

448387

申請日期	88. 9. 6
案 號	88110985
類 別	G06F 17/60

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書

新 型

一、發明 名稱	中 文	一般化決策伺服器
	英 文	"GENERALIZED POLICY SERVER"
二、發明 人	姓 名	1.柯利佛德 L. 海諾 2.羅倫斯 R. 利普思棟 3.大衛 S. 史屈內德
	國 籍	1-3.均美國
	住、居所	1-3.均美國加州西湖威里吉市東紹忍歐克斯路3717號
三、申請人	姓 名 (名稱)	美商網際動態公司
	國 籍	美國
	住、居所 (事務所)	美國加州西湖威里吉市東紹忍歐克斯路3717號
	代 表 人 姓 名	柯利佛德 L. 海諾

裝

訂

線

448387

(由本局填寫)

承辦人代碼：
大類：
I P C 分類：

A6

B6

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06月29日 60/091,130 ☒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

經濟部智慧財產局員工消費合作社印製

五、發明說明(1)

1 網路中資訊之安全遞送

交叉參看有關專利申請案

2 交叉參看有關專利申請案

本專利申請案對：在1998年6月29日，由韓納爾(Hannel)，李斯頓(Lipstone)，及史耐德(Schneider)提出申請，標題為"通用決策伺服器"的美國臨時專利申請案第60/091,130號享有優先權。本專利申請案並且是：在1998年3月4日，由大衛·史耐德(David Schneider)等人提出申請，標題為"存取資訊之分佈型管理"的美國專利申請案(U.S.S.N)第09/034,507號之一續篇部份；因而包含該專利申請案的整個闡述和附圖。本專利申請案中的新資料始於標題為"使用在存取過濾器203中的諸多技術之通則"的章節，並包括一些新附圖26到37。

發明背景

2 發明背景 1. 發明領域

3 1. 發明領域

本發明通常與存取資料之控制有關；且說得更明確些，與存取在分佈型環境中的存取資料之控制有關。

2. 有關技藝之描述

3 2. 有關技藝之描述

網際網路(Internet)已革新了資料通信。已經藉由提供諸多通信協定(protocols)和定址方案來達成，不論：電腦系統的實體硬體(physical hardware)，被連接到的實體網路種類，或者被用來將資訊從一個電腦系統發送到另一個電腦

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(2)

系統的諸多實體網路種類如何，該方案使得世界上任何地方的任何電腦系統和世界上任何地方的任何其它電腦系統交換資訊成為可能。使得兩個電腦系統交換資訊的一切要求是：每個電腦系統都要有一個網際網路位址及針對通信協定所需的軟體；並且，藉由許多實體網路的某種組合，兩個機器之間會有一條路由(route)，它可能用來載送根據通信協定而構築的訊息。

然而，電腦系統可能經由網際網路來交換訊息之如此容易已經造成諸多問題。在一方面，它已經使存取資訊變得前所未有之容易和低廉；在另一方面，它已經使它更難保護資訊。網際網路在兩方面已經使它較難保護資訊：

- 較難限制存取操作。假如可能經由網際網路來存取資訊，就有可能隨著存取網際網路資訊而存取任何人的資訊。一旦有經由網際網路而存取資訊，阻擋熟練入侵者就會變成一種困難的技術問題。
- 經由網際網路，在途中(en route)較難維護安全性。將網際網路建構作為一種分包資訊交換網路(packet switching network)。不可能預測訊息由網路將會採取什麼路由。更不可能保證所有資訊交換(switches)的安全性，或保證包括那些載明其來源或目標的訊息部份：在途中都未曾被讀取或改變。

圖1顯示：目前用來增加可經由網際網路存取資訊之網路安全性的技術。圖1顯示：網路101，它由兩個分離內部網路103(A)和103(B)組成，該內部網路皆由網際網路111所

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明(3)

連接。雖然兩個網路103(A)和103(B)一般說來都不可存取資訊，但是從某種意義說來，它們都是網際網路的一部份；在這些網路中的電腦系統都有網際網路位址，並且都會使用網際網路通信協定來交換資訊。兩個這樣的電腦系統出現在圖1中，就像在網路103(A)中的請求者(requestor)105以及在網路103(b)中的伺服器113那樣。請求者105正在請求存取能夠由伺服器113提供的資料。附接到伺服器113的是一種大量儲存裝置115，該裝置包含正由請求者105請求的資料117。當然，對於其它資料而言，伺服器113可能是請求者，而請求者105則可能是伺服器。而且，在目前上下文中，存取操作被認為是：能夠讀取或改變儲存在伺服器113上之資料或者能夠改變伺服器113之狀態的任何操作。在提出請求方面，請求者105正在使用諸多標準TCP/IP(傳輸控制通信協定/網際網路通信協定)協定中的一種協定。如此處所使用的，通信協定是能夠被用來交換諸多電腦系統之間的資訊之一訊息集的一種描述。

將根據一種通信協定而正在通信的諸多電腦系統之間所發送的一些實際訊息集體稱為：對話(session)。在對話期間，請求者105根據通信協定將訊息發送到伺服器113的網際網路位址，而伺服器113則根據通信協定將訊息發送到請求者105的網際網路位址。請求及回應兩者將會藉由網際網路111而在兩個內部網路103(A)和103(B)之間運行。若伺服器113允許請求者105存取資料，則在對話中從伺服器113流到請求者105的一些訊息將包括被請求資料117。將

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(4)

必要時藉由網際網路而回應訊息之伺服器113的諸多多軟體組件稱為：服務(service)。

若兩個內部網路103(A和B)之擁有者想要確信：只有直接連接到網路103(A和B)之諸電腦系統的使用者才能夠存取資料117，以及請求及回應之內容在那些網路之外皆不為人所知：則該擁有者必須解決兩項問題：確信伺服器113並不會回應來自與連接到內部網路之那些電腦系統不同的電腦系統之請求；以及確信：雖然都是經由網際網路111轉接中(in transit)，可是存取網際網路111資訊的人都無法存取或修改請求及回應。有可能達成這些目標的兩種技術為：防火牆(firewalls)及使用加密的鑿隧道操作(tunneling)。

概念上，防火牆是內部網路與其餘的網際網路111之間的一道障壁(barrier)。防止牆出現在109(A)和(B)處。防火牆109(A)保護內部網路103(A)，而防火牆109(B)則保護內部網路103(B)。藉由一種在電腦系統中運作的通路(gateway)來建構防火牆，該電腦系統被安裝在內部網路被連接到網際網路的地方。包括在通路中的是一種存取過濾器：它是電腦系統中的一套軟體和硬體組件，會針對儲存在內部網路之內的資訊而核對來自內部網路之外的所有請求；並且，若它來自有權存取資訊的來源，則只會將請求發送在內部網路上。在其它方面，它會捨棄該請求。兩個這樣的存取過濾器：存取過濾器107(A)存取過濾器107(B)則出現在圖1中。

五、發明說明 (5)

若能夠肯定答覆兩個問題，則來源有權存取被請求資訊：

- 來源實際上就是享有權利人或物嗎？
- 來源有權存取資料嗎？

將找到第一問題之答案的過程稱為：鑑定。藉著將資訊提供到識別使用者的防火牆，使用者親自對防火牆加以鑑定。在這種資訊中有下列幾項。

- 由一種為使用者所有的鑑定令牌(authentication token)(有時候稱為智慧卡(smartcard))所提供的資訊；
- 使用者機器的作業系統識別；以及
- 使用者機器的IP位址和網際網路網域名稱(domain name)。

防火牆用於鑑定的資訊可能是在頻帶內(in band)，那就是：它是通信協定的一部份；或者，它可能是在頻帶外(out of band)，那就是：它是由一分離通信協定所提供。

像從上述識別資訊列表中顯而易見的那樣，防火牆能夠信賴識別資訊以鑑定使用者達到的程度，端視識別資訊的種類而定。譬如說，在一分包資訊中的IP位址就能夠由能夠截取分包資訊的任何人所改變；因此，防火牆能夠對它賦予少許的信賴，故而將藉由IP位址來鑑定稱為具有一種很低的信賴等級。在另一方面，當識別資訊來自一種令牌時，防火牆就能夠給予該識別資訊一種更高的信賴等級，此乃因為：唯若令牌已經為別人所有，則它應該不會識別使用者。通常，就一項關於鑑定的討論而言，請參看由貝

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (6)

洛文(S. Bellovin)和柴斯維克(W. Cheswick)合著："防火牆與網際網路安全性"一書，該書由阿狄生·韋斯理(Addison Wesley)圖書公司印行，美國麻州，1994年版。

在現代存取過濾器中，在兩個層級處來核對存取操作：網際網路分包資訊或簡稱IP層級，以及應用層級。就從IP層級開始，用於網際網路中的訊息都以分包方式載送，稱之為資料級(datagram)。每一個這樣的分包都有一個標題(header)，它包含指示著分包之來源和目標的資訊。來源和目標各自依據IP位址和埠號(port number)來表示。埠號是用來將電腦內多重業務流(streams of traffic)各個加以分別的一個從1到65535的數字。將針對一些為人所熟知的網際網路通信協定(諸如：HTTP(超本文傳送協定)或FTP(檔案傳送協定))的服務加以指定它們"傾聽"(listen to)的諸多為人所熟知的埠號。存取過濾器具有指示著哪些目標可能會接收來自哪些來源之IP分包資訊的一套規則；且若載明於標題中的來源和目標並未遵從這些規則，則將分包資訊捨棄。譬如說，該規則可能容許或不容許所有從一部電腦到另一部電腦的存取操作；或者，根據IP分包資訊之來源而限制存取一項特定服務(由埠號所載明)。然而，在IP分包資訊之標題中，並沒有關於正在被存取之個別資訊片段的資訊，而關於使用者的唯一資訊則是來源資訊。於是，存取核對是無法在IP層級處完成的，而必須換成是在資訊協定層級處完成的，該存取核對涉及：不是鑑定不可能使用來源資訊之使用者，就是決定使用者是否有權存取

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(7)

一個別資訊片段。

在應用層級處的存取核對通常是在防火牆中由代理伺服器(proxyes)來完成。代理伺服器是一種存取過濾器的軟體組件。之所以稱為代理伺服器，是因為：它可作為存取過濾器中的通信協定之替身(stand-in)用，為了實現關於使用者已經請求之資訊片段的使用者鑑定及/或存取核對。譬如說，一種常用的TCP/IP協定就是超本文傳送協定(hyper-text transfer protocol，或簡稱HTTP)，它被用來將全球資訊網(World-Wide Web)網頁(pages)從一個電腦系統傳送到另一個這樣的電腦系統。若需要個別網頁的存取控制，則必須檢視協定內容，以便決定哪個特定網頁要求被請求。就防火牆的詳細討論而言，請參看貝洛文和柴斯維克之前面參考文獻。

雖然正確執行之存取過濾器操作能夠預防經由網際網路111而未經授權就存取儲存在內部網路中的資料，可是它無法預防經由網際網路111而未經授權就存取轉接中的資料。此事藉由使用加密的鑿隧道操作加以預防。這種鑿隧道操作運作如下：當存取過濾器107(A)接收具有內部網路103(B)中之目標位址的一種來自內部網路103(A)中之一電腦系統的IP分包資訊時，它會對IP分包資訊，包括其標題加以加密；進而增加一項新標題，該標題載明：將存取過濾器107(A)的IP位址當作分包資訊的來源位址，而將存取過濾器107(B)的IP位址當作目標位址。新標題也可能包含：將存取過濾器107(A)識別為已加密分包資訊之來源的

五、發明說明(8)

鑑定資訊；以及存取過濾器107(B)能夠從其中決定已加密分包資訊是否已經被干預的資訊。

因為原始IP分包資訊已經被加密；所以，當它正在通過網際網路111時，標題和原始IP分包資訊的內容兩者都無法被讀取，而標題或原始IP分包資訊的資料則也無法沒有檢測下被修改。當存取過濾器107(B)接收IP分包資訊時，它就使用任何識別資訊來決定分包資訊是否的確來自存取過濾器107(A)。如果是的話，它會將由存取過濾器107(A)增加到分包資訊的標題加以去除，並決定分包資訊是否被干預；如果不是的話，就對分包資訊加以解密(decrypt)，並執行關於原始標題的IP層級存取核對。如果標題通過的話，存取過濾器107(B)就將分包資訊轉遞(forward)到載明於原始標題中之內部網路中的IP位址；或者轉遞到針對通信協定層級存取控制之一代理伺服器。原始IP分包資訊被稱為鑿隧道通過網際網路111。在圖1中，一個這樣的隧道112被顯示在兩個存取過濾器107(A)和107(B)之間。鑿隧道操作之一附加優點是：它會隱藏來自只有從網際網路111中有權存取資訊的那些人的內部網路之結構，此乃因為只有未加密IP位址才是存取過濾器的IP位址。

兩個內部網路103(A)和103(B)的擁有者也能夠使用鑿隧道操作，連同網際網路111；因而使兩個內部網路103(A和B)成為單一虛擬專用網路(VPN)119。藉由隧道112，在網路103(A)和103(B)中的電腦系統能夠彼此安全地通信，並且適用於其它電腦；好像網路103(A)和103(B)都是由一種

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(9)

專用實體鏈路(physical link)而不是由網際網路111加以連接的。的確，可能將虛擬專用網路119加以擴充，以便包括存取網際網路111資訊的任何使用者，進而能夠執行下列各項：

- 以一種允許存取過濾器107對分包資訊加以解密的方式，將被定址到內部網路103中之一電腦系統的網際網路分包資訊加以加密；
- 將一標題增加到被定址到存取過濾器107的已加密分包資訊；以及
- 親自對存取過濾器107加以鑑定。

譬如說，一位具有連接到網際網路111之一可攜式電腦並具有必要的加密和鑑定能力的雇員能夠使用虛擬專用網路，以便安全地檢索(retrieve)來自諸多內部網路其中之一網路中之一電腦系統的資料。

一旦諸多內部網路開始使用網際網路定址操作和網際網路通信協定，並且被連接進入虛擬專用網路中；針對網際網路已經發展出的一些瀏覽器(browsers)也能夠使用在內部網路103中；並且從使用者的觀點看來，在網際網路111中存取資料與在內部網路103中存取資料之間並沒有差別。於是，內部網路103已經變成一種企業內部網路(intranet)，那就是：一種具有和網際網路111相同的使用者界面的內部網路。當然，一旦屬於一實體的所有內部網路都已經被組合成為單一虛擬專用企業內部網路，會再度發生屬於網際網路之特性的存取控制問題--此時，除了有

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明(10)

關內部存取資料之外。雖然在內部網路被連接到網際網路111的地方的諸多防火牆都完美地足以使局外人(outsiders)無法在內部網路中存取資料，可是它們不能使局中人(insiders)無法存取該資料。譬如說，可能就像公司防備其人事資料不受其雇員影響與防備該資料不受局外人影響一樣重要。同時，公司可能想要使有權存取網際網路111資訊的任何人可以很容易地存取：在諸多內部網路103其中之一網路中之一電腦系統上，它的全球資訊網網站。

一種針對由虛擬專用企業內部網路所引起諸多安全性問題的解決方法是：使用防火牆將諸多內部網路加以細分，以及防備內部網路不受經由網際網路而未經授權就存取資訊的影響。現代存取過濾器107皆被設計用來防備內部網路之周界(perimeter)不受未經授權就存取資訊的影響；並且，一般說來，每個網際網路連接才只有一個存取過濾器107。若打算將諸多存取過濾器使用內部網路內；則將會有它們更多的存取過濾器，因而使用多重現代存取過濾器107的虛擬專用網路並不容易規模可伸縮性，那就是：在具有小量存取過濾器的虛擬專用網路中，諸多存取過濾器並不是一項嚴重的負擔；而在具有大量存取過濾器的網路中，它們則是一項負擔。在標題為"使用在存取過濾器203中的諸多技術之通則"章節之前的本專利申請案之一部份中所描述的存取過濾器，實際上解決了先前技藝存取過濾器的規模可伸縮性(scalability)問題；於是，建構具有大量存取過濾器的網路就變得更為容易。

五、發明說明 (11)

在關於本專利申請案之第一部份中所描述的存取過濾器之進一步運作中，已經變得顯而易見的是，若能將技術通用化，則執行存取過濾器203中之存取核對所發展出的諸多技術應該更為有用；若它們能夠使用在與正在IP層級或網際網路通信協定層級處操作之存取過濾器不同的上下文中，且若使它們能夠加以擴充；則使得決策能夠加以制定，不但針對存取資訊集，並且針對可能針對可經由一電腦系統存取資訊的一種實體而執行的任何行動；使得使用者群組能夠包括可經由一電腦系統而執行一項行動的任何種類之實體；並且使得資訊集能夠變成資源集(resource sets)，其中一項資源是能夠經由一電腦系統而控制的任何實體。進一步變得顯而易見的是：若允許決策包括一種時間組件(temporal component)，譬如說，一種只有在非工作時間期間才允許某一使用者群組存取某些資源的組件，則決策應該更為有用；並且，對能夠使諸多屬性與一項描述打怎樣執行決策之行動的決策有關聯也應該是有益的。例如，一項決策可能不但載明能夠存取一已知資源之一已知使用者群組的成員，並且載明打算用於存取操作之網路服務的類別(class)。於是，此處所披露的本發明之一目的是：提供針對通用化存取核對的技術，以及進一步提供其中時間組件和屬性都可能與決策有關聯的決策。

發明概要

本發明藉由一種決策施行系統來達到前述目的，在該系統中，在以下兩個組件之間共享決策施行之工作(task)：

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (12)

包括可擴允決策資料庫之一決策伺服器，以及一決策施行器(policy enforcer)。當決策施行器接收由第一實體所提出之一請求以執行針對第二實體的一項行動時，決策施行器就將該請求傳達到決策伺服器；並且，唯若來自決策伺服器之一回應指示：在資料庫中的決策容許行動，才會允許行動。可能將可擴充決策資料庫加以擴充，以便包括不是由決策施行器所執行的諸多類型之行動。因為如此，所以決策施行系統能夠藉由以下方法來處理諸多新行動類型：擴充決策資料庫以提供針對那些類型之決策，以及增加針對諸多類型之行動的決策施行器。的確，只要行動是由電腦系統中之一決策施行器所控制，電腦系統就沒有必要執行該行動。

將決策評估和決策施行加以分離，也有可能使得：決策施行系統會在決策施行系統所屬之電腦系統的諸多不同層級處很容易地處理決策施行；並且使得：決策施行器都被定位遠離決策伺服器。

在另一觀點中，依據：第一實體之集合，第二實體之集合，以及第一集合之一實體可能針對第二集合之一實體執行的一項行動；將諸多決策加以定義在決策施行系統之一實施例中。在本實施例中，除了行動類型之外，第一實體類型和第二實體類型都是可擴充的。

在本實施例中，行動屬性可能附屬於第一實體之集合或第二實體之集合，該行動屬性會決定打算怎樣執行就是決策之主體(subject)的行動。譬如說，可能將優先級(priority)

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (13)

指定給使用者之集合，或者將頻寬(bandwidth)指定給服務之集合。本實施例的決策資料庫是可擴充的，以便包括諸多新行動屬性類型。

在本發明的另一觀點中，可能將條件附屬於決策施行系統之決策資料庫中的決策。即使當一項決策之行動在其它情況應該被允許時，若未履行附屬於決策的條件，則該行動也將不被允許。這些條件之一類別是時間條件。例如，可能制定一項定義存取資訊的決策，而關於決策之一時間條件則可能將決策之有效性(validity)限制於正常營業時間。

追隨著下列闡述和附圖，與本發明有關的本發明之其它目的及優點對那些熟習於此技藝者而言將是顯而易見的，其中：

附圖概述

2 附圖概述

圖 1 是：經由網際網路，用來控制資訊之存取的諸多技術之總覽(overview)；

圖 2 是：使用納入此處所披露之技術的諸多存取過濾器之一 VPN(虛擬專用網路)之總覽；

圖 3 是：使用在存取過濾器中的一種存取控制資料庫之總覽；

圖 4 顯示：在使用納入此處所披露之技術的諸多存取過濾器之一 VPN 中的存取核對和鑿隧道操作；

圖 5 顯示：由一"漫遊者"(roamer)存取在 VPN 中的資訊；

圖 6 是：使用在定義靈敏度和信賴等級與諸多鑑定和加

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(14)

密技術之間的關係中的一種表；

圖7是：應用SEND(安全加密網路遞送)技術之一實例；

圖8是：決策建立過程之一流程圖；

圖9顯示：用來定義使用者群組之一顯示圖；

圖10顯示：用來定義資訊集之一顯示圖；

圖11顯示：用來定義存取決策之一顯示圖；

圖12顯示：用來定義存取過濾器203之一顯示圖；

圖13A和B都是：定義使用者群組之存取控制資料庫301的一部份之一圖表(schema)；

圖14是：定義資訊集之存取控制資料庫301的一部份之一圖表；

圖15是：定義在VPN中的網站(sites)以及在每個網站處的伺服器，服務，及資源之存取控制資料庫301的一部份之一圖表；

圖16A和B都是：定義決策之存取控制資料庫301的一部份之一圖表；

圖17A，B，及C都是：定義伺服器之存取控制資料庫301的一部份之一圖表；

圖18顯示：使用在IntraMap(映像內)界面中的顯示圖；

圖19顯示：怎樣針對存取控制資料庫301做出改變；

圖20是：存取過濾器203的架構之一詳細方塊圖；

圖21是：一種MMF(記憶體映射檔案)檔案2303的結構之一示意圖；

圖22：是一種使用SKIP(網際網路通信協定之簡單密鑰

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (15)

管理)協定所發送的訊息之一示意圖；

圖23A，B，及C都是：使用在一較佳實施例中之MMF檔案的一種表；

圖24是：IntraMap界面之一建構例之一示意圖；

圖25是：圖解說明在VPN 201中的委託權限(delegation)之一示意圖；

圖26是：一種已經將決策核對和決策施行加以分離的行動控制系統之一方塊圖；

圖27是：一種具有種種的決策致能(policy-enabled)裝置的行動控制系統之一方塊圖；

圖28顯示：一種用來定義通用化決策的語法(syntax)；

圖29顯示：在一較佳實施例中的決策資料庫2901之總覽；

圖30顯示：決策資料庫2901中的諸多屬性和時間間隔之一建構例；

圖31顯示：列示所有已定義時程安排(defined schedules)之一視窗；

圖32顯示：使用在一較佳實施例中，用來定義時程安排規則之一視窗；

圖33顯示：使用在一較佳實施例中，用來將時間間隔應用到決策之一視窗；

圖34顯示：使用在一較佳實施例中，用來顯示屬性之一視窗；

圖35顯示：使用在一較佳實施例中，用來將屬性指定到

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (16)

主體之一視窗；

圖36顯示：用來顯示和修改在一較佳實施例中之一屬性定義之一視窗；以及

圖37顯示：用來顯示和修改在一較佳實施例中之一特點定義之一視窗。

在諸多附圖中的參考數字至少都有三個數字。兩個最右側數字都是在圖內的參考數字；而在那些數字左側的數字則都是圖號，在圖中：由參考數字所識別的項目最先出現。譬如說，在圖2中，具有參考數字203之項目最先出現。

闡述

2 闡述

下列闡述將首先提供：一些容易規模可伸縮性的存取過濾器，它們怎樣被用來控制在企業內部網路中的存取操作，以及它們怎樣能夠用來構築虛擬專用網路之總纜。因此，闡述將提供：使用在存取過濾器中的存取控制資料庫；將它改變，進而將那些改變分佈在諸多存取過濾器中所用的方式；以及個別存取過濾器控制存取操作所用的方式之細節。

一種具有不會妨礙規模可伸縮性之諸存取過濾器的網路：

圖2

3A 一種具有不會妨礙規模可伸縮性之諸存取過濾器的網路：圖2

圖2顯示一種虛擬專用網路(VPN)201，其中：存取資料是由被設計用來避免因多重存取過濾器而引起問題的存取

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (17)

過濾器所控制。VPN 201是由四個內部網路103所組成，藉由網際網路121將它們彼此連接。也經由網際網路121連接到VPN 201的是：一漫遊者217，那就是一種電腦系統，該系統雖然正在由可能存取在企業內部網路201中之資料的人使用者，但是只會藉由網際網路121連接到諸多內部網路。每個內部網路103都有：許多電腦系統或屬於使用者的終端機209，以及許多伺服器211；該伺服器包含：可能由在諸多電腦系統或終端機209處之使用者，或可能由在漫遊者217處之一使用者所存取的資料。然而，並沒有將電腦系統或終端機209，或者漫遊者217直接連接到一伺服器211；換成是，各自經由一存取過濾器203而加以連接，使得：由在使用者系統處之使用者所提出針對伺服器上之資料項的所有查詢(references)至少都會通過一個存取過濾器203。於是，使用者系統209(i)被連接到網路213(i)，該網路被連接到存取過濾器203(a)；而伺服器211(i)則被連接到網路215(i)，該網路也被連接到存取過濾器203(a)，因而由在使用者系統209(i)處之使用者所做出針對存取伺服器211(i)上之資料的任何嘗試都會通過存取過濾器203(a)，在該處，若使用者無權存取資料，就會被拒絕。

既然VPN 201具有任何規模的大小，就會有一相當數目的存取過濾器203；因此，將會立即發生按規模伸縮(scaling)問題。存取過濾器203會避免這些問題，是因為它們都是根據下列原理加以設計的：

- 分佈型存取控制資料庫。每個存取過濾器203都有它

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (18)

自己的存取控制資料庫拷貝，用來控制存取在VPN 201中的資料。將在資料庫之一拷貝中所做的改變傳播到所有其它的拷貝。

分佈型管理。可能委託任何數目的管理員對系統之諸子集合負有責任。所有管理員可能會同時執行他們的工作。

分佈型存取控制。存取控制功能都是在近端(near-end)存取過濾器203處加以執行的。那就是，在客戶機與伺服器之間的路徑中的第一存取過濾器203會決定；存取操作是否被容許；而在路徑中的諸多隨後存取過濾器則不會重複由第一存取過濾器所執行的存取核對。

端對端加密(end-to-end encryption)。加密發生在近端存取過濾器與可能的最遠加密端點(endpoint)之間。此端點不是資訊伺服器本身，就是遠端(far-end)存取過濾器203-最後在從客戶機到伺服器之路由中的那個。動態隧道都是根據目前網路路由選擇(routing)條件加以建立的。

可適性加密和鑑定。根據正在被傳送的資訊靈敏度，將可變加密等級和鑑定要求應用到通過VPN的通信量(traffic)。

將所有的這些設計觀點更加詳細地討論於下。

此時應該指出的是，可能以任何方式來建構存取過濾器203，該方式保證：由可能未經授權就存取該資料的諸多使用者所提出針對在VPN 201中之資料的所有查詢都會通

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (19)

過一存取過濾器203。在一較佳實施例中，存取過濾器203被建構在一伺服器上，並且在由微軟公司(Microsoft Corporation)所製造的Windows NT®(新科技版本的視窗軟體)作業系統下運作。在其它實施例中，存取過濾器203可能被建構作為一種作業系統之組件，及/或可能被建構在VPN 201中之一路由器(router)中。

分佈型決策資料庫：圖3

3分佈型決策資料庫：圖3

每個存取過濾器203都有存取控制資料庫301之一拷貝，它保時了與在VPN 201中之存取控制有關的所有資料。如圖2中之存取過濾器203(a)所顯示的一個存取過濾器，它具有存取控制資料庫301之一主拷貝205。因為如此，所以將存取過濾器203(a)稱為：主決策管理程式(Master Policy Manager)。主拷貝205是：被用來初始化(initialize)一些新存取過濾器203或替換已受損存取控制資料庫301的那個。主決策管理程式電腦的備用裝置是存取過濾器203(b)。備份拷貝(backup) 207是主拷貝205之一鏡像。最後，報表管理程式209包括用來產生報表的軟體：該報表係來自存取控制資料庫301中的資訊，以及來自從所有其它存取過濾器203中所獲得的記錄(logs)。存取控制資料庫301的任何拷貝可能會被必須這麼執行存取操作的任何使用者所改變：就像稍後將要更加詳細描述的那樣，將任何這樣的改變，首先傳播到主決策管理程式205，然後再到虛擬專用網路201中的所有其它存取過濾器203。

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (20)

圖3是：存取控制資料庫301一概念性總覽。資料庫的主要功能是對來自存取過濾器203之一存取請求309作回應，該存取過濾器利用一種該請求是否將被准許或拒絕的指示311來識別使用者和資訊資源。若下列兩者都成立，則該請求將被准許：

- 使用者屬於一使用者群組，其中資料庫301指示：可能存取資訊資源所屬之一資訊集；以及
- 該請求具有一種至少是與屬於資訊資源之靈敏度等級一樣高的信賴等級。

每位使用者均屬於一個或更多使用者群組，而每個資訊資源則均屬於一個或更多資訊集；若使用者所屬的一些使用者群組中沒有一個被拒絕存取資訊資源所屬之一資訊集，以及使用者所屬的任何使用者群組被容許存取資訊資源所屬的任何資訊集；則使用者可能存取資訊資源，假若該請求具有必要之信賴等級的話。

資源之靈敏度等級只是指示著用來存取資源所需的信賴等級之一數值。就大體而論，需要保護資訊資源愈多，其靈敏度等級愈高。請求之信賴等級具有許多組成部份：

- 用來識別使用者之識別技術的信賴等級；譬如說，藉由令牌來識別使用者具有一種比藉由IP位址來識別使用者還高的信賴等級。
- 由經由網路之存取請求所採取路徑的信賴等級；譬如說，包括網際網路的路徑具有一種比只有包括一些內部網路的路徑還低的信賴等級。

五、發明說明 (21)

若對存取請求加以加密，則使用加密技術的信賴等級；加密技術愈強，信賴等級愈高。

將識別技術的信賴等級和路徑的信賴等級各別考慮。然而，路徑的信賴等級可能會受用來加密存取請求之加密技術的信賴等級所影響。若利用一種其信賴等級高於路徑之一部份的信賴等級的加密技術而對請求加以加密，則路徑之一部份的信賴等級被增加到加密技術的信賴等級。於是，若路徑之一部份的信賴等級小於資源之靈敏度等級所需要的；則藉著利用一種具有必要之信賴等級的加密技術來加密存取請求，就能夠解決問題。

可能將包含於資料庫301中的資訊分成六大類：

使用者識別資訊313，它會識別使用者；

使用者群組315，它會定義使用者所屬的群組；

資訊資源320，它會定義蒙受保護的一些個別資訊項，並且載明在何處找到它們；

資訊集321，它會定義資訊資源之群組；

信賴等級資訊323，它會載明資訊資源之靈敏度等級以及使用者識別和網路路徑的信賴等級；以及

決策資訊303，它會依據使用者群組和在VPN 201中的諸多物件(objects)來定義存取權利。

將決策資訊進一步分成：存取決策307，管理決策305，以決策制定者決策306。

存取決策307會定義由使用者群組存取資訊集的權利；

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (22)

- 管理決策305會定義使用者群組定義/刪除/修改在VPN 201中之諸多物件的權利。在諸多物件中則有：存取決策，資訊集，使用者群組，在VPN 201中的位置，伺服器，及服務；以及
- 決策制定者決策306會定義使用者群組制定針對資訊集之存取決策的權利。

載明在資料庫301之管理決策和決策制定者決策兩個部份中的使用者群組都是管理員之使用者群組。在VPN 201中，藉著定義管理員群組以及在資料庫301中他們管轄的物件來委託管理權限(administrative authority)。當然，一既定使用者可能是一般使用者群組317和管理使用者群組319兩者中之一成員。

使用者識別

3 使用者識別

使用者群組利用使用者識別資訊313來識別他們的成員。識別資訊藉由一套可擴充識別技術來識別它的使用者。目前，這些識別技術包括：X.509號證書(certificates)，Windows NT網域識別，鑑定令牌，以及IP位址/網域名稱。用來識別使用者之識別技術種類會決定識別之信賴等級。

在需要強有力識別使用者或與存取過濾器203通信之其它實體的地方，VPN 201就會使用：由昇陽微系統公司(Sun Microsystem, Inc.)所發展出的"網際網路通信協定之簡單密鑰管理"(Simple Key Management for Internet

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (23)

Protocols, 簡稱SKIP)軟體通信協定。該通信協定會管理：公用密鑰(public key)交換，密鑰鑑定，以及對話加密。藉由一種從正在交換資料之各方的公用和專用密鑰中所產生的傳送密鑰(transport key)來執行對話加密。公用密鑰都包括在X.509號證書中，該證書都是在使用通稱為"證書發現通信協定"(Certificate Discovery Protocol, 簡稱CDP)之一分離通信協定的SKIP各方之間交換的。除了已加密訊息之外，一種使用SKIP來加密的訊息還包括：針對訊息之一已加密傳送密鑰，以及針對資料之來源和目標之證書的識別符(identifiers)。訊息接受者使用針對訊息來源之證書的識別符來指出針對來源之公用密鑰的位置；並使用其密鑰和來源之公用密鑰，對傳送密鑰加以解密；進而使用傳送密鑰，對訊息加以解密。SKIP訊息是有自行鑑定性(self-authenticating)，從某種意義說來，它包含一種包括分包資訊內容之密碼摘要(cryptographic digest)的鑑定標題，而任何種類的修改將會使得摘要不正確。就關於SKIP的細節而言，請參看由阿沙·阿濟芝(Ashar Aziz)和馬丁·斐特森(Martin Patterson)所發表的"網際網路通信協定之簡單密鑰管理(SKIP)"專文，該專文能夠上網獲知：1998年2月28日，網址為<http://www.skip.org/inet-95.html>。就關於X.509號證書的細節而言，請參看能夠上網獲知的描述：1997年9月2日，網址為<http://www.rnbo.com/PROD/rmadillo/p/pdoc2.htm>。

在VPN 201中，SKIP也會被諸多存取過濾器203所使用，以便識別它們自己在VPN中的其它存取過濾器203；進

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (24)

而在需要加密的地方，對TCP/IP對話加以加密。當它們正在執行存取核對時，諸多存取過濾器203也能夠使用針對SKIP密鑰之證書來識別使用者。這樣一種識別方法是特別值得信賴的，因而具有一種相當高的信賴等級。這種藉由證書的識別方法之一用途是：針對"漫遊者"217之值得信賴的識別方法。X.509號證書能夠被使用於使用者識別，是因為：它們使密鑰資訊與關於使用者的資訊有關係。

存取過濾器203使用下列來自證書的資訊欄位：

- 屆滿日期：在此日期之後，證書就無效。
- 公用密鑰：一種公用一專用密鑰對的公用半對密鑰，就像使用在Conclave(祕密會議客戶軟體)所使用之基於SKIP密碼術(SKIP-based cryptography)中的那樣。
- 證書當局(Certificate Authority)簽字：與發行證書之當局有關聯的區別名稱。
- 證書序號。
- 主體名稱：發行證書到達之實體名稱。

主體名稱包括下列子欄位(在括弧內的代表字是欄位之一般縮寫)：

- 共用名稱(CN)：主體之既定名稱，譬如說是John Q. Public。
- 國家(C)：主體所在之國家。國家代碼都是載明於X.509號規範(specification)中的2個字母代碼。
- 所存地(L)：主體所在之位置。此欄位通常是主體所在之城市，但可能被使用任何與位置有關的數值。

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (25)

- 組織(O)：主體所屬之組群。此欄位通常是組織之名稱。
- 組織單位(OU)：主體之組織單位。此欄位通常是主體之部門，譬如說，"業務部"。X.509號證書容許這些欄位中高達四個欄位存在。

和諸多存取過濾器203一起使用的證書當局會發行具有所有這些欄位的證書。並且，四個OU欄位可能被用來定義附加分類。在證書中用來描述使用者的資訊皆可供資料庫301之管理員利用，當定義使用者群組時就加以使用。若證書中的資訊正確地反映企業的組織結構；則證書將不但會識別使用者，而且會顯示使用者適合於企業組織的所在；進而達到的程度是，在資料庫301中的使用者群組會反映：組織結構，使用者所屬之使用者群組。

就像稍後將要更加詳細說明的那樣，其中可能定義諸多使用者群組之成員的一個方法是：藉由"證書匹配準則"(certificate matching criteria)，該準則定義屬於一既定使用者群組之成員的證書必須具有的欄位數值。證書匹配準則可能是基於與所需一樣少或一樣多的上述欄位。譬如說，針對工程使用者群組的證書匹配準則可能是：組織欄位和載明工程部的組織單位欄位。識別使用者之其它資訊也可能被使用來定義諸多使用者群組之成員。

資訊集

3 資訊集

資訊集保持諸多個別資訊資源的收集資訊。一項資源可

(請先閱讀背面之注意事項再填寫本頁)

線

五、發明說明 (26)

能與一個別 WWW(全球資訊網)網頁或新聞群組(newsgroup)一樣小，但它最常是由：網路目錄樹(Web directory tree)及其內容，FTP帳戶，或主要 Usenet(新聞網)新聞分類所組成。在圖 2 之諸多伺服器其中之一伺服器中，顯示有兩個資訊集：219(j)和(k)。雖然存取控制資料庫 301 之管理員理應完全決定：何種資訊被包括在一資訊集中；可是，在一既定集合中的資訊通常就是：與課題和有意收看者(audience)兩者都有關係的資訊。針對公司之資訊集實例可能是：HR policies(HR 決策)，HR Personnel Records(HR 人事記錄)，以及 Public Information(公用資訊)。

存取決策 307

3 存取決策 307

概念上，存取決策 307 由以下格式之簡單陳述所組成：

Engineers	allowed access to	工程師	被容許存取
	engineering data		工程資料
Internet	allowed access to	網際網路	被容許存取
	public web site		公用網路

首欄載明使用者群組；末欄載明資訊集。中間那欄則是存取決策-容許或拒絕。

資料庫 301 允許使用者群組和資訊集的分層定義(hierarchical definition)。譬如說，可能將工程師使用者群組定義成包括：硬體工程師使用者群組，軟體工程師使用者群組，以及銷售工程師使用者群組。同樣地，可能將工程資料資訊集定義成包括：硬體工程資料資訊集，軟體工

五、發明說明 (27)

程資料資訊集，以及銷售工程資料資訊集。在使用者群組之層次內，由繼承而獲得存取權利。於是，爲了存取核對，屬於硬體工程師使用者群組之一使用者也會自動地屬於工程師使用者群組。在資訊集之層次內，同樣地由繼承而獲得存取權利。爲了存取核對，屬於硬體工程資料資訊集之一資訊資源也會自動地屬於工程資料資訊集。於是，若有一項賦予工程師存取工程資料的存取決策，則成爲組成工程師的三個使用者群組其中之一使用者群組之一成員的任何使用者都可能存取：屬於組成工程資料的三個資訊集其中任何資訊集的任何資訊資源。在使用者群組和資訊集之定義中使用繼承權(inheritance)會大大地減少在存取控制資料庫301中所需的存取決策307之數目。例如，在上述實例中，單一存取決策就賦予所有的工程師存取所有的工程資料。繼承權也會使得：實際上依據容許存取操作來定義所有的存取決策是有可能的。繼續上述實例，若有一個不屬於"工程師"的"推銷員"(Salespeople)使用者群組，但有一項賦予該使用者群組存取銷售工程資料的存取決策：則成爲"推銷員"之一成員的使用者將能夠存取銷售工程資料，但不是軟體工程資料或硬體工程資料。

當然，一位使用者可能屬於一個以上的使用者群組，而一項資訊資源則可能屬於一個以上的資訊集。也可能會有針對使用者所屬之各種使用者群組以及資訊資源所屬之各種資訊集的不同存取決策。當面對既適用於使用者又適用於使用者正試圖存取之資訊資源的多重存取決策時，存取過濾器203

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(28)

會以一種限制性，而非允許性方式來應用決策：

- 若多重決策容許或拒絕一使用者群組存取一資訊集，則拒絕存取操作的決策佔優勢。
- 若一特定使用者是多重使用者群組之一成員，並且，多重決策容許或拒絕存取資訊集；則拒絕存取操作的決策佔優勢。

一使用者屬於何種使用者群組可能會根據用來識別使用者的識別模式而改變。於是，若根據到當時為止使用者已經提供給存取過濾器203之識別模式，並沒有存取決策適用於使用者所屬之諸使用者群組；則存取過濾器203可能當識獲得附加識別資訊，並決定：附加識別資訊是否將使用者安置在有一項關於資源的決策所針對之一使用者群組中。存取過濾器203可能獲得附加識別資訊，如果：

- 使用者已經安裝使用者識別客戶軟體(User Identification Client，簡稱UIC)(一種會在使用者機器上執行並將關於使用者的識別資訊提供給存取過濾器203的軟體)。
- UIC目前正在使用者機器上執行。
- 使用者已經使得他的UIC彈出(pop-up)，以供進一步鑑定之用(使用者具有一種致能這項特點的圈選框(check box))。

若所有這些要求都成立，則存取過濾器203將會迫使使用者之UIC彈出，並請求另外的識別資訊。將使用者供應的任何識別資訊加以儲存。在每個新的使用者識別資訊片

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (29)

段之後，存取過濾器203會執行相同的評估處理過程：直到獲得將使用者安置在有一項允許或拒絕存取操作決策所針對之一使用者群組中的識別資訊為止；或者，直到使用者放棄其請求為止，將UIC視窗彈出。

管理決策305

3 管理決策305

管理決策305會落實(implement)在VPN 201之存取控制系統中的諸多物件之管理。包括在物件中的有：使用者群組，資訊集，存取決策，以及此處所稱的可用資源(available resources)；那就是：服務，伺服器，存取過濾器，以及組成VPN 201的網路硬體。物件是被一個或更多管理使用者群組所管理。管理一既定物件的管理使用者群組之一成員可能會修改該物件以及它與其它物件的關係，並可能會制定針對該物件的管理決策。就像稍後將要更加詳細說明的那樣，管理物件的管理使用者群組之一成員可能會制定針對該物件的管理決策之事實會使得：該成員委託物件管理權是可能的。譬如說，管理"硬體工程師"使用者群組的管理使用者群組之一成員可能會制定：一項將"硬體工程師"管理權賦予"硬體工程管理員"使用者群組的管理決策，藉以將"硬體工程師"管理權委託給"硬體工程管理員"。應該注意的是：管理資訊集的權利是與制定針對資訊集之存取決策的權利分開的。一使用者群組有權制定關於資訊集的存取決策之事實，並不會賦予使用者群組制定針對資訊集之管理決策的權利；反之亦然。當一存取過

(請先閱讀背面之注意事項再填寫本頁)

訂 · 線

五、發明說明 (30)

濾器203首先被建立時，單一內建安全官員(security officer)使用者群組就具有：管轄所有在VPN 201中的物件以及管轄決策制定者決策306的管理權限。

隨著管理決策的繼承權

3. 隨著管理決策的繼承權

繼承權隨著管理決策而運作，相同方法則是：繼承權隨著存取決策而運作。將諸多使用者群組，資訊集，以及管理決策所指的可用資源加以分層組織。在使用者群組內，都是一既定使用者群組的子集合的使用者群組：都在來自該既定使用者群組的諸多使用者群組之層次(hierarchy)中向下的下一層級處。關於資訊集的情形相同。用與關於存取決策相同的方式，將繼承權應用在層次內。於是，在使用者群組層次內，管轄(control)一使用者群組之一管理使用者也會管轄所有的附屬者(subsidiary)，包含一些使用者群組在內。同樣地，關於資訊集層次，管轄資訊集之一管理使用者也會管轄所有的附屬者，包含一資訊集在內；而管轄針對一資訊集的管理決策之一管理使用者也會管轄針對所有已包含資訊集的存取決策。

還有一種可用資源的自然層次。譬如說，層次中之一層級是：位置。在一既定位置內，在該位置處的諸多伺服器形成向下的下一層級；而在一伺服器內，由伺服器所提供的諸多服務則形成下一層級。具有可用資源樹之任何層級之管轄權的管理使用者群組也會管轄所用的較低層級。譬如說，管理決策將存取過濾器203之管轄權賦予的(諸多)

五、發明說明 (31)

管理員具有針對：在在網站下之所有伺服器，在那些伺服器上執行之所有服務，以及由那些服務所支援之所有資源的管理權利。

委託權限：圖 25

3 委託權限：圖 25

在 VPN 201 中，委託權限是挺容易的，因為：管理物件之管理使用者群組的成員都可能修改該物件，並且制定針對它的管理決策。譬如說，若一管理使用者群組管理一資訊集；則它能夠將資訊集分成兩個子集合，並且制定一些新的管理決策，該決策賦予兩個其它使用者群組中的每個使用者群組管轄兩個子集合中的一個子集合之管理權限。

圖 25 顯示委託權限之一擴充實例。在圖 25 中，使用者群組和其它物件都以圓圈表示；決策制定者決策則以方塊表示；而決策關係則以不同種類的箭頭表示：實線箭頭代表管理決策，點線箭頭代表決策制定者決策，而虛線箭頭則代表存取決策。標示 2501 之附圖的一部份顯示當正在建立存取過濾器 203 時的情形：內建"安全官員"使用者群組 2503 具有管轄所有內建物件 2505 和管轄決策制定者決策 2507 之管理權限。"安全官員"使用者群組 2503 的成員都會使用他們的管理權限，以便：組成物件 2505 之子集合，重新安排物件層次，以及建立決策制定者決策 2507。

在標示 2508 之圖 25 的部份中，可看出："安全官員"使用者群組 2503 之活動的一個活動結果。"安全官員"使用者群組 2503 之一成員已經建立：一"工程管理員"管理使用者群

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (32)

組2509，一"工程師"使用者群組2511，以及一"工程資料"資訊集2513；並且已經賦予"工程管理員"管轄"工程師"和"工程"資料的管理權限。"安全官員"之成員也已經建立決策制定者決策2507，使得："工程管理員"有權制定針對"工程資料"之存取決策，如點線箭頭2510所示。"工程管理員"之一成員已經使用該權利來制定：允許工程師2511之成員存取在"工程資料"2513中之資訊的存取決策，如虛線箭頭2512所示。於是，"安全官員"之成員已經將管轄工程師2511，工程資料2513，以及管轄存取工程資料的管理權限委託給工程管理員2509。

當然，安全官員2503仍然具有管轄工程管理員2509的管理權限；因而能夠使用該權限，以供進一步委託權限之用。將一實例顯示在2517處。"安全官員"2503之一成員已經將"工程管理員"分成兩個子集合："工程人員管理員"(Engineering Personnel Administrators，簡稱EPA)2519和"工程資料管理員"(Engineerng Data Administrators，簡稱EDA)2521。這些子集合之成員都是從工程管理員2509中繼承而得管轄"工程師"2511和"工程資料"2513的管理權利。EPA 2519和EDA 2521的成員會使用這些管理權利來將管轄"工程師"2511的管理權限委託給"工程人員管理員"2519，並將管轄"工程資料"2513的管理權限委託給"工程資料管理員"2521。EPA 2519和EDA 2521的成員已經進一步使用他們的權利來制定針對"工程資料"2513的存取決策以改變存取決策，使得：針對"工程資料"的存取決策是由"工程

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (33)

管理員"2521所制定的，如點線箭頭2523所示，而不是由"工程管理員"2509所制定的，藉以將該項功能委託給"工程資料管理員"2521。

現在，工程人員管理員和工程資料管理員之成員能夠使用他們管轄工程師，工程資料，以及針對工程資料存取決策的管理權利來細加區分(refine)針對工程資料之存取操作。譬如說，"工程人員管理員"之一成員可能將"工程師"細分成："軟體工程師"和"硬體工程師"；而"工程資料管理員"之一成員則可能將"工程資料"細分成："硬體工程資料"和"軟體工程資料"。這樣做，"工程資料管理員"之一成員就可能會以賦予"軟體工程師"存取"軟體工程資料"和賦予"硬體工程師"存取"硬體工程資料"的存取決策來替換賦予"工程師"存取"工程資料"的存取決策。

簡要而言，可說是：具有管轄一使用者群組的諸多管理員皆對正確地定義在使用者群組中之成員資格(membership)負有責任；他們可能將此責任的任何部份委託給其它管理員。同樣地，具有管轄一資訊集的諸多管理員皆對正確地將資訊資源包括在資訊集內負有責任；他們可能將此責任的任何部份委託給其它管理員。後者的管理員當然也必須是針對某種可用資源的管理員，從該資源中可能獲得：正在被增加到資訊集的資訊。可用資源之管理員皆對整體網路和安全性操作負有責任。同樣地，他們可能委託他們的責任。最後，決策制定者管理員都會掌握管轄存取資訊的最後管轄權。他們可能獨自建立與特定資訊集有關的存取

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (34)

決策。從某種意義說來，決策制定者決定針對企業的整體資訊共享決策。針對使用者群組，資訊集，以及可用資源的管理員然後會決定建構細節。

使用諸多存取過濾器203和資料庫301的存取控制：圖4

2使用諸多存取過濾器203和資料庫301的存取控制：圖4

如圖2中所示，存取過濾器203在VPN 201中有一位置，將它安置在使用者正在從其中請求存取資訊資源的客戶機與資訊資源存在其上的伺服器之間。於是，藉由在一使用者與能夠提供使用者存取資訊資源的一項在伺服器上的服務之間的通信中居間調停(interceding)，存取過濾器203能夠控制由使用者存取資源。為了使使用者獲得存取資訊資源，在使用者與服務之間必須建立對話。在目前上下文中，將術語"對話"加以廣義地定義，以便包括一些正派(well-behaved)無連接通信協定(connectionless protocols)。當存取過濾器203發覺使用者嘗試初啓一項具有服務的對話時，它會決定存取操作是否應該被允許。這麼做是根據：使用者的已知身份；資訊正在被存取的資訊資源；資訊的靈敏度等級；以及使用者識別方法，使用者與服務之間路徑，及所使用之任何加密技術的信賴等級。

圖4顯示：一項對話如何能夠涉及一個以上的存取過濾器203。顯示於圖4中的對話402涉及在圖中編號為403(1,...5)的五個存取過濾器203。存取過濾器203皆被設計而使得：只需要在諸多存取過濾器203中的一個存取過濾器中，制定是否准許使用者存取資訊資源的決策。諸多存取

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (35)

過濾器203的這種特點之關鍵是：它們對它們自己彼此鑑定的能力。SKIP被用來做這件事。每一個存取過濾器203都有：使存取過濾器203之密鑰與存取過濾器之名稱相結合，並且由VPN的證書當局所簽署的一種X.509號證書。在資料庫301中，每個存取過濾器都具有：在VPN 201中的所有其它存取過濾器的名稱和IP位址；並且，一項使用SKIP來加密的對話一到達，每個存取過濾器就使用來自在SKIP之討論中如上所述之證書的"主體名稱"(Subject Name)來決定：使用SKIP加密的(SKIP-encrypted)網路通信量是否來自在VPN 201中的另一個存取過濾器203。

若存取過濾器接收中的對話並不是對話的目標(那就是，存取過濾器只是執行像沿著路徑之一IP路由器那樣的功能而已)，則存取過濾器只會從資料庫301中加以驗證(verify)：目標IP位址就是在VPN 201中的某個其它存取過濾器203的IP位址。如果就是這種情形，就容許對話通過而不必附加核對。當請求來到最後存取過濾器203時，最後存取過濾器203就使用SKIP對該請求加以解密，以便證實：該請求的確被第一存取過濾器203所核對，進而證實：該請求在轉接中未曾被修改。

於是，在圖4中，存取過濾器403(1)使用它自己的存取控制資料庫301之拷貝來決定：發起對話的使用者是否已經存取針對該對話所載明的資訊資源。若存取過濾器403(1)如此決定；則它會鑑定對話的一些輸出訊息，並且必要時對它們加以加密，以便達到適當信賴等級。然後，

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (36)

諸如存取過濾器403(2,...,5)會允許對話繼續進行，此乃因為該對話是來自存取過濾器403(1)並已經利用SKIP加密；進而既不會使用它們自己的存取控制資料庫301之拷貝來對訊息加以解密，也不會對訊息加以核對。然後，存取過濾器403(5)會對訊息加以解密，並證實：它們都被加密，因此皆由存取過濾器403(1)所核對；且若訊息都是原封不動的，則將它們轉遞到包含所需資源的伺服器407。在伺服器407與使用者系統401之間傳遞之對話中的諸多訊息都用相同方式加以處理：必要時，利用存取過濾器403(5)對它們加以加密；諸存取過濾器403(2,...,4)會基於由存取過濾器403(5)所執行的鑑定而將它們加以傳遞通過；而存取過濾器403(1)到基於鑑定而將訊息傳遞到系統401，並且必要時，對該訊息加以解密。

這種技術所有效執行的是：為存取過濾器403(1)與存取過濾器403(5)之間的對話而開闢一隧道405；因為隧道，所以只有最接近客戶機的存取過濾器403才需要執行：解密，存取核對，以及重新加密。而且，在諸多內部網路和在網際網路121中，隧道都是同樣安全的。在一種大型VPN中，存取過濾器403(1)處在最佳位置中以核對存取操作，此乃因為：它有權存取關於發起對話之使用者的最詳細資訊。執行在第一存取過濾器401處之存取核對的技術會進一步將存取控制責任均均分佈遍及VPN，因而容許VPN按規模伸縮到任何規模的大小。

端對端加密：圖5

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (37)

3 端對端加密：圖 5

圖 4 之隧道只是從存取過濾器 403(1) 延伸到存取過濾器 403(5) 而已；對話之訊息在使用者所使用的系統 401 與存取過濾器 403(1) 之間都未加密，又在存取過濾器 403(5) 與伺服器 407 之間都未加密。在極為靈敏之資訊的情形下，從近端存取過濾器到經由網路之路徑末端，即：在系統 403(1) 與伺服器 407 之間，可能需要鑑定和加密。

圖 5 顯示：怎樣使用一些存取過濾器 203 來達成此目的。在 VPN 內，除了一些存取過濾器 203 之外，可能和任何客戶端系統 401 或 503，或任何伺服器系統 407 使用鑑定和加密技術。當一客戶端電腦利用加密技術時，它會使用 SKIP 來鑑定對話，並使用一種在客戶端電腦與一被選擇存取過濾器 203 之間所共享的共享機密 (shared secret)，對該對話加以加密，然後會將已加密訊息發送到被選擇存取過濾器 203；藉以有效地闢建客戶端與被選擇存取過濾器 203 之間的隧道，進而使被選擇存取過濾器 203 和第一存取過濾器 203 可作存取核對之用。在第一存取過濾器 203 處，對訊息加以解密並執行存取核對。由於 SKIP 使使用者之證書和已加密訊息可供利用，故而使用者之已鑑定身份能夠被用於存取核對。若存取操作被允許；則對訊息再加密一次，並發送到最接近伺服器 407 的存取過濾器 403(5)，它會對該訊息加以解密。若資料庫 301 包含一種針對伺服器 407 的 SKIP 名稱和加密演算法 (algorithms)；則必要時，存取過濾器 403(5) 檢索針對伺服器 407 的證書，並使用 SKIP，以便

(請先閱讀背面之注意事項再填寫本頁)

表
訂
線

五、發明說明 (38)

必要時為伺服器407而對該對話重新加密。在其它情況，存取過濾器403(5)只是以明碼方式(in the clear)將訊息發送到伺服器407。若為伺服器407而對訊息重新加密，則伺服器407最後會接收已加密訊息並對它加以解密。位居第一存取過濾器203與最後存取過濾器203中間的一些存取過濾器203，都只是注意到該訊息是來自另一存取過濾器並利用SKIP加密，以及將該訊息傳遞而已，如上所述。當伺服器407檢索資訊資源時，它不是以明碼方式將它發送到存取過濾器403(5)，就是利用針對存取過濾器403(5)的密鑰而對包含資源的訊息加以加密。然後，依相反順序，成對地執行上述的解密和加密處理過程：從伺服器407到存取過濾器403(5)；從存取過濾器403(5)到存取過濾器403(1)；以及最後從存取過濾器403(1)到原始客戶端系統401，它會對訊息加以解密。

這種技術的效應是：在客戶機與伺服器之間的路徑上構築隧道，該隧道從在最接近客戶機之路徑上的存取過濾器203延伸到在最接近伺服器之路徑上的存取過濾器203。若客戶機能夠加密和解密，則隧道能夠從最接近客戶機的存取過濾器延伸到客戶機；且若伺服器能夠加密和解密，則隧道同樣地能夠從最接近伺服器的存取過濾器延伸到伺服器。一旦在路徑中的第一存取過濾器203已經被觸及，並已經鑑定對話；就不需要進一步加密或解密，直到最接近伺服器的存取過濾器203已經被觸及為止。而且，在每個存取過濾器203中的存取控制資料庫301都會包含針對：客

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (39)

戶機，伺服器，以及在路由中的諸多存取過濾器203之所有必要的識別和認證(certification)資訊。剛才描述的端對端加密技術之一優點是：與其集中注意力於用來連接VPN到網際網路的諸多存取過濾器，不如將加密負擔分佈遍及網路，藉以增強規模可伸縮性。

圖5顯示：該技術如何隨著對話501而運作，該對話隨著漫遊者而發起，那就是：客戶機503連接到VPN是經由網際網路121。漫遊者503配備有SKIP，就像在一內部網路上的目標伺服器407那樣。當SKIP被配置在漫遊者中時，就將針對存取過濾器403(3)的證書賦予漫遊者，並將針對漫遊者的證書賦予存取過濾器403(3)。當漫遊者503發送一項屬於對話的訊息時，它會將訊息定址到伺服器407，並使用它和存取過濾器403(3)共享之一傳送密鑰，對該訊息加以加密。於是，經由隧道505而將訊息鑿隧道傳送到存取過濾器403(3)。在那裏，存取過濾器403(3)會對該對話加以解密，執行存取核對，進而使用針對存取過濾器403(5)之一傳送密鑰而對該對話重新加密。在路徑中的諸多隨後存取過濾器403容許對話通過，此乃因為：該對話是由存取過濾器403(3)加以鑑定；於是，至少提供隧道507到存取過濾器403(5)。若目標伺服器407配備有SKIP，則存取過濾器403(5)會將隧道延伸到目標伺服器407，如上所述。

基於資料靈敏度的可適性加密和鑑定：圖6和7

3 基於資料靈敏度的可適性加密和鑑定：圖6和7

五、發明說明 (40)

在VPN中，在存取控制方面的一項重要工作是：決定對話所需安全性的最小量。這挺重要的，第一是因為：至少必須保證該最小量；第二則是因為：比需要還多的安全性會浪費資源。將用來決定最小而在存取過濾器203中所使用的諸多技術集體稱為安全加密網路遞送(Secure Encrypted Network Delivery，簡稱SEND)。在SEND中，存取控制資料庫301包含針對每個資訊資源的資料靈敏度等級。資料靈敏度等級會指示與資訊資源有關聯的保密等級(the level of secrecy)，並由對資源負有責任的安全管理員加以指定給資訊資源。諸多等級之一模範集合是：最高機密(Top Secret)，機密(Secret)，專用(Private)，以及公用(Public)。

用來指示資料靈敏度的等級也都被用來指示針對存取請求所需的信賴等級。如前面所描述的，唯若從下列信賴等級中所決定的信賴等級至少與該資訊之資料靈敏度等級一樣大，才會允許存取操作；該信賴等級有：用來識別使用者之技術的信賴等級，存取請求經由VPN 201之路徑的信賴等級，或用來對在路徑上所發送的訊息加以加密之任何加密技術的信賴等級。針對：使用者識別方法，路徑，以及加密演算的信賴等級都被包含在存取控制資料庫301中。關於路徑的信賴等級，將VPN分成一些網路組件，每個網路組件都是諸多IP網路之一連接集合，由存取過濾器203將它和其它組件加以分離。每個網路組件都有一個名稱和一種信賴等級。譬如說，一網際網路組件將會有"公

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (41)

用"信賴等級，而一內部網路組件則可能有"專用"信賴等級。一既定組件的信賴等級可能是基於它的實體安全性，或者是基於組件中之加密硬體的使用。因為將每個存取過濾器203增加到VPN，所以將一種它與VPN之諸組件連接的描述增加到資料庫301。包括在這種描述中的都是：諸多網路的信賴等級。因此，任何存取過濾器203都能夠使用它的資料庫301之拷貝來決定路徑之每個組件的信賴等級；而在一客戶機與一伺服器之間，將會藉由該路徑來載送一項對話。

使用者的信賴等級是從存取請求識別使用者所依照的方式中所決定的。在存取控制資料庫301中，每個使用者群組都有一種或更多與它有關聯的識別技術，而每種識別技術則都有一種最小信賴等級。諸多基本技術為：

- 經由SKIP的證書。使用者藉由在其X.509號證書中的名稱來加以識別，該證書則和SKIP通信協定一起使用，以便鑑定和加密通信量。
- 經由使用者識別客戶軟體的證書。使用者藉由在其X.509號證書中的名稱來加以識別，該證書則經由一種稱為使用者識別客戶軟體的特殊Conclave(秘密會議)客戶軟體模組而傳送到一些附屬存取過濾器203。使用一種口令/回應機制(challenge/response mechanism)，很安全地完成這項傳送。
- 經由使用者識別客戶軟體的Windows Domain ID(視窗網域識別符)。對Microsoft Windows Domain(微軟視窗

五、發明說明 (42)

網域)註冊(log in)且已經安裝使用者識別客戶軟體的使用者自動地具有其Windows身份，包括群組成員資格，並且傳送到一些附屬存取過濾器203。在NetBIOS(網路基本輸入/輸出系統)通信協定的機制內，很安全地完成網路登錄(logon)。

- 鑑定令牌。可能以下列兩種方式來利用鑑定令牌(諸如：由安全性動力公司(Security Dynamics Inc.)和亞贊特公司(Axent Corp.)所製造的那些令牌)：經由使用者識別客戶軟體，以在頻帶外的方式；或者，在Telnet(遠距通信網路)和FTP(檔案傳送協定)通信協定內，以在頻帶內的方式。
- IP位址及/或網域名稱。使用者之電腦的IP位址或全限定(fully qualified)網域名稱。

在SEND之一較佳建構例中，諸多識別技術都有一種從最高安全到最低安全的預定次序。應該將剛才列示的諸多技術加以排列次序，就像它們在上述列表中的那樣：最高安全的技術都是在列表的上端。雖然識別技術的排列次序(ordering)是有些主觀，但是卻反映了：識別技術的通用安全性，以及應用到使用者身份之分佈和確認的嚴密性(rigor)。在VPN 201中的管理員隨後會使有序(ordered)信賴等級與有序識別技術有關係。譬如說，若管理員使"專用"信賴等級與藉由鑑定令牌的識別技術有關係；則想要存取具有"專用"靈敏度等級之一資源的使用者必須親自識別，其方法是藉由：一種鑑定令牌，或者高於識別技術之順序

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(43)

中的鑑定技術的另一種識別技術。存取過濾器的管理員同樣地會：將在VPN中可供利用的諸多密碼演算法，從最高安全到最低安全加以排列次序；使有序信賴等級與有序密碼演算法有關係；將在VPN 201中所使用的諸多網路路徑加以排列次序；以及使有序信賴等級與有序網路路徑有關係。在信賴等級與關於安全性的排列次序之間的這些關係都包括在存取控制資料庫301中，然後，構築一種信賴及靈敏度等級與識別及加密技術有關係的SEND表。圖6是：這樣一種SEND表之一概念性表示法。

SEND表601有三欄：一欄是表示信賴/靈敏度等級的603，一欄是表示最小加密方法的605，以及一欄是表示最小識別方法的607。就關於欄605之諸加密方法的細節而言，請參看由布魯斯·史尼爾(Bruce Schneier)所著："應用密碼術"一書，該書由約翰·威利及後裔(John Wiley & Sons)圖書公司印行，美國紐約，1994年版。表中的每一列609使信賴/靈敏度等級與連接著存取過濾器，客戶機，及伺服器之路徑的最小加密等級和使用者之最小識別等級有關聯。於是，列609(1)使"最高機密"信賴/靈敏度等級與3DES加密演算法和經由SKIP而獲得的使用者證書有關係。希望獲得存取具有靈敏度等級為"最高機密"之一資源的使用者，因此必須具有一種由SKIP所認證的識別等級；且若路徑並不具有"最高機密"信賴等級，則必須利用3DES加密演算法對該對話加以加密。在另一方面，如列609(4)所示，希望獲得存取具有靈敏度等級為"公用"之一

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(44)

資源的使用者可能藉由任何方法加以識別，因而不必要對該對話加以加密。

當初啓一項新對話時，在針對該對話所使用之路徑中的第一存取過濾器203會繼續進行如下：

1. 存取過濾器203會決定正在被存取的資訊資源；並且，在資料庫301中查出(looks up)它的靈敏度等級。

根據SEND表601，針對該靈敏度等級的最小鑑定方法會載明：哪些識別機制可能被存取過濾器所使用，以便識別和鑑定執行存取操作的使用者。

第一存取過濾器203然後會查閱(consults)資料庫301，以便根據使用者所屬的使用者群組和資源所屬之資訊集來決定：使用者是否可存取資源。

第一步驟是根據存取控制資料庫來決定：用來識別使用者的諸多識別方法中，哪些方法具有對該資源之靈敏度等級而言是夠高的信賴等級。

然後，第一存取過濾器203根據具有夠高的信賴等級的每一種識別方法，使用使用者之識別資訊來查閱資料庫301，以便決定：使用者所屬的使用者群組。

第一存取過濾器203也會查閱資料庫301，以便決定：資源屬於哪些資訊集。

已決定了有關的使用者群組和資訊集，第一存取過濾器203就會查閱資料庫301，以便指出一些存取決策的位置，該決策決定：是否打算容許或拒絕存

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(45)

取對話資訊。若發覺到至少一個容許存取操作的決策以及發覺到沒有一個拒絕存取操作的決策，則容許使用者存取操作；在其它情況，則是拒絕存取操作。將步驟b，c及d的細節加以描述於下。

4. 若不拒絕存取操作，則第一存取過濾器203隨後會查閱資料庫301，以便決定組成路由的一些網路組件，該路由是：經由VPN，從客戶機到包含資訊資源的伺服器。

將路由加以考慮成為具有高達三個的邏輯分段(logical segments)：

1. 分段(a)，從客戶機到第一存取過濾器203。此分段可能已經加密或可能未曾加密，端視客戶機是否使用SKIP而定。
2. 分段(b)，從第一存取過濾器203到最接近伺服器而在路徑中的存取過濾器203；以及
3. 分段(c)，從最接近伺服器的存取過濾器203到伺服器；此分段也可能已加密或可能未加密。

若分段(a)和分段(c)存在，則每個分段將由單一網路組件組成。若客戶機在第一存取過濾器上，則分段(a)將不存在；若伺服器在最接近伺服器的存取過濾器上，則分段(c)將不存在。若分段(b)存在，則它將由一個或更多網路組件組成。若在客戶機與伺服器之間只有一個存取過濾器，則分段(b)將不存在。

就每個分段而言：

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(46)

4. 就分段(a)而言，必須由客戶機執行任何加密方法。若分段(a)的信賴等級至少不是與資源之資料靈敏度一樣強有力；或者，若由客戶機所執行的加密方法之信賴等級至少不是與資源之資料靈敏度一樣強有力；則拒絕存取操作。
5. 就分段(b)而言，若在路徑中之任何網路組件的最弱信賴等級大於或等於資源之資料靈敏度，則發送通信量而不必加密。這對應於網路本來就夠安全用來傳送資料的情形。在上表之實例中，可能在任何網路上傳送具有"公用"資料靈敏度等級的資訊資源，如列609(4)所示。然而，諸多存取過濾器203將會使用SKIP來鑑定對話，因而容許諸多隨後存取過濾器通過對話而不會招致：解密，存取核對，以及重新加密的較大開銷(overheads)。若針對路徑的最弱信賴等級小於資源之資料靈敏度，則為針對靈敏度等級所需之最小加密演算法而查閱SEND表，進而使用該演算法，對該對話加以加密。加密使通信鏈路(link)的安全性升級(upgrades)，使它適合於載送該既定靈敏度之資料，因而允許由使用者存取資源。
6. 就分段(c)而言，從最接近伺服器的存取過濾器203到伺服器的路徑部分，第一存取過濾器203根據資料庫301中的資訊而決定：分段(c)以及在分段(c)中所使用之任何加密方法的信賴等級。若路徑的這

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(47)

個分段之信賴等級小於資訊資源之靈敏度等級，並且在那種情形下，若在分段(c)中所使用的加密方法之信賴等級至少不是與所需等級一樣強有力，該所需等級就像在考慮資訊資源之靈敏度等級的SEND表中的最小等級那樣；則第一存取過濾器203將會拒絕存取操作。

上述決定靈敏度和信賴等級的方法保證：只有當需要達到必要的信賴等級時，存取過濾器203才會使用加密方法。在使資料庫301中之網路配置的描述保持既簡單又可管理的時候，此方法會減少將被加密之對話的數目。結果是：關於VPN中的管理和效能方面，會有較好的規模可伸縮性。

圖7提供：資訊資源的靈敏度等級，使用者識別方法的信賴等級，以及和客戶機與伺服器之間的路徑有關聯的信賴等級是怎樣影響由使用者存取資訊資源之一實例。在圖7中，在客戶端703處一配備有SKIP的使用者初啓一項對話701，以便獲得儲存在配備有SKIP的伺服器705處之一資訊資源723。上述討論的分段(a)出現在圖7中的707處；分段(b)出現在709(1,...,4)處；分段(c)出現在711處。資訊資源723具有"機密"之靈敏度等級。該對話遭遇的第一存取過濾器203是存取過濾器203(1)。存取過濾器203(1)使用它的存取控制資料庫之拷貝決定資源723的靈敏度等級。此處，使用者已經使用SKIP證書，而檢視資料庫301中之SEND表601則對存取過濾器203(1)顯示：因為這種使用者

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (48)

識別方法滿足具有"機密"靈敏度等級之資訊資源的要求，所以在707處的分段(a)具有所需信賴等級。因此，第一存取過濾器繼續決定：在VPN中，在存取過濾器203(1)與伺服器705之間位在709(1,...,4)處之分段(b)和位在711處之分段(c)的信賴等級。分段709具有一些子分段：709(1)，709(2)，709(3)，709(4)，以及709(5)；而第一存取過濾器203(1)會核對在資料庫301中的這些分子分段中的每個子分段之信賴等級。分段709(2)是網際網路121，所以它的信賴等級是："公用"，它在分段709中是最小等級。然後，存取過濾器203(1)使用存取控制資料庫301來核對分段711之信賴等級。它的信賴等級是："機密"。於是，在709處之分段(b)只是具有一種對正在存取一"機密"資訊資源703之一對話的路徑而言是太低的信賴等級而已。要處理這個問題，存取過濾器203(1)必須對該話加密，以便將它提升到必要的信賴等級。第一存取過濾器203(1)會查閱SEND表601，以便決定需要何種加密方法；而列609(2)則指示：DES加密方法是足夠的。於是，第一存取過濾器203(1)會使用該演算法來對該對話加密，進而將它發送到存取過濾器203(5)。

在圖7中，連接著客戶機703到存取過濾器203(1)的分段707具有一種對資源之靈敏度等級而言是夠高的信賴等級，於是客戶機703不必對其請求加以加密。當不是這種情況時，唯若客戶機703已經使用一種其信賴等級資源之靈敏度等級而言是足夠的加密方法來對請求加密，存取過

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (49)

濾器 203(1) 才會賦予客戶機 703 存取操作。為此緣故，在圖 5 中的漫遊者 503 必須是配備有 SKIP 的。由於漫遊者 503 經由網際網路 121 來存取：存取過濾器 403(3) 的資訊；故而漫遊者 503 的諸多請求可能從未具有高於“公用”的信賴等級，除非將它們加以加密；並且，為了完全存取在 VPN 201 中的資源，漫遊者 503 就必須使用一種加密方法，諸如：由 SKIP 所提供的一種方法，其信賴等級對最高靈敏度等級而言是足夠的。在存取過濾器 203 的一些實施例中，存取過濾器可能以一種與它在較佳實施例中使用來協商使用者識別模式類似的方式，和客戶機協商打算使用在請求中的加密技術。

針對存取控制資料庫 301 之管理員界面的總覽：圖 8 到 12

3 針對存取控制資料庫 301 之管理員界面的總覽：圖 8 到 12

存取決策依據使用者群組和資訊集來定義存取操作；因此，在可能定義存取決策之前，管理員必須定義使用者群組和資訊集；將怎樣完成此事顯示於圖 8 中。定義使用者群組涉及了步驟 803 到 807：首先定義使用者，然後定義使用者群組，然後再將使用者指定給適當使用者群組。定義資訊集涉及了步驟 809 到 813：首先定義資源，然後定義資訊集，然後再將資源指定到資訊集。當針對在一項決策中所涉及的使用者群組和資訊集而已經完成此事時，就能夠建立存取決策，如在 815 處所示。如前面所指出的，雖然制定針對諸多使用者群組和資訊集之存取決策的權利都由決策制定者決策所決定的；可是用來定義和決定使用者群

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (50)

組之成員資格和資訊集，以及用來為它們而制定管理決策的權利卻都是由管理決策所決定的。

就像從前述中能夠看出的那樣，使用者界面通常被用來定義在兩個實體或關於它們的集合之間的關係。針對存取控制資料庫 301 之圖形使用者界面 (graphical user interface, 簡稱 GUI) 的通用形式對應於該工作。顯示圖包括兩個視窗，每個視窗都包含打算使彼此有關係的一些實體之表示法，而關係則藉由選擇實體和需要之所在來定義的，因而定義關係。

定義使用者群組：圖 9

3 定義使用者群組：圖 9

圖 9 顯示：用來殖民 (populating) 和定義使用者群組的顯示圖 901。在顯示圖中的視窗 903 包含目前定義的使用者群組之一分層顯示圖：視窗 903 與那些用來顯示由 微軟 公司 (Microsoft Corporation) 所製造的 Windows 95 商標之作業系統中的檔案層次之視窗相似。在視窗 903 中，使用著顯示圖 901 之管理使用者具有管理權所針對的諸多使用者群組都呈現黑色；而其它使用者群組則都呈現灰色。在兩個視窗之上的是兩個按鈕帶 (button bars)：911 和 915。按鈕帶 911 列示：用來修改存取控制資料庫 301 的一些可利用顯示圖，而按鈕帶 915 則列示：可能在那些顯示圖上執行的一些操作。於是，在按鈕帶 911 中標示 "使用者群組" 的按鈕被凸顯出，因而指示：顯示圖 901 是用來殖民和定義使用者群組的一個顯示圖。關於按鈕帶 915，當視窗 903 是現用

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(51)

狀態時，有權管理一使用者群組之一管理使用者可能會修改使用者群組，其方法是：在視窗903中選擇使用者群組；並使用在按鈕帶915中的"刪除"(delete)按鈕來刪除使用者群組；或者，使用"新增"(new)按鈕來增加並命名位在層次中的被選擇使用者群組之下的一個新使用者群組。當管理使用者點按(clicks)："應用"(apply)按鈕921時，存取過濾器203就會修改它的存取控制資料庫301之拷貝，以便證實何種東西在顯示圖901上；並且將修改資訊傳播到：在VPN中的所有存取控制資料庫301之拷貝。

視窗909顯示使用者。藉由識別在集合中之使用者所依照的方式，將使用者之一集合指示於顯示圖中。在此情形下，使用者都是藉由IP位址來識別，而他們則都會以IP位址之範圍出現在顯示圖中。按鈕帶913指示：能夠顯示在視窗909中之其它種類的識別方法。就像利用視窗903那樣，當視窗是現用狀態時，能夠使用"新增"和"刪除"兩個按鈕來增加和刪除使用者。要將由使用者識別資訊所載明的(諸多)使用者指定給一使用者群組，GUI之使用就會選擇：一使用者群組，如在917處所顯示的，以及識別資訊之一集合，如在919處所顯示的；然後再使用在按鈕帶913中的"增加到使用者群組"(add to group)按鈕，將識別資訊之集合增加到使用者群組，就像由以下事實所顯示的那樣：在919處之被選擇IP位址之範圍現在會出現在位於917處之被選擇使用者群組之下的層次中。本操作之效應是：使諸多使用者成為"研發"(R&D)使用者群組的成員，該使

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (52)

用者的對話都具有列示在917處的來源IP位址；並且，當使用者點按："應用"按鈕時，於是所有存取控制資料庫301之拷貝都被修改。

圖10顯示：用來定義資訊集的顯示圖1001，此處，視窗1003包含一種資訊集的分層列表，而視窗1005則包含一種可用資源的分層列表。用與使用者群組之列表相同的方法來制定：資訊集的分層列表，以及可用使用者群組的分層列表。再者，顯示圖1001之使用者有管理權限加以管轄的資訊集和可用資源都呈現黑色；而在列表上的其它項目則都呈現灰色。在視窗1001中，可用資源為：網際網路和組成VPN 201的兩個位置。在一種更加開發的VPN 201中，可用資源的列表應該指示：在位置處的伺服器，在伺服器中的服務，以及由服務所提供的資訊項。譬如說，若服務提供一種目錄樹，則應該藉由一個路徑名稱(pathname)來指示包含在目錄樹中的資訊項；該路徑名稱會載明目錄樹之根部(root)，並且會使用通配字元(wildcard characters)來載明在目錄樹之根部以上的一些檔案。當將一資源增加到一伺服器時，可能經由視窗1005來定義資源。於是，已經定義了資源，可能用與一使用者識別資訊被指定給一使用者群組相同的方式來將一資源指定給一資訊集。再者，點按："應用"按鈕會使顯示圖1001中的改變傳播到所有存取控制資料庫301之拷貝。

圖11顯示：用來定義決策的顯示圖1101。將哪一類型的決策正在被定義加以載明於按鈕帶1113中；如在那裏所指

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明(53)

示的，顯示圖1101正在定義存取決策。所有的決策顯示圖都具有相同的通用格式：一視窗1103，它包含使用者群組之一分層顯示圖；一視窗1105，它包含可能定義決策所針對的物件層次之一顯示圖；以及一決策定義視窗1107，它包含一些存取決策定義1108。在物件層次中，顯示圖1101之使用者有權定義決策所針對的物件都呈現黑色；而其它的則呈現灰色。在顯示圖1101中，正在被定義的是存取決策，所以物件都是資訊集。

每個存取決策定義都有四個部份：

- 一現用(active)圈選框1117，它指示由決策定義所定義的存取決策是否現用的，即：正在被用來控制存取操作；
- 存取決策正在被定義所針對的使用者群組1119；
- 存取決策正在被定義所針對的資訊集1123；以及
- 存取操作欄位1121，它指示存取操作是否被容許或拒絕，藉以定義存取決策。

選單帶(menu bar)1109和按鈕帶1115允許決策制定者決策容許如此做的那些管理員加以編輯，增加，刪除，以及啟動(activate)或撤除(deactivate)一種被選擇決策定義1108。每個決策定義1108的現用圈選框1117允許管理員啟動或撤除選擇決策定義1108；存取操作欄位1121允許管理員選擇容許或拒絕作為決策。在按鈕帶1115中的"刪除"按鈕允許管理員刪除一項被選擇決策；而"新增"按鈕則允許管理員制定一種新決策定義1108；要執行此事，管理員會選擇：

(請先閱讀背面之注意事項再填寫本頁)

製

訂

線

五、發明說明 (54)

在視窗1103中之一使用者群組以及在視窗1105中之一資訊集；然後會按"新增"按鈕。新的存取決策定義1108出現在顯示圖1107中；並且，管理員能夠編輯新的存取決策定義，如剛才所描述的。要將改變應用到存取控制資料庫301，並將它傳播到所有的存取過濾器203；管理員會點按在"應用"按鈕1125上。

顯示圖1101也包含一種決策評估者工具程式(policy evaluator tool)，它讓管理員看出：存取決策定義的目前集合怎樣決定針對一既定使用者群組或資源集的存取操作。當管理員點按：按鈕帶1113中的"決策評估"(policy evaluation)按鈕，並從顯示圖1103中選擇一使用者群組時；該工具程式就會顯示：被選擇使用者群組呈現藍色；決策定義允許使用者群組存取而在顯示圖1105中的所有資訊集呈現綠色；而其餘的則呈現紅色；與哪些資訊集可能被使用者群組存取之決定有關的所有決策定義都被凸顯在相同的顏色集合中。若管理員選擇一資訊集，則發生相同的事情；然後，評估者工具程式會顯示：被選擇資訊集呈現藍色，能夠存取資訊集的所有使用者群組呈現綠色，而其餘的則呈現紅色，因而也會凸顯出一些有關的決策定義。使用者也能夠選擇一項決策。在那種情形下，被選擇決策呈現藍色，而受決策影響的使用者群組和資訊集則都呈現藍色或紅色，就像由決策所決定的那樣。使用者能夠另外選擇一個以上的：使用者群組，資訊集，或決策。在那種情形下，評估者工具程式對每項決策顯示：應用到所

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (55)

有的被選項，以及那些決策的效應。評估者工具程式能夠藉由點按在按鈕帶1113中的"決策評估"按鈕來關斷(truned off)，而顏色和凸顯功能(highlights)則能夠藉由點按在按鈕帶1115中的"重新設定評估"(reset evaluation)按鈕來關斷，以便針對一項新的決策評估而準備。

圖12顯示：顯示圖1201被使用來將關於一存取過濾器203的資訊輸入到存取控制資料庫301。視窗1203顯示：存取過濾器203之一分層列表；當視窗是現用狀態時，可能使用在按鈕帶1209中的"新增"和"刪除"兩個按鈕來增加或刪除存取過濾器。視窗1205被用來輸入或顯示關於存取過濾器203的資訊。在視窗1207中的顯示圖是藉由點按在按鈕帶1207中之一按鈕來決定的；如按鈕所顯示的，能夠使用在視窗1207中的顯示圖，以便：輸入並檢視關於諸多存取過濾器203之網路連接的資訊，輸入並檢視關於那些連接之信賴等級的資訊，針對可用伺服器和服务而掃描網路，針對存取過濾器203中所檢測的問題而建立警戒資訊(alerts)，載明針對軟體的可選擇參數，以及載明存取控制資料庫301改變的分配順序。"警戒資訊建立"(alert setup)的凸顯功能指示：顯示於圖12中的顯示圖1205是用來顯示並建立警戒資訊的顯示圖。

用來發明資源的使用者界面：圖18和24

3 用來發明資源的使用者界面：圖18和24

VPN 201的使用者都有一種用來察看在VPN 201內何種資源可供他們利用的界面。在此處稱為IntraMap(映像內)界

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (56)

面 (IntraMap 是 網際網路動力公司 (Internet Dynamics, Incorporated) 之一商標) 的界面，至少會對每位使用者顯示：屬於使用者可能根據針對使用者所屬之使用者集合的存取決策來存取之資訊集的資源。在其它一些實施例中，IntraMap 也可能將資源的靈敏度等級以及使用者之識別方法的信賴等級加以考慮。

藉由一種小爪哇程式 (Java™ applet) 來建構 IntraMap 界面，該程式是在任何配備有 Java 的全球資訊網 (www) 瀏覽器上執行的。使用網路瀏覽器，使用者能夠掃描圖形顯示圖，以便：尋找並存取可供使用者利用的資源；或者，請求存取目前不是可供使用者利用的資源。由使用者存取資源是由應用到使用者和資源的諸多存取決策所決定。圖 18 顯示：由 IntraMap 界面所產生顯示圖 1801。IntraMap 顯示圖 1801 的左側顯示：資源列表 1803；而顯示圖的右側則顯示：尋找 (Find) 欄位 1807，排序 (Sort) 區段 1809，服務 (Services) 區段 1811，以及描述 (Description) 欄位 1813。藉由點按 "輔助" (Help) 按鈕 1815 而使使用 IntraMap 的線上輔助程式 (on-line help 可供利用)。

資源列表 1803 顯示：針對正在使用 IntraMap 界面的使用者而言，在 VPN 201 中之可供利用的資源和資訊。這種列表是分層的。使用者能夠藉由點按在分支上的 "+" 和 "-" 標記來擴展 (expand) 或縮減 (collapse) "樹" 的分支。在列表中的每個登載項 (entry) 1804 都會包括資源名稱。用來顯示登載項之顏色則指示：使用者具有何種存取操作。若登載

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (57)

項1804被顯示呈現藍色：則使用者具有一種針對資源的現用超通信鏈路(hyperlink)，並可能點按資源兩次，以便將它顯示出來。若資源被顯示呈現黑色，則雖然它也可供使用者利用，但卻沒有超通信鏈路可供利用，所以必須使用一種分離應用程式來檢索資源。雖然被顯示呈現灰色的資源都不是直接地可供使用者利用，但是如果使用者選擇一項資源，IntraMap界面就會開啓一對話盒(dialog box)：允許使用者將請求存取操作的電子郵件(e-mail)發送給管理員，該管理員對資源所屬之資訊集的存取決策負有責任。然後，管理員必要時可能修改存取及/或管理決策，以便賦予使用者存取操作。管理員可能進一步賦予資源"隱藏"特性(hidden property)。當資源具有該特性時，唯若使用者屬於存取決策允許存取資源所屬之一資訊集之一使用者群組，資源才會出現在IntraMap界面1801中。若資源不具有隱藏特性，則它總會出現在IntraMap界面1801中。在其它情況，它不會出現。資源可能具有一項比包含在它的登載項1804中的描述還要詳細的描述。當使用者選擇資源時，該項描述就被顯示於描述欄位1813中。

除了資源列表1803之外，IntraMap顯示圖1801還會顯示兩個專業化(specialized)資源列表在1805處。

- "何者最新"(What's New) 1806顯示：來自企業內之其它部門的最近資訊告示(postings)。若管理員已經賦予使用者存取"何者最新"之網頁，則使用者可能將一項新資源之URL(共通資源指標)公告在那裏。

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明 (58)

- "何者最受歡迎"(What's Hot) 1808基於資源多久才被存取，顯示出企業之最受歡迎的資訊資源。

在1811處的服務類型控制表會讓使用者過濾一些按照提供資源的服務類型而打算顯示在資源列表1803中的資源。在服務類型控制表1811中，每種服務類型都有一個圈選框。若該框被圈選，則包括該服務類型且與此服務有關聯的資源都會出現在資源列表中。在其它情況，與此服務有關聯的資源都不會出現在資源列表中。

IntraMap界面讓使用者按照：資訊集，位置，或服務來排序資源列表1803。要執行這件事，使用者會選擇他想要的方式來排序在排序欄位1809中的資源列表。使用者也可能會載明資源種類(categories)被使用在排序欄位中的順序。該界面還具有一種搜尋功能。要執行搜尋功能，使用者會將一搜尋字串(search string)輸入"尋找"欄位1807中。然後依照載明於排序欄位1809中的順序，加以搜尋針對關於字串之諸資源的資源列表和資源描述。搜尋功能只是找尋全部或部份的字組匹配(word matches)而已。情形不是挺靈敏的，顯示出第一次匹，就可能使用一些功能鍵，以便指引(navigate)到其它的匹配。當然，若使用者尚未核對在服務類型欄位1811中之一服務類型，則該服務類型的諸多資源在排序或搜尋操作中都未涉及。

圖24顯示：IntraMap界面之一建構例2401。對於VPN 201的使用者，IntraMap界面以網頁出現，該網頁是由正在圖2之存取過濾器203(c)上執行的報表管理程式209所提供的

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (59)

諸多資源中的一種資源。在VPN 201中之一使用者；或者，甚至於一般大眾(那就是：成為網際網路使用者群組之一成員的某人)都可能用與他可能被賦予存取任何其它資源相同的方式，被賦予存取IntraMap界面。就像從下列描述中將會顯而易見的那樣，針對IntraMap的網頁可能是在VPN 201中的任何伺服器上。建構例2401具有：在工作站(workstation)2403中，由使用者所使用以便審視(look at)IntraMap的組件；在對工作站2403而言是局部的存取過濾器203(I)中的組件；以及在存取過濾器203(c)中的組件，該存取過濾器是報表管理程式209會在其上執行的存取過濾器。當然，存取過濾器203(c)也可能執行一種局部存取過濾器那樣的功能。局部存取過濾器203(I)是藉由VPN 201而連接到報表存取過濾器203(c)，而工作站2403則是藉由區域網路(LAN)213而連接到局部存取過濾器203(I)。

就像稍後將要更加詳細說明的那樣，所有的存取過濾器203都具有一種分層架構(layered architecture)。最底層級是一種網際網路分包資訊(IP)過濾器2419，它只是處理網際網路分包資訊標題而已。分包資訊過濾器2419讀取在網際網路分包資訊標題中的來源和目標位址，並將一套規則應用到分包資訊。就像由規則所決定的那樣，IP過濾器不是接受它們，捨棄它們；就是進一步在VPN 201中路由指引著它們。該規則也會決定：在存取過濾器203內，打算怎樣路由指引諸多被接受分包資訊。架構中的下一層級是服務代理伺服器(service proxies)2427。服務代表伺服器會

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明(60)

截取針對諸如全球資訊網(www)之服務的通信量，並執行關於通信量的存取核對。若存取過濾器203提供服務本身或執行針對提供服務之一伺服器之存取核對，則IP過濾器2419會將針對服務的分包資訊發送到針對服務之一服務代理伺服器2427。服務代理伺服器使用存取控制資料庫301來執行針對服務的通信協定層級之存取核對。譬如說，針對網路(Web)服務的服務代理伺服器可能檢查：正在提出一項針對既定網頁的請求之使用者是否有權存取該網頁。下一個更高層級是服務層級2425；若有關的服務代理伺服器允許一項請求且存取過濾器也是針對該服務的伺服器，則打算處理前往在服務層級2425處之服務的請求。在網頁之情形中，該服務應該指出網頁的位置，並將它轉回給請求者。在IntraMap中，涉及兩種服務：Web(網路)服務和IntraMap服務。在圖2401中，Web服務以WebS 2423出現。針對WebS 2423的代理伺服器是WebP 2421；為了在下列描述中將會變得顯而易見的諸多理由，IntraMap服務只有一個代理伺服器：IntraMap 2417。此外，存取控制資料庫301包括IntraMap資訊2422，它是一種在存取控制資料庫301中之資訊的最佳化版本(optimized version)，可作IntraMap顯示圖的基礎用。

關於在存取過濾器203(c)與存取過濾器203(I)之間的IntraMap建構例的主要差異是：存取過濾器203(c)包括一種具有IntraMap小爪哇程式2411之拷貝的全球資訊網網頁2410。當從存取過濾器203(I)下載(downloaded)到工作站

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(61)

2403中的網路瀏覽器2429時，小爪哇程式2411會產生指向IntraMap伺服器2425的請求，進而使用由IntraMap伺服器2425所轉回的結果來產生IntraMap顯示圖1801。

操作如下：對於工作站2403的使用者，IntraMap可能以針對網頁之一通信鏈路出現。於是，要使用IntraMap，使用都會啟動針對IntraMap網頁2410之一通信鏈路。在工作站2403中的網路瀏覽器2429會對啟動通信鏈路作回應，就像它應該對啟動針對網頁之任何其它通信鏈路作回應那樣：它提出一項針對網頁的請求，並將該請求發送到通信鏈路中所指示的伺服器。在針對IntraMap之通信鏈路的情形中，因為通信鏈路載明在存取過濾器203(c)中的網路伺服器2423，所以請求會經由局部存取過濾器203(I)和VPN 201而前往存取過濾器203(c)。就像對於VPN 201中之一資源的任何其它存取操作那樣，局部存取過濾器203(I)會執行針對IntraMap網頁請求的存取核對。由於該請是針對網頁，故而由網路代理伺服器2421來完全存取核對。在大多數的VPN 201中，對於在VPN 201中的任何使用者而言，IntraMap網頁2410將是可存取的；於是，存取控制資料庫301指示：具有一有效IP來源位址的任何使用者都可能存取IntraMap網頁2410。

當存取過濾器203(c)中收到請求時，IP過濾器2419就會將它轉遞到網路代表伺服器2421，它依序地將請求轉遞到網路伺服器2423，它藉著將IntraMap小爪哇程式2411下載到工作站2403中的網路瀏覽器2429而對該請求作回應，

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明(62)

其中：IntraMap小爪哇程式2411開始在網路瀏覽器2429中執行。在執行期間，它會將一項請求發送到針對IntraMap資訊2422的IntraMap代理伺服器2427。像所有的小爪哇程式一樣，IntraMap小爪哇程式2411會將請求發送到它所處的伺服器，在這種情形下，就是存取過濾器203(c)。然而，就像對於來自工作站2403的任何其它存取操作那樣，請求會藉由局部存取過濾器203(I)而前進。瞧，IntraMap代理伺服器2427會檢測出請求被定址到存取過濾器203(c)中的IntraMap代理伺服器2427，而不是將請求發送到存取過濾器203(c)；從局部存取過濾器203(I)中的存取控制資料庫301之局部拷貝中獲得IntraMap資訊2422；過濾該資訊，使得它載明：只會存取那些屬於使用者所屬的諸多使用者群組所針對的資訊集之資源來產生列表2431；進而經由LAN 213，將它轉回給IntraMap小爪哇程式2411，該程式隨後使用列表2431來產生IntraMap顯示圖1801。在產生顯示圖方面，小爪哇程式2411會應用載明於請求中的任何存取過濾器，也會排序如請求中所載明的列表。列表2431不但指示可供利用的資源，而且包含需要用來提取(fetch)資源的資訊。於是，若資源具有一種超通信鏈路，則將超通信鏈路包括在列表中；若它是一種雖然使用者目前不會存取，但是使用者卻可能請求存取所針對的資源，則列表包括：針對資源之管理員的名字和電子郵件地址。

存取控制資料庫301之細節：圖13到17

3 存取控制資料庫301之細節：圖13到17

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明(63)

在存取過濾器203之一較佳實施例中，在兩個層級處加以建構存取控制資料庫301：一個層級是由圖形使用者界面所使用，以便操縱存取控制資料庫301；而另一個層級則是使用在實際存取核對中。使用由微軟公司所發展出的Microsoft Jet商標之資料庫系統來建構第一層級。第二層級則是使用一些根據第一層級資料庫所編譯的記憶體映射檔案(memory mapped files，簡稱MMF)加以建構的。下列討論將會描述第一層級建構例，並且說明包含在其中的資訊怎樣被使用在存取核對中。在研讀這項討論中，應該記得：實際存取核對是使用MMF加以完成的，就像稍後將要詳細描述的那樣。

就像對於大多數資料庫系統的情形那樣，Microsoft Jet商標之資料庫系統具有一種圖表，那就是：資料庫之邏輯結構的一種描述。圖13到17都是：由針對存取控制資料庫301之圖表的Microsoft Jet商標之資料庫系統所產生的顯示圖。圖13顯示：針對定義諸多使用者群組之資料庫的一部份的圖表1301。顯示圖由兩種要素組成：在資料庫中的"表之類別"(classes of tables)1303的表示法，以及顯示屬於表之某些類別的兩種表之間關係的"通信鏈路"1305的表示法。表之類別的表示法顯示：在1310處的類別名稱；以及在1308處，將被包含在屬於該類別的每一種表中的資料欄位。每一種表的實例都有一種由資料庫系統所指定的識別符(ID)。在表中的其它資料會隨著表之類別而變化。藉著使用在第一表中之第二表的ID來建立一種在屬於表

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(64)

之第一類別的第一表與屬於表之第二類別的第二表之間的通信鏈路，反之亦然。於是，通信鏈路1305顯示：能夠將"使用者群組樹"類別表1307中的一些表和"使用者群組"類別表1309中的一些表加以鏈接。某些通信鏈路在它們的兩個末端處都有數字。該數字指示：在數字所在之末端處，該表可能具有的通信鏈路數目。於是，連接著類別表1309和類別表1307的通信鏈路具有：在針對類別表1309之末端處的數字1，以及在針對類別表1307之末端處的數字 ∞ ；因而指示：類別表1309之諸實例中的任何數目的ID都可能出現在類別表1307之一實例中；但是，類別表1307之一實例中的只有一個ID才可能出現在類別表1309之一實例中。

使用者群組表：圖13

3使用者群組表：圖13

使用者群組表1301包含針對資料庫301中的每個使用者群組之使用者群組類別表1309。在"使用者群組"類別表1309中，特別有興趣的資料包括：群組名稱，它是群組之字元串(character-string)名稱；群組描述，它是群組之字元串描述；以及預先定義的資訊，它指示其中成為群組之一成員的使用者是否為：一位管理員，即，能夠制定管理決策；一位安全官員，即，能夠制定決策制定者決策；或者一位單純的資訊使用者。使用者群組表1301會進一步將諸多使用者群組組織成一種層次列表--不但為了繼承權，而且為了顯示於圖9之視窗903中的使用者群組之分層顯示

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(65)

圖，因而使使用者之識別方法與使用者群組有關聯，以及使警戒資訊與使用者群組有關聯。組織成層次列表是藉由"使用者群組樹"類別表1307中的一些表來完成的。"使用者群組樹"類別表中的每一種表都會將"使用者群組"類別表中之一表鏈接到一種母(parent)使用者群組(也是"使用者群組"之類型)。對於一種特定"使用者群組"表而言，多重"使用者群組樹"表可能存在，端視一特定使用者群組出現在其中之位置的數目而定。

就像已經提及的那樣，有五種不同的方式用來識別至一存取過濾器203之使用者：藉由IP位址範圍，藉由一種全限定網際網路網域名稱，藉由在Microsoft Windows商標之作業系統中的使用者身份，藉由一種鑑定令牌，以及藉由證書。針對藉由證書來識別使用者之表的類別表(table classes)被顯示在1321處。針對藉由IP位址範圍來識別使用者之表的類別表被顯示在1317處；針對藉由IP網域來識別使用者之表的那些類別表被顯示在1319處；針對藉由Microsoft Windows商標之作業系統ID(識別符)來識別使用者之表的那些類別表被顯示在1315處；以及針對藉由鑑定令牌(在圖中，標示為智慧卡)來識別使用者之表的那些類別表被顯示在1323處。最後，類別表1325會定義：針對與使用者群組有關而用於警戒之資訊的一些表。"使用者群組"類別表1309中之一表，可能使它與針對用來識別使用者之任何方式的任何數目的表有關聯。就像此事意謂著那樣，可能同時用很多不同的方式來識別一既定使用者。

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(66)

爲了執行存取核對，存取過濾器203必須決定：正在提出請求之使用者屬於哪些使用者群組。該請求包括使用者識別方法，因而識別方法是決定之起點。在使用者群組表1301中的一些表都會允許存取過濾器203：根據識別方法來決定使用者屬於哪些使用者群組，並且根據那些使用者群組來決定一些決定使用者所屬之其它使用者群組的分層關係。假定使用者是藉由IP位址加以識別，存取過濾器203藉由尋找"IP位址範圍定義"類別表(在1317中)中的一個或更多的表而開始運作，該類別表定義：包括使用者之IP位址在內的IP位址之範圍。這些表中的每一種表都有一條指向"IP位址範圍"類別表(在1317中)的通信鏈路，該類別表使"IP位址範圍定義"類別表中所定義的範圍與一使用者群組ID有關係，就對應於IP位址範圍的使用者群組而言，它依序地可作爲一條指向"使用者群組"類別表1309的通信鏈路之用。"使用者群組"類別表1309中的每一種表都有一條指向"使用者群組樹"類別表1307的通信鏈路，因此能夠順著一些通信鏈路而指向針對一些使用者群組的"使用者群組"類別表，因而由IP位址所載明的一些使用者群組都會繼承存取權利。於是，在處理過程結束時，IP過濾器203已經指出所有使用者群組的位置，它們都與決定使用者是否可能存取資源有關。而且，IP過濾器203根據請求而瞭解：怎樣識別使用者；並根據請求而能夠決定：應該指定何種等級給用於請求中的使用者識別方法。將使用者群組表1301中的資訊加以編譯進入MMF(記

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(67)

憶體映射檔案)中。當使用者初啓一項對話時，使用者會提供一種使用者識別方法給在對話路徑上的第一存取過濾器203；存取過濾器203使用具有MMF的使用者識別方法，以便作出一項等效於以上所說明之一決定的決定。於是，存取過濾器203能夠決定：對於一既定使用者識別方法而言，它是否識別有權存取資訊之一使用者；它是何種使用者識別方法；因此它具有何種信賴等級；以及使用者屬於哪些使用者群組。於是，使用者群組表1301包含了：針對一項存取決策1108之使用者部份所需的所有資訊。

資訊集表：圖14

3 資訊集表：圖14

圖14顯示：針對定義資訊集的一些表之圖表1401。這些表會使諸多資訊集(在圖14中的資源群組)與組成它們的資源有關係，並與資源之網路位置有關係；並且也會將諸多資訊集組織成：在圖10中之1003處所顯示之資訊集的分層列表。在存取控制資料庫301中的每個資訊集都是由"資源群組"類別表1403所表示。藉由表1419而將資源群組類別表中的一些表加以組織成一種針對繼承權和顯示目的的層次。資訊集與掌握中組成它的一些資源之間，以及與儲存它們在其中而在VPN中的一些位置之間的關係都是由"資源群組單元"(resource group elements)類別表1407中的一些表所建立的。可能將"資源群組"類別表鏈接到"資源群組單元"類別表中的任何數目的表。將"資源群組單元"類別表其中之一表鏈接到諸多類別表："網站單元"(Site

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (68)

Elements) 1411, "服務" 1413, 以及 "資源" 1409 中的任何數目的表。針對資料庫 301 中所表示的每一項資源都會有 "資源" 類別表。包括在該表中的有: 資源之 ID; 其名稱; 針對提供資源的服務之 ID; 針對定義資源的靈敏度等級之 ID; 資源描述; 資源管理員的電子郵件地址; 以及一種隱藏旗標 (hidden flag), 它指示著 IntraMap 是否應該將資源顯示給不屬於一些有權存取資源之使用者群組的使用者。IntraMap 界面會獲得它需要的資訊, 該資訊關於來自針對資源之 "資源" 表的一項資源。

兩種類別表: "網站單元" 和 "服務" 中的一些表, 以及兩種類別表: "網站" 1415 和 "伺服器" 1417 中的一些表都是屬於描述著在 VPN 中之資訊位置的類別表 1421。針對在 VPN 中的每一個實體位置都會有 "網站" 類別表; 針對在 VPN 中的每一個伺服器都會有 "伺服器" 類別表; 以及針對在 VPN 中的每一項服務都會有 "服務" 類別表。在 "網站單元" 類別表中的一些表中的通信鏈路都會使諸多網站與諸多伺服器有關係; 在 "伺服器" 類別表中的一些表中的通信鏈路都會使諸多伺服器與它們提供的諸多服務有關係; 以及在 "服務" 類別表中的一些表中的通信鏈路都會使諸多服務與它們寄宿 (host) 的諸多資源有關係。

在決定被請求資源屬於何種資訊集方面, 存取過濾器 203 就從請求中的資訊開始。該請求被包含在一種 IP 分包資訊中, 因此具有: 一標題和一主體 (body)。在標題中, 有: 一 IP 位址, 它載明在虛擬專用網路 201 中之一位置,

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(69)

以及在該位置處之一伺服器；一埠號，它載明關於伺服器之一項服務。而在本體中，則有：以通信協定所規定的形式呈現之資源描述。譬如說，若請求是針對一網頁，則資源描述將是資源之URL。存取過濾器203使用IP位址來指出"網站"類別表的位置，使用在該表中的通信鏈路來指出"網站單元"類別表1411的位置。該表使網站與針對網站處之諸伺服器的伺服器ID(識別符)有關係；並且，存取過濾器203會使用伺服器ID來指出針對網站之諸伺服器的"伺服器"類別表1417中的一些表的位置。然後，它能夠再使用IP位址來指出對應於載明在請求中之伺服器的"伺服器"類別表的位置；並且能夠順著從"伺服器"表到針對服務之"服務"類別表中的一些表的諸多通信鏈路；進而能夠使用來自請求的埠號來尋找適當的"服務"表。一旦它已經發覺適當的"服務"表，它就能夠順著指向"資源"類別表1409中的一些表的諸多通信鏈路，並指出對應於請求中之資源的"資源"表的位置。從那裏，會有一條指向"資源群組單元"類別表1407的通信鏈路，該表使諸多資源與針對它們所屬之資訊集的一些資源群組識別符有關係。諸多資源群組識別符依序地載明"資源群組"類別表1403中的一些表，而這些表都有指向"資源群組樹"類別表中的一些表的諸多通信鏈路，因而能夠決定：載明在請求中之資源所屬的諸多資源群組的層次。已經完成那些事，存取過濾器203就已經發覺：與決定該請求是否應該被准許有關的一些資源群組。針對資源的"資源"表還包含針對資源之靈敏度等級。

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明(70)

再者，將資訊集表1401中的資訊加以編輯進入MMF中。當請求來到在使用者與提供資源的伺服器之間路徑中的第一存取過濾器203時，第一存取過濾器203就會使用MMF檔案，以便作出一項邏輯上等效於剛才所描述之一決定的決定。於是，在檢視包含來自使用者群組表1301和資訊集表1401之資訊的MMF檔案之後，代理伺服器就已經決定：使用者識別方法的信賴等級，資訊資源的靈敏度等級，使用者所屬的一些使用者群組，以及資訊資源所屬的一些資訊集。

決策表：圖16

3 決策表：圖16

圖16顯示：使用於存取控制資料庫301中，用來定義存取決策的一些表；包括在這些決策中的有：存取決策，管理決策，以及決策制定者決策：

- 存取決策使使用者群組與資源群組有關係；
- 管理決策使其成員都是管理員之一使用者群組與下列其中之一有關係：
 1. 另一使用者群組
 2. 一資訊集
 3. 一資源
 4. 在VPN中之一位置(網站)
 5. 一存取過濾器203或其它伺服器
 6. 一項服務
- 決策制定者決策使管理員之使用者群組與資訊集有關係。

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(71)

每項決策都會使"左側"與"右側"有關係，左側總是"使用者群組"類別表1309，而右側則端視決策種類而定，可能是："資源"類別表1409，"資源群組"類別表1403(表示資訊集)，"網站"類別表1415，"服務"類別表1413，"伺服器"類別表1417，或者"使用者群組"類別表1309。於是，決策諸表1601分成三大群組：左側諸表1603，決策諸表1605，以及右側諸表1609。改變決策的權利是分層性的：一使用者群組之成員能夠改變存取決策，就像由針對該群組之管理決策所決定的那樣，該群組之"使用者群組"表指示著：它是諸多管理員中之一類型的一種群組。依序地，那些管理員可能載明與他們的子網域(sub-domain)有關的其他管理決策。

對應於三種決策，在決策諸表1605中有三個類別表：屬於"存取決策"(Policies Access)類別表1611，"管理員決策"(Policies Administer)類別表1613，以及"決策制定者決策"(Policies Policy Maker)類別表1691的一些表。所有的這些類別表共享很多特點：它們都包含：針對決策之左側的使用者群組表之ID，針對表示載明在決策之右側中項目的表之ID，決策(存取操作被容許或被拒絕)的一種指示，決策是否預先定義的且無法被刪除的一種指示，以及決策是否為目前現用的一種指示。類別表之間的差異是：何者可能在決策之右側上，因而就是指向在右側上諸多實體的通信鏈路；在存取決策和決策制定者決策的情形下，右側實體都只是資訊集而已，因此，"存取決策"和"決策制定

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(72)

者決策"兩種類別表中的一些表都只包含指向"資源群組"類別表中的一些表的諸多右側通信鏈路而已；而"管理員決策"類別表中的一些表則可能包含指向下列替換性的："使用者群組"類別表，"資源群組"類別表，"網站"類別表，"伺服器"類別表，"服務"類別表，以及"資源"類別表中的一些表的諸多右側通信鏈路。

賦予由管理決策右側上的使用者群組所載明的使用者群組管轄由右側所載明的諸多實體之集合的權利會有所變化，端視實體種類而定，如下表中所顯示的：

左側	右側	"被容許"存取操作的意義
使用者 群組	任何一個	使用者群組的成員都能夠建立針對目標或已包括項目的管理決策。這樣會容許責任之委託權限。
使用者 群組	使用者群 組	使用者群組的成員都能夠管理目標使用者群組，包括一些套疊式(nested)使用者群組。被容許的管理，包括：將目標使用者群組加以刪除，移動，及拷貝；將它套疊在另一使用者群組中；增加成員給它；以及將其它一些使用者群組套疊在其中
使用者 群組	資訊集	使用者群組的成員都能夠管理資訊集，包括一些套疊式資訊集。被容許的管理，包括：將目標資訊集加以刪除，移動，及拷貝；將它套疊在另一資訊集中；增加成員給它；以及將其它一些資訊集套疊在其中。

五、發明說明(73)

使用者 群組	網站	使用者群組成員都能夠管理網站，包括：來自"可用資源"列表(所有的存取過濾器，伺服器，服務，以及資源)，在網站之下的一些單元。被容許的管理，包括：將網站加以刪除和移動；將它增加到資訊集；以及增加一些位置和存取過濾器給它。為了定義一些新的存取過濾器，管轄企業內部網路位置的管轄權是必需的。
使用者 群組	存取過濾器	使用者群組的成員都能管理存取過濾器，包括：來自"可用資源"列表(所有的伺服器，服務，以及資源)，在存取過濾器之下的一些單元。被容許的管理，包括：將存取過濾器加以刪除和移動；將它增加到資訊集；以及增加一些伺服器或服務給它。
使用者 群組	伺服器	使用者群組的成員都能夠管理伺服器，包括：來自"可用資源"列表(所有的服務和資源)，在伺服器之下的一些單元。被容許的管理，包括：將伺服器加以刪除和移動；將它增加到資訊集；以及增加一些伺服器或服務給它。
使用者 群組	服務	使用者群組的成員都能夠管理服務，包括：來自"可用資源"列表(所有的資源)，在服務之下的一些資源。被容許的管理，包括：將服務加以刪除，移動，及拷貝；將它增加到資訊集；以及增加一些資源給它。
使用者 群組	資源	使用者群組的成員都能夠管理資源。被容許的管理，包括：將資源加以刪除，移動，及拷貝；以及將它增加到資訊集。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (74)

下表描述：當管理使用者群組出現在決策制定者決策左側上時，賦予管理使用者群組的權利。

左側	右側	"被容許"存取操作的意義
使用者群組	資訊集	使用者群組的成員都能夠管理：用來控制由任何使用者群組包括一些套疊式資訊集在內的資訊集的諸多存取決策。他們也可能將資訊集和其後裔(descendants)中的任何資訊集包括在決策制定者決策中。

如上述資訊集表之討論中所指出的，正在執行存取核對的代理伺服器能夠使用"使用者群組"表和"資訊集"表來尋找：在正在提出存取請求之使用者所屬的使用者群組，以及正在被存取之資訊資源所屬的資訊集；並且也能夠使用這些表來決定：使用者識別方法的信賴等級，以及資訊資源靈敏度等級。代理伺服器隨即能夠使用"存取決策"表來尋找：使用者所屬的任何一個使用者群組是否可能存取資訊資源所屬的任何一個資訊集。若發覺任何一個這樣的使用者群組；則使用者可能存取資訊集，如果請求之信賴等級與資訊資源之靈敏度等級一樣高的話。要決定請求之信賴等級，代理伺服器就必須決定：正在被使用之任何加密技術的信賴等級，及/或正在被用於存取操作而在VPN 201中之路徑的信賴等級。這項資訊可在顯示於圖17中的存取過濾器諸表1701中加以獲得，並描述於下。若存取決策或存取請求之靈敏度等級不允許存取操作；則該訊息不予理會，因而將它所屬的任何對話加以棄置。當請求是由成

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明 (75)

為存取資料庫301之一管理使用者群組之一成員的使用者所提出的一項請求時，存取核對處理過程實質上是相同的；只可惜：當存取操作被允許時，根據以上所宣示的規則，它可能會導致修改資料庫。該項修改隨後將被傳播到VPN 201中之所有其它的存取過濾器203。

伺服器表：圖17

3 伺服器表：圖17

圖17顯示：針對對在VPN中的諸多伺服器之操作而言都是特別重要的一些表之圖表。在VPN中，有三種伺服器：

- 陽春伺服器(plain servers)。這些是：有資源儲存在其上並藉由執行服務來存取資源的伺服器。
- 存取過濾器203。
- 決策管理程式伺服器。這些是：會附帶地統合(coordinate)和分配資料庫301，及/或產生關於VPN的操作和狀態的一些報表的存取過濾器203。

存取過濾器203可能附帶地執行像一種陽春伺服器那樣的功能。

針對在VPN中的每一個伺服器都會有"伺服器"類別表1417。在針對每個伺服器之表中的資訊，包括：伺服器之ID，名稱，在Windows NT商標之作業系統中的網域，其網際網路名稱，它是否為一存取過濾器203且附帶地為一決策伺服器，存取資訊是否只有經由存取過濾器203才可以獲得，以及它是否在VPN之內。若伺服器為一存取過濾器203，它會附帶地具有一種存取過濾器203提供給在VPN

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(76)

201中之其它實體的身份識別(identity)，以供鑑定和加密之用。在一較佳實施例中，該身份識別是：由SKIP所使用之針對存取過濾器的X.509號證書。X.509號證書也包括：針對存取過濾器203的公用密鑰。公用密鑰可能屬於很多個名稱空間(name space)中的一個；名稱空間識別符(name space ID，簡稱NSID)是一種針對公用密鑰之名稱空間的識別符；而主密鑰識別符(master key ID，簡稱MKID)則是識別在名稱空間內的公用密鑰。也包括在表中的是：一條指向"證書當局"類別表1711的通信鏈路，該類別表會指示發行針對存取過濾器之X.509號證書的證書當局。當然，與存取過濾器不同的一些伺服器也都有X.509號證書；並且，在那種情形下，它們的"伺服器"表將會具有伺服器之NSID和MKID。

在VPN中的每一個陽春伺服器都會有一項或更多服務在其上執行。譬如說，一項FTP(檔案傳送協定)服務會根據TCP/IP成套協定(protocol suite)中的檔案傳送協定來存取在伺服器上的檔案(資源)。針對陽春伺服器的"伺服器"類別表1417中的每一種表都有：指向定義在伺服器上可供利用的服務和資源之一群表的諸多通信鏈路。如在1719處所顯示的，這些表包括："服務"類別表1413，它表示服務；"資源"類別表1409，它表示經由服務而供利用的資源；以及"服務定義"類別表1715，它會定義服務。

針對圖17諸表中的其餘部份則顯示：包含存取過濾器203所用之資訊的一些圖表。其類別表均顯示在1705處的

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(77)

一些表都會包含：都是一些用來分配資料庫301及/或用來產生報表的決策管理程式而由存取過濾器203所使用的資訊：其類別表均顯示在1717處的一些表都會包含：關於針對正在被一既定存取過濾器203執行之軟體的諸多可選擇參數的資訊；其類別表均顯示在1709處的那些表都會包含：關於代理伺服器及其它軟體模組的資訊，諸多存取過濾器203都會使用該模組來執行在存取過濾器203中的通信協定層級之存取核對；而在1707處的一些表則都會包含：關於針對使用者識別方法和加密種類的信賴和靈敏度定義的資訊。

由參考數字1708所指示的一些表都會包含：關於存取過濾器203所屬之VPN的資訊。存取過濾器203使用此資訊來路由指引對話；並且也會用來決定：針對一既定對話，正在被使用之路徑的信賴等級。"路由選擇表"(Routing table)類別表1721會定義：列示指向可從存取過濾器203存取資訊之所有網路的諸多目前路由的一些表。當那些路由改變時，該表就會被自動地更新。"附屬網路"(Attached Network)類別表1723會定義一些表，該表指示：對每個存取過濾器203而言，存取過濾器203目前所附屬的一些網路；該類別表中的一些表都會包含指向"網路定義"類別表1723中的一些表的諸多通信鏈路，該類別表依序地包含指向"信賴等級定義"(trust definitions)類別表1707中之一定義之一通信鏈路，而該類別表則會指示網路的信賴等級。在此群組中的最後類別表是"點對點連接"(Point to Point Connection)

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(78)

類別表1713，它會定義：描述可經由VPN存取資訊的兩個存取過濾器203之間連接的一些表。有針對來源和目標存取過濾器203的每種組合的一種表，以及指向一種載明在來源和目標兩個存取過濾器203之間路徑之信賴等級的信賴等級定義之一通信鏈路。在此表中的信賴等級是基於針對橫過路徑之訊息所使用的加密技術。

如前面所說明的，"使用者群組"表1301和"資訊集"表1401會提供存取過濾器203所需的資訊，以便決定：決策諸表1601中的存取決策是否允許存取操作；並且，也會提供：關於正在被存取之資源的靈敏度等級的資訊。存取過濾器諸表1701會附帶地提供存取過濾器203所需的資訊，以便決定：正在由對話所採取而在VPN中之路徑的最小信賴等級，以及一些可用加密演算法的信賴等級。於是，若存取過濾器203決定：正想要存取一既定資源之一既定使用者屬於有權存取該既定資源所屬的資訊集之一使用者群組，並且決定：用於使用者之識別方法的鑑定等級並不低於針對資源之靈敏度等級所需的鑑定等級；則存取過濾器203能夠進一步決定：路徑之信賴等級是否夠高；且若信賴等級不夠高，則存取過濾器203藉由選擇一種具有所需信賴等級的加密演算法並對該對話加以加密，就能夠將信賴等級提升為需要量。

可用資訊表：圖15

3可用資訊表：圖15

圖15顯示針對可用資訊諸表1501的圖表。該表皆由存取

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(79)

過濾器203所使用，以便產生可用資源顯示圖1005，如圖10中所示。在1502處所顯示的一些類別表都會使每個伺服器與它的服務有關係，並與由服務所提供的資源有關係。在1504處所顯示的一些類別表會將諸多可用資源加以組織成一種針對繼承權目的的層次；並且也會被使用來產生在1005處所顯示的分層列表；進而藉由順著從"網站單元"表到"伺服器"表的諸多通信鏈路，存取過濾器203就能夠決定：網站，伺服器，服務，以及資源的層次。在1503處的一些類別表，最後會建立一種存取過濾器203的分配樹(distribution tree)。就像稍後將要更加詳細說明的那樣，當存取控制資料庫301被修改時，由那些表所定義的樹就會決定：修改被分配到一些存取過濾器所依照的順序。

修改存取控制資料庫301：圖19

3 修改存取控制資料庫301：圖19

如前面所提及的，每個存取過濾器203都會有一種屬於在圖2之存取過濾器203(a)中之主決策管理程式205的存取控制資料庫301之拷貝的精確副本(exact duplicate)。圖19顯示：怎樣修改存取控制資料庫301的那份拷貝，以及怎樣將修改資訊從存取過濾器203(a)分配到其它存取過濾器203。圖19顯示：具有主決策管理程式205的存取過濾器203(a)；以及另一個存取過濾器203(i)，在該處，使用工作站之一管理員正在修改存取控制資料庫301。需要用來分配和同步修改資訊的訊息1909都是使用SKIP加以加密

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(80)

的，並且經由VPN 201，使用一種稱為"專用通信服務"(private communications service，簡稱PCS)的通信協定加以發送。每個存取過濾器都會有很多存取控制資料庫301的拷貝。任何存取過濾器203最少限度都有兩種拷貝：活資料庫(live database，簡稱LDB)1907，它是目前正在被用來執行存取核對的資料庫；以及鏡像資料庫(mirror database，簡稱MDB)1905，它是：能夠被切換入內，打算用來代替活資料庫1907的資料庫之一拷貝。於是，存取過濾器203(a)具有：一MDB 1905(a)和一LDB 1907(a)；而存取過濾器203(i)則具有：MDB 1905(i)和LDB 1907(i)。

若一存取過濾器203正在被管理員使用來修改存取控制資料庫301，則它將會附帶地具有至少一個工作資料庫(working database，簡稱WDB)1903。工作資料庫是：不是正在被用來控制存取操作的資料庫之一拷貝，因而能夠由管理員加以修改。管理員會使用一種經由網路而連接到存取過濾器之一工作站或PC(個人電腦)而這麼做。工作站或PC會顯示上述的管理圖形使用者界面，進而管理員使用GUI(圖形使用者界面)來做出像由一些管理決策所致能那樣的諸多改變。這些改變可能影響到儲存在存取控制資料庫301中的任何方面的資訊。如以上所指示的，其中諸多改變都是在存取或管理決策方面的改變，因而管理員能夠使用決策評估特點來察看改變之效應。當管理員對變化感到滿意時，他就會點按："應用"按鈕；因而將諸多改變分配到所有的存取過濾器，並納入每個存取過濾器的活資

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(81)

料庫中。

將更新所有活資料庫的處理過程稱為：資料庫同步和分配。該處理過程有三個階段：

- 首先，將修改資訊從產生它們之所在的存取過濾器203(此處，就是存取過濾器203(i))發送到主資料庫所屬的存取過濾器203(此處，就是存取過濾器203(a))。
- 在那種情況，將諸多改變納入主資料庫中。完成此事的方法是：將諸多改變納入鏡像資料庫1905(a)中，然後將活資料庫1907(a)和鏡像資料庫1905(a)交換(swapping)，然後再改變新鏡像資料庫1905(a)。
- 然後，將諸多改變從主決策管理程式分配到其它存取過濾器。

在每個存取過濾器203處，用與利用存取過濾器203(a)相同的方式來完成同步。在VPN 201之存取過濾器203中做出改變所依照的順序是由分配樹1511所決定，使用存取過濾器顯示圖1201依序地將它建立起來。具有主決策管理程式205的存取過濾器203總是樹的根部。依照預設方式(default)，安裝在VPN 201中的第一存取過濾器203具有主決策管理程式205。當安裝了其它存取過濾器203時，就會將它們增加到樹中，作為主決策管理程式的孩子們(children)。

主決策管理程式會將諸多改變循序地分配給它的孩子們。當每個子(child)存取過濾器203都收到它的分配資訊時，它隨後就再分配給它的孩子們。這意謂著：一種自頂

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(82)

層分叉出很多分支(branches)的淺型(shallow)分配樹完成一個分配周期將會比一種自頂層分叉出很少分支的深型(deep)分配樹還快。適當存取資訊的管理員能夠重新配置分配樹，以使分配更加有效。

若兩位管理員已經修改在不同的工作資料庫1903中的相同資訊段(譬如說，存取過濾器定義)，則會發生同步衝突。當此事發生時，主決策管理程式205就會決定：要將哪個修改資訊納入存取控制資料庫301中。

使存取控制資料庫301最佳化：圖21和23

3使存取控制資料庫301最佳化：圖21和23

雖然藉由管理圖形使用者界面(GUI)1915適合於持續儲存和使用；但是對於使用在即時存取核對中而言，資料庫301並不是最佳化的。就像將要更加詳細說明於下那樣，存取過濾器203會使資料庫301中的資料最佳化，那是運轉時間(run-time)存取核對所需的，進而用來產生針對IntraMap的顯示圖。每次在存取過濾器203中收到資料庫301之一新拷貝的時候，它都會執行最佳化(optimization)。依照它們的最佳化形式，資料庫301是諸多記憶體映射檔案(MMF)之一集合，其中以一種允許快速存取的形式來儲存存取決策資訊。之所以如此稱為MMF，是因為：雖然它們都被當作正常檔案來產生，但是隨後卻都附屬於一程式的記憶體空間，並且都是藉由一些記憶體操作，而不是檔案操作加以存取的。藉由使用MMF檔案來達成進一步最佳化，以便產生一些規則：藉由IP來源和目標位址以及針對

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(83)

存取操作被容許或拒絕的埠號，使用該規則來執行訊息之低層級過濾操作。

圖21顯示：MMF檔案2303之一實例。正被談論的MMF檔案是：DBCertificatesbyUserGroup(藉由使用者群組來識別的資料庫"證書")檔案2101，它將用來識別屬於諸多特定使用者群組的證書之證書匹配準則加以映射到：針對由證書匹配準則所載明的諸多使用者群組的記錄，在資料庫301中的一些識別符。於是，檔案2101允許具有會識別已經使用SKIP加以加密之一訊息之來源的證書之一代理伺服器快速決定：由證書加以識別之使用者所屬的諸多使用者群組。在較佳實施例中，證書匹配準則是：X.509號證書中的O(組織)，OU(組織單位)，及CA(證書當局)欄位。

所有的MMF檔案2303都有相同的通用形式，有兩個主要部份：標題部份2103，它包含正被映射所根據的資訊；以及資料部份2105，它包含正被映射所指向的資訊。標題2103包含諸多登載項(entries)2107之一列表。每個登載項都會包含：正被映射所根據之一數值(在這種情形下，就是證書匹配準則(CMC)2109)；以及指向在資料部份2105中之一記錄的指標(pointer)2111，它包含正被映射所指向的資訊(在這種情形下，就是：針對由CMC 2109加以識別之使用者所屬的諸多使用者群組，在資料庫301中的諸多識別符2113之一列表2115)。在標題2103中的諸多登載項都是依照正被映射所根據的資訊(此處，就是CMC 2109)加以排序的，使得：可能使用諸多標準快速搜尋演算法來指出

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(84)

對應於一既定證書匹配準則集合之一登載項2107的位置。

圖23A, B及C提供：被使用在存取過濾器203之一建構例中的諸多MMF檔案2301之一完整列表。根據表中所提供之諸檔案內容的描述，這些檔案與資料庫301中的一些表之間的關係將會顯而易見的。每個MMF檔案2303都是由表中之登載項所表示，該表指示檔案名稱及其內容。將諸多檔案細分成下列群組：2311, 2313, 2319, 2321, 2323, 以及2422。特別感興趣的一些檔案有：DBUsers(資料庫"使用者")檔案2307和DBResources(資料庫"資源")檔案2309，它們都描述決策；DBCertificatesByUserGroup(藉由使用者群組來識別的資料庫"證書")檔案2101，它是詳細顯示於圖21中的MMF檔案；DBResourceIDbyServiceID(藉由IP名稱來識別的資料庫"資源識別符")檔案2315，它會使資源的URL(共通資源指標)與資源ID(識別符)有關係；DBResourcesbyResourceID(藉由資源ID來識別的資料庫"資源")檔案2317，它會使資源與資源群組有關係；以及DBTrustTable(資料庫"信賴等級表")檔案2325，它會建構SEND表601。

而且，下列檔案都被用來編譯規則：

DBServerIDByNameFile(藉由IP名稱來識別的資料庫"伺服器ID"檔案)

DBIPAndTypeByServerIDFile(藉由伺服器ID來識別的資料庫"IP位址和類型")

DBServicePortToProxyPortFile(資料庫"服務埠對代理伺服

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (85)

器埠"檔案)

DBAttachedNetworksByServerIDFile(藉由伺服器ID來識別的資料庫"附屬網路"檔案)

DBRoutingTableFile(資料庫"路由選擇表"檔案)

DBRoutingTablebyServerIDFile(藉由伺服器ID來識別的資料庫"路由選擇表"檔案)

在IntraMap資訊2422中的諸多檔案，最後被過濾，以便產生列表2431，然後再利用IntraMap小爪哇程式2411將它下載到客戶端以供使用。

存取過濾器203之細節：圖20

3存取過濾器203之細節：圖20

圖20是一種存取過濾器203的架構2001之一方塊圖。在顯示於圖20中的建構例中，與一些NIC(網路界面卡)卡2013不同的所有存取過濾器203組件都是以軟體方式來建構的。建構例中的軟體會在微軟公司所製造的Windows NT商標之作業系統下執行。軟體組件分為兩大類：在作業系統之使用者層級2003處，當作應用程式執行的那些組件；以及在作業系統之核心層級(kernel level)2005處所執行的那些組件。就大體而論，在核心層級處所執行的程式會執行：IP層級存取核對，以及加密和鑑定；而在使用者層級處所執行的那些程式則會執行應用層級存取核對。也包括在使用者層級組件中的是：管理存取控制資料庫301的軟體，以及根據存取控制資料庫301而產生針對IP層級存取核對之諸MMF和規則的軟體。下列討論將從核心層級

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(86)

組件開始，繼續討論與存取控制資料庫301有關的使用者層級組件，然後將會討論針對通信協定層級存取核對的組件。

核心層級組件

3 核心層級組件

網路界面卡(Network Interface Card, 簡稱NIC)2013：這些是安裝在存取過濾器203中的乙太網路(ethernet)和令牌環卡(token ring card)。一般說來，配置(configured)有三種網路卡。一種是為：針對網際網路，針對一種廣域網路(wide area network, 簡稱WAN)2011，或者針對連接到另一存取過濾器203之一網路的界面而配置的。另一種是為針對所有客戶端電腦的界面2007而配置的；而第三種則是為針對提供TCP/IP服務之諸伺服器的界面2009而配置的。若不必要將一存取過濾器203置於諸多客戶機與伺服器之間，則可能只有兩種NIC 2013：一種針對WAN 2011，而另一種則針對LAN(區域網路)。若在存取過濾器203之位置處並沒有伺服器存在，或者，若所有的局部客戶機都有權存取所有的局部資訊資源是可接受的；則不必要將存取過濾器置於其間。

填隙軟體(SHIM)2017：在安裝時，將一種填隙(shim)軟體模組插入Windows NT商標之作業系統的兩個層級(NDIS和TDIS層級)之間。這樣會造成針對特定通信協定的所有通信量都會通過SHIM 2017。在建構例中，針對TCP/IP通信協定的所有通信量都會通過SHIM 2017，而非TCP/IP通

(請先閱讀背面之注意事項再填寫本頁)

袋

訂

線

五、發明說明(87)

信協定之通信量則從NIC直接前往一些適當的其它核心模組。SHIH 2017必要時會調用(invokel) SKIP模組來處理TCP/IP通信協定之通信量。

SKIP模組2021：經由SKIP 2021來發送所有的IP網路通信量。若輸入分包資訊不是SKIP類型，即：不需要由SKIP來執行鑑定和解密服務；則SKIP模組2021會將它傳遞到IP過濾器模組2019。同樣地，若不打算對輸出分包資訊加以加密，則SKIP模組2021會將它直接發送到適當的NIC 2013，以供傳輸之用。雖有SKIP類型之分包資訊，但在SKIP模組2021中的鑑定符(authenticator)2024可作為鑑定一項對話之用；而加密器/解密器2022則可作為對在一種對話層級處的資訊加以加密和解密之用。可能利用：任意數目的其它存取過濾器203，使用SKIP的一些伺服器，以及使用SKIP的一些客戶機來完成鑑定以及加密/解密。鑑定和加密演算法都是基於SEND參數，針對輸出分包資訊，由IP過濾器模組2019加以設定的；或者，都是在輸入分包資訊內加以載明的。

SKIP模組2021會為與它對談的每個其它網站維持足夠的狀態資訊，使得：對於大多數的SKIP類型之分包資訊而言，它能夠維持高速操作。分包資訊有時候會"被停留"(parked)，而附加處理(共享機密及暫時密鑰(temporary key)計算)則會被執行。在使用者空間2003中的"skipd"模組2037會執行這種額外處理。

IP過濾器2019：IP過濾器根據一套規則而操作，該規則

五、發明說明 (88)

是：資料庫服務2029之一組件的規則編譯程式，根據存取控制資料庫301中的存取決策加以制定的。IP過濾器的一些基本功能都是用來：

1. 將通信量傳遞到TCP/IP堆疊。
2. 阻擋通信量-將針對特定IP位址的通信量明確地棄置，並且是根據針對緊急情況的諸多特別規則。
3. 棄置通信量-將既不和任何規則匹配又不被任何決策所容許的通信量明確地棄置。
4. 代理處理通信量-不是將通信量遞送到被指示目標，而是將它路由指引到在目前機器上之一代理伺服器應用程式。
5. 執行網路位址轉換-將可能是非法的內部IP位址改變成合法的IP位址。
6. 一建立無法由規則嚴格地決定存取控制操作所針對的一項新對話，就會將決策遞給Pr_ipf(被討論於下)。一般說來，這是針對可能被決策或被前述之VPN鑿隧道操作特點所容許的對話。

IP過濾器2019基於下列資訊而執行這些功能：

由規則編譯程式所產生的規則；

來源和目標IP位址和埠號；

關於輸入分包資訊的加密，或者不加密；以及

關於輸出分包資訊的所需加密和鑑定。

與資料庫301有關的組件

3 與資料庫301有關的組件

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(89)

共享目錄(Shared Directory)2028：VPN 201使用什麼存取過濾器203都會保持駐留其中的單一存取控制資料庫301。在一既定存取過濾器203中之資料庫301的所有版本都被維持在共享目錄2028中。共享目錄2028也包含每個存取過濾器203的登錄檔案(log files)。

專用連接服務(Private Connect Service，簡稱PCS)模組2025：PCS模組2025提供在VPN 201中的"存取過濾器對存取過濾器"通信。所有這樣的通信都會通過PCS。PCS具有它自己的IP埠號，而其訊息則必須被加密。藉由PCS訊息來實行的一些特定功能有：

- 分配樹管理；
- 資料庫301之分配和同步；
- 路由選擇表1721之檢索和分配；
- Windows網域和使用者資訊之檢索；
- 網路掃描；
- 登錄內容之檢索；以及
- 由報表及其它子系統所使用之諸檔案的傳送。

ISDB管理程式2027：ISDB管理程式207會管理資料庫301。它和PCS都是唯一針對在每個存取過濾器203中的資料庫301之諸拷貝的界面。它包含用來讀寫在資料庫301之諸拷貝中之所有表的軟體。

資料庫(DB)服務和規則編譯程式2029：資料庫服務模組2029會產生諸多MMF檔案2301。每次在存取過濾器203中收到資料庫301之一新拷貝的時候，它都會這麼做。它利

(請先閱讀背面之注意事項再填寫本頁)

線
訂

五、發明說明 (90)

用由ISDB管理程式2027所提供的功能來讀取針對一既定存取過濾器203(I)的活資料庫1907(I)並產生諸多MMF 2301。資料庫服務模組2029之一組件是規則編譯程式，它會根據諸多MMF 2301中的一些有關MMF來產生使用在IP過濾器模組2019中的一些規則。該規則會載明存取操作被容許或拒絕所針對的：IP來源，目標，以及埠號。規則編譯程式存在，充當一種DLL以及一種只是調用DLL中之諸常式(routines)的應用程式。在正常操作中，每當在存取過濾器203(I)中，從主決策管理程式205中收到已修改資料庫301時，在DLL中之諸常式都是由資料庫服務模組2029加以調用的。在安裝和啟動程式(bootstrapping)處理過程期間，應用程式被使用在一些特別模式中。

記憶體映射檔案(MMF)2301：像已經說明的那樣，MMF 2301都是由資料庫服務模組2029所產生的資料檔案，並且都被存取過濾器203中的很多其它模組所利用。設計檔案以使下列操作儘可能有效的：

- 從使用者識別方法映射到(諸多)使用者群組；
- 從資訊資源映射到(諸多)資訊集；
- 尋找與諸多使用者群組有關聯的決策；以及
- 尋找與諸多資訊集有關聯的決策。

與鑑定有關的組件

3與鑑定有關的組件

評估程式(Evaluator)2036：評估程式2036是由諸多代理伺服器2031中的每個代理伺服器所使用的諸多DLL之一集

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明 (91)

合。評估程式2036會提供下列功能給諸多代理伺服器：

- 提示(Prompting)使用者另外的"在頻帶內"或"在頻帶外"識別資訊；
- 從鑑定工具程式服務(Authentication Tool Service，簡稱ATS)中獲得"在頻帶外"鑑定資訊；
- 從SKIPd中獲得與目前使用者有關聯的證書；
- 讀取諸多MMF 2301，並決定：存取決策是否允許使用者存取資源；以及
- 若在其它情況下存取操作被容許，則建構針對路徑之信賴/靈敏度等級計算，包括決定存取操作是否可能經由路徑而被容許，如果這樣；則需要何種加密和鑑定方法，以及哪個存取過濾器最接近伺服器。這些功能都是由稱為VPN管理程式的評估程式2036之一組件加以執行的。

鑑定工具程式服務/使用者識別客戶軟體(ATS/UIC)2039和2041：ATS 2039是在一種會搜集和鑑定使用者資訊的客戶機一伺服器應用程式中的伺服器。ATS 2039會在電腦上執行，而在其上則有存取過濾器203之其它組件正在執行。客戶機部份是UIC 2041，它會在基於Windows之客戶機上執行。ATS 2039和UIC 2041都是機制，存取過濾器203會藉由該機制來獲得"在頻帶外"鑑定資訊。ATS 2039和UIC 2041會藉由一項與正在被鑑定之對話分離的對話而通信。ATS 2039會收集並快速存取(caches)它從諸多UIC客戶機中獲得的鑑定資訊，進而提供該資訊給評估程式

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (92)

2046。來自諸客戶機的被快速存取資訊包括：

- Windows ID；
- 身份識別證書；以及
- 鑑定令牌ID。

SKIPd 2037：

大多數的 SKIP'd 功能都是支援 SKIP 模組 2021。那些功能包括：

- 與其它通信夥伴們交換證書資訊。藉由使用證書發現通信協定(CDP)來完成此事。
- 計算狄菲-黑爾曼(Diffie-Hellman)共享機密方法。這種共享機密方法是 SKIP 操作的關鍵。這種計算可能花上一段可觀的時間，並且以一種加密形式將它儲存到磁碟。
- 計算用來加密對話的傳送密鑰。這些密鑰會延續一段時間或資料量。
- 此外，SKIPd 將會提供證書匹配準則給(諸多)評估程式，以便使用在使用者識別方法中。

代理伺服器 2031

3代理伺服器 2031

如前面所說明的，代理伺服器是：在截取針對特定通信協定之通信量的存取過濾器 203 中的軟體。代理伺服器"瞭解"通信協定的是：它正在載取資訊，因而能夠獲得用來識別正在被存取的資源及/或從對話期間正在被交換的訊息中加以鑑定使用者所需的資訊。隨著 IP 過濾器將一些使

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明(93)

用一既定通信協定的訊息從其標準埠重新指引到其非標準埠，除SMTP外的所有代理伺服器都會接收：針對它們的通信協定，在與標準埠不同的一些埠上的訊息。代理伺服器提供它已經從對話中獲得的資訊給評估程式2036，以便決定：使用者是否有權存取資訊資源。若使用者有權存取，則存取過濾器203會將輸入訊息轉遞到它們被定址到的伺服器，並且藉由針對該通信協定的服務，在伺服器中將訊息進一步處理。在下列描述中，使用在一較佳實施例中的每個通信協定都會被討論；當然，其它實施例則可能包括針對其它通信協定的代理伺服器。

Pr_ipf(IP過濾器代理伺服器)：大多數的網路通信量會在少數通信協定上發生，而在存取過濾器203中則會有針對該協定的諸多代理伺服器。然而，甚至在沒有代理伺服器的地方，也必須制定一項存取決策。在某些情形下，可能在核心層級處由IP過濾器2019來制定決策；當它不會制定決策時，IP過濾器2019就提供通信量給Pr_ipf，它會獲得任何它能夠從通信量中獲得與使用者識別方法和資訊資源有關的資訊，進而將該資訊傳遞到評估程式2036，以便決定存取操作是否應該被准許。Pr_ipf事實上並不是一種代理伺服器，由於它只是做出一項針對IP過濾器2019的存取決定而已，故而不會將任何通信量傳遞到標準通信協定軟體。

FTP(檔案傳送協定)：FTP代理伺服器會處理針對檔案傳送協定的TCP/IP分包資訊。在VPN 201之一當前實施例

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(94)

中，只是將存取控制施行到帳戶(登錄)層級；而在其它實施例中，則可能將存取操作控制到檔案存取層級。在通信協定之FTP登錄部份期間，代理伺服器會決定正在被存取的伺服器及帳戶(account)，並且將此資訊提供給評估程式2036，以便決定：使用者是否屬於一使用者群組，該群組的諸多成員可能存取對應於該帳戶的資訊集。代理伺服器使用載明於FTP通信協定中與使用者互相作用的令牌來進一步處理"在頻帶內"鑑定資訊。

FTP實際上是一種非常複雜的通信協定，涉及主動(active)和被動(passive)模式(被使用在網路瀏覽器及某些自動FTP客戶軟體中)。此外，FTP資料傳送是利用一種第二動態決定式TCP(傳輸控制通信協定)對話。這就需要一種FTP代理伺服器與IP過濾器2019之間的特殊界面，使得FTP代理伺服器能夠對IP過濾器2019指示：它應該會容許第二對話。

HTTP(超本文傳送協定)：對於HTTP之公用網域CERN(歐洲粒子物理研究所)建構例而言，HTTP代理伺服器是根據來源碼(source code)而構築的，並且包含所有它的快速存取邏輯(caching logic)。代理伺服器使用評估程式2036來核對指向一URL的每項存取操作。沒有"在頻帶內"鑑定資訊是利用HTTP執行的。

Telnet(遠距通信網路)：Telnet資源由於Telnet註冊的非標準化性質而只被控制到伺服器層級。只是了提供附加的"在頻帶內"鑑定資訊才會使用Telnet代理伺服器。它是諸

五、發明說明(95)

多真實代理伺服器中最簡單的。

NNTP：網路新聞傳送協定(Network News Transfer Protocol，簡稱NNTP)被使用來控制新聞傳送(news feed)和新聞讀取兩種操作。在新聞傳送操作期間，NNTP代理伺服器注視著未編碼訊息。這些訊息都是已經被轉換成美國資訊交換標準碼本文(ASCII text)以供傳輸之用的二進制訊息(binary messages)。這種訊息常被解散成為多重部份(multi-part)訊息，以便將它們保持達到一種合理的尺寸。NNTP代理伺服器會快速存取二進制訊息的所有部份。就每個這樣的訊息而言，若該訊息是將要完成一項多重部份訊息的最後部份，則將整個多重部份訊息加以組合，進而抗病毒(anti-virus)模組2033會針對諸多病毒加以核對該訊息，就像更加詳細描述於下的那樣。在新聞讀取操作期間，將存取操作保護到新聞群組層級。就像在其它代理伺服器中那樣，評估程式2036被使用來決定：目前使用者是否可能存取新聞群組。

真實聲頻通信(Real Audio)：真實聲頻通信代理伺服器容許客戶機存取只有在伺服器層級處才受到保護的真實聲頻通信伺服器。真實聲頻通信協定雖然利用一種標準TCP套接通信連接(socket connection)來建立一項對話，但是隨後就使用一種轉回UP頻道。就像對於FTP那樣，真實聲頻通信代理伺服器具有一種針對IP過濾器2019的界面，該界面允許它對IP過濾器2019指示：轉回UP頻道是被容許的。

SMTP：簡單郵件傳送協定(Simple Mail Transfer Protocol，

(請先閱讀背面之注意事項再填寫本頁)

線

五、發明說明(96)

簡稱SMTP)代理伺服器與其它代理伺服器不同處在於：IP過濾器之代理伺服器的諸多規則都不是被使用來重新指引通信量到SMTP代理伺服器。其實其它代理伺服器會在一個非標準埠上"傾聽"；而SMTP代理伺服器則會在標準埠(25)上傾聽，隨後會執行它自己與標準SMTP伺服器軟體的通信連接。在資料庫301中的存取決策必須明確地容許此存取操作。

IntraMap：當使用者載明針對IntraMap之URL時，報表管理程式209會下載IntraMap小爪哇程式，而被下載之小爪哇程式則嘗試執行一種接回到具有報表管理程式209的存取過濾器203之一套接口(socket)的通信連接。局部存取過濾器203(I)的IP過濾器2019會截取嘗試執行通信連接資訊，進而將它提供給局部存取過濾器103(I)上的IntraMap代理伺服器。藉由尋找在資料庫301之局部拷貝中的回答(answers)並將回答轉回給小爪哇程式，代理伺服器會對來自小爪哇程式的查詢(query)作回應。隨著所有的回答正在被過濾而反映使用者之存取權利。IntraMap代理伺服器並非一種真實代理伺服器是因為：整個通信連接總是由截取通信連接之IntraMap代理伺服器的實例加以完全服務的。

抗病毒模組2033

3 抗病毒模組2033

在一較佳實施例中的抗病毒模組2033是由位於美國加州古柏提諾市(Cupertino, CA.)的趨勢微裝置公司(Trend Micro Devices, Inc.)所提供的諸多DLL之一集合。在其它實

(請先閱讀背面之注意事項再填寫本頁)

袋

訂

線

五、發明說明(97)

施例中，可能使用來自其它來源的抗病毒模組。抗病毒模組2033會針對病毒加以檢查所有進入VPN 201的資料。爲了提供使用者關於資料轉移進行的回授功能(feedback)並預防使用者之客戶軟體程式時間暫停(timing out)，將資料轉移到客戶機並在同時間內加以拷貝進入一種用於病毒檢查的暫時檔案中。然而，並未將資料的最後部份發送到客戶機，直到完成病毒檢查後爲止。該最後部份一處在暫時檔案中就會針對諸多病毒加以檢查暫時檔案。若未偵測出病毒，則將資料的其餘部份發送到客戶機。若發覺病毒，則中止資料轉移。在本實施例中，使用者被通知傳輸失效。若管理員已經這樣載明，則可能將一種警戒資訊發送到管理員。

啓動(launck)，登錄，警戒以及報表模組2027：

此模組的一些組件會執行下列功能

- 啓動-控制起動(startup)工作之初始順序；當建立VPN 201時，該初始順序就會在一存取過濾器203上發生。
- 登錄-一種提供已標準化登錄界面的DLL。
- 警戒-一種注視著所有NT登錄的獨立(standalone)程式，因而找尋載明於資料庫301的警戒條件。使用GUI來載明遞送警戒資訊所利用的方法，以供定義警戒資訊之用。
- 報表-將諸多登錄之一子集合轉遞到一種特別報表登錄，加以濃縮成資料庫，稍後再轉遞到報表管理程式209。

五、發明說明(98)

管理圖形使用者界面1915：

GUI(圖形使用者界面)可能在存取過濾器203上，或者在附屬於存取過濾器203而具有一種32位元Windows商標之作業系統的任何電腦上執行。GUI不論是在存取過濾器203上還是在附屬系統上執行，它都會利用ISDB管理程式2027來讀出或寫入在存取控制資料庫301中之一工作資料庫1903。經由GUI 1915，對存取控制資料庫301做出所有的必要修改。在GUI中之一"應用"操作，被當作一種信號發送到PCS 2025，它會藉由起動前述的分配和同步操作來對信號作回應。

存取過濾器203之操作的詳細實例：圖5和22

3存取過濾器203之操作的詳細實例：圖5和22

在下列描述中，將要詳細說明圖5之端對端加密實例。在該實例中，其PC配備有SKIP之一漫遊者503正在存取：在VPN 201上之一網站之內，一種配備有SKIP的伺服器407。當漫遊者503被建立來存取VPN 201時，它是經由使用一種特別加密類型的存取過濾器403(3)而被這樣建立的。此處，將會假定：正在被漫遊者503所使用的加密類型具有"機密"之信賴等級；並且假定：使用者想要存取在伺服器407上之網頁，該網頁具有"機密"之靈敏度等級。由於正在被存取的是網頁，故而漫遊者503正在使用針對它與伺服器407上之HTTP服務之對話的HTTP通信協定。由於漫遊者503，在VPN 201中的諸多存取過濾器203，以及伺服器407全部配備有SKIP；故而它們全部備有它們自己

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (99)

的公用和專用密鑰。最小限度下，漫遊者503也具有針對存取過濾器403(3)的證書和公用密鑰，它會將針對VPN 201內部之諸伺服器之訊息指引到存取過濾器403(3)；存取過濾器403(3)具有針對漫遊者503的證書和公用密鑰(或者使用證書發現通信協定來獲得它們)；在VPN 201中的所有存取過濾器203具有或能夠得到：彼此的公用密鑰，以及針對在VPN 201中配備有SKIP的諸多伺服器之公用密鑰。此外，在VPN 201中的每個存取過濾器203都會知道：在VPN 201中的所有其它的存取過濾器203及諸多伺服器之IP位址。

被當作漫遊者503與伺服器407之間的HTTP對話之一部份加以發送和接收的所有訊息都是由SKIP加以加密和鑑定的。圖22顯示：由這樣一種SKIP訊息2201所採用的格式。SKIP訊息是由SKIP軟體加以製作在就是SKIP訊息之來源的系統上。此處所顯示的SKIP訊息2201是來自漫遊者503。它的主要組成部份是：

外IP標題2203：外IP標題2203被使用來將SKIP訊息遞送到存取過濾器403(3)。包含在IP標題2203中的有：針對漫遊者503之來源IP位址2209，以及針對存取過濾器403(3)之目標IP位址2206。當漫遊者503被建立來存取VPN 201時，由漫遊者503所使用的目標位址2206就被設立來載明存取過濾器403(3)。來源IP位址2209可能由網際網路服務提供者(Internet service provider)以動態方式指定給漫遊者503；而漫遊者503則加以使用，以便連接到網際網路

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明(100)

121。外IP標題2203還包含一個訊息類別(message type, 簡稱MT)欄位2208, 它會載明: 訊息是一種SKIP訊息。

SKIP標題2205: SKIP標題2205包含當收到SKIP訊息時就用來解密SKIP訊息2201所需的資訊。SKIP標題2205至少包含: 針對目標之證書, 那就是, 針對存取過濾器403(3)之證書的目標NSID(名稱空間識別符)2215和目標MKID(主密鑰識別符)2213; 以及針對來源之證書, 那就是, 針對漫遊者503之證書的來源NSID 2219和來源MKID 2217。此外, SKIP標題2205包含: 針對用來鑑定訊息之演算法(MAC ALG 2226)和用來加密訊息之演算法(CRYPT ALG 2225)的識別符; 以及用來解密訊息的一種已加密傳送密鑰(Kp 2223)和針對用來解密傳送密鑰之演算法的識別符2224。

鑑定標題2211: 鑑定標題2211包含一種訊息鑑定碼(message authentication code, 簡稱MAC)2221, 它是根據在欄位2226中所識別的MAC演算法加以計算出的; 並且它被存取過濾器403(3)使用, 以便驗證: 訊息在沒有干預下抵達。

已加密有效負載(payload)2227: 已加密有效負載2227包含漫遊者503正在發送到伺服器407的已知加密訊息, 它包括: 針對該訊息的IP標題2331, 以及已加密訊息2229。IP標題2331具有: 針對伺服器407的IP位址, 以及針對HTTP通信協定服務的埠號。藉著使用具有由CRYPT ALG(加密演算法識別符)2225所載明之解密演算法的傳送密鑰Kp

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明 (101)

2223，就能夠對已加密有效負載2227加以解密。

處理SKIP訊息2201

3處理SKIP訊息2201

SKIP訊息2201抵達在存取過濾器403(3)的網際網路界面2011上。訊息之處理始於核心層級2005中的SHIM層級處。SHIM 2017會將所有輸入通信量發送到SKIP 2021，它依序地根據MT欄位2208而察覺到：該訊息是一種SKIP訊息。要解密並鑑定訊息，SKIP需要解密傳送密鑰Kp 2223，並且要做的是：它會將SNSID 2219，SMKID 2217，DNSID 2215，以及DMKID 2213提供給SKIPd 2037，SKIPd會用這些ID，以便從SKIPd 2037之證書快速存取儲存器(cache)中檢索針對漫遊者503和存取過濾器403(3)的證書。若證書不在那裏，則SKIPd 2037使用CDP通信協定來提取證書。然後，將證書中的資訊和存取過濾器403(3)之專用密鑰一起使用；以便產生一種共享機密數值，然後使用該數值來解密傳送密鑰Kp 2223，進而產生兩個內部密鑰：Akp和Ekp。SKIP會安全地儲存共享機密數值，以便和未來訊息一起使用，此乃因為該數值之計算要花費可觀的時間量。其次，為整個已收到訊息計算出MAC，並且將Akp和MAC 2221及MAC ALG 2226一起使用，以便驗證：整個SKIP訊息2201未曾被干預。如果就是這種情形，就使用內部密鑰Ekp來解密已加密有效負載2227，以便恢復來自漫遊者503的原始訊息。然後將已解密有效負載2227提供給IP過濾器2019，它會將它的一些規則應用到：來源

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (102)

IP位址，目標IP位址，以及IP標題2231的埠號。若沒有規則拒絕存取操作；則IP過濾器2019遵從另一規則，並將未加密訊息連同SNSID 2219和SMKID 2217重新指引到針對HTTP代理伺服器之埠。IP過濾器2019使用MMF 2301中的DBServicePortToProxyPort檔案來尋找正被談論之埠。

在作業系統之使用者層級2003中的應用層級處繼續訊息之處理。HTTP代理伺服器能掌握的有：伺服器之IP位址，服務之埠號，針對網頁之URL，屬於漫遊者503的使用者之證書，以及用來加密訊息的加密方法。它會使用評估程式2036，以便根據MMF 2301來決定下列各項：

- 由證書所表示之使用者所屬的諸多使用者群組；
- 網頁所屬的諸多資訊集；
- 是否有一項存取決策會允許諸多使用者群組中的至少一個使用者群組存取諸多資訊集中的至少一個資訊集；以及
- 訊息之信賴等級是否至少等於網頁之靈敏度等級。

就從這些工作中的第一項工作開始，評估程式2036會接收針對證書的NSID和MKID，並且使用來具有DBCertificatesByUserGroup檔案之證書的證書匹配準則來獲得：正在發送訊息之使用者所屬的諸多使用者群組之識別符。

評估程式2036藉由採由：伺服器之IP位址，服務之埠號，以及針對網頁之URL來決定資訊集；並且使用：具有DBServerIDByIP(藉由IP位址來識別的資料庫"伺服器ID")

(請先閱讀背面之注意事項再填寫本頁)

袋

訂

線

五、發明說明 (103)

檔案之 IP 位址來決定包含網頁之伺服器，具有 DBServiceIDByPort(藉由埠號來識別的資料庫"服務ID")檔案之埠號來決定關於提供服務之伺服器的服務，以及具有 DBResourceIDByName(藉由 IP 名稱來識別的資料庫"資源ID")檔案之 URL 來得到針對網頁所屬之資訊集的識別符。

隨著能掌握：針對使用者群組和資訊集，在資料庫 301 中的識別符：評估程式 2036 使用 DBResources 檔案來決定：是否有一項存取決策會允許使用者所屬的任何使用者群組存取網頁所屬的任何資訊集。這樣做，它可能只會考慮一些其成員資格都是使用識別模式加以決定的使用者群組，而該識別模式的信賴等級對資源之靈敏度等級而言是足夠的。DBResources 檔案會將每個資訊集識別符映射到：會有一些涉及該資源集的存取決策所針對的諸多使用者群組之一列表。對於每個使用者群組而言，DBResources 檔案會進一步指示：決策是否容許或拒絕存取操作。評估程式 2036 使用 DBResources 檔案，依序地為網頁所屬的每個資訊集而決定：會有一些關於資訊集的存取決策所針對的諸多使用者群組之列表是否包括使用者所屬的諸多使用者群組中的一個使用者群組。若有一項針對任何使用者群組的存取決策拒絕存取操作，則評估程式對 HTTP 代理伺服器指示：存取操作被拒絕；若沒有針對任何使用者群組的存取決策拒絕存取操作且至少有一項決策容許存取操作，則評估程式對 HTTP 代理伺服器指示：存取操作被容許；若沒有針對任何使用者群組的任何種類之存取決策，

(請先閱讀背面之注意事項再填寫本頁)

訂線

五、發明說明 (104)

則評估程式會決定：是否至少會有一個基於證書或令牌之使用者群組具有一項針對資源的容許決策。如果這樣，並且請求客戶機有UIC(使用者識別客戶軟體)正在執行；則聯繫UIC來對使用者要求附加身份證別資訊。若有附加身份識別資訊回來，則重複上述處理過程。在其它情況，評估程式對HTTP代理伺服器指示：存取操作被拒絕。

當然，若存取請求並不具有一種等於網頁之靈敏度等級的信賴等級，則評估程式2036也會拒絕存取操作。評估程式2036從DBResourcesByResourceID檔案中獲得網頁之靈敏度等級，從DBTrustAuthentications(資料庫"信賴等級鑑定")檔案中獲得使用者識別方法之信賴等級，以及從DBTrustEncryptions(資料庫"信賴等級加密")檔案中獲得加密方法之信賴等級。由於SKIP已經利用一種具有"機密"之信賴等級的方法來加密訊息，故而經由網路之路徑的信賴等級與本實例無關。要決定：針對使用者識別和加密方法的信賴等級是否對網頁之靈敏度等級而言是足夠的；評估程式2036就會使用有效地建構SEND表601的DBTrustTable檔案。若信賴等級是足夠的，則評估程式2036對代理伺服器指示：存取操作被容許。

一旦代理伺服器已經確認：打算容許存取載明於訊息中的資訊資源；代理伺服器就會發起一項新對話，針對實際服務：關於伺服器407之HTTP服務。代理伺服器2031會將一項特別訊息發送到IP過濾器2019，因而告訴它：容許特定對話通過；此乃因為：在其它情況，此對話可能會被一

(請先閱讀背面之注意事項再填寫本頁)

第

訂

線

五、發明說明 (105)

些規則所阻擋，或者再度被發送到代理伺服器。針對IP過濾器2019的訊息也包括關於新對話所需的加密方法之資訊，在本實例中，該資訊是：針對最後存取過濾器403(5)，應該對該對話加以加密；並且應該使用適合於資料靈敏度等級就是機密的加密方法。當IP過濾器2019遭遇新對話時，它會發覺到：因為該對話與代理伺服器2031所載明的準則匹配，所以它會將該對話傳遞到SKIP模組。由於就此對話而言加密是必要的，故而訊息將會被重新加密。除了下列各項之外，SKIP模組2021會以如上所述的相同方式來產生一種SKIP訊息2201：

- 針對訊息的外IP標題2203載明：將存取過濾器403(3)當作訊息之來源，而將存取過濾器403(5)當作訊息之目標；
- SKIP標題2205具有：針對存取過濾器403(3)的SNSID 2219和SMKID 2217；以及針對存取過濾器403(5)的DNSID 2215和DMKID 2213；並且，在標題2205中的其它數值也都是：由訊息之來源和目標現在就是存取過濾器403(3)和存取過濾器403(5)之事實所需的那些數值；
- 已加密有效負載2227與以前相同(除了使用一種不同的密鑰而已經將它加密之外；並且必要時為整個新訊息2201而產生MAC 2221。

當代理伺服器正在轉發(relaying)訊息時，它也正在注視著可能包含病毒的檔案傳送類型。當它遭遇病毒時，它會將抗病毒軟體2033應用到這些檔案。若檔案包含病毒，則

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (106)

代理伺服器未能遞送完整檔案，藉以使病毒不致於造成傷害。若存取控制資料庫301這樣指示，則當抗病毒軟體2033檢測出病毒時，代理伺服器就會發送一項警戒資訊。

當SKIP訊息2201在存取過濾器403(5)處被接收時，就將它傳遞到SKIP模組2021，在該處，如前面所描述的，將它鑑定和解密。關於存取過濾器403(3)，藉由如上所述的相同機制，在存取過濾器403(5)上的IP過濾器2019察覺到：因為訊息是指定給HTTP應用通信協定的，所以它會將訊息指引到HTTP代理伺服器2031。該代理伺服器會接受訊息；然後將來自外IP標題2203和SKIP標題2205，它能夠獲得關於訊息之發起者(存取過濾器403(3))的資訊發送到評估程式2036，以便決定：正在被此訊息鼓動的對話是否應該被容許繼續進行。評估程式2036會檢視訊息之來源IP位址以及其它身份識別資訊；並且藉由查出在MMF檔案之DBServerIDByIP檔案中的來源IP位址來決定：針對存取過濾器403(3)，在資料庫301中的識別符；使用該識別符來指出存取過濾器403(3)之證書的位置；以及發覺到：證書資訊與被檢索證書匹配，該被檢索證書與正在被處理的存取過濾器403(3)之訊息有關聯。訊息之來源的存取過濾器403(3)因此而被認為在VPN 201中之一存取過濾器403，所以評估程式2036作出回應是：該對話應該被容許，理由是它是一種已經被在相同VPN 201內之另一存取過濾器403所允許的訊息。將容許訊息的這項決策轉回給HTTP代理伺服器2031。評估程式2036會指導在存取過濾器403(5)上

(請先閱讀背面之注意事項再填寫本頁)

訂
線

五、發明說明 (107)

的HTTP代理伺服器2031：爲了相同的理由，容許從相同對話傳來的任何請求。當HTTP請求被處理時，代理伺服器就用與輸出對話被建立在存取過濾器403(3)上相同的方式來建立一種與在伺服器407上之HTTP服務的輸出通信連接。

當初啓與伺服器407的通信連接時，評估程式2036會查出在MMF檔案之DBServerIDByIP檔案中的伺服器407之IP位址，以便決定：針對伺服器407，在資料庫301中的識別符；使用該識別符來指出伺服器表的位置；進而使用來自該表之證書識別和DBCertificates(資料庫"證書")檔案來尋找針對伺服器407之證書。然後它使用針對存取過濾器403(3)的密鑰以及針對伺服器407的公用密鑰(從證書中獲得)來構築一項SKIP對話，如前面所描述的。將實際訊息加以加密和鑑定，增加SKIP標題2205，並且增加外IP標題2203，因而將訊息指引到伺服器407。

當訊息觸及伺服器407時，在伺服器407中的SKIP就會：核對關於訊息的鑑定資訊，對它解密，進而將已解密訊息轉遞到HTTP服務；該服務會執行存取：由包含於有效負載中之訊息所請求的網頁。已經獲得網頁，HTTP服務會產生一種具有載明將漫遊者503當作目標之IP標題的轉回訊息(return message)。然後，將此轉回訊息加以封裝在一種SKIP訊息2201中，如前面所描述的。此SKIP訊息被指引到存取過濾器403(5)，並且包含在外標題2203和SKIP標題2205中的資訊，該資訊對那些實體之間的訊息而言是必

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (108)

要的。

當回答(reply)訊息觸及存取過濾器403(5)時，在那裏的SKIP模組2021就會對它加以鑑定和解密，並傳送到IP過濾器2019。該訊息被發覺與一現存對話匹配，所以不必要評估；因而將它直接轉遞到HTTP代理伺服器2031。在那裏，將它當作一種HTTP通信協定回答訊息加以核對有效性，進而將它重新傳送回到就是存取過濾器403(3)之HTTP對話的發起者。由於瞭解此對話的發起者可能是在VPN 201中的另一存取過濾器403，故而不會執行抗病毒模組2033的核對操作，就像瞭解必要時存取過濾器會執行核對操作那樣。使用對存取過濾器403(3)與存取過濾器403(5)之間的訊息交換而言是必要的諸多SKIP參數，經由SKIP模組2021，再度處理回答訊息之重新傳輸，並且對它加以加密，如上述。

當此回答訊息來到存取過濾器403(3)時，恰好發生相同的事情，那就是，訊息通過SKIP模組2021和IP過濾器2019，來到HTTP代理伺服器2031。在那裏，將它當作一種HTTP通信協定回答訊息加以核對有效性；可能通過抗病毒模組2033(如果訊息內容類型對它保證的話)；進而將它重新傳送回到就是漫遊者503之HTTP對話的發起者。對於正在將一項訊息從存取過濾器403(3)發送到漫遊者503而言，使用如上所宣示的SKIP參數，經由SKIP模組2021，再度處理回答訊息之傳輸，進而如上述般對它加以加密。然後，在漫遊者503處接收回答訊息；在該處：利用SKIP

(請先閱讀背面之注意事項再填寫本頁)

袋

訂

線

五、發明說明 (109)

對該訊息鑑定和解密，提供訊息給使用者之瀏覽器，並且為使用者而顯示出來。

使用在存取過濾器203中的諸多技術之通則

使用在存取過濾器203中的諸多技術已經用兩種方式加以通用化：

- 將決策評估和決策施行分離，它會允許與存取過濾器不同的實體加以施行決策；以及
- 決策資料庫現在不但允許定義：使用者，使用者群組，資源，以及資源群組；而且允許定義：諸多新使用者識別類型，可能定義決策所針對的諸多新行動類型，以及諸多新資源類型。

下列討論將首先描述：可能怎樣將決策評估和決策施行分離，然後再描述：可能怎樣擴充用來定義決策的諸多類型。

將決策評估和決策施行分離：圖20，26，及27

圖26是一種決策施行系統2601之一方塊圖，其中：已經將決策評估和決策施行分離。在系統2601中，決策的觀念(notion)已經加以通用化，不但包括：存取決策，管理決策，以及決策制定決策；而且包括：使用者可能對一資訊資源執行的任何行動。譬如說，一項決策可能陳述：一特定使用者群組可能印出屬於一特定資訊集的一些文件。

系統2601具有五個主要組件：

- 請求實體2603，它會請求要對資訊資源執行的行動，並且它可能是能夠屬於一使用者群組的任何實體；

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (110)

- 決策施行器2609，它能夠控制被請求行動的效能；
- 諸多資源2611(0,...,n)，它可能是：可由決策施行器2609存取的或裝置控制的任何資訊；
- 決策伺服器2617，它會決定：行動是否被允許；以及
- 決策資料庫2619，它包含諸多決策，決策伺服器2617根據該決策來決定：行動是否被允許。

請求實體2603，決策施行器2609，以及決策伺服器2617能夠各自被定位在任何地方。唯一的要求是：在請求實體2603與決策施行器2609之間以及在決策施行器2609與決策伺服器2617之間都會有訊息傳輸媒體。在請求實體2603與決策施行器2609之間的媒體允許請求實體2603：將一種請求要對一資源R2611(i)執行一項行動的訊息2605發送到決策施行器2619；並且接收一種來自決策施行器2609的行動回應訊息2607，它指示著：是否要採取行動，以及如果這樣的結果。在決策施行器2609與決策伺服器2617之間的媒體允許決策施行器2609：將一項決策請求2613，發送到決策伺服器2617，因而請求決策伺服器2617指示：在決策伺服器資料庫2619中的諸多決策是否允許一既定請求實體採取相對於一既定資源之一既定行動；並且請求決策伺服器2617用一種決策回應2615來對決策請求2613作回應，該回應指示：諸多決策是否會允許載明於決策請求中的行動。應該進一步注意的是：受決策施行器2609控制的行動甚至不需要被電腦系統之一組件所執行。例如，在決策資料庫中的諸多決策可能被圖書館主顧們加以控制存取書本，而

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (111)

載明於決策中的行動則可能是具有一種從書架中提取一本書的圖書館網頁。

決策請求訊息2613以及決策回應訊息2615的格式都是藉由一種決策通信協定加以定義的。目前正在被研發的一些標準決策通信協定之實例是：公用開放決策系統(Common Open Policy System, 簡稱COPS), 該系統可上網獲知：就像1999年6月21日所描述的, 網址為：<http://www.ietf.org/internet-drafts/draft-ietf-rap-cops-06.txt>；以及在使用者服務中的遠程鑑定撥號(Remote Authentication Dial In User Service, 簡稱RADIUS；參考：網際網路標準第RFC2138號)。

決策伺服器2617獲得產生決策回應2615所需的資訊, 然後提供回應給決策施行器2609。決策伺服器2617包括一種包含諸多決策的決策伺服器資料庫2619, 該決策包括：針對請求實體2603已經請求決策施行器2609要對一項資源R2611(i)執行行動的一項或更多決策。決策伺服器2617會查詢決策伺服器資料庫2619, 以便指出一些有關決策的位置, 然後再將它們應用到決策請求2613。做這件事情可能會要求決策伺服器2617要從可由決策伺服器2617存取的任何位置中獲得其它與決策有關的資訊2623。這種處理過程之一實例是：在存取過濾器203之討論中所描述的技術；藉由該技術, 存取過濾器203獲得關於使用者的附加識別資訊。若決策伺服器2617從決策伺服器資料庫2619以及其它資源中獲得的資訊指示著行動被允許, 則決策伺服器

五、發明說明 (112)

2617會發送一種這樣指示的決策回應2615，而決策施行器2609會執行如2610處所指示的行動，並且經由行動回應2607，將結果轉回給請求實體2603；若決策回應2615指示：行動未被允許，則決策施行器2609會發送一種指示著行動未被允許的行動回應2607。

將決策施行器2609和決策伺服器2617分離之一重要優點是：可能在系統內的很多不同層級處建構決策施行器2609，其中瞭解到該系統包括一些由網路所連接的諸多裝置組成的系統。決策伺服器2617可能包含針對任何決策施行器的決策；因此，可能受該決策支配的行動不再受限於在系統之一個或更多層級處所採取的行動。

圖27顯示：一種具有諸多組件的系統2701，該組件都是藉由包括一公用網路2702及一內部網路103的網路加以連接的。在最高層級處，系統2701具有：一個或更多決策決策點(policy decision points)2723，它會決定決策是否允許一項行動；以及一個或更多決策施行點2721，其中諸多決策決策點的決策都會被施行。決策決策點將會包括決策伺服器2617；而決策施行點則會包括決策致能裝置，那就是：一種能夠執行如決策施行器2609般之功能的裝置。在決策決策點與決策施行點之間的通信是藉由決策訊息2725，該訊息則包括：決策請求2613以及決策回應2615。當一實體2603請求要使用資源R2611來執行一項行動時，將會由一種受決策施行點2721所控制的裝置來執行該行動，決策施行點2721將會和決策決策點2723交換決策訊息

五、發明說明 (113)

2725，以便決定：該行動是否被允許；如果是的話，決策施行點2721就會使該行動被執行。

包括在系統2701內的諸多決策致能裝置中有：

- 決策致能路由器2713，它會施行在實體網路中的路由指引通信量之層級處的決策；
- 決策致能附屬裝置2719，它會執行在一裝置之層級處的決策，該裝置附屬於系統2701的網路。一個實例就是印表機，它能夠查閱決策伺服器2617，以便決定：是否要接受一項來自某一實體2603的印出請求。
- 決策致能應用程式2717，它會執行在應用程式之層級處的決策。

每個決策致能裝置都會用像針對決策施行器2609所描述那樣的相同方式來處理決策：當決策致能裝置收到它必須決定該行動請求是否遵從建立在決策伺服器資料庫2619中的諸多存取決策所針對的一項行動請求2703時，它就會將一種決策訊息2725發送到決策伺服器2617；並且當它收到決策訊息時就會作出回應，允許或拒絕如決策訊息所指示的行動。

繼續更加詳細地討論關於圖27之諸決策致能裝置運作所處的層級，決策致能路由器2713可能保持針對它所路由指引的諸多分包資訊之被允許來源和目標的一些表；當路由器2713被初始化時，這些表都是根據由決策伺服器2617所提供的資訊加以建立的；從當時起，當路由器2713收到一種具有來源或目標不在其表中的分包資訊時，它就會將一

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (114)

種決策訊息2725發送到指示著來源或目標的決策伺服器2617，而決策伺服器2617則會藉由指示著是否打算將來源或目標包括在一些表中來對該訊息作回應。當然，當決策伺服器資料庫2619改變時，路由器2713的一些表可能也會由決策伺服器2617發送到路由器2713的訊息來保持更新。就像從前述中能夠看出的那樣，路由器2713會在存取過濾器203之建構例2001中的IP過濾器2019之層級處執行決策核對。

決策致能附屬裝置2719是一種諸如附屬於網路之一印表機的裝置。該裝置能夠對一項由一實體提出的請求作回應，以便隨著決策伺服器2617所發送之一決策訊息而使用它，並且能夠根據它從決策伺服器2617中收到的資訊而繼續進行。這種決策致能附屬裝置2719會允許管轄這些裝置的管轄詳細程度(granularity of control)比在存取過濾器203之層級處的存取核對可能允許的還更加精細。

最後，決策致能應用程式2717會允許：在一種比存取過濾器203可能允許的還要高之層級處的決策施行。只要決策伺服器資料庫2619包含與正在被應用程式存取的諸多資源有關的決策資訊，決策致能應用程式2717就能夠和決策伺服器2617交換決策訊息2725，因而能夠藉以決定：是否要允許或拒絕決策致能應用程式2717之使用者正在請求的行動。決策致能應用程式2717之一實例是：一種建構諸如FTP，HTTP，或SMTP之一網際網路服務的應用程式。這是由圖20中的諸多代理伺服器2031所處理的層級。因為服

五、發明說明 (115)

務現在可能都是決策致能的，所以代理伺服器不再是必要的；換成是，只能夠將網際網通信協定傳遞到服務存在的系統上，該服務將會提供由通信協定所請求的存取操作。如圖27中所示，該服務隨後能夠親自和決策伺服器2617交換決策訊息2725，以便決定：被請求存取操作是否應該被允許。

決策致能應用程式2717之另一實例是：一種文件處理程式。在這種情形下，決策伺服器資料庫2619可能包含一些決策，該決策載明：有權修改諸多文件之集合的諸多使用者之集合。當使用者使用程式來選擇一份文件以供編輯之用時，文件處理程式就能夠和決策伺服器2617交換決策訊息2725；且若來自決策伺服器2617的決策回應指示：使用者可能不會修改文件；則文件處理程式可能對使用者這樣指示，並且拒絕允許使用者修改文件。

就像從前述中能夠看出的那樣，將決策評估和決策施行分離以及決策定義的可擴充性質實際上共同允許：程式能夠對一項資源執行的任何操作成為決策之主體；於是，使得存取控制系統就像圖27中所顯示的那些系統：不但規模可伸縮性又容易管理，而且很容易地適應任何現在或未來的裝置或程式。

此處應該要指出的是：在存取過濾器203中，將決策評估和決策施行加以合乎邏輯地分離，縱使兩者都被包含在相同的裝置中。當依據圖26來審視圖20時，顯而易見的是：GUI 1915；啟動，登錄，警戒以及報表模組2027；資

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (116)

料庫共享目錄2028；ISDB管理程式2027；PCS 2025；以及MMF 2301會建構決策伺服器2617；而其餘的組件則會建構在IP過濾器及網際網路通信協定層級處操作的決策施行器2609。

決策之通則：圖28

在存取過濾器203中，適當存取資訊的管理員：能夠定義新使用者和使用者群組，能夠定義新資源和資訊集，並且能夠增加服務和伺服器。管理員並不能夠定義與存取資訊不同的行動。並且，任何人能夠用來定義新使用者群組的方法都是固定的，而資源則皆受限於資訊之來源。在較佳實施例的通用化決策伺服器中，這些限制都已經被解除。現在，管理員要定義：新行動，用來定義使用者群組的新方法，以及不是資訊集的資源是有可能的。當然，制定這些定義的權利本身就是由決策伺服器資料庫2619中的決策加以決定的，就像關於存取過濾器203中的管理決策及決策制定者決策所說明的那樣。在大多數的系統中，定義：諸多實體類型，資源類型，以及行動類型應該只限於屬於"安全官員"使用者群組的那些人。

將這些新的可能性圖解說明於針對顯示於圖28中之決策陳述的通用化決策語法2801中。通用化決策語法2801描述：在可能操縱決策所針對的視窗中，怎樣將決策呈現給管理員。在圖28中，用斜體字表示的項目都是可能被決策伺服器2617之管理員所定義的諸多決策陳述的組成部份，該管理員有權必需存取決策伺服器資料庫2619。在方

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (117)

括弧中的項目都是使以斜體字表示的項目與定義一項決策有關係的字組。譬如說，，

Employees are allowed to Access the HR Web Site

(雇員們都被容許存取HR網站資訊)

其中：Employees(雇員們)是一使用者群組，Access(存取)是一項行動，而HR Web Site(HR網站)則是一資訊集；該決策陳述允許：屬於"雇員們"使用者群組的任何使用者存取屬於"HR網站"資訊集的任何資源。

繼續更加詳細地討論關於通用化決策語法2801，Entity(實體)表示一使用者群組，其成員都是：由使用在存取過濾器203中的諸多技術中的一種技術；或者由決策伺服器2617之管理員所定義的一種技術加以定義的。針對實體的唯一要求是：它必須是可由決策施行器2609辨識的。Action(行動)表示：可能只是像存取過濾器203中之存取操作那樣的一項行動而已，或者是由決策伺服器2617之管理員所定義的一項行動。針對行動的唯一要求是：使決策施行器2609能夠對一項資源執行行動。Resource(資源)表示一資訊集。然而，在通用化決策伺服器中，一資訊集可能是諸如：印表機或檔案伺服器的諸多裝置之一集合。針對資源的唯一要求是：使決策施行器2609能夠對資源執行行動。

TimeIntervals(時間間隔)2809允許管理員定義一種對於使用通用化決策語法2801而正在被載明之決策的時間限制(temporal restriction)。當決策正在被評估用來決定一既定使用者是否有權存取一既定資源時，唯若評估時間在時間

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (118)

間隔內，才會考慮一項具有時間間隔的決策。譬如說：

Employees are allowed to Access the HR Web Site
from 9:00 am-5:00 pm weekdays

(雇員們都被容許存取HR網站資訊)

平日：從上午9時到下午5時)

它會將由雇員們存取HR網站的時間限制為正常營業時間。在一較佳實施例中，可能將時間間隔定義如下：

每天工作時間之始末的範圍；

工作日期之始末的範圍；

對於每周之工作日及休息日的限制：可選擇將每周的特定工作日，及/或被列示為休息日的日期包括在內或排除在外；

對於每月之工作周的限制：容許將每周，從參考日期起的每隔X周(其中X是從2到12的一個數字)，或者在每一適用月份內的周數表加以規範；

每年之適用月份表。

ActionAttribute(s)(行動屬性)2811都是可能實行被決策陳述允許之行動所用方法的一些由管理員定義的定義。再者，唯一的要求是：決策施行器2609能夠實行如行動屬性所載明的行動。譬如說：

Marketing is allowed to print to the Marketing Printer
with type=color

(行銷員被容許使用具有列印類型為彩色的行銷員之印表機來列印)

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (119)

這項決策包含行動屬性 $\text{type}=\text{color}$ (列印類型=彩色)，該決策允許屬於"行銷員"(Marketing)使用者群組之使用者使用行銷員之印表機的資源來執行彩色列印。

行動屬性的諸多附加實例有：

- 針對網路通信連接所需的服務類別；
- 打算使用的路由或媒體類型；
- 打算適用的結帳費率；
- 這項交易的最大數量；
- 完成交易所容許的最大時間。

就像由語法 [with | when] (具有 | 每逢) 所指示的那樣，能夠將時間間隔和行動屬性，以及和整個決策陳述一起使用。例如，對服務類別設下時間限制的一項決策看起來像這樣：

(Everyone is allowed to access the World Wide Web with
bandwidth=90% when weekends

(每個人都被容許每逢周末就存取具有頻寬=90%的全球
資訊網資訊)

這項決策允許在"每個人"之使用者群組中的實體每逢周末就存取具有頻寬=90%的全球資訊網資訊。當已經將時間間隔應用到行動屬性時，雖若在應用到行動屬性之時間間隔內提出執行行動之請求，才會像載明於行動屬性中那樣地執行載明於決策中的行動。

通用化決策的建構例：圖29和30

圖29顯示決策資料庫2901。決策資料庫2901是決策資料

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (120)

庫301的一種修改；以便適應用語法2801所定義的通用化決策，並且在一種已經將決策評估和決策施行分離的環境中運作。於是，在圖29中，決策查詢2939是來自決策伺服器2617而不是存取過濾器203，因而包括：一種打算執行之行動的說明符(specifier)，以及一種資訊來源或打算執行行動所針對的其它資源的規範(specification)。將決策查詢的結果2941轉回給決策伺服器2617。除了決策是否允許該行動的一種指示外，該結果現在還包括與行動有關的屬性數值。在圖29中而其功能維持不變的諸多圖3中的單元都具有它們在圖3中所具備的參考數字。就從存取決策307開始，資訊之第一附加項目是存取類型定義2929，它會定義：諸多附加行動類別，可能針對它而將決策定義在存取決策307中。其次，會有屬性資訊2927，它會定義：可能附屬於涉及實行一項決策的諸多實體之屬性。包括在屬性資訊2937內的則有下列各種資訊：

屬性指定2937，它會載明打算和屬性一起使用的是何種：使用者群組，資訊集，網站，或服務；

屬性標記2941，它會定義：在使用者界面中，為人所熟知的諸多屬性名稱；以及

屬性特點2939，它實際上會定義：屬性怎樣影響被它指定的諸多使用者群組等等。

時程安排(schedules)資訊2925會定義：可能附屬於決策或屬性的時間間隔。在時程安排資訊2925內，時程安排規則2931實際上會定義時間間隔；而休假日表2933則是一種

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(121)

使用在時程安排規則中的休假日表。資源類型2935會定義：可能定義決策所針對的資源之類型，而使用者ID類型2937則會定義：針對可能定義決策所針對的實體所需的識別方法之類型。

在一較佳實施例中，使用微軟公司之為人熟知的：Microsoft®存取資料庫軟體來建構資料庫2901。存取軟體是一種關係資料庫(relational database)，那就是：將資料庫中的資訊儲存在一些表中。在存取軟體中的一種公用程式(utility)會提供：一些表的圖像以及它們彼此的關係。本申請案的圖13到17以及圖30都是源自那些圖像。在圖30中，出現在圖13到17中的一些表都具有它們在那些圖中所具備的參考數字；而一些新的表則具有開頭是"30"的參考數字。在圖30中的一些表3001顯示：怎樣將用來定義時間間隔和屬性的一些表加以整合進入決策資料庫2901中。更籠統地說，它們顯示：怎樣藉由增加另外一些單元而可能修改一項決策，以及怎樣針對決策而可能定義諸多新單元類型。

時間間隔的詳細建構例

就從時間間隔開始，將這些時間間隔加以定義在時間間隔表3025中。該表包括：一時程安排定義表3023，它會定義可能出現在通用化決策語法2801內的TimeInterval(s)2809中的名稱；以及一時程安排規則表3025，它會定義可能與定義在"時程安排定義"表3023中的名稱有關聯的時程安排規則。一個以上的時程安排規則可能與一既定名稱有

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (122)

關聯。ScheduleDefID(時間安排定義ID)使定義在表3025中的每項時程安排規則都與使用表3023中之規則的時間排程有關係；從Day Mask(工作日掩蔽)到End Date(結束日期)的諸多欄位會定義時間安排規則。"Description"(描述)欄位則載示規則及其目的之描述。

如以下所提及的，可能針對整個決策以及針對決策中的屬性而定義時間間隔。於是，定義在"存取決策"表1611中的每項決策現在都包括一個ScheduleDefID欄位。每個這樣的欄位都會包含：針對打算應用到決策之一時間間隔而在表3023中之一定義的一個ScheduleDefID識別符。於是，當決策伺服器2617正在決定一項決策是否可適用於一項行動請求時，經由：在針對決策之表1611內的登載項中，針對時間間隔的ScheduleDefID欄位；它就能夠指出應用到一項決策之時間間隔的位置。同樣地，"屬性指定"表3007，它會使屬性與：使用者群組，資源集，網站，或服務有關係；該表包括：針對可適用於該特定屬性指定的任何時間間隔的一個ScheduleDefID欄位。最後，用來定義時間間隔的機制也被使用在用來時程安排警戒資訊之一較佳實施例中；於是，在表3023中的諸多登載項也都可以從"AlertSchedules"(警戒資訊時程安排)表3021中指出位置。

屬性的詳細建構例

將用來定義諸多屬性並使它們與可能被應用的：使用者群組，資源群組，網站，以及服務有關係的一些表顯示於圖30中的屬性表3003中。一既定屬性是由三種表："屬性

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (123)

標記"表3005，"屬性"表3011，以及"屬性特定"表3009中的登載項所定義的。"屬性標記"表3005會定義：用於針對在決策定義語法2801內的ActionAttribute(s)中之諸屬性的標記。每個這樣的標記都會有一個登載項，該登載項包括：標記本身，屬性之描述，標記之優先次序(precedence)，以及屬性之類型。標記之優先次序會定義：當一個以上的屬性與決策評估連接時，將會應用哪些屬性。當一項指定具有一種比另一項指定還高的優先次序時，就會將具有較低優先次序的那一項指定不予理會。每個屬性標記登載項都是由一個"AttributeLabelID"(屬性標記ID)加以識別的。

在"屬性"表3011中的每個登載都會載示屬性之目前定義。該定義可能具有用來識別"屬性標記"表3005中之諸登載項的一個或更多"屬性標記ID"欄位。由"屬性標記"表3005中的那個登載項所定義的標記表示由"屬性"表3011中的登載項所定義的屬性。屬性的目前意義是由表3011中的一些欄位加以定義的。包括有：屬性之描述，其類型，它應用到的伺服器之ID，以及關於伺服器的裝置類型。三個欄位："AttributeFeatureID"(屬性特點ID)，"value1"(數值1)，以及"Value2"(數值2)都是特別感興趣的欄位。在那裏，必須至少有一個"AttributeFeatureID"欄位。該欄位會識別"屬性特點"表3009中之一登載項，該表則會定義使用在屬性中的諸多數值之種類和範圍。"Value1"和"Value2"會定義：單一數值(Value1)之目前範圍，或者兩種數值(Value1和Value2兩者)之目前範圍；該數值係選擇自針對"屬

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (124)

性特點"表3009中之屬性而定義的諸多數值之種類和範圍。

就像從前述中將會顯而易見的那樣，"屬性特點"表3009能夠被用來定義諸多新屬性種類。在表3009中的每個登載項都會包括用來指出登載項之位置的"屬性特點ID"識別符及一些欄位如下：

- 類別：屬性所屬的類別之名稱(譬如說：服務品質，結帳費率，或交易之最大數量)；
- 特點ID：唯一定義在其類別內之特點的數字；
- 名稱：使用者藉由它來瞭解特點的名稱；
- 描述：特點的一種描述；
- 數值類型：定義屬性的諸多數值之類型的一種定義(譬如說：需要單一數值還是一對數值，以及資料類型資訊)；
- 特點優先次序：次序的一種指示，依照該次序將諸多特點應用在評估屬性中；
- 數值優先次序：打算選擇範圍中的最高數值還是最低數值的一種指示；以及
- 限制：對於數值之限制的一種指示。

要定義新屬性類別，被決策伺服器2617之決策允許這樣做的管理員只是定義針對"屬性特點"表3009中之新類別的特點，然後再開始定義使用那些特點的屬性。一項特點可能是：對將要施行決策的決策施行器2609而言是很有意思的任何事物。此處應該要注意的是：可能將用來定義諸多

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (125)

新屬性種類的一些上述通用技術使用在決策資料庫2901中的別處，以便定義諸多：新行動，用來識別使用者的新方法，以及新資源類型。

一旦屬性已經藉由三種表：3005，3011及3009中的資訊加以定義，它就會與一個屬性可能應用到的實體有關係。將此實體稱為：屬性之主體。"屬性指定"(AttributeAssignment)表3007會載明這些關係。在表3007中的每個登載項都會使載明在它的"AttributeLabelID"(屬性標記ID)中的屬性與單一主體有關係；此外，它可能使屬性與一使用者群組有關係，而該使用者群組的成員則可能執行一項涉及主體的行動。若登載項未載明一使用者群組，則屬性應用到主體之任何用途；在其它情況，只有當被載明使用者群組使用主體時，屬性才會應用。主體可能是：使用者群組，資源集，網站，或服務；就像藉由諸多欄位。"使用者群組ID"，"資源群組ID"，"網站ID"，以及"伺服器ID"的數值加以載明的那樣。在表3007中的另外一些欄位會指示：屬性是否為現用的(即：打算目前應用的)，應用程式應該何時開始，它何時滿期，以及屬性是否涉及時間間隔，針對時間間隔的"ScheduleDefID"數值。"優先次序"欄位則指示：在指定給一既定實體的諸多屬性中，屬性將會具有的優先次序。

在決定將哪些屬性應用在制定一項決策方面中，決策伺服器2617繼續進行如下：當完成決策評估時，針對指向與決策評估有關的使用者群組，資源群組，網站，或服

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (126)

務其中任何一個的諸多通信鏈路，加以搜尋在表3007中的屬性指定資訊。若執行行動之實體屬於屬性應用所針對之一使用者群組，則順著來自表3007中之屬性指定的諸多通信鏈路走，就會來到表3005中的屬性標記，依序來到表3011中的屬性，最後來到表3009中的屬性特點。這些已鏈接表中的每一種表(除了表3011外)都會包含優先次序資訊，使用該資訊來決定：針對那些順著所有通信鏈路走而發現的屬性，在表3011中有哪些屬性實際上將會應用到決策評估。

針對每個類別的屬性而各別地考慮這些優先次序，就像藉由表3009中的屬性特點加以定義的那樣。在每個類別內，首先考慮：在表3007中的屬性指定中的優先次序。雖然共享相同優先次序的所有指定都會被考慮，但是只有那些具有最高優先次序數值的指定才會進一步被考慮。其次，考慮：針對其餘的已鏈接屬性，在表3005中的屬性標記中的標記優先次序。雖然共享相同標記優先次序的所有標記都會被考慮，但是只有那些具有最高優先次序數值的標記才會進一步被考慮。其次，考慮：針對其餘的已鏈接屬性，在"屬性特點"表3009中的登載項中的特點優先次序。只有那些共享最高特點優先次序的屬性才會被保留。最後，對於在表3011中的每個屬性而言，該屬性被鏈接到"屬性特點"表3009中的相同登載項；在"屬性特點"表3009中的數值優先次序，藉著指示打算選擇的是最高數值還是最低數值而被用來決定：要使用來自表3011中的哪個屬

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線

五、發明說明 (127)

性。

這時候，對於在表3009中的諸多有關屬性特點登載項而言，定義在表3011中最多一個屬性會保持原狀，而在這些登載項中的數值和特點都將會被轉回，以使用於評估決策。在某些情形下，請求可能指示需要何種屬性數值；並且，若它們與載明在決策中的那些數值不匹配，則該請求可能被拒絕；在其它情形下，將諸多屬性數值提供給決策施行2609，以使用於執行行動。

使屬性表3003和時間間隔表3025最佳化

就像在上述存取過濾器203的討論中所描述的以及在圖21和23中所圖解說明的那樣，在一較佳實施例中的決策伺服器2617，藉著從其中產生諸多MMF檔案2303而使決策資料庫2901最佳化。在較佳實施例中，已經增加兩個新MMF檔案，以使表3003和3025中的資訊最佳化。兩個新MMF檔案如下：

- DBProperties(資料庫"特性")檔案：包含能夠應用到其它物件的所有"特性"-屬性及時程安排。此索引(index)是藉由在那些其它物件中的"特性ID"加以編製索引的。
- DBPropertiesMetaData(資料庫"特性元資料")檔案：所有特性都有一個名稱。此檔案是藉由特性類型名稱加以編製索引的(對於包含在DBProperties檔案中的每個特性名稱而言，在索引中具有一個登載項)；並且將一些名稱映射到諸多特性ID之一列表，以使它們在

(請先閱讀背面之注意事項再填寫本頁)

張

訂

線

五、發明說明 (128)

DBProperties檔案中很快地被查出。

針對時間間隔的使用者界面：圖31到33

圖31到33顯示：使用在一較佳實施例中，在圖形使用者界面中所使用的視窗；用來：察看何種時間間隔(或時程安排)已經被定義，定義針對一時間間隔的一項規則，以及使用一時間間隔與一項決策有關聯。就從圖31開始，該圖顯示：一種用來顯示已定義時程安排的視窗3102。子視窗(subwindow)3103會依照名稱列示所有的已定義時程安排；而子視窗3106則會依照名稱列示所有的已定義規則。被顯示資訊是來自："時程安排定義"表3023和"時程安排規則"表3025。

要察看一時程安排名稱表示何種規則，使用者會選擇在子視窗3103中的名稱，如3105處所顯示的，在該處，已經選擇"非工作時間"。此時程安排具有兩個組成規則：一個表示每周之工作日，顯示在3107處；一個表示周六，周日，及休假日，顯示在3109處。當選擇時程安排名稱時，屬於它的(諸多)規則都會被凸顯在視窗3106中。相反地，當選擇規則時，針對使用該規則的諸多時程安排的時程安排名稱都會被凸顯出來。在子視窗3106中的3111處顯示：針對營業時間的規則；而在子視窗3103中則顯示：另外一些時程安排名稱。

要產生一項新時程安排，當子視窗3103處在現用狀態時就點按"新增"按鈕，並輸入新時程安排名稱；然後再選擇新時程安排，並將屬於它的一些規則凸顯在子視窗3102

五、發明說明 (129)

中。要改變指定給一時程安排的一些規則，先選擇時程安排名稱，然後在子視窗3106中選擇針對該名稱的不同規則。要產生針對一現存時程安排的一項新規則，先選擇時程安排之名稱並點按"新增"按鈕，在當時就可能產生新規則，如以下描述的。當處於子視窗3106中時，也能夠點按"新增"按鈕，產生新規則，然後再使新規則與一時程安排名稱有關係，如以上描述的。藉著將規則拖曳(dragging)到時程安排名稱，並且將它棄置在時程安排名稱上，也能夠使一項規則與一時程安排名稱有關係。

將用來產生一項新規則的視窗顯示在圖32中的3201處。這是用來修改一現存規則或產生一項新規則的視窗。要修改一現存規則，就對它點按二次。在視窗中的輸入資訊會允許使用者：依據時程安排之時間的有效性來定義正在被應用到決策或屬性的時間間隔(3203)，定義被選擇時間都有效的每周之工作日(3205)，定義時程安排有效的工作周(3207)，以及定義時程安排有效的每年的一部份(3209)。如圖示，視窗3201將顯示於圖31中的時程安排定義在3111處。該時程安排是由"營業時間"所表示。顯示於視窗3201中的資訊是來自"時程安排規則"表3025，而使用視窗3201所做出的諸多修改則被應用到該表。

圖33顯示：用來將時間間隔增加到一項決策之定義的視窗。視窗3301將由屬於"社團"(Corporate)使用者群組諸多使用者存取"社團"資訊集限定為：在3303處所指示的"營業時間"之時程安排。當使用者點按方框3303時，就會顯

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (130)

示諸多已定義時程安排的整個列表，因而使用者可能選擇其中一個或增加一項新名稱。當使用者點按"定義"按鈕3305時，就會顯示針對被選擇決策的視窗3201。若正在增加一項新名稱，則必要時使用者會針對新時程安排而填寫視窗3201。依據圖30，選擇在圖33中之一時程安排會使"存取決策"表1611中之一"ScheduleDefID"欄位被填寫：針對"時程安排定義"表3023中之登載項的識別符；而表3023則將時程安排名稱包含在它的"名稱"欄位中。若時程安排名稱是新的，則針對新名稱而將一新登載項增加到表3023。若增加或修改一項規則，則"時程安排規則"表3025也會被修改。

針對屬性的使用者界面：圖34到37

針對屬性定義和指定的使用者界面是相似的。圖34顯示：一種列示服務品質(quality of service, 簡稱QoS)類型的諸多目前已定義屬性的視窗3401。這些屬性決定：有多少頻寬(bandwidth)可供一種根據既定決策而正在執行的存取操作利用。在3401處，列示有一些屬性標記或名稱。此處，定義四種QoS屬性：三種表示頻寬數量("高"，"中"，"低")，一種("最高優先級")表示若有衝突時的優先級(Priority)。所有的這些屬性都有一種。的優先次序，如在3405處所顯示的。諸多頻寬屬性全部都由"頻寬"特點加以定義，如在3407處所顯示的。針對每個屬性的"數值"則被定義在3409處。只有"最高優先級"才會有"數值2"。就像載明於視窗3401中的那樣，QoS頻寬屬性中的："高"會接收512000的

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (131)

最大頻寬，"中"會接收64000的最大頻寬，而"低"則會接收32000的最大頻寬。關於"最高優先級"，針對屬性所載明的優先級必須位在針對"數值1"和"數值2"所載明的兩個數值之間。在視窗3401中的資訊當然是來自三種表：3005，3011，以及3009。

圖35顯示：用來將一種QoS屬性指定給使用者群組，資訊集，網站，或服務的視窗3501。在子視窗3503中，顯示：對於所有使用者群組(3507)而言，已經怎樣將"中"，"高"，以及"低"三種QoS頻寬屬性(3509)分別指定給全球資訊網服務，檔案傳送服務，以及遠距存取服務三種主體(3511)；以及已經怎樣將"高"QoS優先級屬性指定給"財務"(Finance)使用者群組主體。諸多不同的指定會反映以下事實：頻寬是一種通信服務的屬性，而優先級則是通信服務之一使用者的屬性。於是，在可供網路服務利用的頻寬內，"財務"使用者群組的諸多成員都具有高優先級。就像由本實例所顯示的那樣，一個以上的行動屬性可能應用到一項決策。若能夠藉著從兩個子視窗3513和3515中分別選擇一些使用者群組和主題來產生針對主題的屬性，則會促進屬性指定。在此視窗中所做的選擇當然都會被應用到"屬性指定"表3007。用與視窗3102觸及諸多用來定義屬性標記和特點的視窗相同的通用方式，就能夠進一步使用視窗3503。

圖36顯示：用來讀取，修改，或產生"屬性標記"表3011中之一登載項的視窗3601。此處，正在讀取的登載項是針

(請先閱讀背面之注意事項再填寫本頁)

張

訂

線

五、發明說明 (132)

對"中"QoS頻寬屬性。在3603處，顯示有：登載項之"標記"，"描述"，及"標記優先次序"欄位的數值。具有適當存取權利的管理員當然能夠經由視窗3601而改變這些欄位的數值。在3605處，顯示：針對與標記有關聯的屬性，來自"屬性"表3011中之登載項的資訊。在那裏顯示有：在登載項中之"數值1"的目前數值，以及特點之名稱。特點名稱當然是來自針對該屬性之"屬性特點"表3009。再者，可能經由視窗3601而編輯這些數值。按鈕3607被用來檢視一種視窗，該視窗會顯示：在"屬性特點"表3009中之特點登載項的完整內容。

圖37顯示該視窗。視窗3701是用來定義針對一既定屬性類別及諸多新屬性類別的諸多新屬性的視窗。視窗當然會依照"屬性特點"表3009中之一登載項的數值而運作。方框3703是諸多屬性類別之一列表；可能藉由增加到列表來定義新類別。方框3705是目前特點之名稱；在它們(類別與名稱)之間會唯一地識別一登載項，而類別與名稱則對應於表3009內的諸多登載項中的"類別"與"名稱"兩個欄位。在這種情形下，登載項是針對QoS"優先級屬性"(Priority attribute)。
"描述"方框3707會包含：在正在被檢視之登載項中的"描述"之數值。3709指示：特點具有哪種數值類型，此處是一對數值，如圖34中所指示的。在3711處，顯示有："特點優先次序"和"數值優先次序"兩個欄位的目前設定值；而在3713處，則會出現任何限制資訊。

結論

五、發明說明 (133)

3 結論

前面的闡述已經對那些熟習於與闡述有關之技藝的人披露：用來建構通用以決策伺服器的最佳模式，該模式目前是此處所披露之通用決策伺服器的諸多開發者所熟知的。如以上描述的，通用決策伺服器的兩項基本特點是：將決策評估與決策施行分離，以及關於能夠制定決策所針對的諸多行動類型的可擴充性。關於將決策評估與決策施行分離，諸多決策施行組件可能被定位在決策應用到之系統中的不同層級處；而諸多決策評估組件則可能是在遠離諸多決策組件之位置的位置處。

雖然用來將決策評估與決策施行分離的技術，以及關於能夠執行諸多行動種類而使決策可擴充的技術都可能被應用到用來定義的任何機制；可是當該技術使用在依據一些行動和諸多實體之集合來定義決策的一些決策施行系統中時，它們都是特別有用的。在這些系統中，也可能使得可能執行行動的諸多實體之類型以及執行行動所針對的諸多實體之類型都是可擴充的。

會增加系統之有用性而在此處所披露之決策施行系統的另外一些特點是：行動屬性，它會定義打算執行由決策授權之一行動所依照的方式以及時間間隔；該時間間隔則會定義：決策有效時或一屬性被應用到一項行動時的時間。一種圖形使用者界面會提供：諸多決策及其組成部份的簡易定義和操縱方法。

就像對那些熟習於有關技藝者而言將會立即顯而易見的

(請先閱讀背面之注意事項再填寫本頁)

張

訂

線

五、發明說明 (134)

那樣，此處所描述的很多技術都可能被應用在任何種類的決策施行系統中；並且，甚至是在一種以此處所描述的方式來定義決策的決策施行系統中最有用的那些技術，也可能用很多不同的方式加以建構。譬如說，可能使用不同的圖形使用者界面，可能使用不同的資料庫系統來建構決策；並且在一既定資料庫系統內，可能使用諸多不同的表安排。於是，此處披露的諸多原理的無限多個其它實施例都有可能；並且，為此緣故，在各方面，打算將"闡述"視為範例而不具限制性；因而決定此處披露之本發明的涵蓋範圍(breadth)並不是來自"闡述"，而是來自像利用被專利法律允許的完全涵蓋範圍所解釋那樣的申請專利範圍。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

四、中文發明摘要(發明之名稱：

一般化決策伺服器

在虛擬專用網路(virtual private network)中，將一種規模可伸縮性存取過濾器(scalable access filter)和像它一樣的其它存取過濾器一起使用，以便控制：針對網路中諸多伺服器(servers)所提供的資訊資源，由在網路中諸多客戶機(clients)處之使用者所執行的存取操作(access)。每個存取過濾器都使用一種存取控制資料庫的局部拷貝(local copy)來決定：存取請求是否由一使用者提出。將局部拷貝中由管理員所做的改變傳播到所有其它的局部拷貝。每位使用者均屬於一個或更多使用者群組(user groups)，而每個資訊資源則均屬於一個或更多資訊集(information sets)。根據存取決策而允許或拒絕存取操作，該決策依據諸多使用者群組和資訊集來定義存取操作。同樣地，由管理決策(administrative policies)來決定管理員的權利。唯若使用者之

英文發明摘要(發明之名稱：

"GENERALIZED POLICY SERVER"

A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base to determine whether an access request made by a user. Changes made by administrators in the local copies are propagated to all of the other local copies. Each user belongs to one or more user groups and each information resource belongs to one or more information sets. Access is permitted or denied according to of access policies which define access in terms of the user groups and information sets. The rights of administrators are similarly determined by administrative policies. Access is further permitted only if the trust levels of a mode of identification of the user and of the path in the network by which the access is made are sufficient for the sensitivity level of the information resource. If necessary, the access filter automatically encrypts the request with an encryption method whose trust level is sufficient. The first access filter in the path performs the access check and encrypts and authenticates the request; the other access filters in the path do not repeat the access check. A policy server component of the access filter has been separated from the access filter and the policies have been generalized to permit administrators of the policy server to define new types of

四、中文發明摘要（發明之名稱：）

識別模式以及在執行存取操作所採取之網路中路徑的信賴等級(trust level)都足夠應付資訊資源的靈敏度等級，才會進一步允許存取操作。必要時，存取過濾器會利用一種其信賴等級足夠應付的加密(encryption)方法，對請求加以自動加密。在路徑中的第一存取過濾器會執行存取核對，進而對請求加以加密和鑑定(authenticate)；而在路徑中的其它存取過濾器則不會重複存取核對。已經將存取過濾器的決策伺服器組件和存取過濾器分離；並且，已經將決策通用化(generalized)，以便允許決策伺服器的管理員定義：能夠制定決策所針對的諸多新行動類型和新實體(entity)類型。現在，決策可能進一步具有時間間隔之規範；在時間間隔期間，決策都在施行中，並且實體可能都和屬性(attributes)有關聯，該屬性則載明：當決策應用時，打算怎樣使用實體。

英文發明摘要（發明之名稱：）

actions and new types of entities for which policies can be made. Policies may now further have specifications for time intervals during which the policies are in force and the entities may be associated with attributes that specify how the entity is to be used when the policy applies.

五、發明說明()

1. 一種用來施行決策的決策施行系統，該決策會定義：在電腦系統中所定義的諸多第一實體可能針對在電腦系統中所定義的諸多第二實體執行哪些屬於其中第一類型的行動，該決策施行系統所屬的類型，包括：

一決策伺服器，它包括諸多決策之一決策資料庫；以及

一決策施行器；它會控制第一行動類型之執行(performance)，並且能夠將一項用來執行第一類型之行動的請求傳達給決策伺服器；唯若來自決策伺服器之一回應指示：決策允許該行動，決策施行器才會允許行動之執行，而該決策施行系統則具有特徵為：

決策資料庫是可以擴充的，以便包括針對屬於其中附加類型之諸行動的決策；因此，可能將一種會控制附加類型之行動之執行的附加決策施行器增加到決策施行系統。

2. 根據申請專利範圍第1項之決策施行系統，進一步具有特徵為：

決策資料庫是屬於依據第一實體之集合和第二實體之集合來定義決策的類別；以及

決策資料庫是可以進一步擴充的，以便包括：一附加第一實體類型及/或一附加第二實體類型。

3. 根據申請專利範圍第2項之決策施行系統，進一步具有特徵為：

一項行動屬性可能在資料庫中與第一實體之集合及/或第二實體之集合有關聯，該行動屬性會載明：打算執行

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

關於在第一實體之集合中的諸多實體及/或在第二實體之集合中的諸多實體而載明在一既定決策中的一項行動所依照的一種方式。

4. 根據申請專利範圍第3項之決策施行系統，進一步具有特徵為：

決策資料庫是可以進一步擴充的，以便包括一附加行動屬性類型。

5. 根據申請專利範圍第1到4項之決策施行系統，進一步具有特徵為：

附加決策施行器會在電腦系統之一層級處控制行動之執行，該層級與決策施行器控制行動之執行所處的層級不同。

6. 根據申請專利範圍第1到4項之決策施行系統，進一步具有特徵為：

諸多決策施行器中至少有一個是在遠離決策伺服器之電腦系統中的一個位置處。

7. 根據申請專利範圍第1到4項之決策施行系統，進一步具有特徵為：

決策施行器會控制不是電腦系統之一部份的第二實體。

8. 一種屬於依據第一實體之集合，第二實體之集合，以及諸多行動來定義決策之類別的決策資料庫，一既定決策會定義：屬於既定第一實體之集合之一實體可能針對屬於既定於第二實體之集合之一實體執行的一項既

(請先閱讀背面之注意事項再填寫本頁)

訂 線

五、發明說明()

定行動；該決策資料庫具有特徵為：

一項另加條件可能在資料庫中與既定決策有關聯，該另加條件會在屬於既定第一實體之集合之一請求實體提出一項請求以執行針對屬於既定第二實體之集合之一實體的既定行動之時決定：請求實體是否可能執行該行動。

9. 根據申請專利範圍第8項之決策資料庫，進一步具有特徵為：

另加條件是一種與既定決策有關聯的時間間隔規範，時間間隔規範會載明時間之間隔；在時間間隔期間，屬於載明在既定決策中的既定第一實體之集合的諸多實體可能執行：針對屬於其中所載明的既定第二實體之集合的諸多實體，其中所載明的既定行動。

10. 一種屬於依據第一實體之集合，第二實體之集合，以及諸多行動來定義決策之類別的決策資料庫，一既定決策會定義：屬於既定第一實體之集合之一實體可能針對屬於既定第二實體之集合之一實體執行的一項既定行動；該決策資料庫具有特徵為：

一項行動屬性可能在資料庫中與既定第一實體之集合及/或既定第二實體之集合有關聯，該行動屬性會載明：打算執行載明在既定決策中之既定行動所依照的一種方式。

11. 根據申請專利範圍第10項之決策資料庫，進一步具有特徵為：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

決策資料庫是可以擴充的，以便包括諸多新行動屬性類型。

12. 根據申請專利範圍第10項之決策資料庫，進一步具有特徵為：

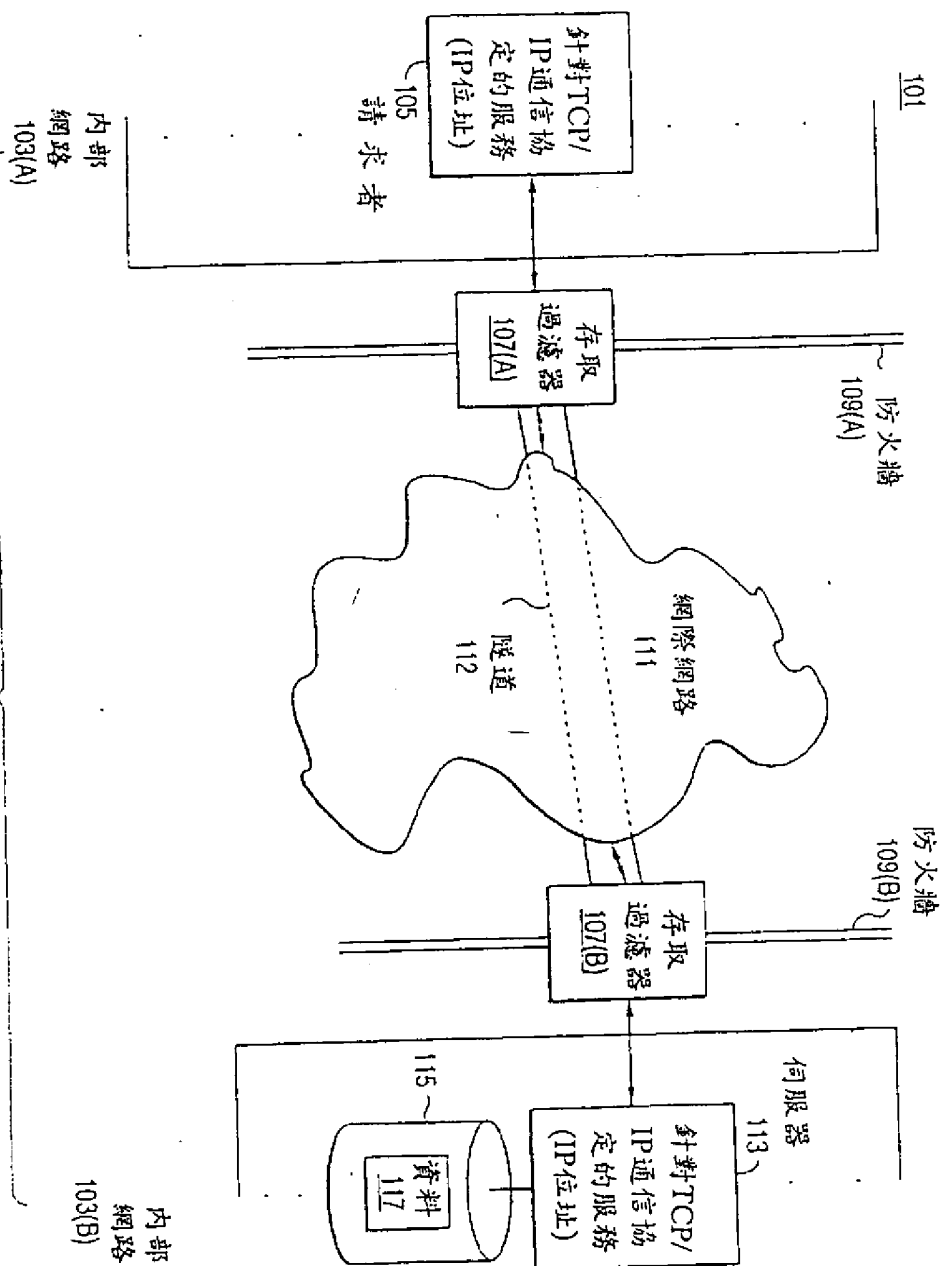
一種行動屬性條件可能在資料庫中與針對既定決策之一行動屬性有關聯，該行動屬性條件會在請求實體提出請求之時決定：屬於既定第一實體之集合之一請求實體是否能夠執行針對在既定第二實體之集合中之一實體的既定行動，該行動是如行動屬性中所載明的。

(請先閱讀背面之注意事項再填寫本頁)

表

訂

線



虛擬專用網路119

圖 1

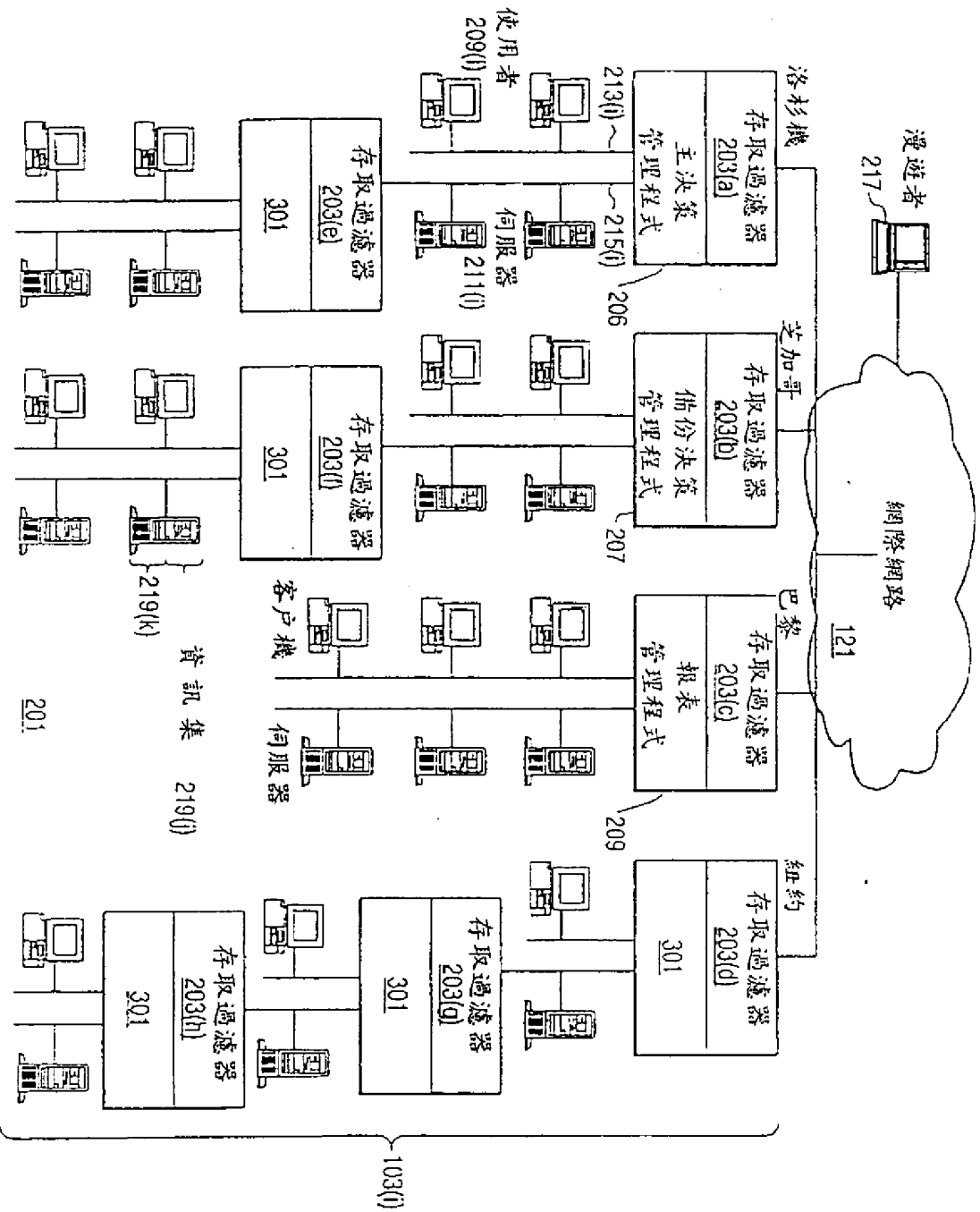
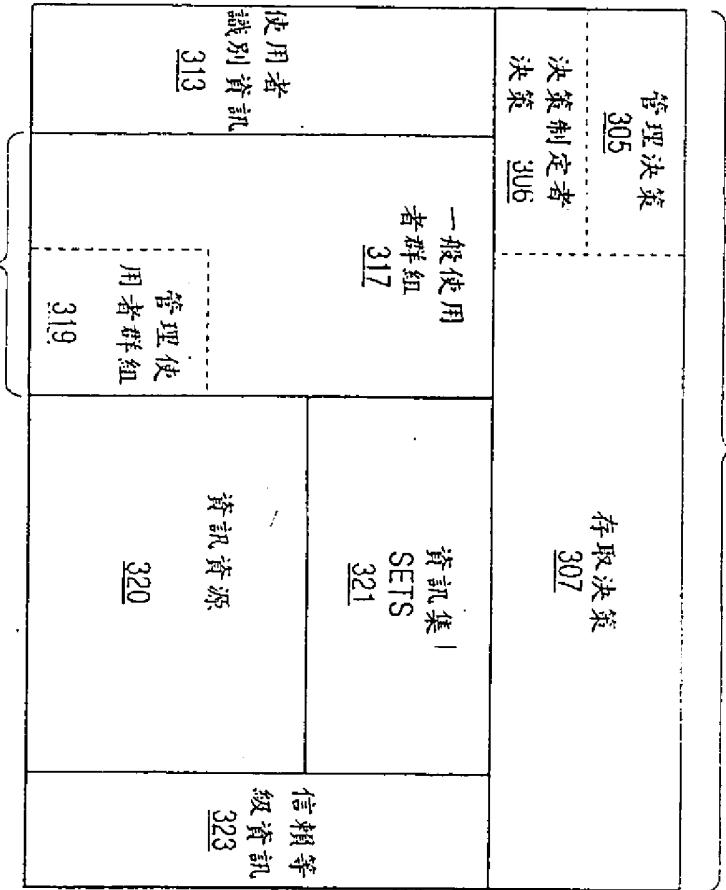


圖 2

301

使用者
群組
315



(使用者，資訊集：309)
前往來自
存取過濾器(AF)203
(請求被允許/不足：311)

圖 3

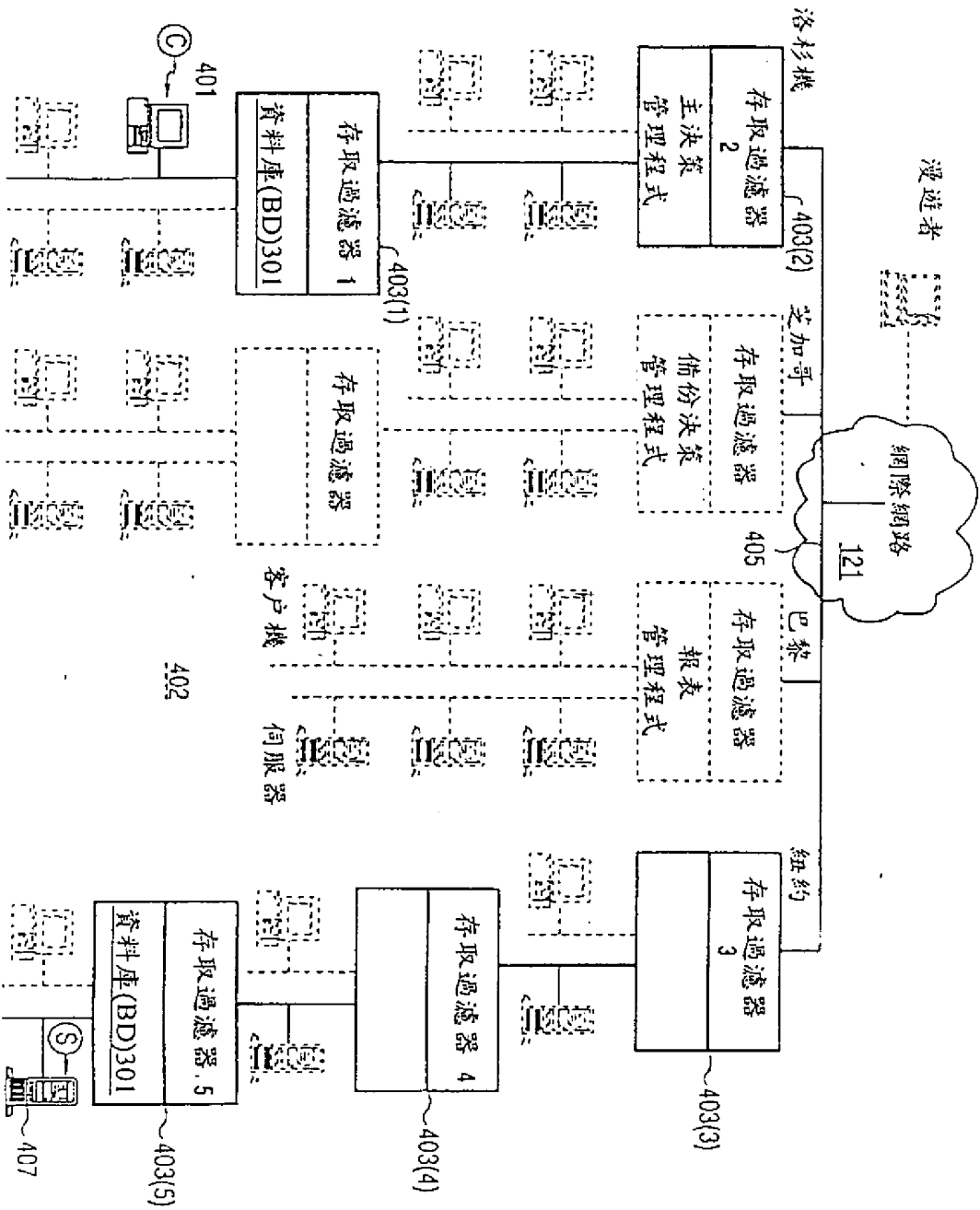


圖 4

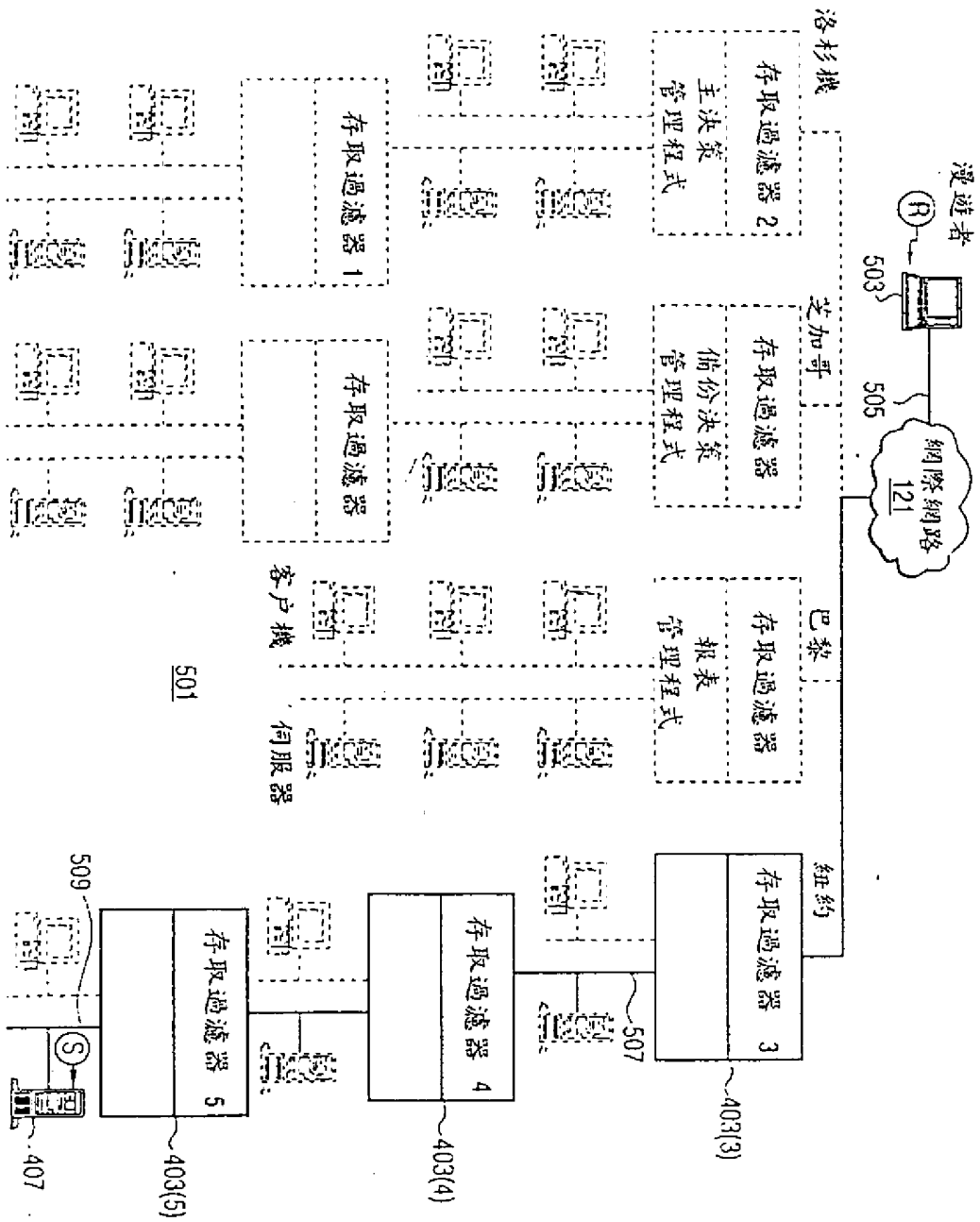


圖 5

情報/資料 靈敏度等級	最小加密方法	最小鑑定方法
最高機密	3DES	經由SKIP的證書
機密	DES	經由SKIP的證書
專用	RC4-40	視窗識別符(Windows ID)
公用	不需加密	不需鑑定

603 609 607

609(1) }
601

四
6

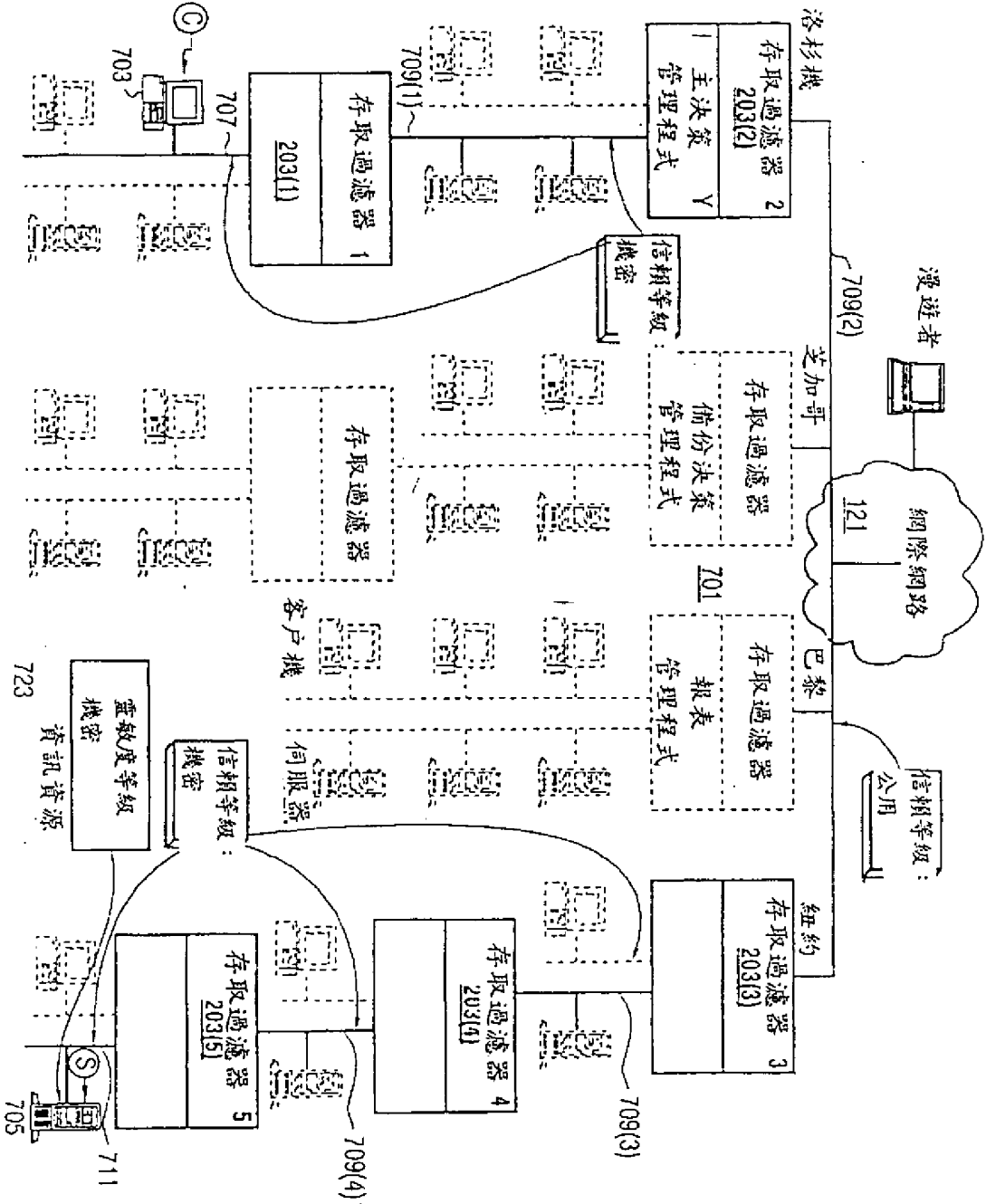


圖 7

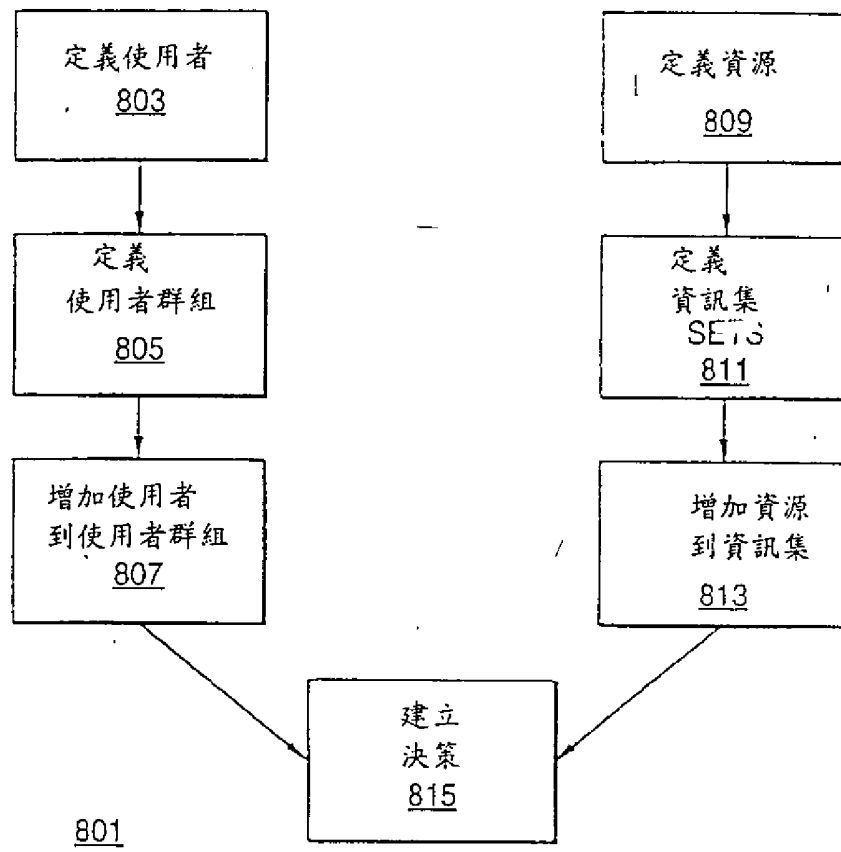


圖 8

FYI for Windows NT

Apply

921

Cut

Copy

Paste

Find

Select All

Sort

Sort

Expand All

Collapse All

New

Delete

Properties

Add to Group

Wizards

915

Alert log

Emergency

911

Main

User Groups

Resource Sets

Policy

Smart Filter

Reports

User Groups:

Administrators

Internet

Intranet

Engineering

917

159.200.200.1

Systems Programmin

Applications Program

Tech Support

Documentation

QA

Corporate

IP: sampleson.com

903

User Definitions:

913

Windows ID

VPN Certificate

Ext. Certificate

Smart Card

IP Range

IP Domain

Low

Choose a tab to see details

159.200.200.1

159.200.200.101

159.200.200.151

159.200.200.176

159.200.200.201

159.200.200.226

159.200.200.100

159.200.200.150

159.200.200.175

159.200.200.200

159.200.200.225

159.200.200.250

919

909

Ready

01/31/97 17:57:41

Apply

Cut

New

Copy

Delete

Properties

1007

Find

Select All

Sort

Sort

Expand All

Collapse All

Alert log

Emergency

911

Main

User Groups

Resource Sets

Policy

Smart Filter

Reports

Resource Sets:

gr1

gr2

Intranet

Intranet

Departments

Locations

Functions

1003

Available Resources:

Intranet

Intranet

rubble

emerald

1005

Error connecting to PSCI

01/31/97

17:06:35

10

1001

1101

EV1 for Windows NT

Apply 1213 X Cui Copy Paste Find Select All Sort Sort Expand All Collapse All

1209 X Delete Properties

Alert log

Emergency

Resource Sets

Policy

Smart Filter

Reports

911 Main

User Groups

Servers:

1203

Administrative User Groups: Administrators

Authentication

Virus

Server

Communication

Miscellaneous

Failed Authentication

Invalid ID

Wrong Password or Smart Card Response

Invalid Certificate

Denied Access

Deny Policy

Both Allow and Deny Policy

No Policy

Severity

High

Medium

Low

Apply

Ed: Default Values

1205

Choose a tab for details

Options

Distribution

Use Default

Copy To Default

Ready

01/31/97 18:46:01

1201

1207

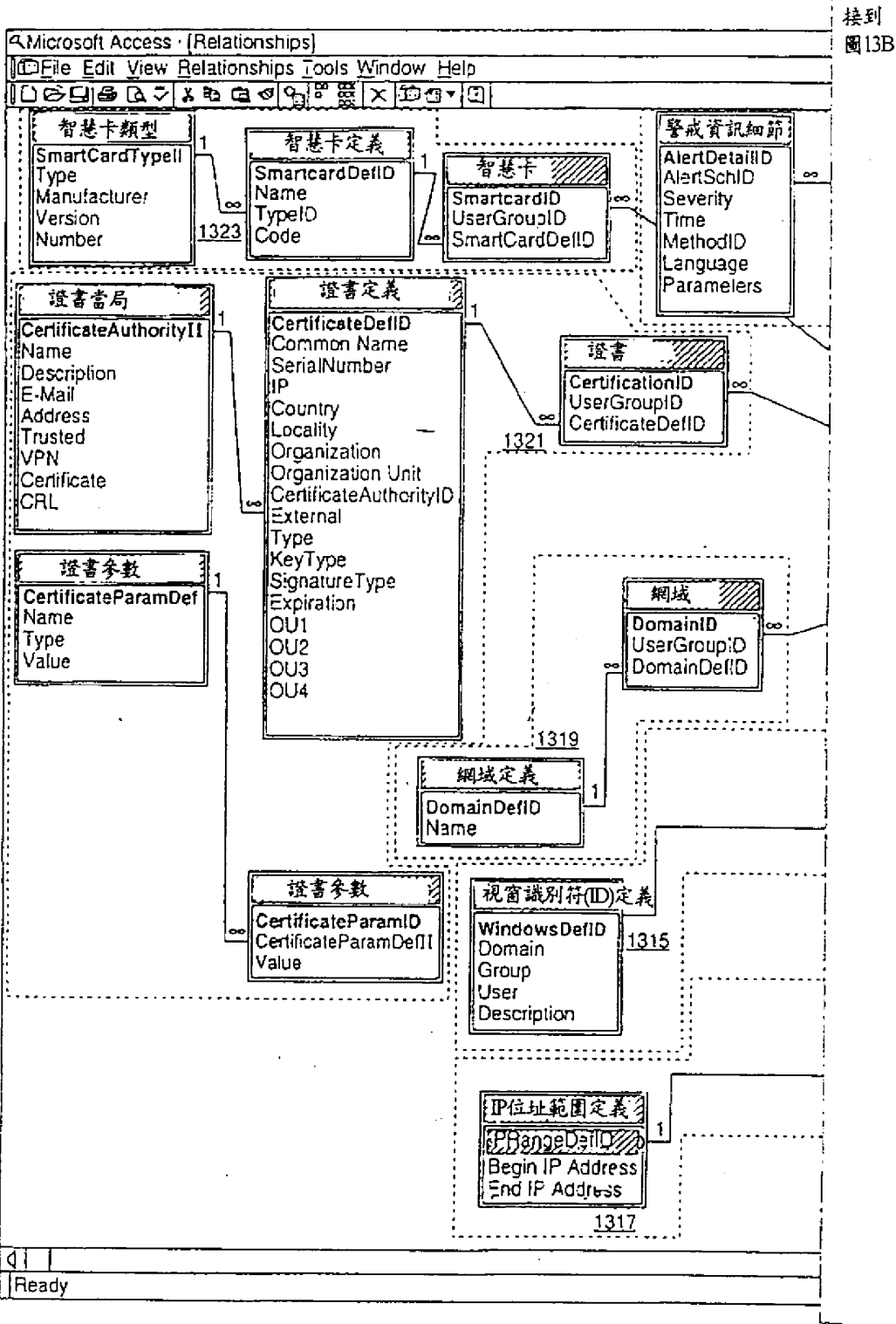


圖 13A

來自
圖 13A:

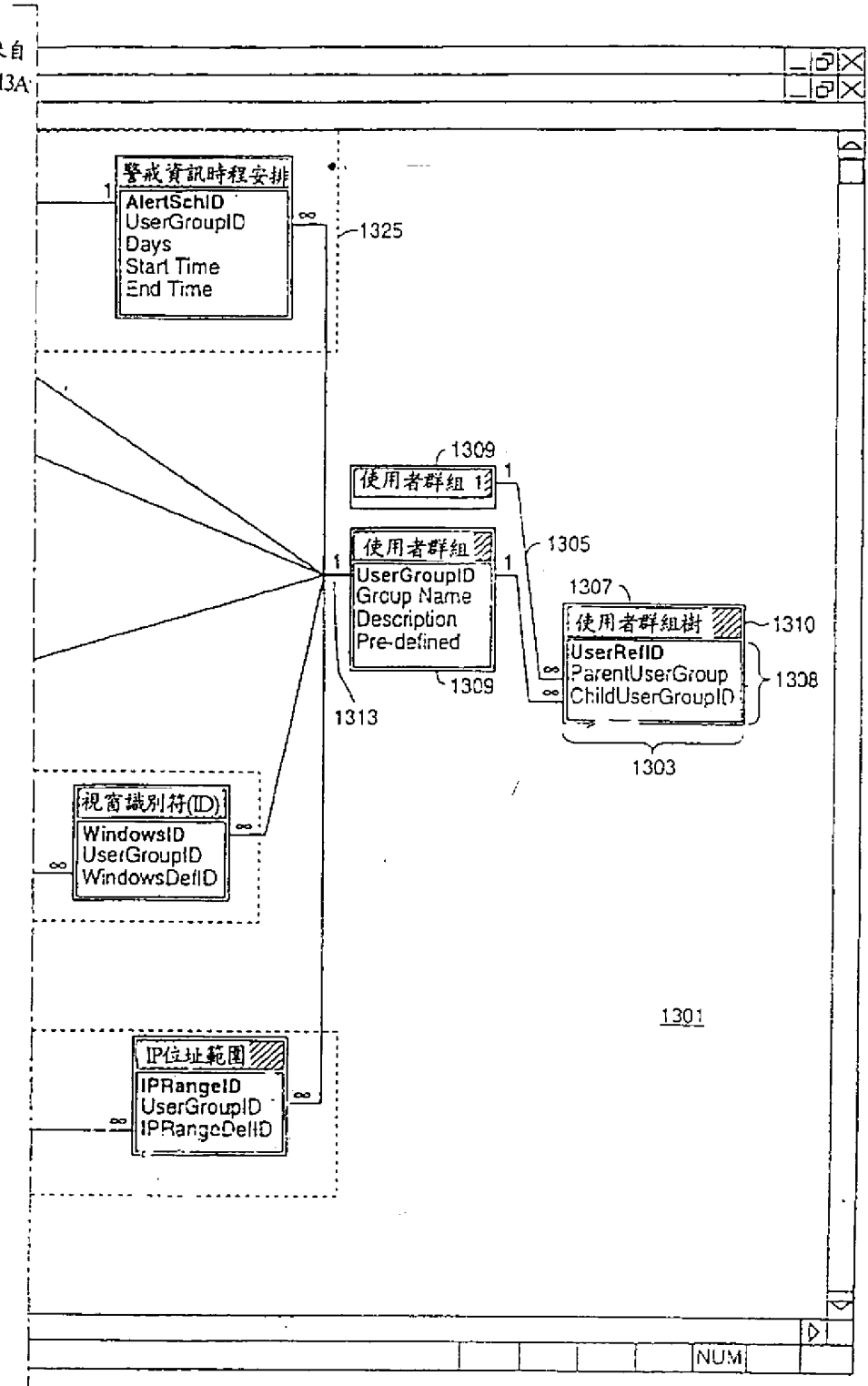
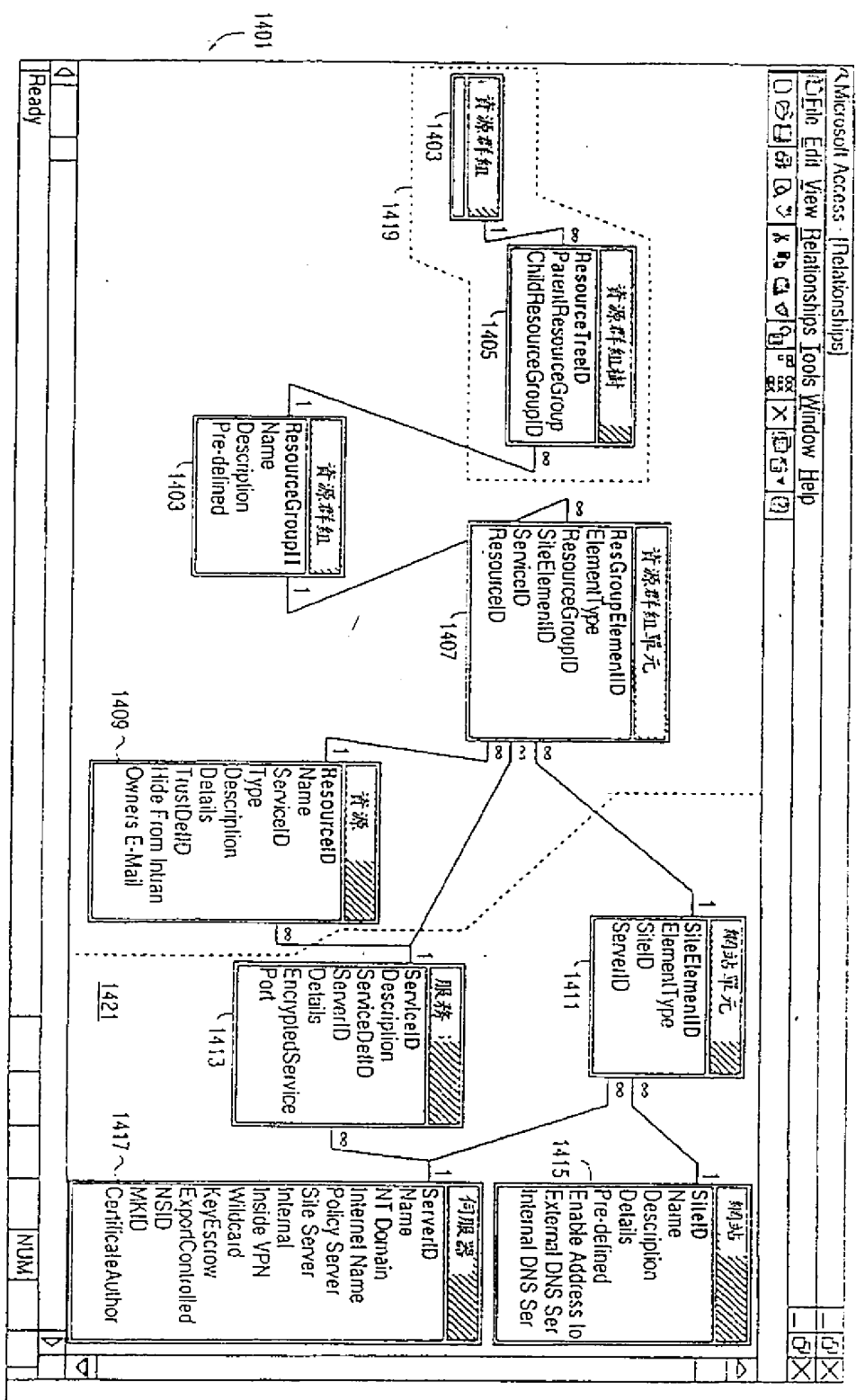


圖 13B



14

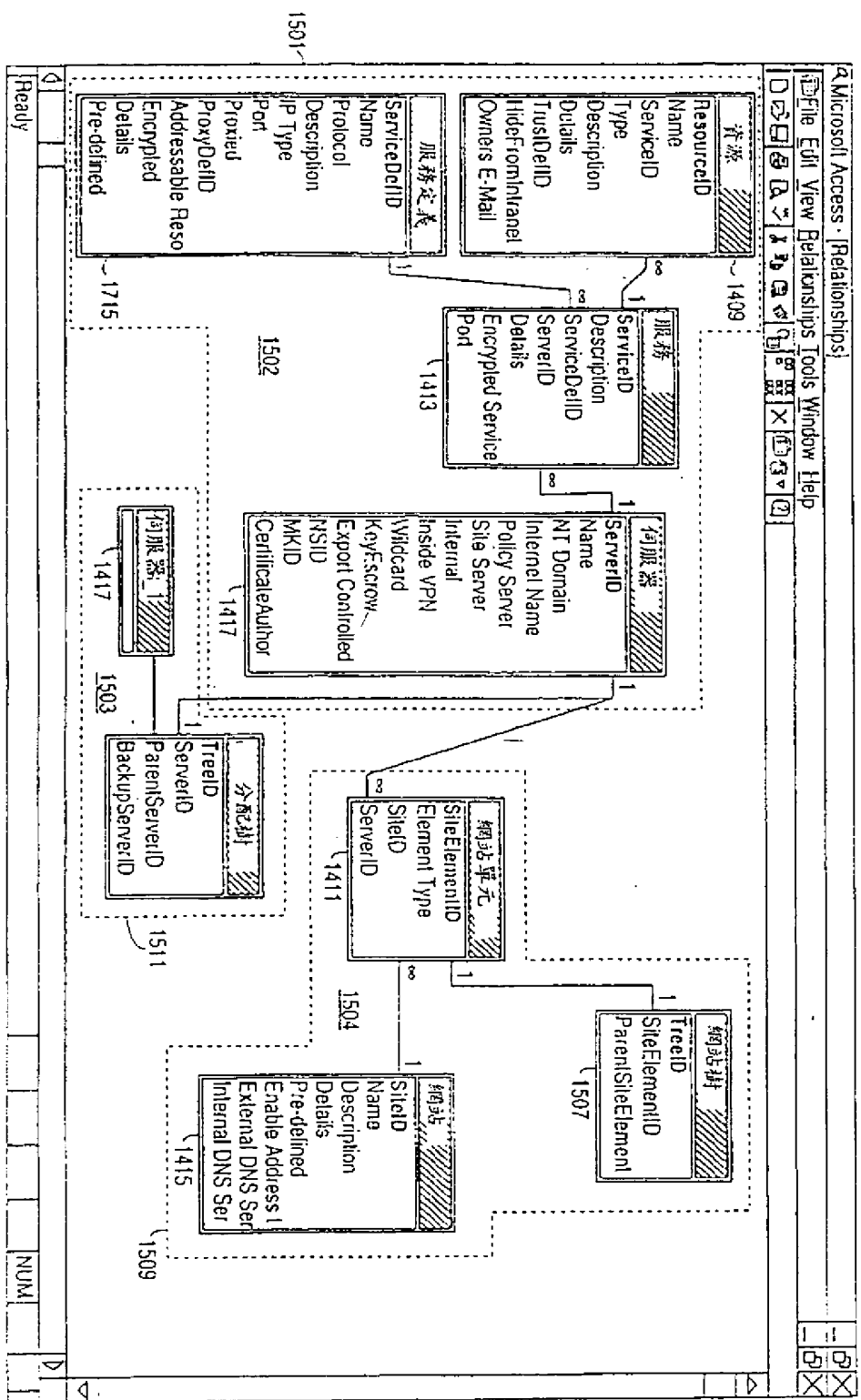
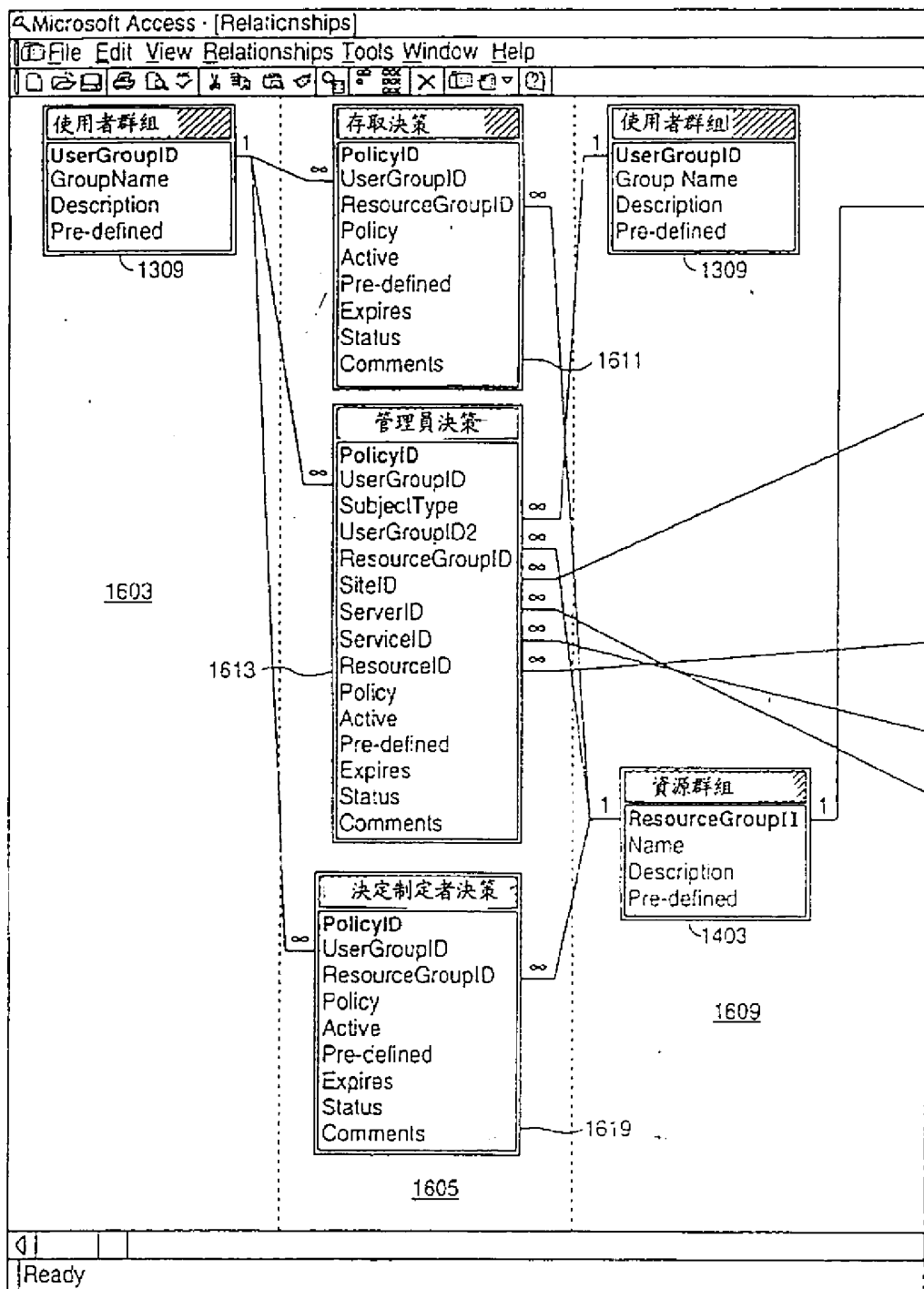


圖 15



接到
圖16B

圖 16A

來自
圖 16A

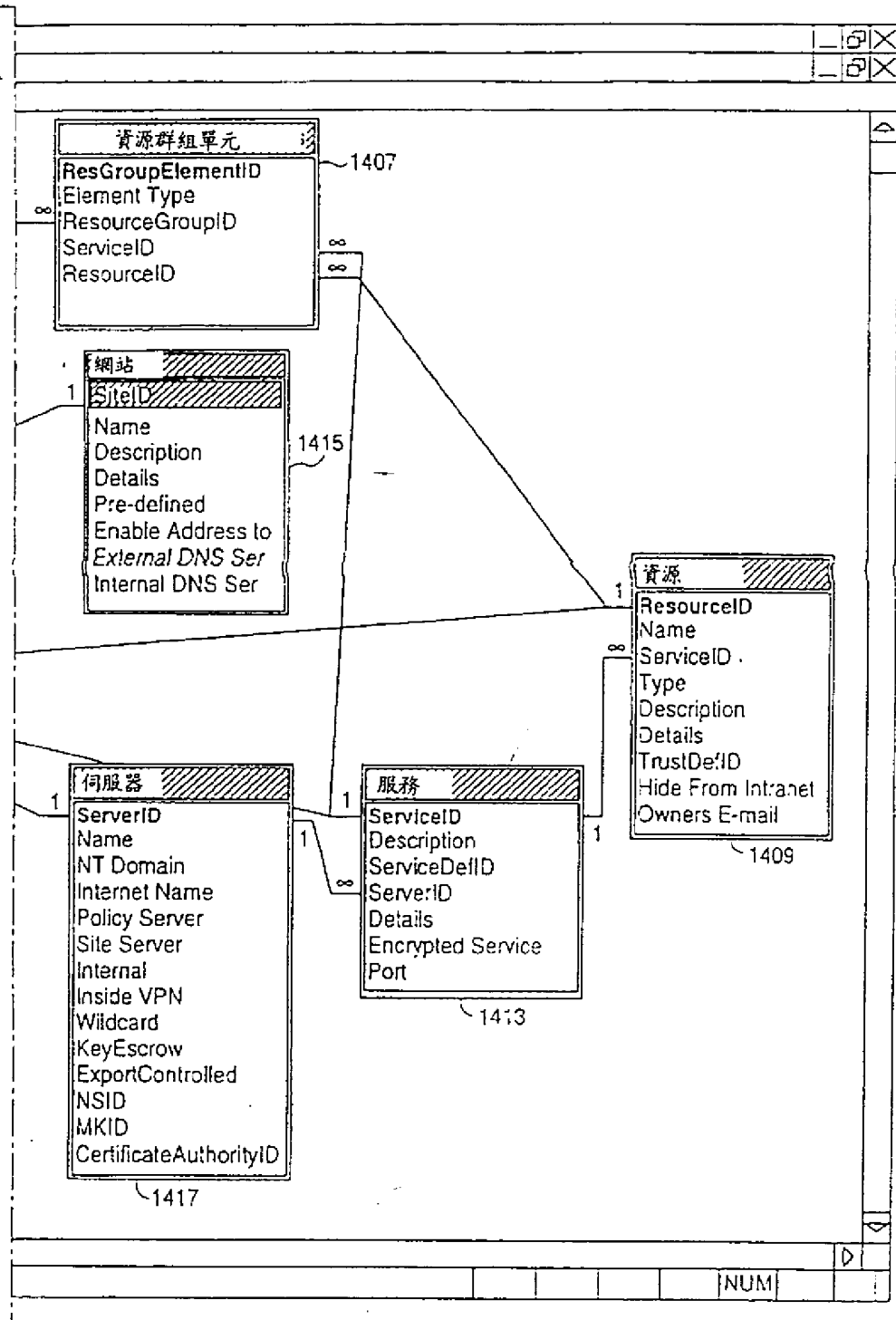
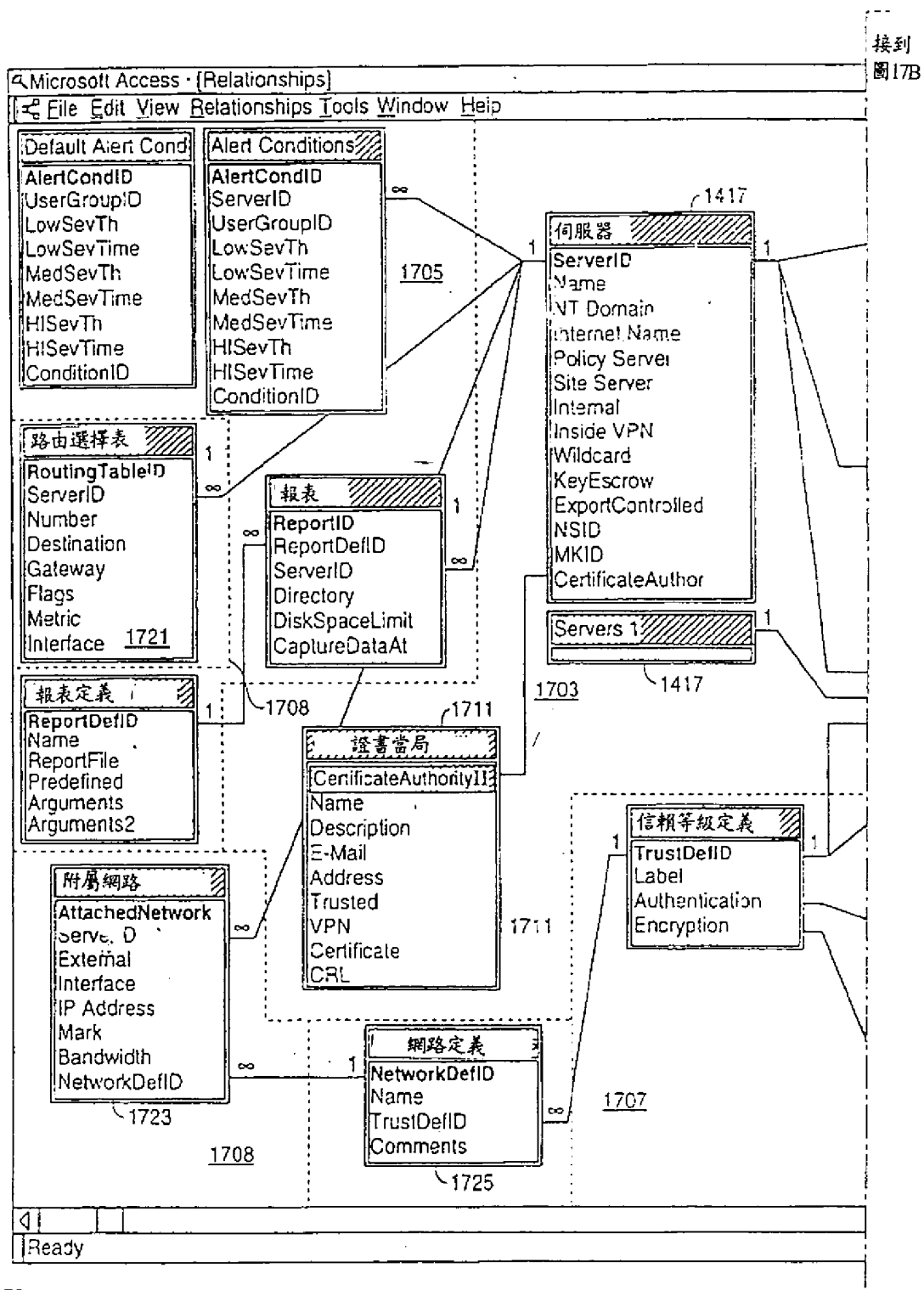


圖 16B



接到
圖17B

來自
圖 17A

接到
圖 17C

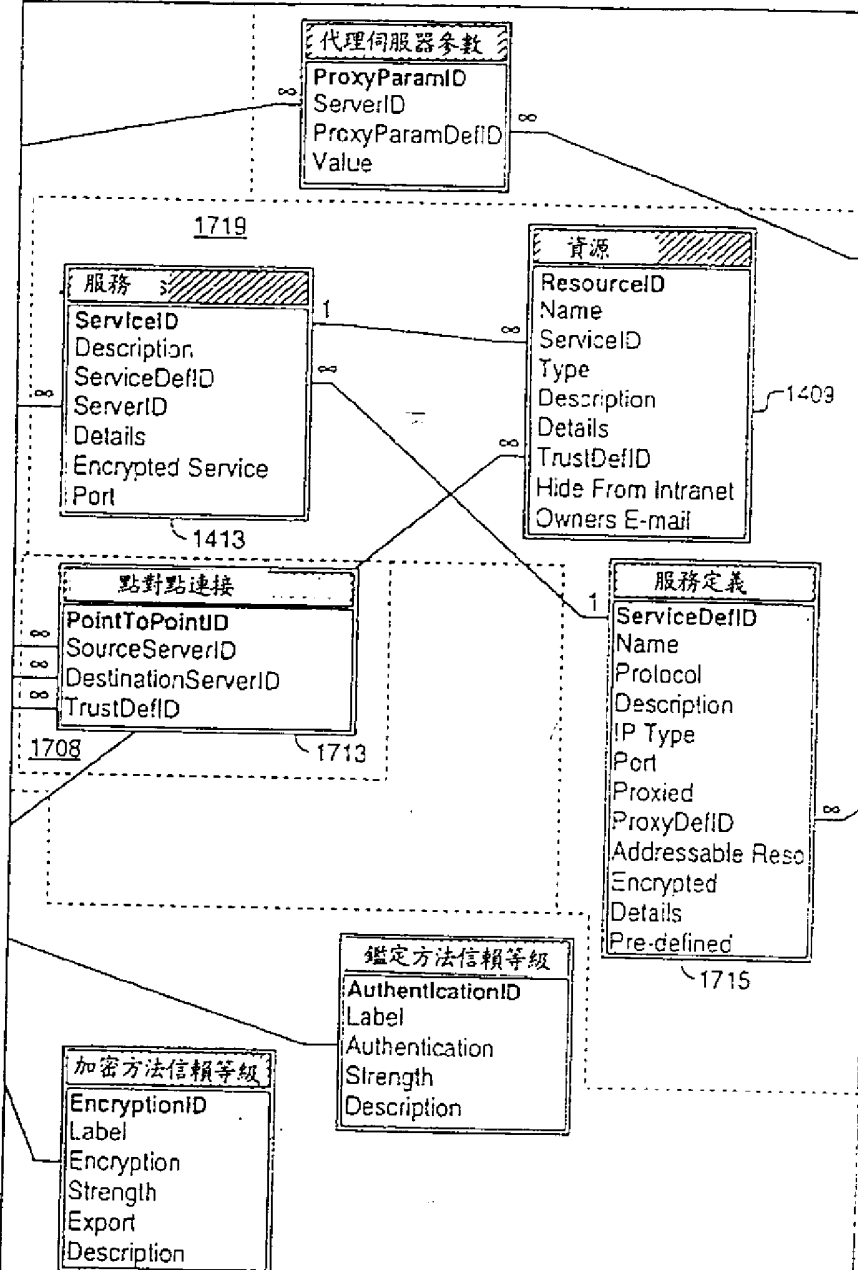


圖 17B

來自
圖17B

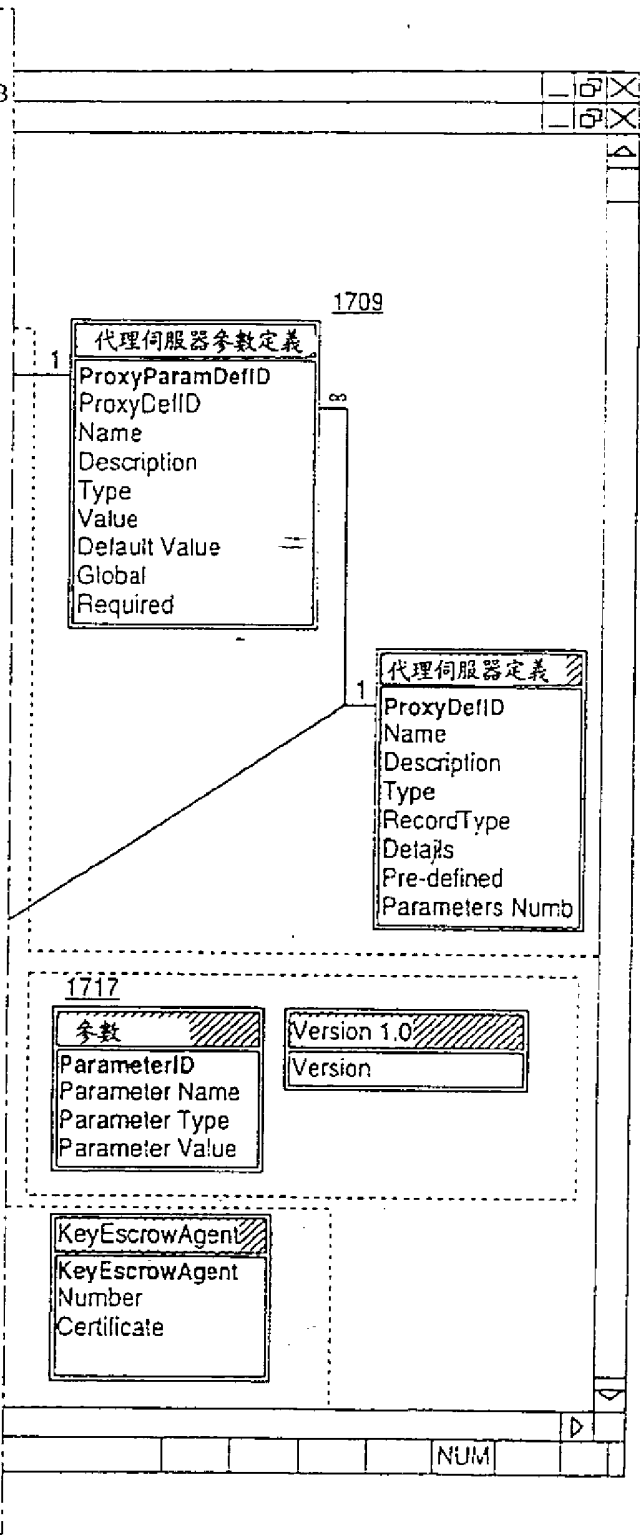


圖 17C

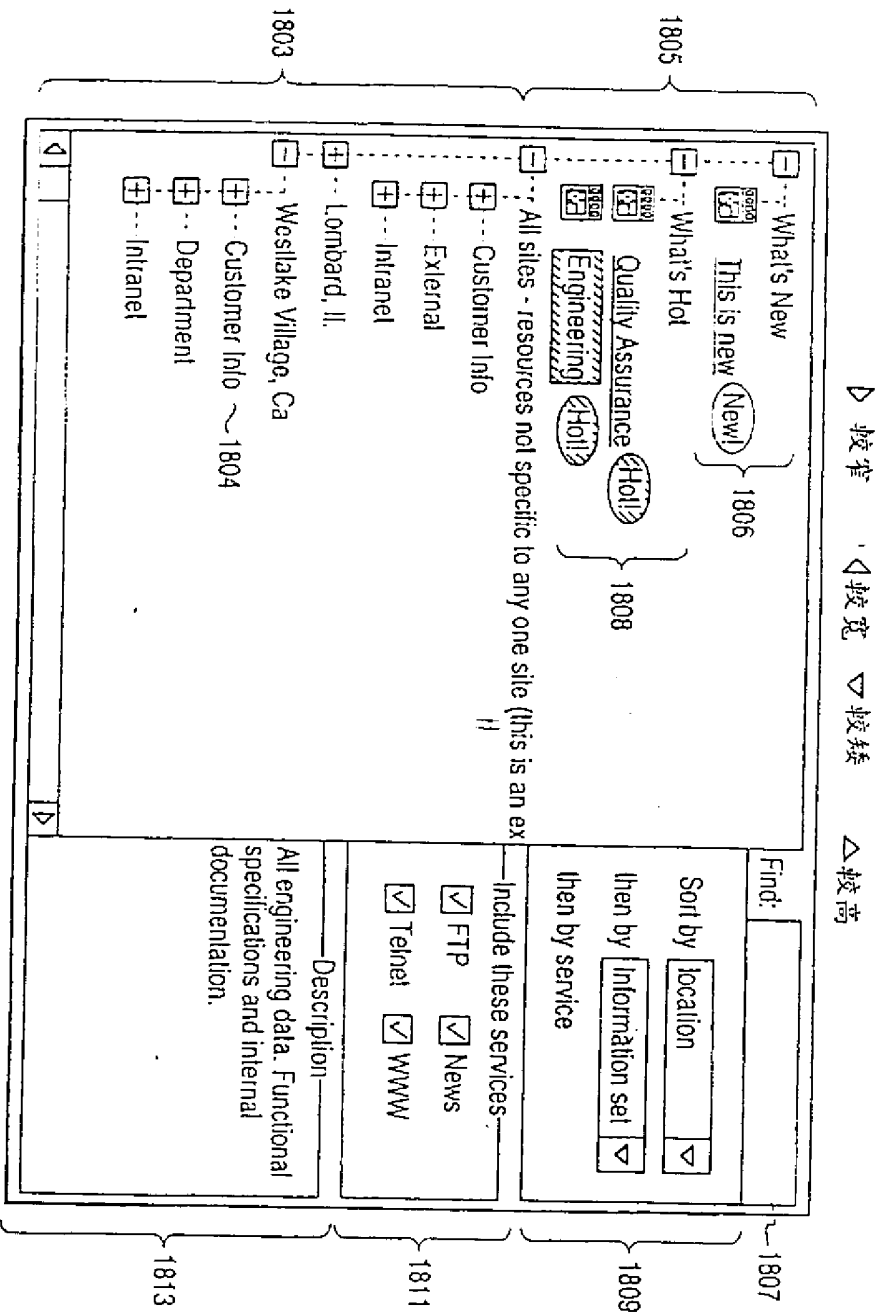


图 18

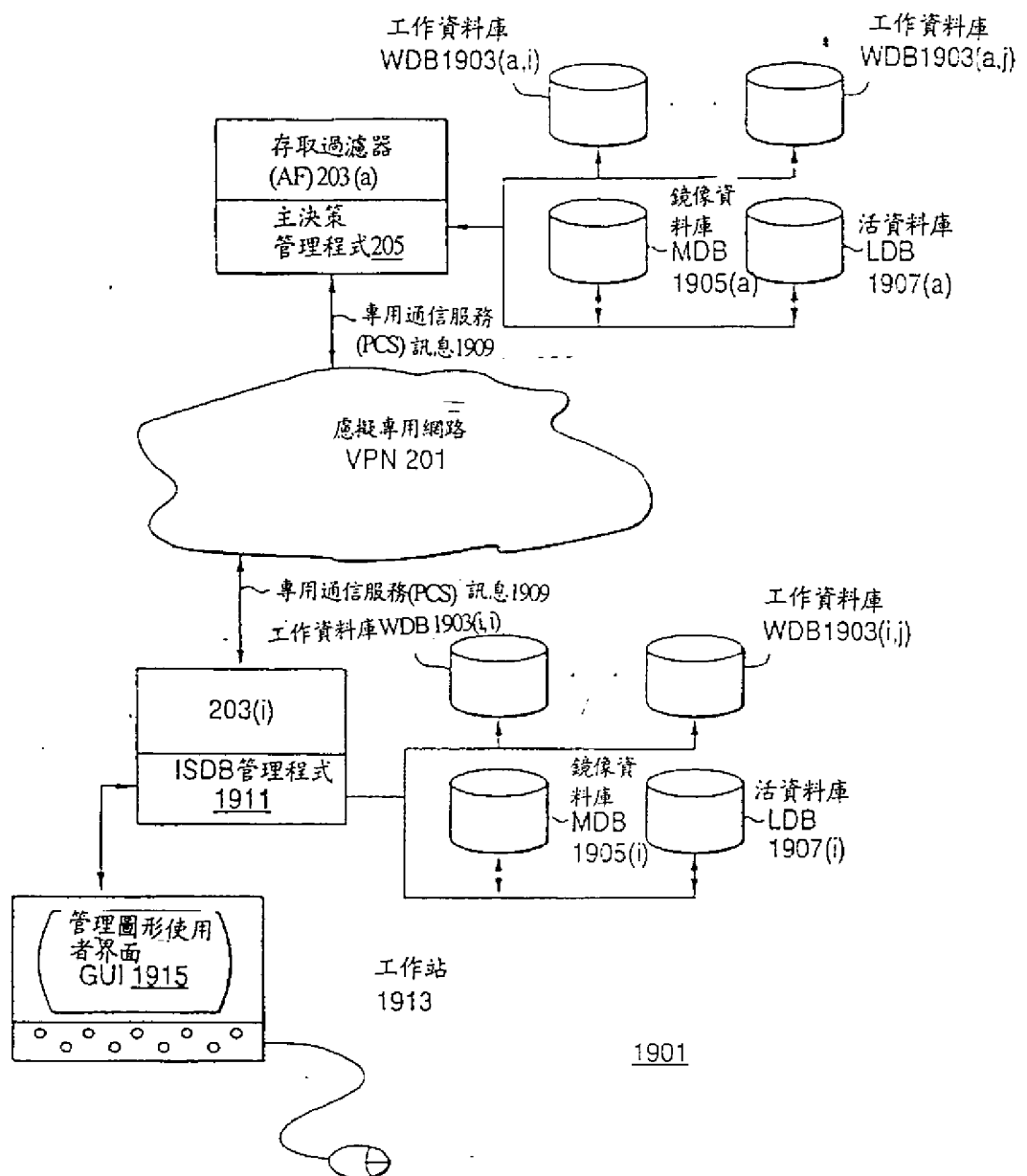


圖 19

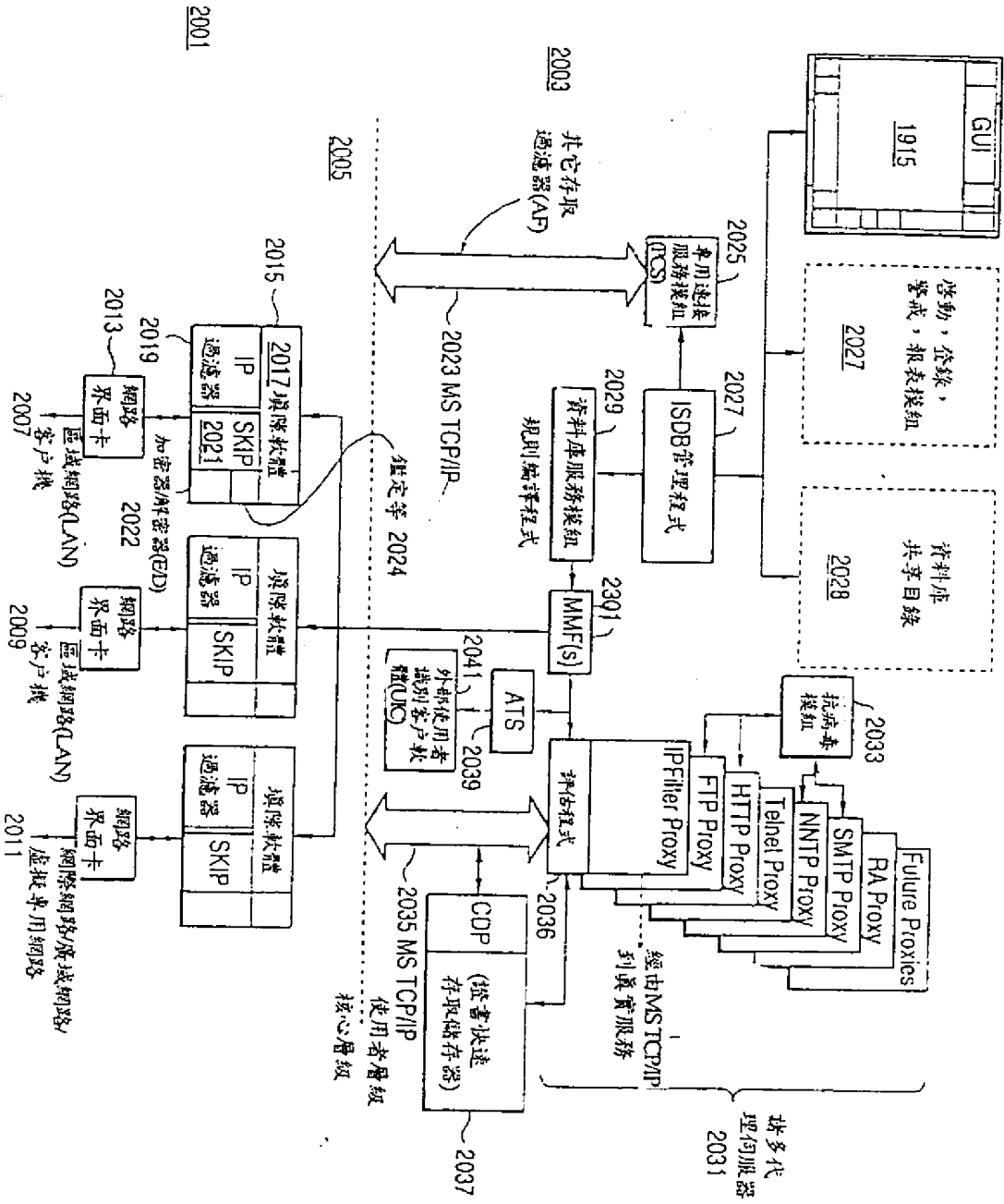
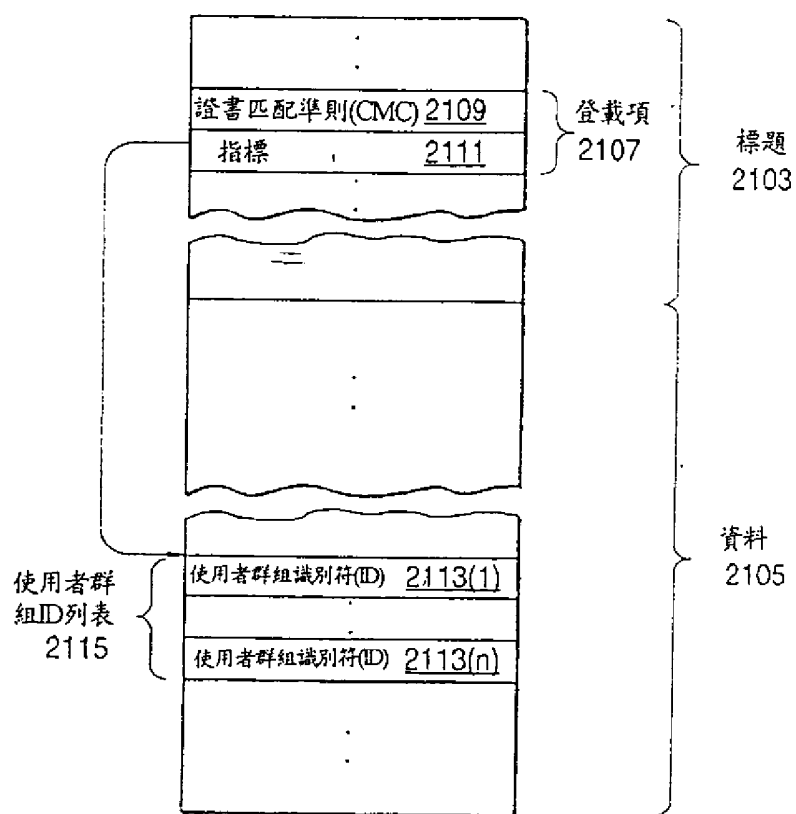


圖 20



"藉由使用者群組來識別的資料庫證書"檔案

2303

圖 21

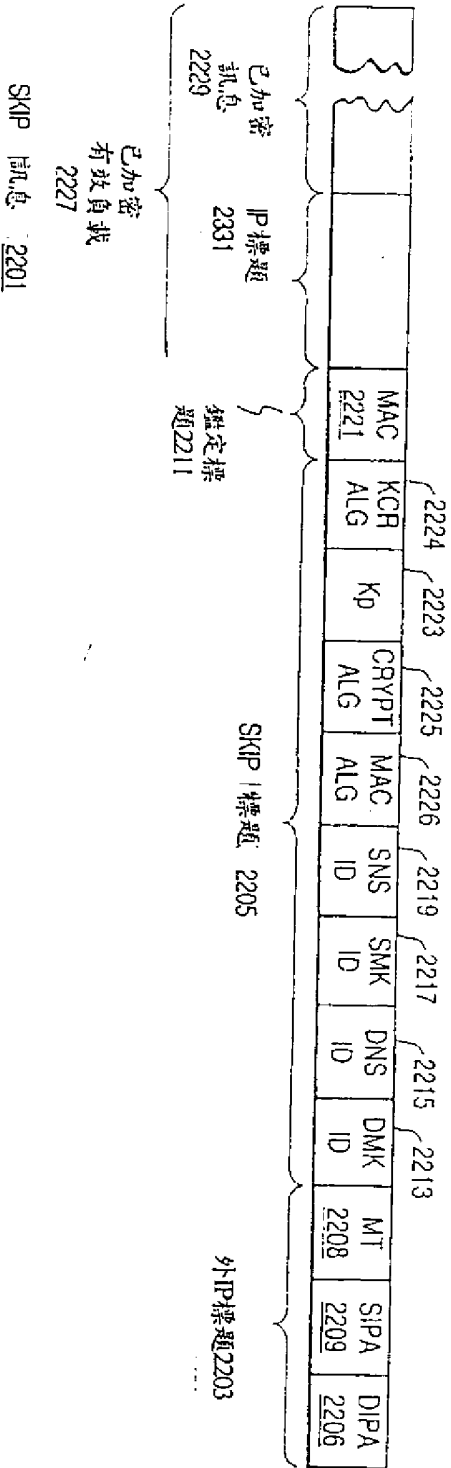


圖 22

MMF檔案名稱	內容
	Policies, User Groups, and Information Sets <u>2303</u>
DBUsersFile <u>2307</u>	Describes policy application from the User Group viewpoint. Maps each DB UserGroupID to a list of ResourceGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBUsersTreeFile	Describes the user groups tree as a flattened array. Maps each DB UserGroup ID to a list of UserGroupIDs for parent user groups.
DBResourcesFile <u>2309</u>	Describes policy application from the Resource Group (information set) viewpoint. Maps each DB ResourceGroupID to a list of UserGroupIDs with flags that indicate whether the policy that relates each pair is an allow or deny policy.
DBResourcesTreeFile	Describes the resource groups tree as a flattened array. Maps each DB ResourceGroupID to a list of ResourceGroupIDs for parent information sets.
	User Identification Information <u>2311</u>
DBIPRangesFile	IP Ranges data. Maps from IPRangeDefID to the IP range data.
DBDomainsFile	IP Domain data. Maps from DomainDefID to the IP domain data.
DBCertificatesFile	Certificate data. Maps from CertificateDefID to the certificate data.
DBWindowsIDFile	Windows ID data. Maps from WindowDefID to the windows ID data.
DBSmartCardIDFile	Smart card (authentication token) data. Maps from Smartcard-DefID to the authentication token data.
DBIPRangesByUserGroup File	Relates IP range matching criteria to user groups. Maps from IP Range data to UserGroupIDs.
DBDomainsByUserGroup File	Relates IP domain matching criteria to user groups. Maps from IP Domain data to UserGroupIDs.
DBCertificatesByUserGroup File	Relates certificates to user groups. Maps from certificate data to UserGroupIDs. <u>2101</u>
DBWindowsIDByUserGroup File	Relates Windows IDs to user groups. Maps from Windows ID data to UserGroupIDs.
DBSmartCardIDByUser GroupFile	Relates Smart Card (authentication token) data to user groups. Maps from authentication token data to UserGroupIDs.

2301

圖 23 A

MMF檔案名稱	內容
	Servers, Services, and Information Resources 2313
DBResourcesByServerIDFile	Relates servers to resources. Maps from ServerIDs to ResourceIDs for resources held on the server identified by the ServerID.
DBResourcesByServiceIDFile	Relates services to resources. Maps from ServiceIDs to ResourceIDs for resources belonging to the service identified by the ServiceID.
DBResourceIDByServiceIDFile	Relates services to their information resources. Maps from ServiceID to ResourceID.
DBResourceIDByNameFile 2315	Relates the IP names (URLs) of resources to resource IDs. Maps from URL to resource ID.
DBResourcesByResourceIDFile 2317	Relates resources to information sets. Maps ResourceID to Resource GroupIDs.
	Servers, Services, IP Information, and Proxies 2319
DBServerIDByIPFile	Relates IP addresses to servers. Maps IP addresses to ServerIDs.
DBServerIDByNameFile	Relates IP names to servers. Maps the IP FQDN (fully qualified domain name) for each server to its ServerID.
DBIPAndTypeByServerIDFile	Relates servers to their locations inside or outside to the VPN. Maps ServerID to the server's IP address and a flag indicating whether the address is inside or outside the VPN.
DBServiceIDByPortFile	Relates services to their port numbers. Maps from ServiceID to port number.
DBServiceIDByServerIDFile	Relates servers to ports for services. Maps from ServerID to a list of port numbers.
DBServicePortToProxyPortFile	Relates service ports to the ports for their proxies. Maps from service port number to proxy port number.
DBProxyIDByServerIDFile	Relates servers to service proxies. Maps from ServerID to ProxyDefID.
DBProxyParametersFile	Relates proxies to configuration data for the proxies. Maps from ProxyDefID to options data

2301

圖 23 B

MMF 檔案名稱	內容
	Access Filter Information <u>2321</u>
DBAttachedNetworksByIPFile	Relates network interfaces in the access filters to information for the interfaces. Maps from the interface's IP address to interface information.
DBAttachedNetworksByServerIDFile	Relates access filters to their network interfaces. Maps from ServerID for the access filter to interface information.
DBRoutingTableFile	Describes the IP routing information for all of the access filters. One block of information.
DBRoutingTableByServerIDFile	Relates access filters to their IP routing information. Maps from ServerID for the access filter to IP routing information.
DBPointToPointFile	Relates a point-to-point description of a network path to data for the path. Maps from PointToPointID for the path to the associated data.
	SEND Information <u>2323</u>
DBTrustTableFile <u>2325</u>	Implements the SEND table. Maps from TrustDefID, indicating a trust level, to AuthenticationIDs for user identification techniques and EncryptionIDs for encryption techniques.
DBCertificateAuthoritiesFile	Relates identifiers for certificate authorities to their data. Maps from CertificateAuthorityID to associated data.
DBTrustAuthenticationsFile	Relates AuthenticationIDs to information about identification techniques. Maps from AuthenticationID to identification technique information.
DBTrustEncryptionsFile	Relates EncryptionIDs to information about encryption techniques. Maps from EncryptionID to encryption type and strength information.
	IntraMap Information <u>2422</u>
DBJavaSiteTable	Maps from names of locations to LocationIDs.
DBJavaResourceTable	Maps from URLs of resources to their ResourceIDs, LocationIDs, and hidden flags.
DBJavaResourcesSetTable	Maps from names of information sets to ResourceGroupIDs, a list of ResourceIDs for all resources contained in the information set, and a list of ResourceGroupIDs for all of the information set's parents.

2301

圖 23 C

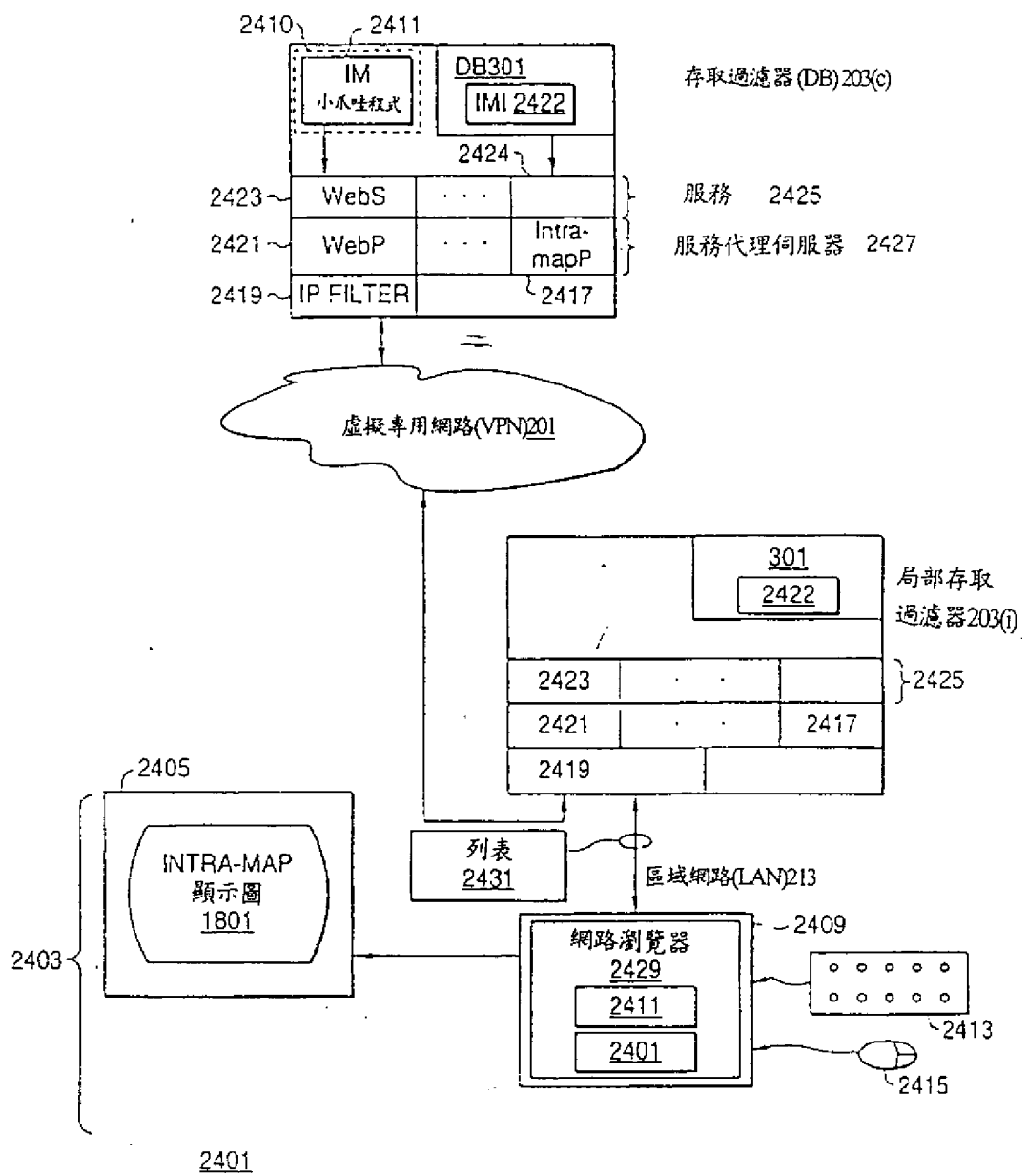


圖 24

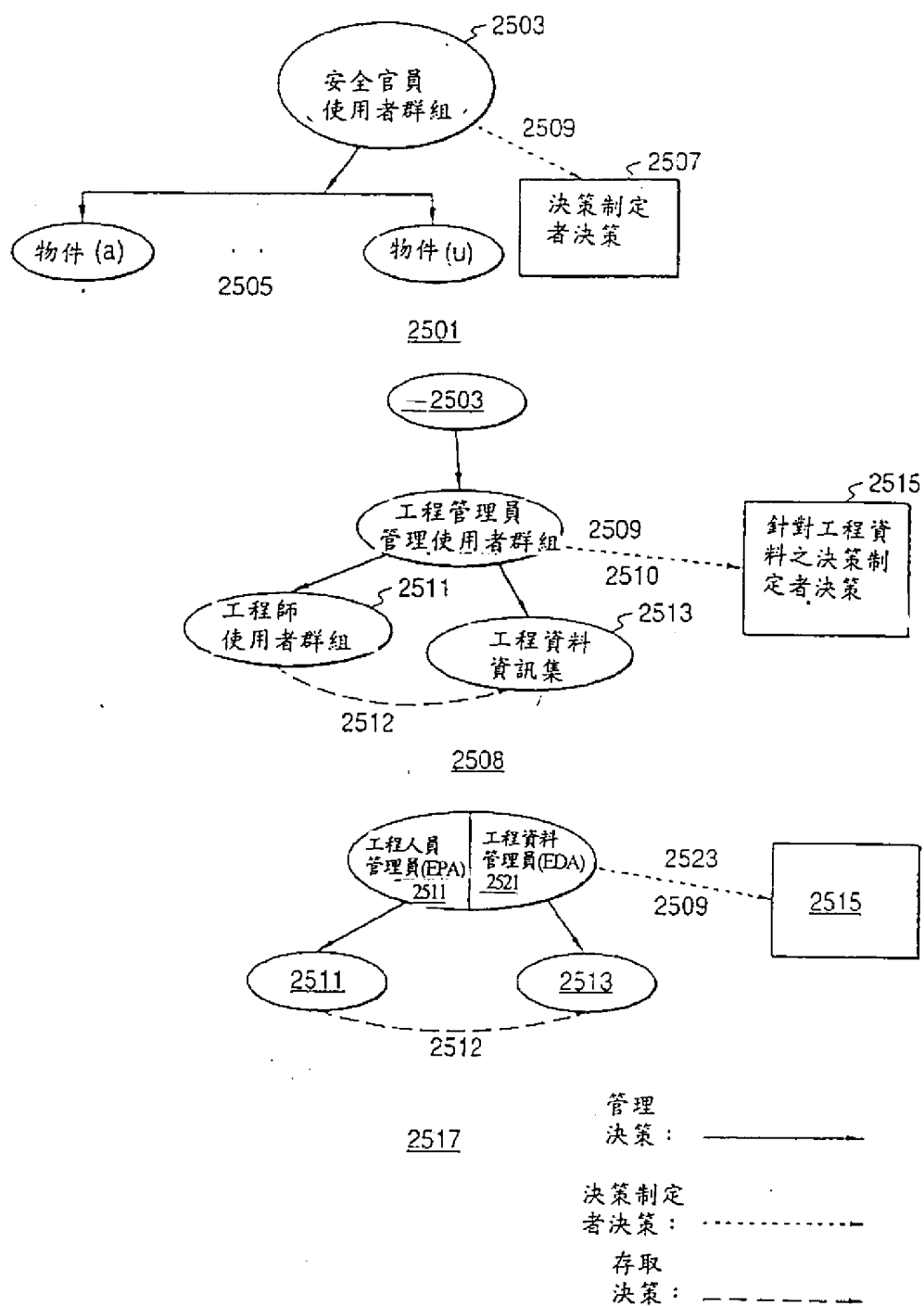


圖 25

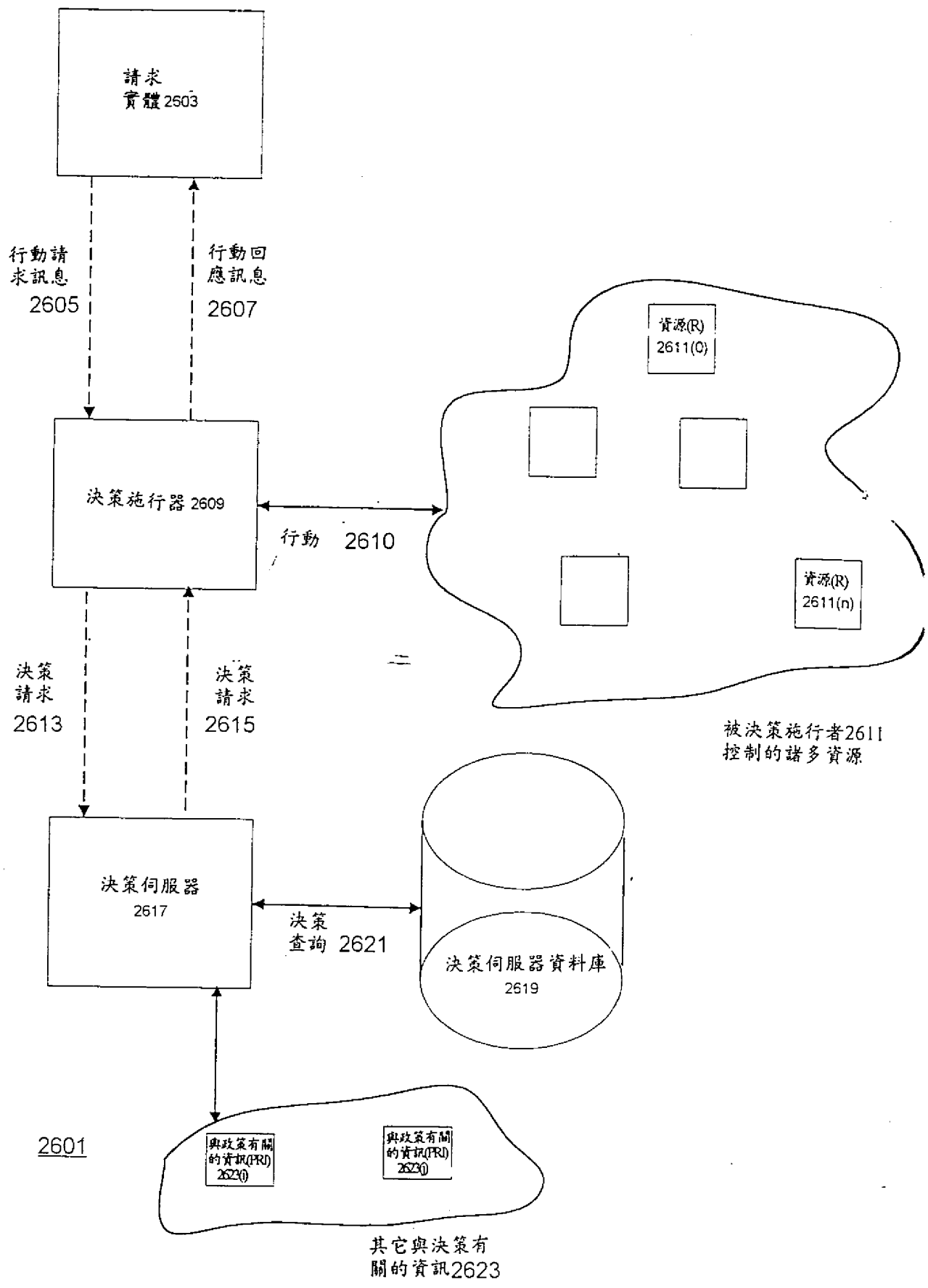


圖 26

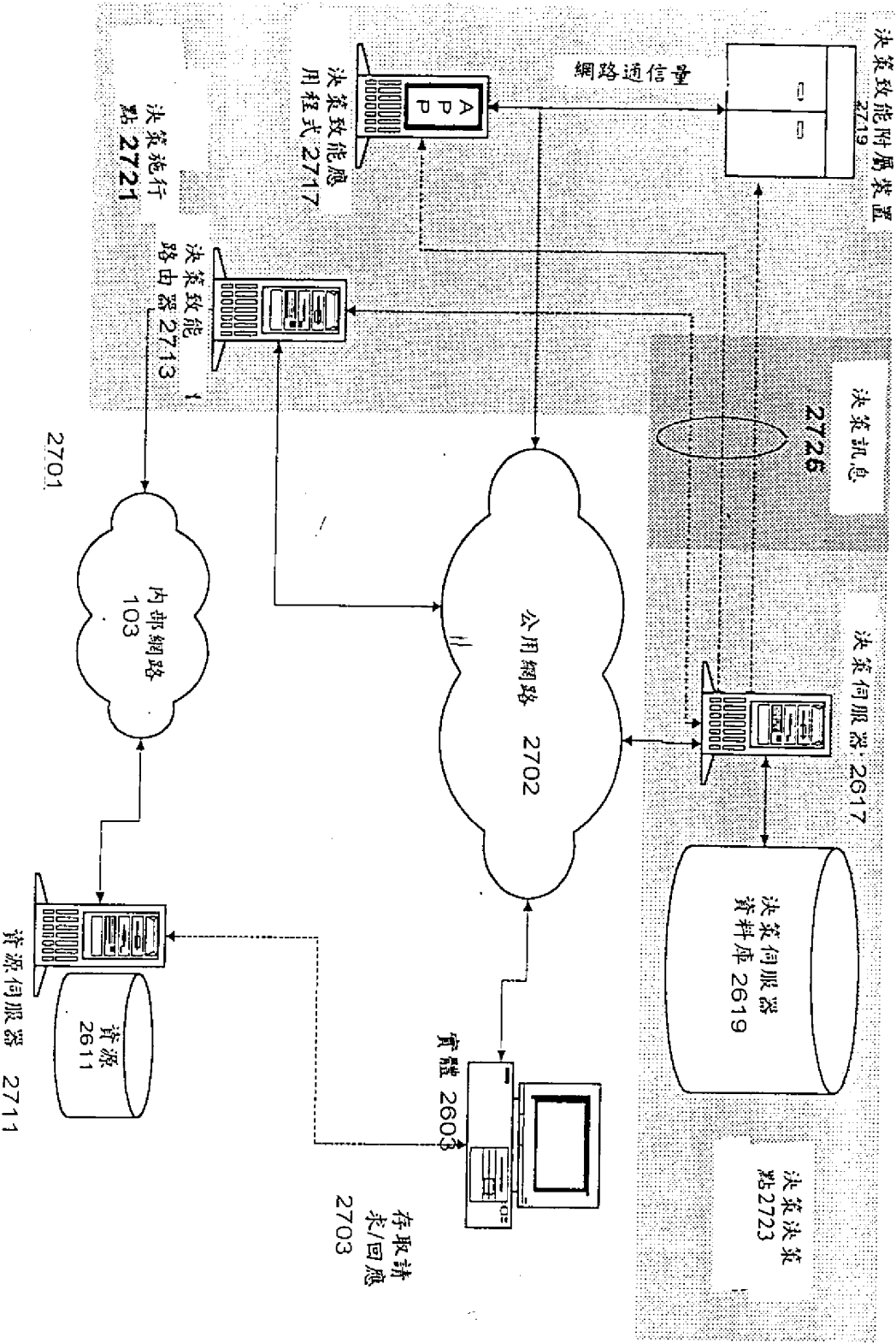
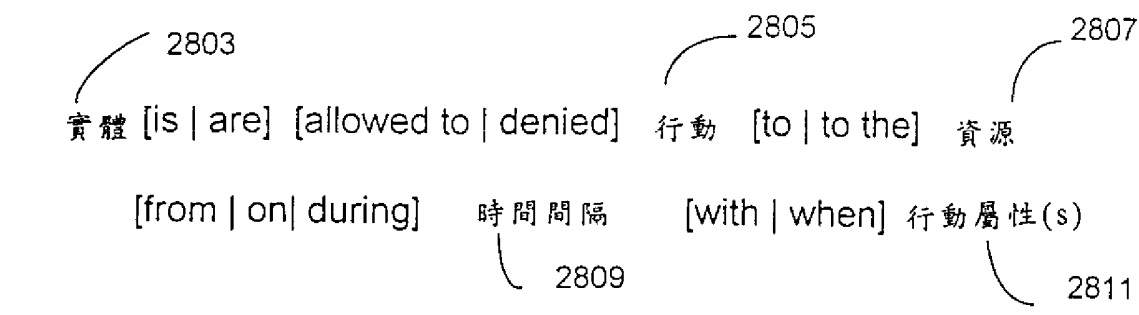


圖 27



2801

圖 28

決策資訊 303

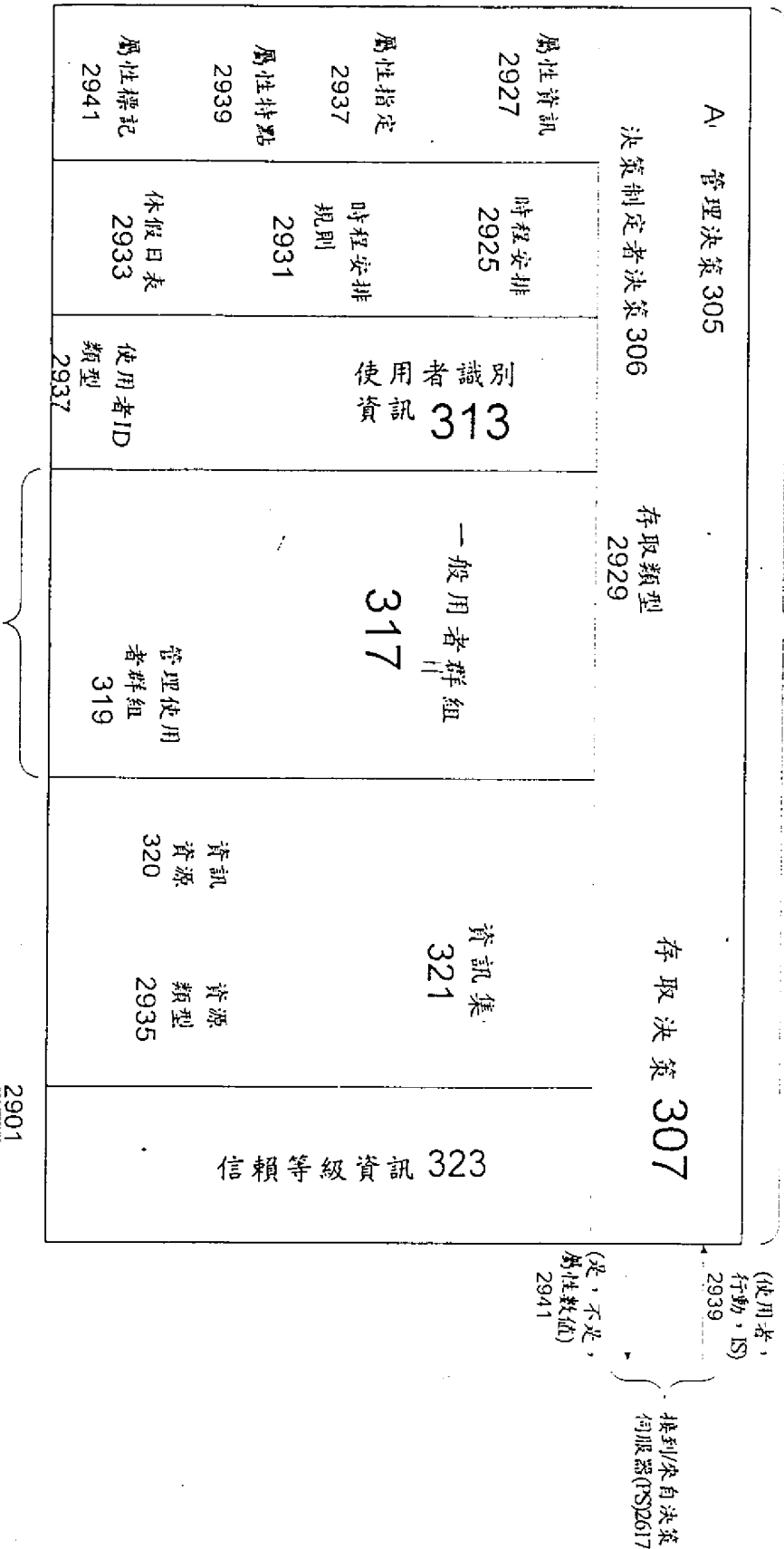
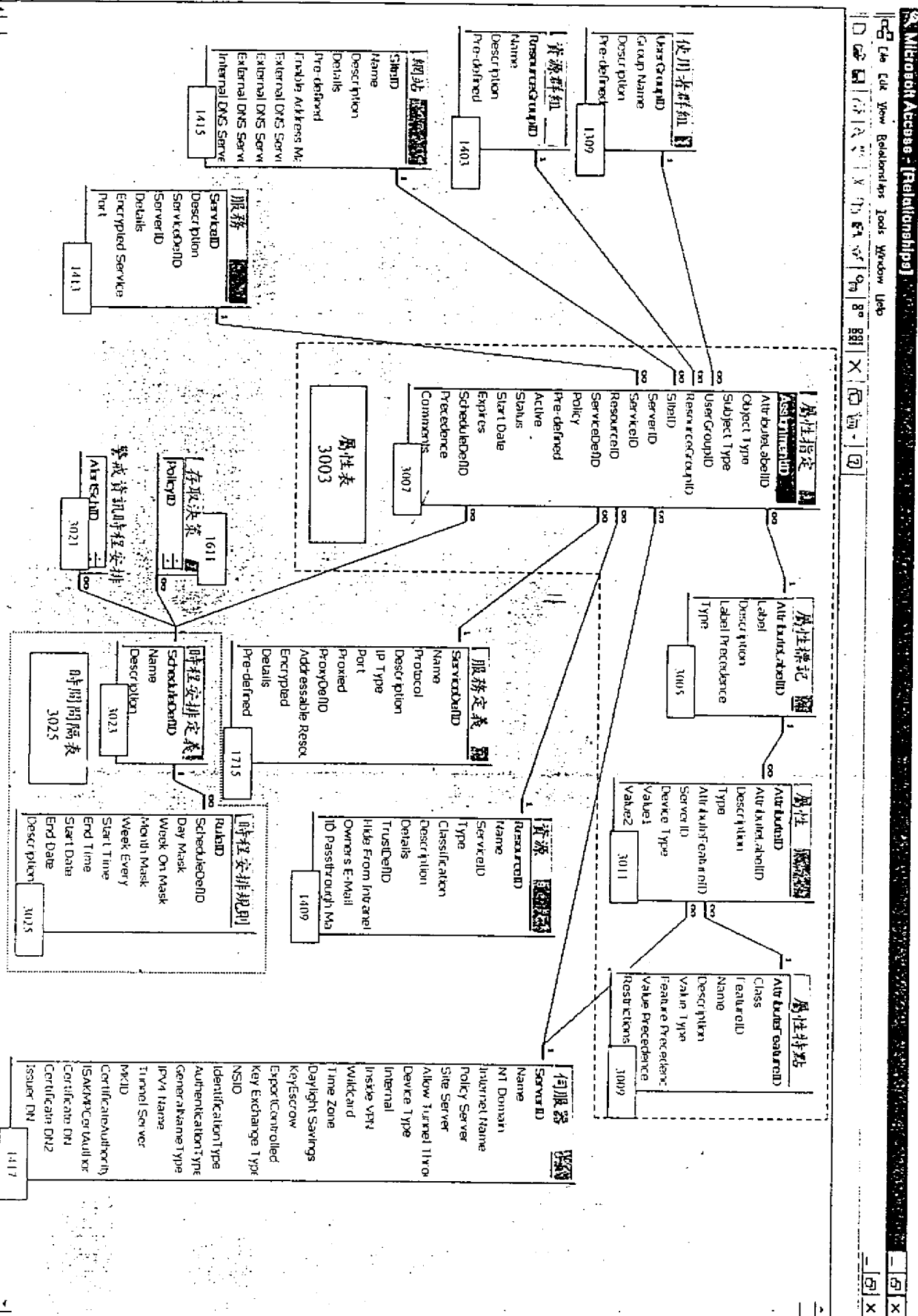


圖 29



Conclave Administrator - abola

Apply Auth Search Copy Paste Find Select Add Edit Expand Collapse Options Exit Help

+ New X Delete Properties

Main User Groups Information Sets Policies Schedules QoS Access Filters Reports Alert Viewer

Schedules: -

- Business Hours 3105
 - 5:00 PM-9:00 AM, Days: MTWTF--
 - Days: S---SH
- Weekends & Holidays
- Workdays - Day Shift
- Workdays - Graveyard Shift
- Workdays - Swing Shift

Rules:

Times Active	Days Active	Weeks Active	Months Active	Description
1:00 AM-9:00 AM	-MTWTF--X	All	All year	Mon-Fri 1am-9am
5:00 PM-1:00 AM	-MTWTF--	All	All year	Mon-Fri 5pm-1am
5:00 PM-9:00 AM	-MTWTF--	All	All year	Mon-Fri 5pm-9am
9:00 AM-5:00 PM	-MTWTF--X	All	All year	Mon-Fri 9am-5pm
All day	S---SH	All	All year	Weekends & Holidays

3103

3111

3107

3109

3106

圖 31

448387

Schedule Rule [X]

Schedule Valid

☐ All day

☒ Starts: 5:00 PM Ends: 9:00 AM

On selected days of week:

☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☐ Sa ☐ Su

☒ Weekdays ☐ Weekends

☐ Exclude Holidays ☐ Holidays

☒ Every week

☐ Every [] weeks starting on []

☐ On selected week of month:

☐ 1st ☐ 2nd ☐ 3rd ☐ 4th ☐ Last

☐ All year

☐ On selected months:

☐ Jan ☐ Feb ☐ Mar ☐ Apr ☐ May ☐ Jun

☐ Jul ☐ Aug ☐ Sep ☐ Oct ☐ Nov ☐ Dec

Description: []

OK
Cancel
Holidays
Help
Advanced <<

3201

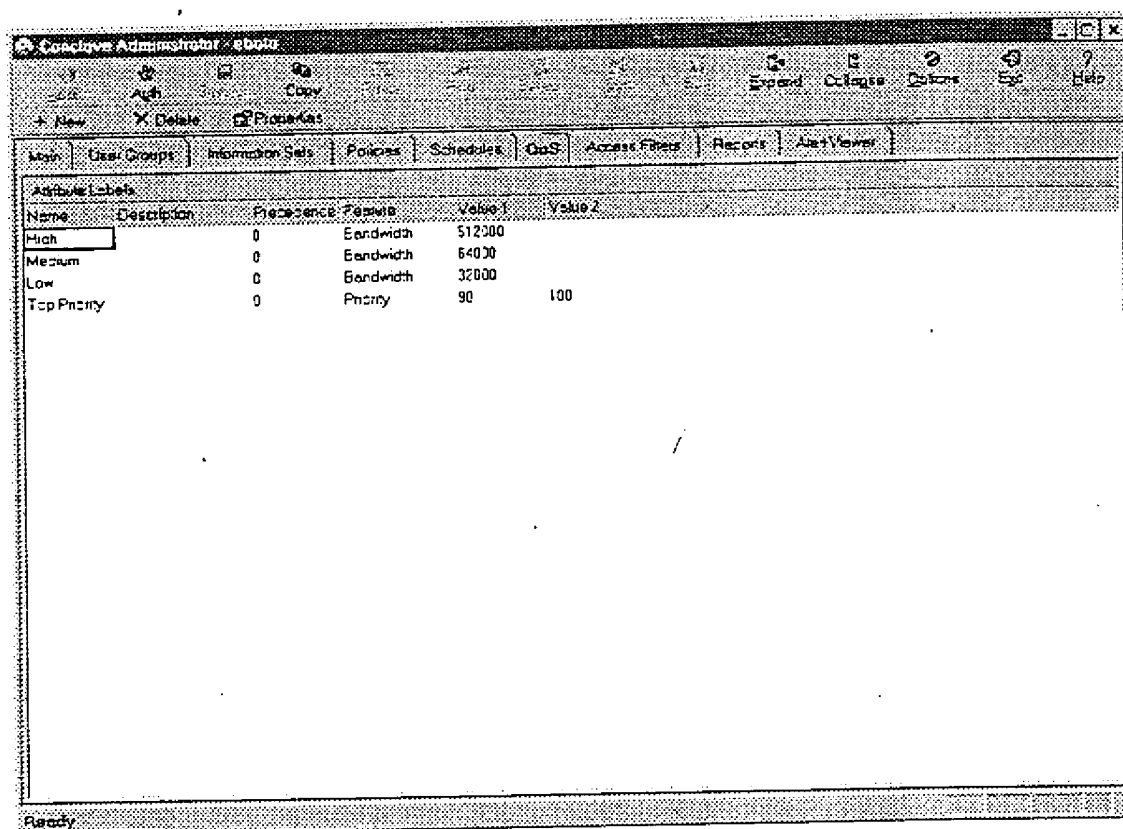
Policy Properties [X]

User Group	Corporate	OK
Information Set	Corporate	Cancel
Policy	State	Help
☒ Allow	☒ Active	
☐ Deny	☐ Inactive	
Comment:	Corporate access to corporate information	Advanced <<
Valid Between		
☐ Start Date		
☐ End Date		
Schedule Name:	Business Hours	Definition

3301

3305

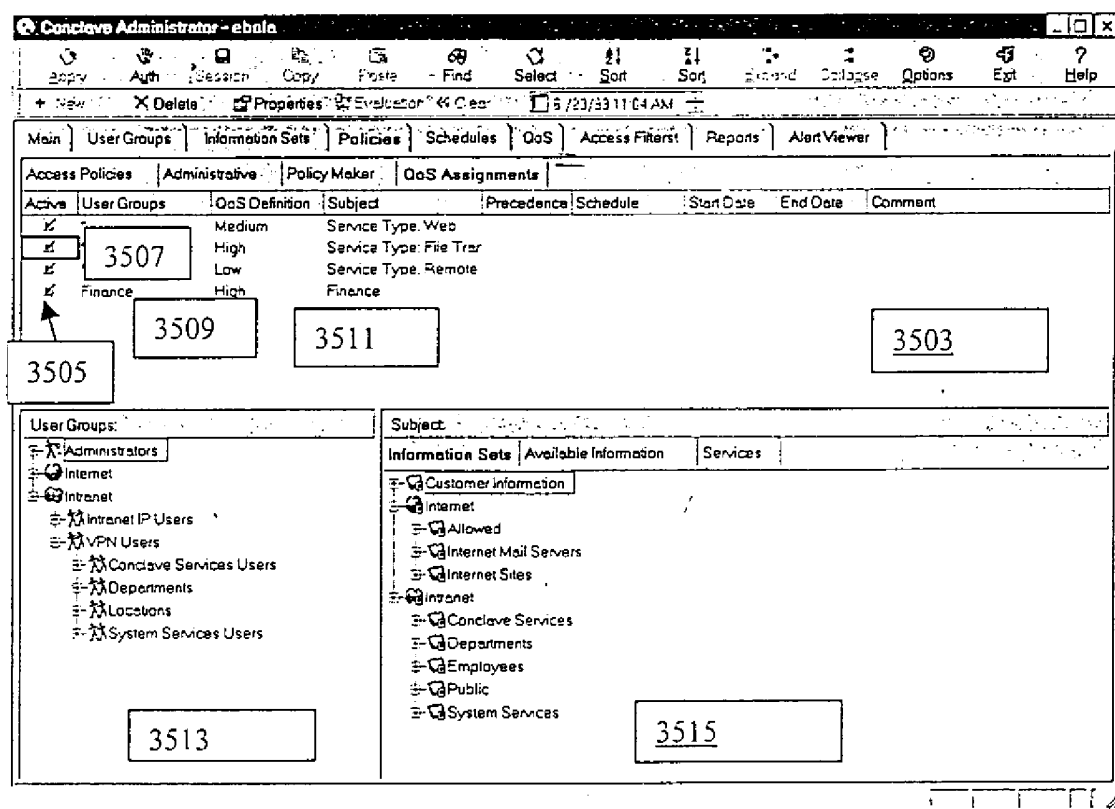
448387



3401

圖 34

448387



3501

圖 35

Attribute Label

Attribute Label: Medium

Description: Medium priority traffic

Label Precedence: 15

Associated Feature

Feature: Bandwidth

Value 1: 64000

Value 2:

Feature Properties

OK

Cancel

Help

3601

圖 36

