

公告本

申請日期	91 年 4 月 18 日
案 號	91108003
類 別	H4L 9/32

A4
C4

(以上各欄由本局填註)

576071

發明專利說明書

一、發明 名稱	中 文	終端通訊系統
	英 文	
二、發明 人	姓 名	(1) 山本正明 (2) 平松孝朗 (3) 鷺尾諭
	國 籍	(1) 日本 (2) 日本 (3) 日本
	住、居所	(1) 日本國東京都千代田區永田町二丁目一番一號山王公園鐵塔N T T都科摩知的財產部內 (2) 日本國東京都千代田區永田町二丁目一番一號山王公園鐵塔N T T都科摩知的財產部內 (3) 日本國東京都千代田區永田町二丁目一番一號山王公園鐵塔N T T都科摩知的財產部內
三、申請人	姓 名 (名稱)	(1) N T T 都科摩股份有限公司 株式会社エヌ・ティ・ティ・ドコモ
	國 籍	(1) 日本
	住、居所 (事務所)	(1) 日本國東京都千代田區永田町二丁目一番一號
	代 表 人 姓 名	(1) 立川敬二

裝

訂

線

(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

日本 2001 年 4 月 19 日 2001-121567 ☒有主張優先權

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)

【技術領域】

本發明，係關於一種終端通訊系統，多數的通訊終端介由網路執行與其他終端通訊的同時，各通訊終端與其他通訊終端可以不介由網路而執行區域通訊。

【習知技術】

從行動終端介由網際網路發訊要求，執行書本訂購，或入場券預約，這種所謂的電子商業交易普遍地被執行。於此類電子商業交易中，商品的訂購是被發送至假想商店，具體而言是與網際網路連接之伺服器。然後，作為商品之入場券，被郵送至訂貨者或便利商店等店鋪。後者的情形中，訂貨者前往店鋪領取入場券。

像這樣的電子商業交易，可由不特定多數的人介由可執行通訊之網際網路等通訊網執行，所以為了防止冒充，必須確實特定發訊者（例如利用者）與收訊者（例如伺服器）。為此，普遍是執行使用公開鑰編碼方式的相互認證。在認證處理中，發訊者將自己的公開鑰發送至認證台，認證台將發訊者的公開鑰以認證台的密碼鑰編碼產生編碼公開鑰，將包含編碼公開鑰之證明書送回發訊者。收訊者也同樣從認證台得到證明書。

接著，發訊者與收訊者在金錢資料或個人資料等通訊前，介由網際網路交換證明書，將被交換之證明書使用認證台之公開鑰解碼，執行相互認證。亦即，於電子商業交易之相互認證是依據經由網際網路之證明書的交換而執行

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明(2)

。

當此類相互認證成功，即執行商業交易。當商業交易成立，訂購之收訊者將商品送至訂貨者，並從訂貨者收取貸款。

另一方面，電子商業交易中，也有不伴隨此類相互認證而執行者。例如利用設置於便利商店等店舖中之服務終端的電子商業交易為其典型例子。在此，服務終端預先連接通訊網，可以說作為自動販賣機而具有功能。利用者操作該服務終端，投入必要的金錢，其主旨介由通訊網通知伺服器，在伺服器之控制下，依據服務終端執行演唱會入場券的發行或遊戲軟體的下載等。接著，利用者可從服務終端領取商品之演唱會入場券或遊戲軟體。

以上，舉2種電子商業交易的型態，兩者中有利有弊。

首先，在前者的電子商業交易中，僅依據介由通訊網之資訊收授來執行電子商業交易，因而利用者不投入金錢即可取得商品。但是，由於攜帶型電話本身不會排出入場券等的商品，利用者只能由郵送收到商品。為此，得到想要的商品須花上時間。

另一方面，後者的電子商業交易，是從服務終端排出商品或提供服務，所以利用者只要到店舖就可以得到想要的商品。但是，在該電子商業交易中，利用者和伺服器不進行相互認證，也不執行金錢資料的收授。因此利用者若不付現金，就無法得到商品。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(3)

該電子商業交易不使用所謂介由通訊網相互認證、金錢資訊收授的手段，是因為使用這些手段，要保護商品提供者和利用者雙方是很困難的。亦即，在利用者立場來看，將為了認證的資訊或金錢資訊輸入沒有來歷保證的服務終端是很危險的，對商品提供者而言也無法得知服務終端的利用者身分，要信賴來自這樣的人所提供之金錢資訊而提供商品是很危險的。

【發明之揭示】

本發明是有鑑於上述情事，目的在提供一種不需伴隨投入金錢這樣繁複的手續，而可經由服務終端執行商業交易的手段。

更具體的說，本發明是依據利用者攜帶之行動終端，和服務終端之間1對1的區域通訊使商業交易成為可能。在執行像這樣的商業交易時，必須採取對策防止服務終端的假冒及金錢資訊的流出。本發明之特徵，即為該對策。

本發明是提供一種終端通訊方法，其特徵為行動終端從伺服器取得特定資料，服務終端依據認證台的密碼鑰從認證台取得被編碼之伺服器證明書，上述行動終端從上述服務終端取得上述伺服器證明書，根據上述認證台的公開鑰查證上述伺服器證明書，上述行動終端限於根據上述伺服器證明書查證上述服務終端為正當時，依據不經由網路之區域通訊，將上述特定資料發訊至上述服務終端。

在最佳形態中，上述伺服器使用上述認證台的公開鑰

五、發明說明(4)

，執行從上述服務終端所取得之伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，將上述服務終端中爲了實行發訊上述特定資料之處理的通訊應用軟體發訊至上述行動終端，上述行動終端依據上述通訊應用軟體之實行執行上述特定資料的發訊。

又其他最佳形態中，上述行動終端從上述認證台取得依上述認證台之密碼鑰被編碼的客戶證明書，上述服務終端從上述行動終端取得上述客戶證明書，根據上述認證台之公開鑰查證上述客戶證明書，限於得到肯定查證結果，執行與上述行動終端之區域通訊。

又其他最佳形態中，上述行動終端經由無線通訊網執行與上述伺服器的通訊。

又其他最佳形態中，上述行動終端依據使用上述認證台之公開鑰執行上述伺服器證明書之解碼，判斷上述服務終端的正當性。

又其他最佳形態中，上述服務終端依據使用上述認證台之公開鑰執行上述客戶證明書之解碼，判斷上述行動終端的正當性。

又其他最佳形態中，上述行動終端與上述服務終端之間的通訊，是依據紅外線通訊或近距離無線通訊所執行。

又其他最佳形態中，上述行動終端與上述服務終端之間的通訊，是編碼通訊。

又其他最佳形態中，上述伺服器以及上述認證台的一方可兼具他方。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(5)

此外，本發明提供一種終端通訊系統，具備認證台、伺服器、服務終端、和行動終端，其特徵為：上述服務終端，具備記憶由上述認證台所發行之伺服器證明書的手段，和對應於來自上述行動終端之要求將上述伺服器證明書發訊至上述行動終端的手段；上述行動終端，具備從上述伺服器取得特定資料的手段，和從上述服務終端取得上述伺服器證明書的手段，和將上述伺服器證明書使用上述認證台之公開鑰查證的手段，和僅於得到肯定上述服務終端之正當性的查證結果時，朝上述服務終端發訊特定資料的手段。

在其他最佳形態中，上述伺服器，具備使用上述認證台之公開鑰，執行從上述服務終端所取得之伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，將上述服務終端為實行發訊上述特定資料之處理的通訊應用軟體發訊至上述行動終端之手段，上述行動終端，依據上述通訊應用軟體之實行執行上述特定資料之發訊。

服務終端，具備從上述行動終端取得上述客戶證明書，將上述客戶證明書依據上述認證台之公開鑰查證，僅於得到肯定上述行動終端之正當性的查證結果時，許可與上述行動終端之區域通訊的手段。

又其他最佳形態中，上述伺服器以及上述認證台的一方可兼具他方。

又本發明，提供一種行動終端，其特徵為具備從伺服

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(6)

器取得特定資料之手段，和根據認證台之密碼鑰從收藏被編碼之伺服器證明書的服務終端取得上述伺服器證明書之手段，和根據上述認證台之公開鑰查證上述伺服器證明書之手段，和僅於得到肯定上述服務終端之正當性的查證結果時，將上述特定資料發訊上述服務終端之手段。

在其他最佳形態中，具備使用上述認證台的公開鑰，執行從上述服務終端所取得之上述伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，從上述伺服器取得上述服務終端中爲了實行發訊上述特定資料之處理的通訊應用軟體的手段，依據上述通訊應用軟體之實行執行上述特定資料之發訊。

又其他最佳形態中，具備從上述認證台取得證明該行動終端之正當性的客戶證明書的手段，和將上述客戶證明書發訊至上述服務終端的手段。

又本發明，提供一種服務終端，其特徵爲具備對應於來自行動終端之要求，發訊從認證台所發行之伺服器證明書的手段，和從上述行動終端，取得上述認證台所發行之客戶證明書的手段，和將上述客戶證明書使用上述認證台之公開鑰查證的手段，和僅於得到肯定上述行動終端之正當性的查證結果時，執行與上述行動終端間的通訊，上述行動終端取得從伺服器所取得之特定資料的手段。

又本發明提供一種程式，是針對介由網路從伺服器被發送至行動終端，依據上述行動終端之控制用電腦所實行之程式，將從通訊對象要求伺服器證明書的處理，和使用

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(7)

某認證台之公開鑰，執行上述伺服器證明書之查證的處理，和限於得到肯定上述通訊對象之正當性的查證結果時，將從上述伺服器所取得之特定資料發訊至上述通訊對象的處理，由上述控制用電腦實行之。

其他最佳形態中，上述程式之內部係包含上述特定資料以及上述公開鑰。

再者，本發明亦可實施於以下所述之形態。首先，伺服器與行動終端執行通訊，對於該行動終端之利用者，透過服務終端已決定何種商品或服務提供時，將某應用軟體程式發訊至行動終端，此應用軟體程式對於行動終端為可卸載，且收藏於電腦可讀取之記憶媒體。該應用軟體程式，係將服務終端之認證處理，和在依據認證確認服務終端之正當性的商品或服務提供所必要之特定資料發訊至服務終端之處理，於行動終端之電腦實行的程式。利用者前往與服務終端可區域通訊之場所，實行行動終端中記憶媒體內之應用軟體程式。其結果，執行行動終端與服務終端間的區域通訊，透過該區域通訊執行服務終端之認證，得到肯定的認證結果時，特定資料從行動終端被發訊至服務終端。此處所稱之記憶媒體，例如為HDD（硬碟裝置），行動終端之記憶體，例如為RAM或UIM卡、SIM卡等。

【為實施發明之最佳形態】

以下，參照圖示針對本發明之實施形態作說明。相關

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明(8)

實施形態，為顯示本發明之一種形態，並非限定本發明，而在本發明之範圍內可任意變更。

< 1.第 1 實施形態 >

< 1 — 1 : 第 1 實施形態之構成 >

< 1 — 1 — 1 : 終端通訊系統之整體構成 >

第 1 圖是顯示關於本發明第 1 實施形態之終端系統的整體構成方塊圖。如同一圖所顯示，該終端通訊系統具備通訊網 N E T 1 A、區域認證台 C A、I P (網際網路傳輸協定) 伺服器 2 0、閘道伺服器 3 0、移動通訊網 N E T 2、行動終端 M S 以及服務終端 T。再者，同一圖中，行動終端 M S 以及服務終端 T 分別以一個圖示，但實際上存在更多行動終端 M S 以及服務終端 T。

通訊網 1 A，作為資料通訊的傳送路徑而具有功能，例如網際網路或專用電線。區域認證台 C A 以及 I P 伺服器 2 0，連接該通訊網 1 A。移動通訊網 1 B，具備複數基地台、複數交換台、以及加入者處理裝置（無圖示），與行動終端間執行無線通訊。閘道伺服器 3 0，為設置於相互連接通訊網 1 A 與移動通訊網 1 B 之閘道中繼交換台的電腦系統。依據本實施形態通訊網 1 A 與移動通訊網 1 B 之間的資料通訊，是依該閘道伺服器 3 0 的功能而實現。

行動終端 M S，可以介由移動通訊網 1 B、閘道伺服器 3 0 以及通訊網 1 A 與 I P 伺服器 2 0 通訊。又服務

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(9)

終端 T 可以介由通訊網 1 A 與區域認證台 C A 通訊。行動終端 M S 和服務終端 T，可以不介由網路，執行 1 對 1 的區域通訊。

包含通訊應用軟體之資源中，設定已對應於該資源之 U R L。I P 伺服器 2 0，抽出從通訊網 1 A 所收訊之包含 G E T 要求的 U R L，將已對應於該 U R L 之資源回覆通訊網 1 A。

行動終端 M S，可為行動電話機或 P D A（個人數位助理）等可攜帶之行動終端，在本例中，行動終端 M S 為行動電話機。又行動終端 M S 介由移動通訊網 1 B 執行資料通訊或聲音通話，與服務終端 T 之間依據紅外線執行資料通訊。再者行動終端 M S 裝載 W W W（全球資訊網）瀏覽器，據此，行動終端 M S 之利用者可以閱覽 I P 伺服器 2 0 的網頁（資源）。又，裝載於行動終端 M S 之 W W W 瀏覽器，具有 Java Applet 之視訊功能，行動終端可於閱覽 W W W 網頁時，下載標籤指定之 Java Applet 在 W W W 瀏覽器上實行。且行動終端 M S，具有實行從 I P 伺服器 2 0 下載之各種通訊應用軟體的功能。

服務終端 T，設置於便利商店等店舖或車站境內，發行演唱會的入場券或車票，或可將遊戲程式或音樂資料發訊至行動終端 M S。服務終端 T，具有介由通訊網 1 A 執行與 I P 伺服器 2 0 或區域認證台 C A 之間資料通訊的介面，更具備與行動終端 M S 之間執行 1 對 1 區域通訊的紅外線介面。

五、發明說明 (10)

本實施形態依據以上所說明之各因素可以執行以下的各種電子商業交易。首先，有來自行動終端 M S 之要求時，I P 伺服器 2 0 對應於該要求發訊交易資料，例如金錢資料、為執行某入場券發行的資料、為取得遊戲程式或音樂資料的取得資料、或具有某些的交換價值之訂單資料等。通常，當該交易資料成功發送至行動終端 M S，即對於行動終端 M S 之利用者執行收費處理。其次，行動終端 M S 之利用者，造訪設置有服務終端 T 之店舖，依據行動終端 M S 執行將服務終端 T 作為對象之電子商業交易的通訊。在該通訊中，交易資料從行動終端 M S 發送至服務終端 T，交易資料為恰當時，依據店舖終端 T 執行商品提供、具體的票券發行處理等。

為了安全地執行此種電子商業交易，關於本實施形態之系統中，設有以下 2 個手段。

A. 行動終端 M S 確認服務終端 T 為正當終端的手段

B. I P 伺服器 2 0 保有之交易資料，僅傳送給正當的行動終端 M S，該交易資料僅從該正當的行動終端 M S，傳給服務終端 T 的手段

首先，針對前者手段 A 作說明。區域認證台 C A，具有執行數位簽名的功能，並保存自己的一套公開鍵 K E Y P 1 和密碼鍵 K E Y S 1。又，有來自可以信賴之對象的要求時，區域認證台 C A 對該對象發行電子證明書。更詳細敘述如以下說明。本實施形態中，區域認證台 C A 的持有者，和 I P 伺服器 2 0 的持有者、服務終端 T

五、發明說明 (11)

的持有者，是依據信賴關係而結合之複數組合，將行動終端 M S 的利用者作為對象，構成提供某種服務之共同體。區域認證台 C A，僅限於確認證明書之要求者為該共同體之一員，執行對該對象之證明書的發行。

此外，區域認證台 C A，為樹狀構造般階層化之複數認證台中的其中一個。在該樹狀構造中，某認證台依據上位認證台被認證，並保存顯示自己依據上位認證台認證之路徑證明書。該路徑證明書，係從上位認證台所發行。接著，某認證台執行下位認證台的認證時，該認證台對於下位認證台，發行顯示下位認證台依自己而被認證之證明書和自己的路徑證明書。

第 1 圖中區域認證台 C A 的下屬中，有服務終端 T。因此，區域認證台 C A，對於服務終端 T，發行顯示服務終端依據自己而被認證之伺服器證明書 C s 和自己的路徑證明書 C r。

伺服器證明書 C s，包含訊息與訊息摘要。首先，訊息中包含以下的資訊。

- 1) 版本號碼：此為表示證明書之版本。
- 2) 序列號碼：此為區域認證台 C A 發行之各證明書中分配的號碼。
- 3) 簽名之演算法：此為，區域認證台 C A 簽署證明書時，所使用之編碼演算法。例如內容為利用雜亂訊號演算法之 S H A — 1、編碼手段之 R S A 的內容。
- 4) 主題：此為關於被證明者之資訊，例如姓名或公司名

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (12)

、國碼等。

5) 有效期限：此為顯示證明書有效之期間。

6) 簽名者：此為包含區域認證台 C A 之姓名、公司名、國碼等。

7) 公開鑰 K E Y P 1：此為區域認證台 C A 之公開鑰。

以上係包含於訊息之資訊的詳情。該訊息先依據區域認證台 C A 之密碼鑰 K E Y S 1 被編碼，可依據區域認證台 C A 之公開鑰 K E Y P 1 解碼。

訊息摘要是將該訊息依據雜亂訊號函數壓縮，並將已壓縮之訊息根據區域認證台 C A 之密碼鑰 K E Y S 1 編碼所產生之資訊。

I P 伺服器 2 0，具有執行依據公開鑰編碼通訊方式之通訊或數位簽名的功能，保存自己的一套公開鑰 K E Y P 2 與密碼鑰 K E Y S 2。此外，I P 伺服器 2 0，從區域認證台 C A 接受認證，具有證明書。該證明書中包含從區域認證台 C A 所發行之路徑證明書 C r。再者，I P 伺服器 2 0 之管理主體與區域認證台 C A 之管理主體為相同，例如為統括地管理某連鎖便利商店之公司。

行動終端 M S，從 I P 伺服器 2 0 取得交易資料時，同時從 I P 伺服器 2 0 取得認證台 C A 之公開鑰 K E Y P 1。然後，行動終端 M S 與服務終端 T 執行電子商業交易之區域通訊時，行動終端 M S，對於服務終端 T，要求從認證伺服器 C A 所取得之證明書，該證明書被發送來時依據公開鑰 K E Y P 1 確認其正當性。接著，僅限

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (13)

於已確認正當性時，行動終端 M S 執行與服務終端 T 電子商業交易之通訊。

其次針對後者的手段作說明。本實施形態中行動終端 M S，僅於使用從 I P 伺服器 2 0 下載之通訊應用軟體時，可將從 I P 伺服器 2 0 所取得之交易資料發訊至外部，通訊應用軟體，確認通訊對象是否為正規的服務終端 T 後，發訊交易資料。此手段，例如可依據以下的方法實現。首先，I P 伺服器 2 0 將交易資料與認證台 C A 之公開鍵 K E Y P 1 作為內部資料包含的同時，將包含從通訊對象取得伺服器證明書之處理，和使用公開鍵 K E Y P 1 執行伺服器證明書之查證處理，和在得到肯定通訊對象之正當性的查證結果時，發訊交易資料至通訊對象之處理的各例程序之通訊應用軟體發送至行動終端 M S。行動終端 M S 實行該通訊應用軟體。該通訊應用軟體例如為 Java Applet。在此 Java Applet 中，介由網際網路執行通訊時，具有只能與該 Java Applet 的下載源通訊的限制。但是，與服務終端 T 之區域通訊，因為並非介由網路之通訊，而在此限制外。由此，行動終端 M S，依據實行該通訊應用軟體，執行與服務終端 T 之通訊，於該實行過程查證出服務終端 T 之正當性時，將交易資料發訊至服務終端 T。若根據本方法，於通訊應用軟體之實行過程僅將交易資料發送至已確認正當性之服務終端 T。因而可防止交易資料的不正當複製。

其次參照第 2 圖，說明行動終端 M S 之構成。如第 2 圖所顯示關於本實施形態之行動終端 M S，具有控制部

五、發明說明 (14)

1 0 0、紅外線收發訊部 1 1 0、無線收發訊部 1 2 0、指示輸入部 1 3 0、液晶顯示部 1 4 0，和於各部門間仲介資料收受之匯流排 1 5 0。

紅外線收發訊部 1 1 0，在控制部 1 0 0 之控制下，與服務終端 T 執行紅外線通訊。無線收發訊部 1 2 0，在控制部 1 0 0 的控制下，與移動通訊網 1 B 之基地台執行無線通訊。

指示輸入部 1 3 0，係由 P B (Push Button) 等各種按鍵以及游標按鍵所構成，當利用者執行輸入操作，即將對應於該輸入操作之操作訊號供給控制部 1 0 0。液晶顯示部 1 4 0，係由液晶面板等顯示裝置所構成，在控制部 1 0 0 的控制之下，顯示各種資訊。

控制部 1 0 0，例如，具有 C P U (中央處理器) 1 1 1、R O M (唯讀型記憶體) 1 1 2、R A M (隨機存取記憶體) 1 1 3，和 E E P R O M 1 1 4，控制行動終端 M S 之各部。R O M 1 1 2 中，除了控制用通訊應用軟體，亦安裝上述之 W W W 瀏覽器、遵循公開鑰編碼方式之通訊應用軟體等各種訊應用軟體。

R A M 1 1 3，作為 C P U 1 1 1 之工作領域而被使用，例如，暫時地收藏從 I P 伺服器 2 0 所下載之 H T M L 資料或通訊應用軟體等。

E E P R O M 1 1 4，具有通訊應用軟體收藏領域 1 1 4 a，和泛用收藏領域 1 1 4 b。通訊應用軟體收藏領域 1 1 4 a 中，收藏從 I P 伺服器 2 0 所下載之通訊應

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (15)

用軟體。泛用收藏領域 1 1 4 b 中，除了收藏從 I P 伺服器 2 0 所下載之路徑證明書 C r 或交易資料，也收藏其他通訊必要之密碼鑰 K E Y S 4、公開鑰 K E Y P 4。此外，實行通訊應用軟體時，C P U 1 1 1 產生亂數，使用此以產生公共鑰 K E Y X，並收藏於泛用收藏領域 1 1 4 b。

其次參照第 3 圖，說明服務終端 T 的構成。如第 3 圖所顯示，關於本實施形態之服務終端 T，具有系統控制部 2 0 0、紅外線介面部 2 1 0、通訊部 2 2 0、輸入部 2 3 0、顯示部 2 4 0、硬碟 2 5 0 和發券部 2 6 0。通訊部 2 2 0，介由通訊網 1 A 執行資料通訊。服務終端 T，依據該資料通訊，執行在 I P 伺服器 2 0 等之間各種資料的收發訊。

系統控制部 2 0 0，例如，具有 C P U、R O M、R A M（省略圖示），作為控制服務終端 T 之各部的控制中樞而具有功能。此外，硬碟 2 5 0 中，記憶有遵循公開鑰編碼通訊方式之通訊應用軟體、使用於實行該通訊應用軟體之密碼鑰 K E Y S 3 和公開鑰 K E Y P 3 等。

紅外線介面部 2 1 0，在與行動終端 M S 之間將使用紅外線之資料通訊遵循公開鑰編碼方式執行。通訊部 2 2 0，介由通訊網 1 A 執行資料通訊。服務終端 T，依據該資料通訊，在與區域認證台之間執行各種資料的收發訊，取得包含伺服器證明書 C s 和路徑證明書 C r 的證明書。

五、發明說明 (16)

輸入部 2 3 0，具有鍵盤或滑鼠等，利用者使用輸入部 2 3 0 可以輸入操作指示。

顯示部 2 4 0，係由液晶顯示裝置或電視螢幕等所構成，顯示輸入部 2 3 0 的操作內容，或對應於來自行動終端 M S 之輸入指示的處理經過。發券部 2 6 0，在系統控制部 2 0 0 的控制下，執行各種入場券的發行，具有印刷功能。

< 1 — 2 : 第 1 實施形態之動作 >

第 4 圖為顯示終端通訊系統之動作的序列圖。

在本實施形態中，為了執行安全的電子交易，事先執行依據區域認證台 C A 之 I P 伺服器 2 0 的認證以及服務終端 T 的認證。第 4 圖中步驟 S 1 ~ S 4 即為此處理。這些處理，到行動終端 M S 之利用者開始電子商業交易為止完成即可。

首先，I P 伺服器 2 0 對於區域認證台 C A，發訊要求證明 I P 伺服器 2 0 為正當之伺服器的認證要求 R E Q 1 (步驟 S 1)。該認證要求 R E Q 1，包含 I P 伺服器 2 0 的公開鑰 K E Y P 2 和所有資訊 I N F 2。所有資訊 I N F 2，係顯示公開鑰 K E Y P 2 之所有者為 I P 伺服器 2 0 的正文資料。

接著，區域認證台 C A，確認 I P 伺服器 2 0 為正當時，使用自己保有之密碼鑰 K E Y S 1 將 I P 伺服器 2 0 的公開鑰 K E Y P 2 以及所有資訊 I N F 2 編碼，產生公

五、發明說明 (17)

開鑰證明書 C 2 。區域認證台 C A ，將包含公開鑰證明書 C 2 和路徑證明書 C r 之認證答覆 R E S 1 發回 I P 伺服器 2 0 (步驟 S 2) 。 I P 伺服器 2 0 ，對應必要對行動終端 M S 發訊路徑證明書 C r 。

另一方面，服務終端 T 爲了證明本身終端的正當性，介由通訊網 1 A ，將伺服器證明書發行要求 R E Q 2 發訊至區域認證台 C A (步驟 S 3) 。伺服器證明書發行要求 R E Q 2 ，包含服務終端 T 之公開鑰 K E Y P 3 和所有資訊 I N F 3 。所有資訊 I N F 3 ，係顯示公開鑰 K E Y P 3 之所有者爲服務終端 T 的正文資料。

接著，當區域認證台 C A 接收伺服器證明書發行要求 R E Q 2 ，區域認證台 C A ，依據將服務終端 T 之公開鑰 K E Y P 3 以及所有資訊 I N F 3 等編碼，發行上述伺服器證明書 C s ，與路徑證明書 C r 同時作爲伺服器證明書發行答覆 R E S 2 發訊至服務終端 T (步驟 S 4) 。只要將伺服器證明書 C s 以認證台 C A 之公開鑰 K E Y P 1 解碼，可得到公開鑰 K E Y P 3 以及所有資訊 I N F 3 。

在本例中，區域認證台 C A ，限於發行伺服器證明書 C s 至其下屬之服務終端 T 。除此以外者，例如行動終端 M S 的利用者，也可能使用自己的個人電腦存取區域認證台 C A 要求認證。但是，區域認證台 C A ，即使有來自像這樣服務終端 T 以外者來的伺服器證明書 C s 的發行要求，仍拒絕該要求。因此該利用者無法取得伺服器證明書 C s 。

五、發明說明 (18)

以上為依據區域認證台 C A 之 I P 伺服器 2 0 的認證以及服務終端 T 的認證。

其次，針對來自行動終端 M S 之要求所執行之電子商業交易作說明。首先，行動終端 M S 介由移動通訊網 1 B 以及通訊網 1 A 存取 I P 伺服器 2 0，當下載要求 R E Q 3 發訊至 I P 伺服器 2 0（步驟 S 5），I P 伺服器 2 0 將下載答覆 R E S 3 回覆行動終端 M S（步驟 S 6）。

下載答覆 R E S 3 中，包含區域認證台 C A 的公開鑰 K E Y P 1 以及路徑證明書 C r、為了以紅外線與服務終端 T 執行通訊之通訊應用軟體、訂單資料等的交易資料。該通訊應用軟體，只有在已確認特定伺服器證明書 C s 時從行動終端 M S 許可發訊交易資料，公開鑰 K E Y P 1，為了確認伺服器證明書 C s 而被使用。

再者，行動終端 M S 也可在交易資料的發訊前，對 I P 伺服器 2 0 要求發訊公開鑰證明書 C 2。接著行動終端 M S，使用從其他安全路徑所取得之 I P 伺服器 2 0 的公開鑰 K E Y P 2，查證從 I P 伺服器 2 0 所取得之公開鑰證明書 C 2，使用附加於此之公開鑰 K E Y P 2 編碼收費資料，並發訊至 I P 伺服器 2 0。

接者，利用者前往店舖，當操作行動終端 M S 以步驟 S 6 啟動已取得之通訊應用軟體，行動終端 M S 與服務終端 T 之間使用紅外線開始 1 對 1 的區域通訊。該區域通訊中，首先，行動終端 M S，將伺服器認證要求 R E Q 4 發

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (19)

訊至服務終端 (步驟 S 7)，服務終端 T，將伺服器認證答覆 R E S 4 回覆行動終端 M S (步驟 S 8)。伺服器認證答覆 R E S 4 中，包含伺服器證明書 C s。

之後，行動終端 M S，執行伺服器認證處理 (步驟 S 9)。具體而言，第 1 步，行動終端 M S 使用區域認證台 C A 的公開鑰 K E Y P 1 解碼伺服器證明書 C s，取出訊息摘要與訊息。第 2 步，行動終端 M S，使用雜亂函數壓縮訊息，產生比較用之訊息摘要。第 3 步，行動終端 M S，比較已解碼之訊息摘要和比較用的訊息摘要，判斷兩者是否一致。第 4 步，行動終端 M S，於兩者一致時認證服務終端 T 為正當，開始資料通訊。又，兩者不一致時，行動終端 M S，認為服務終端 T 為不正當而結束資料通訊。

該認證處理，是根據區域認證台 C A 的公開鑰 K E Y P 1 被執行，重要的是公開鑰 K E Y P 1 係依據通訊應用軟體而被指定。亦即，I P 伺服器 2 0，根據通訊應用軟體，僅對依據特定認證台 (在本例中，為區域認證台 C A) 所認證之服務終端 T，許可行動終端 M S 發訊從 I P 伺服器 2 0 所下載之交易資料。

在使用網際網路證明書的認證方法中，存在有各種認證台，普遍來說，依據任一證明書只要通訊對象被認證，即可執行通訊。但是，像這樣的認證方法中，很有可能會允許不正當複製從 I P 伺服器 2 0 所發行之交易資料。例如行動終端 M S 的利用者使用自己的個人電腦，從適當的

五、發明說明 (20)

認證台得到證明書，再從行動終端 M S 將交易資料發訊至個人電腦。此時，個人電腦因為取得認證台所發行之證明書，行動終端 M S 確認該證明書而將交易資料發訊至個人電腦。如此一來當交易資料被送至個人電腦，可能造成交易資料的不正當複製。為了防止此類交易資料的不正當複製，在本實施形態中，區域認證台 C A 限定給予伺服器證明書 C s 之對象，依據通訊應用軟體使用公開鑰

K E Y P 1 確認伺服器證明書 C s，僅對特定的服務終端 T 許可發訊交易資料。據此，不會發訊交易資料至不正當之服務終端 T，而可以防止交易資料的不正當複製。

其次，服務終端 T 被認證為正當時，行動終端 M S 與服務終端 T 之間，執行資料通訊（步驟 S 1 0）。該資料通訊依以下的順序執行。第 1 步，行動終端 M S 的

C P U 1 1 1 產生亂數，生成公共鑰 K E Y X。第 2 步，C P U 1 1 1，將公共鑰 K E Y X 根據附加於伺服器證明書 C s 之服務終端 T 的公開鑰 K E Y P 3 加以編碼，產生編碼公共鑰 K E Y X'。第 3 步，行動終端 M S 將編碼公共鑰 K E Y X' 發訊至服務終端 T。第 4 步，服務終端 T 將所收訊之編碼公共鑰 K E Y X' 以密碼鑰 K E Y S 3 解碼，取出公共鑰 K E Y X。第 5 步，行動終端 M S 與服務終端 T，使用公共鑰 K E Y X 執行編碼通訊。

此時，訂單資料或個人資料從行動終端 M S 發訊至服務終端 T，但這些係依據公共鑰 K E Y X 被編碼，所以即使假設有第三者盜取這些資料，也極難解讀。接著，服務

五、發明說明（21）

終端 T 以接受由 I P 伺服器 20 所發行之交易資料為條件，將音樂資料或遊戲通訊應用軟體轉送至行動終端 M S，執行演唱會入場券的發行。

依據本實施形態，於服務終端 T 與行動終端 M S 之間執行 1 對 1 的區域通訊中，因根據區域認證台 C A 所發行之伺服器證明書 C s，認證服務終端 T，而可以防止服務終端 T 的冒充，並防止交易資料的不正當複製。

再者，即使服務終端 T 設置於地下街等電波傳遞不到的地方，因為在行動終端 M S 與服務終端 T 之間執行 1 對 1 的區域通訊取得伺服器證明書 C s，所以行動終端可以僅對正當的服務終端發訊交易資料。

並且，I P 伺服器 20 與區域認證台 C A 的管理主體為同一個。也就是說，證明通訊對象之證明書，與使用於該通訊之資料的發行源為相同。由此，若根據本實施形態，使用從發行源所取得之資料，執行與依據證明書之發行源認證之通訊對象的通訊，可提高隱私。

< 2：第 2 實施形態 >

其次，針對本發明之第 2 實施形態，參照圖面作說明。關於第 1 實施形態之通訊系統，以行動終端 M S 認證服務終端 T 為條件，開始資料通訊。對此，在第 2 實施形態的終端通訊系統中，行動終端 M S 與服務終端 T 執行相互認證。第 2 實施形態之終端通訊系統的整體構成，與第 1 圖所顯示之第 1 實施形態的終端通訊系統相同，所以省略

五、發明說明 (22)

該說明。

在本實施形態中，區域認證台 C A，不只對服務終端 T 也對行動終端 M S 發行證明書。發行至行動終端 M S 之證明書中，包含客戶證明書 C c 與路徑證明書 C r。客戶證明書 C c 係證明行動終端 M S 為正當之終端，與上述伺服器證明書 C s 同樣地，包含以密碼鑰 K E Y S 1 編碼之訊息與訊息摘要。

第 5 圖中，顯示關於第 2 實施形態之終端通訊系統的動作序列圖。從認證要求 R E Q 1 到伺服器證明書答覆 R E S 2 為止的處理（步驟 S 1 ~ S 4），與第 4 圖所顯示之第 1 實施形態的終端通訊系統處理相同。

在本實施形態中，因服務終端 T 認證行動終端 M S，行動終端 M S 有必要從區域認證台 C A 取得客戶證明書 C c。為此，行動終端 M S，將客戶證明書發行要求 R E Q 5 發訊至區域認證台 C A（步驟 S 2 1）。該客戶證明書發行要求 R E Q 5，包含行動終端 M S 的公開鑰 K E Y P 4 和所有資訊 I N F 4 等。所有資訊 I N F 4，係顯示公開鑰 K E Y P 4 之行動終端 M S 的正文資料，例如，行動終端 M S 的電話號碼（發出號碼）或識別號碼。

當區域認證台 C A，接收客戶證明書發行要求 R E Q 5，區域認證台 C A 使用自己保有之密碼鑰 K E Y S 1 發行已數位簽名之客戶證明書 C c，將包含此和路徑證明書 C r 之客戶證明書發行答覆 R E Q 6 發訊至行動終端 M S（步驟 S 2 2）。

五、發明說明（ 23）

之後，行動終端 M S 存取 I P 伺服器 2 0，發訊下載要求 R E Q 6（步驟 S 2 3），I P 伺服器 2 0 朝行動終端 M S 發訊下載答覆 R E S 6（步驟 S 2 4）。下載答覆 R E S 6 中，包含第 1 實施形態中已說明之訂單資料等交易資料、通訊應用軟體、以及區域認證台 C A 的公開鑰 K E Y P 1。

接著，從伺服器認證要求 R E Q 4 至伺服器認證為止的處理（步驟 S 7 ~ S 9），與第 1 實施形態相同。伺服器認證處理結束後（步驟 S 9），服務終端 T 對於行動終端 M S 發訊客戶認證要求 R E Q 7（步驟 S 2 5），行動終端 M S 將包含客戶證明書 C c 之客戶認證答覆 R E S 7 回覆服務終端 T（步驟 S 2 6）。

接著，服務終端 T 執行客戶認證處理（步驟 S 2 7）。具體而言，第 1 步，服務終端 T 使用區域認證台 C A 的公開鑰 K E Y P 1 將客戶證明書 C c 解碼，取出訊息摘要以及訊息。第 2 步，服務終端 T 使用雜亂函數壓縮訊息，產生比較用的訊息摘要。第 3 步，服務終端 T 比較已解碼之訊息摘要和比較用的訊息摘要，判斷兩者是否一致。第 4 步，兩者為一致時，服務終端 T 認證行動終端 M S 為正當，開始資料通訊。第 5 步，兩者不一致時，服務終端 T，認為服務終端 T 為不正當而結束資料通訊。僅在行動終端 M S 被確認為正當時，執行與第 1 實施形態相同之資料通訊（步驟 S 1 0）。

如以上所說明，依據本實施形態，於行動終端 M S 與

五、發明說明 (24)

服務終端 T 的 1 對 1 區域通訊中相互地認證通訊對象，所以不僅服務終端 T，也可防止行動終端 M S 的冒充。

再者，使用於認證之伺服器證明書 C s 與客戶證明書 C c 的發行源，為同一區域認證台 C A，所以不須查證已利用區域認證台 C A 之上位認證台所發行之證明書的區域認證台 C A 本身。為此，伺服器認證處理，以及客戶認證處理可變得簡單。

< 3 : 變形例 >

以上，已說明第 1 以及第 2 實施形態，但本發明並不限定於此，例如，亦可能為以下所述的各種變形例。

(1) 上述之各實施形態中行動終端 M S 與服務終端 T，是以紅外線執行通訊，此通訊方式以外，也可採用依據 I r D A (紅外線數據協定) 之通訊方式。此外，也可以無線取代紅外線執行通訊。此時，也可將與基地台之間執行通訊之天線，兼用為與服務終端 T 執行無線通訊之天線。更者，作為無線通訊方式，也可採用使用

2 . 4 G H z 波段在近距離執行無線通訊之 Bluetooth 方式。

(2) 在上述之各實施形態中，I P 伺服器 2 0 和區域認證台 C A，邏輯上功能不同，所以作為個別的裝置來說明，但這兩者亦可為一體的裝置。重要的是，執行服務終端 T 認證之伺服器，和對於行動終端 M S 配訊通訊應用軟體以及訂單資料之伺服器，只要為依據同一主體來管理

五、發明說明 (25)

，物理上這兩者以 1 個伺服器構成，或以 2 個伺服器構成都沒有問題。

(3) 再者，上述各實施形態中，在行動終端 M S 與服務終端 T 之間執行資料通訊 (第 4 圖以及第 5 圖之步驟 S 1 0)，執行已使用所有 S S L (安全編碼技術) 之資料通訊，但在交易資料之收受中也可使用數位簽名。該數位簽名中具有以下所述 2 種形態。

第 1 形態，I P 伺服器 2 0，以自己的密碼鑰 K E Y S 2 產生已編碼之交易資料發訊至行動終端 M S，行動終端 M S 使用被編碼之交易資料在與服務終端 T 之間執行資料通訊。此時的交易資料，因係依據 I P 伺服器 2 0 而沒有數位簽名，所以服務終端 T 依據預先取得之 I P 伺服器 2 0 的公開鑰 K E Y P 2，可以確認交易資料確實是依據 I P 伺服器 2 0 所產生。

第 2 形態，行動終端 M S 與服務終端 T，相互發訊至對方之交易資料中執行數位簽名。例如，執行演唱會的入場券發行時，第 1 步，行動終端 M S，產生金錢資料與訂單資料的同時，產生顯示識別資料、以及交易日期時間之日期資料作為訊息。第 2 步，行動終端 M S，將訊息根據雜亂函數壓縮產生訊息摘要。第 3 步，行動終端 M S，將訊息摘要根據行動終端 M S 的密碼鑰 K E Y S 4 編碼。第 4 步，行動終端 M S，產生亂數生成對話鍵，將對話鍵根據服務終端 T 的公開鑰 K E Y P 3 編碼，產生編碼對話鍵。第 6 步，行動終端 M S，將被編碼之訊息摘要、編碼對

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (26)

話鍵、以及被編碼之訊息匯集整理發訊至服務終端 T。

收訊此之服務終端 T，依以下順序執行訊息的解碼。

第 1 步，服務終端 T，將編碼對話鍵根據自己的密碼鑰 K E Y S 4 解碼，取得對話鍵。第 2 步，服務終端 T，根據對話鍵將編碼之訊息解碼。第 3 步，服務終端 T，使用雜亂函數壓縮已解碼之訊息，產生訊息摘要。第 4 步，服務終端 T，將已編碼之訊息摘要根據行動終端 M S 之公開鑰 K E Y P 4 解碼。第 5 步，服務終端 T 比較已解碼之訊息摘要，和使用雜亂函數所產生之訊息摘要，查證是否一致。第 6 步，服務終端 T，在訊息摘要一致時，理解該訊息確實為從行動終端 M S 所發訊。

再者，從服務終端 T 朝行動終端 M S 發訊交易資料時，也依據同樣的順序執行。

(4) 此外，在上述第 2 實施形態中，行動終端 M S 首先執行伺服器認證處理，之後服務終端 T 執行客戶認證處理，但也可為服務終端 T 執行客戶認證處理後，行動終端 M S 執行伺服器認證處理。具體而言，在第 5 圖所顯示之序列中，可在執行步驟 S 2 5 ~ 2 7 的處理之後，執行步驟 S 7 ~ 9。

(5) 在上述各實施形態中，使用以 I P 伺服器 2 0 所發行之交易資料 (訂單資料)，行動終端 M S 執行與服務終端 T 資料通訊，但本發明並不限定於此，當然也可使用其他伺服器發行之交易資料。例如，I P 伺服器 2 0，為統括某便利商店之伺服器，也存在統括其他店舖的伺服

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (27)

器。更者，設置統括各店舖的各伺服器，亦即統括連鎖便利商店整體之上位伺服器，該上位伺服器，發行各 I P 伺服器 2 0 共通的交易資料。像這樣的情形，行動終端 M S 可從上位伺服器取得交易資料，也可使用上位認證台發行之客戶證明書被認證。

(6) 在上述各實施形態中，從伺服器介由行動終端 M S 將交易資料發送至服務終端 T，但本發明的適用範圍並不是限定於這樣的交易資料流通。

交易資料以外的特定資料，例如音樂資料、畫像資料或者正文資料的流通也適用本發明。

例如以下的系統。伺服器，執行通訊對象的認證，將發訊音樂資料之通訊應用軟體發訊至行動終端 M S。行動終端 M S，實行通訊應用軟體，但該實行過程中，行動終端 M S，從服務終端 T 取得被編碼之伺服器證明書，查證服務終端的正當性。然後，肯定服務終端 T 之正當性的查證結果，亦即僅在可解碼該伺服器證明書時，行動終端 M S 將音樂資料發訊至服務終端 T。服務終端 T，只再生 1 次音樂資料。

只要依據這樣的程式，即可防止音樂資料的不正當複製。

如以上所說明，根據本發明，在行動終端 M S 與服務終端 T 之間執行 1 對 1 的直接通訊時，因防止冒充，可以提高電子商業交易的安全；更者本發明，可以防止行動終端從特定伺服器所取得之交易資料的不正當複製。

五、發明說明 (28)

【圖面說明】

第 1 圖是顯示關於本發明第 1 實施形態之終端通訊系統的整體構成方塊圖。

第 2 圖是顯示於同系統之行動終端 M S 的構成例方塊圖。

第 3 圖是顯示於同系統之服務終端 T 的構成例方塊圖。

第 4 圖是顯示同系統之動作例的序列圖。

第 5 圖是顯示關於本發明第 2 實施形態之終端通訊系統的動作例序列圖。

【圖號說明】

1 A	通訊網
1 B	移動通訊網
2 0	I P 伺服器
3 0	閘道伺服器
1 0 0	控制部
1 1 0	紅外線收發訊部
1 1 1	C P U
1 1 2	R O M
1 1 3	R A M
1 1 4	E E P R O M
1 2 0	無線收發訊部

五、發明說明 (29)

- 1 3 0 指 示 輸 入 部
- 1 4 0 液 晶 顯 示 部
- 2 0 0 系 統 控 制 部
- 2 1 0 紅 外 線 介 面 部
- 2 2 0 通 訊 部
- 2 3 0 輸 入 部
- 2 4 0 顯 示 部
- 2 5 0 硬 碟
- 2 6 0 發 券 部
- C A 區 域 認 證 台
- T 服 務 終 端
- M S 行 動 終 端

(請先閱讀背面之注意事項再填寫本頁)

訂

四、中文發明摘要(發明之名稱：終端通訊系統)

行動終端 M S，從 I P 伺服器 2 0 下載訂單資料的同時，下載 I P 伺服器 2 0 的公開鑰 K E Y P 2。服務終端 T，從 I P 伺服器 2 0 以該密碼鑰 K E Y S 2 預先取得已被數位簽名之伺服器證明書。於行動終端 M S 和服務終端 T 之間，以紅外線執行 1 對 1 的區域通訊。此時，行動終端 M S，將伺服器證明書以 I P 伺服器 2 0 的公開鑰 K E Y P 2 解碼。然後行動終端 M S 查證服務終端 T 的正當性之後，執行特定資料的通訊。

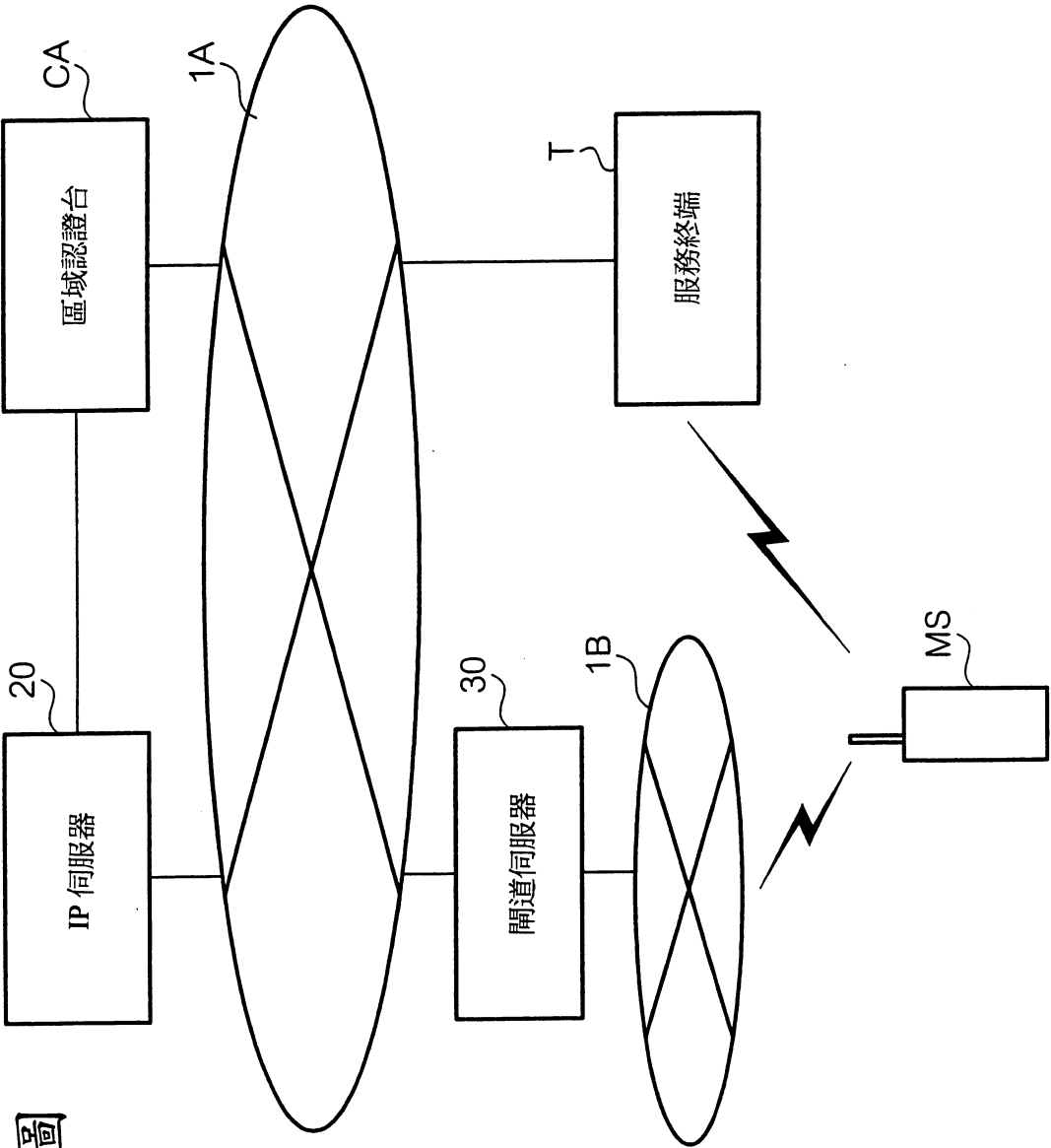
英文發明摘要(發明之名稱：)

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

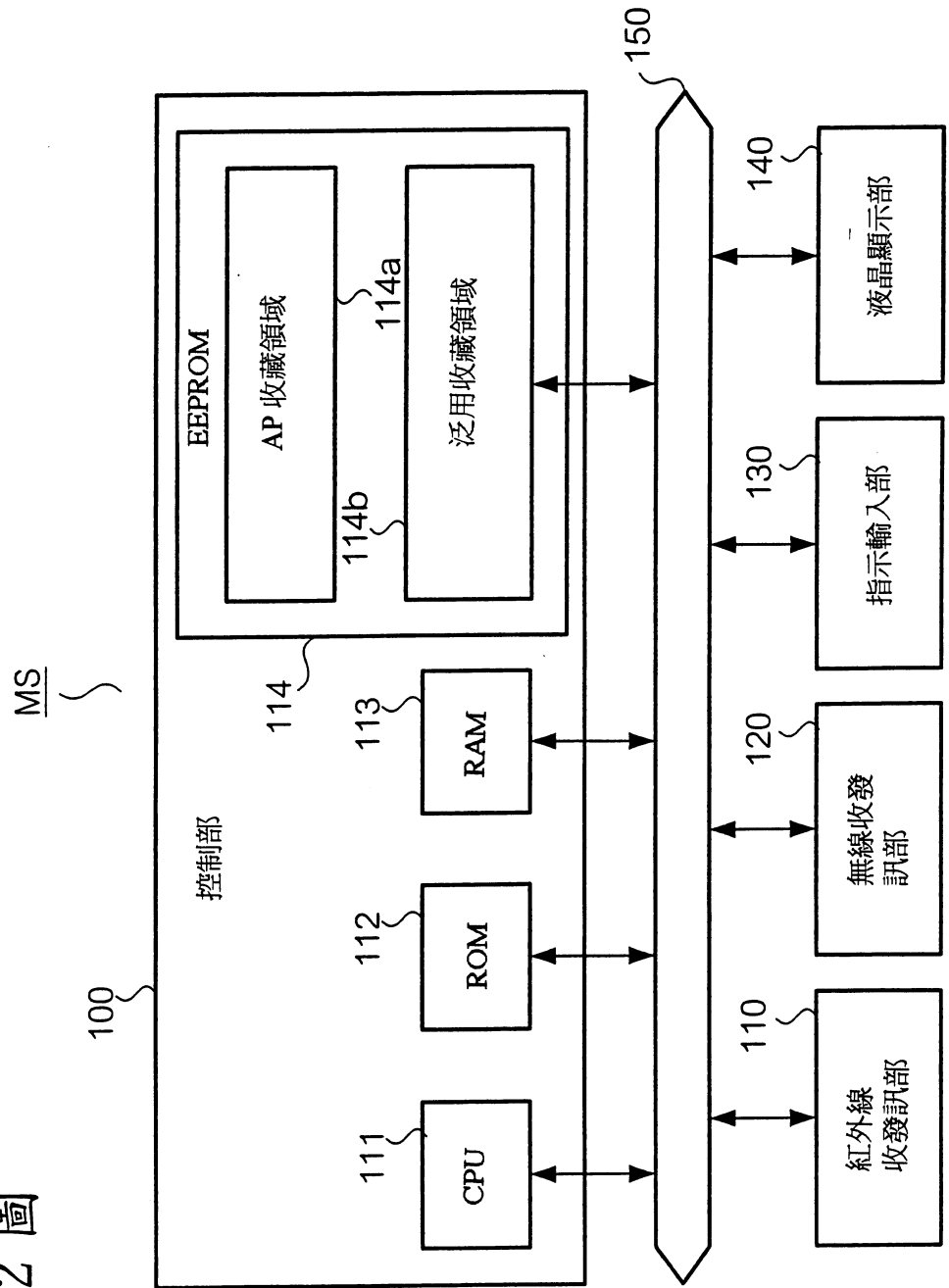
訂

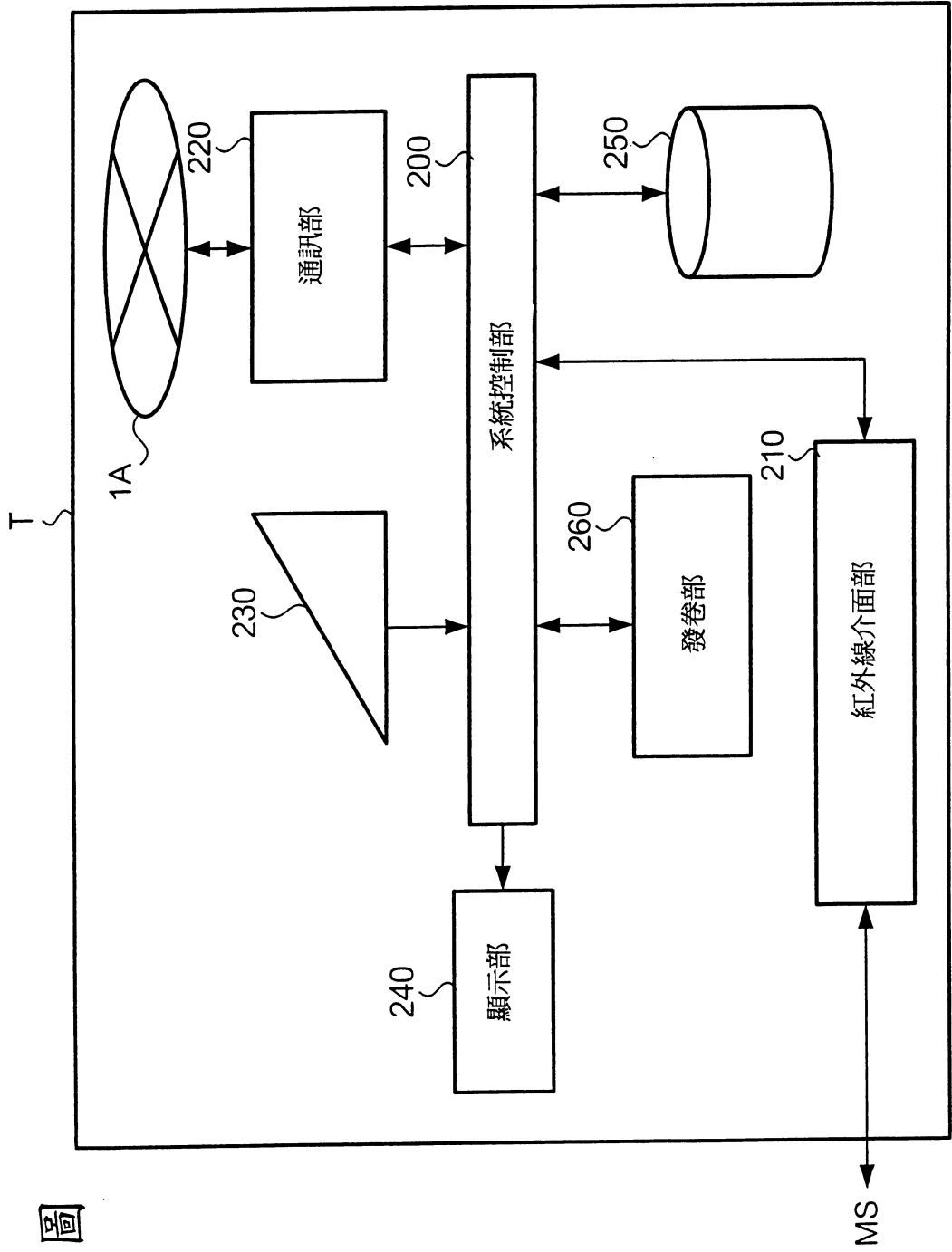
線



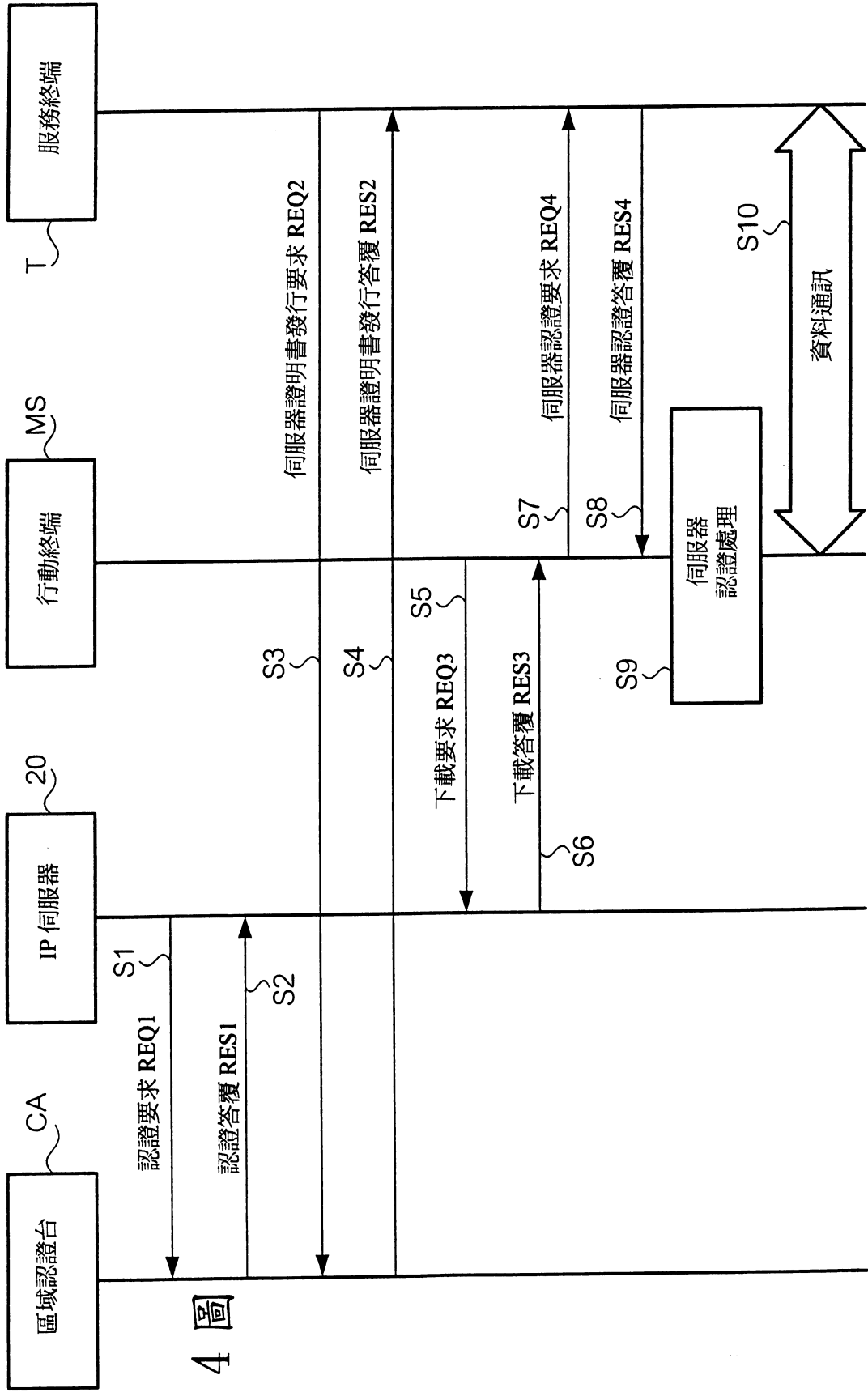
第 1 圖

第 2 圖





第 3 圖



第 4 圖

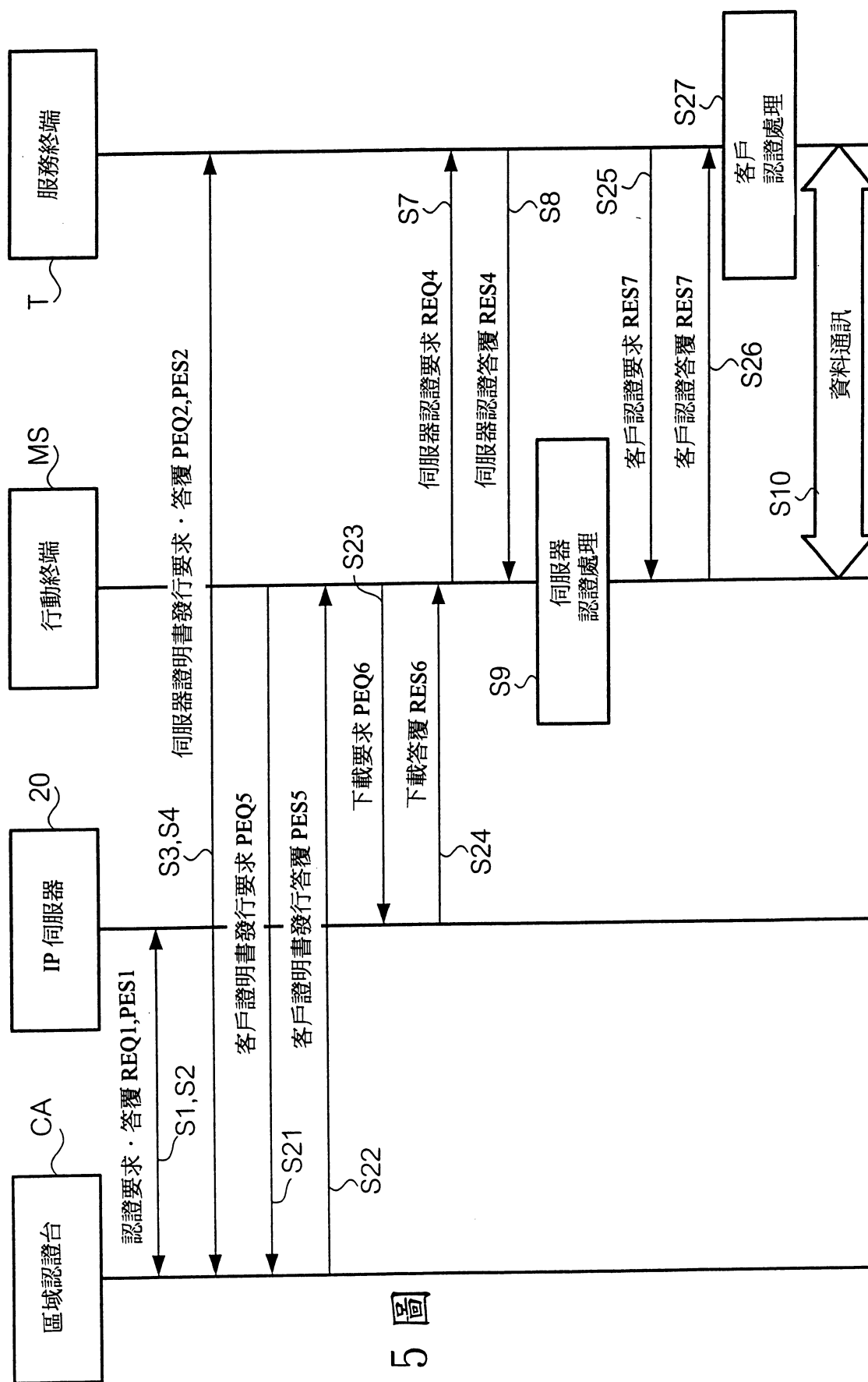


圖 5 第

六、申請專利範圍

第 91108003 號專利申請案

中文申請專利範圍修正本

民國 92 年 12 月 19 日修正

1 . 一種終端通訊方法，其特徵為：

行動終端，從伺服器取得特定資料，

服務終端，依據認證台之密碼鑰從該認證台取得被編碼之伺服器證明書，

上述行動終端從上述服務終端取得上述伺服器證明書，根據上述認證台的公開鑰查證上述伺服器證明書，

上述行動終端，限於根據上述伺服器證明書查證上述服務終端為正當時，依據不經由網路之區域通訊，將上述特定資料發訊至上述服務終端。

2 . 如申請專利範圍第 1 項所述之終端通訊方法，其中，

上述伺服器使用上述認證台之公開鑰，執行從上述服務終端所取得之伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，將上述服務終端中為了實行上述特定資料之處理的通訊應用軟體發訊至上述行動終端，上述行動終端依據上述通訊應用軟體之實行執行上述特定資料的發訊。

3 . 如申請專利範圍第 1 項所述之終端通訊方法，其中，

上述行動終端從上述認證台取得依上述認證台之密碼鑰被編碼的客戶證明書，

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

六、申請專利範圍

上述服務終端從上述行動終端取得上述客戶證明書，根據上述認證台之公開鑰查證上述客戶證明書，限於得到肯定的查證結果時，執行與上述行動終端之區域通訊。

4．如申請專利範圍第1項所述之終端通訊方法，其中，

上述行動終端，經由無線通訊網執行與上述伺服器之通訊。

5．如申請專利範圍第1項所述之終端通訊方法，其中，

上述行動終端，依據使用上述認證台之公開鑰執行上述伺服器證明書之解碼，判斷上述服務終端的正當性。

6．如申請專利範圍第3項所述之終端通訊方法，其中，

上述服務終端，依據使用上述認證台之公開鑰執行上述客戶證明書之解碼，判斷上述行動終端之正當性。

7．如申請專利範圍第1項所述之終端通訊方法，其中，

上述行動終端與上述服務終端之間的通訊，是依據紅外線通訊或近距離無線通訊所執行。

8．如申請專利範圍第1項所述之終端通訊方法，其中，

上述行動終端與上述服務終端之間的通訊，是編碼通訊。

9．如申請專利範圍第1項所述之終端通訊方法，其

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

六、申請專利範圍

中，

上述伺服器以及上述認證台的一方可兼具他方。

10．一種終端通訊系統，具備認證台、伺服器、服務終端、和行動終端，其特徵為：

上述服務終端，

具備記憶由上述認證台所發行之伺服器證明書的手段

，

和對應於來自上述行動終端之要求，將上述伺服器證明書發訊至上述行動終端的手段；

上述行動終端，

具備從上述伺服器取得特定資料的手段，

和從上述服務終端取得上述伺服器證明書的手段，

和將上述伺服器證明書使用上述認證台之公開鑰查證的手段，

和僅於得到肯定上述服務終端之正當性的查證結果時，朝上述服務終端發訊特定資料的手段。

11．如申請專利範圍第10項所述之終端通訊系統，其中，

上述伺服器，具備使用上述認證台之公開鑰，執行從上述服務終端所取得之伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，將上述服務終端中為了實行發訊上述特定資料之處理的通訊應用軟體發訊至上述行動終端之手段，

上述行動終端，依據上述通訊應用軟體之實行執行上

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

六、申請專利範圍

述特定資料之發訊。

1 2 . 如申請專利範圍第 1 0 項所述之終端通訊系統，其中，

服務終端，具備從上述行動終端取得上述客戶證明書，將上述客戶證明書依據上述認證台之公開鑰查證，僅於得到肯定上述行動終端之正當性的查證結果時，許可與上述行動終端之區域通訊的手段。

1 3 . 如申請專利範圍第 1 0 項所述之終端通訊系統，其中，

上述伺服器以及上述認證台的一方可兼具他方。

1 4 . 一種行動終端，其特徵為：

具備從伺服器取得特定資料之手段，

和根據認證台之密碼鑰從收藏被編碼之伺服器證明書的服務終端取得上述伺服器證明書之手段，

和根據上述認證台之公開鑰查證上述伺服器證明書之手段，

和僅於得到肯定上述服務終端之正當性的查證結果時，將上述特定資料發訊上述服務終端之手段。

1 5 . 如申請專利範圍第 1 4 項之行動終端，其中，

具備使用上述認證台的公開鑰，執行從上述服務終端所取得之上述伺服器證明書的查證，限於得到肯定上述服務終端之正當性的查證結果時，從上述伺服器取得上述服務終端中為了實行發訊上述特定資料之處理的通訊應用軟體的手段，

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

六、申請專利範圍

依據上述通訊應用軟體之實行執行上述特定資料之發訊。

1 6 . 如申請專利範圍第 1 4 項所述之行動終端，其中，

具備從上述認證台取得證明該行動終端之正當性的客戶證明書的手段，

和將上述客戶證明書發訊至上述服務終端的手段。

1 7 . 一種服務終端，其特徵為：

具備對應於來自行動終端之要求，發訊從認證台所發行之伺服器證明書的手段，

和從上述行動終端，取得上述認證台所發行之客戶證明書的手段，

和將上述客戶證明書使用上述認證台之公開鑰查證的手段，

和僅於得到肯定上述行動終端之正當性的查證結果時，執行與上述行動終端間的通訊，上述行動終端取得從伺服器所取得之特定資料的手段。

1 8 . 一種記錄有程式之可供電腦讀取的記錄媒體，該程式是針對介由網路從伺服器被發送至行動終端，由上述行動終端的控制用電腦實行之程式，其特徵為該程式

將從通訊對象要求伺服器證明書的處理，

和使用某認證台之公開鑰，執行上述伺服器證明書之查證的處理，

和限於得到肯定上述通訊對象之正當性的查證結果時

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

六、申請專利範圍

，將從上述伺服器所取得之特定資料發訊至上述通訊對象的處理，

由上述控制用電腦實行。

19．如申請專利範圍第18項之記錄有程式之可供電腦讀取的記錄媒體，其中，

上述程式之內部是包含上述特定資料以及上述公開鑰

。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂