行政院國家科學委員會專題研究計畫　成果報告

工作流程觀之授權管理之研究

計畫類別：個別型計畫
計畫編號：NSC94-2416-H-216-004-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：中華大學資訊管理學系

計畫主持人：吳美玉

計畫參與人員：簡其弘、李宗澤

報告類型：精簡報告
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：本計畫可公開查詢

中　華　民　國 95 年 10 月 13 日

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　　工作流程觀之授權管理之研究　　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　　□整合型計畫
計畫編號：**NSC 94-2416-H-216-004**
執行期間：94 年 8 月 1 日至 95 年 7 月 31 日

計畫主持人：吳美玉
共同主持人：無
計畫參與人員：簡其弘、李宗澤

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

執行單位：中華大學資訊管理學系

中　華　民　國　95　年　10　月

行政院國家科學委員會專題研究計畫成果報告

工作流程觀之授權管理之研究

Research on Authorization Management for Workflow View

計劃編號：NSC 94-2416-H-216-004
執行期間：94 年 8 月 1 日至 95 年 7 月 31 日
主 持 人：吳美玉　中華大學資訊管理學系
計劃參與人員：簡其弘、李宗澤

摘要

工作流程管理系統已經被廣泛地應用在企業中，各種工作流程相關的資訊充斥於企業之中，對於企業而言，電腦所儲存的資料是企業內部最重要的資產，相關的資源是有必要去進行安全性的控管。然而，如何以流程導向的知識觀點，使工作流程中的各個參與者，可以依據不同的需求與授權層級，來獲得企業流程中不同的資訊，將所能操作的使用者予以適當的授權管理，以確保企業資源的存取控制能達到安全及有效的管理，是一個很重要的議題。

本研究主要是探討工作流程觀之授權管理，其內容包含如下：(1) 探討組織中眾多工作流程之特性，分析工作流程中之工作與工作間之特性，發掘工作衝突關係，以進行權責區分準則之建立；(2) 分析各種工作流程觀之產生方式，探討各種虛擬工作建立之方式；(3) 依據工作與工作間是否有權責衝突關係，重新規劃工作流程觀中之各個虛擬工作之權限；(4) 探討如何將各個虛擬工作原先之實體工作之角色授權分配，重新發掘符合工作流程觀之角色指派。整體而言，本研究主要是基於以工作與角色為基礎的工作流程授權管理，分析工作流程觀中之各個虛擬工作形成之方式，與重新規劃各個角色對於各個虛擬工作之權限，建立適合於工作流程觀之授權管理，以達到提升整體企業的安全存取控制與管理。

關鍵詞：工作流程觀；授權管理；以角色為基礎的存取控制；權責區分

Abstract

Workflow management system is adopted in enterprise comprehensively. There are several information system relevant workflows in organization. The data stored in computer is the most important assets for enterprise. The resource should be under access control securely. However, how to make that workflow participants possess different needs and levels of authority when obtaining information on business process based on process-oriented knowledge and appropriate authorization management for users is an issue worth studying.

This research mainly investigates the issue concern with the authorization management for workflow view. The research aspects include the following. (1) Investigating the characteristics of workflow in organization, and further analyzing the characteristics between tasks in the workflow and discovering the duty-conflict relationship for authorization rules in order to construct the separation of duty; (2) Analyzing the generation of workflow view, and investigating the conducting methods of each virtual task; (3) Redesigning the permissions of each virtual task in the workflow view based on whether there are duty-conflict relationships between tasks; (4) Investigating how to reassign the roles to virtual tasks in the workflow view based on the original role assignment to physical activity. Overall, this research is to analyze the conducting methods of each virtual task and reassign the roles to virtual tasks in workflow view. Propose the authorization management for workflow view to improve the access control and authorization management for enterprise.

Keywords：Workflow View, Authorization Management, Role-based Access Control, Separation of Duty

一、背景與研究目的

由於企業內部電腦化的普及，各種工作流程相關的資訊充斥於企業之中，對於企業而言，電腦所儲存的資料是企業內部最重要的資產，相關的資源是有必要去進行安全性的控管。而工作流程管理系統（WfMS）已經被廣泛地應用在企業中，工作流程管理系統被認為最能改善企業程序，它是一個有效的流程管理工具，可以幫企業分析、模擬、設計、執行，與控管他們所有的企業流程[6][8]，有了工作流程管理系統的支援，不同的參與者可以有效地協同合作來管理工作流程所控制的企業程序。然而，如何以流程導向的知識觀點，使工作流程中的各個參與者，可以依據不同的需求與授權層級，來獲得企業流程中不同的資訊，亦即在各個工作流程系統中，所能操作的使用者應予以適當的授權管理，以確保企業資源的存取控制能達到安全及有效的管理，使工作流程管理系統能更臻完善，是一個很重要的議題。

因此，本研究目的主要是探討企業工作流程中之工作的特性，以工作權責衝突關係為基礎，當依據不同的角色權限所建構出之工作流程觀，提供適於工作流程觀之授權管理，以期所能操作的使用者，皆有一適當的授權管理。

二、文獻探討

針對企業資訊資源的存取控制，有相當多的文獻探討，其中「以角色為基礎的存取控制」（Role-Based Access Control, RBAC）[1][3][4][5][7][12]方法中，使用者皆被分配到適當的角色，而資源的存取權限則是經由所屬的角色來決定。在決定每個角色所能執行的權限及所能授予的使用者，需滿足相關的權責區分政策。但是隨著產業型態的改變，可能會增加新的工作項目，或是工作需要被重新安排，而在以角色為基礎的存取控制中，權限或是操作並無法完全表示企業內部「工作」的觀念。工作是一個較高層次的表達方式，工作亦可包含子工作，而工作流程更是一個高層次的工作規劃。

因此，不同於以角色為基礎的存取控制，有少許文獻提出了以工作為基礎的存取控制與授權管制[2][13][16]，其中，Sandhu等人所提出的以工作為基礎的授權控制（Task-based Authorization Controls, TBAC）[16]，主要是針對工作執行時期的工作狀態管制，包括閒置、請求、執行、暫停、結束等五個狀態，提供工作執行授權機制，但僅是工作執行狀態的安全管制，並未進一步討論整個工作流程中，工作、角色與使用者間的授權指派與權責區分；而Bertino等人則是探討工作流程環境下，工作與角色的授權管制機制[2]，主要是提出邏輯程式的授權語言來描述授權條件，並提出依據邏輯授權條

件，進行工作流程中工作、角色及使用者授權指派管制的方法。論文中雖然依其授權語言舉例說明靜態與動態的權責區分，但並未著重在權責區分準則之建立說明，且未依據工作之間的關係特性來探討權責區分，致使無法以更簡明的方式來表達授權準則。Schier所提出之以角色與工作為基礎的安全模式[13]，雖已提出由工作衝突來探討相關權責區分準則，但僅僅是原來以角色為基礎的存取控制之延伸，亦即由原本以角色為基礎的存取控制中定義互斥的角色，延伸定義互斥的工作，而未從工作的觀點，進一步分析討論不同的工作權責衝突。

根據工作的權責關係而建立的授權準則之研究，目前主要是以工作流程為觀點，探討以工作權責衝突關係為基礎，提出符合權責區分準則之工作流程授權管理機制，以確保工作流程之執行與存取，有一適當的安全控管與授權管理[10]。對於工作流程觀之相關研究[9][11][14][15]，其主要之貢獻在於提出流程觀（或稱之為虛擬流程）模式，並產生流程觀模式之演算法[9]，或是以工作流程代數（workflow algebra）方法，以達到更嚴謹的工作流程觀之一般化定義[11]，並未進一步探討根據不同的工作流程參與者，所建構出之工作流程觀之安全控管與授權管理。

三、研究方法

我們分析企業環境內之工作流程，依據工作流程中之各個工作與工作間之特性，發掘工作衝突關係，以進行權責區分準則之建立，相關之工作衝突關係包括工作權責衝突關係、工作制衡關係、工作督導關係等。

一個工作流程可依據不同需求而產生出多個工作流程觀，工作流程觀中的一個虛擬工作可能是由多個實際工作所組成，亦或是資料的聚集。所謂的資料聚集方式包括有加總、取平均、最大值及最小值等。組成虛擬工作的實體工作間，是否存在工作權責衝突關係，亦會影響到工作流程觀中之各個虛擬工作之權限。

本研究依據工作與角色為基礎的存取控制，並考量由工作流程形成多個工作流程觀時，參照各個工作流程觀中之各個虛擬工作原先之實體工作之角色授權分配，重新設定符合工作流程觀之角色指派，以達到滿足權責區分目標之授權管理。

本計畫更進一步利用實際應用環境中之工作流程觀個案—訂單處理流程，依據所設計出之工作流程觀之授權管理，發掘出符合相關權責區分準則規範之使用者、角色、虛擬工作，與權限等授權與指派。

四、結果與討論

本計畫完成之工作流程觀之授權管理之研究，將有助於確保在各個工作流程中，所能操作的使用者，依據不同的角色、需求、權限所形成之工作流程觀，予以適當的授權管理，以確保企業資源的存取控制能達到安全及有效的管理，使工作流程管理系統能更臻完善。

于本計畫中，我們完成的研究結果有：

(1) 工作流程中工作與工作間之特性之研究探討

我們分析企業環境內之工作流程，依據工作流程中之各個工作與工作間之特性，發掘工作衝突關係，以進行權責區分準則之建立，有關的工作衝突關係包括工作權責衝突關係、工作制衡關係、工作督導關係等。

(2) 工作流程觀之產生方式之研究探討

工作流程觀或稱子工作流程，又或流程觀，依據不同的角色、需求、權限，將形成不同的工作流程觀。

(3) 工作流程觀之各個虛擬工作之權限設計

依據虛擬工作的組成方式，並考量各個工作是否具有工作衝突關係，設計規劃每個角色對於虛擬工作之合理的權限。

(4) 工作流程觀之各個虛擬工作之角色授權分配之分析與設計

將工作流程觀中之各個虛擬工作原先之實體工作之角色授權分配，重新設計符合工作流程觀之角色指派。

(5) 實際工作流程觀案例應用分析

以訂單處理流程為例，產品經理與業務經理會有不同的工作流程觀，亦會產生不同的虛擬工作與權限，該案例有助於應用分析。

五、計畫成果自評

我們已經完成了計畫書中 90%的工作項目，所提出的工作流程觀之授權管理模型，符合預期的目標。我們的研究—工作流程觀之授權管理，可視為一個非常重要的研究議題，並可作為如何改善整體企業的安全存取控制與授權管理的基礎。總而言之，本研究所提出之工作流程觀之授權管理模型，將有助於確保企業內部的資源，達到一個更安全及有效的管理。

有關核定之經費運用狀況，因為個人懷孕待產之緣故，不便搭機出國，故所核撥之出席國際會議之經費伍萬元，因未動支，已將款項全數繳回。本人感到非常遺憾，未能與同領域之國外著名學者進行學術研討與交流，並辜負了國科會促進學術國際化發展的美意，未來仍期望貴會可以再提供機會參加國際型會議。

參考文獻

1. John Barkley, "Implementing Role Based Access Control Using Object Technology", *First ACM Workshop on Role Based Access Control*, November 1995.
2. Elisa Bertino, Elena Ferrari, Vijayalakshmi Atluri, "A Flexible Model Supporting the Specification and Enforcement of Role-based Authorizations in Workflow Management Systems", *RBAC 97 Workshop*, 1997.
3. David Ferraiolo, Richard Kuhn, "Role-Based Access Control", *In Proceedings of 15th NIST-NCSC National Computer Security Conference*, pages 554-563, October 1992.
4. David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn, "Role-Based Access Control (RBAC): Features and Motivations", *Proceedings of 11th Annual Computer Security Application Conference*, IEEE Computer Society Press, pages 241-248, December 1995.
5. Luigi Giuri, Pietro lglio, "A Role-Based Secure Database Design Tool", *Proceedings 12th Annual Computer Security Applications Conference*, Dec 1996.
6. R. J. van Glabbeek, W. P. Weijland, "Branching Time and Abstraction in Bisimulation Semantics", *Journal of the ACM*, 43(3), pp. 555-600, 1996.
7. Mats Gustafsson, Benoit Deligny, Nahid Shahmehri, "Using NFS to Implement Role-Based Access Control", *Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, June 1997.
8. N. Krishnakumar, A. Sheth, "Managing Heterogeneous Multi-System Tasks to Support Enterprise-Wide Operations", *Distributed and Parallel Databases*, 3(2), pp. 155-186, 1995.
9. Duen-Ren Liu, Minxin Shen, "Workflow Modeling for Virtual Processes: an Order-Preserving Process-View Approach", *Information Systems*, 28(6), pp. 505-532, 2003.
10. Duen-Ren Liu, Mei-Yu Wu, Shu-Teng Lee, "Role-based authorizations for workflow systems in support of task-based separation of duty", *Journal of Systems and Software*, Volume: 73, Issue: 3, pp. 375-387, November – December, 2004.
11. Victor Pankratius, Wolffried Stucky, "A Formal Foundation for Workflow Composition, Workflow View Definition, and Workflow Normalization based on Petri Nets", *the Second Asia-Pacific Conference on Conceptual Modelling* (*APCCM2005*), 2005.
12. Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, "Role-Based Access Control Models", *IEEE Computer*, 29(2), pp.38-47, February 1996.
13. Kathrin Schier, "Multifunctional Smartcards for Electronic Commerce-Application of the Role and Task Based Security Model", *14th Annual Computer Security Applications Conference*, December 1998.

14. Karsten A. Schulz, Maria E. Orlowska, “Facilitating cross-organisational workflows with a workflow view approach”, *Data & Knowledge Engineering*, 51, pp.109-147, 2004.
15. M. Shen, D.R. Liu, “Discovering role-relevant process-views for disseminating process knowledge”, *Expert Systems with Applications*, 26, p301–310, 2004.
16. R. K. Thomas, R. S. Sandhu, “Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management”, *Proceedings of the IFIP WG11.3 Workshop on Database Security*, August 11-13, 1997.