三、發明人：（共 5 人）

姓　名：（中文/英文）

1.蘇沙安　瑪麗　凱霍安

KEOHANE, SUSANN MARIE

2.傑納德　法籃西斯　馬伯替

MCBREARTY, GERALD FRANCIS

3.尚恩　派崔克　莫里安

MULLEN, SHAWN PATRICK

4.潔西卡　凱莉　莫里歐

MURILLO, JESSICA KELLEY

5.強尼　謝明翰

SHIEH, JOHNNY MENG-HAN

住居所或營業所地址：（中文/英文）

1.美國德州奧斯汀市伯克里吉路1911號

1911 BRACKENRIDGE STREET, AUSTIN, TEXAS 78704, U.S.A.

2.美國德州奧斯汀市巴里吉海灣10709號

10709 BAYRIDGE COVE, AUSTIN, TEXAS 78759, U.S.A.

3.美國德州布達市歐克斯鄉村路39號

39 COUNTRY OAKS, BUDA, TEXAS 78610, U.S.A.

4.美國德州霍托市鄉村109路980號

980 COUNTRY ROAD 109, HUTTO, TEXAS 78634, U.S.A.

5.美國德州奧斯汀市鄉村向上區5908號

5908 UPVALLEY RUN, AUSTIN, TEXAS 78731, U.S.A.

國　籍：（中文/英文）

1.-5.均美國　U.S.A.

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2003年05月22日；10/443,675

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明一般係與網路系統有關，特定言之，與分散式檔案系統有關。更特定言之，本發明與用於存取分散式檔案系統之安全特徵有關。

【先前技術】

在通用計算系統例如支援Unix作業系統(operating system；OS)版本的系統中，應用可藉由一組包括一檔案系統的作業系統服務來存取磁碟機上所儲存的資料。檔案系統可由一電腦系統採用以將一較大的檔案集合組織成個別檔案及檔案目錄，並將此等檔案映射於儲存裝置例如碟片上。檔案系統包含兩個基本組件：控制檔案實體呈現之程式及碟片上所儲存的檔案本身。

在分散式計算環境中，許多計算系統可藉由通信網路或其他耦合設備而互連，且可藉由分散式檔案系統來共享檔案。檔案系統輸出者通常係在伺服器節點(控制存取包含檔案系統資料之碟片之計算系統)上得以執行，而檔案系統輸入者通常係在用戶節點(其他所利用以存取碟片上之檔案之計算系統)上得以執行。由用戶節點上的使用者存取所共享檔案係稱作「遠端」存取。由伺服器節點上的使用者存取所共享檔案係稱作「本地」存取。

網路檔案系統係儲存於一網路之一伺服器或節點上，該伺服器或節點係可自通常與網路遠端連接之用戶端(即使用者電腦)來存取。實際鏈路可為如標準的以乙太網路為基

礎的區域網路(local area network；LAN)中之有線鏈路或一無線鏈路，例如藍芽虛擬私人網路(Virtual Private Network；VPN)。透過用戶端存取檔案系統之程序係稱作「裝載一檔案系統」。當裝載一檔案系統時，檔案系統之控制程式自與檔案系統物件之佈局有關之碟片讀取某些資訊。藉由此資訊，檔案系統構造所熟知為「虛擬檔案系統」或Vfs之資料結構。每次打開檔案或使得檔案可存取時，檔案系統建立稱作「vnode」之一資料結構，其與vfs呈連鎖式。

每一vnode包含給定檔案之有關資訊，且包含對實體檔案系統之資料結構之參考。實體檔案系統之資料結構包含例如檔案之所有者、檔案之大小、檔案建立之日期與時間及檔案區塊在碟片上的位置之資訊。檔案系統包括內部資料(稱作元資料)以管理檔案。元資料可包括指示以下資訊之資料：檔案之每一資料區塊所儲存之位置；檔案之記憶體已修改之版本所儲存之位置；及檔案之許可與所有者。

隨著越來越多的公司使用遠端/網路可存取分散式檔案系統以電子儲存且隨後擷取檔案/文件(包括一些具有敏感資訊之檔案/文件)，分散式檔案系統之安全變得更加重要。引入IP安全(IP Security；IPSec)標準套件且其提供兩個基本的安全特徵：認證與加密。換言之，IPSec確保發送及接收機器實際上為所要求之事物且IPSec致動資料在空中得以擾亂使得資料若遭攔截，則其將不可理解。

因而在初始裝載期間，大多數系統需要一使用者認證，其通常包括確認使用者通行碼等。然而，通行碼保護與類

似的安全措施以易破解而出名且很容易危及安全，產業中已認識到，一旦獲得對檔案系統的通用存取，通行碼保護系統對敏感檔案提供極少的保護。

藉由在一授權裝載期間分接入一傳輸中並簡單地如資料自檔案系統傳輸至用戶系統一樣來拷貝資料，更多高級駭客亦取得對檔案系統上所儲存檔案之存取。此點發生的原因為，對於大多數通行碼保護分散式檔案系統而言，一旦數個安全登錄等級(通行碼確認等)得以完成，檔案自檔案系統之實際傳輸以明文方式發生。因而，當傳輸包括非常敏感的資料時，需要額外的安全措施以確保在傳輸期間明文資料不可藉由簡單地拷貝檔案而得到。

透過此後者方法危及敏感資訊之安全的簡易性在一定程度上取決於由授權使用者正在利用以裝載/存取檔案系統之媒體。例如，無線存取/傳輸通常更傾向於偷聽及破解導線完整(有線)網路媒體。然而，即使標準的乙太網路亦可容易地遭到破壞而未偵測到，因而對於發送敏感資料而言，標準的乙太網路亦為一不安全的選項。

如上所述，產業上已藉由對檔案系統之裝載期間所傳輸的所有資料施加冗長的加密而對針對傳輸媒體的不斷增長的安全需要作出回應。目前，存在數個所設計的加密演算法與標準(例如無線運輸層安全)以為用戶系統/節點與充當檔案系統之主機之伺服器之間的傳輸提供安全。對於所有流量而言，利用冗長的加密需要帶給用戶系統與伺服器繁重的處理負擔。系統的整體性能劣化，且希望實施全系統

之加密用於存取其檔案系統之公司會增加大量成本。儘管大多數流量可能不需要此等級的安全(例如非敏感性資訊/檔案)，但加密會建立到通信機制中且應用到用戶系統與伺服器之間的所有流量中。

隨著公司向使用者(可為行動使用者且希望與網路遠端連接)提供遠端存取，利用無線系統來存取檔案系統正在增長。然而無線連接比有線連接更易遭破解。一些無線使用者使用WTLS，但此安全特徵已知為一相對薄弱的安全等級。即使當大多數用戶正透過符記環來存取檔案系統時，一解決方式亦需要一虛擬私人網路(VPN)資料封裝/加密以存取敏感資料。此VPN資料封裝將進一步負面影響伺服器之速度，原因係其對所有資料進行加密與解密。

亦可能配置VPN或一VPN上的伺服器以識別IP位址或子網路且僅需要在某些子網路上進行加密。此解決方式之一問題為，分散式檔案系統伺服器之管理員必須具有關於未屬於網路範圍內之每一無線節點之知識。若已由一組織在其部門範圍內建起一無線網路，則伺服器管理員需要意識到無線網路從而可將子網路新增到IP位址之VPN清單中。

依據前面所述，本發明認識到，具有一種當請求存取一分散式檔案系統上之敏感檔案時可動態實施已增強的裝載安全之方法、系統與資料處理系統係所想要的。一種無論何時需要在一正在進行的會話期間即將存取敏感檔案/資料時會自動提供一安全裝載之方法與系統將會為一受歡迎的改善。若以一無縫方式完成安全裝載使得已授權之使用

者接收對敏感檔案之存取而不必經歷一斷開及重新裝載的認證程序，同時藉由透過更安全的裝載來發送敏感檔案而遮蔽敏感檔案免遭未授權之捕獲將更受歡迎。

【發明內容】

本發明揭示一種方法、系統與電腦程式產品，當請求存取一網路化檔案系統上之敏感檔案時，其可對該檔案系統動態實施已增強的裝載安全。用戶系統啟動一標準的裝載與認證程序用於存取檔案系統之檔案。當用戶系統之使用者嘗試存取一特定標記的敏感檔案時，伺服器執行一終止目前裝載的軟體編碼。重新配置伺服器將重新裝載伺服器之任何嘗試自與用戶所關聯之IP位址發送給一安全埠。當會話已由伺服器終止時，程式化該用戶系統以自動嘗試重新裝載伺服器。在重新裝載操作中，伺服器識別用戶之IP位址並將用戶發送給安全埠。

因而在需要在一正在進行的會話(在一標準裝載上得以啟動)期間即將存取敏感檔案/資料之任何時候會自動提供一安全裝載。因而透過一安全裝載之發送得以以一無縫方式完成使得已授權之使用者可接收對敏感檔案之存取而不必經歷重大的延遲或一可見斷開，該延遲或斷開需要使用者啟動重新裝載及認證程序。同時藉由透過更安全的已建立之裝載來發送敏感檔案而遮蔽敏感檔案免遭未授權之捕獲。

本發明之以上內容以及額外之目的、特徵與優點在以下詳細說明中將顯而易見。

【實施方式】

現在藉由參考圖式且特別藉由參考圖1A來說明一電腦系統之方塊圖，其可用作作為分散式檔案系統之主機之一伺服器或用作用以裝載作為分散式檔案系統之主機之伺服器之一用戶系統。電腦系統100包含透過系統匯流排/互連110所連接之處理器102與記憶體104。電腦系統100亦包含與互連110所耦合之輸入/輸出(I/O)通道控制器(Channel Controller；CC) 109。I/O CC 109提供與I/O裝置106之連接，包括冗餘磁碟陣列(Redundant Array of Disk；RAID) 114。RAID 114儲存由處理器正在執行之應用所需要之已載入記憶體之指令與資料。依據所說明具體實施例，RAID 114為構成檔案系統112之複數個檔案提供儲存媒體。

電腦系統100進一步包含網路連接裝置108，該等網路連接裝置可包括有線線路數據機、無線數據機及乙太網路卡等。存取至I/O裝置106與網路連接裝置108及自該I/O裝置106與網路連接裝置108之存取係透過I/O通道控制器(I/OCC) 109進行發送，如下進一步所述I/O通道控制器包括需要時用於透過一「安全」路徑/通道/埠來完成自動重新建立至/自電腦系統100之一裝載之邏輯組件。

電腦系統100包括作業系統(OS) 122、檔案系統軟體應用124、裝載編碼125及分散式檔案系統網路安全延伸(Distributed Filesystem Network Security Extension；DFNSE) 126。當電腦系統100正在用以充當檔案系統112之主機時，檔案系統軟體應用124對檔案系統112提供基本的存取、維

護與更新。

當位於用戶系統範圍內時，檔案系統軟體應用124包括用戶版本的裝載編碼125，其用於完成充當檔案系統之主機之伺服器之裝載及自動重新裝載。在所述具體實施例中，無論何時伺服器之一已建立的裝載遭毀壞/遺失而用戶未完成對伺服器之卸載時，自動重新裝載程序係由用戶系統來實施。在所述具體實施例中，伺服器可發出一FYN命令以終止目前裝載且從而強制用戶啟動對伺服器之重新裝載。FYN命令係回應於對需要特定安全保護之特定檔案之存取而發出，以下將更詳細地說明此點。

返回圖1A及對檔案系統軟體應用124之說明，當在一伺服器內進行執行時，檔案系統軟體應用124包括用於接收、維護及確認各種使用者與用戶系統之憑證資訊之編碼、用於維護檔案系統112之編碼及用於選擇性啟動一安全軟體(稱作分散式檔案系統網路安全延伸(DFNSE)126)之編碼以及有關回應。DFNSE 126提供本發明特徵之主幹且以下將參考圖3A至3C及4A說明在一伺服器上執行DFNSE 126。在一基本等級上，DFNSE 126決定針對檔案系統112之特定檔案允許/授權安全存取之等級為何及何時啟動本發明之已增強的安全措施。

現在參考圖2說明包含多個互連電腦系統之一範例性網路，該等電腦系統可進行與圖1之電腦系統100類似之配置，其較佳地用以提供伺服器或用戶功能用於分別充當分散式檔案系統之主機或存取分散式檔案系統。網路200包含

以三個(或更多)互連伺服器203為主機之一分散式檔案系統202。網路200亦包含複數個透過一網路主幹210與分散式檔案系統202所連接之用戶系統201。網路主幹210包含一或多個可依據網路協定例如乙太網路或符記環進行配置之網路連接性系統(或子網路)。例如此等子網路可為有線線路或無線區域網路(LAN)或一廣域網路(WAN)例如網際網路。此外，子網路可包括光纖網路。

分散式檔案系統202係透過位於伺服器203之至少一者上之一或多個埠(未顯示)而直接耦合於網路主幹210。用戶系統201可直接耦合於網路主幹(有線線路)或透過藉由無線天線207所說明之一無線媒體而進行通信連接。用戶系統201透過利用該等各種網路配置之一之各種可用媒體來存取分散式檔案系統202，每一網路配置具有一不同等級的易遭破解性。因而，用戶系統201可透過一不安全的無線網路227來存取及裝載檔案系統202或用戶系統201可利用一安全的光纖網路225來裝載檔案系統202。基於簡潔說明本發明之目的，將假設無線網路227為一標準的未進行加密的不安全網路，而假設光纖網路225為一特定的具有加密的安全連接。每一連接係透過伺服器203可用埠之一不同埠進行發送，在該埠處支援檔案系統202之裝載。

圖1B說明代表檔案系統202之一方塊圖並更詳細地描述組成檔案系統202之檔案。如所述，檔案系統202包含一控制區塊131及複數個檔案132a至132n，每一檔案包括一具有標頭/識別項欄334與安全欄336之元資料標記112。標頭/ID

欄334包含關於檔案ID及已存取檔案之使用者之資訊。安全欄係一指示屬於此檔案之安全等級且從而指示所允許之使用者存取之類型之單一位元欄。依據所說明具體實施例，某些需要最高的安全等級且已限制成僅在一安全裝載上得以存取之檔案(例如檔案1與3)在其個別元資料之安全欄336中係採用「1」進行標記。未如此進行標記之其他檔案(例如採用0進行標記)係普通的(例如檔案2)且可由任何已授權使用者存取而不需要特定的安全裝載。

如上所述，本發明在所說明的具體實施例中引入稱作DFNSE(分散式檔案系統網路安全延伸)之一已增強的安全機制。採用DFNSE，檔案系統伺服器可自與檔案或目錄所關聯之檔案許可推斷出當提供由特定使用者存取檔案時所需要的網路安全等級。DFNSE係一伺服器等級的檔案系統安全執行應用及/或程序。因而，採用DFNSE僅需要伺服器具有關於伺服器所正在利用之網路連接或配接器之知識。

特定硬體、邏輯及軟體組件係提供於能向檔案系統提供一裝載以實施DFNSE之每一伺服器內。圖4係說明此等組件中一些組件之方塊圖。如圖4所示，伺服器203可具有兩個乙太網路配接器(或埠)：en0 403 (其係安全的)及en1 405(其係不安全的)。在一具體實施例中，此等配接器之網路佈局係一致的。即，所選擇的子網路本身提供該安全且伺服器可基於所需要的安全等級在子網路之間進行動態選擇。在另一具體實施例中，額外的加密或其他安全特徵係採用安全配接器en0 403提供。

En0 403連接至一光纖網路225，其係用以發送所有敏感資料，而en1 405連接至一標準的以乙太網路為基礎的有線網路221且係用於發送其他(非敏感的)所有的資料通信。En1 405係用於裝載檔案系統之伺服器之預設埠。該範例性具體實施例假設，標準乙太網路可遭到破壞而未加以偵測之簡易性使得乙太網路對於發送敏感資料而言係一不安全選項。在檔案系統裝載期間，具有關於每一檔案之檔案許可334及安全等級336之詳細知識之伺服器追蹤使用者存取且適當基於正在進行存取之檔案之檔案許可決定何時強制用戶切換到安全網路上。依據所說明具體實施例，對於安全發送與不安全發送而言網路佈局係一致的，從而在自不安全子網路至安全子網路之切換期間，不需要額外的硬體及/或發送協定升級來應付不同佈局。

圖4之伺服器203亦包括一裝載控制器407，其為檔案系統202執行傳統的裝載支援與卸載操作以及依據本發明之特徵之重新裝載配置。裝載控制器407包括DFNSE 126且其較佳地係具體化為在伺服器203上執行之軟體編碼。DFNSE 126操作以觸發裝載控制器407透過標準埠En1 405或安全埠En0 403來發送一裝載請求。當加密係實施於安全埠上時，伺服器203亦包括結合DFNSE 126與En0 403所利用之加密模組409。

在檔案系統存取期間，當請求存取敏感操作係在伺服器203上進行接收時，裝載控制器407將用戶之IP位址標記成需要存取敏感資料之位址。接著伺服器203斷開目前連接

(即伺服器向用戶傳送一FYN)。該用戶自動嘗試重新連接，且裝載控制器407在重新裝載期間識別用戶之IP位址。用戶之會話接著定向於一安全插座層(SSL)埠。因而，雖然初級存取係透過標準埠提供，但當需要存取敏感資料/檔案時，存取係動態地切換至SSL安全埠。

現在轉向圖3B，其說明一程序之流程圖，軟體實施DFNSE安全特徵係藉由該程序而實施於充當檔案系統之主機之伺服器之以上軟體/邏輯配置內。如步驟321所示，程序開始於伺服器之標準埠自一用戶所接收之一標準裝載請求。如步驟323所示，提示使用者需要認證資料(通行碼等)且用戶系統之IP位址係自資料訊包擷取。如步驟325所示，會話係在標準的埠上開啟，且IP位址與使用者認證資料係儲存於與特定會話所連接之一參數檔案內。一旦會話已建立，即與存取許可等所關聯之伺服器邏輯組件監視使用者之互動(如步驟327所示)及在步驟329中決定使用者是否正在請求存取敏感檔案。

採用遠端用戶上的使用者授權/憑證及對正在存取之檔案之許可對正在滿足用戶之檔案請求之伺服器進行程式化。若正在存取之檔案不為敏感的，則如步驟331所示在標準埠上向使用者提供常規存取。然而，當用戶正在請求之檔案為在準許存取之前需要一更安全通道之一敏感檔案時，在步驟333處進行下一決定，即決定使用者是否具有適當的存取許可來存取該檔案。若使用者不具有適當的存取許可，則如步驟335所示拒絕該請求。然而，若使用者之憑

證指示使用者具有存取特定檔案之許可，則如步驟337所示啟動DFNSE安全協定。啟動DFNSE使得伺服器藉由向用戶發出一FYN且同時配置一更安全的埠以自具有採用會話參數所保存之IP位址之用戶接受重新裝載來強迫用戶之一卸載。如步驟339所示，伺服器接著透過安全埠提供對檔案之安全存取。

圖3A係實施本發明中所涉及程序之流程圖，其主要自使用者/用戶系統的角度而言。如步驟302所示當使用者(透過用戶系統)首先裝載充當檔案系統之主機之一伺服器且如步驟304所示請求存取檔案系統時，程序開始。當用戶最初裝載NFS檔案系統時，裝載係藉由預設透過一標準的TCP連接而完成。例如，連接可至所熟知的NFS埠2048。伺服器具有結合於此埠之一傾聽插座且依據標準(非安全)協定操作。特別地，在所述具體實施例中，標準協定係藉由當請求存取敏感檔案時所實施之DFNSE協定而得以增強。

當自用戶請求一連接時，伺服器之傾聽插座基本上本身複製且結合於與遠端用戶之連接處。因而傾聽插座保持開啟以處置其他連接請求。用戶認證係啟動於所示步驟306處且在步驟308處決定用戶認證是否成功。若用戶/使用者認證程序不成功，則如步驟310所示拒絕存取檔案系統且斷開裝載。接著如步驟311所示程序結束。或者如步驟309所示開啟一會話且向使用者提供對檔案系統之存取。

如步驟312所示用戶系統監視斷開之連接且如步驟314所示決定連接是否變得無法回應或已在伺服器端過早斷開

(即理想地當伺服器所發出之FYN已接收時)。當連接變得無法回應或斷開時，如步驟316所示用戶啟動已發送至伺服器所指示埠之一重新裝載。

特別地，儘管實際埠對於用戶系統而言可為未知的，但回應於伺服器啟動卸載之重新連接係定向於伺服器之一安全埠上。利用DFNSE安全協定且基於哪個埠係安全的及會話是否需要一安全埠之知識，伺服器可透過一安全埠來請求用戶重新裝載。例如，可使得用戶利用一埠運行安全插座層來重新裝載。特別地，並不需要使用者行動來完成重新裝載與埠切換程序。對伺服器端卸載及隨後之重新裝載之監視在用戶系統處全部作為後台程序發生且使用者(用戶)並未意識到至更安全埠之切換。

對透過伺服器端處之一更安全埠之重新發送所需要之內部處理之更詳細說明係由圖3C之流程圖進行說明。如步驟351所示，當存取敏感檔案由DFNSE識別時，程序開始。如步驟352所示，伺服器檢查目前的埠安全。在步驟354處決定目前之埠安全是否足以存取所請求的檔案(取決於檔案之敏感程度，在所述具體實施例中藉由讀取檔案之安全位元而導出)。若目前的埠安全足以存取所請求的檔案，則如步驟356所示提供該存取。

在一替代具體實施例中，重新裝載功能可選擇性地進行自動化且程序將需要接著決定自動重新裝載之特徵是否已致動。在此替代具體實施例中，若自動重新裝載能力未得以致動，則實際上將提示使用者來透過一安全裝載進行重

新裝載。

返回圖3C所述具體實施例，當埠安全不足夠時，如步驟358所示伺服器藉由為會話選擇一更安全的埠(例如En0)來作出回應。如步驟360所示伺服器快照該會話之認證與裝載參數(包括用戶之IP位址)且將此等參數傳送給更安全埠之控制邏輯組件。傳送發生時具有非常小的延時，因而更安全埠進行自動配置以自該用戶接收一重新裝載並繼續支援處於進程中的會話。已配置安全埠後，給予裝載控制器對應的埠號碼以及用戶之IP位址。如步驟362所示，伺服器終止第一標準埠上的裝載且當自用戶接收到一重新裝載時，透過更安全埠來重新建立該會話。

特別地，回應於伺服器終止最初裝載，用戶啟動由使用者定向於第二安全鏈路之重新裝載。此點重新建立用戶之最初會話，但透過第二埠。重新建立該連接包括檢查用戶之IP位址及將其與所建起以自該IP位址接收該連接之埠進行匹配。整個程序發生在後台中，因而從使用者角度來看已完成一無縫埠切換。

在一替代具體實施例中，屬於特定檔案之安全等級係由已向其提供對特定檔案之存取之使用者(或所選取的用戶系統)決定。因而，若檔案存取許可係限制僅給檔案系統之管理員，則安全等級係較高的，而給予常規雇員之檔案存取許可指示所需要之一相對較低的安全等級。當使用者最初建立該檔案且將存取許可指派給該檔案時已完成檔案之安全等級之決定。一旦將檔案放置於檔案系統內，檔案就

自動地繼承適當的網路安全保護。採用此實施方案，檔案系統(例如UNIX－rwx、rwx、針對使用者之rwx、針對群組之rwx、其他)內之檔案上現存的檔案許可併入本文所提供的安全模型中而不需要延伸的系統管理與配置。因而，本發明不需要在每一檔案基礎上重新配置現存的檔案系統。採用本發明，亦不需要將敏感檔案移至一安全伺服器上。

雖然已參考較佳具體實施例特別顯示及說明本發明，但熟習此項技術者應明白，可進行各種形式及細節的變更而不會背離本發明之精神與範疇。例如，儘管採用所特定參考的NFS來說明本發明，但本發明亦可應用於DFS或AFS及其他類似協定。

【圖式簡單說明】

隨附的申請專利範圍中提出本發明特有的新穎特徵。然而本發明本身及其較佳的使用模式、更多目的與優點藉由參考以上結合附圖對所述具體實施例之詳細說明可最佳地加以理解，其中：

圖1A係在其內部可實施本發明之特徵之一資料處理系統之方塊圖；

圖1B係依據本發明之一具體實施例表示圖1A之檔案系統內具有指示所需安全等級之一安全標記之檔案之一方塊圖；

圖2係依據本發明之一具體實施例於其內部可實施本發明之特徵之一分散式網路之方塊圖；

圖3A係依據本發明一具體實施例之一程序之流程圖，在

透過一標準裝載存取期間藉由該程序向用戶提供對敏感檔案之存取；

圖3B與3C係依據本發明一具體實施例之一程序之流程圖，伺服器藉由該程序來監視且控制用戶對敏感檔案之存取請求以確保對此等檔案之存取係透過一安全通道進行發送；及

圖4係依據本發明之一具體實施例說明在一單一連續會話期間用於無縫地完成檔案系統上之一用戶會話自一標準、不安全通道至一安全通道之切換之邏輯組件之一方塊圖。

【主要元件符號說明】

100	電腦系統
102	處理器
104	記憶體
106	輸入/輸出裝置
108	網路連接裝置
109	輸入/輸出通道控制器
110	系統匯流排/互連
112	檔案系統/元資料標記
114	冗餘碟片陣列
122	作業系統
124	檔案系統軟體應用
125	裝載編碼
126	分散式檔案系統網路安全延伸

131	控制區塊
132a至n	檔案
200	網路
201	用戶系統
202	分散式檔案系統
203	伺服器
207	無線天線
210	網路主幹
221	有線網路
225	安全的光纖網路
227	不安全的無線網路
334	標頭/識別項欄
336	安全欄
en0 403	乙太網路配接器
en1 405	乙太網路配接器
407	裝載控制器
409	加密模組

五、中文發明摘要：

本發明係揭示一種安全協定，當請求存取一網路化檔案系統上之敏感檔案時，該協定可對該檔案系統動態實施已增強的裝載安全。當一用戶系統之使用者嘗試存取一特定標記的敏感檔案時，充當該檔案系統之主機之該伺服器執行一終止該目前裝載，且重新配置該等伺服器埠以透過一更安全的埠來自該用戶接收一重新裝載之軟體編碼。在該重新裝載操作期間向已重新配置伺服器埠之該伺服器提供該用戶之IP位址，且該伺服器與該IP位址匹配。以一無縫方式完成向一安全裝載之切換從而允許已授權之使用者存取敏感檔案，而不必因昂貴的加密及其他資源加強安全特徵而使該伺服器混亂。該使用者並未經歷較大延遲，同時在向該用戶系統傳輸期間，該敏感檔案得以遮蔽而免遭非授權之捕獲。

六、英文發明摘要：

A security protocol that dynamically implements enhanced mount security of a filesystem when access to sensitive files on a networked filesystem is requested. When the user of a client system attempts to access a specially-tagged sensitive file, the server hosting the filesystem executes a software code that terminates the current mount and re-configures the server ports to accept a re-mount from the client via a more secure port. The server re-configured server port is provided the IP address of the client and matches the IP address during the re-mount operation. The switch to a secure mount is completed in a seamless manner so that authorized users are allowed to access sensitive files without bogging down the server with costly encryption and other resource-intensive security features. No significant delay is experienced by the user, while the sensitive file is shielded from un-authorized capture during transmission to the client system.

十、申請專利範圍：

1. 一種於一資料處理系統中用於為傳輸至少一檔案提供安全之方法，該系統包含(1)一儲存媒體，於其上儲存至少一具有一預置存取許可之第一檔案，(2)至少一第一標準埠及一第二安全埠，其係用於連接該資料處理系統與外部用戶系統，及(3)用於透過該第一埠及該第二埠來選擇性發送該至少一檔案之傳輸之邏輯組件，該方法包含：

回應於該外部用戶系統對存取該第一檔案之一請求而檢查該第一檔案之該預置存取許可；及

當該第一檔案之該預置存取許可指示該第一檔案需要安全存取時，透過該第二埠向外部用戶系統動態地發送對該第一檔案之一傳輸。

2. 如申請專利範圍第1項之方法，其進一步包含：

當該預置存取許可指示一常規存取係足夠時，透過該第一標準埠來發送該第一檔案之該傳輸。

3. 如申請專利範圍第1項之方法，其進一步包含：

透過該第一標準埠來致動該資料處理系統之一第一裝載；及

僅當該第一檔案需要安全存取時透過該第二安全埠致動該資料處理系統之一第二裝載。

4. 如申請專利範圍第1項之方法，其中該資料處理系統進一步包含與該第二安全埠關聯之一加密模組，該動態發送步驟包含：

首先利用該加密模組來加密該第一檔案。

5. 如申請專利範圍第1項之方法，其中該資料處理系統進一步包含用於配置該第一標準埠與該第二安全埠來用於支援該用戶系統之一裝載之重新配置邏輯組件，該動態發送步驟包含：

首先配置該第二安全埠以支援自該用戶系統所接收之一重新裝載操作；

藉由該用戶系統終止該第一標準埠上之一目前裝載；及

儲存該目前裝載之會話參數以致動該會話在該第二安全埠上之無縫繼續。

6. 如申請專利範圍第5項之方法，其中該配置與儲存步驟包括：

擷取該用戶系統之一IP位址；

將該IP位址放置於該第二安全埠之一配置中，其中該第二安全埠自該用戶系統自動識別一重新裝載操作，且重新建立與該用戶系統之會話。

7. 如申請專利範圍第1項之方法，其中該預置存取許可係為與該第一檔案所連接之元資料內之一位元，且該方法進一步包含讀取該位元之一值以評估該第一檔案是否需要安全存取。

8. 如申請專利範圍第1項之方法，其中該預置存取許可包括哪些特定使用者得以允許透過一安全存取來存取該第一檔案之一識別，該方法進一步包含：

將該用戶系統之一使用者與具有存取該檔案之許可之該等特定使用者進行比較；及

當該使用者係該等特定使用者之一時，自動啟動透過該第二安全埠對該第一檔案之一傳輸之一重新發送。

9. 如申請專利範圍第1項之方法，其中該第一標準埠透過一第一不安全網路連接至該用戶系統，且該第二安全埠透過一第二安全網路連接至該用戶系統。

10. 如申請專利範圍第1項之方法，其中：

該資料處理系統係具有連接該第一標準埠與該用戶系統之一第一子網路，及連接該第二安全埠與該用戶系統之一第二子網路之一網路內之一伺服器；

該第一檔案係儲存於一檔案系統內；

該檢查步驟包括存取該檔案系統及定位該第一檔案；及

該發送步驟包括當該檔案需要安全存取時，透過該第二子網路來傳輸該檔案，及當該第一檔案不需要安全存取時，透過該第一子網路來傳輸該第一檔案。

11. 一種於一資料處理系統中用於為傳輸至少一檔案提供安全之系統，該資料處理系統包含(1)一儲存媒體，於其上儲存至少一具有一預置存取許可之第一檔案，(2)至少一第一標準埠及一第二安全埠，其係用於連接該資料處理系統與外部用戶系統，及(3)用於透過該第一埠及該第二埠來選擇性發送該至少一檔案之傳輸之邏輯組件，該系統包含：

用於回應於該外部用戶系統對存取該第一檔案之一請求而檢查該第一檔案之該預置存取許可之邏輯組件；及

當該第一檔案之該預置存取許可指示該第一檔案需要安全存取時，用於透過該第二埠向外部用戶系統動態地發送對該第一檔案之一傳輸之邏輯組件。

12. 如申請專利範圍第11項之系統，其進一步包含：

當該預置存取許可指示一常規存取係足夠時，用於透過該第一標準埠來發送該第一檔案之該傳輸之邏輯組件。

13. 如申請專利範圍第11項之系統，其進一步包含：

用於透過該第一標準埠來致動該資料處理系統之一第一裝載之邏輯組件；及

僅當該第一檔案需要安全存取時，用於透過該第二安全埠致動該資料處理系統之一第二裝載之邏輯組件。

14. 如申請專利範圍第11項之系統，其中該資料處理系統進一步包含與該第二安全埠關聯之一加密模組，用於動態發送之該邏輯組件包含：

用於首先利用該加密模組來加密該第一檔案之邏輯組件。

15. 如申請專利範圍第11項之系統，其中該資料處理系統進一步包含用於配置該第一標準埠與該第二安全埠來用於支援該用戶系統之一裝載之重新配置邏輯組件，用於動態發送之該邏輯組件包含：

用於首先配置該第二安全埠以支援自該用戶系統所接收之一重新裝載操作之邏輯組件；

用於藉由該用戶系統終止該第一標準埠上之一目前裝

載之邏輯組件；及

用於儲存該目前裝載之會話參數以致動該會話在該第二安全埠上之無縫繼續之邏輯組件。

16. 如申請專利範圍第15項之系統，其中該配置與儲存步驟包括：

用於擷取該用戶系統之一IP位址之邏輯組件；

用於將該IP位址放置於該第二安全埠之一配置中之邏輯組件，其中該第二安全埠自該用戶系統自動識別一重新裝載操作，且重新建立與該用戶系統之會話。

17. 如申請專利範圍第11項之系統，其中該預置存取許可係為與該第一檔案所連接之元資料內之一位元，且該系統進一步包含讀取該位元之一值以評估該第一檔案是否需要安全存取。

18. 如申請專利範圍第11項之系統，其中該預置存取許可包括哪些特定使用者得以允許透過一安全存取來存取該第一檔案之一識別，該系統進一步包含：

用於將該用戶系統之一使用者與具有存取該檔案之許可之該等特定使用者進行比較之邏輯組件；及

當該使用者係該等特定使用者之一時，用於自動啟動透過該第二安全埠對該第一檔案之一傳輸之一重新發送之邏輯組件。

19. 如申請專利範圍第11項之系統，其中該第一標準埠透過一第一不安全網路連接至該用戶系統，且該第二安全埠透過一第二安全網路連接至該用戶系統。

20. 如申請專利範圍第11項之系統，其中：

該資料處理系統係具有連接該第一標準埠與該用戶系統之一第一子網路，及連接該第二安全埠與該用戶系統之一第二子網路之一網路內之一伺服器；

該第一檔案係儲存於一檔案系統內；

用於檢查之該邏輯組件包括用於存取該檔案系統及定位該第一檔案之構件；及

用於發送之該邏輯組件包括當該檔案需要安全存取時，用於透過該第二子網路來傳輸該檔案及當該第一檔案不需要安全存取時，用於透過該第一子網路來傳輸該第一檔案之構件。

21.一種於一網路中之檔案系統存取控制機制，該網路包含(1)充當一檔案系統之主機，且具有至少一第一標準埠及一第二安全埠之一伺服器，(2)一用戶，及(3)複數個用於連接該伺服器與該用戶之傳輸子網路，其中該等複數個傳輸子網路包括一第一標準子網路及一第二安全子網路，該檔案系統存取控制機制包含：

用於回應於該外部用戶系統對存取該第一檔案之一請求而檢查該第一檔案之該預置存取許可之邏輯組件；及

當該第一檔案之該預置存取許可指示該第一檔案需要安全存取時，用於透過該第二埠向外部用戶系統動態地發送對該第一檔案之一傳輸之邏輯組件。

22. 如申請專利範圍第21項之檔案系統存取控制機制，其進一步包含：

當該預置存取許可指示一常規存取係足夠時，用於透過該第一標準埠來發送該第一檔案之該傳輸之邏輯組件。

23. 如申請專利範圍第21項之檔案系統存取控制機制，其進一步包含：

用於透過該第一標準埠來致動該資料處理系統之一第一裝載之邏輯組件；及

僅當該第一檔案需要安全存取時，用於透過該第二安全埠致動該資料處理系統之一第二裝載之邏輯組件。

24. 如申請專利範圍第21項之檔案系統存取控制機制，其中該資料處理系統進一步包含與該第二安全埠關聯之一加密模組，用於動態發送之該邏輯組件包含：

用於首先利用該加密模組來加密該第一檔案之邏輯組件。

25. 如申請專利範圍第21項之檔案系統存取控制機制，其中該資料處理系統進一步包含用於配置該第一標準埠與該第二安全埠來用於支援該用戶系統之一裝載之重新配置邏輯組件，用於動態發送之該邏輯組件包含：

用於首先配置該第二安全埠以支援自該用戶系統所接收之一重新裝載操作之邏輯組件；

用於藉由該用戶系統終止該第一標準埠上之一目前裝載之邏輯組件；及

用於儲存該目前裝載之會話參數以致動該會話在該第二安全埠上之無縫繼續之邏輯組件。

26. 如申請專利範圍第25項之檔案系統存取控制機制，其中

該配置與儲存步驟包括：

用於擷取該用戶系統之一IP位址之邏輯組件；

用於將該IP位址放置於該第二安全埠之一配置中之邏輯組件，其中該第二安全埠自該用戶系統自動識別一重新裝載操作且重新建立與該用戶系統之會話。

27. 如申請專利範圍第21項之檔案系統存取控制機制，其中該預置存取許可係為與該第一檔案所連接之元資料內之一位元，且該系統進一步包含讀取該位元之一值以評估該第一檔案是否需要安全存取。

28. 如申請專利範圍第21項之檔案系統存取控制機制，其中該預置存取許可包括哪些特定使用者得以允許透過一安全存取來存取該第一檔案之一識別，該系統進一步包含：

用於將該用戶系統之一使用者與具有存取該檔案之許可之該等特定使用者進行比較之邏輯組件；及

當該使用者係該等特定使用者之一時，用於自動啟動透過該第二安全埠對該第一檔案之一傳輸之一重新發送之邏輯組件。

29. 如申請專利範圍第21項之檔案系統存取控制機制，其中該第一標準埠透過一第一不安全網路連接至該用戶系統，且該第二安全埠透過一第二安全網路連接至該用戶系統。

30. 如申請專利範圍第21項之檔案系統存取控制機制，其中：

該資料處理系統係具有連接該第一標準埠與該用戶系統之一第一子網路，及連接該第二安全埠與該用戶系統

之一第二子網路之一網路內之一伺服器；

該第一檔案係儲存於一檔案系統內；

用於檢查之該邏輯組件包括用於存取該檔案系統及定位該第一檔案之構件；及

用於發送之該邏輯組件包括當該檔案需要安全存取時，用於透過該第二子網路來傳輸該檔案及當該第一檔案不需要安全存取時，用於透過該第一子網路來傳輸該第一檔案之構件。

十一、圖式：

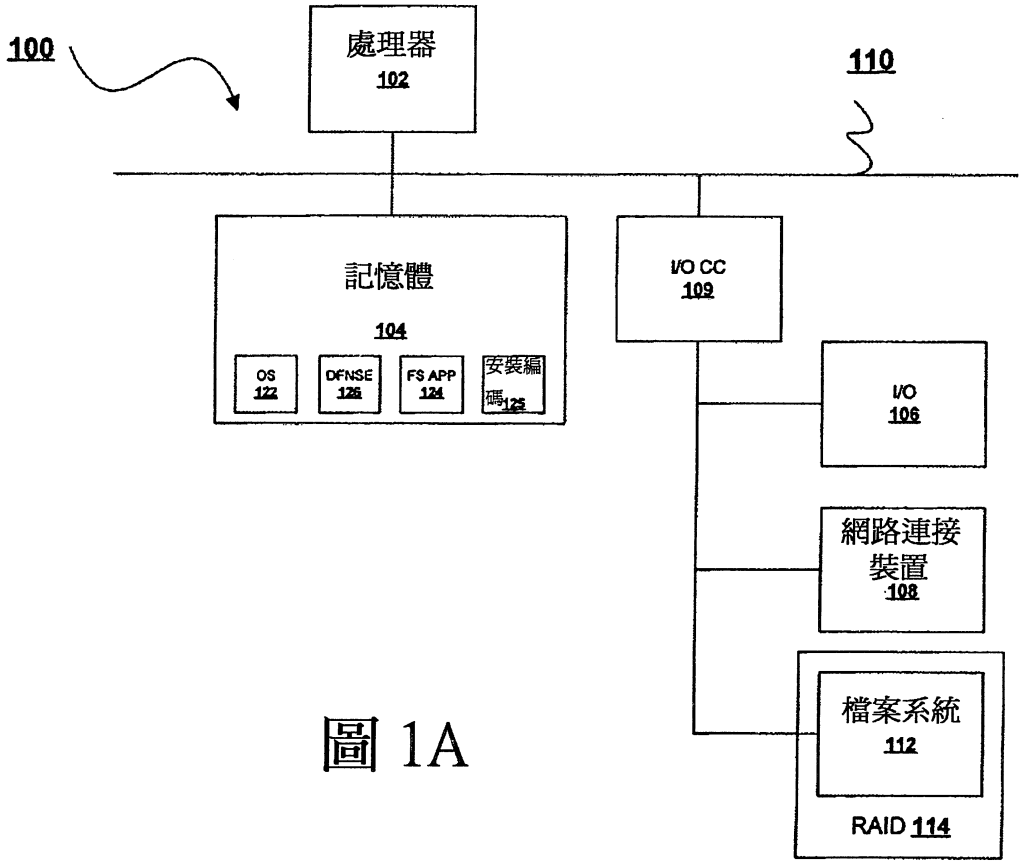
100
處理器
102
110
記憶體
104
OS
122
DFNSE
126
FS APP
124
安裝編碼
125
I/O CC
109
I/O
106
網路連接裝置
108
檔案系統
112
RAID 114

圖 1A

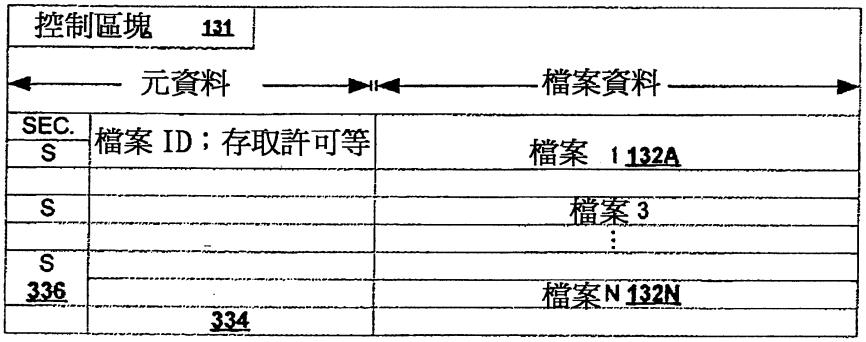
控制區塊 131
元資料
檔案資料
SEC.
S
檔案 ID；存取許可等
檔案 1 132A
S
檔案 3
S
336
檔案N 132N
334

圖 1B

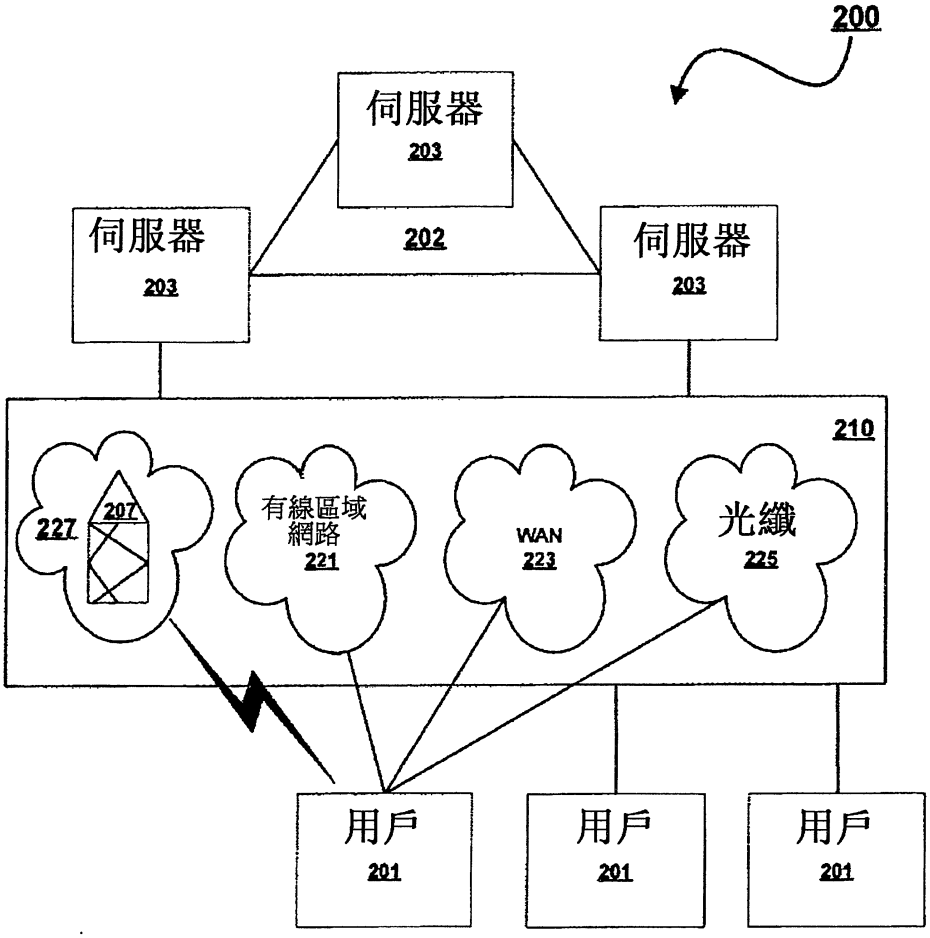
200
伺服器
203
伺服器
203
202
伺服器
203
210
227
207
有線區域
網路
221
WAN
223
光纖
225
用戶
201
用戶
201
用戶
201

圖 2

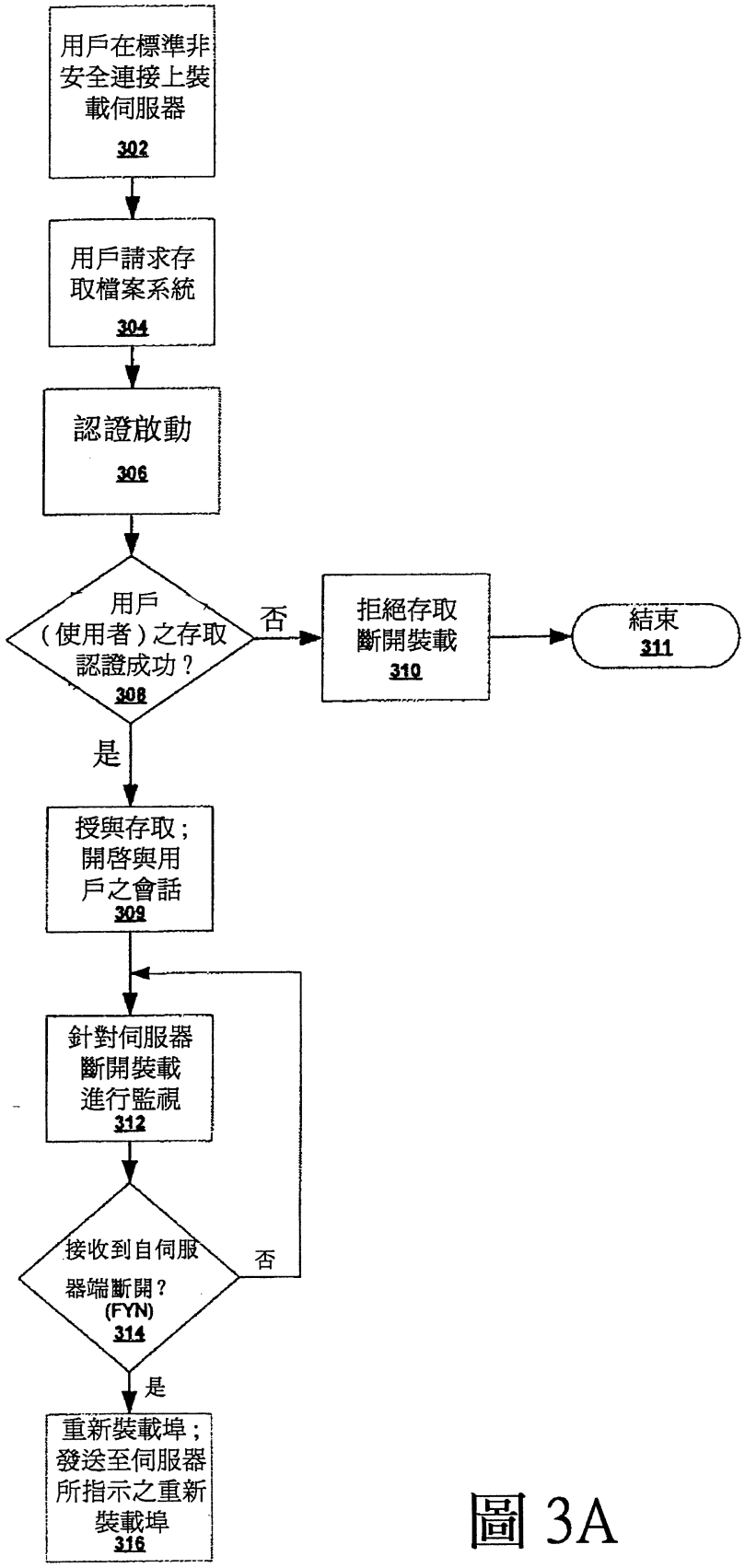
用戶在標準非安全連接上裝載伺服器
302
用戶請求存取檔案系統
304
認證啟動
306
用戶（使用者）之存取認證成功？
308
否
拒絕存取斷開裝載
310
結束
311
是
授與存取；開啓與用戶之會話
309
針對伺服器斷開裝載進行監視
312
接收到自伺服器端斷開？(FYN)
314
否
是
重新裝載埠；發送至伺服器所指示之重新裝載埠
316

圖 3A

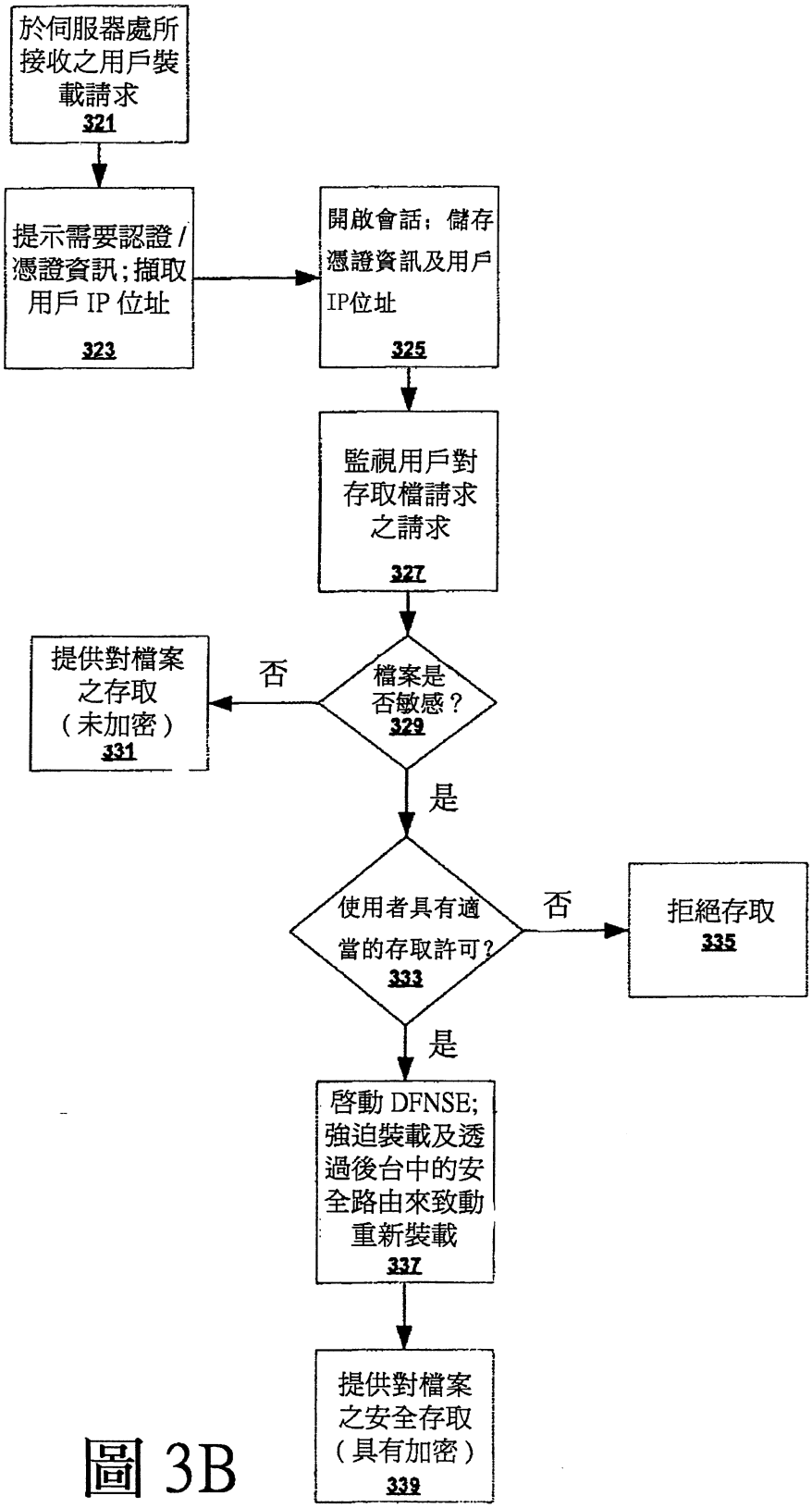
於伺服器處所接收之用戶裝載請求
321
提示需要認證/憑證資訊;擷取用戶 IP 位址
323
開啟會話；儲存憑證資訊及用戶IP位址
325
監視用戶對存取檔請求之請求
327
檔案是否敏感？
329
否
提供對檔案之存取（未加密）
331
是
使用者具有適當的存取許可？
333
否
拒絕存取
335
是
啓動 DFNSE;強迫裝載及透過後台中的安全路由來致動重新裝載
337
提供對檔案之安全存取（具有加密）
339

圖 3B

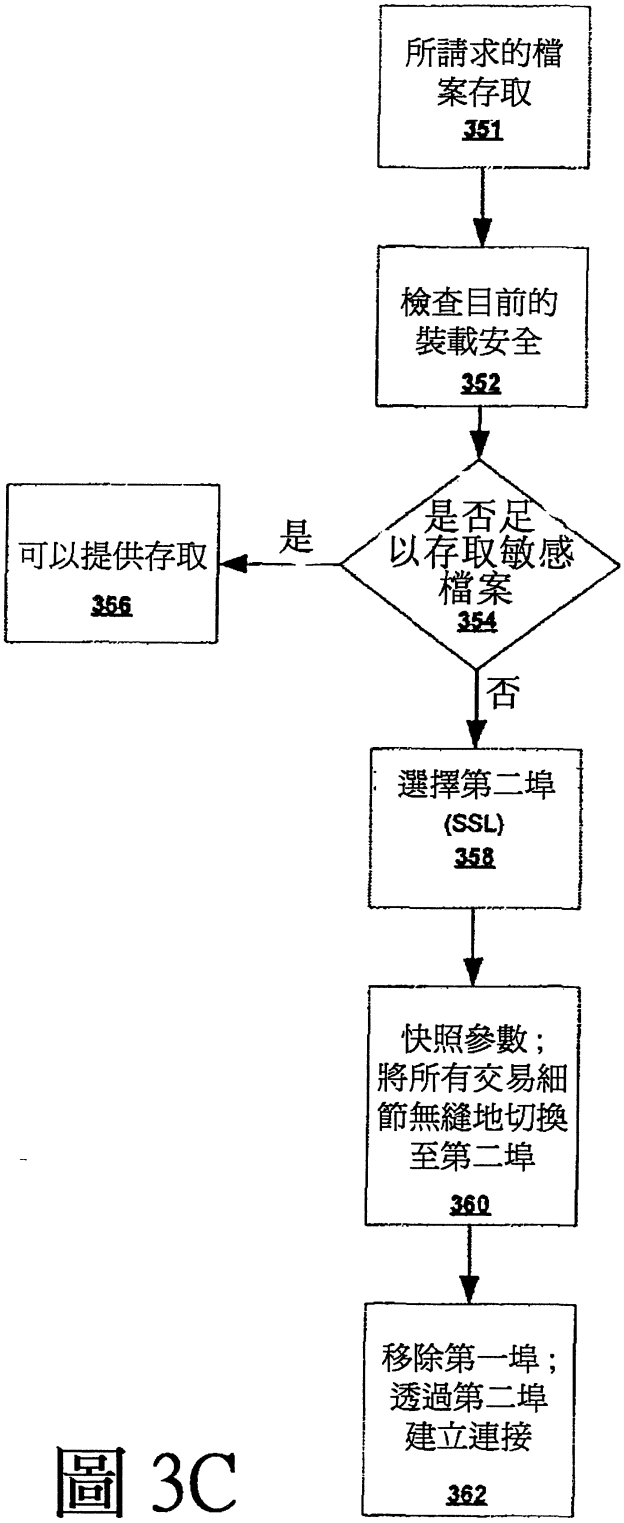
所請求的檔案存取
351
檢查目前的裝載安全
352
是否足以存取敏感檔案
354
是
可以提供存取
356
否
選擇第二埠
(SSL)
358
快照參數；將所有交易細節無縫地切換至第二埠
360
移除第一埠；透過第二埠建立連接
362

圖 3C

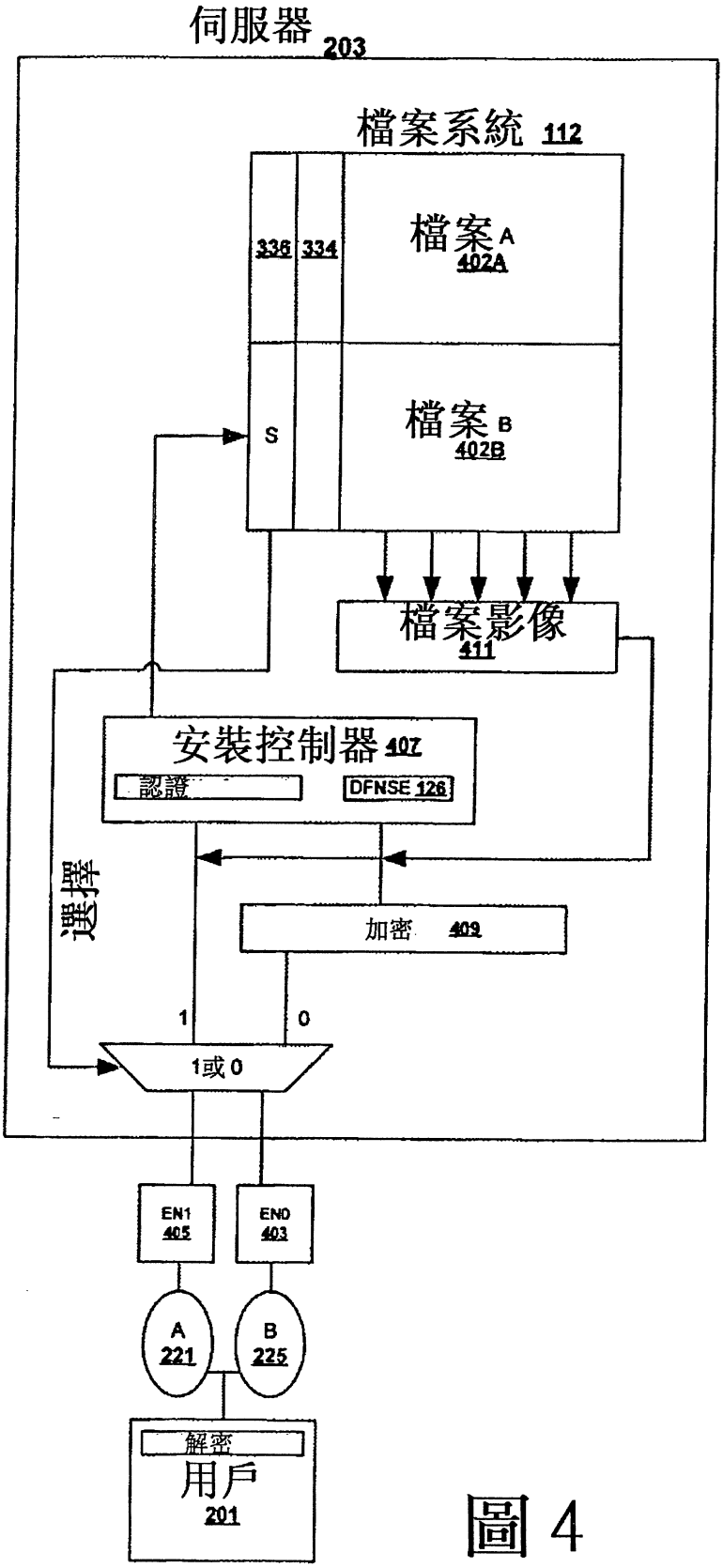
伺服器 203
檔案系統 112
336
334
檔案A 402A
S
檔案B 402B
檔案影像 411
安裝控制器 407
認證
DFNSE 126
選擇
加密 409
1
0
1或0
EN1 405
EN0 403
A 221
B 225
解密
用戶 201

圖 4

七、指定代表圖：

(一)本案指定代表圖為：第（ 3A ）圖。

(二)本代表圖之元件符號簡單說明:

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

公告本

95.12.27
年 月 日修(更)正替換頁

I282229

發明專利說明書

中文說明書替換頁(95年12月)

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：093112916

※ 申請日期：93.5.7　　※IPC 分類：H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

於一資料處理系統中用於為傳輸至少一檔案提供安全之方法與系統及一檔案系統存取控制機制

METHOD AND SYSTEM FOR PROVIDING SECURITY FOR TRANSMISSION OF AT LEAST ONE FILE, AND A FILESYSTEM ACCESS CONTROL MECHANISM

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商萬國商業機器公司

INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）

傑拉德　羅森賽

ROSENTHAL, GERALD

住居所或營業所地址：（中文/英文）

美國紐約州阿蒙市新果園路

NEW ORCHARD ROAD, ARMONK, NY 10504 U. S. A.

國　籍：（中文/英文）

美國 U.S.A.