公告本

申請日期	88.4.7
案號	88105522
類別	G06F 1/60

（以上各欄由本局填註）

88年9月20日 修正補充

A4 C4 新 444154

(修正頁)88年9月

發明 新型 專利說明書

一、發明新型名稱	中文	多重通訊協定檔案伺服器中的檔案存取控制
	英文	"FILE ACCESS CONTROL IN A MULTI-PROTOCOL FILE SERVER"
二、發明創作人	姓名	1. 大衛 西斯 2. 安德拉 柏爾 3. 羅勃特 J. 浩利 4. 馬可 慕勒斯坦 5. 瓊恩 皮爾森
	國籍	均美國
	住、居所	1. 美國加州鄧托拉谷市老西班牙徑245號 2. 美國加州洛斯蓋托市藍丘皮耶塔路785號 3. 美國加州聖荷西市希爾凱斯特路1233號 4. 美國加州摩根丘市威尼斯路15105號 5. 美國加州孟羅公園市沙丘路692號
三、申請人	姓名（名稱）	美商奈特渥克家電用品公司
	國籍	美國
	住、居所（事務所）	美國加州桑尼維爾市東傑凡路495號
	代表人姓名	法蘭絲 B. 拜勒特

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
IPC分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
美國	1998年3月3日	09/035,234	□有☑無主張優先權
專利合作條約	1999年3月2日	PCT/US 99/04550	□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）

發明背景

1. 發明領域

本發明係有關一種多重通訊協定檔案伺服器中之檔案存取控制。

2. 相關技藝

一整合之電腦網路中，多重用户端裝置期望能共享相同檔案之存取。一種已知方法爲提供一用以儲存檔案之網路檔案伺服器，可接收並響應來自該等用户端裝置的檔案伺服器需求。這些檔案伺服器需求係使用一由檔案伺服器與用户端裝置兩者所認可且附著之檔案伺服器通訊協定而提出。因爲檔案係儲存於檔案伺服器，所以多重用户端裝置具有共享存取相同檔案之機會。

於希望由一或更多使用者使用之檔案系統中，期望能限制程式對於檔案系統中之檔案之存取。所限制之存取包括至少以下各方面：(1)使用者鑑定－決定需求之使用者確實爲其所自稱之人士，以及(2)存取控制效力－決定允許一經鑑定之使用者以一特殊方式存取一特殊檔案。當檔案系統係由提出需求之使用者從一檔案伺服器之遠端進行維護時，存取控制通訊協定尚有額外之方面－使用者可提出何需求，以存取檔案或者設定檔案之存取控制。

一項已知技藝中之問題爲：存取控制效力有多重種類之模式，通常各相關於一特殊的檔案系統，且有多重相異之存取控制通訊協定，通常各對應於一存取控制效力的模式。不管這些模式與通訊協定間之差異，檔案伺服器須響

五、發明說明（2）

應來自各使用者的檔案伺服器需求，並且對於各使用者模式須表現一致，而且沒有違反安全性或者令使用者錯愕之存取控制效力的動作。

例如，一普遍使用之第一存取控制模式係有關 Unix 作業系統(或其所衍生)。此第一存取控制模式相關於各檔案對於一檔案擁有者，一擁有者之群組，及所有其他使用者的許可。這些許可允許(擁有者，群組，或者所有其他使用者)對於所讀取，寫入，或者執行指示之檔案的存取。此第一存取控制模式通常由"網路檔案系統"(NFS)檔案伺服器通訊協定，或許加上一附件檔案鎖定通訊協定之"網路鎖定管理員"(NLM)而實行。一普遍使用之第二存取控制模式係有關視窗 NT 作業系統。此第二存取控制模式結合一存取控制清單(ACL)以及存取控制清單(ACL)中指定一個別使用者，一群使用者，或者所有使用者之各檔案，各登錄。各登錄可允許(特定使用者)對於所讀取，寫入，或者執行指示之檔案的存取，或者可特別拒絕存取。此第二存取控制模式通常由"共同網際網路檔案系統" (CIFS)實行。然而， NT 裝置同樣可藉由個人電腦網路檔案系統(PC NFS)之實行而使用網路檔案系統(NFS)通訊協定，且 Unix 裝置同樣可操作 POSIX ACLs (存取控制清單)。此兩種存取控制模式一般使用上重要之相異面包括(1)一檔案可指定何種許可，(2)可指定何種約略程度之特定許可(3)如何識別符合許可之使用者。

一項技藝中已知之方法爲：提供一將所有安全語法映射

五、發明說明（3）

成檔案伺服器中一單一原生作業系統之安全語法的多重通訊協定檔案伺服器，並且使用該單一原生作業系統令檔案存取控制有效。相信"Samba"系統及類似之模擬套件係使用此已知方法。此已知方法有一缺點爲：其將造成該等使用檔案伺服器原生作業系統之安全語法以外用户端裝置之安全錯誤或者錯愕。

技藝中已知之另一方法爲：提供一支援不同檔案其不同類型之安全語法的多重通訊協定檔案伺服器，但嘗試運用使用者之存取控制模式令各使用者的檔案存取控制有效。相信取自網威(Novell)公司之某些"網路管理"產品使用此已知方法。此已知方法有一缺點爲：使用者之存取控制模式可與檔案所設定的存取控制模式非常不同，而造成該等使用關於標的檔案之安全語法以外的用户端裝置之安全錯誤或者錯愕。

因此，期望能提供一種用以於使用多重相異之存取控制模式與多重相異之檔案伺服器通訊協定的用户端裝置間實施檔案安全語法之方法及系統。此項優點於本發明一具體實施例中達成，其中一多重通訊協定檔案伺服器以來自複數個可能之存取控制模式中的一特殊存取控制模式識別各檔案，並實施該特殊存取控制模式對於所有對於該檔案之存取。當檔案伺服器接收一對於使用一具有一不同之存取控制模式的檔案伺服器通訊協定之檔案的檔案伺服器需求時，則檔案伺服器將檔案之存取控制模式所強制的存取控制限制轉換成不同之在取控制模式中的等量限定之存取控

五、發明說明（4）

制限制。檔案伺服器限定使用轉換之存取控制限制的檔案之存取。

發明概述

本發明提供一種用以於使用多重相異之存取控制模式與多重相異之檔案伺服器通訊協定的用户端裝置間實施檔案存取控制之方法及系統。一多重通訊協定檔案伺服器以來自複數個可能模式中之一特殊存取控制模式識別各檔案，並對於所有對該檔案之存取實施該特殊模式。當檔案伺服器接收一對於使用一不同之存取控制模式的檔案之檔案伺服器需求時，則檔案伺服器將對於該檔案之存取控制限制轉換成不同模式中等量限定的限制。檔案伺服器限定使用轉換之存取控制限制的用户端裝置之存取。

一較佳之具體實施例中，各檔案指派有建立檔案或者最後設定該檔案之存取控制限制的使用者之存取控制模式。當一具有一不同之存取控制模式的使用者設定存取控制限制時，該檔案之存取控制模式則變更成新的模式。檔案係組織成一樹狀階層，其中各樹限制爲一或更多存取控制模式（其可限制使用者設定樹中檔案之存取控制限制的能力）。各樹可限制爲唯 NT 模式之格式，唯 Unix 模式之格式，或者混合 NT 或 Unix 模式之格式。

圖示簡述

圖示顯示一用以於用户端裝置間實施相異之存取控制模式的系統區塊圖。

五、發明說明（5）

較佳具體實施例詳述

以下描述中，一本發明之較佳具體實施例係考慮較佳處理步驟與資料結構而描述。然而，熟知此項技藝人士詳閱本申請案後將了解：本發明之具體實施例可使用於一或更多程式控制下作業之多用途處理器(或者配接於特殊處理步驟與資料結構之特殊用途處理器)而實行，並且此處所述之使用這類設備的較佳處理步驟與資料結構而實行無需不當之實驗或者進一步發明。

此處所述之本發明可與以下申請案中所述的發明連用：

○申請案號 08/985,398.一九九七年十二月五日申請，申請人名稱 Andrea Borr ，標題"多重通訊協定所一致化之檔案鎖定"，代理人摘要號碼 NET-023 。

此處本申請案援以合併參考，如同已完整敘述。

揭示之技術附錄係本發明所揭露的一部分，且此處援以合併參考，如同已完整敘述。

系統元件

圖示顯示一用以於用户端裝置間實施相異之存取控制模式的系統區塊圖。

一系統 100 包括一檔案伺服器 110 ，以及一組用户端裝置 120 。

檔案伺服器 110 維護一包括一組檔案 112 之檔案系統 111 。

一較佳之具體實施例中，檔案伺服器 110 使用以下專利權申請案中所述之本發明維護檔案系統 111 ：

五、發明說明（6）

○申請案號 08/471,218. 一九九五年六月五日申請，發明人名稱 David Hitz et al.. 標題"一種用以於一使用非揮發記憶體之搜索子系統中提供同位元的方法"，代理人摘要號碼 NET-004 ；

○申請案號 08/454,921. 一九九五年五月三十一日申請，發明人名稱 David Hitz et al.. 標題"隨處寫檔案系統佈局"，代理人摘要號碼 NET-005 ；

○申請案號 08/464,591. 一九九五年五月三十一日申請，發明人名稱 David Hitz et al.. 標題"用以於一整合一搜索磁碟子系統之檔案系統中分配檔案的方法"，代理人摘要號碼 NET-006。

此處這些申請案各援以合併參考，如同已完整敘述。

檔案伺服器 110 係用以接收來自用户端裝置 120 之檔案伺服器需求 121。檔案伺服器 110 將各檔案伺服器需求 121 進行語法分析，決定檔案伺服器需求 121 中所需求之作業是否經允許(用於送出檔案伺服器需求 121 之用户端裝置 120，以及用於一或更多由檔案伺服器需求 121 所指定之標的檔案 112)。如果係允許，則檔案伺服器 110 於一或更多標的檔案 112 上執行該作業。

檔案伺服器 110 同時用以將檔案伺服器響應 122 傳送至用户端裝置 120。檔案伺服器 110 決定各檔案伺服器需求 121 之響應(可能包括一用以指示需求之作業爲允許的響應)，產生該檔案伺服器響應 122，並將檔案伺服器響應 122 傳送至送出檔案伺服器需求 121 之用户端裝置 120。

五、發明說明（7）

各用户端裝置 120 係用以將檔案伺服器需求 121 傳送至檔案伺服器 110，以及用以接收來自檔案伺服器 110 之檔案伺服器響應 122。

存取控制模式

一較佳之具體實施例中，各用户端裝置 120 可爲一 Unix 用户端裝置 120 或者一視窗 NT 用户端裝置 120。各用户端裝置 120 可使用網路檔案系統(NFS)檔案伺服器通訊協定以提出檔案伺服器需求 121，或者使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定以提出檔案伺服器需求 121。(雖然通常 Unix 用户端裝置 120 使用網路檔案系統(NFS)檔案伺服器通訊協定，而 NT 用户端裝置 120 使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定，但 NT 用户端裝置 120 亦可能藉由使用該檔案伺服器通訊協定之個人電腦網路檔案系統(PC-NFS)的實行作業而使用網路檔案系統(NFS)檔案伺服器通訊協定)。檔案伺服器 110 接收各檔案伺服器需求 121 並且(如果允許則)於檔案伺服器需求 121 所指定之標的檔案 112 上執行需求之作業。

檔案伺服器 110 支援一個以上之存取控制模式，包括一"Unix Perms"存取控制模式(此處作"Unix 安全型態")以及一"NT 存取控制清單(ACL)"存取控制模式(此處作"NT 安全型態")。

Unix 安全型態使用使用者識別字(UIDs)來識別使用者，以及使用群組識別字(GIDs)來 1 識別該等使用者所屬之群組。Unix 安全型態結合以下存取控制限制以及各檔案：

五、發明說明（8）

○一擁有者之使用者識別字(UID)；

○一擁有者之群組識別字(GID)；

○一組"使用者"許可－允許讀取，寫入，或者由擁有之使用者執行檔案等許可；

○一組"群組"許可－允許讀取，寫入，或者由擁有之使用者群組執行檔案等許可；以及

○一組"其他"許可－允許讀取，寫入，或者由所有其他使用者執行檔案等許可。

Unix安全型態係由"網路檔案系統"(NFS)檔案伺服器通訊協定所支援，或許加上"網路鎖定管理員"(NLM)之附件檔案鎖定通訊協定。

網路檔案系統(NFS)係一無等級之通訊協定，所以各網路檔案系統(NFS)檔案伺服器需求121包括提出需求之使用者其使用者識別字(UIDs)與群組識別字(GIDs)。Unix用户端裝置120於使用者之登入階段，藉由參考系統通行密碼檔案(/etc/passwd)與群組檔案(/etc/groups)而決定使用者的使用者識別字(UIDs)與群組識別字(GIDs)。

爲實施使用Unix安全型態之檔案存取控制，檔案伺服器110決定檔案伺服器需求121是否來自擁有之使用者，一擁有使用者群組中之使用者，或者某些其他使用者。爲響應此決定，檔案伺服器110使用該使用者許可，群組許可，或者其他許可之一，以決定是否允許該檔案伺服器需求121。

NT安全型態使用安全識別字(SIDs)以識別使用者及群組

五、發明說明（9）

兩者。NT安全型態結合以下存取控制限制以及各檔案：

○一擁有者之安全識別字(SID)；

○一擁有者群組之安全識別字(SID)；

○一存取控制清單(ACL)。

NT存取控制清單(ACL)包括一或更多存取控制登錄(ACEs)，各包括一指示所應用之使用者或者群組的安全識別字(SID)，以及一組許可。NT安全型態提供三項Unix許可(讀取，寫入，或者執行)與"變更許可"之許可，"取得擁有權"之許可，"刪除"之許可，"刪除子層"之許可，以及其他許可。

NT安全型態係由"共同網際網路檔案系統"(CIFS)通訊協定所支援。NT安全型態進一步描述於以下刊物：R. Reichel."視窗NT安全之內幕"，視窗/磁碟作業系統(DOS)開發者雜誌(一九九三年四月及五月號)，以及Stephen Sutton，"視窗NT安全指南"(ISBN 0201419696)中。

共同網際網路檔案系統(CIFS)係一會期式之通訊協定，所以NT用户端裝置120於決定使用者與使用者群組之安全識別字(SIDs)後的會期連接階段，將NT使用者名稱與通行密碼傳送至檔案伺服器110。檔案伺服器110可驗明使用者本身，或(較佳者)將NT使用者名稱與通行密碼轉寄至一NT主網域控制器。

爲了實施使用NT安全型態之檔案存取控制，檔案伺服器110決定使用者與使用者群組之安全識別字(SID)，以便使用者提出檔案伺服器需求121。檔案伺服器110從應用

五、發明說明（10）

該許可之存取控制登錄(ACEs)彙集授權該使用者的許，然後減去特別拒絕該使用者之許可。爲響應此項彙集與減去，檔案伺服器110決定是否允許檔案伺服器需求121。

雖然本發明一較佳具體實施例係考慮Unix安全型態與NT安全型態而描述，但本發明可以其他存取控制模式而準備，像是由某些Unix裝置及某些其他作業系統所支援之"POSIX ACL"存取控制模式。此處所述之本發明的觀念與特性可準備用於一支援增加或者取代此處詳述之"POSIX ACL"存取控制模式的檔案伺服器110，而無需進一步之發明或者不當的實驗。因此，本發明之範圍與精神包括這類檔案伺服器及其使用方法。

檔案伺服器110將其檔案系統111中所維護之各檔案112指定成具有來自複數個其支援之存取控制模式中的一特定存取控制模式。一較佳具體實施例中，各檔案112係指定使用Unix安全型態或者NT安全型態。檔案伺服器110對於存取該檔案112之所有嘗試實施各檔案112所指定的安全型態。所以，檔案伺服器110對於所有對該標的檔案112提出之檔案伺服器需求121實施指定的安全型態，無論該等檔案伺服器需求121係來自Unix裝置或者NT裝置，以及無論該等檔案伺服器需求121係使用網路檔案系統(NFS)檔案伺服器通訊協定或者共同網際網路檔案系統(CIFS)檔案伺服器通訊協定。

存取控制之實施

如果檔案伺服器110接收一標的檔案112之一檔案伺服

五、發明說明（11）

器需求 121，且該檔案伺服器需求 121 符合安全型態標的檔案 112，則檔案伺服器 110 違反該安全型態強制之檔案 112 的存取控制限制而令檔案伺服器需求 121 有效。

因此檔案伺服器 110 認可並實施於至少以下狀況：

○ NT 安全型態。檔案 112 具有 NT 安全型態，並具有一存取控制限制之對應設定（一 NT 存取控制清單(ACL)），由一用户端裝置 120 使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定而設定。

如果一用户端裝置 120 提出一存取使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定之檔案 112 的檔案伺服器需求 121，那麼可能的話，檔案伺服器 110 實施使用 NT 安全型態之 NT 存取控制清單(ACL)。

如果檔案伺服器 110 可藉由與一 NT 網域控制器之通訊，或者參照一 NT 使用者安全識別字(SID)資料庫，而決定 NT 使用者，則檔案伺服器 110 可實施使用 NT 安全型態之 NT 存取控制清單(ACL)。

如果檔案伺服器 110 無法決定一 NT 使用者，則使用一共同網際網路檔案系統(CIFS)檔案伺服器通訊協定會期所記錄之一 Unix 使用者的使用者識別字(UID)，以決定等效之 Unix 使用者，並且如同檔案伺服器需求 121 係來自該 Unix 使用者而實施 NT 存取控制清單(ACL)。

○ Unix 安全型態。檔案 112 具有 Unix 安全型態，並具有一存取控制限制之對應設定(Unix Perms)，藉由用户端裝置 120 使用網路檔案系統(NFS)檔案伺服器通訊協定而設

五、發明說明（12）

定。

如果用户端裝置120提出一存取使用網路檔案系統(NFS)檔案伺服器通訊協定之檔案112的檔案伺服器需求121，則檔案伺服器110實施使用Unix安全型態之Unix Perms。

然而，檔案伺服器110同樣可接收一未符合標的檔案112之安全型態的檔案伺服器需求121。檔案伺服器110可經由令以下所述有效，違反該未符合之用户端裝置120而實施標的檔案112的安全型態：(1)一用户端裝置120之轉換的使用者識別字，或者(2)一檔案112其轉換之存取控制限制設定。如此處所述，檔案伺服器110令所有Unix安全型態檔案112之轉換的使用者識別字有效有效，且較佳者，(如果可能則)令NT安全型態檔案112之轉換的使用者識別字有效。再者，當檔案伺服器110令檔案112之轉換的存取控制限制有效時，則不對於各檔案伺服器需求121重新計算轉換之控制限制，而是貯藏於檔案112以便再使用。

因此檔案伺服器110同樣認可並實施至少以下狀況：

○ NT安全型態。檔案112具有NT安全型態，並具有一存取控制限制之對應設定(一NT存取控制清單(ACL))，由用户端裝置120使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定而設定。

如果一用户端裝置120提出一存取使用網路檔案系統(NFS)檔案伺服器通訊協定之檔案112的檔案伺服器需求121，則檔案伺服器110決定相關於用户端裝置120提出檔

五、發明說明（13）

案伺服器需求121之Unix使用者。Unix使用者具有一使用者識別字(UID)。

一較佳具體實施例中，檔案伺服器110將Unix使用者映射成一等效之NT使用者。檔案伺服器110將使用者識別字(UID)轉換成一與該Unix使用者等效之使用者的安全識別字(SID)。檔案伺服器110對於該等效之NT使用者(安全識別字(SID))實施等效之NT使用者的存取控制限制(NT存取控制清單(ACL))(安全識別字(SID))。

檔案伺服器110執行以下處理，將Unix使用者映射成一等效之NT使用者：

○用户端裝置120使用網路檔案系統(NFS)檔案伺服器通訊協定接觸檔案伺服器110。網路檔案系統(NFS)檔案伺服器通訊協定之檔案伺服器需求121包括一相關於用户端裝置120之Unix使用者的使用者識別字(UID)。

○檔案伺服器110於Unix通行密碼檔案(/etc/passwd)中查閱使用者識別字(UID)，進而識別該Unix使用者之Unix使用者名稱。Unix使用者名稱係一用以識別Unix使用者之文數字字串。

○檔案伺服器110使用一選定之映射檔案，將Unix使用者名稱轉換成一NT使用者名稱。類似於Unix使用者名稱，NT使用者名稱係一用以識別NT使用者之文數字字串。如果沒有如此轉換Unix使用者名稱，則檔案伺服器110不進行轉換，而使用NT使用者名稱作爲Unix使用者名稱。

五、發明說明（14）

一較佳具體實施例中，映射檔案包括一組記錄，各藉由NT使用者名稱識別一NT使用者，並結合一等效之Unix使用者名稱以及該NT使用者名稱。

○檔案伺服器110接觸一NT網域控制器，以決定一NT使用者名稱之安全識別字(SID)。如果沒有這類NT使用者，則檔案伺服器110使用一選定之參數用於未映射的Unix使用者。一較佳具體實施例中，此選定之參數係以內定值設定成NT使用者"訪客"("guest")。

○檔案伺服器110接觸NT網域控制器，以取得NT使用者爲一成員之所有群組的安全識別字(SIDs)。

檔案伺服器110貯藏使用者識別字(UID)轉安全識別字(SID)之映射持續一段時間，或許大約數小時。

一替代之較佳具體實施例中，或者如果檔案伺服器110無法將Unix使用者映射成NT使用者(例如，如果網域鑑定已關閉)，則檔案伺服器110將NT存取控制清單(ACL)映射成一組等量限定之Unix Perms。檔案伺服器110決定這些Unix Perms以響應NT存取控制清單(ACL)，及響應Unix使用者。檔案伺服器110對於實際之Unix使用者(使用者識別字(UID))實施所映射的存取控制限制(即Unix Perms)。

檔案伺服器110可能執行動態許可映射，其中檔案伺服器110於要求映射時，將NT存取控制清單(ACL)映射成一組Unix Perms。一較佳具體實施例中，檔案伺服器110以檔案112貯藏轉換之Unix Perms。因此，爲了令存取控制

五、發明說明（15）

限制有效，檔案伺服器 110 執行靜態許可映射，其中檔案伺服器 110 於 NT 存取控制清單(ACL)設定時，將 NT 存取控制清單(ACL)映射成一組 Unix Perms。

檔案伺服器 110 執行以下處理，以達成靜態許可映射：

○檔案伺服器 110 決定檔案 112 其擁有者之 NT 使用者，並且將 NT 使用者映射成一等效之 Unix 使用者(檔案伺服器 110 將 NT 使用者之安全識別字(SID)映射成一 Unix 使用者的使用者識別字(UID))。

○檔案伺服器 110 檢查檔案 112 之 NT 存取控制清單(ACL)並且決定是否有任何"拒絕存取"提供。

○如果檔案 112 之 NT 存取控制清單(ACL)沒有"拒絕存取"提供，則檔案伺服器 110 產生一組具有一由 NT 存取控制清單(ACL)供應之檔案存取控制限制所組成的"使用者許可"登錄的 Unix Perms。檔案伺服器 110 將"群組許可"之 Unix Perms 設定成等於"其他許可"的 Unix Perms。如果有人存在，則檔案伺服器 110 將"其他許可"之 Unix Perms 設定成等於 NT 存取控制清單(ACL)登錄"每個人"。

○如果檔案 112 之 NT 存取控制清單(ACL)確實具有"拒絕存取"提供，則檔案伺服器 110 駁回檔案伺服器需求 121。

因爲靜態許可映射並未響應提出檔案伺服器需求 121 之特殊使用者，所以檔案伺服器 110 並未嘗試決定以 NT 存取控制清單(ACL)之何種提供用於該特殊使用者。

五、發明說明（16）

○ Unix 安全型態。檔案 112 具有 Unix 安全型態，並且具有一存取控制限制之對應設定(Unix Perms)，藉由一用户端裝置 120 使用網路檔案系統(NFS)檔案伺服器通訊協定而設定。

如果一用户端裝置 120 提出一存取使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定之檔案 112 的檔案伺服器需求 121，則檔案伺服器 110 決定相關於用户端裝置 120 提出檔案伺服器需求 121 之 NT 使用者。NT 使用者具有一會期識別字(安全識別字(SID))。

檔案伺服器 110 將 NT 使用者映射成一等效之 Unix 使用者。檔案伺服器 110 將安全識別字(SID)轉換成一該 NT 使用者其等效使用者之使用者識別字(UID)。檔案伺服器 110 實施等效之 Unix 使用者(使用者識別字(UID))的存取控制限制(the Unix Perms)。

檔案伺服器 110 執行以下處理，將 NT 使用者映射成一等效之 Unix 使用者：

○ 用户端裝置 120 開始一共同網際網路檔案系統(CIFS)會期(用户端裝置 120 首先使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定接觸檔案伺服器 110)。用户端裝置 120 將其 NT 使用者名稱傳送至檔案伺服器 110。

○ 檔案伺服器 110 使用一映射檔案將 NT 使用者名稱轉換成一 Unix 使用者名稱。如果沒有如此轉換 NT 使用者名稱，則檔案伺服器 110 不進行轉換，而使用 NT 使用者名稱作爲 Unix 使用者名稱。

五、發明說明（17）

○檔案伺服器 110 查閱 Unix 通行密碼檔案(/etc/passwd)中之 Unix 使用者名稱，進而識別 Unix 使用者， Unix 使用者之使用者識別字(UID)， Unix 使用者之主群組，以及 Unix 使用者之主群組識別字(GID)。如果 Unix 通行密碼檔案中沒有這類 Unix 使用者名稱，則檔案伺服器 110 使用一用於未映射之 NT 使用者的選定參數。一較佳之具體實施例中，此選定之參數係以內定值設定成 Unix 使用者"非重要人士"。

○檔案伺服器 110 查閱 Unix 群組檔案(/etc/groups)中之 Unix 使用者名稱，以決定任何其他群組及相關於 Unix 使用者的任何其他群組識別字(GIDs)。

讀取及修改存取控制限制

各檔案 112 具有由檔案伺服器 110 所設定之安全型態，使(a)一於檔案 112 上執行一作業之檔案伺服器需求 121，或者(b)一執行設定檔案 112 之存取控制限制作業的檔案伺服器需求 121，產生期望之結果。

當檔案 112 最初建立時，檔案伺服器 110 將檔案 112 之安全型態設定成等於相關於將其建立的檔案伺服器通訊協定之安全型態。(此受限於由此處所述之存取控制樹所強制的限定)。因此，如果檔案 112 係使用網路檔案系統(NFS)檔案伺服器通訊協定而建立，則檔案 112 之安全型態係設定成 Unix 安全型態。類似地，如果檔案 112 係使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定而建立，則檔案 112 之安全型態係設定成 NT 安全型態。

五、發明說明（18）

當檔案 112 其存取控制限制修改後，則檔案伺服器 110 將檔案 112 之安全型態設定成等於一相關於新的存取控制限制之安全型態。(此係受限於由此處所述之存取控制樹所強制的限定)。因此，如果一用户端裝置 120 設定檔案 112 之 Unix Perms ，則檔案 112 之安全型態係設定成 Unix 安全型態。類似地，如果一用户端裝置 120 設定一檔案 112 之 NT 存取控制清單(ACL)，則檔案 112 之安全型態係設定成 NT 安全型態。

檔案伺服器 110 可接收一檔案伺服器需求 121 ，以讀取或者檢視檔案 112 之存取控制限制。同時，當檔案伺服器 110 接收一對於檔案 112 進行一存取控制限制之增加變更的檔案伺服器需求 121 時，則於進行增加變更前，決定目前檔案 112 之存取控制限制。

因此檔案伺服器 110 認可並且實施至少以下狀況：

○ NT 安全型態。檔案 112 具有 NT 安全型態並且具有一存取控制限制之對應設定(一 NT 存取控制清單(ACL))，由一用户端裝置 120 使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定而設定。

如果一用户端裝置 120 提出一使用網路檔案系統(NFS)檔案伺服器通訊協定而讀取或者修改檔案 112 之存取控制限制的檔案伺服器需求 121 ，則檔案伺服器 110 決定相關於用户端裝置 120 提出檔案伺服器需求 121 之 Unix 使用者。

檔案伺服器 110 執行如以上所述將一 NT 存取控制清單(ACL)映射成一組 Unix Perms ，令檔案存取控制有效之相

五、發明說明（19）

同處理，而以下除外：

不似令存取控制限制有效，檔案伺服器 110 處理存取控制限制之轉換不同於處理檔案伺服器需求 121 讀取或者修改檔案 112 的存取控制限制。

較佳者，檔案伺服器 110 執行動態許可映射，其中檔案伺服器 110 於要求映射時，將 NT 存取控制清單(ACL)映射成一組 Unix Perms。NT 安全型態較 Unix 安全型態爲豐富－例如，Unix 安全型態沒有"拒絕存取"提供。因此，檔案伺服器 110 可能將 NT 存取控制清單(ACL)映射成一組對不同之 Unix 使用者而有不同呈現的 Unix Perms。例如，如果 NT 存取控制清單(ACL)對於一擁有者爲 Charles 之檔案 112 特別供應 Allen 之讀取存取，但特別拒絕 Beth 之讀取存取，則檔案伺服器 110 將對使用者 Allen 與 Beth 各供應不同的 Unix perms。一設定將允許 Allen's 群組之讀取存取，而一設定將不允許 Beth 群組之讀取存取，以諧和由實際 NT 存取控制清單(ACL)所供應的存取。

檔案伺服器 110 執行以下處理，以達成動態許可映射：

○檔案伺服器 110 決定檔案 112 之擁有者的 NT 使用者，並且將 NT 使用者映射成一等效之 Unix 使用者(檔案伺服器 110 將 NT 使用者之安全識別字(SID)映射成一 Unix 使用者的使用者識別字(UID))。

○檔案伺服器 110 檢查檔案 112 之 NT 存取控制清單(ACL)，並且決定是否有任何"拒絕存取"提供。

○如果檔案 112 之 NT 存取控制清單(ACL)沒有"拒絕存取"

五、發明說明（20）

提供，則檔案伺服器 110 產生一組具有由 NT 存取控制清單(ACL)提供之檔案存取控制限制所組成的"使用者許可"與"其他許可"之登錄的 Unix Perms 。檔案伺服器 110 將"群組許可"之 Unix Perms 設定成等於"其他許可"的 Unix Perms 。

○如果檔案 112 之 NT 存取控制清單(ACL)確實具有"拒絕存取"提供，則檔案伺服器 110 嘗試決定是否有任何該提供應用於特殊的 Unix 使用者。如果檔案伺服器可辨別，則產生一組反映目前此特殊檔案 112 與此特殊 Unix 使用者可用之存取控制限制的 Unix Perms 。如果檔案 110 無法辨別，則駁回檔案伺服器需求 121 。(替代上，如果 NT 存取控制清單(ACL)中有任何"拒絕存取"提供，則檔案伺服器 110 可駁回檔案伺服器需求 121 。)

替代之具體實施例中，檔案伺服器 110 可執行類似於令存取控制限制有效的檔案伺服器需求 121 之靜態許可檢查，以讀取或者修改檔案 112 的存取控制限制。

如果檔案伺服器需求 121 嘗試修改不影響存取控制限制之檔案 112 的屬性(像是存取時間或者修改時間)，則檔案伺服器 110 進行該等修改，而無需變更檔案 112 之存取控制限制。

如果檔案伺服器需求 121 嘗試修改某些但非所有檔案 112 之存取控制限制，則檔案伺服器 110 產生一組 Unix Perms 以響應如以上所述之檔案 112 的 NT 存取控制清單(ACL)。檔案伺服器 110 如檔案伺服器需求 121 所指定修改

五、發明說明（21）

產生之 Unix Perms 。如果檔案伺服器 110 無法產生一組 Unix Perms 以響應檔案 112 之 NT 存取控制清單(ACL)，則檔案伺服器 110 駁回檔案伺服器需求 121。

一項設定存取控制限制之差異爲：根據 NT 安全型態，檔案 112 可特別設定成"唯讀"。根據 Unix 安全型態，檔案係僅藉由清除檔案 112 擁有者之寫入許可而設定成唯讀。當一使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定之用户端裝置 120 嘗試以 Unix 安全型態設定一檔案 112 的唯讀屬性時，則檔案伺服器 110 清除該檔案 112 之 Unix Perms 中的檔案 112 擁有者之寫入許可。

○ Unix 安全型態。檔案 112 具有 Unix 安全型態，並且具有一存取控制限制之對應設定(Unix Perms)，由一用户端裝置 120 使用網路檔案系統(NFS)檔案伺服器通訊協定而設定。

檔案伺服器 110 執行以下處理將一組 Unix Perms 映射成一 NT 存取控制清單(ACL)，以藉由一共同網際網路檔案系統(CIFS)用户端裝置 120 顯示或者修改該等 Unix Perms：

○檔案伺服器 110 產生一"擁有者"之 NT 存取控制清單(ACL)登錄，提供如同"使用者許可"之 Unix Perms 登錄的相同存取控制限制。

○檔案伺服器 110 產生一"每個人"之 NT 存取控制清單(ACL)登錄，提供如同"其他許可"之 Unix Perms 登錄的相同存取控制限制。

○如有可能，檔案伺服器 110 產生一實際需求使用者之 NT

五、發明說明（22）

存取控制清單(ACL)登錄，提供如同該使用者之 Unix Perms 登錄的相同存取控制限制。此步驟可能需運用使用者識別字(UID)轉安全識別字(SID)之貯藏，將 Unix 使用者映射成一等效之 NT 使用者。

類似於由一 Unix 使用者修改 NT 存取控制清單(ACL)登錄，如果(由一 NT 使用者修改 Unix Perms 之)檔案伺服器需求 121 嘗試修改不影響檔案 112 之存取控制限制的檔案 112 屬性，則檔案伺服器 110 進行該等修改，無需變更檔案 112 之存取控制限制。

如果檔案伺服器需求 121 嘗試修改某些但非檔案 112 之所有存取控制限制，則檔案伺服器 110 產生一 NT 存取控制清單(ACL)以響應檔案 112 之 Unix Perms 設定，如以上所述。檔案伺服器 110 如檔案伺服器需求 121 所指定而修改產生之 NT 存取控制清單(ACL)。

存取控制子樹

一較佳具體實施例中，檔案系統 111 中之檔案 112 係組織成一具有一組枝節點與一組葉節點之樹狀。一樹之枝節點係一根節點，因而樹之各枝節點係該樹一子樹之根節點。檔案系統 111 中，各枝節點係一目錄，而各葉節點係一檔案 112。一目錄係一種類型之檔案 112，包括有關一以其爲根節點之子樹中該等枝節點與葉節點的資訊。

檔案伺服器 110 結合一存取控制模式之限制設定以及各子樹。一檔案伺服器 110 支援 Unix 安全型態與 NT 安全型態之較佳具體實施例中，檔案伺服器 110 指定各子樹爲唯

五、發明說明（23）

NT格式，唯Unix格式，或者混合格式。

唯NT格式

當檔案伺服器110指定一子樹爲唯NT格式時，則限定檔案112之建立須於檔案112具有NT安全型態之子樹內。檔案伺服器110同時禁止子樹內檔案112之存取控制模式變更成其他NT安全型態以外型態。

根據NT安全型態，新的檔案112從其父層節點承襲NT存取控制清單(ACL)設定。如果一使用網路檔案系統(NFS)檔案伺服器通訊協定之用户端裝置120嘗試於一具有唯NT格式之子樹中建立一檔案112，則該檔案112僅能由與該子樹根節點之NT擁有者的NT使用者等效的Unix使用者建立。檔案伺服器110決定如果提出檔案伺服器需求121之Unix使用者是否等效係藉由(a)將擁有者之NT使用者其安全識別字(SID)映射成一等效的使用者識別字(UID)；(b)將使用者識別字(UID)儲存於其檔案112之記錄中；以及(c)比較該使用者識別字(UID)與檔案伺服器需求121中之使用者識別字(UID)。

根據NT安全型態，有一特殊之"刪除"許可及一特殊之"刪除子層"許可。如果檔案伺服器110無法決定一Unix使用者是否具有這些許可，則其駁回於唯NT格式之子樹中刪除檔案112的檔案伺服器需求121，除非檔案伺服器需求121係來自檔案112之擁有者(擁有者的NT使用者其等效之Unix使用者)或者Unix使用者"根"節點。

根據NT安全型態，有一特殊"變更許可"之許可及一特

五、發明說明（24）

殊"取得擁有者"之許可。如果檔案伺服器 110 無法決定一 Unix 使用者是否具有這些許可，則拒絕於一唯 NT 格式子樹中設定對於檔案 112 之任何許可的檔案伺服器需求 121，除非檔案伺服器需求 121 係來自檔案 112 之擁有者（擁有者之 NT 使用者的等效 Unix 使用者）或者 Unix 使用者"根"節點。

唯 Unix 格式

類似地，當檔案伺服器 110 指定一子樹爲唯 Unix 格式時，則限定於該子樹內之檔案系統 111 所建立爲具有 Unix 安全型態的檔案系統 111。檔案伺服器 110 同時禁止將該子樹內檔案系統 111 之存取控制模式變更成其他 Unix 安全型態以外型態。設定一 NT 存取控制清單(ACL)之嘗試將變更檔案 112 之存取控制模式成爲 NT 安全型態，因而於一唯 Unix 格式之子樹中駁回。

當一使用共同網際網路檔案系統(CIFS)檔案伺服器通訊協定之用户端裝置 120 於一唯 Unix 格式的子樹中建立一檔案 112 時，檔案伺服器 110 將檔案 112 之擁有者設定成與提出該檔案伺服器需求 121 之 NT 使用者等效的 Unix 使用者。檔案伺服器 110 將 NT 使用者之安全識別字(SID)映射成一等效之 Unix 使用者的使用者識別字(UID)，並使用該使用者識別字(UID)設定檔案 112 之擁有者。

根據 Unix 安全型態，沒有"變更許可"之許可或者"取得擁有者"之許可。檔案伺服器 110 永遠拒絕在一唯 Unix 格式之子樹中對檔案 112 設定這些許可的檔案伺服器需求

五、發明說明（25）

121。

混合格式

當檔案伺服器 110 指定一樹層爲混合格式時，則允許以 Unix 安全型態或者 NT 安全型態建立檔案系統 111。檔案伺服器 110 並未禁止於該子樹內將檔案系統 111 之存取控制模式變更成 Unix 安全型態或者 NT 安全型態。

一檔案伺服器 110 之管理員可將一子樹之指定從一第一格式變更成一第二格式(例如，從混合格式變成唯 NT 格式或者唯 Unix 格式)。當第二格式可能與第一格式不相容(例如，一變更成唯 NT 格式之子樹包括 Unix 安全型態的節點)時，則檔案伺服器 110 以不相容之存取控制模式轉換該等檔案 112，如同對於該等檔案 112 設定許可。僅檢查許可之檔案 112 的檔案伺服器需求 121 於檔案 112 處仍具有效力可使用存取控制模式。

雖然此處本發明僅考慮兩存取控制模式而描述，本發明可準備以三或更多存取控制模式使用。這類替代之具體實施例中，有一可能較大數目之子樹格式，包括限定該子樹內之檔案 112 爲一組多重存取控制模式之一的子樹格式，其少於由檔案伺服器 110 認可之所有存取控制模式的集合。

一較佳之具體實施例中，檔案系統 111 之根節點係指定爲具有混合格式。子樹之擁有者的用户端裝置 120 可由檔案伺服器 110 之檔案伺服器需求 121 修改一子樹的格式；因此檔案伺服器需求 121 可將子樹修改成一具有唯 NT 格

五、發明說明（26）

式，唯Unix格式，混合格式。當一新的子樹建立時，檔案伺服器 110 指定新的子樹爲具有如其父層之相同格式；因此，如果於一已爲混合格式(內定值)之子樹內建立則爲混合格式，如果於一已爲唯 NT 格式(內定值)之子樹內建立則爲唯 NT 格式，而如果於一已爲唯 Unix 格式(內定值)之子樹內建立則爲唯Unix格式。

替代之具體實施例

雖然此處已揭示較佳之具體實施例，而本發明之觀念，範圍與精神內仍可能有許多變化，而這些變化於詳閱本申請案後，熟知此項技藝人士將可清楚。

A5
B5

四、中文發明摘要（發明之名稱：多重通訊協定檔案伺服器中的檔案存取控制）

本發明提供一種用以實施使用多重種類之存取控制模式與多重種類之檔案伺服器通訊協定的用户端裝置間其檔案存取控制之方法及系統。一多重通訊協定檔案伺服器以一來自複數個可能模式之特殊存取控制模式識別各檔案。當檔案伺服器接收一使用不同存取控制模式之檔案其檔案伺服器需求時，則檔案伺服器將該檔案之存取控制限制轉換成不同模式等量限定的限制。檔案伺服器限定使用所轉換之存取控制限制的用户端裝置之存取。各檔案指派有建立檔案或者最後設定檔案其存取控制限制之使用者的存取控制模式。當一具有不同之存取控制模式的使用者設定存取控制限制時，則檔案之存取控制模式變更成新的模式。檔

英文發明摘要（發明之名稱："FILE ACCESS CONTROL IN A MULTI-PROTOCOL FILE SERVER"）

The invention provides a method and system for enforcing file access control among client devices using multiple diverse access control models and multiple diverse file server protocols. A multi-protocol file server identifies each file with one particular access control model out of a plurality of possible models, and enforces that one particular model for all accesses to that file. When the file server receives a file server request for that file using a different access control model, the file server translates the access control limits for that file into no-less-restrictive limits in the different model. The file server restricts access by the client device using the translated access control limits. Each file is assigned the access control model of the user who created the file or who last set access control limits for the file. When a user having a different access control model sets access control limits, the access control model for the file is changed to the new model. Files are organized in a tree hierarchy, in which each tree is limited to

A5
B5

四、中文發明摘要（發明之名稱：　　）

案係組織成一樹狀階層，其中各樹限制於一或更多存取控制模式(其可限制使用者設定樹中檔案之存取控制限制的能力)。各樹可限制於唯NT模式之格式，唯Unix模式之格式，或者混合NT或Unix模式之格式。

英文發明摘要（發明之名稱：　　）

one or more access control models (which can limit the ability of users to set access control limits for files in that tree). Each tree can be limited to NT-model-only format, Unix-model-only format, or mixed NT-or-Unix-models format.

A8
B8
C8
D8

六、申請專利範圍

1. 一種用以操作一檔案伺服器之方法，該方法包括以一具有一從複數個安全型態間所選定之第一安全型態識別檔案伺服器上第一檔案之步驟；以及

對於該第一檔案之所有存取實施該第一安全型態。

2. 如申請專利範圍第 1 項之方法，其中該等複數個安全型態包括一視窗 NT 安全型態。

3. 如申請專利範圍第 1 項之方法，其中該等複數個安全型態包括一 Unix 安全型態。

4. 如申請專利範圍第 1 項之方法，包括下列步驟，用以

結合該第一檔案與一檔案系統中一檔案之子集合；以及

將該檔案之子集合限制爲該等複數個安全型態之一安全子集合；

其中於該檔案系統樹中設定許可之嘗試係限定於該安全子集合中。

5. 如申請專利範圍第 4 項之方法，其中該安全子集合包括一視窗 NT 安全型態。

6. 如申請專利範圍第 4 項之方法，其中該安全子集合包括一 Unix 安全型態。

7. 如申請專利範圍第 1 項之方法，包括響應一檔案伺服器需求以一第二安全型態識別該第一檔案之步驟。

8. 如申請專利範圍第 7 項之方法，包括當該檔案伺服器需求成功時，用以結合該第二安全型態以及一對該第一檔案設定許可之檔案伺服器需求的步驟。

六、申請專利範圍

9. 如申請專利範圍第 7 項之方法，其中該用以識別之步驟包括用以將該第一安全型態中一相關於該第一檔案之第一組許可轉換成一該第二安全型態的第二組許可之步驟，其中該第二組許可與該第一組許可係等量的限定。

10. 如申請專利範圍第 1 項之方法，其中該用以實施之步驟包括下列步驟用以

認可一相關於該第一安全型態中該第一檔案之第一組許可；

定義一相關於該第一安全型態之第一使用者型態；

將一使用者從一相關於一第二安全型態之第二使用者型態轉換成該第一使用者型態；以及

使用該第一使用者型態與該第一組許可，實施於一來自該第二使用者型態之檔案伺服器需求。

11. 如申請專利範圍第 10 項之方法，其中該用以轉換之步驟係考慮於實施該步驟時可應用於該第一檔案的存取控制限制而執行。

12. 如申請專利範圍第 10 項之方法，其中該用以轉換之步驟係考慮於設定該存取控制限制時可應用於該第一檔案的存取控制限制而執行。

13. 如申請專利範圍第 1 項之方法，其中該用以實施之步驟包括下列步驟用以

將該第一安全型態中一相關於該第一檔案之第一組許可轉換成一第二安全型態的第二組許可，其中該第

六、申請專利範圍

二組許可與該第一組許可係等量的限定；以及

使用該第二組許可，以該第二安全型態實施一檔案伺服器需求。

14. 如申請專利範圍第 13 項之方法，其中該用以轉換之步驟係考慮於實施該步驟時可應用於該第一檔案的存取控制限制而執行。

15. 如申請專利範圍第 13 項之方法，其中該用以轉換之步驟係考慮於設定該存取控制限制時可應用於該第一檔案之存取控制限制而執行。

16. 一種檔案伺服器，包括：

該檔案伺服器可用之一組檔案，該檔案各具有一從該檔案伺服器可用之複數個安全型態間所選定的相關之安全型態；

其中該檔案伺服器對於該檔案之所有存取實施該相關的安全型態。

17. 如申請專利範圍第 16 項之檔案伺服器，其中該複數個安全型態包括一視窗 NT 安全型態。

18. 如申請專利範圍第 16 項之檔案伺服器，其中該複數個安全型態包括一 Unix 安全型態。

19. 如申請專利範圍第 16 項之檔案伺服器，包括：

該檔案系統中一相關於該複數個安全型態之一安全子集合的檔案之子樹；

其中檔案伺服器將於該子樹中設定許可之嘗試限定於該安全子集合中。

六、申請專利範圍

20. 如申請專利範圍第 19 項之檔案伺服器，其中該安全子集合包括一視窗 NT 安全型態。

21. 如申請專利範圍第 19 項之檔案伺服器，其中該安全子集合包括一 Unix 安全型態。

22. 如申請專利範圍第 16 項之檔案伺服器，其中該檔案伺服器可改變相關於該檔案之安全型態，以響應一檔案伺服器需求。

23. 如申請專利範圍第 22 項之檔案伺服器，其中當該檔案伺服器需求成功時，該檔案伺服器可改變相關於該檔案之安全型態，以響應一檔案伺服器需求。

24. 如申請專利範圍第 22 項之檔案伺服器，其中該檔案伺服器可將第一安全型態中一相關於該檔案之第一組許可轉換成一第二安全型態的第二組許可，其中該第二組許可與該第一組許可係等量的限定。

25. 一種在具有複數個檔案之檔案伺服器中的一資料結構，結合一安全型態以及各具有從該檔案伺服器可用之複數個安全型態間所選定的安全型態之檔案。

26. 如申請專利範圍第 25 項之資料結構，其中該等複數個安全型態包括一視窗 NT 安全型態。

27. 如申請專利範圍第 25 項之資料結構，其中該等複數個安全型態包括一 Unix 安全型態。

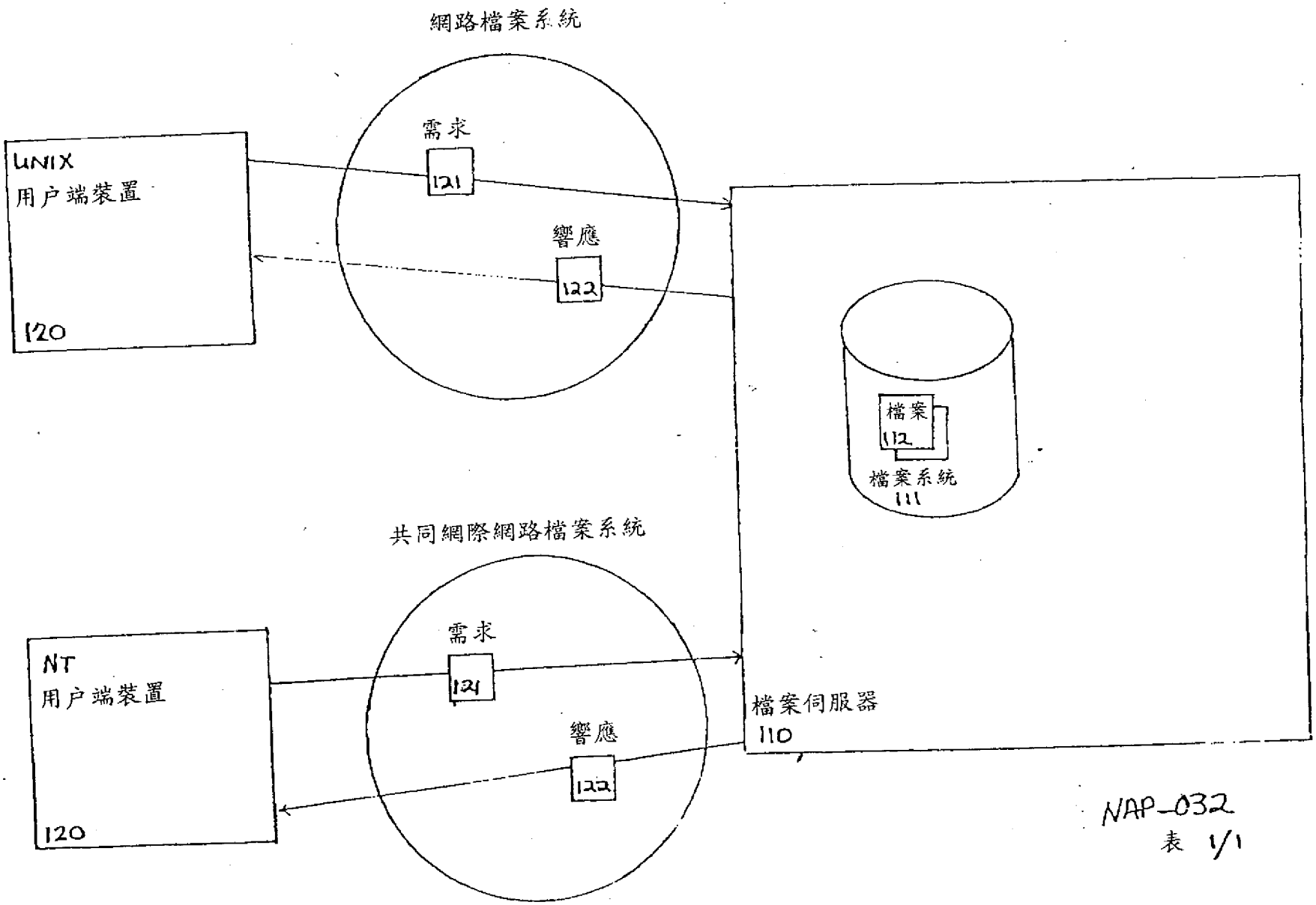
28. 一種在具有複數個檔案及一相關於各具有從該檔案伺服器可用之複數個安全型態間所選定的安全型態之檔案安全型態的檔案伺服器中的資料結構，結合該複數

六、申請專利範圍

個安全型態之一安全子集合以及該檔案伺服器上一可用檔案的子樹。

29. 如申請專利範圍第 28 項之資料結構，其中該安全子集合包括一視窗 NT 安全型態。

30. 如申請專利範圍第 28 項之資料結構，其中該安全子集合包括一 Unix 安全型態。



NAP-032
表 1/1

公告本

申請日期	88.4.7
案號	88105522
類別	G06F 1/60

（以上各欄由本局填註）

88年9月20日 修正補充

A4 C4 新 444154

(修正頁)88年9月

發明 新型 專利說明書

一、發明新型名稱	中文	多重通訊協定檔案伺服器中的檔案存取控制
	英文	"FILE ACCESS CONTROL IN A MULTI-PROTOCOL FILE SERVER"
二、發明創作人	姓名	1. 大衛 西斯 2. 安德拉 柏爾 3. 羅勃特 J. 浩利 4. 馬可 慕勒斯坦 5. 瓊恩 皮爾森
	國籍	均美國
	住、居所	1. 美國加州鄧托拉谷市老西班牙徑245號 2. 美國加州洛斯蓋托市藍丘皮耶塔路785號 3. 美國加州聖荷西市希爾凱斯特路1233號 4. 美國加州摩根丘市威尼斯路15105號 5. 美國加州孟羅公園市沙丘路692號
三、申請人	姓名（名稱）	美商奈特渥克家電用品公司
	國籍	美國
	住、居所（事務所）	美國加州桑尼維爾市東傑凡路495號
	代表人姓名	法蘭絲 B. 拜勒特