公告本

申請日期	85. 10. 03.
案號	85112101
類別	G06F 17/00

（以上各欄由本局填註）

A4
C4

314609

發明 新型 專利說明書

一、發明新型名稱	中文	於一分配系統內對系統資源作安全控制存取之方法與系統
	英文	METHOD AND SYSTEM FOR SECURELY CONTROLLING ACCESS TO SYSTEM RESOURCES IN A DISTRIBUTED SYSTEM
二、發明創作人	姓名	1.丹尼 M. 奈賽特 2.狄龍 D. 脫克
	國籍	均美國
	住、居所	1.美國加州福瑞蒙市瓦巴希河街34810號 2.美國加州桑尼維爾市艾瓦拉路#100,1260號
三、申請人	姓名（名稱）	美商太陽微系統公司
	國籍	美國
	住、居所（事務所）	美國加州悠浮山加西亞街2550號
	代表人姓名	邁可·曲·摩里斯

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

美　國（地區）　申請專利，申請日期：1995.8.18.　案號：08/516,671，□有　□無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（ 1 ）

發明領域

本發明之方法與系統大抵有關於在計算機系統中提供安全性，尤其是關於利用一結合於一目標參考檔或目標能力檔之組識別符以控制對系統資源之存取。

發明背景

在一目標檔取向的系統中，一目標檔爲一包含資料與運算之元件，可召用以處理資料。將呼叫送入目標檔，於是在目標檔上產生運算(亦稱爲「方法」)。各目標檔爲一目標型式，定出可在該型目標檔上執行的運算。一目標檔型式可繼承其他目標檔型式所定義並執行的目標運算。對於目標檔取向的設計及程式技巧之進一步說明請見Bertrand Meyer之「目標檔取向之軟體構造」，Prentice-Hall 1988年版，本文納入作爲參考。

在客户-伺服器之計算中，通常有一組計算機可互相經一連接該等計算機之網路而通訊。這些計算機有些作用爲對其他計算機之服務或功能的提供者。服務或功能的提供者稱爲「伺服器」，服務或功能的消費者則稱爲「客户」。此客户-伺服器模式亦可推廣到同一計算機上運作的不同程式或程序，互相經由一些保護性機構而通訊，且分別作用爲功能之提供者與消費者。

在根據客户-伺服器模式之目標檔取向的分散式系統中，存有提供目標檔取向的介面予其客户之伺服器。這些伺服器支援以資料與相關軟體組成的目標檔以根據此型目標檔所允許的運算處理資料。客户可取得對這些目標檔之存取

五、發明說明（ 2 ）

，且可將呼叫傳送到伺服器而執行呼叫這些目標檔。在伺服器處這些呼叫經由與目標檔相關的軟體而執行，然後這些呼叫的結果傳回客户。

目前許多公司已同意將某些目標檔之定義與介面標準化，以便互相分享這些目標檔。一種設計成能加入此種公司間分享目標檔的系統稱爲「分散式目標檔環境」("DOE")，爲Sun Microsystems, Inc.[1]所建立。

DOE是一種目標檔取向的系統，提供由客户對DOE目標檔之遠距離存取。伺服器之應用檔則執行DOE目標檔。對於任一所予之DOE目標檔，一DOE伺服器可建立一目標參考檔作爲對DOE目標檔之指標。一DOE目標參考檔可在一機器上或在不同的機器間之不同的程序之間傳遞，且其仍指向原來的目標檔。

當一客户應用檔在一位置取得一DOE目標參考檔時，可送出呼叫(方法召用請求)至標的DOE目標檔，然後標的DOE目標檔可執行這些呼叫，可能是更新其內部狀態(其資料)，也可能是回送一些結果至其呼叫者。作爲處理一方法召用之一部分，一伺服器本身可召用其他目標檔，產生一連串之目標檔召請。

這些目標檔分享一些在使用者直接控制之外的實項，產

---

[1] Sun、DOE與Sun Microsystems, Inc.爲Sun Microsystems, Inc.在美國及其他國家之商標或註册商標。

五、發明說明（ 3 ）

生許多安全性的問題。比方說，若想要讓DOE使用者存取一些分散於一大組機器上的目標檔時，但基本上確定只有被授權的使用者才能存取這些目標檔，所以目標檔密封的資料不可由未經授權的使用者取得或改變。

對此種安全性問題的部分解決方法是，有些伺服器對其目標檔提供安全的存取，使只有適當指定的使用者才可存取這些目標檔。當一客户應用檔想要對一安全目標檔存取時，其必須對含有此安全目標檔之執行權的伺服器建立一種「鑑認連繫」。當建立此種連繫時，客户應用檔必須向伺服器證明那一個使用者的客户應用檔正提出。於是比方說此客户應用檔可以代表人類使用者Susan。(作爲進入客户計算機業務的一部分，稱爲Susan的人類使用者可能必須提供一些鑑認資訊如一通行密碼予客户計算機)。在建立了鑑認連繫之後，伺服器則確信所予之連繫爲對一已經授權代表一既定使用者之應用檔。伺服器將記錄此使用者的名字，並將此使用者的名字與既定之連繫相關聯。建立鑑認連繫之技術是眾所週知的，請見比方說「分散式系統中的鑑認：理論與實務」，Butler Lampson、Martin Abadi、Michael Burrows與Edward Wobber合寫，ACM Transactions on Computer Systems, 10(4), 1992年11月。

正常的DOE模式爲客户召用遠方目標檔上的運算。伺服器可要求該請求在一鑑認連繫上發出，且因此可使客户應用檔代表一已鑑認的使用者爲之生效。伺服器接著可進行核對看此已鑑認的使用者是否眞的已被授權進行此運算。

五、發明說明（ 4 ）

當使用者想要一伺服器執行一些要求伺服器進入一些其他的安全伺服器之動作時，複雜性立刻產生。比方說，一使用者可請求一客户應用程式取得一合成文件(例如一含試算表與解說文字之年度銷售報告)，其部分位於第一伺服器上(如文字說明)，部分在第二伺服器上(如圖表)，第一伺服器可鑑認該請求的使用者並驗證該使用者被授權作出請求，但若第一伺服器接著必須存取第二伺服器取得一些資料以完成使用者的請求時，第二伺服器必須鑑認第一伺服器，且必須確證第一伺服器由客户授權存取，或具有適當的存取許可以在目標檔上執行其所請求的動作。此種問題稱爲「委任問題」，只要當客户必須將其部分授權委任一伺服器以使其完成工作時就產生此一問題。

由使用者授權予一既定伺服器，在使用者的名字下動作以存取於一第二伺服器，此必須使用者信任許多機器，而讓這些機器的安全性受到侵襲，或使用者必須僅信任一小部分已知機器，這些機器嚴格限制使用者對所需目標檔之存取。同樣地，接受偏佈於網路上客户之存取請求對伺服器本身產生實質的安全性風險，因此想要發展一種改良的方法與系統以在一分散的網路環境中安全地委任存取控制權利。

本發明爲一種高妙而簡易的方法以解決一網路環境中分散式計算機系統中安全地處理來自各種伺服器之存取請求的問題，下面更加完整地加以說明。

發明總述

五、發明說明（ 5 ）

本發明各實例提供一種改良的方法與系統以在一分散式計算機系統中安全地控制對資源的存取。本發明一實例將一「組識別符」儲存結合於一標的目標檔，然後使用會員資格核對方式以決定代表一使用者而作業的請求對標的目標檔作存取的客户目標檔是否爲此組一會員。以這種方式，本發明避免執行昂貴的密碼作業以驗證請求目標檔的存取權利，如一些已往技術系統中一般使用者。

本發明第二實例將一「組識別符」儲存並結合於一標的目標參考檔，然後將此標的目標參考檔傳到系統中的客户目標檔。因爲標的目標參考檔含有一「組識別符」項目，一第一客户目標檔能夠決定系統中其他客户何者爲此識別組中的會員。此一決定使第一客户目標檔能將標的目標參考檔傳到該組其他會員，不必先與伺服器通訊以求得標的目標檔。以此方式，本發明避免了與伺服器通訊以求得標的目標檔的昂貴處理成本。

符號與專用名詞

下面的詳細說明大部分以計算機中資料位元上運算的方法與符號表示呈現。這些方法說明及符號表示爲資料處理技術中之專家所用的工具，以最有效果地將他們的工作內容傳達予該行其他專家。

本文中「方法」一詞一般爲一系列前後一致的步驟導致一所需結果者，這些步驟需要物理量的實質處理。這些物理量通常(但不必然)爲電或磁信號之形式，能加以儲存、轉移、合併、比較以及其他處理。稱這些信號爲位元、數

五、發明說明（ 6 ）

值、元件、符號、字符、詞語、數字等有時相當方便，主要的原因是一般慣用。但應記住，所有這些詞語及類似的詞語均與適當的物理量相關，且僅爲適用於這些物理量的合宜名稱。

執行本發明各種作業的有效機器包括通用型數位元計算機或類似裝置。通用計算機可以計算機中所存之計算機程式選擇性啓動或重組，也可使用一特殊用途計算機以執行本發明之作業。總而言之，使用本文所述及所提議之方法並不侷限於一種特別的計算機構造。

圖式簡述

圖1爲一實施本發明優選實例之計算機系統的方塊圖。

圖2爲一流程圖，說明第一實例用以安全地控制對系統資源之存取的較佳步驟。

圖3爲一流程圖，說明第二實例用以安全地控制對系統資源之存取的較佳步驟。

發明詳述

較佳方法之概述

本發明各實例提供一種改良的方法與系統以在一分散式計算機系統中安全地控制對資源的存取。本發明一實例將一「組識別符」儲存結合於一標的目標檔，然後使用會員資格核對方式以決定代表一使用者而作業的請求對標的目標檔作存取的客户目標檔是否爲此組一會員。以這種方式，本發明避免執行昂貴的密碼作業以驗證請求目標檔的存取權利，如一些已往技術系統中一般使用者。

五、發明說明（ 7 ）

本發明第二實例將一「組識別符」儲存並結合於一標的目標參考檔，然後將此標的目標參考檔傳到系統中的客户目標檔。因爲標的目標參考檔含有一「組識別符」項目，一第一客户目標檔能夠決定系統中其他客户何者爲此識別組中的會員。此一決定使第一客户目標檔能將標的目標參考檔傳到該組其他會員，不必先與伺服器通訊以求得標的目標檔。以此方式，本發明避免了與伺服器通訊以求得標的目標檔的昂貴處理成本。

較佳系統之概述

圖1爲一計算機系統100實施本發明優選實例之方塊圖。計算機系統100包括一計算機101、一輸入裝置103、一儲存裝置105、及一顯示裝置107。顯示裝置107顯示一繪圖的使用者介面(GUI) 109，GUI經由圖像(icon)呈現資訊，而使用者則藉指出圖像或處理圖像而召用命令。計算機101包含一處理器111、一記憶體113、及一介面115、介面115在處理器111與週邊裝置如輸入裝置103及顯示裝置107之間產生連通。

計算機記憶體含有許多項目包括一客户目標檔117、一合成文件伺服器目標檔119、及一試算表伺服器目標檔121，記憶體113的內容下面將詳加討論。

發明實例

本發明各種實例或許最好以例子加以說明，這裏所說明的兩個實例將在建立與印製一合成文件的情況下加以討論。一合成文件通常包含文字與圖表，比方說，一年度銷售

五、發明說明（ 8 ）

報告含有繪出年度銷售成長之圖表及解釋文字而成爲一種合成文件。通常圖表是在一試算表伺服器的控制下儲存，而合成文件的文字則在一合成文件伺服器的控制下儲存，再加上對圖表之連繫。

雖然這些例子是在一計算機內不同的程序之間進行，但本行一般專家將瞭解本文的教示對分散遍佈於一網路環境下的目標檔與程序同樣適用。

但在各實例中程序開始之前，計算機系統100內必須存有某些前置條件。假設一使用者(或本體)已成功上機且獲得系統100的資格，並已叫出客户目標檔117。本例中，客户目標檔117一般對應於一含文字處理應用程式之程序，本體資格接著與客户目標檔117一起儲存以指示目標檔117是代表本體而動作。而且，此本體與一組在計算機系統100上具有存取特權的其他本體相關連，比方說，一銷售員可與銷售部門的一組人員相關連。系統100中所定義的各組均有一獨一的組識別符與其關聯，此外一種檢查會員資格的機構(如機構123)必須存在以決定一代表本體而動作的目標檔是否爲一特定組別的會員。任何習知的方法或系統以執行會員資格機制者均可加以使用以執行系統100的此種情況。

第一實例

圖2爲一流程圖，說明第一實例用以安全地控制對系統資源存取之優選步驟，圖2的步驟一般均回應於使用者之輸入而起始。假設本體在客户檔117上起始一請求以建立一試算表(步驟201)，回應於此輸入，客户目標檔117送出一建

五、發明說明（ 9 ）

立請求到試算表伺服器目標檔(步驟203)，此請求指示一試算表目標檔應立即起始，此請求並含與使用者相關的組識別符，合成文件伺服器以之代表使用者而作業。

試算表伺服器目標檔接受請求而建立試算表目標檔(步驟205)，接著試算表伺服器目標檔將試算表目標檔與組識別符一起儲存，再加上該組會員相對於試算表目標檔所具有的存取權利指示(步驟207)。最後，試算表伺服器目標檔產生一無法僞造的號碼，並將此無法僞造的號碼與試算表目標檔一起儲存(步驟209)。以這種方式，當一客户目標檔提出一無法僞造的號碼，請求對伺服器目標檔作存取時，試算表伺服器目標檔可作出一些保證使請求的客户能具有存取試算表目標檔的權力。此無法僞造的號碼通常稱爲「能力」(capability)。一無法僞造的號碼是難以用計算方式決定的。

試算表伺服器目標檔接著將一試算表目標參考檔送至客户目標檔117(步驟211)。此優選實例中，試算表目標參考檔包含前次產生的無法僞造的號碼。

一旦試算表伺服器目標檔將程序控制還給客户目標檔時，客户目標檔找到一代表該組一本體作業的合成文件伺服器(步驟213)。其次，客户目標檔送出一請求到合成文件伺服器119以建立一合成文件(步驟215)。建立請求含有一種合成文件應建立之指示，建立請求亦含有試算表目標參考檔，使合成文件伺服器知道那一個試算表目標檔納入於其合成文件中。最後，建立請求含有一所選的組識別符，使

五、發明說明（ 10）

合成文件伺服器稍後能決定一請求對合成文件存取的本體是否被授權存取該合成文件。

合成文件伺服器建立合成文件，並將試算表目標參考檔與組識別符儲存於合成文件中(步驟217)。其次，合成文件伺服器產生一無法偽造的號碼並將此無法偽造的號碼與合成文件目標檔一起儲存，以這種方式，當由客户目標檔提出一無法偽造的號碼，請求對合成文件目標檔存取時，合成文件伺服器目標檔可作出一些保證使請求的客户具有存取合成文件目標檔的權利。

合成文件伺服器目標檔119接著將一合成文件目標參考檔送到客户目標檔117(步驟219)。此優選實例中，合成文件目標參考檔包含由合成文件伺服器目標檔所產生的無法偽造的號碼。

在隨後一些即時點上，客户目標檔送出一印出請求到合成文件伺服器(步驟221)，印出請求將合成文件參考檔與客户本體的識別符傳到合成文件伺服器。客户使用任何習知的鑑認機構對合成文件伺服器證明其具有代表客户本體作業的權利。將合成文件參考檔與客户本體之識別符傳到合成文件伺服器，合成文件伺服器於是能夠決定印出那一合成文件，並可驗證該客户目標檔117是否獲得許可印出合成文件，方式是檢查建立合成文件時所規定的屬於該組的鑑認識別符，並將目標參考檔中無法偽造的號碼與目標檔中無法偽造的號碼比較。

爲了印出合成文件，合成文件伺服器必須具有與試算表

五、發明說明（ 11）

目標檔相關的資料，因此合成文件伺服器送出一取得資料請求至試算表伺服器(步驟223)。取得資料請求含有試算表目標參考檔，於是試算表伺服器知道那一個試算表目標檔由其檢索資料。取得資料請求並含本體的識別符，合成文件伺服器以之代表本體而作業。

合成文件伺服器將對試算表伺服器自我鑑認(步驟225)。任何習知的鑑認本體的技巧均可用以執行申請者實例此種情況。若合成文件伺服器成功地加以鑑認了，則試算表伺服器企圖決定合成文件伺服器是否具有存取權力，使它能由試算表目標檔檢索資料。爲決定存取權力，試算表伺服器由試算表目標檔檢索組識別符，試算表伺服器接著送出組識別符與鑑認的本體識別符至會員資格機構123，再加上一請求決定該鑑認的本體是否爲該組之會員，具有對試算表目標檔存取的權利(步驟227)。任何習知的檢查組會員資格的機構均可用以執行申請者實例之此種情況。

若合成文件伺服器的鑑認本體爲所規定組別的會員，則試算表伺服器再作出另一核對以確定該合成文件被授權存取試算表目標檔。試算表伺服器由試算表伺服器參考檔檢索該無法僞造的號碼，並將之與試算表伺服器目標檔內儲存的無法僞造的號碼比較(在一優選實例中此步驟最好第一個執行)(步驟229)。若兩無法僞造的號碼符合，則試算表伺服器容許合成文件伺服器由試算表目標檔檢索必須的資料，接受目標檔所存的存取權利(步驟231)。

一旦檢出了試算表資料，合成文件伺服器送出合成文件

五、發明說明（ 12 ）

資料到一印表伺服器印出(步驟233)。

關於第一實例其中一種好處是無需密碼作業以決定是否請求對目標檔作存取的客户被授權存取該目標檔，而是第一實例在試算表目標檔的狀態資料中維持一「組識別符」，然後使用該「組識別符」決定該代表使用者作業的請求客户是否爲該適當組別的會員，而完成此種授權核對。此種組別會員資格核對執行起來一般比密碼作業便宜。

第一實例的另一優點爲試算表伺服器只用試算表目標檔所維持的狀態資料即可決定誰已存取一既定目標檔。在其他已往技術之執行中，這是不可能的，因爲只有目標參考檔儲存存取權利資訊，存取權利資訊並未與目標檔本身一起儲存。

第二實例

圖3之流程圖說明第二實例用以安全控制對系統資源之存取的優選步驟。圖3的步驟通常回應於使用者之輸入而起始，假設本體在客户檔117起始一請求而建立一試算表(步驟301)，回應於此輸入，客户目標檔117送出一「建立」請求至試算表伺服器目標檔(步驟303)，此請求指示一試算表目標檔應立即起始，此請求並含與該主體相關的組識別符，代表主體使合成文件伺服器作業。

試算表伺服器目標檔接受該請求，並建立試算表目標檔(步驟305)，然後試算表伺服器目標檔將一試算表目標參考檔送到客户目標檔117(步驟307)。第二實例中，試算表目標參考檔包含組識別符與建立請求一起送出，爲一指示該

五、發明說明（ 13 ）

組存取特權之項目，及一試算表目標檔識別符。試算表目標參考檔可經由一密碼單向混雜功能在目標參考資料上產生一密碼核對和，此密碼核對和並與試算表目標參考檔連在一起或存入其中，於是試算表目標參考檔具有較高的防偽性。

一旦試算表目標檔伺服器將程序控制還給客户目標檔，客户目標檔送出一請求至合成文件伺服器119以建立一合成文件(步驟309)。建立請求含有一合成文件應予建立之指示，建立請求並含試算表目標參考檔，使合成文件伺服器知道那一個試算表目標檔併入其合成文件。最後，建立請求含有一所選的組識別符，使合成文件伺服器能決定一代表某些主體請求對合成文件存取的目標檔是否被授權存取該合成文件。

合成文件伺服器建立合成文件，並將試算表目標參考檔存入合成文件(步驟311)，合成文件伺服器目標檔119接著送出一合成文件目標參考檔至客户目標檔117(步驟313)。在第二實例中，合成文件目標參考檔包含組識別符，一指示該組中各該存取權利之項，一合成文件識別符，及一由合成文件伺服器在建立合成文件參考檔時所產生的密碼核對和。

稍後客户目標檔及時送出一印出請求到合成文件伺服器(步驟315)，印出請求將合成文件參考檔與客户本體的身分傳到合成文件伺服器，客户使用任何習知的鑑認機制對合成伺服器證明其具有代表客户本體作業的權利(步驟317)。

五、發明說明（ 14 ）

以此方式合成文件伺服器瞭解要印出那一合成文件，並可用下面詳述的密碼核對和驗證客户目標檔117可否印出合成文件。

爲了印出合成文件，合成文件伺服器必須具有與試算表目標檔相關的資料，因此合成文件伺服器送出一「取得資料」。請求至試算表伺服器(步驟319)。取得資料請求含有試算表目標參考檔，使試算表伺服器知道試算表目標檔由其檢索資料，取得資料請求並含本體之身分，代表本體使合成文件伺服器作業。

試算表伺服器鑑認合成文件伺服器(步驟321)，任何習知的鑑認本體之技巧均可使用以執行申請者第二實例之此種情況。若成功鑑認了合成文件伺服器，則試算表伺服器企圖決定合成文件伺服器是否具有存取權利使其能由試算表目標檔檢索資料(步驟323)。爲決定存取權利，試算表伺服器檢索與試算表目標參考檔有關的組識別符，然後試算表伺服器由試算表目標參考檔檢索試算表識別符，最後，試算表伺服器將所檢出的資訊送到會員資格機構123，加上一請求以決定該鑑認之本體是否爲該識別組之一會員，而具有對試算表目標檔之存取權利。任何習知的檢查組會員資格之機構均可使用以執行申請者第二實例之此種情況。

若鑑認的本體爲該識別組之一會員，則試算表伺服器再作出另一檢查以確證該合成文件被授權存取該試算表目標檔。試算表伺服器由試算表目標參考檔檢索密碼核對和，然後爲試算表目標檔重新計算密碼核對和(步驟325)。其次

五、發明說明（15）

，試算表伺服器將所檢出的核對和與重新計算的核對和比較(步驟327)，若兩核對和符合，則試算表伺服器允許合成文件伺服器由試算表目標檔檢索必需的資料，並接受目標參考檔中存取之權利。

一旦檢索了試算表資料，合成文件伺服器將合成文件資料送到印表伺服器印出(步驟329)。

第二實例其中一好處爲客户目標檔藉維持何組被授權使用目標參考檔之狀態，以及那些其他會員在此組之內，可將與該組相關的目標參考檔傳到該組中另一本體，不必與伺服器作任何訊息交換。避免與試算表伺服器之此種交互作用可改進性能與效率。

修正例

雖然爲了說明這裏已經描述了幾個特別實例，但在不偏離本發明精神與範圍下可作出各種修正，因此本發明並不侷限於上述各實例。

比方說，該兩實例根據目前技術所廣爲習知的技術有許多方式可加以修正。第一實例中，組識別符可以不只是存在目標檔內，而且可以與目標參考檔一起送出作爲對客户之一暗示，當目標參考檔傳到第二客户時，此暗示可用以將一與伺服器交換之訊息旁路，第一客户可檢查第二客户是否在此組之內。若無此暗示，第一客户必須由伺服器請求組識別符，因而涉及了訊息交換。

第二實例中，伺服器可快取目標參考檔與目標檔，當它們都呈現以供使用時。在一後續的呈現時，伺服器可將客

五、發明說明（ 16 ）

户所送出的目標參考檔與快取記憶體中的核對，此意即爲若目標參考檔由同一組中一不同客户所提出，則伺服器不必重新計算密碼核對和，此將減少伺服器爲該存取所作之計算，因此增加其性能。

四、中文發明摘要（發明之名稱：於一分配系統內對系統資源作安全控制存取之方法與系統）

本發明各實例提供一種改良的方法與系統以在一分散式計算機系統中對資源作安全控制存取。本發明一實例將一「組識別符」儲存並結合於一標的目標檔，然後使用會員資格核對方式決定一請求對標的目標檔作存取之客户目標檔是否爲具有對標的目標檔存取權利之該組會員。以此方式，本發明避免進行昂貴的密碼作業以驗證請求目標檔之存取權利，如一些已往技術系統中一般使用者。

本發明第二實例將一「組識別符」儲存並結合於一標的目標參考檔，然後將此標的目標參考檔傳到系統中的客户目標檔。因爲標的目標參考檔含有一「組識別符」項目，

，

英文發明摘要（發明之名稱：METHOD AND SYSTEM FOR SECURELY CONTROLLING ACCESS TO SYSTEM RESOURCES IN A DISTRIBUTED SYSTEM）

Embodiments of the present invention provide an improved method and system for securely controlling access to resources in a distributed computer system. One embodiment of the present invention stores and binds a group identification to a target object and then uses membership checking to determine whether a client object which requests access to the target object is a member of a group with access rights to the target object. In this way, the present invention avoids performing costly cryptographic operations in order to verify access rights of requesting objects, as was common in some prior art systems.

A second embodiment of the present invention stores and binds a group identification to a target object reference and then passes the target object reference to client objects in the system. Since the target object reference includes a group identification entry, a first client object is able to determine which other clients in the system are members of the identified group. This determination allows the first client object to pass the target object reference to the other members of the group without first communicating with the server for the target object. In this way, the present invention avoids the costly transaction costs of communicating with the server for the target object.

A5
B5

四、中文發明摘要（發明之名稱：　　）

一第一客户目標檔能夠決定系統中其他客户何者爲此識別組中的會員。此一決定使第一客户目標檔能將標的目標參考檔傳到該組其他會員，不必先與伺服器通訊以求得標的目標檔。以此方式，本發明避免了與伺服器通訊以求得標的目標檔的昂貴處理成本。

英文發明摘要（發明之名稱：　　）

六、申請專利範圍

1. 一種在一分散式計算機系統中用以控制對系統資源之存取而在一計算機系統中執行的方法，該方法包含步驟如下：

由一客户目標檔送出一請求到一試算表伺服器，以將一「組識別符」結合於一試算表目標檔：

在該試算表伺服器的控制下，

取得一試算表目標檔；

將組識別符與試算表目標檔一起儲存：

產生一無法僞造的核對和；

將該無法僞造的核對和與試算表目標檔一起儲存；

將該無法僞造的核對和送到客户目標檔：

在該客户目標檔的控制下，

送出一請求至合成文件伺服器以印出一合成文件；

在合成文件伺服器的控制下，

送出一請求至試算表伺服器，請求試算表伺服器從一試算表目標檔送回資料，該請求含有一「組識別符」及該無法僞造的核對和：

在試算表伺服器的控制下，

基於該「組識別符」之分析，允許或拒絕對試算表目標檔之存取。

2. 一種在一分散式計算機系統中便於對系統資源作存取控制而在一計算機系統中執行的方法，該分散式計算機系統含一客户目標檔，一第一伺服器目標檔、一標的目標檔、及一第二伺服器目標檔，各目標檔屬於計算機系統

六、申請專利範圍

中所有之一或多個目標檔之特定組別，該方法包含步驟如下：

在第一伺服器目標檔的控制下，

將一「組識別符」與目標檔一起儲存，該「組識別符」識別系統中對標的目標檔具有存取特權該組目標檔；

在第二伺服器目標檔的控制下，

取得一容器目標檔；

送出一請求至第一伺服器目標檔請求對標的目標檔作存取，該請求含一本體識別符，其識別一主體，第二伺服器目標檔代表該主體而作業；以及

在第一伺服器的控制下，

使用標的目標檔中所存的組識別符與來自第二伺服器之請求中所含之本體識別符而驗證該第二伺服器是否能存取該標的目標檔。

3. 根據申請專利範圍第2項之方法，其中取得容器目標檔之步驟並含步驟如下：

在第一伺服器目標檔的控制下，

送出一標的目標參考檔至客戶目標檔，標的目標參考檔指示標的目標檔在計算機系統中之位置；

在客戶目標檔的控制下，

找出客戶目標檔所屬之代表該組一會員而作業的第二伺服器；

送出一請求至所找到之第二伺服器，請求第二伺服

六、申請專利範圍

器取得一參照標的目標檔之容器目標檔，由客户目標檔對第二伺服器目標檔之請求含有標的目標參考檔，該請求並含一「組識別符」，以資識別該客户目標檔所屬之組：

在第二伺服器的控制下，

取得該容器目標檔；以及

將標的目標參考檔與組識別符儲存於容器目標檔中。

4. 根據申請專利範圍第2項之方法，其中由第二伺服器將請求送至第一伺服器之步驟並含步驟如下：

在客户目標檔的控制下，

送出一請求至第二伺服器以使用該容器目標檔，該請求含有該客户目標檔之參考檔及該客户目標檔本體之識別符；以及；

在第二伺服器的控制下，

回應於來自客户目標檔之請求，送出一請求至第一伺服器以存取標的目標檔，該請求含有標的目標檔之參考檔及第二伺服器代表作業的本體之識別符。

5. 根據申請專利範圍第4項之方法，並含步驟如下：

在第一伺服器的控制下，

使用由第二伺服器送到第一伺服器之本體身分鑑認第二伺服器。

6. 根據申請專利範圍第5項之方法，並含步驟如下：

當鑑認了第二伺服器，並確定爲具有對標的目標檔存

六、申請專利範圍

取權利之該組一會員時，以下述之請求方式決定第二伺服器是否被授權存取該標的目標檔，

由第一伺服器之參考檔檢索一無法偽造的號碼，

將該檢出的無法偽造的號碼與標的目標檔所存的一無法偽造的號碼比較，以及

當該兩無法偽造的號碼符合時，允許第二伺服器存取標的目標檔，接受第二伺服器之存取權利。

7. 根據申請專利範圍第2項之方法，其中驗證該第二伺服器可否存取標的目標檔之步驟並含步驟如下：

在第一伺服器的控制下，

由標的目標檔檢索該「組識別符」；

將檢出的組識別符與本體識別符送出一會員資格機構，加上一請求以決定該本體是否爲具有對標的目標檔存取權利之該組會員；以及

當決定第二伺服器將代表一本體作業，而該本體爲對標的目標檔具有存取權利之該組會員時，允許第二伺服器存取標的目標檔。

8. 根據申請專利範圍第2項之方法，並含步驟如下：

由客户目標檔送出一請求至第一伺服器目標檔，該請求指示第一伺服器目標檔應建立標的目標檔；以及

在第一伺服器目標檔的控制下，

建立標的目標檔；且

儲存該組會員相對於標的目標檔所擁有之存取權利指示。

六、申請專利範圍

9. 一種計算機系統，用以在一分散式計算機系統中便於對系統資源作存取控制，該分散式計算機系統含一客户目標檔，一第一伺服器目標檔、一標的目標檔及一第二伺服器目標檔，各目標檔屬於該計算機系統中所具有之一或多個特定目標檔組，該系統包含：

第一伺服器目標檔構組成，

將一「組識別符」與標的目標檔一起儲存，該「組識別符」識別系統中對標的目標檔具有存取特權的目標檔組；

第二伺服器目標檔構組成，

取得一容器目標檔；

送出一請求至第一伺服器目標檔請求存取標的目標檔，該請求含有一本體識別符以識別一主體，第二伺服器目標檔代表該本體而作業；以及

第一伺服器構組成，

使用標的目標檔所存的組識別符及來自第二伺服器之請求中所含之本體識別符驗證該第二伺服器是否可以存取該標的目標檔。

10. 根據申請專利範圍第9項之系統，其中取得該容器目標檔並含一系統，其中：

第一伺服器目標檔構組成，

送出一標的目標參考檔至客户目標檔，該標的目標參考檔指示標的目標檔在計算機系統中的位置；

客户目標檔構組成，

六、申請專利範圍

找出一第二伺服器，其代表客户目標檔所屬組別一會員而作業；以及

送出一請求至所找出的第二伺服器，請求第二伺服器取得一參照標的目標檔之容器目標檔，由客户目標檔對第二伺服器目標檔之請求含有標的目標參考檔，該請求並含有一「組識別符」識別客户目標檔所屬之組別；以及

第二伺服器構組成，

取得容器目標檔；以及

將標的目標參考檔與組識別符存入該容器目標檔。

11. 根據申請專利範圍第9項之系統，其中由第二伺服器送出請求至第一伺服器並含一系統，其中：

客户目標檔構組成，

送出一請求至第二伺服器以使用容器目標檔，該請求含有容器目標檔之參考檔及客户目標檔本體之識別符；以及

第二伺服器構組成，

回應於來自客户目標檔之請求，送出一請求到第一伺服器以存取標的目標檔，該請求含有標的目標檔之參考檔以及該本體之識別符，第二伺服器代表該本體而作業。

12. 根據申請專利範圍第11項之系統，並含：

第一伺服器構組成，

使用由第二伺服器送至第一伺服器之本體身分鑑認

六、申請專利範圍

第二伺服器。

13. 根據申請專利範圍第12項之系統，並含許多機構構組成：

當鑑認了第二伺服器並確定爲具有存取標的目標檔權利之組別之會員時，確定第二伺服器是否以下述請求方式被授權存取標的目標檔，

由第一伺服器之參考檔檢索一無法僞造的號碼；

將所檢出的無法僞造的號碼與存於標的目標檔之一無法僞造的號碼比較；以及

當該兩無法僞造的號碼符合時，允許第二伺服器存取標的目標檔，接受第二伺服器之存取權利。

14. 根據申請專利範圍第9項之系統，其中驗證第二伺服器可否存取標的目標檔並含一系統，其中：

第一伺服器構組成，

由標的目標檔檢索組識別符；

將所檢出的組識別符與本體識別符送至一會員資格機構，加上一請求決定該本體是否爲具有對標的目標檔存取權利之該組會員；以及

當確定第二伺服器代表一本體作業，而該本體爲該組具有對標的目標檔存取權利之會員時，允許第二伺服器存取標的目標檔。

15. 根據申請專利範圍第9項之系統，並含許多機構構組成：

由客户目標檔送出一請求至第一伺服器目標檔，該請

六、申請專利範圍

求指示第一伺服器目標檔應建立標的目標檔；以及

其中第一伺服器目標檔構組成，

建立標的目標檔；及

儲存該組會員相對於標的目標檔所具有之存取權利指示。

16. 一種計算機程式，用以在一分散式計算機系統中便於對系統資源作存取控制，該分散式計算機系統含有一客戶目標檔，一第一伺服器目標檔、一標的目標檔及一第二伺服器目標檔，各目標檔屬於計算機系統中所有之一或多個特定的目標檔組，該程式包含：

第一伺服器目標檔之代碼，構組成，

將一「組識別符」與標的目標檔一起儲存，該「組識別符」識別系統中對標的目標檔具有存取特權之目標檔組；

第二伺服器目標檔之代碼，構組成，

取得一容器目標檔；

送出一請求至第一伺服器目標檔請求存取標的目標檔，該請求含有一本體識別符，其識別第二伺服器目標檔所代表作業之本體；以及

第一伺服器之代碼，構組成，

使用標的目標檔中所存之組識別符及來自第二伺服器之請求中所含之本體識別符驗證該第二伺服器可否存取標的目標檔；

其中這些代碼的儲存於一有形之媒體上。

六、申請專利範圍

17. 根據申請專利範圍第16項之程式，其中取得該容器目標檔並含：

第一伺服器目標檔之代碼，構組成，

送出一標的目標參考檔至客户目標檔，該標的目標參考檔指示標的目標檔在計算機系統中之位置；

客户目標檔之代碼，構組成，

找出代表客户目標檔所屬之組別一會員而作業之第二伺服器；以及

送出一請求至所找出之第二伺服器請求第二伺服器取得一參照標的目標檔之容器目標檔，由客户目標檔對第二伺服器目標檔之請求含有標的目標參考檔，該請求並含有一「組識別符」，其識別客户目標檔所屬之組別；以及

第二伺服器之代碼，構組成，

取得容器目標檔；以及

將標的目標參考檔與組識別符存入該容器目標檔。

18. 根據申請專利範圍第16項之程式，其中由第二伺服器送出請求至第一伺服器並含：

客户目標檔之代碼，構組成，

送出一請求至第二伺服器以使用容器目標檔，該請求含有容器目標檔之參考檔及客户目標檔本體之識別符；及

第二伺服器之代碼，構組成，

回應於來自客户目標檔之請求，送出一請求到第一

六、申請專利範圍

伺服器以存取標的目標檔，該請求含有標的目標檔之參考檔及第二伺服器所代表作業之本體識別符。

19. 根據申請專利範圍第18項之程式，並含：

第一伺服器之代碼，構組成，

使用由第二伺服器送至第一伺服器之本體身分鑑認第二伺服器。

20. 根據申請專利範圍第19項之程式，並含代碼構組成：

當鑑認了第二伺服器並確定爲該組對標的目標檔具有存取權利之一會員時，以下述所請求之方式確定第二伺服器是否被授權存取標的目標檔，

爲第一伺服器由參考檔檢索一無法僞造的號碼：

將所檢出的無法僞造的號碼與標的目標檔所存之一無法僞造的號碼比較；以及

當兩無法僞造的號碼符合時，允許第二伺服器存取標的目標檔，接受第二伺服器之存取權利。

21. 根據申請專利範圍第16項之程式，其中驗證第二伺服器可否存取標的目標檔並含：

第一伺服器之代碼，構組成，

由標的目標檔檢索組識別符；

將所檢出的組識別符與本體識別符送到一會員資格機構，加上一請求決定該本體是否爲該組對標的目標檔具有存取權利之一會員；以及

當確定第二伺服器代表該組具有對標的目標檔存取權利之一會員之本體作業時，允許第二伺服器存取標的目

六、申請專利範圍

標檔。

22. 根據申請專利範圍第16項之程式，並含代碼構組成：

由客戶目標檔送出一請求至第一伺服器目標檔，該請求指示第一伺服器目標檔應建立標的目標檔；以及

其中第一伺服器目標檔之代碼構組成，

建立標的目標檔；及

儲存該組會員相對於標的目標檔所具有之存取權利指示。

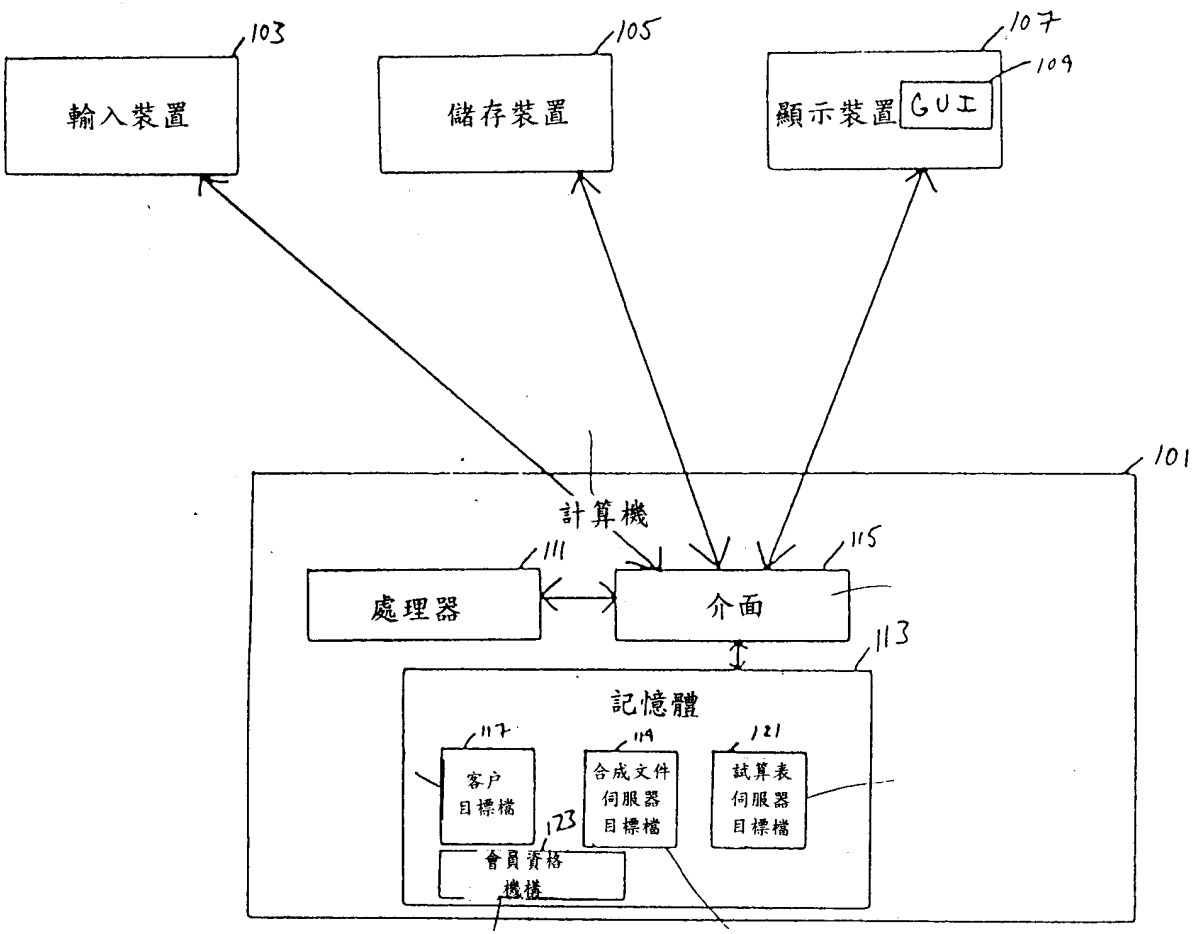
100
103
輸入裝置
105
儲存裝置
107
顯示裝置
109
GUI
101
計算機
111
處理器
115
介面
113
記憶體
117
客戶
目標檔
119
合成文件
伺服器
目標檔
121
試算表
伺服器
目標檔
123
會員資格
機構

圖 1

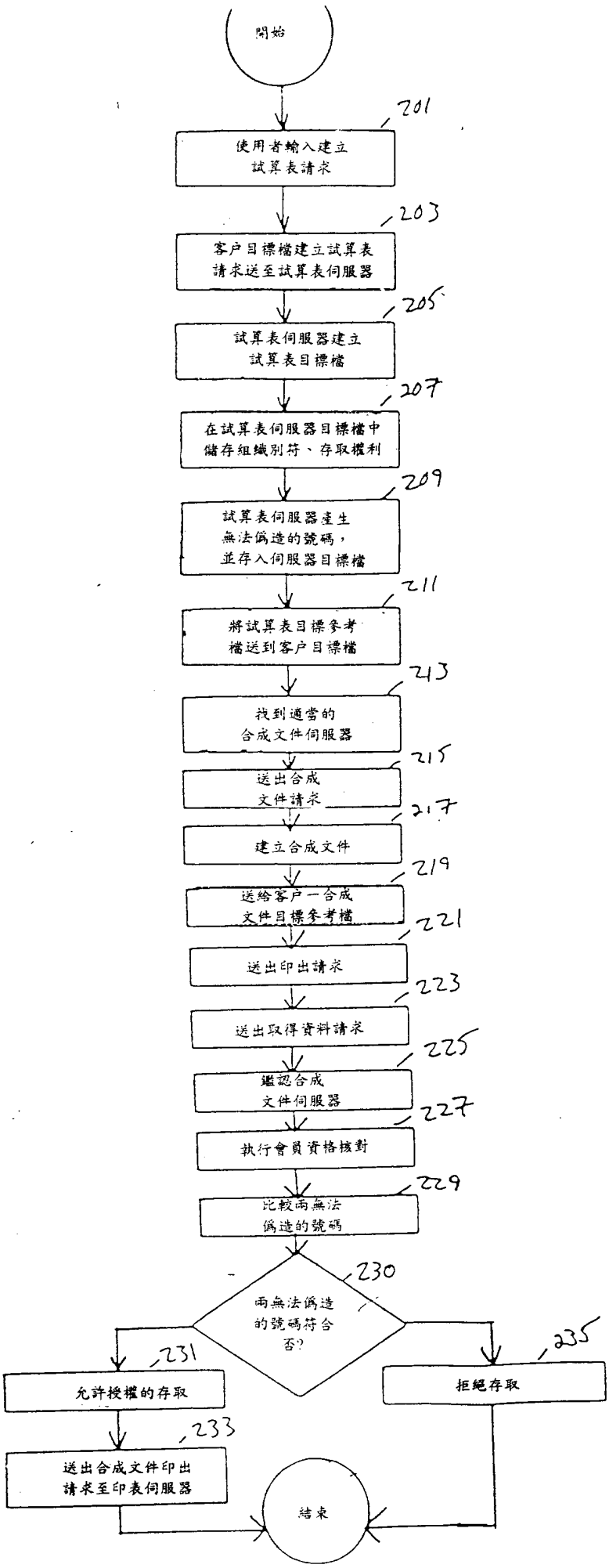
開始
201
使用者輸入建立試算表請求
203
客戶目標檔建立試算表請求送至試算表伺服器
205
試算表伺服器建立試算表目標檔
207
在試算表伺服器目標檔中儲存組織別符、存取權利
209
試算表伺服器產生無法偽造的號碼，並存入伺服器目標檔
211
將試算表目標參考檔送到客戶目標檔
213
找到適當的合成文件伺服器
215
送出合成文件請求
217
建立合成文件
219
送給客戶一合成文件目標參考檔
221
送出印出請求
223
送出取得資料請求
225
鑑認合成文件伺服器
227
執行會員資格核對
229
比較兩無法偽造的號碼
230
兩無法偽造的號碼符合否?
231
允許授權的存取
233
送出合成文件印出請求至印表伺服器
235
拒絕存取
結束

圖 2

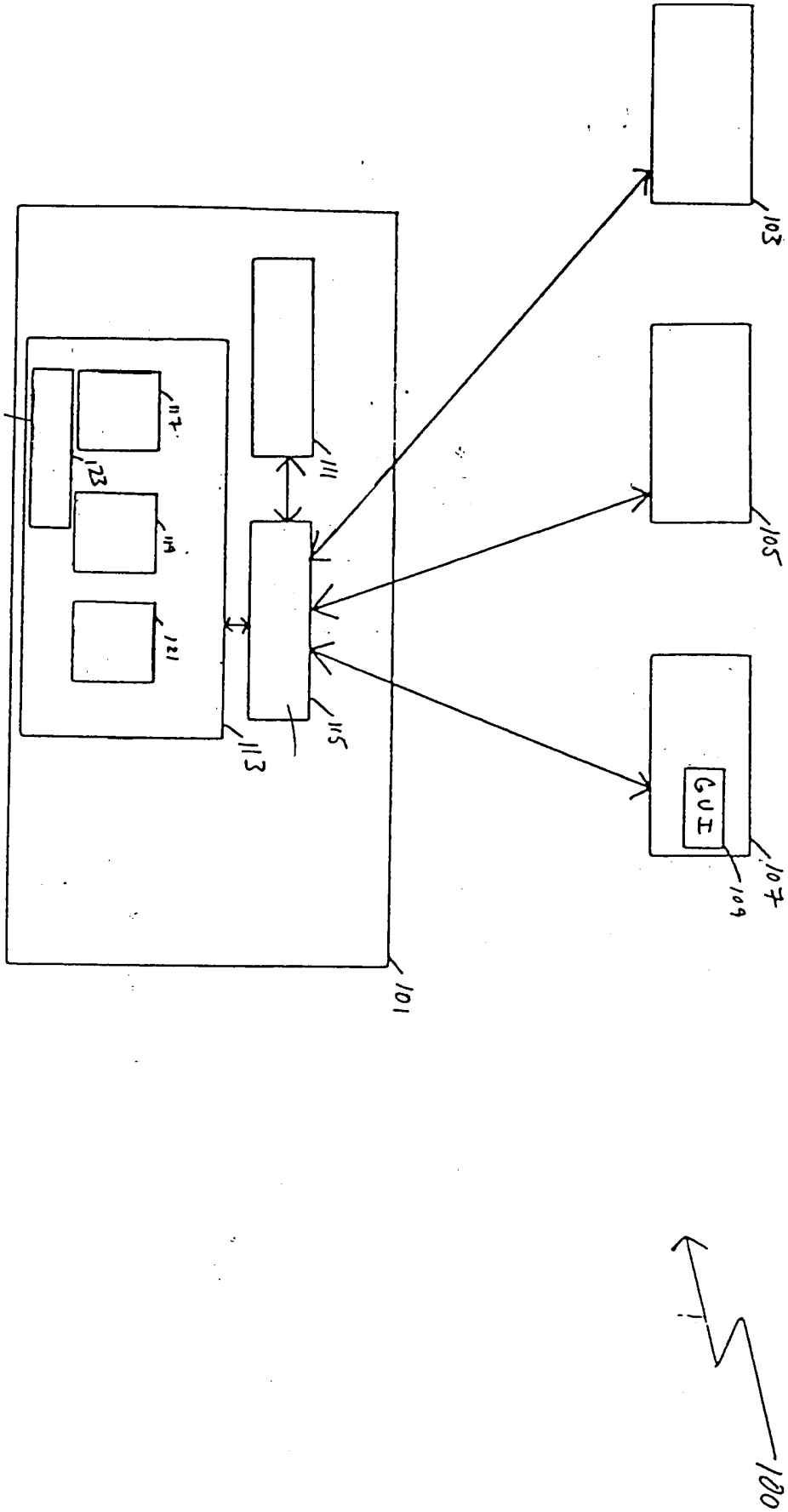

圖 1

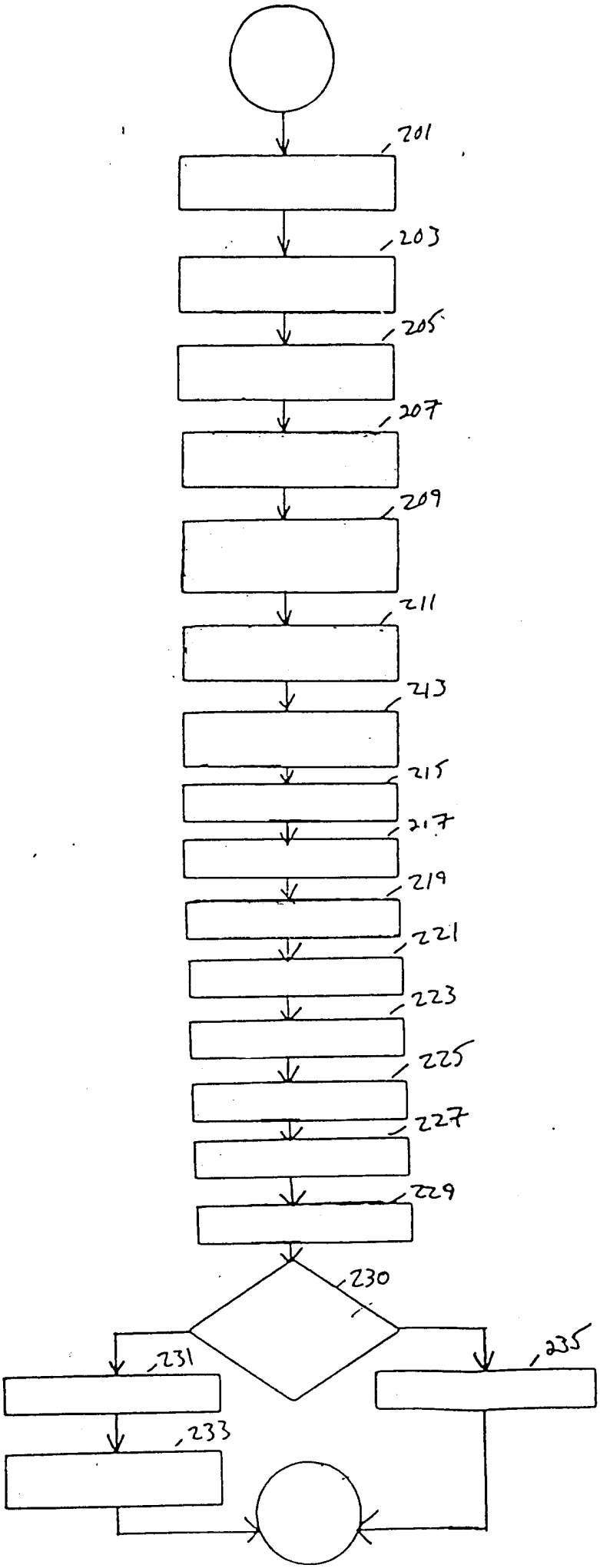
201
203
205
207
209
211
213
215
217
219
221
223
225
227
229
230
231
233
235

圖 2

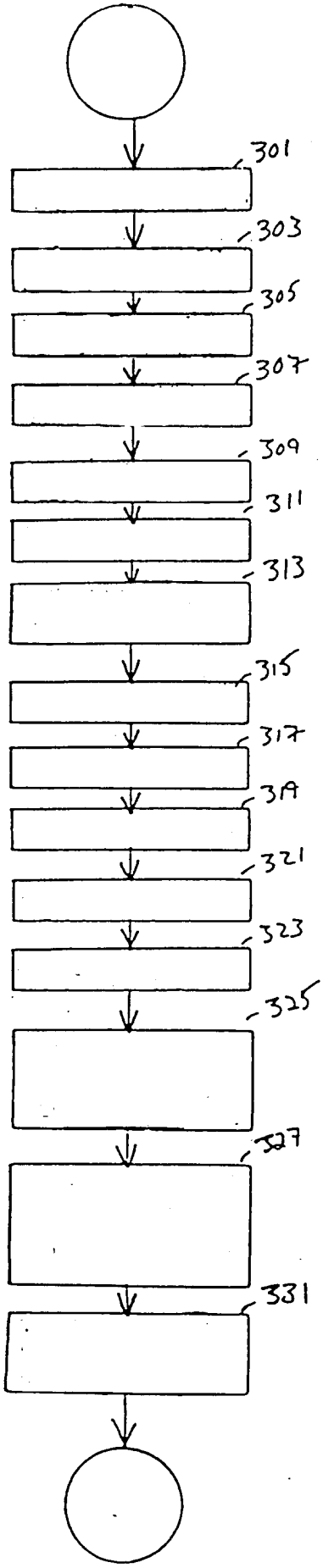

圖 3

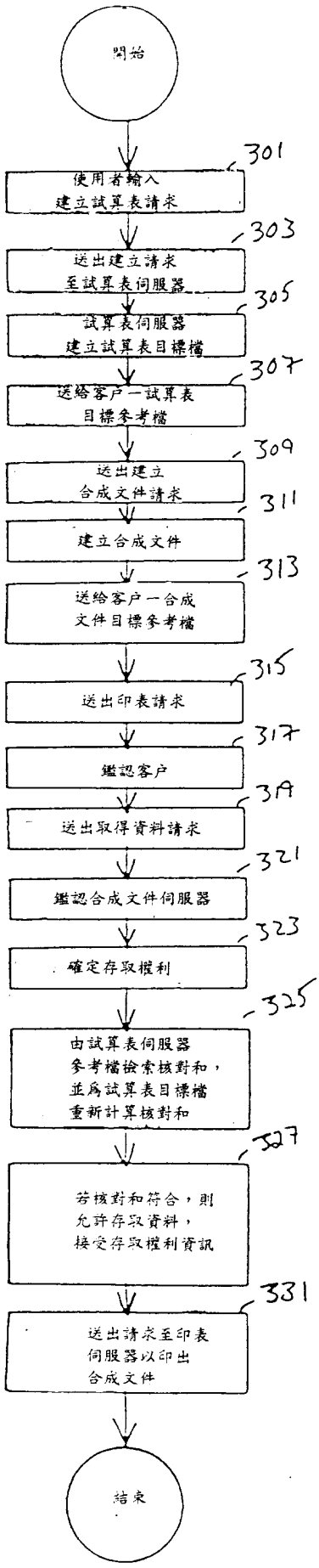
開始
301
使用者輸入
建立試算表請求
303
送出建立請求
至試算表伺服器
305
試算表伺服器
建立試算表目標檔
307
送給客戶一試算表
目標參考檔
309
送出建立
合成文件請求
311
建立合成文件
313
送給客戶一合成
文件目標參考檔
315
送出印表請求
317
鑑認客戶
319
送出取得資料請求
321
鑑認合成文件伺服器
323
確定存取權利
325
由試算表伺服器
參考檔檢索核對和，
並爲試算表目標檔
重新計算核對和
327
若核對和符合，則
允許存取資料，
接受存取權利資訊
331
送出請求至印表
伺服器以印出
合成文件
結束

圖 3