數位典藏系統之權限控管

張益嘉　　林金龍　　何建明

中央研究院

資訊科學研究所

{eiga,eddy,hoho}@iis.sinica.edu.tw

摘要

隨著網際網路(Internet)的蓬勃發展，以網頁為基礎(Web-based)的服務也越趨於多樣與完整。再者網際網路是屬於開放性的環境，亦即所有使用者都能夠在網際網路上獲取所需的資訊，但敏感或機密性的資料是不允許被任意的存取，因此便突顯權限管理的重要。然而目前的數位典藏環境大部份都是建構在網際網路之上，而數位典藏的內容更是研究人員的心血與成果，所以對於數位典藏系統操作的更是要嚴格管控。另外針對典藏內容的特性，其對於權限管控的要求可能要細分至單一筆典藏資料，因此本研究展示一個適用於目前數位典藏環境需求的權限管理架構與機制，在此權限管理架構中所採用的角色為基礎的執行權管控(Role-based Access Control，RBAC)，並且提供單一登入(Single Sign-On，SSO)以避免於不同數位典藏環境間多次的切換。

關鍵字：權限管控、RBAC、SSO

1.前言

目前數位典藏已經成為國家型的計畫 ，所以不管在人力或物力上都有相當的投入。所以如何確保研究者的研究成果不被隨意引用與存取，以成為相當重要的課題。再者一個數位典藏環境之中是由多人來完成典藏資料的著錄與維護，所以如何在不同的職務付予合適的職權，是數位典藏之權限控管必備的功能。再者由於特定的典藏資料具備有獨立與完整性，每筆典藏資料都可視為研究人員的研究報告，所以權限控管也必須要細分至每一筆。而且目前的數位典藏環境都是以 Web-based 為主流，每項典藏運作可能為數個網頁來完成，所以應將數個網頁視為同一群，然後再為其權限命名。所以本研究提出一個整合現今廣受討論的執行權管控機制 RBAC，以解決多使用者與多職務間的複雜關係，隨著數位典藏發展的越趨於完備，使用者便有可能會在不同的典藏環境作切換，為了提供使用者一致的使用經驗，架構之中也引入 SSO 的概念，以避免重複登入的不便。

2.文獻探討

2.1 著作權

數位化再加上網際網路的便利性，使得所有資訊皆可即時傳送到世界各角落，而所伴隨而來的法律問題是不可乎視的。由國家科學委員會之數位典藏計劃辦公室所規劃推動的「數位典藏國家型科技計劃」，其計劃目標與推動策略係承襲「數位博物館」、「國家典藏數位化」、「國際數位

圖書館」三個計劃的經驗，以國內主要的典藏機構之典藏為對象，做一系統的數位化典藏資料庫建置。而將書面或以其它型態保存之原始資料典籍，透過數位技術轉為電子文件或資料，再整合建立為整合性的電子資料庫系統。並將資料庫中的資訊劃歸為三個不同等級的數位化產品，即：典藏級、公共資訊級和電子商務級[7]。

(1) 典藏級是具有保密性的數位化產品，暫不對外公開。
(2) 公共資訊級則是完全免費。
(3) 電子商務級的是提供給加值業者的素材，而進行公開販賣。

我國對於資料庫建立之發展有迫切之需求，但基於學術資訊流通之考量且能方便地使用他人著作，所以只著重單篇著作的著作權問題，並未對具有原創性之資料庫進行著作權的保護，所以數位典藏資料庫的使用權限管控更顯重要[8]。

2.2 權限控管

簡單的說，權限控管就是針對資訊系統內的各項資源，區分出不同等級的價值和風險性，針對企業內的資訊系統使用者，區分出不同等級之使用權和可信賴性，對兩者的等級做適度的管理行為。另外身份鑑別(Authentication)、執行權管制(Access Control)與稽核(Audit)是確保資訊與系統安全的基礎[3]，因此接續將更深入探討每個層面。

1.身份鑑別(Authentication)

身份鑑別主要是建立一個獨特的特性(Identity)而有別於他人，而這個特性通常可為以下之一或數個。(1)某些只有使用者知道的，例如密碼。(2)某些是使用者擁有的，例如信用卡或智慧卡。(3)某些是使用者的生物特徵，例如指紋或聲紋等。目前最常被採用的是密碼式的身份鑑別，但密碼有可能會被盜取或破解，而生物特徵也有可能依時間而有所變化，所以比較好的組合是以使用者生物特徵為憑証，持此憑証與系統服務做相互加密認證。

2.執行權管制(Access Control)

執行權管制大致上可分為強制型的執行權管控(Mandatory Access Control，MAC)、隨意型的執行權管控(Discretionary Access Control，DAC)與角色為基礎的執行權管控(Role-based Access Control，RBAC)[1]。

(1).強制型的執行權管控(MAC)：MAC指的是由系統管理者統一規範安全政策與資源屬性，且強制實施，使用者無法自行更動，適用於高機密性的單位，例如國防單位。MAC又是以資訊的機密等級作為執行權管制的依據，因此又稱為以規則為基礎（Rule-based)的執行權管制。

(2).隨意型的執行權管控(DAC)：DAC是由使用者自訂系統操作權限與資源屬性。由於DAC是以個體(使用者)為單位作為執行權管控的識？，所以DAC又稱為以個體為基礎(Identity-based)的執行權管制。

(3). 角色為基礎的執行權管控

(Role-based Access Control，RBAC) RBAC 是由美國國家標準局(NIST)所提出，且是目前被廣泛討論的一種執行權管控。在 RBAC 中系統權限(Permission)並不像 DAC 是直接付予使用者，而是付予角色(Role)。在企業之中不同的職務就像不同的角色，依據職務上的需求而給予適當的權限，再指派使用者至角色上。然而一個使用者也有可能會同時被指派到多個角色上。而角色間是具有繼承的關係，所以角色與角色間會形成階層式(Role Hierachies)的結構關係。故在 RBAC 中可分為五個元素：使用者(User)、角色(Role)、權限(Permission)、會期(Session)與限制(Constraints) [2]，元素間的關係如圖 1 所示：

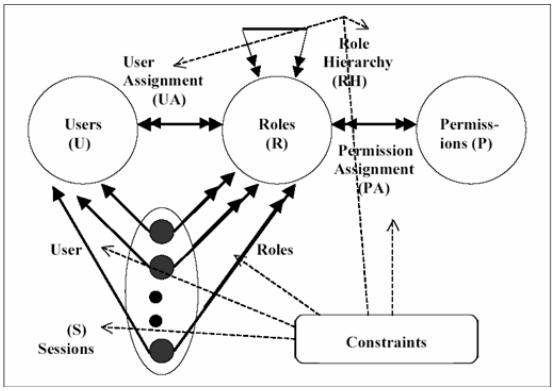

圖1：RBAC 模式[2]

(1)使用者：直接與系統有互動行為的人，更廣義來說也可是個軟體代理人(Software agent)、機器人(robot)，甚至是電腦網路(Networks of computers)。

(2)會期：是將一個使用者對映至數個可能的角色，而在這個會期的生命週期內所對映角色中所付予的權限都是有效的(activated)。

(3)角色：可視為企業中的職務，依職務性質的不同給予不同的權限。

(4)權限：執行權管控中對於單一或數個物件的特定操作。

(5)限制：規範其它元素的限制，例如階層關係、角色互斥關係等。

3.稽核(Audit)

稽核最主要是將使用者在系統之中所執行的操作完全的紀錄，以備未來當系統發生任何異常時，作為緊急應變的依據。所以稽核包括兩項工作，一是彙整稽核資料，另一是分析稽核資料以發現或診斷安全性上的漏洞。但稽核資料的分析通常是在系統安全被侵犯時才會去執行，這是被動的防護。現今，有些系統是採用即時性防護，即時分析稽核資料以監測系統異常的操作與存取，並且採取必要的措施。

2.3 單一登入(Single Sign-On)

當使用者在一個提供多個服務或系統的環? 之中，為了存取這些服務或系統，使用者就必須在切換的同時又要經過一道身份的認證，這樣將造成使用上的不便。所以SSO的概念便興起，使用者只要經過身份認證一次便可在不同的服務或系統上切換，如此可以帶來以下的效益[5]：

(1)減少多次身份認證所花的時間，相對的也減少身份認證出錯的可能性。

(2)避免使用者同時保有多個認證資訊而造成混亂。

(3)管理者可以集中管理使用者擁有的存取權並減少維護的時間。

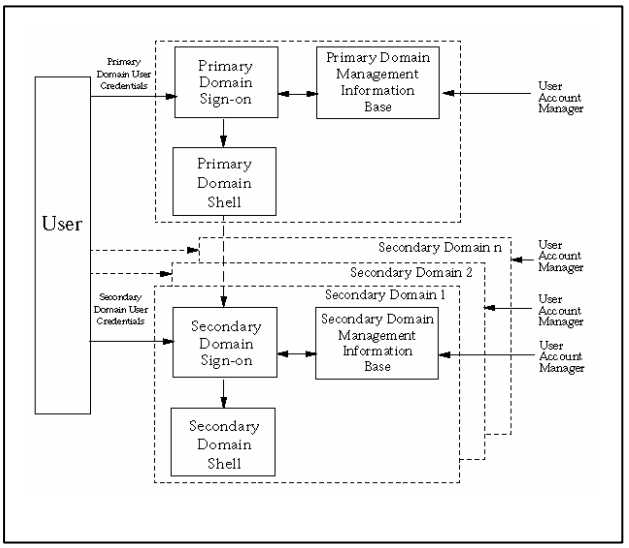

圖2：SSO意示圖[5]

2.4 執行權管控列表(Access control list，ACL)

ACL是一種用來說明使用者擁有那些權限(rights)的列表。通常為二維的表格一維是所有使用者，另一維是系統權限或物作相關操作。

2.5 其它權限控管系統

以下將以Passgo technologies的Webthority Secure Web Access Management與國內叡揚資訊的Scorpio權限控管系統加以探討與比較。

1.Webthority Secure Web Access Management：為Passgo所開發的web-based 權限控管系統，主要可以管控企業有價值的資料與減少管理異值性與分散性網站的成本，並透過信任的機制提供既有企業網路互通[4]。

2. Scorpio權限控管系統：為中文Web架構之Single Sign-on工具。提供系統管理者建立、維護與查詢組織相關資訊，並將此資訊與功能權限連結，尚且提供系統使用記錄的查詢與清除作業、使用者之使用狀況查詢，並以使用者→角色→權利→功能的組合構成權限控管之基本架構[6]。

三種權限控管系統比較表如下所示：

表1：比較表

	Webthority	Scorpio	數位典藏之權限控管
權限指定方式	RBAC	RBAC	RBAC
權限劃分方式	以整個網站為單位	單一功能操作	數個網頁為單位
權限細分至每一筆資料	否	否	是
提供 SSO	是	是	是
提供稽核	是	是	是

3．數位典藏系統之權限控管

權限管理系統主要是確保每一個數位典藏環境針對不同的使用者提供合適的服務，亦即希望數位典藏系統在適當的時間(right time)提供適當的資訊(right information)給適當的人(right people)。為了達到以上的理念，現今權限管控系統架構如圖3所示。

從圖3中可知，使用者透過Internet並採用SSL(Secure Sockets Layer)登入至任一個數位典藏系統，數位典藏系統再將使用者驗証資訊傳送至身份認証伺服器(Authentication Server)以進行使用者認証。若使用者通過身份認証便可登入典藏系統以進行系統操作。

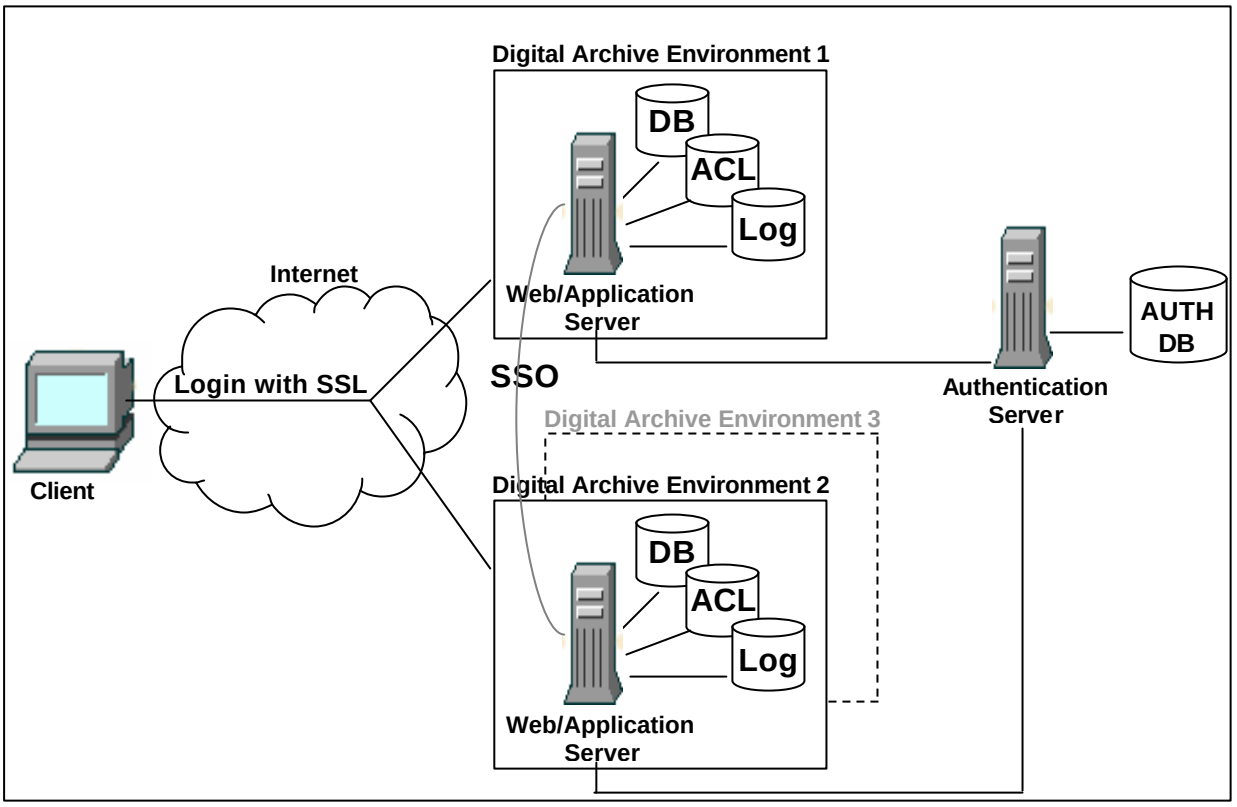

圖3：權限管控系統架構圖

為了避免使用者在多個數位典藏環境多次登入的費時，架構中也採用單一登入(SSO)的機制，使用者只要登入一次便可在不同的數位典藏環境做切換。由架構圖中可得知在每一個數位典藏環境中是由網站或應用系統伺服器(Web/Application Server)、數位典藏資料庫(DB)、執行權管控列表(ACL)與系統日誌(Log)所組成，以下將分述之：

(1) 網站或應用系統伺服器(Web/Application Server)：主要是提供數位典藏操作的系統平台。

(2) 數位典藏資料庫(DB)：主要是提供數位典藏資料儲存的資料庫。

(3) 執行權管控列表(ACL)：目前權限管理系統是採用RBAC的執行權管控，所以ACL主要是定義典藏系統權限與角色間的對應關係。在目前典藏系統最小權限的定義是以一個完整的操作功能為基準，然而在一個Web-based的系統環境之下，通常為數個網頁完成一個操作功能，所以這些網頁便被隸屬於同一個權限。圖4為網頁與權限隸屬關係圖，由圖中可知三個不同的操作功能擁有不同的網頁架構，但依其操作功能區分成三種權限。

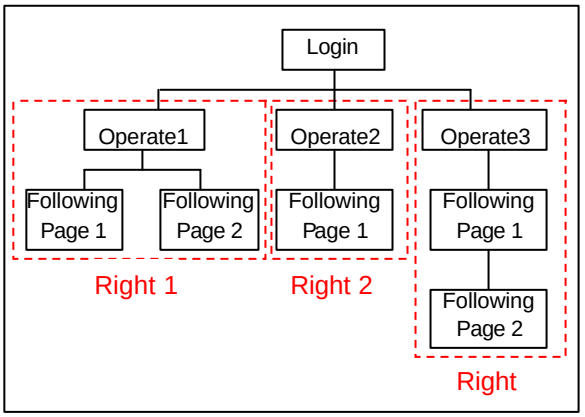

圖4：網頁與權限隸屬關係圖

(4) 系統日誌(Log)：主要是提供典藏系統稽核的機制。紀錄使用者何時

操作典藏系統及針對那一筆典藏資料所做的異動。而目前系統日誌內容如表2所示：

表2：系統日誌內容

Name	Type	Nullable	Comments
ID	numeric(5)	N	自動編號
RECORD_TYPE	varchar(50)	Y	記錄類型
RECORD_NO	varchar(50)	Y	記錄識別碼
LOG_DATE	Date	N	日期
PROCESS	varchar(50)	N	執行程序
USER_NAME	varchar(50)	N	使用者帳號
GROUP_NAME	varchar(50)	Y	群組名稱
REMARK	varchar(50)	Y	備註

權限管理系統與使用者的循序圖(Sequence diagram)如圖5所示，使用者由登入頁面進行登入的動作，緊接著對使用者驗證資訊進行驗證，若失敗則輸出錯誤訊息，若成功則取得使用者所擁有的權限，接著使用者進行典藏系統的操作，此時可能會發生三種狀況，(1)當使用者閒置過久，而使得session time out，將顯示錯誤訊息。(2) 若使用者所操作的功能是使用者未被核准，則顯示使用者並無此項操作的權限。(3) 使用者取得功能操作的執行結果。

權限管理系統資料庫設計如圖6所示，主要可分為 User_Info、Role_User、Role_Info、Function_Role 與 Function_Info 等五項，將分述如下：

(1) User_Info：主要是紀錄使用者基本資料，包括使用者帳號、密碼、姓名、性別等資料，這項資料將儲存於驗證資料庫以便進行身份驗證。
(2) Role_User：主要是紀錄使用者所屬的角色，以下四項資料將儲存於典藏環境中的ACL資料庫。
(3) Role_Info：主要是紀錄角色相關資料，包括角色名稱與描述。
(4) Function_Role：主要是紀錄角色所擁有的權限。
(5) Function_Info：主要是紀錄權限相關的資訊，包括權限名稱與描述。

在此權限管控架構之中，如何達到細分至每一筆資料，目前的做法是在典藏資料新增的同時，將建立者所屬的角色名稱與典藏資料一併儲存，而隸屬同一角色的使用者才可針對典藏資料進行維護。

4.結論

由於本研究是基於數位典藏環境對權限控管的需求而設計的架構，而架構之中也導入現今廣被採用的 RBAC 與 SSO 等概念。而且本研究所提出的權限控管架構大致上已經落實在目前已開發或開發中的數位典藏系統，雖然目前權限控管原則上已經能夠符合數位典藏環境上的需求，但為了使得權限控管機制更加完備，未來還是須要持續進行改善，不管是在效能或安全性上都可以再加以擴充。

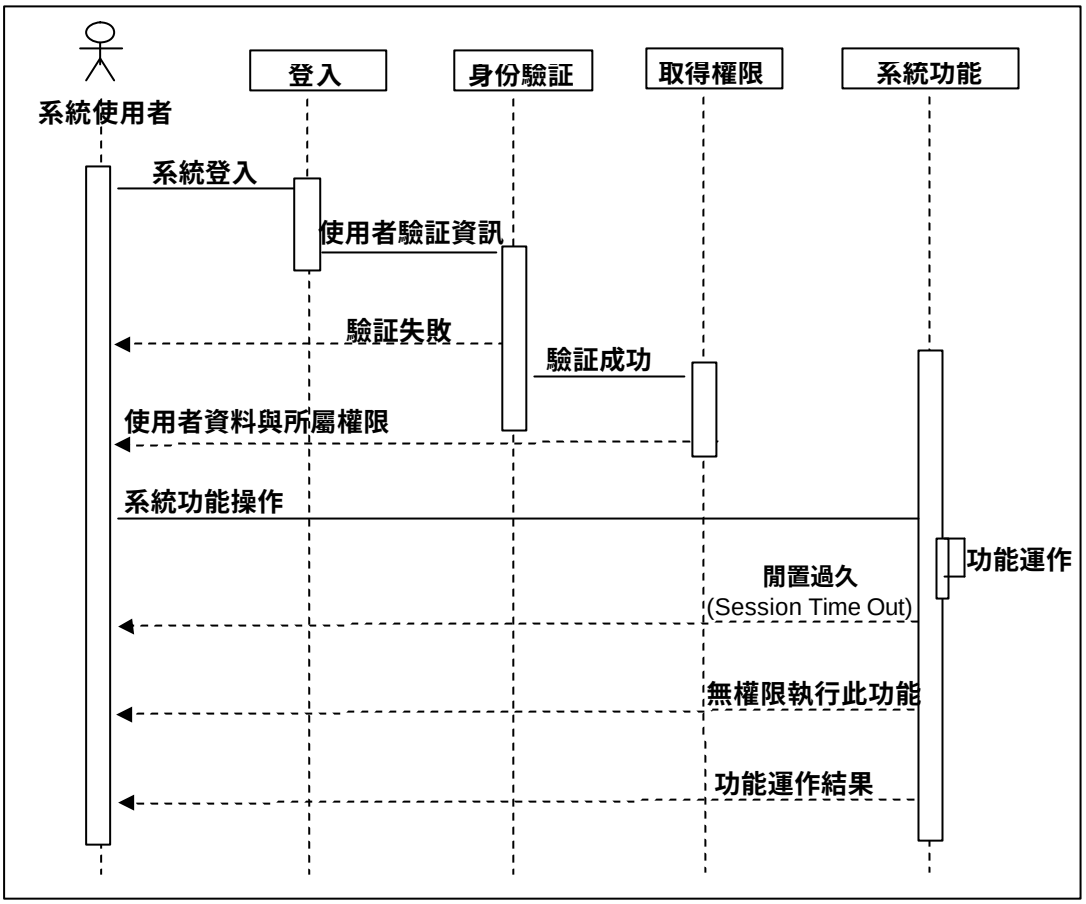

圖5：權限管理系統循序圖

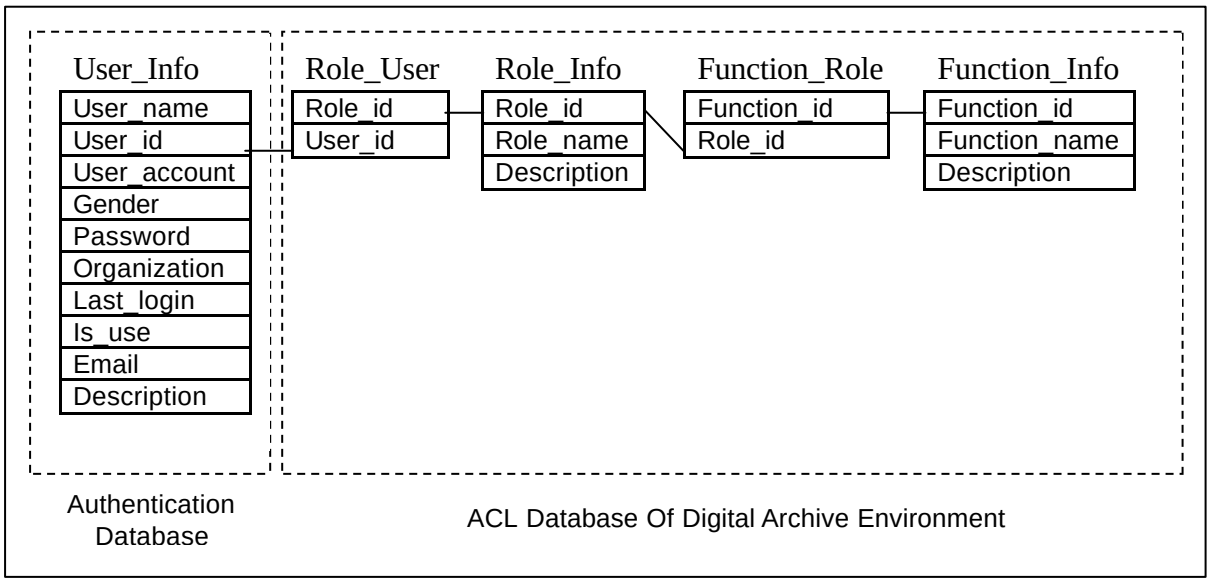

圖6：權限管理系統資料庫設計

參考文獻

[1]. 黃景彰，使用 XML 設計執行權管制資訊流，國立交通大學資訊管理研究所未出版碩士論文，2000。

[2]. Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman,"Role-Based Access Control Models," IEEE Computer, Volume 29, Number 2, February 1996.

[3]. Ravi Sandhu and Pierangela Samarati, "Authentication, Access Control and Audit," ACM Computing Surveys, 50th anniversary commemorative issue, Volume 28, Number 1, March 1996.

[4]. Passgo Technologies - Webthority Secure Web Access Management，http://www.passgo.com/products/webthority/index.htm

[5]. The Open Group, http://www.opengroup.org/security/sso/sso_intro.htm

[6]. 叡揚資訊－Scorpio 權限控管系統，http://www.gss.com.tw/product/Scorpio.htm

[7]. 行政院立法委員質詢答復系統-建置電子線上資料庫而涉及的著作權保護問題，http://210.69.7.199/qa/300000000s5222000069.htm

[8]. 數位時代著作權法律問題，http://nt1.moeaipo.gov.tw/ipo/月刊/9004/03-數位時代著作權法律問題(90-4).htm