視覺化權限管理模型實作之研究

陳儷穎，謝文恭
文化大學資訊管理研究所

摘 要

本研究以 partial order 表示資訊資源與存取權限，並繪製存取控制權限關係圖，以幫助資訊管理人員有效控管資訊資源存取。良好的圖形介面，是簡化資訊安全控管的利器。目前各種應用系統提供的存取控制功能，尚無完整友善的圖形介面，本研究將針對此一缺失，提出更友善的另類圖形介面，並以實作之方式展現，使資源存取控制的管理簡化。

關鍵字：存取控制、使用者介面、資源管理。

The Study of Building a Visual Access Control Model

Li-Ying Chen , Wen-Gong Shieh
Chinese Culture University

ABSTRACT

We present information resources and their access control in partial orders and diagrams for easy and effective access control. A good graphic interface is a powerful tool for simplifying information management. However, in current application systems, integrated and user-friendly graphic interfaces are not provided for access control. Therefore, for the lack of such interfaces, we create a visual access control model. We also demonstrate our idea of simplifying access control management through a simple prototype.

Keywords: Access Control, User Interface, Resource Management.

壹、前言

目前應用系統存取控制工具，大多以視窗系統爲基礎，而實際的操作仍爲表格式的介面，鮮少有讓管理者一目了然就清楚知道資源存取控制的情形。其介面通常顯示兩個表格，分別列出人員與權限，當管理者欲授予權限時，必須逐列加入，此方法不能直接表示人員、資源與權限之間的關係，無法提供管理者一個具有整體權限設定架構的友善圖形介面。

本研究的圖形介面存取控制，主要以二維向量空間來表示，如圖 1 是一個簡單的圖形介面實例，圖中虛線交叉點（座標 20,12）之總醫師（角色，以三角形表示）有三項工作權限（以圓形表示），即交叉點左下角矩形區域內之三項工作權限：住院醫囑、手術室管理及醫師排班。座標大小即決定權限大小，只要透過滑鼠移動圖中角色與工作權限之座標，即可改變角色所擁有之工作權限。

過去文獻中有幾種關於人員、資源與權限等元件 (object) 的表達方式，早期使用 access matrix 來表示 (Graham & Denning 1972)，此種表示方法主要缺點是無法直接表達各個 object 之間的關係；另外有以 partial order 來表示 object 之間的關係，甚至更複雜到使 partial order 形成一個 Lattice，例如 Lattice-based access control model 即使用 Lattice 來探討存取控制 (Sandhu 1993)。

Partial order 的應用，使得存取權限的表達，得以 Hasse diagram 的方式圖示化，而 partial order 維度的理論，則進一步提供了透過編碼方式，將 partial order 對應到三度空間視覺領域的可能性。例如，使用 N-Grid model 應用於群組授權的控制模式 (Shieh et. al. 1990)，即是將 partial order 之 Hasse diagram 座標化，該座標即隱含有可圖形化的介面。

然而將 partial order 之 Hasse diagram 座標化，在視覺上仍有問題存在，可能會因爲座標維度太高，即 partial order 維度太高，而無法在三度空間視覺領域中顯示出來。

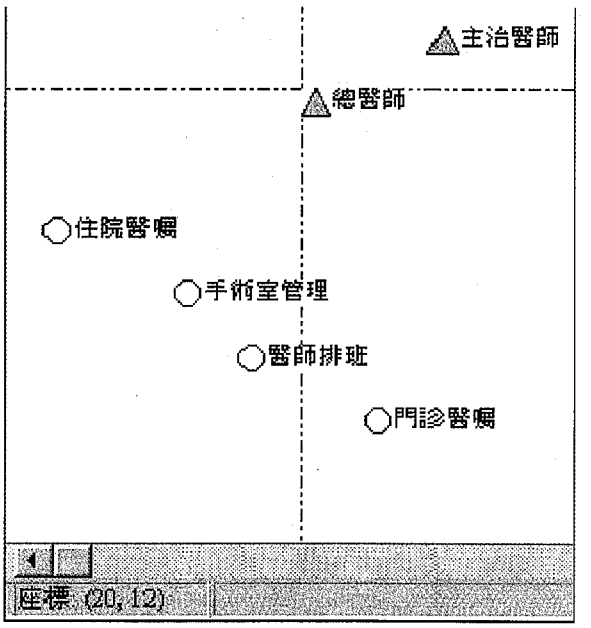

圖1：角色與工作權限向量圖形

本研究以 partial order 表示資訊資源與存取權限，並以例外表示方法展現超過二維以上 partial order 圖形，讓圖形介面存取控制模型得以在二維向量空間中繪製出來，可以清楚展現出人員、資源與權限的關係，並配合使用權限授予時的限制條件，幫助資訊管理人員管理資源存取控制。

貳、創新構想

視窗系統的出現，不僅僅代表使用者介面的改變，更顛覆了傳統人類使用電腦的習慣，以較符合實際環境的方式，並依循著我們的思考模式，建構出 "what you see is what youget" 的人性化介面。同樣的，本研究也秉持著相同的理念，以異於傳統的作法，提出創新的圖形化介面，應用在存取控制的管理上，此介面不但改變原有的權限管理操作習慣，更在視覺畫面、管理者認知以及系統內部運作等方面，有截然不同的重新詮譯與定義。

一、視覺畫面

㈠向量空間介面，主要的權限管理畫面爲視覺化的向量空間。

㈡物件化，各別的角色與權限物件化，放置在向量空間中，可利用滑鼠任意移動。

二、管理者認知

㈠座標相對大小即決定權限大小。

㈡滑鼠拖拉各物件改變座標相對位置即代表權限的改變。

三、系統內部運作

㈠系統內部只存放著各角色與權限的座標。

㈡內含座標自動計算之演算法。

詳細內容請參考本文第伍節之實作模型。

參、文獻探討

一、partial order及其維度理論(Hirugachi 1951)

若 R 是一個集合 S 上之 partial order，則 S 必須是一個非空的集合，且內部各元素 (element) 間具有反身性 (reflexive)、遞移性 (transitive)、不對稱性 (anti-symmetric) 的關係。例如 S={1,2,3,4,6,9}，各元素之整除關係 (relationship) 爲 D，D 即爲 S 上的一個 partial order。即 D={(m,n) | m,n ∈ S,m 整除 n}，對所有 m,n ∈ S，如果 m 整除 n，則之關係存在 D 中。一個 partial order 可藉由無向圖形表示，稱爲 Hasse diagram，雖然 Hasse diagram 是無向圖，但其線段隱含方向性。如圖 2 是一個 partial order D 的 Hasse diagram，如果存在 (m,n) 則 Hasse diagram 存在有一路徑是從 m 點往上至 n 點。

若對所有 m,n ∈ S，partial order R 中皆存在 (m,n) 或 (n,m)，則 R 是一個 S 上之 total order。partial order 可應用

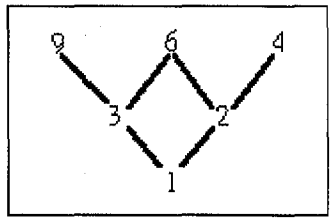

圖2：partial order D
資料來源：(shieh et. al., 1990)

topological sort 轉換爲若干個 total order，例如兩個由 partial order D 轉換出來的 total order T1 與 T2 如下：

T1=(1,3,9,2,6,4)

T2=(1,2,4,3,6,9)

請注意 T1=(1,3,9,2,6,4)，代表 T1 中 (1,3)，(3,9)，(9,2)，... 等等之關係存在，且其 Hasse diagram 成爲一條垂直線。

partial order 可使用 realizer 重新建構出來，realizer 被定義爲「partial order 轉換出來的 total order 之集合，且這些 total order 經由交集的運算產生原來的 partial order」。

partial order 之維度意義如下，包含 total order 個數最少的 realizer，其 total order 個數即爲此 partial order 之維度。例如 {T1,T2} 恰爲 partial order D 之 realizer，且其 total order 個數只有 2，亦爲最小，故 D 是二維的 partial order。

二、partial order觀念的存取控制

有學者提出 N-Tree 二維度的 partial order 來表示群組授權 (Sandhu 1988)，如圖 3。圖中的 A、B、C、D 代表各個群組，當授予某些資源的權限給各個群組時，具有以下的特性：

㈠ separation，授予某些資源的權限給群組 B 時，群組 C 並不同時擁有此權限，也就是群組 B 與群組 C 之權限無法比較，符合不對稱性（anti-symmetric）的關係。

㈡ sharing，授予某些資源的權限給群組 D 時，群組 A、B、C 也同樣的可以擁有此權限。

㈢ oversight，不論授予某些資源的權限給群組 B、C 或 D 時，群組 A 也同樣的可以擁有此權限，符合遞移性（transitive）。

利用 partial order 觀念所設計的存取控制模型，主要的優點是可以表示 object 與 object 之間的關係，並以 Hasse diagram 表示，但 object 的數量越多時，其關係越複雜。

三、N-Grid存取控制模型

An N-grid Model for Group Authorization (Shieh et. al. 1990)，主要觀念是將 n 維 partial order 對應到 n-dimensional 向量空間來表現子群組的關係，換言之所有的 object 都可以對應至向量空間中的某一個點。以向量空間座標點來比較權限的大小，在權限檢查運算確實提升效率。特別是當維度在三維之內時，可以將 partial order 對應到三度空間視覺領域，用以提供圖形化之介面。

不過所謂的 n-dimensional 向量空間是沒有限制其維度，當維度超過三維，圖形會變得很複雜，在觀念上必須以抽象圖形概念來想像。

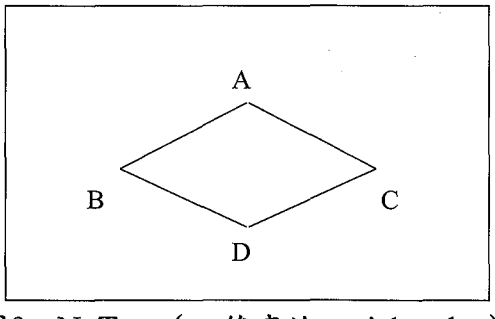

圖3：N-Tree（二維度的partial order）
資料來源：(Sandhu 1988)

四、Role-based存取控制模型

爲了減化權限分配的複雜度，有學者提出 Role-based 存取控制模型的觀念(Sandhu & Coyne 1996)，將各個資源所組成的子集合加上特別的角色名稱，以表示某一角色所擁有的資源權限，而角色代表組織或企業中的某一個職務名稱或工作名稱，再給予人員各個角色以指派職務，藉此也可達到當人員指派新職務時，更動最少的權限設定，只要變換人員的角色即可，這是 role-based 存取控制模型最大的優點之一。

肆、圖形表示法則

一、Hasse diagram

以 Hasse diagram 來表示 partial order 中的角色與工作權限之間的關係如圖 4 。

㈠三角形，代表角色。

㈡圓形，代表工作權限。

㈢箭頭，代表各元件之間的關係。

㈣權限關係，箭頭起點的角色擁有其終點所指的工作權限，或其所指的角色擁有之工作權限，例如總醫師除了擁有醫師排班這個工作權限之外，還擁有專科醫師與住院醫師所擁有的工作權限（即手術室管理與住院醫囑）。又例如主治醫師則擁有圖形中所有的工作權限。

二、向量圖形

以向量圖形表示 partial order 中的角色與工作權限之間的關係如圖 5 ，圖中爲兩個座標軸的二維向量圖形，十字虛線爲輔助視覺效果的作用，代表角色的座標對應至兩個座標軸與原點所形成的一個矩形區域，在此區域中所有的工作權限爲該角色所擁有，所以在向量圖形中要表示角色與工作權限之間的關係，必須考慮到每一個角色與工作權限所在的位置，因爲其座標的大小直接影響到它們之間的關係。

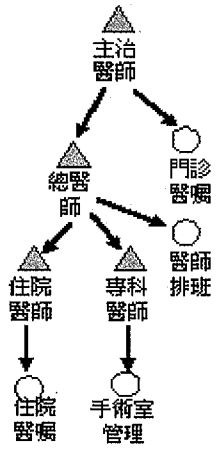

圖4：角色與工作權限Hasse diagram

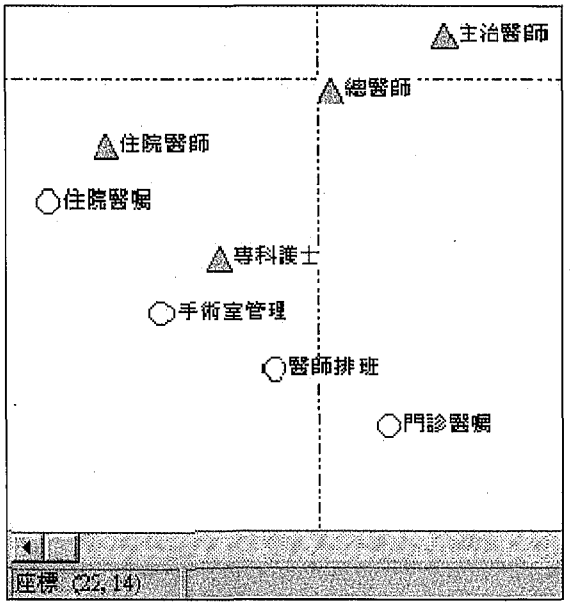

圖5：角色與工作權限向量圖形

以向量圖形表示 partial order(圖 5)，會比 Hasse diagram 表示來得清楚 (圖 4)。Hasse diagram 可以隨意的在一個平面上畫出，因爲它容許箭頭在繪製時交叉，也不必特別考慮或限定每一個角色與工作權限擺放的位置，所以當圖形較爲複雜的時候，較難看出某一角色擁有的所有工作權限。

三、向量圖形座標計算

本研究提供圖形產生器自動繪製圖形，管理者只要輸入像圖 4 的 Hasse diagram 中，角色與工作權限之間的關係，系統自動產生如圖 5 的向量圖形，每一個角色與工作權限有相對應的座標，並繪製出圖形，其座標演算法則已有相關的文獻探討，主要有兩種解決方法：

㈠ *Total Order 搜尋法 (Shieh et. al. 1990)*

透過 partial order 之維度理論，以地毯式尋找座標，任何 Hasse diagram 均可找到相對應的座標 (不限維度)，但缺點是較耗時。

㈡先深搜尋法 (*Sandhu 1988*)

透過執行兩次圖形理論的先深搜尋演算法尋找座標 (限二維)，計算速度較 total order 搜尋法快，但只適用於 Hasse diagram 爲 rooted tree(二維) 的情況。

四、向量圖形例外表示法

當 partial order 對應至向量空間是三維以上圖形時，本研究視爲例外，採用角色負向工作權限的例外表示法來解決，主要是分析前述先深搜尋法產生的二維座標，將所有依該座標尚無法表達全部工作權限的角色，同時放大其座標，以確保所有角色擁有足夠 (甚至多餘) 的工作權限，再將角色不應該擁有的多餘工作權限，記錄在角色負向工作權限中，所以每一個角色均存在有各自的負向工作權限，而其實際擁有的工作權限，也必須扣除負向工作權限。

五、限制條件於向量圖形中之意義

本研究之存取控制條件包含 (1) 使用者扮演某一角色之最大人數限制與 (2) 互斥角色，前者爲角色中的一個數值屬性，用來限制可扮演此角色之使用者最大人數，後者在下段文中詳細說明。

互斥角色爲一組任何使用者不得同時扮演之角色，互斥角可作爲權限授予時的

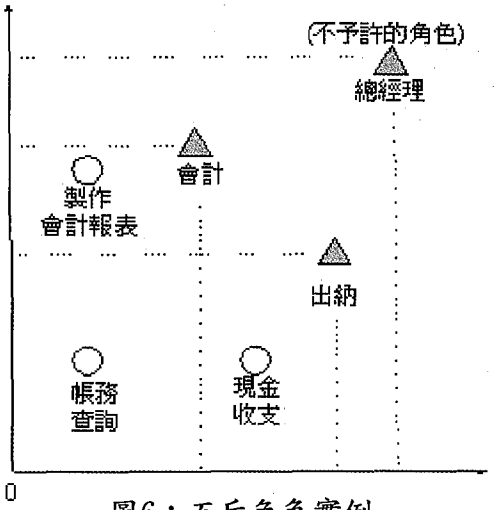

圖6：互斥角色實例

限制條件，例如某公司規定會計與出納工作不得由同一人擔任，則會計與出納爲互斥角色，他們擁有之工作權限必存在差異，爲滿足此種限制條件的要求，角色的座標圖形必須符合下列幾種條件：

㈠任兩角色若爲互斥的，其中一方所擁有的工作權限必須不被另一方所完全包含，如圖 6 中之會計與出納。

㈡不予許有任一角色同時包含互斥角色，也就是任一角色的座標不可同時大於互斥角色，如圖 6 中的總經理是不被予許的。

㈢互斥角色所擁有的工作權限之異動，不得違反前述不被另一方所完全包含之條件，如圖 6 中若將現金收支或製作會計報表之工作權限刪除，則會計與出納不再被視爲互斥角色。

以上是互斥角色在圖形觀念上的意義，若以實作的角度來考量，則有幾項操作介面上的關鍵點必須檢驗互斥角色的完整性：

㈠指定互斥角色或異動互斥角色時：檢驗互斥角色是否符合前述三項圖形狀況，檢驗目前使用者並未同時擁有互斥角色。

㈡授予使用者角色時：不予許使用者同時扮演互斥角色。

㈢新增或異動角色時：新的角色座標不可同時大於互斥角色。

㈣異動工作權限時：不予許異動後，互斥角色之權限有包含之情形。

伍、實作模型

一、模型概念

此模型主要目的是要將資源權限的分配情形展現在向量圖形上，讓管理者可以清楚的看出目前組織內部資源存取控制的狀況，爲了避免使展現出來的向量圖形太複雜，必須使用抽象概念的元件來簡化圖形，主要包含以下三個元件：

㈠人員，代表個人的基本元件。

㈡角色，代表組織中某一個職務的名稱。

㈢工作權限，代表組織中各個工作名稱，再針對各個工作權限定義可使用的應用程式或檔案等。

進一步說明上述三個元件之間的關係，哪些部分應該展現在向量圖形中，其基本概念如圖 7，詳細說明如下：

㈠向量圖形介面，向量圖形介面主要的元件有角色與工作權限，此介面以向量座標的方式，提供管理者管理角色所應有的工作權限，爲了簡化圖形與避免經常性的工作權限異動，人員則不在向量圖形中展現。

㈡人員與角色之間，所有人員並不直接授予其特定的工作權限，必須透過角色做爲橋樑，只授予人員應扮演的角色。

㈢角色與工作權限之間，管理者必須

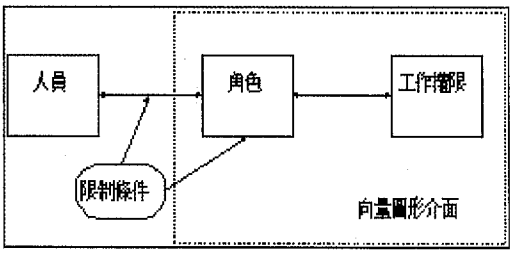

圖7：圖形介面存取控制模型概念圖

事先定好組織或企業內部所有的角色與所有的工作權限，再授予角色該擁有之工作權限，也就是說角色爲各個工作權限所形成的子集合。

㈣限制條件，人員與角色的限制條件，包含某一角色授予給人員時的最大人數限制，與互斥角色的限制。

二、系統功能

根據上述的概念圖，說明了本研究之權限管理模型主要的核心在於向量圖形介面上，且要有一個幫助管理者使用此介面之輔助工具，故由此模型實作出的權限管理工具必須提供以下功能：

㈠存取控制模型以向量空間圖示化。

㈡一目了然的展現存取控制關係圖形。

㈢提供管理人員自行繪製圖形。

㈣管理人員輸入相關資料後，由管理工具自動產生圖形。

㈤修改權限時（改變座標），可直接拖拉圖形中的各元件。

㈥提供各種限制條件的建立與檢驗

㈦提供各種查詢存取控制權限的功能。

㈧提供驗證存取控制權限的功能。

三、系統架構

以實作的角度而言，本研究之權限管理工具系統架構如圖 8 ，詳細說明如下：

㈠存取控制資料庫：儲存各個元件的基本屬性、權限授予規則與限制。

㈡存取控制管理工具，提供基本的權限管理功能，包含元件屬性與權限的異動和查詢，並將異動的資料儲存於存取控制資料庫中。

㈢向量圖形介面，爲內部管理工具與管理者之間的橋樑介面，有關權限的異動與查詢均透過此操作介面，管理者可以使用此介面繪製所需的圖形。

㈣權限規則截取，提供傳統表列式的權限輸入介面，並將資料儲存於存取控制資料庫中。

㈤圖形產生器，內含一些演算方法，將管理者輸入的資料轉換爲向量圖形。

陸、向量圖形操作介面

圖 9 爲本系統提供給管理者基本的操作介面，管理者主要都是在這個介面上操作角色與工作權限的關係，由於此模擬系統之操作介面有別於以往傳統的方式，所以當管理者移動圖形上任何角色或工作權限時，必須維持下列三者的一致性。

㈠系統內部資料儲存的意義

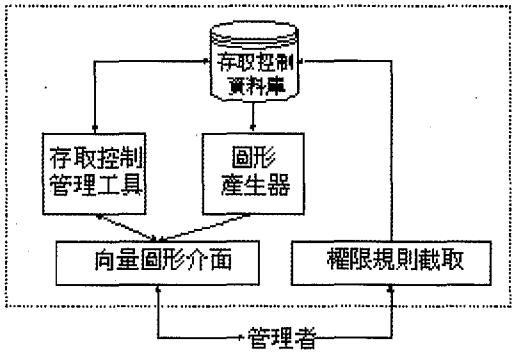

圖8：圖形介面存取控制實作架構圖

㈡視覺表達的意義
㈢管理者認知的意義

一、負向工作權限

㈠系統部資料儲存的意義

系統內部記錄各角色必須扣除的工作權限爲負向工作權限，且各角色只能記錄比其座標小之負向工作權限。

㈡視覺表達的意義

在視覺表達上爲圖 9 中字體顏色較淡之工作權限

㈢管理者認知的意義

當管理者在圖形中看到字體較淡之工作權限時，應清楚知道這些工作權限爲某角色之負向工作權限。

二、角色實際擁有的工作權限

點選任一個角色圖形使其出現黃底字（如圖 9 中的 role3 ），實際擁有的工作權限爲角色至原點（畫面左下角）圍成的矩形區域中所有工作權限。

㈠系統內部資料儲存的意義

各角色與工作權限僅儲存座標值，至於負向工作權限的處理上，系統內部仍有記錄此角色的負向工作權限。

㈡視覺表達的意義

在視覺表達上則將此角色的負向工作權限隱藏，並於右上角的小視窗中提示此角色的負向工作權限。

㈢管理者認知的意義

管理者可透過輔助線清楚看到此角色實際擁有的工作權限，而不被負向工作權限所混淆。

三、增加角色所擁有的工作權限

㈠移動角色

將角色拖拉 (drag and drop) 使其座標放大，由輔助線幫助管理者看出是否包含應有的工作權限。

1. 系統內部資料儲存的意義：先檢查是否違反已定義的互斥角色原則，並由管理者確認移動後，系統內部記錄爲修改角色的座標值。
2. 視覺表達的意義：改變角色位置，同時隱藏此角色之負向工作權限
3. 管理者認知的意義：管理者必須體認到角色位置的移動，即代表權限的更動。

㈡移動工作權限

較不建議使用此種方法，因爲工作權限的移動可能影響其他角色的權限。將工作權限拖拉 (drag and drop) 使其座標縮小，由輔助線幫助管理者看出是否包含在該角色中。

1. 系統內部資料儲存的意義：先檢查是否違反已定義的互斥角色原則，並由管理者確認移動後，系統內部記錄爲修改工作權限的座標值。
2. 視覺表達的意義：改變工作權限位置。
3. 管理者認知的意義：管理者必須體認到工作權限位置的移動，即代表權限的更動。

㈢移除角色與工作權限之負向關係

欲增加之工作權限爲該角色之負向工作權限時使用此方法，選擇功能表列中的角色、編輯負向工作權限，移除該角色的負向工作權限。

1. 系統內部資料儲存的意義：刪除該角色與工作權限之負向關係記錄。

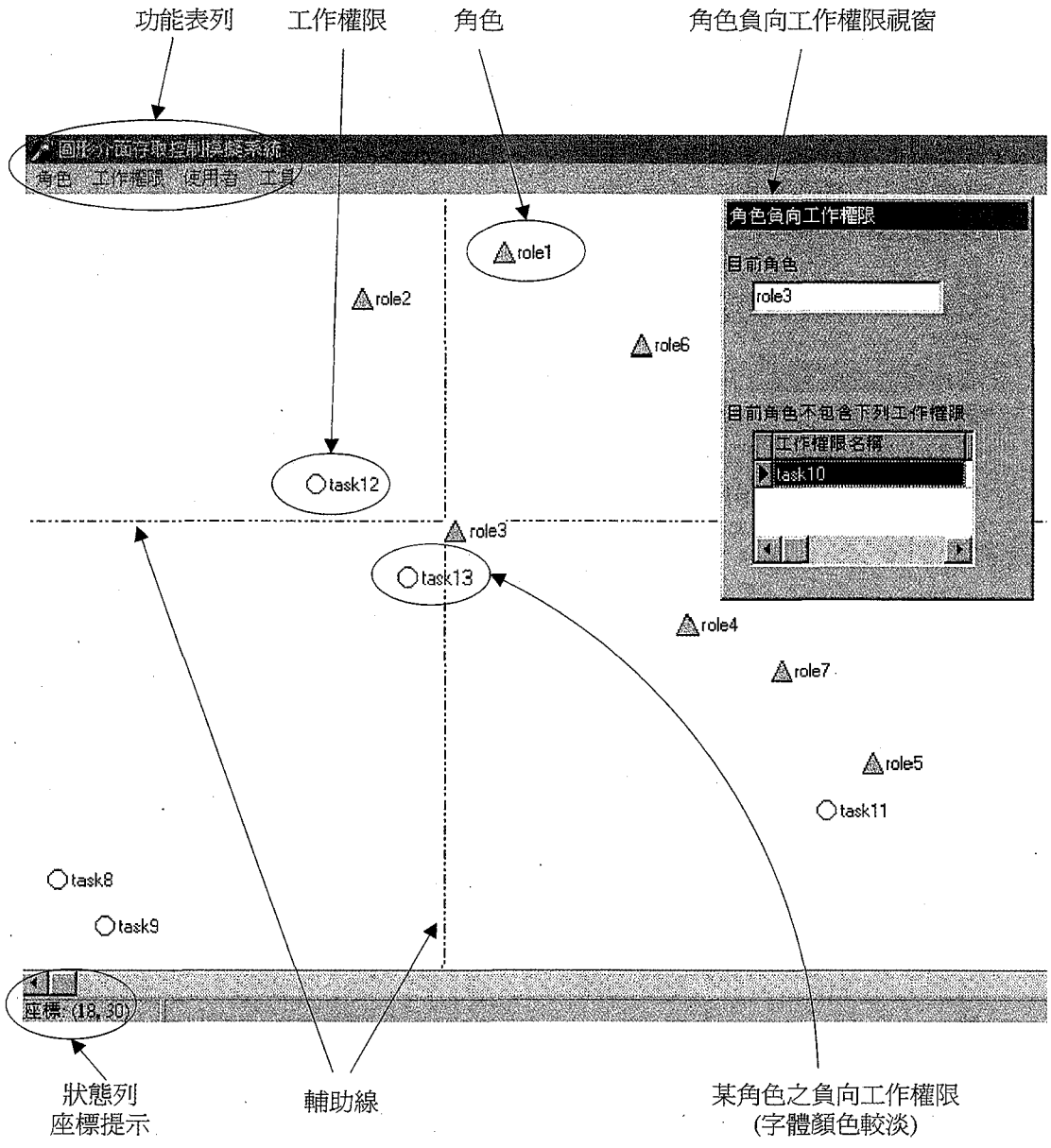

圖9：模擬系統操作介面

2. 視覺表達的意義：若此工作權限不是其他任一角色之負向工作權限，則取消文字顏色變淡使其正常化。
3. 管理者認知的意義：管理者可從圖形中得知該角色已擁有此工作權限。

四、移除角色所擁有的工作權限

㈠移動角色

將角色拖拉 (drag and drop) 使其座標縮小，由輔助線幫助管理者看出是否不包含應移除的工作權限。系統內部記錄、

視覺表達與管理者的認知如同第四點中的移動角色所述，唯一有差異的是當角色移動後，若其本身的負向工作權限已不再被該角色所包含時，則下列三者的意義爲：

1. 系統內部資料儲存的意義：刪除該角色與工作權限之負向關係記錄。
2. 視覺表達的意義：若此工作權限不是其他任一角色之負向工作權限，視覺上取消文字顏色變淡使其正常化。
3. 管理者認知的意義：管理者應體認到角色未擁有此工作權限，是因爲工作權限的座標比角色的座標大的原故，而非負向工作權限的關係。

㈡移動工作權限

較不建議使用此種方法，因爲工作權限的移動可能影響其他角色的權限。將工作權限拖拉 (drag and drop) 使其座標放大，由輔助線幫助管理者看出是否不包含在該角色中。統內部記錄、視覺表達與管理者的認知如同第三點中的移動工作權限所述，唯一有差異的是當移動的工作權限爲該角色之負向工作權限時，則下列三者的意義爲：

1. 系統內部資料儲存的意義：將該角色與工作權限之負向關係記錄刪除。
2. 視覺表達的意義：若此工作權限不是其他任一角色之負向工作權限，視覺表達上必須取消文字顏色變淡使其正常化。
3. 管理者認知的意義：管理者應體認到角色未擁有此工作權限，是因爲工作權限的座標比角色的座標大的原故，而非負向工作權限的關係。

㈢加入角色與工作權限之負向關係

選擇功能表列中的角色、編輯負向工作權限，加入該角色的負向工作權限。

1. 系統內部資料儲存的意義：增加該角色與工作權限之負向關係記錄。
2. 視覺表達的意義：將工作權限之文字顏色屬性變淡，又因目前已點選該角色，所以此工作權限不顯示在畫面上。
3. 管理者認知的意義：管理者可從圖形中得知該角色已不再擁有此工作權限。

五、操作介面實例

㈠實例一（二維的 *partial order*）

圖 10 是二維的向量圖形，不需要使用負向工作權限即可完全表達角色之權限，圖中所點選的角色爲總醫師，透過十字虛線輔助視覺效果，代表總醫師擁有的工作權限，爲其座標至原點之左下方所圍成之矩形區域中所有的工作權限，分別爲住院醫囑、手術室管理、醫師排班。

㈡實例二（三維的 *partial order*）

圖 11 是以醫療系統爲例的三維 partial order 圖形，角色包含護理長、住院醫師、書記組長，護理長與住院醫師是負責醫療工作，書記組長是負責行政工作，以下是使用系統的自動繪圖精靈將角色與工作權限產生向量圖形的步驟：

1. 管理者輸入所有的角色。
2. 管理者輸入所有的工作權限。
3. 管理者輸入角色與角色之間的直接從屬關係，或輸入角色與工作權限之間的直接從屬關係。
4. 系統自動產生向量圖形，如圖 12。
5. 系統自動產生角色負向工作權限，代表該角色必須扣除的工作權限。

由於三維 partial order 無法直接表示在二維向量圖形上，所以使用角色負向工作權限之方式來表達。但以一般環境而

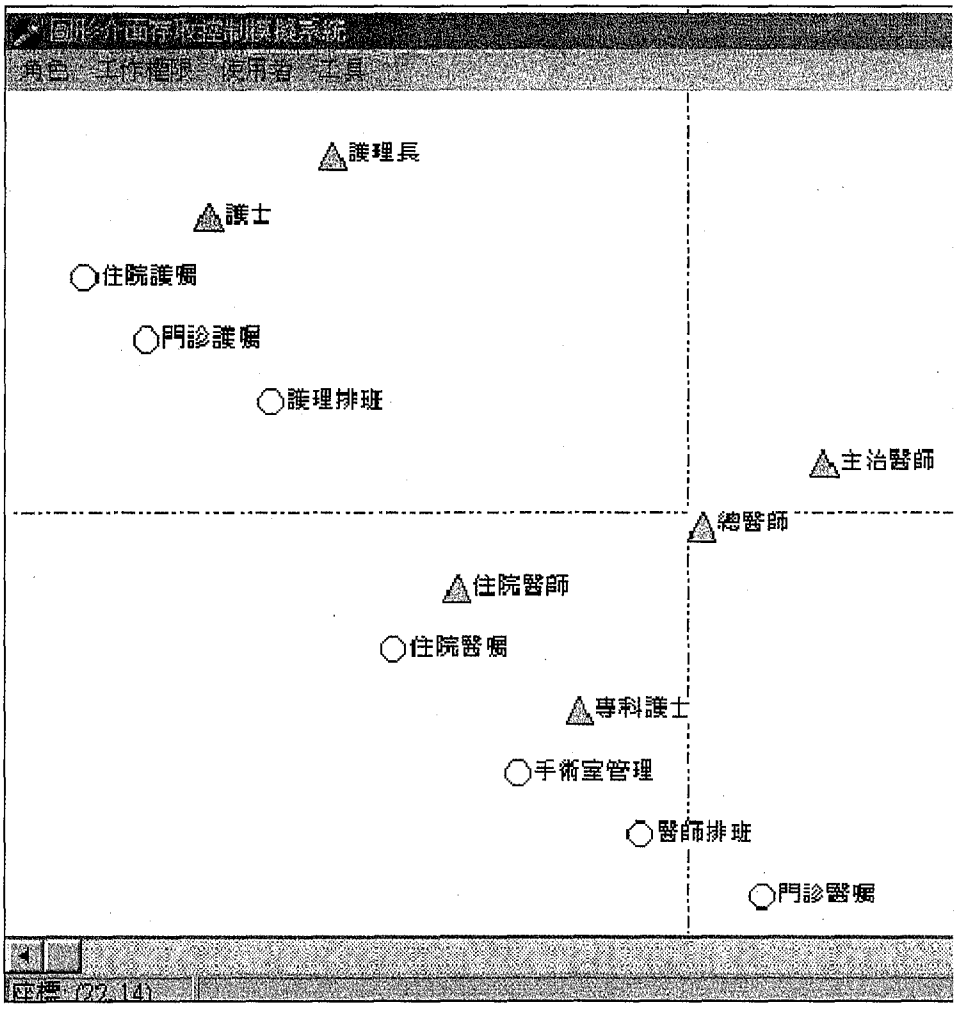

圖10：權限管理工具介面實例一

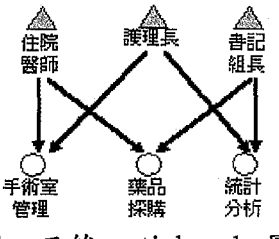

圖11：三維partial order圖形

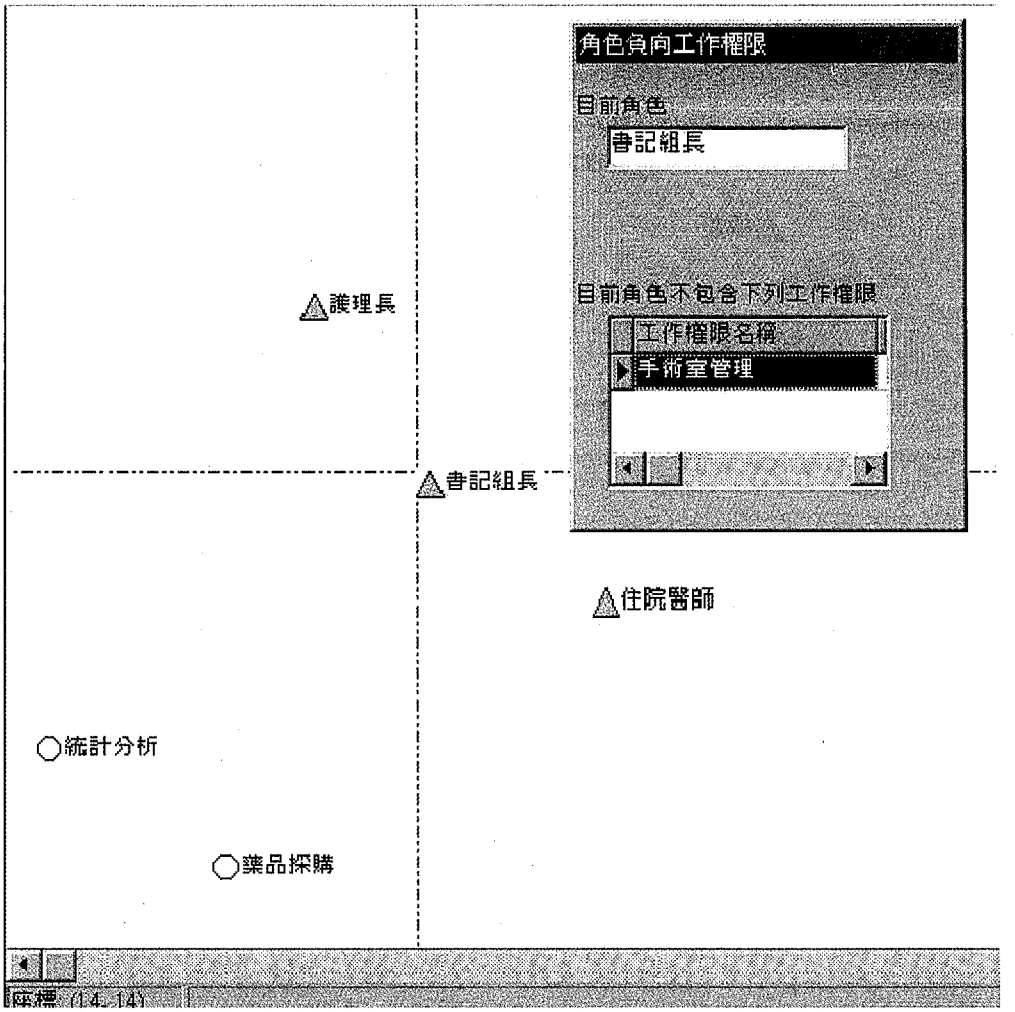

圖12：權限管理工具介面實例二

言，很少有三維以上的 partial order 圖形，在此例中的住院醫師事實上不會親處理藥品採購，這類行政工作通常交由書記組長處理，如此則移除了住院醫師與藥品採購之間的關係，其整體關係變成二維 partial order 圖形，就得以在二維向量空間中顯示，換言之圖形維度由三維降至二維，簡化圖形介面的複雜性。

㈡實例三（二維的 *partial order*）

以某上市公司的財務系統爲例，所有工作權限依序編號分別爲：1. 傳票查詢、2. 待轉傳票登入、3. 正式傳票轉入、4. 財務管理報表、5. 過帳、6. 審核付款、7. 應收帳款認列、8. 帳款核准、9. 出納付款、10. 出納付款核准；每個角色擁有的工作權限分別爲：財務人員擁有編號 1、2 的工作權限，總帳維護人員擁有編號 1、2、3、4、5 的工作權限，主辦會計擁有編號 1、2、6、7 的工作權限，主計課長擁有編號 1、2、3、4、5、6、7、8 的工作權限，出納人員擁有編號 1、2、9 的工作權限，出納課長擁有編號 1、2、9、10 的工作權限；以上採用傳統 access control list 方式表達，只能得知個別角色擁有的工作權限。

若以二維向量圖形表示如圖 13 ，圖中所點選的角色爲出納人員，透過十字虛線輔助視覺效果，代表出納人員擁有的工作權限，爲其座標至原點之左下方所圍成之矩形區域中所有的工作權限，分別爲出納付款、傳票查詢、待轉傳票登入。

二維向量圖形表示方法，除了具有清晰的視覺效果表達各別角色擁有的工作權限以外，更可以從圖中獲得角色之間關係的資訊，分別爲 separation 、 sharing 、 oversight 。

1. separation ，總帳維護人員與主辦會計，此兩角色擁有的工作權限均不被對方包含，彼此都擁有對方所沒有的專屬工作權限，表示兩者權限無法比較。從圖 13 中兩角色連成的線段若爲左上至右下，即可判斷其符合 separation 的特性，具有不對稱性 (anti -symmetric) 的關係，以 partial order 觀念稱爲 incompatible ，實際意義爲職掌分權 (separation of duty) 的關係。
2. sharing ，增加財務人員擁有的工作權限時，總帳維護人員、主辦會計、主計課長等角色亦同時擁有新增的工作權限。從圖 13 中任兩角色連成的線段若爲右上至左下，即可判斷其符合 sharing 的特性，在此例中的總帳維護人員與主辦會計，除了符合 separation 的

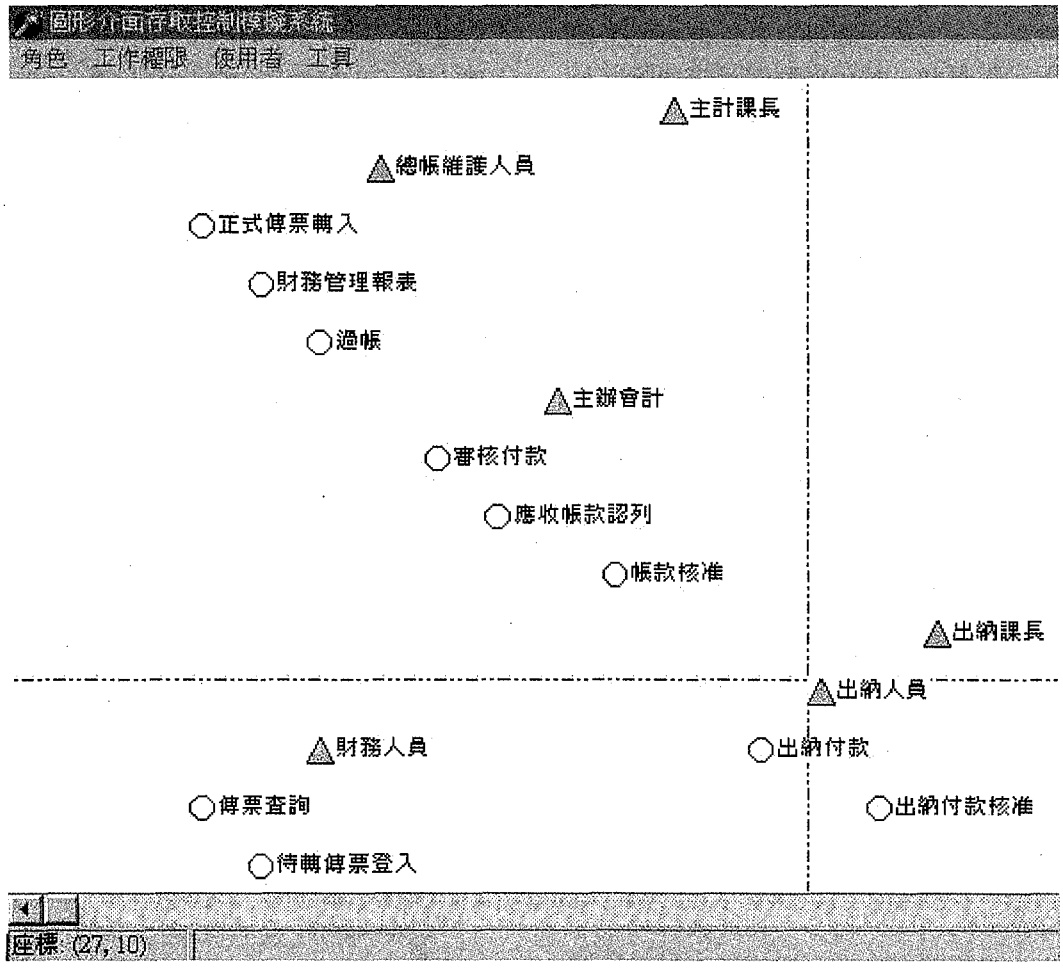

圖13：權限管理工具介面實例三

特性，亦同時分別與財務人員符合 sharing 的特性，以 partial order 觀念表示不論 incompatible 或 compatible ，均可同時符合 sharing 的特性。

3. oversight ，不論增加工作權限給財務人員、總帳維護人員或主辦會計時，主計課長亦同時擁有新增的工作權限。從圖 13 中主計課長與財務人員之間的連線，可先透過總帳維護人員或主辦會計，再間接連線至財務人員，且線段均爲右上至左下，即可判斷其符合 oversight 的特性，具有遞移 (transitive) 的關係。

以管理者的角度而言，使用向量圖形操作介面管理角色與工作權限，不但一目了然得知各角色的關係與各別擁有的工作權限，更幫助了解組織整體架構與職掌，使權限管理簡化。

柒、結論與未來展望

本研究將存取控制管理工具，以異於傳統之向量圖形介面呈現，展現另類的存取控制管理方式，輔助管理者在存取權限上的控制，並以實際系統模擬。此介面不但改變原有的權限管理操作習慣，更在視覺畫面、管理者認知以及系統內部運作等方面，有截然不同的重新詮譯與定義。但此系統僅止於觀念與操作上的雛型，仍存在許多有待努力之研究方向如下：

- 本研究僅使用兩種座標計算之演算法則，未來可再深入研究其他更快速、更完整之演算方法。
- partial order 圖形超過二維以上之例外表示方法，可再探討更具視覺清晰效果的表示方法。
- 系統中的輔助操作介面仍有待改善，例如圖形的放大、縮小，輔助說明等等。
- 未來可將圖形介面存取控制工具與實際系統結合，眞正應用於實際系統的存取控制。
- 本研究僅考慮兩種存取控制的限制條件，包含使用者扮演某一角色之最大人數限制與互斥角色，未來可納入其他限制條件。
- 未來可針對各組織的管理者進行系統測試，實際評估本研究之圖形介面存取控制工具對管理者的幫助。

參考文獻

1. Graham, G. S. and Denning, P. J. "Protection - Principles and practice," Proceedings AFIPS Spring Joint Computer Conference 1972, pp: 417-429.
2. Hirugachi, T. "On the dimension of partially ordered sets," Science Rep. Kanazawa Univ., (1) 1951, pp: 77-94.
3. Sandhu, R. S. "The NTree: A Two Dimension Partial Order for Protection Groups," ACM Transactions on Computer Systems, (6:2) 1988, pp: 197-222.
4. Sandhu, R. S. "Lattice-Based Access Control Models," Computer, (26:11) 1993, pp: 9-19.
5. andhu, R. S. and Samarati, P. "Access Control: Principles and Practice," IEEE Comm. Magazine 1994, Sep, pp: 40-48.
6. Sandhu, R. S. and Coyne, E. J. "Role-Based Access Control Models," IEEE Computer 1996, Feb, pp: 38-47.
7. Shieh, W. G., Weems, B., and Kavi, K. M. "An N-grid Model for Group Authorization," Computer Security Applications Conference 1990, pp:384-392.