行政院國家科學委員會專題研究計畫 成果報告

一個應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式之設計與建置(個別型研究計畫類)
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 98-2218-E-009-019-
執 行 期 間 ：98 年 10 月 01 日至 99 年 07 月 31 日
執 行 單 位 ：國立交通大學資訊管理研究所

計 畫 主 持 人：羅濟群

計畫參與人員：碩士班研究生-兼任助理人員：何秉賢
碩士班研究生-兼任助理人員：李芳儀
碩士班研究生-兼任助理人員：陳光禹
博士班研究生-兼任助理人員：黃俊傑

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 99 年 08 月 23 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

一個應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式之設計與建置

The Design and Implementation of Location-Aware Role-Based Access Control Model with Flexibility and Reputation Management for Web Services

計畫類別：■ 個別型計畫　□ 整合型計畫
計畫編號：NSC　98－2218－E－009－019－
執行期間：98 年 10 月 01 日至 99 年 07 月 31 日

計畫主持人：羅濟群
共同主持人：
計畫參與人員：黃俊傑、何秉賢、陳光禹、李芳儀

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：國立交通大學資訊管理研究所
中　華　民　國　99 年 8 月　23　日

行政院國家科學委員會專題研究計畫成果報告

一個應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式之設計與建置

The Design and Implementation of Location-Aware Role-Based Access Control Model with Flexibility and Reputation Management for Web Services

計畫編號：NSC 98－2218－E－009－019－

執行期限：98 年 10 月 1 日至 99 年 7 月 31 日

主持人：羅濟群　　國立交通大學資訊管理研究所

計畫參與人員：

黃俊傑、何秉賢、陳光禹、李芳儀　　國立交通大學資訊管理研究所

中文摘要

於Web Service平台提供認證與資源之存取控制等安全服務是相當重要。認證服務是為保障服務提供者與需求者雙方身份之確認；存取控制可以保障合法的需求者存取到符合它存取權限內的資料。現有存取控制機制以「以角色為基底的存取控制機制」應用圍最廣泛。延伸存取控制標記語言它是應用在 Web Service 上的一種結合存取控制機制的標記語言，它將 RBAC 整合至該語言內。也有學者提出以地理位置為基礎之存取控制機制。但是這些架構都缺乏一些元素來滿足Web Service的存取控制要求。因此，提出以位置為基底並兼具彈性與信譽管理的存取控制機制。在此機制下，Web Service 伺服器依據目前需求者所在之位置資訊、該需求者在此位置下信譽度、結合所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度等參數結合政策定義之資料庫，做為具彈性以角色為基底控制機制設計之基礎。所有信譽值的計算是由領域代理者完成。實作結果，證明本研究可以達到雙向認證之目的及滿足具彈性之存取控制要求，使得需求者必須依當時之條件存取到符合該條件的資料內容。

關鍵字：雙向認證、以角色為基底存取控制機制、延伸存取控制標記語言、以位置為基底並兼具彈性與信譽管理的存取控制機制

Abstract

Role Based Access Control (RBAC) is a kind of access control which assigns the access privilege to a role. The extensible access control markup language (XACML) is a standard access control language for web services. Current XACML only supports the RBAC model or an extension of RBAC, like geographic based RBAC. However, reputation information and the trust value of routing path, etc., are also the important factors while designing a flexible access control mechanism for web service. This paper introduces an access control mechanism called flexible access control. Flexible access control is a combination of requester's role, location, requester's reputation, and the trust degree of the routing path. The service provider easily calculates the requester's access privilege with respect to a specific resource. If a requester is in an unsecure network domain, the routing path is not trusted by the service provider, or the requester's reputation is significantly low, the requester's access privilege will be less than the role which was initially assigned. We implement this mechanism using XACML. The implementation results show that the proposed mechanism is feasible.

Keywords: Role based access control, Extensible access control markup language, Flexible access control, Location, Reputation

一、緣由與目的

行動商務已經成為應用現行網路環境發展而成的應用服務，而此應用服務可藉由以服務為導向之架構(Service-Oriented Architecture, SOA)建構而成，並使用 Web Services 做為發展所需要的服務。這是因為 Web Services 具有跨平台、整合性強與開放標準等特性，因此提供了一個彈性大的系統整合環境。然而，以 Web Services 做為開發之應用環境之資訊安全需求，並不只有認證與傳輸的安全性。對 Web Services 而言，存取控制機制也是一個很重要的安全要求，藉由此機制之執行，可以確保所有需求端(client to server 或 server to server)獲得適合的角色，並以此角色結合相關的環境參數，以獲得滿足他的角色與在此環境下的相關存取權力。

本計劃主要探討以 Web Services 發展架構下，探討一個以位置為基底並兼具彈性與信譽管理之 RBAC 機制之設計與建置。故於以位置為基底並兼具彈性與信譽管理之 RBAC 機制之設計就在驗證此方法之可行性。本系統在描述如何讓 Web Service 可以提供認證與存取控制的安全服務，並讓任一使用者必須完成身份認證後才能與 Web Service 建立連線通道。Web Service 再根據使用者目前所處的環境及與此使用者相關的信譽資訊，進行信賴程度評估，做為給予存取權限調整之依據。故同一個使用者對同一受體(Object)的存取權限之初始化完後，並非無法調整。系統依據信賴程度評估結果，動態調整存取權限，其存取能力必須小於或等於對該受體存取能力之初始值。為滿足上述之要求，本計劃實作一個「一個應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式(The Design and Implementation of Location-Aware Role-Based Access Control Model with Flexibility and Reputation Management for Web Services, LA-RBAC-RM-WS)」系統。其相關模組及實作結果將於後續章節作描述。

本計畫工作項目包含(1)探討現行 SAML 與具延展的存取控制標記語言(Extensible Access Control Markup Language, XACML)之標準規範 (2)Web Services 安全通信架構與協定研究與設計 (3)應用於 Web Services－以位置為基底之存取控制機制之研究與設計(4)應用於 Web Services－以資料內容為基底之存取控制機制之研究與設計(5)應用於 Web Services－以信譽及信賴管理為基底之存取控制機制之研究與設計(6)實作應用於 Web Services－以位置為基底並兼具彈性與信譽管理之 RBAC 機制，並探討本機制之效益評估。

二、文獻探討

本小節將 Web Services 架構、Web Services 安全規範標準及存取控制機制做相關的文獻做概略性文獻討論。

2.1 Web Services 架構

Web Services 可以視為一種介面，描述一組可經由標準 XML 訊息存取的網路操作，它使用標準且正式的 XML 觀念來描述，以提供服務時所需的細節，包括訊息格式、傳輸通訊協定和位置。而服務導向架構主要的角色有：服務要求者、服務提供者及服務登錄，如下圖 1 及圖 2。

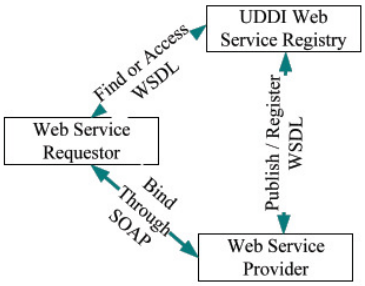


圖 1：網路服務導向架構

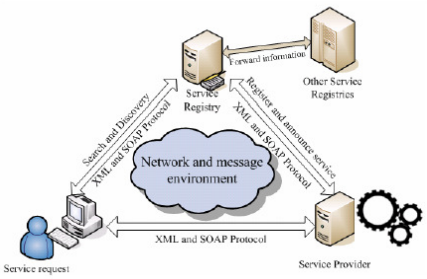


圖 2：網路服務導向架構

使用 Web Services 為基礎發展任何服務系統時，必須考慮到三個重要的因素[2] [3] [4] ：網路服務的發現(Discovery)、網路服務的品質(Quality of Service)及網路服務的安全(Security)。其中於網路服務安全上，則是保證網路服務是否成功的重要因素，惟有提供足夠的安全機制，包括：認證服務、資料加/解密、數位簽章服務、安全的傳輸通道、授權及存取控制機制等等。經由上述的安全機制，以確保是合法的使用者依據授權政策之內容，執行符合存取控制規則之權限以取得受保證的資料，並於資料傳輸過程，不需擔心資料被竊取或篡改等問題。故安全機制的建立對 Web Services 而言是非常重要。

2.2 Web Services 安全規範標準

對於 Web Services 的安全性問題，IBM、Microsoft 和 Verisign 聯合發佈了一個關於 Web Services 安全性（Web Services Security，WS-Security）的規範，該規範提供了一套幫助 Web Services 開發者保護 SOAP 訊息交換的機制。這個規範已經被 OASIS 所接受，並且成立一個 Web Services 技術委員會（Web Services Technical Committee，The WSS TC），以促使 WS-Security 成為開放標準。

由於 XML 本身無法提供網路交易安全的特性，故 OASIS 發表安全宣示標記語言(SAML)，是以 XML 為基礎發展而成的，最新的規格為 SAML 2.0。 目的是提供採用 Web Services 的不同站臺，可以藉由 SAML 彼此溝通，並且安全地交換授權及認證，主要透過四種宣示以提高 XML 架構的安全性：認證宣示(Authentication Assertion)、屬性宣示(Attribute Assertion)、決策宣示(Decision Assertion)及授權宣示(Authorization Assertion)。藉由 SAML 可以整合 Web-based 的安全機制達到單一登入的功效，能夠讓多家服務供應商跨站臺使用，並且以標準架構及協定提供資源共享的服務。SAML 的認證方式相當簡單，就如同一般登入方式，所不同的是帳號資料庫並不見得存在於該網站上，而可能是在遠端其他公司的伺服器。只要雙方允許彼此交換 SAML 憑證，使用者就可以藉由另一方的登入資訊取得存取站臺的權限。依據兩個站臺間的友好程度，可以決定使用者的授權層級，讓站臺管理者保有自行調整的彈性。SAML 規格中定義了 SAML 身份識別聲明如何被請求、產生以及通過驗證。另外，SAML 運用了產業的標準協定及訊息架構，例如:XML 簽章（XML Signature）、XML 加密（XML Encryption）及 SOAP。SAML 可以容易地整合在標準的環境中使用，例如 HTTP 及一般的瀏覽器中。同樣地，其它的安全機制也可以使用 SAML 作為授權及確認層，例如:SAML 補足 SOAP 中不足的安全功能。故 SAML 可視為不同安全技術跨越 Web services 的一項重要產業標準。

OASIS 除了制定 SAML 規範外，還制定 XACML 規範[10]，目前正制定 XACML 3.0 草案。在整個規範中有兩個 profiles 是非常重要的，包括 SAML profile 與 RBAC profile。其中 SAML profile 主要是定義如何使用 SAML 2.0 來保護、傳送及對 XACML schema instances 的需求。整個運作架構如圖 3 所示。

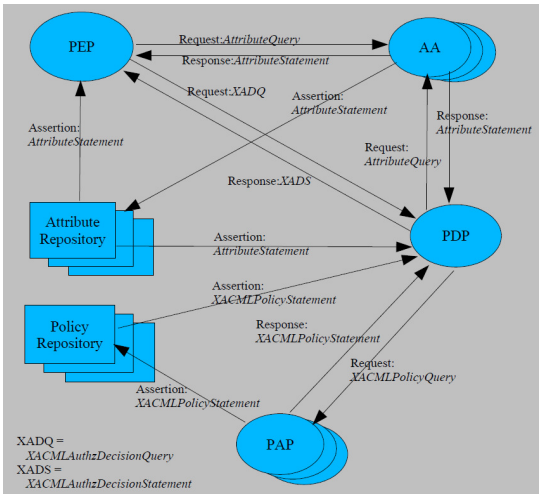


圖 3: XACML 之運行架構

XACML 整個核心主要是在描述 XACML schema，該 schema 是遵守 W3C XML schema。其 data-flow model 與 policy language model，如下圖 4 及圖 5 所示。

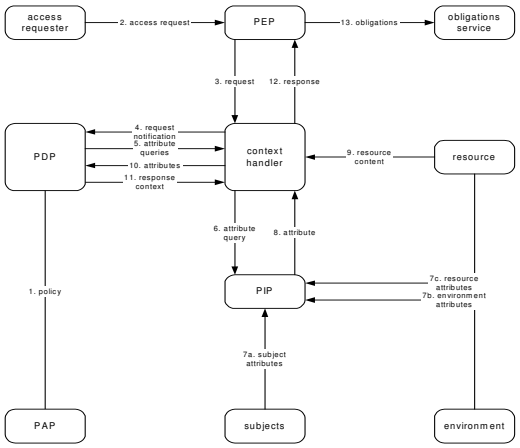


圖 4: Data-flow Model

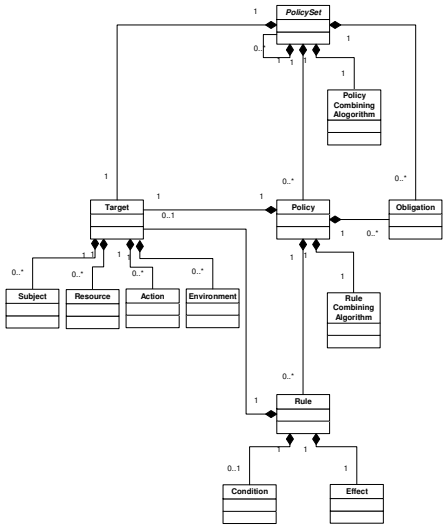


圖 5: Policy Language Model

2.3 存取控制機制

目前的存取控制機制已日趨成熟，其中以近來常被提及的 Role Based Access Control, RBAC [7] ，以角色為基礎的存取控制最為熱門，因為它藉由角色指派來分開主受體，使得主體獲得授權以及受體可接受的存取限制這兩項動作透過角色來完成，而並非傳統存取控制機制的將指派動作連貫在一起。目前 RBAC 已成為 NIST(National Institute of Standard and Technology)的標準之一[5] [8] ，並於 2001 年完成標準制定。在此標準中 RBAC 的基本元素共有七個：使用者(User)、角色(Role) 、權限(Permissions) 、操作(Operations)、物件(Objects)、會期(Sessions)及限制(Constraint) 。若以模式來描述 RBAC，可分成核心 RBAC($RBAC_0$)(Core RBAC) 、階層式 RBAC (Hierarchical RBAC)($RBAC_1$) 、限制式 RBAC($RBAC_2$)(Constraint RBAC)及將前三個模式結合在一起，形成 $RBAC_3$ (Combines RBAC)。下圖 6 為 $RBAC_3$。

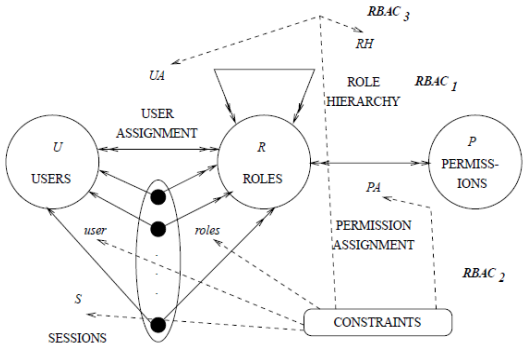


圖 6: Combines RBAC

此外，以位置為基底所形成的存取控制概念[1] [6] ，亦被很多學者提出。但此方式仍無法滿足 Web Service 的彈性存取控制的要求。此外，對於信譽度的計算方式及其分類方式，[9] 有作詳盡的描述。對於信譽度的計算，其模式非常多，須依需求而來制定。

三、研究方法

本研究是以 Web Services 發展架構下，探討與設計一個以位置為基底並兼具彈性與信譽管理之 RBAC 機制，以達系統安全之目的。並藉由系統實作說明其成效。以下即就本研究之機制、架構與實作之內容做描述。

3.1 身份認證

本研究於身份認證部份，採以憑證為基底的雙向身份認證機制。換句話說，由於 Web Service 與需求者都經由合法程序向憑證伺服器註冊以取得憑證，所有憑證都有憑證伺服器的簽章，未來可藉由簽章的驗證，以確定該憑證的合法性及憑證擁有者的資訊。故未來需求者向 Web Service 請求服務時，藉由雙方憑證資訊完成身份認證之目的。

3.2 存取控制機制

本機制為具彈性的存取控制機制。此機制結合 RBAC 模式與使用者 Profile 存取控制機制。在使用者 Profile 中，包含該需求者的信譽值、所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度。其中需求者在某一次交易下的信譽值計算方式如下：

$$REP\_Trans_{U_i}^{d_j} = \alpha_1 \times (F(A) + F(FR) + F(PD)/3) + \alpha_2 \times ((\sum_{U=\{U_l | U_l \in d_i \wedge U_l \neq U_i\}}^{U_l \to U_i} (F(A) + F(FR) + F(PD)/3))/\#U)$$

其中 $\alpha_1 + \alpha_2 = 1$；$F(A)$ 表示該需求者曾經發生過幾次攻擊；$F(FR)$ 表示該需求者曾經發生過多少次的錯誤請求；$F(PD)$ 表示該需求者曾經發生過多少次的大量封包傳遞。此外，$F(\cdot) = e^{-q \times n}$。$q$ 是一個參數介於 0 和 1 之間，此參數控制信譽度對存取控制機制的影響程度；n 表示請求的發生次數。

在某一個領域下信譽度的計算方式如下，其中 $\beta_1 + \beta_2 = 1$：

$$REP_{U_i}^{d_j} = \beta_1 \times REP\_Trans_{U_i}^{d_j}(T_{t-1}) + \beta_2 \times REP\_Trans_{U_i}^{d_j}(T_t)$$

整體信譽度的計算方式如下：

$$AREP_{U_i} = (\sum_{V=\{d_j | d_j \in D \wedge REP_{U_i}^{d_j}\}}^{U_i \prec d_j} f \times REP_{U_i}^{d_j})/\#V$$

其中 $U_i \prec d_j$ 表示 U_i 曾經拜訪過領域 d_j；f 表示衰退函數，所呈現的含意指的是愈早被拜訪的領域對整體信譽度的影響愈少；相反的，愈晚被拜訪的領域對整體信譽度的影響愈多。

同理，每個領域信譽度的計算方式也採用同樣的方法，除了 $F(\cdot)$ 的項目不一樣。此函數項目包括封包轉送錯誤次數、路由錯誤發生的次數及未提供保護的次數。最後，可以算出整個路由路徑的信任值為 $\prod_i RPT_{d_i}$。

該需求者的 Profile 以下列方式表示：

$$\{User, Domain, SLV, REP, AREP, RPT\} \to ARET \times SLV \times RPT = PRF$$

最後，該需求者可以獲取的權限以下述關係表示之：

$$PRA \subseteq PRMS \times ROLES \times PRF$$

其中 $PRMSAss_p(r, prf) = \{p \in PRMS | (p, r, prf) \in PA\}$。

3.3 系統架構

本 LA-RBAC-RM-WS 系統之設計是依據本研究所提的以位置為基底並兼具彈性與信譽管理的 RBAC 模式機制的架構設計而成。本系統採模組化的設計，軟體實作部份共分七個模組：憑證管理子系統(Certificate Management Subsystem, CMS)、角色管理子系統(Role Management Subsystem, RMS)、身份認證子系統(User Authentication Subsystem, UAS)、信任評價子系統(Trust Evaluation Subsystem, TES)、資源存取控制子系統(Resource Access Control Subsystem, RACS)、服務提供子系統(Service Provision Subsystem, SPS)及操作介面子系統(Operation Interface Subsystem, OIS)。其系統架構如下圖 7 所示。

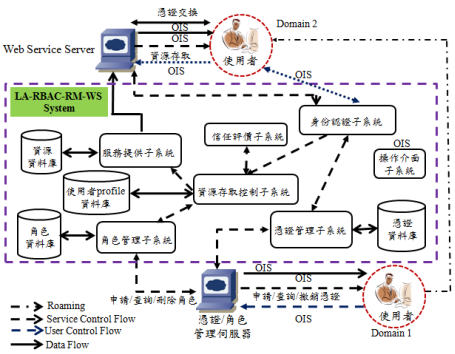


圖 7:LA-RBAC-RM-WS 系統架構圖

本系統共有四個資料庫，包括：憑證資料庫、角色資料庫、使用者 profile 資料庫及資源資料庫。此外，本系統共有兩個伺服器，包括：憑證/角色管理伺服器與 Web Service 伺服器。以下就伺服器、資料庫功能及七個子系統作細部說明。

憑證/角色管理伺服器與 Web Service 伺服器之細部說明：

- 憑證/角色管理伺服器：此伺服器提供兩個功能，包括：憑證管理與角色管理。憑證管理提供讓所有人可以申請憑證、撤銷憑證及憑證驗證等功能；角色管理提供讓合法的使用者向 Web Service 伺服器請求角色的要求，作為未來請求資源時之依據。另外，角色管理還提供刪除角色、變更角色及角

色查詢的功能。為達上述功能，此伺服器提供兩個子系統：憑證管理子系統及角色管理子系統。

- Web Service 伺服器：此伺服器提供資源供需求者使用。當需求者完成身份認證及資源存取控與信管理後，即可依其最後評價之結果獲取相對應之資源。為達上述功能，此伺服器提供四個子系統：身份認證子系統、信任評價子系統、資源存取控制子系統及服務提供子系統。

憑證資料庫、角色資料庫、使用者 profile 資料庫及資源資料庫之細部說明：

- 憑證資料庫：主要儲存憑證資料的資料庫，供憑證管理子系統及身份認證管理子系統查詢使用。
- 角色資料庫：主要儲存角色資料的資料庫，供角色管理子系統及資源存取控制子系統使用。此資料庫儲存所有角色資訊及使用者相對應之角色資訊。
- 使用者 profile 資料庫：此資料庫主要儲存需求者依所在位置資訊、信譽值、整體信譽值、路由路徑之信任值及所在位置之安全層級及最後計算之評價結果。此外，當需求從一個領域到另一個領域時或定期更新時，其 profile 會被重新決定並寫回至此資料庫。
- 資源資料庫：此資料庫是提供所有資源給所有需求者。此資源最後會由服務提供子系統傳送給需求者。

憑證管理、角色管理、身份認證、信任評價、資源存取控制、服務提供及操作介面子系統之細部說明：

- 憑證管理子系統(CMS)：CMS 負責憑證申請、發放與撤銷等工作。當需求者發起憑證申請，CMS 審核使用者資訊後，產生憑證並對此憑證簽署後送給使用者，並將使用者資訊送至角色管理子系統。此外，所有憑證是由憑證管理伺服器所產生，依照 X.509 V3 的格式產生，故所有憑證都由該伺服器簽署過，未來所有使用者可下載該伺服器的公開金鑰以驗證該憑證的合法性。下圖 8、圖 9 及圖 10 為 CMS 操作概念。

圖 8：憑證管理子系統操作概念

圖 9：憑證管理子系統操作概念

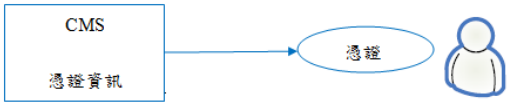


圖 10：憑證管理子系統操作概念

- 角色管理子系統(RMS)：RMS 負責角色授予、更新與刪除等工作。當需求者獲得憑證的同時，該子系統依照使用者資訊將授予它一個角色。此外，RMS 會與資源存取控制子系統連結，當需求者發起對 Web Service 資源做存取時，資源存取控制子系統便會呼叫 RMS 查看該需求者原有的角色，及存取權限。下圖 11 及圖 12 為 RMS 操作概念。

圖 11：角色管理子系統操作概念

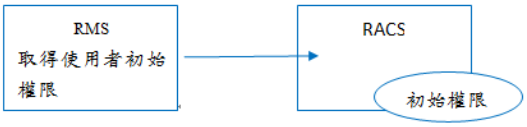


圖 12：角色管理子系統操作概念

- 身份認證子系統(UAS)：UAS 負責 Web Service 與需求者雙向認證工作。當需求者向 Web Service 提出資源存取需求時，需先藉由雙方交換自己的憑證資訊，確認身份及憑證是否有效後，方

能進行後續的資源存取。此外，UAS 會與資源存取控制子系統連結，當需求者完成身份認證後，UAS 會將使用者資訊傳送給資源存取控制子系統。下圖 13 為 UAS 操作概念。

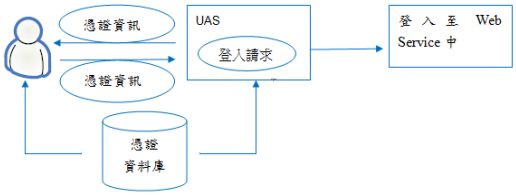


圖 13：身份認證子系統操作概念

- 信任評價子系統(TES)：TES 負責對需求者進行評價，此評價之結果將傳遞給資源存取控制子系統，作為需求者存取資源之依據。TES 計算模式包括根據使用者目前所處的環境及與此使用者相關的信譽資訊，進行信賴程度評估。下圖 14 為 TES 架構圖。因此，TES 所輸入參數包括使用者所在位置、路由路徑、路由路徑各個節點的 Trust 值及使用者的 Trust 值來計算最終該使用者的信譽值。下圖 15 為 TES 操作概念。

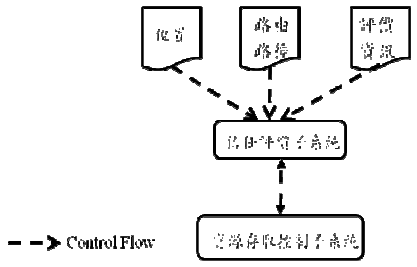


圖 14：信任評價子系統架構圖

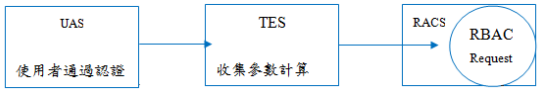


圖 15：信任評價子系統操作概念

- 資源存取控制子系統(RACS)：RACS 負責接受需求者對 Web Service 的資源需求，當它收到需求後會與 RMS 及 TES 連結，以決定該資源被存取之權限調整。此外，當 RACS 完成對該資源之存取調整後會將需求傳遞給服務提供子系統，才能讓需求者獲得該資源或回傳不能讀取之結果。下圖 16、圖 17 及圖 18 為 RACS 操作概念。

圖 16：資源存取控制子系統操作概念

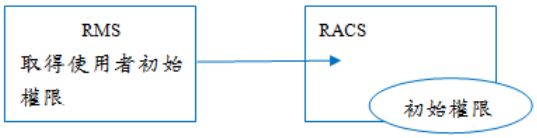


圖 17：資源存取控制子系統操作概念

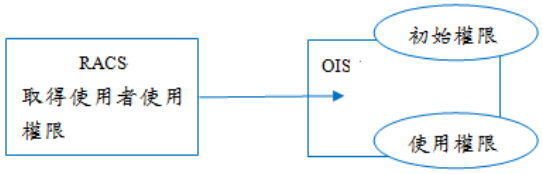


圖 18：資源存取控制子系統操作概念

- 服務提供子系統(SPS)：SPS 負責提供需求者所需之資源。RACS 必須與服務提供子系統產生連結，以決定該需求者對某一資源的使用權。下圖 19 為 SPS 操作概念。

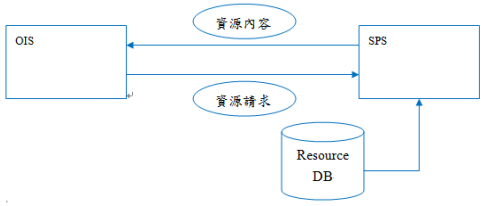


圖 19：服務提供子系統操作概念

- 操作介面子系統(OIS)：OIS 負責提供使用者介面讓使用者與子系統間可以溝通，例如：當使用者有對憑證發出請求時，它必須與 CMS 產生連結；當使用者有對角色查詢發出請求時，它必須與 RMS 產生連結；當使用者進行身份認證請求時，它必須與 UAS 產生連結；當使用者有對使用權限查詢發出請求時，它必須與 RACS 產生連結。此外，當資源存取子系統完成對

該資源之存取調整後會將需求傳遞給 SPS，也需透過操作介面子系統才能讓需求者獲得該資源或回傳不能讀取之結果。下圖 20、圖 21 及圖 22 為 OIS 操作概念。

圖 20：操作介面子系統操作概念

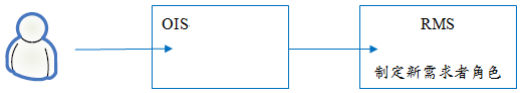


圖 21：操作介面子系統操作概念

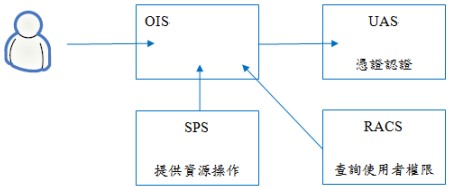


圖 22：操作介面子系統操作概念

LA-RBAC-RM-WS 系統之 use-case 如下圖 23 所示。

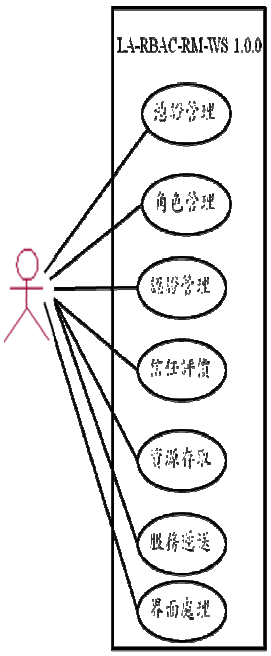


圖 23：LA-RBAC-RM-WS 系統之 use-case

- **Use-Case 1**：憑證管理
  Actors：需求者、系統管理者
  Goals：憑證管理功能，包含新增、查詢與撤銷功能。
- **Use-Case 2**：角色管理
  Actors：需求者、系統管理者
  Goals：角色管理功能，包含新增、更新、查詢與撤銷功能。
- **Use-Case3**：身份認證管理
  Actors：需求者、系統管理者
  Goals：雙向認證功能。
- Use-**Case 4**：信任評價管理
  Actors：資源存取控制子系統
  Goals：信任評價計算。
- **Use-Case 5**：資源存取控制
  Actors：身份認證子系統、信任評價子系統、角色管理子系統、服務遞送子系統
  Goals：資源存取控制功能。
- Use-**Case 6**：服務遞送
  Actors：需求者、資源存取控制子系統
  Goals：服務傳遞功能。
- **Use-Case 7**：介面管理
  Actors：需求者、系統管理者
  Goals：使用者操作介面功能。

3.4 實作環境與結果

本小節將依照上述的系統架構實作此系統。下述為實作此系統所需的軟體：

- Java SDK Jre6.0 或以上，以及任一 Java SDK
- Sun's XACML Implementation 1.2
- OpenSSL 0.9.8k
- Eclipse 3.5
- MySQL 5.1.44

本實作模擬有 5 個路由領域，每個使用者均需向 CMS 註冊以獲得憑證，並獲得相對的角色。之後，任一使用者可以在任一個路由領域提出資源需求，Web Service 將依照需求者所在位置、信譽資訊、結合所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度等參數結合，以計算出評價結

果。最後，再將此需求者本身的角色及其結果，以產生相對於該需求者的最新的存取權限。Web Service 再 SPS 將可允許的需求資源傳給該需求者。下圖 24 為 LA-RBAC-RM-WS 系統之測試環境架構圖。

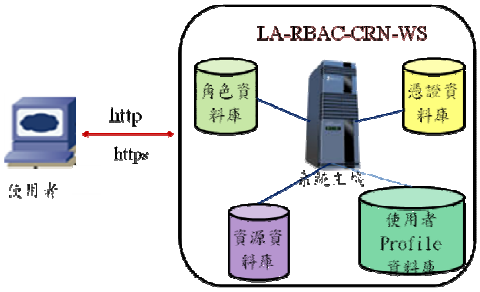


圖 24：LA-RBAC-RM-WS 系統之測試環境架構圖

下述為實作之結果：圖 25 及圖 26 為憑證申請與憑證驗證之畫面。圖 27 為某一個資料表之完整內容。圖 28、圖 29 及圖 30 為同一個需求者，但是因為在不同領域、資料路由路徑亦不同及它本身的信譽值有所改變等因素下，故能存取的內容亦不同，故本研究可以達到彈性存取控制之目的。

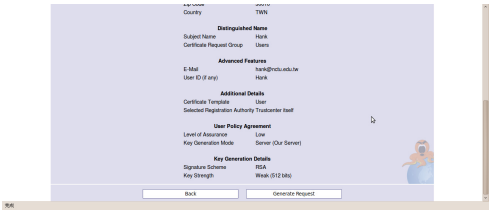


圖 25：憑證請求

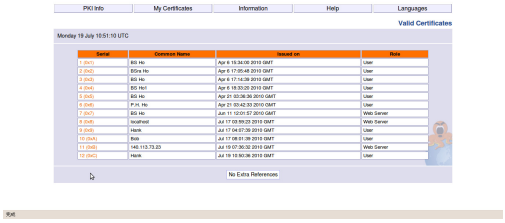
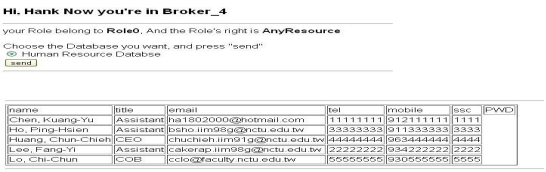


圖 26：憑證要求被 CA 所簽署

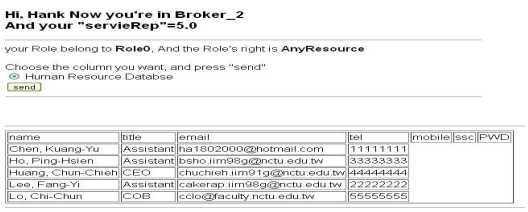
name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111	912111111	1111	123
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333	911333333	3333	456
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444	963444444	4444	789
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222	934222222	2222	987
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555	930555555	5555	654

圖 27：某一個資源之資料表



name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111	912111111	1111	
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333	911333333	3333	
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444	963444444	4444	
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222	934222222	2222	
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555	930555555	5555	

圖 28：需求者在 domain4 下要求此資源所能存取的權限



name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111			
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333			
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444			
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222			
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555			

圖 29：需求者在 domain2 下要求此資源所能存取的權限

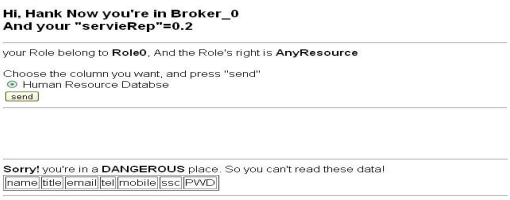


圖 30：需求者在 domain0 下要求此資源所能存取的權限

3.5 安全性分析

本小節就本研究所提的以位置為基底並兼具彈性與信譽管理的存取控制機制之安全性作分析：認證與存取控制兩個機制作說明。

由於本研究於認證部份是採用雙向認證方式，即是 Web Service 與需求者雙方進行憑證交換，且憑證內含憑證伺服器的簽章，故可以確認此憑證的合法性，以完成相互認證之目的。此外，Web Service 與需求者端間的通訊採 SSL 機制，故可以確保通訊過程的安全。

於存取控制方面，本研究採 RBAC 模式與使用者 Profile 相互搭配所形成的具彈性的存取控制機制。RBAC 模式本身就是確保合法的使用者只能存取其權限範圍下可存取的內容；再加上本機制會依據使用者所在領域、信譽資訊、結合所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度

等參數結合，以發展出一個具彈性的存取控制機制，使得需求者所能獲得的資源是小於或等於原本屬於該角色下所能授予的，故此存取控制機制滿足安全性的要求。

四、結論與建議

行動商務已經成為應用現行網路環境發展而成的應用服務，使用 Web Services 做為發展所需要的服務，已經成為一種趨勢。對 Web Services 而言，資訊安全的實踐是一個非常重要的議題。而存取控制機制即是其中一個很重要的安全要求，藉由此機制之執行，可以確保所有需求端，獲得適合的角色，並以此角色結合相關的環境參數，以獲得滿足他的角色與相當環境下的相關存取權力。

本研究主要探討如何實踐一個具有彈性的存取控制機制。為此，本研究提出以位置為基底並兼具彈性與信譽管理之 RBAC 機制之設計。在此機制下，Web Service 伺服器依據目前需求者所在之位置資訊、該需求者在此位置下信譽度、結合所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度等參數結合政策定義之資料庫，做為具彈性以角色為基底控制機制設計之基礎。所有信譽值的計算是由領域代理者完成。

另由實作結果可證實，本研究採以憑證為基礎的雙向認證達到身份認證之目的；此外，使用彈性的存取控制機制，使得需求者在不同領域及因本身的信譽值改變得不同因素下，即使採同樣的需求，仍會依情境獲得相對可獲得的資源。

五、計畫成果自評

本計畫所提的應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式，針對需求端之所在位置、可信賴度及其信譽度及資料繞送路徑(包括路由路徑及伺服器轉送路徑)之信賴度等參數結合政策定義之資料庫，做為具彈性以角色為基底控制機制設計之基礎。實作結果，證明本研究可以達到雙向認證之目的及滿足具彈性之存取控制要求，使得需求者必須依當時之條件存取到符合該條件的資料內容。因此，本研究機制應可提供在此環境下滿足具彈性效果的存取控制機制且符合雙向認證的要求。

參考文獻

[1] A. Matheus, Declaration and Enforcement of Fine Grained Access Restrictions for A Service-based Geospatial Data Infrastructure, In *Proceedings of the 10th ACM symposium on Access control models and technologies (SACMAT'05),* pp. 21–28.

[2] Chi-Chun Lo, Chi-Hua Chen, Hsiang-Ting Kao, Chih-Chien Lu, Ding-Yuan Cheng, "Research on Developing Healthy-Life Map Guiding System," 6th International Conference on Service Systems and Service Management (ICSSSM'09), Xiamen, China, June 8th-10th, 2009.

[3] Chi-Chun Lo, Ding-Yuan Cheng,Chi-Hua Chen, and Jin-Shaiang Yan, "Design and Implementation of Situation-Aware Medical Tourism Service Search System, " Management Track within WiCOM: Information Systems and Management 2008, Dalian, China, October 14-16th, 2008.

[4] Chi-Chun Lo, Ding-Yuan Cheng, Ping-Chi Lin, Kuo-Ming Chao, "A Study on Representation of QoS in UDDI for Web Services Compositions," International Workshop on Computational Intelligence in Security for Information Systems CISIS'08.

[5] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, Vol. 4, No. 3, pp. 224-274, 2001.

[6] M.L. Damiani, E. Bertino, B. Catania, and P. Perlasa, GEO-RBAC: A Spatially Aware RBAC, *ACM Transactions on Information Systems and Security*, Vol. 00, No. 00, 2006, pp.1-34.

[7] R. Sandhu, Role-Based Access Control Models, *IEEE Computer*, vol. 29, issue 2, Feb. 1996, pp. 38-47.

[8] R. S. Sandhu, D. Ferraiolo and R. Kuhn, "The NIST Model for Role-Based Access Control：Towards a Unified Standard," Proceedings of the 5th ACM Workshop on Role-Based Access Control, pp. 26-27, 2000.

[9] Q. Zhang, T. Yu, and K. Irwin, A Classification Scheme for Trust Functions in Reputation-Based Trust Management, *The Workshop of Trust, Security, and Reputation on the Semantic Web at ISWC 2004*, 7-11 Nov. 2004.

[10] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#XACML20.

無研發成果推廣資料

98 年度專題研究計畫研究成果彙整表

計畫主持人：羅濟群	計畫編號：98-2218-E-009-019-
計畫名稱：一個應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式之設計與建置(個別型研究計畫類)	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	3	3	100%	人次	
		博士生	1	1	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	1	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	1	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：□已發表 □未發表之文稿 ■撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本計畫所提的應用於網頁服務以位置為基底並兼具彈性與信譽管理的 RBAC 模式，針對需求端之所在位置、可信賴度及其信譽度及資料繞送路徑(包括路由路徑及伺服器轉送路徑)之信賴度等參數結合政策定義之資料庫，做為具彈性以角色為基底控制機制設計之基礎。實作結果，證明本研究可以達到雙向認證之目的及滿足具彈性之存取控制要求，使得需求者必須依當時之條件存取到符合該條件的資料內容。因此，本研究機制應可提供在此環境下滿足具彈性效果的存取控制機制且符合雙向認證的要求。