 472-486.
12. Staab, S. “Knowledge Representation with Ontologies: The Present and Future,” *IEEE Computer Society* 2004, pp: 72-81.
13. Strader, T. J., Lin, F.R. and Shaw, M. J. “Information Infrastructure for Electronic Virtual Organization Management,” *Decision Support Systems* (23:1) 1998, pp: 75-94.
14. Uschold, M. and Gruninger, M. “Ontologies: Principles, Methods and Applications,” *The Knowledge Engineering Review* (11:2) 1996, pp: 93-136.
15. Wiig, K.M., *Knowledge Management Foundations: Thinking about Thinking—How People and Organizations Create, Represent, and Use Knowledge*, Arlington, TX: Schema Press, 1993.
16. Zhu, H.H., Chen, D.F. and Zhang, X.C. “Research of Knowledge Chain in Intelligent Control,” *Robotics, Intelligent Systems and Signal Processing*, 2003.

四、計畫成果自評

本計畫為一個虛擬企業知識權限管理與分享完整的解決方案的研究，第二年度之進度主要包括三個階段：

- (1) 虛擬企業知識分享之存取控制技術發展：為本階段最重要的工作，主要的工作有：「存取控制模型發展」、「存取控制方法設計」、「存取控制演算法設計」、「存取控制策略規範設計」與「協同工作者信任評估方法開發」。
- (2) 主要的工作有：「設計知識管理及分享的流程」及「設計虛擬企業知識管理與分享的流程」。
- (3) 設計虛擬企業環境知識分享之存取控制系統的主架構：本階段首先探討「代理人的相關

技術」，進一步設計「虛擬企業環境知識分享之存取控制系統架構」，主要產出有「企業知識存取控制系統架構」及「虛擬企業知識存取控制系統架構」，接著進行主架構中各主要模組的細部設計的工作，本階段的產出將作為本計劃第三年「虛擬企業環境知識分享之存取控制發展」的基礎。

第二年的研究工作，大致依據上述之計畫進度依序完成之，唯階段一中的「存取控制演算法設計」在計畫執行中發現，較適於系統開發階段進行，因此待進行知識實體層設計或實際之知識管理系統建置時，進行細部系統分析與設計時再一併進行。第二年中最主要之產出截至目前為止，已獲下列具體成果，並摘要簡介如下附件所示。

第二年之部分研究成果被摘列於本成果報告的下面附件中，本計畫累計第一及二年的主要之研究成果並已發表至相關研究刊物，截至目前為止，與執行本計畫之相關著作已投稿國外 SCI 期刊並已獲接受 2 篇、國內 TSSCI 期刊已獲接受 1 篇、準備中有 1 篇、國內外研討會有 7 篇，如下所列。

(1) 國外 SCI 期刊：

Tsung-Yi Chen, Knowledge Sharing in Virtual Enterprises via an Ontology-based Access Control Approach, Computers in Industry, Vol. 59, Issue 5, pp. 502-519, 2008. (SCI/EI)

Tsung-Yi Chen, A Multiple-layer Knowledge Management System Framework Considering User Knowledge Access Privileges, International Journal of Software Engineering and Knowledge Engineering (IJSEKE). (SCI) (In press)

(2) 國內 TSSCI 期刊：

陳宗義、陳裕民、蘇彩好，設計一個多層式本體論為基之虛擬企業知識表達模型，資訊管理學報，第 15 卷，第 1 期，2008。(TSSCI)

林家柔，陳宗義，陳品元，陳裕民，以本體論為基之虛擬企業知識分享機制研發，管理與系統期刊。(TSSCI)(準備中)

(3) 國內外研討會：

Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang, Hui-Chuan Chu, Designing a Trust Evaluation Method for Resource Sharing among Enterprises, The 7th International Symposium on Knowledge and Systems Science, Beijing, China, 2006.

Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang and Hui-Chuan Chu, Resource Sharing to Support Cross-organizational Collaborative Activities in Virtual Enterprise Using a Novel Trust Method, The 7th Asian Pacific Industrial Engineering and Management Systems Conference (APIEMS 2006), Bangkok, Thailand, 2006.

Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang, Hui-Chuan Chu, Access Management in Multi-layer Knowledge Management Systems, e-Manufacturing & DFM Symposium 2007, Taipei, Taiwan, 2007.

Tsung-Yi Chen, Yuh-Min Chen, Chin-Bin Wang and Hui-Chuan Chu, On an Ontology-based Access Control Approach for Knowledge Sharing in Virtual Enterprises, The 11th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2007, Orlando, Florida, USA, July 8-11, 2007.

Tsung-Yi Chen, Yuh-Min Chen, Hui-Chuan Chu, Chui-Cheng Chen, Knowledge Access Control Policy Language Model for Resource Management in Virtual Enterprises, IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 2007. (EI)

林家柔，陳宗義，陳品元，陳裕民，以本體論為基之虛擬企業知識分享機制研發，第九屆電子化企業經營管理理論暨實務研討會，大葉大學。

Tsung-Yi Chen, Yuh-Min Chen, Hui-Chuan Chu, On a Multi-phase Trust Model of Supporting Decision-making for Resource Sharing in Virtual Teams, The 9th Asia Pacific Industrial

附件：計畫第二年之部分研究成果

1. Ontology-based knowledge access control model for VEs

In this subsection, based on characteristics of VEs, specific requirements of knowledge sharing for VE workers and the multiple-layer knowledge representation framework, a knowledge access control model for VEs is proposed and represented in a Class model of UML.

Figure 1 illustrates this model. This model is capable of accommodating requirements for knowledge security in a distributed VE environment and offers a flexible mechanism for security managers to determine who can access what knowledge, when and how the use of knowledge is to be constrained and breadth and depth of knowledge sharing. The following subsections separately define all elements and relationships in this model.

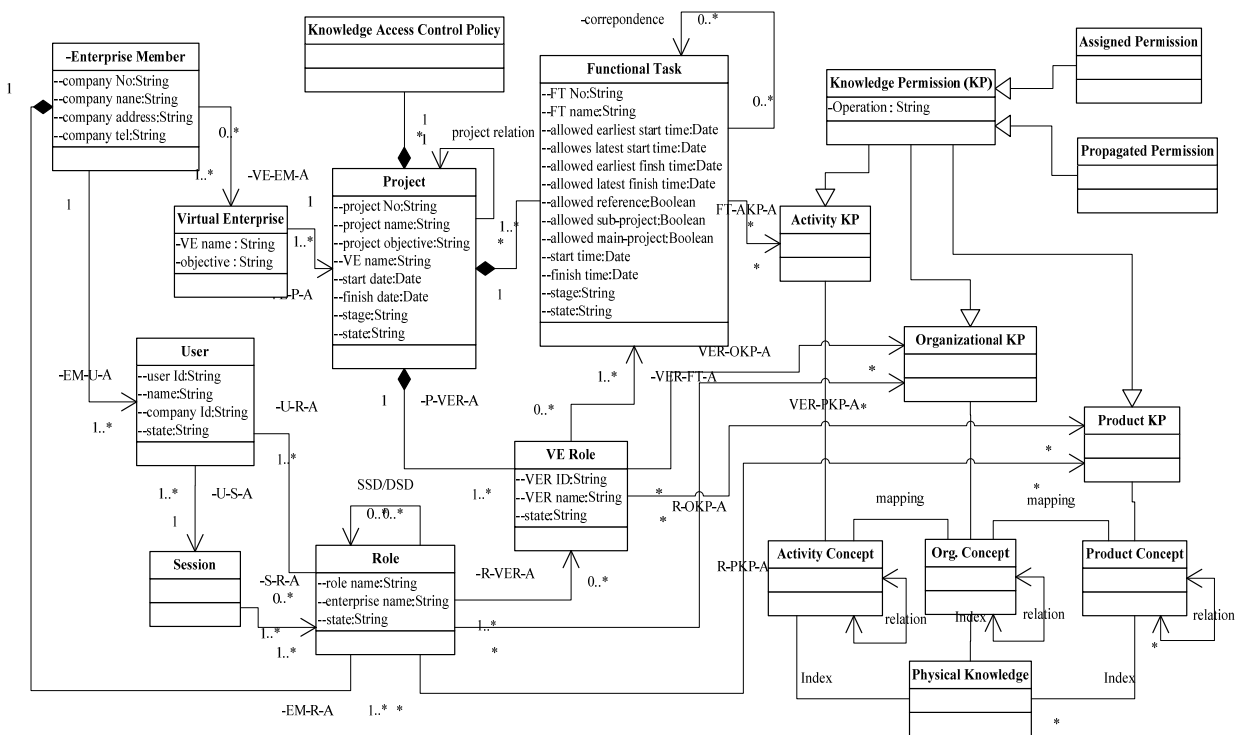


圖 1：虛擬企業知識存取控制模型

Based on the concepts of RBAC model and developed with reference to the Virtual Enterprise Access Control (VEAC) model, the knowledge access control model for VEs proposed in this study has main elements such as User, Session and Role in the RBAC model. Other main elements are defined as follows:

- **Virtual Enterprise (VE):** VE refers to a group of enterprises with different specialties and core competences that have formed a temporary strategic alliance whose operations are performed through separation of duty and collaboration.
- **Project (P):** Project refers to the basic unit of VE activities and can be further decomposed into several sub-projects based on VE task requirements.
- **Enterprise Member (EM):** Organizations directly participate in a VE. In a VE environment, enterprises may simultaneously participate in more than one VE; thus, coexisting competitive and cooperative relationships between enterprise members are possible.
- **Virtual Enterprise Role (VER):** Created to perform VE functions and tasks, each VER may

be performed by internal roles of different EMs. Upon formation of a VE, VERs are created; they disappear when the VE ceases to exist.

- **Functional Task (FT):** A functional task is the basic unit of a VE task, while the main activities of a project can be decomposed into multiple FTs in a sequential order and then assigned to different VERs for execution. Knowledge is assigned by VE at a conceptual layer to FTs according to knowledge required. Therefore, through conceptual knowledge, physical knowledge of VE and its EMs can be assigned to FTs, thus enabling workers responsible for performing those tasks to use such knowledge according to their access permission.
- **Conceptual Knowledge Ontology:** Three ontological types presented in knowledge conceptual layer are organizational ontology, activity ontology and product ontology. Conceptual knowledge ontology describes special concepts, similar to key words required for querying knowledge documents, which are related to all semantic contents of physical knowledge. Therefore, when users request access to a special concept, their access permission must be confirmed against that concept along with other related concepts to determine if specific restrictions, like those concerning “read” or “write,” should be imposed.
- **Knowledge Permission (KP):** Knowledge permission refers to knowledge and a set of its executable operations such as “read” and “write”. Knowledge permission includes: (1) *assigned permission* assigned through relationships between elements, and (2) *propagated permission* assigned through propagation and extension of conceptual knowledge in the knowledge conceptual layer. Knowledge permission can be granted through various dimensions of the three ontological types and is further divided into three types: Activity KP, Organizational KP and Product KP, each corresponding to a different body of conceptual knowledge.
- **Physical Knowledge (Physical K):** Referring to data in various formats whether it be data physically stored in a repository or the knowledge stored in someone’s brain, physical knowledge may belong to a VE or an EM, and objects of physical knowledge can correspond to multiple items of conceptual knowledge in organizational ontology, activity ontology or product ontology. Therefore, the specific conceptual knowledge and the knowledge permission concerning a physical knowledge object must be identified.
- **Knowledge Access Control Policy (KACP):** KACP identifies which knowledge is protected and shared according to the relations among projects and the shared rules, and which activities are forbidden in the VE scope. Each project involves a KACP, which can be performed automatically by the knowledge access control system in VE. The KACP can be dynamically created, enforced and modified by administrators when the VE environment changes. The main rules described in KACP have: (1) rules of knowledge sharing among projects, describing the knowledge sharing strategy and relations among projects; (2) rules of knowledge usage in a project, including constraints on VERs, FTs, knowledge permissions and assignments between elements; (3) rules of knowledge sharing of various cooperation modes, identifying the level of knowledge sharing according to the cooperation mode between VERs, and (4) rules of exception handling, which can be classified into rules of permitted exception handling and rules of forbidden exception handling. A KACP language model used to construct the KACP is proposed in detail in the following Section 2.

2. Knowledge access control policy language model

An authorization policy has temporal properties. Consequently, an access control policy for the management of knowledge and user authorization in VEs must easily be updated to capture the changing requirements of applications and users. The Knowledge Access Control Policy (KACP) language model for VEs designed in this study, as Fig. 2 illustrates, is represented in UML's class model and mainly targets contents of knowledge text. This model features an Object-Subject-Action-Condition access control policy consisting of multiple sets of authorization rules that jointly determine user's knowledge access permissions. Therefore, regarding specific conceptual or physical knowledge (object), authorization (action) to execute certain knowledge is granted to certain users (subject) under certain restrictions (conditions). The KACP language model for VEs has been proposed to (1) provide a method that effectively describes knowledge access control policy for VEs, (2) reduce costs and complexity in knowledge access control, (3) improve flexibility in managing knowledge access permission, (4) enhance security of VE knowledge sharing, and (5) make the management of knowledge access permission adaptive to changing needs in a business environment in a timely manner.

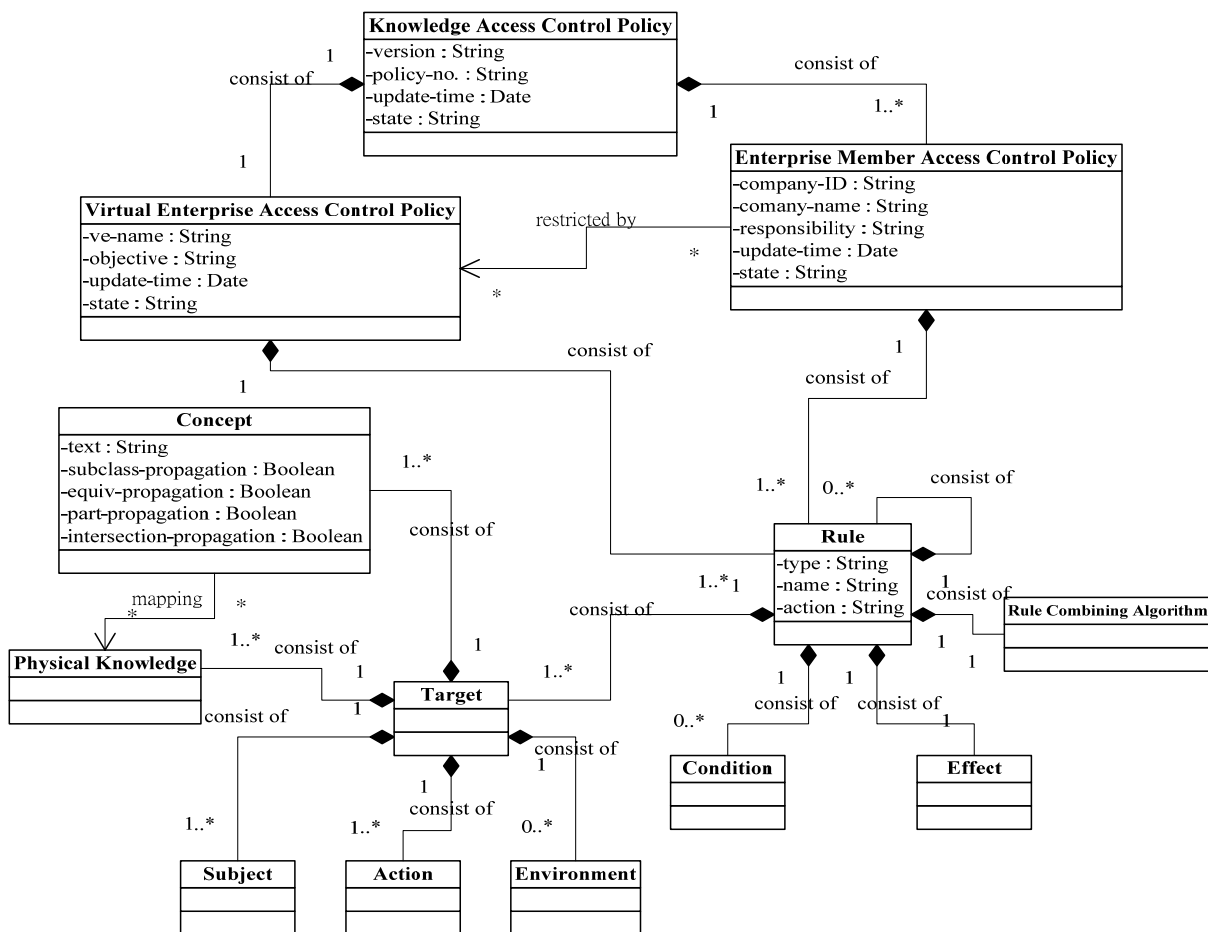


圖 2：知識存取策略語言模型

The KACP language model has the following main components.

- *Knowledge Access Control Policy (KACP)*. A KACP consists of one Virtual Enterprise Access Control Policy (VEACP) and many Enterprise Member Access Control Policies (EMACPs), which are sets of rules.
- VEACP, a set of rules, describes the regulation and constraint on knowledge access control and sharing in a VE to manage the VE's knowledge.
- EMACP, Consisting of a series of rules, EMACP describes rules and conditions for enterprise knowledge access control for each EM. Its rules shall not be in conflict with the VEACP, it

belongs to and must comply with sharing rules agreed upon by VE so to make available knowledge in need of sharing.

- *Rule* element is the most basic unit of VEACP and EMACP and corresponds to the conventional concept of authorization. The principal components of rule have a target, effect, condition, and rule combining algorithm. Each rule permits or denies one or more subjects to performing actions on one or more concepts or physical knowledge under some conditions.
- *Target* element involved in a rule defines the set of objects, subjects, environment and actions to which the rule or policy applies. The set of objects involves two different levels of knowledge: concept and physical knowledge.
- *Concept* element is the basic unit of three ontologies in knowledge conceptual layer. Five attributes are involved in the element. The text attribute describes the content of the concept for explaining the meaning of the concept. Other four attributes, namely subclass-propagation, equiv-propagation, part-of-propagation and intersection-propagation attributes, are Boolean data type for determining whether knowledge access authorization can be propagated from the concept to other concepts that are associated with it by relations.
- *Physical Knowledge* element may be data, information and any format knowledge owned by the VE or one of its enterprise members.
- *Subject* element is an actor whose attributes can be referenced by a predicate. Actor may be user, enterprise role, enterprise member, VE role or VE.
- *Action* element is an operation on conceptual or physical knowledge.
- *Environment* element provides a set of attributes that are relevant to an authorization decision and are independent of a certain subject, knowledge and action.
- *Rule Combining Algorithm* compresses the output from the embraced rules. The KACP language model has four rule combining algorithms: deny overrides, permit overrides, first applicable, and only-one-applicable. Based on the selected combining algorithm, an authorization decision can be permit, deny, not applicable or indeterminate.
- *Condition* element represents additional constraints that further refine rule applicability.
- *Effect* is the intended consequence of a satisfied rule—either “Permit” or “Deny.”

出席國際學術會議心得報告

計畫編號	NSC 96-2221-E-343-002-
計畫名稱	以本體論為基之支援虛擬企業知識分享的存取控制技術發展(II)
出國人員姓名 服務機關及職稱	陳宗義助理教授 南華大學電子商務管理系
會議時間地點	新加坡
會議名稱	IEEE 國際工業工程與管理研討會
發表論文題目	虛擬企業知識存取控制語言模型

一、參加會議經過

我於台北時間 1 December, 2007 即會議開始前一天，一大早即從台南出發至高雄小港國際機場，搭乘中華航空高雄至新加坡的直飛班機，當日中午抵達新加坡樟宜機場，立即搭乘公車前往預訂的飯店，在簡單的午餐之後，我立即步行前往此次研討會的飯店，了解位置及交通所需時間，之後隨即展開這一次令人難忘的行程。藉由這次參加研討會的機會，我另外規劃參訪新加坡魚尾獅公園及克拉克碼頭等著名景點，之後於研討會結束後直奔樟宜國際機場搭乘返台班機於晚上回到台南。

在本次研討會的四天的議程中，早上時段大會主要安排工業工程與產業管理相關領域的學者進行一個場次的專題演講，早上十一點以後才安排分成六到十個 Section 不等的進行論文的報告，議程其所涵蓋的議題如下：

- Decision Analysis and Methods (DA)
- E-Business and E-Commerce (EB)
- Engineering Economy and Cost Analysis (EC)
- Ethics, Education and Training (EET)
- Facilities Planning and Management (FPM)
- Global Manufacturing and Management (GM)
- Human Factors (HF)
- Information Engineering (InfoE)
- Intelligent Manufacturing (IntM)
- Maintenance Modeling and Engineering (MME)
- Manufacturing Systems (MS)
- Operations Research and Application (OR)
- Project Management (PM)
- Production Planning and Control (PPC)
- Quality and Reliability Engineering (QRE)
- The CATER System for Vehicle Mass Customization (S1)
- Design Chain Management (S2)

- Advanced Planning and SCM in Process Industry (S3)
- Advanced Statistical Process Control (S4)
- The Science in Service Development (S5)
- Supply Chain Management (SCM)
- Service Innovation and Management (SIM)
- Systems Modeling and Simulation (SMS)
- Safety and Security (SS)
- Technology and Knowledge Management (TM)

二、與會心得

The IEEE International Conference on Industrial Engineering and Engineering Management，每年由不同的國家分別爭取主辦權，今年是由新加坡大學主辦。本研討會的主要目的為提供全世界主要以亞洲國家為主，在工業工程及工程管理的專家學者一個溝通互動的平台，讓專家學者面對面的討論在產業工程中最新的創新、理論及實務的經驗。此次會議中，與會學者與專家主要來自亞洲的東南亞地區，其中有許多來自於產業界且具有豐富實務經驗的專家，但參與人員仍然以學術界的學者為主。所發表之數百篇論文中其議題與內容極具實用性與開創性，並在學術上有極高之價值。

The IEEE International Conference on Industrial Engineering and Engineering Management 每年在新加坡舉辦，今年獲接受發表文章約有 5、6 百篇之多，齊聚來自全球二、三十個國家的專家學者參加，有幸能與這些學者專家一同討論、聆聽及宣讀研究心得。此次大會並邀請了剛當選香港城市大學校長的 Professor Way Kuo(院士)為與會者進行 keynote presentation。本人所提之論文「虛擬企業知識存取控制語言模型」經大會審核，獲准展示於與會學者，進行面對面互動。有三位學者提出他們的疑問與看法，經我進一步的解釋與其他學者參與討論之後，讓我獲益良多。藉由參加本次的會議報告與討論的過程，不只達到學術交流的目的，更能夠見識到許多國際知名學者的氣度涵養令人印象深刻，參加本次會議不僅開拓研究的視野亦可提升個人的修養與內涵。要成為一位優秀的國際性學者，除了不斷地充實自己各方面的能力避免閉門造車之外，更需不斷地吸取國際舞台的經驗，甚至參加國際性的研究計畫，因此參加國際性研討確實有其必要性。