公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：95106213

※ 申請日期：95.2.24　※IPC 分類：H04L 9/32(2006.01)

一、發明名稱：（中文/英文）

資料通訊系統、代行系統伺服器、電腦程式及資料通訊方法

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

日商飛力凱網路股份有限公司
FELICA NETWORKS, INC.

代表人：（中文/英文）

河內　聰一

住居所或營業所地址：（中文/英文）

日本國東京都品川區大崎 1-11-1
GATE CITY OSAKI WEST TOWER 1-11-1, OSAKI SHINAGAWA-KU, TOKYO, 141-0032, JAPAN

國　籍：（中文/英文）

日本 JAPAN

三、發明人：（共 2 人）

姓　名：（中文/英文）

1. 德野　行太
   TOKUNO, KOTA
2. 疋田　智治
   HIKITA, TOMOHARU

國　籍：（中文/英文）

1. 日本 JAPAN
2. 日本 JAPAN

四、聲明事項：

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

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 日本；2005 年 03 月 03 日；特願 2005-058868

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種資料通訊系統、代行系統伺服器、電腦程式及資料通訊方法。

【先前技術】

如今，由於資訊處理技術之發展以及網路技術之多樣化，一般可經由網路，自PC(個人電腦)等資訊處理裝置，簡便地對伺服器等裝置所持有之大量資訊進行存取。

又，例如，對於先前僅限於通話功能之行動電話，如今亦可藉由通訊協定轉換等，經由網際網路等網路簡便地對大量資訊進行存取，且具有與資訊處理裝置同等之功能。

另一方面，可經由讀寫器(R/W)而與其他伺服器等資訊處理裝置進行通訊之非接觸式IC卡得到實用化。進而，揭示有如下技術，將該非接觸式IC卡或者具有非接觸式IC卡功能之裝置(以下稱為非接觸式IC卡模組)搭載於行動電話等小型輕便之行動通訊終端上，例如於外部系統與非接觸式IC卡之間進行通訊(例如參照專利文獻1(日本專利特開2002-133373號公報))。

該先前文獻1中，可於非接觸式IC卡模組中登錄複數個應用程式。上述應用程式藉由屬於服務提供者側之服務提供管理系統等而製成。

使用者例如根據使用者之用途而登錄複數種應用程式，並置於讀寫器上方而使非接觸式IC卡模組進行資訊處理，藉此使用者可享受服務提供系統所提供之服務。

再者，執行對非接觸式IC卡模組所記憶之資訊進行讀取或寫入等資訊處理時，藉由自屬於發行以及/或者運用該非接觸式IC卡之事業者側的管理系統，對非接觸式IC卡進行通訊處理，而進行資訊處理。

【發明內容】

然而，與行動通訊終端所具有之非接觸式IC卡模組進行通訊處理時，於管理系統側，考慮到安全性而必須對該行動通訊終端進行驗證，但由於對行動通訊終端進行管理之各提供者(電信業者等)之驗證方式不同或者無驗證機構，故而造成驗證不統一或不充分。

因此，沒有實現驗證處理之靈活性，即，使用者側無法自驗證方式相異之服務提供系統享受服務等，無法對非接觸式IC卡模組高效執行資訊處理，又，提供者側對管理系統可對應之驗證方式的選擇受到限定等。

本發明係鑒於上述問題開發而成者，本發明之目的在於提供一種新穎且經改良之資料通訊系統、代行伺服器、電腦程式及資料通訊方法，該資料通訊系統可結合1或2種驗證機構對行動通訊終端進行驗證，並對該行動通訊終端所具有之非接觸式IC卡模組執行通訊處理。

為解決上述問題，根據本發明之第1觀點，提供一種資料通訊系統，其具有：一個以上行動通訊終端，其等各自包含對應外部請求而進行資訊處理之非接觸式IC卡模組；服務提供系統，其藉由該非接觸式IC卡模組之資訊處理而提供服務；以及代行系統，其代替該服務提供系統而與非接

觸式IC卡模組進行通訊處理。上述資料通訊系統之行動通訊終端，具備請求部，其為使非接觸式IC卡模組與代行系統進行通訊處理，而請求服務提供系統所持有之資訊即表示已授予行動通訊終端且關於該通訊處理之許可證的已授權許可證資訊；服務提供系統具備獲取部，當受到一個行動通訊終端請求時，其獲取該請求源之行動通訊終端之已授權許可證資訊；該所獲取之已授權許可證資訊，藉以系統驗證金鑰由上述服務提供系統加密，進而藉以用戶端驗證金鑰由行動通訊終端加密後發送至代行系統，該系統驗證金鑰係保存於代行系統以及服務提供系統雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰係保存於行動通訊終端以及代行系統雙方且可於該雙方間對資訊進行加密/解密；代行系統具備：驗證部，其依據來自行動通訊終端之已授權許可證資訊而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即(1)藉由使用系統驗證金鑰而對服務提供系統進行驗證之系統驗證處理、(2)藉由用戶端驗證金鑰而對行動通訊終端進行驗證之第1用戶端驗證處理、及(3)藉由使用識別行動通訊終端之識別資訊而對行動通訊終端進行驗證之第2用戶端驗證處理；判斷部，其於驗證部之驗證處理後，根據已授權許可證資訊中所設定之許可證而判斷通訊允許/通訊不允許；通訊部，當上述判斷部判斷為允許通訊時，其與非接觸式IC卡模組進行通訊處理。再者，雖例舉上述識別資訊對行動通訊終端進行識別之情形加以說明，但並非限定於該例，例如，亦

可為識別資訊對儲存於行動通訊終端之用戶端應用程式進行識別等，又，系統驗證金鑰或者用戶端驗證金鑰亦可間隔特定時間而更新為其他系統驗證金鑰或用戶端驗證金鑰。

根據本發明，於資料通訊系統中，行動通訊終端自服務提供系統獲取已授權許可證資訊，並將該已授權許可證資訊發送至代行系統，藉此，代行系統藉由執行自1或2種以上驗證處理中選擇至少一個並進行組合後的驗證處理，而根據該已授權許可證資訊，驗證服務提供系統以及行動通訊終端之可靠性。驗證結果為，若允許通訊處理，則行動通訊終端所具有之非接觸式IC卡模組與通訊部進行通訊處理。藉由該結構，可根據服務提供系統之安全級別等，對代行系統之驗證處理進行選擇、組合後進行驗證，故而可進行通用性較高之驗證處理，其結果，可不依賴行動通訊終端之機種，對非接觸式IC卡模組進行資訊處理，而可實現通用性較高之資料通訊系統。

亦可構成為，驗證部接收選擇1或2種以上之驗證處理中一個或二個以上進行組合後之驗證處理的選擇指示，並按照所接收之上述選擇指示而執行驗證處理。藉由該結構，接收來自服務提供系統或代行系統之請求作為選擇指示，並執行驗證處理，藉此可進行靈活性、通用性更高之驗證處理。

亦可構成為，上述通訊部所進行之通訊處理，係於非接觸式IC卡模組中執行寫入處理或讀取處理之處理。

亦可構成為上述驗證部，針對成為上述讀取處理對象之資料，接收對該資料進行加密的處理，或者將依據資料而製成之電子簽章添加至該資料的處理其中之一或兩者之處理的選擇指示，並按照所接收之選擇指示進行處理。

亦可構成為上述驗證部，針對成為上述寫入處理對象之資料，接收對加密資料進行解密的處理，以及依據預先添加有電子簽章之資料而驗證該資料之可靠性的處理其中之一或兩者之處理的選擇指示，並按照該選擇指示進行處理。

亦可構成為，上述服務提供系統與上述代行系統之通訊係經由行動通訊終端而進行。

亦可構成為上述第1用戶端驗證處理，係向行動通訊終端發送詰問碼(challenge code)，並接收依據該詰問碼與已授權許可證資訊而製成之回應，藉此進行驗證之詰問/回應方式的驗證處理。再者，並非限定於該例，例如，本發明之該第1用戶端驗證處理亦可為，藉由接收依據詰問碼與已授權許可證資訊及用戶端驗證金鑰所製成之回應，而進行驗證等。

亦可構成為上述行動通訊終端為行動電話。藉由該結構，無關行動電話之提供者、或機種等差異，可於代行系統側進行驗證處理，故而可對非接觸式IC卡模組執行資訊處理。

為解決上述課題，根據本發明之其他觀點，提供一種代行系統伺服器，其代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務之服務提供伺服器，

並與該非接觸式IC卡模組進行通訊處理。上述代行系統伺服器具備：接收部，其自該行動通訊終端接收經過加密之已授權許可證資訊，該已授權許可證資訊表示關於非接觸式IC卡模組與代行系統伺服器之通訊處理之許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由行動通訊終端加密，而該系統驗證金鑰保存於代行系統伺服器以及服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且可於該雙方之間對資訊進行加密/解密；驗證部，其依據來自行動通訊終端之已授權許可證資訊而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用系統驗證金鑰而對服務提供系統進行驗證之系統驗證處理、藉由使用用戶端驗證金鑰而對行動通訊終端進行驗證之第1用戶端驗證處理、以及藉由使用識別行動通訊終端之識別資訊而對行動通訊終端進行驗證之第2用戶端驗證處理；判斷部，其於上述驗證部之驗證處理後，根據已授權許可證資訊而判斷通訊允許/通訊不允許；通訊部，當上述判斷部判斷為允許通訊時，其與非接觸式IC卡模組進行通訊處理。

根據本發明，代行系統伺服器中，上述接收部接收自行動通訊終端發送之已授權許可證資訊，並依據該已授權許可證資訊，執行自1或2種以上驗證處理中選擇至少一個進行組合後之驗證處理，藉此驗證服務提供系統、行動通訊終端之可靠性。驗證結果為，若允許通訊處理，則行動通

訊終端所具備之非接觸式IC卡模組與通訊部進行通訊處理。藉由該結構，可對應服務提供伺服器側之安全級別等，自可執行的1或2種以上驗證處理中選擇適當驗證處理，並進行組合而由代行系統伺服器執行，故而可進行通用性較高之驗證處理，其結果，可不依賴行動通訊終端之機種等，而對非接觸式IC卡模組執行資訊處理。

亦可構成為上述驗證部，接收選擇1或2種以上驗證處理中一或兩個以上進行組合後之驗證處理的選擇指示，按照所接收之選擇指示執行驗證處理。

為解決上述課題，藉由本發明其他觀點，提供一種電腦程式，其使電腦作為代行系統伺服器而起作用，該代行系統伺服器代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務的服務提供伺服器，與該非接觸式IC卡模組進行通訊處理。上述電腦程式具有：接收步驟，其自該行動通訊終端接收經過加密之已授權許可證資訊，該已授權許可證資訊表示關於非接觸式IC卡模組與代行系統伺服器之通訊處理的許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由該行動通訊終端加密，而該系統驗證金鑰保存於代行系統伺服器以及服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且於該雙方之間可對資訊進行加密/解密；驗證步驟，其依據來自行動通訊終端之已授權許可證資訊，而執行包含以下驗證處理之複數個驗證處

理中至少一個驗證處理，即藉由使用系統驗證金鑰而對服務提供系統進行驗證的系統驗證處理、藉由使用用戶端驗證金鑰而對行動通訊終端進行驗證的第1用戶端驗證處理、或者藉由使用識別行動通訊終端之識別資訊而對行動通訊終端進行驗證的第2用戶端驗證處理；判斷步驟，於上述驗證處理之後，根據已授權許可證資訊而判斷通訊允許/通訊不允許；通訊步驟，當上述判斷結果為允許通訊時，進行與非接觸式IC卡模組之通訊處理。

為解決上述課題，根據本發明其他觀點，提供一種代行系統伺服器之資料通訊方法，該代行系統伺服器代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務的服務提供伺服器，與該非接觸式IC卡模組進行通訊處理。上述資料通訊方法包含：接收步驟，其自該行動通訊終端接收經過加密之已授權許可證資訊，該已授權許可證資訊表示關於非接觸式IC卡模組與代行系統伺服器之通訊處理的許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由行動通訊終端加密，而該系統驗證金鑰保存於代行系統伺服器以及服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且於該雙方之間可對資訊進行加密/解密；驗證步驟，其依據來自行動通訊終端之已授權許可證資訊，而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用系統驗證金鑰而對服務提供系

統進行驗證的系統驗證處理、藉由使用用戶端驗證金鑰而對行動通訊終端進行驗證的第1用戶端驗證處理、以及藉由使用識別行動通訊終端之識別資訊而對行動通訊終端進行驗證的第2用戶端驗證處理；判斷步驟，於執行驗證步驟之後，根據已授權許可證資訊而判斷通訊允許/通訊不允許；通訊步驟，當判斷步驟之判斷結果為允許通訊時，進行與非接觸式IC卡模組之通訊處理。

【實施方式】

以下，關於本發明之較佳實施形態，參照附圖加以詳細說明。再者，以下說明以及附圖中，針對具有大致相同功能及結構之結構要素，付與相同符號而省略重複說明。

(關於資料通訊系統)

首先，參照圖1，就本實施形態之資料通訊系統100加以說明。圖1係本實施形態之資料通訊系統之一例概略說明圖。

如圖1所示，資料通訊系統100具備服務提供系統101、代行系統105、行動通訊終端103(103a、103b、...103n)、通訊網104、通訊網106、通訊網108、資訊處理裝置109(109a、109b、...109n)、讀/寫裝置(R/W)111(111a、111b、...111n)、基地台113、封包通訊網115、閘道器117。

上述服務提供系統101係根據行動通訊終端103之請求而生成已授權許可證資訊的系統。又，服務提供系統101製作行動通訊終端103所執行之用戶端應用程式(client application)等。

服務提供系統101係，藉由對上述非接觸式IC卡模組執行資料寫入或讀取等資訊處理，而向使用行動通訊終端103之使用者提供服務的系統。

例如，服務提供系統101所提供之服務為對應商品購入款額所付與之點數時，若藉由行動通訊終端103中所儲存之用戶端應用程式發送於網路上在線購入商品之商品購入資訊，而使該商品購入成立，則向代行系統105發出請求，以使用戶端應用程式根據該商品購入費用將所產生之點數資訊儲存至非接觸式IC卡模組。

再者，詳情於下文進行敘述，由於依賴對代行系統105進行通訊處理而必須驗證行動通訊終端103，因此在此之前用戶端應用程式自服務提供系統101獲取已授權許可證資訊之一部分(例如使用條件)或者全部。其後，代行系統105使資料記憶至非接觸式IC卡模組。

又，非接觸式IC卡模組所記憶之資料，例如可例示為上述點數資訊、電子貨幣等。又，有時亦將該資料總稱為電子價值資訊，該電子價值資訊表示網路上進行交易之資訊即具有貨幣價值等特定價值之資訊。進而，有時亦根據貨幣收入，將加算非接觸式IC卡模組中電子貨幣之餘額，記錄為費用。

此處，服務提供者係操作服務提供系統101，並進行搭載於行動通訊終端103上之用戶端應用程式的製作以及提供等業務之事業主體。

其次，上述代行系統105係代替服務提供系統進行如下處

理之系統：將非接觸式IC卡模組(非接觸式IC卡)之發行或管理、及用戶端應用程式相關之環境設定資訊等登錄至非接觸式IC卡模組內的記憶區域；刪除其環境設定資訊；讀取非接觸式IC卡模組內之記憶區域中所儲存之電子價值資訊；或者將電子價值資訊寫入非接觸式IC卡模組中等。

代行系統105代替上述服務提供系統101，使非接觸式IC卡模組執行資料讀/寫等資訊處理。即，服務提供系統101無法使非接觸式IC卡模組直接執行，而是將對非接觸式IC卡模組之一切處理權限轉讓於代行系統105。

再者，本實施形態中，例舉說明行動通訊終端103中具備非接觸式IC卡模組之情形，而該非接觸式IC卡模組係包括非接觸式IC卡在內，具有非接觸式IC卡之功能之裝置的總稱。

又，代行系統105，以服務提供系統101為單位，製作使代行系統105與服務提供系統101之間安全的系統驗證金鑰。所製成之系統驗證金鑰分別儲存於代行系統105與服務提供系統101中。再者，該系統驗證金鑰之製作亦可於服務提供系統101側進行。

再者，關於本實施形態之系統驗證金鑰，例舉說明按每個服務提供系統101製作一個之情形，但並不限定於該情形，例如，亦可實施為僅製作服務提供系統101所提供之用戶端應用程式種類數的系統驗證金鑰。

系統驗證金鑰係機密性極高之秘密資訊，故而儲存於具有防竄改特性等之記憶機構等中。又，系統驗證金鑰，例

如使用於代行系統105與服務提供系統101之相互驗證等。

又，亦可實施為該系統驗證金鑰為RSA等非對稱金鑰、DES或AES等對稱金鑰等任何金鑰。再者，為對稱金鑰之情形時，由於必須秘密地將金鑰發送至對方，故而並非通過通訊網直接發送，而是藉由附有內容證明之郵寄等其他方式進行發送。

當上述代行系統105中登錄服務提供系統101相關之資訊，且儲存系統驗證金鑰時，行動通訊終端103執行用戶端應用程式，代行系統105進行驗證，則代行系統105代替服務提供系統101，與該行動通訊終端103中所具備之非接觸式IC卡模組進行存取。

再者，存取係以下經由通訊網對資訊進行處理之資訊處理的總稱，例如系統之使用、與系統或伺服器之連接、檔案之參照、檔案之保存、檔案之刪除或者檔案之變更等。

其次，行動通訊終端103(103a、103b、...103n)係1或2個以上可進行通訊之終端，其具有經由基地台113進行通話之功能，可藉由基地台113、封包通訊網115及閘道器117而與服務提供系統101進行存取。

即，行動通訊終端103可執行具有瀏覽功能之用戶端應用程式，接收使用者對URL等之指定，自Web伺服器接收依照HTML之Web資料，並顯示於畫面。

又，行動通訊終端103除具備上述通話功能、瀏覽功能之外，亦具有可經由R/W111無線交換資料之非接觸式IC卡模組(包含非接觸式IC卡等)。

非接觸式IC卡模組，當將行動通訊終端103近距離置於R/W111等之上方時，可通過無線經由R/W111，將非接觸式IC卡模組內所記憶之資料，例如發送至代行系統105等。

又，行動通訊終端103，持有用以對代行系統105進行存取時，與代行系統105進行相互驗證之驗證金鑰(用戶端驗證金鑰)。再者，該用戶端驗證金鑰為機密性極高之秘密資訊，故而儲存於具有防竄改特性等之記憶機構等中，然而也並非必須。

又，亦可實施為該用戶端驗證金鑰為RSA等非對稱金鑰、DES或AES等對稱金鑰等任何金鑰。再者，為對稱金鑰之情形時，由於必須秘密地將金鑰發送至對方，故而並非通過通訊網直接發送，而是藉由郵寄等其他方式進行發送。

又，詳情於下文進行敘述，行動通訊終端103持有，對儲存於行動通訊終端103內之用戶端應用程式進行識別的用戶端應用程式識別資訊。代行系統105亦可依據該用戶端應用程式識別資訊，對行動通訊終端103進行驗證。再者，行動通訊終端103並非必須持有用戶端應用程式識別資訊，亦可並不持有該用戶端應用程式識別資訊。

再者，如圖1所示，本實施形態之資料通訊系統100中，服務提供系統101與行動通訊終端103藉由通訊網108等而連接，行動通訊終端103與代行系統105藉由通訊網106等而連接。即，由於並不存在直接連接代行系統105與服務提供系統101之網路，而無法直接進行通訊，故而若不經由上述行動通訊終端103，則代行系統105與服務提供系統101無法

進行資料交換。

因此，可藉由間接插入由行動通訊終端103之用戶端應用程式所進行之通訊處理，而將來自服務提供系統101之資訊發送至代行系統105。

再者，本實施形態之行動通訊終端103與服務提供系統101之間的通訊網104等中，並非限定於HTTP或HTTPS等TCP/IP通訊，若為行動通訊終端103所具備之通訊功能，則任何情形時均可實施，例如，可例示非接觸式IC卡、接觸式IC卡、紅外線(Ir)，QR碼(Quick Response Code，快速回應碼)等二維條形碼，或者電子郵件(SMTP等)。該通訊，尤其有效於自服務提供系統101向行動通訊終端103之用戶端應用程式發送已授權許可證資訊等時的通訊方式。

又，本實施形態之行動通訊終端103與代行系統105之間的通訊網106中，可例示藉由HTTP或HTTPS等TCP/IP通訊而進行。

(服務提供系統101)

繼而，參照圖2，就本實施形態之服務提供系統101加以說明。再者，圖2係本實施形態之資料通訊系統中所具備之服務提供系統的概略說明圖。

如圖2所示，服務提供系統101具有服務提供伺服器201。如上所述，服務提供伺服器201可經由通訊網108等而與行動通訊終端103進行資料交換。

又，如圖2所示，服務提供伺服器201具備許可證獲取部211、通訊部231、許可證驗證部241。

許可證獲取部211，若自行動通訊終端103接收請求資訊，則依據該請求資訊自許可證資料庫(未圖示)中獲取相應許可證，並生成已授權許可證資訊。

如上所述，許可證獲取部211持有系統驗證金鑰220b，其對應於代行系統105側所持有之系統驗證金鑰220a。

上述請求資訊中包含有指定自身行動通訊終端103之資訊。再者，詳情於下文進行敘述。許可證獲取部211根據上述請求資訊中所包含之資訊而獲取相應許可證，並使用上述系統驗證金鑰220b生成已授權許可證資訊。

通訊部231可經由通訊網108、閘道器117、封包通訊網115、基地台113而與行動通訊終端103進行通訊，通訊部231自行動通訊終端103接收請求資訊等資料，或者向行動通訊終端103發送已授權許可證資訊等資料。

(許可證獲取部211)

其次，參照圖3，就本實施形態之許可證獲取部之已授權許可證資訊的生成處理加以說明。圖3係本實施形態之許可證獲取部之已授權許可證資訊生成處理的概略說明圖。

如圖3所示，許可證獲取部211接收使用條件資訊(或者簡稱為「使用條件」)以及個別資訊之輸入，並生成將使用條件資訊與個別資訊設為一組之已授權許可證資訊。進而，許可證獲取部211，使用預先於代行系統105與服務提供系統101之間所製成之系統驗證金鑰220b，對已授權許可證資訊進行加密。

再者，許可證獲取部211除藉以系統驗證金鑰220b對已授

權許可證資訊進行加密之外，例如亦可將簽章資料添加至已授權許可證資訊，該簽章資料係求出所生成之已授權許可證資訊之雜湊值，並藉以系統驗證金鑰220b對其進行加密，藉此而製成者。

上述個別資訊包含自行動通訊終端103發送而來的請求資訊。個別資訊中包含有例如用以識別非接觸式IC卡模組之「IC卡ID」、或用以識別行動通訊終端103中所儲存之用戶端應用程式的「用戶端應用程式ID」等。

又，上述使用條件資訊係來自行動通訊終端103之請求資訊所包含之個別資訊所對應的資訊，且係成為用以設定服務提供之允許/不允許之判斷材料的許可證資訊。

關於使用條件資訊，若例如將用戶端應用程式儲存於行動通訊終端103，並將用戶端應用程式登錄於代行系統105，則服務提供系統101中製成用以使服務可使用之使用條件資訊。

使用條件資訊係設定為使該服務提供系統101所提供之服務可使用的條件，例如使用條件資訊中，設定有「有效期間開始時間」以及「有效期間結束時間」，並根據該等時間而確定服務可使用之期間。又，藉由設定「使用次數」，可確定服務可使用之期間中可使用的次數。

再者，上述使用條件資訊並非係以個別資訊為單位製成內容相異之資訊，例如，亦可於將全部包含"*"之ID設定為個別資訊之「IC卡ID」的情形時，製成「有效期間開始時間」與「有效期間結束時間」一律設定為特定時間之全部

相同內容的使用條件資訊。該情形時，例如，可按照服務內容，針對全部使用者所持有之非接觸式IC卡模組，設置服務可使用之對象。

又，於進行包含驗證行動通訊終端103是否可使用服務在內的驗證處理之情形時，無需個別資訊中所包含之寫入非接觸式IC卡模組之資料(寫入資料)或者自非接觸式IC卡模組內之記憶區域所讀取之資料(讀取資料)。再者，自代行系統105對非接觸式IC卡模組進行寫入/讀取處理時，上述寫入資料或者讀取資料為必須資料。

再者，例舉說明有本實施形態之許可證獲取部211藉由輸入使用條件與個別資訊而生成已授權許可證資訊之情形，但並非限定於該例，例如，亦可實施為藉由輸入使用條件而生成已授權許可證資訊。即，已授權許可證資訊中包含一部分(使用條件等)或者全部(使用條件、個別資訊等)。再者，並非特別指定之情形時，已授權許可證資訊表示包含一部分(使用條件等)或者全部(使用條件、個別資訊等)之資訊。

(行動通訊終端103)

繼而，參照圖4，就本實施形態之行動通訊終端103加以說明。圖4係本實施形態之行動通訊終端103之一例概略結構方塊圖。

如圖4所示，行動通訊終端103具備應用程式部203，其儲存於記憶體或者HDD等中作為應用程式而起作用；執行部213，其根據來自應用程式部203之請求而執行處理；以及

非接觸式IC卡模組223。

應用程式部203如上所述，係由服務提供系統101所製成之用戶端應用程式。因此，若行動通訊終端103經由通訊網等自服務提供伺服器201接收用戶端應用程式，則可將其例如以可執行之方式儲存至EEPROM等記憶體或HDD中。

例舉說明本實施形態之應用程式部為包含1或2個以上模組或者組件的軟體之情形，但並非限定於該例，例如亦可實施為由1或2個以上元件所形成之電路等硬體之情形。上述情形時，可自服務提供系統101通過通訊網以外之郵寄方式而提供應用程式部203，使得使用者自行藉由安裝硬體等而實施。

再者，用戶端應用程式儲存時，例如對自服務提供伺服器201所傳遞來之用戶端應用程式進行識別之用戶端應用程式ID亦可儲存於相同記憶機構內。該用戶端應用程式ID用於對代行系統101進行存取時之驗證。

執行部213係包含預先裝入行動通訊終端103中之1或2個以上模組的軟體。若自應用程式部203產生通訊處理等請求，執行部213經由通訊網而對伺服器進行存取、或將自通訊對方發送而來之資料反饋至應用程式部203。

非接觸式IC卡模組223，可例示有非接觸式IC卡、具有非接觸式IC卡功能之裝置或者半導體元件等。進而非接觸式IC卡係具備天線且可進行調變-解調變並以接近距離進行無線通訊之IC卡。藉由上述無線通訊，可自非接觸式IC卡所具備之記憶機構中讀出資料、或將資料寫入記憶機構中。

行動通訊終端103與伺服器(服務提供伺服器201、代行系統伺服器205)之間進行通訊之情形時，首先，行動通訊終端103之應用程式部203對執行部213進行通訊請求。

再者，如上所述，本實施形態之資料通訊系統100之行動通訊終端103與伺服器之通訊中，設有自行動通訊終端103產生開始通訊之觸發，但並非限定於該例。

當應用程式部203對伺服器產生通訊請求時，執行部213經由通訊網嘗試對伺服器進行存取。再者，考慮到此時之安全性，根據直接通訊對方而進行驗證，因此將實施加密或添加電子簽章等之處理。詳情於下文進行敘述。

若於伺服器進行驗證，則於執行部213與伺服器之間建立連接，進而上述通訊請求為非接觸式IC卡模組223相關之資訊處理之情形時，伺服器(代行系統伺服器205)與非接觸式IC卡模組223之間進行相互驗證，並於該雙方之間開始通訊處理。

其次，參照圖2，就行動通訊終端103所具備之應用程式部203加以具體說明。

如圖2所示，應用程式部203中具備請求部204、加密部206、回應生成部207以及ID獲取部208。

請求部204，為與代行系統伺服器205或服務提供伺服器201進行通訊而生成請求資訊，且具有藉由將請求資訊傳送至執行部213而進行通訊請求之功能。

請求部204，於生成上述請求資訊時，自HDD等記憶機構(未圖示)中獲取個別資訊，並設定成請求資訊。

加密部206，使用與代行系統伺服器205所持有之用戶端驗證金鑰221a相對應之用戶端驗證金鑰221b，對資料進行加密。藉由該加密，代行系統伺服器205側之行動通訊終端驗證部217，藉以與該用戶端驗證金鑰221b相對應之用戶端驗證金鑰221a成功解密時，可使行動通訊終端103之可靠性正當化。

回應生成部207至少具有使用詰問/回應方式而生成回應之功能。回應生成部207獲取來自代行系統伺服器205之詰問碼並根據該詰問碼(或亂數種子(seed)等)而生成回應。再者，回應藉由求出詰問碼之雜湊值而生成，但並非限定於該例，例如亦可添加詰問碼以及根據使用者之輸入而接收之密碼後，求出雜湊值而生成回應。

又，回應生成部207，詳情於下文進行敘述，而使用上述加密部206所持有之用戶端驗證金鑰221b，將已授權許可證資訊與回應設為一組進行加密。

ID獲取部208自記憶機構中獲取識別應用程式部203之用戶端應用程式ID。再者，用戶端應用程式ID並未儲存於記憶機構中之情形時，ID獲取部208亦可生成用以於顯示畫面顯示並未獲取用戶端應用程式ID之訊息的畫面資訊。

(回應生成部207)

繼而，參照圖5，就本實施形態之回應生成部207之加密處理加以說明。圖5係本實施形態之回應生成部207之加密處理之一例概略說明圖。

如圖5所示，回應生成部207接收詰問(詰問碼)、已授權

許可證資訊及用戶端驗證金鑰221b作為輸入，並使用雜湊函數求出該等資訊之雜湊值(HMAC：Hashing for Message Authentication Code，雜湊訊息身份驗證代碼)。

所求出之雜湊值(回應)與上述已授權許可證資訊所包含之使用條件資訊(圖5所示之「使用條件」)一併，經由通訊網106，由執行部213發送至代行系統105。該發送處理中，經由通訊網106僅發送已授權許可證資訊中的使用條件資訊。再者，個別資訊儲存於行動通訊終端103之記憶機構(未圖示)等中，並預先或另行自該行動通訊終端103發送至代行系統105。又，代行系統105側亦可持有曾經由行動通訊終端103所發送之個別資訊的一部分(用戶端應用程式ID等)或者全部。

再者，例舉說明有本實施形態之資料通訊系統100中藉由回應生成部207進行HMAC運算之情形，但並非限定於該例，例如亦可實施為回應生成部207輸入詰問與已授權許可證資訊後求出雜湊值。再者，所求出之雜湊值，進而由回應生產部207，藉由使用用戶端驗證金鑰221b而受到加密，藉此生成回應。亦可使所生成之回應與已授權許可證資訊中所包含之使用條件資訊(圖5所示之「使用條件」)一併，經由通訊網106，由執行部213發送至代行系統105，繼而於代行系統105側，根據詰問、已授權許可證資訊中所包含之使用條件資訊以及個別資訊，與上述同樣地求出雜湊值(回應)，並藉以發送源之用戶端驗證金鑰221a對所接收之回應進行解密，進而比較雙方之回應而檢驗其一致不一致。

作為上述輸入資訊之詰問，係如上所述使用有詰問/回應方式之詰問碼，且由代行系統伺服器205生成。

又，作為對回應生成部207之輸入資訊的已授權許可證資訊中一部分資訊(圖5所示之「使用條件」)，與發送回應一併，或者於其他任意時間，經由通訊網106，由執行部213直接發送至代行系統105。此係為使其作為驗證時的判斷材料。

(代行系統105)

其次，參照圖2，就本實施形態之代行系統105加以說明。再者，圖2係本實施形態之資料通訊系統之概略說明圖。

如圖2所示，代行系統105具備代行系統伺服器205。如上所述，代行系統伺服器205可經由通訊網106等而與行動通訊終端103交換資料，進而可經由通訊網104、R/W111與行動通訊終端103所具備之非接觸式IC卡模組進行通訊。

如圖2所示，代行系統伺服器205具備接收部214、驗證部215、判斷部225、通訊部235、驗證處理管理部245。當自判斷部225產生指示時，通訊部235經由行動通訊終端103之執行部213與非接觸式IC卡模組223進行通訊。

再者，自行動通訊終端103發送如下具體之通訊處理內容：寫入資料至非接觸式IC卡模組223所具備之記憶機構的記憶區域之特定位址的處理、讀取儲存於非接觸式IC卡模組223所具備之記憶機構的記憶區域之特定位址之資料的處理等。

驗證部215進而具備系統驗證部216，其使用系統驗證金

鑰220a對服務提供系統101進行驗證；行動通訊終端驗證部217，其對用戶端(行動通訊終端103)進行驗證；詰問/回應驗證部218，其通過詰問/回應方式對行動通訊終端103進行驗證；ID驗證部219，其藉以用戶端應用程式ID對行動通訊終端103進行驗證。

系統驗證部216，於可使用系統驗證金鑰220a對由服務提供伺服器201所加密之資料進行解密之情形時，可針對作為發送源之服務提供伺服器201的可靠性進行驗證。

行動通訊終端驗證部217，亦與上述相同，於可使用用戶端驗證金鑰221a對由行動通訊終端103所加密之資料進行解密之情形時，可對作為發送源之行動通訊終端103的可靠性進行驗證。

當自行動通訊終端103產生詰問之請求時，詰問/回應驗證部218生成詰問碼，並發送至行動通訊終端103，並且根據詰問及另外所接收之已授權許可證資訊，求出雜湊值而製成比較對照用回應。且，若自行動通訊終端103接收到回應，則將該回應與比較對照用回應進行比較，並確認一致/不一致。若雙方一致，則判斷具有可靠性，故而可驗證行動通訊終端103。

當接收到自行動通訊終端103發送而來之用戶端應用程式ID時，ID驗證部219預先自用戶端應用程式ID資料庫(未圖示)檢索相應用戶端應用程式ID。

檢索結果為相應用戶端應用程式ID已存在之情形時，則判斷通訊源之行動通訊終端103為可靠。再者，用戶端應用

程式ID資料庫中儲存有全部所登錄之用戶端應用程式ID。用戶端應用程式ID亦可經過加密，並經由行動通訊終端103例如自服務提供系統101發送至代行系統105。

判斷部225，接收上述驗證部215之驗證結果，進而參照已授權許可證資訊中所包含之上述說明之「使用次數」、「有效期間開始時間」以及「有效期間結束時間」，判斷是否可提供服務。

當接收到例如自內部連接至代行系統伺服器205之控制臺、或管理服務提供系統之管理者所使用之資訊處理裝置中選擇有1或2種以上驗證處理之選擇資訊時，驗證處理管理部245藉由選擇資訊中所揭示之驗證處理，而指示(驗證處理之選擇指示)驗證部216執行驗證處理。

更具體地加以說明，驗證部215於執行驗證處理時，以何種方式或種類之驗證處理而執行，係於驗證處理管理部245進行詢問處理後再執行驗證處理。

因此，若產生來自驗證部215之詢問，則驗證處理管理部245指示驗證部215藉以選擇資訊中所揭示之1或2種以上驗證處理而執行。再者，上述選擇資訊係發送自相應服務提供系統101或者代行系統105所連接之控制臺等。

根據其指示內容，藉由驗證部215所具備之系統驗證部216、行動通訊終端驗證部217、詰問/回應驗證部218或者ID驗證部219中至少一個而執行驗證處理。

驗證處理管理部245，為對驗證部215指示驗證處理，例如，持有驗證處理資料庫(未圖示)，該驗證處理資料庫係識

別服務提供系統101之服務提供系統ID與選擇資訊相關聯。

若自控制臺接收到選擇資訊，驗證處理管理部245則參照選擇資訊中所設定之服務提供系統ID，更新驗證處理資料庫中所儲存之相應選擇資訊。

再者，例舉說明有本實施形態之驗證部215所具備之各驗證部(216、217、218)驗證是否可對加密資料進行解密之情形，但並非限定於該例，例如，亦可於資料中添加電子簽章之情形時，各驗證部(216、217、218)根據該資料製成電子簽章，並藉由判斷資料中所添加之電子簽章與製作後之電子簽章一致/不一致而進行驗證。

(驗證處理之組合)

根據需要可改變設定於選擇資訊中之驗證處理的組合。驗證處理中存在複數種驗證處理。代行系統105可自所提供之複數種驗證處理中組合選擇適當之驗證處理。

此處，參照圖6，就驗證處理管理部245自控制臺等接收之驗證處理之選擇畫面加以說明。圖6係用以選擇本實施形態之驗證處理之選擇畫面的概略說明圖。

圖6所示之選擇畫面係用以選擇驗證處理之畫面，例如顯示於藉以LAN等內部連接於代行系統伺服器205之控制臺等上。再者，並非限定於該例，例如，選擇畫面亦可顯示於運用服務提供系統101之管理者所使用之資訊處理裝置中。該情形時，為驗證其為管理者所使用之資訊處理裝置，需要資訊處理裝置接收登錄密碼等，且代行系統伺服器205進行驗證。

如圖6所示，選擇畫面中，顯示有選擇行動通訊終端驗證部217所進行之驗證行動通訊終端103之驗證處理的勾選框601a、及選擇詰問/回應驗證部218所進行之驗證處理的勾選框601b等。藉由配合安全級別而選擇上述勾選框601，可實現各種驗證處理之組合。

點擊該勾選框601，而選擇由代行系統105所進行之驗證處理之方式。圖6所示之選擇例中，選擇有勾選框601a、勾選框601b、勾選框601d、勾選框601e。

若點擊「更新」按鈕，則於控制臺側生成選擇資訊，並將選擇資訊發送至驗證處理管理部245。藉由以上方式，代行系統105可靈活應對服務提供系統101側所希望進行之驗證處理。又，藉由組合驗證處理，可根據服務提供系統101自由選擇、改變安全級別。

再者，勾選框601d所示之讀取處理時的簽章添加，主要係為防止竄改自非接觸式IC卡模組223所讀取之資料而於代行系統105側添加電子簽章的功能。該功能，例如驗證部215所具備之各部均具有。

又，勾選框601e所示之寫入處理時的簽章添加，主要係為防止竄改自服務提供系統101側寫入至非接觸式IC卡模組223之資料而於服務提供系統101側添加電子簽章的功能。因此，選擇該功能之情形時，於代行系統105側必須確認依據所接收之資料而製成之電子簽章與發送而來之電子簽章的一致/不一致。再者，對寫入非接觸式IC卡模組223之資料的竄改進行檢測之該功能，例如驗證部215所具備之

各部均具有。

同樣，勾選框601f所示之讀取處理時的加密，主要係預先假定自非接觸式IC卡模組223所讀取之資料被盜聽之風險，而於代行系統105側對資料進行加密的功能。該功能，例如驗證部215所具備之各部均具有。因此，選擇該功能之情形時，於代行系統105側經過加密之資料，必須於服務提供系統101側進行解密。

勾選框601g所示之寫入處理時的加密，主要係假定自服務提供系統101側寫入非接觸式IC卡模組223之資料被盜聽之風險，而於服務提供系統101側對上述資料進行加密的功能。因此，選擇該功能之情形時，必須於代行系統105側，使用特定系統驗證金鑰等金鑰，對所接收之資料進行解密。再者，對寫入該非接觸式IC卡模組223之資料進行解密之該功能，例如驗證部215所具備之各部均具有。

(與非接觸式IC卡模組之通訊處理)

其次，參照圖7，包含本實施形態之驗證部215之驗證處理在內，就與非接觸式IC卡模組之通訊處理加以說明。圖7係表示驗證本實施形態之系統驗證部216、行動通訊終端驗證部217以及ID驗證部219進行驗證時的驗證處理，以及與非接觸式IC卡模組之通訊處理的概略序列圖。

如圖7所示，執行針對行動通訊終端103之驗證處理之情形時，應用程式部203首先對服務提供伺服器201進行存取(S701)。再者，應用程式部203已經保存有已授權許可證資訊，且該已授權許可證資訊為有效之情形時，則不對服務

提供伺服器201進行存取。

又，關於用以對服務提供伺服器201進行存取之服務提供伺服器201之位址，例如，以服務提供伺服器201之URL等為依據，應用程式部203通過執行部213進行存取。

若自應用程式部203接收到個別資訊，則如上所述，服務提供伺服器201生成已授權許可證資訊(S702)，並將該已授權許可證資訊發送至請求源之行動通訊終端103之應用程式部203(S703)。

繼而，應用程式部203通過執行部213將所接收之已授權許可證資訊發送至代行系統伺服器205(S705)。由於並不自服務提供系統101直接將已授權許可證資訊發送至代行系統伺服器205，故而可提高兩個伺服器之安全獨立性。

此處，發送處理(S705)中，例舉說明ID獲取部208所獲取之用戶端應用程式ID亦一併發送之情形，但並非限定於該例，例如，亦可於未選擇使用用戶端應用程式ID之ID驗證處理之情形時，並不發送用戶端應用程式ID。

其次，若自行動通訊終端103接收到已授權許可證資訊與用戶端應用程式ID，代行系統伺服器205則首先依據該用戶端應用程式ID執行ID驗證部219之ID驗證處理(S707)。

ID驗證部219之ID驗證處理，於用戶端應用程式預先登錄作為應用程式部203時，確認是否與代行系統伺服器205之資料庫(用戶端應用程式資料庫)中所儲存之用戶端應用程式ID一致。

若ID驗證處理(S707)結束，繼而執行行動通訊終端驗證

部217之行動通訊終端103的驗證處理(S709)。該驗證處理，藉由行動通訊終端103是否可使用與加密已授權許可證資訊時所使用之用戶端驗證金鑰221b相對應之用戶端驗證金鑰221a進行解密，而進行驗證。若行動通訊終端驗證部217可進行解密，則可驗證為可靠之行動通訊終端103。

再者，例舉說明有本實施形態之資料通訊系統100中進行行動通訊終端103之驗證處理(S709)之情形，但並非限定於該例，亦可於資料通訊系統100中，例如並不進行下文所述之詰問/回應之驗證處理時，執行行動通訊終端103之驗證處理(S709)等。該情形時，可簡化驗證處理，故而可實現處理之效率化。

又，例舉說明有本實施形態之資料通訊系統100中進行行動通訊終端103之驗證處理(S709)之情形，但並非限定於該例，例如，亦可實施為資料通訊系統100中並不執行行動通訊終端103之驗證處理(S709)。

繼而，若行動通訊終端驗證部217之行動通訊終端103的驗證處理(S709)結束，則依據其所解密之已授權許可證資訊，系統驗證部216執行服務提供系統101之驗證處理(S711)。

系統驗證部216，藉由是否可使用與服務提供系統101側進行加密時所使用之系統驗證金鑰220b相對應之系統驗證金鑰220a進行解密，而對藉以行動通訊終端驗證部217之驗證處理(S709)所解密之已授權許可證資訊進行驗證。若系統驗證部216可解密，則可驗證為可靠之服務提供伺服器

201。

再者，例舉說明有本實施形態之驗證部215所具備之系統驗證部216、行動通訊終端驗證部217，藉由是否可對加密資料進行解密而進行驗證之情形，但並非限定於該例，例如於資料中添加有電子簽章之情形時，系統驗證部216、行動通訊終端驗證部217亦可依據該資料製成電子簽章，並藉由判斷資料中所添加之電子簽章與製作後之電子簽章的一致/不一致而進行驗證。

以上，若ID驗證部219、行動通訊終端驗證部217、系統驗證部216各自之驗證處理結束，判斷部225依據來自驗證部215之驗證結果以及已授權許可證資訊中所包含之許可證「使用條件」，判斷是否可對請求源之行動通訊終端103的非接觸式IC卡模組223進行通訊，而決定通訊處理(S713)。

若判斷部225決定與非接觸式IC卡模組223進行通訊處理(S713)，則通訊部235，經由通訊網106、閘道器117、封包通訊網115及基地台113，進而經由行動通訊終端103所具備之執行部213，與非接觸式IC卡模組223進行相互驗證(S715)。再者，進行相互驗證時，通訊部235確認通訊對方之「IC卡ID」與已授權許可證資訊中所包含之「IC卡ID」是否一致。

再者，本實施形態相關之通訊部235，並非限定於經由閘道器117及封包通訊網115等，進而經由行動通訊終端103所具備之執行部213而與非接觸式IC卡模組223進行相互驗

證之情形，例如，亦可實施為通訊部235經由R/W(讀/寫)111而與非接觸式IC卡模組223進行相互驗證(S715)。

若通訊部235與非接觸式IC卡模組223之相互驗證結束(S715)，通訊部235則於行動通訊終端103之驗證處理時根據請求要求而接收(S705)，或者於驗證處理後，藉由將記錄有另外所接收之通訊處理內容之通訊處理資訊發送至非接觸式IC卡模組223，而執行與非接觸式IC卡模組223之通訊處理(S717)。再者，該通訊處理(S717)係使用相互具有之加密金鑰/解密金鑰之安全通訊，但並非限定於該例。

非接觸式IC卡模組223，例如若接收設置將點數資訊“80”自通訊部235寫入記憶機構之記憶區域(例如位址“A”)之處理為通訊處理內容的通訊處理資訊，則按照該通訊處理內容將點資訊“80”寫入位址“A”。進而若該寫入處理結束，則將回應資訊作為處理結果發送至通訊部235。若存在後續通訊處理，則繼續執行通訊處理。

繼而，參照圖8，包含本實施形態之驗證部215之驗證處理在內，就與非接觸式IC卡模組之通訊處理加以說明。圖8係表示本實施形態之詰問/回應驗證部218及ID驗證部219進行驗證之情形時的驗證處理、以及與非接觸式IC卡模組之通訊處理的概略序列圖。

如圖8所示，執行針對行動通訊終端103之驗證處理之情形時，應用程式部203，首先對服務提供伺服器201進行存取(S801)。再者，如上所述，應用程式部203已經保存有已授權許可證資訊，且該已授權許可證資訊為有效之情形

時，不對服務提供伺服器201進行存取。

若自應用程式部203接收到個別資訊，則如上所述，服務提供伺服器201生成已授權許可證資訊(S802)，並將該已授權許可證資訊發送至請求源之行動通訊終端103的應用程式部203(S803)。

繼而，應用程式部203通過執行部213對代行系統伺服器205進行存取，並請求驗證處理(S805)。再者，該請求處理(S805)中，例舉說明ID獲取部208所獲取之用戶端應用程式ID亦一併發送之情形，但並非限定於該例，例如亦可於未選擇用戶端應用程式ID之ID驗證處理之情形時，不發送用戶端應用程式ID。

繼而，若自行動通訊終端103接收到用戶端應用程式ID，則ID驗證部219依據該用戶端應用程式ID而執行ID驗證處理(S807)。

若上述ID驗證部219之ID驗證處理結束，繼而，詰問/回應驗證部218生成詰問碼，並經由通訊網發送至行動通訊終端103(S809)。

應用程式部203，若自代行系統伺服器205接收詰問碼，則依據該詰問碼以及已授權許可證資訊，生成回應(S811)。再者，關於回應，已經加以說明，故而省略詳細說明。

繼而，應用程式部203通過執行部213將上述回應發送至代行系統伺服器205(S813)。又，於發送回應至代行系統伺服器205之同時，亦發送已授權許可證資訊(S813)。再者，

亦可實施為另外發送上述已授權許可證資訊。

繼而，接收到回應之詰問/回應驗證部218，根據已經生成之詰問碼以及自行動通訊終端103所發送之已授權許可證資訊，藉由進行與回應生成部207大致相同之處理，而生成回應。

再者，藉由行動通訊終端103對自行動通訊終端103所發送之已授權許可證資訊進行加密之情形時，詰問/回應驗證部218使用用戶端驗證金鑰221a進行解密後生成回應。

又，藉由服務提供伺服器201對自行動通訊終端103所發送之已授權許可證資訊進行加密之情形時，詰問/回應驗證部218使用系統驗證金鑰220a進行解密後生成回應。

詰問/回應驗證部218生成回應後，對來自行動通訊終端103之回應與所生成之回應加以比較，驗證其一致/不一致。詰問/回應驗證部218若確認回應一致，則可確認發送源之行動通訊終端103與服務提供伺服器201之可靠性，並結束驗證。

以上，詰問/回應驗證部218、ID驗證部219之各個驗證處理結束後，判斷部225依據來自驗證部215之驗證結果以及已授權許可證資訊中所包含之許可證「使用條件」，判斷是否可對請求源之行動通訊終端103之非接觸式IC卡模組223進行通訊，而決定通訊處理(S817)。

再者，判斷部225，例如，亦可經由通訊部235請求行動通訊終端103，以使已授權許可證資訊中所包含之個別資訊自行動通訊終端103發送。若產生個人資訊之請求，則行動

通訊終端103所具備之執行部213獲取個人資訊並發送至代行系統伺服器205。

又，並非限定於該例，判斷部225亦可根據需要，自用戶端應用程式ID資料庫中，檢索已授權許可證資訊中所包含之識別行動通訊終端103的「行動設備硬體ID」，並加以確認。再者，用戶端應用程式ID資料庫之資料構造，包含「用戶端應用程式ID」、「行動設備硬體ID」、識別該行動設備之所有者之「所有者ID」、識別非接觸式IC卡模組等之「IC卡ID」等項目。

若判斷部225決定與非接觸式IC卡模組223之通訊處理(S817)，通訊部235藉由經由通訊網106、閘道器117、封包通訊網115以及基地台113，進而經由行動通訊終端103所具備之執行部213，而與非接觸式IC卡模組223進行相互驗證(S819)。再者，進行相互驗證時，通訊部235確認通訊對方之「IC卡ID」是否與已授權許可證資訊中所包含之「IC卡ID」一致。

再者，並非限定於本實施形態之通訊部235經由閘道器117及封包通訊網115等，進而經由行動通訊終端103所具備之執行部213而與非接觸式IC卡模組223進行相互驗證之情形，例如，亦可為通訊部235經由R/W(讀/寫)111而與非接觸式IC卡模組223進行相互驗證(S819)。

通訊部235與非接觸式IC卡模組223之相互驗證結束後(S819)，通訊部235，於行動通訊終端103進行驗證處理時、或者驗證處理後，藉由將記錄有另外所接收之通訊處理內

容之通訊處理資訊發送至非接觸式IC卡模組223，而實施與非接觸式IC卡模組223之通訊處理(S821)。關於通訊處理(S821)，由於與上述通訊處理(S717)實質上相同，故而省略詳細說明。

此處，僅例舉ID驗證部219之ID驗證處理的情形作為圖7或圖8所示之驗證處理的變形例，就本實施形態該之驗證處理加以說明。再者，省略說明與圖7或圖8所示之驗證處理實質上相同之處理。

如圖7或圖8所示，僅為ID驗證部219之ID驗證處理之情形時，行動通訊終端103並不將已授權許可證資訊發送至代行系統伺服器205，而僅發送用戶端應用程式ID即可。因此，無需對服務提供系統101進行存取，但其會導致安全級別降低，則假冒行動通訊終端103之可能性增大。

上述行動通訊終端103將用戶端應用程式ID發送至代行系統伺服器205之後，由於與圖7或圖8所示之一連串驗證處理實質上相同，故而省略詳細說明。

(寫入處理)

其次，參照圖9，就本實施形態之對非接觸式IC卡模組223之寫入處理加以說明。再者，圖9係本實施形態之對非接觸式IC卡模組的寫入處理之概略序列圖。

再者，關於圖9所示之寫入處理，由於已經說明故而省略圖7或圖8所示之驗證處理而加以說明，但並非限定於該例，寫入處理亦預先執行驗證處理。

如圖9所示，對非接觸式IC卡模組223實施資料之寫入處

理之情形時，應用程式部203，首先對服務提供伺服器201進行存取，並發送包含個別資訊之請求資訊(S901)。

若自應用程式部203接收到個別資訊，則如上所述，服務提供伺服器201生成寫入用已授權許可證資訊(S902)，並將該已授權許可證資訊發送至請求源之行動通訊終端103之應用程式部203(S903)。

繼而，應用程式部203通過執行部213向代行系統伺服器205請求進行寫入處理(S905)。再者，省略詳細說明，代行系統伺服器205中進行行動通訊終端103之驗證處理。

若代行系統伺服器205內之判斷部225允許通訊處理，則通訊部235與非接觸式IC卡模組223進行相互驗證(S907)。再者，由於與已經說明之情形大致相同，故而省略詳細說明。

相互驗證(S907)結束後，繼而，代行系統伺服器205內之通訊部235，對應用程式部203請求寫入非接觸式IC卡模組223內記憶機構之資料(S909)。

應用程式部203通過執行部213，將所接收之寫入用已授權許可證資訊以及成為寫入對象之資料，發送至代行系統伺服器205(S911)。

再者，可例示該發送處理(S911)時成為寫入對象之資料，由應用程式部203製成之情形，或自服務提供伺服器201直接發送之情形等。

又，該發送處理(S911)時，成為寫入對象之資料以及寫入用已授權許可證資訊，如圖3所示，藉以用戶端驗證金鑰

221b進行加密。

驗證部215接收到上述寫入對象資料以及寫入用已授權許可證資訊後，藉由系統驗證部216或行動通訊終端驗證部217等，對所加密之寫入對象資料及寫入用已授權許可證資訊進行解密。藉由該解密，驗證部215可針對作為資料發送源之服務提供伺服器201或行動通訊終端103之可靠性進行驗證(S913)。

判斷部225對所接收之已授權許可證資訊中所設定之「使用次數」等使用條件是否適當進行確認(S915)，若確認為適當，則指示執行對通訊部235之寫入處理。再者，除「使用次數」等使用條件之外，如上所述，判斷部225亦可對行動設備之硬體ID等進行確認。

通訊部235，藉由將上述寫入對象之資料以及寫入用指令等發送至非接觸式IC卡模組223，可對該非接觸式IC卡模組223之記憶區域的指定位置寫入資料(S917)。經過以上步驟，本實施形態之寫入處理之一連串操作結束。

再者，圖9所示之寫入處理中，列舉有對寫入對象之資料或寫入用許可證資訊進行加密之情形，但並非限定於該例，例如，寫入處理中，亦可為均不進行加密之情形、代替加密而添加電子簽章之情形、添加電子簽章並對附有該電子簽章之資料進行加密之情形等。即，如上所述，可組合加密或電子簽章等安全環境而執行。

(讀取處理)

繼而，參照圖10，就本實施形態之對非接觸式IC卡模組

223之讀取處理加以說明。再者，圖10係本實施形態之對非接觸式IC卡模組的讀取處理之概略序列圖。

再者，關於圖10所示之讀取處理，由於已經說明故而省略圖7或圖8所示之驗證處理而加以說明，但並非限定於該例，本實施形態之讀取處理亦預先執行驗證處理。

如圖10所示，應用程式部203通過執行部213向代行系統伺服器205請求進行讀取處理(S1005)。再者，省略詳細說明，代行系統伺服器205中進行行動通訊終端103之驗證處理。

若代行系統伺服器205內判斷部225允許通訊處理，則通訊部235與非接觸式IC卡模組223進行相互驗證(S1007)。再者，由於與已經說明之情形大致相同故而省略詳細說明。

相互驗證(S1007)結束後，繼而，代行系統伺服器205內通訊部235，藉由發送讀取用指令等，而對非接觸式IC卡模組223之記憶區域的指定位置所儲存之資料進行讀取(S1009)。非接觸式IC卡模組223讀取資料後將該資料作為答覆發送至通訊部235。再者，可讀取之記憶區域的指定位置(指定位址)例如設為藉由來自應用程式部203之請求時(S1005)等之處理而接收資料。

代行系統伺服器205，若自非接觸式IC卡模組223接收到資料，則由系統驗證部216等，藉以系統驗證金鑰220a對該資料進行加密(S1011)。

繼而，代行系統伺服器205經由通訊網106等，將加密讀取資料發送至行動通訊終端103(S1013)。

應用程式部203，若接收到經過加密之讀取對象之資料，則將包含該加密資料以及個別資訊之讀取用請求資訊，發送至服務提供伺服器201(S1015)。

許可證驗證部241若獲取上述請求資訊，則藉以用於服務提供伺服器201之資料加密處理時之系統驗證金鑰220a所對應的系統驗證金鑰220b進行解密。藉由該解密，許可證驗證部241可針對作為資料發送源之服務提供伺服器201之可靠性進行驗證。(S1017)。

又，許可證驗證部241，依據所接收之請求資訊中所設定之「用戶端應用程式ID」等而自許可證資料庫(未圖示)檢索相應許可證，並確認該許可證中所設定之「使用次數」等使用條件是否適當(S1017)。再者，除「使用次數」等使用條件之外，如上所述，判斷部225亦可對行動設備之硬體ID等進行確認。

許可證驗證部241之驗證處理(S1017)結束後，將非接觸式IC卡模組223之讀取資料發送至行動通訊終端103(S1019)。應用程式部203將上述資料顯示於畫面上。

例如，服務提供系統101存在付與點數之服務作為所提供之服務時，將非接觸式IC卡模組223中所儲存之點數餘額狀態顯示於畫面上，藉此使用者可進行確認。經過以上步驟，本實施形態之讀取處理之一連串操作結束。

再者，圖10所示之讀取處理中，例舉有對讀取對象之資料進行加密之情形，但並非限定於該例，例如，讀取處理中，亦可為均不進行加密之情形、代替加密而添加電子簽

章之情形、添加電子簽章並對附有該電子簽章之讀取資料進行加密之情形等。即，如上所述可組合加密或電子簽章等安全性環境而執行。

再者，圖7~圖10所示之一連串處理，既可使用專用硬體進行，亦可使用軟體進行。藉由軟體而進行一連串處理之情形時，將構成該軟體之程式安裝於通用電腦或微電腦等資訊處理裝置中，使上述資訊處理裝置，作為代行系統伺服器205、服務提供伺服器201、行動通訊終端103而起作用。

程式可預先記錄於作為內置於電腦中之記錄媒體的硬碟或ROM等中。或者，並非限於硬碟驅動器，程式亦可臨時或永久儲存(記錄)於軟碟片、CD-ROM(Compact Disc Read Only Memory，唯讀光碟)，MO(Magneto Optical，磁光)碟片，DVD(Digital Versatile Disc，數位影音光碟)等。

又，亦可經由人造衛星等，將程式無線傳送至電腦，或經由稱作LAN(Local Area Network，局域網)、網際網路之網路，將程式有線傳送至電腦。

此處，本說明書中，描述用以使電腦中進行各種處理之程式的處理步驟，並非必須按照序列圖所揭示之順序而依照時間順序進行處理，亦可包含並列或個別執行之處理(例如並列處理或者依據對象之處理)。

又，程式既可由一個電腦進行處理，亦可由複數個電腦分散處理。

經過以上步驟，結束本實施形態之資料通訊系統100之說明，而使用該資料通訊系統100則存在以下效果。

(1)可提供複數個驗證功能，並可對應各服務提供系統101之安全級別對其等進行自由組合。進而服務提供者考慮到安全性以及系統構建成本等，可容易地進行設定/變更。例如，可以下述方式組合驗證處理：於提高服務提供系統101之安全級別之情形時，運用一次性許可證，降低安全級別之情形時，僅運用用戶端應用程式ID驗證。

(2)使用許可證驗證功能之情形時，例如，服務提供者可藉由對應安全策略確定許可證期限，而靈活運用無期限許可證、或一次性許可證等。

(3)由於設置許可證發行單位為行動通訊終端103以限制可使用服務之設備，故而可使第三者之非法使用變得困難。

(4)由於可統一管理應用程式部203與伺服器等之通訊狀態，故而例如可於通訊網不能連接時易於進行重試。

(5)可減少應用程式部203之通訊量。

(6)藉由提供可於代行系統105側定製之驗證功能，可減少代行系統與服務提供系統之間的系統構建工時。

(7)由於使用有非接觸式IC卡模組223與代行系統105之間的相互驗證，故而可省略服務提供系統101驗證代行系統105之步驟。

(8)即使並不製作識別行動通訊終端103之識別資訊，亦可藉由使用有系統驗證金鑰等之驗證步驟，而執行資料通訊系統，因此可實現具有通用性之資料通訊系統，並且可不依賴行動通訊終端103之提供者、機種等，而對非接觸式IC卡模組執行通訊處理，以提供服務。

以上，參照附圖，就本發明之較佳實施形態加以說明，但本發明並非限定於該例。業者應瞭解，專利申請範圍中所揭示之技術思想範疇內的各種變更例或者修正例，亦屬於本發明之技術範圍。

上述實施形態中，例舉說明有資料通訊系統100具備服務提供系統101、代行系統105各1個之情形，但本發明並非限定於該情形。例如，亦可實施為資料通訊系統100中，按各服務提供者單位具備複數個服務提供系統101。又，亦可實施為資料通訊系統100中具備複數個代行系統105。

上述實施形態中，例舉說明有服務提供系統101所具備之各部由硬體組成之情形，本發明並非限定於該例。例如，亦可為上述各部係包含1或2個以上模組或者組件之程式。

上述實施形態中，例舉說明有代行系統105所具備之各部由硬體責成之情形，但本發明並非限定於該例。例如，亦可為上述各部係包含1或2個以上模組或者組件之程式。

上述實施形態中，例舉說明有行動通訊終端103所具備之應用程式部203以及執行部213為包含1或2個以上模組或者組件之程式之情形，但並非限定於該例，例如，亦可為包含1或2個以上元件之電路等硬體之情形。

又，上述實施形態中，例舉說明有行動通訊終端103係具備非接觸式IC卡模組223之行動電話之情形，但若為可經由通訊網與外部進行通訊，且具備非接觸式IC卡模組223，則本發明並非限定於該例。例如，亦可為行動通訊終端103為筆記型PC、PDA(Personal Digital Assistant，個人數位助

理)等。

又，上述實施形態中，例舉說明有通訊部235經由通訊網106、閘道器117、封包通訊網115以及基地台113，進而經由行動通訊終端103所具備之執行部213，而進行與非接觸式IC卡模組223相互驗證等一連串通訊之情形，但本發明並非限定於該例。例如，亦可為通訊部235經由通訊網104及資訊處理裝置109所具備之R/W111，進而經由行動通訊終端103所具備之執行部213，而與非接觸式IC卡模組223進行通訊。

如上所述，根據本發明，資料通訊系統中驗證通訊對方時，可組合1或2種以上驗證處理中對應安全級別所選擇的驗證處理並執行，故而可靈活應對提供服務側之請求。

[產業上之可利用性]

本發明可適用於資料通訊系統、代行系統伺服器、電腦程式及資料通訊方法。

【圖式簡單說明】

圖1係本實施形態之資料通訊系統之一例概略說明圖。

圖2係本實施形態之資料通訊系統所具備之服務提供系統的概略說明圖。

圖3係本實施形態之許可證獲取部之已授權許可證資訊生成處理的概略說明圖。

圖4係本實施形態之行動通訊終端之一例概略結構方塊圖。

圖5係本實施形態之回應生成部之加密處理的一例概略

說明圖。

圖6係用以選擇本實施形態之驗證處理的選擇畫面之概略說明圖。

圖7係表示本實施形態之系統驗證部、行動通訊終端驗證部以及ID驗證部進行驗證之情形時的驗證處理，以及對非接觸式IC卡模組的通訊處理之概略序列圖。

圖8係表示本實施形態之詰問/回應驗證部以及ID驗證部進行驗證之情形時的驗證處理，以及對非接觸式IC卡模組的通訊處理之概略序列圖。

圖9係本實施形態之對非接觸式IC卡模組的寫入處理之概略序列圖。

圖10係本實施形態之對非接觸式IC卡模組的讀取處理之概略序列圖。

【主要元件符號說明】

100	資料通訊系統
101	服務提供系統
103(103a，103b，...103n)	行動通訊終端
104，106，108	通訊網
105	代行系統
109(109a，109b，...109n)	資訊處理裝置
111(111a，111b，...111n)	讀/寫裝置
113	基地台
115	封包通訊網
117	閘道器

201	服務提供伺服器
203	應用程式部
204	請求部
205	代行系統伺服器
206	加密部
207	回應生成部
208	ID獲取部
211	許可證獲取部
213	執行部
214	接收部
215	驗證部
216	系統驗證部
217	行動通訊終端驗證部
218	詰問/回應驗證部
219	ID驗證部
220a，220b	系統驗證金鑰
221a，221b	用戶端驗證金鑰
223	非接觸式IC卡模組
225	判斷部
231，235	通訊部
241	許可證驗證部
245	驗證處理管理部
601a~601g	勾選框

五、中文發明摘要：

本發明之目的在於提供一種資料通訊系統，其組合1或2種驗證機構而對行動通訊終端等進行驗證，並對非接觸式IC卡模組執行通訊處理，其中代行系統(105)具備驗證部(215)，其依據來自行動通訊終端之已授權許可證資訊而執行以下至少一個驗證處理，即藉由使用系統驗證金鑰而對服務提供系統(101)進行驗證的處理、藉由使用用戶端驗證金鑰而對行動通訊終端(103)進行驗證的處理、或者藉由使用識別行動通訊終端之識別資訊而對行動通訊終端進行驗證的處理；判斷部(225)，其根據已授權許可證資訊而判斷通訊允許/通訊不允許；通訊部(235)，當上述判斷部判斷為通訊允許時，其與非接觸式IC卡模組進行通訊處理。

六、英文發明摘要：

十、申請專利範圍：

1. 一種資料通訊系統，其具備：一個以上行動通訊終端，其等各自具有對應外部請求而進行資訊處理之非接觸式IC卡模組；服務提供系統，其藉由上述非接觸式IC卡模組之資訊處理而提供服務；及代行系統，其代替該服務提供系統而與上述非接觸式IC卡模組進行通訊處理，且

上述行動通訊終端具備請求部，其為使上述非接觸式IC卡模組與上述代行系統進行通訊處理，而請求上述服務提供系統所持有之資訊，即表示已授予上述行動通訊終端且關於該通訊處理之許可證的已授權許可證資訊，

上述服務提供系統具備獲取部，當受到上述行動通訊終端之一個請求時，其獲取該請求源之行動通訊終端之已授權許可證資訊，

上述所獲取之已授權許可證資訊，藉以系統驗證金鑰由上述服務提供系統加密，進而藉以用戶端驗證金鑰由上述行動通訊終端加密後發送至上述代行系統，上述系統驗證金鑰保存於上述代行系統以及上述服務提供系統雙方且可於該雙方之間對資訊進行加密/解密，上述用戶端驗證金鑰保存於上述行動通訊終端以及上述代行系統雙方且可於該雙方之間對資訊進行加密/解密，

上述代行系統具備：驗證部，其依據來自上述行動通訊終端之已授權許可證資訊而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用上述系統驗證金鑰而對上述服務提供系統進行驗證之系統驗

證處理、藉由使用上述用戶端驗證金鑰而對上述行動通訊終端進行驗證之第1用戶端驗證處理、以及藉由使用識別上述行動通訊終端之識別資訊而對上述行動通訊終端進行驗證之第2用戶端驗證處理；

判斷部，其於上述驗證部之驗證處理後，根據上述已授權許可證資訊所設定之許可證而判斷通訊允許/通訊不允許；

通訊部，當上述判斷部判斷為允許通訊時，其與上述非接觸式IC卡模組進行通訊處理。

2. 如請求項1之資料通訊系統，其中上述驗證部，接收選擇上述1或2種以上驗證處理中一個或者兩個以上進行組合後之驗證處理的選擇指示，並按照所接收之上述選擇指示執行驗證處理。

3. 如請求項1之資料通訊系統，其中上述通訊部所進行之通訊處理，係對上述非接觸式IC卡模組執行寫入處理或者讀取處理之處理。

4. 如請求項3之資料通訊系統，其中針對成為上述讀取處理對象之資料，接收對該資料進行加密的處理，或者將依據資料而製成之電子簽章添加至該資料的處理中其中之一或兩者之處理的選擇指示，上述驗證部係按照所接收之上述選擇指示進行處理。

5. 如請求項3之資料通訊系統，其中針對成為上述寫入處理對象之資料，接收對加密資料進行解密的處理，以及依據預先添加有電子簽章之資料而驗證該資料之可靠性的

處理中其中之一或者兩者之處理的指示，上述驗證部係按照該選擇指示進行處理。

6. 如請求項1之資料通訊系統，其中上述服務提供系統與上述代行系統之通訊係經由上述行動通訊終端而進行。

7. 如請求項1之資料通訊系統，其中上述第1用戶端驗證處理，係向上述行動通訊終端發送詰問碼，並接收依據該詰問碼以及上述已授權許可證資訊而製成之回應，藉此進行驗證之詰問/回應方式的驗證處理。

8. 如請求項1之資料通訊系統，其中上述行動通訊終端為行動電話。

9. 一種代行系統伺服器，其代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務之服務提供伺服器，與該非接觸式IC卡模組進行通訊處理，且其具備：

接收部，其自該行動通訊終端接收經過加密之已授權許可證資訊，該已加密授權許可證資訊表示關於上述非接觸式IC卡模組與代行系統伺服器之通訊處理之許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由上述行動通訊終端加密，而該系統驗證金鑰保存於上述代行系統伺服器以及上述服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且可於該雙方之間對資訊進行加密/解密；

驗證部，其依據來自上述行動通訊終端之已授權許可證資訊而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用上述系統驗證金鑰而對上述服務提供系統進行驗證之系統驗證處理、藉由使用上述用戶端驗證金鑰而對上述行動通訊終端進行驗證之第1用戶端驗證處理、以及藉由使用識別上述行動通訊終端之識別資訊而對上述行動通訊終端進行驗證之第2用戶端驗證處理；

判斷部，其於上述驗證部之驗證處理後，根據上述已授權許可證資訊中所設定之許可證而判斷通訊允許/通訊不允許；

通訊部，當上述判斷部判斷為通訊允許時，其與上述非接觸式IC卡模組進行通訊處理。

10. 如請求項9之代行系統伺服器，其中上述驗證部，接收選擇上述1或2種以上驗證處理中一或兩個以上進行組合後之驗證處理的選擇指示，並按照所接收之上述選擇指示執行驗證處理。

11. 如請求項9之代行系統伺服器，其中上述通訊部所進行之通訊處理，係對上述非接觸式IC卡模組執行寫入處理或讀取處理之處理。

12. 如請求項11之代行系統伺服器，其中針對成為上述讀取處理對象之資料，接收對該資料進行加密的處理、或將依據資料而製成之電子簽章添加至該資料的處理中其中之一或兩者之處理的選擇指示，上述驗證部係按照所接

收之上述選擇指示進行處理。

13. 如請求項11之代行系統伺服器，其中針對成為上述寫入處理對象之資料，接收對加密資料進行解密的處理，或依據預先添加有電子簽章之資料而驗證該資料之可靠性的處理中至少其中之一的處理之選擇指示，上述驗證部係按照該選擇指示進行處理。

14. 一種電腦程式，其使電腦作為代行系統伺服器而起作用，該代行系統伺服器代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務的服務提供伺服器，與該非接觸式IC卡模組進行通訊處理，且其具備：

接收步驟，其自該行動通訊終端接收經過加密之已授權許可證資訊，該已加密授權許可證資訊表示關於上述非接觸式IC卡模組與代行系統伺服器之通訊處理的許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由上述行動通訊終端加密，該系統驗證金鑰保存於上述代行系統伺服器以及上述服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且可於該雙方之間對資訊進行加密/解密；

驗證步驟，其依據來自上述行動通訊終端之已授權許可證資訊，而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用上述系統驗證金鑰而

對上述服務提供系統進行驗證的系統驗證處理、藉由使用上述用戶端驗證金鑰而對上述行動通訊終端進行驗證之第1用戶端驗證處理、以及藉由使用識別上述行動通訊終端之識別資訊而對上述行動通訊終端進行驗證之第2用戶端驗證處理；

判斷步驟，於上述驗證處理之後，根據上述已授權許可證資訊而判斷通訊允許/通訊不允許；

通訊步驟，上述判斷結果為允許通訊處理時，進行與上述非接觸式IC卡模組之通訊處理。

15. 一種資料通訊方法，其係代行系統伺服器之資料通訊方法，該代行系統伺服器代替藉由行動通訊終端所具備之非接觸式IC卡模組進行資訊處理而提供服務的服務提供伺服器，與該非接觸式IC卡模組進行通訊處理，且其包括：

接收步驟，其自該行動通訊終端接收經過加密之已授權許可證資訊，該授權許可證資訊表示關於上述非接觸式IC卡模組與代行系統伺服器之通訊處理的許可證，並藉以系統驗證金鑰由上述服務提供伺服器加密，進而藉以用戶端驗證金鑰由上述行動通訊終端加密，而該系統驗證金鑰保存於上述代行系統伺服器以及上述服務提供伺服器雙方且可於該雙方之間對資訊進行加密/解密，該用戶端驗證金鑰保存於該行動通訊終端以及上述代行系統伺服器雙方且可於該雙方之間對資訊進行加密/解密；

驗證步驟，其依據來自上述行動通訊終端之已授權許

可證資訊，而執行包含以下驗證處理之複數個驗證處理中至少一個驗證處理，即藉由使用上述系統驗證金鑰而對上述服務提供系統進行驗證的系統驗證處理、藉由使用上述用戶端驗證金鑰而對上述行動通訊終端進行驗證之第1用戶端驗證處理、以及藉由使用識別上述行動通訊終端之識別資訊而對上述行動通訊終端進行驗證之第2用戶端驗證處理；

判斷步驟，執行上述驗證步驟之後，根據上述已授權許可證資訊而判斷通訊允許/通訊不允許；

通訊步驟，上述判斷步驟之判斷結果為允許通訊處理時，進行與上述非接觸式IC卡模組之通訊處理。

十一、圖式：

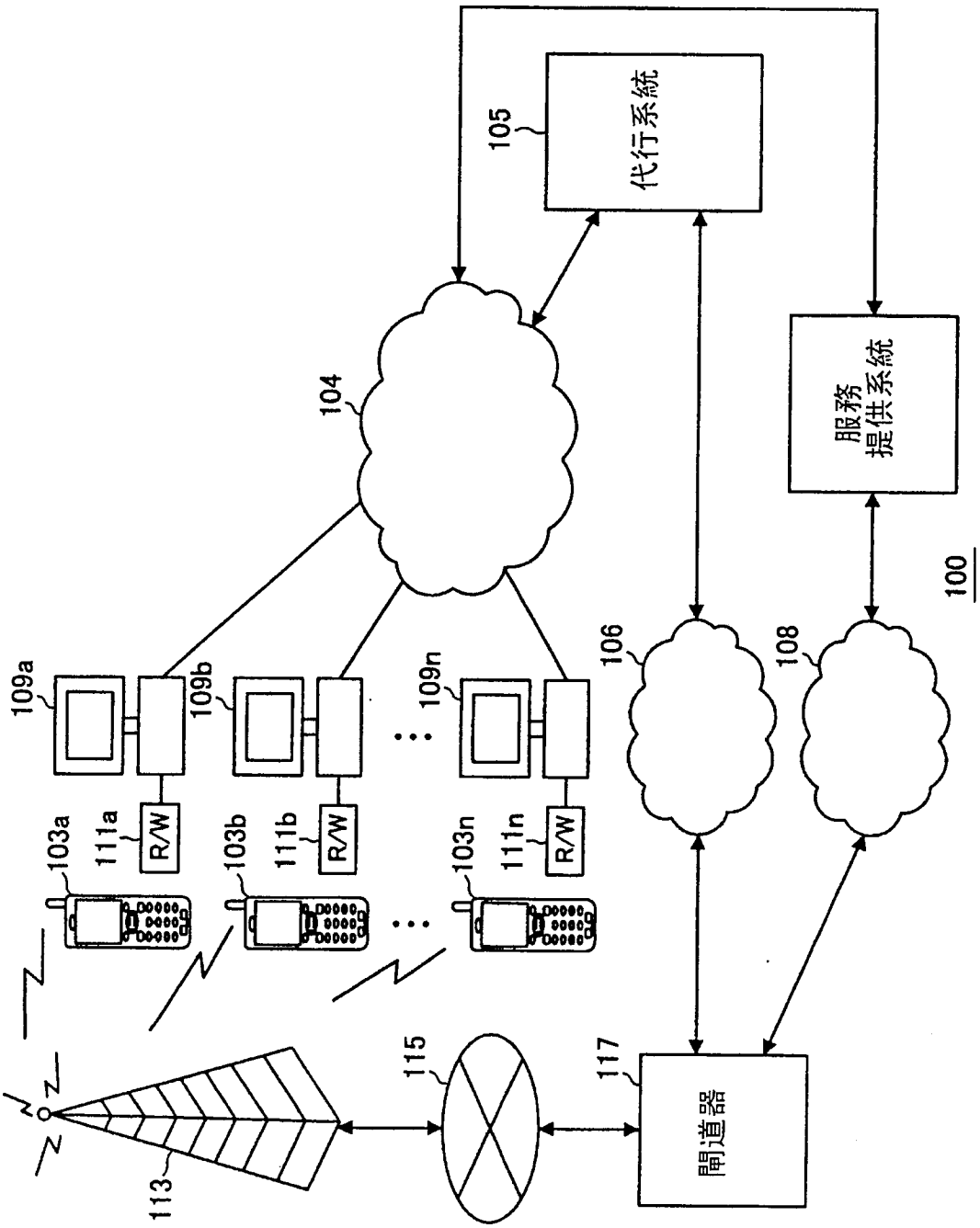

代行系統
105
服務
提供系統
104
100
106
108
109a
109b
109n
103a
111a
R/W
103b
111b
R/W
103n
111n
R/W
115
117
閘道器
113

圖 1

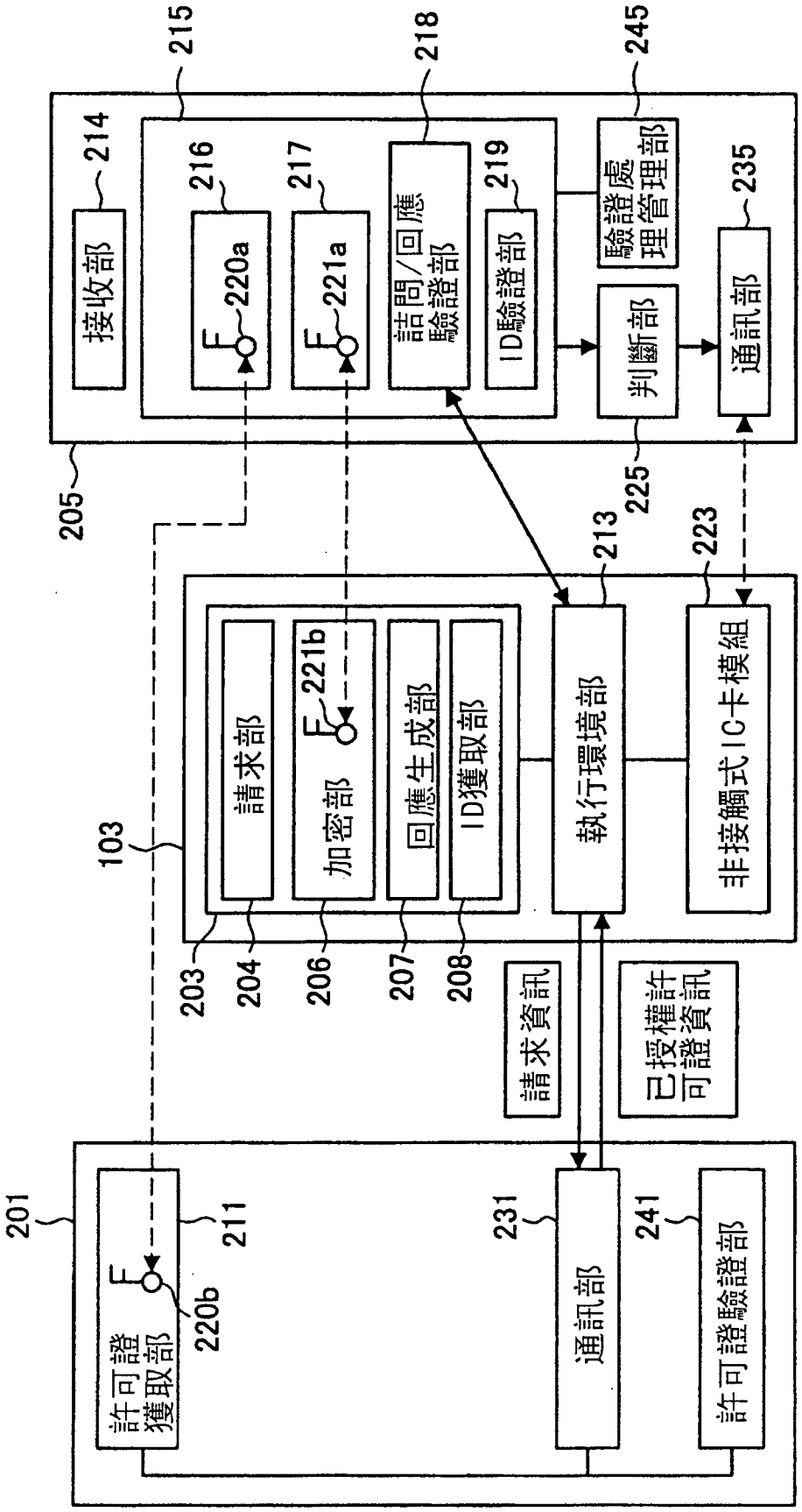

201
211
220b
許可證
獲取部
231
通訊部
241
許可證驗證部
205
215
214
接收部
216
220a
217
221a
218
詰問/回應
驗證部
219
ID驗證部
245
驗證處
理管理部
判斷部
235
通訊部
225
213
223
103
請求部
221b
加密部
回應生成部
ID獲取部
執行環境部
非接觸式IC卡模組
203
204
206
207
208
請求資訊
已授權許
可證資訊

圖2

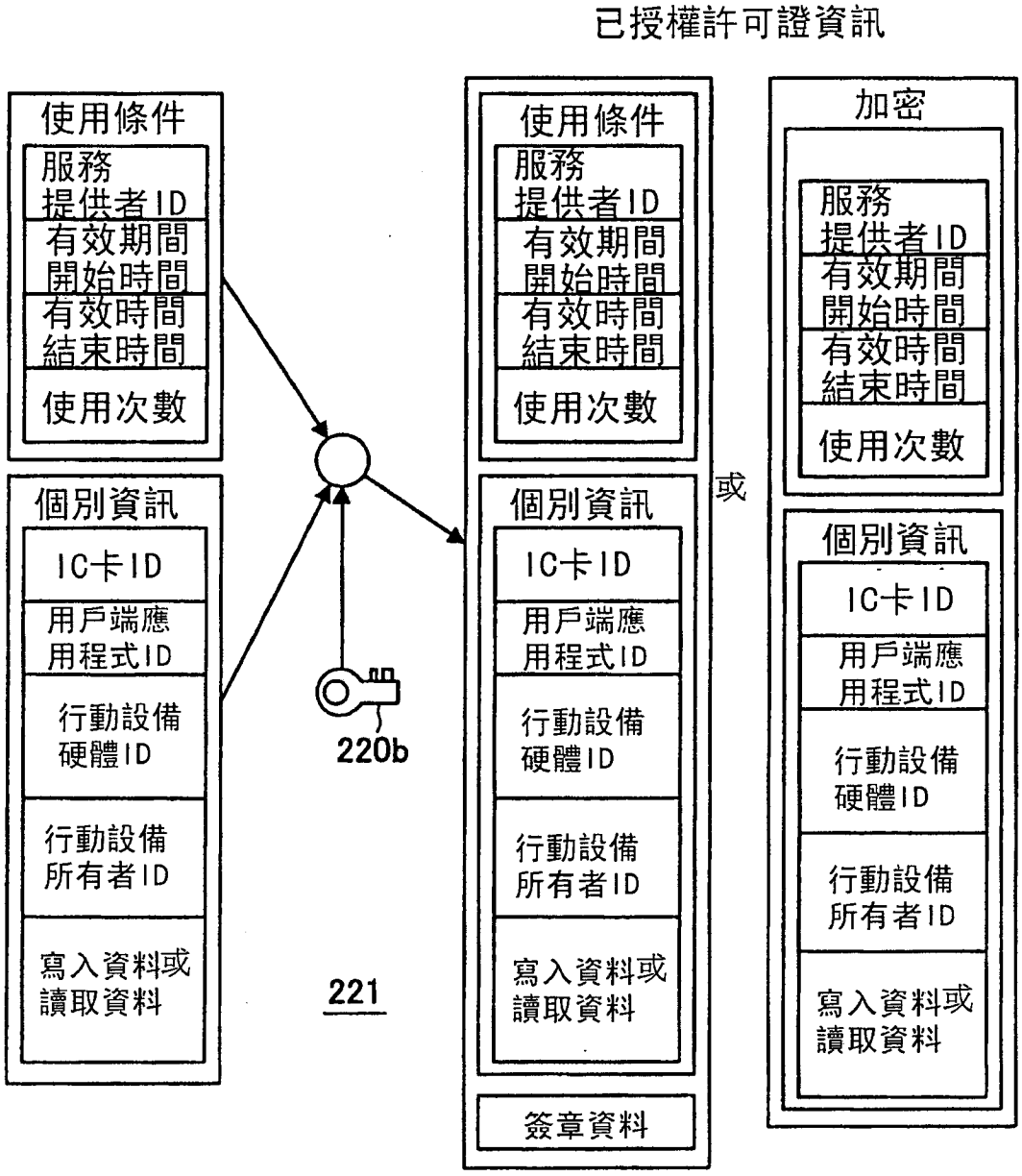

已授權許可證資訊
使用條件
服務提供者ID
有效期間開始時間
有效時間結束時間
使用次數
個別資訊
IC卡ID
用戶端應用程式ID
行動設備硬體ID
行動設備所有者ID
寫入資料或讀取資料
220b
221
使用條件
服務提供者ID
有效期間開始時間
有效時間結束時間
使用次數
個別資訊
IC卡ID
用戶端應用程式ID
行動設備硬體ID
行動設備所有者ID
寫入資料或讀取資料
簽章資料
或
加密
服務提供者ID
有效期間開始時間
有效時間結束時間
使用次數
個別資訊
IC卡ID
用戶端應用程式ID
行動設備硬體ID
行動設備所有者ID
寫入資料或讀取資料

圖3

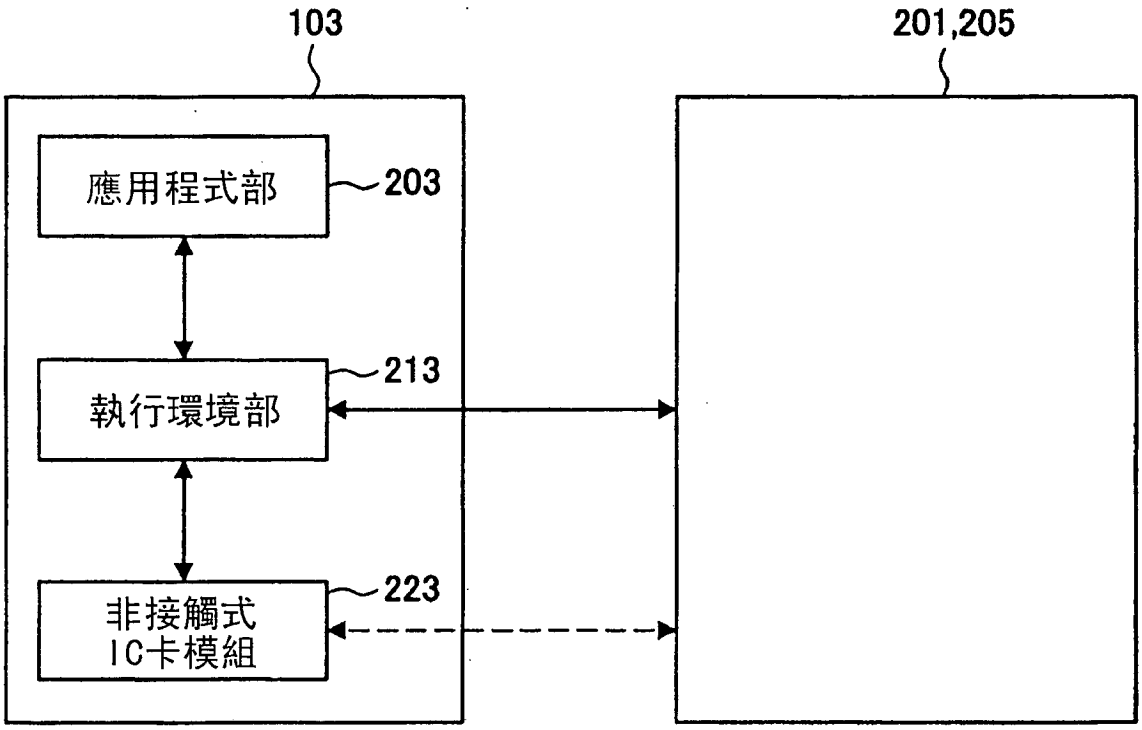
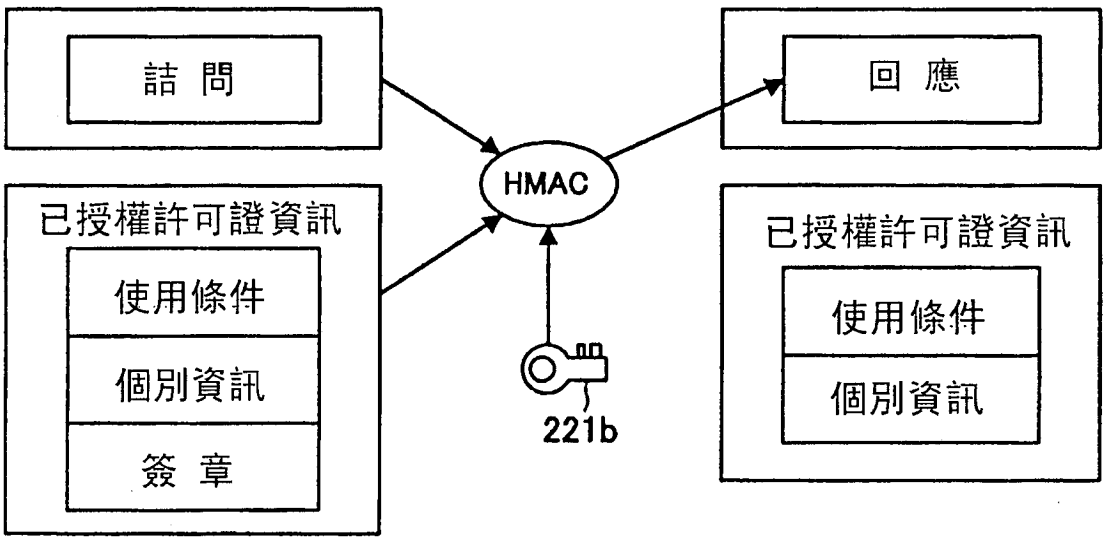

103
201,205
應用程式部
203
執行環境部
213
非接觸式
IC卡模組
223

圖4


詰 問
回 應
HMAC
已授權許可證資訊
使用條件
個別資訊
簽 章
221b
已授權許可證資訊
使用條件
個別資訊

207

圖5

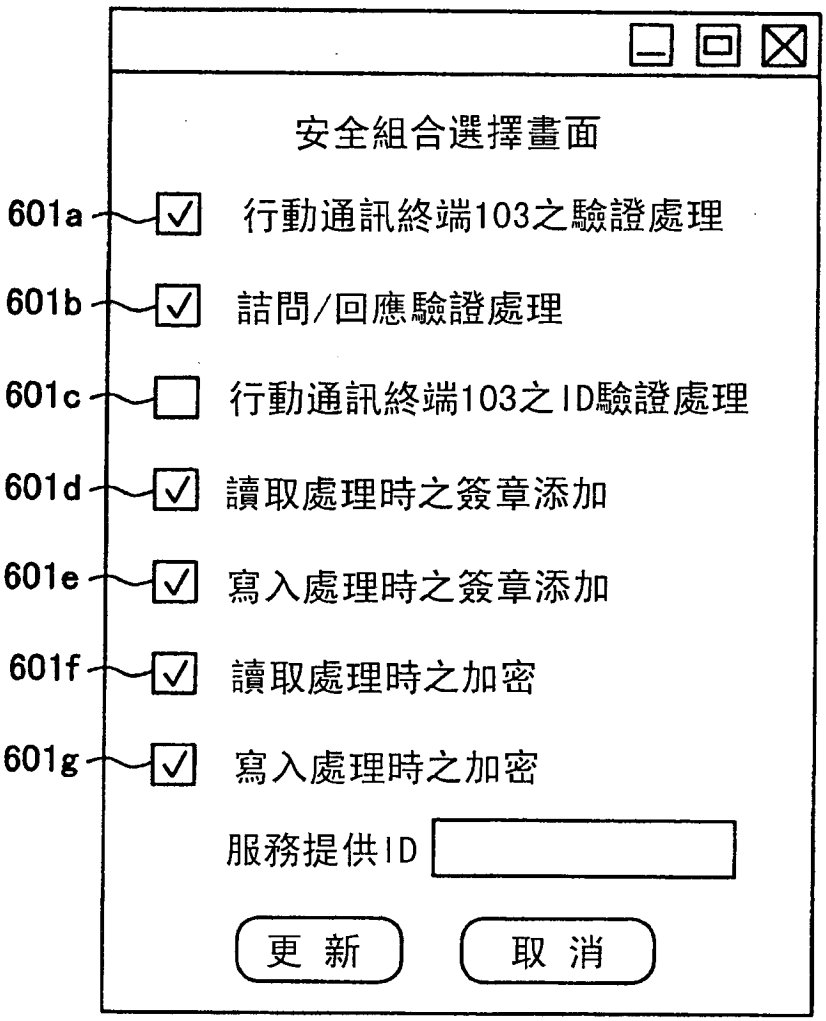

安全組合選擇畫面
601a
行動通訊終端103之驗證處理
601b
詰問/回應驗證處理
601c
行動通訊終端103之ID驗證處理
601d
讀取處理時之簽章添加
601e
寫入處理時之簽章添加
601f
讀取處理時之加密
601g
寫入處理時之加密
服務提供ID
更 新
取 消

圖6

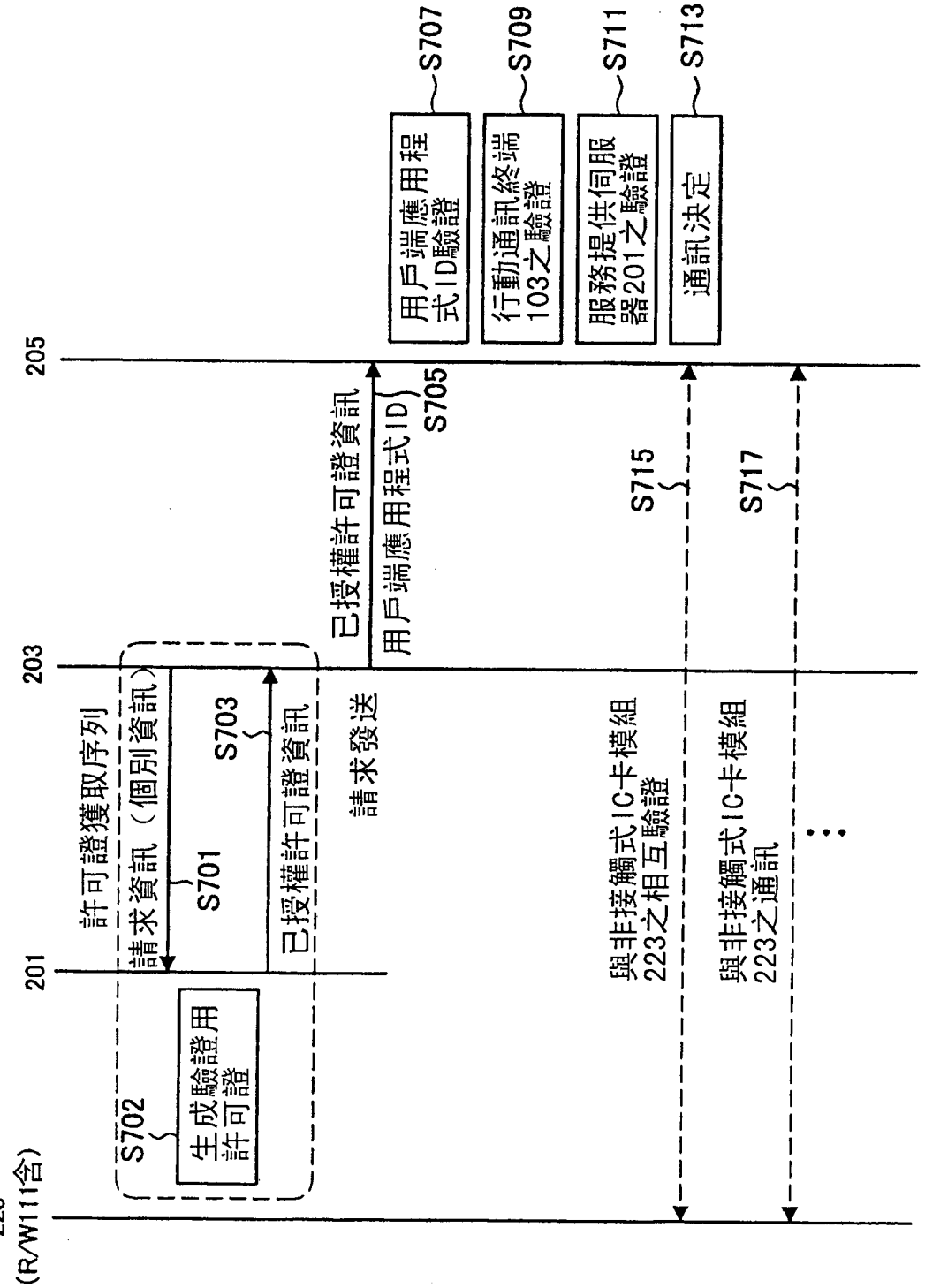

223
(R/W11合)
201
203
205
許可證獲取序列
請求資訊（個別資訊）
S701
S702
生成驗證用許可證
S703
已授權許可證資訊
請求發送
已授權許可證資訊
用戶端應用程式ID
S705
與非接觸式IC卡模組223之相互驗證
S715
與非接觸式IC卡模組223之通訊
S717
用戶端應用程式ID驗證
S707
行動通訊終端103之驗證
S709
服務提供伺服器201之驗證
S711
通訊決定
S713

圖7

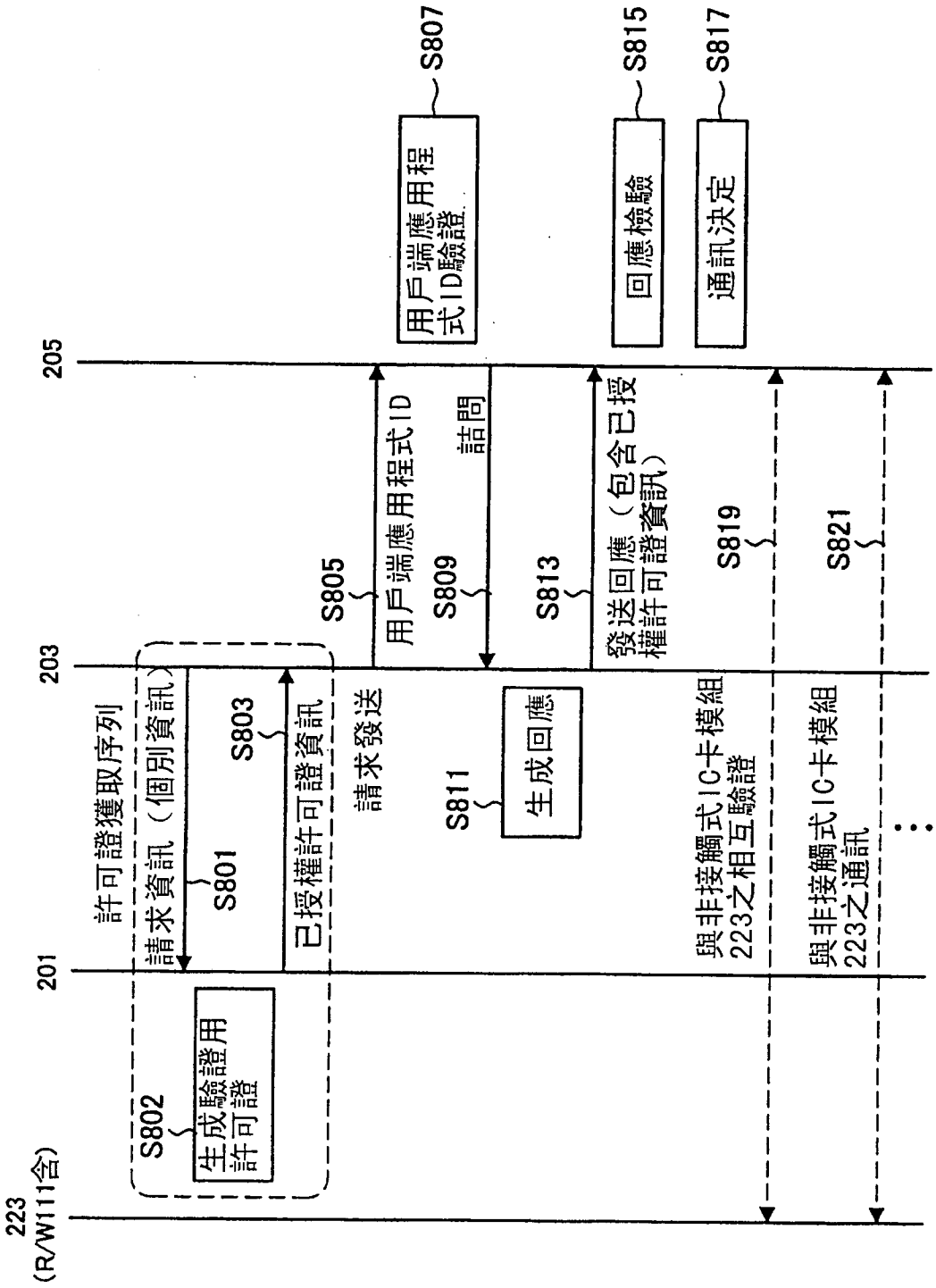

223
(R/W111含)
201
許可證獲取序列
203
205
S802
生成驗證用許可證
請求資訊（個別資訊）
S801
S803
已授權許可證資訊
請求發送
S805
用戶端應用程式ID
S807
用戶端應用程式ID驗證
S809
詰問
S811
生成回應
S813
發送回應（包含已授權許可證資訊）
S815
回應檢驗
S819
與非接觸式IC卡模組223之相互驗證
S817
通訊決定
S821
與非接觸式IC卡模組223之通訊

圖8

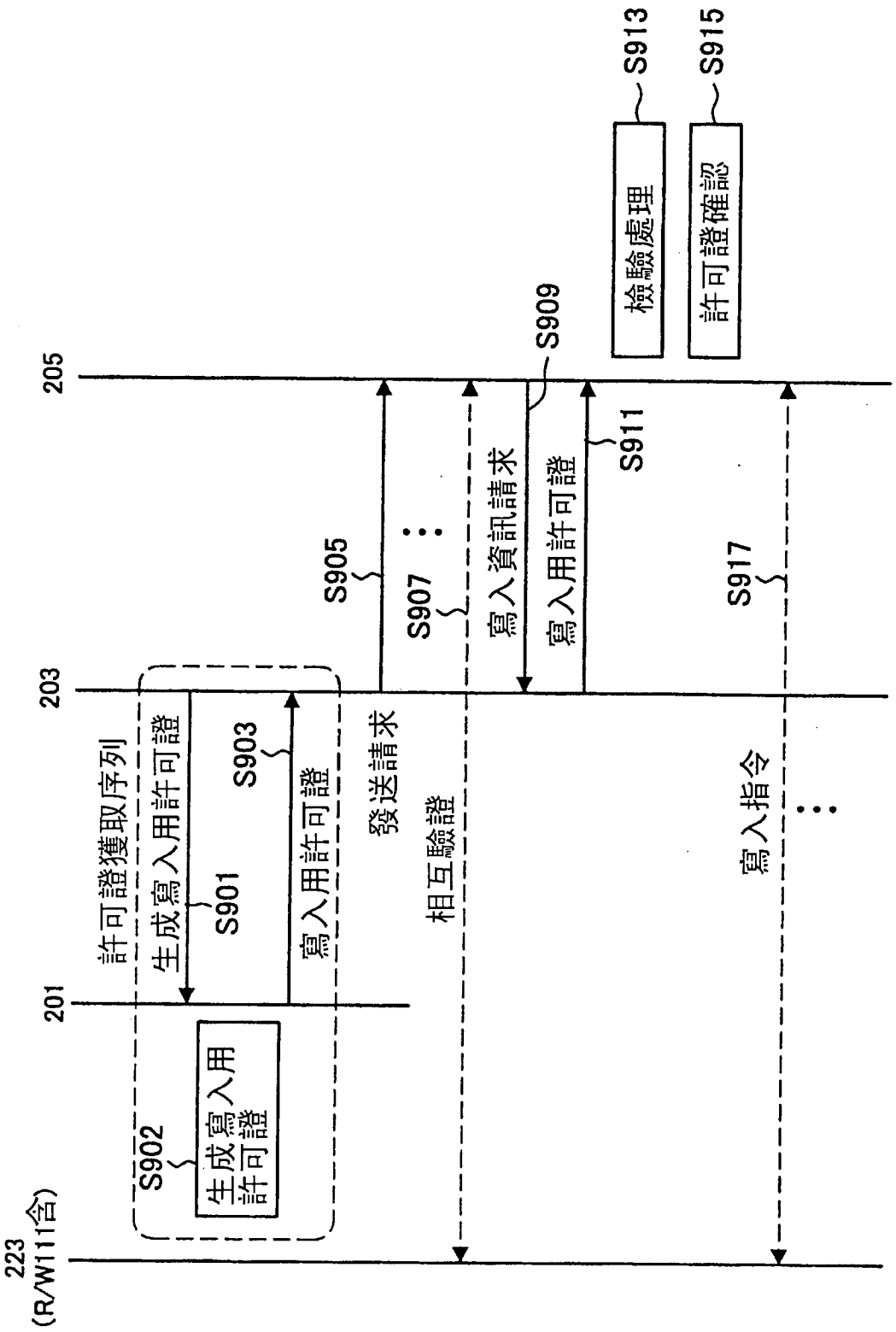

223
(R/W111含)
201
203
205
許可證獲取序列
生成寫入用許可證
S901
S902
生成寫入用
許可證
S903
寫入用許可證
發送請求
S905
相互驗證
S907
寫入資訊請求
S909
寫入用許可證
S911
檢驗處理
S913
許可證確認
S915
S917
寫入指令

圖9

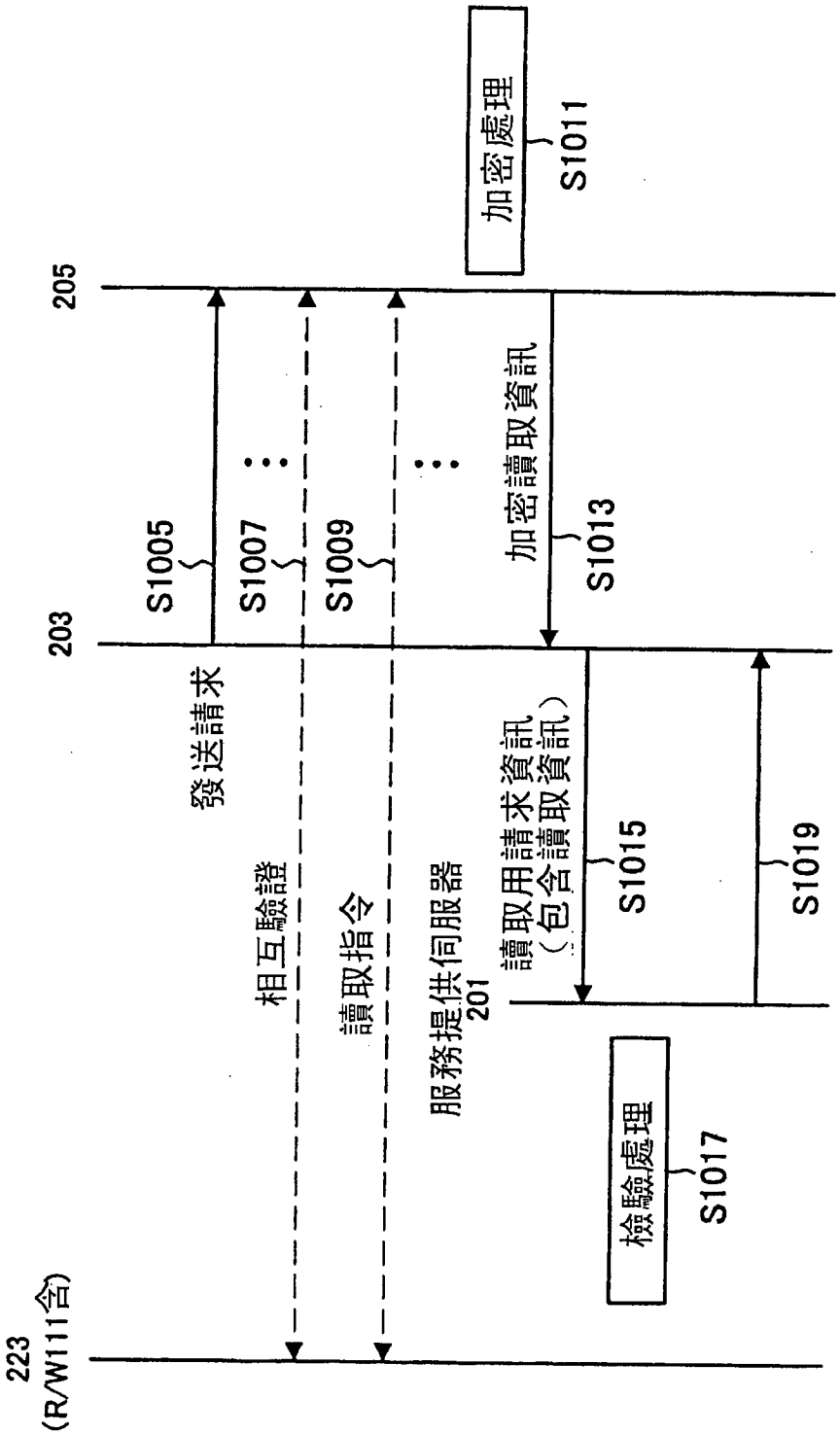

223
(R/W111含)
服務提供伺服器
201
203
205
發送請求
相互驗證
讀取指令
讀取用請求資訊
（包含讀取資訊）
檢驗處理
加密處理
加密讀取資訊
S1005
S1007
S1009
S1011
S1013
S1015
S1017
S1019

圖10

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100	資料通訊系統
103(103a，103b，...103n)	行動通訊終端
104，106，108	通訊網
105	代行系統
109(109a，109b，...109n)	資訊處理裝置
111(111a，111b，...111n)	讀/寫裝置
113	基地台
115	封包通訊網
117	閘道器

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)