行政院國家科學委員會專題研究計畫 成果報告

應用具情境認知之以角色為基礎的存取控制模型於RFID安全性管理

研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 96-2416-H-216-004-
執 行 期 間 ：96年08月01日至97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-兼任助理人員：林彥廷
碩士班研究生-兼任助理人員：呂鍾鑫
碩士班研究生-兼任助理人員：陳逸瑋

報 告 附 件 ：出席國際會議研究心得報告及發表論文

公 開 資 訊 ：本計畫可公開查詢

中 華 民 國 97年11月29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

應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理

計畫類別：☑ 個別型計畫　□ 整合型計畫
計畫編號：NSC 96-2416-H-216-004
執行期間： 96 年 08 月 01 日至 97 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：林彥廷、呂鍾鑫、陳逸瑋

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　97 年　11　月　28　日

行政院國家科學委員會專題研究計畫成果報告

應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理

Applying the Context-Aware Role-Based Access Control Model to RFID Security Management

計劃編號：NSC 96-2416-H-216-004
執行期間：96 年 8 月 1 日至 97 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：林彥廷、呂鍾鑫、陳逸瑋

摘要

無線射頻辨識（RFID）技術的應用日漸廣泛，因為利用 RFID 的無線傳輸特性，可以提供多種作業上的便利性與快速的效用，但是其引發的個人隱私性與安全性是一個重要的議題。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 RFID 技術於企業流程環境，已經無法滿足企業安全性或個人隱私性考量之需求。因此，企業利用 RFID 機制於各項流程控管時，必須考量相關的情境資訊，更有彈性地授予與控管 RFID 讀取器的存取權限，讓各項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。

本計畫主要為應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理之研究，確保企業運用 RFID 技術於各項流程時，對於資訊資源提供適當的授權管理。研究內容主要包括：(1) 依各項流程所需，訂定滿足權責區分之各個 RFID 讀取器的存取權限之規則；(2) 分析各種影響 RFID 讀取器之存取控制與授權管理之情境資訊；(3) 依據 RFID 讀取器於各企業流程所扮演之不同角色是否有權責衝突關係，及依據相關情境資訊，彈性地調整各個 RFID 讀取器及所扮演角色對於相關 RFID 標籤物品之權限之規則；(4) 利用具情境認知之以角色為基礎的存取控制模型應用於 RFID 零售業之雛形系統實作。

關鍵詞：以角色為基礎之存取控制、情境認知、無線射頻辨識、授權管理

Abstract

Radio Frequency Identification (RFID) technology is applied in widespread scope. It provides convenience and speedy to many business processes due to its characteristic of wireless transmission. But the privacy and security for RFID is an important issue. However, conventional authorization management of role-based access control cannot satisfy the privacy and security considerations for more and more complex enterprise workflow while using RFID. Therefore, the access control for using RFID enterprise has to refer the context information in order to authorize and control the RFID reader permissions. It will make enterprise information resource with more perfect and safe access control and authorization management.

This project mainly applies the context-aware role-based access control to RFID security management in order to provide adequate authorization management while business adopts the RFID technology in business processes. The research aspects include the following. (1) Defining the authorization rules for each RFID reader based on its process in order to construct the separation of duty; (2) Analyzing the context information affects the RFID reader access control and authorization management; (3) Redesigning the permissions of each RFID reader for objects contained RFID tag on whether there are duty-conflict relationships between RFID readers and related context information; (4) Developing the prototyping system for retail business using RFID based on the context-aware role-based access control model.

Keywords：Role-based Access Control, Context-Aware, Radio Frequency Identification, Authorization Management

一、背景與研究目的

無線射頻辨識（Radio Frequency Identification, RFID）技術的應用日漸廣泛，無論是零售業商品之結帳、盤點、進貨與退換貨作業流程，醫療院所的病人、病歷及藥品管理，藝術品、精品的防竊或追蹤，交通道路的自助收票，亦或是圖書館的藏書管理等，皆已有實際應用的案例，在在皆顯示 RFID 的應用層面遍及各行各業，為未來產業的發展趨勢。雖然 RFID 為政府與業界日漸推廣的技術，因為利用 RFID 的無線傳輸特性，可以提供多種作業上的便利性與快速的效用，但是仍有許多廠商不敢貿然引進，主要乃基於 RFID 其無線傳輸的特性，所引發的個人隱私性與安全性的疑慮。

無論利用 RFID 於何種企業的控管流程，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。而使用者購買了具有 RFID 標籤（RFID tag）的商品，亦不希望有任何個人隱私或消費習慣的資訊洩漏。目前針對企業資訊資源的存取控制，已經有相當多的研究探討，其中「以角色為基礎的存取控制」（Role-Based Access Control, RBAC）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時，需滿足相關的權責區分（Separation of Duty）政策。此外需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，本研究主要是應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理，探討企業運用 RFID 技術來進行各種流程控管時，如何利用 RFID 中介軟體來進行完善且具彈性的安全管理。RFID 中介軟體將依據 RFID 讀取器於各流程所扮演之角色，事先規範每一個 RFID 讀取器滿足權責區分之存取權限，再考量於特定的時間或特定的地點欲執行的相關工作，感知目前已在該環境的其他 RFID 讀取器及其扮演的角色、權限等相關情境資訊，即時地提供適當的 RFID 存取之授權管理，以期對企業運用 RFID 技術來進行各項流程控管時，可以獲取更適宜、更彈性的企業資源存取之授權管理，並維護相關的隱私性與安全性。

二、文獻探討

本計畫之相關文獻包含了以角色為基礎的存取控制（Role-Based Access Control, RBAC）、權責區分（Separation of Duty）、情境（Context）、情境認知（Context-Aware）、

無線射頻辨識（Radio Frequency Identification, RFID）技術等。

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）[2][7][8][10][16][17]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。權責區分（Separation of Duty）為以角色為基礎的存取控制模型中最重要的特色之一，權責區分是一個對於多人控制政策的安全策略，尤其在需要兩個或多個不同的人共同完成一件工作時[8][10][12][15][18]。有別於傳統以角色為基礎的存取控制之研究，目前有越來越多的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][5][6][9][19][20]，即時、動態地的檢驗、調整以給予使用者適當之權限。

RFID 為日漸廣泛的技術，目前已有越來越多的文獻著重在 RFID 的安全性之研究[1][11][13][14][21]，包括介紹 RFID 的相關應用，亦或是安全性問題之探討，而一個最基本的 RFID 系統包含讀取器、標籤，及應用系統[11]。雖然已有少數文獻提出一個以角色為金鑰管理基礎的企業 RFID 標籤加密與隱私管理[22]，但是僅依照存取角色的不同，給予不同的權限以取得相對應的金鑰與部分內容資訊，未考量到情境環境的變化，無法提供更有包容、靈活、彈性的安全性管理。

三、研究方法

首先我們分析企業環境運用 RFID 技術於各項之企業流程時，依據所應用流程中之各項工作與目的間之特性，發掘可能之衝突關係，以進行權責區分準則之建立，使 RFID 讀取器之存取權限有一初步之規範。並研究可能會影響 RFID 讀取器之存取控制與授權管理之情境資訊，探討可能影響存取控管的情境資訊後，依據 RFID 讀取器應用於各項企業流程中之需求特性，並根據相關的情境資訊，讓 RFID 讀取器在任何時間、任何地點，欲執行特定工作來存取 RFID 標籤物品的相關資訊時，能重新依據當時的環境資訊，做出更具彈性與安全性的存取與授權規範。

此外，依據所提出之適用於 RFID 安全性管理之具情境認知與以角色為基礎的存取控制模型，實作一雛形系統，以便驗證本研究所提出之存取控制模型之可行性。

四、結果與討論

本計畫完成應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理之研究與實作，將有助於確保應用 RFID 技術於企業工作流程運作時，依據不同的 RFID 讀取

器所扮演之角色、需求，在適當的情境給予合理的授權管理，以確保企業透過 RFID 技術於相關的資源存取控制能達到更有彈性、安全及有效的管理，使 RFID 的安全性管理能更臻完善。

于本計畫中，我們完成的研究結果有：

(1) RFID 讀取器於各企業流程中所扮演之角色與權限分析

我們分析企業環境內運用 RFID 技術於各工作流程，分析當使用者欲使用 RFID 讀取器存取 RFID 標籤資料的工作需求、特性，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) 各種會影響 RFID 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：環境情境、讀取器情境、標籤情境與感測情境等四大類。環境情境即任何跟使用者、RFID 讀取器以及 RFID 標籤有關之周遭環境資訊，例如：時間、地理位址等；讀取器情境表示跟 RFID 讀取器有關之資訊，如讀取器種類和目前是否閒置等；標籤情境表示跟 RFID 標籤有關之資訊，如標籤種類、用途和目前使用情形；感測情境表示跟使用者、RFID 讀取器以及 RFID 標籤所在地的溫度、亮度及溼度等相關資訊。

(3) 依據權責關係與相關情境資訊，重新規劃 RFID 授權存取準則之方法設計

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 RFID 讀取器以及 RFID 標籤有關之周遭環境情境資訊比對，確保存取控管。當每位要使用 RFID 讀取器的使用者，皆需受到存取規則的控管，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應用於 RFID 零售業雛形系統實作

以零售業為雛形系統實作環境為例，經由模擬讀取器與感測器的資料收集，接收環境、使用者、RFID 讀取器與 RFID 標籤的相關情境資訊，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 95%的工作項目，所提出的適用於 RFID 安全性管理之具情境認知與以角色為基礎的存取控制模型，符合預期的目標。我們的研究可視為一個非常重要的研究議題，並可作為如何改善使用 RFID 技術之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之可行性。本計畫目前已有一

篇碩士論文、兩篇國內研討會論文、一篇 EI 等級國際研討會論文成果發表。總而言之，本計畫所提出之存取控制模型，將有助於確保企業運用 RFID 技術來進行各項流程控管時，對於資訊資源達到一個更有效及彈性的授權管理，並維護相關的隱私性與安全性，在學術研究上並已有初步的成果發表。

參考文獻

1. John Ayoade, Osamu Takizawa, Koji Nakao, “A Prototype System of the RFID Authentication Processing Framework”, 3rd International Workshop in Wireless Security Technologies, April 2005.
2. John Barkley, “Implementing Role Based Access Control Using Object Technology”, *First ACM Workshop on Role Based Access Control*, November 1995.
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. G. Chen, D. Kotz, , “A Survey of Context-Aware Mobile Computing Research,” tech. report TR2000-381, Dept. of Computer Science, Dartmouth College, Hanover, N.H., 2000.
5. Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind K. Dey, Mustaque Ahamad, Gregory D. Abowd, “Securing Context-Aware Applications Using Environment Roles”, SACMAT’01, May 3-4, 2001.
6. 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.
7. David Ferraiolo, Richard Kuhn, “Role-Based Access Control”, *In Proceedings of 15th NIST-NCSC National Computer Security Conference*, pages 554-563, October 1992.
8. 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.
9. 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

10. Virgil D. Gligor, Serban I. Gavrila, David Ferraiolo, “On the Formal Definition of Separation-of-Duty Policies and Their Composition”, *Proceedings of IEEE Symposium on Security and Privacy*, IEEE Computer Society, May 1998.
11. Knospe Heiko, Pohl, Hartmut, “RFID Security”, Information Security Technical Report, Volume 9, Issue 4, December 2004, pp. 39-50.
12. J. Joshi, E. Bertino, B. Shafiq, A. Ghafoor, “Dependencies and Separation of Duty Constraints in GTRBAC”, *Proceedings of the eighth ACM Symposium on Access Control Models and Technologies* (*SACMAT 2003*), p51-63, June 2-3, 2003.
13. Byungil Lee, Howon Kim, “A Design of Privacy Conscious RFID System Using Customizing Privacy Policy Based Access Control”, EUC Workshops 2005, LNCS 3823, 2005, pp. 673 – 682.
14. Su Mi Lee, Young Ju Hwang, Dong Hoon Lee, Jong In Lim, “Efficient Authentication for Low-Cost RFID Systems”, ICCSA 2005, LNCS 3480, 2005, pp. 619–627.
15. Michael J. Nash, Keith R. Poland, “Some Conundrums Concerning Separation of Duty”, *Proceedings of IEEE Computer Society Symposium on Security and Privacy*, IEEE Computer Society Press, May 1990.
16. Ravi Sandhu, Venkata Bhamidipati, “The URA97 Model for Role-Based Administration of User-Role Assignment”, *In T. Y. Lin and Xiaolei Qian, editors, Database Security XI: Status and Prospects*, *North-Holland*, 1997.
17. 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.
18. Richard T. Simon, Mary Ellen Zurko, ”Separation of Duty in Role-Based Environments”, *10th Computer Security Foundations Workshop*, June 10-12, 1997.
19. Marc Wilikens, Simone Feriti, Marcelo Masera, “A context-Related Authorization an Access Control Method Based on RBAC: A case study from the health care domain”, SACMAT’02, June 3-4, 2002, pp.117-124.
20. Beika Zhan, Bernd Kurz, “A Multi-Context Visual Web Page Authoring Tool”, Proceedings of the 3rd Annual Communication Networks and Services Research Conference, 2005.

21. 奚正德, 張克章, “RFID 相關應用與安全機制簡介”, 資通安全專論, 2006 年 9 月

22. 陳俊德, 李昆霖, 吳盈杰, “架構一個以角色為金鑰管理基礎的企業 RFID 標籤加密與隱私管理”, 數位科技與創新管理國際研討會, 2006 年

出席國際學術會議心得報告

計畫編號	NSC 96-2416-H-216 -004
計畫名稱	應用具情境認知之以角色為基礎的存取控制模型於 RFID 安全性管理
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	2008/8/19-21 美國拉斯維加斯
會議名稱	Nineteenth International Conference on Systems Engineering (ICSEng 2008)
發表論文題目	Applying Role-based Access Control in Combining the Chinese and Western Medicine Systems

一、參加會議經過

ICSEng 2008 之全名為 Nineteenth International Conference on Systems Engineering，ICSEng 2008 共收到超過 130 篇之論文投稿，每篇論文經過至少兩位的審稿者審查，最終有 93 篇被接受為完整論文發表，及四篇海報論文，且有 IEEE Computer Society Order Number，由此可見 ICSEng 2008 是一個成功、歷史悠久、且具貢獻的國際研討會。

此次 ICSEng 2008 在每天早上各安排了一場專題演講，在三天的議程裡，本人選擇了第三天的「系統永續性」（System Sustainability）之專題演講，結果未料一早到會場欲參與該場專題演講，才看到臨時取消的公告，對於主辦單位的諸多安排，個人認為尚有改進之處。

ICSEng 2008 三天的議程裡，共分成 12 個場次，本人論文被分配至第十二場次，場次名稱為電腦輔助醫療診斷系統，該場次安排五篇論文發表，其中有兩篇論文之作者為同一研究單位，故由其中一位作者同時報告兩篇。

二、與會心得

此次 ICSEng 2008 舉辦地點在美國內華達州立大學拉斯維加斯分校，本人第一次前往美國，很高興該研討會是在學校內舉辦，而非飯店內舉辦，讓本人有幸參觀美國大學的校園、上課教室，瞭解到美國的教育與文化。

由於舉辦地點在美國拉斯維加斯，拉斯維加斯原是沙漠中的一個綠洲，故天氣炎熱，在研討會期間的氣溫，高達華氏一百多度，約有攝氏 42 度，比其台灣的最高氣溫，仍高出許多，故本人非常無法適應該地的氣溫，建議往後若欲前往該地參與研討會的學者，需先有萬全的心理準備。

此外，本人以往參與的研討會以亞洲地區所舉辦的居多，此次有機會參與在美國舉辦的研討會，讓我收穫良多，在此次會議中，瞭解到西方文化與東方文化的差異，在以往所參加的研討會，大部分的主席及與會者，會讓論文發表者報告完之後，再開始發問、互相交流，而此次所參加的研討會，主席及與會者，會隨時中斷論文發表者的報告，對於有興趣的研究議題，討論熱烈，彼此會主動提出自我的觀點，對於西方文化的研究態度，實有增長見聞之收穫。