以工作爲基礎的存取控制之權責區分授權準則設計[1]

劉敦仁、吳美玉、黃景彰
交通大學資訊管理研究所

摘 要

以「角色爲基礎的存取控制」主要是依據權責衝突的角色，來建立授權準則以達到權責區分之目的。然而爲因應企業環境之改變，企業之運作需提供有效的工作管理與工作爲基礎的存取控制，因此若僅以角色爲基礎的機制，並無法有效的管理企業之工作。近來雖已有以角色與工作爲基礎的存取控制之研究，但並未探討權責區分授權準則或是僅爲原來以角色爲基礎的存取控制之簡單延伸，並未從工作之間不同的權責關係考量權責區分之授權準則。本研究提出新的分析觀點，從企業制訂規劃工作的角度，分析與定義不同的工作權責衝突關係，包括制衡、督導查核與非獨攬性等，並依據所定義的工作權責衝突關係來探討使用者、角色與工作之授權及指派，進而設計授權準則以達到在角色與工作爲基礎的存取控制模式中之權責區分。本研究不僅定義新的工作權責關係，更推導出符合工作權責關係之新的授權準則，包括督導查核及相依執行等權責區分準則。

關鍵詞：角色爲基礎的存取控制、工作爲基礎的存取控制、授權準則、權責區分

[1] 本文部份摘要內容收錄於第十三屆龍騰論文經營管理類入選獎，得獎論文集（吳美玉 et al. 1999）

Designing Authorization Rules for Separation of Duty in Task-based Access Control

Duen-Ren Liu, Mei-Yu Wu, Jing-Jang Hwang
Institute of Information Management
National Chiao Tung University

ABSTRACT

Mutual-exclusive roles are the basis for designing authorization rules to achieve separation of duty in role-based access control (RBAC) models. However, current RBAC models are not adequate to provide effective management of tasks within enterprises. Although research has been done in the context of role and task-based access control, there has been little work on the design of authorization rules to achieve separation of duty in this context. The designed authorization rules are merely simple extensions from the authorization rules of RBAC models. In addition, different duty-relationships among tasks are not considered. This work presents a novel view to analyze different duty-relationships among tasks from the aspect of how enterprises design and plan tasks. Several kinds of duty-conflict tasks are defined to represent various duty-relationships such as balancing, supervising and non-arbitrary relationships among tasks. Moreover, authorization rules for assigning tasks to roles and users are designed to achieve separation of duty. The proposed work not only defines new duty-conflict tasks but also deduces new authorization rules to achieve variations of separation of duty including supervision-based and execution-dependent separation of duty, etc.

Keywords: Role-based Access Control, Task-based Access Control, Separation of Duty, Authorization Rules

壹、緒論

由於企業內部電腦化的普及，各種資訊系統充斥於企業之中，對於企業而言，電腦所儲存的資料是企業內部最重要的資產。而網路的產生，使資料能以更便捷的方式存取，但是在一個開放的環境中，資源是有必要去進行安全性的控管。在各個應用系統中，所能操作的使用者應予以適當的授權管理，以確保企業資源的存取控制能達到安全及有效的管理，是一個很重要的議題。

針對企業資訊資源的存取控制，有相當多的文獻探討，其中「以角色爲基礎的存取控制」（ Role-Based Access Control, RBAC ）(Barkley 1995; Ferraiolo & Kuhn 1992; Ferraiolo et al. 1995; Giuri & Lglio 1996; Gustafsson et al. 1997; Sandhu et al. 1996)，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，需訂定「權責區分授權準則」（簡稱「權責區分準則」），以滿足相關的權責區分（ Separation of Duty ）政策。所謂的權責區分是一個對於多人控制政策的安全策略 (Simon & Zurko 1997)，主要是將衝突的權責予以區分授權予不同的角色或使用者負責，避免權責不分、獨攬、舞弊之情形。權責區分準則大略可分爲「靜態權責區分」即一個使用者不可擁有兩個互相衝突的角色，與「動態權責區分」即一個使用者可以擁有兩個互相衝突的角色，但是不能同時啓動擔任。

以角色爲基礎的存取控制，由於是以角色爲存取權限指派的單位，變動性較少，且其爲較高層次、抽象化的存取控制描述方式，因此優於傳統的強制性存取控制與隨意性存取控制，較能滿足複雜的企業環境需求。但是隨著產業型態的改變，可能會增加新的工作項目，或是工作需要被重新安排，而在以角色爲基礎的存取控制中，權限（ permission ）或是操作（ operation ）並無法完全表示企業內部「工作」的觀念。工作是一個較高層次的表達方式，工作亦可包含子工作，而工作流程更是一個高層次的工作規劃。因此基於角色不易更動的特性，而工作項目可能會有所增減、修改，我們若僅以角色爲基礎的存取控制之概念來管理企業的存取權限是不夠的。

以角色爲基礎的存取控制無法表達工作高層次的意涵，企業要符合現代多變的潮流，不僅要有適當的授權管理與存取機制，並且要能夠具有適應性，能機動的調整每個使用者及角色所授予的工作項目。因此需要發展出一套以角色與工作爲基礎的存取控制之授權機制，同時兼顧以角色分派的優點，與滿足工作變動性的特點，建立權責區分之授權準則。因此，本研究之目的在於設計授權準則，以達到在以角色與工作爲基礎的存取控制模式中之權責區分，使企業對於企業內部工作與資源的授權管理有所依據，確保企業資源的存取控制達到安全有效的管理。

不同於以角色爲基礎的存取控制，有少許文獻提出了以工作爲基礎的存取控制與授權管制 (Bertino et al. 1997; Schier 1998; Thomas & Sandhu 1997)，其中，Sandhu 等人所提出的以工作爲基礎的授權控制（ Task-based Authorization Controls ）(Thomas & Sandhu 1997)，主要是針對工作執行時期的工作狀態管制，並未進一步討論工作、角色與使用者間的授權指派與權責區分；而 Bertino 等人則是探討工作流程環境下，工作與角色的授權管制機制 (Bertino et al. 1997)，主要是提出邏輯程式的授權語言來描述授權條件，並提出依據邏輯授權條件，進行工

作流程中工作、角色及使用者授權指派管制的方法。論文中雖然依其授權語言舉例說明靜態與動態的權責區分，但並未著重在權責區分準則之建立說明，且未依據工作之間的關係特性來探討權責區分，致使無法以更簡明的方式來表達授權準則。

Schier 所提出之以角色與工作爲基礎的安全模式 (Schier 1998)，雖已提出由工作衝突來探討相關權責區分準則，但僅僅是原來以角色爲基礎的存取控制之延伸，亦即由原本以角色爲基礎的存取控制中定義互斥的角色，延伸定義互斥的工作，而未從工作的觀點，進一步分析討論不同的工作權責衝突。此外其所探討的權責區分準則，仍是以角色爲基礎的權責區分之延伸，亦即由互斥的角色授權給使用者的權責區分準則，延伸出由互斥的工作授權給使用者的類似權責區分授權準則，所探討的權責區分亦僅包括簡單的靜態與動態權責區分。

本研究認爲企業職務角色間之權責衝突，是基於所賦予職務角色之工作權責衝突，才造成職務角色之權責衝突，因此本研究從工作的觀點分析探討企業內部所制訂的工作與工作間不同的權責衝突關係，進一步定義出不同的工作權責衝突關係，並以此爲基礎，探討工作授權予角色，角色授權予使用者之權責區分授權準則。

本文提出新的分析觀點，從企業制訂規劃工作的角度，深入分析企業內部工作與工作之間的關係。本研究認爲企業所制訂規劃的工作，代表了所欲賦予角色（職務）或使用者的權責，當一工作分配指派給某一個角色或人員時，即代表了此角色或人員肩負了此一工作之工作權責。而企業在制訂與規劃工作時，會設計相對應權責之工作，例如制衡與督導權責之工作，以確保工作執行之正確性，達到稽核之目的。因此，企業內部工作權責與工作權責之間存在不同的權責衝突關係，例如採購工作與驗收工作具備制衡之權責關係，而開支票工作與稽核支票工作則是具備督導查核之權責關係。本研究將具有對應權責之工作關係，概稱爲工作權責衝突關係，主要是若將對應權責之工作一起交由某個使用者或某個角色執行時，會造成權責獨攬、舞弊、權責無法區分的情形。本研究共定義了工作權責衝突、工作制衡、督導查核、存取物件、協調合作與非獨攬性等工作權責衝突關係。

依據所定義的各項工作權責衝突關係，本研究進一步訂定工作授權予角色、角色授權予使用者之「權責區分授權準則」（簡稱「權責區分準則」），所訂定的準則包括靜態、動態、相依執行、存取物件等工作權責及督導查核之不同權責區分準則。因此，本研究的主要貢獻便是從工作的觀點分析企業內部不同的工作權責衝突關係，並依據所定義的工作權責衝突關係建立權責區分之授權準則，更推導出符合工作權責關係之新的授權準則，包括督導查核及相依執行等權責區分準則。使企業易於管理企業內部工作的指派與授權，並符合企業內部的安全政策，以達到在以工作爲基礎的存取控制環境中之權責區分。「以工作爲基礎的存取控制」亦須結合角色概念，因此亦稱爲「以角色與工作爲基礎的存取控制」。

在本文中，第貳節詳細介紹相關的文獻探討，包括以角色爲基礎的存取控制、權責區分、以工作爲基礎的存取控制與授權管制等，第參節介紹工作權責衝突分析，第肆節則根據第參節之分析，說明以角色與工作爲基礎的權責區分，而在第伍節說明相關的分析與討論，並在第陸節做出結論以及討論未來的研究方向。

貳、文獻探討

本節針對以角色爲基礎的存取控制、

權責區分準則及工作爲基礎的存取控制之相關文獻加以說明。Ferraiolo 提出以角色爲基礎的存取控制（Role-Based Access Control, RB AC）概念 (Ferraiolo & Kuhn 1992)，並說明以角色爲基礎的存取控制爲一種非隨意性的存取控制。在以角色爲基礎的存取控制模式 (Ferraiolo & Kuhn 1992; Ferraiolo e t al. 1995)，一個使用者可以擁有數個角色，一個角色也可以由數個使用者所擁有，而權限的指派並非一一分派給使用者，而是指派給角色。如此減少了不少管理上的麻煩，在組織或人事變動的時候，也能夠更方便的更改存取控制規則。而 Sandhu 等人所提出的模式中 (Sandhu et al. 1996)，以角色爲基礎的存取控制是由下列幾項元素所組成：使用者、角色、權限，與會期。所謂的使用者即眞實世界的人，或者代表人的身份執行的程式；而角色即在組織中的某個角色，我們可以將其視爲權限的集合，或者視爲使用者與權限的集合，以銀行環境爲例，「出納」與「會計」皆爲一種角色；而權限即存取系統中物件的權限；會期即使用中的角色集合，使用者可以動態選擇所需的角色，僅使用需要的權限，以達成最少權限（least privilege）的功效。

權責區分（Separation of Duty）(Ferraiolo et al. 1995; Gligor et al. 1998; Nash & Poland 1990; Sandhu et al. 1996; Simon & Zurko 1997) 爲以角色爲基礎的存取控制模式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。權責區分最主要的目的，就是將互相衝突的工作分由不同的人來負責，以防止舞弊。譬如「採購人員」與「付款人員」，不應有人同時屬於此兩種互相衝突的角色。權責區分大略可分爲「強互斥」（strong exclusion）或稱「靜態權責區分」（static separation of duty）與「弱互斥」（weak exclusion）或稱「動態權責區分」（dynamic separation of duty）(Ferraiolo et al. 1995; Gligor et al. 1998; Sandhu et al. 1996; Simon & Zurko 1997)。所謂「靜態權責區分」即爲一個使用者不可擁有兩個互相衝突的角色；而「動態權責區分」則爲一個使用者可以擁有兩個互相衝突的角色，但是不能同時啓動擔任它們，動態的權責區分可爲企業帶來賦有彈性的管理。目前所發表的文獻中，以 Gligor 等人 (Gligor et al. 1998) 所討論的權責區分準則最多，其所分類的權責區分共十一個操作。雖然文中所討論的權責區分類型最多，但有很多屬語意不明，並且尚有未考慮到的情形，例如未考慮以工作之間的相關性來決定執行順序與權責區分準則。

僅以角色爲基礎的存取控制來作爲達到企業權責區分之目標，尚欠缺企業眞正運作的活動特性－以工作爲導向的企業環境。一個工作是某個角色對於一群物件範圍所能執行操作的權力 (Coulouris et al. 1998)，工作可爲一單一的活動或是包含多個子工作。Sandhu 等人所提出的以工作爲基礎的授權控制 (Thomas & Sanhu 1997)，主要是針對工作執行時期的工作狀態管制，提供工作執行授權機制；Schier 則提出以角色與工作爲基礎的安全模式 (Schier 1998)；而 Bertino 等人則是探討工作流程環境下，工作與角色的授權管制機制 (Bertino et al. 1997)，相關介紹請參考第壹節之說明。

參、工作權責衝突分析

企業所制訂規劃的工作，代表了所欲賦予角色或使用者的權責，當一工作分配指派給某一個角色或人員時，即代表了此角色或人員肩負了此一工作之工作權責。

而企業在制訂與規劃工作時，會設計相對應權責之工作，例如制衡與督導權責之工作，以確保工作執行之正確性，達到稽核之目的。以下即深入說明爲何以工作的觀點來分析企業內部不同的工作權責衝突關係，並深入分析企業內部工作與工作之間的關係。

一、以工作爲基礎的企業環境

所謂的工作即某個角色對於一群物件範圍所能執行操作的權力 (Coulouris et al. 1998) ，亦即一個公司內部的任何企業活動，皆可稱爲一件工作。在以角色爲基礎的存取控制模式中，所謂的角色可視爲一個使用者或是一群使用者在組織中所能執行的交易集合 (Ferraiolo & Kuhn 1992)，亦即角色是一些職務功能的集合 (Ferraiolo et al. 1995) ，因此，角色眞正應該隱含有職務與工作兩層的意義。此處的工作與操作 (operation) 又不盡相同，所謂的操作即對於以角色爲基礎的存取控制物件的特定存取模式 (Ferraiolo et al. 1995)，操作是較低層次的概念，沒有階層性的關係，而工作是更高層次的表達，並具有階層關係，工作包含有子工作的概念，因此將工作從角色中獨立出來，如此一來，不但能比較明確的區分其眞正的意義、減少混淆，而且另一方面，在組織內部的職務較少更動，而工作則隨時可能會有新的工作項目加入，或是工作內容有修改，因此若將兩者獨立分開，則可減少因爲少部分的工作更動，而修改相關的角色設定。在企業內部的工作並不是各自獨立的，工作與工作間可區分成下列之關係：

- 工作與子工作關係：一件工作可以包含多個子工作，例如「發出一張支票」工作，可細分爲「準備一張空白支票」、「填入金額、日期資料」、「稽核資訊」等子工作。

- 工作流程：根據工作流程管理協會 (Workflow Management Coalition, WfMC) 的定義，工作流程即是「將企業處理流程一部分或全部的自動化。在這自動化的過程中，是爲了達成某特定目標的所有活動，依照規則予以執行，而這些活動間是以傳遞文件、資訊來達成整個流程的完整執行。」(WfMC 1996)，工作與工作之間，除了有工作與子工作之間的包含性，還有工作與工作之間的相互合作流程關係。

- 工作執行順序：在企業內部的工作，具有執行的先後順序之關係，有些工作可同時進行，有些則會有執行先後順序的規範。

- 工作相依性：若一工作之執行是與另一工作之執行相關，則稱此兩工作具有工作相依性。例如同屬於一工作流程執行 (Workflow Instance) 之工作即具備工作相依性，流程執行之工作存在執行相關之關係，依照訂定的流程順序執行工作，以完成一處理流程。訂定權責區分之授權準則時須考慮工作之相依性，以一簡單之採購流程包括採購與驗收兩項工作爲例，驗收工作之授權指派須考量與其相依之採購工作之授權指派情形，才能確實達到權責區分。

定義一：【工作相依性】若工作 T_i 之執行是與工作 T_j 之執行相關，則稱工作 T_i 與工作 T_j 具有工作相依性，以〝$T_i \sim T_j$〞表示，而以〝$T_i \not\sim T_j$〞表示工作 T_i

與工作 T_j 不具有相依性。

- 工作權責衝突：企業內部工作的分派與指派，代表了權責的劃分，當一工作分配指派給某一個角色或人員時，即代表了此角色或人員肩負了此一工作之工作權責，因此，若有任何兩個工作一起交由某人或是某個角色執行時，則可能造成權責獨攬，權責無法區分的情形發生時，則我們稱此兩個工作具有「工作權責衝突」關係。

二、工作權責衝突關係

在公司內部，有大大小小的工作，而這些工作間有些是不可皆由同一個角色或是同一個人執行，如果無法避免此種情形發生，則可能產生一些弊病，如在一個開支票過程中，從準備一張空白支票填入相關資訊，到由主管稽核支票日期、金額等資訊，再將此支票送出去的過程中，開支票及稽核支票的動作就不應該交由同一個人處理，如此可能會造成監守自盜的行政舞弊。

定義二：【工作權責衝突關係】任何兩個工作具備有權力與責任互相衝突關係時，我們以 $T_i \oplus T_j$ 表示工作 T_i 與工作 T_j 間具有工作權責衝突關係。

企業內部工作的制訂爲了防止舞弊，確保工作被正確的執行，通常在制訂一工作時，會制訂一與其相對應之督導、核定、或區分之工作，如採購與驗收即具有工作權責衝突之關係，「工作權責衝突」尚可區分爲工作制衡關係、督導查核關係、存取物件工作權責衝突、非獨攬性工作權責，及協調合作關係，分述如下：

定義三：【工作制衡關係】具備平等、平行之地位的工作具有互相工作制衡性質，以 $T_i \equiv T_j$ 表示工作 T_i 與工作 T_j 爲互相制衡之工作。

具有工作制衡關係的工作，其執行的角色位階應屬於組織關係中之平行關係。如會計與出納此兩者之工作即具有工作制衡關係。其中 $T_i \equiv T_j$ 具備有交換性，亦即 $T_i \equiv T_j$ 等於 $T_j \equiv T_i$。而工作制衡關係亦是一種工作權責衝突關係，亦即 $T_i \equiv T_j \Rightarrow T_i \oplus T_j$。本文以符號“$\Rightarrow$”表示隱含推論。因此工作制衡關係除了應滿足本身特有的規範外，尚須滿足工作權責衝突關係之限制。另外，具備相互制衡關係之工作的分派與指派是必須交由不同的角色與不同的人員執行，以區別權責，進而達到權責制衡的目的。

定義四：【督導查核關係】具有監督、查察、核可權責關係之工作，以 $T_i \succ T_j$ 表示工作 T_i 具有督導查核工作 T_j 的權責關係。

具有督導查核關係的工作，其執行的角色位階應屬於組織關係中之直屬關係與成員關係。如主管與辦事員之稽核與採購等工作即屬於督導查核關係的工作。我們以〝$T_i \succ T_j$〞表示工作 Ti 有督導查核工作 T_j 的權責關係，換言之，執行工作 T_i 的角色位階應比執行工作 T_j 的角色位階來得高。我們以〝$R_x \succ R_y$〞表示角色 R_x 的職務位階高於角色 R_y 的職務位階。$T_i \succ T_j$ 並不具備有交換性，亦即 $T_i \succ T_j$ 並不等於 $T_j \succ T_i$。而督導查核關係亦是一種工作權責衝突關係，亦即 $T_i \succ T_j \Rightarrow T_i \oplus T_j$。因此督導查核關係除了應滿足本身特有的規範外，尚須滿足工作權責衝突關係之限制。

定義五：【存取物件工作權責衝突】兩個

工作具有工作權責衝突關係在於存取特定物件時，以 $T_{i\ OBJx} \oplus_{OBJy} T_j$ 表示工作 T_i 存取 OBJ_x 而工作 T_j 存取 OBJ_y 時有工作權責衝突。

定義六：【存取物件工作制衡關係】兩個工作具有工作制衡關係在於存取特定物件時，以 $T_{i\ OBJx} \equiv_{OBJy} T_j$ 表示工作 T_i 存取 OBJ_x 而工作 T_j 存取 OBJ_y 時有工作制衡關係。

定義七：【存取物件督導查核關係】兩個工作具有督導查核關係在於存取特定物件時，以 $T_{i\ OBJx} \succ_{OBJy} T_j$ 表示工作 T_i 存取 OBJ_x 而工作 T_j 存取 OBJ_y 時有督導查核關係。

對於兩個互相工作權責衝突的工作，若其眞正衝突的原因在於存取特定之物件，則我們可以較不嚴格的規範此兩個工作，仍可被執行，但不能針對有衝突的物件存取，有如此關係存在之工作，稱爲具有「存取物件工作權責衝突」關係。以開支票此工作 T 爲例，包含有子工作 T_1 －準備空白支票，填入金額、日期，和子工作 T_2 －稽核支票內容資訊，與子工作 T_3 －發出支票。其中，T_1 與 T_2 即具有督導查核關係，即 $T_2 \succ T_1$。而子工作 T_2 具有督導查核子工作 T_1 的關係，在於針對同一張支票－物件 OBJ ，即 $T_{1\ OBJ} \succ_{OBJ} T_2$。準備空白支票，填入金額、日期，與稽核支票內容資訊此兩種工作之所以權責衝突，在於針對同一張支票，若是對於不同張之支票，則可彈性的允許此種工作並不具有工作權責衝突關係。

因爲工作制衡關係亦是一種工作權責衝突關係，因此存取物件工作制衡關係，亦是一種存取物件工作權責衝突，即 $T_{i\ OBJx} \equiv_{OBJy} T_j \Rightarrow T_{i\ OBJx} \oplus_{OBJy} T_j$。同理，存取物件督導查核關係，亦是一種存取物件工作權責衝突，即 $T_{i\ OBJx} \succ_{OBJy} T_j \Rightarrow T_{i\ OBJx} \oplus_{OBJy} T_j$。$OBJ_x$ 亦可等於 OBJ_y，亦即 x 可等於 y，表示是對同一物件之存取權責衝突關係。

定義八：【非獨攬性工作權責】所有的工作不可全部授權給同一個角色及人員，或是由同一個角色、人員執行。我們以〝σT〞表示工作 T 具有非獨攬性的特性。而以 $\sigma_{role} T \geq 2$ 與 $\sigma_{subject} T \geq 2$ 表示對於角色與人員的最小限制。

以〝σT〞表示工作 T 具有非獨攬性的特性，而以不同的下標註解是針對角色（role）或是人員（subject）的規範，此處所定義的最小角色數目與人員數目爲「2」，但是依據組織不同的需求，授權或執行工作 T 所需的最小角色數目與人員數目可再調整。

定義九：【協調合作關係】需會辦單位一起合作完成之工作，且存在子工作間具有工作權責衝突關係，以 $\bowtie T$ 表示工作 T 需要多個單位的協調合作以完成。而以 $\bowtie_{subtask} T \geq 2$、$\bowtie_{department} T \geq 2$、$\bowtie_{role} T \geq 2$ 與 $\bowtie_{subject} T \geq 2$ 分別表示對於子工作、部門、角色與人員的最小限制。

工作 T 需要相關單位、人員的相互協調以完成該工作，表示該工作最少可再區分成兩個以上的子工作，並且要交由至少兩個以上的單位、角色與人員執行，此處之子工作（subtask）、部門（department）、角色（role）與人員（subject）至少需兩個是最少需求，可依公司內部實際運作狀況而調整。另外，對於工作 T 所包含的子工作，具備有下述關係：

$\exists$ subtask $T_i, T_j, T_i \in T$ and $T_j \in T$ and $\bowtie T \Rightarrow T_i \oplus T_j$。此處之〝$\oplus$〞表示

具有工作權責衝突關係，包括工作制衡、督導查核或是存取物件等權責衝突關係。

肆、工作爲基礎的權責區分

當工作指派給某一個角色、使用者，或是由某一個主體啓動執行時，會有不同的權責產生，如果將具有工作權責衝突關係的工作指派給同一個角色或使用者，將會造成權責不分，因此在本節中，我們將依據第參節所定義的工作權責衝突關係來探討相關的授權準則，以達到權責區分的理想。所謂授權準則，即在企業內部或自動化工作流程管理中，每個使用者（員工）可以擔任哪些角色的分派依據，及該角色可以執行的工作、存取的物件等。要設計一套好的授權準則，必須考量清楚公司內部相關的權責區分政策，亦即事先定義清楚每個員工所能扮演的職位角色，及可執行的工作、可存取的物件等，做好相關的權力與責任的規範，以防止舞弊的情況發生。

對於不同的企業工作環境，會有不同的授權準則規範，但仍有一些基本的權責區分準則，因此，本節所設計之授權準則，乃分析現有組織中的實際工作環境，並依據第參節所定義之工作權責衝突關係、工作制衡、督導查核、存取相依物件工作權責衝突、非獨攬性工作權責，以及協調合作等關係，探討使用者、角色與工作之授權及指派，進而設計授權準則以達到在工作爲基礎的存取控制之權責區分。在不同的強制階段時期包括指派或執行時期，會有不同程度的規範、限制，如下列所述：

- 指派時期：所謂的指派時期，即在事前的使用者（組織人員）、角色、工作、及可存取的物件，兩兩之間的指派、授權，亦即事前定義好每個人員所能擔任的角色，每個角色所能執行的工作，以及各個工作所被允許存取的物件有哪些。針對指派時期所制訂的權責區分準則爲靜態權責區分。
- 執行時期：所謂的執行時期，即眞正欲執行、完成某項工作的期間，包括啓動擔任角色，該角色所能執行的工作，以及每個工作所對應可存取的物件，執行時期尚包含三部分：啓動擔任角色、執行工作及存取物件。針對執行時期所制訂的權責區分準則包括動態權責區分、相依執行權責區分及相依存取物件權責區分。動態權責區分主要是規範使用者（主體）是否可同時啓動擔任角色、執行工作及存取物件，相依執行權責區分主要規範執行相依工作的授權準則，相依存取物件權責區分則是針對相依工作存取物件之規範。相依工作爲先後執行但具備相依性之工作，例如同屬於一工作流程執行之工作間具有執行相關之關係。訂定權責區分之授權準則時須考慮工作之相依性，才能確實達到權責區分。

執行時期的規範相對於指派時期是較不嚴格的，在指派時期，具有工作權責衝突關係的工作，不可同時授權給同一個角色，或是授權給不同的角色，但此擁有互相工作權責衝突的角色同時授權指派給同一個人員亦不允許；而在執行時期的限制則較不嚴格，對於具有工作權責衝突關係的工作，分別授權給不同角色，再指派給同一個人員時，仍可允許，但不能同時啓動擔任該擁有互相工作權責衝突的角色。

以下小節的授權準則皆依據此概念衍生，我們相信依據工作權責衝突關係來建構的授權準則，可具備較有直覺化、較有

表1： 授權準則相關函數代表意義說明

函　數	代　表　意　義
authorized_tasks(R)	角色R被授權所能執行的工作集合
authorized_roles(S)	人員S被授權所能擔任的角色集合
authorized_tasks(S)	人員S被授權所能執行的工作集合
authorized_objects(T)	工作T被授權所能存取的物件集合
active_tasks(R)	角色R啓動執行的工作集合
active_roles(S)	人員S啓動擔任的角色集合
active_tasks(S, R)	人員S以角色R啓動執行的工作集合
active_objects(S, R, T)	人員S以角色R執行工作T啓動存取的物件集合
activated_roles(S)	人員S已啓動擔任過的角色集合
executed_tasks(S, R)	人員S以角色R所執行過的工作集合
accessed_objects(S, R, T)	人員S以角色R執行工作T所存取過的物件集合

表2： 授權準則相關函數隱含意義說明

函　數	隱　含　意　義
T ∈ active_tasks(R)	T ∈ authorized_tasks(R)
R ∈ active_roles(S)	R ∈ authorized_roles(S)
T ∈ active_tasks(S, R)	R ∈ active_roles(S) ； T ∈ authorized_tasks(R)
O ∈ active_objects(S, R, T)	T ∈ active_tasks(S, R) ； O ∈ authorized_objects(T)
R ∈ activated_roles(S)	R ∈ authorized_roles(S)
T ∈ executed_tasks(S, R)	R ∈ authorized_roles(S) ； T ∈ authorized_tasks(R)
O ∈ accessed_objects(S, R, T)	R ∈ authorized_roles(S) ; T ∈ authorized_tasks(R) ; O ∈ authoriged-objects(T)

彈性的特性，並能達到權責區分的目標。表 1 僅就描述授權準則所需之函數說明。本文是以符號 O 表示物件（ Object ），T 代表工作（ Task ），R 表示角色（ Role ），S 代表主體（ Subject ）。爲使說明清晰，本文以使用者與人員來做爲主體之說明。描述授權準則所需之函數尚包含有隱含之意義，如表 2 之說明。以第一列爲例， T ∈ active_tasks(R) 隱含有 T ∈ authorized_tasks(R) 之意義，亦即 T ∈ active_tasks(R) ⇒ T ∈ authorized_tasks (R)，角色 R 可啓動執行工作 T ，表示角色 R 已被授權可執行工作 T 。

一、權責區分準則：依據工作權責衝突關係

本節介紹依據工作權責衝突關係所推導制訂的權責區分準則，依據工作制衡關係所制訂的權責區分準則與工作權責衝突的情況一樣，因爲工作制衡關係亦是一種工作權責衝突關係，即 $T_i \equiv T_j \Rightarrow T_i \oplus T_j$ ，而在工作制衡之權責區分，並無特

殊之規則增加，因此亦適用依據工作權責衝突關係所制訂的權責區分準則。

㈠靜態工作權責區分

所謂靜態權責區分即一個使用者不可以擁有擔任兩個互相權責衝突的角色之權限，而兩個角色之所以互相權責衝突，是因爲其所授予之工作與另一角色所授予之工作互相權責衝突。當角色擁有權責衝突的工作，或是權責衝突的工作授權給不同的角色，但同時授權給同一個人員，則可能造成權責無法區分、舞弊行爲發生的疑慮情形，如「採購工作」與「出納工作」爲權責衝突的工作，則此兩種工作不應由同一個角色或人員同時擁有該工作的授權。在靜態的權責區分準則設計上，可再細分爲角色、工作，以及使用者、角色與工作兩種指派的情況討論。

在角色與工作兩者之間的指派關係中，當兩個工作具有權責衝突關係時，則不可授權給同一角色。例如在銀行的作業環境中，假設開支票與稽核的工作是屬於權責衝突關係，則當櫃員已被賦予執行開支票工作的情況下，就無法再賦予櫃員有稽核的工作。其正規表示法如規則 1 ：工作 T_i 與工作 T_j 具有工作權責衝突關係時，若工作 T_i 已經授權給角色 R ，則不能再授予角色 R 有執行工作 T_j 的權限。

規則 1 ：【靜態工作權責區分（角色、工作）】

$\forall T_i, T_j \in TaskSet, R \in RoleSet$

$T_i \in authorized\_tasks(R)$ and $(T_i \oplus T_j) \Rightarrow T_j \notin authorized\_tasks(R)$

在使用者、角色與工作三者間的指派關係中，使用者不可被授權擔任權責衝突之角色。承上述例子，櫃員 R_1 可執行開支票 T_1 與收款 T_3 兩項工作；主管 R_2 可擔任稽核 T_2 與批核 T_4 兩項工作，而開支票 T_1 與稽核 T_2 是權責衝突之工作，所以當某甲已被授權擔任櫃員 R_1 的角色情況下，就無法再被授權擔任主管 R_2 的角色。其正規表示法如規則 2 ：工作 T_i 與工作 T_j 具有工作權責衝突關係時，工作 T_i 與工作 T_j 分別授權給角色 R_x 與 R_y ，且角色 R_x 已授權給人員 S 時，則不能再授予人員 S 有擔任角色 R_y 的權限。

規則 2 ：【靜態工作權責區分（使用者、角色、工作）】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S \in SubjectSet$ and $x \neq y, i \neq j$

$T_i \in authorized\_tasks(R_x)$ and $T_j \in authorized\_tasks(R_y)$ and

$R_x \in authorized\_roles(S)$ and $(T_i \oplus T_j) \Rightarrow R_y \notin authorized\_roles(S)$

㈡動態工作權責區分

所謂動態權責區分即一個使用者可以擁有擔任兩個互相權責衝突的角色之權限，但是不能同時啓動擔任。例如「請購工作」與「採購工作」爲互相權責衝突的工作，根據動態權責區分，此兩種工作可分別授予不同的角色，可由同一個人員同時擁有此兩個角色的授權，但是不可同時啓動擔任。

在動態工作權責區分中，若是在指派時期允許兩個互相權責衝突的工作被授權給同一角色，則表示該企業內部有定義不明的職務工作，因此我們採取較嚴格的限制，不允許此種情形存在，亦即角色與工作兩者之間的指派關係仍須依據靜態工作權責區分之規則 1 。

在使用者角色與工作三者之間的動態工作權責區分關係中，須遵循規則 3 ：若工作 T_i 與工作 T_j 具有工作權責衝突關係，且工作 T_i 與工作 T_j 分別授權給角色 R_x 與角色 R_y ，而人員 S 亦被授予擔任角色 R_x 與角色 R_y 的權限，且人員 S 啓動擔

任角色 R_x ，則人員 S 不可再啓動擔任角色 R_y 。

規則 3 ：【動態工作權責區分 - 啓動擔任角色】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$(T_i \oplus T_j)$ and $T_i \in authorized\_tasks(R_x)$ and $T_j \in authorized\_tasks(R_y)$ and $R_y \in authorized\_roles(S)$ and $R_x \in active\_roles(S) \Rightarrow Ry \notin active\_roles(S)$

規則 3 －人員不可同時啓動擔任擁有工作權責衝突的角色，爲較嚴格之規範，但若放寬限制，使用者可同時啓動擔任擁有互相工作權責衝突的角色，但不允許同時啓動執行具有工作權責衝突關係之工作，如規則 4 所示：工作 T_i 與工作 T_j 具有工作權責衝突關係，人員 S 以角色 R_x 啓動執行工作 T_i ，且角色 R_y 被授予執行工作 T_j 的權限，則人員 S 可啓動擔任角色 R_y ，但人員 S 不可以角色 R_y 啓動執行工作 T_j 。

規則 4 ：【動態工作權責區分 - 啓動執行工作】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$(T_i \oplus T_j)$ and $T_i \in active\_tasks(S, R_x)$ and $R_y \in active\_roles(S)$ and

$T_j \in authorized\_tasks(R_y) \Rightarrow T_j \notin active\_tasks(S, R_y)$

若再放寬限制，對於兩個互相權責衝突的工作，若其眞正衝突的原因在於存取特定之物件，則我們可以較不嚴格的規範此兩個工作，使用者可同時啓動擔任擁有互相工作權責衝突的角色，允許同時啓動執行工作，但不允許執行具有存取物件權責衝突關係之工作去啓動存取特定物件，如規則 5 ：人員 S 以角色 R_x 執行工作 T_i 去啓動存取物件 OBJ_m ，工作 T_i 存取物件 OBJ_m 與工作 T_j 存取物件 OBJ_n 間有工作權責衝突關係，且工作 Tj 亦被授予存取物件 OBJ_n 的權限，則人員 S 目前可以角色 R_y 啓動執行工作 T_j ，但不能以角色 R_y 執行工作 T_j ，但不能以角色 R_y 執行工作 T_j 去啓動存取物件 OBJ_n 。

規則 5 ：【動態工作權責區分 - 啓動存取物件】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, OBJ_m, OBJ_n \in ObjectSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$OBJ_m \in active\_objects(S, R_x, T_i)$ and $(T_{i\ OBJm} \oplus_{OBJn} T_j)$ and $T_j \in active\_tasks(S, R_y)$ and $OBJ_n \in authorized\_objects(T_j) \Rightarrow OBJ_n \notin active\_objects(S, R_y, T_j)$

㈢相依執行工作權責區分

若一工作之執行是與另一工作之執行相關，則此兩工作具有工作相依性，例如同屬於一工作流程執行之工作即具備工作相依性。相依工作是先後執行但具備相依性之工作，工作之間存在某些執行相關性，這些相關性並不一定是要互相衝突的關係。相依執行工作權責區分主要是針對執行時期具備相依性及工作權責衝突關係之工作所制訂的規範，於執行時期同時啓動擔任角色、執行工作及存取物件，相依執行工作權責區分須依循動態工作權責區分一具工作權責衝突關係的工作，不可指派給同一個角色（規則 1 ），否則會有企業內部職務工作劃分不明之慮；而兩個擁有互相權責衝突工作的角色，可同時指派給同一個人，但是不可同時啓動擔任此互相衝突的角色（規則 3 ）；或是遵循放寬限制之規則 4 或規則 5 。

此外，相依執行工作權責區分須遵循之規則爲使用者可先後啓動擔任擁有權責

衝突工作的角色，但不可啓動執行具相依性且互相權責衝突的工作，其權責區分準則如規則 6 ：工作 T_i 與工作 T_j 具有工作權責衝突關係及相依性，人員 S 以角色 R_x 已執行過工作 T_i ，且角色 R_y 被授予執行工作 T_j 的權限，則人員 S 可啓動擔任角色 R_y ，但人員 S 不可以角色 R_y 啓動執行有相依性的工作 T_j 。

規則 6 ：【相依執行工作權責區分－相依性】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$(T_i \oplus T_j)$ and $(T_i \sim T_j)$ and $T_i \in executed\_tasks(S, R_x)$ and $R_y \in active\_roles(S)$ and $T_j \in authorized\_tasks(R_y) \Rightarrow T_j \notin active\_tasks(S, R_y)$

如果要制訂更嚴格的權責區分準則，使人員 S 可先後啓動擔任擁有權責衝突工作的角色，必須其授權之工作不具備相依性，如規則 7 ：工作 T_i 與工作 T_j 具有權責衝突關係，且工作 T_i 與工作 T_j 分別授權給角色 R_x 與角色 R_y ，且人員 S 已啓動擔任過角色 R_x ，若人員 S 目前可再啓動擔任角色 R_y ，則必須是工作 T_i 與工作 T_j 不具備相依性。

規則 7 ：【相依執行工作權責區分－非相依性】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$(T_i \oplus T_j)$ and $T_i \in authorized\_tasks(R_x)$ and $T_j \in authorized\_tasks(R_y)$ and $R_x \in activated\_roles(S)$ and $R_y \in active\_roles(S) \Rightarrow T_i \not\asymp T_j$

㈣相依存取物件工作權責區分

相依執行工作權責區分爲使用者可先後啓動擔任擁有權責衝突工作的角色，但不可執行具相依性且互相權責衝突的工作，存取物件工作權責區分則是再放寬限制，人員可先後啓動擔任此擁有存取物件權責衝突工作的角色，可執行具相依性之工作，但不可執行具有存取物件權責衝突關係之工作來存取特定物件。相依存取物件工作權責區分是針對執行時期相依性工作具有存取物件工作權責衝突關係所制訂之準則，於執行時期同時啓動擔任角色、執行工作及存取物件，仍須依循動態工作權責區分，遵循規則 1 與規則 3 （或是遵循放寬限制之規則 4 或規則 5 ）。此外，若工作具備有相依性，且工作有存取物件工作權責衝突關係，則其正規表示式如規則 8 ：人員 S 以角色 R_x 執行工作 T_i 已存取過物件 OBJ_m ，工作 T_i 存取物件 OBJ_m 與工作 T_j 存取物件 OBJ_n 間有工作權責衝突關係，工作 T_i 與工作 T_j 具備有相依性，且工作 T_j 亦被授予存取物件 OBJ_n 的權限，則人員 S 目前可以角色 R_y 啓動執行工作 T_j ，但不能以角色 R_y 執行工作 T_j 去啓動存取物件 OBJ_n 。

規則 8 ：【相依存取物件工作權責區分】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, OBJ_m, OBJ_n \in ObjectSet, S \in SubjectSet$, and $x \neq y, i \neq j$

$OBJ_m \in accessed\_objects(S, R_x, T_i)$ and $(T_{i\ OBJm} \oplus_{OBJn} T_j)$ and $(T_i \sim T_j)$ and $OBJ_n \in authorized\_objects(T_j)$ and $T_j \in active\_tasks(S, R_y) \Rightarrow OBJ_n \notin active\_objects(S, R_y, T_j)$

二、權責區分準則：依據工作督導查核關係

工作督導查核關係亦是一種工作權責衝突關係，即 $T_i \succ T_j \Rightarrow T_i \oplus T_j$ ，因此須遵循依據工作權責衝突關係所制訂的權責區分準則。此外，依據工作督導查核關係

所新制訂的權責區分準則於以下小節說明。工作 T_i 有督導查核工作 T_j 的權責關係時，則執行工作 T_i 的角色位階應比執行工作 T_j 的角色位階來得高，我們以〝$R_x \succ R_y$〞表示角色 R_x 的職務位階高於角色 R_y 的職務位階。

㈠靜態督導查核權責區分

靜態督導查核權責區分仍須依循靜態工作權責區分，遵循規則 1 與規則 2。此外，若是兩工作間存在有督導查核關係時，主要是對於角色授權之限制，對於使用者（人員）之授權仍然依循規則 2。靜態督導查核權責區分須滿足規則 9：工作 T_i 具有督導查核工作 T_j 關係時，且工作 T_i 與工作 T_j 分別授權給角色 R_x 與 R_y，則角色 R_x 的職務位階必定高於角色 R_y 的職務位階。

規則 9：【靜態督導查核權責區分〈全部〉】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet,$ and $x \neq y, i \neq j$

$T_i \in authorized\_tasks(R_x)$ and $T_j \in authorized\_tasks(R_y)$ and $(T_i \succ Tj) \Rightarrow R_x \succ R_y$

上述表示式是所有授權可執行工作 T_i 的角色 R_x 皆高於可執行工作 T_j 的角色 R_y，但若組織的定義、限制只要存在一個較高層級的角色即可，即並非全部大於，則其督導查核關係的正規表示式可改爲規則 10：工作 T_i 具有督導查核工作 T_j 關係時，若角色 R_y 已授權可做工作 T_j，則必存在一個授權可執行工作 T_i 的角色 R_x，且此角色 R_x 的職務位階高於角色 R_y 的職務位階。

規則 10：【靜態督導查核權責區分〈存在一個〉】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet,$ and $x \neq y, i \neq j$

$\forall R_y(T_j \in authorized\_task(R_y))$ and $(T_i \succ T_j) \Rightarrow \exists R_x\ (T_i \in authorized\_task(R_x)$ and $R_x \succ R_y)$

㈡動態督導查核權責區分

動態督導查核權責區分除了需滿足依據工作權責衝突關係所制訂的動態工作權責區分準則，遵循規則 1 及規則 3（或是遵循放寬限制之規則 4 或規則 5），尚須滿足規則 11：人員 S_A 與 S_B 分別以角色 R_x 與 R_y 啓動執行工作 T_i 與工作 T_j，且工作 T_i 具有督導查核工作 T_j 的關係，則角色 R_x 的職務位階必須高於角色 R_y 的職務位階。

規則 11：【動態督導查核權責區分 - 啓動執行工作】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, S_A, S_B \in SubjectSet$ and $x \neq y, i \neq j$

$T_j \in active\_tasks(S_B, R_y)$ and $T_i \in active\_tasks(S_A, R_x)$ and $(T_i \succ T_j) \Rightarrow R_x \succ R_y$

若是督導查核關係，可彈性的針對存取特定物件，使工作具有「存取物件督導查核」關係，則權責區分準則如規則 12：人員 S_A 以角色 R_x 執行工作 T_i 去啓動存取物件 OBJ_m，人員 S_B 以角色 R_y 執行工作 T_j 去啓動存取物件 OBJ_n，且工作 T_i 存取物件 OBJ_m 有督導查核工作 T_j 存取物件 OBJ_n 的關係，則角色 R_x 的職務位階必須高於角色 R_y 的職務位階。

規則 12：【動態督導查核權責區分 - 啓動存取物件】

$\forall T_i, T_j \in TaskSet, R_x, R_y \in RoleSet, OBJ_m, OBJ_n \in ObjectSet, S_A, S_B \in SubjectSet$ and $x \neq y, i \neq j$

$OBJ_m \in$ active_objects(S_A, R_x, T_i) and $OBJ_n \in$ active_objects(S_B, R_y, T_j) and $T_i \ {}_{OBJm}\succ_{OBJn} \ T_j \Rightarrow R_x \succ R_y$

㈢相依執行督導查核權責區分

相依執行督導查核權責區分是針對執行時期相依性工作具督導查核關係所制訂的規範，於執行時期同時啓動擔任角色執行工作及存取物件，仍須依循動態督導查核權責區分之規則 11 與規則 12 。由於具備督導查核關係之工作亦具有工作權責衝突關係，因此，相依執行督導查核權責區分亦須依循動態工作權責區分及相依執行工作權責區分，即遵循規則 1 、規則 3 (或是放寬限制之規則 4 或規則 5) 及規則 6 。此外，相依執行督導查核權責區分尚須滿足規則 13 ：工作 T_j 已由人員 S_B 以角色 R_y 執行過，而工作 T_i 目前由人員 S_A 以角色 R_x 啓動執行，且工作 T_i 具有督導查核工作 T_j 的關係，並具備相依性，則角色 R_x 的職務位階必須高於角色 R_y 的職務位階。

規則 13 ：【相依執行督導查核權責區分】

$\forall T_i, T_j \in$ TaskSet, $R_x, R_y \in$ RoleSet, $S_A, S_B \in$ SubjectSet and $x \neq y, i \neq j, A \neq B$ $T_j \in$ executed_tasks(S_B, R_y) and $T_i \in$ active_tasks(S_A, R_x) and ($T_i \succ T_j$) and ($T_i \sim T_j$) $\Rightarrow R_x \succ R_y$

㈣相依存取物件督導查核權責區分

相依存取物件督導查核權責區分主要是針對執行時期相依性工作具有存取物件督導查核關係所制訂的規範，於執行時期同時啓動角色，仍須依循動態督導查核權責區分之規則 11 與規則 12 。由於具備存取物件督導查核關係亦具有存取物件工作權責衝突關係，因此，存取物件督導查核權責區分仍須依循動態工作權責區分及存取物件工作權責區分，即遵循規則 1 、規則 3 (或是放寬限制之規則 4 或規則 5) 及規則 8 。此外，存取物件督導查核權責區分尚須遵循規則 14 ：人員 S_B 以角色 R_y 執行工作 T_j 已存取過物件 OBJ_n ，人員 S_A 以角色 R_x 執行工作 T_i 去啓動存取物件 OBJ_m ， T_i 與 T_j 爲相依的工作，且工作 T_i 存取物件 OBJ_m 有督導查核工作 T_j 存取物件 OBJ_n 的關係，則角色 R_x 的職務位階必須高於角色 R_y 的職務位階。

規則 14 ：【相依存取物件督導查核權責區分】

$\forall T_i, T_j \in$ TaskSet, $R_x, R_y \in$ RoleSet, $OBJ_m, OBJ_n \in$ ObjectSet,

$S_A, S_B \in$ SubjectSet, and $x \neq y$, $i \neq j$, $A \neq B$

$OBJ_n \in$ accessed_objects(S_B, R_y, T_j) and $OBJ_m \in$ active_objects(S_A, R_x, T_i) and ($T_i \sim T_j$) and $T_i \ {}_{OBJm}\succ_{OBJn} \ T_j \Rightarrow R_x \succ R_y$

三、權責區分準則：依據非獨攬性工作權責

非獨攬性權責區分規範具非獨攬性工作權責的工作不可全部授權給同一個角色及人員，或是由同一個角色、人員執行。本文僅說明角色限制之權責區分準則，人員限制之權責區分準則與角色限制之權責區分準則類似，請參考文獻 (吳美玉 民 88) 。

㈠靜態非獨攬性權責區分

一個角色不可被授權執行所有相關的工作，依循規則 15 ：工作 T 至少存在兩個子工作 T_i 與 T_j ，其分別授權給不同的角色 R_x 與 R_y ，而工作 T 具有至少由兩個角色完成的非獨攬性工作權責，則表示角色 R_x 與角色 R_y 定非同一個角色，亦即 x 一定不等於 y 。

規則 15 ：【靜態非獨攬性權責區分－角色限制】

$\exists T_i, T_j, T \in TaskSet, \exists R_x, R_y \in RoleSet$, and $i \neq j$

$T_i, T_j \in T$ and $T_i \in$ authorized_tasks (R_x) and $T_j \in$ authorized_tasks(R_y) and $\sigma_{role}\, T \geq 2 \Rightarrow R_x \neq R_y$ (ie. $x \neq y$)

(二)動態非獨攬性權責區分

一個角色不可啓動執行所有相關的工作，依循規則 16 ：工作 T 包含一子工作 T_i ，而工作 T 具有至少由兩個角色完成的非獨攬性工作權責，則子工作 T_i 可交由角色 R_x 執行，表示存在另一子工作 T_j 已由角色 R_y 執行過，或是由角色 R_y 啓動執行，亦或是尚有一子工作 T_j 尚未被啓動執行，而該子工作已經授權給角色 R_y 。

規則 16 ：【動態非獨攬性權責區分－角色限制】

$\exists R_x, R_y \in RoleSet, T_i, T_j, T \in TaskSet$, and $i \neq j$

$T_i \in T$ and $\sigma_{role}\, T \geq 2$ and $T_i \in$ active_tasks(R_x)

$\Rightarrow \exists T_j \in T$ and $T_j \in$ executed_tasks (R_y) and $R_x \neq R_y$

或 $\exists T_j \in T$ and $T_j \in$ active_tasks(R_y) and $R_x \neq R_y$

或 $\exists T_j \in T$ and T_j not activated and $\exists R_y$ and $T_j \in$ authorized_tasks(R_y) and $R_x \neq R_y$

四、權責區分準則：依據協調合作關係

需要互相溝通協調以完成的工作可劃分爲多個子工作，協調合作中所規範的多個子工作與非獨攬性的多個子工作不同，非獨攬性的多個子工作間不一定存在有工作權責衝突關係，而協調合作關係中至少應存在兩個子工作間有工作權責衝突關係，亦即：

$\exists T_i, T_j, T \in TaskSet$ and $i \neq j$ and $T_i \in T$ and $T_j \in T$ and $\bowtie T \Rightarrow T_i \oplus T_j$

因此，爲達成協調合作的權責區分，至少需由兩個以上的部門、角色或人員相互協調、合作以完成該項工作，此外，具有督導查核、工作制衡或是存取物件等工作權責衝突關係之子工作，必須依據上述各對應之授權準則加以規範。協調合作權責區分準則對於人員與角色之限制與非獨攬性權責區分準則類似，詳細說明請參考文獻（吳美玉 1999）。

伍、分析與討論

在第肆節中，我們提出了以工作爲基礎的權責區分準則，但僅就單一工作之分派授權，本節進一步考慮角色階層性的繼承及工作的階層特性，來探討工作之分派授權。本節並且以本文所提出的權責區分準則，與相關文獻包括以角色與工作爲基礎的存取控制及以角色爲基礎的存取控制之權責區分準則，作一比較與分析。

一、角色與工作的階層性

在本研究中，授權準則的設計不僅僅考量角色的繼承性，並顧慮到工作的包含性，所謂角色的繼承性即上層的角色可以繼承下層角色的權限，我們可以角色與角色的指派來建構角色的階層性 (Sandhu & Munawer 1998) 。例如，總經理可繼承財務經理與採購經理的權限，而財務經理與採購經理又分別可繼承一般辦事員的權限。工作的階層性，即一個工作可以包含多個子工作。在第肆節所介紹的授權準則，僅就單一的角色與工作設計，如果能把角色與工作的階層性納入考量，將是一

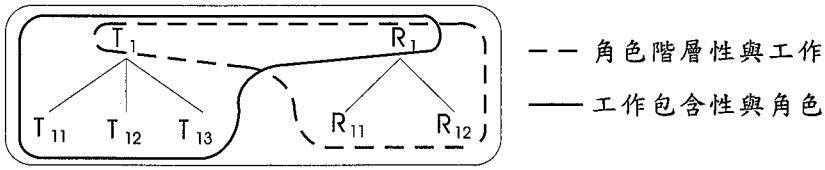

圖1：工作與角色之階層圖例

個較完整的授權準則規劃，對於企業內部的安全政策更能有效的控管，圖 1 爲一簡單的角色與工作階層圖。

在授權準則的設計中，仍可依據第肆節所述的觀念繼續擴充，如圖 1 中虛線所示，若角色 R_{11} 或角色 R_{12} 授權可執行工作 T_1 ，則因爲角色的繼承關係，角色 R_1 亦可執行工作 T_1 。而圖 1 中實線所示，因爲 T_1 包含三個子工作，所以 R_1 若被授權可執行工作 T_1 ，亦即同時可執行工作 T_1 的所有子工作 T_{11} 、 T_{12} ，及 T_{13} 。

此時若工作 T_{11} 與 T_{12} 屬靜態的工作權責衝突關係，又角色 R_{11} 與角色 R_{12} 分別可執行工作 T_{11} 與工作 T_{22} ，則表示角色 R_{11} 與 R_{12} 爲互相衝突關係，則角色 R_1 不可同時繼承執行角色 R_{11} 與角色 R_{12} 的權限。舉例說明，假設角色 R_1 爲銀行主管，而角色 R_{11} 是收款櫃員、角色 R_{12} 是放款櫃員，則角色 R_{11} 具有開立支票之權限，而角色 R_{12} 具有發出支票之權限。雖然角色 R_1 之位階位於角色 R_{11} 與 R_{12} 之上，可繼承下層角色 R_{11} 與角色 R_{12} 的權限，但是因爲兩者爲互相衝突的角色，所執行的工作亦屬工作權責衝突關係，所以該繼承將有所限制。

而在確立工作之間是否具有權責衝突關係時，若將工作的包含性考量進來，假設工作 T_1 包含有子工作 T_{11} 與 T_{12} ，工作 T_2 包含有子工作 T_{21} 與 T_{22} ，則設定含有階層性工作之權責區分的步驟可分爲二，一爲確立工作間的權責衝突，二即依據第肆節所述之授權準則以達到權責區分。若子工作 T_{11} 與子工作 T_{21} 具有工作權責衝突關係，則其上層之工作 T_1 與工作 T_2 亦具有工作權責衝突關係。若工作 T_1 與子工作 T_{21} 具有工作權責衝突關係，則工作 T_1 與工作 T_2 亦具有工作權責衝突關係，反之亦然。經由上述方式判斷正確的工作權責衝突關係，一旦確立兩兩工作間之權責衝突關係後，即可依據所需的權責區分程度，依第肆節所述之準則加以檢查規範。

二、分析比較

本研究針對以工作爲基礎的存取控制模式所設計之權責區分準則，符合了以角色與工作爲基礎的存取控制之權責區分規範，表 3 爲本研究所設計的權責區分準則與以角色爲基礎的存取控制（ RBAC ）的權責區分準則 (Simon & Zurko 1997) 之比較。

本研究所提出之靜態工作權責區分滿足 RBAC 模式中的靜態權責區分，相對的，本研究之動態工作權責區分、相依存取物件、非獨攬性與相依執行工作權責區分，分別滿足 RBAC 之動態權責區分與以物件爲基礎的動態權責區分、操作的動態權責區分，及以歷史資料爲基礎的動態權責區分，而本研究尚包括靜態、動態督導查核權責區分、相依執行督導查核、相依存取物件督導查核、靜態與動態協調合作權責區分等。

另外， Schier 安全模式 (Schier 1998) 雖已提出以角色與工作爲基礎的安全模式之概念，來設計權責區分準則，但僅僅是原來以角色爲基礎的存取控制之擴充，分

表3：以角色爲基礎的存取控制與本研究的權責區分準則之比較

RBAC之權責區分準則	本研究之權責區分準則
靜態權責區分	靜態工作權責區分
動態權責區分	動態工作權責區分
以物件爲基礎的動態權責區分	相依存取物件工作權責區分
操作的動態權責區分	非獨攬性權責區分
以歷史資料爲基礎的動態權責區分	相依執行工作權責區分
（未提供）	靜態、動態督導查核權責區分 相依執行督導查核權責區分、 相依存取物件督導查核權責區分 靜態、動態協調合作權責區分

表4：Schier安全模式(Schier 1998)與本研究的權責區分準則之比較

Schier之權責區分準則	本研究的權責區分準則
靜態權責區分	靜態工作權責區分
動態權責區分	動態工作權責區分
（未提供）	相依執行工作權責區分；相依存取物件工作權責區分 靜態督導查核權責區分；動態督導查核權責區分 相依執行督導查核權責區分；相依存取物件督導查核權責區分 靜態、動態非獨攬性權責區分；靜態、動態協調合作權責區分

別考量角色與工作的衝突，並直接指派給使用者，或是角色與工作的衝突設定，再一起指派給使用者。而在我們的模式中，是以工作權責衝突關係爲基礎，訂定相關的授權準則，由工作間之工作權責衝突關係，考量每個角色所能賦予的工作執行權限，進而決定每個使用者可以擔任的角色，如此一來，可以減少指派次數，並達到一致性。由表 4 可知， Schier 之模式中僅僅提供靜態與動態權責區分，而本研究尚有相依執行工作權責區分、相依存取物件工作權責區分、督導查核、非獨攬性、協調合作權責區分等。

陸、結論與未來研究

本研究提出新的分析觀點，從企業制訂工作的角度來分析不同之工作權責關係。主要思維是企業爲確保工作執行之正確性，達到稽核之目的，企業在制訂與規劃工作時，會制訂相對應權責之工作。本研究定義了工作相依性與工作權責衝突、督導查核及協調合作等工作權責關係。依此定義設計出權責區分之授權準則，由工

作間之工作權責衝突關係，考量每個角色所能賦予的工作執行權限，進而決定每個使用者可以擔任的角色。由不同的工作權責關係推導制訂的權責區分準則，包括靜態與動態工作權責區分、靜態與動態督導查核權責區分、相依執行權責區分等。所提出的權責區分準則兼顧以角色分派的優點，並補足工作變動性的特點，使企業對於工作相關的授權管理有所依據，對於職務的授權與工作的規劃有較完善的控管。

以角色與工作爲基礎的存取控制模式，可幫助在以工作爲基礎的環境中建立相關的權責區分，使其同時兼具存取控制與授權管制。藉由此授權模式的提出，可使企業對於管理內部工作的分派與授權，能更符合企業內部的安全政策，實現權責區分的政策。本文主要是就工作之授權分派建立授權準則，以滿足企業所需的權責區分政策，隨著產業競爭力的提升，企業會有新的工作或工作流程加入，未來之研究將進一步對於新增之工作或工作流程，設計符合權責區分準則之授權指派方法。

此外，對於不同的企業工作環境，會有不同的授權準則規範。如何設計完備的授權準則，以適用不同的企業工作環境，並以正規化方法證明其完備性與正確性，相當具有挑戰性。未來之研究將整合授權準則與工作爲基礎的存取控制機制，以實作一符合權責區分之企業資源存取控制系統，並實際應用在一企業工作環境中，進行安全性分析探討，並進一步探討如何以正規化方法證明授權準則之完備性與正確性。

致謝

本研究由教育部追求卓越計畫－「下一世代資訊通訊網路尖端技術及應用」，編號 89-E-FA04-1-4 之第九分項計畫之第四子計畫「以角色爲基礎的安全管理」所贊助

參考文獻

1. 吳美玉，指導教授：劉敦仁、黃景彰，『設計授權準則以達到在工作爲基礎的存取控制模式中之權責區分』，第十三屆龍騰論文經營管理類入選獎，得獎論文集， 1999.
2. 吳美玉、民 88 ，設計授權準則以達到在工作爲基礎的存取控制模式中之權責區分，國立交通大學資訊管理研究所碩士論文。
3. 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, December 1995, pp: 241-248.
4. David Ferraiolo, Richard Kuhn, "Role-Based Access Control", In Proceedings of 15th NIST-NCSC National Computer Security Conference, October 1992, pp: 554-563.
5. Elisa Bertino, Elena Ferrari, Vijayalakshmi Atluri, "A Flexible Model Supporting the Specification and Enforcement of Role-based Authorizations in Workflow Management Systems", RBAC 97 Workshop, 1997.
6. John Barkley, " Implementing Role Based Access Control Using Object Technology", First ACM Workshop on Role Based Access Control, November 1995.
7. Kathrin Schier, "Multifunctional Smartcards for Electronic Commerce-Application of the Role and Task Based Security Model", 14th Annual Computer

Security Applications Conference, December 1998.

8. Luigi Giuri, Pietro Iglio, "A Role-Based Secure Database Design Tool", Proceedings 12th Annual Computer Security Applications Conference, Dec 1996.
9. Mats Gustafsson, Benoit Deligny, Nahid Shahmehri, "Using NFS to Implement Role-Based Access Control", Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, June 1997.
10. 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.
11. Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, "Role-Based Access Control Models", IEEE Computer, 29(2), February 1996, pp: 38-47.
12. Ravi Sandhu, Qamar Munawer, "The RRA97 Model for Role-Based Administration of Role Hierarchies", ACSAC98 conference, December 1998.
13. Richard T. Simon, Mary Ellen Zurko, "Separation of Duty in Role-Based Environments", 10th Computer Security Foundations Workshop, June 10-12, 1997.
14. R. K. Thomas, R. S. Sandhu, "Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management", Proceedings of the IFIP WG11.3 Workshop on Database Security, August 11-13, 1997.
15. 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.
16. Workflow Management Coalition, "Workflow Management Coalition: Terminology & Glossary" , (http://www.aiim.org/wfmc/standards/docs/glossary.pdf)