I874350

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I874350 B**

(45)公告日： 中華民國 114 (2025) 年 03 月 01 日

(21)申請案號：109102813　(22)申請日： 中華民國 109 (2020) 年 01 月 30 日

(51)Int. Cl.：　*H04L9/32　(2006.01)*　*H04L9/28　(2006.01)*

H04L67/00　(2022.01)

(30)優先權：2019/01/31　日本　2019-015232

(71)申請人：日商關連風科技股份有限公司 (日本) CONNECTFREE CORPORATION　(JP)

日本

(72)發明人：帝都　久利寿 TATE, KRISTOPHER ANDREW (US)

(74)代理人：洪澄文；洪茂

(56)參考文獻：

TW	201835784A	CN	101401360B
US	2003/0084293A1	US	2004/0103213A1
US	2009/0180489A1	US	2015/0372916A1

審查人員：葉昌倫

申請專利範圍項數：18 項　圖式數：19　共 63 頁

(54)名稱

資料傳送方法、通訊處理方法、通訊裝置以及通訊處理程式

(57)摘要

資料傳送方法，包括：複數裝置分別根據從各裝置具有的公開密鑰依照散列函數算出的散列值，決定各裝置的 IP 位址的步驟；複數裝置分別保持反映各裝置的連接關係之狀態資訊的同時，也傳送顯示狀態資訊內容的通知信息至其它裝置的步驟；複數裝置分別根據從其它裝置接收的通知信息，更新各裝置保持的狀態資訊的步驟；以及根據各裝置保持的狀態資訊邏輯性規定的裝置集合間，決定上述集合內包含的裝置間保持之資料傳送收件位址的裝置的搜尋中使用的路由表的步驟。

指定代表圖：

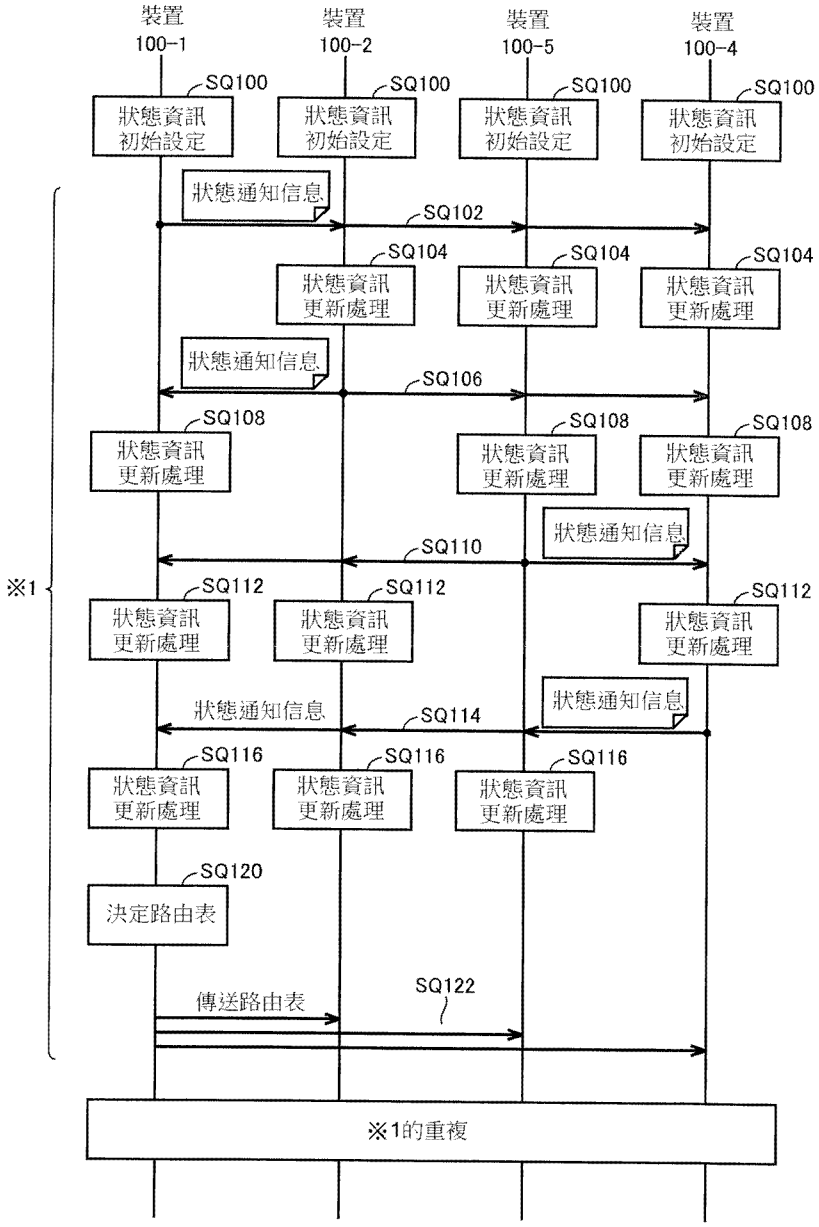


圖15

符號簡單說明：

SQ100:狀態資訊初始設定

SQ102:狀態通知信息

SQ104:狀態資訊更新處理

SQ106:狀態通知信息

SQ108:狀態資訊更新處理

SQ110:狀態通知信息

SQ112:狀態資訊更新處理

SQ114:狀態通知信息

SQ116:狀態資訊更新處理

SQ120:決定路由表

SQ122:傳送路由表

公告本

第 109102813 號
112 年 7 月 13 日修正替換本

I874350

【發明摘要】

【中文發明名稱】　資料傳送方法、通訊處理方法、通訊裝置以及通訊處理程式

【中文】

資料傳送方法，包括：複數裝置分別根據從各裝置具有的公開密鑰依照散列函數算出的散列值，決定各裝置的IP位址的步驟；複數裝置分別保持反映各裝置的連接關係之狀態資訊的同時，也傳送顯示狀態資訊內容的通知信息至其它裝置的步驟；複數裝置分別根據從其它裝置接收的通知信息，更新各裝置保持的狀態資訊的步驟；以及根據各裝置保持的狀態資訊邏輯性規定的裝置集合間，決定上述集合內包含的裝置間保持之資料傳送收件位址的裝置的搜尋中使用的路由表的步驟。

【指定代表圖】　圖15

【代表圖之符號簡單說明】

SQ100:狀態資訊初始設定

SQ102:狀態通知信息

SQ104:狀態資訊更新處理

SQ106:狀態通知信息

SQ108:狀態資訊更新處理

SQ110:狀態通知信息

SQ112:狀態資訊更新處理

SQ114:狀態通知信息

SQ116:狀態資訊更新處理

SQ120:決定路由表

SQ122:傳送路由表

【發明說明書】

【中文發明名稱】 資料傳送方法、通訊處理方法、通訊裝置以及通訊處理程式

【技術領域】

【0001】 本揭示，係有關於具有已認證IP位址的裝置間的資料通訊技術。

【先前技術】

【0002】 近年來的資料通訊技術(Information and Communication Technology：ICT)的進步驚人，連接至Internet(網際網路)等網路的裝置，不限於習知的個人電腦、智慧手機等資訊處理裝置，擴大至各種物體(thing)。這樣的技術趨勢，稱作「IoT(Internet of Things；物聯網)」，不斷提議各種技術及服務以及實用化。假設未來地球上的數十億人與數百億或數兆裝置同時連接的世界。為了實現這樣的網路化的世界，有必要提供可以更簡單、更安全、更自由連接的解決方法。

【0003】 通常，網路上，使用靜態或動態分配至各裝置的IP(網際網路通訊協定)位址，實現裝置間的資料通訊。

【0004】 為了實現裝置間的資料通訊，從傳送源的裝置送出的資料一定轉送至收件位址的裝置。這樣的資料轉送處理，稱作「路由」等。為了實現這樣的路由，網路上配置多數路由器(Router)。

【0005】 如日本專利公開平成5年第022293號公報(專利文獻1)揭示，路由器，具有記憶路徑資訊的路徑資訊表，根據收訊框中的internetworking(網間互通)用位址、路徑資訊表的內容，決定路徑進行收訊框的中繼(參照日本專利公開平成5年第022293號公報的段落[0005]以及[0006]等)。

[先行技術文獻]

[專利文獻]

【0006】 [專利文獻1] 日本專利公開平成5年第022293號公報

【發明內容】

[發明所欲解決的課題]

【0007】 根據上述專利文獻1，假設是多數裝置存在的網路的話，也需要多數路由器，又，各路由器的任務也變大。因此，多數裝置存在的網路中，以各裝置可以獨立實現資料通訊的構成為佳。本揭示，提供用以實現如此構成的解決方法。

[用以解決課題的手段]

【0008】 根據本揭示的形態，提供連接複數裝置的網路中的資料傳送方法。資料傳送方法，包括：複數裝置分別根據從各裝置具有的公開密鑰依照散列函數算出的散列值，決定各裝置的IP位址的步驟；複數裝置分別保持反映各裝置的連接關係之狀態資訊的同時，也傳送顯示狀態資訊內容的通知信息至其它裝置的步驟；複數裝置分別根據從其它裝置接收的通知信息，更新各裝置保持的狀態資訊的步驟；根據各裝置保持的狀態資訊邏輯性規定的裝置集合間，決定上述集合內包含的裝置間保持之資料傳送收件位址的裝置的搜尋中使用的路由表的步驟。

【0009】 通知信息，也可以包含根據各裝置決定的IP位址算出之用以明確指定各裝置的識別資訊。

【0010】 資料傳送方法，可以更包含：複數裝置分別傳送各裝置具有的公開密鑰及連結至上述公開密鑰的電子證書至其它裝置的步驟；接收公開密鑰及電子證書的裝置中，根據從公開密鑰依照散列函數算出的散列值，決定公開密

鑰及電子證書的送信源的裝置的IP位址的步驟。

【0011】 決定的IP位址，包含預定的特定用固有值也可以。

決定的IP位址，也可以包含對應決定上述IP位址的裝置種類的值。

【0012】 根據本揭示的其它形態，提供連接至網路的裝置中的通訊處理方法。通訊處理方法，包括：根據從公開密鑰依照散列函數算出的散列值，決定自裝置的IP位址的步驟；保持反映與其它裝置的連接關係的狀態資訊的同時，也傳送顯示狀態資訊內容的通知信息至其它裝置的步驟；根據從其它裝置接收的通知信息，更新狀態資訊的步驟；以及根據各裝置保持的狀態資訊，邏輯性規定的裝置集合間，保持資料傳送收件位址的裝置的搜尋中使用的路由表的步驟。

【0013】 通知信息，包含根據決定的自裝置的IP位址算出之用以明確指定自裝置的識別資訊也可以。

【0014】 通訊處理方法，也可以更包括：根據狀態資訊，判斷集合中自裝置作為根節點(root node) 動作時，決定路由表的步驟。

【0015】 保持路由表的步驟，也可以包括從其它裝置接收路由表的步驟。

【0016】 狀態資訊及通知信息，也可以包含用以明確指定視作根節點(root node)的裝置的識別資訊。更新的步驟，也可以包括：接收的通知信息內包含的視作根節點的裝置與狀態資訊內包含的視作根節點的裝置不一致時，根據預定的規則，決定一方的裝置為根節點的步驟。

【0017】 通訊處理方法，也可以更包括：從認證機關取得連結至公開密鑰的電子證書的步驟；以及傳送公開密鑰及電子證書至其它裝置的步驟。

【0018】 通訊處理方法，也可以更包括：從其它裝置接收公開密鑰以及連結至公開密鑰的電子證書時，判斷電子證書正當性的步驟；判斷電子證書正當時，根據從公開密鑰依照散列函數算出的散列值，決定其它裝置的IP位址的步驟。

【0019】 決定的IP位址，也可以包含預定的特定用固有值。

決定的IP位址，也可以包含對應決定上述IP位址的裝置種類的值。

【0020】 根據本揭示的其它形態，提供連接至網路的裝置中的通訊處理方法。通訊處理方法，包括：接收其它裝置具有的公開密鑰及連結至上述公開密鑰的電子證書的步驟；判斷電子證書正當性的步驟；判斷電子證書正當時，決定根據從公開密鑰依照散列函數算出的散列值決定的IP位址，作為其它裝置的已認證IP位址的步驟；以及回應來自其它裝置的要求，提供對應其它裝置的已認證IP位址的服務之步驟。

【0021】 也可以決定公開密鑰，使根據從上述公開密鑰依照散列函數算出的散列值決定的IP位址與預定的格式一致。

【0022】 根據本揭示的又其它形態的裝置，包括用以連接至網路的網路界面以及連接至網路界面的控制部。控制部，實行：根據從公開密鑰依照散列函數算出的散列值，決定自裝置的IP位址的處理；保持反映與其它裝置的連接關係之狀態資訊的同時，也傳送顯示狀態資訊內容的通知信息至其它裝置的處理；根據從其它裝置接收的通知信息，更新狀態資訊的處理；以及根據各裝置保持的狀態資訊邏輯性規定的裝置集合間，保持資料傳送收件位址的裝置的搜尋中使用的路由表的處理。

【0023】 根據本揭示的又其它形態，提供通訊處理程式，用於具有用以連接至網路的網路界面之電腦。通訊處理程式，當透過電腦實行通訊處理程式時，使電腦實行上述通訊處理方法。

[發明效果]

【0024】 根據本揭示，多數裝置存在的網路中，可以提供各裝置可以獨立實現資料通訊的構成。

【圖式簡單說明】

【0025】

[圖1] 係顯示根據本實施形態的網路系統的一全體構成例之模式圖。

[圖2] 係顯示根據本實施形態的裝置的硬體構成例之模式圖。

[圖3] 係顯示根據本實施形態的裝置的程式及資料的構成例模式圖。

[圖4] 係用以說明根據本實施形態的網路系統中的IP位址的認證程序圖。

[圖5] 係顯示根據本實施形態的網路系統中利用的IP位址內埋入的一種類特定資訊例圖。

[圖6] 係顯示根據本實施形態的網路系統中裝置提供已認證IP位址的處理程序流程圖。

[圖7] 係用以說明有關根據本實施形態的網路系統中的IP位址通知的處理圖。

[圖8] 係用以說明有關根據本實施形態的網路系統中的IP位址通知的處理圖。

[圖9] 係顯示有關根據本實施形態的網路系統中的IP位址通知的處理程序的程序圖。

[圖10] 係用以說明利用根據本實施形態的網路系統之服務提供的應用軟體例圖。

[圖11] 係用以說明利用根據本實施形態的網路系統之服務提供的其它應用軟體例圖。

[圖12] 係用以說明根據本實施形態的網路系統中的一路由例圖。

[圖13] 係用以說明根據本實施形態的網路系統中的路由實現方法圖。

[圖14] 係用以說明根據本實施形態的網路系統中的其它路由實現方法圖。

[圖15] 係顯示有關根據本實施形態的網路系統中的路由實現之處理程序的程序圖。

[圖16] 係顯示根據本實施形態的網路系統中使用的狀態資訊及狀態通知信息的一資料構造例圖。

[圖17] 係顯示根據本實施形態的網路系統中狀態通知信息的狀態資訊更新例圖。

[圖18] 係顯示有關根據本實施形態的網路系統中的路由表決定之處理程序流程圖。

[圖19] 係顯示有關根據本實施形態的網路系統中各裝置的封包傳送接收之處理程序流程圖。

【實施方式】

【0026】 關於本揭示的實施形態，一邊參照圖面，一邊詳細說明。又，關於圖中的相同或相當部分，附上相同符號，不重複其說明。

【0027】 <A. 網路1的全體構成>

首先，說明關於根據本實施形態的網路系統1的全體構成。

【0028】 圖1係顯示根據本實施形態的網路系統1的一全體構成例之模式圖。參照圖1，網際網路(internet)或內部網路(intranet)等的任意網路2中，假設連接複數裝置100–1、100–2、100–3、100–4、100–5、…(以下，有時也總稱為「裝置100」)。一部分的裝置100，經由與存取點4之間確立的無線通訊連接至網路2也可以。或者，另外一部分的裝置100，經由與行動通訊基地台6之間確立的無線通訊連接至網路2也可以。

【0029】 這樣，網路2，包含區域網路(LAN)、廣域網路(WAN)、無線存取網路(RAN)以及網際網路中之任一也可以。

【0030】 連接至網路的裝置100，可以分別看作網路的「節點(node)」，以下的說明中，有時也稱裝置100為「節點(node)」。

【0031】 根據本實施形態的網路系統1中，裝置100之間，根據如後所述的程序，實現資料通訊。又，裝置100間的物理連接方法怎樣都可以。

【0032】 裝置100，包含具有以下機能的任意裝置，係使用分別具有的IP位址，進行與其它裝置資料通訊的機能。裝置100，有可能構成為通訊裝置單體，

而且有可能構成為某種物體的一部分或者編入某種物體。

【0033】 更具體地，裝置100，例如，個人電腦、智慧型手機、平板電腦、使用者的身體(例如，手腕、頭等) 上安裝的可穿戴裝置(例如，智慧型手錶、AR眼鏡等)都可以。又，裝置100，也可以是設置在智慧家電、互聯汽車(connected car)、工廠等的控制機器或其一部分。

【0034】 根據本實施形態的網路系統1，更包括1或複數認證機關200。各認證機關200，係以1或複數伺服器構成的電腦。使用1或複數認證機關200，根據如後所述的程序，認證各裝置100具有的IP位址。結果，各裝置100將會具有已認證IP位址。

【0035】 本說明書中，「已認證IP位址」，對通訊目標或第三者，意味保證各裝置100保持的IP位址的正當性的狀態。更具體地，「已認證IP位址」，意味透過不可逆的密碼學散列函數產生的同時，也是透過認證機關直接或間接認證的IP位址(關於細節，之後敘述)。藉由使用這樣的「已認證IP位址」，可以保證各裝置100在資料通訊中使用的IP位址不是偽裝的。

【0036】 結果，網路系統1內包含的任意裝置100，根據各裝置100具有的IP位址，將會唯一明確指定。即，各裝置，根據各裝置具有的IP位址，可以決定成為資料傳送收件位址或送出目標的裝置。

【0037】 IP位址，假設是連接至網際網路的裝置100間的資料通訊中也可以使用的Global IP address(全球IP位址)，但也可以是只在特定的網路內利用的私人IP位址。

【0038】 IP位址，根據版本，構成位址的位元數不同。現在制定的IPv4(Internet Protocol Version 4(網際網路協定版本4))中，規定32位元的位址區間，現在制定的IPv6(Internet Protocol Version 6(網際網路協定版本6))中，規定128位元的位址區間。本實施形態中，以根據IPv6的IP位址為主說明。但是，對於以

更多位元數規定的網路位址，或以更少位元數規定的網路位址，也可以應用本揭示。

【0039】 <B. 裝置100的構成例>

其次，說明關於根據本實施形態的網路系統1中使用的裝置100的硬體以及軟體的構成例。

【0040】 圖2係顯示根據本實施形態的裝置100的硬體構成例之模式圖。參照圖2，裝置100，作為主要的元件，包含處理電路(processing circuitry)的控制部110。

【0041】 控制部110，係用以實現根據本實施形態的機能提供及處理實行之演算主體。控制部110也可以構成為處理器使用圖2所示的處理器及記憶體，實行記憶體內收納的電腦可讀指令(computer readable instructions)(圖3所示的OS(作業系統及通訊處理程式)。或者，也可以使用編入相當於電腦可讀指令的電路之ASIC(特殊應用積體電路)等硬佈線(hard-wired)電路，實現控制部110。又，或者，FPGA(現場可程式化閘陣列)加上實現相當於電腦可讀指令的電路，藉此實現控制部110也可以。又，適當組合處理器及記憶體、ASIC、FPGA等，實現控制部110也可以。

【0042】 使用圖2所示的處理器及記憶體的構成中，控制部110，包含處理器102、主記憶體104、儲存體106以及ROM(唯讀記憶體)108。

【0043】 處理器102，係依序讀出電腦可讀指令實行的演算電路。處理器102，例如以CPU(中央處理單元)、MPU(微處理單元)、GPU(圖形處理單元)等構成。使用複數處理器102實現控制部110也可以(多處理器的構成)，使用具有複數核心的處理器實現控制部110也可以(多核心的構成)。

【0044】 主記憶體104，係DRAM(動態隨機存取記憶體)、SRAM(靜態隨機存取記憶體)等揮發性記憶裝置。處理器102，在主記憶體104上展開儲存體106

或ROM(唯讀記憶體)108中收納的各種程式中指定的程式，藉由與主記憶體104合作，實現根據本實施形態的各種處理。

【0045】 儲存體106，例如HDD(硬碟)、SSD(固態硬碟)、快閃記憶體等非揮發性記憶裝置。儲存體106內，收納以處理器102實行的各種程式、如後述的各種資料。

【0046】 ROM108，固定收納以處理器102實行的各種程式、如後述的各種資料。

【0047】 如圖2所示的處理器102實行記憶體內收納的電腦可讀指令的構成中，記憶體相當於儲存體106及ROM108。

【0048】 在此，說明關於裝置100的記憶體內收納的程式及資料的一例。

【0049】 圖3，係顯示根據本實施形態的裝置100的程式及資料的構成例模式圖。參照圖3，裝置100的記憶體(儲存體106及/或ROM108)中，例如作為包含電腦可讀指令的程式，收納OS160、通訊處理程式170、各種應用軟體300。

【0050】 OS160，係提供用以實現以裝置100實行的處理的基本機能之程式。通訊處理程式170，主要是用以實現根據本實施形態的機能提供及處理實行的程式。又，通訊處理程式170，有時也利用OS160提供的程序庫等，實現根據本實施形態的機能提供及處理實行。

【0051】 各種應用軟體300，係用以實現裝置100提供的各種機能的程式，使用者可以任意安裝。典型地，各種應用軟體300，提供利用通訊處理程式170中提供的資料通訊機能的各種處理。

【0052】 又，裝置100的記憶體(儲存體106及/或ROM108)內，例如收納私有密鑰172、公開密鑰174、電子證書176，作為根據本實施形態的機能提供以及處理實行的實現所需要的資料。私有密鑰172及公開密鑰174，根據任意的加密/解密演算法產生的所謂密鑰對。私有密鑰172，在與其它裝置的加密通訊中使

用。公開密鑰174，根據後述的程序在各裝置100的IP位址決定中使用。電子證書176，係根據認證機關200對公開密鑰174發行，用以擔保裝置100的IP位址正當性。通常，電子證書176，包含使用認證機關200的私有密鑰根據各裝置100的公開密鑰174算出的散列值(電子簽名)等。接收電子證書176的裝置100，使用認證機關200的公開密鑰，確認電子證書176以及連結至電子證書176的公開密鑰174的正當性。

【0053】 之後敘述關於密鑰對(私有密鑰172及公開密鑰174)的產生、電子證書176的取得以及這些資料的利用程序等。

【0054】 又，沒必要設置儲存體106及ROM(唯讀記憶體)108兩方，根據裝配形態，只設置任一方也可以。又，設置儲存體106及ROM(唯讀記憶體)108兩方時，例如關於密鑰對(私有密鑰172及公開密鑰174)，收納在ROM108內，提高機密性也可以。

【0055】 再次參照圖2，裝置100，更包含網路界面120，用以連接裝置100至網路。網路界面120，經由網路與其它裝置進行資料通訊。

【0056】 網路界面120，例如，包含乙太網路(註冊商標)埠、USB(通用序列匯流排)埠、IEEE1394等序列埠、傳統平行埠等有線連接端子。或者，網路界面120，也可以包含用以與裝置、路由器、行動通訊基地台等無線通訊的處理電路及天線等。對應網路界面120的無線通訊，例如，可以是Wi–Fi(註冊商標)、藍牙(註冊商標)、ZigBee(註冊商標)、LPWA(低功率廣域網路)、GSM(註冊商標)、W–CDMA、CDMA200、LTE(長期演進技術)、第5代行動通訊系統(5G)其中任一。

【0057】 裝置100，作為可選擇的元件，也可以包含顯示部130、輸入部140以及媒體介面150。

【0058】 顯示部130，係用以將處理器102中的處理結果等提示給外部之元件。顯示部130，例如，也可以是LCD(液晶顯示器)、有機EL(場致發光)顯示器

等。又，顯示部130，可以是穿戴至使用者頭部的頭戴式顯示器，也可以是投射影像至螢幕上的投影器。

【0059】 輸入部140，係用以接受操作裝置100的使用者的輸入操作之元件。輸入部140，例如，可以是鍵盤、滑鼠、顯示部130上配置的觸控面板、裝置100的筐體內配置的操作鍵等。

【0060】 媒體介面150，從收納各種程式(電腦可讀指令)及/或各種資料的非暫時性(non-transitory)的媒體152讀出各種程式及/或各種資料。

【0061】 媒體152，例如可以是DVD(數位多功能影音光碟)等光學媒體、USB記憶體等的半導體媒體等。媒體介面150，採用對應媒體152種類的構成。透過媒體介面150讀出的各種程式及/或各種資料，收納在儲存體106等內也可以。

【0062】 又，各種程式及/或各種資料不經由媒體152安裝至裝置100，從網路上的分送伺服器安裝需要的程式及資料至裝置100也可以。在此情況下，經由網路界面120，取得需要的程式及資料。

【0063】 如上述，顯示部130、輸入部140、媒體介面150，因為是可選擇的元件，例如經由USD等的任意界面從裝置100外部連接也可以。

【0064】 實現根據本實施形態的機能提供及處理實行的是控制部110，本申請案的技術範圍，至少包含用以實現控制部110的硬體及/或軟體。硬體，如上述，不是只由處理器及/或記憶體形成的構成，也可以包含使用ASIC等的硬佈線(hard-wired)電路或使用FPGA的構成。即，控制部110可以透過通用電腦內安裝程式實現，也可以實現為專用晶片。

【0065】 又，處理器實行的軟體，不只經由媒體152流通，也可以包含經由分送伺服器適當下載。

【0066】 又，用以實現根據本實施形態的機能提供及處理實行的構成，不限於圖2所示的控制部110，可以使用實現的適合時代的任意技術裝配。

【0067】 <C. 已認證IP位址>

其次，說明關於對各裝置100提供已認證IP位址的處理等。

【0068】 (c1：IP位址的決定處理)

根據本實施形態的網路系統1中，典型地，使用已認證IP位址，認證各裝置100的IP位址。例如，可以使用公開密鑰基礎結構(PKI：public key infrastructure)，認證各裝置100的IP位址。

【0069】 圖4，係用以說明根據本實施形態的網路系統1中的IP位址的認證程序圖。又，圖4中的「S1」～「S4」等符號，對應圖6所示的步驟號碼。

【0070】 參照圖4，裝置100，具有私有密鑰172及公開密鑰174構成的密鑰對。藉由輸入公開密鑰174至預定的散列函數180，算出散列值178，利用其算出的散列值178全部或一部分，使用作為裝置100的IP位址190。

【0071】 隨著這樣的IP位址190的決定處理，裝置100，傳送公開密鑰174至認證機關200，附帶認證機關200對公開密鑰174發行的電子證書176。裝置100，傳送自裝置的公開密鑰174及電子證書176至其它的裝置。其它的裝置，根據裝置100公開的公開密鑰174及電子證書176，確認裝置100的IP位址190的正當性。確認IP位址190的正當性時，利用正當性被確認的IP位址190，開始資料通訊。自裝置及其它裝置，可以互相進行直接通訊，除了直接通訊的處理之外，還可以包含認證機關200中的詢問處理。

【0072】 這樣，根據本實施形態的網路系統1中，可以認證IP位址190本身，藉由裝置本身保持這樣的已認證IP位址190，不使用對各裝置靜態或動態分配的IP位址，可以建構獨立網路。

【0073】 以下，詳細說明關於用以提供根據本實施形態的網路系統1中的已認證IP位址的處理。

【0074】 密鑰對的私有密鑰172及公開密鑰174，由裝置100本身作成也可

以，從外部提供預先收納至裝置100內也可以。從外部提供的情況下，裝置100只取得私有密鑰172，關於公開密鑰174以本身產生也可以。

【0075】 作為密鑰對的公開密鑰174的產生方法的一例，使用隨機數產生器產生的既定長度的位元例(例如，512位元)作為私有密鑰172的同時，還依照眾所周知的密碼演算法(例如，橢圓曲線密碼演算法)，根據私有密鑰172產生既定長度的位元例(例如，256位元)構成的公開密鑰174也可以。又，裝置100本身產生密鑰對的情況下，隨機數產生器，利用OS160提供的機能實現也可以，使用ASIC等的硬佈線(hard-wired)電路實現也可以。

【0076】 散列函數180，可以利用眾所周知的不可逆密碼學散列函數(例如，BLAKE)。散列函數180，算出既定長度的位元列(例如，256位元)構成的散列值178。

【0077】 散列函數180中，不只是公開密鑰174，輸入任意關鍵字也可以。作為任意關鍵字，使用連結至既定組織的信息也可以。作為連結至既定組織的信息，使用包含上述既定組織具有的商標名稱之信息也可以。例如，使用既有組織保有的已登錄商標名稱(例如，「connectFree」)作為輸入散列函數180內的關鍵字也可以。藉由採用這樣的裝配方式，既定組織以外的第三者，可以防止無上述既定組織允許實施根據本實施形態的網路系統1以及關聯的方法、程式等。

【0078】 使用根據散列函數180算出的散列值178的全部或一部分作為IP位址190。例如，算出256位元(以16進位表示64位數)的散列值178時，決定64位數的散列值178中任意的32位數(例如前半32位數)作為對應IPv6的IP位址190(128位元)也可以。或者，決定64位數的散列值178中前半8位數作為對應IPv4的IP位址190(32位元)也可以。

【0079】 或者，考慮對應IPv6的IP位址190(128位元)，根據散列函數180

算出128位元的散列值178也可以。在此情況下，可以決定算出的散列值178全部作為對應IPv6的IP位址190(128位元)。

【0080】 根據本實施形態，以裝置100的公開密鑰174為基礎，可以決定裝置100中固有的IP位址190。這樣，使用透過裝置100決定的IP位址190，可以連接裝置100至網際網路等的網路。又，裝置100，即使管理網際網路服務提供者(ISP)等的全球IP位址的服務事業者(伺服器)不存在，也可以使用本身決定的IP位址190進行資料通訊。又，裝置100，即使管理裝配在存取點等的DHCP(動態主機組態協定)伺服器等的私有IP位址的伺服器不存在，也可以使用本身決定的IP位址190，連接至網際網路等全球網路進行資料通訊。因此，可以提高關於連接至網際網路等網路的使用者體驗及使用者的便利性。

【0081】 (c2：固有文字列)

裝置100決定的IP位址190，也可以明確指定是根據本實施形態的處理程序決定。為了進行這樣的特定，例如，IP位址190內包含預定的特定用固有值(固有文字列)也可以。即，決定的IP位址，包含預定的特定用固有值(固有文字列)也可以。

【0082】 例如，固定16進位表示的IP位址190的前頭2位數(前頭開始第1位數及第2位數)為預定的固有文字列(例如，「FC」)也可以。通常，因為散列函數180是一方向性函數，不能根據IP位址190反算公開密鑰174。因此，決定的IP位址190直到滿足既定條件 (此時，前頭2位數成為預定的固有值)為止，利用隨機數產生器，重複產生私有密鑰172及公開密鑰174也可以。即，公開密鑰174，根據依照散列函數從公開密鑰174算出的散列值決定的IP位址190，決定與預定的格式一致也可以。

【0083】 這樣，由於IP位址190內包含預定的特定用固有值(例如，前頭2位數「FC」)，第三者可以判斷裝置100的IP位址190是否由裝置100本身決定。

【0084】 (c3：種類特定資訊)

裝置100決定的IP位址190內，也可以包含明確指定裝置100種類的資訊。為了進行這樣的特定，例如，IP位址190內包含對應裝置100種類的值也可以。即，決定的IP位址190，包含對應決定其IP位址190的裝置100種類的值也可以。

【0085】 例如， 16進位表示的IP位址190的前頭開始第3位數及第4位數內埋入對應裝置100種類的值(種類特定資訊)也可以。

【0086】 圖5，係顯示根據本實施形態的網路系統1中利用的IP位址內埋入的一種類特定資訊例圖。圖5所示的種類特定資訊，預先收納在各裝置100的控制部110的ROM108(參照圖2)等之內也可以。例如，可以使用對應圖5所示的裝置種類的值。

【0087】 如圖5所示，例如，裝置100種類是個人電腦時，IP位址190的前頭開始第3位數及第4位數內，設定表示個人電腦的值「00」。

【0088】 如上述，通常，因為散列函數180是一方向性函數，不能根據IP位址190反算公開密鑰174。因此，決定的IP位址190直到滿足既定條件 (此時，前頭第3位數及第4位數成為表示裝置100種類的值)為止，利用隨機數產生器，重複產生私有密鑰172及公開密鑰174也可以。即，公開密鑰174，根據依照散列函數從公開密鑰174算出的散列值決定的IP位址190，決定與預定的格式一致也可以。

【0089】 這樣，由於IP位址190內包含表示裝置100種類的值，第三者，根據裝置100決定的IP位址190，可以明確指定上述表示裝置100的種類。

【0090】 (c4：公開密鑰174的登錄及電子證書176的取得)

其次，說明關於公開密鑰174的登錄及電子證書176的取得。

【0091】 裝置100，從認證機關200取得用以證明公開密鑰174正當性的電子證書176。作為取得電子證書176的程序，從裝置100傳送公開密鑰174至認證

機關200登錄的同時，也從認證機關200取得連結至登錄的公開密鑰174的電子證書176。

【0092】 更具體地，裝置100(控制部110)，經由網路，傳送公開密鑰174及電子證書的發行要求(以下，也稱作「證書簽名要求」)至認證機關200。認證機關200回應從裝置100接收的證書簽名要求，登錄公開密鑰174的同時，也發行連結至登錄的公開密鑰174的電子證書176。於是，認證機關200，經由網路，傳送電子證書176至裝置100。

【0093】 典型地，電子證書176，包含電子證書176的所有者資訊(此例中，裝置100)、電子證書176的發行者資訊(此例中，認證機關200)、發行者的數位簽名以及電子證書176的有效期限等。

【0094】 認證機關200，透過既定組織營運也可以，連結至透過既定組織營運的路徑認證機構的中間認證機關也可以。又，當公開密鑰174的登錄及連結至公開密鑰174的電子證書176的發行時，對於既定組織既定的手續費及/或維持費是必需的也可以。

【0095】 根據本實施形態，通過公開密鑰174的登錄及公開密鑰174的取得，由於公開密鑰174透過認證機關200直接認證，根據公開密鑰174決定的IP位址190也透過認證機關200間接認證。透過這樣的認證機關200的認證，裝置100利用已認證IP位址190，也可以經由網路實現資料通訊。

【0096】 又，連結至公開密鑰174的電子證書176內，為了提高機密性，也可以包含關聯裝置100屬性的資訊(以下，也稱作「屬性資訊」)。關聯裝置100的屬性資訊，例如，可以使用裝置100的OS160、通訊處理程式170的版本資訊、構成裝置100的硬體(例如，處理器、儲存體等)的序號等。此時，裝置100，傳送公開密鑰174及證書簽名要求之際，傳送裝置100的屬性資訊至認證機關200也可以。又，電子證書176內包含的裝置100屬性資訊，透過眾所周知的不可逆密碼

學散列函數等加密也可以。

【0097】 這樣，由於裝置100的屬性資訊包含在電子證書176內，回應來自裝置100本身的證書簽名要求，可以認證發行電子證書176。即，可以更防止裝置100以外的裝置冒充裝置100使用裝置100的公開密鑰174及電子證書176。

【0098】 (c5：處理程序)

其次，說明關於用以提供各裝置100中已認證IP位址的處理程序。

【0099】 圖6係顯示根據本實施形態的網路系統1中裝置100提供已認證IP位址的處理程序流程圖。圖6所示的處理程序，分別在各裝置100中實行，圖6所示的各步驟，透過各裝置100的控制部110實行。

【0100】 參照圖6，裝置100，取得根據任意演算法產生的密鑰對(私有密鑰172及公開密鑰174)(步驟S1)。此密鑰對，裝置100本身產生也可以，裝置100從外部取得也可以。或者，裝置100也可以從外部只取得私有密鑰172，在內部產生公開密鑰174。

【0101】 接著，裝置100，藉由輸入公開密鑰174至預定的散列函數180，算出散列值178，根據其算出的散列值178的全部或一部分決定裝置100的IP位址190(步驟S2)。即，裝置100，根據依照散列函數180從公開密鑰174算出的散列值178，決定自裝置的IP位址。

【0102】 又，為了使IP位址190內包含固有文字列(例如，IP位址190的前頭開始第1位數及第2位數)及/ 或種類特定資訊(例如，IP位址190的前頭開始第3位數及第4位數)，產生適當的密鑰對(私有密鑰172及公開密鑰174)也可以。

【0103】 又，裝置100，傳送公開密鑰174及電子證書的發行要求(證書簽名要求)至認證機關200(步驟S3)。認證機關200，回應從裝置100接收的證書簽名要求，登錄公開密鑰174的同時，也發行連結至登錄的公開密鑰174的電子證書176。於是，認證機關200，經由網路傳送電子證書176至裝置100。於是，裝置

100接收並收納來自認證機關200的電子證書176(步驟S4)。

【0104】 這樣，裝置100，從認證機關取得連結至公開密鑰174的電子證書176。

【0105】 又，步驟S2的處理與步驟S3及S4的處理的實行順序不拘。

【0106】 <D. 資料通訊處理>

其次，說明關於利用已認證IP位址的裝置100間的資料通訊處理。

【0107】 (d1：IP位址的通知)

首先，說明關於根據本實施形態的網路系統1中裝置100間的IP位址通知的處理。

【0108】 圖7及圖8，係用以說明有關根據本實施形態的網路系統1中的IP位址通知的處理圖。圖7及圖8中，例示3個裝置100–1、100–2、100–3之間交換IP位址。又，2個裝置100之間也可以同樣的處理，而且更多的裝置100之間也可以同樣的處理。

【0109】 圖7及圖8所示的狀態中，裝置100–1、100–2、100–3各自根據上述程序，裝置100–1、100–2、100–3分別決定IP位址190–1、190–2、190–3，又，也分別完成登錄公開密鑰174–1、174–2、174–3至認證機關200以及從認證機關200取得電子證書176–1、176–2、176–3。

【0110】 如圖7及圖8所示，各裝置100，定期性或每一活動，傳送(廣播)各裝置具有的公開密鑰174以及連結至公開密鑰174的電子證書176。即，各裝置100，傳送公開密鑰174以及電子證書176至其它裝置。又，公開密鑰174包含在電子證書176內時，只傳送電子證書176也可以。

【0111】 圖7中顯示，例如，裝置100–1，傳送(傳播)公開密鑰174–1以及連結至公開密鑰174–1的電子證書176–1。圖7所示的例中，裝置100–2及100–3可以接收裝置100–1傳送的公開密鑰174–1以及電子證書176–1。於是，在裝置100–

2及100–3判斷電子證書176–1是否正當方面，當判斷正當時，根據連結的公開密鑰174–1決定裝置100–1的IP位址190–1，分別登錄至連接表194–2及194–3。

【0112】 在此，連接表，因為進行資料通訊包含各裝置100的資訊，各裝置100，參照連接表，明確指定收件地址的裝置100的IP位址等的同時，也確立需要的通訊期(session)。

【0113】 更具體地，裝置100–2，首先，判斷裝置100–1廣播的電子證書176–1是否正當。判斷此正當性的處理中，驗證電子證書176–1的完整性。

【0114】 作為驗證完整性處理的一例，首先，裝置100–2，確認電子證書176–1的所有者資訊、電子證書176–1的發行者資訊、發行者的數位簽名的存在。於是，裝置100–2，判斷電子證書176–1是否在有效期限內。還有，裝置100–2，判斷電子證書176–1的發行源是否可以信賴。尤其，電子證書176–1由中間認證機關發行時，裝置100–2，明確指定連結至發行電子證書176–1的中間認證機關之路徑認證機關的同時，也判斷上述明確指定的路徑認證機關是否可以信賴。例如，明確指定的路徑認證機關與收納在裝置100–1內的1或複數路徑認證機關之中任一一致時，判斷可以信賴電子證書176–1的發行源。

【0115】 通過如上的判斷處理時，裝置100–2，決定裝置100–1廣播的電子證書176–1是正當的。於是，裝置100–2，藉由對預定的散列函數180輸入裝置100–1廣播的公開密鑰174–1，算出散列值178–1，利用其算出的散列值178–1全部或一部分，決定裝置100–1的IP位址190–1。在此，裝置100–1及裝置100–2，具有共同的散列函數180。又，裝置100–1及裝置100–2之間，根據散列值178–1決定IP位址190–1的處理也是共同的。

【0116】 根據如上的處理，裝置100–2，可以決定裝置100–1的IP位址190–1。於是，裝置100–2，追加決定的裝置100–1的IP位址190–1的登錄(entry)至連接表194–2。又，連結至IP位址190–1登錄公開密鑰174–1也可以。

【0117】 又，裝置100–3中，也實行與裝置100–2相同的處理，裝置100–3的連接表194–3中，追加決定的裝置100–1的IP位址190–1的登錄(entry)至連接表194–2。又，連結至IP位址190–1登錄公開密鑰174–1也可以。

【0118】 透過如圖7所示的處理，裝置100–2及裝置100–3可以取得裝置100–1的IP位址190–1。

【0119】 圖8中顯示，例如，裝置100–2傳送(廣播)公開密鑰174–2及連結至公開密鑰174–2的電子證書176–2。圖8所示的例中，假設裝置100–1及100–3可以接收裝置100–2傳送的公開密鑰174–2及電子證書176–2。於是，裝置100–1及100–3，在判斷電子證書176–2是否正當方面，當判斷正當時，根據連結的公開密鑰174–2決定裝置100–2的IP位址190–2，分別登錄至連接表194–1及194–3。

【0120】 裝置100–1及100–3中實行的一連串處理，因為與參照圖7說明的處理相同，不重複詳細的說明。透過如圖8所示的處理，裝置100–1及裝置100–3，可以取得裝置100–2的IP位址190–2。

【0121】 還有，裝置100–3也可以傳送(廣播)公開密鑰174–3及連結至公開密鑰174–3的電子證書176–3。假設裝置100–1及100–2可以接收裝置100–3傳送的公開密鑰174–3及電子證書176–3。於是，裝置100–1及100–2在判斷電子證書176–3是否正當方面，當判斷正當時，根據連結的公開密鑰174–3決定裝置100–3的IP位址190–3，分別登錄至連接表194–1及194–2。透過這樣的處理，裝置100–1及裝置100–2，可以取得裝置100–3的IP位址190–3。

【0122】 圖9，係顯示有關根據本實施形態的網路系統1中的IP位址通知的處理程序的程序圖。圖9中，對應圖7及圖8，顯示3個裝置100–1、100–2、100–3中的處理程序。

【0123】 裝置100–1，傳送(廣播)公開密鑰174–1及連結至公開密鑰174–1的電子證書176–1(程序SQ10)。

【0124】 裝置100–2，一接收到裝置100–1傳送的公開密鑰174–1及電子證書176–1，就判斷電子證書176–1的正當性(程序SQ11)。判斷電子證書176–1為正當時，裝置100–2，根據公開密鑰174–1決定裝置100–1的IP位址190–1(程序SQ12)，登錄決定的裝置100–1的IP位址190–1至連接表194–2(程序SQ13)。

【0125】 同樣地，裝置100–3，一接收到裝置100–1傳送的公開密鑰174–1及電子證書176–1，就判斷電子證書176–1的正當性(程序SQ14)。判斷電子證書176–1為正當時，裝置100–3，根據公開密鑰174–1決定裝置100–1的IP位址190–1(程序SQ15)，登錄決定的裝置100–1的IP位址190–1至連接表194–3(程序SQ16)。

【0126】 又，裝置100–2，傳送(廣播)公開密鑰174–2及連結至公開密鑰174–2的電子證書176–2(程序SQ20)。

【0127】 裝置100–1，一接收到裝置100–2傳送的公開密鑰174–2及電子證書176–2，就判斷電子證書176–2的正當性(程序SQ21)。判斷電子證書176–2為正當時，裝置100–1，根據公開密鑰174–2決定裝置100–2的IP位址190–2(程序SQ22)，登錄決定的裝置100–2的IP位址190–2至連接表194–1(程序SQ23)。

【0128】 同樣地，裝置100–3，一接收到裝置100–2傳送的公開密鑰174–2及電子證書176–2，就判斷電子證書176–2的正當性(程序SQ24)。判斷電子證書176–2為正當時，裝置100–3，根據公開密鑰174–2決定裝置100–2的IP位址190–2(程序SQ25)，登錄決定的裝置100–2的IP位址190–2至連接表194–3(程序SQ26)。

【0129】 又，裝置100–3，傳送(廣播)公開密鑰174–3及連結至公開密鑰174–3的電子證書176–3(程序SQ30)。

【0130】 裝置100–1，一接收到裝置100–3傳送的公開密鑰174–3及電子證書176–3，就判斷電子證書176–3的正當性(程序SQ31)。判斷電子證書176–3為正當時，裝置100–1，根據公開密鑰174–3決定裝置100–3的IP位址190–3(程序SQ32)，登錄決定的裝置100–3的IP位址190–3至連接表194–1(程序SQ33)。

【0131】 同樣地，裝置100–2，一接收到裝置100–3傳送的公開密鑰174–3及電子證書176–3，就判斷電子證書176–3的正當性(程序SQ34)。判斷電子證書176–3為正當時，裝置100–2，根據公開密鑰174–3決定裝置100–3的IP位址190–3(程序SQ35)，登錄決定的裝置100–3的IP位址190–3至連接表194–2(程序SQ36)。

【0132】 又，程序SQ10～SQ16的處理、程序SQ20～SQ26的處理、程序SQ30～SQ36的處理，可以任意順序或並排實行。

【0133】 這樣，各裝置100，從其它裝置一接收到公開密鑰174及連結至公開密鑰174的電子證書176，就判斷電子證書176的正當性(程序SQ11、SQ14、SQ21、SQ24、SQ31、SQ34)。於是，各裝置100，判斷電子證書176為正當時，根據依照散列函數從公開密鑰174算出的散列值，決定其它裝置的IP位址 (程序SQ12、SQ15、SQ22、SQ25、SQ32、SQ35)。

【0134】 如上述，根據本實施形態的網路系統1中，以其它裝置100傳送的電子證書176被判斷為正當作為條件，根據連結至電子證書176的公開密鑰174，決定上述其它裝置100的IP位址190。以連結至公開密鑰174的電子證書176為正當的判斷作為條件，因為根據公開密鑰174決定IP位址190，可以保證公開密鑰174的正當性以及IP位址190的正當性。因此，裝置100之間可以實現確實的資料通訊。

【0135】 又，依照本實施形態的網路系統1中，根據各裝置100廣播的公開密鑰174，因為可以知道各裝置100的IP位址，管理IP位址的伺服器即使不存在，裝置100之間也可以直接連接。尤其，虛擬私人網路(VPN)伺服器等即使不存在，裝置100之間也可以實現確保隱私性的通訊，可以削減用以維持VPN伺服器的成本、消耗電力。

【0136】 (d2：應用例)

依照本實施形態的網路系統1中，因為各裝置100之間可以互相認證IP位址，可以只根據IP位址明確指定通訊目標。藉由利用這樣的已認證IP位址，可以

提供各種伺服器。以下，說明關於利用已認證IP位址提供的一伺服器例。

【0137】 圖10係用以說明利用根據本實施形態的網路系統1之服務提供的應用軟體例圖。圖10所示的應用軟體例中，假設網頁式(Web base)的應用軟體伺服器及存取上述應用軟體伺服器的行動終端分別為裝置100。應用軟體伺服器，提供對應存取源的行動終端的已認證IP位址的固有網頁(Web page)。

【0138】 圖10(a)中，顯示應用軟體伺服器保持的一網路管理表210例。網路管理表210中，規定過去曾存取或者連結至有存取預定的行動終端的已認證IP位址212顯示初始畫面的初始畫面資訊214、顯示喜愛的應用軟體資訊216。網路管理表210的內容，使用者以手動更新，或者，根據使用者的操作透過應用軟體伺服器更新也可以。

【0139】 應用軟體伺服器，一接收到來自行動終端的存取，就以給予上述行動終端的已認證IP位址為關鍵，參照網路管理表210，決定對應的初始畫面資訊214及應用軟體資訊216。於是，應用軟體伺服器，根據決定的初始畫面資訊214及應用軟體資訊216，決定提供給存取源的行動終端的網頁(Web page)內容。

【0140】 圖10(b)中顯示，例如，應用軟體伺服器提供網路銀行(on-line banking)的伺服器時的Web畫面例。例如，給予已認證IP位址1的行動終端的顯示器上提示的Web畫面例220A中，配置「存入手續」、「帳戶餘額確認」、「轉帳手續」等基本帳戶管理的按鍵。另一方面，給予已認證IP位址2的行動終端的顯示器上提示的Web畫面例220B中，顯示匯率的時間性變化圖的同時，也配置「外匯買入」、「外匯賣出」等有關外匯的按鍵。

【0141】 這樣的初始畫面，例如，藉由參照網路管理表210的初期畫面資訊214等可以決定。還有，藉由參照網路管理表210的應用軟體資訊216等，不只是初始畫面，還可以提供對應每行動終端(即，操作行動終端的使用者)喜愛的服務。

【0142】 如上述，網頁(Web page)的應用軟體伺服器，回應來自行動終端的要求，提供對應上述行動終端的已認證IP位址的伺服器。藉此，根據行動終端的已認證IP位址，可以客製化存取應用軟體時提供的初始畫面及各種服務內容。

【0143】 圖11，係用以說明利用根據本實施形態的網路系統1之服務提供的其它應用軟體例圖。圖11所示的應用軟體例中，假設旅館等的利用管理伺服器以及存取上述利用管理伺服器的行動終端分別為裝置100。圖11所示的應用軟體例中，可以使用行動終端作為電子鎖(使用證)。

【0144】 圖11(a)中，顯示伺服器保持的一利用管理表230例。利用管理表230中，收納通過預約網站等預約的內容(房間號碼234及可使用時間236)，連結至給予上述預約操作中使用的移動終端的網路位址232。

【0145】 使用者操作本身的行動終端，利用預約網站預約住宿時，伺服器，隨同給予其住宿預約中使用的行動終端之網路位址，也追加預約內容至利用管理表230。

【0146】 如圖11(b)所示，住宿設施240的各房間前，配置無線通訊單元242。預定住宿的使用者具有住宿預約使用的行動終端，接近預約的房間時，無線通訊單元242與行動終端進行無線通訊。又，行動終端與無線通訊單元242之間的無線通訊，自動開始也可以，使用者進行明確表示的操作之後開始也可以。

【0147】 給予使用者保持的行動終端之網路位址，與利用管理表230的網路位址232的任一登錄一致時，根據對應的房間號碼234以及可使用時間236，使用者解鎖預約對象的房間。這樣，伺服器，回應來自行動終端的要求，提供對應上述行動終端的已認證IP位址之服務。

【0148】 圖11中，作為典型例，例示關於使用行動終端作為旅館等住宿設施的各房間鑰匙之構成，但不限於此，可以作為任意的使用證使用。例如，行動端終本身，可以用作娛樂設施等各種設施、音樂會等各種活動的入場券。還

有，也可以使用行動終端本身作為鐵路、飛機的票。

【0149】 根據本實施形態的網路系統1中，因為認證裝置100的IP位址本身，如同既存技術，不需要用以顯示票的應用軟體等，可以利用裝置100本身作為使用證。

【0150】 這樣，根據本實施形態的網路系統1中，因為可以取得行動終端的已認證IP位址，不需要用以實現認證處理的應用軟體等，可以對各行動終端提供固有的服務。又，行動終端與伺服器等裝置間進行資料通訊，因為意味取得已認證IP位址，提供行動終端固有的服務需要的時間等也變得極短，相較於利用應用軟體進行認證處理的構成，可以縮短提供服務需要的等待時間等。

【0151】 (d3：路由)

其次，說明關於根據裝置100間的資料通訊的處理。根據本實施形態的網路系統1中，各裝置100具有路由機能以及資料轉送機能，透過這樣的機能，可以實現可以獨立進行資料通訊的網路。

【0152】 說明根據本實施形態的網路系統1採用的路由。以下的說明中，作為典型例，假設資料以「封包」的形式傳送。

【0153】 圖12係用以說明根據本實施形態的網路系統1中的一路由例圖。圖12中，例如，說明包含7個裝置100–1～裝置100–7的網路中的路由。

【0154】 如圖12所示，透過上述的IP位址的通知處理，交換IP位址的裝置100之間，可以確立連接10。確立連接10的裝置100之間，以一種對等網路(peer-to-peer)交換資料。又，裝置100間的連接10內，可以採用包含TCP(傳輸控制協定)以及UDP(用戶資料包協定)的任意協定。

【0155】 例如，考慮傳送以裝置100–1到裝置100–7作為收件地址的發送封包時，透過裝置100–1中的路由，從裝置100–1傳送發送封包到裝置100–5(路徑RT1)，接著，透過裝置100–5中的路由，從裝置100–5傳送發送封包到裝置100–

6(路徑RT2)，最後，透過裝置100–6中的路由，從裝置100–6傳送發送封包到裝置100–7(路徑RT3)。

【0156】 根據本實施形態的網路系統1內包含的各裝置100，為了實現圖12圖所示的路由，具有以下所示的機能。

【0157】 圖13係用以說明根據本實施形態的網路系統1中的路由實現方法圖。參照圖13，根據本實施形態的網路系統1中，邏輯性分割網路系統1內包含的複數裝置100為1或複數節點群30(節點群30–1、30–2、30–3、…)，各節點群30共有路由表32(路由表32–1、32–2、32–3、…)。

【0158】 節點群30，意味邏輯性規定的裝置100集合，如之後敘述，根據各裝置100保持的狀態資訊40內容決定。

【0159】 路由表32，成為資料傳送的收件地址(發送封包的收件地址)之裝置100搜尋中使用的表，典型地，可以利用分散散列表(Distributed Hash Table：DHT)實現。路由表32，包含用以明確指定對應的節點群30內包含的裝置100(節點)之識別資訊及其位置等。

【0160】 各節點群30，包含成為根節點34(根節點34–1、34–2、34–3、…)的裝置100。根節點34中，階層式邏輯連接成為1或複數節點36的裝置100。

【0161】 圖14，係用以說明根據本實施形態的網路系統1中的其它路由實現方法圖。

【0162】 參照圖14，網路系統1內包含的各裝置100，保持反映各裝置100的連接關係(邏輯性或物理性連接關係)的狀態資訊40(狀態資訊40–1、40–2、40–3、…)。狀態資訊40，反映各裝置100與其它裝置之間的連接關係。

【0163】 又，各裝置100，傳送顯示保持的狀態資訊40內容的狀態通知信息42給周期性(例如，每數分鐘)存在周圍的其它裝置100。各裝置100，根據來自其它裝置100的狀態通知信息42，根據需要更新自裝置的狀態資訊40。

【0164】 圖14中，顯示裝置100–1傳送狀態通知信息42的例，網路系統1內包含的各裝置100分別傳送狀態通知信息42。藉由各裝置100根據來自其它裝置100的狀態通知信息42更新狀態資訊40，邏輯性規定圖13所示的樹狀構造。

【0165】 又，不需要預先決定關於是否以任一裝置100作為根節點34。各裝置100的狀態資訊40中，初始設定顯示上述裝置作為根節點34動作時的值。之後根據從其它裝置接收的狀態通知信息42，透過更新狀態資訊40，自主決定應動作為根節點34的裝置100、應動作為通常的節點36的裝置100。

【0166】 圖15，係顯示有關根據本實施形態的網路系統1中的路由實現之處理程序的程序圖。圖15中，顯示著眼於圖14中所示的裝置100–1、100–2、100–5、100–4的交換。

【0167】 參照圖15，連接至網路系統1時，首先，裝置100–1、100–2、100–5、100–4分別初始設定各自的狀態資訊40(程序SQ100)。

【0168】 於是，裝置100–1，傳送顯示自裝置的狀態資訊40內容的狀態通知信息42至周邊的裝置100(程序SQ102)。接收來自裝置100–1的狀態通知信息42的各裝置，根據接受的狀態通知信息42，實行對自裝置的狀態資訊40的更新處理(程序SQ104)。

【0169】 同樣地，裝置100–2，傳送顯示自裝置的狀態資訊40內容的狀態通知信息42至周邊的裝置100(程序SQ106)。接收來自裝置100–2的狀態通知信息42的各裝置，根據接受的狀態通知信息42，實行對自裝置的狀態資訊40的更新處理(程序SQ108)。

【0170】 同樣地，裝置100–5，傳送顯示自裝置的狀態資訊40內容的狀態通知信息42至周邊的裝置100(程序SQ110)。接收來自裝置100–5的狀態通知信息42的各裝置，根據接受的狀態通知信息42，實行對自裝置的狀態資訊40的更新處理(程序SQ112)。

【0171】 同樣地，裝置100–4，傳送顯示自裝置的狀態資訊40內容的狀態通知信息42至周邊的裝置100(程序SQ114)。接收來自裝置100–4的狀態通知信息42的各裝置，根據接受的狀態通知信息42，實行對自裝置的狀態資訊40的更新處理(程序SQ116)。

【0172】 這樣，複數裝置100，分別保持反映各裝置100的連接關係之狀態資訊40(程序SQ100)的同時，也傳送顯示狀態資訊40內容的狀態通知信息42至其它裝置 (程序SQ102、SQ106、SQ110、SQ114)。又，複數裝置100，分別根據從其它裝置接收的狀態通知信息42，更新裝置100保持的狀態資訊40(程序SQ104、SQ108、SQ112、SQ116)。這些處理，周期性實行也可以。

【0173】 又，程序SQ102及SQ104、程序SQ106及SQ108、程序SQ110及SQ112以及程序SQ114及SQ116，可以以互相獨立的時序實行。因此，可以是任何實行順序，也可以各個並排實行。

【0174】 各裝置100的狀態通知信息42的傳送結果，決定作為根節點34動作的裝置100時，作為根節點34動作的裝置100(圖15中顯示的例中，裝置100–1)決定路由表32(程序SQ120)。這樣，根據各裝置100保持的狀態資訊40，邏輯性規定的節點群30(裝置100的集合)之間，實行決定上述節點群30內包含的裝置100間保持的路由表32的處理。又，路由表32，用於成為資料傳送的收件地址的裝置搜尋。

【0175】 於是，作為根節點34動作的裝置100，傳送決定的路由表32至作為其它自裝置的子孫節點動作的其它裝置100(程序SQ122)。

【0176】 於是，重複程序SQ102～SQ120的處理。

說明的方便上，圖15中，顯示各裝置100初始設定狀態資訊40的例，但實際上，假設網路系統1內新加入任意裝置100到任意裝置100從網路系統1脫離的情況。這樣的情況下，實行作為根節點34動作的裝置100的變更或者路由表32的內

容更新等的處理。

【0177】 其次，說明關於狀態資訊40及狀態通知信息42的細節。

本實施形態的網路系統1中，根據鄰接的裝置100間交換的狀態通知信息42，藉由各裝置100依序更新本身的狀態資訊40，邏輯性建構如圖13所示的階層式連接裝置100的節點群30。

【0178】 圖16，係顯示根據本實施形態的網路系統1中使用的狀態資訊40及狀態通知信息42的一資料構造例圖。圖16(a)中，顯示狀態資訊40的一資料結構例，圖16(b)中，顯示狀態通知信息42的一資料結構例。

【0179】 參照圖16(a)，狀態資訊40，作為設定項目，包含Parent ID401、Children402、RootID403、height404、2進位表示(Binary Representation)405。

【0180】 Parent ID401內，收納用以明確指定各裝置100的母節點裝置之識別資訊(典型地，之後敘述的Key ID)。

【0181】 Children402內，收納用以明確指定各裝置100的子節點裝置之識別資訊(典型地，之後敘述的Key ID)。又，子節點裝置，因為不限於1個，Children402內，以列表形式收納1或複數的裝置。

【0182】 Root ID403內，收納識別資訊(典型地，之後敘述的Key ID)，用以明確指定作為各裝置所屬的節點群30的根節點34動作的裝置100。

【0183】 height404內，收納各裝置所屬的節點群30中各裝置的height。height，意味各裝置所屬的節點群30中從根節點34到葉節點的邊緣數最大值。即，根據height的大小，可以決定節點群30中從根節點34到葉節點的深度。

【0184】 2進位表示405內，各裝置所屬的節點群30中，收納用以明確指定搜尋對象的裝置(節點)的識別資訊。

【0185】 又，狀態資訊40，作為新設定項目，也可以包含time stamp(時間戳記)。time stamp(時間戳記)，例如，可以是顯示各裝置100的更新時刻之資訊，

也可以是顯示狀態通知信息42的時刻之資訊。

【0186】 各裝置100，具有稱作用以明確指定自裝置的Key ID的識別資訊。Key ID，在網路系統1中使用可以單一明確指定裝置100的識別資訊。典型地，Key ID，使用各裝置100具有的IP位址，或者從IP位址根據散列函數算出的散列值也可以。

【0187】 參照圖16(b)，狀態通知信息42，顯示狀態資訊40的內容。更具體地，狀態通知信息42包含Parent ID421、Root ID422、height423、Key ID424。

【0188】 Parent ID421內，收納與狀態資訊40的Parent ID401相同的值。Root ID422內，收納與狀態資訊40的Root ID403相同的值。height423內，收納與狀態資訊40的height404相同的值。Key ID424內，收納自裝置的識別資訊即Key ID。

【0189】 這樣，狀態資訊40以及狀態通知信息42，包含Key ID(自裝置的識別資訊)，作為用以明確指定各裝置100的識別資訊。此時，Key ID(自裝置的識別資訊)，採用根據各裝置100決定的IP位址算出的值也可以。

【0190】 又，狀態資訊40以及狀態通知信息42，包含識別資訊(Key ID)，用以明確指定視作各裝置100的根節點34之裝置100。

【0191】 圖16中，顯示狀態資訊40以及狀態通知信息42都是初始設定的狀態。即，Parent ID401中，設定「null」，RootID403中，設定自裝置的Key ID的值(圖16的例中，Key ID1)，height404中設定「0」。

【0192】 如圖16(a)所示，初始設定的狀態資訊40，根據來自其它裝置的狀態資訊40適當更新。以下，說明關於狀態資訊40的更新例。

【0193】 圖17，係顯示根據本實施形態的網路系統1中狀態通知信息42的狀態資訊40更新例圖。圖17中，例如，圖12所示的網路系統1中，顯示裝置100–1、100–5、100–6以此順序形成樹狀構造的情況下更新狀態資訊40內容。

【0194】 裝置100–1、100–5、100–6的狀態資訊40在初始設定後，根據來自其它裝置的狀態通知信息42，依序更新。結果，任一狀態資訊40中，Root ID403內也收納表示裝置100–1的「Key ID1」，height404內收納節點群中的根節點34到葉節點的邊緣數最大值的「2」。

【0195】 各狀態資訊40中的Parent ID401以及Children402內，收納對應節點間的連接關係之Key ID。

【0196】 2進位表示405內，例如，收納對應離葉節點的距離的位元數的識別資訊。圖17中，例如，顯示3種類的例(「0」、「01」、「001」)。也可以意味構成2進位表示405值的位元數越多，離葉節點越遠。即，意味作為2進位表示405具有「0」的裝置100，更接近對應的葉節點，作為2進位表示405具有「001」的裝置100，離對應的葉節點更遠。

【0197】 根據圖17所示的各裝置的狀態資訊40，明確指定節點群的樹狀構造，作為根節點34動作的裝置100，根據明確指定的樹狀構造，決定路由表32，提供給屬於同一節點表的各裝置。透過這樣的程序，可以實現節點群及上述節點群的根節點34的決定以及根節點34中路由表32的決定。

【0198】 又，因為來自各裝置100的狀態通知信息42的傳送時機在各裝置100中任意決定，不一定全部裝置中狀態資訊40的更新完成。因此，各裝置100，當更新狀態資訊40時，以進行延續數代的版本管理為佳。即，保持狀態資訊40更新前後兩方的內容為佳。此時，作為根節點34動作的裝置100，各裝置100保持的狀態資訊40中，根據適當的版本的狀態資訊40，決定路由表32。

【0199】 圖18，係顯示有關根據本實施形態的網路系統1中的路由表決定之處理程序流程圖。圖18所示根據路由表決定的處理，包含節點群30的決定以及狀態資訊40的更新等的處理。圖18所示的各步驟，以裝置100的控制部110(參照圖2)實行(典型地，透過處理器及記憶體合作實現)。

【0200】 參照圖18，連接至其中一個網路時，裝置100初始設定自裝置的狀態資訊40(步驟S100)。

【0201】 接著，裝置100，判斷狀態通知信息42的傳送條件成立與否(步驟S102)。例如，判斷離前次狀態通知信息42的經過時間是否到達預定的時間。

【0202】 狀態通知信息42的傳送條件成立時(步驟S102中YES)，裝置100，根據現在的狀態資訊40產生狀態通知信息42，傳送狀態通知信息42至其它裝置(步驟S104)。又，狀態通知信息42的傳送條件不成立的話(步驟S102中NO)，跳過步驟S104的處理。

【0203】 這樣，裝置100，保持反映與其它裝置的連接關係的狀態資訊40的同時，也實行傳送顯示狀態資訊40內容的狀態通知信息42至其它裝置之處理(步驟S100～S104)。

【0204】 接著，裝置100，判斷是否從其它裝置接收狀態通知信息42(步驟S106)。從其它裝置接收狀態通知信息42的話(步驟S106中YES)，裝置100，根據接收的狀態通知信息42，判斷狀態資訊40的更新是否必要(步驟S108)。判斷狀態資訊40的更新是必要時(步驟S108中YES)，裝置100，更新自裝置的狀態資訊40(步驟S110)。判斷狀態資訊40的更新不是必要時(步驟S108中NO)，跳過步驟S110的處理。

【0205】 這樣，裝置100，根據從其它裝置接收的狀態通知信息42，實行更新狀態資訊40的處理(步驟S106～S110)。

【0206】 另一方面，沒有從其它裝置接收狀態通知信息42的話(步驟S106中NO)，跳過步驟S108及S110的處理。

【0207】 在此，說明關於步驟S18及S110的處理細節。

圖13所示的節點群30，由於決定任意裝置作為根節點34，可以決定各樹狀構造內包含的裝置。作為這樣的根節點34動作的裝置100，根據各裝置100的Key

ID值決定也可以。即，更新狀態資訊40的處理中，接收的狀態通知信息42內包含的視作根節點的裝置(由Root ID422內收納的Key ID明確指定的裝置100)與狀態資訊40內包含的視作根節點的裝置(由Root ID403內收納的Key ID明確指定的裝置100)不一致時，根據預定規則，實現決定一方的裝置100為根節點的處理。

【0208】 本實施形態中，作為預定規則的一例，利用Key ID的大小關係。例如，某範圍的裝置之間決定Key ID最小裝置作為上述範圍的根節點34也可以。此時，各裝置100，參照從相當於母節點的其它裝置接收的狀態通知信息42內包含的Root ID422(參照圖16(b))，判斷是否要更新狀態資訊40。

【0209】 具體地，以下的(1)及(2)的條件成立時，更新狀態資訊40的內容。

【0210】 (1) 狀態資訊40的Root ID403值>從母節點接收的狀態通知信息42的Root ID422值

而且

(2) 狀態資訊40的height404值<從母節點接收的狀態通知信息42的height423值

在此，(1)的條件意味，母節點辨識的根節點34的Key ID，比上述裝置辨識的根節點34的Key ID小，(2)的條件意味，母節點屬於比上述裝置辨識的樹狀構造深的樹狀構造。

【0211】 於是，(1)及(2)的條件成立時，上述裝置，為了套入母節點更新狀態資訊40內容。更具體地，如以下所示，狀態資訊40的Parent ID401、Root ID403、height404，更新從母節點接收的狀態通知信息42內包含的值。

【0212】

・狀態資訊40的Parent ID401←從母節點接收的狀態通知信息42的Key ID424值

・狀態資訊40的RootID403←從母節點接收的狀態通知信息42的Root ID422

值

・狀態資訊40的height404←從母節點接收的狀態通知信息42的height423值+1(增加height423值)

又，決定根節點34的規則，怎樣的規則都可以，決定某範圍的裝置間以Key ID最大的裝置為上述範圍的根節點34也可以，決定最接近Key ID的任意設定值的裝置作為根節點34也可以，此時，只要適當變更上述(1)的條件即可。

【0213】 接著，裝置100，判斷是否從其它裝置接收足夠數量的狀態通知信息42(步驟S112)。從其它裝置接收足夠數量的狀態通知信息42的話(步驟S112中YES)，如下，裝置100，根據各裝置100保持的狀態資訊40，在節點群30(邏輯性規定的裝置100的集合)之間，實行保持成為資料傳送收件地址的裝置搜尋中使用的路由表32之處理(S116、S118、S122、S124)。

【0214】 更具體地，裝置100，根據狀態資訊40，判斷自裝置是否作為根節點34動作(S114)。

【0215】 自裝置作為根節點34動作時(步驟S114中YES)，裝置100，根據自裝置的狀態資訊40以及其它裝置的狀態資訊40，決定路由表32(步驟S116)，傳送決定的路由表32至其它裝置(步驟S118)。

【0216】 這樣，裝置100，根據狀態資訊40，判斷節點群30中自裝置100作為根節點動作時，實行決定路由表32的處理。

【0217】 另一方面，自裝置不作為根節點動作時(步驟S114中NO)，裝置100，傳送自裝置的狀態資訊40至設定為根節點的裝置(步驟S120)，判斷是否從作為根節點動作的裝置接收路由表32(步驟S122)。從作為根節點動作的裝置接收路由表32的話(步驟S122中YES)，裝置100，收納接收的路由表32(步驟S124)。這樣，裝置100，由於從其它裝置100接收路由表32，保持路由表32。

【0218】 又，不從作為根節點動作的裝置接收路由表32的話(步驟S122中

NO)，跳過步驟S124的處理。又，不從其它裝置充分接收足夠數量的狀態通知信息42的話(步驟S112中NO)，重複步驟S102以下的處理。

【0219】 於是，圖18所示的步驟S102～S124的處理，重複實行。

圖19係顯示有關根據本實施形態的網路系統1中各裝置100的封包傳送接收之處理程序流程圖。圖19(a)中，顯示自裝置中應傳送的封包產生時的處理，圖19(b)中，顯示從其它裝置接收封包時的處理 。圖19(a)及圖19(b)所示的各步驟，由裝置100的控制部110(參照圖2)實行(典型地，透過處理器及記憶體合作實現)。

【0220】 參照圖19(a)，裝置100，透過各種應用軟體300等，判斷是否給予以其它裝置作為收件地址的發送封包(步驟S200)。不給予以其它裝置作為收件地址的發送封包的話(步驟S200中NO)，重複步驟S200以下的處理。

【0221】 另一方面，給予以其它裝置作為收件地址的發送封包的話(步驟S200中YES)，裝置100，參照路由表32，傳送發送封包至對應到達收件地址裝置的路徑的其它裝置(步驟S202)。此時，裝置100，如果收件地址裝置包含在自裝置的子孫節點的話，傳送發送封包至對應到達上述子孫節點的路徑的子節點。另一方面，如果收件地址裝置沒包含在自裝置的子孫節點的話，傳送發送封包至自裝置的母節點。根據上述，結束發送封包的傳送處理。

【0222】 參照圖19(b)，判斷是否從其它裝置接收發送封包(步驟S250)。沒從其它裝置接收發送封包的話(步驟S250中NO)，重複步驟S250的處理。

【0223】 另一方面，從其它裝置接收發送封包的話(步驟S250中YES)，裝置100，判斷接收的發送封包是否傳給自裝置 (步驟S252)。接收的發送封包傳給自裝置的話 (步驟S252中YES)，裝置100，接收上述傳送裝置，輸出至對應的應用軟體300(步驟S254)。這樣，接收封包時的處理結束。

【0224】 相對於此，接收的發送封包不是送給自裝置的話(步驟S252中NO)，裝置100，參照路由表32，傳送發送封包至對應到達收件住址裝置的路徑

的其它裝置(步驟S256)。參照此路由表32決定發送端的處理，與步驟S202相同。這樣，接收封包時的處理結束。

【0225】 如上述，根據本實施形態的網路系統1中，每節點群(邏輯性規定的裝置100集合)決定共有路由表32。這樣，由於採用每節點群共有的路由表32，當傳送資料給網路系統1內包含的任意裝置時，可以以更短時間決定其傳送路徑。

【0226】 根據本實施形態的網路系統1中，網路系統1內包含的各裝置100，傳送顯示保持的狀態資訊40內容的狀態通知信息42至其它裝置100。於是，各裝置100，從其它裝置100接收狀態通知信息42時，根據其接收的狀態通知信息42內容，適當更新自裝置保持的狀態資訊40內容。藉由周期性或定期性實行這樣的狀態通知信息42及狀態資訊40的更新處理，即使網路系統1中的裝置100的加入・脫離或連接拓樸空間變化等產生時，也可以維持適當的路由表32。

【0227】 <E.優點>

根據本實施形態的網路系統1，多數裝置存在的網路中，可以提供各裝置可以獨立實現資料通訊的解決方法。

【0228】 這次揭示的實施形態全部的點係例示，不應認為是限制。本發明的範圍不是上述的說明，而是根據申請專利範圍表示，意圖包含與申請專利範圍均等的意義及範圍內的全部變更。

【符號說明】

【0229】

1:網路系統

2:網路

4:存取點

6:行動電話基地台

10:連接

30:節點群

32:路由表

34:根節點

34–1,34–2,34–3:根節點

36:節點

40:狀態資訊

42:狀態通知信息

100:裝置

102:處理器

104:主記憶體

106:儲存體

108:ROM(唯讀記憶體)

110:控制部

120:網路界面

130:顯示部

140:輸入部

150:媒體介面

152:媒體

160:OS(作業系統)

170:通訊處理程式

172:私有密鑰

174:公開密鑰

176:電子證書

178:散列值

180:散列函數

190:IP位址

194:連接表

200:認證機關

210:網路管理表

212:已認證IP位址

214:初期畫面資訊

216:應用軟體資訊

220A,220B:畫面例:

230:利用管理表

232:網路位址

234:房間號碼

236:可使用時間

240:住宿設施

242:無線通訊單元

300:應用軟體

405:2進位表示

RT1,RT2,RT3:路徑

【發明申請專利範圍】

【請求項1】 一種連接複數裝置的網路中的資料傳送方法，上述資料傳送方法，包括：

上述複數裝置分別僅根據從各裝置具有的公開密鑰依照散列函數算出的散列值的全部或一部分，決定各裝置的IP位址全體的步驟；

上述複數裝置分別保持反映各裝置的連接關係之狀態資訊的同時，也傳送顯示上述狀態資訊內容的通知信息至其它裝置的步驟；

上述複數裝置分別根據從其它裝置接收的上述通知信息，更新各裝置保持的狀態資訊的步驟；以及

根據各裝置保持的上述狀態資訊邏輯性規定的裝置集合間，決定上述集合內包含的裝置間保持之資料傳送收件位址的裝置的搜尋中使用的路由表的步驟。

【請求項2】 如請求項1之資料傳送方法，其中，

上述通知信息，包含根據由上述決定各裝置的IP位址全體的步驟所決定的IP位址算出之用以明確指定各裝置的識別資訊。

【請求項3】 如請求項1或2之資料傳送方法，更包括：

上述複數裝置分別傳送各裝置具有的公開密鑰及連結至上述公開密鑰的電子證書至其它裝置的步驟；以及

接收上述公開密鑰及上述電子證書的裝置中，根據從上述公開密鑰依照散列函數算出的散列值，決定上述公開密鑰及上述電子證書的送信源的裝置的IP位址的步驟。

【請求項4】 如請求項1或2之資料傳送方法，其中，

上述決定的IP位址，包含預定的特定用固有值。

【請求項5】 如請求項1或2之資料傳送方法，其中，

上述決定的IP位址，包含對應決定上述IP位址的裝置種類的值。

【請求項6】 一種連接至網路的裝置中的通訊處理方法，包括：

僅根據從公開密鑰依照散列函數算出的散列值的全部或一部分，決定自裝置的IP位址全體的步驟；

保持反映與其它裝置的連接關係的狀態資訊的同時，也傳送顯示上述狀態資訊內容的通知信息至其它裝置的步驟；

根據從其它裝置接收的上述通知信息，更新上述狀態資訊的步驟；以及

根據各裝置保持的上述狀態資訊，邏輯性規定的裝置集合間，保持資料傳送收件位址之裝置的搜尋中使用的路由表的步驟。

【請求項7】 如請求項6之通訊處理方法，其中，

上述通知信息，包含根據由上述決定自裝置的IP位址全體的步驟所決定的自裝置的IP位址算出之用以明確指定自裝置的識別資訊。

【請求項8】 如請求項6或7之通訊處理方法，更包括：

根據上述狀態資訊，判斷上述集合中自裝置作為根節點(root node) 動作時，決定上述路由表的步驟。

【請求項9】 如請求項6或7之通訊處理方法，其中：

保持上述路由表的步驟，包括從其它裝置接收上述路由表的步驟。

【請求項10】 如請求項6或7之通訊處理方法，其中：

上述狀態資訊及上述通知信息，包含用以明確指定視作根節點(root node)的裝置的識別資訊；

上述更新上述狀態資訊的步驟，包括：上述接收的通知信息內包含的視作根節點的裝置與上述狀態資訊內包含的視作根節點的裝置不一致時，根據預定的規則，決定一方的裝置為根節點的步驟。

【請求項11】 如請求項6或7之通訊處理方法，更包括：

從認證機關取得連結至上述公開密鑰的電子證書的步驟；以及

傳送上述公開密鑰及上述電子證書至其它裝置的步驟。

【請求項12】 如請求項6或7之通訊處理方法，更包括：

從其它裝置接收上述公開密鑰以及連結至上述公開密鑰的電子證書時，判斷上述電子證書正當性的步驟；以及

判斷上述電子證書正當時，根據從上述公開密鑰依照散列函數算出的散列值，決定上述其它裝置的IP位址的步驟。

【請求項13】 如請求項6或7之通訊處理方法，其中，

上述決定的自裝置的IP位址，包含預定的特定用固有值。

【請求項14】 如請求項6或7之通訊處理方法，其中，

上述決定的自裝置的IP位址，包含對應決定上述IP位址的裝置種類的值。

【請求項15】 一種連接至網路的裝置中的通訊處理方法，包括：

接收其它裝置具有的公開密鑰及連結至上述公開密鑰的電子證書的步驟；

判斷上述電子證書正當性的步驟；

判斷上述電子證書正當時，將僅根據從上述公開密鑰依照散列函數算出的散列值的全部或一部分決定的IP位址全體，決定作為上述其它裝置的已認證IP位址的步驟；以及

回應來自上述其它裝置的要求，提供對應上述其它裝置的上述已認證IP位址的服務之步驟。

【請求項16】 如請求項15之通訊處理方法，其中，

決定上述公開密鑰，使根據從上述公開密鑰依照上述散列函數算出的散列值決定的IP位址與預定的格式一致。

【請求項17】 一種通訊裝置，包括：

網路界面，用以連接至網路；以及

控制部，連接至上述網路界面；

其中，上述控制部，實行：

僅根據從公開密鑰依照散列函數算出的散列值的全部或一部分，決定自裝置的IP位址全體的處理；

保持反映與其它裝置的連接關係之狀態資訊的同時，也傳送顯示上述狀態資訊內容的通知信息至其它裝置的處理；

根據從其它裝置接收的上述通知信息，更新上述狀態資訊的處理；以及

根據各裝置保持的上述狀態資訊邏輯性規定的裝置集合間，保持資料傳送收件位址之裝置的搜尋中使用的路由表的處理。

【請求項18】一種通訊處理程式，用於具有用以連接至網路的網路界面之電腦，當透過上述電腦實行上述通訊處理程式時，使上述電腦實行請求項6～16中任一項的通訊處理方法。

【發明圖式】

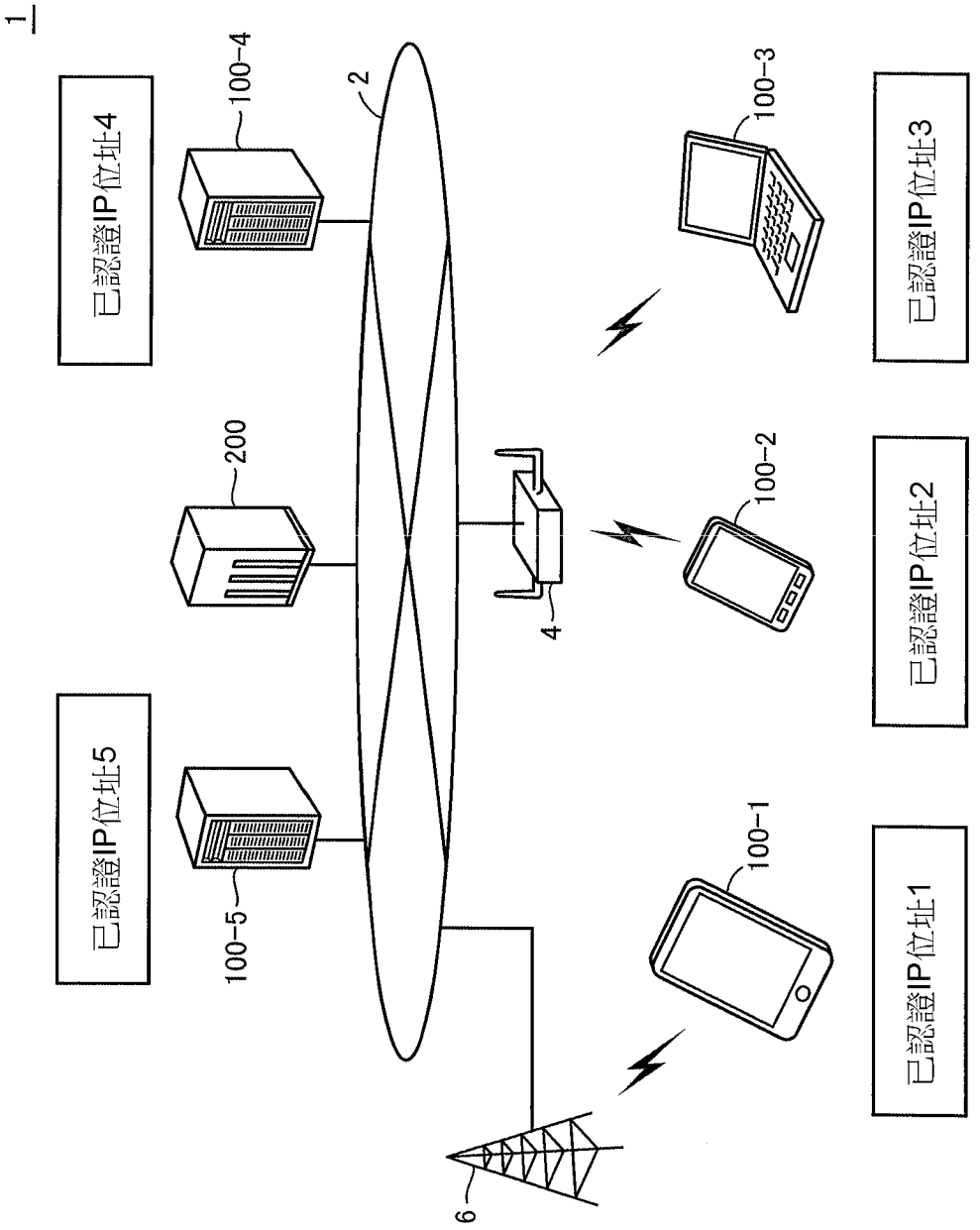

1
已認證IP位址4
100-4
2
100-3
已認證IP位址3
200
4
100-2
已認證IP位址2
已認證IP位址5
100-5
100-1
已認證IP位址1
6

圖1

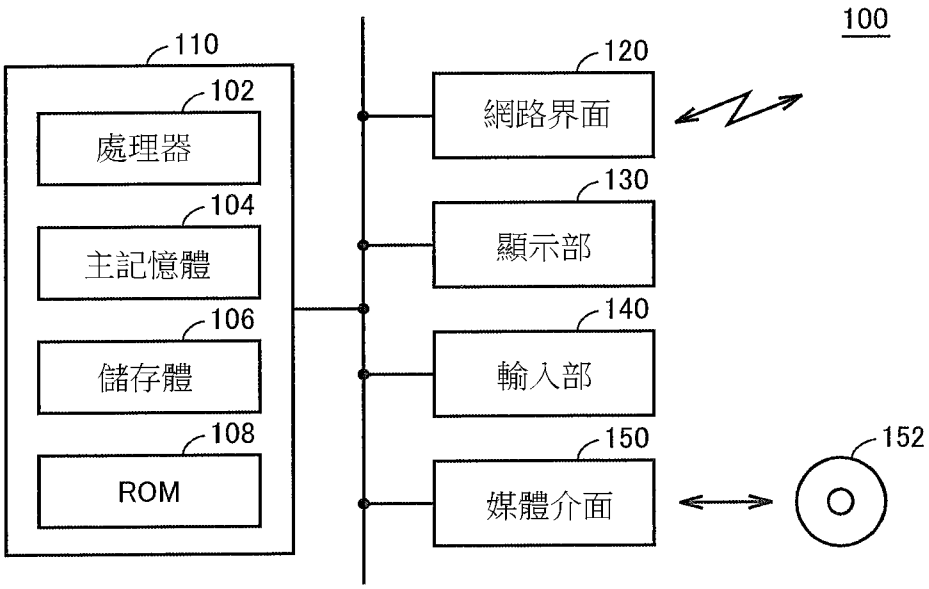

100
110
102
處理器
104
主記憶體
106
儲存體
108
ROM
120
網路界面
130
顯示部
140
輸入部
150
媒體介面
152

圖2

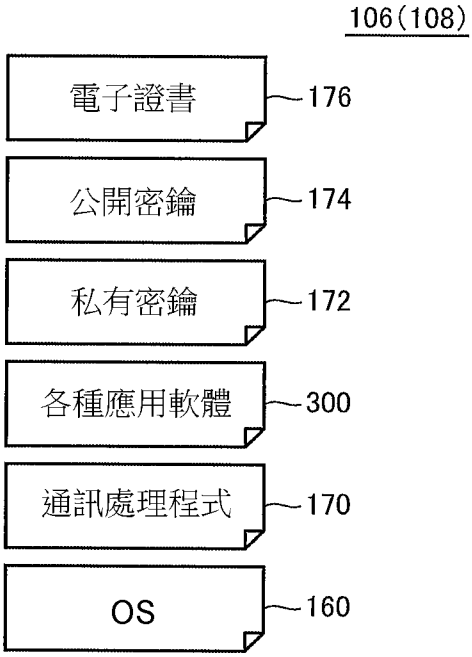

106(108)
電子證書
176
公開密鑰
174
私有密鑰
172
各種應用軟體
300
通訊處理程式
170
OS
160

圖3

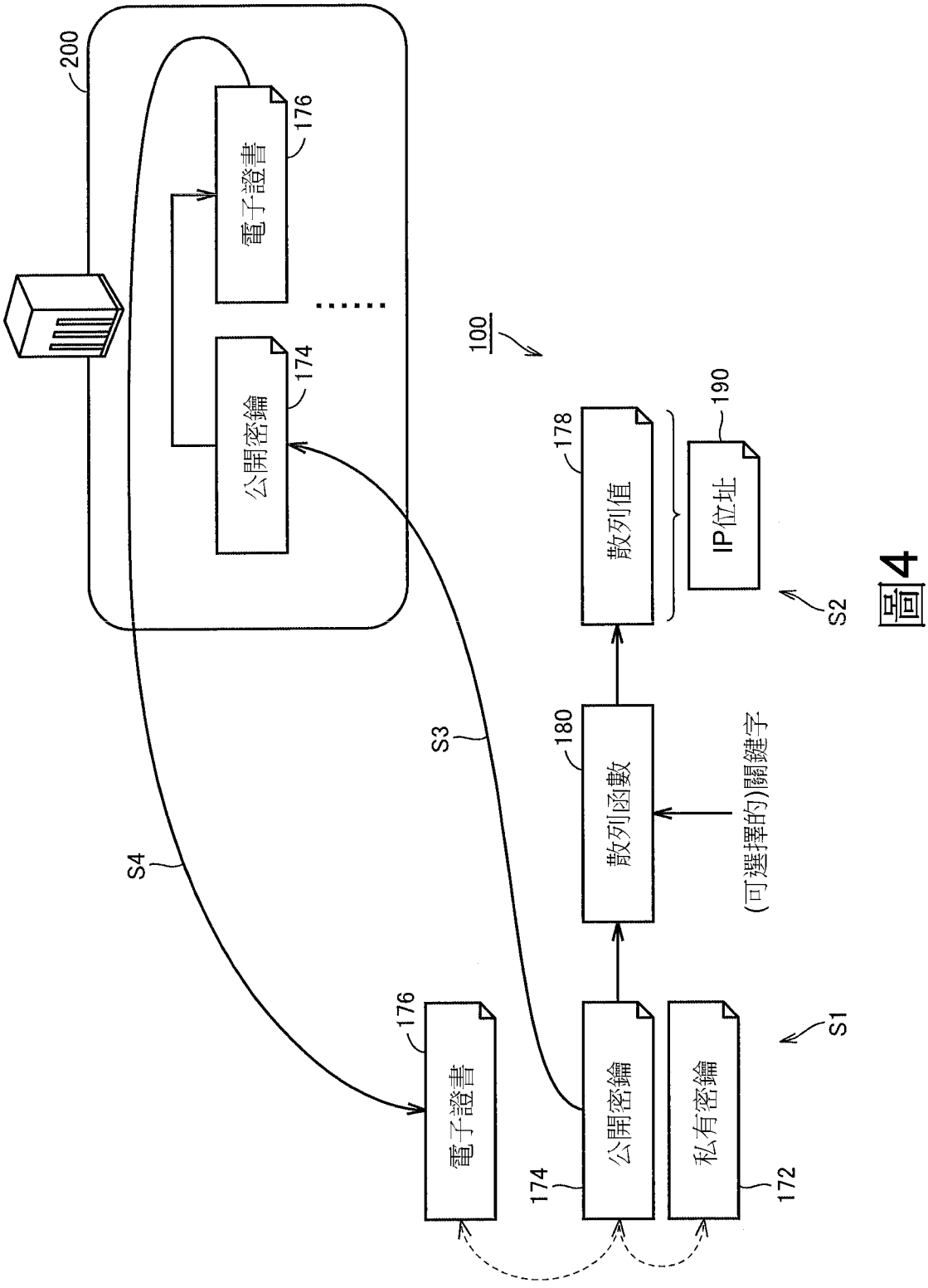

200
176
電子證書
174
公開密鑰
100
178
散列值
190
IP位址
S2
S3
S4
180
散列函數
(可選擇的)關鍵字
176
電子證書
174
公開密鑰
私有密鑰
172
S1

圖4

值(16進位表示)	裝置的種類
00	個人電腦(PC)
01	智慧型手機、平板電腦、可穿戴裝置
02	資訊家電
03	車輛
04	儀器

圖5

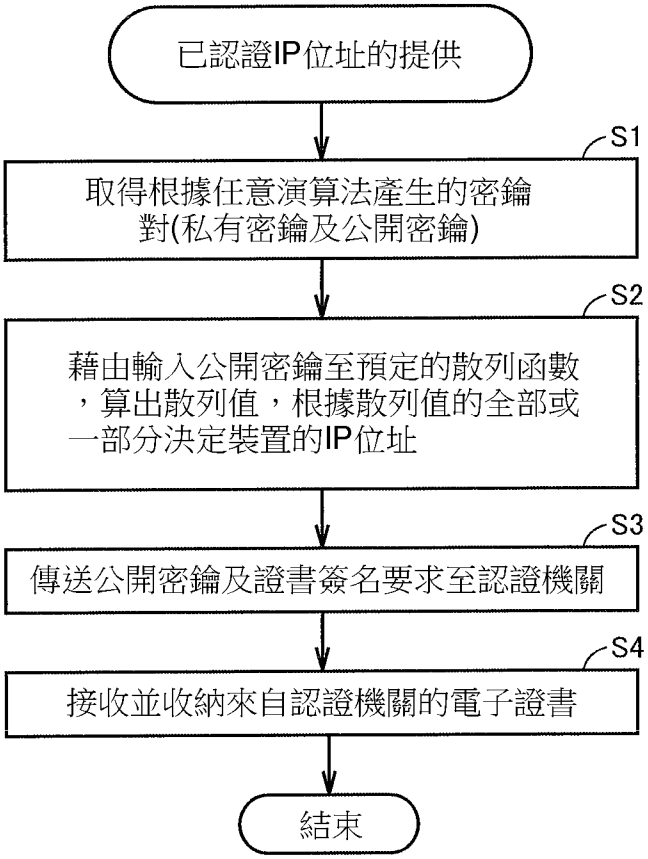

已認證IP位址的提供
S1
取得根據任意演算法產生的密鑰對(私有密鑰及公開密鑰)
S2
藉由輸入公開密鑰至預定的散列函數，算出散列值，根據散列值的全部或一部分決定裝置的IP位址
S3
傳送公開密鑰及證書簽名要求至認證機關
S4
接收並收納來自認證機關的電子證書
結束

圖6

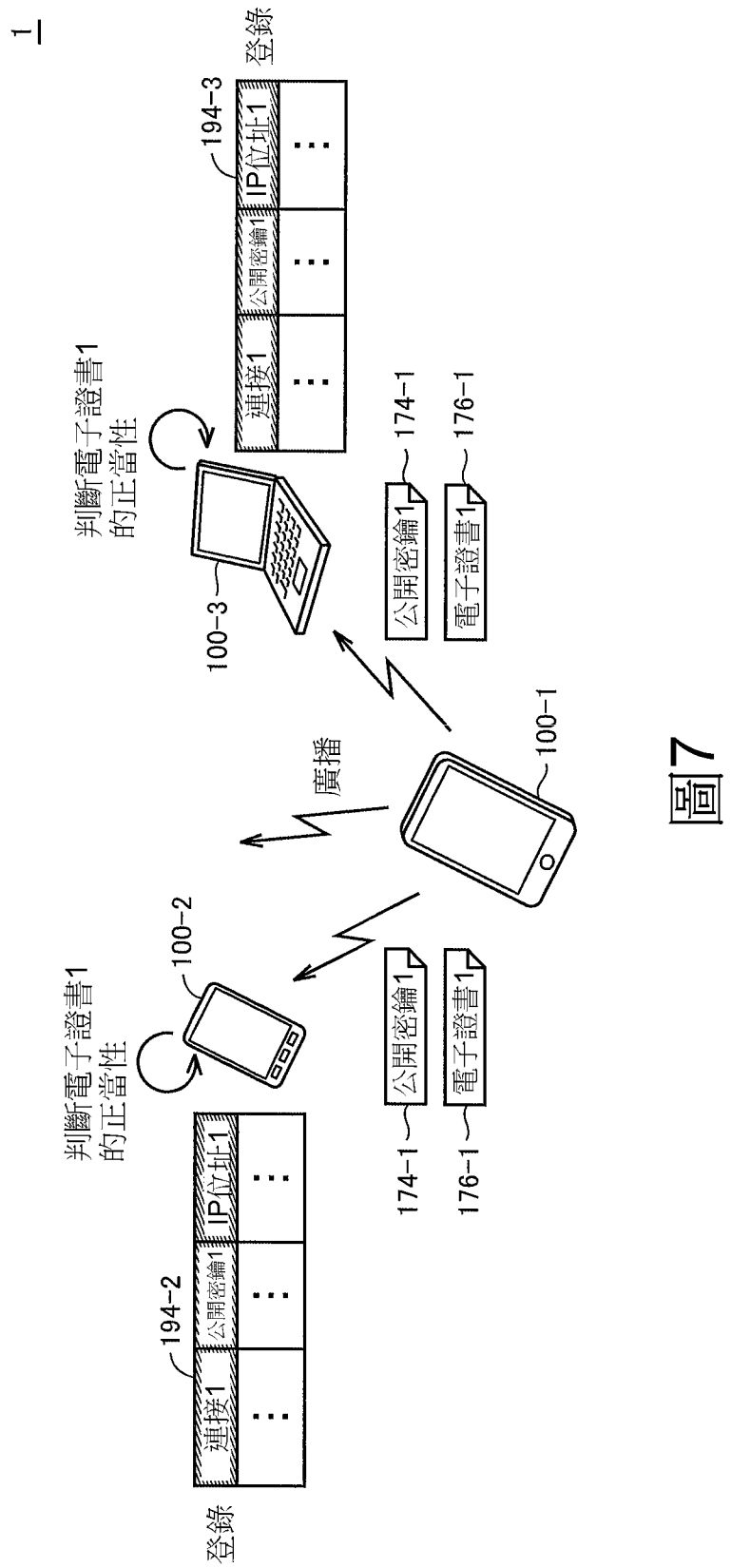

1
登錄
194-3
連接1
公開密鑰1
IP位址1
判斷電子證書1的正當性
100-3
174-1
公開密鑰1
176-1
電子證書1
廣播
100-1
100-2
判斷電子證書1的正當性
174-1
公開密鑰1
176-1
電子證書1
登錄
194-2
連接1
公開密鑰1
IP位址1

圖7

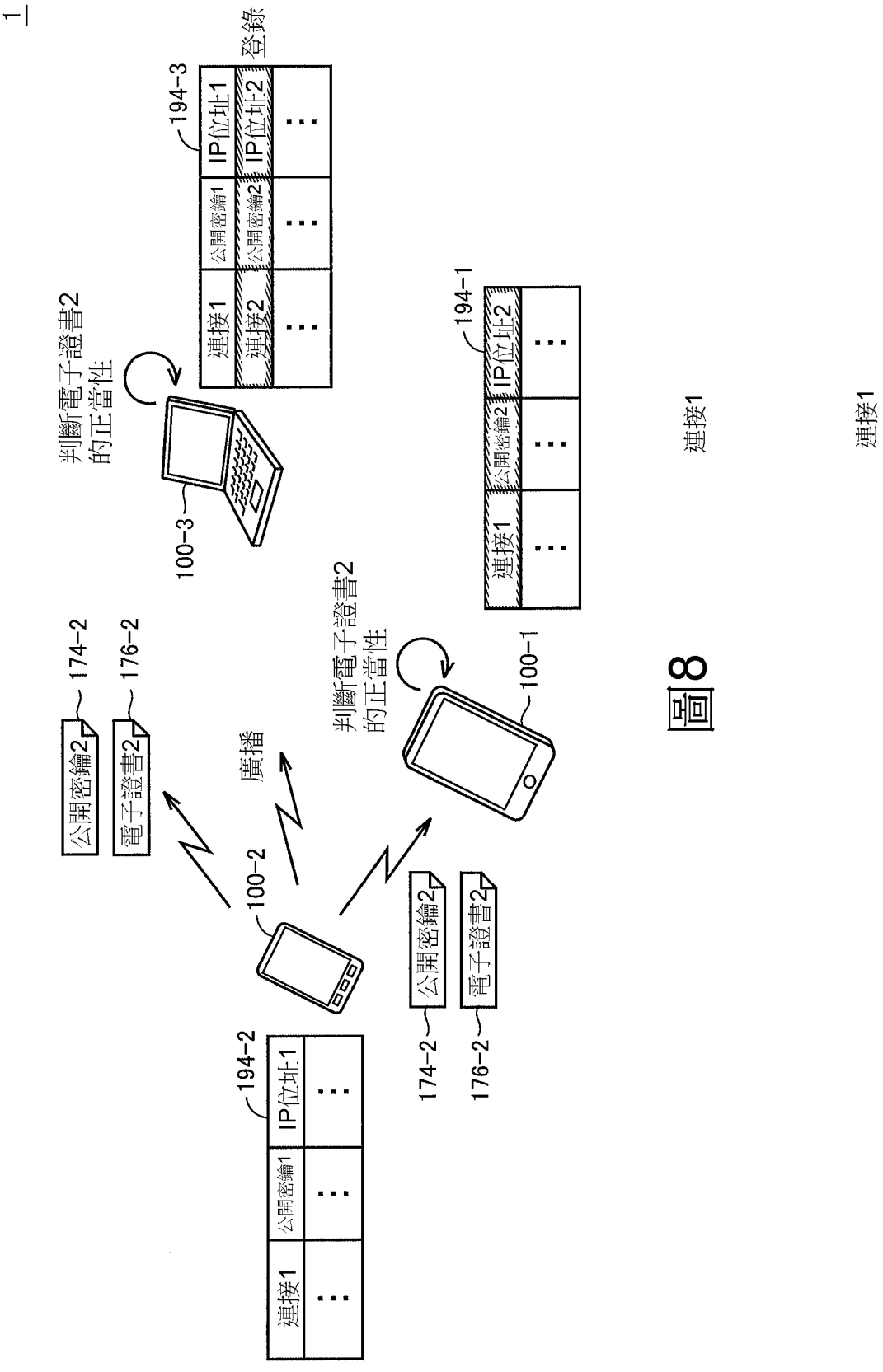

1
登錄
194-3
連接1
公開密鑰1
IP位址1
連接2
公開密鑰2
IP位址2
判斷電子證書2的正當性
100-3
194-1
連接1
公開密鑰2
IP位址2
判斷電子證書2的正當性
100-1
174-2
公開密鑰2
176-2
電子證書2
廣播
100-2
194-2
連接1
公開密鑰1
IP位址1
174-2
公開密鑰2
176-2
電子證書2
連接1
連接1

圖8

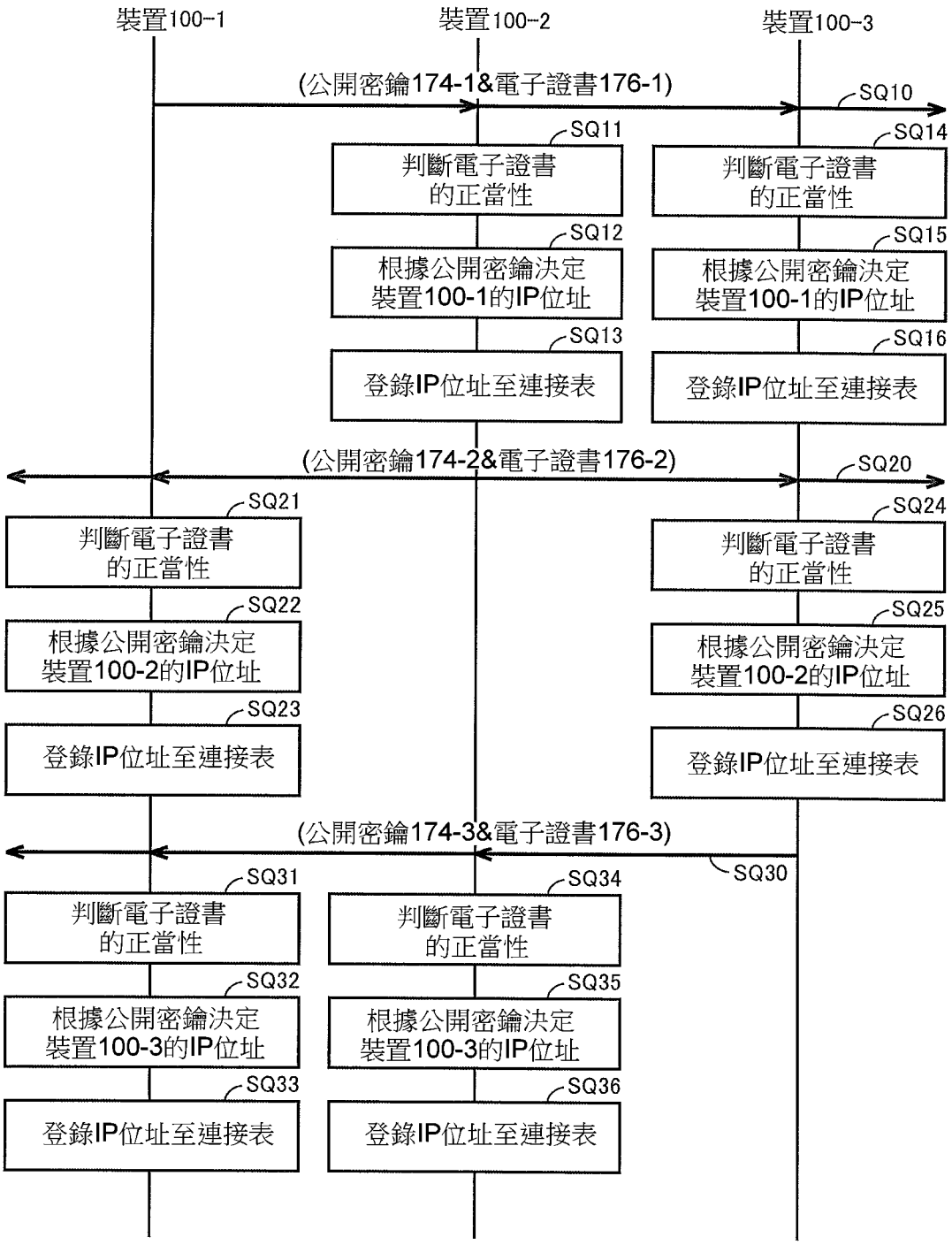

裝置100-1
裝置100-2
裝置100-3
(公開密鑰174-1&電子證書176-1)
SQ10
SQ11
判斷電子證書的正當性
SQ14
判斷電子證書的正當性
SQ12
根據公開密鑰決定裝置100-1的IP位址
SQ15
根據公開密鑰決定裝置100-1的IP位址
SQ13
登錄IP位址至連接表
SQ16
登錄IP位址至連接表
(公開密鑰174-2&電子證書176-2)
SQ20
SQ21
判斷電子證書的正當性
SQ24
判斷電子證書的正當性
SQ22
根據公開密鑰決定裝置100-2的IP位址
SQ25
根據公開密鑰決定裝置100-2的IP位址
SQ23
登錄IP位址至連接表
SQ26
登錄IP位址至連接表
(公開密鑰174-3&電子證書176-3)
SQ30
SQ31
判斷電子證書的正當性
SQ34
判斷電子證書的正當性
SQ32
根據公開密鑰決定裝置100-3的IP位址
SQ35
根據公開密鑰決定裝置100-3的IP位址
SQ33
登錄IP位址至連接表
SQ36
登錄IP位址至連接表

圖9

(a)

210

IP位址	初始畫面	優先號
fc03:0:0:0:2ba:ff:fe9a:4ca2	0005	82849416
fc03:0:0:0:2ba:ff:28ca:8a00	0004	18384678
fc03:0:0:0:2ba:ff:a8b2:4052	0015	98587518
⋮	⋮	⋮

212 214 216

(b)

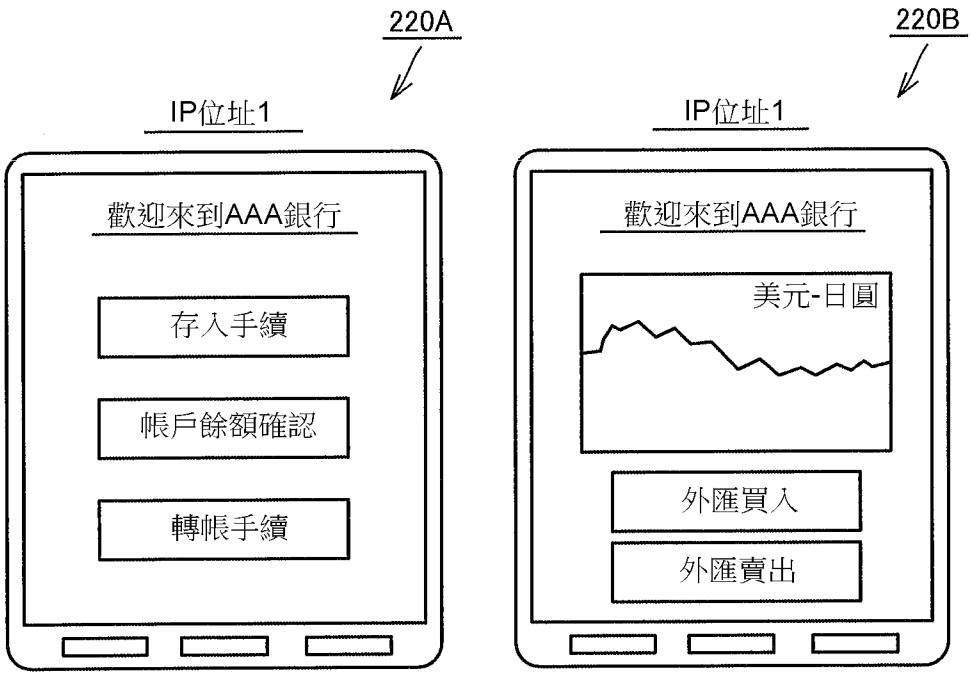


圖10

230

(a)

IP位址	房間號碼	有效期限
fc03:0:0:0:2ba:ff:fe9a:4ca2	2001	180801:15:00-180802:10:00
fc03:0:0:0:2ba:ff:28ca:8a00	2002	180801:15:00-180804:10:00
fc03:0:0:0:2ba:ff:a8b2:4052	2003	180802:15:00-180804:10:00
⋮	⋮	⋮

232 234 236

(b)

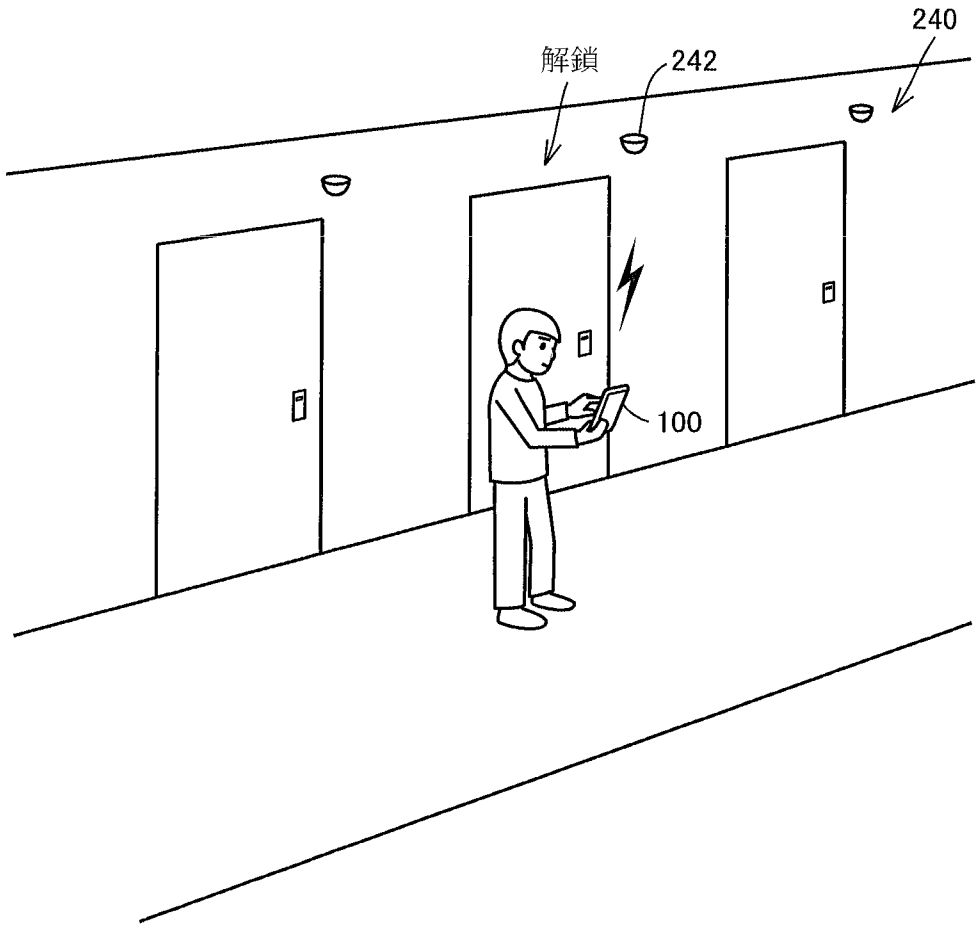


圖11

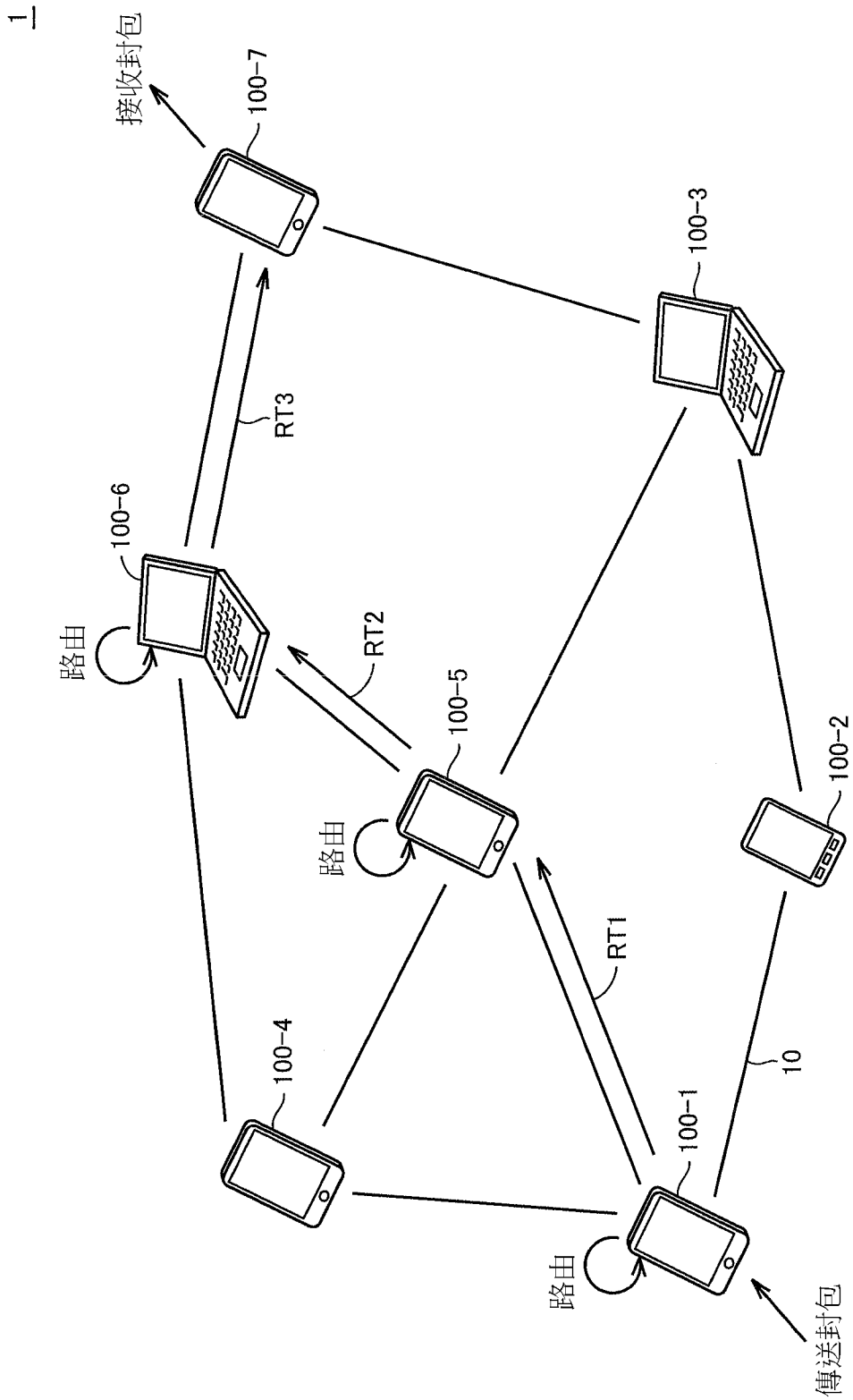

1
接收封包
100-7
100-3
RT3
100-6
路由
RT2
100-5
路由
100-2
RT1
100-4
10
100-1
路由
傳送封包

圖12

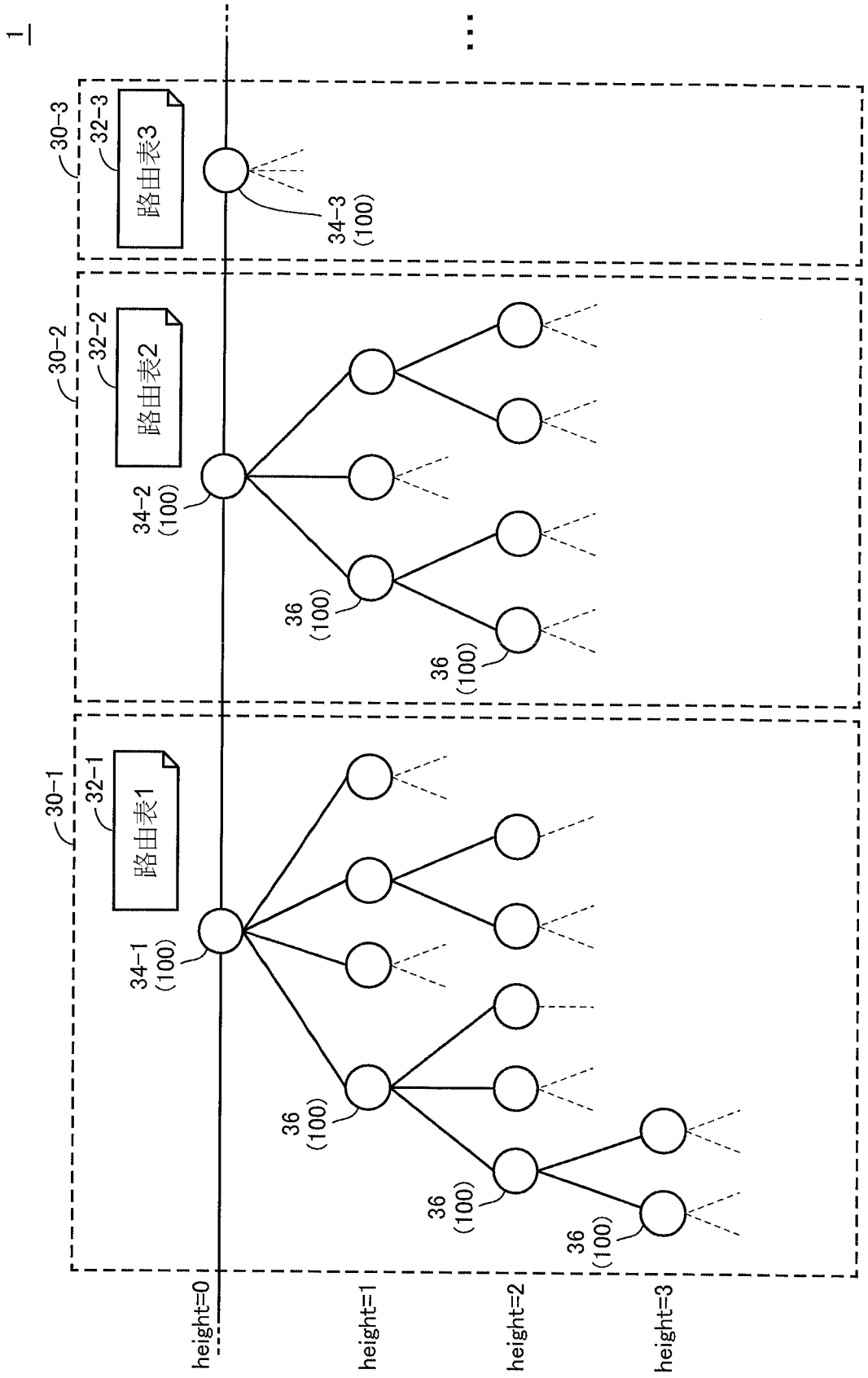

1
30-1
32-1
路由表1
34-1
(100)
30-2
32-2
路由表2
34-2
(100)
30-3
32-3
路由表3
34-3
(100)
36
(100)
height=0
height=1
height=2
height=3

圖13

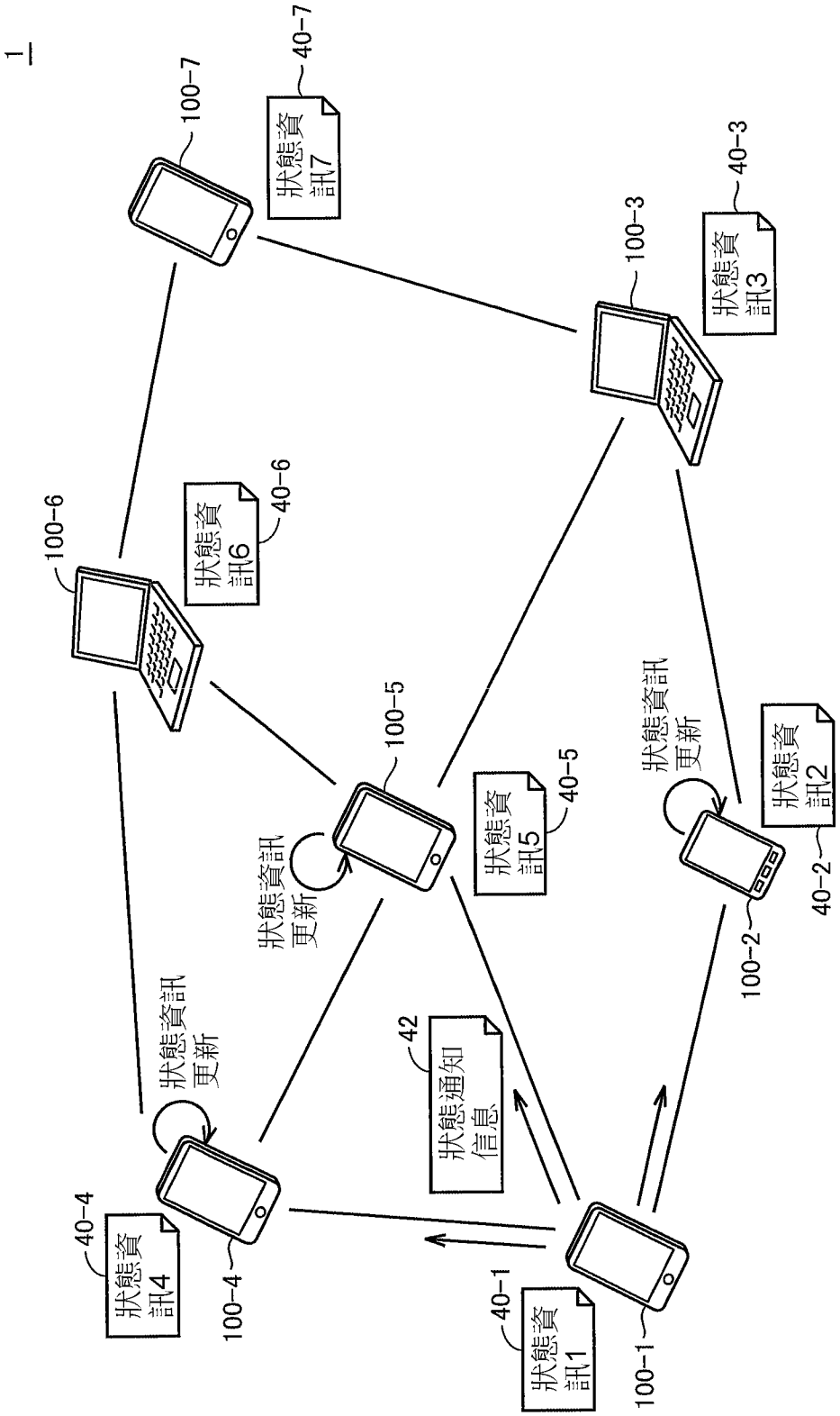

1
100-7
40-7
狀態資訊7
100-3
40-3
狀態資訊3
100-6
40-6
狀態資訊6
100-5
狀態資訊更新
40-5
狀態資訊5
狀態資訊更新
40-2
狀態資訊2
100-2
狀態資訊更新
42
狀態通知信息
40-4
狀態資訊4
100-4
40-1
狀態資訊1
100-1

圖14

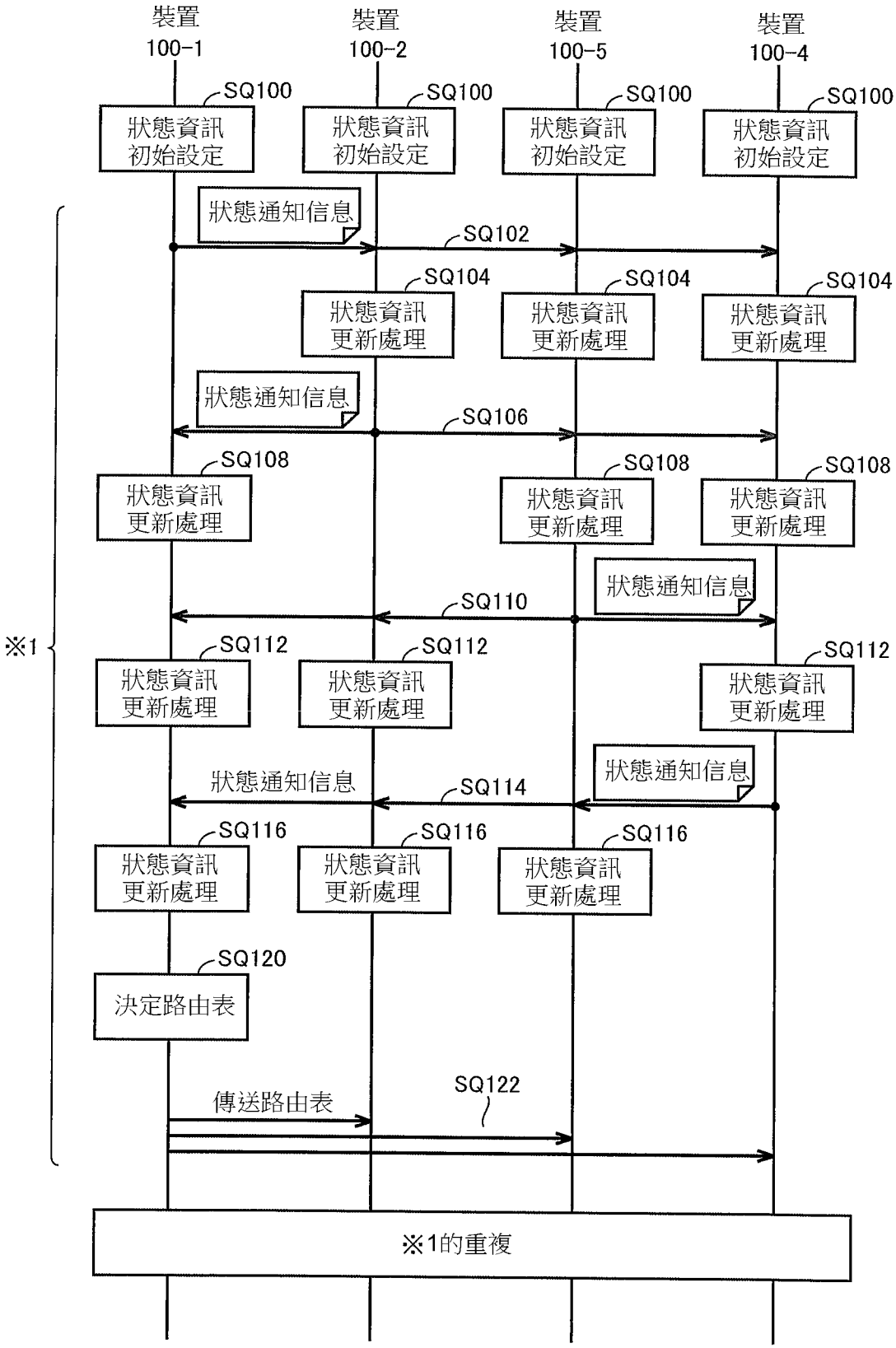

裝置
100-1
裝置
100-2
裝置
100-5
裝置
100-4
SQ100
狀態資訊
初始設定
狀態通知信息
SQ102
SQ104
狀態資訊
更新處理
SQ106
SQ108
SQ110
SQ112
SQ114
SQ116
SQ120
決定路由表
傳送路由表
SQ122
※1
※1的重複

圖15

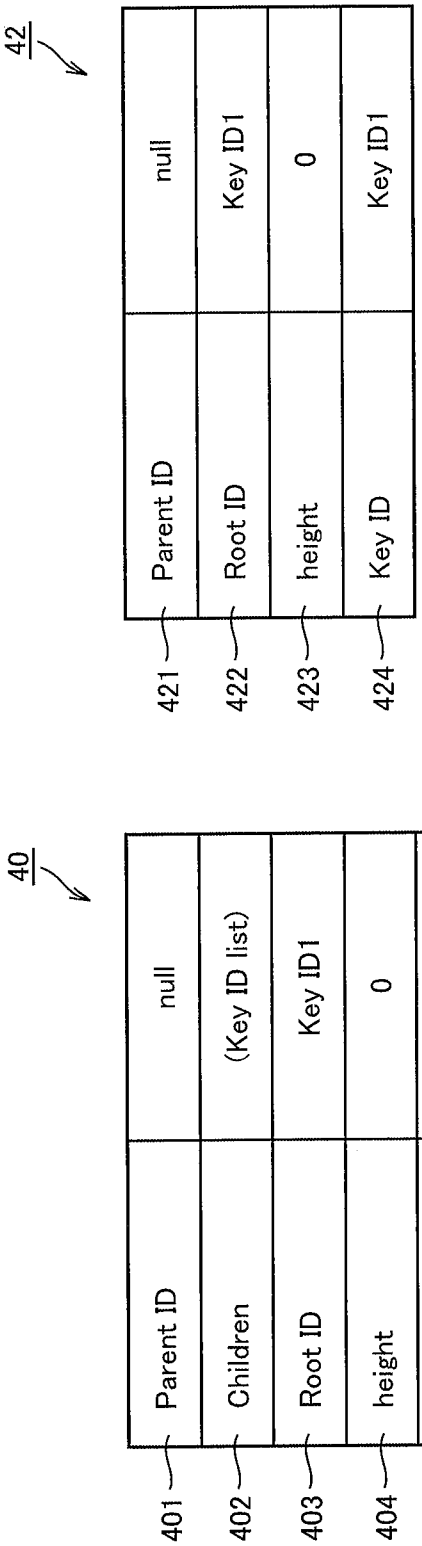

40
Parent ID
null
401
Children
(Key ID list)
402
Root ID
Key ID1
403
height
0
404
Binary Representation
405
(a)
42
Parent ID
null
421
Root ID
Key ID1
422
height
0
423
Key ID
Key ID1
424
(b)

圖16

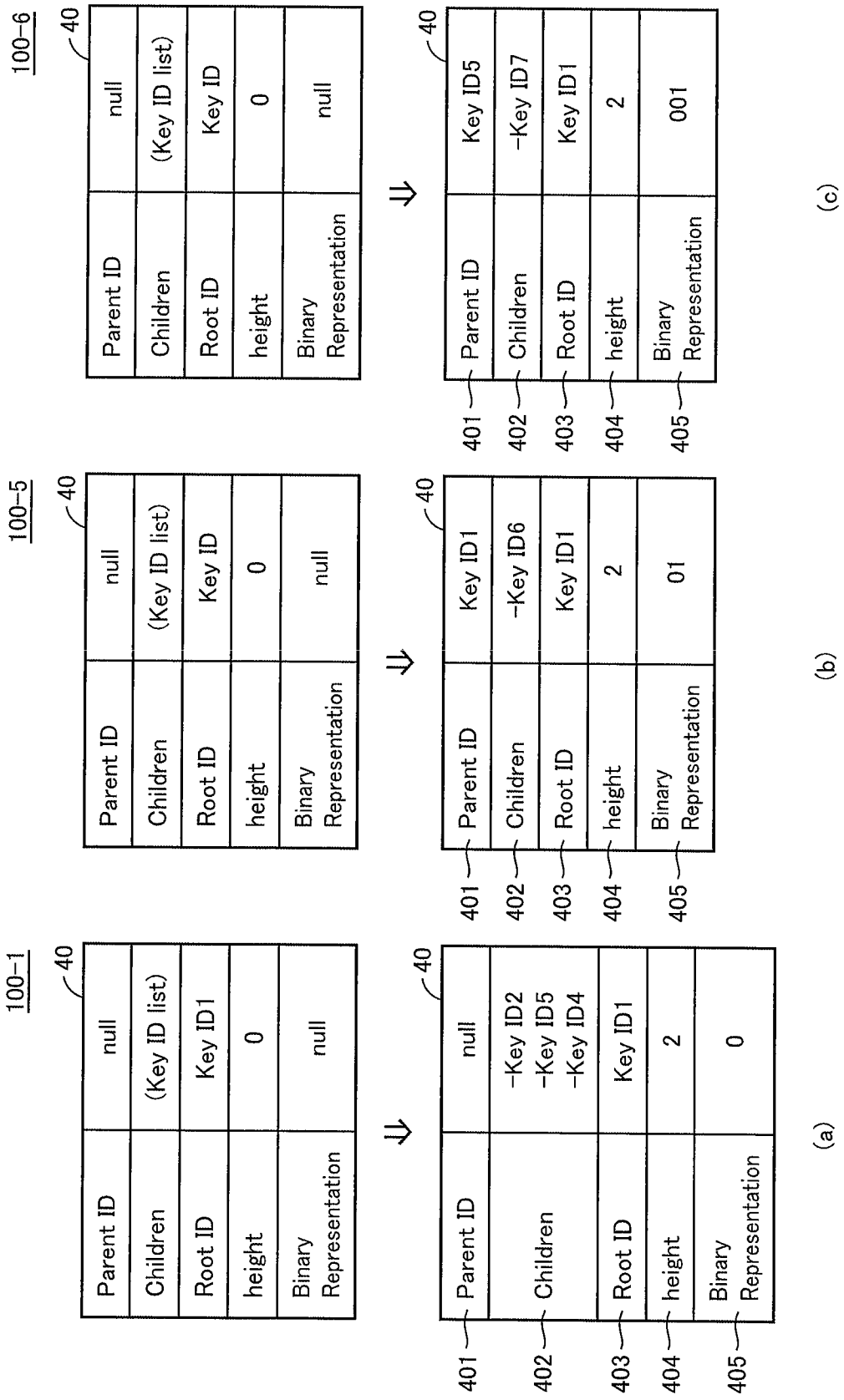

100-1
100-5
100-6
40
Parent ID
Children
Root ID
height
Binary Representation
null
(Key ID list)
Key ID1
0
2
01
001
-Key ID2
-Key ID5
-Key ID4
-Key ID6
-Key ID7
Key ID5
Key ID
401
402
403
404
405
(a)
(b)
(c)

圖17

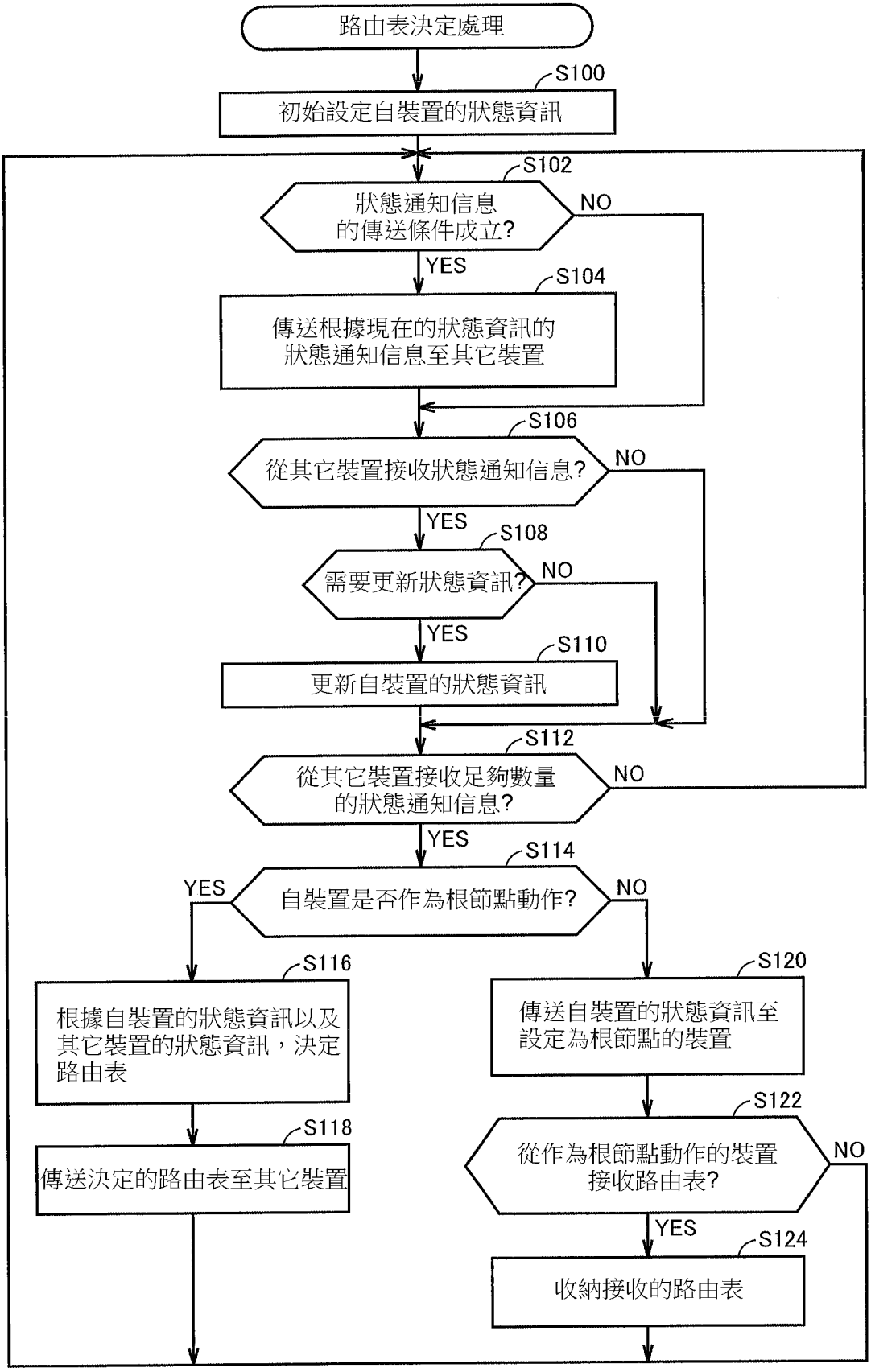

路由表決定處理
S100
初始設定自裝置的狀態資訊
S102
狀態通知信息
的傳送條件成立?
NO
YES
S104
傳送根據現在的狀態資訊的
狀態通知信息至其它裝置
S106
從其它裝置接收狀態通知信息?
NO
YES
S108
需要更新狀態資訊?
NO
YES
S110
更新自裝置的狀態資訊
S112
從其它裝置接收足夠數量
的狀態通知信息?
NO
YES
S114
自裝置是否作為根節點動作?
YES
NO
S116
根據自裝置的狀態資訊以及
其它裝置的狀態資訊，決定
路由表
S118
傳送決定的路由表至其它裝置
S120
傳送自裝置的狀態資訊至
設定為根節點的裝置
S122
從作為根節點動作的裝置
接收路由表?
NO
YES
S124
收納接收的路由表

圖18

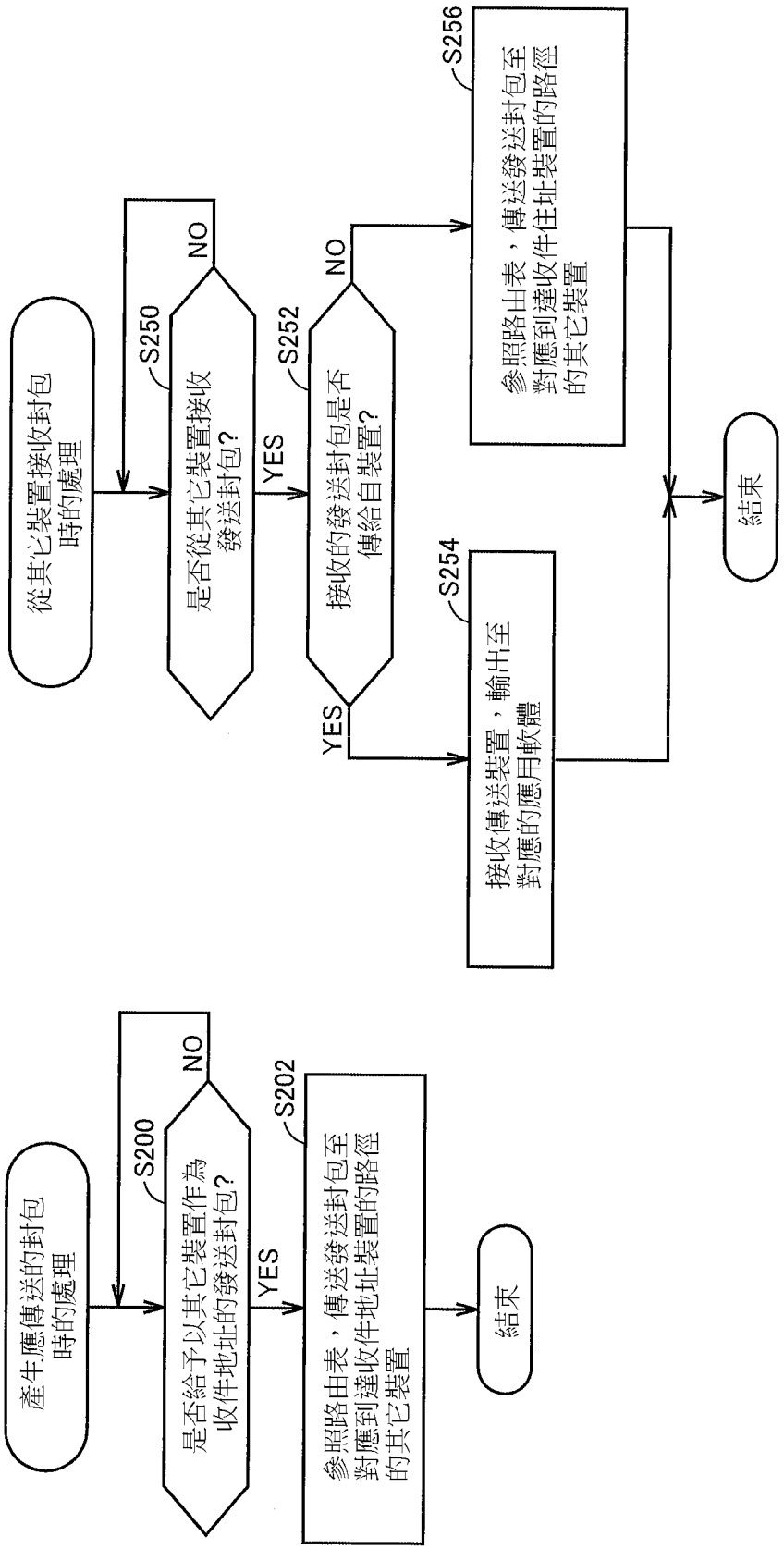

產生應傳送的封包時的處理
S200
是否給予以其它裝置作為收件地址的發送封包?
NO
YES
S202
參照路由表，傳送發送封包至對應到達收件地址裝置的路徑的其它裝置
結束
(a)
從其它裝置接收封包時的處理
S250
是否從其它裝置接收發送封包?
NO
YES
S252
接收的發送封包是否傳給自裝置?
NO
YES
S254
接收傳送裝置，輸出至對應的應用軟體
S256
參照路由表，傳送發送封包至對應到達收件住址裝置的路徑的其它裝置
結束
(b)

圖19