中山管理評論 1997年12月
第五卷第四期 pp.779-796

現代企業網路中使用者識別與存取授權之整合設計

Designing a System to Integrate Both Functions of User Authentication and Access Authorization in the Internet/Intranet Environment

黃景彰 Jing-Jang Hwang
國立交通大學
National Chiao Tung University

吳國禎 Kou-Chen Wu
國立交通大學
National Chiao Tung University

摘 要

本研究的目的是針對現代企業資訊網路資源使用管理的問題，設計一個使用者身份識別與存取授權的管理機制，此機制不僅能配合現代企業組織彈性變化的特性，也能滿足Internet/Intranet整合的企業資訊網路環境中資源使用的安全管理需求。在本研究所提出的適合現代企業網路的安全管理架構中，我們結合了ITU-T Rec. X.509公開金鑰證書和角色扮演存取授權(RBAC)的觀念，形成一個使用者身份識別和存取授權整合的設計。本方法的優點：(1)將身份識別和存取授權結合爲單一模組，可以提供更高的安全性；(2)以角色扮演作爲存取授權之基礎，較傳統的方法更適用於現代組織；(3)延伸X.509公開金鑰證書的設計，並配合智慧卡的使用，可以達成以個人自行負責爲基礎的身份識別管理。

關鍵字：網際網路，企業網路，身份識別，存取授權，角色扮演。

Abstract

This paper addresses the issue of security management in the Internet/Intranet environment. A system is designed which combines both functions of user authentication and access authorization. The design utilizes CCITT X.509 public-key certificates in a model of Role-Based Access Control (RBAC). The design offers three major benefits: (1) Less security flaws in the system, due to implementing two major functions into a single module; (2) Making the system adaptable to organizational changes, given the RBAC model; (3) Achieving greater security through the utilization of the public-key certificate, which can be saved in a smart card and is under the control of its owner.

Keywords: Internet, Intranet, authentication, authorization, RBAC.

壹、前言

根據學者 Don Tapscott(1996)的觀察，企業組織使用資訊設施有數個階段的演進過程。初期可從辦公室自動化的工作效率提昇開始，然後有團體工作網路的出現，配合業務流程的改變，以形成高效率的團隊。接著是企業內的資訊網路，將公司內部的業務加以整合，間接造成組織結構的改變。進而是企業間的電腦連線，使得企業對外的合作更密切。最後則是不同行業間商業網的形成，改變了產業結構，也造成社會發展的改變。

企業資訊網路的發展，目前最熱門的可說是 Intranet。關於 Intranet 的定義，眾說紛紜，但我們可以從兩方面去認識它。它可說是將 Internet 的技術應用於組織內部網路；另一方面，從應用軟體組合的觀念來看 Intranet ，它應該包含的功能有：訊息的交換、工作流程管制、資料庫管理、安全管理、應用程式開發平台、網路整合、目錄服務等(Mellanie Hills, 1997; Ryan Bernard, 1996)。

在一個 Internet 和 Intranet 完善整合的資訊流世界，組織內的員工可以很方便地在系統中完成資訊的交換，組織外部的使用者，也可以被允許進入組織的 Intranet 系統獲得需要的資訊。來自 Internet 的使用者可能只是單純地在 Internet 上漫遊，搜集一些公開的資訊，也可能是這個組織的業務往來對象，透過 Internet 進入 Intranet 瞭解共同合作的業務處理的進度。例如檢視訂單處理的進度，或是合作計畫進行的細節等。在這樣的資訊流世界中，特別是一個牽涉商業利益或軍事機密的組織，安全的管理顯得尤其重要。

企業網路環境資訊安全的討論可歸納包括下列的議題：安全政策的制定、資訊內容的保護、資訊網路整合的考量，以及資源使用的管理等(程捷生，1997 ； Charles P. Pfleeger, 1989; Robert L. Frank, CISSP, 1996)。其中，資源使用的管理和前三項議題有著緊密的關係。

資源使用管理的主要目的是使得軟、硬體等資訊設備的使用，與資訊內容的取得，既能滿足企業組織內部使用者的需求，又能符合安全管理政策的規範。基本上，對於企業運作及商業交易資料等資產的保護，只要著重於內部人員的身份識別與存取授權即可。但是因爲 Intranet 的伺服器(Service Server)及使用者(Client)可能遍佈在企業各處，其身份識別及存取控制必然較傳統企業的封閉網路複雜。此外，當 Intranet 和 Internet 整合後，雖然可擴展業務往來的對象，使資訊的流通更方便，但因爲使用者的身份與數目變多，更增加了安全性的風險，因此，需要一個新的使用者身份識別及存取授權控制的方法。

本研究的目的是針對現代企業資訊網路資源使用管理的問題，設計一個使用者身份識別與存取授權的管理機制，此機制不僅能配合現代企業組織彈性變化的特性，也能滿足 Internet/Intranet 整合的企業資訊網路環境中，資源使用的安全管理需求。

本篇研究的內容將先探討已發表文獻中，有關資源使用的使用者身份識別和存取授權的方法。其次，我們將提出一個適合現代企業網路的安全管理架構，並將身份識別和存取授權加以結合。最後，我們將分析此方法的特點，以及未來研究的方向。

貳、文獻回顧

已發表的文獻中，對於資訊系統資源的存取控制及使用者身份識別有相當多的討論，敘述如下。

一、存取控制

系統內部儲存的存取控制資料的形式，最基本的是「使用者：物件」的二維存取管理矩陣(Access Control Matrix)，矩陣中的每一元素代表該使用者對該物件的存取權限。當組織的成員或系統的資源有所增減時，這個存取管理矩陣也要做適當的調整。

由此二維矩陣所衍生的方法有使用者權利列法(Capability List)和物件授權

列法(Access Control List)。使用者權利列法是將二維矩陣以列(List)的資料結構方式儲存，每一位使用者都能對應到一權利列，列舉了該使用者的存取權利。物件授權列法也是將二維矩陣以列的資料結構方式儲存，每一個物件對應到一個授權列，列舉該物件被授權使用的使用者及其存取權。

當組織中的 Intranet 使用存取控制矩陣方法時，任一提供服務的伺服器都要儲存一份存取矩陣資料；組織內使用者或物件有變動時，都要將每一個伺服器的資料更新。所以，傳統的存取管理矩陣模式是不適合於 Intranet 環境的。

對於應用矩陣式存取控制方法於現代組織，會產生上述欠缺效率的管理問題，我們可以用角色扮演的存取控制(Role-Based Access Control, RBAC) (National Institute of Standards and Technology, 1996; Ravi S. Sandhu 等人, 1996) 方法加以解決。

RBAC 的使用者存取權力之授權，是決定於使用者在組織中所扮演的角色(即所擔任的職務)。因爲每一種角色的功能受限於組織的政策，所以，每一個組織提供給相同角色的功能，也會因組織的不同而有異。在 RBAC 機制中，系統管理者依據組織的各種職務功能，去定義各種角色，然後將對物件的存取權限授權給這些角色；最後再依據組織員工特定的工作責任和資格，指定他們可以扮演的角色。組織使用者(users)、角色(roles)，以及作業權限(permitted operations)三者間的關係如下圖所示。

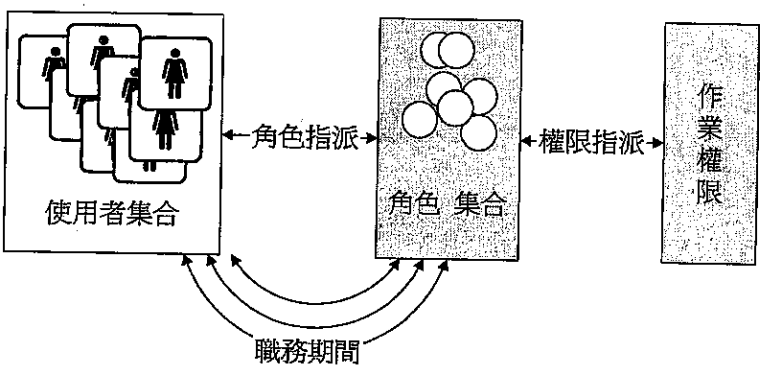

圖 1　角色扮演存取控制示意圖

由上圖我們可以看到，使用者透過角色建立起對物件存取權利的關係。使用者對應於角色的關係，可以隨著職務的更動而有所改變，不同的時候可以擔任不同的角色，稱爲「職務期間(session)」。角色和作業權限的關係雖然變動性較低，但是隨著組織安全管理的存取控制政策的改變，一個角色可能被賦予新

的權限，或是撤銷一些既有的權限。透過這種簡單的角色指派(role assignment)與權限的授與(permission assignment)， RBAC 可以適用於一個改變中的組織環境，作爲一種有效的存取管理機制。

關於 RBAC ，除了上述的簡單模式之外，還可以加入適當的條件限制(constraints)，以形成一個實際的管理機制。以任務區隔(separation of duties)的限制爲例，在做角色指派時，應避免讓一個人同時扮演兩種須做區隔的角色，否則可能會產生舞弊的機會。例如，同一人不可同時擔任採購經理(purchasing manager)和掌管會計應付帳的經理(accounts payable manager)兩種角色；同樣地，同一人可以在不同的專案計劃中擔任程式設計師(programmer)和測試師(tester)的角色，但卻不應該在同一專案計劃中，同時擔任這兩種角色。

二、身份識別

一個好的存取控制管理的前題，是要有好的使用者身份識別機制。在網路電腦系統中，它不像人和人之間可以面對面地相互驗證身份，所以要依賴使用者與電腦之間一些共享的訊息，來驗證一個使用者的身份，通行碼(password)的檢查可以說是最常使用的方法。

通行碼身份識別方法的理論基礎是假設一個正確輸入通行碼的使用者，就是該通行碼的合法使用者。一般電腦系統中，使用者身份的識別是藉由檢查使用者在登入(login)時，所輸入的通行碼來達成；系統會將使用者所鍵入的通行碼和內部的記錄做一比對，一旦通過了身份識別，系統會進一步決定該使用者對資源的使用權限。在電腦網路環境中，因爲通行碼在傳遞的過程中容易被竊聽，而且使用者每次使用網路服務時，都要重複地輸入通行碼，所以，通行碼身份識別方法不適合應用在電腦網路的環境。

Needham 和 Schroeder (1978)首先提出以密碼學的方法，在大型電腦網路上進行使用者身份的識別。而後 Denning 和 Sacco (1981)兩人則針對 Needham 和 Schroeder 協定中可能的漏洞，提出了以時間戳記爲基礎的憑證，作爲解決的方法，這也就形成了日後 Kerberos(J.T.Kohl, 1991)身份識別系統的理論基礎。

Kerberos 是一個 1980 年代由麻省理工學院的 Athena 計劃所發展的身份識別與金鑰交換的協定。其目的是要藉由公正的中央識別伺服器(authentication server)和通行票產生伺服器(ticket granting server)，爲使用者產生在有效期間可以重複使用的通行票，使得網路上相互通信的雙方，能夠確認彼此的身份，並且交換一個

通訊期間金匙(session key)，使得交換的訊息能以安全的密文方式傳遞。

CCITT 所提出的 X.509 協定(ITU-T Recommendation X.509|ISO/IEC 9594-8,1990)，也定義了三種讓網路上交換訊息的雙方可以藉由公開金鑰證書達到相互識別身份的方法。公開金鑰證書中包含了版本(version)、序列編號(serial number)、簽章演算法識別碼(signature algorithm ID)、證書核發單位名稱(issuer name)、有效期間(validity period)、使用者(subject)、使用者的公開金鑰資訊(subject public-key information)、上述欄位的數位簽章等內容。當通訊的雙方都已獲得彼此的公開金鑰證書後，可以由單向(One-way)、雙向(Two-way)，或三向(Three-way)的識別程序，來識別彼此的身份。

單向識別僅有由受驗者將識別資料傳給驗證者的單一資料傳遞動作。它可以達到以下的識別功能：(1)識別受驗者的身份，身份識別資料確實是由受驗者所產生；(2)識別驗證者的身份，身份識別資料確實是要傳送給驗證者；(3)保障身份識別資料在網路傳輸過程未被竄改，並確實是由受驗者所送出。

雙向識別程序較單向識別程序多加上一個由驗證者回覆給受驗者的訊息，除了具備單向識別的功能外，還多了以下的識別功能：(1)回覆給受驗者的身份識別資料確實是由驗證者所產生，並確實是要傳給受驗者；(2)保障回覆資料在網路傳輸過程的完整性與來源證明。

三向識別程序較雙向識別多了一個由受驗者回覆給驗證者的訊息，可以達到讓驗證者知道受驗者已收到自己的身份證明並且驗證無誤。單向與雙向識別是以檢查時間戳記是否逾時，來對抗重播攻擊(Replay Attack)，而三向識別程序則只要檢查亂數是否重複，即可對抗重播攻擊。

三、身份識別與存取授權之整合

傳統的系統安全方法是將存取管制與身份確認，分成兩個階段來完成。在 Internet 與 Intranet 結合的環境中，進入組織內電腦系統的使用者，除了一般的訪客(guest)身份較不定，需要做嚴格的存取管制外，其它的使用者身份如組織內的員工、組織業務往來的對象，這些使用者的身份較確定，如果能將身份確認和存取授權控制做適當的結合，應該可以減少整個系統安全所需儲存的機密資訊，藉由整合身份識別和存取控制成單一的模組，也可以提升整個系統的安全性。

L. Harn 和 H.-Y. Lin (1992)提出了以密碼學的方法，整合傳統的使用者通行碼，和「使用者：物件」存取控制矩陣。整合身份識別的通行碼和存取控制方

法，使得使用者在每次的存取要求時都要確認身份，較傳統的識別與存取控制分開的做法要提供更多的安全保障。但是，此方法中使用者的通行碼不同於傳統的通行碼可由使用者自己去變更，而是在註冊階段，由系統依據使用者對所有系統資源的存取權限計算出來的值，因此，對使用者較不具親和力。除此之外，當系統中新增一項資源時，所有相關使用者的通行碼均會改變，需要重新計算通行碼的值。

OSF(Open Software Foundation, 1993) 的 DCE(Distributed Computing Environment)則將 Kerberos 系統和使用者存取授權的授與相結合，形成下圖所示的架構。

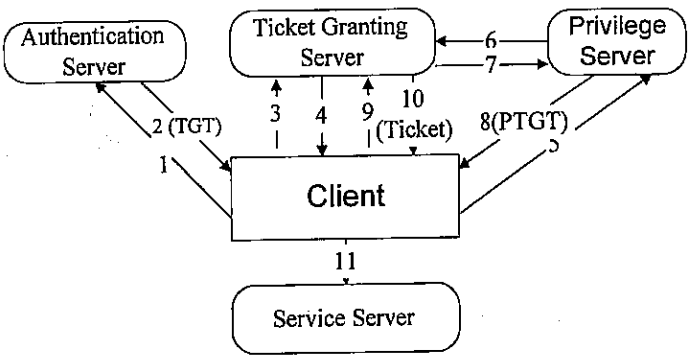

圖 2　DCE Kerberos (Ping Lin, Lin Lin, 1996)

DCE Kerberos 將授權伺服器(Privilege Server)加入原始的 Kerberos 架構中。使用者通過中央識別伺服器(Authentication Server)的身份識別後(步驟 1,2)，再拿通行票產生伺服器(Ticket Granting Server)所產生的通行票(步驟 3,4)向授權伺服器要求授權通行票(Privilege TGT, PTGP)(步驟 5,6,7,8)。使用者最後再持授權通行票向通行票產生伺服器要求一般服務的通行票(步驟 9,10)，以便向伺服器(Service Server)要求服務(步驟 11)。

授權伺服器就如同一個中央式的存取授權機制，使用者從授權伺服器得到的授權通行票就相當於該使用者的存取授權憑證。 DCE Kerberos 將原始的 Kerberos 和 Privilege Server 結合，同時解決了一般提供服務的伺服器所需要的身份識別與存取授權的問題。雖然使用者可以持同一個通行票，重複地向同一伺服器要求服務，但網路中若有許多的伺服器時，使用者仍需爲不同的服務去要求不同的通行票。

四、小結

在上述討論中，我們回顧了企業網路資源的存取控制、使用者身份識別，以及整合這兩個機制的方法。我們認爲現代企業網路的安全管理機制，應以角色扮演的存取授權方法爲基礎，以滿足現代組織變動的特性，並應整合存取授權和使用者身份識別，既可以減少管理系統安全所需儲存的資訊，也可以提升整個系統的安全性。

參、本文所提出的方法

本文所提出的企業網路使用者身份識別和存取授權的方法，包含下列四部份：(1)使用者角色之指派(2)使用者職務資訊(role profile)之儲存(3)安全管理的系統(4)使用者身份識別程序。

一、企業組織 RBAC 角色之指派

現代組織的特色之一是變動性，不論是內部人員扮演的角色功能，或是與外界訊息交換的往來對象(例如 EDI partner)，常常因應組織的需要而做調整。因此，對於一個現代組織而言，存取控制矩陣顯得並不十分適合。考量到使用者對伺服器資源存取的權限，常取決於使用者在組織中扮演的角色，所以我們以角色爲基礎的存取授權模式做爲安全管理政策的基礎。

已發表的文獻對角色扮演存取控制的討論是針對組織內部的員工，每一員工有基本的隸屬角色，表示他們和企業組織所屬部門的關係。此外，員工偶爾也需要扮演職務支援的角色，這個角色產生的原因是因組織跨部門的專案計劃常需從各個部門徵調員工，形成一個暫時的工作團隊。但在一個 Internet/Intranet 的環境，電腦系統的使用者除了組織員工外，還有業務往來的合作對象，以及在 Internet 上漫遊的訪客(guest)。所以，在 Internet/Intranet 環境，適當的 RBAC 架構應如下圖所示：

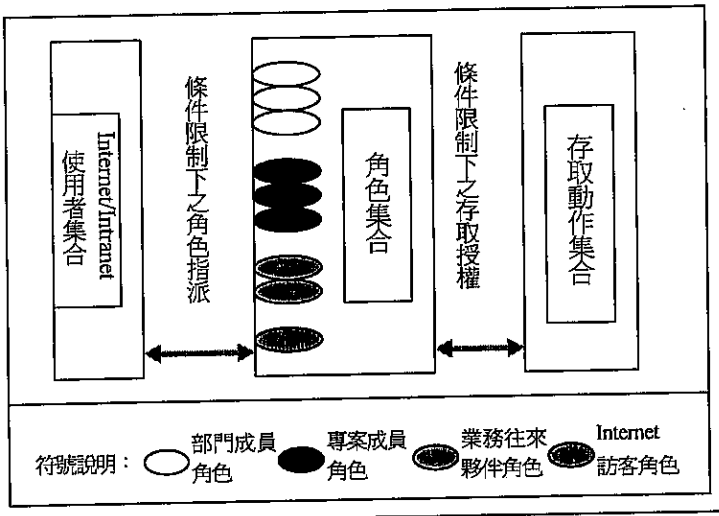

圖 3　Internet/Intranet 使用者角色扮演的架構圖

在角色集合的部分，組織內部的員工都會隸屬於某一部門，所以，這種隸屬的關係是靜態穩定的。專案成員的角色則是因專案計劃的存在而動態地產生，組織內部員工因爲業務的需要而加入某一專案計劃時，就具備了該專案成員的角色。業務往來夥伴可以是企業電子資料交換(EDI)的對象，企業和交易往來對象建立了電子資料交換的合作契約後，可以爲該契約關係產生一個往來夥伴的角色。 Internet 訪客角色則是爲 Internet 上眾多漫遊的使用者提供一個角色，在嚴格的存取管制下，他們也可以瀏覽組織所公佈的資訊。

當所需要的角色都已經建立之後，組織就要根據安全管理的政策，授權個別角色對各系統資源的存取動作。在 RBAC 方法的最後一個步驟就是依照使用者的職務及能力，指派他們擔任的角色，一個使用者可以擔任的角色的集合稱作一個使用者職務資訊(user profile)。以下圖某公司資訊處組織圖爲例：

由圖中可知，資訊處王零以先生同時擔任有「資訊部經理」、「資料中心課長」兩種角色。此外，爲了更新企業內部網路建設，公司成立一專案計劃「網路設施更新專案」，王零以先生以其專業知識和經驗，又被網羅爲成員之一。所以，就王零以先生而言，他個人的使用者職務資訊包括「資訊部經理」、「資料中心課長」、「網路設施更新專案成員」等三個角色。由王先生個人的使用者職務資訊的內容，就可以顯示他所扮演的角色，於是乎決定他對組織資源的存取權力。

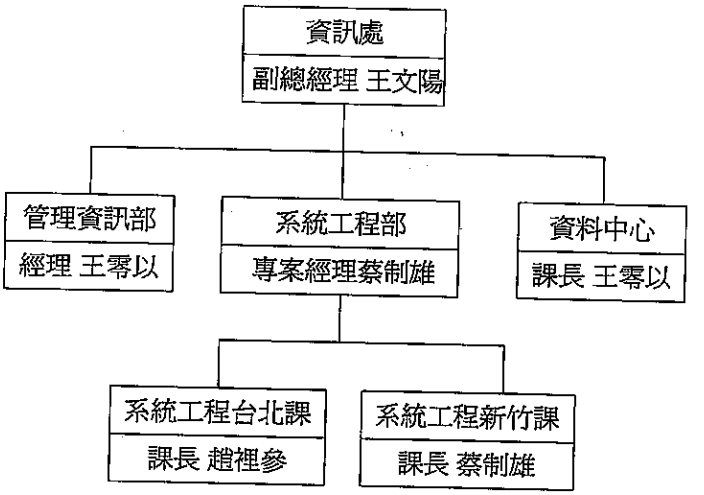

圖 4 、組織內角色扮演之圖例

二、使用者職務資訊之儲存

所有使用者的 user profile 可以集中地儲存在伺服器上，但缺點是所有的伺服器都需要儲存使用者身份確認和 user profiles 資料。上述集中式儲存 user profile 的方法，也可以改由分散地由每個使用者自己儲存。

目前使用者個人資訊或加密金鑰，多數存放在個人電腦的硬碟上，但是從智慧卡(smart card)與全球資訊網應用結合的趨勢來看(Trisha Gorman,1997)，在使用者端將智慧卡與瀏覽器搭配使用，可以爲 Internet 提供更高層次的安全性。智慧卡最主要的用途是作爲攜帶使用者個人資訊的工具，包括個人的私密金鑰及公開金鑰證書等都可以儲存在智慧卡上的記憶體中。受限於成本的考量，智慧卡與讀卡機的使用在短期內還無法在 Internet 上普及，但企業組織卻相當適合採用這項設備來強化其安全管理。

以智慧卡來儲存使用者個人私密的資料，意謂著傳統爲達到安全控管目的而集中儲存的存取控制資料，其儲存與保管的部分責任將轉移到個別的使用者。如果能將使用者身份識別的機制，和存取授權的資訊進一步結合，則可以進一步簡化並減少智慧卡上儲存的資料內容。

爲辨別使用者的身份，我們希望應用 CCITT X.509 公開金鑰憑證的概念，來做爲使用者端身份識別的機制。 X.509 公開金鑰證書的目的，主要是存放證書核發單位(Certificate Authority, CA)對使用者公開金鑰的簽章，以識別公開金

鑰證書所有人的名稱與公開金鑰之間的連結關係。若要將它和角色扮演的存取控制相整合，我們將擴充 X.509 憑證的內容，使它能包含使用者角色扮演的資訊。

ITU-T 在 1993 年所提出的 X.509 第二版中，公開金鑰證書包含了下列的欄位：版本(version)、序列編號(serial number)、簽章演算法識別碼(signature algorithm ID)、證書核發單位名稱(issuer name)、有效期間(validity period)、使用者(subject)、核發單位的唯一識別代碼(issuer unique identifier)、使用者的唯一識別代碼(subject unique identifier)、使用者的公開金鑰資訊(subject public-key information)，以及上述欄位的數位簽章等。

在 1994 年，ITU-T 提出了 X.509 的第三版。和第二版不同的地方在於增加了擴充欄位(extensions)，包括擴充欄位識別碼(extnID)、擴充欄位必要性值(critical value)、及擴充欄位值(extnValue)。此擴充欄位提供了更大的彈性，讓公開金鑰證書可以攜帶更多公開金鑰相關的資訊，例如使用者或核發單位的金鑰識別號碼(Identifier)、核發證書的政策、金鑰使用的限制、秘密金鑰的使用期間限制等等資訊。除了上述正式定義的擴充欄位外，還可以視需要定義私有擴充欄位(Private Extension)，我們可以將使用者在組織內角色扮演的 user profile 資訊，放在這個私有擴充欄位內，將角色扮演存取控制和 X.509 做一個完善的結合。

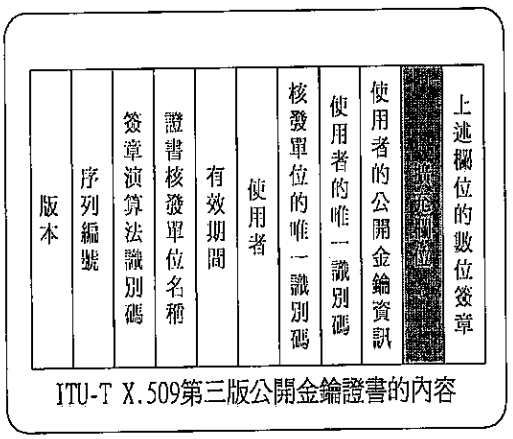

圖 5　ITU-T X.509 公開金鑰證書擴充欄位之應用

使用者儲存在私有擴充欄位的 user profile 資訊，可以是文字型式也可以是符號代碼，只要能表示該使用者擔任的角色即可。使用者的 user profile 和他的

公開金鑰值，同為此證書的主要內容，由證書核發單位對這兩樣資訊及相關的資料簽章，所以掌管證書核發的單位和資源存取授權的單位最好是同一個，或是可以密切配合，以方便 X.509 證書核發的作業。 由核發單位簽發的數位證書將儲存在使用者個人的智慧卡上，再交給使用者保管。

三、安全管理系統

有了角色扮演的存取控制機制，以及以 X.509 公開金鑰證書為基礎的使用者 user profile，我們就可以建構一個完整的 Internet/Intranet 安全管理系統。

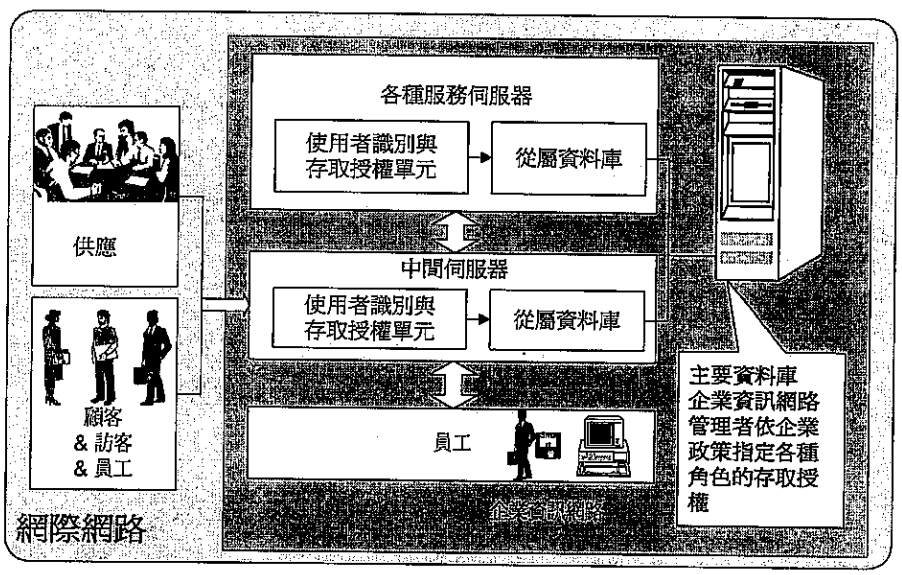

圖 6　Internet/Intranet 安全管理系統

如圖六所示的系統，主要包含 Internet 內部和來自 Intranet 的使用者、中間伺服器(Intermediate Server)、服務伺服器(Service Server)，以及主從式 RBAC 角色存取授權之資料庫。

Intranet 的使用者包括訪客(guests)、供應商(suppliers)、客戶(customers)及組織內部員工(employees)等，其中訪客、 供應商及客戶都是透過 Internet 進入 Intranet 的使用者。使用者若想進入 Intranet 取得各個伺服器的服務，須要先經過中間伺服器的身份識別程序，以確認進入 Intranet 使用者的身份。中間伺服器可以是一個全球資訊網伺服器(WWW Server)，通過這一識別程序的使用者，才可以得知 Intranet 中有那些提供服務的伺服器；而未通過這一階段檢驗的使

用者，則完全不知道 Intranet 有那些資源服務。

中間伺服器所做的身份識別程序，會要求使用者提供他個人的 X.509 公開金鑰證書。組織內部的員工，以及交易往來的供應商或客戶，因爲是屬於較固定的使用者族群，可以擁有組織所發給的智慧卡，所以可以通過這一層的身份識別。但是，對於一般來自於 Internet 上以瀏覽爲目的的訪客，因爲不一定擁有智慧卡及組織所核發的 X.509 證書，所以，只允許他得到最外層中間伺服器所公佈的資訊。爲了保護組織內部的資源，訪客通常不被允許進入 Intranet 中。

使用者通過了外層的中間伺服器的身份識別進入 Intranet 後，可以由此外層的伺服器提供的表列，得知企業內部還有那些伺服器。這時外層的伺服器可以依使用者的 X.509 證書上所記錄的使用者角色，決定使用者是否可以再進一步進入企業內部其它的伺服器。當使用者向內部提供服務的伺服器發出存取要求時，伺服器都會再對使用者進行身份識別和授權的檢查，以增加安全性。

爲了讓所有的伺服器能對使用者做存取授權的檢查，在伺服器端要儲存各種角色所允許的存取授權資料、 RBAC 的存取限制規則，以及 user profile 之撤銷或暫停使用等資訊。「角色：存取授權」的對應資料記錄了該角色對於各種資源的存取授權，而存取限制規則定義了使用者在扮演角色時的額外限制，這兩者的變動性低且對所有伺服器的重複性高。因此，在整個 Intranet 中可以利用 X.500 分散式資料庫的觀念，即由 Intranet 系統安全管理者管理一個主要(Master)資料庫，其中存放角色所對應的存取授權、被撤銷或暫停的 user profile ， RBAC 的存取限制規則等資料，並且將這些資料複製到其它的伺服器從屬(Slave)資料庫中，包括中間伺服器及服務伺服器的從屬資料庫，而各個伺服器可以再針對自身的需求對從屬資料庫的內容做進一步的修改。

四、使用者身份識別之程序

中間伺服器和服務伺服器對使用者進行的身份識別程序如下：

1. 使用者將含 user profile 的 X.509 憑證連同存取要求傳給伺服器。
2. 伺服器任選一個隨機亂數 r 做爲 nonce ，用憑證上的公開金鑰加密，傳回給使用者。
3. 使用者以私密金匙解密得到 r 後，將之簽章並傳回給伺服器。
4. 伺服器以公開金匙解密，並檢查 r 是否相同於步驟二所產生的 nonce。

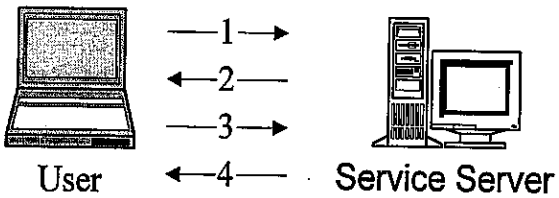

圖 7　使用者身份識別程序

在步驟 1 中，伺服器可以得到來自使用者的 X.509 證書及資源存取要求。由該證書，伺服器可以得到使用者的 user profile ，其內容爲使用者個人所能扮演角色之集合。雖然在 X.509 證書中有記錄使用者的識別名稱，但爲確認使用者確實爲證書的所有人，仍需進一步進行身份識別的動作。

步驟 2~4 的目的主要是確認客戶端使用者就是證書的所有人。爲識別使用者的身份，伺服器用證書的公開金匙將隨機變數 r 加密，伺服器若能夠在步驟 4 驗證傳回來的值是 r ，則伺服器有理由相信該使用者就是證書的所有人。這個識別的原理是藉由使用者是否能安全控制他的私密金匙，來識別他的身份。使用者的私密金匙和 X.509 證書一樣，都是存在使用者的智慧卡上，使用者要存取智慧卡上的資料，都要先輸入一個 PIN(Personal Identity Number)，藉由 PIN 可以爲使用者的私密金匙提供多一層的保障。

在上述的過程中，由伺服器選擇一隨機亂數，較由使用者選擇隨機變數的方式要來得好。隨機亂數若是由使用者選擇，則在伺服器上還要儲存使用者所選用的隨機亂數，以作爲檢查重播攻擊(replay attack)之用；但若由伺服器來選擇，則伺服器只要確定步驟 2 與 4 的亂數相同即可。因此，可以減少伺服器所需花費的儲存空間。

使用者若通過了身份識別的程序，伺服器可以相信客戶端使用者就是 X.509 公開金匙證書的所有人，因此建立了使用者與角色扮演存取控制 user profile 的關係。根據 user profile 所記錄的使用者所能扮演的角色，伺服器可以決定使用者的存取要求是否同意，或者是退回。

肆、分析與討論

傳統的電腦系統對資源的存取是採用「使用者：物件」存取控制矩陣的方

式，做爲安全管理的方法。在進行對使用者的存取授權檢查之前，使用者還要先通過身份的識別。若將這種方法應用到現代組織中，會遇到的缺點及本文所提出方法的改善如下表所示：

表一 本方法與傳統方法之比較

	傳統方法的缺點	本研究所提方法對傳統方法缺點之改善
1	使用者或資源物件數目有增減時，存取控制矩陣的更動會顯得麻煩且沒有效率。	以角色扮演做爲存取控制的方法，使得組織內每一個提供服務的伺服器的存取授權的管理對象是角色，而不是個別的使用者，所以可以簡化安全管理的問題。
2	使用者在不同的服務伺服器上都要通過身份識別，使用者需要記住他在每一個伺服器上的通行碼。除此之外，通行碼在網路上傳遞時，可能會被截聽。	我們以兩階段的身份識別方法來解決： (1)使用者需輸入個人的 PIN ，來取得個人智慧卡上的資料。 (2)以 X.509 公開金鑰證書，進行使用者與提供服務的伺服器之間的身份識別。雖然組織內可能有許多的伺服器，但使用者不需去記其個人在每一個伺服器的身份代碼及通行密碼，也不必擔心密碼被竊聽。
3	若組織內有若干個提供服務的伺服器，則每個伺服器都要儲存使用者身份識別與存取授權的資料，對系統管理而言是一負擔。	我們將使用者所能扮演角色的 user profile 包含在 X.509 證書內，並存放在智慧卡上。當使用者發出存取要求時，需將 X.509 證書送給伺服器， 伺服器可以同時進行身份識別與存取授權的檢查。組織內的每一個伺服器不需存放存取控制矩陣或是使用者身份識別的資料，因此可以簡化管理的工作。

針對身份識別和存取授權的方案， Claude Laferriere 和 Richard Charland (1993)提出四個評估的準則：安全度(Effectiveness), 受保護資源之最小單位(Granularity), 彈性(Flexibility), 績效(Performance)。對於本文所提出的方法，我們可以用上述準則來加以檢驗。

表二 本文提出方法之評估

評估標準	本文提出方法之評估
安全度 (Effectiveness)	每次使用者要求登入網路系統或是存取資源時，都要經過身份識別與存取授權檢查的程序，依 Harn 和 Lin 所述，身份識別與存取授權檢查兩種服務整合的方法，較分開的方法提供更多的安全。
受保護資源之最小單位 (Granularity)	本方法所保護的對象，大至整個 Intranet 伺服器資源資訊的保護，小至系統內部各種資源及服務，均對使用者進行身份識別與存取授權之檢查。
彈性 (Flexibility)	透過角色扮演存取授權之權利的授與和撤銷，使得各種系統資源或服務之加入或移除，或是使用者之新增均較傳統的方法容易且有彈性。

評估標準	本文提出方法之評估
績效(Performance)	以角色扮演作爲存取授權的基礎，各種角色的存取授權規則可由Intranet 管理者作集中式設定，可以簡化管理的問題。 此外， DCE Kerberos 的方法中，使用者向不同的伺服器要求服務時，都要先取得不同的通行票(Ticket)。本方法中，使用者只要有一張存放個人所扮演角色 user profile 之智慧卡即可。因此，就使用者取得服務的績效而言，優於 DCE Kerberos 的方法。

伍、結論

在本篇文章中，我們提出了一個可以施行於企業內部及企業交易往來對象的資源存取控制方法。此方法是以角色扮演爲基礎，所以較傳統的矩陣式存取控制適用於現代組織 Internet/Intranet 的安全管理。此外，我們將使用者個人角色扮演的資訊和 X.509 公開金鑰證書結合，並搭配智慧卡的使用，可以有效地整合身份識別與物件的存取授權。

本方法的優點是：(1)以角色扮演爲存取控制的基礎，使用者僅需記一組個人的識別碼和通行密碼，而各伺服器均以一致的方法來檢查使用者的存取要求，因此，可以簡化組織資源的存取管理。(2)擴充 X.509 公開金鑰證書以包含使用者個人角色扮演的資訊，並將之儲存在智慧卡上，可以提供較佳的身份識別管理。(3)整合身份識別與存取授權的安全管理方法，相較於分開獨立的功能模組，對於資源存取的保護，可以提供更多的安全性。

本方法的缺點是：(1)因爲 user profile 是存放在使用者端的智慧卡上，所以使用者角色扮演資訊之更新與撤除的管理，應制定一套類似公開金鑰證書之發放與徹銷的規則。(2)智慧卡使用的安全管理上，其資訊之保護是仰賴使用者輸入正確的 PIN 值，如果 PIN 值被他人取得，那麼對使用者進行的身份識別程序將無法判別真正的使用者身份。(3)公開金鑰證書的發放和使用者角色扮演之授權，分別是公開金鑰證書授權單位與組織安全管理者之職責，本方法之實行須賴此二單位之密切配合。

本文提出的方法，可以適用於有既定的職務指派安全管理政策的組織中，解決資源使用管理的問題。我們可以更進一步擴充此一理論基礎，討論其他的應用，例如，在包含許多組織的環境中，每個組織的職務指派政策不同時，要如何提供這些組織間使用者互惠的服務，也是值得繼續研究的課題。

參考文獻

程捷生，1997，Intranet 及 Internet 防火牆策略，台北：儒林。

蔡啓仁，1997，Challenges for building a financial public key infrastructure, 1997 資訊安全會議論文集：152-157。

羅景原、黃景彰、樊國楨，1997，「公開金鑰管理組織運作架構」，1997 資訊安全會議論文集：15-22。

Charles P. Pfleeger. 1989. ***Security in computing***, Prentice-Hall International, Inc.,Englewood Cliffs, New Jersey.

Claude Laferriere, Richard Charland. 1993. Authentication and authorization techniques in distributed systems. ***Proceedings. The institute of electrical and electronics engineers 1993 international carnahan conference on security technology: Security technology***, 164-170.

Don Tapscott. 1996. ***The digital economy***, McGraw-Hill Book Co., New York.

Dorothy E. Denning, Giovanni Maria Sacco. 1981. Timestamps in key distribution protocols. ***Communications of the ACM***, 24(8).

Ethan Sanderson, Karen A. Forcht. 1996. Information security in business environment. ***Information Management & Computer Security***, 4(1):32-37.

Gregory R. Doddrell. 1995. Information security and the Internet. ***Information Management & Computer Security***, 3(4):15-19.

Gregory R. Doddrell. 1995. Security environment reviews. ***Information Management & Computer Security***, 3(4): 3-14.

ITU-T SG/7 | ISO/IEC JTC1/SC21/WG4. 1990. ***ITU-T Recommendation X.509| ISO/IEC 9594-8, Information Technology-Open Systems Interconnection-The Directory : Authentication Framework.***

J.T. Kohl. 1991. The evolution of the Kerberos service. ***European conference proceedings***, 295-313.

Ken Lindup. 1996. The role of information security in corporate governance. ***Computers & Security***, 15:477-485.

L. Harn, H. -Y. Lin. 1992. Integration of user authentication and access control. ***IEE PROCEEDINGS-E***, 139(2).

Mellanie Hills. 1997. ***Intranet business strategies***, John Wiley & Sons, Inc.

National Institute of Standards and Technology. 1996. ***Role-Based Access Control (RBAC): Features and Motivations.*** (http://walts.ncsl.nist.gov/rbac/newpaper/rbac.html)

Open Software Foundation. 1993. ***OSF DCE application development guide***, Sec. 13.7 and Ch.42.

Ping Lin, Lin Lin. 1996. Security in enterprise networking: A quick tour. ***IEEE communication magazine***, 56-61.

Ravi Kalakota, Andrew B. Whinston. 1996. ***Frontiers of electronic commerce***, Addison-Wesley Publishing Company, Reading Massachusetts.

Ravi S. Sandhu, Edward J. Coyne, Hal L.Feinstein Charles E. Youman. 1996. Role-based access control models. ***IEEE computer***, 38-47.

Robert L. (Bob) Frank, CISSP. 1996. Security issues in the virtual corporation. ***Computers & Security***, 15 :471-476.

Roger M. Needham, Michael D. Schroeder. 1978. Using encryption for authentication in large networks of computers. ***Communications of the ACM***, 21(12).

RSA Laboratories. 1996. ***Answers to frequently asked questions about today's cryptography***, Version 3.0.

Ryan Bernard. 1996. ***The corporate Intranet***, John Wiley & Sons, Inc., New York.

S. H. von Solms and Isak VenderMerve. 1994. The management of computer security profiles using a role-oriented approach. ***Computers and Security***.

Terry Bernstein, Anish B. Bhimani, Eugene Schultz, Carol A. Siegel. 1996. ***Internet security for business***, John Wiley & Sons, Inc., New York.

Thornton A. May. 1996. Internet and Intranet: The faces of the wired economy. ***Information Management & Computer Security***, 4(5):3-6.

Trisha Gorman. 1997. ***Smart cards come to the Web—are you ready?***, NetscapeWorld. (http://www.netscapeworld.com/netscapeworld/nw-03-1997/nw-03-smartcard.html)

TrustedWeb. 1997.***TrustedWeb technical summary***. (http://www.trustedweb.com)