I304190
（此處由本局於收文時黏貼條碼）

公告本 463093

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：95134475

※申請日期：95年09月18日　　※IPC分類：G07F 7/00
G06Q 20/00

一、發明名稱：

(中) 網路結帳輔助裝置
(英)

二、申請人：(共 1 人)

1.姓　名：（中）ＪＣＢ股份有限公司
（英）JCB CO., LTD.
代表人：（中）1.信原啓也
（英）1.NOBUHARA, HIROYA
地　址：（中）日本國東京都港區南青山五丁目一番二二號
（英）1-22, Minamiaoyama 5-chome, Minato-ku, Tokyo, Japan
國籍：（中英）日本　　JAPAN

三、發明人：(共 2 人)

1.姓　名：（中）田中俊
（英）TANAKA, SHUN
國　籍：（中）日本
（英）JAPAN

2.姓　名：（中）川勝實之
（英）KAWAKATSU, MITSUYUKI
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　　；2006/07/07；2006-188341 ☑有主張優先權

I304190
（此處由本局於收文時黏貼條碼）

公告本 463093

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：95134475

※申請日期：95年09月18日　　※IPC分類：G07F 7/00
G06Q 20/00

一、發明名稱：

(中) 網路結帳輔助裝置
(英)

二、申請人：(共 1 人)

1.姓　名：（中）ＪＣＢ股份有限公司
（英）JCB CO., LTD.
代表人：（中）1.信原啓也
（英）1.NOBUHARA, HIROYA
地　址：（中）日本國東京都港區南青山五丁目一番二二號
（英）1-22, Minamiaoyama 5-chome, Minato-ku, Tokyo, Japan
國籍：（中英）日本　　JAPAN

三、發明人：(共 2 人)

1.姓　名：（中）田中俊
（英）TANAKA, SHUN
國　籍：（中）日本
（英）JAPAN

2.姓　名：（中）川勝實之
（英）KAWAKATSU, MITSUYUKI
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　　；2006/07/07；2006-188341 ☑有主張優先權

(1)

九、發明說明

【發明所屬之技術領域】

本發明係有關於網路結帳輔助裝置。

【先前技術】

先前，在行動電話機中儲存了信用卡或銀行卡等之卡片識別資訊(卡號)及私密號碼，當被輸入至行動電話機的私密號碼，和所儲存之私密號碼爲一致時，藉由在行動電話機之顯示器上顯示卡號，就可使行動電話機也具備卡片之機能(例如，參照專利文獻 1)。

可是，此種附帶卡片機能的行動電話機上，存在著以下說明之課題。

〔專利文獻 1〕

日本特開 2002-64597 號公報

【發明內容】

〔發明所欲解決之課題〕

對專利文獻 1 所記載之附帶卡片機能的行動電話機的資料儲存、抹消等，是藉由通訊而進行。換言之，該行動電話機，係以被網路連接爲前提。

如此，若向可連接網路之行動電話機，儲存卡號或私密號碼，則因不正當存取等，這些卡號或私密號碼被惡意第三者竊聽、篡改的危險性並非少到完全沒有，會造成安全上的問題。

(2)

於是，若將行動電話機構成爲不可連接網路的話，則搞不好可以使上述竊聽或篡改的疑慮消失。

可是，行動電話機，係除了基本的通話機能以外，也具有網路通訊機能這是目前一般常見的，要使行動電話機變成不可連接網路之構成，這在現實上是有困難的。又，爲了要維持現狀的行動電話機之構成不變，且使已被儲存之卡號或私密號碼無法從外部讀出，是必須要具備加密程式等，會使構成變得複雜。

又，在專利文獻 1 之行動電話機的情形，即使不藉由透過網路的不正當存取，也只要顯示在行動電話機之顯示器上的卡號，一度被第三者偷看到，則第三者便可能使用該卡號，在網際網路上進行信用結帳所致之網路商業交易，就這點來說，安全性亦較低。

此外，本案專利申請人，係有鑑於上記這種僅用卡號就可進行網路商業交易之情事，而正在開始用運一種除了卡號之提示外，仍須經過提示持卡會員所預先訂定的固定密碼來進行持卡會員的本人認證，才能進行網路商業交易的此種網路結帳系統。

可是，若該固定密碼也一旦被第三者得知，則第三者還是可假冒持卡會員來進行網路商業交易，這也不能說是必然的安全。

本發明係有鑑於以上之先前問題點而研發，其目的在於，使得不正當存取等造成卡號或私密號碼被竊聽、篡改的危險性消失，且能夠更安全地進行網路商業交易的網路

(3)

結帳輔助裝置。

〔用以解決課題之手段〕

申請項1之發明，係

一種網路結帳輔助裝置，係屬於可搬型之網路結帳輔助裝置，其特徵爲，具備：顯示器；和卡片資訊儲存部，是以無法從外部讀出之狀態預先儲存著，至少包含信用卡或轉帳卡等之卡片契約者之識別資訊的卡片資訊；和認證資訊儲存部，是以無法從外部讀出之狀態預先儲存著，用來進行前記契約者之本人認證的認證資訊；和OTP生成資訊儲存部，是以無法從外部讀出之狀態預先儲存著，被前記卡片資訊所關連對應且爲前記網路結帳輔助裝置所固有之OTP生成資訊；和輸入手段，將前記認證資訊加以輸入；和認證手段，基於從前記輸入手段所輸入之輸入資訊，由前記網路結帳輔助裝置之操作者，進行是否爲前記契約者的本人認證，若已經確認爲本人時，則至少讀出前記卡片資訊當中的前記識別資訊，並顯示於前記顯示器上；和一次性密碼生成手段，在前記卡片資訊被顯示後，基於前記OTP生成資訊，生成一次性密碼，並顯示於前記顯示器上；當藉由前記一次性密碼，進行了前記契約者之本人認證，且已確認爲本人時，使得使用前記識別資訊之結帳所致之網路商業交易成爲可行。

申請項2之發明，係

一種網路結帳輔助裝置，係屬於，信用卡或轉帳卡等

(4)

之卡片契約者的行動電話或個人電腦等的契約者終端，和進行前記契約者本人認證的認證伺服器，是彼此連接網路而成之網路結帳系統中，在進行使用了前記契約者之識別資訊的結帳所致之網路商業交易之際，所被使用的可搬型之網路結帳輔助裝置，其特徵爲，前記網路結帳輔助裝置係具備：顯示器；和卡片資訊儲存部，是以無法從外部讀出之狀態預先儲存著，至少包含前記契約者之識別資訊的卡片資訊；和認證資訊儲存部，是以無法從外部讀出之狀態預先儲存著，用來進行前記契約者之本人認證的認證資訊；和OTP生成資訊儲存部，是以無法從外部讀出之狀態預先儲存著，被前記卡片資訊所關連對應且爲前記網路結帳輔助裝置所固有之OTP生成資訊；和輸入手段，將前記認證資訊加以輸入；和認證手段，基於從前記輸入手段所輸入之輸入資訊，由前記網路結帳輔助裝置之操作者，進行是否爲前記契約者的本人認證，若已經確認爲本人時，則至少讀出前記卡片資訊當中的前記識別資訊，並顯示於前記顯示器上；和一次性密碼生成手段，在前記卡片資訊被顯示後，基於前記OTP生成資訊，生成一次性密碼，並顯示於前記顯示器上；前記契約者終端，是藉由將前記一次性密碼發送至前記認證伺服器，來進行前記契約者的本人認證，當已確認爲本人時，則使前記網路商業交易成爲可行。

若依據申請項1及申請項2之發明，則若藉由網路結帳輔助裝置進行契約者之本人認證的結果，確認爲本人的

話，則由於即使是契約者本身也無法獲知卡片資訊，而卡片資訊是以無法從外部讀出之狀態而被儲存，因此，異於卡片資訊會外露之先前的信用卡，可提高卡片資訊的隱匿性，防止網路商業交易中的卡片資訊之不正當使用。

又，由於網路結帳輔助裝置係爲可搬型，因此無論契約者身處何處，都可使用行動電話、在宅的個人電腦、外出地的個人電腦，來進行安全的網路商業交易，增加網路商業交易的便利性。

又，因爲契約者的本人認證時，是使用基於網路結帳輔助裝置中所儲存之契約者固有之 OTP 生成資訊而作成之一次性密碼，因此，即使第三者獲得一次性密碼，也不能使用在下次的網路商業交易中。

一次性密碼生成用之 OTP 生成資訊，因爲是以無法從外部讀出之狀態而被儲存，因此即使是契約者本人，也無從得知 OTP 生成資訊，只有正在操作網路結帳輔助裝置的契約者本人會獲知生成結果之一次性密碼。換言之，由於第三者所致之一次性密碼生成是不可能發生，因此，可更加保證網路商業交易的安全性。

而且，該一次性密碼的生成，係只有在網路結帳輔助裝置上顯示了卡片資訊後才會進行，因此，不具有網路結帳輔助裝置的第三者，就算僅得知識別資訊，也是不能生成一次性密碼。又，即使第三者竊得了網路結帳輔助裝置，若沒有用來輸入網路結帳輔助裝置的認證資訊，也是無法生成一次性密碼。

(6)

換言之，契約者，係在藉由網路結帳輔助裝置之認證手段接受了本人認證後，還會藉由認證伺服器而接受到本人認證，最終而言，一直到可進行網路商業交易爲止是必須要經過基於 2 種互異之認證資訊的本人認證，因此能更加防止第三者所致之假冒，提高網路商業交易的安全性。

申請項 3 之發明，係

一種網路結帳輔助裝置，其特徵爲，前記認證資訊，係爲前記契約者所預先訂定的私密號碼；前記輸入手段，係爲數字鍵。

若依據申請項 3 的發明，則由於可使輸入手段及認證手段構成較爲廉價，因此可謀求促進網路結帳輔助裝置之利用。

申請項 4 之發明，係

一種網路結帳輔助裝置，其特徵爲，前記認證資訊，係爲將前記契約者的指紋、虹膜、聲帶、臉部照片等之生物性特徵加以數值化而成的生物資訊。

若依據申請項 4 之發明，則因爲可以高精度來進行契約者之本人認證，因此可以成爲即使網路結帳輔助裝置遭竊，也不必擔心遭到惡用的網路結帳輔助裝置。

申請項 5 之發明，係

一種網路結帳輔助裝置，其特徵爲，前記 OTP 生成資訊，係爲共通金鑰；前記一次性密碼生成手段，係偵測所定操作鍵之壓下，而將前記操作鍵被壓下之日期所成之日期資料，以前記共通金鑰予以加密然後生成一次性密碼。

(7)

申請項6之發明，係

一種網路結帳輔助裝置，其中，前記OTP生成資訊，係由共通金鑰，和前記一次性密碼每次被生成時就被更新的利用次數資訊所構成；前記一次性密碼生成手段，係偵測所定操作鍵之壓下，而將前記利用次數資訊以共通金鑰予以加密而生成一次性密碼；在前記一次性密碼被生成後，將前記OTP生成資訊儲存部內的利用次數資訊加以更新。

此處所生成之一次性密碼，係使用共通金鑰，將在所定按鍵被按下之日期所成之日期資料或者每次一次性密碼生成時就會被更新的利用次數資訊予以加密而成者。亦即，由於是屬於只有正在操作網路結帳輔助裝置的契約者才可能作成的密碼，因此不持有網路結帳輔助裝置的第三者，是無法假冒契約者來進行網路商業交易，可更加提升網路商業交易的安全性。

申請項7之發明，係

一種網路結帳輔助裝置，其特徵爲，前記網路結帳輔助裝置，係具備抗外力入侵性(Tamper Proofness)。

若依據申請項7之發明，則由於網路結帳輔助裝置是具備抗外力入侵性，故可謀求更加提升對第三者所致之卡片資訊、認證資訊、OTP生成資訊之竊聽、篡改的安全性提升。

〔發明效果〕

(8)

若依據本發明的網路結帳輔助裝置，則若藉由網路結帳輔助裝置進行契約者之本人認證的結果，確認爲本人的話，則由於即使是契約者本身也無法獲知卡片資訊，而卡片資訊是以無法從外部讀出之狀態而被儲存，因此，異於卡片資訊會外露之先前的信用卡，可提高卡片資訊的隱匿性，防止網路商業交易中的卡片資訊之不正當使用。

又，由於網路結帳輔助裝置係爲可搬型，因此無論契約者身處何處，都可使用行動電話、在宅的個人電腦、外出地的個人電腦，來進行安全的網路商業交易，增加網路商業交易的便利性。

又，因爲契約者的本人認證時，是使用基於網路結帳輔助裝置中所儲存之契約者固有之 OTP 生成資訊而作成之一次性密碼，因此，即使第三者獲得一次性密碼，也不能使用在下次的網路商業交易中。

一次性密碼生成用之 OTP 生成資訊，因爲是以無法從外部讀出之狀態而被儲存，因此即使是契約者本人，也無從得知 OTP 生成資訊，只有正在操作網路結帳輔助裝置的契約者本人會獲知生成結果之一次性密碼。換言之，由於第三者所致之一次性密碼生成是不可能發生，因此，可更加保證網路商業交易的安全性。

而且，該一次性密碼的生成，係只有在網路結帳輔助裝置上顯示了卡片資訊後才會進行，因此，不具有網路結帳輔助裝置的第三者，就算僅得知識別資訊，也是不能生成一次性密碼。又，即使第三者竊得了網路結帳輔助裝置

，若沒有用來輸入網路結帳輔助裝置的認證資訊，也是無法生成一次性密碼。

換言之，契約者，係在藉由網路結帳輔助裝置之認證手段接受了本人認證後，還會藉由認證伺服器而接受到本人認證，最終而言，一直到可進行網路商業交易爲止是必須要經過基於 2 種互異之認證資訊的本人認證，因此能更加防止第三者所致之假冒，提高網路商業交易的安全性。

【實施方式】

以下，針對本發明之理想實施形態，基於添附圖面來詳細說明。圖 1(a)係網路結帳輔助裝置 1 的外觀圖，圖 1(b)係網路結帳輔助裝置 1 的電氣硬體之構成圖。

網路結帳輔助裝置 1，係在信用卡或轉帳卡等之卡片契約者之契約者終端(行動電話或個人電腦等)，和進行契約者本人認證的認證伺服器(通常是由持卡會員所保有)，是彼此有網路連接而成的網路結帳系統中，當契約者是使用該當契約者之識別資訊來進行結帳，以進行網路購物等之網路商業交易之際所被使用者；如圖 1(a)所示，具有可收容於手掌程度的外形，是由薄型且可手持搬運的框體 10 所構成，在框體 10 的外表面上，外露出顯示器 11、和按鍵操作部 12。

此外，本實施例的顯示器 11，係爲 8 位數顯示之顯示器；按鍵操作部 12，係由 0～9 的數字鍵 12a，和開始鍵 12b 所構成。

框體 10 的內部，係如圖 1(b)所示，是除了顯示器 11、按鍵操作部 12 以外，還有用來作爲卡片資訊儲存部 13、認證資訊儲存部 15、認證手段 14、OTP 生成手段 16、OTP 生成資訊儲存部 17、計時手段 18 而發揮各種機能的硬體(CPU、記憶體)，和用來驅動這些硬體電氣零件(顯示器 11、按鍵操作部 12、CPU、記憶體)的驅動用電源 19(電池)所構成。

此外，本實施例的框體 11 中，係除了顯示器 11 和按鍵操作部 12 之驅動用電源 19 以外，還設有內藏 SIM 等 IC 卡的插槽，在該當插槽中插入 IC 卡而使用。然後，上記 CPU 和記憶體，係使用該 IC 卡中含有者。如後述，卡片資訊儲存部 13、認證資訊儲存部 15、OTP 生成資訊儲存部 17 中，由於係記憶著每位契約者互異之資訊，因此，將此類資訊儲存在 IC 卡之記憶體中，插入插槽而使用，藉此，框體 10 本身係可爲各契約者皆爲共通，且框體 10 本身係不保有個人資訊，因此，除了可提升框體 10 的生產性，同時可使框體 10 的取用、管理更爲容易。

又，本實施例之驅動用電源 19，雖然爲鈕扣型電池，但亦可爲太陽電池或充電池等。又，網路結帳輔助裝置 1 係亦可設計成，在通常時保持電源 OFF 狀態，而在例如，當有按鍵操作部 12 之任一鍵被操作時，才啓動電源。

本實施例之卡片資訊儲存部 13、認證資訊儲存部 15、OTP 生成資訊儲存部 17，具體而言，是由儲存著後述之卡片資訊、認證資訊、OTP 生成資訊之每一者的記憶體所

構成；記憶體係在實體上爲將這些資訊綜合儲存之 1 個記憶體，亦可爲 2 個以上之記憶體。

本實施例之認證手段 14 及 OTP 生成手段 16，具體而言，係由被儲存在記憶體的程式所構成；網路結帳輔助裝置 1 內的 CPU，會從記憶體中讀出該當程式並執行，以實現這些認證手段 14 及 OTP 生成手段 16 之機能。此外，在不具備 CPU、記憶體的網路結帳輔助裝置上，認證手段 14、OTP 生成手段 16 之機能，亦可使用電子零件以電路方式來加以實現。

本實施例的網路結帳輔助裝置 1，係從基於與信用卡組織(credit card brand)的授權契約而發行信用卡的發卡銀行(若爲轉帳卡，則是發行轉帳卡的銀行或者卡片發行公司)來對每一位持卡會員也就是契約者，於發卡銀行中以每位契約者所固有之卡片資訊、認證資訊、OTP 生成資訊是被記錄在記憶體之狀態下，所發配出來者(發配的形態可爲借給、讓渡)；且被構成爲，在發配後，記憶體的儲存內容(卡片資訊儲存部 13、認證資訊儲存部 15、OTP 生成資訊儲存部 17)，是無法從外部讀出。

又，即使是被發配網路結帳輔助裝置 1 的契約者本身，也無法從外部讀出記憶體的記錄內容。契約者本身，係只有契約者的本人認證被進行、且確認爲本人時，才能藉由卡片資訊被顯示在顯示器 11 上，而僅能得知該當卡片資訊，除此以外的狀態下，卡片資訊係被隱匿化。

之所以設計成不讓記憶體的儲存內容可從外部讀出的

理由，是因爲網路結帳輔助裝置 1 是不具備連接網際網路等之網路的介面，是屬於非網路連接型的終端。

此外，爲了更加提升對記憶體儲存內容之竊聽、篡改的安全性，網路結帳輔助裝置 1、或內藏於網路結帳輔助裝置 1 的 SIM 等 IC 卡，係亦可具備抗外力入侵性(若試圖分解、或從記憶體直接讀取內容，則記憶體的記錄內容會被抹除、或是程式變成無法啓動之性質)。

以下，針對網路結帳輔助裝置 1 之各部細節加以說明。

卡片資訊儲存部 13，係爲將至少包含契約者之識別資訊的卡片資訊，以無法從外部讀出之狀態預先記憶而成的記憶體；本實施例之卡片資訊，係由契約者固有之識別資訊(卡號)、有效期限、和安全碼(以所定之方法預先加密過的 3 位數之 10 進位數。通常在塑膠型的信用卡的簽名板上有被印出。藉由該數字，就可確認該卡片的真正性)所構成。又，亦可包含名義人名。又，卡片資訊亦可僅單純由識別資訊來構成。又，有效期限、安全碼、名義人名之全部並不需要一定被卡片資訊所包含，亦可適宜地組合 1 者以上來構成卡片資訊。

認證資訊儲存部 15，係契約者所訂定之私密號碼，或將契約者的指紋、虹膜、聲帶、臉部照片等之生物性特徵予以數值化而成之生物資訊等，進行契約者本人認證所需之認證資訊，以無法從外部讀出之狀態，預先儲存成的記憶體。

此外，認證資訊儲存部 15 中所儲存之認證資訊，係異於網路結帳系統中的認證伺服器在契約者本人認證時所用之認證資訊，係爲網路結帳輔助裝置 1 爲了進行契約者本人認證所必須之認證資訊。又，認證伺服器中的認證資訊和網路結帳輔助裝置 1 中的認證資訊，係爲種類互異者。

OTP 生成資訊儲存部 17，係爲網路結帳輔助裝置 1 所固有之 OTP 生成資訊，是以無法從外部讀出之狀態而先儲存而成之記憶體；本實施例之 OTP 生成資訊，係爲網路結帳輔助裝置 1 上所固有的共通金鑰；共通金鑰，係在進行被 OTP 生成手段 16 所生成之一次性密碼之驗證的伺服器(後述之實施例中的認證伺服器)中，和儲存在卡片資訊儲存部 13 之識別資訊，建立有關連對應。

此外，共通金鑰，係於網路商業交易中，只會被儲存在進行契約者本人認證之認證伺服器、和網路結帳輔助裝置 1 的金鑰；在本實施例中，後述之 OTP 生成手段 16，在生成一次性密碼時會使用到。

認證手段 14，係爲用來進行確認網路結帳輔助裝置 1 之操作者，是否爲可利用卡片資訊儲存部 13 中所儲存之識別資訊的契約者(持卡會員)之本人認證的手段；係確認從輸入手段(本實施例中係爲數字鍵 12a)所輸入之輸入資訊，和認證資訊儲存部 15 中所儲存之認證資訊是否一致，當爲一致時，則視爲網路結帳輔助裝置 1 之操作者爲該當契約者本人，而至少將卡片資訊儲存部 13 中所儲存之

卡片資訊當中的識別資訊予以讀出，並顯示於顯示器 11 上的手段。

本實施例的認證手段 14，係操作者壓下了按鍵操作部 12 的開始鍵 12b，就接受開始鍵 12b 之壓下偵測而開始啓動。然後，一旦操作者壓下了相當於輸入手段的數字鍵 12a 而輸入了 4 位數的數字，則認證手段 14，係確認所輸入之數字，和認證資訊儲存部 15 中所儲存之私密號碼是否一致，若爲一致，則在顯示器 11 上顯示出卡片資訊。

認證資訊若像本實施例是私密號碼，則作爲輸入手段係只要數字鍵即可，輸入資訊和認證資訊之一致判斷處理也可容易進行，可以較廉價的構成來實現網路結帳裝置 1，可謀求促進網路結帳裝置 1 之利用。

本實施例之認證資訊雖然係爲 4 位數的私密號碼，但認證方法及認證資訊並非侷限於此，亦可適宜地組合複數種認證方法所致之認證手段，若採用複數認證手段，則其可換來認證精度之提高，可防止第三者所致之網路結帳輔助裝置的惡用。

例如，認證手段 14，若採用生物計量認證方法，則認證資訊係爲生物計量資訊(指紋、虹膜、臉部照片等之生物性特徵予以數值化而成之資料)，又，輸入手段係改爲用來輸入這些生物計量資訊的掃描器、麥克風、數位攝影機等。

由於生物計量認證方法，係爲高精度的認證方法，因此即使網路結帳輔助裝置 1 被第三者竊取，則只要不是身

爲網路結帳輔助裝置 1 所被發配的契約者，就無法使用網路結帳輔助裝置 1，而可防止遭到惡用。

又，本實施例之認證資訊的私密號碼中，除了數字以外，還可含有英文字母；此時，除了數字鍵以外，網路結帳輔助裝置還需要備有英文字母鍵。

OTP 生成手段 16，係在藉由認證手段 14 而顯示出卡片資訊後，基於 OTP 生成資訊儲存部 17 中所儲存之 OTP 生成資訊(本實施例中係爲共通金鑰)，來生成一次性密碼，並顯示於顯示器 11 上的手段。

該一次性密碼，係從契約者終端被發送至認證伺服器，並由認證伺服器進行契約者本人認證之際，與在認證伺服器上基於 OTP 生成資訊所生成之一次性密碼進行核對時所使用。然後，當這些一次性密碼的核對結果爲一致，而被認證伺服器確認爲本人時，使用該當契約者之識別資訊的結帳所致之網路商業交易，就變成可行。

本實施例中，在認證手段 14 所致之認證被進行過，且卡片資訊被顯示於顯示器 11 上後，一旦操作者按下開始鍵 12b，則開始鍵 12b 被按下這件事，即成爲令 OTP 生成手段啓動之契機，而會生成、顯示一次性密碼。

此外，本實施例之 OTP 生成手段 16，雖然係由詳細後述的時間同步方式來生成一次性密碼，但亦可以其他的生成方式，例如：計數器同步方式、或挑戰&回應方式，來生成一次性密碼。

計時手段 18，係爲本實施例之 OTP 生成手段 16 以時

間同步方式生成一次性密碼時所必須的手段，係爲計時的手段。此外，計時手段 18，係可由即時時鐘來構成，或可將計時程式儲存於記憶體，由 CPU 將該當計時程式讀出並執行而實現計時機能的方式。又，OTP 生成手段 16，係當以時間同步方式以外的方式來生成一次性密碼的時候，係可不須計時手段 18，取而代之而附加上各生成方式所必須之手段。

本實施例中，OTP 生成手段 16 係如前述，認證手段 14 係接受在顯示器 11 上顯示之卡片資訊，而成爲開始鍵 12b 之壓下偵測等待狀態。OTP 生成手段 16，係一旦測出開始鍵 12b 之壓下，則將測出壓下之事傳達給計時手段 18。計時手段 18，係計時開始鍵 12b 被測出壓下之日期，將日期資料(年月日時分秒。秒係以 30 秒爲單位)交付給 OTP 生成手段 16。

然後，OTP 生成手段 16，係從 OTP 生成資訊儲存部 17 讀出共通金鑰，將所被交付之日期資料，以讀出之共通金鑰予以加密，將其轉換成十進位數，顯示於顯示器 11。此外，本實施例之加密方式，雖然是採用共通金鑰加密方式，但亦可用其他的加密方式。

若依據以上說明之網路結帳輔助裝置 1，則藉由網路結帳輔助裝置 1 來進行契約者之本人認證，並確認爲本人時，認證手段 14 所顯示之卡片資訊，係被輸入至從可進行卡片結帳之加盟店的網站或認證伺服器所發送過來之顯示於契約者終端上的卡片資訊輸入畫面後，就可被發送至

網站或認證伺服器。

如此，若藉由網路結帳輔助裝置 1，進行契約者之本人認證而確認爲本人，亦即，若所輸入之輸入資訊，是和網路結帳輔助裝置中所儲存之認證資訊一致，則由於即使是契約者本身也無法獲知卡片資訊，而卡片資訊是以無法從外部讀出之狀態而被儲存，因此，異於卡片資訊會外露之先前的信用卡，可提高卡片資訊的隱匿性，防止網路商業交易中的卡片資訊之不正當使用。

又，由於網路結帳輔助裝置係爲可搬型，因此無論契約者身處何處，都可使用行動電話、在宅的個人電腦、外出地的個人電腦，來進行安全的網路商業交易，增加網路商業交易的便利性。

又，OTP 生成手段 16 所顯示的 OTP 生成手段 16，係在被輸入至從進行契約者之本人認證的認證伺服器所發送過來之顯示於契約者終端的一次性密碼輸入畫面後，除了被發送至認證伺服器，還藉由與認證伺服器所生成之一次性密碼的核對，當爲一致時，則確認爲本人，使用契約者識別資訊的結算所致之網路商業交易就變成可進行。

如此，因爲契約者的本人認證時，是使用基於網路結帳輔助裝置中所儲存之契約者固有之 OTP 生成資訊而作成之一次性密碼，因此，即使第三者獲得一次性密碼，也不能使用在下次的網路商業交易中。

一次性密碼生成用之 OTP 生成資訊，因爲是以無法從外部讀出之狀態而被儲存，因此即使是契約者本人，也無

從得知 OTP 生成資訊，只有正在操作網路結帳輔助裝置的契約者本人會獲知生成結果之一次性密碼。換言之，由於第三者所致之一次性密碼生成是不可能發生，因此，可更加保證網路商業交易的安全性。

而且，該一次性密碼的生成，係只有在網路結帳輔助裝置上顯示了卡片資訊後才會進行，因此，不具有網路結帳輔助裝置的第三者，就算僅得知識別資訊，也是不能生成一次性密碼。又，即使第三者竊得了網路結帳輔助裝置，若沒有用來輸入網路結帳輔助裝置的認證資訊，也是無法生成一次性密碼。

換言之，契約者，係在藉由網路結帳輔助裝置之認證手段接受了本人認證後，還會藉由認證伺服器而接受到本人認證，最終而言，一直到可進行網路商業交易爲止是必須要經過基於 2 種互異之認證資訊的本人認證，因此能更加防止第三者所致之假冒，提高網路商業交易的安全性。

此外，認證資訊儲存部 15 係亦可設計成，除了上述認證資訊以外，還會以認證手段 14 所進行之一致判定處理，發現輸入資訊和認證資訊並不一致時，預先儲存著可接受輸入資訊重新輸入的次數(錯誤容許次數)。此時，網路結帳輔助裝置 1 或認證手段 14，係構成爲也要具備計數手段(計數器)。

然後，在認證手段 14 進行一致判定處理的流程中，當輸入資訊和認證資訊不一致時，則每次在其發生時，計數手段就會從 1 起往上計算，並比較被加算後的數字與錯

誤容許次數，當加算後的數字超過了錯誤容許次數時，以降就使認證手段 14 不進行自身的處理，並且也使 OTP 生成手段 16 不啓動，以使認證流程及 OTP 生成流程不被進行。

藉此，就可防止惡意第三者盜用網路結帳輔助裝置 1 來處理認證資訊然後輸入，結果導致卡片資訊或一次性密碼被不幸被顯示在顯示器 11 上。

此外，當加算後的數字沒有超過錯誤容許次數，而輸入資訊和認證資訊一致時，認證手段 14 雖然會在顯示器 11 上進行卡片資訊之顯示，但此時被計數的數字，會被重設(初期化)變成 0。

此處，將網路結帳輔助裝置 1 的操作程序及顯示器 11 之畫面遷移之一例，示於圖 5。此外，本實施例之顯示器 11，係爲 8 位數的英數字.記號顯示用顯示器。

首先，一旦開始鍵 12b 被操作者按下，則網路結帳輔助裝置 1 的電源便啓動(S200)，在顯示器 11 上會顯示「APPLI」(S210)，因此當想在開始鍵 12b 被按下後(S225)還要顯示卡片資訊時，操作者係按下數字鍵 12a 的「1」(S230)；當想要進行認證資訊(私密號碼)之變更時，則按下數字鍵 12a 的「2」(S330)。

由於當「1」被按下的時候(S230)，顯示器 11 上會顯示「PIN」，所以操作者係將作爲認證資訊的 4 位數私密號碼，從數字鍵 12a 中選擇出來並按下(S240)。其後，開始鍵 12b 被按下(S245)，已按下之私密號碼，若和認證資

訊儲存部 15 中所儲存之認證資訊一致，則將卡片資訊儲存部 13 中所儲存之卡片資訊當中，首先將識別資訊(以下稱之爲卡號)的前 8 位數，顯示於顯示器 11(S250)。

接著，一旦開始鍵 12b 被按下(S255)，則卡號的後 8 位數會被顯示在顯示器 11 上(S260)。

接著，一旦開始鍵 12b 被按下(S265)，則有效期限和安全碼會被顯示在顯示器 11 上(S270)。此外，S265 和 S270 之流程並非必須，亦可僅顯示出卡片資訊當中的卡號即可。

接著，一旦開始鍵 12b 被按下(S275)，則顯示器 11 會顯示「OTP＝1」，而進行要生成、顯示一次性密碼，或是否結束之選擇。此處，在開始鍵 12b 被按下後(S290)，再按下數字鍵 12a 的「1」(S295)，則顯示器 11 上會顯示催促認證資訊之輸入的「PIN」(S305)，因此，操作者係再度從數字鍵 12a 按下 4 位數的私密號碼，並按下開始鍵 12b(S310)。

已按下之私密號碼，若和認證資訊儲存部 15 中所儲存之認證資訊一致，則基於 OTP 生成資訊儲存部 17 中所儲存之 OTP 生成資訊，生成一次性密碼，並將其顯示在顯示器 11 上(S315)。

然後若開始鍵 12b 再次被按下(S320)，則網路結帳輔助裝置 1 的電源就被切斷。

當數字鍵 12a「1」以外的鍵被按下，或任一鍵都沒被按下、經過了預先決定之所定時間後(S300)，則網路結帳

輔助裝置 1 會自動地切斷電源。

此外，S240 和 S305 中所輸入之私密號碼，係亦可爲卡片資訊顯示用和一次性密碼生成用是個別的私密號碼，此時，認證資訊儲存部 15 中，是將各個私密號碼予以區別而儲存。

又，本實施例中，雖然是在一次性密碼顯示於顯示器 11 的流程(S315)之前，以 S305 再度向操作者催促輸入認證資訊，但是，亦可設計成省略 S305，僅須 S310 之開始鍵 12b 按下，就可生成一次性密碼。

S225 之後，若數字鍵 12a 的「2」被按下(S330)，則顯示器 11 上會顯示「CHANGE？」(S335)。

一旦開始鍵 12b 被按下(S340)，則在顯示器 11 上會顯示「PIN」，催促私密號碼之輸入，因此，操作者係從數字鍵 12a 按下 4 位數之私密號碼後(S345)，再按下開始鍵 12b(S350)，若已被按下之私密號碼，是和認證資訊儲存部 15 中所儲存之認證資訊一致，則用來催促變更後之私密號碼輸入的「NEW1」會顯示於顯示器 11 上，因此，操作者係從數字鍵 12a 按下變更後的私密號碼(S355)，然後再按下開始鍵 12b(S360)。

其次，因爲於顯示器 11 上會顯示用來催促再次輸入變更後私密號碼的「NEW2」，因此操作者要再度從數字鍵 12a 按下變更後之私密號碼(S365)，然後按下開始鍵 12b(S370)。

若 S355 中被按下之私密號碼，和 S365 中所按下之私

密號碼一致，則顯示器 11 上會顯示旨在表示私密號碼變更已完成之「COMPLETE」(S375)，因此一旦在經過確認後，開始鍵 12b 被按下(S380)，則私密號碼的變更程序就完成，電源會被切斷。

此外，爲了提升安全性，S355 和 S365 中，即使有從數字鍵 12a 進行輸入，所輸入的值也不會被顯示在顯示器 11 上，較爲理想。

〔實施例 1〕

以下，針對被發給了圖 1 所示之網路結帳輔助裝置 1 的信用卡契約者也就是信用卡會員(以下稱之爲持卡會員)，去使用網路結帳輔助裝置 1，從具有通訊機能的個人電腦或行動電話，藉由使用該當持卡會員之卡號的結帳，來進行網路購物等之網路商業交易(以下稱之爲網路商業交易)時的一實施例，加以說明。

本實施例之網路結帳系統的系統構成和網路連接關係，示於圖 2 的系統構成圖。又，本實施例之網路結帳系統中的網路商業交易之流程，示於圖 3 的流程圖。

此外，本實施例中，網路結帳系統中提供網路商業交易服務者，係爲信用卡組織(credit card brand)。

持卡會員，假設係除了預先對發卡銀行進行信用卡的申辦，接受信用卡的發行，同時還從發卡銀行，接受發配了儲存有每位持卡會員所固有之認證資訊(持卡會員在申辦信用卡時所登錄之私密號碼或指紋資訊等之生物資訊)

、卡片資訊(每位持卡會員所固有之卡號、有效期限)、OTP生成資訊(共通金鑰)的網路結帳輔助裝置1。

又，本實施例中，雖然圖1(b)所示之網路結帳輔助裝置1之構成當中，除了顯示器11和按鍵操作部12和驅動用電源19之構成，係預先儲存在SIM等IC卡中，並藉由在設於框體10之IC卡插槽(未圖示)中插入該當IC卡，來實現網路結帳輔助裝置1之機能，但是，網路結帳輔助裝置並非一定要具備IC卡，當不具備IC卡的情況，係只要網路結帳輔助裝置本身，有具備CPU或記憶體即可。

又，本實施例的網路結帳輔助裝置1，雖然係爲利用了使用持卡會員識別資訊之結帳、亦即卡片結帳的網路商業交易中所被使用者，但當持卡會員只希望進行網路商業交易，不希望先前之塑膠型磁卡、IC卡等所成之信用卡所致之真實的面對面交易的情況下，亦可不受到信用卡之發行。

又，當信用卡組織，也有進行發卡銀行之業務的情況下，亦可從信用卡組織來發配網路結帳輔助裝置1。

會員終端2，係爲契約者之終端，是持卡會員使用網路結帳輔助裝置1進行網路商業交易所需之終端，係爲至少具有通訊機能和瀏覽顯示機能的個人電腦、行動電話等終端

加盟店終端3，係除了向會員終端2提供虛擬店舖(網站)，接受商品或服務之訂購以外，還向發卡銀行側委託已下訂之持卡會員的本人認證，在進行過持卡會員之本人

認證後，對收單銀行(基於與信用卡組織之授權契約，進行加盟店之獲得.契約.管理業務等)，委託進行授權(調查所訂購之商品或服務之金額份的信用額度在持卡會員身上是否還有剩餘，若有剩餘信用額度則將該金額份確保成結帳用)的終端。

收單銀行終端 4，係爲將從加盟店終端 3 所受取的授權委託，再委託給發卡銀行側(授權再轉送)之終端。

仲介伺服器 5，係擔任加盟店終端 3 和後述之認證伺服器 7 的仲介，亦即，是在會員終端 2 和加盟店終端 3 之間，擔任持卡會員之認證服務之仲介角色的伺服器。

仲介伺服器 5，在本實施例中係爲信用卡組織所營運的伺服器，是儲存著用來識別使用網路結帳輔助裝置 1 的網路商業交易服務所對應之加盟店的加盟店識別資訊，和用來識別使用網路結帳輔助裝置 1 之網路商業交易服務所對應之發卡銀行的發卡銀行識別資訊。

此外，本實施例之網路結帳系統中，當混合有不使用網路結帳輔助裝置 1 之網路商業交易服務存在時，則仲介伺服器 5，需要將不支援使用網路結帳輔助裝置 1 之商業交易服務的加盟店及發卡銀行的識別資訊，和上記加盟店識別資訊及發卡銀行識別資訊加以區別而儲存。

發卡銀行終端 6，係爲接取從收單銀行終端 4 收到的授權委託，進行授權之終端。

認證伺服器 7，係在進行網路商業交易之際，早於授權，先進行持卡會員本人認證的伺服器。本實施例中，認

證伺服器 7，係爲發卡銀行所營運的伺服器，是連接著發卡銀行終端 6，並且是將可能進行使用網路結帳輔助裝置 1 之網路商業交易的持卡會員的卡片資訊(卡號、有效期限)及 OTP 生成資訊(網路結帳輔助裝置 1 所固有之共通金鑰)，以彼此互相建好關連的狀態，加以儲存。換言之，每 1 持卡會員，都被建立關聯有卡片資訊和 OTP 生成資訊，而被儲存在認證伺服器 7 中。

此外，往認證伺服器 7 的這些資訊之儲存，係在向持卡會員發配網路結帳輔助裝置 1 之同時期，或約略該時期之前後時進行。

圖 2 中，會員終端 2、加盟店終端 3、仲介伺服器 5、認證伺服器 7 間，係分別藉由網際網路等網路 9a 而連接；加盟店終端 3、收單銀行終端 4、發卡銀行終端 6，係分別藉由專線 9b 而連接。

此外，發卡銀行終端 6 及認證伺服器 7，係對每個發卡銀行個別準備，其分別皆是對會員終端 2、收單銀行終端 4、仲介伺服器 5，以網路 9a、專線 9b 而連接。

又，加盟店終端 3 也是對每個加盟店個別準備，其分別皆是對會員終端 2、仲介伺服器 5、收單銀行終端 4，以網路 9a、專線 9b 而連接。

以下，基於圖 3 之流程圖及圖 2 之系統構成圖，說明使用網路結帳輔助裝置 1 的網路商業交易之流程。持卡會員，係從會員終端 2，透過網路 9a，向虛擬店舖(Web 網站)的加盟店終端 3 進行存取，並閱覽商品或服務。然後

，一旦決定了要訂購之商品或希望的服務，則會員終端 2，係向加盟店終端 3，發送關於訂購商品或希望服務是希望用卡片結帳所致之網路商業交易之意旨。

加盟店終端 3，係令會員終端 2，顯示如圖 4(a)所示之卡片資訊輸入畫面 100，並向會員終端 2 請求輸入並發送卡號及卡片之有效期限。

於是，一旦持卡會員按下了網路結帳輔助裝置 1 的開始鍵 12b，則網路結帳輔助裝置 1 的認證手段 14 便啓動，網路結帳輔助裝置 1 成爲等待認證之狀態。接下來，持卡會員，係將本人認證所必須之輸入資訊(本實施例中係爲 4 位數的私密號碼)，從數字鍵 12a 進行輸入。此外，此處所輸入之 4 位數的私密號碼，是預先在持卡會員申辦卡片時就已經決定妥當，且已經被儲存在網路結帳輔助裝置 1 內的認證資訊儲存部 15 中。

認證手段 14，係將認證資訊儲存部 15 中所儲存之認證資訊加以讀出，並確認是否和從數字鍵 12a 所輸入之輸入資訊一致。然後，當兩者爲一致時，認證手段 14，係從卡片資訊儲存部 13 讀出作爲卡片資訊的卡號和有效期限，並顯示於顯示器 11 上。

然後，若卡號和有效期限全部在顯示器 11 上顯示完畢，則認證手段 14，係將顯示完畢的意旨，傳達給 OTP 生成手段 16。藉此，OTP 生成手段 16，係成爲後述之一次性密碼生成等待狀態。

此外，本實施例中，由於顯示器 11 所能顯示的位數

限制爲 8 位數，因此認證手段 14，係先將從卡片資訊儲存部 13 讀出之卡號進行分割處理而分成前 8 位和後 8 位，然後在顯示器 11 上，先顯示卡號的前 8 位。持卡會員，係基於該顯示，在卡片資訊輸入畫面 100 的卡號輸入欄 100a 中輸入卡號的前 8 位數。

一旦卡號的前 8 位數的輸入結束，則持卡會員係按下開始鍵 12b。認證手段 14，係接受開始鍵 12b 的按下偵測，而將卡號的後 8 位數顯示於顯示器 11 上。持卡會員，係基於該顯示，在卡片資訊輸入畫面 100 的卡號輸入欄 100a 中輸入卡號的後 8 位數。

一旦卡號的後 8 位數的輸入結束，則持卡會員係按下開始鍵 12b。認證手段 14，係接受開始鍵 12b 的按下偵測，而將有效期限以 4 位數(MM(月)/YY(年))顯示出來。持卡會員，係基於該顯示，在卡片資訊輸入畫面 100 的有效期限輸入欄 100b 中，輸入有效期限。

此外，當顯示器的顯示領域、可顯示位數還有餘裕時，當然亦可將卡號一次全部顯示在顯示器上，又，亦可將卡號和有效期限一次全部顯示出來。又反之，當顯示器的可顯示位數是少於 8 位數時，認證手段 14 係可配合可顯示位數，將從卡片資訊儲存部 13 中讀出之卡片資訊予以預先分割妥當，藉由開始鍵 12b 或其他任意鍵的按下，而依序地顯示出已分割之卡片資訊。

如以上，網路結帳輔助裝置 1，係僅當所輸入之輸入資訊，是和認證資訊儲存部 15 中所儲存之認證資訊一致

時，才在顯示器 11 上顯示卡片資訊，因此，若不知道認證資訊，則第三者即使盜取網路結帳輔助裝置 1，也無從得知內部的卡片資訊。因此，相較於有印出卡片資訊的先前信用卡，安全性較高，不會有卡片資訊被惡用在網路商業交易的疑慮。

持卡會員係輸入完卡號及有效期限(此外，圖 4 之卡片資訊輸入畫面 100 中雖未顯示，但亦可將訂購之商品.服務名、金額、訂購日、加盟店名、商品的發送地等資訊，顯示於同一畫面上)，便點選卡片資訊輸入畫面 100 內的送訊鈕 100c。藉由送訊鈕 100c 被點選，在加盟店終端 3 側，已輸入之卡片資訊會被發送(S10)。

從會員終端 2，接收到訂購之商品.服務名、金額、訂購日、加盟店名、商品的發送地等相關之訂購資訊，和訂購商品之結帳所用的卡片的卡號和有效期限等之卡片資訊的加盟店終端 3，係除了已接收到的卡片資訊以外，還將對每一加盟店賦予之加盟店識別資訊，發送到透過網路 9a 而連接之仲介伺服器 5，要求確認持卡會員是否是接受使用網路結帳輔助裝置 1 之商業交易服務的會員(認證執行可否確認)(S20)。

仲介伺服器 5，係確認已收到之加盟店識別資訊，是否和所保有之加盟店識別資訊一致(加盟店認證)。若這些資訊一致，則從有參加使用網路結帳輔助裝置 1 之商業交易服務的加盟店的加盟店終端 3，就可向仲介伺服器 5 進行存取。若不一致，則由於來自沒有參加使用網路結帳輔

助裝置 1 之商業交易服務的加盟店的加盟店終端 3 的存取係爲不正當存取，因此不會進入以後的流程。

仲介伺服器 5，係基於從有參加使用網路結帳輔助裝置 1 之商業交易服務的加盟店終端 3 所收到之持卡會員的卡片資訊，特定出發行了該當持卡會員之卡號的發卡銀行，向已被特定之發卡銀行的認證伺服器 7，發送卡片資訊，並要求確認持卡會員是否是接受使用網路結帳輔助裝置 1 之商業交易服務的會員(認證執行可否確認)(S30)。

本實施例之仲介伺服器 5 中，係儲存著識別發卡銀行的發卡銀行識別資訊，仲介伺服器 5，係基於已收到之卡片資訊來檢索發卡銀行識別資訊，特定出發卡銀行。

換言之，本實施例的仲介伺服器 5，係並非直接進行認證執行可否確認，而是進行加盟店認證，同時基於從加盟店終端 3 接收到的卡片資訊，特定出發行了持卡會員之卡號的發卡銀行，向已被特定之發卡銀行的認證伺服器 7，傳送卡片資訊，並負責將從該當認證伺服器 7 所接收到的認證執行可否結果，傳送至加盟店終端 3。

此外，在本實施例中，仲介伺服器 5 雖然是由信用卡組織所營運的伺服器，但亦可由各個加盟店終端 3 來具備其，此時，就可直接從加盟店終端 3 向認證伺服器 7，進行認證執行可否確認的要求。又，亦可在認證伺服器 7 上，進行加盟店認證。

認證伺服器 7，係藉由確認從仲介伺服器 5 所收到之卡片資訊是否已經有被登錄在認證伺服器 7 中，來進行持

有該當卡片資訊之持卡會員是否爲接受了使用網路結帳輔助裝置 1 之商業交易服務的持卡會員之確認(認證執行可否確認)，並將其結果，回送給仲介伺服器 5(S40)。此外，認證執行可否確認結果，係若從仲介伺服器 5 接收到的卡片資訊是有被登錄在認證伺服器 7 中則爲「可」，若沒有被登錄則爲「否」。

然後，接收到認證執行可否確認結果的仲介伺服器 5，係將該結果傳送至加盟店終端 3(S50)。

當持卡會員之認證執行可否確認結果爲「可」時，則意味著該持卡會員係爲接受了使用網路結帳輔助裝置 1 之商業交易服務，因此加盟店終端 3，係進入進行該持卡會員的本人認證要求的流程(S60)。具體而言，加盟店終端 3 係對會員終端 2，發送認證執行可否結果，同時還發送之前進行過認證執行可否確認之發卡銀行的認證伺服器 7 的 URL 資訊。

從加盟店終端 3 收到認證要求的會員終端 2，係基於所收到之 URL，向之前被仲介伺服器 5 所存取之同一認證伺服器 7 進行存取，進行認證要求(S70)。此外，S70 的流程，係從 S60 起以一連串方式進行；可以用作爲會員終端 2 使用之個人電腦或行動電話的瀏覽器所一般具備之重新導向機能等來加以實現，讓持卡會員不會有所意識，就可在會員終端 2 內部自動進行處理之流程。

認證伺服器 7，係向會員終端 2，催促一次性密碼之送訊，並基於從會員終端 2 所接收到的一次性密碼，進行

持卡會員的認證(S80)。

具體而言，認證伺服器 7，係從存取過來的會員終端 2，接收卡片資訊及訂購資訊，並確認擁有該卡片資訊的持卡會員，是否爲剛才從加盟店終端 3 透過仲介伺服器 5、受到認證執行可否確認要求的持卡會員。此確認係預定之所定時間前留下是否有從仲介伺服器 5 接收該當卡片會員之卡片資訊的日誌，並藉由確認從會員終端 2 接收到之持卡會員之卡片資訊，是否和所定時間前留在日誌中之卡片資訊一致而爲之。

此外，訂購資訊，係可不是從會員終端 2 發送，而是亦可設計成，在 S20、30 的流程中，從加盟店終端 3 透過仲介伺服器 5 而發送至認證伺服器 7；或亦可在從加盟店終端 3 向會員終端 2 發送認證伺服器 7 的 URL 資訊之際，一起被發送，而在會員終端 2 向認證伺服器 7 進行存取之際，轉送給認證伺服器 7。

又，認證伺服器 7 所進行之，存取過來之會員終端 2 的持卡會員，和從加盟店終端 3 接受認證執行可否確認要求之持卡會員是否爲同一的確認，可並不僅藉由卡片資訊之核對，而是亦可設計成，從會員終端 2 及加盟店終端 3(直接或透過仲介伺服器 5)雙方接收訂購資訊，而也一併進行這些資訊的核對。

認證伺服器 7，一旦確認了是從之前接受認證執行可否確認要求之持卡會員的網路結帳輔助裝置 1 來的存取，則認證伺服器 7 係基於所收到之訂購資訊，作成如圖 4(b)

所示之一次性密碼輸入畫面 101，並發送至有存取之會員終端 2。

圖 4(b)之一次性密碼輸入畫面 101 中，會顯示持卡會員正在進行網路商業交易之對象也就是加盟店名、欲訂購之商品.服務之金額、訂購日。

一旦在會員終端 2 上顯示出一次性密碼輸入畫面 101，則持卡會員，係按下網路結帳輔助裝置 1 的開始鍵 12b。網路結帳輔助裝置 1 的 OTP 生成手段 16，係一旦偵測到開始鍵 12b 按下，則從一次性密碼生成等待狀態，進入一次性密碼生成流程。

OTP 生成手段 16，係將儲存在 OTP 生成資訊儲存部 17 中的共通金鑰讀出，藉由計時手段 18 進行計時，將根據開始鍵 12b 被按下的日期所成之日期資料(年月日秒、秒係爲 30 秒單位)，以該共通金鑰進行加密而生成一次性密碼，並將其轉換成 10 進位數，顯示於顯示器 11 上。此外，本實施例之加密方式係採用共通金鑰加密方式。又，由於本實施例之顯示器 11 之可顯示位數係爲 8 位數，因此顯示器 11 上會顯示出所生成之一次性密碼的前 6～8 位數。

持卡會員，係在顯示於會員終端 2 之一次性密碼輸入畫面 101 的密碼輸入欄 101a 中，輸入被顯示在網路結帳輔助裝置 1 之顯示器 11 上的一次性密碼，並點選送訊鈕 101b，則已輸入之一次性密碼會被發送至認證伺服器 7。

此外，一次性密碼的輸入結束後，持卡會員再度按下

網路結帳輔助裝置 1 的開始鍵 12b，就可使網路結帳輔助裝置 1 之顯示器 11 上所顯示之一次性密碼變成不顯示，這在安全性的觀點上較爲理想。又在此同時，也將電源關閉，在省電觀點上較爲理想。

從會員終端 2 接收到一次性密碼的認證伺服器 7，首先係藉由會員終端 2 之識別號碼等之核對、或該當會員終端 2 個別生成並發送過來之對一次性密碼輸入畫面 101 是否有回訊，確認該會員終端 2 是否爲剛才要求一次性密碼送訊之對方。

確認後，認證伺服器 7，係基於要求一次性密碼之送訊之前就接收到之持卡會員的卡片資訊，從 OTP 生成資訊之中，取出和該卡號關連登錄的共通金鑰，並將認證伺服器 7 從會員終端 2 接收一次性密碼之日期所成之日期資料(年月日秒、秒係爲 30 秒單位)，以該共通金鑰進行加密而生成一次性密碼，並將其轉換成十進位數。此外，本實施例之加密方式，係採用共通金鑰加密方式。

如此一來，認證伺服器 7，係確認認證伺服器 7 所生成之一次性密碼，和之前從會員終端 2 所接收到之一次性密碼，是否一致。若爲一致，則可證明該一次性密碼，係確實爲藉由僅儲存於網路結帳輔助裝置 1 和認證伺服器 7 的共通金鑰，在幾乎同時刻所作成之一次性密碼。

換言之，將一次性密碼發送至認證伺服器 7 的會員終端 2 之操作者，係爲該當一次性密碼生成時所用之共通金鑰、及該當共通金鑰所關聯到之卡片資訊所被儲存之網路

結帳輔助裝置 1 之操作者；且係爲可利用該當卡片資訊的持卡會員本人，藉此，要求網路商業交易的持卡會員的本人確認就被進行了。

此外，一次性密碼生成手段，是採用本實施例此種時間同步方式時，網路結帳輔助裝置 1 在生成一次性密碼時所用的日期，和認證伺服器 7 在生成一次性密碼時所用的日期，係不一定嚴密地相同，因此，考慮到從認證伺服器 7 生成一次性密碼起，至持卡會員按下網路結帳輔助裝置 1 的開始鍵 12b，網路結帳輔助裝置 1 生成一次性密碼爲止的時間差，本實施例中，係將日期資料的秒解析力設爲 30 秒。

可是，只有當被兩者所生成之一次性密碼是完全一致的情況下，才能認可持卡會員之真正性，持卡會員按下網路結帳輔助裝置 1 的開始鍵 12b 以生成一次性密碼，因此，若一直到認證伺服器 7 從會員終端 2 接收一次性密碼爲止的期間是經過了 30 秒以上的情形下，光是如此，一次性密碼就會不一致，導致無法認證的事態增加，反而會有損網路商業交易的便利性。

因此，認證伺服器 7，係當即使從會員終端 2 收到之一次性密碼是不一致時，仍會將從會員終端 2 收到之一次性密碼的日期，往前後錯開 N 次回×30 秒份，在認證伺服器 7 側上重新生成一次性密碼，若和會員終端 2 側上所生成之一次性密碼一致，則視爲持卡會員的本人確認成功。

此外，N 係考慮安全性的精度，而預先決定妥當。亦

即，當想要提高安全性精度時，則將 N 設定得較小；當想要降低安全性精度而以持卡會員側的便利性爲優先時，則將 N 設定得較大。

認證伺服器 7，係將一次性密碼核對所致之持卡會員的認證結果，發送至會員終端 2(S90)。此外，具體而言，認證伺服器 7，係對會員終端 2，除了發送認證結果，還發送加盟店終端 3 的 URL 資訊，並從會員終端 2 向加盟店終端 3 轉送認證結果。

收到認證結果的會員終端 2，係將該當認證結果(本人認證 OK、本人認證 NG)，再轉送至加盟店終端 3(S100)。此外，S100 的流程，係和 S70 同樣地，從 S90 起以一連串方式進行；可藉由會員終端 2 的瀏覽器之重新導向機能來實現，實際上，係讓持卡會員不會有所意識，而在會員終端 2 內部自動進行處理之流程。

加盟店終端 3，係從會員終端 2 接收認證結果，且認證結果爲，持卡會員被確認爲本人時(本人認證 OK)，則向收單銀行進行該當持卡會員的授權要求，因此，除了向收單銀行終端 4，發送持卡會員之卡片資訊、和結帳希望金額(持卡會員所欲訂購之商品.服務之機能)所成之交易資料以外，還發送該當認證結果(S110)。此外，交易資料，係亦可在 S10 中，從會員終端 2 有訂購資訊和卡片資訊送訊時之時點上就已被生成，且被記憶在加盟店終端 3 中，而是將其加以讀出。

收單銀行終端 4，係基於從加盟店終端 3 接收到之交

易資料和認證結果，並基於本人認證 OK 的持卡會員之卡號，來特定出卡片發行源的發卡銀行，並向已特定之發卡銀行的發卡銀行終端 6，轉送交易資料和認證結果(S120)。

收到交易資料和認證結果之發卡銀行終端 6，係基於未圖示之會員資料庫中所儲存之每位會員的會員資訊或授信資訊，來確認交易資料中所含之結帳希望金額，是否爲受到授權委託之持卡會員的信用額度範圍內。若結帳希望金額是在信用額度範圍內，則當成授權 OK，結帳希望金額份的信用額度會被確保下來。

然後，發卡銀行終端 6，係將授權的結果(授權 OK、授權 NG)發送至收單銀行終端 4(S130)，然後收單銀行終端 4，係向加盟店終端 3，轉送授權結果(S140)。

然後，加盟店終端 3，係從收單銀行終端 4 接收到授權結果後，將該結果通知給會員終端 2(S150)。具體而言，當授權結果爲 OK 時，則加盟店和持卡會員之間，使用該當持卡會員之卡號的結帳所致之網路商業交易係爲成立之意旨的畫面會發送至會員終端 2，並顯示在會員終端 2 上。又，當授權結果爲 NG 時，係將網路商業交易不成立之意旨的畫面發送至會員終端 2，並顯示之。

此外，本實施例中，認證伺服器 7 中的使用一次性密碼之本人認證，係在會員終端 2 和加盟店終端 3 之間每次進行網路商業交易時，就會被進行。換言之，本實施例之 OTP 生成手段 16 所生成之一次性密碼，係僅限 1 次的網

路商業交易中是有效的，所以即使未持有網路結帳輔助裝置的第三者竊聽到一次性密碼，第三者仍無法僞裝成持卡會員而進行以降的網路商業交易，因此可更加提升商業交易的安全性。

〔實施例 2〕

其次，針對被發配網路結帳輔助裝置 1a(未圖示)之持卡會員，去使用該當網路結帳輔助裝置 1a，從具有通訊機能的個人電腦或行動電話，藉由使用該當持卡會員之卡號的結帳，進行網路商業交易時之一實施例，加以說明。

本實施例和之前的實施例 1 的不同點是，網路結帳輔助裝置所具備之 OTP 生成手段 16 的一次性密碼生成方法，和 OTP 生成資訊儲存部 17 的儲存內容，和圖 3 中的會員終端 2 與認證伺服器 7(本實施例中係爲認證伺服器 7a)之間的認證流程(S80、S90)的內容等。

亦即，雖然在先前之實施例 1 中，一次性密碼生成方法係設計成時間同步方式，但在本實施例中，是採用利用次數同步方式。伴隨於此，本實施例之網路結帳輔助裝置 1a 中，圖 1 中所記載之計時手段 18，是被取代成計數手段 18a(未圖示)。

關於網路結帳輔助裝置 1、1a 和認證伺服器 7、7a，除了上述相異點以外之構成，以及 S80、S90 以外之流程，因爲是和圖 1～圖 3 所示之實施例相同，所以以下使用圖 1～圖 3，僅說明圖 3 的 S80、S90 之部份的詳細流程。

(38)

本實施例之 OTP 生成資訊儲存部 17 中所儲存之 OTP 生成資訊，係由網路結帳輔助裝置 1a 所固有之共通金鑰，和利用次數資訊所構成。

其中，共通金鑰，係以在 OTP 生成資訊儲存部 17 內不可改寫的狀態而被儲存，且於進行 OTP 生成手段 16 所生成之一次性密碼之驗證的認證伺服器 7a 中，是被建立關連對應至被儲存在卡片資訊儲存部 13 的卡號。

利用次數資訊，係和共通金鑰同樣地，於認證伺服器 7a 中，被建立關連對應至卡片資訊儲存部 13 中所儲存的卡號。

換言之，這些 OTP 生成資訊，係以和卡號建立關連的狀態，在認證伺服器 7a 中也被儲存；當認證伺服器 7a 從會員終端 2 接收一次性密碼之際，與會員終端 2 同樣地，認證伺服器 7a 上也會生成一次性密碼，藉由確認兩者是否一致，就可進行一次性密碼的妥當性驗證、持卡會員之認證。

又，利用次數資訊，係爲僅當有來自 OTP 生成手段 16 的改寫指令時才可以改寫之資訊，藉由計數手段 18a，0 次、1 次、2 次這種一次加 1 的加算，或 100 次、99 次、98 次這種一次減 1 的減算後，加算或減算後的數值，會被儲存在 OTP 生成資訊儲存部 17 中，利用次數資訊會被更新。此外，加算或減算，係爲預先決定。

此外，計數手段 18a，係亦可被含在 OTP 生成手段 16，或可有別於 OTP 生成手段 16 而另外設置，但後者的時

候，必須要由 OTP 生成手段 16 來控制計數手段 18a，使得利用次數資訊的改寫會被進行。

圖 3 的 S80 中，首先，認證伺服器 7a，係向會員終端 2，催促一次性密碼之送訊，並基於從會員終端 2 所接收到的一次性密碼，進行持卡會員的認證。

具體而言，認證伺服器 7a，係從存取過來的會員終端 2，接收卡片資訊及訂購資訊，並確認擁有該卡片資訊的持卡會員，是否爲剛才從加盟店終端 3 透過仲介伺服器 5、受到認證執行可否確認要求的持卡會員。此確認係預定之所定時間前留下是否有從仲介伺服器 5 接收該當卡片會員之卡片資訊的日誌，並藉由確認從會員終端 2 接收到之持卡會員之卡片資訊，是否和所定時間前留在日誌中之卡片資訊一致而爲之。

此外，訂購資訊，係可不是從會員終端 2 發送，而是亦可設計成，在 S20、30 的流程中，從加盟店終端 3 透過仲介伺服器 5 而發送至認證伺服器 7a；或亦可在從加盟店終端 3 向會員終端 2 發送認證伺服器 7a 的 URL 資訊之際，一起被發送，而在會員終端 2 向認證伺服器 7a 進行存取之際，轉送給認證伺服器 7a。

又，認證伺服器 7a 所進行之，存取過來之會員終端 2 的持卡會員，和從加盟店終端 3 接受認證執行可否確認要求之持卡會員是否爲同一的確認，可並不僅藉由卡片資訊之核對，而是亦可設計成，從會員終端 2 及加盟店終端 3(直接或透過仲介伺服器 5)雙方接收訂購資訊，而也一併進

行這些資訊的核對。

認證伺服器 7a，一旦確認了是從之前接受認證執行可否確認要求之持卡會員的網路結帳輔助裝置 1 來的存取，則認證伺服器 7a 係基於所收到之訂購資訊，作成如圖 4(b)所示之一次性密碼輸入畫面 101，並發送至有存取之會員終端 2。

圖 4(b)之一次性密碼輸入畫面 101 中，會顯示持卡會員正在進行網路商業交易之對象也就是加盟店名、欲訂購之商品.服務之金額、訂購日。

一旦在會員終端 2 上顯示出一次性密碼輸入畫面 101，則持卡會員，係按下網路結帳輔助裝置 1 的開始鍵 12b。網路結帳輔助裝置 1 的 OTP 生成手段 16，係一旦偵測到開始鍵 12b 按下，則從一次性密碼生成等待狀態，進入一次性密碼生成流程。

OTP 生成手段 16，係將 OTP 生成資訊儲存部 17 中所儲存之共通金鑰和利用次數資訊予以讀出，並將該當利用次數資訊，以共通金鑰加密而生成一次性密碼，將其轉換成 10 進位數，顯示於顯示器 11 上。

此外，本實施例中，是將利用次數資訊，使用所定之一次性密碼生成演算法，來生成一次性密碼。

又，由於本實施例之顯示器 11 之可顯示位數係爲 8 位數，因此顯示器 11 上會顯示出所生成之一次性密碼的前 6～8 位數。

此外，OTP 生成資訊，係除了上記利用次數資訊和共

通金鑰以外，亦可含有其他僅網路結帳輔助裝置 1a 與認證伺服器 7a 兩者可獲知的任意資訊(例如，原則(policy)等)；此時，利用次數資訊，和該當任意之資訊，亦可被共通金鑰所加密，來生成一次性密碼。

OTP 生成手段 16，係在生成一次性密碼後，對計數手段 18a，將剛才讀出之利用次數資訊，加算或減算 1，然後將 OTP 生成資訊儲存部 17 的利用次數資訊予以改寫、更新。

持卡會員，係在顯示於會員終端 2 之一次性密碼輸入畫面 101 的密碼輸入欄 101a 中，輸入被顯示在網路結帳輔助裝置 1 之顯示器 11 上的一次性密碼，並點選送訊鈕 101b，則已輸入之一次性密碼會被發送至認證伺服器 7a。

此外，一次性密碼的輸入結束後，持卡會員再度按下網路結帳輔助裝置 1 的開始鍵 12b，就可使網路結帳輔助裝置 1 之顯示器 11 上所顯示之一次性密碼變成不顯示，這在安全性的觀點上較爲理想。又在此同時，也將電源關閉，在省電觀點上較爲理想。

從會員終端 2 接收到一次性密碼的認證伺服器 7a，首先係藉由會員終端 2 之識別號碼等之核對、或該當會員終端 2 個別生成並發送過來之對一次性密碼輸入畫面 101 是否有回訊，確認該會員終端 2 是否爲剛才要求一次性密碼送訊之對方。

確認後，認證伺服器 7a，係基於要求一次性密碼之送訊之前就接收到之持卡會員的卡片資訊，從 OTP 生成資訊

之中，取出和該卡號關連登錄的共通金鑰和利用次數資訊，並將利用次數資訊以共通金鑰加密而生成一次性密碼，並將其轉換成十進位數。

此外，本實施例中，是將利用次數資訊，使用所定之一次性密碼生成演算法，來生成一次性密碼。又，OTP 生成資訊中，若含有任意之資訊，則除了利用次數資訊以外，該當任意資訊也會一併被共通金鑰所加密。

如此一來，認證伺服器 7a，係確認認證伺服器 7a 所生成之一次性密碼，和之前從會員終端 2 所接收到之一次性密碼，是否一致。若爲一致，則可證明該一次性密碼，係確實爲藉由僅儲存於網路結帳輔助裝置 1 和認證伺服器 7a 的利用次數資訊和共通金鑰所作成之一次性密碼。

換言之，將一次性密碼發送至認證伺服器 7a 的會員終端 2 之操作者，係爲該當一次性密碼生成時所用之利用次數資訊和共通金鑰、及該當利用次數資訊和共通金鑰所關聯到之卡片資訊所被儲存之網路結帳輔助裝置 1 之操作者；且係爲可利用該當卡片資訊的持卡會員本人，藉此，要求網路商業交易的持卡會員的本人確認就被進行了。

認證伺服器 7a，係將一次性密碼核對所致之持卡會員之認證結果(本人認證 OK、本人認證 NG)，發送至會員終端 2，同時還將之前一次性密碼生成時所用到的利用次數資訊，以預先決定之演算方法進行加算或減算，並將其演算結果當成認證伺服器 7a 內的利用次數資訊，加以改寫、更新。

此外，一次性密碼生成方式，在採用如本實施例的利用次數同步方式時，即使會員終端 2 及網路結帳輔助裝置 1a 的操作者是正當的持卡會員，可是仍有可能因網路結帳輔助裝置 1a 在生成一次性密碼時所用的利用次數資訊、和認證伺服器 7a 在生成一次性密碼時所用的利用次數資訊爲不同，導致一次性密碼不一致的情形。

持卡會員，即使以網路結帳輔助裝置 1a 生成一次性密碼，但也並不必然保證會被發送至認證伺服器 7a，當持卡會員在網路商業交易的中途不慎發生斷線時，或者，有可能原本就不是要進行網路商業交易，而是操作網路結帳輔助裝置 1a 來亂玩而不慎生成了一次性密碼。此種情況下，由於網路結帳輔助裝置 1a 的利用次數資訊係被更新，可是認證伺服器 7a 的利用次數資訊未被更新，所以，當然所生成之一次性密碼就不會一致。

可是，若只有當被兩者所生成之一次性密碼是完全一致的情況下，才能認可持卡會員之真正性，則會導致認證 NG 增加，反而有損網路商業交易之便利性。

因此，認證伺服器 7a，係當即使從會員終端 2 收到之一次性密碼是不一致時，仍會將認證伺服器 7a 中所儲存之利用次數資訊在所定範圍(例如，利用次數資訊+N)內加以變更，在認證伺服器 7a 側重新生成一次性密碼，若和會員終端 2 側上所生成之一次性密碼一致，則視爲持卡會員的本人確認成功。

此外，N 係考慮安全性的精度，而預先決定妥當。亦

即，當想要提高安全性精度時，則將 N 設定得較小；當想要降低安全性精度而以持卡會員側的便利性爲優先時，則將 N 設定得較大。

如以上，若使用本發明之網路結帳輔助裝置來進行網路商業交易，則在將卡片資訊輸入至卡片資訊輸入畫面之際，被輸入至網路結帳輔助裝置的輸入資訊，只要和網路結帳輔助裝置中所儲存之認證資訊不一致，則即使是持卡會員本身也無從得知卡片資訊，因此，和卡片資訊會外露之先前的信用卡不同，卡片資訊的隱匿性較高，可防止網路商業交易中的卡片資訊之不正當使用。

又，由於網路結帳輔助裝置係爲可搬型，因此無論持卡會員身處何處，都可使用行動電話、在宅的個人電腦、外出地的個人電腦，來進行安全的網路商業交易，增加網路商業交易的便利性。

又，網路商業交易被進行之際的持卡會員之本人認證，係依據網路結帳輔助裝置所生成之一次性密碼，和認證伺服器所生成之一次性密碼是否一致而爲之。

此一次性密碼，係網路結帳輔助裝置所固有，且僅被儲存在網路結帳輔助裝置及認證伺服器中，而且是使用即使是持卡會員本身都無從得知的共通金鑰，將在每次偵測到所定鍵按下之日期所成之日期資料或者一次性密碼之生成時就被更新的利用次數資訊予以加密而成者。

亦即，由於是屬於只有正在操作網路結帳輔助裝置的持卡會員才可能作成的認證資訊，因此不持有網路結帳輔

助裝置的第三者，是無法假冒持卡會員來進行網路商業交易，可更加提升網路商業交易的安全性。

而且，該一次性密碼的生成，係只有在網路結帳輔助裝置上顯示了卡片資訊後才會進行，因此，不具有網路結帳輔助裝置的第三者，就算僅得知卡號，也是不能生成一次性密碼。又，即使第三者竊得了網路結帳輔助裝置，若沒有用來輸入網路結帳輔助裝置的認證資訊，也是無法生成一次性密碼。換言之，由於無論第三者是否有得到網路結帳輔助裝置，都無法假冒持卡會員來進行網路商業交易，因此商業交易的安全性可受到保證。

此外，一次性密碼之生成方法，係不限於上記實施例的時間同步方式，只要是在網路結帳輔助裝置和認證伺服器之間，能夠進行擁有網路結帳輔助裝置之持卡會員之本人認證即可。

又，由於網路結帳輔助裝置係採用網路非連接型的構成，所以一度被儲存於網路結帳輔助裝置中的卡片資訊、認證資訊、OTP 生成資訊，係無法被不正當存取等所讀出，而且就連被發配網路結帳輔助裝置的持卡會員，也是無法將其讀出。

假設，若網路結帳輔助裝置是可連接個人電腦或行動電話等之終端，則當網路結帳輔助裝置和終端的連接中，發生了某種不良情況時，該不良的原因，究竟是在網路結帳輔助裝置側、還是在終端側，此種責任劃分點會不明確。因此，採用網路非連接型之構成的網路結帳輔助裝置，

對於責任劃分點的明確而言，是有效的。

此處，不持有網路結帳輔助裝置的持卡會員，在本實施例之網路結帳系統中，進行網路商業交易時的事前登錄之系統構成及流程，示於圖 6。

持卡會員，係從會員 PC，向卡片公司(信用卡組織或發卡銀行)所營運之持卡會員專用的 WEB 網站進行存取，並輸入了只有持卡會員知道的會員資訊(出生年月日、電話號碼、帳戶號碼等)，然後發送至 WEB 網站(圖 6 中，(1))。

接收到會員資訊的卡片公司的 WEB 網站，係向有登錄該當會員資訊之卡片公司的基幹系統進行存取，並向基幹系統委託進行所收到之會員資訊、和基幹系統中所登錄之會員資訊的核對(圖 6 中，(2))。基幹系統，係向 WEB 網站回送核對結果(圖 6 中，(3))。

若核對結果爲 OK，則視爲持卡會員之本人確認成功，並從 WEB 網站，向會員 PC，要求密碼之登錄。會員 PC，係將密碼發送給 WEB 網站(圖 6 中，(4))。

從會員 PC 接收到密碼的 WEB 網站，係將該當密碼，登錄至卡片公司之認證伺服器 7(圖 6 中，(5))。

此處所登錄之密碼，係爲固定密碼，並非在網路結帳輔助裝置上所生成的那種一次性密碼。換言之，未持有網路結帳輔助裝置的持卡會員，在網路結帳系統上進行網路結帳的時候，持卡會員的認證方法，係只能藉由固定密碼的方法；一旦卡號和固定密碼被第三者一度獲知，則以後

第三者就能夠假冒持卡會員來進行網路結帳。

又，未持有網路結帳輔助裝置之持卡會員，係爲了登錄密碼，而向持卡會員之 WEB 網站進行存取，經過本人認證後才能進行密碼登錄作業，因此對持卡會員側造成的負擔較大。

甚至，不只是持卡會員的負擔大，即使在卡片公司側，也是需要架設用來讓持卡會員登錄密碼的 WEB 網站，架設用來進行持卡會員之本人認證的基幹系統。

又，網路結帳輔助裝置係構成爲，通常不會外露卡號，而僅爲持卡會員所獲知，或只有在輸入了僅持卡會員具有之認證資訊，才會顯示出卡號；甚至，由於網路結帳之際，持卡會員之本人認證所使用的密碼，係並非固定密碼，而是一次性密碼，因此，第三者要假冒持卡會員來進行網路商業交易是極爲困難的。

以上，雖然說明了網路結帳輔助裝置 1 的實施例，但是，本發明的網路結帳輔助裝置，係並非被限定於具備上記實施例所說明之全部構成要件的網路結帳輔助裝置 1，而是可作各種變更及修正，實現每個目的所必須之構成要件可任意組合，來架構本發明之網路結帳輔助裝置。又，關於所述變更及修正也當然屬於本發明之申請專利範圍中。

例如，在實施例中，雖然說明了使用信用卡的卡號的網路結帳，但只要是至少藉由卡號來進行網路結帳的卡片，除了信用卡以外，像是轉帳卡等之卡片所致之實施例，

也是屬於本發明之申請專利範圍中。

又，本實施例中，雖然是使用卡片結帳之網路商業交易中所使用，但當持卡會員只希望進行網路商業交易，不希望先前之塑膠型磁卡、IC卡等所成之信用卡所致之真實的面對面交易的情況下，亦可不受到信用卡之發行；本發明之網路結帳輔助裝置之擁有者，是不需要一定得持有先前之塑膠型的信用卡。

又，例如，實施例中雖然說明了，1個網路結帳輔助裝置1的卡片資訊儲存部13中，儲存著具有1種卡片資訊之1持卡會員的卡片資訊，並在認證資訊儲存部15中儲存1種認證資訊的情形，但亦可在卡片資訊儲存部13中儲存複數之卡號。此時的認證資訊，係可爲了顯示複數卡號而爲共通的認證資訊，也可爲卡號和認證資訊分別對應，隨著所輸入之認證資訊不同，顯示器11上顯示之卡號也不同。

又，母子信用卡等、同一或複數卡號，是被複數人使用的情況，係亦可隨著每個人而儲存不同之認證資訊在認證資訊儲存部15中，也可儲存共通的認證資訊。

又，上記實施例中，雖然敘述了卡片資訊和OTP生成資訊，是在網路結帳輔助裝置1、1a及認證伺服器7、7a上，分別被建立關連之意旨，但爲了防止卡片資訊之竊聽，而將卡片資訊和OTP生成資訊，非以直接而是以間接方式建立關連者，也是包含於申請專利範圍中。

具體而言，圖3之S10中被會員終端2輸入之卡片資

訊，是於 S20、30 中，經由加盟店終端 3、仲介伺服器 5，最終會被發送至認證伺服器 7、7a，但是，認證伺服器 7、7a 係在此時，將所收到之卡片資訊之中的卡號，轉換成和該當卡號不同的獨特之號碼，並經由仲介伺服器 5，發送至加盟店終端 3(於 S40、50 中)。

甚至，該獨特號碼，係從加盟店終端 3 被送往會員終端 2，經由會員終端 2 而被發送至認證伺服器 7、7a(於 S60、70 中)。

接收到該當獨特號碼的認證伺服器 7、7a，係藉由和最初把卡號轉換成獨特號碼時的相反的轉換規則，將獨特號碼轉換成卡號，將轉換成的卡號所關聯到的 OTP 生成資訊，用於一次性密碼之生成。

如此，藉由將卡號和卡號以外以外之獨特號碼和 OTP 生成資訊建立關連，除了 S10、S20、S30 中卡號被發送以外，在網路 9a 上都不會有卡號流通，因此卡號被竊聽的可能性會大幅降低，對安全性的提升有所貢獻。

又，上記實施例中雖然說明了，會員終端 2 是向加盟店終端 3 發送卡片資訊，認證伺服器 7、7a，是基於來自加盟店終端 3 的請託，而於圖 2 的 S80 中，進行持卡會員之本人認證的情形，但是，本發明並不一定侷限於此。

例如，亦可先由會員終端 2 去存取認證伺服器 7，然後認證伺服器 7、7a 會將持卡會員專用的認證資訊輸入畫面發送給會員終端 2，基於被輸入至該當認證輸入畫面的卡片資訊和一次性密碼，在會員終端 2 和認證伺服器 7、

7a之間進行持卡會員之本人認證；在其結果爲確認是本人以後，在所定條件(例如所定時間、所定次數、所定加盟店等)內，由會員終端 2 去存取加盟店終端 3 的網站，而進行網路商業交易。

換言之，本發明的網路結帳輔助裝置，基本上係設計成在會員終端 2、和卡片公司側的認證伺服器 7、7a 之間，被使用於持卡會員之本人認證，且在認證後，就可實際在加盟店的網站等中進行網路商業交易；並非必然以來自加盟店終端 2 的本人認證委託爲前提。

本發明中的各手段、資料庫，係僅爲邏輯性地區別其機能而劃分，在實體上或事實上係亦可爲同一領域而爲之。又，取代資料庫改用資料檔案當然也可，資料庫之記載中亦包含資料檔案。

上記實施例中，雖然說明了，網路結帳系統上的終端或伺服器，是信用卡組織(商業交易服務之提供主體)、發卡銀行(持卡會員之獲得.對持卡會員發行卡片的主體)、收單銀行(加盟店的獲得.契約.管理主體)、加盟店之各自所營運，但是，這些都僅是概念上、角色上的區別，實體上，會有發卡銀行和收單銀行爲同一者的情形，或也有信用卡組織、發卡銀行、收單銀行爲同一者的情形。

因此，例如，於本說明書中，網路結帳輔助裝置 1、1a，係並非被限定於從發卡銀行所發配。又，網路結帳系統的提供主體也不一定必須是信用卡組織。又，發卡銀行終端 6 和認證伺服器 7、7a 和收單銀行終端 4 也可爲同一

者。又，仲介伺服器 5、其他終端或伺服器之任何者均可以是同一者。

此外，實施本發明時，是將記錄著實現本實施形態之機能的軟體之程式的記憶媒體供給給系統，由該系統的電腦將記憶媒體中所儲存之程式加以讀出並執行，而加以實現。

此時，從記憶媒體中讀出之程式本身係會實現實施形態之機能，記憶該程式的記憶媒體則則構成本發明。

作爲用來供給程式的記憶媒體，例如可使用磁碟、硬碟、光碟、光磁碟、磁帶、不揮發性記憶卡等。

又，不僅是藉由電腦執行已讀出之程式，來實現上述實施形態之機能，而是基於該程式之指示，由電腦上運作中的作業系統等進行實際之處理的部份或全部，藉由該處理來實現前記實施形態之機能的情況，也被涵蓋在本發明中。

甚至，被從記憶媒體中讀出之程式，是被寫入至被插入在電腦的機能擴充板或連接至電腦的機能擴充單元上所具備的不揮發性或揮發性之記憶手段後，基於該程式之指示，由機能擴充板或機能擴充單元所具備的演算處理裝置等來進行實際之處理的部份或全部，藉由該處理來實現前記實施形態之機能的情況，也被涵蓋在本發明中。

【圖式簡單說明】

〔圖 1〕本發明之網路結帳輔助裝置之外觀及電氣硬

體構成的構成圖。

〔圖 2〕使用網路結帳輔助裝置的網路結帳系統的概略連接構成圖。

〔圖 3〕網路結帳系統中的網路商業交易之處理流程之一例的圖。

〔圖 4〕網路結帳系統中的網路商業交易之處理流程中，顯示於會員終端之畫面之一例的圖。

〔圖 5〕本發明之網路結帳輔助裝置之操作程序及顯示器畫面遷移的圖示。

〔圖 6〕未網路結帳輔助裝置之網路結帳系統，被持卡會員利用之際，持卡會員之本人認證所需之密碼登錄用所必要之系統概略連接構成圖。

【主要元件符號說明】

1：網路結帳輔助裝置

10：框體

11：顯示器

12：按鍵操作部

12a：數字鍵

12b：開始鍵

13：卡片資訊儲存部

14：認證手段

15：認證資訊儲存部

16：OTP 生成手段

(53)

17：OTP 生成資訊儲存部

18：計時手段

19：驅動用電源

2：會員終端

3：加盟店終端

4：收單銀行終端

5：仲介伺服器

6：發卡銀行終端

7：認證伺服器

9a：網路

9b：專線

五、中文發明摘要

發明之名稱：網路結帳輔助裝置

〔課題〕使卡號或私密號碼被竊聽、篡改的危險性消失，提供可更安全地進行網路商業交易的網路結帳輔助裝置。

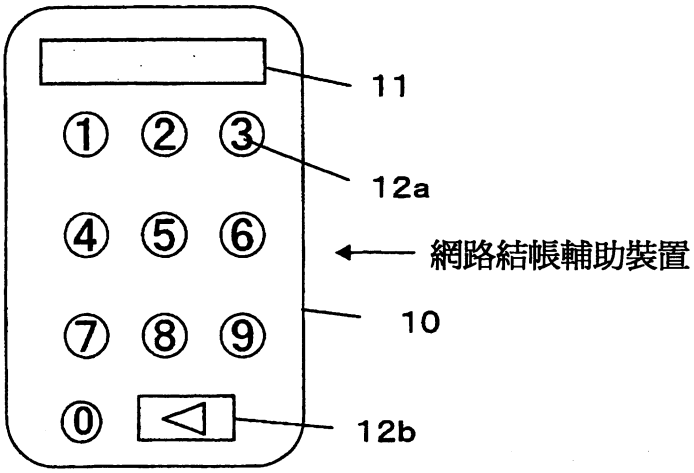
〔解決手段〕具備：顯示器 11；和至少包含卡片契約者之卡片資訊，是以無法從外部讀出之狀態而預先儲存的卡片資訊儲存部 13；和契約者之認證資訊是以無法從外部讀出之狀態而預先儲存的認證資訊儲存部 15；和 OTP(One Time Password)生成資訊是以無法從外部讀出之狀態而預先儲存的 OTP 生成資訊儲存部 17；和數字鍵 12a；和基於來自數字鍵 12a 之輸入資訊，將進行操作者本人認證的卡片資訊顯示於顯示器 11 上的認證手段 14；和在卡片資訊被顯示後，基於 OTP 生成資訊來生成一次性密碼，並顯示於顯示器 11 的 OTP 生成手段 16；藉由一次性密碼來進行契約者之本人認證，使得網路商業交易成爲可進行。

六、英文發明摘要

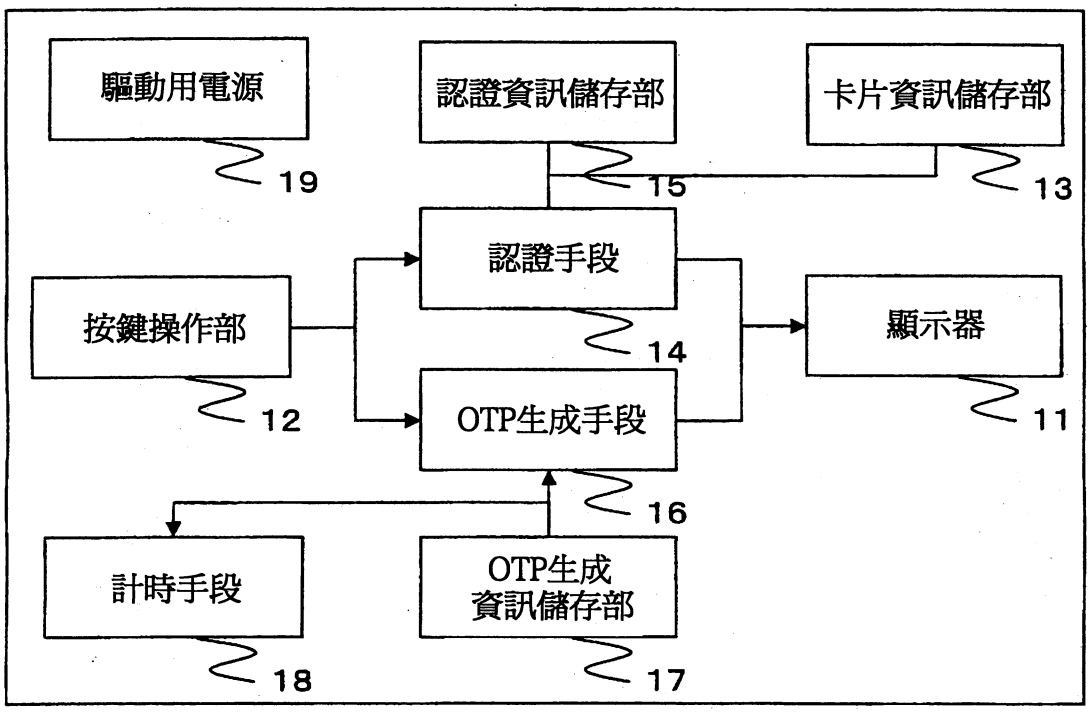
發明之名稱：

圖1

(a)



(b)



↑ 網路結帳輔助裝置1

圖2

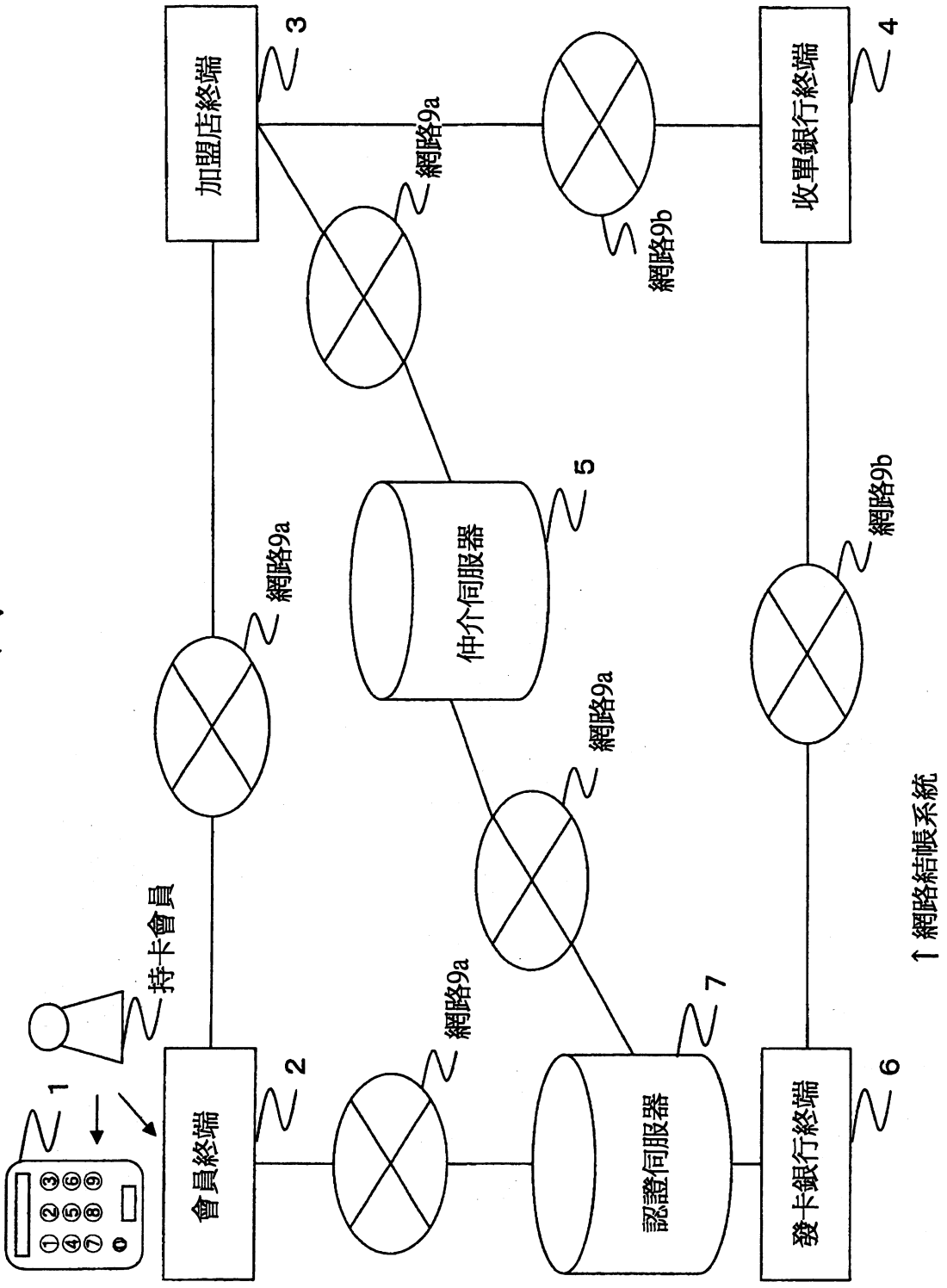

加盟店終端
3
網路9a
網路9b
收單銀行終端
4
伸介伺服器
5
網路9a
網路9b
持卡會員
1
會員終端
2
網路9a
認證伺服器
7
發卡銀行終端
6
↑網路結帳系統

圖3

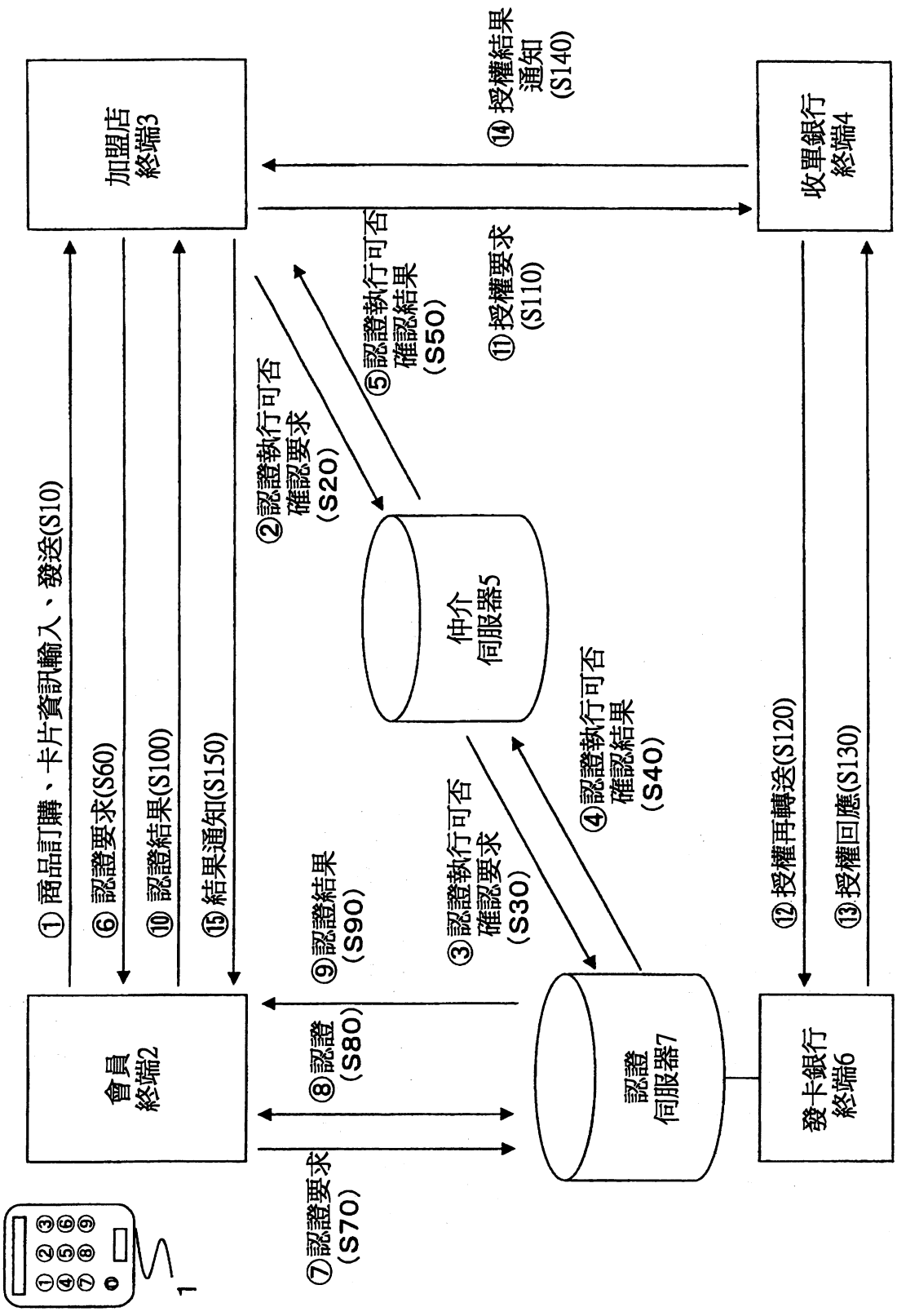
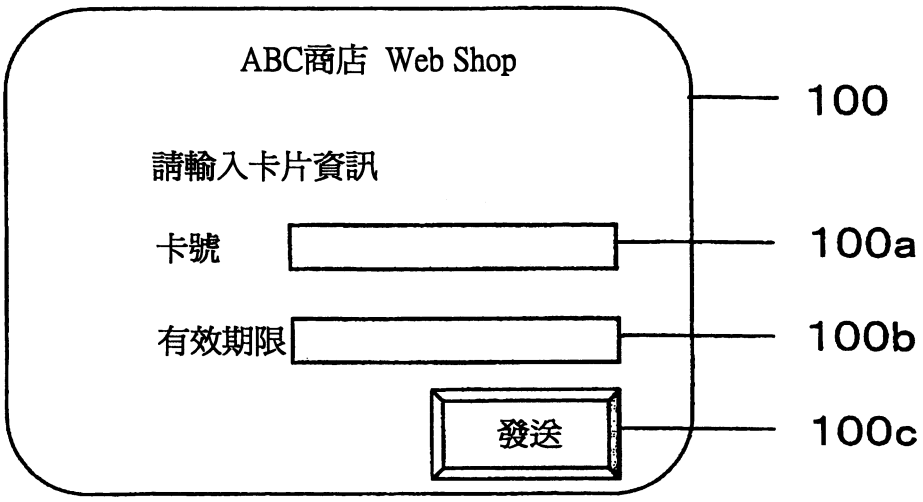

加盟店
終端3
收單銀行
終端4
會員
終端2
仲介
伺服器5
認證
伺服器7
發卡銀行
終端6
1
①商品訂購、卡片資訊輸入、發送(S10)
②認證執行可否
確認要求
(S20)
③認證執行可否
確認要求
(S30)
④認證執行可否
確認結果
(S40)
⑤認證執行可否
確認結果
(S50)
⑥認證要求(S60)
⑦認證要求
(S70)
⑧認證
(S80)
⑨認證結果
(S90)
⑩認證結果(S100)
⑪授權要求
(S110)
⑫授權再轉送(S120)
⑬授權回應(S130)
⑭授權結果
通知
(S140)
⑮結果通知(S150)

圖4

(a)


ABC商店 Web Shop
100
請輸入卡片資訊
卡號
100a
有效期限
100b
發送
100c

(b)

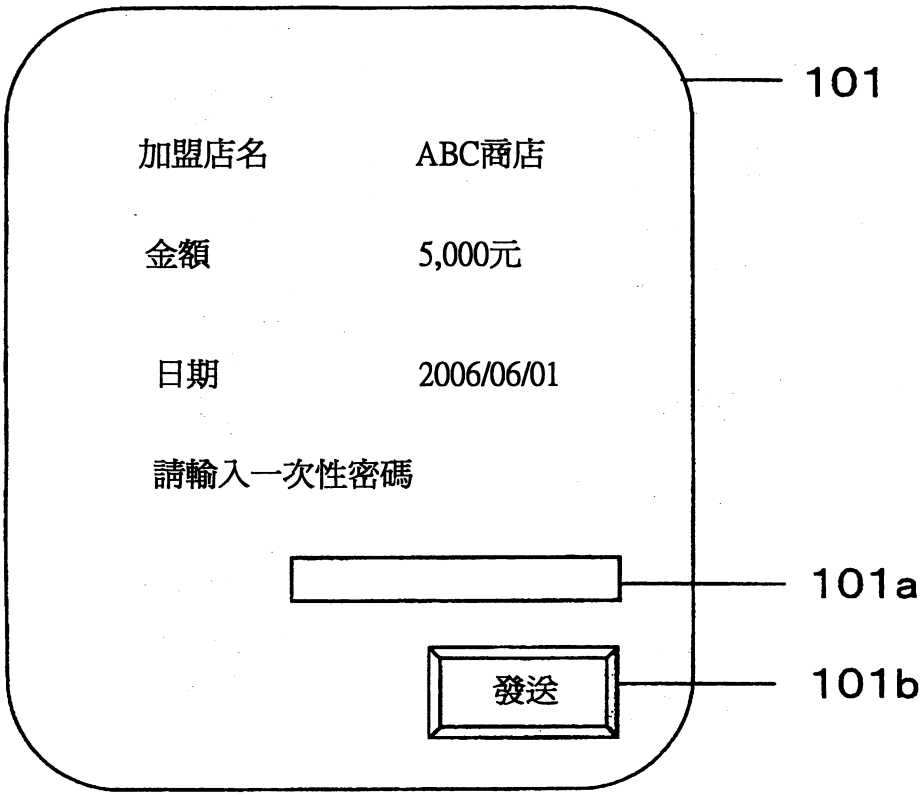

101
加盟店名
ABC商店
金額
5,000元
日期
2006/06/01
請輸入一次性密碼
101a
發送
101b

圖5

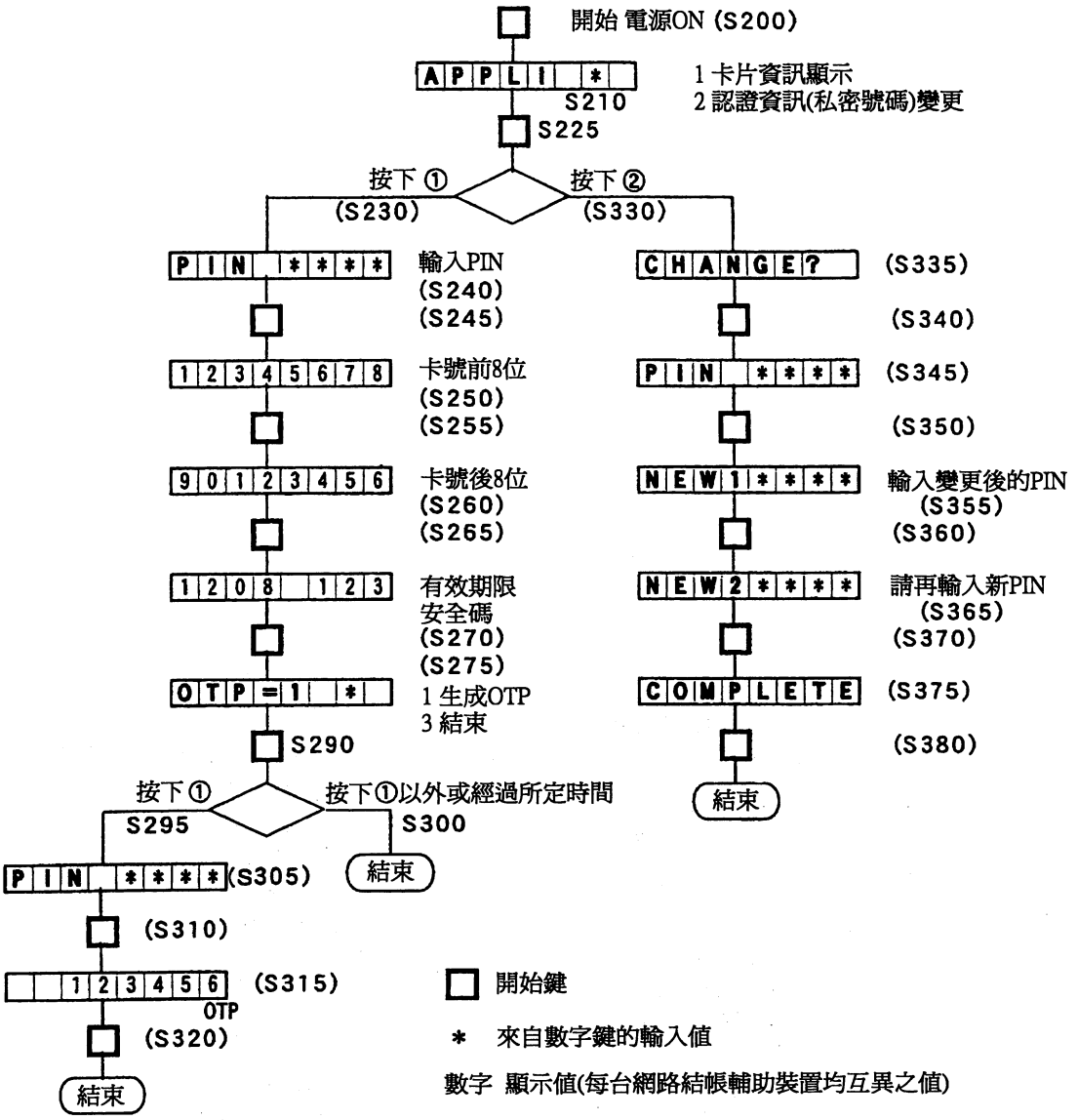
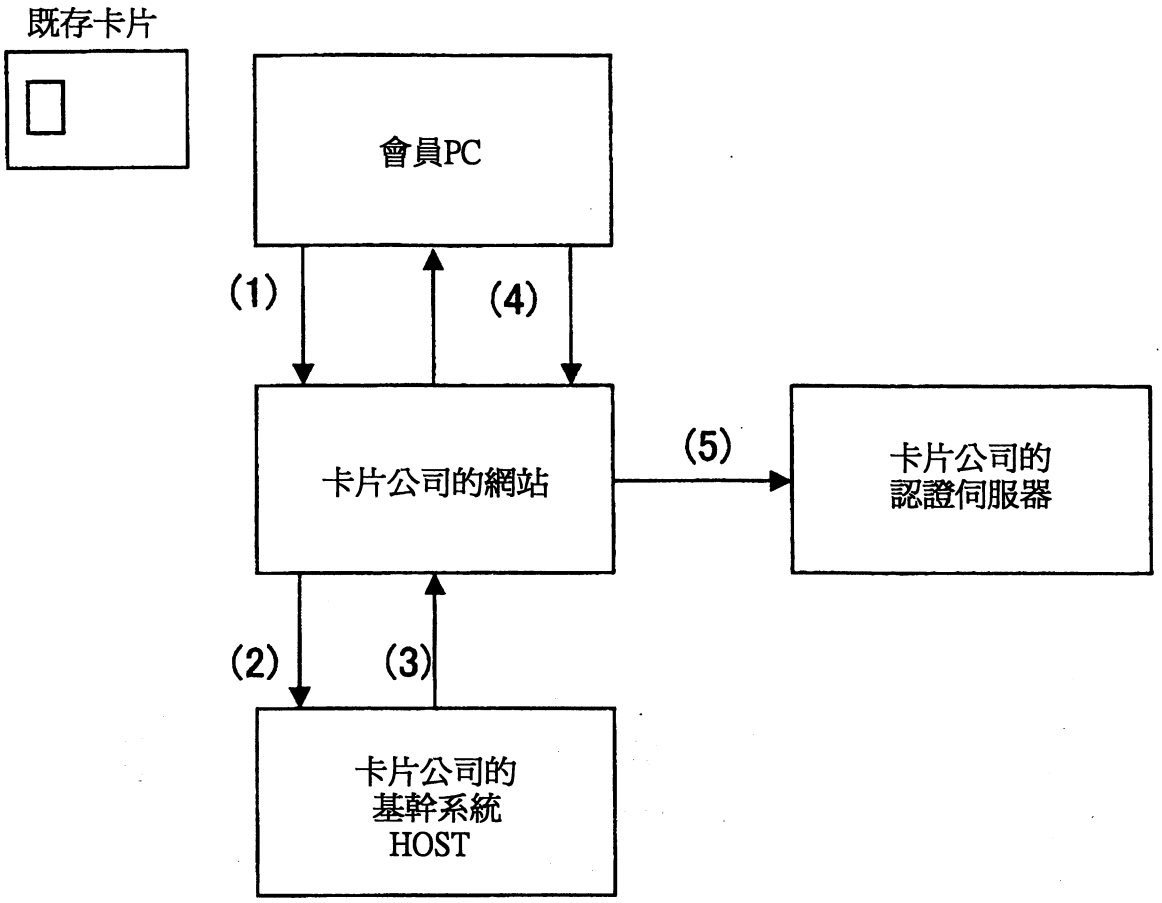

開始 電源ON (S200)
APPLI *
S210
1 卡片資訊顯示
2 認證資訊(私密號碼)變更
S225
按下 ①
(S230)
按下 ②
(S330)
PIN ****
輸入PIN
(S240)
(S245)
12345678
卡號前8位
(S250)
(S255)
90123456
卡號後8位
(S260)
(S265)
1208 123
有效期限
安全碼
(S270)
(S275)
OTP=1 *
1 生成OTP
3 結束
S290
按下 ①
S295
按下①以外或經過所定時間
S300
結束
PIN ****
(S305)
(S310)
123456
OTP
(S315)
(S320)
結束
CHANGE?
(S335)
(S340)
PIN ****
(S345)
(S350)
NEW1****
輸入變更後的PIN
(S355)
(S360)
NEW2****
請再輸入新PIN
(S365)
(S370)
COMPLETE
(S375)
(S380)
結束
開始鍵
* 來自數字鍵的輸入值
數字 顯示值(每台網路結帳輔助裝置均互異之值)
粗字 引導(每台網路結帳輔助裝置均共通之字樣)

圖6



七、指定代表圖

（一）、本案指定代表圖為:第（1）圖

（二）、本代表圖之元件代表符號簡單說明：

1：網路結帳輔助裝置
10：框體
11：顯示器
12：按鍵操作部
12a：數字鍵
12b：開始鍵
13：卡片資訊儲存部
14：認證手段
15：認證資訊儲存部
16：OTP 生成手段
17：OTP 生成資訊儲存部
18：計時手段
19：驅動用電源

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(1)

97年8月5日修(更)正替換頁

十、申請專利範圍

第95134475號專利申請案

中文申請專利範圍修正本

民國97年8月5日修正

1.一種網路結帳輔助裝置，係屬於可搬型之網路結帳輔助裝置，其特徵爲，

具備：

顯示器；和

卡片資訊儲存部，是以無法從外部讀出之狀態預先儲存著，至少包含信用卡或轉帳卡等之卡片契約者之識別資訊的卡片資訊；和

認證資訊儲存部，是以無法從外部讀出之狀態預先儲存著，用來進行前記契約者之本人認證的認證資訊；和

OTP生成資訊儲存部，是以無法從外部讀出之狀態預先儲存著，被前記卡片資訊所關連對應且爲前記網路結帳輔助裝置所固有之OTP(One Time Password，一次性密碼)生成資訊；和

輸入手段，將前記認證資訊加以輸入；和

認證手段，基於從前記輸入手段所輸入之輸入資訊，由前記網路結帳輔助裝置之操作者，進行是否爲前記契約者的本人認證，若已經確認爲本人時，則至少讀出前記卡片資訊當中的前記識別資訊，並顯示於前記顯示器上；和

一次性密碼生成手段，在前記卡片資訊被顯示後，基於前記OTP生成資訊，生成一次性密碼，並顯示於前記顯

示器上；

當藉由前記一次性密碼，進行了前記契約者之本人認證，且已確認爲本人時，使得使用前記識別資訊之結帳所致之網路商業交易成爲可行。

2.一種網路結帳輔助裝置，係屬於，信用卡或轉帳卡等之卡片契約者的行動電話或個人電腦等的契約者終端，和進行前記契約者本人認證的認證伺服器，是彼此連接網路而成之網路結帳系統中，在進行使用了前記契約者之識別資訊的結帳所致之網路商業交易之際，所被使用的可搬型之網路結帳輔助裝置，其特徵爲，

前記網路結帳輔助裝置係

具備：

顯示器；和

卡片資訊儲存部，是以無法從外部讀出之狀態預先儲存著，至少包含前記契約者之識別資訊的卡片資訊；和

認證資訊儲存部，是以無法從外部讀出之狀態預先儲存著，用來進行前記契約者之本人認證的認證資訊；和

OTP生成資訊儲存部，是以無法從外部讀出之狀態預先儲存著，被前記卡片資訊所關連對應且爲前記網路結帳輔助裝置所固有之OTP生成資訊；和

輸入手段，將前記認證資訊加以輸入；和

認證手段，基於從前記輸入手段所輸入之輸入資訊，由前記網路結帳輔助裝置之操作者，進行是否爲前記契約者的本人認證，若已經確認爲本人時，則至少讀出前記卡

片資訊當中的前記識別資訊，並顯示於前記顯示器上；和

一次性密碼生成手段，在前記卡片資訊被顯示後，基於前記 OTP 生成資訊，生成一次性密碼，並顯示於前記顯示器上；

前記契約者終端，是藉由將前記一次性密碼發送至前記認證伺服器，來進行前記契約者的本人認證，當已確認爲本人時，則使前記網路商業交易成爲可行。

3.如申請專利範圍第 1 項或第 2 項所記載之網路結帳輔助裝置，其中，

前記認證資訊，係爲前記契約者所預先訂定的私密號碼；

前記輸入手段，係爲數字鍵。

4.如申請專利範圍第 1 項或第 2 項所記載之網路結帳輔助裝置，其中，

前記認證資訊，係爲將前記契約者的指紋、虹膜、聲帶、臉部照片等之生物性特徵加以數值化而成的生物資訊。

5.如申請專利範圍第 1 項或第 2 項所記載之網路結帳輔助裝置，其中，

前記 OTP 生成資訊，

係爲共通金鑰；

前記一次性密碼生成手段，係

偵測所定操作鍵之壓下，而將前記操作鍵被壓下之日期所成之日期資料，以前記共通金鑰予以加密然後生成一

次性密碼。

6.如申請專利範圍第 1 項或第 2 項所記載之網路結帳輔助裝置，其中，

前記 OTP 生成資訊，

係由共通金鑰，和前記一次性密碼每次被生成時就被更新的利用次數資訊所構成；

前記一次性密碼生成手段，係

偵測所定操作鍵之壓下，而將前記利用次數資訊以共通金鑰予以加密而生成一次性密碼；

在前記一次性密碼被生成後，將前記 OTP 生成資訊儲存部內的利用次數資訊加以更新。

7.如申請專利範圍第 1 項或第 2 項所記載之網路結帳輔助裝置，其中，

前記網路結帳輔助裝置，係具備抗外力入侵性(Tamper Proofness)。