行政院國家科學委員會專題研究計畫 成果報告

具情境認知之以角色為基礎的存取控制模型之研究與實作
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 95-2416-H-216-006-
執 行 期 間 ：95 年 08 月 01 日至 96 年 08 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：碩士班研究生-兼任助理：詹智翔、曾文鈴、馮堯保

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 96 年 11 月 30 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

具情境認知之以角色為基礎的存取控制模型之研究與實作

計畫類別：☑ 個別型計畫　　□ 整合型計畫
計畫編號：NSC 95-2416-H-216-006
執行期間： 95 年 08 月 01 日至 96 年 08 月 31 日

計畫主持人：吳美玉
共同主持人：無
計畫參與人員：詹智翔、曾文鈴、馮堯保

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：中華大學資訊管理學系

中　華　民　國　96 年　11　月　30　日

行政院國家科學委員會專題研究計畫成果報告

具情境認知之以角色為基礎的存取控制模型之研究與實作

The Research and Implementation on Context-Aware Role-Based Access Control Model

計劃編號：NSC 95-2416-H-216-006
執行期間：95 年 8 月 1 日至 96 年 8 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：詹智翔、曾文鈴、馮堯保

摘要

隨著資訊科技快速的進步，企業中的使用者可以不受時空限制地存取企業內部資訊，造成企業資訊資源安全控管的嚴重問題。然而，傳統以角色為基礎的存取控制之授權管理機制對於日趨複雜的企業工作流程環境，已經無法滿足安全性考量之需求。因此，企業資訊資源的存取控制機制要能依據相關情境資訊，更有彈性地授予與控管使用者權限，讓企業資訊資源可以獲得一個更完善、更安全的存取控制與授權管理環境。

本計畫主要為研發與實作具情境認知之以角色為基礎的存取控制模型，整合權責區分與情境認知機制，協助在企業工作流程中，以期對於資訊資源提供適當的授權管理。研究內容主要包括：(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) 分析各種具影響性之存取控制與授權管理情境資訊，例如：工作流程環境、使用者身分識別、時間、位置、設備狀態等相關資訊；(3) 依據不同角色與工作之間是否有權責衝突關係，及依據相關情境資訊，重新規劃各個使用者、角色對於工作之權限；(4) 發展與實作具情境認知之以角色為基礎的存取控制模型雛形系統於智慧型空間，用以驗證結合情境資訊之以角色為基礎的存取控制模型，能使企業的存取控制與授權管理更具彈性及有效性。

關鍵詞：以角色為基礎之存取控制、情境認知、權責區分、工作流程、授權管理

Abstract

The evolution of Information Technology (IT) makes user easier to access enterprise information resource without time and space constraints. However, conventional authorization management of role-based access control can not satisfy the safety consideration for more and more complex enterprise workflow. Therefore, the access control of enterprise information resource has to refer the context information in order to authorize and control the user permissions. It will make enterprise information resource with more perfect and safe access control and authorization management.

This project mainly investigates the issue concern with the context-aware role-based access control for workflow. The research aspects include the following. (1) Investigating the characteristics of workflows 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 context information affects the access control and authorization management, for example, workflow environment, user identification, time, location, and status of facilities etc.; (3) Redesigning the permissions of each user on whether there are duty-conflict relationships between tasks and related context information; (4) Developing and implementing the prototype system of context-aware role-based access control model for smart space to validate the proposed model effectively for enterprise.

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

一、背景與研究目的

企業在運作過程中所涉及與涵蓋的資訊，如同其他重要的企業資產，對組織具有一定的價值與產生影響，有必要針對企業資訊資源進行適當的考量與保護。針對企業資訊資源的存取控制，已經有相當多的研究探討，但是，隨著資訊科技快速的進步，企業中的使用者可以不受時間與空間的限制，透過像個人數位助理（PDA）、行動電話等個人資訊設備，經由適當的管道（如網際網路）接收或傳送企業內部的資訊，造成企業內部資訊資源安全控管的嚴重問題。因此，企業資訊資源的存取控制機制必須要能夠更有包容、靈活、彈性地進行對使用者權限之授予與控管，資訊系統必須要有能力判斷並確認安全地情境（Context）條件，進一步依據使用者被授權角色以及相關情境資訊，即時、動態地的檢驗、調整以給予使用者適當之權限，讓企業資訊資源可以獲得一個更完善、安全的存取控制與授權管理環境。

因此，本研究的目的主要在於以工作與角色為基礎的工作流程授權管理，結合情境資訊作為安全的限制條件，分析相關情境資訊，彈性地重新規劃各個使用者、角色對於各項工作、資源之權限，建立結合情境認知之以角色為基礎的授權管理，以求提升整體企業的安全存取控制與授權管理。

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][5][6][8][9][11]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。

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][12][13]，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）[13]，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。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]。

有別於傳統以角色為基礎的存取控制之研究，僅有少許相關文獻提出運用情境資訊結合既有存取控制機制之研究 [3][4][7]。其中，Georgiadis 等人所提出的結合情境資訊與以團隊為基礎的存取控制 [7]，主要是將一群特殊使用者集合成一團隊（team），屬於團隊的使用者有權限使用該團隊的資源，並依據時間及所在地點即時進行權限之指派，但並未進一步以個別的角色為指派基礎，無法達到角色繼承之概念，進而減少權限指派之次數；對於網路服務（Web Services）之情境認知（Context-Aware）存取控制之研究[3][4]，Bhatti 等人主要是提出以 XML 為基礎的以角色為基礎的存取控制（X-RBAC）[3]，結合情境認知存取控制，建構網路服務環境所需的設置與建構，而 Feng 等人則提出一個加入情境認知和服務導向的以角色為基礎的存取控制模型（CSRBAC）[4]，以提升對於網路服務管理的靈活性與安全性。但是，對於情境認知存取控制之研究，僅單純考量結合簡單的時間、地點等情境資訊作為進一步的限制條件，無法應付目前知識密集的企業運作環境。

三、研究方法

首先我們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，發掘可能之工作衝突關係，以進行初步權責區分準則之建立，緊接著分析各種具影響性之存取控制與授權管理之情境資訊，根據分析結果，可能影響存取控管的情境資訊如下所示：

1. 計算情境：如網路服務品質、通訊頻寬、通訊花費，以及鄰近資源，如：印表機、顯示器、工作站…等。
2. 使用者情境：使用者的喜好設定、位置、鄰近的使用者等，甚至可以包括使用者當前的社交狀態。
3. 時間情境：每日、每週、每月的某一個時刻，或是一年的某一個季節等情境因素。
4. 實體情境：像是亮度、噪音程度、溫度等。

探討可能影響存取控管的情境資訊後，依據初步之權責區分準則與相關情境資訊，重新規劃工作權限，藉由設計具情境認知之以角色為基礎的存取控制方針，以確保企業內部的重要的資訊資源有適當的存取控管與授權管理。

此外，發展與實作具情境認知之以角色為基礎的存取控制模型雛形系統於智慧型空間，因智慧型空間即是具有計算、通訊與感知的環境，以便驗證本研究所提出之具情境認知之以角色為基礎的存取控制模型之可行性。

四、結果與討論

本計畫完成之具情境認知之以角色為基礎的存取控制模型之研究與實作，將有助於提升企業內部相關資源與工作流程之存取控制與授權管理，使企業資訊資源的存取控制機制能依據相關情境資訊，更有彈性地授予與控管使用者權限，讓企業資訊資源可以獲得一個更完善、更安全且具彈性的存取控制與授權管理。

于本計畫中，我們完成的研究結果有：

(1) 工作流程特性分析，建立權責區分之準則

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，依據使用者不同的角色、需求、權限，以進行權責區分準則之建立。

(2) 各種具影響性之存取控制與授權管理情境資訊之分析

任何可以描述一個個體狀況的資訊，皆可形成影響存取控管與授權管理的情境資訊，本研究分析所得具影響性的情境資訊包括：計算情境、使用者情境、時間情境與實體情境等四大類。

(3) 依據權責關係與相關情境資訊，重新情境認知地規劃工作權限之方針設計

由使用者的情境資訊，與欲擔任角色的情境需求比對，確保授權管理；再經由角色的情境資訊，與欲執行工作與操作權限的情境需求比對，確保存取控管；此外亦建立情境衝突解決方針，以確保使用者、角色、工作及相關權限的動態存取控管與授權管理。

(4) 具情境認知之以角色為基礎的存取控制模型雛形系統實作

以智慧型實驗室為雛形系統實作環境為例，經由無線網路與感測器，接收環境與使用者的相關情境資訊，再依據具情境認知之以角色為基礎的存取控制模型中之方針，開發更具彈性且兼具安全性之存取控管之雛形系統。

五、計畫成果自評

我們已經完成了計畫書中 90%的工作項目，所提出的具情境認知之以角色為基礎的存取控制模型，符合預期的目標。我們的研究—具情境認知之以角色為基礎的存取控制模型，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，且經由實作之雛形系統，可驗證所提出之存取控制模型可行。總而言之，本研究所提出之具情境認知之以角色為基礎的存取控制模型，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。

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. Rafae Bhatti, Elisa Bertino, Arif Ghafoor, “A Trust-based Context-Aware Access Control Model for Web-Services”, *Proceedings of the IEEE International Conference on Web Services* (*ICWS’04*), 2004.
4. Xu Feng, Xie Jun, Huang Hao, and Xie Li, “Context-Aware Role-Based Access Control Model for Web Services”, *GCC 2004 Workshops*, LNCS 3252, pp. 430–436, 2004.
5. David Ferraiolo, Richard Kuhn, “Role-Based Access Control”, *In Proceedings of 15th NIST-NCSC National Computer Security Conference*, pages 554-563, October 1992.
6. 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.
7. Christos K. Georgiadis, Ioannis Mavridis, George Pangalos, Roshan K. Thomas, “Flexible Team-Based Access Control Using Contexts”, *Proceeding of Sixth ACM Symposium on Access Control Models and Technologies* (*SACMAT 2001*), pp.21-27, 2001.
8. Luigi Giuri, Pietro lglio, “A Role-Based Secure Database Design Tool”, *Proceedings 12th Annual Computer Security Applications Conference*, Dec 1996.
9. 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.
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. 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.
12. Kathrin Schier, “Multifunctional Smartcards for Electronic Commerce-Application of the Role and Task Based Security Model”, *14th Annual Computer Security Applications Conference*, December 1998.
13. 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.

出席國際學術會議心得報告

計畫編號	NSC 95-2416-H-216-006
計畫名稱	具情境認知之以角色為基礎的存取控制模型之研究與實作
出國人員姓名 服務機關及職稱	吳美玉 中華大學資訊管理學系助理教授
會議時間地點	96/07/28-96/07/31 西班牙巴塞隆納
會議名稱	International Conference on Security and Cryptography, 2007
發表論文題目	Role and Task Based Authorization Management for Process-View

一、參加會議經過

ICETE 之全名為 International Conference on E-business and Telecommunication，ICETE 為一個聯合研討會（Joint conference），包含有 ICE-B, WINSYS, SECRYPT 與 SIGMAP，ICETE 2007 共收到來至六十多個不同國家的論文，論文接受率為 41%，且由 IEEE、WfMC、ACM 及 UPC 等單位贊助與合作，茲可證明 ICETE 為一個成功、且具貢獻的國際研討會。

本人此次參與及被接受的論文為 ICETE 其中之 SECRYPT 此研討會，SECRYPT 之全名為 International Conference on Security and Cryptography。SECRYPT 2007 所接受的論文包括以下五個資訊安全與密碼學重要的領域：存取控制與入侵偵測、網路安全與協定、密碼學技術與金鑰管理、資訊保證，及資訊系統安全等。本人所被接受的論文屬於存取控制與入侵偵測領域。

此次 ICETE 2007 共安排了六場專題演講，其中有一位義大利的學者談及「衛星網路中跨層級的資源配置」，是一個本人非常感興趣的議題，在無線網路的環境中，如何對稀有資源進行有效的配置，是一個值得研究的領域，而要跨越不同的層級，如實體層、資料連結層、網路層，及傳輸層等，使得在衛星網路中，有較佳的動態頻寬配置，有較好的資源管理等，更是重要的研究議題，經由該專題演講，瞭解該學者所提出之嶄新的技術，收穫良多。

而本人所實際參與報告之場次九，包括本人共有五位學者發表相關研究，其他四位學者分別來自義大利、瑞士、塞爾維亞，及西班牙等不同國家，從各學者的報告，與主席、報告者、聽眾的互動過程中，學習到國外學者對於一個研究主題相關的研究方法、步驟、成果，及報告技巧等。此外，報告最後與國際學者的問答互動過程中，更增加自己對自我研究主題的自信心，國外學者不同的見解，也讓本人拓展視野，此次參與之會議，實感收穫良多。

二、與會心得

由於此次所參與之研討會延後公布論文接受清單，且舉辦時間在暑假旺季，故在得知本人之研究被該會所接受後，後續花了許多時間在預定機票與飯店，甚至預訂不到在研討會開會前的班機，最後訂到研討會第一天一早出發，而當天到達的班機，此外亦預訂不到從研討會地點巴塞隆納回程的班機，因此多花費了從巴塞隆納搭乘火車到馬德里的費用，再從馬德里搭機返回台灣，故經過此次經驗，學習到往後若欲在旅遊旺季出國參加研討會，必須要有事先詳盡的規劃與準備。

在從台北前往研討會地點—西班牙巴塞隆納的班機，途中經由倫敦轉機，於機場巧遇本人博士學位的口試委員，國立交通大學資訊科學與工程研究所所長 曾文貴教授，曾教授在資訊安全、密碼學、網路安全等領域有卓越的成果，經與其交談後，得知曾教授亦是欲前往巴塞隆納參加 SECRYPT 2007 會議，並於會議中擔任主持人，讓本人更加確信此 SECRYPT 2007 國際研討會之重要性。

本人非常感謝國家科學委員會的經費補助，使得本人有機會參與 SECRYPT 2007 這樣高水準的國際研討會，並能與國外學者面對面交流意見，學習到相關的研究方法、成果，及報告技巧等。此外，亦聆聽到同領域的研究，例如有位學者發表—「針對不同環境中的 XML 文件之存取控管模型」，深信自己之研究領域乃屬蓬勃發展之研究領域，藉此提升自我信心。另外亦有一位加拿大的教授，以授課方式來講述艱深難懂的定理與數學式，學習到如何將研究中難以讓他人瞭解的學理與公式，以風趣幽默之授課方式表達，值得學習。

三、考察參觀活動(無是項活動者省略)

此次 ICETE 2007 國際研討會安排了一場西班牙當地的文化藝術參觀活動—佛朗明歌舞，由於所安排的時間在晚上，素聞西班牙的治安不佳，且本人在抵達西班牙巴塞隆納的第一天晚上即遭遇心懷不軌之強盜集團，幸於出發前，詳細瞭解自保措施，故未造成損失，因此基於安全考量，本人未參加該會所規劃之參觀活動。

四、建議

經過此次參與之會議，瞭解到最新的研究議題，學習到國外學者的研究方法與報告技巧等，實感收穫良多，故在此再次感謝國家科學委員會的經費補助，使得本人有機會參與這樣高水準的國際研討會，增廣見聞，建議貴會應繼續補助國內學者參加這樣的國際盛事，以促進國內研究學者的研究能量。

五、攜回資料名稱及內容

此次參加 ICETE 2007 所攜回之資料名稱如下：

1. ICETE2007 研討會最終版議程與摘要集
2. ICETE2007 論文集光碟
3. 出席 ICETE2007 研討會並報告論文之證書